

Blockchain na Educação: Análise Competitiva de Plataformas para Emissão de Diplomas

Blockchain in Education: Competitive Analysis of Diploma Issuing Platforms

José Gladistone da Rocha

Ministério da Defesa
Secretária de Planejamento Baseado em
Capacidade
Brasília, DF, Brasil
jgladistone@gmail.com

Carlo Kleber da S. Rodrigues

Centro de Matemática Computação e Cognição
(CMCC)
Universidade Federal do ABC (UFABC)
Santo André, SP, Brasil
carlo.kleber@ufabc.edu.br

RESUMO

Pesquisas recentes têm se dedicado ao desenvolvimento de plataformas Blockchain para a emissão de diplomas de conclusão de cursos. Neste contexto, este artigo tem o objetivo de analisar competitivamente três importantes plataformas: BlockCerts, EduCTX e OpenCerts. Os experimentos de avaliação contemplam a discussão de aspectos teóricos e modelagem matemática, considerando os seguintes critérios: eficiência, segurança, consumo energético e escalabilidade sistêmica. Os resultados obtidos mostram que a plataforma EduCTX é aquela que tem melhor desempenho, pois apresenta maior eficiência e menor consumo energético. Como principal contribuição, este artigo se constitui em um relevante referencial para o desenvolvimento de novas plataformas, pois é capaz de identificar as principais características associadas aos mais recentes projetos. Ao final, conclusões e trabalhos futuros encerram este artigo.

Palavras-chave

Plataformas; Blockchain; Educação; Diplomas

ABSTRACT

Recent research has focused on the development of Blockchain platforms for issuing diplomas for completing courses. This article aims to competitively analyze three important platforms: BlockCerts, EduCTX, and OpenCerts. The evaluation experiments include discussion of theoretical aspects and mathematical modeling, considering the following performance metrics: efficiency, security, energy consumption, and systemic scalability. The results obtained show that the EduCTX platform is the one with the best performance, as it presents greater efficiency and lower energy consumption. As its main contribution, this article constitutes a relevant reference for the development of new platforms, as it is capable of identifying the main characteristics associated with the most recent projects. Finally, conclusions and future work close this article.

Keywords

Platforms; Blockchain; Education; Diplomas

1. INTRODUÇÃO

A tecnologia Blockchain tem seu início no ano 2008, quando são descritos os fundamentos da moeda digital descentralizada Bitcoin [1]. Essa tecnologia implementa um registro público global lógico, composto por blocos de dados encadeados de forma segura e imutável. O objetivo é garantir segurança, privacidade, transparência, descentralização e confiabilidade nas operações executadas no sistema computacional [1, 2].

Propostas de plataformas computacionais baseadas em Blockchain têm sido apresentadas em inúmeras áreas. Particularmente, no setor educacional [3, 4], a Blockchain pode abordar desafios comuns, mas ainda sem soluções de fato práticas, e.g., verificação de credenciais acadêmicas, compartilhamento de registros de alunos com segurança e criação de plataformas educacionais eficientes e transparentes [5]. Todavia, deve-se dizer que o emprego da Blockchain na educação ainda está em seus estágios iniciais [6].

Ante o exposto, este artigo analisa competitivamente três plataformas educacionais baseadas em Blockchain para emissão de diplomas de instituições de ensino. As plataformas analisadas são: BlockCerts [7], EduCTX [8] e OpenCerts [9]. Para tanto, os experimentos de análise contemplam discussão de aspectos teóricos e modelagem matemática, considerando os seguintes critérios: eficiência, segurança, consumo energético e escalabilidade sistêmica.

Neste contexto, como principal contribuição, esta pesquisa oferta relevantes subsídios para o desenvolvimento de novas plataformas Blockchain, pois é capaz de identificar as principais características associadas aos mais recentes projetos.

O restante deste trabalho está organizado como segue. A Seção 2 explica os fundamentos conceituais. Trabalhos relacionados estão na Seção 3. A Seção 4 explica a metodologia de escolha das três plataformas analisadas. Na Seção 5, detalham-se as três plataformas. A Seção 6 traz a análise competitiva dessas plataformas. Por fim, a Seção 7 encerra este trabalho com conclusões e trabalhos futuros.

2. FUNDAMENTOS

2.1 Tipos de Implementações

A tecnologia Blockchain permite que os dados, organizados em blocos encadeados, sejam distribuídos por toda a rede de nós participantes, formando uma corrente que cresce continuamente à medida que novos dados são adicionados na base de dados [1].

A autenticidade dos dados pode ser verificada por qualquer nó da rede, de forma anônima ou não, dependendo de como a rede é implementada: de forma pública, privada, consórcio ou híbrida [2, 10, 8]. As Blockchains públicas se destacam pela descentralização, transparência e acessibilidade [11]. As Blockchains privadas oferecem maior controle, segurança e privacidade, sendo mais apropriadas para ambientes corporativos e governamentais. As Blockchains híbridas e de consórcio, por sua vez, oferecem flexibilidade e eficiência, conforme a demanda do contexto de aplicação seja requerida [3, 11].

No caso de emissão de diplomas acadêmicos, uma implementação do tipo consórcio/híbrida é a opção mais adequada para a maioria das instituições, pois ela permite combinar a segurança e a escalabilidade de uma rede pública com a flexibilidade e o controle de uma rede privada [8], cujas características mais desejáveis estão na Tabela 1 [12, 13].

