REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

ARQUITETURA EM BLOCKCHAIN: REGISTRO E VERIFICAÇÃO DE EVIDÊNCIAS DE HORAS COMPLEMENTARES EM CURSOS SUPERIORES

BLOCKCHAIN ARCHITECTURE FOR RECORDING AND VERIFYING COMPLEMENTARY ACADEMIC ACTIVITY EVIDENCE IN HIGHER EDUCATION

Ciências Exatas e da Terra • 21/11/2026

REGISTRO DOI: 10.70773/revistatopicos/795001318

Gustavo de Andrade Pacheco[1]

Luis Cuevas Rodriguez[2]

RESUMO

O registro e a validação de horas complementares no ensino superior envolvem certificados de diferentes emissores, aplicação de regras acadêmicas e acompanhamento de decisões que podem exigir auditoria. Este estudo propõe uma arquitetura híbrida baseada em blockchain permissionada para registrar, validar e verificar evidências dessas atividades, considerando integridade, rastreabilidade, governança e privacidade. A pesquisa adota a abordagem Design Science Research, com especificação de requisitos, concepção de componentes e contratos inteligentes, demonstração por seis cenários hipotéticos e avaliação analítica de segurança, confiabilidade e eficiência potencial. A solução combina serviços de aplicação, armazenamento institucional fora da cadeia e registros distribuídos de hashes, estados e decisões, preservando a avaliação humana da pertinência dos certificados. A análise indica que os mecanismos especificados são conceitualmente adequados para detectar alterações posteriores ao registro, apoiar o controle de acesso, contabilizar horas e preservar o histórico de validações e revogações. Entretanto, a tecnologia não assegura a veracidade dos documentos apresentados nem elimina todas as duplicidades, e sua adoção implica custos e requisitos de governança. Conclui-se que o uso da blockchain apresenta justificativa mais consistente em contextos de verificação interinstitucional, devendo sua viabilidade operacional ser investigada por meio de implementação e comparação com soluções centralizadas.

Palavras-chave: Blockchain permissionada; Atividades complementares; Arquitetura de software; Verificação de documentos; Rastreabilidade.

ABSTRACT

The recording and validation of complementary academic activities

in higher education involve certificates issued by different organizations, the application of academic rules, and decisions that may require auditing. This study proposes a hybrid architecture based on a permissioned blockchain to record, validate, and verify evidence of these activities, considering integrity, traceability, governance, and privacy. The research follows the Design Science Research approach, encompassing requirements specification, the design of components and smart contracts, demonstration through six hypothetical scenarios, and an analytical assessment of security, reliability, and potential efficiency. The architecture combines application services, institutional off-chain storage, and a distributed ledger containing hashes, states, and decisions, while retaining human judgment regarding the relevance of certificates. The analysis suggests that the specified mechanisms are conceptually suited to detecting post-registration modifications, supporting access control, calculating validated hours, and preserving the history of approvals and revocations. However, the technology does not establish the truthfulness of submitted documents or eliminate every form of duplication, and its adoption entails additional costs and governance requirements. The study concludes that blockchain is more strongly justified in interinstitutional verification settings; operational feasibility remains to be examined through implementation and comparison with centralized alternatives.
Keywords: Permissioned Blockchain; Complementary Academic Activities; Software Architecture; Document Verification; Traceability.

1. INTRODUÇÃO

As atividades complementares integram a formação acadêmica em diversos cursos de graduação, permitindo o reconhecimento de experiências relacionadas ao ensino, à pesquisa, à extensão e ao

desenvolvimento profissional. Em cursos de Engenharia, essas atividades podem incluir participação em eventos científicos, monitorias, projetos de iniciação científica, minicursos e outras experiências previstas nos regulamentos institucionais. Sua integralização exige procedimentos de comprovação, análise e contabilização das cargas horárias, de acordo com critérios estabelecidos por cada instituição.

A comprovação dessas atividades frequentemente envolve a apresentação de certificados e declarações em formato digital, submetidos a sistemas acadêmicos ou encaminhados aos setores responsáveis. Embora esses procedimentos facilitem a organização documental, a validação pode exigir conferência manual da origem, do conteúdo e da carga horária declarada, além da identificação de submissões duplicadas e da aplicação de limites por categoria. A ausência de mecanismos adequados de rastreabilidade também pode dificultar a reconstituição das decisões tomadas durante o processo de avaliação.

Tecnologias de registro distribuído, como a blockchain, têm sido investigadas para apoiar a emissão, o gerenciamento e a verificação de credenciais acadêmicas. Rustemi et al. (2023) sistematizam pesquisas voltadas à verificação de certificados, enquanto Tanim et al. (2026) apresentam uma arquitetura para microcredenciais baseada em contratos inteligentes e armazenamento descentralizado. Terzi et al. (2026), por sua vez, abordam a integração de credenciais verificáveis com mecanismos de identidade, privacidade e governança institucional. Esses trabalhos demonstram o interesse na utilização de arquiteturas distribuídas para a gestão de registros acadêmicos.

Entretanto, o registro de evidências de horas complementares apresenta particularidades em relação à emissão e à verificação de diplomas ou microcredenciais. Nesse processo, documentos provenientes de diferentes emissores são submetidos à avaliação de uma instituição, que precisa verificar sua pertinência acadêmica, aplicar regras de aproveitamento, consolidar horas por categoria e manter o histórico de decisões, incluindo eventuais revogações. Assim, o problema envolve não apenas a integridade dos arquivos, mas também a rastreabilidade do processo de validação e a aplicação consistente das regras institucionais.

A adoção de blockchain, contudo, não representa necessariamente a alternativa mais adequada para qualquer cenário. Wüst e Gervais (2018) destacam a importância das condições de confiança e do compartilhamento de responsabilidades na escolha dessa tecnologia. Estudos recentes também discutem os compromissos entre arquiteturas convencionais e soluções distribuídas, considerando desempenho, complexidade operacional e governança (Wang et al., 2026; de Alwis et al., 2025). Dessa forma, torna-se necessário examinar em quais condições uma blockchain permissionada pode agregar valor a um sistema de gestão de horas complementares, especialmente quando há necessidade de auditoria independente ou compartilhamento de registros entre instituições.

