

Entrega de Trabalho de Conclusão de Curso I

ICEI - PUC Minas - Engenharia de Software



PUC Minas

Comparação Empírica entre Mecanismos Centralizados e Descentralizados de Autenticação

Uma análise comparativa entre modelos de autenticação centralizados e descentralizados

Aluno: Douglas Viana Fernandes

Orientadores: Cleiton Tavares, Danilo Maia, Leonardo Vilela, Raphael Ramos

Contextualização da Pesquisa

A autenticação digital é um pilar de segurança em sistemas modernos, mas ainda depende majoritariamente de modelos centralizados, como OAuth 2.0 e OpenID Connect. Com o avanço de aplicações distribuídas e exigências mais rígidas de privacidade, cresce o interesse por soluções descentralizadas baseadas em blockchain, que prometem maior auditabilidade e autonomia do usuário. Nesse cenário, torna-se essencial compreender tecnicamente como cada abordagem se comporta e em que medida a descentralização pode complementar ou até superar os modelos tradicionais dependendo do contexto.

Problema

Os sistemas de autenticação mais utilizados atualmente dependem de provedores centralizados para validar identidades. Essa centralização cria vulnerabilidades críticas: pontos únicos de falha, risco ampliado de ataques, baixa auditabilidade e pouca autonomia do usuário sobre seus próprios dados.

Justificativa

Apesar do potencial da blockchain, ainda não há comparações empíricas claras que mostrem se ela realmente supera os modelos tradicionais em segurança, desempenho e operação. Portanto, esse estudo visa comparar e enfatizar as principais diferenças entre sistemas de autenticação centralizados e descentralizados, visando entender as opções de abordagem de autenticação em diferentes contextos.

Objetivo da pesquisa

Comparar, com base em evidências empíricas publicadas, mecanismos de autenticação tradicionais e modelos descentralizados baseados em blockchain, identificando benefícios, limitações e condições de adoção prática.

Desdobramentos do objetivo (objetivos específicos)

01 — Levantamento de Métricas

Identificar e organizar métricas empíricas sobre segurança, desempenho e auditabilidade em modelos centralizados e descentralizados.

02 — Matriz Comparativa

Construir uma comparação estruturada entre abordagens tradicionais (ex.: OAuth 2.0) e soluções baseadas em blockchain.

03 — Análise Crítica

Avaliar trade-offs, benefícios e limitações técnicas reportadas na literatura recente.

04 — Diretrizes de Engenharia

Sintetizar recomendações que auxiliem na adoção prática de autenticação descentralizada.

Trabalhos relacionados

A Comprehensive Formal Security Analysis of OAuth 2.0 - Daniel Fett, Ralf Küsters, Guido Schmitz (2019)

O artigo apresenta a primeira análise formal realmente abrangente do protocolo OAuth 2.0 em um modelo web expressivo. Até então, a maior parte das pesquisas focava em falhas de implementações específicas ou modelos altamente simplificados, sem tratar de forma completa os elementos essenciais da Web moderna (como redirecionamentos, iframes, cookies e navegadores maliciosos). Os autores constroem um modelo formal detalhado que incorpora todos os quatro grant types do OAuth — Authorization Code, Implicit, Resource Owner Password Credentials e Client Credentials — e permitem que múltiplas instâncias do protocolo rodem simultaneamente, inclusive com RPs e IdPs maliciosos.

A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology - Kaneriya, Jayana; Patel, Hiren (2023)

O artigo apresenta um modelo de emissão e verificação de credenciais educacionais baseado em blockchain, projetado para aumentar segurança, auditabilidade e privacidade no compartilhamento de documentos acadêmicos. Os autores destacam problemas recorrentes em sistemas tradicionais, como falsificação de diplomas, manipulação de registros, processos lentos de verificação e ausência de autonomia dos estudantes sobre seus dados. Para resolver esses desafios, o estudo propõe um framework usando Ethereum, IPFS e contratos inteligentes para garantir descentralização, prova criptográfica de atributos e controle granular sobre quais dados são revelados ao verificador. O modelo implementa quatro contratos principais — enrolamento, emissão de credenciais, consentimento e verificação — além de serviços off-chain para criptografia e armazenamento distribuído.

Materiais e Métodos

O estudo foi dividido em quatro etapas principais: (i) definição e caracterização dos materiais analisados; (ii) extração sistemática das métricas relevantes; (iii) normalização qualitativa dos dados; e (iv) síntese anaítica por meio de matriz comparativa. No TCC I, essas etapas foram planejadas e formalizadas; no TCC II, serão tratadas integralmente e concluídas.

Tabela 2. Matriz Comparativa Baseada em Evidências Empíricas Publicadas

Dimensão	Centralizado	Blockchain
Segurança	Vulnerável a ataques estrutu- rais: <i>mix-up</i> , <i>token substitu- tion</i> , <i>open redirect</i> (Fett et al.).	Resiliente por natureza; consenso distribuído; provas criptográficas (Zhang et al.; Kaneriya & Patel).
Desempenho	Autenticação média de 5– 50 ms dependendo do IdP.	Aproximadamente 150 ms para geração/validação OTP (Zhang et al.); cerca de 1 s para verificação completa (Kaneriya & Patel).
Auditabilidade	Logs privados e modificáveis; dependência do servidor.	Imutabilidade, verificabi- lidade pública; prova de inclusão em árvore de Mer- kle.
Operacionalidade / Adoção	Alta maturidade; baixa com- plexidade de integração.	Alta complexidade técnica; barreiras organizacionais; ne- cessidade de habilidades es- pecíficas.

Cronograma do TCC II

Tabela 3. Cronograma Previsto para o TCC II

Atividade	Ago	Set	Out	Nov
Revisão e atualização da literatura	X			
Extração das métricas	X	X		
Normalização dos dados		X		
Construção da matriz comparativa		X	X	
Análise crítica e discussão			X	
Conclusão e ameaças à validade			X	X
Revisão, ajustes finais e entrega				X

Obrigado!