



Instituto Federal da Bahia
Campus Salvador

Programa de Pós-Graduação em Engenharia de Sistemas de Produtos

**SISTEMA BLOCKCHAIN PARA
GERENCIAMENTO DE SOLICITAÇÃO DE
MEDICAMENTOS POR VIA JUDICIAL**

Mário Augusto Santos do Amor Divino

DISSERTAÇÃO DE MESTRADO

Salvador
2023

MÁRIO AUGUSTO SANTOS DO AMOR DIVINO

**SISTEMA BLOCKCHAIN PARA GERENCIAMENTO DE
SOLICITAÇÃO DE MEDICAMENTOS POR VIA JUDICIAL**

Esta Dissertação de Mestrado foi apresentada ao Programa de Pós-Graduação em Engenharia de Sistemas de Produtos da Instituto Federal da Bahia, como requisito parcial para obtenção do grau de Mestre em Engenharia de Sistemas e Produtos.

Orientador: Dr. Allan Edgard Silva Freitas

Salvador
2023

FICHA CATALOGRÁFICA ELABORADA PELO SISTEMA DE BIBLIOTECAS DO IFBA, COM OS
DADOS FORNECIDOS PELO(A) AUTOR(A)

A524s Amor Divino, Mário Augusto Santos do

Sistema blockchain para gerenciamento de solicitação de medicamentos por via judicial / Mário Augusto Santos do Amor Divino; orientador Allan Edgard Silva Freitas -- Salvador, 2023.

81 p.

Dissertação (Programa de Pós-Graduação em Engenharia de Sistemas de Produtos) -- Instituto Federal da Bahia, 2023.

1. Rastreabilidade de medicamento. 2. Medicamento por via judicial. 3. Blockchain privada e permissionada. 4. Auditoria em blockchain. I. Freitas, Allan Edgard Silva, orient. II. TÍTULO.

CDU 615:658



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA BAHIA
R. Emídio dos Santos - Bairro Barbalho - CEP 40301-015 - Salvador - BA - www.portal.ifba.edu.br

INSTITUTO FEDERAL DA BAHIA
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO

**PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE SISTEMAS E PRODUTOS -
PPGESP**

**SISTEMA BLOCKCHAIN PARA GERENCIAMENTO DE SOLICITAÇÃO DE
MEDICAMENTOS POR VIA JUDICIAL**

MÁRIO AUGUSTO SANTOS DO AMOR DIVINO

Produto(s) Gerado(s): Dissertação

Orientador: Prof. Dr. Allan Edgard Silva Freitas

Banca examinadora:

Prof. Dr. Allan Edgard Silva Freitas

Orientador – Instituto Federal da Bahia (IFBA)

Prof. Dr. Renato Lima Novais

Membro Interno – Instituto Federal da Bahia (IFBA)

Prof. Dr. Josielson Costa da Silva

Membro Externo – Universidade Federal da Bahia (UFBA)

Trabalho de Conclusão de Curso aprovado pela banca examinadora em 16/08/2023

Em 09 de agosto de 2023.



Documento assinado eletronicamente por **ALLAN EDGARD SILVA FREITAS, Professor Titular**, em 16/08/2023, às 16:34, conforme decreto nº 8.539/2015.



Documento assinado eletronicamente por **Josielson Costa da Silva, Usuário Externo**, em 16/08/2023, às 17:43, conforme decreto nº 8.539/2015.



Documento assinado eletronicamente por **RENATO LIMA NOVAIS, Docente Permanente**, em 17/08/2023, às 16:40, conforme decreto nº 8.539/2015.



A autenticidade do documento pode ser conferida no site http://sei.ifba.edu.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3054723** e o código CRC **EC1D3CCA**.

AGRADECIMENTOS

Agradeço a Deus pela oportunidade de expandir e compartilhar saberes. A meus pais por acreditarem, incentivarem e investirem na minha formação moral e intelectual. Ao Professor Orientador Doutor Allan Edgard Silva Freitas por todo apoio, inspiração e encaminhamentos. A todo corpo docente e administrativo do Instituto Federal de Educação, Ciência e Tecnologia da Bahia e ao Programa de Pós-Graduação em Engenharia de Sistemas e Produtos. A Secretaria de Saúde do Município de Salvador, coordenação e colegas de trabalho que possibilitaram o meu trabalho com vistas a ganhos a área da saúde pública e ao cidadão paciente. Aos amigos, familiares e confrades espíritas pelo apoio e suporte em tempos tão desafiadores a todos.

"Por mais se te fale de calamidades e crises, não permitas que o desânimo te alugue o coração para os comícios da rebeldia."

—EMMANUEL

RESUMO

A demanda de medicamentos por via judicial sobrecarrega o Sistema Único de Saúde (SUS) brasileiro, podendo ocorrer pedidos em duplicidade devido a diferentes possibilidades do fluxo de atendimento. O paciente que necessita de medicamento e não encontra na rede pública de assistência, pode adquiri-lo através da abertura de processo judicial na Defensoria Pública. Após a petição, o processo é encaminhado a uma das secretarias de saúde onde o fármaco é comprado e fornecido ao cidadão. Para realizar o atendimento, as organizações atuam em conjunto. A partir da pesquisa exploratória realizada na Secretaria Municipal de Saúde de Salvador junto a gestão farmacêutica, foi constatada que não existe integração entre os sistemas de informação do órgão judicial e das secretarias de saúde. Essa falta de comunicação ocasiona alguns problemas na execução do serviço, tal como solicitações duplicadas e consequente perda de receita, pois o paciente pode solicitar em mais de uma secretaria e obter o fármaco. A frágil auditoria é outro problema neste contexto, porquanto cada organização mantém um sistema próprio e banco de dados com arquitetura centralizada, onde as informações podem ser apagadas ou alteradas com relativa facilidade. O uso de *blockchain* pode permitir melhor rastreabilidade, tornando a gestão das petições descentralizada, segura, resiliente e auditável, propiciando a economicidade e transparência necessárias ao processo. O objetivo deste trabalho é desenvolver o sistema *blockchain* JudMed que atua por meio de contrato inteligente que gerenciará *tokens* associados aos pleitos judiciais em tela. É um sistema unificado para integrar as organizações de forma segura, resiliente, descentralizada, fortemente auditável e capaz de garantir que cada ente público execute apenas as operações inerentes ao seu fluxo de trabalho. Como consequência da integração, o pleito judicial ganha rastreabilidade e os dados obtidos fornecem métricas para aprimorar o serviço e o atendimento ao cidadão, que chega a ultrapassar 900 dias de espera para obter seu remédio. O produto final desta proposta está composto pela rede entre as organizações, API web para interface das operações, sistema web para a execução das funções e um contrato inteligente que funciona como o contrato digital para garantir a correta execução das regras do negócio que regem o serviço. Uma prova de conceito foi realizada em ambiente simulado e validada com gestores e especialistas da Secretaria de Saúde de Salvador, e a percepção desta prova indica que o uso do JudMed poderá prover melhor controle da movimentação e gerência da requisição de medicamentos com ganhos significativos ao processo.

Palavras-chave: Rastreabilidade de Medicamento, Medicamento por Via Judicial, Blockchain Privada e Permissionada, Auditoria em Blockchain

ABSTRACT

Judicial demand for medication overloads the Brazilian Unified Health System (SUS), and duplicate requests may occur due to different possibilities in the flow of care. The patient of the Unified Health System (SUS) who needs medication and cannot find it in the public assistance network, can acquire it through the opening of a judicial process at the Public Defender's Office. After the petition, the process is forwarded to one of the health departments where the drug is purchased and provided to the citizen. To provide the service, the organizations work together. According to exploratory research carried out at the Municipal Health Department of Salvador with pharmaceutical management, there is no integration between the information systems of the judicial body and the health departments. This lack of communication causes some problems in the execution of the service, such as duplicate requests and consequent loss of revenue, as the patient can request from more than one office and obtain the drug. The fragile audit is another problem in this context, as each organization maintains its own system and database with a centralized architecture, where information can be deleted or changed with relative ease. The use of blockchain can allow better traceability, making the management of petitions decentralized, secure, resilient and auditable, providing the economy and transparency necessary for the process. The objective of this work is to present the JudMed blockchain system that works through a smart contract that will manage tokens associated with the lawsuits on screen. It is a unified system to integrate organizations in a safe, resilient, decentralized, highly auditable way and capable of guaranteeing that each public entity performs only the operations inherent to its work process. As a result of the integration, the lawsuit gains traceability and the data obtained provide metrics to improve the service and the service to the citizen who waits for more than 900 days to obtain their remedy. The final product of this proposal is composed of the network between organizations, web API for the operations interface, web system for the execution of functions and a smart contract that works like the digital contract to guarantee the correct execution of the business rules that govern the service. . A proof of concept was carried out in a simulated environment and validated with managers and specialists from the Salvador Health Department, and the perception of this proof indicates that the use of JudMed can provide better control of the movement and management of the medication request with significant gains to the process of the Health Unic System.

Keywords: Drug Traceability, Medicine through the Courts, Private and Permitted Blockchain, Blockchain Audit.

SUMÁRIO

Capítulo 1—Introdução	16
1.1 Solicitação de Medicamentos no SUS	16
1.2 Pesquisa Exploratória e Problemas Identificados	17
1.3 Blockchain como Solução a Rastreabilidade	17
1.4 Motivações	18
1.4.1 Economicidade ao Estado	18
1.4.2 Melhoria no Tempo de Atendimento para o Paciente do Sistema Único de Saúde (SUS)	18
1.5 Objetivos	18
1.5.1 Objetivos Gerais	18
1.5.2 Objetivos Específicos	19
1.6 Outros Resultados e Atividades	19
Capítulo 2—Revisão Bibliográfica	20
2.1 Medicamentos Judicializados no Brasil	20
2.1.1 Direito à Saúde	20
2.1.2 Fatores que Contribuem para o Aumento de Solicitações Judiciais Relacionadas a Medicamentos	21
2.1.3 Impactos Financeiros	21
2.1.4 Tempo de Atendimento	21
2.2 Princípios de Blockchains	22
2.2.1 Segurança e Privacidade	24
2.2.1.1 Resistência a Adulteração:	24
2.2.1.2 Resistência a Ataque <i>Distributed Denial of Service</i> (DDOS):	25
2.2.1.3 Resistência a Ataque de Duplo Gasto:	25
2.2.1.4 Resistência a Ataque de Consenso 51%:	25
2.2.2 Rastreabilidade	26
2.3 Hyperledger	26
2.4 Hyperledger Fabric	27
2.4.1 Membership Service Provider (MSP)	27
2.4.2 Canais	27
2.4.3 Consenso e Ordenação	28
2.4.4 <i>Ledger</i>	29
2.4.5 Estado Global	29
2.4.6 Blockchain	29

2.4.7	<i>Chaincode e Transações</i>	32
2.5	Framework Minifabric	32
Capítulo 3—Análise de Trabalhos Correlatos		34
3.1	Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud	34
3.2	Blockchains everywhere—a use-case of blockchains in the pharma supply-chain	34
3.3	Drugledger: A practical blockchain system for drug traceability and regulation	35
3.4	Governance on the drug supply chain via goin blockchain	35
3.5	A new era of food transparency powered by blockchain	36
3.6	Comparativo com a Solução Proposta	36
Capítulo 4—Blockchain JudMed		38
4.1	O modelo de Negócio e a utilização de Blockchain	38
4.2	Metodologia	39
4.3	Fluxo do Processo Judicial na Rede	40
4.4	Consenso e Ordenação com Raft	40
4.5	Canal, <i>Ledger</i> e Transações	42
4.6	Acesso Seguro	42
4.7	Arquitetura	43
4.8	Operações, Códigos e Comandos na Rede em Ambiente Simulado	43
4.8.1	Inicialização dos Nós da Rede com o Minifabric	43
4.8.2	Inicialização da API Rest e da Aplicação Web	45
4.8.3	Codificação Para Criar um Processo Judicial	47
4.8.4	Aplicação Web JudMed	47
4.9	Testes de Funcionalidade	49
4.9.1	Ambiente	49
4.9.2	Teste 1: Tentativa de Criação de Processo sem ser o Ministério Público	50
4.9.3	Teste 2: Tentativa de Criação de Processo Duplicado	50
4.9.4	Teste 3: Movimentação de Processo entre as organizações	51
4.9.5	Teste 4: Acompanhamento pelo Paciente do SUS	52
4.9.6	Teste 5: Auditoria de um Processo Judicial	52
4.9.7	Teste 6: <i>Dashboard</i> Gerencial	54
4.10	Resultados da Implementação	54
4.11	Implantação da Blockchain JudMed	55
Capítulo 5—Prova de Conceito		57
5.1	Realização dos Processos na Prova de Conceito	58
5.2	Avaliações e Percepções Finais na Prova de Conceito	59

Capítulo 6—Conclusão	63
Apêndice A—Gerenciamento do Projeto	67
A.1 Questionário Aplicado	67
A.2 Estória Global do Usuário	67
A.3 Cronograma de Desenvolvimento	70
A.4 Pacote de Atividades	71
Apêndice B—Comandos Framework Minifabric	72
Apêndice C—Smart Contract	75
C.1 Inicializa o Ledger	75
C.2 Cria o Ativo	75
C.3 Verifica se o Ativo existe pelo id	76
C.4 Pesquisa o Ativo pelo Número do Processo	76
C.5 Movimenta o Ativo	77
C.6 Audita o Ativo	77
Apêndice D—Endpoints	79
Apêndice E—Outros Resultados e Atividades	80

LISTA DE FIGURAS

2.1	Blocos de transação encadeados numa Blockchain (ZHENG et al., 2017) .	24
2.2	Arquitetura Hyperledger (GREVE et al., 2018)	28
2.3	Estado Global em Hyperledger Fabric - Fonte: (GROUP et al., 2017) . .	30
2.4	Blockchain Hyperledger Fabric - Fonte: (GROUP et al., 2017)	31
2.5	Blocos Hyperledger Fabric - Fonte: (GROUP et al., 2017)	31
2.6	Transações Hyperledger Fabric - Fonte: (GROUP et al., 2017)	33
4.1	Questionamentos para sistemas Candidatos a aplicação de Blockchain (Elaboração Própria, 2023)	39
4.2	Big Picture com o resultado da aplicação da solução (Elaboração Própria, 2021)	41
4.3	Diagrama de Sequência - Solicitação de Medicamento Judicial (Elaboração própria, 2021)	44
4.4	Arquivo Spec.yaml para a Secretario Municipal de Saúde e Ministério Público (Elaboração Própria, 2021)	45
4.5	Arquivo Spec.yaml para a Secretaria Estadual de Saúde (Elaboração Própria, 2021)	46
4.6	Rede Implantada nas Máquinas e Aplicações (Elaboração Própria, 2021)	47
4.7	Cadastro do Processo Judicial - <i>Chaincode</i> (Elaboração Própria, 2021) .	48
4.8	Cadastro do Processo Judicial - POST/API (Elaboração Própria, 2021) .	48
4.9	Apresentação Aplicação JudMed (Elaboração Própria, 2021)	49
4.10	Tela de erro de cadastro de processo não sendo usuário do Ministério Público (Elaboração Própria, 2021)	50
4.11	Tela de erro de cadastro processo duplicado (Elaboração própria, 2021) .	51
4.12	Tela de cadastro de processo com sucesso - (Elaboração Própria, 2021) .	51
4.13	Tela de Movimentação de processo - (Elaboração Própria, 2021)	52
4.14	Tela de acompanhamento para o paciente dos SUS - (Elaboração Própria, 2021)	53
4.15	Tela de Auditoria (Elaboração Própria, 2021)	53
4.16	Tela de Dashboard (Elaboração Própria, 2021)	54
4.17	Diagrama de Implantação (Elaboração Própria, 2021)	56
5.1	Fluxo do Processo de Cadastro do Ativo Na Prova de Conceito (Elaboração Própria, 2023)	60
5.2	Fluxo do Processo de Movimentação do Ativo Na Prova de Conceito (Elaboração Própria, 2023)	60

LISTA DE FIGURAS

5.3	Fluxo do Processo de Acompanhamento do Ativo Na Prova de Conceito (Elaboração Própria, 2023)	61
5.4	Fluxo do Processo de Auditoria do Ativo Na Prova de Conceito (Elaboração Própria, 2023)	61
5.5	Fluxo do Processo de Visualização de dashboard Na Prova de Conceito (Elaboração Própria, 2023)	62
A.1	Cronograma de Desenvolvimento (Elaboração Própria, 2021)	70
A.2	Pacote de Atividades (Elaboração Própria, 2021)	71
B.1	spec.yaml Minifabric (Elaboração Própria, 2022)	73
B.2	Resultado do comando Minifabric Stats (Elaboração Própria, 2022) . . .	74

LISTA DE TABELAS

2.1	Números da demanda judicial referente à judicialização da saúde em 2019 (BATISTA et al., 2020)	22
2.2	Identificação dos processos por tempo de tramitação, desfecho dos processos arquivados e motivo do julgamento improcedente. Londrina/PR, 2011 a 2017 (BATISTA et al., 2020)	22
3.1	Tabela comparativa com trabalhos correlacionados (Elaboração Própria, 2021)	37
A.1	Estórias do Usuário (BATISTA et al., 2020)	69
D.1	Endpoints	79
E.1	Outros resultados e atividades	<u>80</u>

LISTA DE SIGLAS

SUS	Sistema Único de Saúde	16
FDA	<i>Food and Drug Administration</i>	17
ANVISA	Agência Nacional de Vigilância Sanitária	18
RDC	Regime Diferenciado de Contratação	17
SNCM	Sistema Nacional de Controle de Medicamentos	17
DLT	<i>Distributed Ledger Technology</i>	23
P2P	<i>Peer to Peer</i>	23
SC	<i>Smart Contract</i>	23
ECDSA	<i>Elliptic Curve Digital Signature Algorithm</i>	24
DDOS	<i>Distributed Denial of Service</i>	25
RFID	<i>Radio Frequency Identification</i>	26
PoET	<i>Proof of Elapsed Time</i>	25
PoW	<i>Proof of Work</i>	25
PBFT	<i>Practical Byzantine Fault Tolerance</i>	25
CFT	<i>Crash Fault Tolerant</i>	25
BFT	<i>Byzantine Fault Tolerant</i>	25
RENAME	Relação Nacional de Medicamentos Essenciais	21

Capítulo 1

Neste capítulo são apresentados o contexto do problema, motivações, objetivos e a prospecção da solução utilizando a tecnologia blockchain.

INTRODUÇÃO

1.1 SOLICITAÇÃO DE MEDICAMENTOS NO SUS

O direito à saúde está garantido pela Constituição Federal do Brasil (BRASIL, 1988) logo, o estado deve assegurar toda assistência aos cidadãos por meio de consultas médicas, exames diagnósticos e oferta de fármacos (MACEDO; LOPES; BARBERATO-FILHO, 2011). Para viabilizar os atendimentos, são realizados investimentos federais no Sistema Único de Saúde (SUS). De acordo com dados do Fundo Nacional de Saúde, foram disponibilizados em 2022 aproximadamente R\$ 10 bilhões para a assistência farmacêutica (FNS, 2023).

No trabalho de (MACEDO; LOPES; BARBERATO-FILHO, 2011), é informado que após consulta médica, seja na rede pública ou privada, uma receita é emitida e o paciente pode buscar o apoio farmacológico nas unidades de saúde municipais ou estaduais, obtendo o fármaco de imediato caso esteja disponível. O elenco de medicamentos para atendimento no SUS passa por constantes ajustes, surgindo novos e específicos produtos ou ocorrendo substituições. O problema é que com essa dinâmica, alguns remédios não são encontrados na rede, todavia podem ser insubstituíveis para a eficácia dos tratamentos. Essa demanda não atendida vai de encontro a um direito constitucional e requer tratativa especial pelos órgãos.

Para atender ao cidadão que não encontra o fármaco na rede pública, o Ministério Público ou Defensoria Pública e as secretarias de saúde atuam de forma complementar. De acordo com (DAO, 2021), a partir da constatação da ausência, o cidadão pode entrar com ação individual por meio da Defensoria Pública, que inclusive atua na defesa coletiva, ajuizando ação civil pública. O Ministério Público também pode instaurar inquérito civil e ajuizar ação civil pública com um pedido liminar. Além disso, é visto em (MACEDO; LOPES; BARBERATO-FILHO, 2011), que outras entidades, como a Ordem dos Advogados do Brasil e as associações de defesa dos direitos dos pacientes, podem receber as reclamações por meio de suas comissões temáticas, e realizar orientações e encaminhamentos específicos. Com o pleito judicial instaurado, o paciente ou um oficial de justiça

solicita o fármaco a uma das secretarias de saúde e esta se responsabiliza pela logística da compra à entrega do medicamento.

1.2 PESQUISA EXPLORATÓRIA E PROBLEMAS IDENTIFICADOS

Conforme pesquisa exploratória realizada por entrevistas com o gestor farmacêutico do município de Salvador, foi relatada a ausência de integração entre os sistemas de informação das entidades envolvidas, no que se refere a solicitações judiciais de medicamentos. Com a falta da integração podem ocorrer pedidos atendidos por mais de uma secretaria de saúde, gerando um duplo investimento para atender o mesmo processo. Quando necessário, as movimentações do processo são analisadas para garantir o adequado atendimento pela secretaria responsável. A auditoria é prejudicada pela existência de diferentes bancos de dados com tecnologias convencionais e centralizados, onde registros podem ser facilmente alterados e sob governanças distintas, passíveis de inconsistências, dificultando o rastreo.

1.3 BLOCKCHAIN COMO SOLUÇÃO A RASTREABILIDADE

Com a necessidade de rastreamento de materiais para evitar desvios, falsificações, controle de qualidade e identificação de produtos deteriorados, algumas entidades reguladoras, como a *Food and Drug Administration (FDA)* dos EUA, estabeleceram normativas que visam melhorias no gerenciamento da cadeia de suprimentos. No Brasil, em 2016, foi criada a Lei 13.410 e o Regime Diferenciado de Contratação (RDC) 157, que estabeleceram a criação do Sistema Nacional de Controle de Medicamentos (SNCM) visando regulamentar o rastreo de fármacos.

A pesquisa em (NG et al., 2021) afirma que, com o advento da pandemia da COVID-19, a necessidade de maior rastreabilidade e auditoria de insumos de saúde, torna premente o uso de tecnologias como da *blockchain*, surgindo trabalhos que tratam o rastreo, da compra à entrega de vacinas de forma segura, transparente e auditável. A Rede Nacional de Dados em Saúde do governo federal já no ano de 2020 adotou a tecnologia para promover segurança e acompanhamento no envio do registro de vacinações pelos municípios e estados (DONIDA et al., 2021).