Diante desse contexto, a pesquisa procura responder à seguinte questão: como estruturar e avaliar conceitualmente uma arquitetura híbrida baseada em blockchain permissionada para o registro, a validação e a verificação de evidências de horas complementares no ensino superior, considerando integridade, rastreabilidade, governança e privacidade? O objetivo geral consiste em propor e

analisar uma arquitetura de software para essa finalidade. Especificamente, busca-se identificar os requisitos do processo de validação, justificar as decisões arquiteturais, especificar os componentes e mecanismos de registro e verificação e avaliar qualitativamente o comportamento esperado da solução diante de cenários de uso e riscos identificados.

A pesquisa adota a abordagem Design Science Research (DSR), orientada à concepção e à avaliação de artefatos destinados à solução de problemas práticos (Hevner et al., 2004; Peffers et al., 2007). O artefato desenvolvido consiste em uma arquitetura conceitual que combina serviços de aplicação, armazenamento institucional fora da cadeia e blockchain permissionada. Sua avaliação é conduzida de maneira analítica e descritiva, mediante cenários de demonstração e análise de requisitos, ameaças e limitações. Não são realizados testes experimentais ou implantação em ambiente institucional, de modo que os benefícios discutidos representam capacidades e impactos potenciais da arquitetura.

A contribuição do trabalho consiste na especificação de uma arquitetura voltada às particularidades da gestão de horas complementares, articulando regras acadêmicas, decisões humanas, registros verificáveis e mecanismos de auditoria. Além desta introdução, o artigo apresenta a fundamentação teórica e os trabalhos relacionados na Seção 2, a metodologia na Seção 3, o projeto da arquitetura na Seção 4, sua demonstração e avaliação analítica na Seção 5 e as considerações finais na Seção 6.

2. FUNDAMENTAÇÃO TEÓRICA E TRABALHOS RELACIONADOS

2.1. Blockchain Permissionada, Integridade e Registros Auditáveis

A blockchain é uma tecnologia de registro distribuído que utiliza mecanismos criptográficos para encadear transações e permitir a verificação de sua integridade. Diferentemente de um banco de dados administrado por uma única organização, uma rede blockchain pode compartilhar a manutenção e a validação dos registros entre diferentes participantes. Entretanto, essa característica não torna sua adoção necessária em todos os sistemas. Wüst e Gervais (2018) propõem critérios para avaliar sua aplicabilidade, considerando a existência de múltiplos responsáveis pela escrita dos dados, as relações de confiança entre eles e a disponibilidade de uma autoridade central confiável.

Nas redes permissionadas, os participantes são previamente identificados e suas operações estão sujeitas a políticas de acesso e validação. O Hyperledger Fabric constitui uma plataforma de referência nesse modelo, oferecendo serviços de gerenciamento de identidades, políticas de endosso e execução de contratos inteligentes, denominados chaincodes. Sua arquitetura separa a execução, a ordenação e a validação das transações, permitindo estabelecer regras de confiança adequadas às organizações participantes (Androulaki et al., 2018). Todavia, a distribuição dos registros não implica necessariamente governança descentralizada, especialmente quando todos os nós permanecem sob uma mesma administração.

A comparação com sistemas convencionais é relevante porque mecanismos de integridade e auditoria também podem ser implementados sem blockchain. Bancos de dados associados a assinaturas digitais, registros protegidos e controles de acesso podem atender a diferentes requisitos de segurança. A RFC 9162, por exemplo, especifica registros verificáveis baseados em árvores de

Merkle para transparência de certificados digitais TLS, demonstrando a possibilidade de verificar a inclusão e a consistência de registros sem utilizar blockchain (Laurie; Messeri; Stradling, 2021). Dündar, Öztürk e Mutlu (2024) discutem as diferenças entre blockchain e bancos de dados convencionais, destacando a necessidade de considerar desempenho, descentralização e requisitos de confiança na seleção da tecnologia.

Assim, o principal diferencial potencial de uma blockchain permissionada não está exclusivamente na proteção contra alterações, mas na possibilidade de manter um histórico compartilhado, sujeito a regras comuns e verificável por organizações administrativamente independentes. Essa escolha implica custos adicionais de infraestrutura, coordenação e governança, que devem ser considerados na concepção da arquitetura.

2.2. Blockchain na Gestão de Credenciais Acadêmicas

A utilização de blockchain na educação tem sido investigada principalmente para emissão, armazenamento, compartilhamento e verificação de credenciais acadêmicas. Rustemi et al. (2023), em uma revisão sistemática de 34 estudos, examinam abordagens para verificação de certificados e diplomas, identificando diferentes mecanismos de registro e validação. Essas aplicações buscam reduzir a dependência de procedimentos manuais e oferecer meios de conferir a integridade dos documentos. Entretanto, a correspondência entre um arquivo e seu registro criptográfico não comprova, isoladamente, a legitimidade de sua emissão ou a veracidade das informações nele declaradas.

Arquiteturas híbridas representam uma alternativa para conciliar verificabilidade e proteção de dados. Nesse modelo, documentos e informações pessoais permanecem em repositórios externos, enquanto a blockchain registra referências criptográficas e informações necessárias à verificação. Tanim et al. (2026) desenvolveram uma solução para microcredenciais acadêmicas utilizando Hyperledger Besu, contratos inteligentes e armazenamento descentralizado IPFS. A arquitetura contempla emissão, verificação e revogação de credenciais, tendo sido submetida a testes de desempenho. Terzi et al. (2026), por sua vez, apresentam uma arquitetura baseada em Hyperledger Indy, integrada a plataformas educacionais, com ênfase na interoperabilidade, em identidades descentralizadas e na divulgação seletiva de informações.

