Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Integrando Smart Contracts e KIP em um Blockchain: Estudo de Caso em uma Redação Jornalística

Guilherme Oliveira Loiola

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Orientador
Prof. Dr. Edison Ishikawa

Brasília
2024

CIP - Catalogação na Publicação

Oliveira Loiola, Guilherme.
O956i Integrando Smart Contracts e KIP em um Blockchain: Estudo de Caso em uma Redação Jornalística / Guilherme Oliveira Loiola; orientador Edison Ishikawa. -- Brasília, 2024.
51 p.

Monografia (Graduação - Ciência da Computação) -- Universidade de Brasília, 2024.

1. Rede colaborativa. 2. Jornalismo. 3. Autenticação de documentos. 4. Processos Intensivos em Conhecimento. 5. Tecnologias distribuídas. I. Ishikawa, Edison, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Integrando Smart Contracts e KIP em um Blockchain: Estudo de Caso em uma Redação Jornalística

Guilherme Oliveira Loiola

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Prof. Dr. Edison Ishikawa (Orientador)
CIC/UnB

Prof. Dr. Jorge Henrique Cabral Fernandes
CIC/UnB

Dr. Márcia Marques
FAC/UnB

Prof. Dr. Marcelo Grandi Mandelli
Coordenador do Bacharelado em Ciência da Computação

Brasília, 20 de setembro de 2024

Dedicatória

Equipado com seus cincos sentidos,
O homem explora o universo ao seu
Redor e chama a aventura de ciência .
- EDWIN P. HUBBLE (1889-19553)
Dedico essa obra à minha família.

Agradecimentos

Primeiramente, agradeço minha família, especialmente meus pais e avós, que sempre me incentivaram a buscar soluções através do estudo e do trabalho. Orientação esta que me inspirou a perseguir meus objetivos da mesma forma. Quero ressaltar a importância de todo o esforço que fizeram para garantir minha chance de ingressar na Universidade. Hoje, demonstro minha gratidão e declaro que minhas conquistas sempre terão parte deles.

Aos meus amigos, pela companhia ao longo de toda a caminhada. Tenho sorte de contar com pessoas tão boas, que compartilham vivências e conversas sinceras.

Ao meu orientador, Professor Dr. Edison Ishikawa, por compartilhar todo o conhecimento valioso. Agradeço também pela compreensão durante os obstáculos do projeto e pelo seu lado humano, sempre disponível para conversas e momentos fortalecedores.

Aos momentos de amor que induzem boas ações. Que Deus perpetue essa sensação.

Ao Portal Periódicos CAPES pelo acesso a recursos e publicações acadêmicas que foram fundamentais para o desenvolvimento deste trabalho e para meus estudos durante a formação.

Sou grato pela oportunidade de ter estudado com grandes pessoas na Universidade de Brasília. Sinto privilegiado pelos desafios enfrentados, pelos aprendizados adquiridos e pelas novas perspectivas que esse ambiente me proporcionou. O sentimento que persiste é que os estudos sempre orientarão minhas escolhas.

Resumo

Com o avanço do jornalismo, os profissionais adaptaram suas práticas para utilizar ferramentas tecnológicas na obtenção de dados disponíveis na web e na produção de conteúdos. Nesse sentido, este trabalho propõe a criação de uma rede colaborativa que permita a autenticação de documentos por meio da interação dos participantes dessa rede, ou seja, um *peopleware* que promova a credibilidade da informação. Para isso, foi implementada uma prova de conceito para a modelagem e execução de Processos Intensivos em Conhecimento (KIP, do inglês Knowledge Intensive Process) no contexto de uma redação jornalística, utilizando smart contracts e tecnologia blockchain.

A validação da proposta foi realizada por meio da criação de um motor de inferência que verifica se todos os campos e proposições lógicas foram autenticados antes da publicação no livro razão do blockchain. O blockchain utilizado foi importado do framework Hyperledger Fabric.

Quanto às possibilidades futuras, a integração com outras tecnologias distribuídas pode promover a criação de um ecossistema colaborativo para a validação de informações. O projeto pode ser escalado e tornar-se open source, permitindo sua adoção em larga escala por redações jornalísticas. Outras ideias incluem o uso de inteligência artificial para análise de dados, a implementação de mecanismos de segurança aprimorados e o desenvolvimento de ferramentas de visualização de dados para facilitar a interpretação das informações verificadas.

Palavras-chave: Rede colaborativa, Jornalismo, Autenticação de documentos, Peopleware, Processos Intensivos em Conhecimento (KIP), Smart contracts, Blockchain, Hyperledger Fabric, Validação de informações, Tecnologias distribuídas

Abstract

With the advancement of journalism, professionals have adapted their practices to use technological tools for obtaining data available on the web and producing content. In this context, this work proposes the creation of a collaborative network that allows document authentication through the interaction of the network participants, a peopleware that promotes the credibility of information. For this, a proof of concept was implemented for the modeling and execution of Knowledge Intensive Processes (KIP) in the context of a journalistic newsroom, using smart contracts and blockchain technology.

The proposal was validated through the creation of an inference engine that verifies whether all fields and logical propositions have been authenticated before being published in the blockchain ledger. The blockchain used was imported from the Hyperledger Fabric framework.

Regarding future possibilities, the integration with other distributed technologies can promote the creation of a collaborative ecosystem for information validation. The project can be scaled and become open source, allowing its widespread adoption by journalistic newsrooms. Other ideas include the use of artificial intelligence for data analysis, the implementation of enhanced security mechanisms, and the development of data visualization tools to facilitate the interpretation of verified information.

Keywords: Collaborative network, Journalism, Document authentication, Peopleware, Knowledge Intensive Processes (KIP), Smart contracts, Blockchain, Hyperledger Fabric, Information validation, Distributed technologies

Sumário

Lista de Figuras

Capítulo 1

Introdução

Na era do jornalismo precedente à Internet, a forma mais comum de se manter atualizado era por meio de assinatura de jornais impressos. Com o advento da Internet, o acesso às notícias se tornou mais fácil e gratuito. Os leitores passaram não só a ler as notícias por meio das mídias sociais, mas também a produzir conteúdo [1] e propagá-lo, sem as qualidades necessárias a uma notícia.

Essa forma de interagir por meio das mídias sociais dissemina as informações de maneira imediata, interativa e massiva. Os produtores de conteúdo divulgam notícias em plataformas sociais com alta velocidade de distribuição, assim a divulgação de notícias é ampliada e resulta em um grande volume de informação [2]. Consequentemente, houve adaptações no jornalismo e meios de comunicação. Com a diminuição das vendas de notícias impressas e de anunciantes, os recursos financeiros das empresas de comunicação foram reduzidos. Com isso, houve a necessidade de reduzir custos, o que resultou na demissão abundante de profissionais nas redações jornalísticas. Isso levou à precarização da profissão, uma vez que menos jornalistas na redação tiveram que produzir a mesma ou mais quantidade de notícias, muitas vezes com salário menor, o que levou à sua queda de qualidade. Neste novo cenário, o jornalista, para aumentar a sua produtividade, precisou aprender a atuar de forma contemporânea, tendo que dominar o conhecimento tecnológico para obter os dados disponíveis na web ou produzir novos conteúdos no ambiente computacional [3].

Outro ponto decorrente do aumento na utilização das mídias sociais é a propagação de informações enganosas (*fakenews*). As novas tecnologias permitem a fácil manipulação de conteúdo, e as redes sociais disseminam essa informação adulterada ou falsa rapidamente e em grande escala [4]. Como resultado, muitos leitores ficam desinformados, frequentemente acreditando que uma *fakenews* é verdadeira. Neste contexto, uma notícia produzida por um veículo de comunicação responsável é confrontado por uma massa de *fakenews*. Isto leva à queda da reputação do veículo de comunicação ou do jornalista responsável no

imaginário desse leitor desinformado. Segundo a UNESCO, a solução para esse problema é os veículos de comunicação aderirem mais fortemente aos padrões profissionais e éticos do jornalismo. Significa evitar a publicação de informações não apuradas e tomar distância de informações que interessem somente a uma minoria, ou seja, que não é de interesse público [4].

Outro problema com o uso das plataformas de mídias sociais para a veiculação de notícias é a perda da independência do veículo de comunicação. Por exemplo, se um veículo de comunicação publica uma notícia que vá de encontro aos interesses da plataforma de mídia social, essa notícia pode ser censurada ou até o veículo de comunicação ser bloqueado. Esses problemas podem resultar em perdas econômicas, a diminuição do alcance das publicações, entre outros prejuízos.

Para gerar uma notícia de qualidade, é preciso um processo de construção de pauta de interesse público, que garanta a verificação dos fatos, investigue o assunto em profundidade, seja ético, que o processo de produção da notícia seja transparente. Uma equipe multidisciplinar trabalhando de forma cooperativa contribuiria significativamente para aumentar a qualidade desse processo.

Segundo Mia, uma solução possível para o desafio é uma rede de blocos de dados públicos, assinados criptograficamente e idênticos, que permite aos jornalistas autenticar conteúdo, publicar e cancelar a publicação de forma responsável [5]. Por conseguinte, caracterizando um uso potencial de aplicações em Blockchain.

Blockchain é um livro-razão aberto e distribuído com a funcionalidade de registro entre partes que estabelecem transações de forma eficiente, verificável e permanente. Além disso, o livro-razão pode ser acionado para transações automaticamente por meio de programação [6]. Mas, ainda, podemos entender o Blockchain como um ambiente em que contratos são incorporados em código e armazenados em bancos de dados transparentes e compartilhados de forma distribuída. Garante dessa maneira proteção contra exclusão, adulteração e revisão não autorizadas [6]. Por isso, uma redação jornalística em Blockchain é a uma boa alternativa para enfrentar os desafios de uma jornalismo independente, de transparente e cooperativo.

1.1 Definição do Problema

Plataformas de mídias sociais frequentemente comprometem a independência dos veículos de comunicação e dos jornalistas. Devido à intervenção de algoritmos arbitrários ou interesses de seus proprietários, essas plataformas podem censurar conteúdos publicados ou até banir os criadores de notícias [7]. Uma alternativa para enfrentar essa centralização são as plataformas *peer-to-peer*, como BitTorrent [8]. Embora essas aplicações descen-

tralizadas reduzam a influência centralizada, elas ainda enfrentam desafios significativos, como a falta de garantias sobre os direitos de propriedade intelectual, rastreabilidade, e a integridade do conteúdo. Problemas que podem ser mitigados pela integração da tecnologia Blockchain, que oferece soluções para a transparência e a integridade em sistemas *peer-to-peer*.

A tecnologia Blockchain permite definir processos de negócios por meio de *smart contracts*. O problema é que os *smart contracts* são inflexíveis comparados, por exemplo, com esteiras automatizadas de *build/deploy* utilizadas na computação em nuvem. Por outro lado, uma redação jornalística é muito dinâmica, tendo seus processos adaptados às novas situações constantemente. Os processos de uma redação jornalística são intensivos em conhecimentos [9].

Neste contexto, a tecnologia Blockchain seria uma solução interessante para implementar uma redação jornalística no qual os jornalistas cooperariam para a produção de notícias. O problema é coordenar esta equipe para produção de notícias de qualidade por meio de um processo transparente. Este processo transparente poderia ser implementado por *smart contracts* de um Blockchain. No entanto,*smart contracts* tiram a flexibilidade necessária a uma redação jornalística. A questão de pesquisa é como implementar uma redação jornalística em Blockchain usando *smart contracts* sem tirar a sua característica de alta dinamicidade.

Uma possível solução é integrar processos intensivos em conhecimento (KIPO) com *smart contracts*. Quando se usa a KIPO de forma convencional, temos ontologias que são verificadas por um motor de inferência. O resultado dessa execução utilizando *smart contract* é persistido pela Blockchain. As autenticações serão cumpridas conforme os níveis de acesso dos usuários da rede (*software* como *peopleware*) até a publicação da matéria jornalística como notícia ou seu arquivamento. Como gerar *smart contracts* baseados em uma ontologia? Esta arquitetura aparentemente flexibiliza o conceito de DAO (*Descentralized Autonomous Organization*), necessária a uma redação jornalística cujas regras de negócios são altamente dinâmicas por se tratar de uma KIPO.

1.2 Objetivo

Modelar e implementar uma prova de conceito de redação jornalística com *smart contracts* flexibilizada por meio de integração com a KIPO.

1.2.1 Objetivos Intermediários

1. Propor um modelo para o Blockchain da redação jornalística

2. Propor uma arquitetura com níveis de acesso no *software* para os humanos envolvidos e suas interações
3. Implementar rede de teste Blockchain que persiste o documento após verificação da ontologia
4. Integração das tecnologias
5. Simular e testar a prova de conceito
6. Avaliar os resultados
7. Publicar os resultados

1.3 Metodologia

Usaremos uma adaptação da metodologia DSR (*Design Science Research*) da Dresch.

1. Identificação do problema / Conscientização do problema
2. Revisão da literatura
3. Proposição dos artefatos / Escolha do artefato
4. Implementação do artefato
5. Avaliação dos resultados
6. Publicação dos resultados

1.4 Estrutura do Trabalho

Este trabalho está estruturado da seguinte forma:

- Capítulo 1: Este capitulo contextualiza o problema e introduz os objetivos esperados.
- Capítulo 2: Apresenta a fundamentação teórica com a finalidade de discorrer sobre o contexto que o trabalho é inserido, além de fundamentar a proposta com outras realizações de tópicos relacionados.
- Capítulo 3: Retrata a arquitetura proposta e os fluxos de utilização desenhados para a aplicação.
- Capítulo 4: Descreve as etapas de implementação do sistema e resultados de execução observados.

- Capítulo 5: Encerra o trabalho descrevendo os pontos principais desenvolvidos no trabalho. Assim como manifesta possíveis trilhas de evolução da aplicação.

Diante dos desafios apresentados, como a propagação de *fakenews* e a perda de independência dos veículos de comunicação, surge a necessidade de explorar soluções tecnológicas que possam assegurar a integridade e a qualidade das notícias. Nesse sentido, o uso de tecnologias descentralizadas, como o Blockchain, desponta como uma alternativa viável para enfrentar esses obstáculos. No próximo capítulo, será abordada a fundamentação teórica que sustenta essa proposta, explorando como essas inovações podem ser aplicadas para preservar a credibilidade e a transparência no jornalismo.

Capítulo 2

Fundamentação Teórica

2.1 Aplicações Descentralizadas com Foco na Integridade de Informações

O jornalismo se dedica a fornecer à sociedade um relato preciso e contextualizado dos fatos [10]. A contribuição principal do jornalismo é a informação. Ela é o elemento essencial da produção. A sua veracidade influencia diretamente na credibilidade do veículo de comunicação [11]. A verdade é obtida por meio da apuração e verificação dos fatos [10]. Portanto, as empresas jornalísticas visam alcançar altos padrões de qualidade. Isso é realizado por meio da verificação da veracidade das informações para apresentar as notícias de maneira íntegra.

Outra propriedade importante nas organizações jornalísticas é a Transparência Editorial (TE). TE é a publicização de informações acerca da organização e de seus processos jornalísticos que elevem a confiabilidade das notícias produzidas. Assim, quanto menor a transparência, maior o risco de perda da credibilidade [12].

As propriedades discutidas são: veracidade, credibilidade e transparência, cada uma impactando as organizações de maneiras distintas. Baseado na afirmação de Rodrigues, a pesquisa e a transmissão de informações estão frequentemente vinculadas aos interesses dos detentores do poder, que controlam essas informações [13]. Desse modo, esses detentores estarão atentos a qualquer possível impacto em seus negócios.

Uma consequência disso é a visualização da informação como um fator econômico. Um ponto importante são os critérios de decisão para a divulgação das informações que agora estão associados com fatores econômicos, muitas vezes, ignorando valores como a ética jornalística e o interesse público [13]. Logo, quem controla a divulgação da informação pode exercer essa influência nos indivíduos que estão inseridos nessa sociedade, assim direcionando para um cenário inapropriado no quesito de diversidade de ideias.

Tendo em vista que a influência ocasionada pelo controle de informações pode ser indevida, a revisão sobre as estruturas atuais dos veículos de comunicação é uma questão relevante. A solução a ser considerada deve fortificar as propriedades retrocitadas que impactam os processos jornalísticos. Ou seja, significa promover um ambiente confiável e com possibilidade de acompanhamento das etapas de produção pelos usuários.

