UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

JOÃO MARCELO FERNANDES DA SILVA JUNIOR

ANÁLISE DE VIABILIDADE DE UMA INFRAESTRUTURA BASEADA EM BLOCKCHAIN PARA O CONTROLE ACADÊMICO

CAMPINA GRANDE - PB

2022

JOÃO MARCELO FERNANDES DA SILVA JUNIOR

ANÁLISE DE VIABILIDADE DE UMA INFRAESTRUTURA BASEADA EM BLOCKCHAIN PARA O CONTROLE ACADÊMICO

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Orientador : Professor Dr. Kyller Costa Gorgônio

CAMPINA GRANDE - PB

2022

JOÃO MARCELO FERNANDES DA SILVA JUNIOR

ANÁLISE DE VIABILIDADE DE UMA INFRAESTRUTURA BASEADA EM BLOCKCHAIN PARA O CONTROLE ACADÊMICO

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA:

Professor Dr. Kyller Costa Gorgônio

Orientador – UASC/CEEI/UFCG

Professor Dr. Rohit Gheyi

Examinador – UASC/CEEI/UFCG

Professor Dr. Francisco Vilar Brasileiro

Professor da Disciplina TCC – UASC/CEEI/UFCG

Trabalho aprovado em: 02 de Setembro de 2022.

CAMPINA GRANDE - PB

RESUMO

Documentos acadêmicos são utilizados para registrar todos os dados relativos à vida acadêmica de um aluno, tais como habilidades adquiridas, disciplinas cursadas, cursos realizados, entre outros. Esses documentos são utilizados para comprovar os seus dados como aluno e também o vínculo com uma instituição de ensino. Entretanto, ao decidir solicitar esse documentos, a confecção e compartilhamento com outras instituições torna-se um problema devido ao tempo gasto e a burocracia envolvida nesses processos, principalmente no que diz respeito à checagem de autenticidade dos documentos. A blockchain é uma tecnologia que permite o registro de dados descentralizados que podem ser compartilhados com segurança, ou seja, é uma base de dados distribuída e com segurança garantida. Esse trabalho pretende analisar soluções baseadas em blockchain para permitir o registro, verificação e autenticidade de dados acadêmicos de um aluno de graduação e propor uma infraestrutura para uso sistema de controle acadêmico da Universidade Federal de Campina Grande.

Análise de Viabilidade de uma Infraestrutura Baseada em Blockchain para o Controle Acadêmico

João Marcelo Fernandes da Silva Junior
Universidade Federal de Campina Grande
Campina Grande, Paraíba, Brasil
joao.marcelo.junior@ccc.ufcg.edu.br

Kyller Costa Gorgônio
Universidade Federal de Campina Grande
Campina Grande, Paraíba, Brasil
kyller@computacao.ufcg.edu.br

RESUMO

Documentos acadêmicos são utilizados para registrar todos os dados relativos à vida acadêmica de um aluno, tais como habilidades adquiridas, disciplinas cursadas, cursos realizados, entre outros. Esses documentos são utilizados para comprovar os seus dados como aluno e também o vínculo com uma instituição de ensino. Entretanto, ao decidir solicitar esse documentos, a confecção e compartilhamento com outras instituições torna-se um problema devido ao tempo gasto e a burocracia envolvida nesses processos, principalmente no que diz respeito à checagem de autenticidade dos documentos. A blockchain é uma tecnologia que permite o registro de dados descentralizados que podem ser compartilhados com segurança, ou seja, é uma base de dados distribuída e com segurança garantida. Esse trabalho pretende analisar soluções baseadas em *blockchain* para permitir o registro, verificação e autenticidade de dados acadêmicos de um aluno de graduação e propor uma infraestrutura para uso sistema de controle acadêmico da Universidade Federal de Campina Grande.

PALAVRAS-CHAVE

Blockchain, educação, documentos acadêmicos.

1. INTRODUÇÃO

O avanço tecnológico atualmente oferece uma maior facilidade na execução de processos em diferentes áreas da sociedade. Concorrentemente, cresce a preocupação com a segurança e confiabilidade dos dados envolvidos. Nesse contexto encontram-se os processos relacionados a solicitação de documentos acadêmicos, por parte dos alunos, às instituições de ensino, que apesar das facilidades trazidas pelas tecnologias, ainda possuem bastante burocracia envolvida, a qual visa garantir segurança porém torna o processo lento.