Além dos mecanismos tecnológicos, a participação de diferentes instituições exige estruturas de governança capazes de estabelecer responsabilidades e critérios de confiança. A revisão sistemática de de Alwis, Shrestha e Sarker (2025), que analisou 63 estudos, evidencia a importância de considerar direitos de decisão, responsabilização e coordenação entre participantes na aplicação de blockchain à acreditação educacional. Esses aspectos são particularmente relevantes quando os registros precisam ser reconhecidos ou auditados por organizações distintas.

2.3. Trabalhos Relacionados e Delimitação da Contribuição

Enquanto Tanim et al. (2026) abordam o gerenciamento de microcredenciais acadêmicas, Terzi et al. (2026) concentram-se na interoperabilidade e na governança de credenciais verificáveis. Essas abordagens diferem do processo de aproveitamento de horas

complementares, que envolve a avaliação institucional de evidências provenientes de diferentes emissores.

Sob a perspectiva arquitetural, Wang, Shukur e Zainol Ariffin (2026) apresentam uma avaliação experimental de alternativas para gestão de credenciais digitais integradas a sistemas de aprendizagem. O estudo compara uma solução monolítica, uma arquitetura de microsserviços, uma variante com Hyperledger Fabric e outra com ancoragem em blockchain pública, considerando desempenho e requisitos operacionais. Seus resultados reforçam a necessidade de avaliar os compromissos entre diferentes configurações, sem presumir que a introdução da blockchain proporcione, por si só, maior eficiência.

Os trabalhos examinados evidenciam avanços na verificação de credenciais, na interoperabilidade e na integração de serviços distribuídos. Entretanto, seu foco predominante difere do processo de aproveitamento de horas complementares, no qual certificados provenientes de diferentes emissores são apresentados pelos estudantes e submetidos à avaliação acadêmica. Esse processo envolve classificação por categoria, limites de carga horária, identificação de possíveis duplicidades, decisões humanas de aprovação ou rejeição, acumulação de horas e eventual revogação de registros anteriormente validados. Tais operações exigem associar a integridade documental às regras institucionais e à rastreabilidade das decisões.

Nesse contexto, o presente trabalho propõe uma arquitetura híbrida especificamente orientada ao gerenciamento de evidências de horas complementares. Sua contribuição consiste em integrar armazenamento institucional, registro distribuído e contratos

inteligentes responsáveis por regras objetivas e transições de estado, preservando a avaliação humana da legitimidade e da pertinência das atividades. Diferentemente de estudos voltados predominantemente à emissão de credenciais, a proposta enfatiza o ciclo de submissão, validação, contabilização, verificação e revogação de evidências acadêmicas, considerando as condições em que a governança compartilhada pode justificar o emprego de blockchain permissionada.

3. METODOLOGIA

3.1. Caracterização da Pesquisa e Design Science Research

A pesquisa caracteriza-se como aplicada, de abordagem qualitativa e natureza projetual, tendo como finalidade propor e avaliar conceitualmente uma arquitetura de software para o registro e a verificação de evidências de horas complementares em cursos superiores. A investigação não envolve a implementação de um sistema funcional ou sua implantação em ambiente institucional, concentrando-se na especificação do artefato e na análise de seu comportamento esperado diante de requisitos e situações representativas do domínio.

Adota-se a abordagem Design Science Research (DSR), orientada à construção e à avaliação de artefatos destinados à solução de problemas relevantes em sistemas de informação (Hevner et al., 2004). Como referência para a organização da pesquisa, utiliza-se a Design Science Research Methodology (DSRM), proposta por Peffers et al. (2007), que compreende seis etapas: identificação do problema e motivação, definição dos objetivos da solução, concepção e

desenvolvimento do artefato, demonstração, avaliação e comunicação dos resultados.

3.2. Procedimentos de Concepção, Demonstração e Avaliação

A identificação do problema e a definição dos objetivos fundamentaram-se na caracterização dos procedimentos de submissão e validação de atividades complementares e na revisão bibliográfica sobre blockchain, credenciais acadêmicas, segurança da informação e arquiteturas distribuídas. Os estudos examinados subsidiaram a identificação de limitações, requisitos e alternativas tecnológicas, sem a aplicação de um protocolo formal de revisão sistemática.

Na etapa de concepção, foram especificados os requisitos funcionais e não funcionais, os atores envolvidos, a organização dos componentes, o modelo de armazenamento e as operações dos contratos inteligentes. As decisões arquiteturais consideraram a comparação entre soluções centralizadas e blockchain permissionada, a separação entre dados registrados dentro e fora da cadeia e a necessidade de preservar a avaliação humana da legitimidade dos certificados. O resultado dessa etapa constitui a arquitetura apresentada na Seção 4.

A demonstração foi estruturada por meio de seis cenários hipotéticos de utilização, abrangendo registro regular de evidências, submissão duplicada, verificação por terceiros, alteração de documentos, tentativa de validação não autorizada e revogação de registros. Para cada cenário, foram identificadas as condições de entrada, as regras aplicáveis e o comportamento esperado dos componentes da arquitetura. Essa demonstração permite examinar

a correspondência entre os requisitos especificados e os mecanismos propostos, sem representar uma execução experimental do sistema.

A avaliação adotou uma abordagem analítica e descritiva, fundamentada nos requisitos e nos cenários de demonstração, considerando segurança, confiabilidade e eficiência potencial. Foram examinados os mecanismos previstos para proteção da integridade, controle de acesso, rastreabilidade das decisões e aplicação de regras acadêmicas, bem como as ameaças e os riscos residuais associados. Também foram discutidos os compromissos de governança e complexidade operacional em comparação com uma alternativa centralizada convencional.

