

Relatório de Dissertação

**Adriano Busson de Jesus**

## Mestrado em Computação – Universidade Federal Fluminense (UFF) – Instituto de Computação

Av. Gal. Milton Tavares de Souza, s/nº São Domingos - Niterói – RJ CEP: 24210-346

[busson.adriano@gmail.com](mailto:busson.adriano@gmail.com)

# Título

## Utilização de blockchain e Zero Knowledge Proof para tornar uma entidade central de dados de usuários concorrentes em confiável e em conformidade com a LGPD.

1. **Identificação do professor orientador e do aluno**

Orientador: Antônio Augusto de Aragão Rocha

Aluno: Adriano Busson de Jesus (M048.223.002)

1. **Linha de Pesquisa**

Ciência de dados

1. **Resumo de Artigos**

**4.1. Preserving Privacy in Private Blockchain [1]:**

# Autores: Prabhakaran Ariyappampalayam Krishnamurthy, Saad Shahid e Oisen Boydel

**Gerenciamento de Privacidade em Blockchains Privadas**

O gerenciamento da privacidade de dados em blockchains privadas, particularmente a definição de quais participantes podem acessar quais informações, é um desafio significativo. Soluções existentes apresentam limitações, especialmente no contexto de dados sensíveis, como os Registros Eletrônicos de Saúde (EHR ou RES). Este artigo propõe uma abordagem inovadora baseada em criptografia assimétrica para mitigar as deficiências das técnicas atuais.

**Problemas Identificados**

**Requisitos de Privacidade no Uso de Blockchains Privadas**

Blockchains privadas manipulam dados utilizando "entidades de estado", que representam ativos ou informações específicas. No caso de um sistema EHR, os dados sensíveis podem incluir históricos médicos, prescrições e diagnósticos, sendo necessário limitar o acesso a stakeholders específicos (ex.: médicos, farmácias e seguradoras). Modelos tradicionais de transação, como mensagens P2P ou globais, enfrentam dificuldades em restringir o acesso, expondo dados desnecessariamente a participantes não autorizados.

**Soluções Existentes e suas Limitações**

As plataformas de blockchain privadas, como o Hyperledger Fabric, oferecem coleções de dados privadas e técnicas como computação multipartidária (MPC) e criptografia baseada em atributos para restringir o acesso aos dados. No entanto, essas abordagens enfrentam problemas como:

**Exponencialidade de combinações em coleções de dados privadas:** À medida que aumenta o número de organizações participantes, o número de combinações possíveis cresce exponencialmente.

**Exposição de dados em texto simples no livro-razão:** Mesmo com criptografia, atributos privados podem ser identificados facilmente.

**Sobrecarga computacional e dependência de módulos externos no MPC:** Necessidade de infraestrutura adicional e execução de transações on-chain, aumentando a complexidade e o custo.

**Recriptografia constante na criptografia baseada em atributos:** A cada mudança nos atributos, todos os dados precisam ser recriptografados, aumentando a complexidade temporal.

**Solução Proposta:** Criptografia Assimétrica com RSA

**Abordagem**

A proposta baseia-se no uso de criptografia de chave assimétrica, atribuindo pares de chaves (pública e privada) a cada participante. Dados sensíveis são criptografados utilizando a chave pública do usuário autorizado, e a descriptografia ocorre off-chain pelo detentor da chave privada correspondente. Esse modelo oferece controle granular de acesso e maior segurança contra acessos não autorizados.

**Arquitetura**

**Algoritmo:** RSA

**Modo de cifra:** ECB (Electronic Code Book) sem preenchimento (no padding).

**Tamanho da chave**: 256 bytes.

**Modelos de estado:** Um armazena as chaves criptográficas, enquanto outro contém os dados reais.

**Vantagens da Abordagem**

**Privacidade Granular:** Cada atributo pode ser acessado individualmente por usuários autorizados, sem impactar outros atributos.

**Redução de Sobrecarga Computacional:** O processo de descriptografia é realizado off-chain, reduzindo os custos de processamento na rede.

**Flexibilidade no Controle de Acesso:** Adicionar ou remover usuários para um dado específico não afeta os outros estados, ao contrário de modelos como o Hyperledger Fabric.

**Comparação com o Estado da Arte**

**Hyperledger Fabric:** Embora ofereça coleções de dados privadas, enfrenta desafios como o aumento exponencial de combinações de acesso e a exposição de dados em texto simples no livro-razão. A abordagem proposta supera esses problemas ao armazenar dados em formato criptografado e permitir alterações granulares.

**MPC:** A computação multipartidária exige infraestrutura complexa e comunicação segura entre participantes. A proposta elimina a necessidade de um módulo externo, tratando a criptografia e descriptografia fora da blockchain.

**Criptografia Baseada em Atributos:** Apesar de possibilitar a criptografia para múltiplos atributos simultaneamente, a recriptografia constante para atualizações torna-se inviável em cenários dinâmicos. A abordagem assimétrica permite mudanças sem recriptografar os dados existentes.

**Limitações e Desafios**

Apesar dos avanços, a solução proposta apresenta algumas limitações:

**Consistência de Dados no Consenso:** A ausência de preenchimento em RSA aumenta a vulnerabilidade a ataques de dicionário.

**Sobrecarga de Armazenamento e Computação:** O crescimento linear dos requisitos de armazenamento e processamento pode impactar o desempenho em redes de grande escala.

**Dependência de Transações Off-Chain:** A necessidade de processar dados descriptografados fora da cadeia adiciona complexidade operacional.