Segundo (ZHANG; XUE; HUANG, 2016), *blockchain* é indicada para o desenvolvimento de soluções pertinentes à rastreabilidade, uma vez que possui os recursos da imutabilidade das transações, foco em segurança, descentralização dos dados e forte auditoria. A imutabilidade das transações é atraente para aplicações na área da saúde, pois cria trilhas de auditoria, mantendo a confiabilidade e a integridade dos dados da saúde do paciente (ZHANG; XUE; LIU, 2019). Diferindo dos sistemas que utilizam bancos de dados centralizados, mantém os dados distribuídos nos integrantes da rede e utiliza algoritmos de consenso para garantir que todas as máquinas estejam sincronizadas e possuam as mesmas informações.

Na investigação por trabalhos correlatos foram encontradas propostas que abordam o acompanhamento de produtos abrangendo toda a cadeia de fornecimento, da fabricação à entrega aos clientes finais, como visto em (ALANGOT; ACHUTHAN et al., 2017). Ainda

foi apresentado o monitoramento da temperatura de fármacos em transporte para garantir a chegada íntegra do produto na rede comercial, demonstrado em (BOCEK et al., 2017). Os autores em (NG et al., 2021) afirmam que existem muitos trabalhos que abordam o tema *blockchain* na área da saúde, entretanto ainda existem poucas implementações práticas.

1.4 MOTIVAÇÕES

1.4.1 Economicidade ao Estado

A perda financeira por meio de pedidos duplicados na rede pode ocorrer considerando medicamentos atendidos com um alto grau de complexidade, possuindo assim preços elevados, a exemplo do medicamento Besponsa indicado como monoterapia para o tratamento de adultos com leucemia, com valor de R\$ 83.898,70 em agosto de 2023 informado em (BESPONSA, 2023). A tabela de preços da Agência Nacional de Vigilância Sanitária (ANVISA) em 2022 apresentou valores que iniciam na ordem dos centavos e atingem 2 milhões de reais aproximadamente. A contribuição para a economia de recursos motiva este trabalho com vistas a proporcionar novos atendimentos aos cidadãos.

1.4.2 Melhoria no Tempo de Atendimento para o Paciente do SUS

No Brasil, quando a pessoa é portadora de doença grave e não possui os recursos financeiros suficientes para suprir o tratamento, passa a depender de forma vital do acolhimento e suporte do estado. Um atendimento público ágil pode refletir em cuidado eficaz aos pacientes (BATISTELLA et al., 2019). O conforto farmacológico necessita chegar quanto antes, assim sendo, otimizar a comunicação entre os entes públicos e o cidadão é outro motivador deste trabalho. A partir da disponibilização do rastreamento, acompanhamento pelo paciente e garantir a fila de atendimento, o sistema público ganha em transparência e confiabilidade.

1.5 OBJETIVOS

1.5.1 Objetivos Gerais

O objetivo deste trabalho é desenvolver um sistema com a tecnologia *blockchain* que possibilite integrar as organizações de forma segura, resiliente, descentralizada, fortemente auditável e capaz de garantir que cada ente público execute apenas as operações inerentes ao seu perfil. Para alcançar o objetivo geral com as características requeridas foram desenvolvidos a rede operacional entre os *hosts*, um contrato inteligente digital, uma API para acesso às operações e uma aplicação Web como interface de entrada e apresentação dos dados.

A partir da unificação dos sistemas, trazer uma visão homogênea e distribuída das informações em tempo real, sem qualquer hierarquia tecnológica. Ainda apresentar alguns indicadores iniciais para a gestão do serviço mediante *dashboard*.

1.5.2 Objetivos Específicos

1. Criar um Consórcio Privado e Permissionado entre os entes públicos;
2. Implementar a segurança por via do controle de acesso a rede;
3. Disponibilizar um banco de dados distribuído e consistente;
4. Fornecer forte auditoria;
5. Desenvolver indicadores que auxiliem a gestão.

1.6 OUTROS RESULTADOS E ATIVIDADES

Esta pesquisa foi apresentada no evento *Blockchain & Cryptocurrency Conference 2022*, Barcelona em 11 novembro de 2022 e posteriormente aprovada para publicação no periódico *Blockchain & Cryptocurrency Journal* em 2023. Ademais, foi apresentado no Congresso da Sociedade Brasileira da Computação no evento Colóquio em *Blockchain* e Web Descentralizada, em João Pessoa, em 8 agosto de 2023. O software JudMed teve o seu registro aprovado no Instituto Nacional da Propriedade Industrial (INPI) em julho de 2023. Os autores participaram de um *TestBed* do Comitê Técnico de *Blockchain* que criou uma rede entre universidades federais, sendo elas: Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Universidade Federal do Pará, Rede Nacional de Pesquisa e Universidade Federal de Varginha. Foi realizado um treinamento com a tecnologia blockchain a equipe técnica da Secretaria de Saúde do Município de Salvador, cronogramas e informações complementares estão dispostos no Apêndice E.

No capítulo 2 é apresentado a revisão bibliográfica que possibilitou o desenvolvimento do produto desta pesquisa, o capítulo 3 traz a análise de trabalhos correlatos que abordam a rastreabilidade de materiais utilizando blockchain, no capítulo 4 é visto o desenvolvimento e os testes do produto blockchain JudMed, no capítulo 5 é apresentado a prova de conceito que ocorreu com a área de coordenação farmacêutica do município de Salvador e a conclusão é vista no capítulo 6.

Capítulo**2**

Neste capítulo é apresentada toda a revisão bibliográfica para a elaboração do trabalho, contemplando a área das petições judiciais relacionados a saúde pública, as características técnicas da blockchain e os frameworks Hyperledger Fabric e Minifabric.

REVISÃO BIBLIOGRÁFICA

2.1 MEDICAMENTOS JUDICIALIZADOS NO BRASIL

2.1.1 Direito à Saúde

O direito à saúde está garantido pela Constituição Federal do Brasil (BRASIL, 1988), logo, o Estado possui o dever de garantir os meios para cumpri-lo. Também o artigo 12 do Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais, reconhece que toda pessoa tem direito de desfrutar do mais elevado nível de saúde física e mental, sendo um direito indispensável para o exercício de outros direitos humanos. Em (YORK, 2011) é dito que para estabelecer concretamente o direito à saúde são necessários os elementos:

1. Disponibilidade: Funcionamento satisfatório do sistema público de saúde e dos programas de saúde;
2. Acessibilidade: As instalações, bens e serviços de saúde devem ser acessíveis a todas as pessoas sem discriminação, dentro da jurisdição do Estado-parte, respeitando etnias e culturas;
3. Qualidade: As instalações, bens e serviços de saúde devem ser cientificamente apropriados e com boa qualidade.

A promoção da saúde de forma igualitária entre os membros da sociedade não é satisfeita se para uns é fornecido o tratamento adequado e para outros não. A disponibilidade de fármacos faz parte desse conjunto de ações sociais e inclusive não atende a todos. Como afirmam (BATISTA et al., 2020), a solicitação de medicamento por via judicial é um instrumento de adequação e faz parte de um evento conhecido no Brasil como judicialização da saúde.

“ Os Poderes Legislativo e Executivo não estão cumprindo seu papel constitucional. Dessa forma, cabe ao Judiciário dirimir tais conflitos, por meio da concessão de direitos fundamentais sociais requeridos pelo cidadão. Se os Poderes Legislativo e Executivo agem de forma desinteressada pela efetivação dos direitos fundamentais sociais, por isso, deve o Judiciário viabilizar, a todos, o acesso aos bens cuja fruição lhes tenha sido injustamente recusada pelo Estado. ” (BATISTA et al., 2020).

Para aquisição de medicamento por via judicial é necessário apresentar:

1. Comprovação, por meio de laudo médico fundamentado e circunstanciado expedido pelo médico que assiste o paciente, da imprescindibilidade ou necessidade do medicamento, assim como da ineficácia, para o tratamento da moléstia, dos fármacos fornecidos pelo SUS;
2. Incapacidade financeira do paciente de arcar com o custo do medicamento prescrito;
3. Existência de registro do medicamento na Agência Nacional de Vigilância Sanitária (ANVISA).

2.1.2 Fatores que Contribuem para o Aumento de Solicitações Judiciais Relacionadas a Medicamentos

Alguns fatores relacionados ao aumento das solicitações judiciais por fármacos foram identificados por (BATISTELLA et al., 2019) em estudo realizado na cidade de Londrina, no estado do Paraná. Foi visto que os principais aspectos que impactam as requisições judiciais são: a ausência dos fármacos na Relação Nacional de Medicamentos Essenciais (RENAME), o convencimento de médicos e pacientes pela indústria farmacêutica na adoção de remédios ainda não padronizados no SUS. Ademais, no referido estudo os autores identificaram que a maioria das prescrições foi originada no setor privado, podendo indicar parcerias entre médicos e laboratórios fabricantes visando padronizar determinados medicamentos na rede SUS.

2.1.3 Impactos Financeiros

O investimento elevado com a judicialização da saúde tem implicações orçamentárias significativas para o SUS, pois ocasiona despesa elevada e não programada pelos gestores públicos. Conforme o Tribunal de Contas da União (TCU) foram gastos em 2015, 1 bilhão de reais em petições judiciais relacionados à saúde. O estudo realizado por (BATISTELLA et al., 2019) demonstrou que no Brasil houve um significativo aumento no gasto com fármacos no SUS, onde passou de R\$14,3 bilhões em 2010 para quase R\$20 bilhões em 2015, representando um crescimento de 40%. A Tabela 2.1 demonstra que a solicitação de medicamento foi o principal causador de processos em 2019.

2.1.4 Tempo de Atendimento

O tempo de atendimento nas demandas judiciais por remédios é fator crucial na assistência terapêutica, ainda mais considerando a urgência por medicamentos específicos

para amenizar ou equacionar problemas de saúde que podem ser graves (BATISTELLA et al., 2019). A Tabela 2.2 demonstra os tempos de atendimento na cidade de Londrina entre os anos 2011 e 2017 que ultrapassaram 900 dias, o que pode ser totalmente ineficaz para não agravar o problema ou manter a vida dos assistidos. Para efetivamente melhorar o atendimento é necessário rever o tempo de duração desses processos e fornecer uma resposta mais ágil ao usuário durante o tempo de espera pela decisão judicial.

Tabela 2.1 Números da demanda judicial referente à judicialização da saúde em 2019 (BATISTA et al., 2020)

Assunto	Núm. de Processos
Fornecimento de Medicamentos	119.771
Planos de Saúde	109.778
Tratamento Médico-Hospitalar	45.104
Erro médico	7.665
Hospitais e Outras Unidades de Saúde	5.835
Exame de Saúde e/ou Aptidão Física	4.677
Saúde Mental	1.771
Financiamento do SUS	1.592
Vigilância Sanitária e Epidemiológica	559
Terceirização do SUS	179
Doação e Transplante de Órgãos; Tecidos e Partes do Corpo Humano	126

Tabela 2.2 Identificação dos processos por tempo de tramitação, desfecho dos processos arquivados e motivo do julgamento improcedente. Londrina/PR, 2011 a 2017 (BATISTA et al., 2020)

Tempo de Tramitação	Número de Processos	Percentual Relacionado ao Total
100 a 300 dias	76	12,6
301 a 500 dias dias	105	17,4
501 a 700 dias dias	106	17,5
701 a 900 dias dias	97	16,0
Acima de 900 dias dias	220	36,5

2.2 PRINCÍPIOS DE BLOCKCHAINS

A tecnologia *Blockchain* surgiu em 2008 quando apresentada no artigo acadêmico “Bitcoin: um Sistema Financeiro Eletrônico *Peer-to-Peer*” com autoria de Satoshi Nakamoto

(NAKAMOTO, 2008), pseudônimo do criador ou do grupo de criadores da tecnologia. A primeira geração foi marcada pelas moedas virtuais, entretanto os projetos ganharam expansão para outras áreas a partir do surgimento dos contratos inteligentes ou **Smart Contract (SC)** na segunda geração da tecnologia em 2015. O termo SC foi formalizado por Nick Szabo na década de 90, e significa: um protocolo de transação informatizado que executa os termos de um contrato (GREVE et al., 2018). Quando uma transação é submetida ao contrato, a execução se dá de forma independente e automática. Essa nova abordagem permitiu a execução de lógica de negócios com regras pré-estabelecidas entre os membros da rede.

O livro razão distribuído ou **Distributed Ledger Technology (DLT)** é o principal conceito de uma *blockchain*. Em um DLT são registradas todas as movimentações de um ativo e não há reversão de transações. Como exemplo, suponhamos uma transação de *bitcoins* entre duas pessoas, a pessoa A transfere equivocadamente 5 *bitcoins* para a pessoa B quando o correto seria transferir 3, não há reversão, portanto a pessoa B deve fazer o estorno de 2 *bitcoins* a pessoa A, desta forma a transação inicial que deveria ser de 3 *bitcoins* da pessoa A para a B, transforma-se equivalentemente em duas transações com o mesmo saldo final nas carteiras de A e B.

Quando uma transação é submetida, cada nó da rede realiza sua validação e após as confirmações os dados são inseridos em um bloco de transações. Quando um bloco é formado, passa a ter um endereço **hash** que está associado a cada transação contida nele. Todos os blocos estão interligados de forma encadeada, onde cada um conhece o endereço do anterior e assim de forma sucessiva formam o encadeamento. Por consequência do endereçamento associado a cada transação contida no bloco, não é possível exclusão, pois, neste caso, o bloco com a transação excluída passaria a ter um novo endereço *hash* e não seria reconhecido pelo bloco anterior, rompendo assim a cadeia.

As principais características da *blockchain* são a descentralização, persistência, anonimato e auditabilidade. Os maiores desafios são o controle do tamanho dos blocos, a segurança e o alto custo energético causado, por exemplo, pelo algoritmo de consenso *Proof of Work* para admissão de novos membros. A rede é do tipo **Peer to Peer (P2P)** onde um nó se comunica diretamente com os demais e pode ser emissor e receptor das informações, prescindindo de um ente centralizador, como caracterizado no modelo cliente-servidor (ZHENG et al., 2017). A Figura 2.1 demonstra a arquitetura de blocos encadeados de uma *blockchain*. O primeiro bloco é conhecido como **gênesis**. Cada bloco contém: as transações, um contador de transações, uma marca temporal do momento da sua criação e um campo *nonce* que é incrementado a cada criação de novo endereço *hash*.

Cada participante possui uma **assinatura digital** com um par de chaves, pública e privada, conhecida como assinatura assimétrica (ZHENG et al., 2017). Todas as transações são criptografadas com a chave privada do emissor. Ao receber a transação, o receptor que possui a chave pública do emissor, descriptografa a mensagem confirmando a autenticidade.

Buterin (2015) classifica os sistemas *blockchain* em três tipos:

1. Pública: São mediadas geralmente com criptomoeda como sistema de incentivo a participação. Qualquer pessoa ou ente pode participar da rede enviando e recebendo

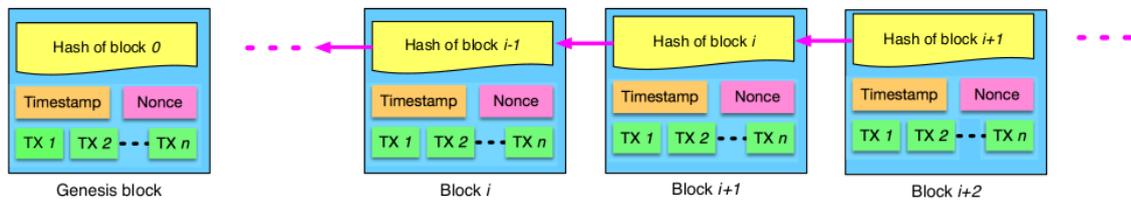


Figura 2.1 Blocos de transação encadeados numa Blockchain (ZHENG et al., 2017)

transações e podem ser estabelecidas provas computacionais para a obtenção do acesso;

2. Privada: Grupo fechado que habilita membros com interesse comum em colaboração. As permissões são centralizadas em uma organização. A escrita e a leitura podem ser públicas ou restritas, dependendo da política de acesso;
3. Consorciada: Caracterizada por definir um conjunto de nós que fazem parte da rede com direito de leitura público ou restrito, por conta desta característica é considerada parcialmente descentralizada.

2.2.1 Segurança e Privacidade

Embora os sistemas tradicionais de gerenciamento de banco de dados distribuído sejam uma plataforma consolidada em sistemas de saúde, eles têm limitações substanciais, como a incapacidade de oferecer suporte ao compartilhamento de dados *peer-to-peer*, suscetibilidade a adversários externos (por exemplo, *hacking*) e a ausência de um trilha de auditoria imutável. De acordo com (NG et al., 2021), os recursos exclusivos, como transparência, rastreabilidade, não-repúdio (ou seja, incapacidade de refutar a validade da assinatura), desintermediação (ou seja, remoção de intermediários para a tomada de decisão) e imutabilidade, *blockchain* poderia potencialmente resolver esses problemas, permitindo-lhe oferecer vantagens importantes sobre as plataformas convencionais.

Para garantir segurança e privacidade em sistemas *blockchain*, os seguintes requisitos devem ser satisfeitos: consistência do livro razão distribuído, integridade das transações, disponibilidade de sistema e dados, prevenção ao duplo gasto e confidencialidade (ZHANG; XUE; LIU, 2019).

2.2.1.1 Resistência a Adulteração: Antes do envio, a transação é encriptada com uma função *hash* como a SHA 256 e em seguida assinada digitalmente pelo emissor utilizando um algoritmo de criptografia, por exemplo, o *Elliptic Curve Digital Signature Algorithm* (ECDSA). Considerando como exemplo uma tentativa de adulteração na rede Bitcoin, caso um minerador malicioso altere uma transação e reenvie a rede, os participantes realizam o consenso para confirmarem os dados e durante a checagem da

autenticidade mediante chave pública do emissor concluem que difere da chave do envio original e detectam a tentativa maliciosa.

O consenso pode ocorrer de diferentes maneiras, seja com o uso de algoritmos de loteria, como *Proof of Elapsed Time* (PoET) e *Proof of Work* (PoW), ou através do uso de métodos baseados em votação, tais como *Practical Byzantine Fault Tolerance* (PBFT) e RAFT (GROUP et al., 2017). Dentre os mecanismos baseados em votação destacam-se os modelos *Crash Fault Tolerant* (CFT) e *Byzantine Fault Tolerant* (BFT). Enquanto o mecanismo CFT assume que alguns nós responsáveis pelo consenso podem falhar, o mecanismo BFT admite que além de falhar, alguns nós podem agir de maneira maliciosa. Segundo (MIERS et al., 2020), a escolha adequada à solução irá depender das características da rede.

2.2.1.2 Resistência a Ataque *Distributed Denial of Service* (DDOS): Um ataque DDOS ou Negação Distribuída de Serviço, ocorre quando uma máquina central que funciona como servidor de dados recebe um número de requisições simultâneas que vão além da sua capacidade de processamento (ZHANG; XUE; LIU, 2019). Um ataque DDOS em sistemas *blockchain* é bastante dificultado porque os nós da rede são autônomos e estão distribuídos tornando o processamento descentralizado, logo a ofensiva precisa alcançar pelo menos metade mais um dos nós e torná-los *offline*, pois desta maneira não haveria um número suficiente para o consenso tornando o sistema inoperante. Considerando uma rede com muitos participantes ou com alcance mundial, esse tipo de ataque tem pouca probabilidade de êxito.

2.2.1.3 Resistência a Ataque de Duplo Gasto: Os autores em (ZHANG; XUE; LIU, 2019), explicam que o ataque de duplo gasto decorre da movimentação de um ativo por mais de uma vez, por exemplo, o mesmo *bitcoin* sendo transferido para duas carteiras, duplicando o gasto. Para prevenir esse tipo de ataque, as transações são verificadas por cada participante que utilizam um protocolo de consenso que detecta a segunda transação equivocada, evitando a confirmação e mantendo o livro razão ou *Ledger* consistente na *blockchain*.

2.2.1.4 Resistência a Ataque de Consenso 51%: Um ataque de 51% acontece quando um grupo malicioso consegue participar da rede formando um conluio. Os atacantes tornam-se a maioria dos votantes do consenso, permitindo que transações equivocadas aconteçam. Em redes não permissionadas como o Bitcoin a qual utiliza o algoritmo de loteria *Proof of Work* ou prova de trabalho, o ataque pode ocorrer caso os nós maliciosos tornem-se a maioria dos mineradores, confirmando transferências ilegais ou reversão de transações. Numa rede grande como a rede Bitcoin é muito difícil subverter a maioria dos nós para formar esse conluio, pois, para tornar-se minerador é necessário resolver prova computacional complexa com alto grau de processamento e conseqüente elevado custo energético (ZHANG; XUE; LIU, 2019). Numa rede *blockchain* do tipo privada e permissionada como o Hyperledger Fabric que utiliza o protocolo Raft como apresentado por (HU; LIU, 2020), os nós maliciosos precisariam entrar no consórcio após anuência e con-

firmação de todos os nós presentes para então como membro, conseguir enviar transações, alterando o estado do ledger, não se caracterizando como um ataque de 51%.

2.2.2 Rastreabilidade

Uma cadeia de suprimentos pode ser composta por diversas organizações como produtoras, fornecedoras, distribuidoras e consumidores finais. Para que o produto chegue às mãos do cliente com a originalidade e qualidade esperadas, a logística precisa ser segura e rastreável, evitando violações. Produtores, fornecedores e distribuidores buscam prestadores de serviços de rastreabilidade certificados pelo governo com o intuito de inspecionar o envio dos produtos. As empresas contratadas para o rastreamento emitem certificados de inspeção durante o trajeto. Os autores em (LU; XU, 2017), afirmam que, para gerenciar as informações e emitir certificados, esses serviços empregam sistemas de informação para o rastreamento. Os sistemas com esta finalidade que utilizam bancos de dados centralizados apresentam um potencial ponto de falha e fazem com que a rastreabilidade não atenda completamente aos requisitos de segurança ideais a rede de abastecimento.