Os resultados dessa avaliação são apresentados na Seção 5 e correspondem a capacidades e limitações inferidas do projeto arquitetural. Não foram realizadas medições de desempenho, testes de segurança, experimentos com usuários ou validação em ambiente institucional. Consequentemente, as conclusões não estabelecem ganhos quantitativos ou eficácia operacional comprovada, mas delimitam as condições e os aspectos que deverão ser investigados em implementações futuras. A comunicação do artefato e de sua avaliação é realizada por meio deste artigo, completando a organização da pesquisa segundo o DSRM.

4. PROJETO DA ARQUITETURA HÍBRIDA

4.1. Requisitos e Atores do Sistema

A arquitetura proposta busca atender às necessidades de registro, validação e verificação de evidências de horas complementares,

considerando as limitações discutidas nas seções anteriores. O sistema contempla seis perfis de atuação: estudante, coordenação ou comissão de atividades complementares, secretaria acadêmica, verificador externo ou auditor, administrador da rede e, opcionalmente, emissor da atividade. A avaliação da legitimidade e da pertinência dos documentos permanece sob responsabilidade institucional, enquanto os componentes computacionais apoiam a aplicação de regras objetivas e a rastreabilidade das decisões. A Tabela 1 apresenta os requisitos funcionais (RF) e não funcionais (RNF) que orientam o projeto arquitetural.

Tabela 1. *Requisitos funcionais (RF) e não funcionais (RNF).*

ID	Requisito
RF01	Autenticar usuários e controlar permissões conforme seus papéis institucionais.
RF02	Permitir a submissão de evidências com arquivo, categoria, carga horária e descrição da atividade.
RF03	Calcular o hash SHA-256 do arquivo e registrar sua referência e metadados mínimos na blockchain.
RF04	Detectar submissões idênticas do mesmo estudante e apoiar a identificação de possíveis duplicidades.
RF05	Aplicar regras objetivas de categorias, cargas horárias e limites de aproveitamento.
RF06	Permitir a aprovação ou rejeição de evidências pela coordenação, com registro do motivo.
RF07	Preservar o histórico das decisões, responsáveis e versões das regras aplicadas.
RF08	Verificar a correspondência entre o arquivo e seu registro, informando a situação da evidência.

RF09	Consolidar horas validadas e disponibilizar comprovantes verificáveis.
RF10	Permitir a revogação autorizada de evidências, preservando o histórico.
RNF01	Segurança: integridade, autenticação, autorização e rastreabilidade das operações.
RNF02	Privacidade: minimização dos dados registrados na cadeia e proteção das informações pessoais.
RNF03	Auditabilidade: reconstituição do histórico por participantes autorizados.
RNF04	Disponibilidade: tolerância a falhas e mecanismos de recuperação dos serviços.
RNF05	Usabilidade: acesso às funcionalidades sem manipulação direta de credenciais blockchain pelos usuários.
RNF06	Manutenibilidade e interoperabilidade: regras versionadas e interfaces padronizadas para integração acadêmica.

Fonte: *Elaborada pelos autores (2026).*

4.2. Justificativa da Blockchain Permissionada e Governança

A escolha da blockchain considera a necessidade de manter registros compartilhados e verificáveis, especialmente quando diferentes organizações participam de sua manutenção e auditoria. Entretanto, sistemas centralizados com assinaturas digitais, controles de acesso e mecanismos de auditoria também podem atender a diversos requisitos de integridade documental. Portanto, a adoção da blockchain deve considerar as relações de confiança, os participantes e os custos envolvidos (Wüst; Gervais, 2018; Dündar; Öztürk; Mutlu, 2024).

A Tabela 2 compara qualitativamente uma arquitetura centralizada convencional e uma blockchain permissionada de consórcio, com base nas características discutidas na literatura (Wang; Shukur; Zainol Ariffin, 2026).

Tabela 2. *Comparação entre arquitetura centralizada e blockchain permissionada.*

Critério	**Arquitetura centralizada convencional**	**Blockchain permissionada de consórcio**
Integridade	Hashes, assinaturas e registros protegidos.	Mecanismos criptográficos e histórico replicado.
Auditabilidade	Depende dos mecanismos de auditoria do operador.	Permite verificação por participantes autorizados.
Governança	Administração concentrada em uma organização.	Possibilidade de governança compartilhada.
Complexidade	Geralmente menor, com infraestrutura convencional.	Maior, devido aos nós, identidades e políticas da rede.
Independência institucional	Depende do operador ou de verificações externas.	Pode reduzir a dependência de uma única administração.
Desempenho	Pode apresentar menor sobrecarga operacional.	Acrescenta processamento de endosso, ordenação e validação.

Fonte: *Elaborada pelos autores (2026), com base na literatura.*

A principal justificativa da blockchain está, portanto, na possibilidade de compartilhar a manutenção e a verificação dos registros entre

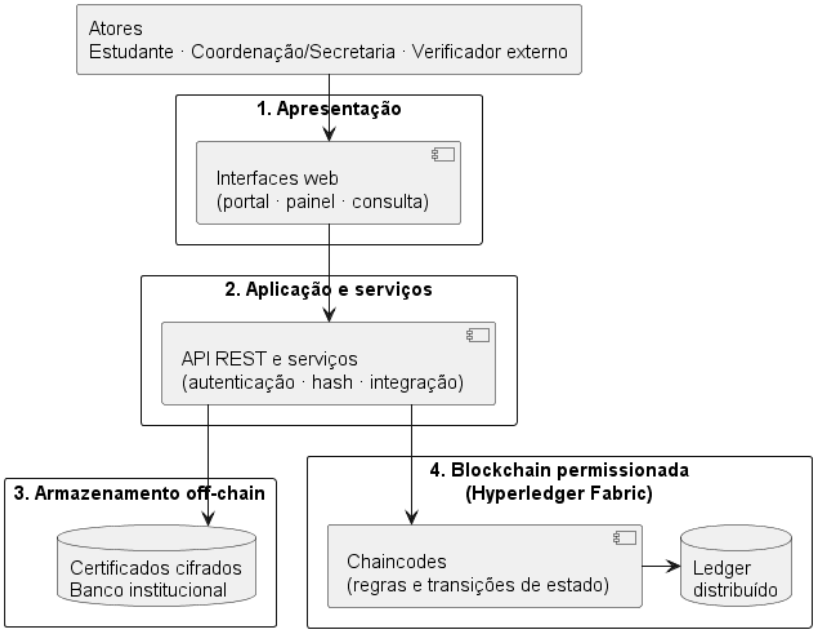
organizações independentes, e não exclusivamente na proteção contra adulterações. Essa vantagem depende de mecanismos efetivos de governança, incluindo definição de responsabilidades, permissões e critérios de participação (de Alwis; Shrestha; Sarker, 2025). Uma rede composta apenas por nós de uma mesma instituição não demonstraria, por si só, independência administrativa.