2.2 Algoritmos de Consenso

Os algoritmos de consenso são fundamentais para garantir a segurança da rede, a imutabilidade dos dados, a escalabilidade sistêmica e a descentralização de decisão [2, 8, 1].

A forma como os algoritmos de consenso funciona varia de um para outro, mas todos eles envolvem os passos básicos a seguir [1].

1. Proposta de um novo bloco: Um nó da rede propõe um novo bloco, contendo um conjunto de dados;
2. Validação do bloco: Os outros nós da rede verificam se o bloco é válido, ou seja, se ele segue as regras do protocolo e se as transações são legítimas;
3. Consenso: Os nós chegam a um acordo sobre a ordem em que os blocos devem ser adicionados à Blockchain;
4. Adição do bloco à Blockchain: O bloco validado é adicionado à Blockchain, e o processo se repete.

3. REVISÃO DA LITERATURA

Esta seção discorre sobre algumas plataformas Blockchain voltadas para operação na área educacional, incluindo a atividade de emissão de diplomas acadêmicos. Essas plataformas estão sumarizadas na Tabela 2.

Em [24], os autores analisam a plataforma Blockcerts, que tem as funções de emissão, visualização, compartilhamento e verificação de certificados. O certificado possui informações sobre o estudante, a qualificação, a data de emissão, entre outros detalhes. Após a emissão, é criado um *hash* único que representa

o certificado, e esse *hash*, juntamente com outros metadados, é registrado na rede, onde sua autenticidade pode ser verificada.

Em [20], os autores implementam um sistema de credenciamento para uso acadêmico focado na prevenção de fraudes em credenciais acadêmicas, denominado Acachain, visando reduzir o uso de recursos e o envolvimento de pessoas no processo.

Em [14], os autores implantam um sistema, na Universidade de Birmingham, de emissão de certificados chamado BTCert, propondo aprimorar a verificação de autenticidade de certificados e estabelecer um método seguro para revogá-los. O sistema permite que os estudantes autenticados em sua rede possam ver seus certificados e compartilhá-los a terceiros. O sistema utiliza a Blockchain pública do Bitcoin para armazenar os dados de autenticidade e um banco de dados local para os certificados.

A plataforma chamada Disciplina é proposta pelos autores em [15] para gerenciar históricos escolares com o uso da Blockchain, criando duas camadas de dados, uma privada, contendo dados sensíveis do estudante e uma pública, abrangendo a informação necessária para validar a autenticidade dos blocos privados.

Em [17] e [8], os autores propõem uma plataforma de gerenciamento de credenciais no ensino superior usando a

Blockchain, chamada EduCTX. Nessa plataforma, além de emissão e verificação de certificados, os estudantes podem armazenar todos os seus certificados de diferentes instituições. A plataforma funciona através de um consórcio entre as universidades, cada uma age como par na Blockchain, armazenando uma cópia do banco de dados, que pode ser consultada com uma chave de acesso própria. Outra função do sistema é gerenciar os créditos ganhos por disciplinas e cursos concluídos pelos estudantes.

Em [9], os autores implantam uma plataforma, denominada OpenCerts, para prover emissão padronizada e verificação de certificados para instituições de ensino. Outras instituições e empregadores podem usar o sistema para verificar a autenticidade dos certificados. Os certificados são emitidos em um arquivo de formato próprio e possuem um código digital único, que juntamente com os dados do estudante são guardados na Blockchain, e são utilizados para verificação de autenticidade.

O projeto Qualichain, criado pelos autores de [19], visa criar uma plataforma descentralizada para armazenar, compartilhar e verificar o currículo acadêmico e profissional dos usuários. A aplicação sugere acompanhar a vida acadêmica dos estudantes, apoiar empresas em contratações e colaborar na montagem de currículos escolares.

Em [18], os autores propõem uma plataforma chamada Blockchain of Learning Log (BOLL), visando à movimentação de informações acadêmicas através de contratos inteligentes entre instituições de ensino. Na proposta, a aplicação conta com um banco de dados em MongoDB para armazenar os dados do estudante, gerando melhoria na performance e acessibilidade de dados.

Os autores de [21] propõem um sistema que garante alta eficiência e segurança durante o processo de emissão de certificados, chamado BSCW. Os estudantes são responsáveis pelo gerenciamento dos certificados, concedendo acesso a terceiros para verificação de autenticidade. Contratos

inteligentes na Blockchain são utilizados para gerenciar identidades e certificados.

Em [22], os autores apresentam uma solução em Blockchain para a verificação de diplomas acadêmicos, chamada DocsChain. Os autores argumentam que o processo atual de verificação de diplomas é demorado e custoso, propondo um sistema que incorpora o fluxo de trabalho existente nas instituições de ensino de emissão de diplomas, usando reconhecimento óptico de caracteres (OCR) para extrair os dados dos documentos impressos e armazená-los na Blockchain junto com os detalhes do template OCR usado. O artigo descreve a arquitetura e o funcionamento da aplicação, bem como os resultados experimentais que mostram a sua eficiência e segurança.

Em [16], os autores propõem um sistema para emissão e validação de diplomas usando contratos inteligentes na rede da

diplomas. Essa contribuição se revela pela comparação de três das plataformas constantes na Tabela 2, a saber: BlockCerts [7], EduCTX [17, 8] e OpenCerts [9].