Sistemas descentralizados e resilientes como os baseados em *blockchain* tornam-se boas alternativas. O rastreamento em tempo real pode agregar ainda mais na confiabilidade, a exemplo do projeto Manifest, que é uma parceria entre a Microsoft e a empresa Mojix para ajudar fábricas, distribuidores e varejistas a rastrear mercadorias usando *blockchain* e dispositivos *Radio Frequency Identification* (RFID). Os contratos inteligentes na *blockchain* definem e automatizam as regras de negócio e podem, por exemplo, verificar se todas as informações regulatórias exigidas estão presentes e válidas antes de registrar a próxima movimentação. Caso o setor logístico passe por alterações em suas regras, novos acordos entre os integrantes podem ser incluídos no contrato inteligente digital. Nesse ambiente complexo e dinâmico a trilha de auditoria traz transparência e confiança, iniciando na produção dos materiais e alcançando até a entrega aos clientes finais.

2.3 HYPERLEDGER

Conforme (GROUP et al., 2017), o Hyperledger é um projeto da Linux Foundation para desenvolvimento de *blockchains*, tem seu código aberto e é modular, o que possibilita a evolução por meio da comunidade de desenvolvedores. O Hyperledger agrupa uma série de *frameworks*, em destaque:

1. Fabric: Para desenvolvimento de *blockchains* permissionadas e empresariais;
2. Explorer: Aplicação web que disponibiliza informações da rede como participantes, transações, contratos inteligentes e ativos;
3. Sawtooth: Plataforma modular para desenvolver, implementar e executar DLT em soluções permissionadas e não permissionadas. Utiliza como mecanismo de consenso o PoET, para um mínimo esforço computacional no que se refere a permissão de entrada dos participantes;
4. Iroha: Bibliotecas para implementação de DLT em infraestruturas já existentes;

5. Indy: Trata-se de um *Software Development Kit* (SDK) para o Hyperledger que oferece componentes para adicionar novos recursos para a gestão de identidades descentralizada.

2.4 HYPERLEDGER FABRIC

O Hyperledger Fabric é um *framework* utilizado para desenvolvimento de *blockchains* permissionadas e empresarial. Possui uma arquitetura em módulos, com isso possibilita a expansão e melhorias mediante customização dos componentes tais como o mecanismo de consenso, ordenação, filiação de membros e a mensageria responsável por disseminar os blocos para todos os nós (GREVE et al., 2018).

2.4.1 Membership Service Provider (MSP)

É o recurso responsável pela filiação de membros da rede Fabric. Em particular, um MSP abstrai todos os mecanismos e protocolos criptográficos por trás da emissão e validação de certificados e autenticação do usuário (FABRIC, 2022b). É importante observar que as identidades MSP nunca expiram, elas só podem ser revogadas, adicionando-as às Listas de Revogação de Certificados (CRLs) apropriadas. Um conjunto de parâmetros precisa ser especificado para permitir a validação da identidade (certificado) e a verificação de assinatura, alguns em destaque:

- Lista de certificados de Autoridades de Certificação autoassinados (X.509) para constituir a raiz de confiança;
- Lista de certificados X.509 para representar CAs intermediárias que este provedor considera para validação de certificado;
- Lista de certificados X.509 que representam os administradores deste MSP;
- Lista de Unidades Organizacionais com membros válidos no serviço MSP;
- Conjunto de Listas de Revogação de Certificados (CRLs), cada uma correspondendo exatamente a uma das Autoridades de Certificação MSP listadas (intermediárias ou raiz).

Na Figura 2.2 é apresentada a arquitetura modular da plataforma Hyperledger Fabric.

2.4.2 Canais

O canal em uma rede Fabric representa o consórcio entre os nós membros ou *peers* pertencentes às organizações. Ao ingressarem em um canal, os *peers* são autenticados e autorizados a realizar transações. O canal também é composto por nós âncora (*anchor peers*), nós de ordenamento das transações (*order peers*), ativo (*ledger*) e contrato inteligente (*chaincode*). Os *anchor peers* são responsáveis por comunicar-se com os *orderer peers* para obter os blocos contendo as transações, e disseminá-los para os demais nós de

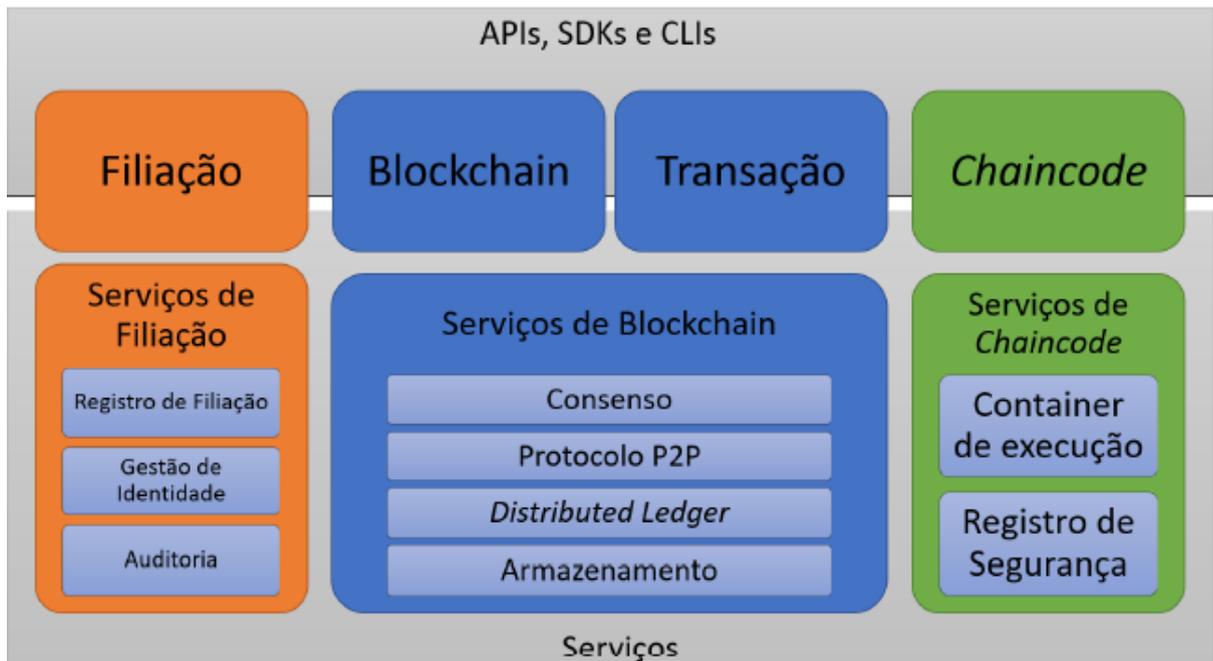


Figura 2.2 Arquitetura Hyperledger (GREVE et al., 2018)

suas organizações (GREVE et al., 2018). Os *order peers* realizam a ordenação dos blocos após o consenso entre eles. O Hyperledger Fabric possibilita a criação de vários canais, portanto as organizações podem participar de múltiplas redes *blockchain* independentes.

2.4.3 Consenso e Ordenação

O mecanismo de consenso numa rede Fabric é baseado em votação para manter o *ledger* consistente. O *framework* suporta algoritmos tolerantes a falhas como o *Crash Fault Tolerance* (CFT) e tolerante a entes maliciosos como o *Byzantine Fault Tolerance* (BFT). A ordenação e o consenso ocorrem com os nós ordenadores distribuídos na rede. Por meio de votação, a formação dos blocos acontece de forma determinística, impedindo novas ramificações ou *forks* na rede. Os ordenadores ainda gerenciam as organizações que fazem parte do canal. O algoritmo de consenso e ordenação padrão do Fabric na versão 2.0 é o Raft. As fases para efetivar uma transação no Hyperledger Fabric são descritas abaixo:

1. **Fase 1 (Proposta):** A aplicação cliente envia uma proposta de transação para o *peer* de sua organização, ele então invoca o *chaincode* e faz uma proposta de atualização do *Ledger*. Caso o *chaincode* considere a atualização válida, o *peer* faz o endosso do resultado. O *peer* não atualiza sua cópia do *ledger* ainda neste momento, apenas retorna a resposta da proposta de transação com sucesso para a aplicação cliente;
2. **Fase 2 (Ordenação e empacotamento da transação no bloco):** A aplicação

cliente que recebeu a resposta da proposta de transação com o endosso da fase 1 faz o envio da transação endossada para o nó ordenador que funciona em conjunto com outros nós ordenadores formando o serviço de ordenação. O serviço de ordenação insere a transação no bloco, empacota-o e salva no *ledger* e distribui por todos os *peers* do consórcio para validação e *commit* final na fase 3;

3. **Fase 3 (Validação e *commit*):** O nó ordenador distribui o bloco para todos os *peers* ligados a ele. Cada *peer* no canal verifica o endosso de todas as transações. Se o bloco estiver consistente acontece o *Commit* final e a transação passa a ser imutável no *ledger*, não podendo existir reversão ou exclusão.

2.4.4 Ledger

O livro razão ou *ledger* contém o estado atual de um ativo como um diário de transações. Partindo do exemplo de uma conta bancária onde o ativo é a conta do cliente, temos o estado atual da conta que é o saldo bancário, mas ainda temos os registros de créditos e débitos que justificam o valor disponível na conta. O Hyperledger Fabric apresenta o valor atual (**estado global atual**) do *ledger* e o histórico das transações *blockchain*. O *ledger* é iniciado com o bloco gênese (primeiro bloco de transações) e fica restrito a um canal compartilhado apenas com os membros associados a ele. (FABRIC, 2022a).

Um *ledger* armazena o histórico de transações que são os fatos sobre o estado atual de um ativo. Embora os fatos de um objeto de negócios possam mudar, o histórico de fatos sobre ele é imutável (FABRIC, 2022a).

A rede contém várias cópias de um *ledger* que são mantidas consistentes por meio do consenso. O termo DLT é frequentemente associado a esse tipo de *ledger* que é logicamente singular, mas possui réplicas distribuídas na rede.

2.4.5 Estado Global

No Hyperledger Fabric, um *ledger* possui duas partes distintas, o estado global e a *blockchain*. Cada uma delas representa um conjunto de informações sobre os objetos de negócios.

O estado global é um banco de dados que contém os valores atuais dos ativos. O Fabric por padrão apresenta as opções CouchDB e LevelDB, ambos do tipo NoSql, isso torna mais fácil para um programa acessar diretamente o valor atual em vez de ter que calculá-lo percorrendo todo o log de transações. Os estados do *ledger* são expressos como pares chave-valor e podem mudar com frequência, pois os estados podem ser criados, atualizados ou excluídos. A Figura 2.4 demonstra a arquitetura do estado global no Hyperledger Fabric.

2.4.6 Blockchain

A *blockchain* é um log sequencial de transações que registra todas as mudanças que resultam no estado atual do ativo. As transações são inseridas nos blocos, permitindo o armazenamento do histórico de mudanças. A estrutura de dados da *blockchain* é muito

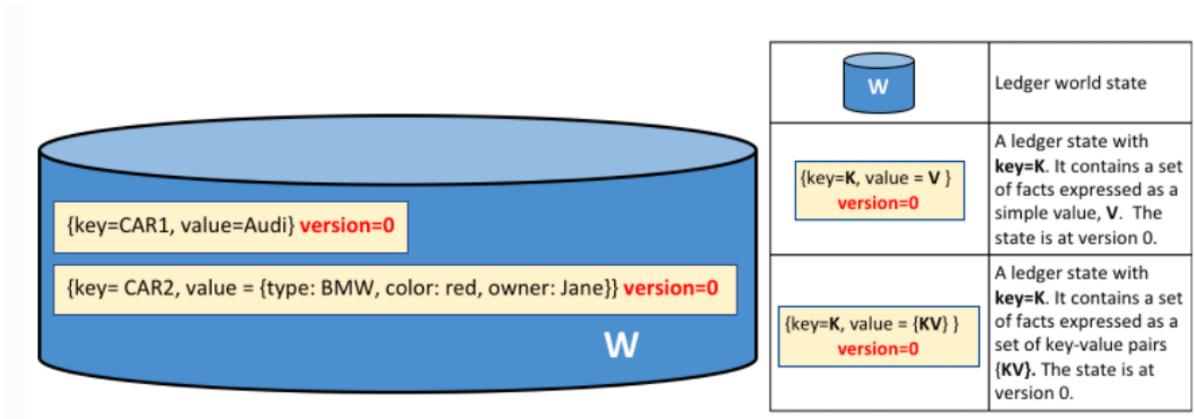


Figura 2.3 Estado Global em Hyperledger Fabric - Fonte: (GROUP et al., 2017)

diferente do estado global ou atual porque, uma vez escrita, não pode ser modificada, é imutável.

As transações podem consultar ou atualizar o estado do ativo. O sequenciamento de blocos, bem como o sequenciamento de transações dentro de blocos, é estabelecido quando os blocos são criados pela primeira vez por um componente do Hyperledger Fabric chamado serviço de ordenação.

O cabeçalho de cada bloco inclui um *hash* das transações do bloco, bem como um *hash* do cabeçalho do bloco anterior. Dessa forma, todas as transações no *ledger* são sequenciadas e vinculadas criptograficamente. Esse *hashing* e vinculação tornam os dados do *ledger* muito seguros. Mesmo se um nó que hospeda o *ledger* fosse adulterado, ele seria incapaz de convencer todos os outros nós de que ele tem a *blockchain* "correta" porque o *ledger* é distribuído por uma rede de nós independentes.

A *blockchain* é sempre implementado como um arquivo, ao contrário do estado global, que usa um banco de dados. A Figura 2.4 apresenta o modelo de arquitetura da *blockchain* no Hyperledger Fabric (FABRIC, 2022a) onde a *blockchain* B contém os blocos B0 (bloco gênese), B1, B2, B3. No diagrama, podemos identificar que o bloco B2 possui os dados D2 que contém as transações: T5, T6, T7. B2 tem um cabeçalho de H2, que contém um *hash* criptográfico de todas as transações em D2, bem como o endereço *hash* do H1 do bloco anterior (B1). Desta forma todos estão imutavelmente ligados.

O bloco gênese é o ponto de partida para o *ledger*, embora não contenha nenhuma transação do usuário, possui a transação de configuração com o estado inicial do canal. (FABRIC, 2022a). Um bloco é composto por três seções, vista na Figura 2.5. A primeira seção (**H0..H3**) é o cabeçalho que contém:

- Número do bloco: Um número inteiro começando em 0 (o bloco gênese) e incrementado em 1 para cada novo bloco criado na *blockchain*;
- *Hash* do Bloco Atual: O *hash* de todas as transações contidas no bloco atual;

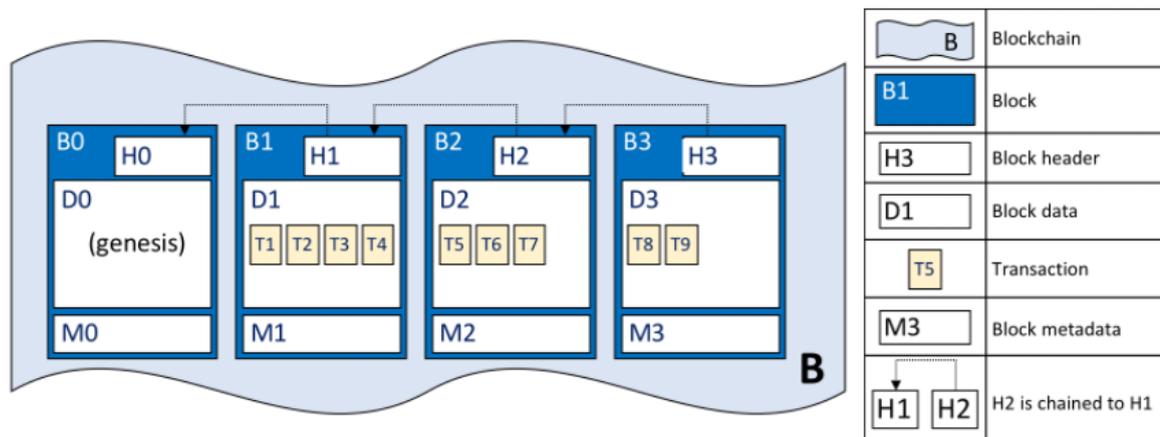


Figura 2.4 Blockchain Hyperledger Fabric - Fonte: (GROUP et al., 2017)

- *Hash* do cabeçalho do bloco anterior: Esse campo é o endereço do bloco e é criado como um hash criptográfico dos dados do bloco.

A segunda seção (**D0..D3**) é a de dados que contém uma lista de transações ordenadas. A terceira seção (**M0..M3**) são os metadados do bloco que contém o certificado e a assinatura do criador do bloco verificado pelos nós da rede. Subsequentemente, o *committer* do bloco adiciona um indicador válido/inválido para cada transação em um *bitmap* que inclusive reside nos metadados, bem como um *hash* das atualizações de estado a fim de detectar bifurcações.

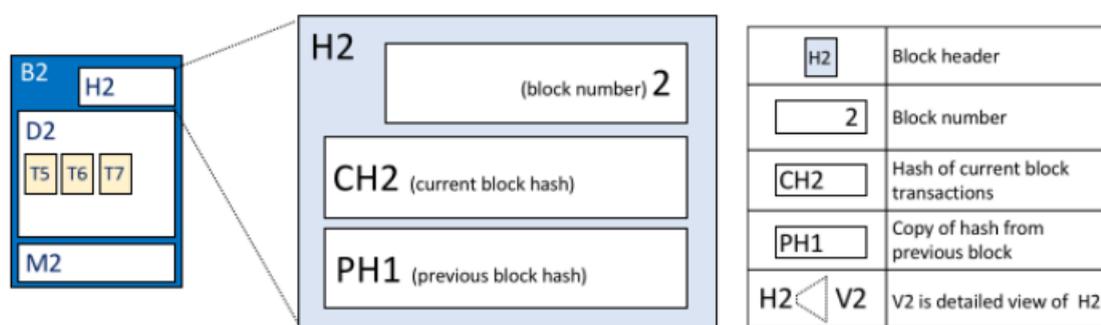


Figura 2.5 Blocos Hyperledger Fabric - Fonte: (GROUP et al., 2017)

2.4.7 Chaincode e Transações

Numa rede Fabric o contrato inteligente é conhecido como *Chaincode* e pode ser escrito nas linguagens: Go, Java, e Node.js . Para realizar a interação com o *chaincode*, são realizadas transações. Existem dois tipos de transações: *Invoke* e *Query*. A transação do tipo *invoke* executa uma função que altera o estado do ledger, enquanto a transação *query* realiza uma consulta. Através do *invoke* é possível a um cliente acessar uma função específica contida em um *chaincode* (DHILLON; METCALF; HOOPER, 2017).

Os aplicativos são isolados dos detalhes do mecanismo de consenso pelo Hyperledger Fabric SDK; eles simplesmente invocam um *chaincode* e são notificados quando a transação foi incluída no *blockchain* (válida ou inválida). O ponto-chave é que apenas as transações assinadas pelo conjunto necessário de organizações endossantes resultarão em uma atualização do estado global do ativo. A Figura 2.6 apresenta os seguintes campos que compõem uma transação:

- Cabeçalho: Ilustrado por **H4**, captura alguns metadados essenciais sobre a transação, por exemplo, o nome do *chaincode* e sua versão;
- Assinatura: Sinalizado como **S4**, contém uma assinatura criptográfica, criada pelo aplicativo cliente. Este campo é utilizado para verificar se os detalhes da transação não foram adulterados, pois requer a chave privada da aplicação para gerá-la;
- Proposta: Este campo representador por **P4**, codifica os parâmetros de entrada fornecidos por um aplicativo para o *chaincode* que cria a proposta de atualização do *ledger*. Quando o *chaincode* é executado, esta proposta fornece um conjunto de parâmetros de entrada, que, em combinação com o estado global atual, determina o novo estado global do ativo;
- Resposta: Vista em **R4**, captura os valores antes e depois do estado atual, e se a transação for validada com sucesso, ela será aplicada ao *ledger* para atualizar o estado do ativo final;
- Endossos: Conforme mostrado em **E4**, esta é uma lista de respostas de transações assinadas por cada organização, necessário para satisfazer a política de endosso. Cada endosso codifica efetivamente a resposta de transação específica de cada organização, o que significa que ao incluir qualquer resposta de transação que não corresponda aos endossos suficientes, será rejeitada como inválida e não atualizará o estado global.

2.5 FRAMEWORK MINIFABRIC

O Minifabric é um framework da Hyperledger Foundation sob a licença Apache 2.0 e tem o objetivo de reduzir o tempo de criação e implantação de redes Hyperledger Fabric (LI TONG; JONES, 2021). Os comandos no Minifabric são menores e sua execução agrupa uma série de etapas do Fabric. Utiliza todos os recursos tais como a criação de

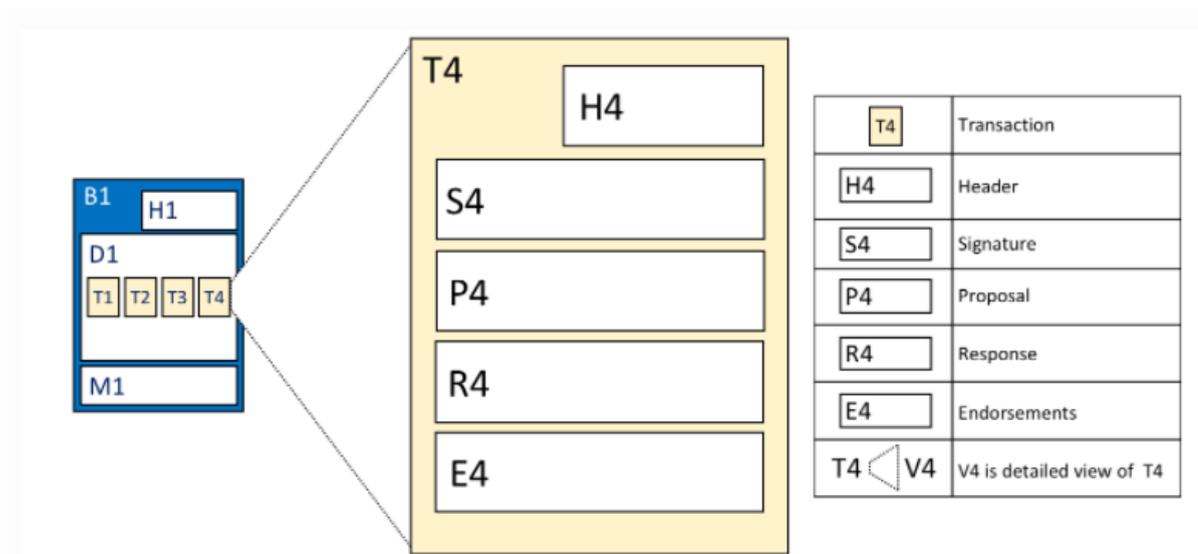


Figura 2.6 Transações Hyperledger Fabric - Fonte: (GROUP et al., 2017)

organizações e canais, instalação e operação em *chaincodes*, persistência e consulta do *ledger*. Permite configurar, monitorar e expandir uma rede como: adicionar novas organizações, consultar, criar, ingressar e atualizar um canal. Pode ser implantado com Docker(BOETTIGER, 2015) ou Kubernetes(BURNS; BEDA; HIGHTOWER, 2019). É possível instalar em sistemas operacionais Linux ou Windows. No Apêndice B são apresentados os comandos necessários para iniciar uma rede hyperledger fabric a partir do *framework* Minifabric.