Propõe-se uma blockchain permissionada de consórcio, utilizando o Hyperledger Fabric como plataforma de referência, por disponibilizar gerenciamento de identidades, políticas de endosso, mecanismos de privacidade e contratos inteligentes (chaincodes) (Androulaki et al., 2018). A participação de instituições independentes constitui uma configuração prevista no projeto, cuja viabilidade deverá ser examinada em implementação futura.

4.3. Organização da Arquitetura e Modelo de Dados

A arquitetura adota uma organização híbrida em quatro camadas, apresentada na Figura 1: (i) apresentação, com interfaces para estudantes, coordenação, secretaria e verificadores; (ii) aplicação e serviços, responsável por autenticação, autorização, cálculo de hashes, integração e orquestração; (iii) armazenamento fora da cadeia (*off-chain*), destinado aos arquivos e dados institucionais; e (iv) blockchain permissionada, responsável pelo registro compartilhado e pela execução das regras de negócio. Essa separação é compatível com abordagens híbridas utilizadas em sistemas recentes de credenciais acadêmicas (Tanim et al., 2026; Wang; Shukur; Zainol Ariffin, 2026).

Figura 1. *Arquitetura híbrida proposta para registro e verificação de evidências de horas complementares.*



Fonte: *Elaborada pelos autores (2026).*

A camada de aplicação integra o armazenamento institucional e a blockchain sem expor sua complexidade aos usuários. O repositório externo mantém os certificados cifrados, dados pessoais e justificativas detalhadas. Na blockchain são previstos o identificador da evidência, a referência pseudonimizada do estudante, o hash SHA-256 do arquivo, a categoria, as horas declaradas e validadas, o estado do registro, as referências das decisões e a versão das regras utilizadas.

A separação entre dados registrados dentro e fora da cadeia busca reduzir a exposição de informações pessoais, preservando os elementos necessários à verificação e à auditoria. A aplicação administra as credenciais técnicas de acesso à rede e mantém mecanismos de vinculação entre as operações realizadas e os responsáveis institucionais. Contudo, a assinatura de uma transação por uma credencial administrada pela aplicação não comprova

isoladamente a participação de determinado usuário, exigindo controles complementares de autenticação e auditoria.

4.4. Contratos Inteligentes e Fluxos Operacionais

Os contratos inteligentes implementam regras objetivas e controlam as transições de estado das evidências, que podem assumir as situações submetida, validada, rejeitada ou revogada. A análise da legitimidade dos certificados continua sob responsabilidade da coordenação acadêmica, enquanto os contratos verificam condições previamente especificadas e registram as operações autorizadas. A Tabela 3 apresenta suas principais funções.

Tabela 3. *Principais funções dos contratos inteligentes*

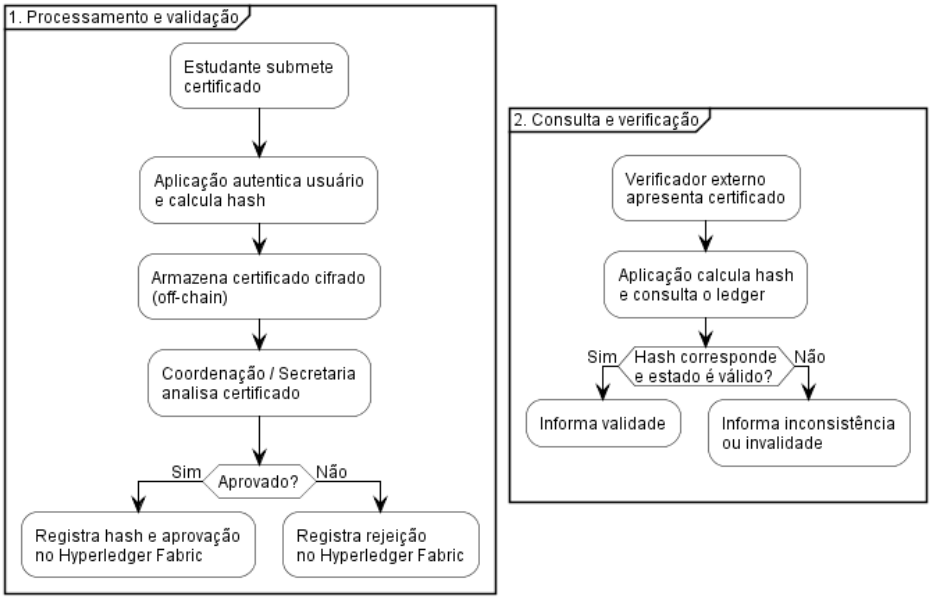
Função	**Solicitante**	**Regras aplicadas**
RegistrarEvidencia	Estudante, via aplicação	Verifica condições iniciais e registra a submissão.
ValidarEvidencia	Coordenação	Verifica autorização, aplica limites e registra a aprovação.
RejeitarEvidencia	Coordenação	Registra a rejeição e seu motivo.
RevogarEvidencia	Coordenação e secretaria	Exige autorizações distintas, revoga a evidência e atualiza o saldo.
VerificarEvidencia	Verificador autorizado	Consulta a correspondência do hash e a situação do registro.
ConsultarSaldo / ConsultarHistorico	Usuários autorizados	Recupera horas computadas e histórico conforme as permissões.