4. METODOLOGIA DE ESCOLHA

São seis fatores considerados para a seleção das três plataformas analisadas neste artigo. Esses fatores estão indicados na Tabela 3. Para cada um desses fatores, são observados os critérios apresentados na Tabela 4 para efeito de pontuação. Os valores da pontuação são dados pela observação de cada fator em cada plataforma: se existe ou não, bem como pelo grau de sua existência, conforme os seguintes valores: 5 (quando evidenciado plenamente); 3 (quando evidenciado, mas necessita de melhorias); e 1 (quando não evidenciado) [3, 13, 25, 17, 26].

Tabela 1: Tabela de características de um sistema de emissão de diplomas

Características	Definição
Alta disponibilidade	A emissão de diplomas não pode ser interrompida
Segurança	A proteção dos dados dos alunos é fundamental
Integração com sistemas acadêmicos	Facilitar a automatização dos processos
Escalabilidade	Capacidade de lidar com um grande volume de diplomas
Custo-benefício	A solução precisa ser economicamente viável

Tabela 2: Comparativo Geral das Plataformas

Plataforma	Referência	Ano	Ecosistema	Consenso	Rede	Piloto
Blockcerts	[7]	2016	Bitcoin	PoW	Pública	não
BTcert	[14]	2018	Bitcoin	PoW	Pública	não
Disciplina	[15]	2018	Ethereum	PoS	Consórcio	não
ECS	[16]	2018	Ethereum	-	-	sim
EduCTX	[17, 8]	2018	Ark	DPoS	Consórcio	não
BOLL	[18]	2019	Ethereum	PoW	Privada	sim
OpenCerts	[9]	2019	Ethereum	PoW	Consórcio	não
Qualichain	[19]	2019	Ethereum	PoA	Consórcio	não
UZHBC	[13]	2019	Ethereum	PoS	Pública	não
Acachain	[20]	2020	Hyperledger	Kafka	Privada	sim
BSCW	[21]	2020	Ethereum	PoS	Pública	sim
Docchain	[22]	2020	-	PoE	Privada	sim
Tolob	[23]	2021	Hyperledger	Kafka	Consórcio	sim

Ethereum, chamado ECS. Nesse contrato estão todas as informações necessárias para a emissão do diploma. Os autores concluem que, devido às características da Blockchain, a emissão de certificados se torna confiável e reduz os problemas com falsificações.

Em [23], os autores propõem um sistema de integração e compartilhamento de dados entre instituições de ensino, chamado Tolob, visando proporcionar uma cadeia cruzada para aprendizagem aberta. A aplicação é baseada em uma rede Blockchain de consórcio, implementada em IBM Hyperledger. Finalmente, em [13], os autores propõem um sistema na Universidade de Zurique chamado UZHBC.

Ante o exposto, este artigo busca contribuir para o desenvolvimento e a implementação de projetos relacionados ao desenvolvimento de plataformas baseadas em Blockchain para educação, considerando em especial a necessidade da emissão de

Sob a metodologia descrita, a partir da Tabela 5, vê-se então que as três melhores plataformas são: Blockcerts, Opencerts, EduCTX. Essas plataformas são as mais bem pontuadas nos seis fatores indicados.

Tabela 3: Fatores a serem considerados

Fatores	Descrições
Interoperabilidade	A plataforma deve se integrar facilmente com os sistemas existentes da instituição.
Escalabilidade	Capacidade de processar um grande número de transações por segundo sem comprometer a segurança ou a descentralização.

Segurança	A proteção dos dados dos alunos e instituições é fundamental. Resistência a ataques e garantias de que os dados são imutáveis e confiáveis.
Suporte	A disponibilidade de documentação, comunidade e suporte técnico é essencial.
Comunidade	Tamanho e atividade da comunidade de desenvolvedores e usuários.
Desenvolvimento	Facilidade para desenvolvedores criarem aplicativos e contratos inteligentes.

5. PLATAFORMAS SOB ANÁLISE

As plataformas sob análise são caracterizadas individualmente nas subseções a seguir, ressaltando seus correspondentes desafios, tecnologias e forma de operação. Esta subdivisão adotada facilita a análise comparativa entre as plataformas sob análise.

5.1 Plataforma Blockcerts

5.1.1 Desafios

Tabela 4: Critérios observados para cada fator considerado

Fatores	Critérios
Interoperabilidade	Compatibilidade com padrões de interoperabilidade; Capacidade de integração com outras plataformas; Facilidade de configuração; e Documentação técnica.
Escalabilidade	Capacidade de escalonamento; Desempenho sob carga; Estabilidade e confiabilidade.
Segurança	Autenticação e autorização; Criptografia e proteção de dados; Controle de acesso; Testes e avaliações regulares.
Suporte	Suporte e ajuda mútua; Comunicação eficaz.
Comunidade	Integração com outras comunidades; Documentação e recursos; Engajamento e participação; Qualidade do conteúdo compartilhado.
Desenvolvimento	Equipe e processo de desenvolvimento.

- Escalabilidade: A infraestrutura do Blockcerts precisa ser melhorada para lidar com o aumento do número de transações. Isso pode incluir a atualização dos nós da rede, a melhoria da conectividade e o aumento da capacidade de armazenamento.

- Interoperabilidade e Padronização: A falta de padronização em relação aos metadados e aos formatos de dados pode dificultar a interoperabilidade entre diferentes sistemas.
- Complexidade técnica: A tecnologia Blockchain e a criptografia envolvidas nos Blockcerts podem ser complexas para muitos usuários e instituições. Isso exige treinamento e conhecimentos específicos para a implementação e gestão desses sistemas.

5.1.2 Tecnologias

Além da Blockchain, as principais tecnologias empregadas nesta plataforma são elencadas a seguir.