Capítulo

3

Neste capítulo são apresentados os principais trabalhos relacionados com o enfoque em rastreabilidade de materiais e aplicações de *blockchain* para rastreio de fármacos.

ANÁLISE DE TRABALHOS CORRELATOS

Não foram identificadas abordagens no estado da arte ou ferramentas que tratem a comunicação tecnológica entre as organizações vinculadas a demanda de petições judiciais ligadas a medicamentos, com isso foram analisadas propostas de rastreio de materiais em âmbito geral.

3.1 TRACE AND TRACK: ENHANCED PHARMA SUPPLY CHAIN INFRASTRUCTURE TO PREVENT FRAUD

A proposta trazida por (ALANGOT; ACHUTHAN et al., 2017) utiliza *blockchain* para evitar que produtos não regulamentados ou falsificados entrem na cadeia de suprimentos dos EUA. Os autores afirmam que há um número crescente de produtos farmacológicos falsificados sendo produzidos e comercializados e a autoridade fiscalizadora *Food and Drug Administration* (FDA), estabeleceu a lei de qualidade e segurança de medicamentos que exige a adoção de mecanismos mais seguros para rastreio dos fármacos.

Na arquitetura da solução, o autor segmenta o sistema em três planos, um plano de dados que coleta as informações, um plano de controle que contém a *blockchain* como intermediário e um plano de aplicação na nuvem. A *blockchain* proposta é privada entre os órgãos da cadeia de suprimentos, porém não deixa claro qual mecanismo de permissão de acesso está utilizando. Este projeto contempla auditoria e está ligado a FDA que é o órgão público regulador da área. Da mesma maneira faz o acompanhamento do material de forma síncrona com o movimento físico por meio de Internet das Coisas e prevê o rastreio até as mãos do cliente final.

3.2 BLOCKCHAINS EVERYWHERE-A USE-CASE OF BLOCKCHAINS IN THE PHARMA SUPPLY-CHAIN

A *blockchain* desenvolvida pela empresa MODUM.IO AGO é apresentada no trabalho de (BOCEK et al., 2017). O objetivo é fazer o monitoramento da temperatura dos fármacos

durante o transporte. Os dados imutáveis do monitoramento fazem com que haja a validação mediante contrato de fornecimento de temperatura ideal para o pacote em trânsito. Um aplicativo *mobile* inicia a leitura dos sensores térmicos que estão acoplados às embalagens e então envia os dados para a *blockchain* Ehtereum (DANNEN, 2017) em um servidor web com banco de dados Postgress. Remetente e destinatário acompanham visualmente as temperaturas registradas durante o percurso e caso atinja um valor abaixo ou acima do especificado, todos os integrantes são informados pelo contrato inteligente.

A Empresa desenvolveu um projeto-piloto que monitorou 55 remessas e realizou 7.576 leituras de temperatura, obtendo apenas 3 falhas de leitura, desta forma demonstrou um resultado consistente. Neste trabalho houve a implementação de uma *blockchain* privada, mas o autor não detalhou como estabeleceu as permissões de acesso. Realiza auditoria de transações e a comunicação com a *blockchain* se dá de forma síncrona com a movimentação do material, não informou se utiliza servidor próprio ou serviços de armazenamento em nuvem.

3.3 DRUGLEDGER: A PRACTICAL BLOCKCHAIN SYSTEM FOR DRUG TRACEABILITY AND REGULATION

No trabalho de (HUANG; WU; LONG, 2018) é apresentado um sistema *blockchain* chamado **Drugledger** cujo objetivo é realizar o rastreo do fármaco da produção até a chegada na farmácia e faz o rastreo não sincronizado com o fluxo físico do medicamento. É privada e permissionada e faz a separação dos serviços em três módulos: provedor de certificados, consultas e segurança. Utiliza criptografia assimétrica com as chaves públicas e privadas de cada organização. Foca inclusive na privacidade financeira das transações para evitar concorrência desleal e vantagens comerciais. Com as chaves de origem e destino só permite a próxima transação se a chave seguinte for a do destinatário esperado. Este trabalho diferenciou-se por trazer uma estratégia para controlar o crescimento dos blocos de transações. O autor associa o tempo de vida do bloco com a data de validade do lote dos medicamentos rastreados, essas transações ficam registradas na *blockchain*, mas não são recriadas nos blocos seguintes, desta maneira otimiza o armazenamento. O autor afirma sobre a criação de um protótipo, entretanto não informa nenhum dado de simulação, mesmo que prévio para avaliação.

3.4 GOVERNANCE ON THE DRUG SUPPLY CHAIN VIA GCOIN BLOCKCHAIN

Utilizando conceitualmente a *blockchain* **Gcoin** os autores (TSENG et al., 2018) desenvolvem a rastreabilidade de fármacos para combater a falsificação, o que diverge de outras propostas é que neste trabalho o governo tem o papel regulatório fornecendo as licenças para as organizações que fazem parte da cadeia de suprimentos tal como fabricantes, distribuidores e vendedores. A *blockchain* verifica a validade de cada transação onde só é permitido o próximo movimento do fármaco se a transação anterior estiver válida, caso ocorra alguma transação não reconhecida, sinaliza aos participantes imediatamente mediante contrato inteligente e o lote fica retido na *blockchain*, só podendo ser movimentado após fiscalização governamental.

A *blockchain* proposta é pública e permissionada, pois só participa quem tem a licença de minerador fornecida pelo governo, possibilitando criar e verificar transações. A *blockchain* armazena um QR Code com todos os dados sintetizados da transação. Não deixou claro na arquitetura se a disponibilidade do sistema ocorre em nuvem ou em servidor próprio. Faz o rastreo assíncrono com a movimentação física do medicamento e utiliza aplicativo *mobile* para a leitura e interação por QR Code.

3.5 A NEW ERA OF FOOD TRANSPARENCY POWERED BY BLOCKCHAIN

No estudo de caso em (YIANNAS, 2018) é apresentada a utilização da *blockchain* desenvolvida pela empresa IBM para o rastreo de alimentos junto a empresa varejista Walmart que de acordo com autor, está presente em 28 países e quase 12.000 lojas com 260 milhões de clientes aproximadamente.

A rastreabilidade de alimentos é um grande desafio para as maiores empresas comerciantes destes produtos. Problemas como deterioramento e falsificação são enfrentados com grande frequência. Com este desafio posto, a IBM em conjunto com a Walmart decidiram desenvolver um sistema em *blockchain* para rastrear e identificar os materiais.

Foi realizada uma prova de conceito com um projeto-piloto, conseguindo reduzir o tempo de localização de lotes na rede de 6 dias para 2 segundos. Após a validação em cenário de produção, o projeto tornou-se o sistema **IBM Food Trust** (KAMATH, 2018) utilizado hoje pelas empresas fornecedores e varejistas, incluindo Walmart, Kroger, Wegmans, Tyson, Driscolls, Nestlé, Unilever, Danone, McCormick e Dole.

A *blockchain* fornece acompanhamento síncrono com o movimento físico dos produtos mediante armazenamento de QR Code, é privada e permissionada e utiliza a auditoria das transações para identificar o rastreo de forma ágil. Possui aplicativo *mobile*, não deixou explícito se o servidor é próprio ou está em nuvem e não inclui o cliente final no rastreo.

3.6 COMPARATIVO COM A SOLUÇÃO PROPOSTA

Os requisitos técnicos e características do sistema JudMed foram comparados com as propostas apresentadas nas seções anteriores. Não foram encontradas alternativas que tratam especificamente das solicitações judiciais de medicamentos, assim como o rastreo até as mãos do usuário de sistemas públicos de atendimento. Os trabalhos analisados que levam em conta o cliente final, abordam os que podem pagar pelo produto no momento da sua necessidade, o cliente ou paciente do Sistema Único de Saúde (SUS) depende da logística dos órgãos públicos para obterem medicamentos, em vista disso, a segurança do processo e o tempo de atendimento são grandes aliados no cuidado à saúde.

A proposta que mais se aproximou ao contexto foi a *Governance on The Drug Supply Chain via Gcoin blockchain* exceto por ser uma *blockchain* pública e utilizar moeda virtual para que os integrantes participem da rede, diferindo da JudMed que é um consenso privado que confirma as transações ao invés de aquisição de qualquer tipo de *token* de acesso à rede. Os trabalhos foram numerados como segue e o comparativo apresentado na Tabela 3.1

1. *Trace and Track: Enhanced Pharma Supply Chain Infrastructure to Prevent Fraud;*
2. *Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain;*
3. *Drugledger: A Practical Blockchain System for Drug Traceability and Regulation;*
4. *Governance on the Drug Supply Chain via Gcoin Blockchain;*
5. *A New Era of Food Transferecy Powered By Blockchain.*

Tabela 3.1 Tabela comparativa com trabalhos correlacionados (Elaboração Própria, 2021)

Requisitos do Produto	JudMed	1	2	3	4	5
Blockchain privada	SIM	SIM	SIM	SIM	NÃO	SIM
Blockchain permissionada	SIM	NÃO	NÃO	SIM	SIM	SIM
Fornece Auditoria	SIM	SIM	SIM	NÃO	SIM	SIM
Possui App. Móvel	SIM	NÃO	SIM	NÃO	SIM	SIM
Rastreabilidade até cliente final	SIM	SIM	NÃO	NÃO	SIM	NÃO
Atende usuário de sistema público	SIM	SIM	NÃO	SIM	SIM	NÃO
Atende Solicitação Judicial de Medicamento	SIM	NÃO	NÃO	NÃO	NÃO	NÃO

Capítulo

4

Neste capítulo são apresentados a rede blockchain JudMed, a metodologia utilizada, o modelo de negócios, a arquitetura da solução, o fluxo do processo judicial com a implantação da blockchain, os softwares desenvolvidos e os testes de funcionalidades.

BLOCKCHAIN JUDMED

4.1 O MODELO DE NEGÓCIO E A UTILIZAÇÃO DE BLOCKCHAIN

Para avaliar se a tecnologia *blockchain* traz maiores benefícios do que as tecnologias tradicionais é preciso considerar alguns fatores. A Figura 4.1 traz alguns questionamentos que devem orientar a decisão de adoção ou não. Tendo por base o guia disposto em (101BLOCKCHAINS.COM, 2022) as seguintes perguntas foram consideradas para verificar a necessidade da utilização de uma *blockchain* para atender as demandas judiciais por medicamentos:

1. Necessita de órgão intermediário? Não, cada organização detém um papel específico para o serviço e não centraliza as decisões, comunicando-se diretamente com os outros integrantes da rede;
2. Existe um ativo digital? Sim, a petição judicial para aquisição de medicamento já é um ativo digital nos sistemas das organizações, a JudMed irá unificá-lo;
3. É necessário um banco de dados compartilhado? Sim, todos os entes públicos precisam ter a mesma visão dos dados o mais rápido possível para evitar fraudes;
4. Possui muitas equipes envolvidas? Sim, cada organização pública possui um setor de tecnologia da informação e sistemas próprios;
5. É necessário um ambiente confiável? Sim, o ativo judicial precisa ser movimentado e acompanhado com segurança;
6. Precisa de alto desempenho? Não, as transações envolvendo os processos não são numerosas, logo o custo de armazenamento e recuperação não causam impactos significantes no desempenho;

7. Precisa de grande armazenamento? Não, por conta do número baixo de transações não há um consumo elevado de armazenamento;
8. Necessário uma solução contratual? Sim, o consórcio necessita seguir as regras operacionais pré-estabelecidas de forma automatizada;
9. O sistema suporta mudança de regra? Sim, as instituições são regidas por leis regulatórias que podem mudar e exigir adequações no contrato inteligente.

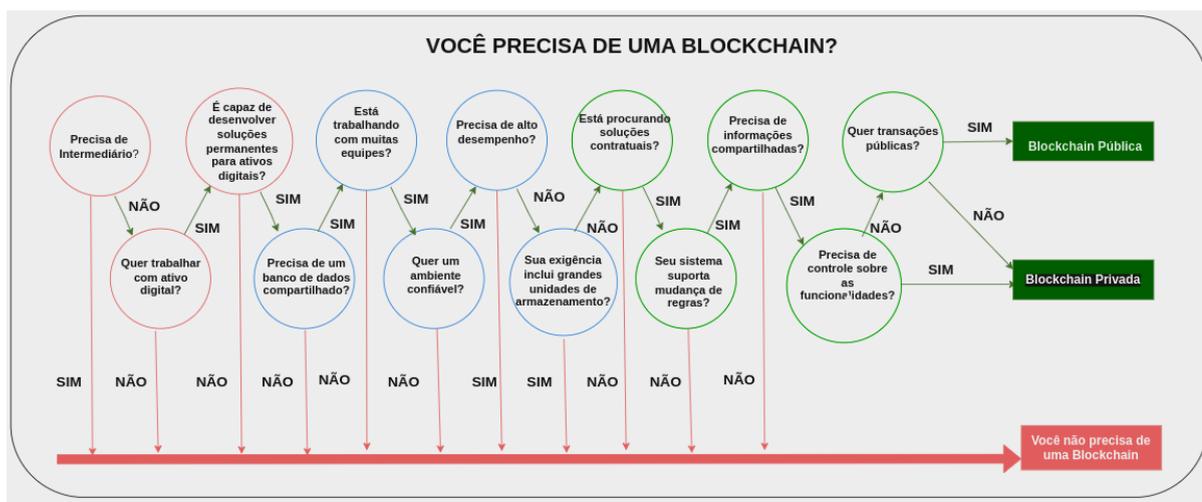


Figura 4.1 Questionamentos para sistemas Candidatos a aplicação de Blockchain (Elaboração Própria, 2023)

4.2 METODOLOGIA

O problema de pesquisa foi identificado durante entrevistas com a gestão farmacêutica do município de Salvador. Visto que as solicitações de fármacos por via judicial apresentam frágil controle e gerenciamento entre as secretarias de saúde e os órgãos judiciais, a tecnologia *blockchain* foi entendida como ideal por suas características para atender a demanda dessa integração. Por meio de revisão bibliográfica buscou-se identificar trabalhos já desenvolvidos ou em curso abordando o tema, entretanto, nenhum abrangeu a demanda apresentada.

Confirmando a viabilidade para o desenvolvimento, foi realizada a análise de requisitos mediante um questionário apresentado no Apêndice A.1 e da história contada pelo gestor farmacêutico com o apoio do analista de processos de negócios. Foram mapeadas as regras de negócio vistas no Apêndice A.2, validadas com o corpo gerencial. Após detalhamentos das rotinas, o sistema foi desenvolvido seguindo o cronograma do Apêndice A.3 e as entregas cíclicas dos itens consoante o pacote de atividades visto no Apêndice A.4.

Na implementação foram disponibilizadas a rede *blockchain* e uma aplicação para as operações dos usuários. Inicialmente a rede foi experimentada em ambiente simulado em

computador pessoal, em seguida, feita a implantação em máquinas da secretaria de saúde do município de Salvador para realizar a prova de conceito. Foram convidados os usuários vinculados a rotina para testar o fluxo com o sistema *blockchain*. Os participantes da prova de conceito foram o gestor farmacêutico, o analista de processos e o analista de sistemas da secretaria de saúde do município.

Na validação foram utilizados 15 petições obtidas no portal de dados abertos do Tribunal de Justiça do Estado da Bahia. Foram avaliadas as operações de cadastro e movimentação do processo, acompanhamento pelo paciente, painel com gráficos e dados gerenciais e auditoria.

Os dados sensíveis ou pessoais do cidadão requerente não são utilizados no sistema *blockchain*, apenas o identificador do processo aberto no órgão judicial serve como chave para as transações, logo, o sistema *blockchain* desenvolvido permaneceu conforme a Lei Geral de Proteção de Dados Pessoais (LGPD). Apesar de ser um problema identificado na cidade de Salvador, a questão é nacional e a implementação pode abarcar outros municípios que possuam interesse.

4.3 FLUXO DO PROCESSO JUDICIAL NA REDE

Para desenvolvimento do sistema foi utilizado o framework Hyperledger Fabric (ANDROULAKI et al., 2018) onde todos os *peers* são clientes e servidores, não possibilitando desta forma a centralização das informações em nenhuma instituição. O controle entre as entidades ocorre sem qualquer tipo de hierarquia tecnológica ou institucional, obedecendo apenas às regras do negócio presentes no contrato inteligente que no Hyperledger Fabric é chamado de *chaincode*. Os *scripts* e artefatos da rede foram gerados através da ferramenta Minifabric (LODI et al., 2021) e dentre eles encontra-se a configuração das organizações, arquivos de conexão e materiais criptográficos que são as credenciais de acesso para cada nó na rede. Através da execução dos *scripts* ocorre a criação e configuração da rede com todos os artefatos necessários.

No fluxo do processo judicial apresentado na Figura 4.2 o paciente se desloca até a unidade de saúde em busca do fármaco, caso encontre, será atendido pela farmácia da unidade, caso não, ele se dirige até o órgão judicial com o intuito de abrir uma solicitação, o que determina o início da interação com a *Blockchain* JudMed. Ao receber o paciente, o órgão judicial verifica o relatório médico e abre a requisição, enviando o processo a *blockchain* e tornando-o um ativo digital para a rede, acessível às organizações públicas do consórcio. Com o processo aberto, o paciente vai até uma das secretarias que então verifica-o na *blockchain* e abre a solicitação de compra do remédio. Todas as operações são enviadas para a JudMed e o paciente acompanha todas as movimentações até a chegada do fármaco para a retirada. Todo o fluxo pode ser acompanhado pelos gestores e pelo paciente, o que traz ganhos de transparência na gestão do serviço público.

4.4 CONSENSO E ORDENAÇÃO COM RAFT

O algoritmo **Raft** implementado na JudMed é o padrão adotado pelo Hyperledger Fabric a partir da versão 1.4. Ele é confiável, replicado, redundante e tolerante a falhas ou *Crash*

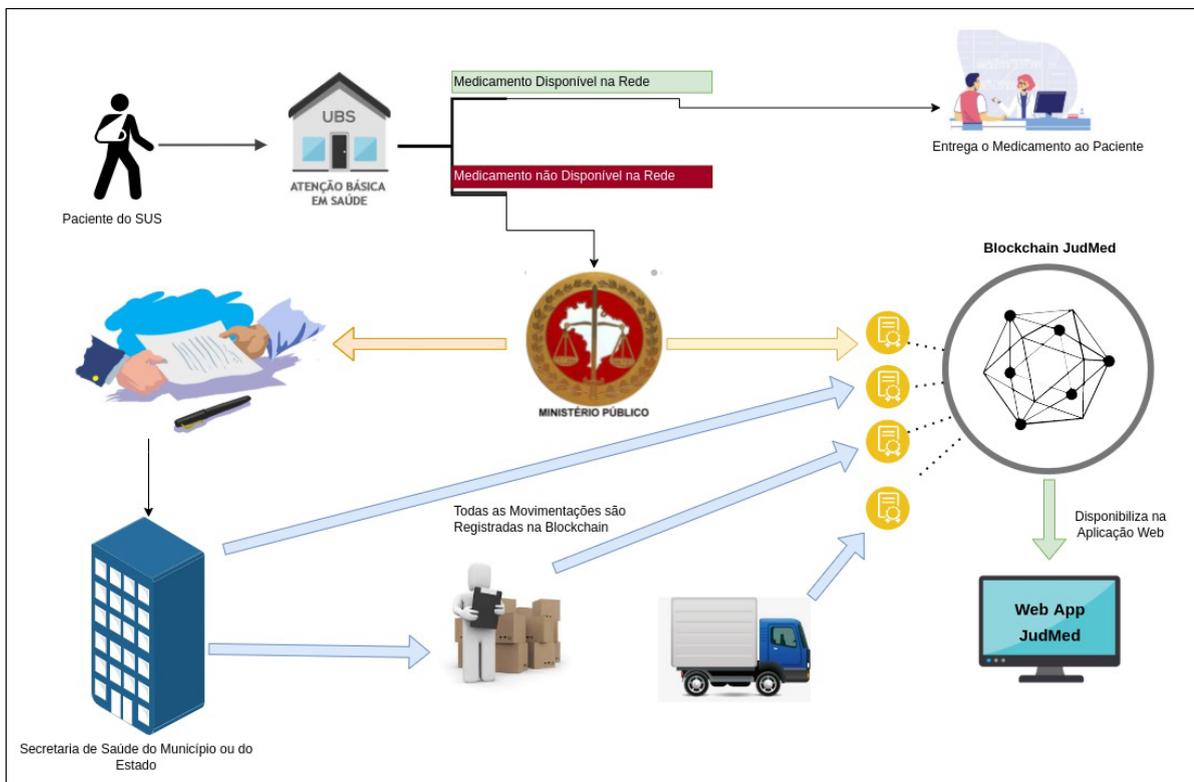


Figura 4.2 Big Picture com o resultado da aplicação da solução (Elaboração Própria, 2021)

Fault Tolerant (CFT). O protocolo é utilizado em sistemas distribuídos para gerenciar e manter a consistência do log que registra as mensagens replicadas entre os nós da rede (HU; LIU, 2020). Na JudMed, existe um nó ordenador em cada uma das organizações formando o conjunto do consenso. De forma global, cada nó ordenador, esteja ele em uma das secretarias de saúde ou no órgão judicial, mantém uma máquina de estado finito (FSM) (HU; LIU, 2020) que recebe entradas no log que é avaliado coletivamente, garantindo que a sequência esteja consistente em todos os nós. Para funcionar é necessário que a maioria dos nós esteja em funcionamento, no caso da *blockchain* JudMed com três organizações inicialmente, ao menos duas precisam estar ativas. Quando um processo judicial é movimentado, todas as organizações verificam se a assinatura da transação é do autor que de fato a criou, então todos endossam e confirmam o processo em seu banco de dados e *blockchain* locais.