**Conclusão**

A proposta de utilização de criptografia assimétrica para garantir privacidade em blockchains privadas representa um avanço significativo, permitindo controle refinado sobre os dados. Embora a abordagem resolva várias limitações de métodos existentes, desafios como vulnerabilidades em preenchimento de RSA e sobrecargas computacionais permanecem. A pesquisa futura deve focar em mitigar essas limitações, explorando melhorias na arquitetura de consenso e otimização do armazenamento.

**4.2. A Tecnologia Blockchain sob a Perdpectiva da Lei Geral de Proteção de Dados [2]:**

# Autores: Vinícius Elias Brunoni

# A tecnologia blockchain, amplamente reconhecida por sua segurança, transparência e descentralização, enfrenta desafios consideráveis ao ser aplicada em conformidade com a Lei Geral de Proteção de Dados (LGPD). A seguir, exploram-se os principais aspectos analisados no artigo, com foco nos desafios, conflitos e possíveis soluções para compatibilizar a blockchain com os requisitos legais da LGPD.

# Principais Desafios da Proteção de Dados em Blockchains

# Imutabilidade e Direito à Edição ou Exclusão de Dados

# A imutabilidade das blockchains, essencial para garantir rastreabilidade e segurança, entra em choque direto com o direito dos titulares à exclusão ou edição de seus dados pessoais, conforme estabelecido pela LGPD. Esse conflito técnico exige soluções que conciliem a preservação da integridade das blockchains com os direitos dos titulares.

# Estrutura Descentralizada versus Necessidade de Controle

# A proteção de dados tradicionalmente depende de um controlador central responsável por gerenciar e proteger os dados. Na blockchain, a descentralização dificulta a identificação clara de controladores e operadores, complicando a aplicação da LGPD, que exige essa definição para garantir a responsabilização.

# Anonimização de Dados

# Embora a anonimização possa mitigar riscos, nem sempre é suficiente para atender plenamente à LGPD, pois a reidentificação de dados pseudonimizados ainda é possível em alguns cenários. Esse fator aumenta a complexidade de adequar blockchains a ambientes regulamentados.

# Conflitos Entre Blockchain e LGPD

# Direito à Exclusão versus Imutabilidade

# A LGPD garante aos titulares o direito de solicitar a exclusão de seus dados. Contudo, a característica imutável das blockchains torna tecnicamente inviável apagar informações de maneira definitiva. Essa incompatibilidade exige o desenvolvimento de mecanismos alternativos, como a dissociação de dados pessoais dos registros imutáveis.

# Transparência versus Privacidade

# A transparência intrínseca da blockchain, onde transações são frequentemente visíveis a todos os participantes, pode comprometer a privacidade dos dados pessoais. Esse paradoxo sublinha a necessidade de um equilíbrio entre a abertura dos registros e a proteção de informações sensíveis, assegurando conformidade com o princípio de minimização de dados.

# Soluções Possíveis para Conformidade

# Blockchains Privadas ou Permissionadas

# A implementação de blockchains privadas ou permissionadas pode facilitar o controle sobre os dados e os participantes da rede, possibilitando uma melhor adequação aos princípios da LGPD. Nesse modelo, a governança pode ser mais rigorosa e adaptável às exigências legais.

# Edição e Anonimização de Dados

# Tecnologias que viabilizam a edição ou anonimização em blockchains são fundamentais para garantir o direito à exclusão. Embora desafiadoras, essas abordagens oferecem um caminho viável para conciliar os direitos individuais e a imutabilidade técnica.

# Zero-Knowledge Proof (ZKP)

# O uso de provas de conhecimento zero (ZKP) permite verificar informações sem revelar os dados subjacentes, preservando a privacidade e atendendo às exigências da LGPD. Essa tecnologia se destaca como uma solução promissora em ambientes que requerem transparência e confidencialidade simultâneas.

# Conclusões: Blockchain e LGPD

# A blockchain, ao mesmo tempo que oferece segurança e transparência, apresenta desafios substanciais para a conformidade com a LGPD devido à sua descentralização e imutabilidade. Esses atributos, que representam sua força tecnológica, entram em conflito com princípios fundamentais da LGPD, como a capacidade de editar ou excluir dados pessoais.

# A ausência de um controlador central dificulta a implementação de responsabilidades claras, aumentando as incertezas jurídicas em sistemas descentralizados. Contudo, o artigo enfatiza que soluções inovadoras, como o uso de Zero-Knowledge Proof e práticas de design alinhadas à proteção de dados, podem viabilizar a conformidade regulatória. Para isso, é crucial que plataformas blockchain sejam projetadas com a LGPD em mente desde sua concepção, assegurando o respeito aos direitos dos titulares.

# A implementação bem-sucedida de blockchains em conformidade com a LGPD dependerá de avanços tecnológicos e regulamentares que equilibrem a descentralização e a proteção de dados, sem comprometer a funcionalidade essencial dessa tecnologia.

**4.3. Zero knowledge proof and ZK-SNARK for private blockchains [3]:**

# Autores: Anatoly Konkin · Sergey Zapechnikov

O artigo examina métodos de prova de conhecimento zero (ZKP) aplicados às redes blockchain corporativas, com foco em sua implementação, desempenho e escalabilidade. Ele aborda as limitações de segurança e privacidade inerentes aos blockchains, principalmente devido à replicação de dados entre nós, e propõe soluções baseadas em ZKP para superar esses desafios sem comprometer características essenciais, como transparência e rastreabilidade.