Com a tecnologia Blockchain, propõe-se um sistema distribuído que atende os requisitos de modernidade web e oferece uma boa alternativa também para o fim dos monopólios provenientes de sistemas centralizados. Baseando-se em registros distribuídos, o Blockchain cria redes com imparcialidade das informações. Em vez de confiar em uma única entidade central, as notícias são validadas e armazenadas em vários nós independentes [14].

Portanto, a modelagem do trabalho foi baseado em Blockchain, no *framework* Hyperledger Fabric, cujo objetivo é alcançar a divulgação de informações com qualidade, permitindo definir o processo de autenticação via ontologia e disponibilizar um ambiente contributivo. Por exemplo, enquanto os autores de notícias criam o conteúdo, registrado de forma segura na rede, os revisores são responsáveis por verificar a autenticidade das notícias.

A seguir, serão apresentados os conceitos principais e trabalhos relacionados com Blockchain para aplicações baseadas em arquitetura distribuída.

2.2 Atuações no Contexto do Jornalismo Digital

2.2.1 Atuação Híbrida do Jornalista Contemporâneo

Nos últimos anos, a figura do jornalista passou por uma transformação significativa, impulsionada pela introdução de novas tecnologias e relações entre os diferentes atores no campo da comunicação. Atualmente, o jornalista encontra-se em um cenário de hibridização, no qual a separação tradicional entre comunicação e jornalismo se torna cada vez mais difusa. Esse profissional trabalha diante do computador que serve como fonte de informação e espaço de redação. A transição para o jornalismo digital colocou o jornalista moderno em uma posição de maior versatilidade, atuando como produtor de conteúdo e assessor de comunicação, circulando entre diferentes atuações profissionais [15].

Outra transformação perceptível é a crescente influência de corporações nas decisões editoriais, afetando a seleção de notícias e, muitas vezes, comprometendo a independência jornalística. Embora a liberdade de expressão tenha avançado significativamente, surgem novos desafios, como o avanço tecnológico e a intensa concorrência entre diferentes plataformas de comunicação. Nesse ambiente de mudança, o jornalista contemporâneo se vê

em meio a uma reflexão sobre sua função e relevância, considerando que o público tem acesso a múltiplas fontes de informação além da mídia tradicional .

Atualmente, a mídia perde o controle da disseminação de informações. A opinião pública é moldada não apenas pelos meios tradicionais, mas também por entidades e movimentos sociais com interesses corporativos. Sant'Anna chama isso de 'mídia corporativa', evidenciando a influência das corporações no conteúdo jornalístico. Nesse cenário, o jornalista atua em um ambiente mais híbrido, muitas vezes acumulando funções [16].

2.2.2 Funções Atuais do Jornalista

A redefinição das responsabilidades dos jornalistas na era digital é um aspecto importante na compreensão do jornalismo contemporâneo. As atividades de seleção de conteúdo e de verificação de fatos estão sendo transformadas. Discursos que promovem papéis jornalísticos democráticos nem sempre foram transparentes em relação à lógica comercial que permeia o setor.

Atualmente, o desafio é recuperar a confiança do público. Uma proposta frequentemente sugerida é o afastamento do modelo comercial [17]. O envolvimento autêntico com o público e a construção de uma interação honesta são chaves para que a confiança seja restabelecida. Contudo, hoje ainda se espera que o público consiga diferenciar as notícias falsas das reais, o que não ocorre de maneira confiável.

A teoria institucional de Taylor [18] sugere que os jornalistas nunca tiveram total autonomia para definir seus papéis, necessitando negociar sua legitimidade dentro de normas sociais mais amplas. Além disso, a crescente presença de atores desonestos complicou ainda mais a definição dos papéis jornalísticos. A legitimidade dos jornalistas como árbitros independentes da verdade está sendo questionada, e não está claro como se adaptarão a essa situação [19].

Outra complicação refere-se à ampliação de quem pode ser considerado um ator jornalístico. A distinção entre jornalistas e outros profissionais que atuam em organizações de notícias, como profissionais de marketing, está mais complicada.

Portanto, o papel do jornalista no contexto atual vai além de simplesmente relatar os fatos. Envolve a negociação de sua autoridade no cenário de comunicação, onde diferentes atores influenciam sobre o que é considerado jornalismo e como suas funções são desempenhadas.

2.2.3 Jornalismo Colaborativo: Integração com Blockchain

Uma das vertentes do jornalismo na era digital é o jornalismo colaborativo, formado em estruturas de interesse comum entre jornalistas e veículos de comunicação. As redes

sociais desempenham um papel notável, possibilitando a troca de informações e fontes para o trabalho jornalístico. Uma realidade distinta do jornalismo industrial, quando informações privilegiadas, como cadernos de fontes, eram mantidas em sigilo dentro das organizações.

A crescente colaboração entre jornalistas independentes e veículos está na essência desse novo formato de jornalismo, desafiando as práticas das redações convencionais. Além disso, o contato direto entre jornalistas e o público tornou-se uma parte fundamental do trabalho. Através de redes sociais ou e-mails, os jornalistas recebem sugestões de correções, complementações e interpretações alternativas dos fatos. Esse tipo de interação também permite que o público compartilhe suas próprias produções, aproximando mais o jornalismo dos leitores [20].

Essa mudança no perfil das atividades do jornalismo contemporâneo demanda novos métodos de apuração e divulgação de notícias, além da implementação de soluções colaborativas. Dessa forma, a proposta é a utilização do Blockchain como rede colaborativa independente. O Blockchain pode facilitar o trabalho cooperativo distribuído e autenticação das informações compartilhadas. Vale ressaltar, que a colaboração descentralizada pode ter definido múltiplos papéis de atuação. Estes papéis serão utilizados para definir as diferentes funções presentes na rede de testes.

O termo 'atividade' descreve os trabalhos específicos realizados por um profissional de uma determinada profissão. Cada atividade é uma tarefa com um início, meio e fim. No trabalho, uma atividade é parte do que o profissional faz na sua rotina. A função define o papel do profissional no trabalho e como suas interações com os demais participantes.

A estrutura composta por pauteiro, redator e editor, usada neste modelo, é uma simplificação de uma organização comumente observada nas redações brasileiras. No contexto tradicional, o pauteiro define as diretrizes iniciais, o redator elabora e valida as informações, e o editor finaliza o processo com a publicação [20].

Essa estrutura simplificada, pode ser representada em um cenário de digitalização do jornalismo. No ambiente digital, o pauteiro trabalha na preparação do material, estabelecendo as regras de negócio e ontologias necessárias para a autenticação dos documentos. O redator valida se os campos e informações estão em conformidade com essas regras e foram autenticados corretamente, garantindo a integridade e confiabilidade dos dados. Por fim, o editor publica a notícia na rede Blockchain, completando o ciclo de produção jornalística de maneira descentralizada.

2.3 Processos Intensivos em Conhecimento

Segundo Hagen et al. [21], um processo negocial é uma sequência de atividades que visa entregar valor ao cliente. Os processos são iniciados e encerrados por meio de eventos que, normalmente, necessitam de recursos como pessoas, ferramentas, dados e outros.

Um processo de negócio é geralmente representado por um modelo de negócio que visa analisar um fluxo de trabalho na organização. Esses modelos desempenham um papel importante para preencher a lacuna entre o domínio do negócio e a tecnologia da informação (TI), servindo como uma ferramenta fundamental para o planejamento da arquitetura de TI e a identificação de requisitos para sistemas de informação [22].

As abordagens tradicionais para modelagem de processos geralmente são um fluxo de atividades bem estruturadas que uma organização realiza para atingir seus objetivos. No entanto, nem todos os processos apresentam um controle claramente definido. Na realidade, os processos de negócios podem ser classificados de acordo com sua complexidade e estrutura [22].

Quanto à estrutura, um processo de negócio pode ser estruturado, semiestruturado ou não estruturado. Processos estruturados são completamente predefinidos, facilmente modelados e repetitivos, com uma sequência fixa de atividades. Processos semiestruturados combinam elementos de processos estruturados e não estruturados; para esses processos, o próximo passo não é predefinido para todas as atividades, mas apenas para algumas delas. Já os processos não estruturados têm um fluxo imprevisível de atividades, com frequentes variações de uma instância para outra, e geralmente envolvem ou trocam uma quantidade significativa de conhecimento durante sua execução [21].

2.4 Blockchain

Esta seção baseia-se no livro [23] ao explicar os conceitos necessários para entender melhor o funcionamento da tecnologia Blockchain.

Compreender sistemas distribuídos é essencial para entender o capítulo, uma vez que o Blockchain é uma tecnologia distribuída. Um sistema distribuído é um paradigma computacional que envolve dois ou mais nós trabalhando por um objetivo comum. Um nó é um ponto individual dentre a rede de usuários, podendo receber e transmitir informações para os demais nós.

Os nós podem operar de maneiras distintas: podem ser honestos, falhos, maliciosos e possuir seu próprio processamento e memória. Coordenar um sistema onde os nós têm comportamentos variados pode ser um grande desafio. O sistema deve ser tolerante a falhas, garantindo que o objetivo seja alcançado mesmo que parte dos nós falhe. Além

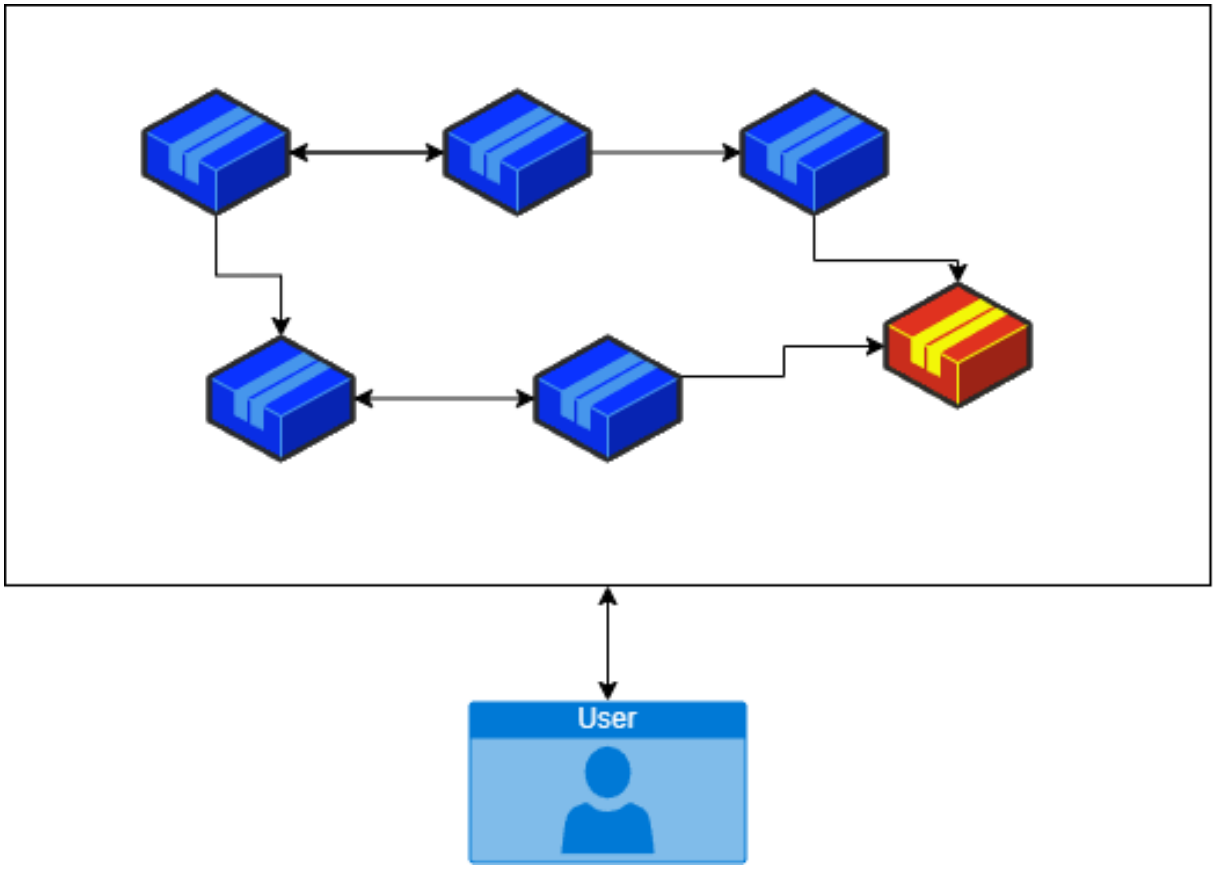

Figura 2.1: Redundância de nós em um sistema distribuído

das falhas de funcionamento não intencionais, é possível que um nó atue na tentativa maliciosa de quebrar o funcionamento da rede. A Figura 2.1 demonstra com simplicidade uma rede de nós com apenas um nó falho (na cor vermelha e amarela).

Em 2009, a primeira implementação prática do conceito foi realizada como lançamento do bitcoin, que utilizou o algoritmo *Proof of Work* (PoW) para atingir o consenso entre os nós. O consenso é um processo de aceitação entre os nós sobre o estado final dos dados. O mecanismo necessário para esse consenso deve atender aos seguintes requisitos:

Acordo: todos os nós honestos decidem o mesmo valor.

Terminação: todos os nós honestos terminam sua execução e chegam a uma decisão.

Validação: o valor acordado entre todos os nós honestos deve ser o mesmo e igual ao valor inicial de algum dos nós honestos.

Tolerância a falhas: o algoritmo de consenso deve ser hábil a executar mesmo na presença de nós maliciosos.

Integridade: os nós decidem apenas uma vez.

Outro conceito ligado ao Blockchain é o de *smart contract* que encapsula as regras de negócio que serão executadas em determinada condição. Sua característica principal é o funcionamento programado sem possibilidade de interferência de terceiros . Ou até mesmo como um conjunto de cláusulas contratuais que podem ser incorporadas em um software e um hardware para evitar sua violação/inadimplemento e controlá-lo por meios digitais [24].

Uma definição mais contextualizada de *smart contract* é apresentada por Sthéfano como um acordo unilateral ou bilateral, quase inviolável, previamente pactuado entre os integrantes, assim reduzido à linguagem computacional apropriada (algoritmos). Assim, o acordado é armazenado e executado em uma base de banco de dados descentralizado (Blockchain) [25].

2.4.1 Ansa Check

Um exemplo de projeto que aplica os conceitos abordados é o Ansa Check, uma iniciativa da agência de notícias italiana Ansa. Este projeto foi criado para combater a desinformação por meio de ferramentas e mecanismos eficazes.

Segundo o site oficial [26], o Ansa Check é uma tecnologia que visa abordar a verificação de informações por meio da automação. Utilizando um conjunto de algoritmos de inteligência artificial, incluindo a análise de linguagem natural, o projeto avalia a veracidade de notícias e informações.

O processo de verificação começa com a identificação de notícias e informações que possam ser falsas ou imprecisas. Analisado meio de uma combinação de fatores, como o uso de palavras-chave, a análise de dados e o monitoramento das redes sociais. As fontes incluem sites de notícias, blogs e redes sociais, permitindo que as notícias sejam avaliadas antes de serem publicadas.

Já o funcionamento é baseado em um amplo conjunto de dados de referência. O sistema compara o conteúdo de uma notícia recém-publicada com informações de fontes consideradas confiáveis e verifica a correspondência entre elas. Além disso, o sistema avalia a reputação da fonte da notícia e histórico de publicações anteriores.

Por outro lado, ferramentas automatizadas dependem da qualidade dos dados de referência. Caso os dados utilizados possuírem imprecisões, então as verificações ficam imprecisas. Ademais, a análise da linguagem natural utilizada pelas notícias pode possuir uma interpretação mais complexa do que os algoritmos suportam.

2.4.2 MOGPlay

Já na publicação de Inês Rito [27], os comportamentos no consumo das mídias sociais mudam em resposta às novas tecnologias, dando origem a um novo padrão de produção dos conteúdos.

Entre eles, o jornalismo de multidões representa uma nova forma de construir notícias democráticas, contando com cidadãos comuns que, ao estarem presentes em locais de notícias de última hora, capturam mídias relevantes usando seus dispositivos. Um exemplo que demonstra esse fato são os desastres naturais que os cidadãos frequentemente conseguem registrar e compartilhar mais rapidamente que as próprias equipe de jornalismos. Essa circunstância revela um *delay* da captura das mídias entre os dois grupos. Assim, há um espaço para atuação protagonizada tanto de cidadãos comuns e quanto de jornalistas profissionais.