- *Open Badges*: é um tipo de credenciamento digital que representa habilidades, conhecimento ou realizações adquiridas por uma pessoa. São emitidos por organizações, instituições de ensino ou empresas, e podem ser compartilhados em redes sociais, currículos ou portfólios.
- JSON-LD (JavaScript Object Notation for Linked Data): é um formato de dados que combina a simplicidade do JSON com a capacidade de representar dados conectados e semânticos, como os utilizados em RDF (Resource Description Framework) e Linked Data.
- Padrão W3C Verifiable Credentials: define um formato comum para representar credenciais digitais, incluindo os Blockcerts. Esse padrão permite a interoperabilidade entre diferentes sistemas e plataformas.

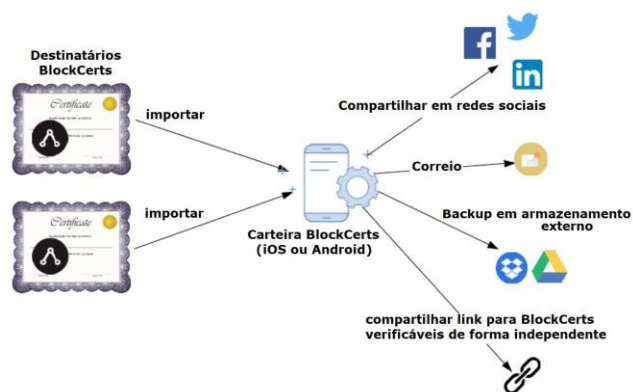


Figura 1: Recebendo e Compartilhando certificados com Blockcerts. Fonte: de [27]

5.1.3 Operação

A Figura 2 apresenta, de forma simplificada, a operação de Blockcerts para a emissão de diplomas. A identidade é separada das requisições sob uma perspectiva de camadas arquiteturais.

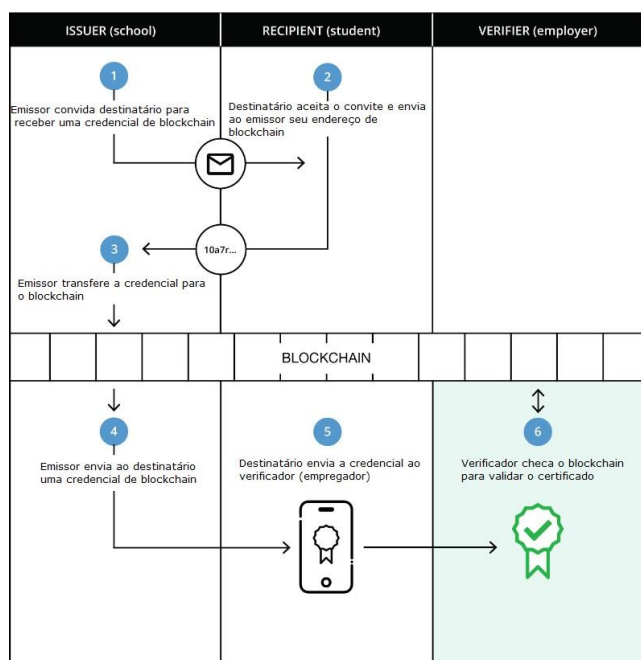


Figura 2: Funcionamento da Blockcerts. Fonte: de [27]

5.2 Plataforma EduCTX

5.2.1 Desafios

- Gerenciamento de *tokens*: O EduCTX utiliza *tokens* para representar créditos e outras informações relacionadas aos estudantes. O gerenciamento desses *tokens* de

Tabela 5: Comparativo das Plataformas entre os Diferentes Fatores

	Interoperabilidade	Escalabilidade	Segurança	Suporte	Comunidade	Desenvolvimento	TOTAL
Blockcerts	5	5	5	5	3	5	28
BTcert	5	5	5	3	3	5	26
Disciplina	3	5	3	3	1	5	26
EduCTX	5	5	5	3	5	5	28
OpenCerts	5	5	5	5	3	5	28
Qualichain	5	5	5	3	3	3	24
UZHBC	3	5	5	3	3	5	24

forma segura e eficiente é um desafio importante.

- Integração com sistemas legados: A integração do EduCTX com os sistemas existentes nas instituições de ensino pode ser complexa e demandar tempo e recursos.
- Governança: A definição de um modelo de governança para a plataforma é fundamental para garantir a sua sustentabilidade e o envolvimento de todos os *stakeholders*.

- Escalabilidade: A medida que o número de usuários e certificados aumenta, a rede baseada em Blockchain precisa ser capaz de processar um grande volume de transações de forma eficiente.
- Interoperabilidade: Garantir que os certificados emitidos pelo EduCTX sejam compatíveis com outros sistemas e plataformas é um desafio complexo, especialmente considerando a diversidade de formatos e padrões existentes no setor educacional.

5.2.2 Tecnologias

Além da Blockchain, as principais tecnologias utilizadas nesta plataforma são citadas a seguir.

- Contratos inteligentes: essa tecnologia é usada para fazer a emissão, verificar a autenticidade e gerenciar permissões de acesso aos certificados. Os contratos inteligentes são também utilizados para registrar o histórico de alterações feitas no certificado e também proporcionar a integração com outras plataformas e sistemas.
- JSON-LD (JavaScript Object Notation for Linked Data): uso análogo ao da plataforma Blockcerts.
- Identidade descentralizada: é usada para fornecer uma forma segura e descentralizada de gerenciar identidades e credenciais, pois permite aos usuários a criação de suas próprias identidades descentralizadas. É possível gerenciar credenciais, como certificados de conclusão de curso, diplomas e outros documentos importantes por meio da verificação da identidade dos usuários e, assim, garantir que as credenciais sejam emitidas e verificadas de forma segura.
- *Open Registries of Identities and Credentials*: são registros

descentralizados que armazenam informações sobre identidades e credenciais.