**Problema e Solução Proposta**

A principal limitação das blockchains corporativas é a exposição de dados devido à replicação nos nós da rede, impactando negativamente a segurança e a privacidade. Embora ferramentas modernas forneçam mecanismos para transações privadas, como soluções "off-chain", essas abordagens introduzem complexidade arquitetural e comprometem a rastreabilidade. Para resolver esses problemas, o artigo sugere o uso de ZKP, com destaque para protocolos NIZK (provas não interativas) e zk-SNARK, que atendem aos requisitos de privacidade ao mesmo tempo que preservam a transparência da blockchain.

**Privacidade em Blockchain**

O artigo categoriza os problemas de privacidade em três tipos:

1. **Privacidade de Identidade**: Relaciona-se ao anonimato de remetentes e destinatários. Em blockchains públicos, utiliza-se endereços pseudo-aleatórios para ofuscar contas.
2. **Privacidade de Transações**: Trata da confidencialidade de dados transacionais, frequentemente implementada com protocolos "off-chain", como o Tessera para Besu e o Hyperledger Fabric. No entanto, esses mecanismos perdem a rastreabilidade e transparência inerentes ao blockchain.
3. **Privacidade de Contratos Inteligentes**: Diz respeito à ocultação de termos ou códigos-fonte de contratos inteligentes. Embora relevante, este aspecto não foi abordado no artigo.

**Métodos ZKP e Protocolos NIZK**

As provas de conhecimento zero permitem verificar declarações sem revelar informações adicionais. O artigo detalha os métodos NIZK, que eliminam a necessidade de comunicação interativa entre provador e verificador. O esquema NIZK é composto por três etapas:

1. **Setup (λ)**: Define os parâmetros de segurança do esquema.
2. **Prova (w, x)**: Gera provas a partir de dados secretos (w) e informações públicas (x).
3. **Verificar (x, π)**: Valida a prova gerada, retornando um valor booleano.

Os critérios avaliados para os protocolos incluem complexidade algorítmica, tempo para gerar e verificar provas, tamanho das transações, resistência pós-quântica e uso de código-fonte aberto.

**zk-SNARK em Blockchain Corporativo**

Os zk-SNARKs foram destacados como adequados para blockchains corporativos, devido ao seu baixo tempo de geração de provas, tamanho reduzido e aplicação em casos como a propriedade de ativos digitais. Os experimentos foram realizados na plataforma Masterchain, baseada em Ethereum, utilizando a ferramenta ZoKrates para implementar zk-SNARK. O artigo ilustra o processo de autenticação para transações envolvendo ativos digitais, detalhando o papel do Trusted Third Party (TTP), a geração de HMAC e o uso de contratos inteligentes para validação e transferência de ativos.

**Resultados Experimentais**

Os experimentos usaram diversas funções hash (GOST, SHA-256, Pedersen) para criar gráficos acíclicos e gerar provas de conhecimento. A Tabela 2 no artigo resume os parâmetros de desempenho, com destaque para:

* Tempo de geração de provas: baixo.
* Tempo de verificação: relativamente alto.
* Tamanho das provas e transações: reduzido.

**Conclusão**

O artigo conclui que os protocolos ZKP, especialmente NIZK e zk-SNARK, podem superar as limitações de privacidade do blockchain corporativo, preservando a rastreabilidade e eliminando desvantagens associadas a soluções "off-chain". No entanto, melhorias no desempenho, especialmente no tempo de verificação e na eficiência das funções hash, ainda são necessárias para ampliar a aplicabilidade prática dos métodos.

**4.4. The Zero Knowledge Proof Technique Limitations and Challenges [4]:**

# Autores: Sajjad Mohammed Shlaka · Hala Bahjat Abdul Wahab

O artigo aborda as limitações e os desafios enfrentados pelas técnicas de prova de conhecimento zero (ZKP - Zero Knowledge Proof) em processos de autenticação e proteção de privacidade. A análise destaca os fatores que impactam o desempenho desses protocolos em diferentes aplicações e sugere melhorias para superar os obstáculos enfrentados.

A técnica ZKP é amplamente reconhecida como uma solução promissora em sistemas que exigem alta privacidade e segurança. No entanto, há lacunas em sua implementação prática, pois muitas vezes é tratada apenas como um conceito matemático estático, desconsiderando as implicações práticas em sistemas dinâmicos e reais.

**Problema**

Apesar de sua aplicabilidade em várias áreas, as informações atualmente disponíveis sobre ZKP nem sempre são úteis para solucionar problemas práticos. Pesquisadores têm focado em abordagens matemáticas, negligenciando aspectos práticos, como desempenho em tempo real e interoperabilidade com outras tecnologias. Isso limita a adoção do ZKP em cenários sensíveis, como redes blockchain e serviços baseados em localização.

**Solução Proposta**

O estudo sugere aprimorar a utilização da técnica ZKP, investigando suas aplicações em autenticação e privacidade. Uma análise detalhada de casos de uso recentes foi apresentada, destacando o potencial de ZKP para lidar com as limitações atuais.

**Análise da Literatura e Usos do ZKP**

**1. Blockchain**

O ZKP pode validar transações em blockchain sem revelar informações pessoais, como os detalhes do remetente ou destinatário. Isso garante privacidade e segurança em ambientes descentralizados.

**2. Hyperledger Ursa**

A biblioteca criptográfica Hyperledger Ursa implementa um protocolo de validação por prova de intervalo (ZKRP - Zero Knowledge Range Proof), possibilitando autenticação sem comprometer a privacidade. Essa tecnologia suporta redes blockchain modulares e permite controle de tráfego em tempo real com alto nível de segurança.

**3. Localização**

O protocolo Zk-Pol, utilizado em Serviços Baseados em Localização (LBS - Location-Based Services), assegura privacidade e segurança. No entanto, devido ao custo computacional, é mais adequado para LBSs tolerantes a atrasos, sendo menos eficiente para aplicações que demandam respostas em tempo real.