O projeto ARTICONF propõe um conjunto de ferramentas confiáveis, resilientes e globalmente sustentáveis para o desenvolvimento de aplicações descentralizadas para atender a esta necessidade. O seu objetivo é superar as preocupações relacionadas com a privacidade, a confiança e a autonomia associadas às plataformas proprietárias de redes sociais inundadas por notícias falsas. Uma das ferramentas do ARTICONF é novo aplicativo para jornalismo coletivo chamado MOGPlay.

O MOGPlay se concentra no gerenciamento de conteúdo audiovisual gerado por cidadãos e fornece uma plataforma Blockchain com a arquitetura baseada em microserviços. Todas as partes envolvidas na produção profissional de notícias são recompensadas. Além da transmissão ao vivo, o MOGPlay oferece um mercado para negociação de conteúdo audiovisual entre cidadãos e jornalistas gratuitos, utilizando um token interno. Dessa forma, a plataforma fortalece a participação ativa dos cidadãos.

Um desafio do jornalismo de multidões é a qualidade dos conteúdos. Os usuários podem apresentar diferentes níveis de conhecimento sobre o assunto, o que pode levar a uma desigualdade na qualidade das informações. Além disso, certas regiões podem enfrentar dificuldades no acesso às ferramentas necessárias, resultando em menor contribuição para a base de conhecimento.

2.4.3 Nostr

A tecnologia Nostr adota uma abordagem colaborativa para a verificação de notícias, utilizando a sabedoria coletiva para validar as informações. A plataforma permite a participação ativa de leitores e especialistas no processo de verificação. Qualquer pessoa pode contribuir para a validação de uma notícia, tornando o processo democrático. As informações apresentadas nesta seção são baseadas no site oficial [28].

Nostr é um protocolo de comunicação descentralizado mas sem um servidor central ou controle corporativo. Em vez de usar Blockchain, o Nostr opera através de uma arquitetura *peer-to-peer* (P2P), onde os clientes (dispositivos dos usuários) se conectam a *relays* (servidores) para enviar e receber mensagens. Cada usuário é identificado por uma chave pública, e todas as postagens são assinadas digitalmente. Os dados são transmitidos em *relays* , que não se comunicam diretamente entre si, apenas com os usuários [29].

A verificação no Nostr é essencialmente um processo coletivo. Isso significa que várias pessoas podem se envolver na verificação da mesma notícia. As conclusões alcançadas por diferentes verificadores são comparadas e contrastadas, o que busca uma avaliação imparcial da notícia.

O Nostr enfrenta desafios relacionados à consistência dos dados devido à distribuição através de *relays* . A dependência desses *relays* pode causar inconsistências na entrega e sincronização das mensagens, resultando em possíveis atrasos ou falhas na comunicação, o que pode afetar a experiência do usuário. Ou seja, em alguns casos existe uma inconsistência dos dados entre diferentes nós.

Em suma, o Nostr oferece uma solução democrática para a verificação de notícias, ressaltando a importância da colaboração e transparência. No entanto, para atingir seu pleno potencial, o Nostr deve enfrentar desafios relacionados à qualidade das contribuições, coordenação entre verificadores, consistência dos dados e escalabilidade da plataforma.

2.4.4 Banco Central e o DREX

A implementação do sistema de autenticação de documentos baseado em Blockchain, desenvolvido nesta dissertação, é contextualizada também pela escolha do Banco Central do Brasil pelo Hyperledger Besu para a criação do Real Digital. Essa escolha sublinha a importância e a eficácia das tecnologias da Fundação Hyperledger, que abrange diversos *frameworks*, incluindo o Hyperledger Fabric, adotado para o sistema proposto.

O Hyperledger Besu foi selecionado pelo Banco Central devido à sua robustez e flexibilidade para aplicações financeiras complexas. Desenvolvido como um cliente da Ethereum, compatível com a EVM *(Ethereum Virtual Machine)*, o Besu oferece uma infraestrutura segura e eficiente para a emissão e gestão de moedas digitais, como o Real Digital. A tecnologia DLT (*Distributed Ledger Technology*) do Besu garante a imutabilidade dos registros e a execução de contratos inteligentes, essenciais para a transparência e segurança das transações financeiras. Além disso, o sistema permite a tokenização de ativos, uma abordagem fundamental para modernizar o sistema financeiro e promover a inclusão financeira [30] [31].

A implementação do Real Digital com o Hyperledger Besu é um exemplo claro de como a tokenização e a digitalização podem transformar o setor financeiro. Dados sobre

a evolução do sistema financeiro, a crescente importância dos dados e as tendências de produtividade demonstram o impacto potencial da tecnologia Blockchain na economia moderna. A digitalização e a redução de custos associados ao armazenamento e análise de dados são características chave que facilitam essa transformação [32].

Por outro lado, o Hyperledger Fabric, empregado no sistema de autenticação de documentos nesta dissertação, oferece características específicas para atender às necessidades de controle de privacidade e permissão de dados. O Fabric é projetado para redes privadas e permissionadas, adequadas para ambientes onde a integridade e a autenticidade dos dados são cruciais. Sua arquitetura modular e flexível permite a criação de soluções adaptadas a ambientes controlados, como o proposto para a autenticação de documentos.

A escolha do Banco Central pelo Hyperledger Besu fortalece a argumentação a favor do ecossistema Hyperledger na totalidade. A eficácia e a confiabilidade demonstradas pelo Besu em um projeto de alta relevância, como o Real Digital, evidenciam o potencial do ecossistema Hyperledger para atender a uma ampla gama de necessidades tecnológicas. Reforça assim a escolha do Hyperledger Fabric para o desenvolvimento do sistema de autenticação de documentos, evidenciando a versatilidade e a robustez das soluções oferecidas pela Fundação Hyperledger.

A comparação entre Hyperledger Besu e Hyperledger Fabric ressalta a flexibilidade do ecossistema Hyperledger para diferentes aplicações. Enquanto o Hyperledger Besu é ideal para ambientes financeiros e criptomoedas, o Hyperledger Fabric é mais adequado para redes privadas e permissionadas, como o sistema de autenticação de documentos. A escolha criteriosa do *framework* para cada aplicação específica demonstra a capacidade do ecossistema Hyperledger em fornecer soluções eficazes e adaptáveis para diversos contextos [33].

Capítulo 3

Arquitetura Proposta

3.1 Arquitetura da Rede Hyperledger Fabric

Para explicar a arquitetura, foram elaborados diagramas que representam a estrutura proposta para a aplicação. Cada diagrama demonstra os componentes ou um fluxo de utilização dos componentes pelo usuário. O primeiro diagrama na Figura 3.1 apresenta uma visão geral da aplicação. Composta por três aplicativos: rede de testes Hyperledger Fabric, *gateway* de conexão segura e *frontend*. Cada aplicativo possui um função indispensável. O cerne da aplicação é a utilização da rede Blockchain para armazenamento seguro dos registros. Já para obter requisições de sucesso é necessário ter sucesso na integração com o *gateway* que possui os caminhos dos certificados responsáveis pela autorização das requisições. Por último, temos o componente do *frontend* que utiliza ferramentas do Google Firebase para implementar suas funcionalidades.

Na Figura 3.1 em *fabric-samples* foi definido a estrutura mínima para funcionamento do Blockchain. Porém, por se tratar de um sistema distribuído ter a redundância de cada componente é necessário, em caso de falhas. Por isso, a Figura 3.2 exibe a arquitetura configurada da rede inicial do Hyperledger Fabric.

A Figura 3.2 apresenta os componentes da arquitetura utilizada. PEER1 e PEER2 são os nós (pares do inglês peer) do Blockchain. Os pares hospedam o *smart contract* e uma cópia do *ledger*. LEDGER representa as cópias do livro-razão. Além dos nós, um servidor denominado ORDERER é essencial para determinar a ordem das operações a serem registradas no livro-razão. No contexto do Hyperledger Fabric, o *smart contract* é o código que define a estrutura do ativo e as funções de acesso do Blockchain.

Os *smart contracts* S1 e S2 são responsáveis por definir como as funções de leitura, escrita e atualização dos registros no *ledger* compartilhado devem ser realizadas.

No Hyperledger Fabric, o livro razão (*ledger*) é uma estrutura composta por duas partes principais. O primeiro componente é o estado do mundo (*world state*), que é uma

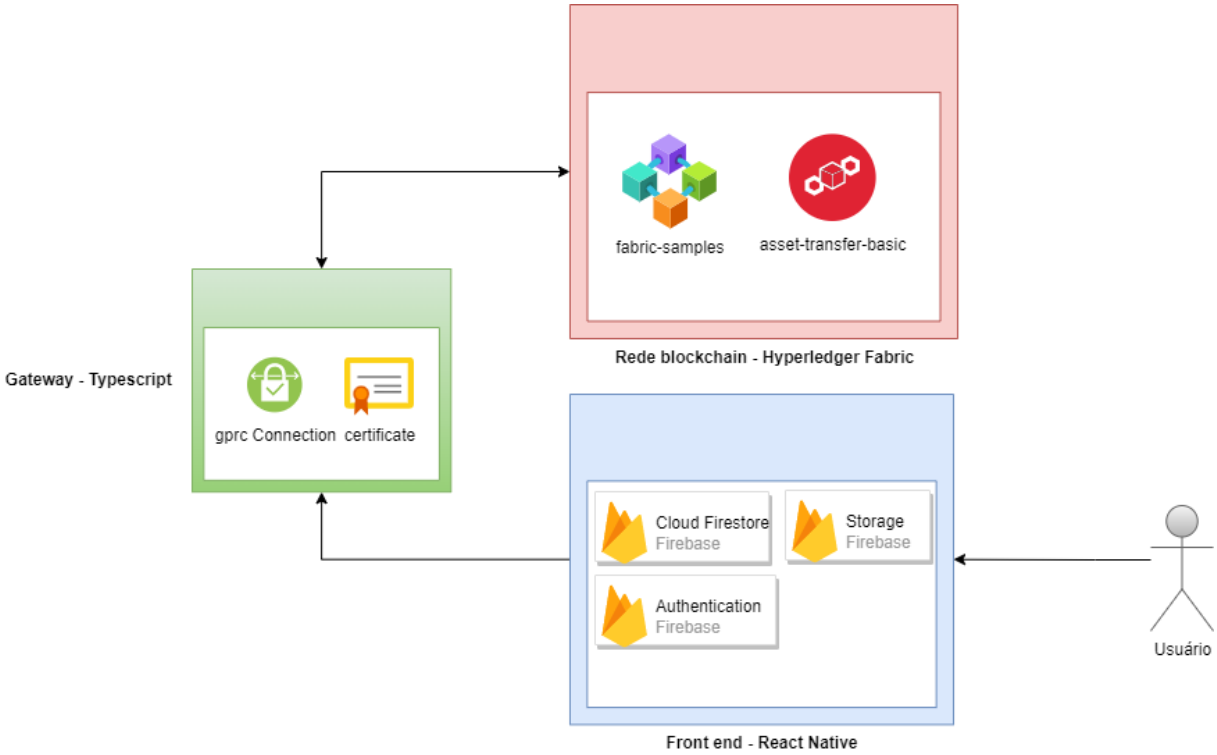

Figura 3.1: Visão geral da aplicação

base de dados que armazena os valores atuais do livro razão, permitindo acesso direto às informações. O segundo componente é a blockchain, ou seja, um log de transações imutável que registra todas as modifciações feitas até o estado atual, oferecendo o histórico completo e auditável das transações.

Para identificar uma organização é emitido um certificado próprio (CA) que identifica cada uma das organizações CA0, CA1 e CA2. CHANNEL é um canal de comunicação que interliga os nós e as aplicações do Blockchain, ou seja direcionando as execuções das aplicações para seus respectivos responsáveis. CC1 são as informações de configuração do canal. Cada organização possui um nome, um ID e um diretório MSP (Provedor de Serviços de Membro), onde informações de segurança, como políticas, são armazenadas. Políticas detalham quem pode realizar operações como leitura, escrita e administração dentro da organização.

São as organizações que gerenciam os pares. No diagrama PEER1 faz parte de R1 e PEER2 de R2. R0 possui a função apenas de ordenamento, então não realiza votações e está associado ao canal. Ou seja, para qualquer decisão final, é necessário alcançar um consenso mediante votação das organizações. Na rede, a configuração geral do canal é denominada CC1 e deve ser aprovada pelas organizações envolvidas para estar em vigor.

No âmbito do canal, as organizações R1 e R2 têm a responsabilidade de adicionar pares,

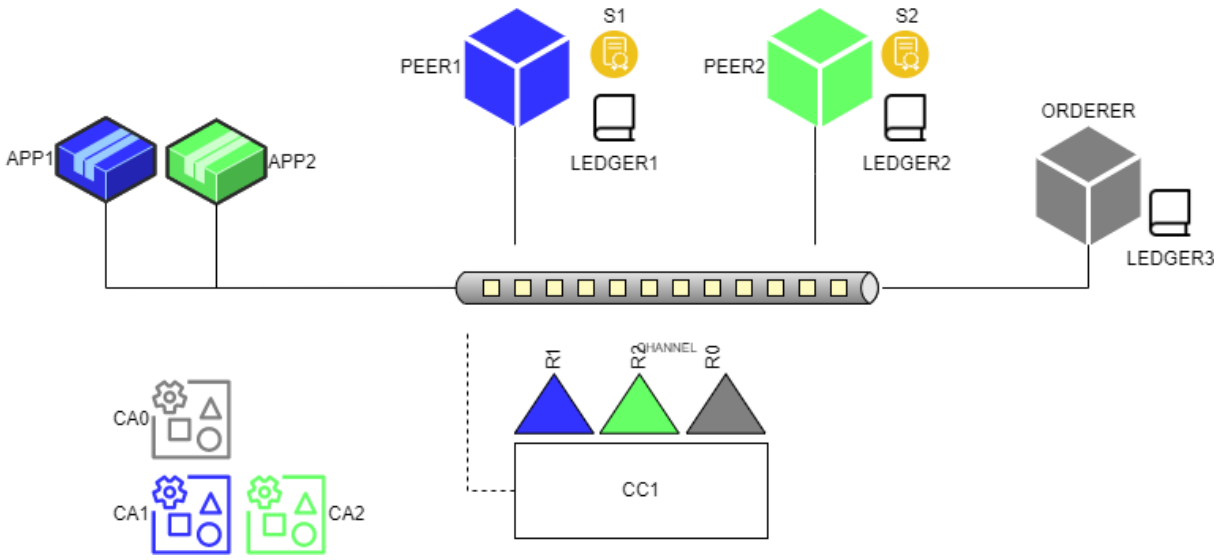

Figura 3.2: Rede de testes Hyperledger Fabric. Fonte: Adaptado de hyperledger-fabricdocs, Creative Commons.

identificados como o PEER1 e PEER2, a uma subdivisão designada como CC1. Enquanto isso, a organização R0 desempenha o papel de supervisionar o serviço de ordenação do canal, representado como ORDERER. É de suma importância ressaltar que todos esses nós, independentemente de suas funções individuais, mantêm uma cópia idêntica do livro-razão (LEDGER) do canal. É neste registro que todas as transações são inscritas de forma imutável. Pode ser enfatizado que o serviço de ordenação lida apenas com o aspecto de registro das transações, sem se preocupar com o estado atual dos ativos ou com quaisquer outros detalhes das transações.

Adicionalmente, para interagir com o canal e, por conseguinte, com toda a rede, as organizações R1 e R2 possuem suas respectivas aplicações, denominadas APP1 e APP2. Através dessas aplicações, é possível o envio e recebimento de informações do canal. Um ponto de importância a ser observado é que cada uma das organizações envolvidas na rede possuem uma Autoridade de Certificação (CA). Componente encarregado de geração dos certificados dentro de cada organização.