5.2.3 Operação

O fluxo do processo de operação do EduCTX ocorre na sequência indicada a seguir.

1. Inicialmente o estudante define a instituição e, em seguida, a instituição define o contrato e requer um endereço Blockchain do EduCTX.

2. O aluno envia para um múltiplo endereço Blockchain o endereço personalizado. Usando a sua carteira (criada na configuração inicial do sistema), checka o endereço personalizado com o múltiplo endereço.
3. Caso o endereço personalizado Blockchain não seja parte do múltiplo endereço Blockchain, esse endereço personalizado é descartado, do contrário, solicita ao estudante que assine randomicamente a mensagem de confirmação com o endereço personalizado da Blockchain. Usando a carteira, assina a mensagem com a sua chave privada (criada na configuração inicial do sistema).
4. E informada à instituição a mensagem assinada. A instituição recebe do estudante a confirmação de assinatura da mensagem.
5. A Instituição, usando a carteira, verifica a assinatura da mensagem. Se a mensagem não é corretamente verificada, o processo é finalizado; do contrário, a instituição, usando a carteira e o múltiplo endereço são usados para checkar o número de *tokens*.

5.3 Plataforma OpenCerts

5.3.1 Desafios

- **Padronização:** Há múltiplos formatos, o que resulta na falta de um padrão universal para representar os OpenCerts. Isso dificulta a interoperabilidade entre diferentes sistemas e plataformas. Além do mais, a falta de uma definição clara de quais metadados devem ser incluídos em um certificado e em qual formato ainda é um ponto de discussão.
- **Confiança e Validação:** nem todos os emissores de OpenCerts possuem a mesma credibilidade, o que pode levantar dúvidas sobre a validade de um certificado. É necessário desenvolver infraestruturas confiáveis para armazenar e validar os certificados, garantindo a integridade dos dados.
- **Escalabilidade:** grande volume de emissão de certificados pode sobrecarregar os sistemas e dificultar a gestão. Quanto ao seu desempenho, é preciso garantir que os sistemas de verificação sejam capazes de processar um grande volume de solicitações de forma eficiente.
- **Privacidade e Segurança:** os dados pessoais contidos nos certificados devem ser protegidos contra acessos não autorizados e vazamentos. Há vulnerabilidades, pois os sistemas de emissão e verificação de certificados podem ser alvos de ataques cibernéticos.

5.3.2 Tecnologias

Além da Blockchain, as principais tecnologias envolvidas incluem as citadas a seguir:

- **JSON-LD (JavaScript Object Notation for Linked Data):** uso análogo ao da plataforma Blockcerts.
- **OpenAttestation:** é um padrão que define como criar documentos verificáveis, incluindo certificados. Ele fornece um conjunto de ferramentas e um esquema para garantir a autenticidade e a integridade dos documentos.
- **Web3:** é a próxima geração da Internet, em que tem-se a infraestrutura descentralizada necessária, como contratos inteligentes e armazenamento descentralizado. É um ambiente em que os usuários têm controle sobre seus próprios dados e identidades.
- **Smart contracts:** uso análogo ao da plataforma EduCTX.
- **Identidade descentralizada:** uso análogo ao da plataforma EduCTX.
- **Open Registries of Identities and Credentials:** uso análogo ao da plataforma EduCTX.
- **InterPlanetary File System (IPFS):** é o padrão de armazenamento de arquivos.

5.3.3 Operação

A operação para compartilhar o certificado pode ser resumida da forma descrita a seguir:

1. Inicialmente é realizada a criptografia do certificado e, em seguida, hospeda-se/implementa-se o certificado criptografado na Internet, ou seja, o certificado deve ser acessível a partir de uma URL.
2. Em seguida deve-se compartilhar URL em redes públicas (e.g., LinkedIn) para se ter acesso a ele.
3. A Figura 3 apresenta o esquema de funcionamento do OpenCerts.

6. COMPARAÇÃO

Esta Seção apresenta o comparativo das plataformas citadas na Seção anterior, cujas caracterizações estão na Tabela 6. Os critérios selecionados para a comparação dos sistemas de certificação baseados em Blockchain foram escolhidos para fornecer uma análise abrangente e relevante das capacidades e características de cada sistema. Esses critérios incluem: privacidade, consumo energético, escalabilidade, segurança e eficiência.

A análise comparativa entre essas plataformas constitui o aspecto central do presente estudo, buscando identificar as abordagens mais eficientes sem comprometer a segurança ou a funcionalidade. Tenciona-se apontar a plataforma que, segundo os critérios propostos, melhor se adéqua ao emprego na emissão de certificados educacionais.