Fonte: *Elaborada pelos autores (2026).*

O processamento compreende quatro fluxos principais. No registro, o estudante submete a evidência, a aplicação calcula seu hash e armazena o arquivo cifrado, enquanto o contrato cria o registro na blockchain. Na validação, a coordenação confere a integridade e a pertinência do documento, aprova ou rejeita a solicitação e o sistema atualiza as horas computáveis. Na verificação, a aplicação compara o hash do arquivo apresentado ao registro e consulta sua situação, respeitando as permissões de acesso. Na revogação, a coordenação solicita a alteração, a secretaria autoriza e o contrato registra a nova situação, preservando o histórico anterior.

A Figura 2 apresenta os principais fluxos de atividades relacionados à submissão, à validação e à verificação das evidências. O diagrama evidencia a interação entre os usuários, os serviços de aplicação, o armazenamento externo e a blockchain, distinguindo a análise acadêmica da verificação criptográfica dos registros.

Figura 2. *Fluxos de processamento, validação e verificação de evidências de horas complementares.*



Fonte: *Elaborada pelos autores (2026).*

A detecção de duplicidades utiliza inicialmente a comparação de hashes de arquivos submetidos pelo mesmo estudante. Esse mecanismo identifica arquivos idênticos, mas não necessariamente certificados modificados que representem a mesma atividade, exigindo informações complementares ou análise humana. De modo semelhante, a correspondência criptográfica comprova a integridade em relação ao documento registrado, mas não a autenticidade de sua emissão.

A autorização acadêmica e o endosso técnico da blockchain constituem mecanismos distintos. As permissões institucionais controlam quem pode tomar decisões, enquanto as políticas de endosso determinam as condições técnicas de validação das transações na rede. As regras acadêmicas são previstas em configurações versionadas, permitindo identificar os critérios aplicados em cada decisão.

4.5. Privacidade, Segurança e Limitações Operacionais

A proteção dos dados considera os princípios de finalidade, necessidade e segurança previstos na Lei Geral de Proteção de Dados Pessoais (Brasil, 2018). Para minimizar a exposição, documentos e informações diretamente identificáveis permanecem fora da blockchain, enquanto a rede registra referências criptográficas e metadados restritos. Identificadores pseudonimizados reduzem a associação direta dos registros aos estudantes, mas não garantem anonimização irreversível, especialmente diante da possibilidade de correlação entre informações.

A arquitetura prevê autenticação institucional, segregação de permissões, proteção das chaves criptográficas e mecanismos de auditoria capazes de vincular operações às autorizações correspondentes. A disponibilidade depende tanto da configuração dos nós e do serviço de ordenação do Hyperledger Fabric quanto da continuidade dos serviços de aplicação e armazenamento externo, que também necessitam de redundância e recuperação de dados.

A permanência dos registros na blockchain exige atenção às solicitações de correção e eliminação de dados pessoais, cuja análise depende das condições legais e das obrigações institucionais de conservação. A utilização de armazenamento externo e pseudonimização constitui uma medida de mitigação, não uma garantia automática de conformidade com a LGPD.

5. DEMONSTRAÇÃO E AVALIAÇÃO ANALÍTICA

5.1. Demonstração por Cenários de Uso

A demonstração da arquitetura foi estruturada por meio de seis cenários hipotéticos representativos do processo de gerenciamento

de horas complementares em cursos superiores. Os cenários contemplam operações regulares e situações de inconsistência ou uso indevido, permitindo examinar a correspondência entre os requisitos estabelecidos e os mecanismos previstos no projeto. Por se tratar de um artefato conceitual, os comportamentos descritos representam respostas esperadas, não resultados de execução de um sistema implementado. A Tabela 4 apresenta os cenários, seus comportamentos esperados e os requisitos associados.

Tabela 4. *Cenários de demonstração da arquitetura proposta.*

Cenário	**Situação**	**Comportamento esperado**	**Requisitos**
C1. Registro regular	Estudante submete certificado de minicurso de 8 horas.	Registro do hash; análise da coordenação; inclusão das horas no saldo, se aprovadas conforme as regras.	RF02, RF03, RF05, RF06, RF09
C2. Submissão duplicada	Mesmo estudante reenvia arquivo idêntico.	Identificação da correspondência entre hashes, evitando nova contabilização da mesma evidência.	RF04
C3. Verificação por terceiro	Auditor consulta evidência registrada.	Consulta do estado e dos metadados permitidos; conferência do hash quando o arquivo é apresentado.	RF08, RNF03
C4. Documento adulterado	Carga horária de certificado registrado é	Hash do documento alterado não corresponde ao registro original.	RF08, RNF01

	alterada de 8 para 80 horas.		
C5. Validação não autorizada	Usuário sem permissão tenta aprovar evidência.	Operação rejeitada pelos mecanismos previstos de autenticação e autorização.	RF01, RF06, RNF01
C6. Revogação	Evidência validada é posteriormente considerada indevida.	Revogação mediante autorizações previstas, atualização do saldo e preservação do histórico.	RF07, RF10, RNF03

Fonte: *Elaborada pelos autores (2026).*

Em conjunto, os cenários permitem examinar a cobertura dos requisitos da arquitetura, sem constituir evidências experimentais de seu funcionamento ou de sua resistência a ataques.

5.2. Avaliação de Segurança, Confiabilidade e Eficiência

A avaliação analítica considera três critérios relacionados aos objetivos da pesquisa: segurança, confiabilidade e eficiência potencial. A segurança compreende a integridade dos registros, o controle de acesso e a proteção de informações; a confiabilidade envolve consistência das decisões, rastreabilidade e auditabilidade; e a eficiência corresponde às possibilidades de automatização das tarefas e redução de verificações manuais. A análise considera os mecanismos descritos na Seção 4 e os riscos que permanecem mesmo quando esses mecanismos são previstos. A Tabela 5 relaciona as principais ameaças às contramedidas propostas e aos respectivos riscos residuais.