3.2 Arquitetura da Aplicação

3.2.1 *Gateway* de Conexão

Após a definição da arquitetura e configuração da rede Blockchain, a próxima etapa é a criação do *gateway* que integra as funcionalidades externas da aplicação com a rede Blockchain. Oferece uma interface para lidar com solicitações e transações na rede, ou

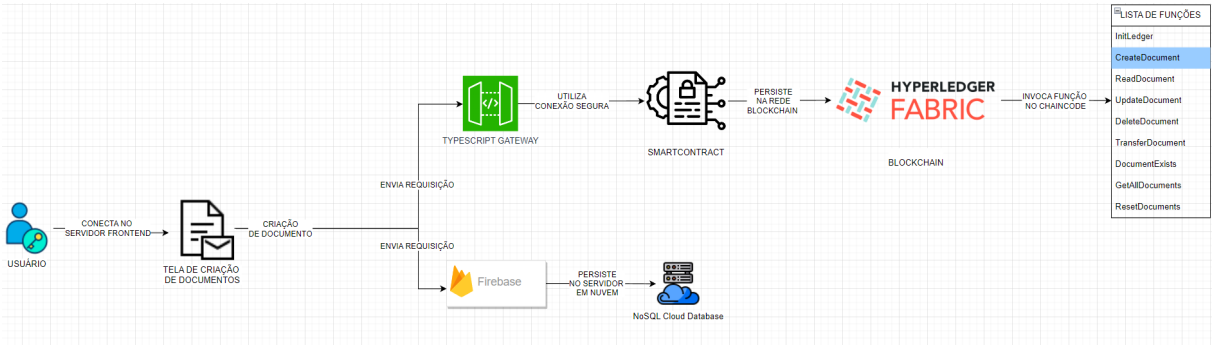

Figura 3.3: Diagrama sobre Criação de Documentos

seja, formaliza a interação entre o usuário e o servidor de acesso. O *gateway* possui sua função bem delimitada resumida por dois tópicos representados no seu componente da Figura 3.1. São eles: conexão segura *gRPC* e os certificados criptográficos necessários para transações no Blockchain. Cabe ressaltar, que o *gateway* também é uma aplicação própria.

A Figura 3.3 mostra a utilização do *gateway* para a criação de documentos

O *gateway* atua como um intermediário entre a camada de apresentação da aplicação e a infraestrutura Blockchain. Sua função é a intermediação das requisições originadas no *frontend*, convertendo-as em transações compreensíveis para a rede Blockchain.

Ademais, o *gateway* possui os certificados necessários para interagir com a rede Blockchain. Por isso, apenas as aplicações com esses recursos conseguem produzir requisições válidas. Em outras palavras, o *gateway* estabelece conexões seguras com os componentes da rede Blockchain. Consiste no papel da comunicação entre a aplicação e a rede, sendo responsável pelo envio de transações para a Blockchain e pelo recebimento de respostas. Isso garante que as operações solicitadas pelo *frontend* sejam efetivamente registradas no *ledger* da rede Blockchain.

O tratamento de erros e respostas é outra função crítica do *gateway*. Em cenários onde ocorrem erros durante o processamento das transações, o componente deve gerenciar essas situações e fornecer respostas apropriadas para o *frontend*. Isso inclui o tratamento de exceções, a detecção de falhas na validação das transações e a gestão de situações inesperadas, contribuindo para uma experiência do usuário mais robusta e confiável. Fica definido então que a disponibilização das funcionalidades para o usuário final são tratadas a nível de *gateway* .

3.2.2 *Frontend*

No sentido de disponibilizar o uso da aplicação para um usuário final, a escolha estratégica do React como a tecnologia para o *frontend* da aplicação é destacada. Essa camada é responsável por fornecer as interfaces: de criação, autenticação, modificação e leitura de documentos.

O React, uma biblioteca JavaScript mantida pelo Facebook, destaca-se pela eficiência no desenvolvimento de interfaces de usuário devido à sua estrutura de componentes independentes e reutilizáveis. Em aplicações complexas, essa componentização facilita a organização, manutenção e escalabilidade do código. Além disso, o React oferece suporte robusto à integração com outras tecnologias, como Blockchain, tornando-o adequado para funcionalidades diversificadas. Sua estrutura modular simplifica o processo de criação de documentos, e sua escolha para o *frontend* é fundamentada na eficiência, usabilidade e integração. [34].

A escolha do React como tecnologia para o *frontend* da aplicação é fundamentada na busca por uma arquitetura que alinhe usabilidade e integração. A componentização e suporte à integração diversificada fazem do React uma escolha estratégica para atender às exigências de uma aplicação que visa facilitar a autenticação de documentos em ambientes jornalísticos.

Aliado ao *frontend* em React a aplicação utiliza algumas ferramentas do Google Firebase para implementar funcionalidades desejáveis à aplicação. O Cloud Firestore é utilizado como banco de dados NoSQL para armazenar registros de documentos no formato de chave-valor. Já o Authentication gerencia a autenticação dos usuários, garante assim o controle de acesso seguro da plataforma. Por fim, o Storage do Firebase é responsável pelo armazenamento de arquivos, no caso do projeto são as imagens associadas às notícias. Os elementos do *frontend* podem ser visualizados em Figura 3.4

Banco de Dados em Nuvem

Concomitantemente à interação com a rede Blockchain Hyperledger Fabric, a aplicação incorpora uma abordagem híbrida, em que as requisições dos usuários podem ser encaminhadas para dois destinos distintos. Isto pode ser observado no diagrama da Figura 3.3. Além do *gateway* que direciona as operações para a Blockchain, as requisições também são processadas pelo banco de dados em nuvem denominado Cloud Firestore uma ferramenta da plataforma Firebase da Google. Este desempenha um papel fundamental na armazenagem e gerenciamento de informações complementares à operação da aplicação, dessa forma servindo como um livro de rascunho para os registros antes de persistência final no livro-razão.

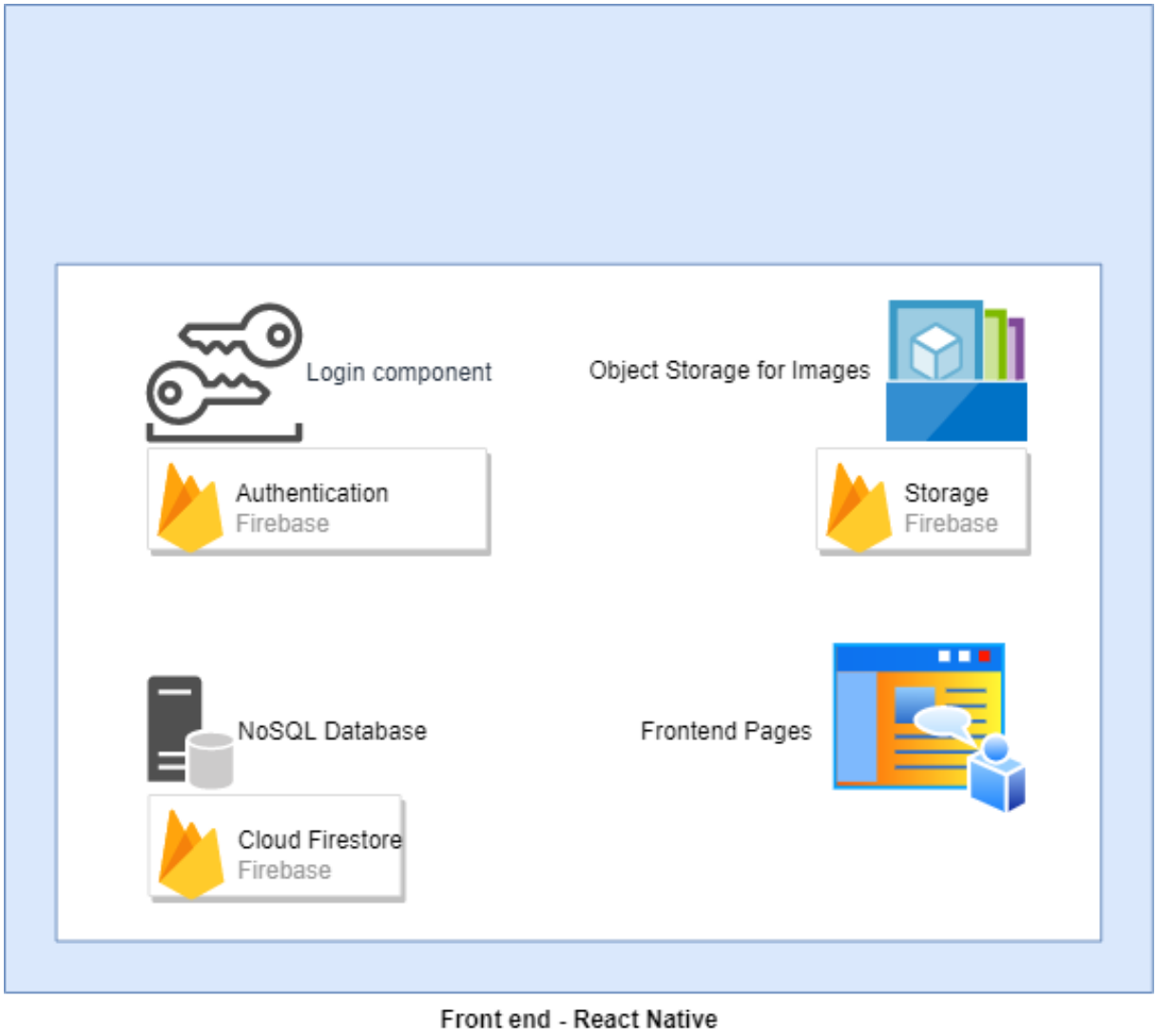

Figura 3.4: Visão geral do frontend

Essa abordagem possibilita um suporte provido da implementação para oferecer funcionalidades auxiliares de armazenamento e processamento de dados. Uma das características mais notáveis do uso de um banco de dados NoSQL é a utilidade como repositório para informações relacionadas à aplicação, tais como informação do usuário e outros dados necessários para promover o uso da aplicação.

Por esse motivo, é interessante a separação de dados estratégicos que necessitam de imutabilidade garantidas pela Blockchain daqueles que são dinâmicos, adequados ao ambiente do Firebase. Afinal, é possível que um documento fique apenas na versão de desenvolvimento e nunca chegue no estado de notícia publicada. O Cloud Firestore proporciona flexibilidade e escalabilidade para o armazenamento e recuperação de dados com baixo tempo de resposta, facilitando a implementação de funcionalidades de interatividade e

atualização instantânea.

Portanto, a aplicação emprega dois bancos de dados distintos para atender a diferentes necessidades. A Blockchain, por meio do Hyperledger Fabric, concentra-se em manter registros transacionais imutáveis e seguros para notícias já publicadas. Enquanto o Google Firebase, com seu Cloud Firestore, oferece uma infraestrutura complementar que permite o armazenamento e a recuperação eficaz das matérias jornalísticas, contribuindo para uma experiência do usuário mais dinâmica. Também facilitando a criação funções auxiliares para aplicação como um centro de documentação privada da redação jornalística.

Camada de Login

Para o controle de acesso da aplicação, a funcionalidade sugerida opera em conjunto com o *frontend* para a etapa de autenticação de usuários. A ferramenta utilizada é denominada Firebase Authentication.

Neste sentido, quando um usuário acessa inicialmente a aplicação, ele é redirecionado para a tela de login, onde é obrigatório fornecer credenciais válidas para continuar. Somente após a autenticação bem-sucedida, o usuário da redação jornalística acessa à tela inicial da aplicação, desbloqueando todas as funcionalidades e recursos disponíveis.

Dentre as funcionalidades disponíveis, é notável que as requisições compreendem tanto operações de leitura quanto de escrita, permitindo aos usuários acessar, criar, atualizar e autenticar documentos na rede Blockchain. Oferecendo uma experiência funcional aos usuários, capacitando-os a gerenciar e verificar informações na Blockchain de acordo com seu nível de acesso.

Fluxo de Autenticação de Documentos

Com as funcionalidades anteriores prontas para execução, então é delineado a etapa de autenticação de documentos, que garante a validade dos registros. Para realizar essa autenticação, é requerida a presença de um usuário autorizado, denominado revisor. Também é necessário um usuário permitido para criação do documento, sendo este o próprio revisor ou não. Estes usuários têm permissão para acessar as telas específicas de suas ações, como a autenticação, que interage com os registros previamente armazenados e realizar verificações de validação.

O processo inicia-se quando um usuário autorizado registra na aplicação um novo documento ou modifica campos de um documento existente (Figura 3.5). Em seguida, o revisor faz login na aplicação e utiliza a funcionalidade de autenticação de documentos. Nesta tela, é feito a busca por meio identificador do documento que possibilita recuperar os estados de validação de cada campo existente. Por meio de uma interface intuitiva, o

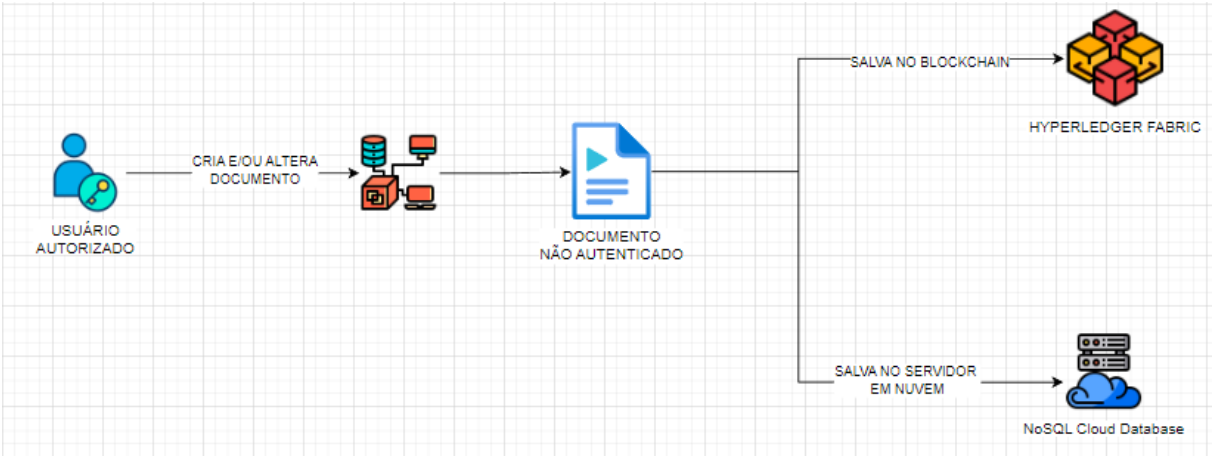

Figura 3.5: Interação usuário na etapa de autenticação

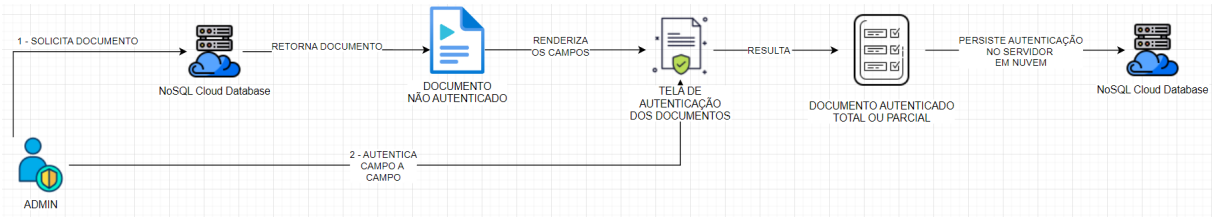

Figura 3.6: Interação revisor na etapa de autenticação

revisor pode selecionar os campos do documento que deseja autenticar, confirmando sua validade. O fluxo do revisor é representado na Figura 3.6.

Uma vez que o revisor conclui a seleção dos campos a serem autenticados, a aplicação facilita o processo de envio dessas informações para a coleção correspondente no Google Firebase. Este passo mantém um registro organizado das ações de autenticação, permitindo a rastreabilidade das atividades realizadas.

Ao realizar o envio, os dados são devidamente registrados no Cloud Firestore. Assegura assim que as informações relacionadas à autenticação sejam armazenadas de forma acessível em tempo real para os usuários autorizados.

As funções de criação e autenticação de documento desempenham papéis complementares para estabelecer um fluxo de autenticação de documentos. Combinando as funções, o fluxo de autenticação é estabelecido da seguinte forma: o usuário cria o documento, enquanto o revisor verifica e autentica os campos aprovados. Somente os documentos que receberam a validação total do revisor são considerados válidos na rede Blockchain, criando um sistema sólido de autenticação de documentos.

Apresentação da Metodologia de Validação utilizando Ontologia

Uma ontologia oferece uma abordagem modular para definir os elementos operacionais ou de um domínio, permitindo que tais definições sejam reutilizáveis e compartilháveis [35]. Contrasta com a organização de dados baseada em sistemas estruturados convencionais de banco de dados relacionais, devido ao valor semântico atribuído aos elementos a serem descritos, já que as ontologias são consideradas "mundos abertos"[36].

Neste contexto, foi desenvolvido uma Ontologia para Processos Intensivos em Conhecimento (KIPO abreviação em inglês), com correspondências a uma ontologia que descreve os conceitos do Scrum [37]. O objetivo é classificar e organizar semanticamente um processo que inicialmente não possui estrutura definida, utilizando seus conceitos fundamentais: artefatos, atividades, processos, agentes e regras de negócio. Com isso, fornecer um contexto claro para um ambiente colaborativo, facilitando a resolução de problemas.