4.5 CANAL, LEDGER E TRANSAÇÕES

O processo aberto no órgão judicial é o ativo controlado no *ledger* ou livro razão, onde constam todas as transações de criação e movimentação do processo. O canal compartilhado entre as instituições funciona como o consórcio onde apenas os participantes permitidos operam no *ledger*. A visão unificada e privada dos dados entre as organizações também é assegurada pelo canal. Cada movimento é registrado e comunicado a todas as partes, possibilitando posterior auditoria. As operações são disponibilizadas e controladas pelo contrato inteligente (ZHENG et al., 2017) através das permissões específicas para cada integrante, como exemplo a abertura da petição judicial que só pode ser realizada pelo órgão judicial, tal qual a solicitação do medicamento por uma das secretarias de saúde. O *chaincode* que contém as operações foi desenvolvido na linguagem Node.js (HAHN, 2016).

4.6 ACESSO SEGURO

O mecanismo de chaves criptográficas assimétricas (uma chave pública e uma privada) utilizadas para codificar e decodificar a mensagem torna o acesso à rede seguro. As chaves são geradas pelo próprio Hyperledger Fabric CA utilizado como autoridade certificadora em cada organização. Todas as secretarias e o órgão judicial possuem a chave pública de todos os participantes, logo, quando um processo é movimentado ele é assinado com a chave privada do autor e checado por cada organização, porquanto todos possuem a chave pública do autor para decodificar a mensagem e assim fazer o endosso da transação.

As informações pessoais não são armazenadas na JudMed, elas continuam sob guarda das instituições públicas e nenhum dado sensível é persistido e exibido na *blockchain*. Caso a informação precise ser retirada nos sistemas institucionais, estas são excluídas do estado global da *blockchain* que funciona como um banco de dados, não sendo mais operável. O dado excluído é exibido apenas para o órgão judicial quando em auditoria, onde a busca é realizada diretamente nos blocos encadeados das transações, na *blockchain*. Uma vez que a informação tenha sido excluída do sistema das organizações públicas, a chave mantida na *blockchain* não reportará a nenhum paciente, desta forma não infringe

a Lei Geral de Proteção de Dados (OLIVEIRA; HERBELLA, 2020).

4.7 ARQUITETURA

Para realizar a entrada das instituições e o ingresso ao canal, os seguintes componentes de software são instalados:

1. Contêineres com imagens docker contendo os recursos e configurações da rede;
2. Contrato Inteligente ou *Chaincode*;
3. *Ledger* (Estado Global e Blockchain);
4. Nó ordenador com o protocolo Raft;
5. API Rest para operações no *ledger*;
6. Aplicação Web JudMed para utilização da API Rest e fazer a interface das operações para o usuário.

A Figura 4.3 mostra o diagrama de sequência com o fluxo da operação de solicitação de medicamento mediante abertura de um novo processo. O início do ciclo de vida na *blockchain* JudMed ocorre quando um operador cadastra o processo através da aplicação web no órgão judicial, esse registro é enviado pela interface (API Rest) que logo faz a chamada ao controlador (*chaincode*) e então se a transação estiver consistente o processo é efetivado e distribuído como um ativo digital da rede.

4.8 OPERAÇÕES, CÓDIGOS E COMANDOS NA REDE EM AMBIENTE SIMULADO

4.8.1 Inicialização dos Nós da Rede com o Minifabric

1. Após configuração do arquivo `spec.yaml` apresentado na Figura 4.4. O comando abaixo inicia a rede na máquina hospedeira criando os nós da Secretaria Municipal de Saúde e do Ministério Público:

```
[ ./minifab up -o sms.ba.gov.br -e 7050 -s couchdb -n chaincodejudmed -l node -p ];
```

2. A Secretaria Estadual de Saúde é iniciada na máquina virtual configurando o arquivo `spec.yaml` visto na Figura 4.5, executando:

```
[ ./minifab netup -o sesab.com.br ];
```

3. Após inicialização da Secretaria de Saúde do Município no *host*, é gerado o arquivo de configuração do canal para incluir a organização Secretaria de Saúde do Estado, executando:

```
[ ./minifab channelquery ];
```

Diagrama de Sequência - Solicitação de Medicamento Judicial

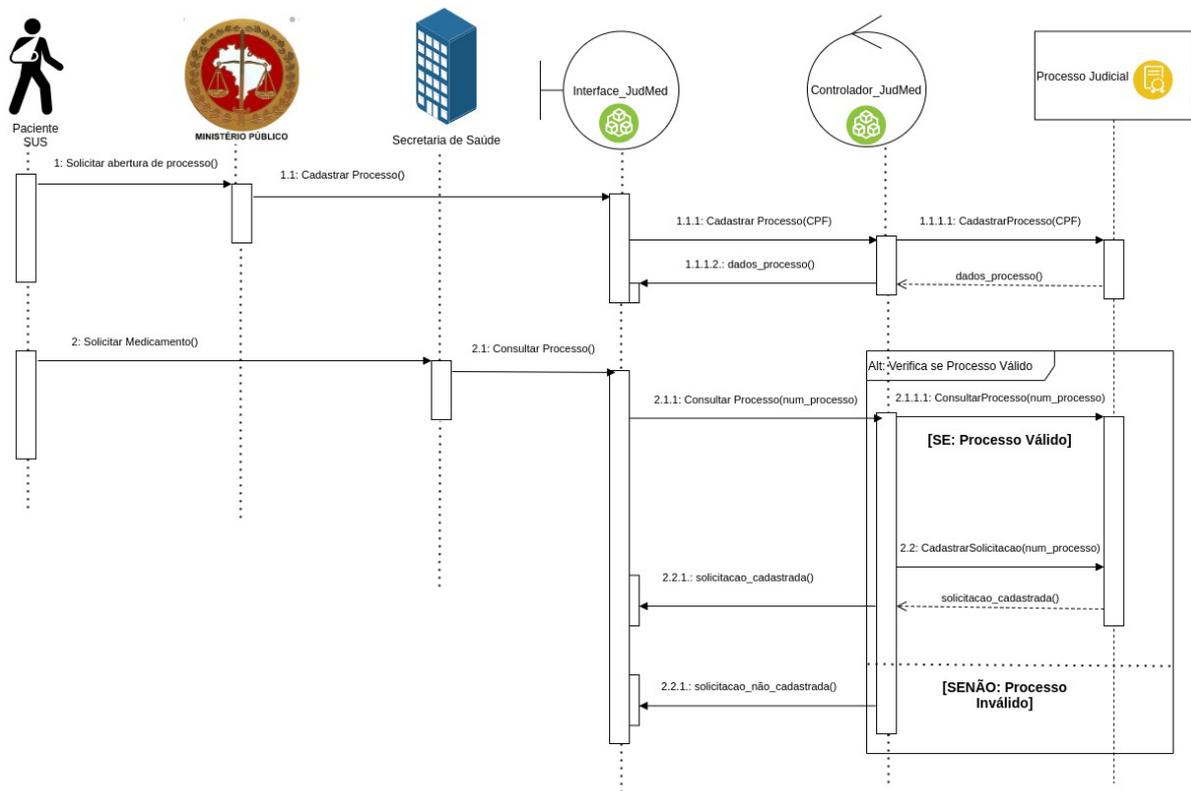


Figura 4.3 Diagrama de Sequência - Solicitação de Medicamento Judicial (Elaboração própria, 2021)

4. No *host* da Secretaria de Saúde do Estado após obter o arquivo **JoinResquestOrg-Join** enviamos para inclusão do conteúdo no arquivo de configuração do canal da rede no *host* na Secretaria Municipal de Saúde, em seguida é executado o seguinte comando para a entrada da Secretaria de Saúde do Estado no consórcio:

```
[ ./minifab orgjoin ];
```

5. Após atualização do arquivo de configuração do canal no *host* Secretaria Municipal de Saúde e Ministério Público, o canal é atualizado para fazer a descoberta da nova organização como segue:

```
[ minifab channelsign,channelupdate,discover ];
```

6. Para concluir, a entrada da Secretaria de Saúde do Estado é feito o envio do arquivo *endpoints* para o *host* da Secretaria de Saúde do Estado e executado os comandos na própria organização:

```
[ ./minifab approve, discover, commit;]
```

```
fabric:
  cas:
    - "ca1.sms.ba.gov.br"
  peers:
    - "peer1.sms.ba.gov.br"
    - "peer1.mp.ba.gov.br"
  orderers:
    - "orderer1.smsorderer.ba.gov.br"
  settings:
    ca:
      FABRIC_LOGGING_SPEC: DEBUG
    peer:
      FABRIC_LOGGING_SPEC: DEBUG
    orderer:
      FABRIC_LOGGING_SPEC: DEBUG
  netname: "ChainJudMedA"
  container_options: "--restart=always --log-opt max-size=10m --log-opt max-file=3"
```

Figura 4.4 Arquivo Spec.yaml para a Secretario Municipal de Saúde e Ministério Público (Elaboração Própria, 2021)

4.8.2 Inicialização da API Rest e da Aplicação Web

Na Figura 4.6 é exibida a rede em funcionamento nas máquinas hospedeira e virtual através dos terminais de comandos shell no Sistema Operacional Ubuntu. À esquerda da imagem encontra-se a máquina hospedeira, portanto as organizações Secretaria de Saúde

```
fabric:  
cas:  
- "ca1.sesab.com.br"  
peers:  
- "peer1.sesab.com.br"  
orderers:  
- "orderer1.sesaborderer.ba.gov.br"  
settings:  
  ca:  
    FABRIC_LOGGING_SPEC: DEBUG  
  peer:  
    FABRIC_LOGGING_SPEC: DEBUG  
  orderer:  
    FABRIC_LOGGING_SPEC: DEBUG  
netname: "ChainJudMedB"
```

Figura 4.5 Arquivo Spec.yaml para a Secretaria Estadual de Saúde (Elaboração Própria, 2021)

do Município e Ministério Público, logo abaixo está a API Rest aguardando requisições e ao lado o terminal com a execução da aplicação web JudMed. A direita está a máquina virtual com a organização Secretaria de Saúde do Estado.

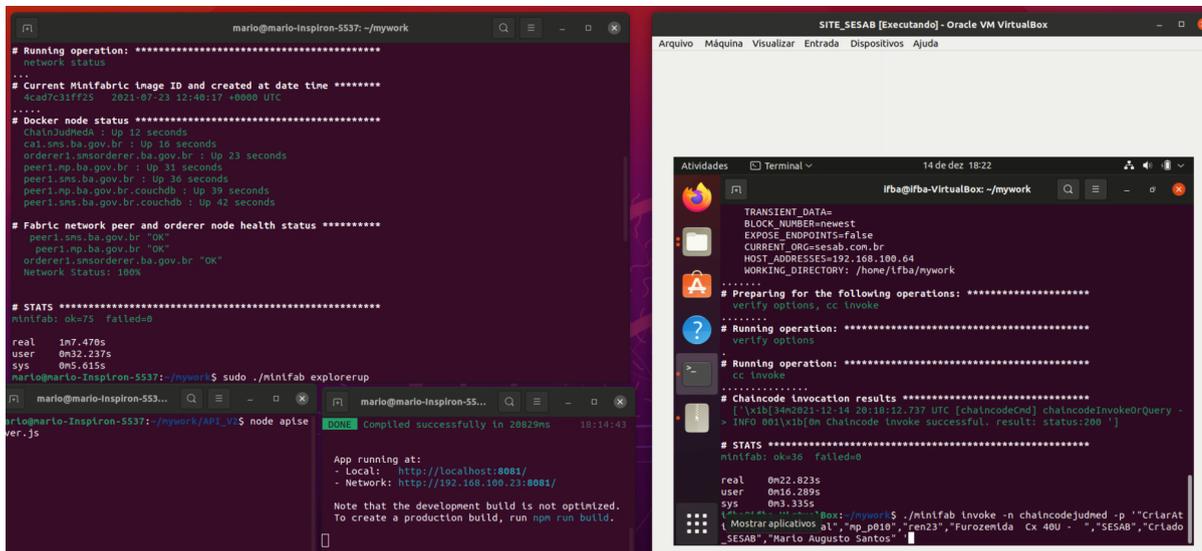


Figura 4.6 Rede Implantada nas Máquinas e Aplicações (Elaboração Própria, 2021)

4.8.3 Codificação Para Criar um Processo Judicial

O *chaincode* da Figura 4.7 demonstra o cadastro do ativo na *blockchain*. Antes da criação é verificado na **linha 53** se a petição já existe e na **linha 62** a qual organização o usuário pertence. Caso seja um novo processo e o usuário pertencente ao Ministério Público, ocorre a criação do ativo na **linha 69** e o envio a *blockchain* na **linha 77**.

A Figura 4.8 apresenta a chamada **Http Post** na API Web que acessa o *chaincode* e a função para a criação do ativo. Nas **linhas 110 e 111** é obtido o caminho da pasta no servidor que contém as credenciais do usuário utilizado pela API e logo após ocorre o acesso à função no *chaincode*. Das **linhas 121 a 123** acontece a conexão e o acesso ao canal. Na **linha 125** é feita a chamada da função de criação do ativo passando como parâmetros todos os campos captados no *body* ou corpo da requisição web.

4.8.4 Aplicação Web JudMed

A aplicação web JudMed foi desenvolvida em **Node.js** no *back-end* e no *front-end* em *Vue.js*. As transações são enviadas ao *chaincode* mediante requisições a API que está no *web server Express.js* publicado no servidor da instituição a qual foi implantada. Para fazer a conexão da API ao *chaincode* foi criado um usuário pertencente a cada organização. Foram desenvolvidas as telas de cadastro de processo judicial, movimentação, acompanhamento, auditoria e *Dashboard* gerencial. Na aplicação web são validados os campos de preenchimento obrigatório verificados em *client-side*. Todas as validações de

```

50 async CriarAtivoProcessoJudicial(ctx, id, numRename, nomeComercialMedicamento, instancia, status) {
51
52   const exists = await this.AssetExists(ctx, id);
53   if (exists) {
54     console.log('O processo de número ' + id + ' já foi cadastrado e não pode ser repetido. ');
55     throw new Error('O processo de número ${id} já foi cadastrado e não pode ser repetido. ');
56     return;
57   }
58
59   const cid = ctx.clientIdentity;
60   let MSPID_ORIGEM = cid.getMSPID();
61
62   if (MSPID_ORIGEM !== 'mp-ba-gov-br') {
63     console.log('Usuário você pertence a organização ' + MSPID_ORIGEM + ' apenas usuários do Ministério Público podem cadastrar um processo judicial. ');
64     throw new Error('Usuário você pertence a organização ${MSPID_ORIGEM} apenas usuários do Ministério Público podem cadastrar um processo judicial. ');
65     return;
66   }
67
68   else {
69     const asset = {
70       ID: id,
71       NumRename: numRename,
72       NomeComercialMedicamento: nomeComercialMedicamento,
73       Instancia: instancia,
74       Status: status,
75     };
76
77     ctx.stub.putState(id, Buffer.from(JSON.stringify(asset)));
78     return JSON.stringify(asset);
79   }
80 }

```

Figura 4.7 Cadastro do Processo Judicial - *Chaincode* (Elaboração Própria, 2021)

```

105 app.post('/api/CadastrarProcessoJudicial/', async function (req, res) {
106   try {
107
108     let ccp = JSON.parse(fs.readFileSync(ccpPath, 'utf8'));
109
110     const walletPath = path.join('/home/mario/mywork/API/wallets/', 'sms.ba.gov.br');
111     const wallet = await Wallets.newFileSystemWallet(walletPath);
112     console.log('Wallet path: ${walletPath}');
113
114     const identity = await wallet.get('Admin');
115     if (!identity) {
116       console.log('An identity for the user does not exist in the wallet');
117       return;
118     }
119
120     const gateway = new Gateway();
121     await gateway.connect(ccp, { wallet, identity: 'Admin', discovery: { enabled: true, asLocalhost: true } });
122
123     const network = await gateway.getNetwork('mychannel');
124
125     const contract = network.getContract('chaincodejudmed');
126
127     await contract.submitTransaction('CriarAtivoProcessoJudicial', req.body.id, req.body.numRename,
128                                     req.body.nomeComercialMedicamento, req.body.instancia, req.body.status);
129
130     res.send('Transaction has been submitted');
131
132     await gateway.disconnect();
133
134   } catch (error) {
135     console.error('Falha ao submeter transação: ${error}');
136     res.status(500).json({error: error});
137   }

```

Figura 4.8 Cadastro do Processo Judicial - POST/API (Elaboração Própria, 2021)

regras de negócio são executadas no *chaincode* com retornos de sucesso ou de erro ao submeter as transações.

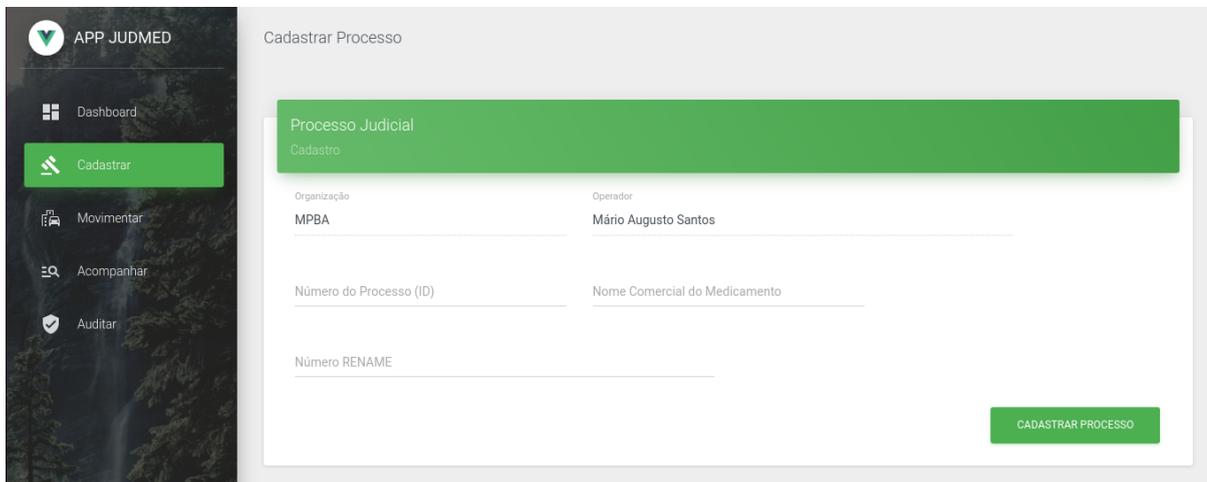


Figura 4.9 Apresentação Aplicação JudMed (Elaboração Própria, 2021)

4.9 TESTES DE FUNCIONALIDADE

Foram testados através da criação e implantação da rede *blockchain* em ambiente simulado: consórcio privado e respectivo ingresso permissionado, validação de transações, papéis das organizações, consenso para validar o envio e tornar persistente as informações e recuperação de dados para auditoria.

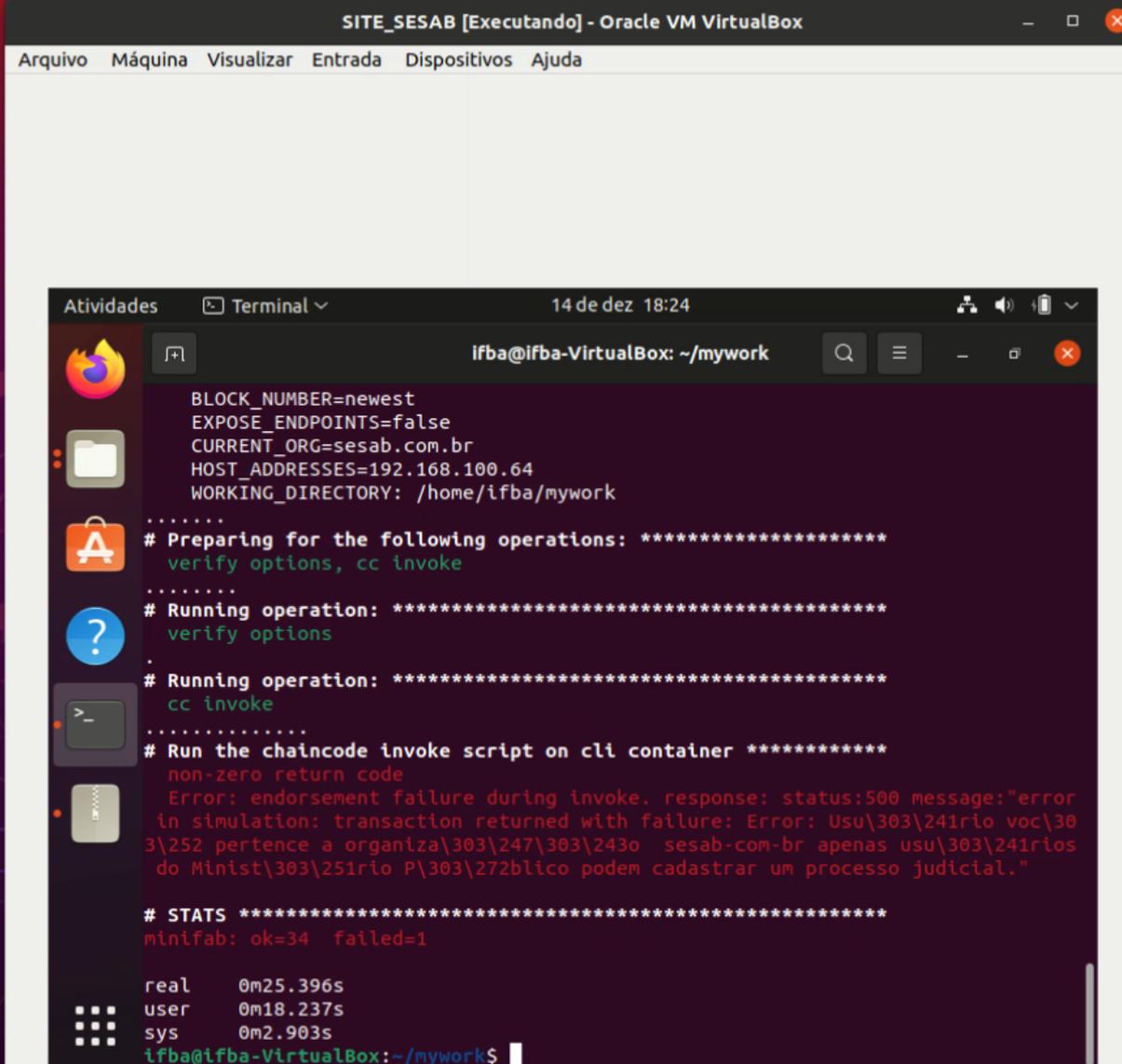
Os testes no *chaincode* ocorreram em duas máquinas, uma hospedeira e uma virtual. No host físico foram configuradas as organizações Ministério Público e Secretaria de Saúde do Município e na máquina virtual a Secretaria de Saúde do Estado. Após iniciar a rede em ambas as máquinas foram testadas as funções do *chaincode* com as regras de negócio que norteiam a relação entre as entidades e o paciente do Sistema Único de Saúde (SUS). As informações trafegadas foram visualizadas e validadas em todos os nós da rede. Nas subseções seguintes são demonstradas a configuração do ambiente e o detalhamento das validações das regras apresentando o resultado de suas execuções.