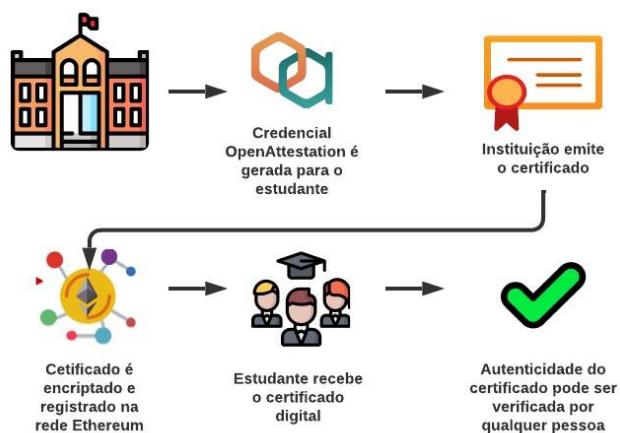


Figura 3: Funcionamento do Opencerts

6.1 Privacidade

As três plataformas apresentadas oferecem tratamento semelhantes quanto à questão da privacidade. Apenas o *hash* da emissão dos certificados é armazenado para provar que o certificado é legítimo, sendo utilizado pelo sistema para fazer esta verificação.

Após a emissão, o certificado fica na propriedade do estudante, que tem a liberdade de escolher onde guardar este certificado. As três plataformas oferecem aplicativos móveis para o estudante armazená-los: Blockcerts Wallet, MetaMask para EduCTX e MySkillsFuture para OpenCerts.

Apesar de as três plataformas terem comportamentos similares em termos de privacidade, as plataformas EduCTX e OpenCerts têm vantagem por serem implantadas em redes em consórcio, onde o acesso às transações pode ser limitado pelas instituições participantes [2], já o BlockCerts emprega a rede pública.

6.2 Consumo Energético

O consumo energético é influenciado principalmente pelo tipo da rede utilizado na implementação e o mecanismo de consenso utilizado pelo ecossistema ao validar uma transação. Em [28], o experimento realizado mostra o consumo energético aproximado por transação de diferentes implementações.

Ao analisar a Figura 4, nota-se que redes públicas consomem mais recursos do que as demais. Comparando as plataformas, Blockcerts utiliza aproximadamente 10^9 Joules por transação. EduCTX e OpenCerts utilizam aproximadamente 1 Joule por transação, caracterizando as mesmas como as plataformas que melhor aproveitam os recursos energéticos, ou seja, sendo as mais econômicas neste quesito.

6.3 Segurança

Esta Seção considerará, para avaliar o critério segurança, os seguintes princípios: disponibilidade, integridade e

confidencialidade, que, em conjunto, resultarão na avaliação do aspecto segurança.

A disponibilidade é a que garante que as informações estarão sempre prontas para serem usadas legitimamente. Como nenhum dado do estudante é armazenado na Blockchain, apenas o *hash* do certificado para futura verificação de autenticidade, pode-se concluir que a disponibilidade dos dados nas plataformas estudadas está no controle do estudante, já que ele detém a posse do certificado emitido.

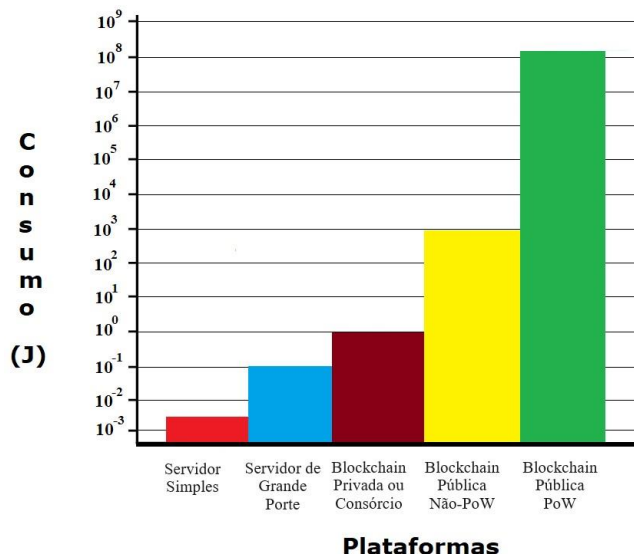


Tabela 6: Caracterização das Plataformas

	BlockCerts	EduCTX	OpenCerts
Ano do Projeto	2016	2018	2019
Ecossistema	Bitcoin	Ark	Ethereum
Mecanismo de Consenso	PoW	DPoS	PoW
Controle da ID	OpenBadge	ECTX	OpenAttestation
Linguagem de Programação	Python	Solidity	JavaScript
Tipo de Rede	Pública	Consórcio	Consórcio
Código Livre	Sim	Sim	Sim
Consumo (J)	Alto	Baixo	Baixo

Figura 4: Consumo Energético por Transação (J).

Em relação à integridade, aplica-se o entendimento de que o conceito teórico da Blockchain atende adequadamente aos requisitos em todas as plataformas. Em particular, o atributo da imutabilidade garante a integridade, pois qualquer alteração em um bloco implica uma alteração em todos os blocos subsequentes, o que resultaria em uma tarefa complexa em termos computacionais.

Por sua vez, a confidencialidade pode ser garantida empregando práticas de segurança da informação por meio da autenticação, autorização e auditoria no sistema. As plataformas citadas fazem uso da criptografia de dados nas transações, utilizando a chave pública do estudante na emissão dos certificados. Assim, apenas o estudante tem e pode conceder acesso aos seus dados, utilizando sua chave privada para compartilhar o certificado com outras instituições, por exemplo. As plataformas são comprometidas com a identidade auto soberana de todos os participantes e permitem o total controle do destinatário sobre seus dados.

Disso posto, por adotarem mecanismos que empregam a criptografia dos dados com uso de chaves duplas, a disponibilidade e integridade proveniente do encapsulamento por meio de blocos encadeados por meio de funções *hash*, resultam em modelos de grande semelhança, onde conclui-se que, no quesito segurança, as três plataformas se equiparam.