A integração da KIPO com os conceitos de Ontologia do Scrum proporciona uma descrição completa de processos complexos em tempo de execução, funcionando como uma ontologia de tarefa e fornecendo instruções altamente aplicáveis para o contexto das tarefas desejadas [38].

A utilização da modelagem de informação por meio de ontologias apresenta a vantagem de permitir a expansão direta dos conceitos necessários [35]. Por exemplo, é possível instanciar um documento, como um item do Backlog, e então atribuir a esse item uma proposição lógica que deve ser validada. Com o uso de ontologias é possível modelar um conjunto de proposições que direcionam ao fluxo desejado. No contexto deste estudo, que aborda a redação jornalística dinâmica, a integração entre Scrum e KIPO deve ser suficiente para atingir os objetivos da prova de conceito. Dado que cada ontologia pode ser traduzida para uma tarefa no contexto do Scrum. Já o documento pode ser observado como a história a ser concluída no Scrum também.

Sobre o processo de autenticação de documentos, é utilizado para confirmar a veracidade dos campos a ontologia que age como o mecanismo de validação iterando sobre todos os campos e proposições definidas, a fim de confirmar o *status* do documento. O diagrama que estamos prestes a apresentar é uma representação visual do processo citado. Começa quando um usuário autorizado inicia a solicitação para recuperar o *status* de um documento, solicitando que a ontologia Scrum entre em ação. Por esse motivo é resgatado os registros no banco de dados do Google Firebase, onde a coleção sobre *status* do documento é armazenada. Após resgatado os registro com detalhes de autenticação, então o código em Typescript é capaz de dizer se existe ou não uma versão totalmente autenticada.

Essa representação visual ajudará a compreender o processo, destacando as interações entre a ontologia Scrum, o Firebase e os campos do documento. É uma peça importante

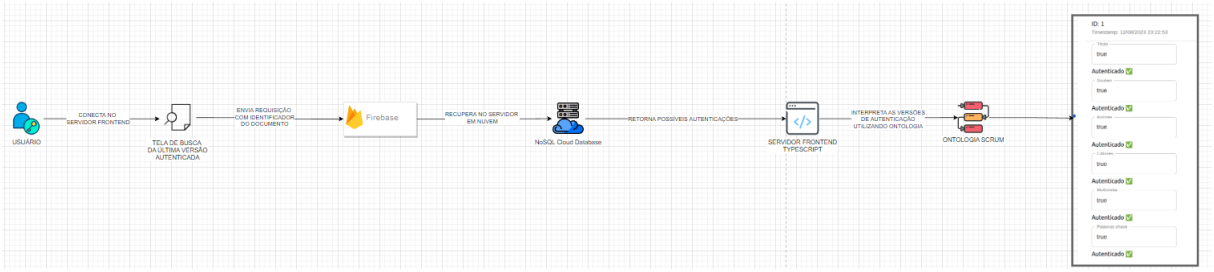

Figura 3.7: Recupera última versão autenticada via ontologia

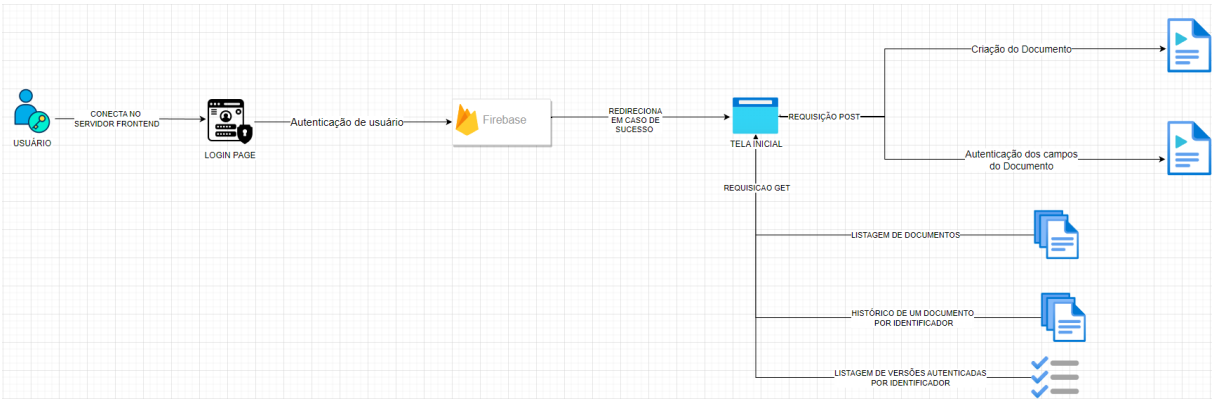

Figura 3.8: Diagrama sobre o fluxo do aplicativo

no versionamento das autenticações dos dados no Blockchain.

Demais Funcionalidades

Além disso, existem operações de leitura com a capacidade de listar documentos, recuperar documentos específicos por meio de um identificador único (ID), acessar o histórico de autenticação de um documento específico para fins de rastreamento e também resgatar apenas a última versão autenticada de um documento. Portanto, essa gama de funcionalidades garante que os usuários possam tanto consultar informações quanto contribuir para a integridade da Blockchain.

Na conclusão deste capítulo, apresentamos uma visão abrangente da arquitetura proposta para a aplicação. Esta arquitetura é composta por três camadas principais: a rede Blockchain Hyperledger Fabric, o *gateway* de conexão em Typescript e o *frontend* de interação com o usuário, cada um desempenhando um papel fundamental na funcionalidade geral da aplicação.

A rede Blockchain Hyperledger Fabric fornece a base para armazenar e gerenciar documentos com segurança. Ela garante que os registros sejam à prova de adulteração, um requisito crítico para documentos confiáveis.

O *gateway* de conexão em Typescript age como uma interface intermediária que permite que o *frontend* da aplicação interaja de forma segura com a rede Blockchain. Ele disponibiliza métodos e funcionalidades para criar, autenticar e consultar documentos na rede, simplificando a complexidade subjacente da Blockchain.

O *frontend* de interação com o usuário é a face visível da aplicação, onde os usuários podem criar novos documentos, autenticar campos desses documentos e acessar informações detalhadas sobre os registros. A ontologia Scrum também é hospedada nessa parte da aplicação e desempenha a função de validação dos campos e proposições dos documentos.

No próximo capítulo, exploraremos em detalhes a implementação prática dessa arquitetura, destacando os desafios encontrados e os resultados alcançados. Ao final deste estudo, espera-se que a arquitetura proposta tenha fornecido uma solução eficaz para a criação e autenticação de documentos para uma redação jornalística, contribuindo para maior segurança e confiabilidade nas transações de documentos.

Capítulo 4

Implementação

4.1 Visão Geral da Implementação

A implementação da arquitetura exigiu um planejamento cuidadoso, com cada etapa conduzindo à seguinte. Tudo começa com a configuração da rede, uma base sólida para que as interações subsequentes possam ocorrer. A partir dessa fundação, os demais componentes foram integrados de maneira que a evolução do sistema ocorresse de forma orgânica.

O primeiro passo, foi a criação da rede Hyperledger Fabric, ponto central para o funcionamento de todo o sistema. Com essa estrutura configurada, foi possível avançar para a definição e implementação das regras que definem as transações dentro dessa rede, através dos *smart contracts*. Os contratos, determinam as condições sob as quais os dados são manipulados.

Com a rede funcional, existe a possibilidade de comunicação interna na rede. Para isso, os canais foram criados, permitindo uma segmentação controlada das transações. A capacidade de gerenciar as permissões dentro da rede garantiu que os diferentes participantes possam interagir de forma independente, segundo as regras estabelecidas.

Com a estrutura interna consolidada, foi a vez de preparar a interface de comunicação entre os usuários e a rede. O *gateway* passou a ser o ponto de contato entre a rede blockchain e requisições externas. A implementação do *gateway*, ao se integrar com os contratos e canais já em funcionamento, permitiu que as operações começassem a ser utilizadas de maneira simples pelo *frontend*.

Seguindo essa linha de progresso, o desenvolvimento do *frontend* trouxe a interação direta com o usuário. Por meio de uma interface acessível, as funcionalidades da rede blockchain começaram a ser expostas, oferecendo o ponto de contato entre o usuário e a infraestrutura já montada. A escolha de *React Native* para esse propósito facilitou o desenvolvimento de uma interface simples.

Paralelamente, o uso do Firebase para armazenamento de dados e autenticação foi introduzido de maneira a complementar o que já estava funcionando. A flexibilidade oferecida por esse banco de dados secundário ajudou a lidar com a necessidade de um armazenamento mais dinâmico. Enquanto, a autenticação de usuários foi facilitada pelo integração nativa entre as ferramentas do Firebase.

Por fim, a ontologia *Scrum* foi incorporada ao processo de autenticação de documentos. Esse modelo organizacional trouxe uma camada de simplicidade e previsibilidade ao gerenciamento das etapas de autenticação, permitindo que os processos fossem completados de forma coordenada. Com os demais componentes devidamente implementados, a etapa final relacionada às ontologias pôde ser integrada, acrescentando a validade do conteúdo dos campos de cada documento e a alternativa de inclusão de regras de negócio adicionais para concluir uma autenticação para o documento.

4.2 Implementação e Manipulação da Rede Hyperledger Fabric

A configuração inicial da rede é facilitada através da clonagem de um repositório base disponível publicamente no GitHub [39]. Este repositório, denominado *fabric-samples*, contém *scripts* e exemplos fundamentais para a criação e o gerenciamento de uma rede local de Hyperledger Fabric. Ao clonar este projeto, os desenvolvedores têm acesso a uma série de *scripts* que automatizam processos complexos, permitindo uma experimentação prática com o Hyperledger Fabric. A estrutura inicial da rede padrão *fabric-samples* fornecida pelo *framework* Hyperledger Fabric é composta por duas organizações de nós (*peers*) e uma organização de ordenadores (*orderers*).

Os *scripts* fornecidos no diretório da rede de teste oferecem diversas opções para configuração e operação da rede. Entre essas opções, destaca-se a inicialização dos nós da rede, a criação e configuração de canais, a implantação de *smart contracts* e a capacidade de desligar a rede quando necessário. Cada uma dessas operações exige um entendimento dos componentes da rede e dos conceitos subjacentes do Hyperledger Fabric.

Por exemplo, o modo de operação para iniciar os nós da rede estabelece a infraestrutura básica necessária para o funcionamento da rede de Blockchain, enquanto a criação de canais envolve a configuração de canais privados que permitem transações específicas entre grupos de participantes. A implantação de *smart contracts* é uma etapa importante que envolve a instalação e a instância de contratos inteligentes, exigindo uma compreensão da lógica de programação e do fluxo de deploy dos contratos. Por outro lado, o comando para desligar a rede permite a desativação controlada da infraestrutura, o que é relevante para realizar manutenções e testar o comportamento da rede em condições de parada.

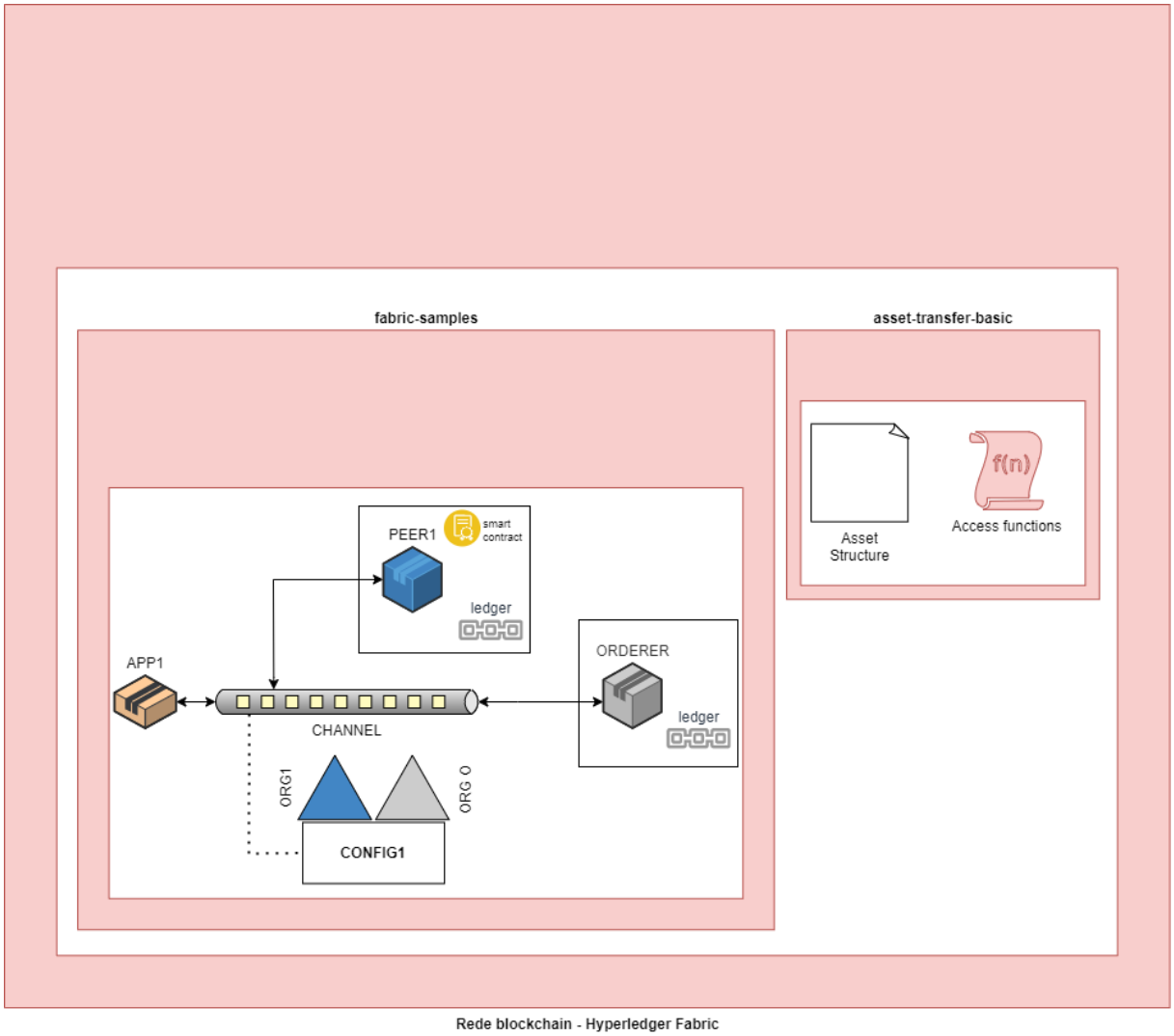

Figura 4.1: Componentes únicos - Rede Blockchain

O aprendizado adquirido através da documentação oficial do Hyperledger Fabric é significativo. A documentação detalha os fundamentos do Hyperledger Fabric, incluindo a arquitetura, a configuração e a operação dos componentes da rede. Fornece também orientações sobre melhores práticas, exemplos de configuração e casos de uso que ajudam a entender como aplicar o *framework* em cenários reais. O estudo dessas documentações permite não apenas o domínio das funcionalidades básicas do Hyperledger Fabric, mas também a capacidade de personalizar e otimizar a rede para atender a requisitos específicos de desenvolvimento e aplicação.

Esses *scripts* oferecem um nível elevado de personalização e são projetados para simplificar o processo de aprendizado e teste, proporcionando uma compreensão mais aprofundada dos princípios e das práticas de operação do Hyperledger Fabric. A utilização eficaz desses recursos exige uma familiarização com a arquitetura da rede, o funcionamento

dos componentes e as melhores práticas de configuração e segurança. Assim, apesar da automação fornecida pelos *scripts*, a operação completa e eficiente da rede exige um conhecimento técnico sólido e a habilidade para adaptar os processos às necessidades específicas do desenvolvimento e da aplicação.

4.3 Implementação dos Componentes da Aplicação

4.3.1 Implantação do *Smart contract*

O *smart contract* é o componente que executa as transações na rede, definindo as regras e a lógica de negócios que governam a interação com o livro-razão distribuído. A implantação do *smart contract* permite que operações específicas sejam executadas na rede e registrem transações no livro-razão.

Durante o processo de *package*, é possível especificar diversas configurações, como o nome, a linguagem de programação, a versão implantada e o caminho para o código-fonte do *smart contract*. A correta implantação é uma etapa crítica na configuração de uma rede Hyperledger Fabric, pois define como as transações serão processadas e validadas pela rede.