Atualmente, a maioria das instituições de ensino possuem um sistema próprio de armazenamento das informações e documentos dos alunos, os quais podem ser acessados apenas por servidores específicos ou pelos alunos de forma restrita em sites ou sistemas dedicados para esse fim. Em geral, esses documentos são armazenados em banco de dados internos da instituição de ensino com acesso restrito ao seu pessoal de Tecnologia da Informação (TI) [1]. Dessa forma, ao necessitar de algum documento acadêmico para comprovação de informações, seja para transferência de instituição ou para entrevistas de emprego, o aluno necessita solicitar à instituição o documento autenticado, geralmente por meio de assinaturas dos servidores responsáveis.

A blockchain é uma tecnologia que permite o registro de dados descentralizados que podem ser compartilhados com segurança. A *blockchain* é uma tecnologia inovadora introduzida em 2008 servindo como suporte para a criação da criptomoeda *bitcoin* [2]. Atualmente a *blockchain* é utilizada em várias áreas da sociedade, sempre com o objetivo de garantir descentralização, autenticidade e transparência dos dados. Um dos domínios adequados para a adoção da tecnologia blockchain é o ensino superior, no qual os princípios da autenticação de documentos, transparência, imutabilidade e confiança são as principais vantagens que tornam essa combinação adequada [3]. Documentos acadêmicos como o histórico acadêmico registram todos os dados relativos à vida acadêmica do aluno, e servem como um certificado de aprendizado. A *blockchain* permite colocar a responsabilidade e controle sobre os dados acadêmicos sobre o aluno, sem a necessidade de verificação por intermediários, por exemplo a instituição acadêmica [4].

Esse trabalho tem como objetivo analisar o uso de infraestruturas baseadas em *blockchain* na educação para armazenamento, verificação e compartilhamento de documentos acadêmicos, por exemplo diplomas e certificados. Analisar a viabilidade de algumas das infraestruturas analisadas para uso no sistema de controle acadêmico da Universidade Federal de Campina Grande.

2. CONCEITOS

Nessa seção são apresentados conceitos importantes para melhor compreensão deste trabalho.

2.1 Blockchain

A tecnologia *blockchain* surgiu como suporte para a criação da moeda *bitcoin* [2]. Trata-se de um banco de dados distribuído, nas quais os dados, em forma de transações, são armazenados em blocos e adicionados no final de uma cadeia de outros blocos. Os blocos são estruturas que armazenam transações e uma referência ao bloco anterior. Após todas as transações serem armazenadas no bloco, o *hash* que identifica o bloco é gerado, o qual é adicionado ao bloco posterior [5]. A operação de geração desse *hash* é determinística, dessa forma sempre que for executada com as mesmas informações, resultará na mesma saída. Essa característica torna impossível a alteração dos dados de um bloco sem que seja necessário o recálculo dos blocos subsequentes [2].

Existem pelo menos dois tipos de *blockchain*: públicas e privadas [5]. No primeiro tipo, todos os dados armazenados na *blockchain* são publicamente acessíveis. No segundo tipo, apenas nós selecionados podem acessar os dados. Existe ainda um terceiro tipo chamado de *blockchain* permissionada, que permite um modelo híbrido, onde parte dos dados é acessível ao público, porém o registro de novos dados e acesso a dados específicos são acessados apenas por nós selecionados. A Figura 1 ilustra a estrutura de uma *blockchain*.

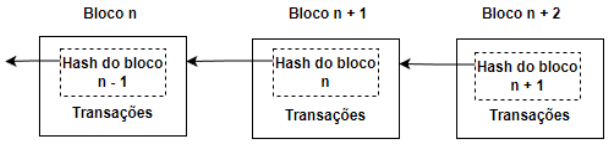

Figura 1: Representação da estrutura de uma *blockchain*. Fonte: Autoria própria.

2.2 Smart Contracts

O conceito de Smart Contracts foi introduzido por Nick Szabo [6]. Smart Contracts são códigos computacionais capazes de facilitar, executar e forçar o cumprimento de um acordo, por meio da Blockchain, de forma automática e segura. Os Smart Contracts apresentam um alto nível de segurança pois permitem que dois ou mais indivíduos, mesmo sem se conhecerem, façam negócios entre si sem que haja a necessidade de uma entidade centralizada como intermediária [7]. A partir do momento que as partes entram em acordo sobre o contrato, sua execução é iniciada pelos computadores, não podendo mais ser alterada ou interrompida.

3. METODOLOGIA

Esse trabalho foi realizado a partir da análise de sistemas baseados em *blockchain* para armazenamento e verificação de documentos acadêmicos, como diplomas e certificados de ensino superior. Os trabalhos científicos analisados foram buscados a partir das palavras-chave *blockchain*, educação e verificação. Os trabalhos para análise foram selecionados considerando as melhores propostas do uso da *blockchain* para armazenamento, verificação e compartilhamento de documentos acadêmicos, alinhado à viabilidade do uso no sistema Controle Acadêmico da Universidade Federal de Campina Grande.