6.4 Eficiência

A eficiência pode ser mensurada pela quantidade de *Transações por Segundo* (TPS) que cada plataforma é capaz de realizar [29]. As TPS podem ser calculadas utilizando a Equação 1.

$$TPS = \frac{TPB}{TB} \quad (1)$$

TPB são as *Transações por Bloco*, que consiste no número de transações suportadas dentro de um bloco. Como nem todas as transações têm o mesmo tamanho (em bytes), esse valor pode variar. A Tabela 7 apresenta o número máximo de transações suportadas em um bloco de cada ecossistema. Já TB é *Tempo do Bloco*, que consiste na latência da rede ao gerar um bloco de transações. Em outras palavras, é o tempo, em segundos, que o emissor espera para concluir uma transação. A Figura 5 apresenta os números de cada ecossistema [29].

Tabela 7: Número Máximo de Transações por Bloco

Bitcoin	Ethereum	Ark
2020	230	150

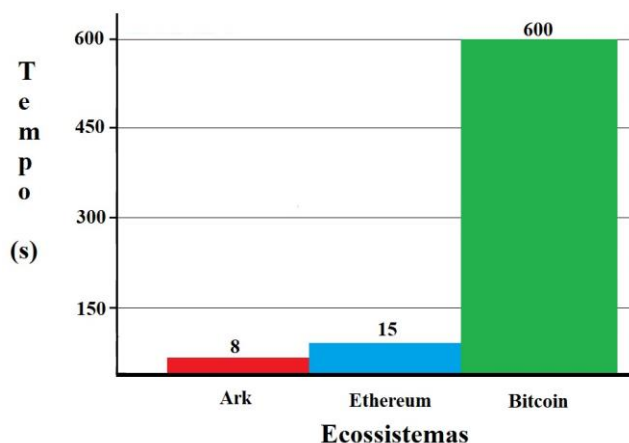


Figura 5: Tempo de Bloco (em segundos).

A Tabela 8 demonstra os resultados do cálculo das TPS mínimas que as plataformas podem apresentar. Esses valores são obtidos a partir da aplicação da Equação 1 com os valores apresentados na Tabela 7 e os valores apresentados na Figura 5. Assim, para as três plataformas, verifica-se que o mecanismo da EduCTX é o mais eficiente de todos, seguido do OpenCerts, e ficando o BlockCerts como o menos eficiente.

Tabela 8: Transações Por Segundo

BlockCerts	EduCTX	OpenCerts
3,3	18,75	15,3

6.5 Escalabilidade

A escalabilidade é um dos principais desafios enfrentados pelas redes Blockchain [30], quanto maior o número de participantes, maior o número de transações, levando a tempos de processamento mais longos.

As redes públicas apresentam maior dificuldade devido ao grande número de nós. Em uma rede privada ou em consórcio, esse número pode ser limitado. Outro ponto fundamental é o mecanismo de consenso utilizado na implementação. As plataformas apresentadas dependem da capacidade da rede Blockchain subjacente de processar e validar transações. Quanto mais transações a rede pode lidar, maior é a

quantidade de certificados que podem ser emitidos e verificados.

Valendo-se da base teórica antes apresentada, em razão do ecossistema utilizado em sua implantação, com o conjunto entre rede em consórcio, o mecanismo de consenso DPoS e os números obtidos na Tabela 8, a plataforma EduCTX apresenta os melhores resultados em escalabilidade, com o crescimento exponencial da sua rede de participantes, seguida das plataformas OpenCerts e BlockCerts.

6.6 Sumarização dos Resultados

Para o preenchimento dos valores na Tabela 9, adotou-se a seguinte escala de valores: 5 pontos para o melhor posicionado; 3 pontos para o segundo lugar e 1 ponto para o pior posicionado.

Diante do observado na Tabela 9, verifica-se que a plataforma mais bem pontuada foi a EduCTX, ficando em segundo lugar o OpenCerts, e BlockCerts em último lugar.

Tabela 9: Sumarização dos resultados.

Critérios	BlockCerts	EduCTX	OpenCerts
Privacidade	1	5	5
Consumo Energético	1	5	5
Segurança	5	5	5
Eficiência	1	5	3
Escalabilidade	3	5	3
TOTAL	11	25	21

7. CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho teve como objetivo comparar três plataformas de Blockchain que empregam a funcionalidade de emissão de Certificados/Diplomas acadêmicos e, assim, verificar, segundo os critérios de privacidade, consumo energético, segurança, eficiência e escalabilidade, qual plataforma melhor se comporta para esse fim.

De forma geral, foi possível observar que a plataforma EduCTX é a que apresenta maior efetividade, ficando em segundo lugar a plataforma OpenCerts e, por fim, a BlockCerts. Entretanto, apesar dos resultados desfavoráveis para a plataforma BlockCerts, não significa que venha a mesma ser de qualidade sofrível. A pontuação foi necessária apenas para identificar qual plataforma apresentava melhores condições segundo os quesitos propostos.

Como trabalhos futuros, sugere-se aumentar o número de critérios a serem observados e englobar um número maior de plataformas Blockchains para emprego educacional na emissão de certificados/diplomas acadêmicos.