Estrutura de Dados e suas Funções de Manipulação

O código do *smart contract* segue a estrutura de dados de um programa em Go e utiliza a biblioteca *hyperledger/fabric-contract-api-go/contractapi* [40] para a implementação adequada dos *smart contracts*. Dessa forma, as funções e transações são capazes de efetivar a execução na rede. A principal finalidade deste é permitir operações com o livro-razão, como a criação, leitura, atualização e exclusão de documentos.

A definição das transações envolve a estruturação do ativo que será registrado e manipulado na rede Blockchain. Para o nosso caso de estudo, essa estrutura compreende inicialmente a versão dos documentos que serão armazenados e gerenciados na rede. Para definir a estrutura do ativo é disponibilizado a aplicação *asset-transfer-basic* interna do repositório *fabric-samples*, veja na Figura 4.1. Neste projeto *asset-transfer-basic*, é disponibilizado uma estrutura padrão e um template das funções e bibliotecas necessárias para geração correta do binário do *smart contract*.

É importante destacar que os campos atribuídos a esse registro são os próprios elementos de autenticação do documento, constituindo uma parte fundamental do processo completo de autenticação de documentos.

Detalhando a estrutura *Document*, cada campo é projetado para armazenar um atributo específico do documento, como título, autores, editores, conteúdo, palavras-chave,

```go
import (
    "encoding/json"
    "fmt"
    "github.com/hyperledger/fabric-contract-api-go/contractapi"
)

type SmartContract struct {
    contractapi.Contract
}

type Document struct {
    ID         string `json: "id"`
    Title      string `json: "name"`
    Soutien    string `json: "soutien"`
    Text       string `json: "text"`
    Authors    string `json: "authors"`
    Editors    string `json: "arrival_time"`
    Multimedia string `json: "multimedia"`
    Keywords   string `json: "keywords"`
}
```

Figura 4.2: Estrutura de Dados utilizada para armazenar os Documentos no livro-razão

entre outros. A Figura 4.2 apresenta a estrutura utilizada para representar os documentos na aplicação, segue também por uma breve descrição da finalidade de cada campo.

ID: Identifica de maneira exclusiva cada documento no livro-razão.

Title: Armazena o título do documento.

Soutien: Armazena o resumo do documento, fornecendo uma visão geral do conteúdo.

Text: Armazena todo o corpo do texto.

Authors: Mantém os nomes dos autores que contribuíram para a criação do documento.

Editors: Mantém os nomes dos editores que revisaram e aprovaram o documento antes de sua publicação.

Multimedia: Indica o tipo de conteúdo multimídia associada ao documento, como texto, imagem, áudio ou vídeo. No trabalho, foi utilizado o conteúdo textual, mas há possibilidade de expansão.

Keywords: Contém palavras-chave que ajudam a categorizar e identificar o conteúdo do documento, facilitando a pesquisa e a organização.

Funções de Manipulação dos Ativos na Blockchain

Depois, são definidas as funções que possibilitam a manipulação dos ativos na Blockchain. Essas funções implementam a lógica de negócios por trás de cada operação definida no

```go
func (s *SmartContract) ReadDocument(ctx contractapi.TransactionContextInterface, id string) (*Document, error) {
    documentJSON, err := ctx.GetStub().GetState(id)
    if err != nil {
        return nil, fmt.Errorf("failed to read from world state: %v", err)
    }
    if documentJSON == nil {
        return nil, fmt.Errorf("the document %s does not exist", id)
    }

    var document Document
    err = json.Unmarshal(documentJSON, &document)
    if err != nil {
        return nil, err
    }

    return &document, nil
}
```

Figura 4.3: Função de leitura no Smart Contract

smart contract, garantindo que as operações sejam executadas conforme as políticas de governança da rede.

A Figura 4.3 apresenta um trecho de código com a função utilizada na leitura de um documento do *smart contract*. A seguir, uma breve descrição de todas as funções disponíveis:

InitLedger: Responsável por inicializar o *ledger* com documentos de exemplo. Popula o *ledger* com informações iniciais que representam documentos jornalísticos, como título, autores, editores e palavras-chave.

CreateDocument: Cria novos documentos no *ledger*. Recebe informações como título, autores, editores e palavras-chave de entrada e armazena esses atributos no *ledger*.

ReadDocument: Permite a leitura de um documento específico no *ledger*. A partir do ID do documento fornecido, busca os detalhes correspondentes no *ledger* e retorna as informações do documento.

UpdateDocument: Atualiza os atributos de um documento existente no *ledger*. Recebe um ID de documento como entrada, verifica se o documento existe e atualiza os detalhes conforme necessário.

DeleteDocument: Exclui um documento do *ledger* com base em seu ID. Verifica se o documento existe e, em seguida, remove-o do *ledger*.

TransferDocument: Transfere a propriedade de um documento de um autor para outro. Recebe o ID do documento e o novo autor como entrada, atualizando as informações de autoria.

DocumentExists: Verifica se um documento com o ID fornecido existe no *ledger*.

GetAllDocuments: Obtém uma lista de todos os documentos presentes no *ledger*.

ResetDocuments: Redefine todos os documentos no *ledger,* removendo-os completamente. É útil para fins de teste e limpeza do *ledger*.

Com a conclusão da implementação das funções do *smart contract*, a próxima etapa é o *deploy*, necessário para garantir que o código esteja disponível conforme as definições estabelecidas.

Primeiramente, o *smart contract* é empacotado em um arquivo contendo todos os componentes necessários para sua execução futura. Esse pacote é então instalado nos nós da rede, assegurando sua disponibilidade para execução após a aprovação.

Durante a fase de aprovação do *smart contract* no Hyperledger Fabric, todas as organizações que fazem parte do canal são convidadas a revisar e votar sobre a definição proposta. Cada organização pode emitir um voto a favor, contra ou, em alguns casos, optar por se abster, caso não tenha uma posição clara sobre a proposta.

O consenso é alcançado com base na votação das organizações, sendo necessário que a maioria delas aprove a definição do *smart contract* para que ele seja aprovado. Esse mecanismo garante que todas as partes envolvidas concordem com o código a ser implantado na rede.

Após a aprovação pela maioria das organizações no canal, a definição do *smart contract* é considerada oficial e é então confirmada no canal. Significa que a versão aprovada do *smart contract* é registrada no *ledger* compartilhado da rede, tornando-se uma parte integrante do mesmo. Assim, as transações solicitadas pelo *smart contract* ficam disponíveis para interação com o livro-razão.

4.3.2 Implantação dos Canais

A criação de canais é fundamental para o funcionamento da rede Hyperledger Fabric, pois eles são responsáveis por receber transações e invocar as funções correspondentes no *smart contract*, sendo essenciais para a execução das operações. Os canais também desempenham o papel de aprovação do *deploy* de *smart contracts*, exigindo uma votação entre as organizações participantes para a implantação de um novo código-fonte. Além disso, a gestão dos acessos é realizada através das políticas de permissão que determinam as ações permitidas para cada organização ou nó. Alterações nessas políticas podem ser feitas, desde que aprovadas pelas organizações envolvidas [41].

A capacidade de segmentar o acesso aos dados por meio da criação de canais é uma característica marcante do Hyperledger Fabric. Isso permite que as organizações compartilhem informações de maneira seletiva, garantindo a confidencialidade e a privacidade

necessárias para diversas operações. Por exemplo, uma redação jornalística pode melhorar a colaboração entre sua equipe interna e colaboradores externos sem comprometer a confidencialidade das histórias em desenvolvimento.

Nesse contexto, as organizações desempenham um papel vital nos canais do Hyperledger Fabric. Cada organização representa um conjunto de participantes com responsabilidades compartilhadas, como escritores, editores, revisores e gerentes em uma redação jornalística. Cada organização contribui com seus representantes, que participam das discussões e deliberações. Essa estrutura organizacional permite uma abordagem colaborativa e estruturada para a criação e autenticação de documentos, garantindo a integridade e a transparência ao longo de todo o processo editorial. Além disso, as decisões tomadas no canal são baseadas em protocolos e políticas estabelecidos pelas organizações.

4.3.3 Implementação do *Gateway*

Após concluir a etapa de aprovação e registro do *smart contract* na rede, avança-se para a fase de invocação e execução das operações definidas. Essas operações podem ser iniciadas por solicitações provenientes do *frontend* da aplicação ou de outras fontes de entrada. Cada solicitação contém as informações necessárias e o contrato pertinente para a execução da operação.

A solicitação de transação é enviada ao *gateway,* de conexão, que atua como intermediário entre o *frontend* e a rede Blockchain. O gateway valida a solicitação, verificando a precisão dos parâmetros e assegurando que o usuário tenha as permissões apropriadas para realizar a operação. Os aplicativos podem invocar as operações definidas no *smart contract* por meio de chamadas de função no *gateway*, que se encarrega de formatar os parâmetros da transação e garantir sua integridade durante o processo.

Uma das funções do *gateway* é o gerenciamento de identidades, que permite a autenticação segura das transações. Utilizando certificados digitais, o *gateway* assegura que apenas entidades autorizadas possam realizar transações. Assim, a máquina responsável pelo *gateway* deve ter sua identidade e acessos comprovados por meio de certificados digitais.

Na implementação do *gateway* em TypeScript, utilizou-se a biblioteca *hyperledger/fabric-gateway*, que oferece diversas funcionalidades essenciais para interagir com a rede Hyperledger Fabric [42].

Como descrito anteriormente, a integração do *gateway* com a rede Blockchain é possibilitada pelos certificados digitais, que validam a identidade da aplicação durante o processo de conexão. A classe importada da biblioteca padrão encapsula as operações principais, como a conexão com a rede, a submissão de transações e as consultas de es-

```
app.get('/documents', async (req: Request, res: Response) => {
    try {
        const contract = await newContract();
        const result = await contract.evaluateTransaction('GetAllDocuments');
        res.json(JSON.parse(utf8Decoder.decode(result)));
    } catch (error) {
        res.status(500).send(error);
    }
});

async function getAllDocuments(contract: Contract): Promise<void> {
    console.log('\n--> Evaluate Transaction: GetAllDocuments, function returns all the current Documents on the ledger');

    const resultBytes = await contract.evaluateTransaction('GetAllDocuments');

    const resultJson = utf8Decoder.decode(resultBytes);
    const result = JSON.parse(resultJson);
    console.log('*** Result:', result);
}
```

Figura 4.4: *Endpoint* e respectiva função de leitura do *Gateway*

tado. Através dessa classe, os aplicativos podem se comunicar com a rede Blockchain conhecendo apenas o contrato de comunicação estabelecido pelo *gateway.*

O primeiro passo é estabelecer uma conexão segura com a rede, o que envolve a verificação de informações para autenticação. Com a conexão estabelecida com sucesso, inicia-se a interação com a rede e o resgate do *smart contract* para a submissão das transações.

A integração pode ser ilustrada com o exemplo da criação de um novo documento jornalístico. O aplicativo invoca a função **createDocument**, fornecendo os parâmetros necessários. O objeto responsável por instanciar o *smart contract* constrói a transação com base nesses parâmetros e a submete à rede.

Outro exemplo, também mostrado na Figura 4.4, é a função **getAllDocuments**, que resgata a lista de todos os documentos. Nesse caso, somente o contexto atual do *smart contract* é necessário, pois não são requeridos parâmetros adicionais. Ao chamar esse método, a funcionalidade verifica a presença dessa função na rede e, se existente, retorna uma lista de todos os documentos.

Com a implementação bem-sucedida do *gateway* de conexão, alcança-se um marco significativo no desenvolvimento da aplicação. Pois, abstrai a complexidade da interação com a rede Blockchain, permitindo que o desenvolvimento de funcionalidades auxiliares seja mais direto, concentrando os esforços na criação de novas funcionalidades em vez de se preocupar com detalhes técnicos da integração com a Blockchain.

Além disso, a modularidade do design arquitetural facilita a manutenção e a expansão do código ao longo do tempo. Novas funcionalidades podem ser adicionadas com relativa facilidade, e as classes podem ser reutilizadas em diferentes contextos.

Este capítulo abordou como a conexão segura é estabelecida e como os *smart contract*s são utilizados para realizar transações na rede Hyperledger Fabric. A combinação de

configurações de segurança robustas, conexões criptografadas e interações eficientes com os *smart contracts* demonstra uma compreensão sólida dos princípios de Blockchain e segurança da informação. A capacidade de utilizar as bibliotecas e APIs de maneira eficaz reflete o conhecimento adquirido durante o trabalho com essas tecnologias.

4.3.4 Implementação do *Frontend* Utilizando React Native

A implementação do *frontend* da aplicação é responsável pela interação com o usuário final. Para esse propósito, foi escolhida a ferramenta React Native, fundamentada em sua capacidade de oferecer uma experiência de usuário de alta qualidade e eficiência no desenvolvimento.

A seleção do React Native como a tecnologia para o *frontend* foi motivada por fatores reconhecidos na indústria. Desenvolvido no repositório do Facebook, o React Native é um *framework* que utiliza JavaScript para criar aplicativos móveis [43]. Essa abordagem proporciona benefícios significativos:

- **Ampla Comunidade e Suporte:** a comunidade ativa em torno do React Native proporciona fácil acesso à documentação, tutoriais e bibliotecas de terceiros, acelerando o processo de desenvolvimento [44].
- **Performance Comparável a Nativos:** o React Native permite a criação de aplicativos com desempenho próximo ao de aplicativos nativos, oferecendo uma experiência de usuário fluida e responsiva [34].
- **Desenvolvimento Eficiente:** a reutilização de componentes e lógica de negócios entre aplicativos móveis e web, por meio do uso de JavaScript, melhora a eficiência do desenvolvimento [45].

No escopo específico do projeto, optou-se por uma abordagem simplificada no desenvolvimento das interfaces. A decisão de simplificar o design das telas baseou-se na premissa de que a funcionalidade deve ser visível e acessível ao usuário, permitindo um esforço maior na compreensão e integração com a rede Blockchain.

O fluxo da aplicação pode ser visualizado na Figura 3.8. A seguir, serão apresentadas as telas de interação disponibilizadas no *frontend*.

A tela inicial da aplicação, conforme mostrado na Figura 4.5, é a tela de login, utilizada para autenticar o usuário antes do acesso às funcionalidades da aplicação.

Após a autenticação, o usuário é redirecionado para a página inicial. Nesta página, é apresentado um breve resumo das funcionalidades disponíveis no autenticador de documentos. A tela inicial é ilustrada na Figura 4.6.

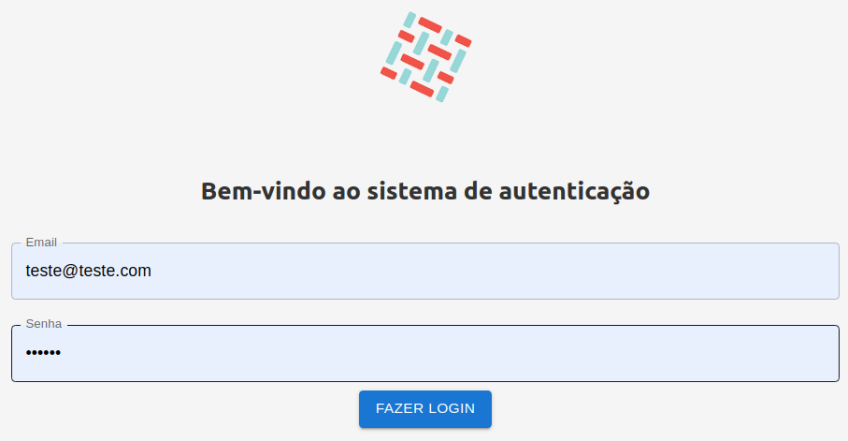

Figura 4.5: Tela de Login

Na página inicial, o usuário pode escolher entre a: criação e autenticação de documentos, conforme ilustrado nas Figuras 4.7 e 4.8. Além disso, o usuário pode acessar outras funcionalidades, como a listagem das versões autenticadas de um documento e a visualização de registros já persistidos na rede Blockchain. A tela adicional possibilita intervenções manuais, em caso de necessidade. Pode ser vista na Figura 4.9

4.3.5 Google Firebase para Banco de Dados Secundário e Etapa de Login

Após a implementação das etapas essenciais da aplicação, como a rede de testes Hyperledger, o *gateway* e o *frontend*, foi observada uma boa utilização do Cloud Firestore como banco de dados secundário na arquitetura proposta. O Cloud Firestore, uma solução oferecida pela plataforma Firebase, é um banco de dados NoSQL que proporciona flexibilidade e escalabilidade para armazenamento e consulta de dados com baixo tempo de resposta, sendo uma escolha estratégica para a implementação da solução.