Os trabalhos foram analisados de forma qualitativa, observando aspectos específicos das soluções propostas, como plataforma da *blockchain* utilizada (Bitcoin, Ethereum, desenvolvimento próprio), se possui aplicação desenvolvida para acesso a rede *blockchain* e forma de armazenamento na rede *blockchain*. A forma de armazenamento difere, pois é possível que apenas o *hash* do documento seja enviado para a *blockchain* e o documento propriamente dito, seja armazenado em um banco de dados local, como o PostgreSQL.

3.1 Trabalhos analisados

Em [8] os autores abordam o uso da *blockchain* para emissão e validação de certificados digitais com o objetivo de solucionar o problema de falsificação dos certificados na educação. Nesse estudo é proposto a criação de um sistema chamado Unicert e a implementação de uma *blockchain* chamada Unicoin, com a proposta de tornar o processo de emissão e verificação de certificados digitais mais fácil.

Na arquitetura do sistema o usuário interage com a aplicação Unicert enviando os dados do certificado, a aplicação então registra os dados em um banco de dados local PostgreSQL e envia o *hash* do documento para a *blockchain* Unicoin. A Figura 2 apresenta a arquitetura da solução apresentada.

Essa abordagem apresenta ser mais completa devido a implementação da aplicação e também da *blockchain* utilizada, além de apresentar um maior nível de segurança já que o registro é realizado tanto em um banco de dados local, como também na *blockchain*.

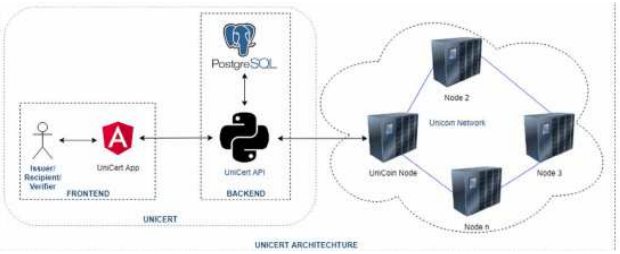

Figura 2: Arquitetura da Unicert. Fonte: [8].

Em [9] é proposta a plataforma CredenceLedger baseada em uma *blockchain* permissionada para verificação descentralizada de documentos educacionais. A utilização da *blockchain* permissionada permite que apenas informações selecionadas pelo dono dos dados possam ser visualizadas em uma consulta, porém é capaz de armazenar todas as informações necessárias. Todas as permissões de acesso podem ser configuradas pelo autor dos dados no momento em que as informações são salvas a partir de metadados.

Para acesso às informações de um certificado é necessário realizar uma solicitação ao autor, que através de um aplicativo desenvolvido pela plataforma, pode aprovar ou não o acesso às informações. A partir do acesso às informações é possível efetuar a validação do documento digital. A CredenceLedger não faz uso de criptomoedas para registro de informações, e sim de um valor hexadecimal, o que segundo a plataforma é uma vantagem. A figura 3 apresenta a arquitetura da CredenceLedger.

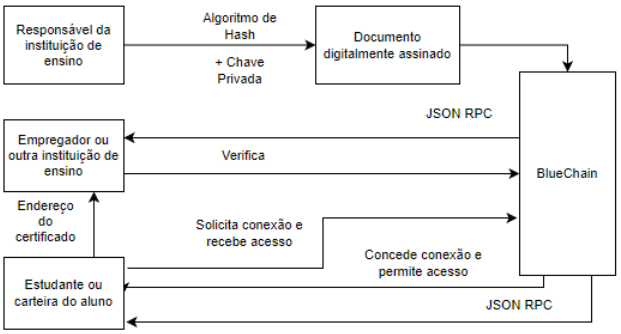

Figura 3: Arquitetura da CredenceLedger. Fonte: Adaptado de [9].

Em [10] é proposta uma plataforma global descentralizada baseada na tecnologia *blockchain* chamada EduCTX. Essa

plataforma permite gerenciar, atribuir e compartilhar credenciais para alunos, instituições de ensino e outras potenciais partes interessadas como empresas, instituições e organizações. Na plataforma são registrados *tokens* e transações que representam uma evidência confiável de habilidades e conhecimentos adquiridos pelo indivíduo, como também certificados, diplomas, cursos e experiências profissionais. Todas essas informações podem ser consultadas por partes interessadas como empresas empregadoras e instituições de ensino. Cada indivíduo tem seu próprio endereço na EduCTX onde é atribuído por uma instituição credenciais adquiridas. A plataforma permite a todos usuários o uso de uma aplicação web, que provê uma visão geral dos tokens recebidos pelo indivíduo. As instituições também possuem um endereço na EduCTX e o acesso a uma aplicação web que permite que gerenciam e transfiram tokens para os indivíduos. A plataforma EduCTX é baseada em uma *blockchain* permissionada e é desenvolvida para a rede Ethereum utilizando smart contracts. Na Figura 3 é apresentada uma representação da plataforma EduCTX.