8. REFERÊNCIAS

- [1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/en/bitcoin-paper>, 2008. Acesso em 25 setembro 2023.
- [2] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564, 2017.
- [3] Younghun Chae. Blockchain technology in education: A comprehensive review in transparency. *2023 Congress in Computer Science, Computer Engineering, Applied Computing*, 2023.
- [4] Nazmus Sakib Hossain Shahriar Hisham Haddad Sharaban Tahora, Bilash Saha. Blockchain technology in higher education ecosystem: Unraveling the good, bad, and ugly. *Department of Computer Science, Kennesaw State University, Georgia, United States*, 2023.
- [5] Abhishek Pingre Shailesh Rathod Shreya Mendhe Tushar Pawade, Fatebahadur Nandwanshi. A blockchain-based higher education credit platform. *International Journal of Ingenious Research, Invention and Development*, 3(1):87–95, 2024.
- [6] Karamjeet Kaur. Blockchain technology in education: Applications and challenges. *Cross-Currents: An International Peer-Reviewed Journal on Humanities Social Sciences*, 10(4):128–133, 2024.
- [7] Merija Jirgensons and Janis Kapenieks. Blockchain and the future of digital learning credential assessment and management. *Journal of Teacher Education for Sustainability*, 20:145–156, 06 2018.
- [8] Kristjan Kosić Marjan Herić Aida Kamisalić Muhamed Turkanović, Marko Holbl. EduCTX: A blockchain-based higher education credit platform. *University of Maribor*, pages 1–20, 2017.
- [9] GovTech Singapore. Opencerts: An easy way to check and verify your opencerts certificates. <https://www.opencerts.io>, 2019. Acesso em 25 setembro 2023.
- [10] Rafael Nasser Gustavo Robichez Hélio Lopes Marcos Kalinowski Paulo Henrique Alves, Rodrigo Laigner. Desmistificando blockchain: Conceitos e aplicações. *Sociedade Brasileira de Computação*, 2023.
- [11] Rogério Antônio Casagrande Miguel Sombrio, Luciano Antunes. Blockchain para autenticação de documentos em instituições de ensino. *REVISTA CADERNO PEDAGÓGICO*, 21(10):1–19, 2024.
- [12] Sergio Vargas Abdulghafour Mohammad. Challenges of using blockchain in the education sector. *Applied Sciences*, 12(6380):2–27, 2022.
- [13] Jerinas Gresch. An educational blockchain for the university of zurich (uzhbc). *University of Zurich*, 2018.
- [14] Birmingham University Blockchain Lab. Btcert. <https://github.com/BlockTechCert/BTCert>, 2018. Acesso em 25 setembro 2023.
- [15] Kirill Kuvshinov, I.I. Nikiforov, J. Mostovoy, Dmitry Mukhutdinov, Kirill, Andreev, and Vladislav Podtelkin. Disciplina: Blockchain for education. 2018.
- [16] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen. Blockchain and smart contract for digital certificate. In *2018 IEEE International Conference on Applied System Invention (ICASI)*, pages 1046–1051, 2018.
- [17] Muhamed Turkanović, Marko Holbl, Kristjan Kosić, Marjan Herić, and Aida Kamisalić. EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, 6:5112–5127, 2018.

- [18] Patrick Ocheja, Brendan Flanagan, Hiroshi Ueda, and Hiroaki Ogata. Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*, 14(1):4, Mar 2019.
- [19] Christos Kontzinos, Ourania I. Markaki, Panagiotis Kokkinakos, Vagelis Karakolis, Stavros Skolidakis, and John E. Psarras. Decentralised qualifications' verification and management for learner empowerment, education reengineering and public sector transformation: The qualichain project. 2020.
- [20] Kiratijuta Bhumichitr and Songsak Channarukul. Acachain: Academic credential attestation system using blockchain. In *Proceedings of the 11th International Conference on Advances in Information Technology, IAIT2020*, New York, NY, USA, 2020. Association for Computing Machinery.
- [21] Wolfgang Prinz, Sabine Kolvenbach, and Rudolf Ruland. Blockchain for education: Lifelong learning passport. *ERICIM News*, 2020, 2020.
- [22] Saqib Rasool, Afshan Saleem, Muddesar Iqbal, Tasos Dagiklas, Shahid Mumtaz, and Zia ul Qayyum. Docschain: Blockchain-based iot solution for verification of degree documents. *IEEE Transactions on Computational Social Systems*, 7(3):827–837, 2020.
- [23] Jun Xiao, Yi Jiao, Yin Li, and Zhujun Jiang. Towards a trusted and unified consortium-blockchain-based data sharing infrastructure for open learning; tolfob architecture and implementation. *Sustainability*, 13(24), 2021.
- [24] Fernando Vidal, Feliz Gouveia, and Christophe Soares. Analysis of blockchain technology for higher education. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pages 28–33, 2019.
- [25] Besnik Selimi Elva Leka. Bcert - a decentralized academic certificate system distribution using blockchain technology. *International Journal on Information Technologies Security*, 12(4), 2020.
- [26] Sanzar Adnan Alam Tanvir Ahmed Aadeef, Fahad Monir. Educational certification on ethereum blockchain: Analysis on how bcert and uzhhc differ. *Independent University Bangladesh*, 2023.
- [27] Site do blockcerts. 2024. Acesso: em 22 Ago 2024.
- [28] Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. The energy consumption of blockchain technology: Beyond myth. *Business I& information systems engineering*, 62(6):599–608, 2020.
- [29] Michael Catt. Blockchain fundamentals: Latency and capacity — featuring the ark ecosystem, Jul 2018.
- [30] Anamika Chauhan, Om Prakash Malviya, Madhav Verma, and Tejinder Singh Mor. Blockchain i& scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 122–128, 2018.