A escolha do Cloud Firestore como banco de dados secundário foi baseada em fatores estratégicos. Primeiramente, a flexibilidade necessária na estrutura e no conteúdo das ontologias na etapa de autenticação evidenciou a necessidade de um modelo de dados adaptável. Diferentemente do modelo de armazenamento em uma rede Blockchain, onde mudanças nas estruturas exigem um consenso entre os participantes, o Cloud Firestore permite armazenar dados de forma adaptável através de sua estrutura de documentos e coleções, eliminando a necessidade de um esquema rígido.

Existem vantagens significativas associadas a essa escolha. O Cloud Firestore, com seu modelo de documentos e coleções, permite armazenar ontologias de autenticação que apresentam campos distintos dependendo do contexto.

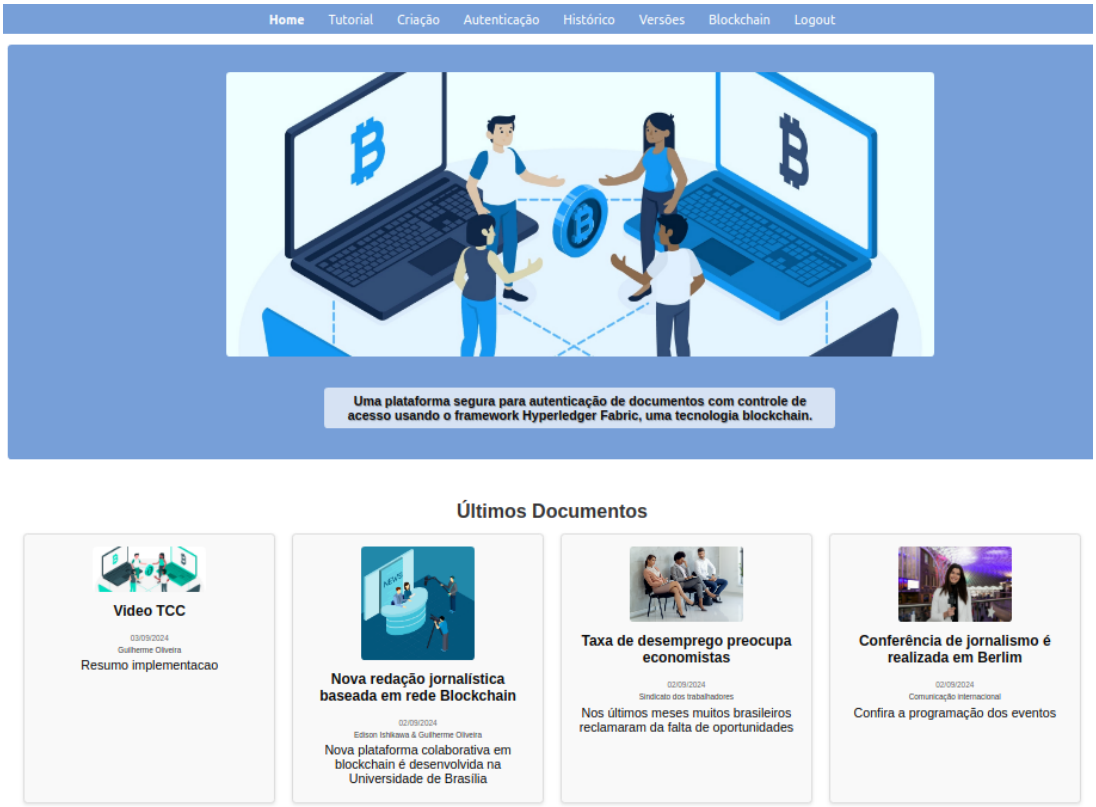

Figura 4.6: Página inicial

Além disso, a integração nativa com o serviço de Firebase Authentication da Google simplifica consideravelmente o gerenciamento de identidades e a autenticação de usuários. Os usuários, por exemplo, podem fazer login usando suas contas do Google, eliminando a necessidade de criar um sistema de autenticação do zero. O Firebase Authentication oferece recursos avançados de segurança, como autenticação multifator e verificação de e-mail, fortalecendo ainda mais a camada de segurança do sistema.

Com a integração do Firebase Authentication, o sistema de autenticação Blockchain adiciona uma camada adicional de segurança. A autenticação do usuário se torna um processo mais rigoroso, envolvendo tanto a verificação do Firebase quanto a validação de identidade via certificados no Blockchain, garantindo que as interações sejam realizadas somente por usuários devidamente autorizados.

Outra vantagem notável na escolha do Cloud Firestore é a abundância de recursos de documentação oficial fornecidos pelo Google Firebase. Esta documentação aborda desde conceitos básicos até casos de uso avançados, como modelagem de dados, consultas complexas e otimização de desempenho. Além disso, a comunidade Firebase é ativa, proporcionando fóruns e grupos de discussão para compartilhamento de conhecimentos e resolução de problemas. Esta documentação reduz a complexidade da integração do

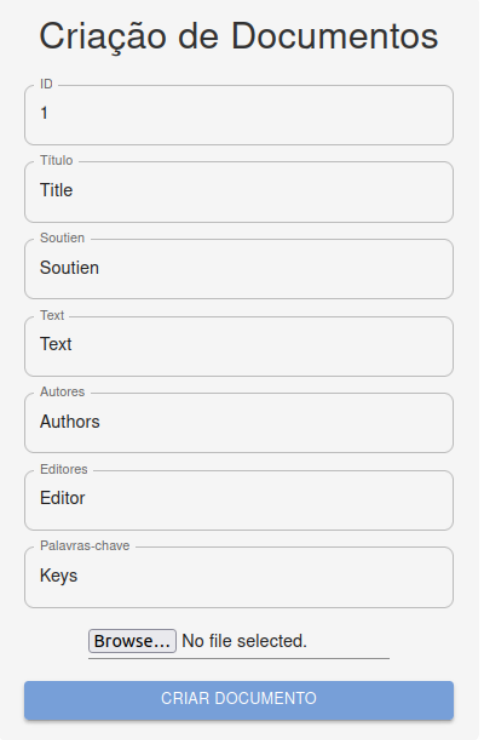

Figura 4.7: Criação de documentos

Firestore na aplicação e permite que os desenvolvedores alcancem resultados rapidamente [46].

Coleções no Firestore

No Firestore, os dados foram organizados em duas coleções principais relacionadas aos documentos: *documents* e *documentsStatus*. Essas coleções estão ilustradas na Figura 4.10. A coleção *documents* armazena os mesmos campos registrados na rede Blockchain, oferecendo redundância que contribui para a tolerância a falhas. Por outro lado, a coleção *documentsStatus* é responsável por armazenar o histórico de autenticação dos campos do documento. A coleção de usuários é armazenada separadamente na seção específica de autenticação de usuários.

Devido à flexibilidade inerente ao modelo NoSQL, as estruturas de dados no Firestore podem ser ajustadas com facilidade para atender a novas necessidades e requisitos, sem a rigidez dos esquemas pré-definidos. O banco de dados Firebase atua como banco de dados secundário, funcionando como um *blackboard* na arquitetura proposta. Neste contexto, o *blackboard* desempenha a função de um espaço de trabalho flexível e adaptável para a homologação e teste de mudanças. Durante o desenvolvimento e ajuste de novas funcionalidades, o esquema no Firestore pode ser alterado e novos elementos adicionados

Figura 4.8: Autenticação de documentos

sem impactar diretamente o sistema produtivo da Blockchain. Isso permite um ambiente de teste dinâmico, onde mudanças podem ser validadas e refinadas antes de serem persistidas na Blockchain, garantindo que apenas alterações verificadas e ajustadas sejam incorporadas ao sistema final.

4.3.6 Ontologia Scrum

A implementação dos componentes fundamentais da aplicação foi concluída. Agora, pode-se finalizar a implementação com o último recurso para autenticação de documentos: a ontologia. A aplicação da ontologia Scrum simplifica o processo de autenticação ao garantir a execução das etapas de acordo com procedimentos e regras definidas. Cada tarefa de autenticação pode ser associada a um campo do documento. Posteriormente, a conclusão da autenticação de um documento segue a lógica do Scrum, onde todas as tarefas precisam ser concluídas para que a história, ou seja, a autenticação completa do documento, seja finalizada.

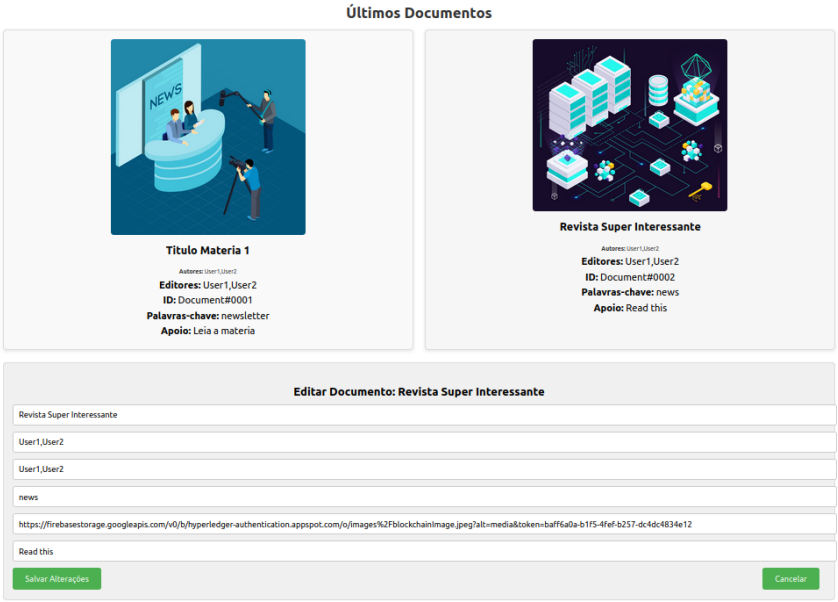

Figura 4.9: Tela de registros no Blockchain

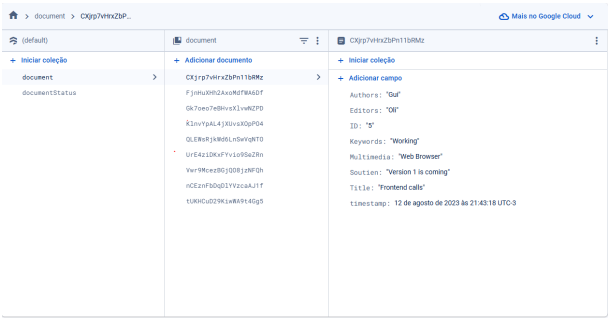

Figura 4.10: Coleções sobre Documentos no Google Firebase

No caso da autenticação parcial de um documento, apenas alguns campos são validados inicialmente. O progresso para a autenticação total ocorre à medida que todas as tarefas de autenticação são concluídas, validando todos os campos necessários. Este processo permite uma compreensão gradual do *status* de autenticação do documento, partindo de uma validação parcial para alcançar a validação completa.

Como introduzido na ferramenta Google Firebase, discute-se como os estados de cada campo são armazenados na coleção *documentsStatus* do banco de dados em nuvem. A escolha de um banco de dados NoSQL, como o Firestore, é fundamental devido à sua capacidade de armazenar ontologias de forma flexível. Permite não apenas a gestão dos estados dos campos, mas também oferece um ambiente propício para a criação dinâmica de novos campos e a definição de proposições lógicas.

O Firestore facilita aos usuários a adição de novos campos personalizados conforme necessário, além de permitir a definição de lógicas proposicionais para validar esses campos. Uma proposição lógica é uma sentença que pode ser avaliada como verdadeira ou falsa [47]. Essa funcionalidade é essencial para que os usuários possam adaptar a estrutura de autenticação de documentos de acordo com requisitos específicos da área negocial, ampliando as possibilidades dos processos intensivos em conhecimento. A opção de campos adicionais pode ser visualizado no último campo no inferior da Figura 4.8.

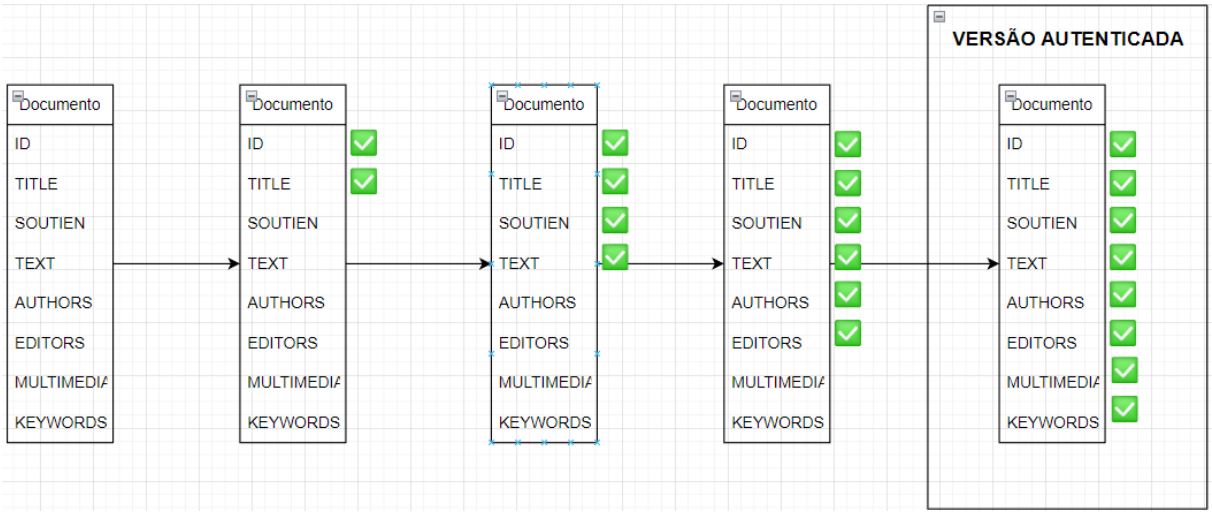

Figura 4.11: Fluxo de Autenticação das Ontologias.

Neste capítulo, foram explorados os principais componentes e etapas envolvidos na criação da prova de conceito para autenticação de documentos. A aplicação abrangeu áreas como integração de tecnologias distribuídas, desenvolvimento de *smart contracts* e gestão de processos intensivos em conhecimento (KIP). A adoção da ontologia Scrum proporcionou uma abordagem estruturada para a autenticação, permitindo a divisão eficiente dos documentos em tarefas específicas.

A configuração da rede Blockchain Hyperledger Fabric desempenhou um papel fundamental ao estabelecer uma base robusta para garantir a integridade e a rastreabilidade dos documentos autenticados. Paralelamente, o uso do Firestore como banco de dados NoSQL ofereceu flexibilidade para armazenar diversas ontologias e suportar a criação dinâmica de campos e proposições lógicas.

Ao integrar essas tecnologias, o projeto demonstrou sua capacidade de fornecer solução para instituições que necessitam de processos eficientes de autenticação documental. Por exemplo, no jornalismo, isso poderia significar a validação precisa e auditável de informações antes da publicação, garantindo a credibilidade e a precisão das notícias.

Além disso, enfatizou-se a importância do *peopleware* na fase de autenticação pós-criação do documento. A intervenção humana continua essencial para validar e assegurar que os critérios definidos pela ontologia Scrum sejam integralmente cumpridos, mantendo a confiança no processo de autenticação.

A conclusão bem-sucedida da prova de conceito abre caminho para futuros desenvolvimentos, incluindo a expansão de funcionalidades e a aplicação de testes rigorosos. Este avanço representa um passo significativo em direção ao objetivo de desenvolver um sistema de autenticação de documentos adaptável e funcional, alinhado com as demandas contemporâneas de segurança e eficiência.

Capítulo 5

Conclusão

5.1 Contribuições e Relevância do Projeto

O projeto ofereceu uma solução prática para a autenticação de documentos no ambiente jornalístico, utilizando o Hyperledger Fabric, um *framework* Blockchain de código aberto e permissionado. A escolha deste *framework* permitiu a criação de uma rede Blockchain privada adaptada às necessidades específicas de uma redação jornalística.

O sistema desenvolvido utiliza a tecnologia Blockchain para garantir a integridade dos documentos, que são registrados de forma criptografada e distribuída. Abordagem que fortalece a segurança dos documentos e promove maior transparência nas operações jornalísticas. A descentralização proporcionada pela Blockchain evita a dependência de uma única entidade centralizada. Em vez disso, a tecnologia favorece uma rede colaborativa onde a validação é realizada de maneira distribuída. Aumentando a confiança no sistema, pois a integridade dos documentos é garantida por uma rede de participantes, e não por um único ponto de controle. Este modelo descentralizado reduz o risco de fraudes, uma vez que qualquer tentativa de alterar informações exigiria a concordância da maioria dos membros da rede.