**4. Autenticação**

Em sistemas descentralizados, ZKP possibilita autenticação segura com anonimato e proteção de dados confidenciais. Assinaturas de grupo dinâmico e provas de conhecimento zero não interativas (NIZKP) oferecem benefícios como infalsificabilidade, rastreabilidade e anonimato.

**Problemas e Desafios**

O ZKP enfrenta desafios em aplicações práticas, como:

**Complexidade Computacional:** O custo computacional elevado pode limitar sua aplicação em sistemas que requerem alta eficiência em tempo real.

Interoperabilidade: Implementações diferentes do ZKP podem apresentar dificuldades de integração em sistemas heterogêneos.

**Fiabilidade em Redes Hostis:** Nós maliciosos em redes distribuídas podem comprometer a privacidade e segurança, exigindo melhorias em protocolos de autenticação descentralizada.

**Protocolo Fiat-Shamir**

Um dos exemplos mais notáveis do uso do ZKP é o sistema de identificação Feige-Fiat-Shamir, desenvolvido em 1988. Ele permite que um provador demonstre conhecimento de informações confidenciais sem revelá-las ao verificador. No entanto, sua limitação está na necessidade de comunicações paralelas e no uso de aritmética modular, que podem ser otimizados para melhorar sua eficiência.

**Conclusão**

A técnica ZKP é fundamental para aprimorar autenticação e proteção de privacidade em ambientes diversos, como blockchain e sistemas de localização. O artigo recomenda o uso do protocolo Fiat-Shamir e sugere melhorias para lidar com os desafios, como redução de custos computacionais e aumento da interoperabilidade. Com esses avanços, o ZKP pode superar as limitações atuais e se tornar uma solução ainda mais robusta para segurança e privacidade em sistemas digitais.

**4.5. Olympus: a GDPR compliant blockchain system [5]:**

# Autores: Ricardo Martins Gonçalves, Miguel Mira da Silva & Paulo Rupino da Cunha

# Motivação – Problema:

# Crescente adoção do blockchain e da necessidade de torná-lo compatível com a GDPR.

# A imutabilidade inerente ao blockchain entra em conflito com o direito de retificação e apagamento de dados pessoais, garantidos pela legislação.

# Demanda crescente por sistemas que possam armazenar dados pessoais de forma segura e transparente, garantindo conformidade com as regulamentações, sem comprometer a integridade do blockchain.

# O sistema proposto busca preencher essa lacuna ao unir segurança e conformidade regulatória.

# Solução Proposta:

# Sistema "Olympus", incompatibilidade - GDPR

# Direito de exclusão e retificação de dados.

# Arquitetura híbrida, dados pessoais armazenados fora da cadeia (off-chain) em um sistema distribuído (IPFS),

# Apenas os hashes desses dados são gravados no blockchain permissionado (Hyperledger Fabric).

# Permitindo que os dados possam ser apagados ou modificados conforme exigido pelo GDPR, sem comprometer a segurança e a verificabilidade dos dados.

# Principais aspectos da solução proposta:

# Blockchain Permissionado:

# Hyperledger Fabric: A plataforma blockchain utilizada é permissionada, ou seja, somente participantes autorizados podem interagir com o sistema, o que garante controle sobre quem pode acessar e validar as transações.

# Armazenamento de Hashes: Em vez de armazenar diretamente os dados pessoais no blockchain, são armazenados apenas hashes criptográficos desses dados.

# O hash serve como uma assinatura única que permite verificar a integridade e autenticidade dos dados, sem expô-los diretamente no blockchain.

# Armazenamento Off-chain:

# IPFS (Interplanetary File System): Os dados pessoais são armazenados em um sistema de armazenamento distribuído chamado IPFS, que oferece maior flexibilidade para lidar com as exigências do GDPR.

# Como os dados são armazenados fora do blockchain, é possível modificá-los ou excluí-los conforme necessário.

# Conformidade com o GDPR: Como os dados pessoais podem ser manipulados no IPFS (modificados ou apagados), o sistema consegue cumprir os direitos de retificação e apagamento estabelecidos pelo GDPR, superando o problema da imutabilidade do blockchain.

# Verificabilidade e Segurança:

# Hashes no Blockchain: Os hashes dos dados armazenados no IPFS garantem que qualquer modificação nos dados seja detectada, mantendo a integridade das informações e permitindo a verificação de sua autenticidade.

# Privacidade e Auditoria: Mesmo que os dados pessoais sejam armazenados fora do blockchain, a auditoria e a verificabilidade permanecem garantidas, pois o hash dos dados permite a validação sem necessidade de acesso aos dados sensíveis.

# Processo de Armazenamento e Verificação:

# O processo de armazenamento começa com o envio dos dados pessoais para o IPFS, onde são armazenados de forma distribuída.

# Em seguida, é gerado um hash criptográfico desse conjunto de dados, que é então armazenado no Hyperledger Fabric.

# No caso de uma auditoria ou verificação, o hash pode ser comparado com os dados armazenados no IPFS para garantir que não houve alterações indevidas.

# Benefícios da Abordagem Híbrida:

# Conformidade Legal: Ao permitir que os dados sejam modificados ou apagados fora da cadeia, o sistema garante conformidade com as exigências do GDPR, algo que os sistemas de blockchain tradicionais não conseguem oferecer.

# Segurança e Privacidade: A privacidade dos dados pessoais é mantida, já que os dados não são armazenados diretamente no blockchain, e a segurança é garantida por meio do uso de hashes.