Tabela 5. *Ameaças, contramedidas e riscos residuais*

Ameaça	**Contramedida proposta**	**Risco residual**
Adulteração após o registro	Hash SHA-256 associado ao registro na blockchain.	Não identifica falsificações anteriores ao registro.
Submissão duplicada	Comparação de hashes e análise de metadados.	Arquivos modificados podem representar a mesma atividade.
Validação não autorizada	Autenticação, controle de acesso e registro das autorizações.	Comprometimento de credenciais ou falhas na autorização.
Alteração indevida de decisões	Histórico distribuído, políticas de endosso e auditoria.	Conluio, falhas de governança ou concentração administrativa.
Exposição de dados pessoais	Armazenamento externo, pseudonimização e controle de acesso.	Vazamentos no repositório e reidentificação por metadados.
Indisponibilidade de serviços	Replicação dos registros, redundância e recuperação de dados.	Falhas nos serviços de aplicação, no armazenamento ou na rede.
Certificado falso na origem	Avaliação humana e eventual confirmação pelo emissor.	Aprovação indevida de documentos fraudulentos.

Fonte: *Elaborada pelos autores (2026)*

Quanto à segurança, o registro de hashes permite verificar se determinado arquivo corresponde à versão registrada, enquanto os mecanismos de autorização restringem as operações aos

responsáveis previstos. Entretanto, essas propriedades dependem da implementação correta dos controles e não garantem a veracidade dos documentos submetidos. Da mesma forma, as assinaturas técnicas das transações precisam ser associadas aos registros de autenticação institucional para apoiar a responsabilização dos usuários.

Em relação à confiabilidade, a arquitetura prevê a manutenção de históricos de estados, responsáveis e versões das regras acadêmicas. Esses elementos podem apoiar a reconstituição das decisões e a aplicação consistente dos critérios objetivos. A possibilidade de auditoria independente, contudo, depende da participação efetiva de organizações distintas na governança da rede. Uma implantação administrada exclusivamente por uma instituição não eliminaria a concentração de confiança.

Quanto à eficiência, a automatização de verificações objetivas, a consolidação das horas e a consulta aos registros podem reduzir atividades manuais de conferência e acompanhamento. Em contrapartida, a blockchain acrescenta etapas de processamento e custos de infraestrutura. Sem medições de tempo, carga de trabalho ou utilização de recursos, não é possível determinar se a arquitetura apresenta desempenho ou eficiência operacional superiores aos de uma solução centralizada.

5.3. Discussão dos Resultados e Limitações

A análise realizada indica aderência conceitual entre os requisitos e os mecanismos previstos na arquitetura, embora sua efetividade dependa de implementação e validação experimental. A combinação de armazenamento externo, contratos inteligentes e

registro distribuído permite estruturar um histórico verificável das decisões acadêmicas, mantendo separados os documentos e as informações necessárias à auditoria. Essa conclusão refere-se à adequação conceitual da arquitetura aos requisitos estabelecidos, e não à comprovação experimental de seu funcionamento.

As escolhas arquiteturais apresentam semelhanças com soluções recentes de credenciais acadêmicas. Tanim et al. (2026) demonstram a aplicação de contratos inteligentes e armazenamento externo ao gerenciamento de microcredenciais, enquanto Terzi et al. (2026) destacam a importância da privacidade, da interoperabilidade e da governança institucional. A presente proposta diferencia-se pelo foco no aproveitamento de horas complementares, processo que incorpora decisões humanas, regras de carga horária e acompanhamento acumulativo das evidências.

A comparação arquitetural de Wang, Shukur e Zainol Ariffin (2026) também reforça a necessidade de considerar os compromissos entre mecanismos de confiança distribuída e complexidade operacional. No contexto deste trabalho, a blockchain permissionada apresenta maior justificativa quando diferentes instituições precisam participar da manutenção ou verificação dos registros sem depender exclusivamente de uma administração central. Em cenários restritos a uma única instituição, uma solução convencional com mecanismos criptográficos e auditoria pode atender a parte significativa dos requisitos com menor complexidade.

A principal limitação da pesquisa decorre de seu caráter conceitual. Os cenários não foram executados em protótipo, os mecanismos de segurança não foram submetidos a testes e não houve avaliação com estudantes, coordenadores ou secretarias. Também não foram

mensurados custos, latência, vazão ou esforço administrativo. Desse modo, as conclusões estabelecem possibilidades e restrições fundamentadas no projeto, sem demonstrar melhorias quantitativas ou efetividade operacional.

6. CONSIDERAÇÕES FINAIS

Este artigo apresentou uma arquitetura híbrida baseada em blockchain permissionada para o registro, a validação e a verificação de evidências de horas complementares em cursos superiores. A proposta foi desenvolvida segundo a abordagem Design Science Research, contemplando a identificação de requisitos, a definição dos componentes arquiteturais e a demonstração e avaliação analítica por meio de cenários de uso. A arquitetura combina serviços de aplicação, armazenamento institucional fora da cadeia e contratos inteligentes, buscando integrar mecanismos de integridade documental, rastreabilidade das decisões e aplicação de regras acadêmicas.

Em resposta à questão de pesquisa, a análise indica que uma arquitetura dessa natureza pode estruturar o gerenciamento das evidências por meio de registros criptograficamente verificáveis, controle de transições de estado e preservação do histórico de aprovações, rejeições e revogações. Sua principal contribuição está na articulação desses mecanismos com as particularidades do aproveitamento de horas complementares, incluindo a classificação das atividades, os limites de carga horária, a contabilização acumulativa e a participação humana na avaliação dos documentos. A utilização de blockchain permissionada apresenta maior justificativa quando há necessidade de governança compartilhada e verificação dos registros por organizações independentes.