Outro aspecto significativo do projeto foi a criação de uma interface de usuário desenvolvida em React, que facilita a interação com o sistema. Esta interface oferece uma experiência clara e acessível, permitindo que jornalistas e outros profissionais possam criar, autenticar e verificar documentos de forma eficiente. A abordagem granular da autenticação, que permite a validação campo a campo dos documentos, é particularmente relevante para o ambiente jornalístico, onde a precisão e a veracidade das informações são importantes.

O sistema também permite uma gestão eficiente das responsabilidades dentro da redação. A arquitetura do sistema suporta diferentes papéis interativos, como escritores, revisores e administradores, refletindo a estrutura de interações de diferentes níveis nas re-

dações. Esta flexibilidade melhora a eficiência dos fluxos de trabalho e facilita a adaptação às necessidades de cada organização jornalística.

A combinação do Hyperledger Fabric com uma interface desenvolvida em React demonstra a importância de considerar a usabilidade ao desenvolver soluções tecnológicas. O sistema foca na experiência do usuário final, garantindo que a tecnologia Blockchain possa ser utilizada de maneira acessível por profissionais com diversos níveis de experiência técnica. Dessa forma, projeto contribui para o campo da tecnologia Blockchain e oferece uma resposta adaptada às necessidades das redações jornalísticas na era digital.

5.2 Desafios e Limitações

A fase experimental do projeto, ainda que limitada pelo contexto de um trabalho de conclusão de curso, demonstrou com sucesso a funcionalidade esperada da aplicação, atingindo seus objetivos primários. A implementação de uma arquitetura baseada no Hyperledger Fabric, em conjunto com outras tecnologias, como TypeScript no *gateway* e React no *frontend*, exigiu um planejamento detalhado e apresentou desafios significativos de integração.

Um dos principais obstáculos foi conciliar as três aplicações, cada uma com suas próprias especificidades tecnológicas. A necessidade de separar o *gateway* do *frontend* tornou-se evidente durante o desenvolvimento, uma vez que as dependências entre as tecnologias eram empacotadas em formatos distintos. Inicialmente, a primeira tentativa foi fazer com que o *frontend* autorizasse diretamente as requisições para a rede blockchain, mas falhas surgiram devido à incompatibilidade nos formatos binários de empacotamento. Isso forçou a reestruturação da arquitetura, evidenciando a complexidade ao realizar a integração de tecnologias distintas. Essa descoberta foi fundamental para o sucesso da aplicação, que passou a operar de forma mais modular.

Além disso, o projeto foi replicado no laboratório da Universidade de Brasília, onde a rede foi configurada em máquinas distintas das usadas no desenvolvimento. Nessa etapa, foram testadas todas as funcionalidades. A aplicação foi visualizada por alunos e professores, incluindo o orientador do projeto, o que permitiu um primeiro nível de análise do sistema.

Apesar de a aplicação ter funcionado conforme o esperado, a fase experimental não incluiu testes mais robustos com um número maior de usuários ou em condições de produção. A limitação de tempo – cerca de um ano – reservada ao desenvolvimento do projeto restringiu a possibilidade de avaliações mais amplas quanto à escalabilidade, usabilidade e acessibilidade da solução. No entanto, essa limitação também abre espaço para estudos

futuros, que poderão aprofundar essas questões em cenários de maior complexidade e com uma base de usuários mais diversificada.

Portanto, a fase experimental foi bem-sucedida dentro dos objetivos estabelecidos, apesar dos desafios inerentes ao desenvolvimento de um sistema completo a partir do zero. A integração entre diferentes tecnologias foi superada, e a aplicação mostrou-se funcional. Testes mais extensivos em ambientes de produção permanecem como uma etapa a ser explorada em futuros desenvolvimentos, oferecendo novas oportunidades para validar a solução em larga escala.

5.3 Impacto e Aplicações Práticas

A adoção do sistema de autenticação de documentos baseado em Blockchain, desenvolvido ao longo desta dissertação, representa uma possibilidade para o campo do jornalismo. A principal contribuição do sistema é a melhoria da integridade e transparência dos documentos jornalísticos. Utilizando o Hyperledger Fabric para registrar os documentos de forma criptografada e imutável, o sistema permite que usuários confiem na autenticidade das informações. Em uma era de crescente desinformação, a capacidade de verificar a origem e a veracidade dos documentos é fundamental para manter a confiança do público.

A gestão mais eficiente das responsabilidades dentro das redações é outro benefício importante. A capacidade de gerenciar papéis como escritores, revisores e administradores ajuda a organizar o fluxo de trabalho dentro da redação, definindo diferentes níveis de interação na produção de conteúdo de qualidade. Ajustes nessa área podem resultar em um processo editorial mais eficaz, com a responsabilidade pela autenticação dos documentos com passos bem definidos.

A possibilidade de expansão para autenticar diferentes tipos de mídia é uma potencial aplicação prática do sistema. Atualmente, o sistema se concentra na autenticação de documentos, mas pode ser adaptado para autenticar imagens, códigos, websites e outros tipos de conteúdo digital. A expansão para diferentes tipos de mídia ampliaria a utilidade do sistema e atenderia a uma variedade maior de necessidades na era digital.

A abordagem adotada pode estimular o desenvolvimento de novas soluções baseadas em Blockchain, incentivando a inovação em tecnologias distribuídas. A combinação de Blockchain com interfaces amigáveis e soluções práticas pode servir como modelo para outras implementações tecnológicas, oferecendo soluções para problemas semelhantes em diversos domínios. Integrar tecnologias distribuídas com práticas acessíveis abre novas possibilidades para criar novas soluções.

5.4 Perspectivas Futuras

A presente pesquisa abre diversas possibilidades para o desenvolvimento de aplicativos baseados em Blockchain no campo da comunicação. Especificamente, a aplicação desenvolvida demonstra a viabilidade da modernização na manipulação das estruturas de dados na comunicação web. O uso de Blockchain pode transformar como os dados são gerenciados, oferecendo uma solução para garantir a integridade das informações em plataformas jornalísticas. Isto inclui a criação de um sistema de verificação de fatos descentralizado e um modelo de desenvolvimento coletivo para projetos jornalísticos, ambos fundamentais para assegurar a qualidade e a independência no jornalismo moderno.

Além disso, a pesquisa destaca a importância da tokenização e descentralização das informações. A tokenização permite uma representação digital dos ativos, o que pode aumentar a segurança das transações. A descentralização contribui para uma maior democratização do poder, permitindo que múltiplos moderadores participem da gestão das informações, reduzindo a concentração de controle e melhorando a confiabilidade das publicações.

Outro aspecto relevante para o futuro é a potencial integração de soluções de Blockchain com tecnologias emergentes, como a Inteligência Artificial (IA). A combinação dessas tecnologias pode melhorar significativamente a análise de dados, otimizar processos de autenticação e ampliar as capacidades dos sistemas descentralizados. A integração de IA pode permitir a detecção automática de inconsistências e anomalias, além de promover a personalização dos serviços oferecidos.

O uso do Hyperledger não só fortalece a confiabilidade das aplicações desenvolvidas, mas também demonstra a adaptabilidade da tecnologia Blockchain para diferentes necessidades. Este exemplo reforça a validade do uso do Hyperledger Fabric para a autenticação de documentos, evidenciando seu papel em aprimorar as práticas na comunicação. A escolha do ecossistema Hyperledger como tecnologia para a implementação do sistema é ainda mais respaldada pela sua adoção por instituições de relevância, como o Banco Central do Brasil, que utiliza o Hyperledger para sua própria solução de Blockchain. Evidencia dessa maneira a robustez do framework para aplicações de alta complexidade, fortificando a decisão de utilizar o Hyperledger Fabric no desenvolvimento do sistema proposto [30] [31].

Em síntese, o projeto não apenas proporciona uma solução para a autenticação de documentos, mas também serve como um modelo para futuras implementações tecnológicas no campo da comunicação. A integração de Blockchain com uma interface intuitiva e a gestão eficiente dos fluxos de trabalho demonstram o potencial transformador da tecnologia na modernização das operações jornalísticas.

Referências

[1] Ghinea, Gheorghita, Benedito Medeiros Neto, Maria de Fátima Ramos Brandão e Edison Ishikawa: *The communication, coordination, cooperation, and connection dimensions, when using framework and collaborative systems in the newsroom—a case study in the bbc london.* Digital Convergence in Contemporary Newsrooms: Media Innovation, Content Adaptation, Digital Transformation, and Cyber Journalism, páginas 63–85, 2022. 1

[2] Wang, Xiaowan, Huiyin Xie, Shan Ji, Liang Liu e Ding Huang: *Blockchain-based fake news traceability and verification mechanism.* Heliyon, 2023. 1

[3] Junior, Walter Teixeira Lima: *Big data, jornalismo computacional e data journalism: estrutura, pensamento e prática profissional na web de dados.* Estudos em Comunicação, 12:207–222, 2012. 1

[4] Ireton, Cherilyn e Julie Posetti: *Journalism, fake news & disinformation: handbook for journalism education and training.* Unesco Publishing, 2018. 1, 2

[5] Li, Mia Shuang: *What can blockchain actually do for journalism*, 2020. 2

[6] Iansiti, Marco, Karim R Lakhani *et al.*: *The truth about blockchain.* Harvard business review, 95(1):118–127, 2017. 2

[7] Christofoletti, Rogério e Guilherme Longo Triches: *Interesse público no jornalismo: uma justificativa moral codificada.* Revista Famecos, 21(2):484–503, 2014. 2

[8] Qiu, Dongyu e Rayadurgam Srikant: *Modeling and performance analysis of bittorrent-like peer-to-peer networks.* ACM SIGCOMM computer communication review, 34(4):367–378, 2004. 2

[9] Wang, Shuai, Liwei Ouyang, Yong Yuan, Xiaochun Ni, Xuan Han e Fei Yue Wang: *Blockchain-enabled smart contracts: architecture, applications, and future trends.* IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11):2266–2277, 2019. 3

[10] Kovach, B., T. Rosenstiel e W. Dupont: *Os elementos do jornalismo: O que os jornalistas devem saber e o público exigir.* Geração Editorial, 2003, ISBN 9788575090732. `https://books.google.com.br/books?id=6KAGQwAACAAJ`. 6

[11] Palacios, Marcos: *Fake news e a emergência das agências de checagem: terceirização da credibilidade jornalística.* Políticas da língua, da comunicação e da cultura no espaço lusófono. Braga: Edições Húmus, páginas 77–90, 2019. 6

[12] Guerra, Josenildo Luiz: *Transparência editorial: a credibilidade jornalística à luz dos sistemas de gestão da qualidade.* Revista Latinoamericana de Ciencias de la Comunicación, 11(20), 2014. 6

[13] Rodrigues, Horácio Wanderlei, Gabriela Natacha Bechara e Leilane Serratine Grubba: *Era digital e controle da informação.* Revista Em Tempo, 20(1), 2020. 6

[14] Kim, Byeowool e Yongik Yoon: *Journalism model based on blockchain with sharing space.* Symmetry, 11(1):19, 2018. 7

[15] Adghirni, Zélia Leal: *O jornalista: do mito ao mercado.* Repositório Institucional da UnB, 2005. 7

[16] Ruellan, Denis: *Le professionnalisme du flou: identité et savoir-faire des journalistes français.* (No Title), 1993. 8

[17] Vos, Tim P e Teri Finneman: *The early historical construction of journalism's gatekeeping role.* Journalism, 18(3):265–280, 2017. 8

[18] Hall, Peter A e Rosemary CR Taylor: *Political science and the three new institutionalisms.* Political studies, 44(5):936–957, 1996. 8

[19] André, Hendryo, Marcelo Engel Bronosky e David Candido dos Santos: *Reflexões sobre o papel social de um jornalismo em transformação.* Revistas uepg, 2005. 8

[20] Ghedini, Fred: *Rumo à taxonomia das funções e atividades no jornalismo brasileiro - uma análise preliminar.* Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina, 2024. 9

[21] Hagen, Cornelia Richter-von, Dietmar Ratz e Roman Povalej: *Towards self-organizing knowledge intensive processes.* Journal of Universal Knowledge Management, 2:148–169, 2005. 10

[22] Santos França, Juliana Baptista dos, Joanne Manhães Netto, Juliana do E Santo Carvalho, Flávia Maria Santoro, Fernanda Araujo Baião e Mariano Gomes Pimentel: *Kipo: the knowledge-intensive process ontology.* Softw. Syst. Model., 14(3):1127–1157, 2015. 10

[23] Bashir, Imran: *Mastering blockchain.* Packt Publishing Ltd, 2017. 10

[24] Szabo, Nick: *Formalizing and securing relationships on public networks.* First monday, 1997. 12

[25] Taherdoost, Hamed: *Smart contracts in blockchain technology: A critical review.* Information, 14(2):117, 2023. 12

[26] team, Ansa: *ansa.it.* `https://www.ansa.it/sito/static/ansa_check.html`, acesso em 2024. 12

[27] Rito Lima, Inês, Vasco Filipe, Claudia Marinho, Alexandre Ulisses, Antorweep Chakravorty, Atanas Hristov, Nishant Saurabh, Zhiming Zhao, Ruyue Xin e Radu Prodan: *Articonf decentralized social media platform for democratic crowd journalism*. Social Network Analysis and Mining, 13(1):116, 2023. 13

[28] team, Nostr: *nostr.com*. `https://nostr.com/`, acesso em 2024. 13

[29] team, Nostr: *nostr-protocol*. `https://nostr.com/the-protocol`, acesso em 2024. 14

[30] team, Exame: *exame-drex*. `https://exame.com/future-of-money/conheca-a-tecnologia-por-tras-da-hyperledger-besu-rede-escolhida-pelo-bc-para-ab` acesso em 2024. 14, 47

[31] team finsidersbrasil: *finsidersbrasil-drex*. `https://finsidersbrasil.com.br/noticias-sobre-fintechs/banco-central-escolhe-hyperledger-besu-para-piloto-do-real-digital-que-comeca-em-` acesso em 2024. 14, 47

[32] team bcb: *banco-central-drex*. `https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/JP-Morgan_4.9.23.pdf`, acesso em 2024. 15

[33] team cointelegraph: *cointelegraph-drex*. `https://br.cointelegraph.com/news/what-does-hyperledger-besu-offer-to-real-digital`, acesso em 2024. 15

[34] team, React: *react-native*. `https://reactnative.dev/docs/getting-started`, acesso em 2024. 20, 36

[35] Isotani, Seiji e Ig Ibert Bittencourt: *Dados abertos conectados: em busca da web do conhecimento*. Novatec Editora, 2015. 24

[36] McGuinness, Deborah L, Frank Van Harmelen *et al.*: *Owl web ontology language overview*. W3C recommendation, 10(10):2004, 2004. 24

[37] Sutherland, Jeff: *SCRUM: A arte de fazer o dobro de trabalho na metade do tempo*. Leya, 2014. 24

[38] Pinto, Guilherme Braga: *Sistema semântico para controle de processos de negócios intensivos em conhecimento integrado ao scrum: estudo de caso de uma redação jornalística contemporânea*. Biblioteca Digital da Produção Intelectual Discente, 2023. 24

[39] team, Hyperledger: *hyperledger-run*. `https://hyperledger-fabric.readthedocs.io/en/release-2.5/getting_started_run_fabric.html`, acesso em 2024. 28

[40] team, Hyperledger: *hyperledger-go-api*. `https://github.com/hyperledger/fabric-contract-api-go`, acesso em 2024. 30

[41] team, Hyperledger: *hyperledger*. `https://hyperledger-fabric.readthedocs.io/en/release-2.5/network/network.html`, acesso em 2024. 33

[42] team, Hyperledger: *hyperledger-gateway*. `https://hyperledger-fabric.readthedocs.io/en/latest/write_first_app.html`, acesso em 2024. 34

[43] team, React: *react-repository*. https://github.com/facebook/react, acesso em 2024. 36

[44] team, React: *react-native-community*. https://reactnative.dev/community/communities, acesso em 2024. 36

[45] team, React: *react-native-components*. https://reactnative.dev/docs/getting-started, acesso em 2024. 36

[46] team, Google: *google-firebase-docs*. https://firebase.google.com/docs?hl=pt-br, acesso em 2024. 39

[47] Menezes, Paulo Blauth e Paulo Blauth Menezes: *Matemática discreta para computação e informática*. Departamento de Informática Teórica Instituto de Informática / UFRGS, 2005. 42