# Escalabilidade: O uso do IPFS para armazenamento de dados off-chain reduz a carga no blockchain, tornando o sistema mais escalável em termos de volume de dados.

# Essa abordagem híbrida proporciona um equilíbrio entre os benefícios do blockchain e a necessidade de conformidade com a legislação de proteção de dados, resolvendo um dos maiores desafios para a adoção de blockchain em setores que lidam com dados pessoais sensíveis.

# Arquitetura do Sistema:

# A arquitetura do sistema "Olympus" é baseada em uma combinação de blockchain permissionado (Hyperledger Fabric) e armazenamento off-chain distribuído (IPFS), garantindo conformidade com a GDPR.

# Hyperledger Fabric (Blockchain Permissionado):

# Rede Permissionada: Apenas participantes autorizados podem interagir com a rede, garantindo controle sobre o acesso.

# Armazenamento de Hashes: O blockchain armazena apenas hashes criptográficos dos dados pessoais. Isso mantém a integridade dos dados sem armazenar informações sensíveis diretamente na cadeia.

# Imutabilidade Controlada: O Hyperledger Fabric oferece um nível de controle sobre as permissões de leitura e escrita, adequando-se a casos de uso que exigem a colaboração de várias entidades sem confiança mútua.

# IPFS (Interplanetary File System):

# Armazenamento Off-chain: O IPFS armazena os dados pessoais fora do blockchain. Isso permite que os dados sejam modificados ou apagados conforme necessário, atendendo às exigências do GDPR, como o direito de retificação e exclusão.

# Sistema Distribuído: O IPFS funciona como uma rede de armazenamento distribuída, onde os dados são fragmentados e distribuídos em diferentes nós, garantindo redundância e disponibilidade.

# Fluxo de Dados:

# Inserção de Dados: Os dados pessoais são primeiramente inseridos no IPFS, onde recebem um identificador único.

# Geração de Hashes: Um hash criptográfico é gerado para representar os dados e é gravado no Hyperledger Fabric.

# Conformidade com o GDPR:

# Retificação e Exclusão de Dados: Como os dados são armazenados off-chain no IPFS, eles podem ser alterados ou removidos em conformidade com o GDPR, enquanto os hashes armazenados no blockchain garantem que qualquer alteração possa ser detectada.

# Auditabilidade Sem Violação de Privacidade: Mesmo com a possibilidade de modificar os dados off-chain, a integridade do sistema é mantida. O hash no blockchain garante a verificabilidade, mas sem revelar informações sensíveis diretamente.

# Segurança e Privacidade:

# Segurança dos Hashes: O uso de hashes criptográficos garante que os dados armazenados no IPFS possam ser validados, mas sem expor o conteúdo real ao blockchain.

# Controle de Acesso: No Hyperledger Fabric, as permissões são controladas, garantindo que apenas entidades autorizadas possam acessar ou modificar o sistema.

# Desafios e Escalabilidade:

# Escalabilidade do Sistema: A abordagem híbrida permite que o sistema seja escalável, já que o blockchain não armazena diretamente os dados volumosos, mas apenas os hashes, reduzindo a sobrecarga de armazenamento.

# Desempenho: O sistema foi projetado para lidar com grandes volumes de dados, usando o IPFS para evitar a sobrecarga do blockchain e garantir alta disponibilidade e redundância.

# Interoperabilidade:

# Integração com Outras Plataformas: O uso de IPFS e Hyperledger Fabric facilita a interoperabilidade com outras soluções, permitindo que a arquitetura possa ser utilizada em diferentes indústrias e em diversos cenários de conformidade regulatória.

# Essa arquitetura garante que o sistema "Olympus" ofereça uma solução robusta e escalável para armazenar dados pessoais de maneira compatível com o GDPR, aproveitando a segurança e a imutabilidade do blockchain sem comprometer os direitos de privacidade dos usuários.

# Imutabilidade vs. Privacidade:

# A maioria das soluções anteriores falha em oferecer um equilíbrio eficaz entre a imutabilidade, característica central do blockchain, e as necessidades de privacidade, como o direito de retificação e esquecimento. Em muitas abordagens, a solução acaba sacrificando um desses aspectos.

# Outras Abordagens de Privacidade no Blockchain:

# Soluções como zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) têm sido investigadas para proteger a privacidade dos dados no blockchain, mas sua aplicação em larga escala ainda apresenta dificuldades técnicas e limitações de eficiência.

# Outro conceito relevante é o uso de canais laterais (sidechains) para gerenciar a privacidade dos dados de forma mais flexível do que o blockchain principal, mas essa abordagem também enfrenta desafios quanto à interoperabilidade e segurança.

# Diferencial do Olympus:

# Ao contrário de outras abordagens que dependem unicamente de técnicas de criptografia avançadas para garantir privacidade, o Olympus adota uma abordagem híbrida, usando blockchain apenas para armazenar hashes e mantendo os dados pessoais fora da cadeia, permitindo modificação e exclusão conforme necessário, sem comprometer a verificabilidade.

# Essa arquitetura híbrida supera as limitações das abordagens puramente on-chain, proporcionando uma solução mais prática e escalável para a conformidade com o GDPR.

# Comparações Técnicas e Discussões:

# O artigo também discute como o Olympus se diferencia de abordagens puramente descentralizadas, em que a governança sobre os dados pessoais é mais complexa e difícil de aplicar de forma eficaz em conformidade com as regulamentações de privacidade.

# A avaliação técnica do Olympus mostra que sua arquitetura híbrida não apenas resolve os problemas de conformidade, mas também mantém um bom desempenho em termos de segurança, verificabilidade e auditabilidade, algo que nem todas as soluções comparadas conseguem alcançar.