4.9.1 Ambiente

A configuração da máquina hospedeira foi: 6 Gb de Memória RAM, 1 Tb de armazenamento e Processador Core I5. A máquina virtual foi criada com a ferramenta Oracle VM Virtualbox com a configuração de 1,5 Gb de Memória RAM, placa de rede em modo *bridge* e 40 Gb de armazenamento. O Sistema operacional utilizado nas máquinas foi o Linux Ubuntu na versão 21.04.

4.9.2 Teste 1: Tentativa de Criação de Processo sem ser o Ministério Público

A primeira validação é a de criação de um processo não sendo usuário do Ministério Público, o teste é realizado na máquina virtual onde foi implantada a organização Secretaria de Saúde do Estado, obtendo um erro apresentado na Figura 4.10.



```
SITE_SESAB [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

Atividades Terminal 14 de dez 18:24
ifba@ifba-VirtualBox: ~/mywork

BLOCK_NUMBER=newest
EXPOSE_ENDPOINTS=false
CURRENT_ORG=sesab.com.br
HOST_ADDRESSES=192.168.100.64
WORKING_DIRECTORY: /home/ifba/mywork
.....
# Preparing for the following operations: *****
verify options, cc invoke
.....
# Running operation: *****
verify options
.
# Running operation: *****
cc invoke
.....
# Run the chaincode invoke script on cli container *****
non-zero return code
Error: endorsement failure during invoke. response: status:500 message:"error
in simulation: transaction returned with failure: Error: Usu\303\241rio voc\30
3\252 pertence a organiza\303\247\303\243o sesab-com-br apenas usu\303\241rios
do Minist\303\251rio P\303\272blico podem cadastrar um processo judicial."

# STATS *****
minifab: ok=34 failed=1

real    0m25.396s
user    0m18.237s
sys     0m2.903s
ifba@ifba-VirtualBox:~/mywork$
```

Figura 4.10 Tela de erro de cadastro de processo não sendo usuário do Ministério Público (Elaboração Própria, 2021)

4.9.3 Teste 2: Tentativa de Criação de Processo Duplicado

Na tela de cadastro na Figura 4.11 é informado um processo já existente obtendo a resposta de erro, evitando assim que o processo seja duplicado. Em seguida na Figura

4.12 é informado um novo processo válido, obtendo êxito na criação.

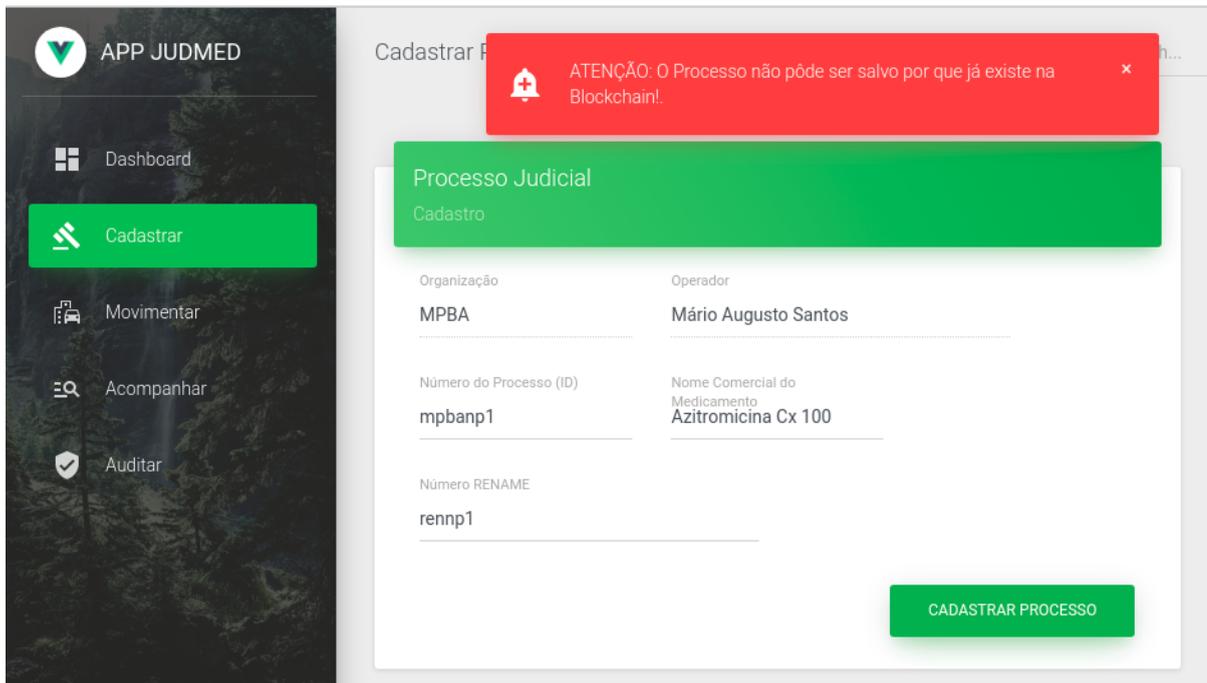


Figura 4.11 Tela de erro de cadastro processo duplicado (Elaboração própria, 2021)

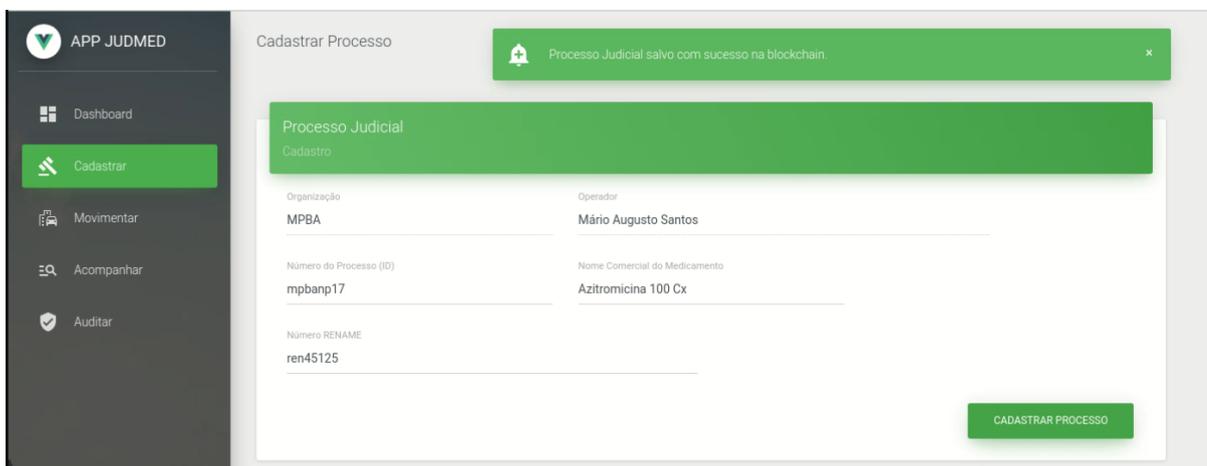


Figura 4.12 Tela de cadastro de processo com sucesso - (Elaboração Própria, 2021)

4.9.4 Teste 3: Movimentação de Processo entre as organizações

Na tela de movimentação na Figura 4.13 é informado um processo criado no órgão Judicial para a próxima movimentação, como exemplo, Solicitado na Secretaria Municipal de

Saúde, logo, esta organização assume o fluxo da compra a entrega ao paciente do SUS.

APP JUDMED

Movimentar Processo

Processo Judicial
Movimentar Processo Judicial

Número do Processo (ID)
mpbanp17

PESQUISAR PROCESSO

Nome Comercial do Medicamento
Azitromicina 100 Cx

Número RENAME
ren45125

Status Atual
Solicitado_SMS

Organização Atual
MPBA

Organização Movimentação
SMS

Operador
Mário Augusto Santos

Novo Status do Processo
Solicitado na Secretaria Municipal de Saude

MOVIMENTAR PROCESSO

Figura 4.13 Tela de Movimentação de processo - (Elaboração Própria, 2021)

4.9.5 Teste 4: Acompanhamento pelo Paciente do SUS

A partir do *peer* presente na Secretaria Municipal de Saúde e instanciado na máquina hospedeira, a pesquisa é realizada na tela de acompanhamento e apresentada na Figura 4.14 onde é informado o status atual do pleito a partir do número identificador no Ministério Público sem exibir nenhum dado pessoal ou sensível do paciente. No exemplo da imagem, o paciente tem ciência que sua solicitação está na fase de compra do fármaco pela Secretaria a qual ele se dirigiu.

4.9.6 Teste 5: Auditoria de um Processo Judicial

Na máquina hospedeira que representa o Ministério Público e a Secretaria de Saúde do Município é verificada na tela de auditoria todos os lançamentos realizados para o processo judicial fictício de identificador "mpbanp1", fornecendo toda a rastreabilidade ao Ministério Público.

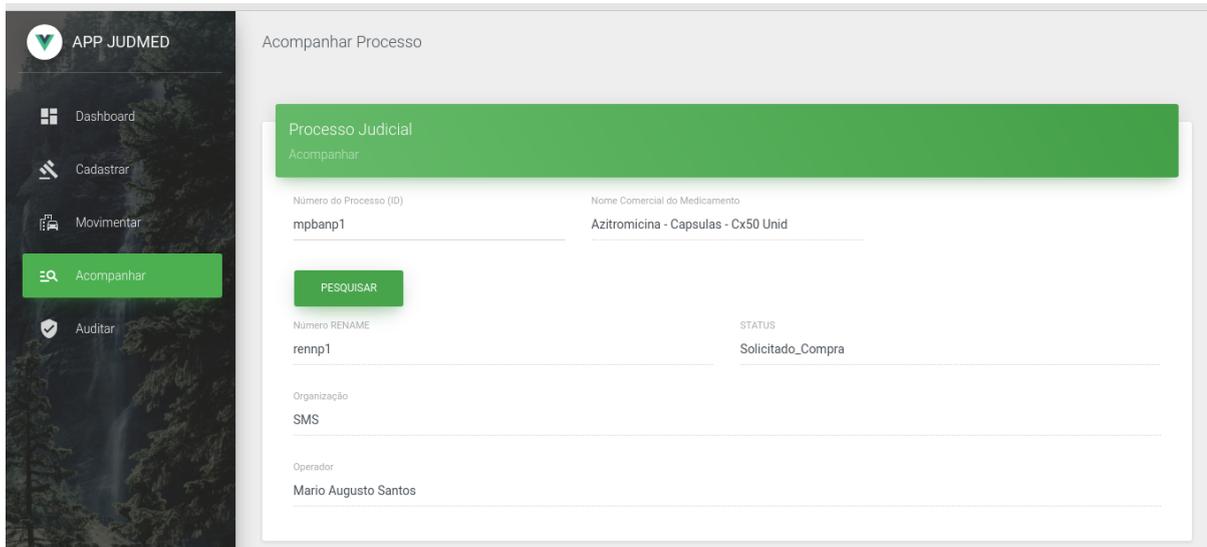


Figura 4.14 Tela de acompanhamento para o paciente dos SUS - (Elaboração Própria, 2021)

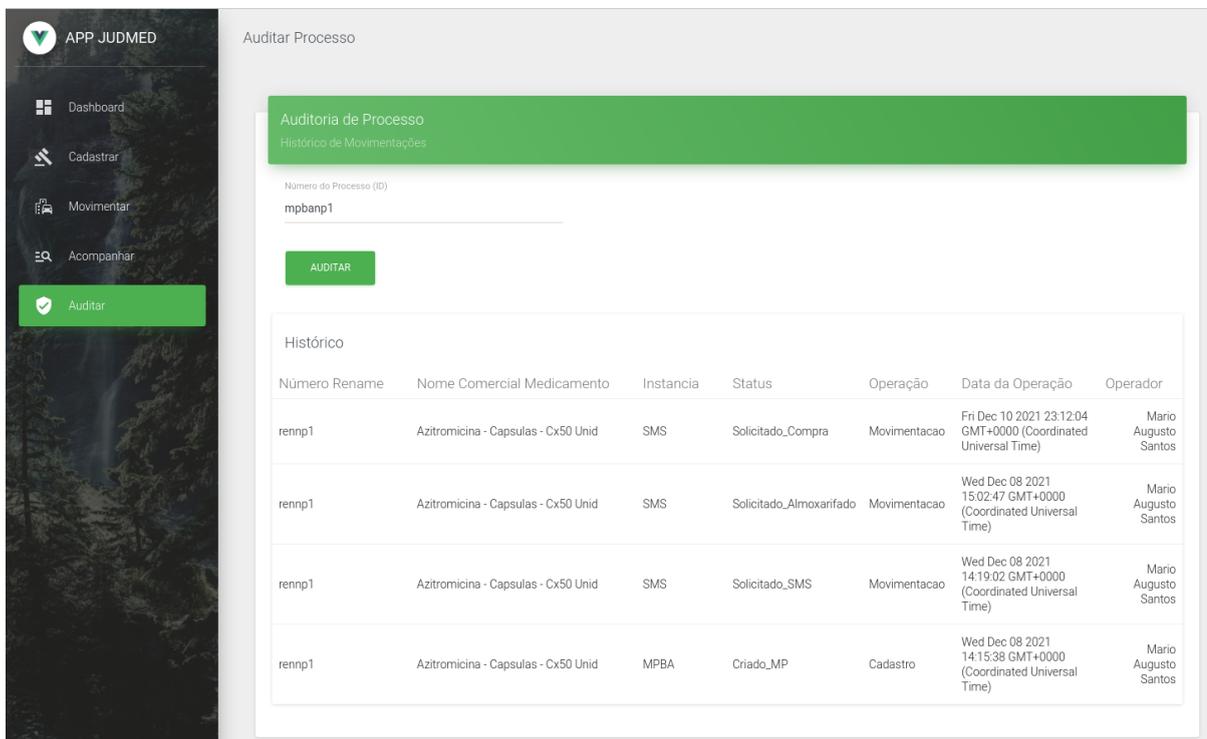


Figura 4.15 Tela de Auditoria (Elaboração Própria, 2021)

4.9.7 Teste 6: Dashboard Gerencial

O *Dashboard* gerencial demonstrado na Figura 4.16 exibiu os medicamentos mais solicitados na rede, o total financeiro movimentado, o total de petições abertas e o número pendentes de conclusão. Esses dados iniciais podem ajudar no planejamento e na execução do serviço de forma integrada entre os órgãos públicos.

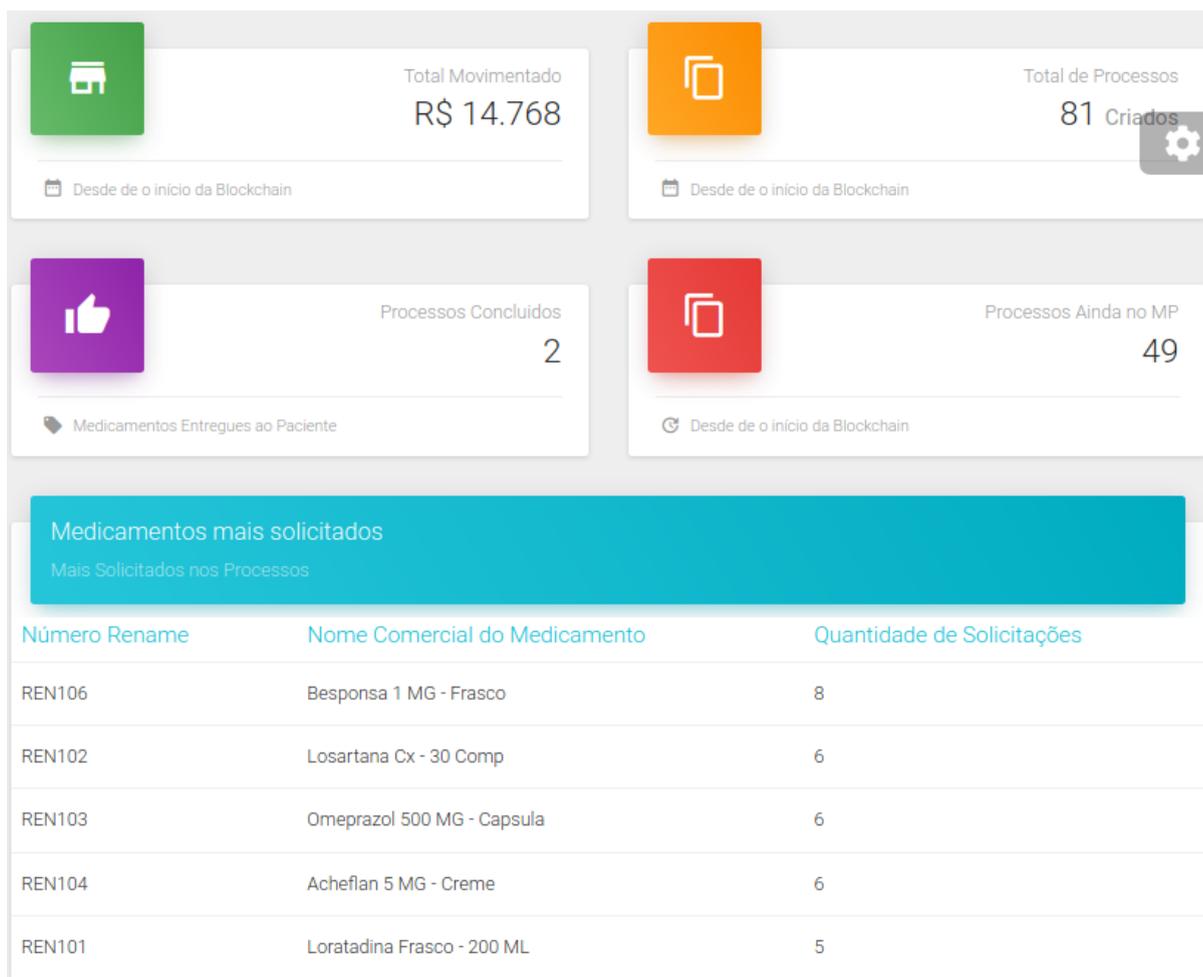


Figura 4.16 Tela de Dashboard (Elaboração Própria, 2021)

4.10 RESULTADOS DA IMPLEMENTAÇÃO

Após configuração dos arquivos `spec.yaml` de forma simplificada nas máquinas, ocorreu a execução da inicialização da rede com o **Minifabric**, ativando todos os **containers docker** em um total de **1 minuto e 40 segundos** em cada **host**, deixando a rede operacional, é possível que este tempo seja otimizado em um ambiente de execução com configuração mais robusta. Durante a inicialização foram gerados os arquivos e *scripts*

necessários para operacionalizar a rede, como a configuração do canal e o material criptográfico de cada organização.

De forma prática e organizada, tudo ficou disposto no diretório de trabalho **mywork**. Após iniciar a rede, foram necessários executar manualmente os seguintes passos: colocar as organizações em um mesmo canal, configurar no canal da rede as informações do *host* da Secretaria de Saúde do Estado, descoberta e aprovação da nova entidade, permissões de leitura, escrita e aprovação de transações. Todo fluxo posterior a criação dos nós da rede foi manual, realizando comandos ou trocando arquivos entre as organizações como visto anteriormente e **esse aspecto pode ser melhorado futuramente reduzindo as etapas manuais** e agilizando a entrada de novas organizações.

Na petição judicial gerenciada na *blockchain*, constou o número no Ministério Público, os dados relacionados ao medicamento e as informações sobre a movimentação do ativo sem armazenar nem expor dados sensíveis do paciente. Houve o controle sobre quem pôde acessar e executar cada função, o que demonstrou a eficácia do *chaincode*, chamado pela API e executado pela aplicação web. Ao verificar a existência de um mesmo processo judicial na *blockchain* foi evitada a duplicidade, impedindo nova solicitação.

As transações submetidas levaram em média **5 segundos para serem confirmadas após o consenso** com o protocolo **Raft**, o que pode ser otimizado quando implantada em máquina servidora com mais recursos de infraestrutura. Para a auditoria foi executada a função de busca, recuperando todas as informações do pleito judicial auditado e para o paciente do SUS a tela de acompanhamento trouxe o estado atual da petição.

No *Dashboard* inicial foram disponibilizadas informações gerenciais como medicamentos mais solicitados, total financeiro movimentado, processos abertos e pendentes, auxiliando ao gestor com uma visão gerencial da rede.

4.11 IMPLANTAÇÃO DA BLOCKCHAIN JUDMED

Para implantar a rede em cada organização é previsto um servidor preferencialmente com o sistema operacional Linux Ubuntu em versão igual ou superior a 20, podendo ser implantado em máquina física ou virtual. São instalados os seguintes softwares: Hyperledger Fabric e Minifabric, Docker e servidor web Express.Js. Nos contêineres docker estão os *peers* que fazem a comunicação e operações na rede, os blocos de transação contendo os *ledges* e o banco de dados CouchDB. No servidor web Node Express.Js são implantados a API e aplicação web JudMed. Com o número do processo o paciente do SUS acessa o sistema JudMed pelo navegador web. Na Figura 4.17 é apresentado o diagrama de implantação.