A avaliação conceitual também evidenciou limitações relevantes. A correspondência entre hashes permite identificar alterações em relação aos documentos registrados, mas não comprova a autenticidade de sua emissão ou a veracidade das informações apresentadas. Da mesma forma, a identificação de arquivos idênticos não impede todas as formas de reaproveitamento indevido de evidências. A proteção dos dados pessoais, a segurança das credenciais e a confiabilidade das decisões dependem de controles institucionais e operacionais adicionais. Além disso, os benefícios associados à descentralização devem ser ponderados diante dos custos e da complexidade de manutenção de uma rede permissionada.

O estudo limita-se à especificação e à avaliação analítica de um artefato conceitual, sem implementação, experimentação ou validação com usuários. Como trabalhos futuros, propõe-se desenvolver um protótipo baseado em Hyperledger Fabric, verificar o funcionamento dos contratos inteligentes e dos mecanismos de autorização e comparar a solução com uma arquitetura centralizada convencional. Recomenda-se, ainda, avaliar indicadores de desempenho, esforço administrativo, usabilidade e custos operacionais, além de investigar a integração com emissores de certificados e os requisitos de governança e proteção de dados em cenários interinstitucionais.

DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL

Durante a elaboração deste artigo, foi utilizada a ferramenta ChatGPT (OpenAI) como apoio à organização do manuscrito, à redação e revisão de trechos textuais, ao aprimoramento da clareza e da terminologia científica e à discussão de aspectos da arquitetura

proposta. As sugestões geradas foram submetidas à análise e revisão dos autores, que assumem integral responsabilidade pelo conteúdo científico, pela precisão das informações, pelas referências utilizadas e pelas conclusões apresentadas. A inteligência artificial não foi utilizada para produzir dados ou resultados experimentais.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDROULAKI, Elli et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains. In: EUROPEAN CONFERENCE ON COMPUTER SYSTEMS (EUROSYS), 13., 2018, Porto. **Proceedings** [...]. New York: ACM, 2018. Artigo 30, p. 1-15. Disponível em: https://doi.org/10.1145/3190508.3190538. Acesso em: 11 nov. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-normaatualizada-pl.html. Acesso em: 11 nov. 2026.

DE ALWIS, Anju; SHRESTHA, Anup; SARKER, Tapan. Exploring governance for accreditation in the education sector using blockchain technology: a systematic literature review. Discover Education, v. 4, artigo 57, 2025. Disponível em: https://doi.org/10.1007/s44217-025-00449-y. Acesso em: 11 nov. 2026.

DÜNDAR, Ahmet Anıl; ÖZTÜRK, Saim Buğrahan; MUTLU, Hakan. Interaction between blockchain technology and conventional databases: a systematic literature review. **Journal of Millimeterwave Communication, Optimization and Modelling,** v. 4, n. 1, p. 7-12, 2024. Disponível em: https://jomcom.org/index.php/1/article/view/75. Acesso em: 11 nov. 2026.

HEVNER, Alan R. et al. Design science in information systems research. **MIS Quarterly,** v. 28, n. 1, p. 75-105, 2004. Disponível em: https://doi.org/10.2307/25148625. Acesso em: 11 nov. 2026.

LAURIE, Ben; MESSERI, Eran; STRADLING, Rob. **Certificate Transparency Version** 2.0. RFC 9162. [S. l.]: RFC Editor, 2021. Disponível em: https://doi.org/10.17487/RFC9162. Acesso em: 11 nov. 2026.

PEFFERS, Ken et al. A design science research methodology for information systems research. **Journal of Management Information Systems,** v. 24, n. 3, p. 45-77, 2007. Disponível em: https://doi.org/10.2753/MIS0742-1222240302. Acesso em: 11 nov. 2026.

RUSTEMI, Avni et al. A systematic literature review on blockchain-based systems for academic certificate verification. **IEEE Access,** v. 11, p. 64679-64696, 2023. Disponível em: https://doi.org/10.1109/ACCESS.2023.3289598. Acesso em: 11 nov. 2026.

TANIM, Abrar Mahbub et al. Design and development of a blockchain-enabled decentralized framework for academic microcredentials. **IET Software,** v. 2026, n. 1, artigo 7326873, 2026. Disponível em: https://doi.org/10.1049/sfw2/7326873. Acesso em: 11 nov. 2026.

TERZI, Sofia et al. Governance and interoperability of verifiable educational credentials: an information systems architecture based on Hyperledger Indy. **Computers, Materials & Continua,** v. 89, n. 1, artigo 68, 2026. Disponível em: https://doi.org/10.32604/cmc.2026.084524. Acesso em: 11 nov. 2026.

WANG, Haoliang; SHUKUR, Zarina; ZAINOL ARIFFIN, Khairul Akram. A cloud-native blockchain-integrated architecture for digital credential management in learning management systems: empirical performance evaluation and deployment trade-offs. **Applied Sciences,** v. 16, n. 12, artigo 6198, 2026. Disponível em: https://doi.org/10.3390/app16126198. Acesso em: 11 nov. 2026.

WÜST, Karl; GERVAIS, Arthur. Do you need a blockchain? In: CRYPTO VALLEY CONFERENCE ON BLOCKCHAIN TECHNOLOGY (CVCBT), 1., 2018, Zug. **Proceedings** [...]. IEEE, 2018. p. 45-54. Disponível em: https://doi.org/10.1109/CVCBT.2018.00011. Acesso em: 11 nov. 2026.

---

[1] Discente do Curso de Engenharia de Software na Fundação Centro de Análise, Pesquisa e Inovação Tecnológica (FUCAPI) Manaus – AM – Brasil. E-mail: acesse o artigo original para visualizar o e-mail

[2] Professor Doutor, Fundação Centro de Análise, Pesquisa e Inovação Tecnológica (FUCAPI) Manaus – AM – Brasil. E-mail: acesse o artigo original para visualizar o e-mail