# Comparações Técnicas e Discussões:

# Embora várias soluções blockchain tentem abordar a questão da conformidade com o GDPR, o Olympus propõe uma abordagem única e eficiente que combina a segurança e verificabilidade do blockchain com a flexibilidade do armazenamento off-chain.

# Essa abordagem é mais viável e escalável do que as soluções tradicionais baseadas em blockchain puro ou técnicas de criptografia complexas.

# Avaliação do Sistema:

# A avaliação do sistema Olympus concentra-se em dois aspectos principais: desempenho e conformidade com o GDPR.

# A solução mostrou-se eficiente, com impacto mínimo na latência e no processamento das transações, mesmo com grandes quantidades de dados off-chain.

# Desempenho:

# Latência e Escalabilidade: A avaliação de desempenho revelou que a arquitetura do sistema consegue lidar com grandes volumes de dados sem comprometer a performance. Como o blockchain armazena apenas hashes dos dados pessoais, a quantidade de dados armazenados no blockchain permanece baixa, o que reduz a sobrecarga de armazenamento e processamento.

# Armazenamento Off-chain: O uso do IPFS para armazenamento fora da cadeia também foi avaliado em termos de capacidade de recuperação de dados, redundância e resiliência a falhas, com resultados positivos para garantir que os dados estejam disponíveis mesmo em redes distribuídas.

# Conformidade com o GDPR:

# Direitos de Retificação e Apagamento: O sistema mostrou-se eficaz em permitir que os dados sejam apagados ou retificados off-chain, garantindo que o Olympus está em conformidade com os requisitos de privacidade estabelecidos pelo GDPR, como o direito ao esquecimento.

# Verificabilidade e Segurança: A integridade dos dados é mantida por meio do uso de hashes, que possibilitam a verificação de que os dados armazenados no IPFS não foram alterados indevidamente. Isso garante a auditabilidade e segurança dos dados pessoais, sem comprometer a conformidade regulatória.

# Desafios Identificados:

# Armazenamento Off-chain: Um dos desafios apontados na avaliação do sistema é a gestão eficiente de grandes volumes de dados no IPFS, particularmente em cenários de alta escalabilidade.

# Embora o sistema seja eficiente no gerenciamento de dados off-chain, a dependência de redes distribuídas como o IPFS pode apresentar limitações em termos de latência e custo de recuperação de dados.

# Integração com Outras Soluções: O uso do Hyperledger Fabric e do IPFS implica a necessidade de integração contínua com outras soluções de blockchain e armazenamento distribuído, o que pode aumentar a complexidade de implementação em certos cenários.

# Conclusão da Avaliação:

# O Olympus oferece uma solução eficiente e viável para o desafio de conformidade com o GDPR no contexto do blockchain.

# O sistema foi avaliado positivamente em termos de desempenho, com baixa latência e alta escalabilidade, e garante conformidade total com os requisitos de proteção de dados, como retificação e apagamento.

# No entanto, os desafios em torno da escalabilidade e da gestão de dados off-chain ainda podem exigir melhorias futuras.

# Conclusão e Trabalhos Futuros:

# Destaca o sucesso do sistema Olympus em superar os desafios de conformidade com o GDPR no uso de blockchain, ao implementar uma abordagem híbrida de armazenamento off-chain.

# A solução equilibra imutabilidade, auditabilidade e privacidade, oferecendo uma arquitetura escalável que garante o direito à retificação e apagamento de dados pessoais.

# Os autores reconhecem que, embora a solução funcione bem em termos de desempenho e segurança, desafios como a escalabilidade no armazenamento off-chain ainda precisam ser explorados mais profundamente.

# Escalabilidade e Desempenho:

# Aperfeiçoar a eficiência do sistema em cenários com grandes volumes de dados, especialmente no uso de IPFS.

# A infraestrutura off-chain do IPFS pode enfrentar desafios relacionados à latência e à capacidade de recuperação de dados em larga escala.

# Melhorar a escalabilidade do sistema para que ele possa ser aplicado em redes maiores e mais complexas, sem comprometer a segurança ou a conformidade com o GDPR.

# Interoperabilidade:

# Investigar maneiras de melhorar a interoperabilidade do Olympus com outros sistemas blockchain e soluções de armazenamento distribuído.

# Isso permitiria que o sistema fosse adotado em uma variedade maior de indústrias e ambientes corporativos.

# Avaliar formas de integrar o sistema com outras tecnologias emergentes de proteção de dados e blockchain.

# Segurança e Privacidade:

# Continuar a pesquisa em aprimoramentos de segurança que aumentem a privacidade dos dados armazenados no IPFS, garantindo que as informações sensíveis sejam protegidas de maneira robusta.

# Explorar novas técnicas, como Zero-Knowledge Proofs (ZKP), para aumentar a privacidade e garantir que os dados off-chain possam ser verificados sem serem revelados.

# Governança e Compliance:

# Desenvolver novos modelos de governança que possam garantir a conformidade contínua do sistema com o GDPR, à medida que as regulamentações de proteção de dados evoluem.

# Propor métodos mais automatizados para gerenciar os direitos de privacidade dos usuários de forma eficiente e auditável.

**4.6. zk-Oracle: Trusted Off-chain Compute and Storage for Decentralized Applications [6]:**

# Autores: Binbin Gu - Faisal Nawab

**Problema Identificado**

O artigo aborda os desafios de desempenho e custo associados a transações on-chain, típicas de aplicações descentralizadas (DApps). Essas operações frequentemente enfrentam:

**Custo elevado e latência para processamento na blockchain.**

Dependência de soluções off-chain, que introduzem riscos de segurança devido à ausência das garantias de integridade e confiabilidade encontradas em sistemas on-chain.