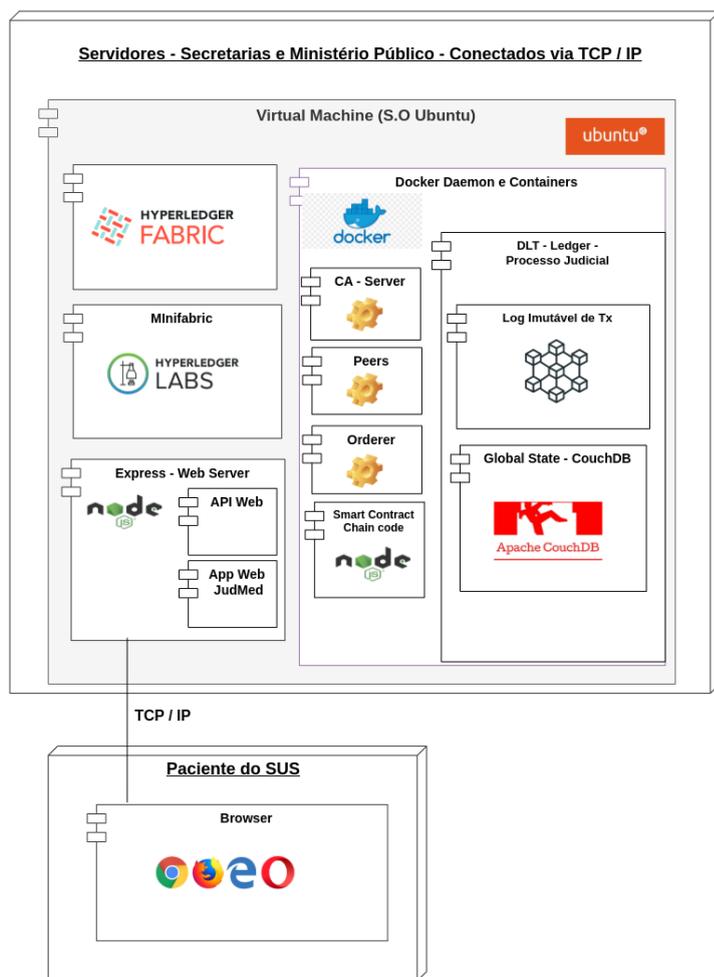


Figura 4.17 Diagrama de Implantação (Elaboração Própria, 2021)

Capítulo 5

Neste capítulo são apresentados a prova de conceito do produto com a área farmacêutica do município de Salvador, atores envolvidos e resultados da execução em ambiente simulado na Secretaria de Saúde de Salvador.

PROVA DE CONCEITO

A prova de conceito teve o intuito de checar junto a profissionais da área se os objetivos da criação deste produto foram atendidos. Foram avaliados a integração das organizações mediante consórcio privado, o banco de dados único e distribuído, a correta execução das regras de negócio através do contrato inteligente, a trilha de auditoria, o acompanhamento pelo paciente do SUS e o painel para a gestão do serviço.

Não foram testados aspectos técnicos da integração da rede entre as organizações públicas, ainda pela ausência de um acordo que possibilite os testes em cenário real, os referidos aspectos foram verificados em ambiente simulado apresentado na Seção 4.1 onde foi testada a rede da *blockchain* JudMed e apresentados os resultados dos testes de comunicação entre as máquinas que exerceram o papel de servidor em cada um dos integrantes do consórcio.

A rede *blockchain* foi iniciada no ambiente e depois foram utilizados quinze processos reais do portal de dados abertos do Tribunal de Justiça do Estado da Bahia.

Reproduzimos seu fluxo, validado por um gestor farmacêutico e o analista de negócios da gestão municipal de saúde pública de Salvador. Decorreram as seguintes validações: consórcio privado e respectiva entrada autorizada, transações para criação e movimentação de processos, papéis da organização, consenso para validar a submissão e tornar persistente a informação e recuperação de dados para auditoria.

Não houve armazenamento nem exposição de dados sensíveis do paciente. Foi verificado o controle de acesso para executar cada função em cada ambiente. Com a criação e visualização do ativo nos nós distribuídos foi verificada a eficácia do **chaincode** chamado pela API e executado pela aplicação web. Ao checar a existência do mesmo pleito judicial na *blockchain* pelo número do processo, foi evitada a duplicidade, impedindo um novo registro. A função de busca foi realizada para a auditoria, recuperando todas as informações do ativo auditado. Para o paciente do SUS, a tela de monitoramento inclusive, trouxe o estado atual da solicitação.

5.1 REALIZAÇÃO DOS PROCESSOS NA PROVA DE CONCEITO

Foram realizadas quatro rodadas de execução dos fluxos dos processos com os atores **Paciente do SUS**, **Secretaria de Saúde** e **Ministério Público**. Cada ator utilizou uma máquina específica que representou uma entidade pública do consórcio, da mesma forma, cada um com seu respectivo acesso a partir do seu **certificado digital** e suas **chaves criptográficas**, assim, foram testadas as atividades de cada um, mediante o seu perfil.

Os atores participantes possuem anos de experiência na área farmacêutica municipal, foram eles:

- **Coordenador de assistência farmacêutica do município** para a operação de entrada do processo na rede, auditoria e gestão do serviço, representando o órgão judicial (**Ator Ministério Público**);
- **Analista de Processo da área farmacêutica do município** para os papéis de operador de sistema responsável por movimentar o processo representando a secretaria de saúde (**Ator Secretaria de Saúde**);
- **Analista de Sistemas** para realizar a solicitação e acompanhar o processo judicial representando o paciente do SUS (**Ator Paciente do SUS**).

1. **Primeira rodada:** O ator Paciente do SUS solicitou abertura do processo judicial ao ator Ministério Público que então verificou através de uma busca na tela de cadastro de processos que se tratava de um novo pleito, efetivando assim o cadastro na blockchain com os dados informados e o ativo ficou com o Status de **Cadastrado no Órgão Judicial**. Com o processo instaurado na esfera judicial o ator Paciente do SUS solicitou o medicamento ao ator Secretaria de Saúde. O ator Secretaria de Saúde verificou na tela de movimentação se o processo já estava sendo atendido, e, constatando que se tratava de uma nova solicitação, mudou o status do ativo na blockchain para **Solicitado na Secretaria de Saúde** na tela de movimentações. Na sequência, foram realizadas as alterações de status: **Solicitado Almoxxarifado; Solicitado Compra; Disponível Retirada** representando o fluxo de atendimento pela Secretaria de Saúde. Após as movimentações do ator Secretaria Municipal o ator Paciente do SUS verificou o status atual do processo na tela de acompanhamento, identificando que o fármaco já estava **disponível para retirada** e solicitou o recebimento ao ator Secretaria Municipal que por fim atualizou o status final da blockchain para **Entregue ao Paciente**. Ainda na primeira rodada o ator Secretaria Municipal de Saúde tentou realizar o cadastro do ativo na rede, recebendo a mensagem na tela de cadastro que **não seria possível pois o usuário não pertencia a organização Ministério Público**.
2. **Segunda rodada:** O ator Paciente do SUS solicitou ao ator Secretaria de Saúde o mesmo processo da primeira rodada e foi constatado através de mensagem em tela que **o pedido já existia na blockchain e por tanto não poderia ser solicitado novamente**.

3. **Terceira rodada:** foram realizados novos cadastros de processos para o acompanhamento pelos atores nos painéis gerenciais onde foram vistos **o número de processos já atendidos, o número de processos que não foram movimentados e a lista de medicamentos mais solicitados.**
4. **Quarta rodada:** foi checado na tela de acompanhamento o **status atualizado dos processos movimentados nas rodadas um e dois**, verificado por todos os atores. Também na quarta rodada, foi visto a auditoria de alguns dos processos movimentados, **demonstrando toda a trilha dos ativos através da tela de auditoria.**

5.2 AVALIAÇÕES E PERCEPÇÕES FINAIS NA PROVA DE CONCEITO

1. Na perspectiva do coordenador farmacêutico do município de Salvador, a integração em tempo real entre as organizações públicas dará agilidade e segurança ao processo que antes ocorria por contato telefônico;
2. Uma visão unificada das informações com indicadores para os gestores facilita as tomadas de decisão para a melhoria do serviço, como exemplo a indicação para entrada de fármacos na lista RENAME (Relação Nacional de Medicamentos Essenciais), evitando desta forma futuros processos judiciais;
3. Identificação em tempo hábil dos possíveis gargalos de atendimento aos cidadãos em fila de espera acima de um prazo médio estipulado para atendimento, respeitando o tempo de execução da logística de aquisição do fármaco;
4. A quantidade de dados foi entendida como baixa ao nível de armazenamento e processamento na rede, não demandando outros investimentos em equipamento de infraestrutura computacional dos servidores;
5. A não identificação direta do paciente foi entendida como necessária para manter a privacidade do paciente cidadão;
6. A possibilidade de futura integração com o aplicativo Vida+ Cidadão que fornece informações relacionadas a saúde do paciente do SUS residentes em Salvador/Bahia.

Mesmo com a percepção de um sistema de cadastro de informações tradicional, a compreensão dos participantes foi que os aspectos da integração, da segurança, da agilidade e da privacidade dos dados em uma rede privada entre as organizações traz grandes benefícios a esse fluxo de atendimento. Foi dito que para viabilizar a integração em produção será necessário ter um Mínimo Produto Viável e apresentar aos outros órgãos públicos, e se de acordo, treinar em blockchain as equipes de tecnologia da informação e estruturar a implantação da rede em cada nó.

A seguir são apresentados os diagramas dos processos relacionados aos fluxos na blockchain que serviram como bases para o passo a passo da prova de conceito.

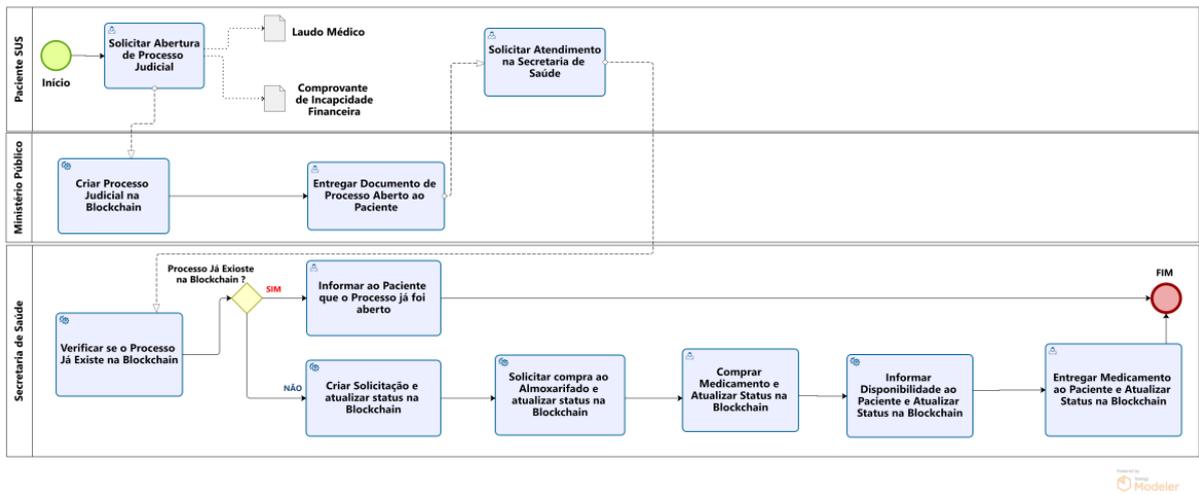


Figura 5.1 Fluxo do Processo de Cadastro do Ativo Na Prova de Conceito (Elaboração Própria, 2023)

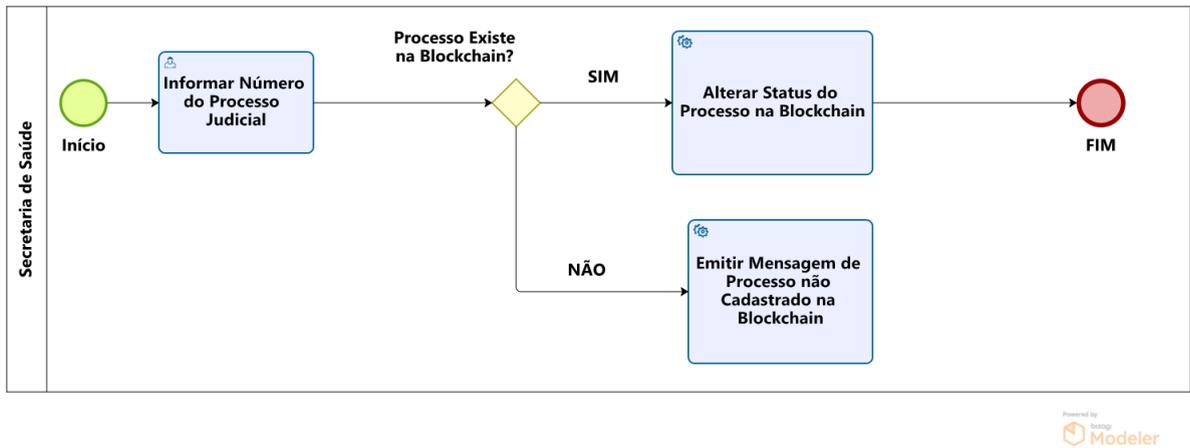


Figura 5.2 Fluxo do Processo de Movimentação do Ativo Na Prova de Conceito (Elaboração Própria, 2023)

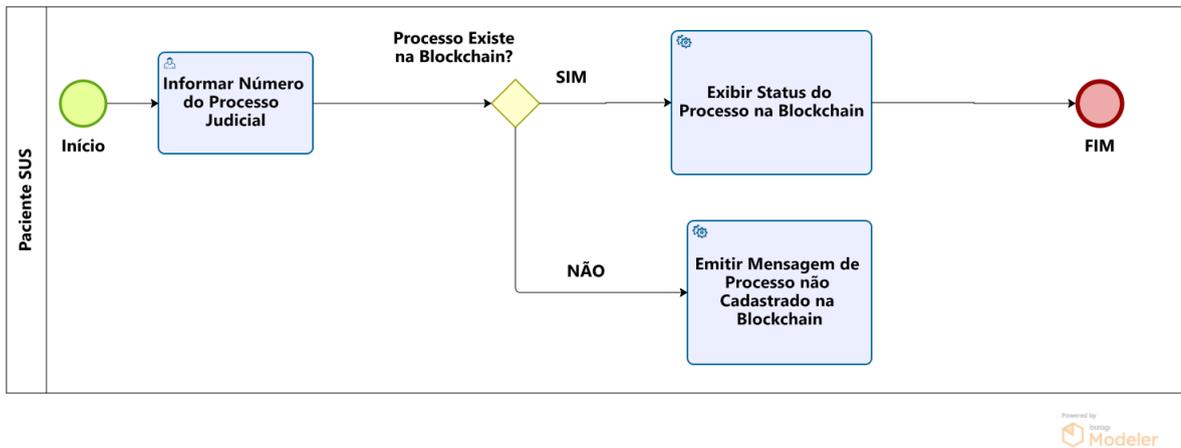


Figura 5.3 Fluxo do Processo de Acompanhamento do Ativo Na Prova de Conceito (Elaboração Própria, 2023)

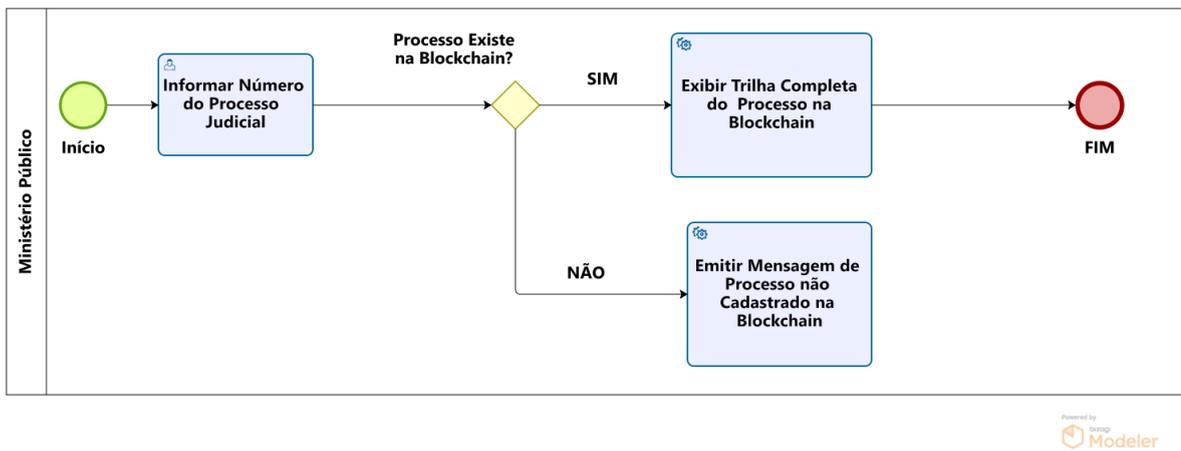


Figura 5.4 Fluxo do Processo de Auditoria do Ativo Na Prova de Conceito (Elaboração Própria, 2023)

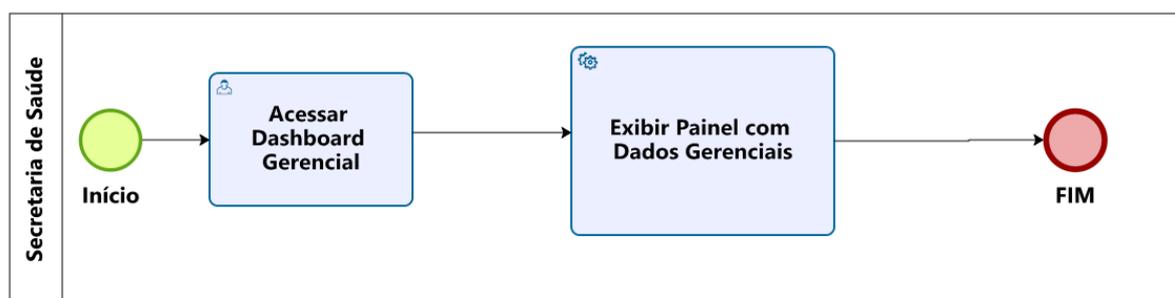


Figura 5.5 Fluxo do Processo de Visualização de dashboard Na Prova de Conceito (Elaboração Própria, 2023)

Capítulo

6

CONCLUSÃO

A integração das organizações com a *blockchain* JudMed traz os benefícios da descentralização, transparência, resiliência, irrefutabilidade, contribuindo com as instituições e com as pessoas que dependem da logística para o cuidado e tratamento da saúde por meio de fármacos. O acompanhamento possibilita a obtenção ágil e a análise dos dados através do *dashboard* deve prover uma melhoria contínua em todo o fluxo de aquisição do material.

A prova de conceito trouxe a visão do funcionamento em ambiente controlado e forneceu uma visão sistêmica do processo como um ativo da *blockchain*, possibilitando análise prática do funcionamento ao gestor farmacêutico do município de Salvador.

Para efetivar a integração em produção se faz necessário a apresentação de um Mínimo Produto Viável. aprovação para a criação do consórcio e treinamento entre as organizações públicas no que se refere a demanda judicial de medicamentos com *blockchain*.

A limitação da rede é estar operável com no mínimo duas organizações para haver o consenso das transações com o protocolo Raft e as operações apresentam um tempo de resposta com uma maior latência por conta do percurso do dado até efetivar-se como um ativo na *blockchain*.

Após concluir o consórcio entre as organizações, possíveis contribuições futuras são: utilizar a Internet das Coisas para rastreamento em tempo real dos fármacos e fazer a leitura de dados com *smartphones*, utilizando etiquetas *Radio Frequency Identification* (RFID) ou QRCode, automatizando o lançamento das informações tal como desenvolver sob demanda. outras funções no *dashboard* na aplicação web JudMed. A utilização de *blockchain* pode auxiliar a gestão, promovendo melhorias constantes no atendimento ao paciente do Sistema Único de Saúde, evitando pedidos duplicados, garantindo a fila de atendimento e identificando possíveis gargalos para a obtenção do fármaco em tempo hábil para a terapêutica.

REFERÊNCIAS BIBLIOGRÁFICAS

- 101BLOCKCHAINS.COM. *Você precisa de blockchain?* 2022. Disponível em: <<https://101blockchains.com/pt/voce-precisa-de-blockchain/>>.
- ALANGOT, B.; ACHUTHAN, K. et al. Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud. In: SPRINGER. *International Conference on Ubiquitous Communications and Network Computing*. [S.l.], 2017. p. 189–195.
- ANDROULAKI, E. et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: *Proceedings of the thirteenth EuroSys conference*. [S.l.: s.n.], 2018. p. 1–15.
- BATISTA, A. B. R. et al. A judicialização da saúde e a questão do fornecimento de medicamentos pelo ente estatal. Universidade Federal de Uberlândia, 2020.
- BATISTELLA, P. M. F. et al. Judicialização na saúde em município de grande porte. *Revista Mineira de Enfermagem*, Revista Mineira de Enfermagem, v. 23, p. 1–7, 2019.
- BESPONSA. *Consulta Remédios*. 2023. Disponível em: <<https://consultaremedios.com.br/besponsa/p>>. Acesso em: 27 ago 2023.
- BOCEK, T. et al. Blockchains everywhere—a use-case of blockchains in the pharma supply-chain. In: IEEE. *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. [S.l.], 2017. p. 772–777.
- BOETTIGER, C. An introduction to docker for reproducible research. *ACM SIGOPS Operating Systems Review*, ACM New York, NY, USA, v. 49, n. 1, p. 71–79, 2015.
- BRASIL, S. F. do. Constituição da república federativa do brasil. *Brasília: Senado Federal, Centro Gráfico*, 1988.
- BURNS, B.; BEDA, J.; HIGHTOWER, K. *Kubernetes: up and running: dive into the future of infrastructure*. [S.l.]: O’Reilly Media, 2019.
- BUTERIN, V. B. V. *On Public and Private Blockchains*. [S.l.]: ”Ethereum Foundation Blog”, 2015.
- DANNEN, C. *Introducing Ethereum and solidity*. [S.l.]: Springer, 2017.
- DAO, G. *Judicialização da saúde: Como acionar a Justiça gratuita e conseguir seu medicamento*. 2021. Disponível em: <<https://www.jornalcontabil.com.br/como-acionar-a-justica-gratuita-e-conseguir-seu-medicamento/>>.

DHILLON, V.; METCALF, D.; HOOPER, M. The hyperledger project. In: *Blockchain enabled applications*. [S.l.]: Springer, 2017. p. 139–149.

DONIDA, B. et al. Making the covid-19 pandemic a driver for digital health: Brazilian strategies. *JMIR Public Health and Surveillance*, JMIR Publications Inc., Toronto, Canada, v. 7, n. 6, p. e28643, 2021.

FABRIC, H. *Ledger*. 2022. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/ledger/ledger.html#what-is-a-ledger>.

FABRIC, H. *Membership Service Provide*. 2022. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/msp.html>.

FNS. *Consulta FNS*. 2023. Disponível em: <https://consultafns.saude.gov.br/#/consolidada>. Acesso em: 27 ago 2023.

GREVE, F. G. et al. Blockchain e a revolução do consenso sob demanda. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos*, 2018.

GROUP, H. A. W. et al. Hyperledger architecture. *Hyperledger.org*, v. 1, p. 15, 2017.

HAHN, E. *Express in Action: Writing, building, and testing Node.js applications*. [S.l.]: Simon and Schuster, 2016.