Embora técnicas como estruturas de dados autenticadas e computação verificável existam para mitigar tais riscos, ambas apresentam limitações. Estruturas autenticadas exigem confiança em entidades específicas, enquanto métodos verificáveis, como zk-SNARKs, podem ser computacionalmente caros, com exemplos extremos demonstrando tempos inviáveis para aplicações práticas.

**Solução Proposta: zk-Oracle**

**O zk-Oracle é uma solução híbrida on-chain/off-chain projetada para:**

Computação confiável e armazenamento eficiente off-chain.

Geração e verificação de provas zk-SNARK otimizadas, acelerando o desempenho e reduzindo custos associados.

A principal contribuição do zk-Oracle está no estudo e implementação de técnicas para acelerar a geração de provas zk com métodos de dosagem horizontal e vertical, otimizando tanto a computação quanto o armazenamento.

**Estratégia Técnica**

**Estruturas de Dosagem**

O artigo propõe dois padrões para dividir o processamento e melhorar o desempenho:

**Dosagem Horizontal:**

Divide o conjunto de dados em pequenos lotes processados sequencialmente.

Ideal para cálculos independentes entre si.

**Dosagem Vertical:**

Fragmenta o programa em módulos menores, permitindo execução paralela ou sequencial, dependendo da lógica.

**Otimização do Tamanho das Provas**

**Método de agregação:** Combina múltiplas provas zk em uma única.

**Provas recursivas:** Encadeiam a lógica de várias provas zk, aumentando a expressividade. Contudo, o custo computacional associado ainda é elevado.

**Modelo de Segurança**

**O zk-Oracle assume que nós off-chain não são confiáveis, prevenindo:**

**Desvios de protocolo (falhas bizantinas).**

Conspiração entre provedores off-chain e consumidores.

**Para garantir a integridade do sistema, o contrato inteligente on-chain:**

Verifica a validade das provas zk.

Puni provedores maliciosos com a retirada de fundos de garantia.

**Experimentação e Resultados**

**Implementação**

**Ferramentas:** ZoKrates (ferramenta zk-SNARK), Javascript e Python para componentes off-chain, Solidity para contratos inteligentes.

Infraestrutura: Rede Ethereum Goerli (PoS) e hardware com especificações medianas (Intel Core i5, 8 GB RAM).

**Resultados**

**Geração de provas zk:**

Melhorias significativas no tempo de geração de provas em comparação aos métodos convencionais.

**Exemplo:** Treinar um modelo de regressão logística com 10.000 amostras levou apenas 100 segundos, contra 6000 segundos de métodos tradicionais, graças à divisão em lotes.

**Custos on-chain:** Pequenos em comparação às operações mais pesadas, como inferência de redes neurais.

**Contribuições e Limitações**

**Contribuições**

Desenvolvimento de um modelo híbrido confiável e eficiente para DApps.

Redução do custo e tempo de processamento com técnicas inovadoras de dosagem e otimização.

Compatibilidade com ferramentas zk-SNARK existentes.

**Limitações**

**Dosagem Horizontal:** Não funciona para cálculos que exigem o carregamento completo dos dados na memória.

**Dosagem Vertical:** Limitações práticas em programas altamente interdependentes.

Custos de provas recursivas: Embora expressivas, ainda apresentam desafios computacionais significativos.

**Conclusão**

O artigo demonstra que o zk-Oracle pode acelerar significativamente a geração de provas zk-SNARK, atingindo ganhos de desempenho de até 550 vezes mais rápido que métodos tradicionais. A solução proposta combina segurança e eficiência para aplicações descentralizadas, reduzindo os custos on-chain e possibilitando maior escalabilidade para sistemas baseados em blockchain.

**4.7. A New Approach to Financial Distribution Systems Leveraging Hyperledger Besu and Consortium Blockchain [7]:**

# Autores: Md. Raisul Hasan Shahrukh · Nafees Mansoor

# O artigo apresenta um sistema de distribuição financeira utilizando blockchain de consórcio, destacando os recursos oferecidos pelo Hyperledger Besu. O estudo enfatiza a transformação das infraestruturas financeiras legadas, estabelecendo um novo padrão para as comunidades acadêmica e industrial. O objetivo principal é comparar o sistema blockchain proposto com abordagens tradicionais, demonstrando vantagens em termos de transparência, eficiência e privacidade de dados.

# Problemas Abordados

# O sistema proposto analisa as limitações dos sistemas tradicionais de distribuição financeira, que incluem:

# Complexidade nas transações;

# Falta de transparência e controle;

# Escalabilidade limitada.

# Para isso, utiliza o benchmarking como ferramenta para avaliar o desempenho do Hyperledger Besu, especialmente na automação financeira.

# Solução Proposta

# A proposta baseia-se no uso de contratos inteligentes desenvolvidos em Solidity para gerenciar recursos financeiros em um ambiente privado e autorizado.

# As características principais incluem:

# Eficiência: Automatização de processos financeiros.

# Privacidade: Uso de redes privadas do Hyperledger Besu para proteger dados sensíveis.

# Transparência: Garantida pela imutabilidade da blockchain.

# Fluxo de Operações

# O sistema opera utilizando contratos inteligentes em várias funções:

# Controle de Transações: O contrato verifica a disponibilidade de fundos e autentica os destinatários.

# Criação de Blocos: Quando os requisitos são atendidos, um bloco é criado e replicado na rede.

# Registro e Validação de Contas Bancárias: Implementação de algoritmos para registro seguro das contas.

# Algoritmos Implementados

# Algoritmo 1 – Funções Financeiras

# Autenticação do Remetente: Identificação da organização como responsável pelas transações.

# Gerenciamento de Beneficiários: Adição e remoção de destinatários são condicionadas à validação organizacional.

# Consultas de Saldo: Proporciona informações atualizadas sobre os fundos.

# Algoritmo 2 – Registro e Validação de Contas Bancárias

# Hash de Contas Bancárias: Garante a autenticidade dos dados ao associar contas bancárias a hashes únicos.

# Verificação Sistemática: Comparação de dados fornecidos com informações armazenadas para garantir a integridade.

# Algoritmo 3 – Migração de Contratos Inteligentes

# Integração de ferramentas como Docker, Truffle e Metamask para criar um ambiente de teste robusto e otimizado para Hyperledger Besu.

# Avaliação de Desempenho

# A avaliação foi conduzida em um ambiente controlado utilizando ferramentas como o Hyperledger Caliper para medir:

# Throughput (TPS): Número de transações por segundo, indicando escalabilidade.

# Latência: Tempo necessário para processar transações, refletindo a eficiência.

# Os testes foram realizados em diferentes funções do sistema, com destaque para as funções addRecipient, sendAllowance, e registerBankAccount. Resultados mostram que o sistema mantém alta taxa de transferência até alcançar um ponto de saturação.

# Comparações com Outras Soluções

# Blockchain Tradicional

# O sistema proposto demonstra vantagens significativas em termos de escalabilidade e eficiência, superando o desempenho das blockchains tradicionais em diversos cenários.

# Hyperledger Fabric

# Embora o Hyperledger Fabric tenha se destacado em cenários de pico de tráfego, o Hyperledger Besu demonstrou desempenho superior na maioria das métricas de avaliação.

# Conclusão

# O sistema proposto mostra-se uma solução robusta e escalável para distribuição financeira em blockchains de consórcio. Apesar de suas limitações em cenários de alto tráfego, oferece vantagens claras em privacidade, eficiência e gerenciamento de recursos. O estudo destaca a necessidade de continuar explorando otimizações e novos caminhos de pesquisa no espaço blockchain.

# Referências Bibliográficas

1. "**Preserving Privacy in Private Blockchain Networks**" - Ariappampalayam Krishnamoorthi, P., Shahid, S., Boydell, O. (2022). Preserving Privacy in Private Blockchain Networks. In: Lee, K., Zhang, LJ. (eds) Blockchain – ICBC 2021. ICBC 2021. Lecture Notes in Computer Science(), vol 12991. Springer, Cham.

Acesso: <https://link.springer.com/chapter/10.1007/978-3-030-96527-3_8>

1. **"** **A tecnologia blockchain sob a perdpectiva da lei geral de proteção de dados "**: Este artigo analisa como a tecnologia blockchain pode ser ajustada para cumprir a LGPD, discutindo a utilização de armazenamento off-chain para dados sensíveis e a blockchain para dados não sensíveis.
   * Acesso: [Revista de Direito, Governança e Novas Tecnologias](https://revistaft.com.br/a-tecnologia-blockchain-sob-a-perspectiva-da-lei-geral-de-protecao-de-dados/)( [RevistaFT](https://revistaft.com.br/a-tecnologia-blockchain-sob-a-perspectiva-da-lei-geral-de-protecao-de-dados/) ).
   * <https://revistaft.com.br/a-tecnologia-blockchain-sob-a-perspectiva-da-lei-geral-de-protecao-de-dados/>
2. "**Zero knowledge proof and ZK-SNARK for private blockchains**" - Konkin, A., Zapechnikov, S. Zero knowledge proof and ZK-SNARK for private blockchains. *J Comput Virol Hack Tech* **19**, 443–449 (2023).

Acesso: <https://link.springer.com/article/10.1007/s11416-023-00466-1>

1. "**Zero knowledge proof and ZK-SNARK for private blockchains**" - Konkin, A., Zapechnikov, S. Zero knowledge proof and ZK-SNARK for private blockchains. *J Comput Virol Hack Tech* **19**, 443–449 (2023).

Acesso: <https://link.springer.com/article/10.1007/s11416-023-00466-1>

1. "**Olympus: a GDPR compliant blockchain system**" - Este artigo da International Journal of Information Security, apresenta um sistema blockchain que é compatível com o GDPR, utilizando armazenamento off-chain para dados sensíveis e blockchain para dados não sensíveis, garantindo a integridade e a conformidade dos dados.
   * Acesso: <https://link.springer.com/article/10.1007/s10207-023-00782-z>
2. "**zk-Oracle: trusted off-chain compute and storage for decentralized applications**" - Gu, B., Nawab, F. zk-Oracle: trusted off-chain compute and storage for decentralized applications. *Distrib Parallel Databases* **42**, 525–548 (2024).
   * Acesso: <https://link.springer.com/article/10.1007/s10619-024-07444-6>
3. "**A New Approach to Financial Distribution Systems Leveraging Hyperledger-Besu and Consortium Blockchain**" - M. R. Hasan Shahrukh and N. Mansoor, "A New Approach to Financial Distribution Systems Leveraging Hyperledger-Besu and Consortium Blockchain," *2023 26th International Conference on Computer and Information Technology (ICCIT)*, Cox's Bazar, Bangladesh, 2023, pp. 1-6.
   * Acesso: <https://ieeexplore.ieee.org/document/10441085>

## Niterói, 16 de Dezembro de 2024.

Professor: Antônio Augusto de Aragão Rocha Aluno: Adriano Busson de Jesus