HU, J.; LIU, K. Raft consensus mechanism and the applications. In: IOP PUBLISHING. *Journal of Physics: Conference Series*. [S.l.], 2020. v. 1544, n. 1, p. 012079.

HUANG, Y.; WU, J.; LONG, C. Drugledger: A practical blockchain system for drug traceability and regulation. In: IEEE. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (Smart-Data)*. [S.l.], 2018. p. 1137–1144.

KAMATH, R. Food traceability on blockchain: Walmart's pork and mango pilots with ibm. *The Journal of the British Blockchain Association*, The British Blockchain Association, v. 1, n. 1, p. 3712, 2018.

LI TONG; JONES, R. L. D. *Minifabric*. 2021. Disponível em: <https://github.com/hyperledger-labs/minifabric>.

LODI, G. C. et al. *Sistema de monitoramento dos processos de manutenção e vida de produto utilizando a tecnologia blockchain*. Dissertação (Mestrado) — Universidade Tecnológica Federal do Paraná, 2021.

LU, Q.; XU, X. Adaptable blockchain-based systems: A case study for product traceability. *Ieee Software*, IEEE, v. 34, n. 6, p. 21–27, 2017.

- MACEDO, E. I. d.; LOPES, L. C.; BARBERATO-FILHO, S. Análise técnica para a tomada de decisão do fornecimento de medicamentos pela via judicial. *Revista de Saúde Pública*, SciELO Brasil, v. 45, p. 706–713, 2011.
- MIERS, C. C. et al. Blockchains com hyperledger: conceitos, instalação, configuração e uso. *Sociedade Brasileira de Computação*, 2020.
- NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p. 21260, 2008.
- NG, W. Y. et al. Blockchain applications in health care for covid-19 and beyond: a systematic review. *The Lancet Digital Health*, Elsevier, v. 3, n. 12, p. e819–e829, 2021.
- OLIVEIRA, I. A.; HERBELLA, R. T. Lei geral de proteção de dados e o direito ao esquecimento. *ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498*, v. 16, n. 16, 2020.
- TSENG, J.-H. et al. Governance on the drug supply chain via gcoin blockchain. *International journal of environmental research and public health*, Multidisciplinary Digital Publishing Institute, v. 15, n. 6, p. 1055, 2018.
- YIANNAS, F. A new era of food transparency powered by blockchain. *Innovations: Technology, Governance, Globalization*, MIT Press, v. 12, n. 1-2, p. 46–56, 2018.
- YORK, N. *Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais*. 2011.
- ZHANG, J.; XUE, N.; HUANG, X. A secure system for pervasive social network-based healthcare. *Ieee Access*, IEEE, v. 4, p. 9239–9250, 2016.
- ZHANG, R.; XUE, R.; LIU, L. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, ACM New York, NY, USA, v. 52, n. 3, p. 1–34, 2019.
- ZHENG, Z. et al. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE. *2017 IEEE international congress on big data (BigData congress)*. [S.l.], 2017. p. 557–564.



GERENCIAMENTO DO PROJETO

A.1 QUESTIONÁRIO APLICADO

1. Como é o fluxo da solicitação judicial até a entrega do medicamento ao paciente?
2. Quais os dados do processo judicial são importantes registrar na solicitação?
3. Possui dados estatísticos sobre as solicitações?
4. Qual o principal identificador para o medicamento que está sendo solicitado? código Remume? Rename? Anvisa?
5. Além do cadastro das solicitações, quais recursos você gostaria que o sistema tivesse?
6. Quem lançará os dados no sistema?
7. Você gostaria de disponibilizar o acompanhamento para o paciente?
8. Já existe uma interlocução com a Sesab para tratar esse problema de solicitações em duplicidade?

A.2 ESTÓRIA GLOBAL DO USUÁRIO

O paciente possui uma comorbidade e vai buscar atendimento médico, o médico prescreve um medicamento adequado ao tratamento e o paciente vai buscar o fármaco na rede pública de assistência à saúde. O medicamento pode não estar presente na rede de assistência, logo o paciente vai solicitar via pleito judicial no Ministério Público ou na Defensoria Pública. O paciente pode ir diretamente nos órgãos supracitados ou tentar obter o medicamento via Câmara de Conciliação em Saúde, onde estão presentes os membros da esfera da saúde e jurídica e é avaliada se o medicamento está na rede ou se tem algum genérico para atender, caso não tenha o medicamento o processo é aberto lá mesmo na câmara, caso tenha algum fármaco genérico o paciente é orientado a conversar com o médico para avaliar se atende, caso atenda o médico refaz a prescrição, o paciente vai obter

o medicamento e encerra o fluxo, caso não atenda o pleito é aberto na própria câmara de conciliação. Depois do processo aberto, um oficial da procuradoria do município busca a secretaria para atender, a solicitação que então é aberta e o medicamento poderá ser comprado pela Secretaria por dispensa de licitação ou registro de preço. O mais comum é ser por licença de licitação, pois quase sempre o medicamento não se encontra no sistema de registro de preços, onde é feito uma licitação com cotação de preços e o processo é um pouco mais demorado. Quando adquirido mediante a compra, o medicamento é encaminhado ao Almoxarifado e segue para a Assistência Farmacêutica que comunica ao paciente agendando a entrega do medicamento em mãos, até pelo risco do valor do fármaco. O número de solicitações judiciais não é grande, mas geralmente o custo dos fármacos envolvidos é alto. Em casos onde a responsabilidade é definida como município, estado ou união, a solicitação pode ser realizada em qualquer uma das esferas, o que pode causar a duplicidade e a perda de receita. Hoje, quando a Assistência Farmacêutica do Município de Salvador recebe uma solicitação, verifica via telefone junto ao estado se a solicitação já não foi aberta lá juntamente. O Ministério Público e a Defensoria Pública podem acompanhar o pleito e o paciente hoje é comunicado pela Assistência Farmacêutica para verificar o andamento. Os principais dados de registro do processo são: O número no Ministério Público ou na Defensoria Pública, o número da solicitação na secretaria, os dados do paciente e o número RENAME que identifica o medicamento nacionalmente. Por vezes ocorre algo e o paciente não retira o medicamento ou veio a óbito e não deu tempo de usá-lo, com isso é interessante comunicar na rede para poder ser encaminhado a alguma unidade que tenha a necessidade.

Tabela A.1 Estórias do Usuário (BATISTA et al., 2020)

Estória	Descritivo
1	Como operador do órgão judicial, clicar em “cadastrar processo” no menu lateral levará para a página de cadastro do ativo com todos os campos a serem preenchidos.
2	Como operador da secretaria de saúde do município ou do estado, clicar em “movimentar processo” no menu lateral levará para a página de movimentação do processo, clicando em abrir solicitação assumirá o ativo para nesta secretaria.
3	Como operador da secretaria de saúde do município ou do estado, clicar em “movimentar processo” no menu lateral levará para a página de movimentação do processo, clicando em enviado ao almoxarifado ou solicitado compra ou disponível almoxarifado ou disponível retirada irá movimentar o ativo com os respectivos status.
4	Como cidadão solicitante e em posse do número do processo no órgão judicial clicar em “acompanhar o processo” no menu lateral levará para a página de acompanhar o status atual do ativo.
5	Como operador do órgão judicial, clicar em “auditar processo” no menu lateral levará para a página de auditoria do ativo. Ao pesquisar com o numero de processo será exibida o histórico de movimentação do ativo.
6	Como administrador, clicar em “dashboard” no menu lateral levará para a página com dados gráficos e estatísticos sobre os ativos.

A.3 CRONOGRAMA DE DESENVOLVIMENTO

CRONOGRAMA DE DESENVOLVIMENTO

NOME DA TAREFA	DATA DE INÍCIO	DATA DE TÉRMINO
Instalação e configuração do Hyperledger Fabric e Minifabric em localhost (Instância que faz o papel da Secretaria de Saúde do Município e o Órgão Judicial na blockchain)	1/3/2021	10/3/2021
Criação e configuração da máquina virtual que representa a Secretaria de Saúde do Estado	11/3/2021	20/3/2021
Instalação e configuração do Hyperledger Fabric e Minifabric na máquina virtual	21/3/2021	25/3/2021
Criação do Contrato Inteligente e da API : Pesquisar Processo no Ministério Público	26/3/2021	10/4/2021
Criação do Contrato Inteligente e da API : Registrar Solicitação de Medicamento nas Secretarias.	11/4/2021	21/4/2021
Criação do Contrato Inteligente e da API : Movimentar Processo.	22/4/2021	15/5/2021
Criação do Contrato Inteligente e da API : Auditar Processo.	16/5/2021	1/6/2021
Iniciação da Rede em Localhost e na Máquina Virtual e instalação do contrato inteligente	2/6/2021	2/6/2021
Aplicação Web: Tela de Abertura de Processo no Ministério Público	3/6/2021	20/6/2021
Aplicação Web: Tela de Abertura de Processo nas Secretarias	21/6/2021	5/7/2021
Aplicação Web: Movimentar Processo nas Secretarias	6/7/2021	30/7/2021
Aplicação Web: Auditar Processo	31/7/2021	15/8/2021
Aplicação Web : Acompanhar Processo pelo Paciente	16/8/2021	25/8/2021
Aplicação Web: Dashboard	26/8/2022	30/9/2021

Figura A.1 Cronograma de Desenvolvimento (Elaboração Própria, 2021)

A.4 PACOTE DE ATIVIDADES

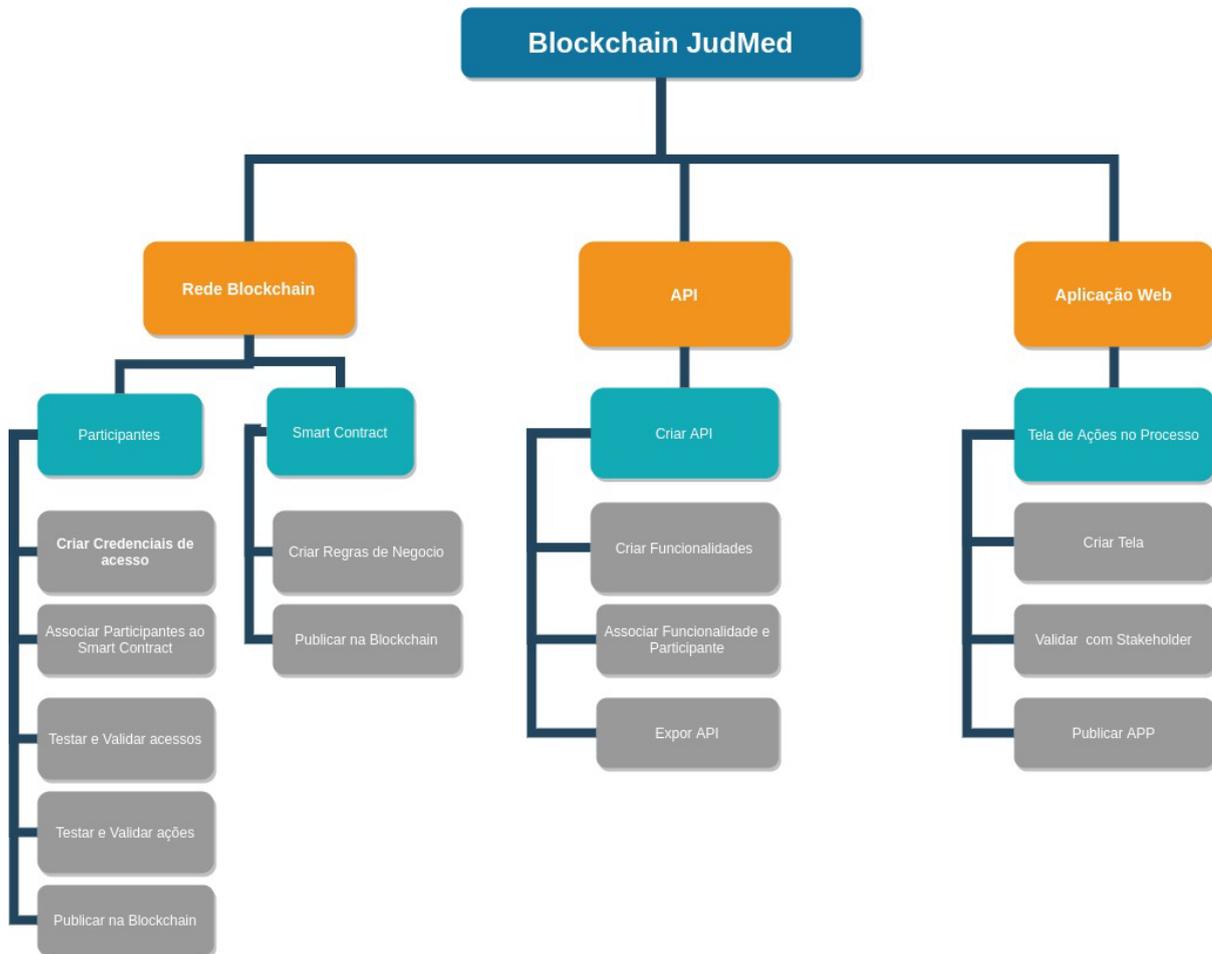


Figura A.2 Pacote de Atividades (Elaboração Própria, 2021)



COMANDOS FRAMEWORK MINIFABRIC

Para criar e iniciar uma rede Fabric como exemplo, a partir do Linux Ubuntu 16.4, é necessário fazer o *download* do binário minifabric com o comando:

- [`mkdir -p /mywork cd /mywork curl -o minifab -sL https://tinyurl.com/yxa2q6y1 chmod +x minifab`].

Após o *download* é necessário configurar o arquivo **spec.yaml** visto na Figura B.1 que é onde está toda a estrutura da organização como *peers*, nós ordenadores, entidades certificadoras, logs e etc.

Em seguida deve realizar a configuração do arquivo **spec.yaml** e executar o comando:

- [`minifab up`]

Esse comando realiza o *download* das imagens docker que executarão nos contêineres. Em seguida, a rede é criada e iniciada nos *contêineres* contendo a organização já admitida em um canal com um *ledger* escrito na linguagem Golang. Todos os arquivos gerados são colocados na pasta "**mywork**". Caso deseje acompanhar visualmente a rede com gráficos e monitorar transações, organizações, canais e *ledgers* é possível iniciar um contêiner com a ferramenta Hyperledger Explorer com o comando:

- [`minifab explorerup`]

Alguns outros comandos importantes do Minifabric:

1. `minifab stats`: Traz o status atual da rede e se todos os *peers* estão ativos, visto na Figura B.2;
2. `minifabric down`: Desativa a rede em todos os contêineres docker;
3. `minifabric cleanup`: Além de parar a rede exclui todos os artefatos criados, "limpando" a instalação na pasta "**mywork**".

```
fabric:
  cas:
    - "ca1.org0.example.com"
    - "ca1.org1.example.com"
  peers:
    - "peer1.org0.example.com"
    - "peer2.org0.example.com"
    - "peer1.org1.example.com"
    - "peer2.org1.example.com"
  orderers:
    - "orderer1.example.com"
    - "orderer2.example.com"
    - "orderer3.example.com"
  settings:
    ca:
      FABRIC_LOGGING_SPEC: DEBUG
    peer:
      FABRIC_LOGGING_SPEC: DEBUG
    orderer:
      FABRIC_LOGGING_SPEC: DEBUG
  ### use go proxy when default go proxy is restricted in some of the regions.
  ### the default goproxy
  goproxy: "https://proxy.golang.org,direct"
  ### the goproxy in China area
  goproxy: "https://goproxy.cn,direct"
  ### set the endpoint address to override the automatically detected IP address
  ### could be a public IP address or a dns name
  endpoint_address: 104.196.45.144
  ### set the docker network name to override the automatically generated name.
  netname: "mysite"
  ### set the extra optins for docker run command
  container_options: "--restart=always --log-opt max-size=10m --log-opt max-file=3"
```

Figura B.1 spec.yaml Minifabric (Elaboração Própria, 2022)

```
.....
# Docker node status *****
dev-peer1.sms.ba.gov.br-chaincodejudmed_1.5.3-61f9 : Up 34 seconds
dev-peer1.mp.ba.gov.br-chaincodejudmed_1.5.3-61f92 : Up 33 seconds
ChainJudMedA : Up About a minute
ca1.sms.ba.gov.br : Up 2 minutes
orderer1.smsorderer.ba.gov.br : Up 2 minutes
peer1.mp.ba.gov.br : Up 2 minutes
peer1.sms.ba.gov.br : Up 2 minutes
peer1.mp.ba.gov.br.couchdb : Up 2 minutes
peer1.sms.ba.gov.br.couchdb : Up 2 minutes

# Fabric network peer and orderer node health status *****
peer1.sms.ba.gov.br "OK"
peer1.mp.ba.gov.br "OK"
orderer1.smsorderer.ba.gov.br "OK"
Network Status: 100%

# STATS *****
minifab: ok=30 failed=0
```

Figura B.2 Resultado do comando Minifabric Stats (Elaboração Própria, 2022)

SMART CONTRACT

C.1 INICIALIZA O LEDGER

```
1
2 async InitLedger(ctx) {
3
4     var data = new Date();
5
6     const assets = [
7     {
8         ID: 'initN001',
9         NumRename: 'Init',
10        NomeComercialMedicamento: 'Init',
11        Instancia: 'MPBA',
12        Status: 'Init',
13        TipoOperacao: 'InicializacaoJudMed',
14        Operador: 'IniciadorAuto',
15        Data: data.toString(),
16    },
17
18    ];
19
20    for (const asset of assets) {
21        asset.docType = 'asset';
22        await ctx.stub.putState(asset.ID, Buffer.from(JSON.stringify(asset)));
23        console.info(`Asset ${asset.ID} initialized`);
24    }
25 }
```

C.2 CRIA O ATIVO

```
1 async CriarAtivoProcessoJudicial(ctx, id,
2   numRename, nomeComercialMedicamento, instancia, status, operador) {
3
```

```

4 | var data = new Date();
5 | const exists = await this.AssetExists(ctx, id);
6 |
7 | if (exists) {
8 |   throw new Error('O processo de n mero
9 |     ${id} ja foi cadastrado e nao pode ser repetido. ');
10 |   return;
11 | }
12 |
13 | const cid = ctx.clientIdentity;
14 | let MSPID_ORIGEM = cid.getMSPID();
15 |
16 | if (MSPID_ORIGEM !== 'sms-ba-gov-br') {
17 |   throw new Error('Usuario voce pertence
18 |     a organizacao ${MSPID_ORIGEM} apenas usuarios
19 |     do Ministerio Pblico podem
20 |     cadastrar um processo judicial. ');
21 |   return;
22 | }
23 |
24 | else {
25 |   const asset = {
26 |     ID: id,
27 |     NumRename: numRename,
28 |     NomeComercialMedicamento: nomeComercialMedicamento,
29 |     Instancia: instancia,
30 |     Status: status,
31 |     TipoOperacao: 'Cadastro',
32 |     Operador: operador,
33 |     Data: data.toString(),
34 |   };
35 |   ctx.stub.putState(id, Buffer.from(JSON.stringify(asset)));
36 |   return JSON.stringify(asset);
37 | }
38 | }

```

C.3 VERIFICA SE O ATIVO EXISTE PELO ID

```

1 | async AssetExists(ctx, id) {
2 |   const assetJSON = await ctx.stub.getState(id);
3 |   return assetJSON && assetJSON.length > 0;
4 | }

```

C.4 PESQUISA O ATIVO PELO NÚMERO DO PROCESSO

```

1 | async PesquisarProcessoJudicialPorNumero(ctx, id) {
2 |   const assetJSON = await ctx.stub.getState(id);
3 |   if (!assetJSON || assetJSON.length === 0) {
4 |     console.log('O processo judicial de n mero ' + id + ' n o existe. ');
5 |     return;

```

```

6     }
7     return assetJSON.toString();
8 }

```

C.5 MOVIMENTA O ATIVO

```

1  async MovimentarProcesso(ctx, id,
2    numRename, nomeComercialMedicamento,
3    instancia, status, operador) {
4
5    var data = new Date();
6    const exists = await this.AssetExists(ctx, id);
7
8    if (!exists) {
9      throw new Error('O processo de n mero ${id} n o existe. ');
10     return;
11   }
12   else
13   {
14     const updatedAsset = {
15       ID: id,
16       NumRename: numRename,
17       NomeComercialMedicamento: nomeComercialMedicamento,
18       Instancia: instancia,
19       Status: status,
20       TipoOperacao: 'Movimentacao',
21       Operador: operador,
22       Data: data.toString()
23     };
24
25     ctx.stub.putState(id, Buffer.from(JSON.stringify(updatedAsset)));
26
27     return JSON.stringify(updatedAsset);
28   }
29 }
30 }

```

C.6 AUDITA O ATIVO

```

1  async AuditarProcessoJudicial(ctx, id) {
2    console.info('getting history for key: ' + id);
3    let iterator = await ctx.stub.getHistoryForKey(id);
4    let result = [];
5    let res = await iterator.next();
6
7    while (!res.done) {
8      if (res.value) {
9        console.info('Hist rico —>: ${res.value.value.toString('utf8')}');
10       const obj = JSON.parse(res.value.value.toString('utf8'));
11       result.push(obj);

```

```
12     }
13     res = await iterator.next();
14     }
15     await iterator.close();
16     return result;
17
18 }
```



ENDPOINTS

Tabela D.1 Endpoints

Verbo	URL	Descritivo
GET	/api/BuscarTodosProcessos	Busca todos os ativos criados.
GET	/api/PesquisarProcessoPorNumero/:numero, <i>processo</i>	Busca o ativo pelo número do processo.
GET	/api/AuditarProcesso/:id	Audita a movimentação do ativo.
POST	/api/CadastrarProcessoJudicial/	Cadastro o ativo.
POST	/api/MovimentarProcesso/	Movimenta o ativo.



OUTROS RESULTADOS E ATIVIDADES

Tabela E.1 Outros resultados e atividades

Tipo	Nome	Local	Data
Apresentação	Blockchain and Cryptocurrency Conference	Barcelona	11/11/2022
Publicação de Artigo	Blockchain and Cryptocurrency Journal	—	01/11/2023
Registro de Software	JudMed	—	05/05/2023
Apresentação	CSBC - Colóquio em Blockchain e WD	João Pessoa	11/08/2023
Participação	CT Blockchain Universidades Federais	—	—
Treinamento	Treinamento em Blockchain	SMS	06/06/2022

1. CSBC - Congresso da Sociedade Brasileira de Computação
2. WD - Web Descentralizada
3. CT - Comitê Técnico
4. SMS - Secretaria Municipal de Saúde de Salvador