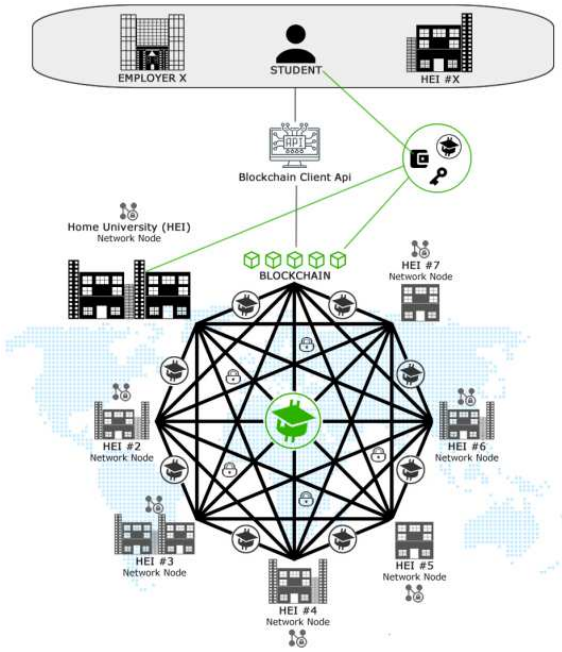

Figura 3: Representação alto nível da plataforma EduCTX. Fonte: [10]

Em [11] e [12] é apresentada uma solução chamada GT-RAP, Serviço de Registro, Autenticação e Preservação Digital de Documentos. É um sistema com suporte para registro, validação e preservação de diplomas acadêmicos baseados no uso da *blockchain.* Nessa abordagem, as instituições de ensino, na qual o aluno é egresso, são responsáveis pela emissão do diploma, o aluno é portador do diploma e os receptores são outras instituições de ensino, organizações e empresas privadas para as quais o portador precisa apresentar o diploma. Essa abordagem faz uso das redes *blockchain* da bitcoin e Ethereum. Na Figura 4 é apresentada uma visão geral do serviço proposto.

Figura 4: Visão geral do GT-RAP. Fonte: [11]

4. AVALIAÇÃO

Os pontos avaliados de cada solução proposta para a solução do problema tratado neste trabalho foram:

- Rede *blockchain* utilizada: se a tecnologia *blockchain* utilizada foi de desenvolvimento próprio ou utilizou-se alguma plataforma existente como Bitcoin ou Ethereum;
- Uso de Smart Contracts se foi utilizado a tecnologia de Smart Contracts;
- Forma de armazenamento das informações na rede: se dados armazenados na *blockchain* são informações dos documentos ou *hash* do endereço do banco de dados em que o documento está armazenado;
- Tipos de documentos acadêmicos utilizados: quais os documentos que a solução propôs utilizar (diploma, certificado, histórico acadêmico, etc.);
- Tipo de *blockchain* utilizada: pública, privada ou permissionada.

Esses pontos são avaliados para analisar a viabilidade da proposta para uso no contexto do controle acadêmico da Universidade Federal de Campina Grande (UFCG).

Na Tabela 1, são mapeados os pontos avaliados para cada solução estudada.

Solução	Implementação *blockchain*	Uso de Smart Contracts	Forma de armazenamento	Documentos abordados	Tipo de *blockchain*
Unicert	Própria	Não	Hash do documento	Certificados	Permissionada
CredenceLedger	Ethereum	Não	Hash do documento	Diversos dados acadêmicos	Permissionada
EduCTX	Ethereum	Sim	Informações dos documentos registrados na rede	Diversos dados acadêmicos	Permissionada
GT-RAP	Bitcoin e Ethereum	Não	Informações dos documentos registrados na rede	Diploma	Permissionada

Tabela 1: Pontos avaliados para cada solução analisada.

Todos os pontos avaliados acima foram definidos baseados nas características em comum apresentadas em todos os trabalhos estudados e que são importantes no momento de implementar uma infraestrutura semelhante.

Além dos pontos avaliados acima, existem outros critérios que podem ser importantes para avaliar a viabilidade das infraestruturas, por exemplo o custo da implementação e manutenção. No entanto, esses critérios não foram discutidos nos trabalhos nos quais as infraestruturas estudadas foram propostas, dessa forma a avaliação desse critério não foi possível neste presente trabalho.

5. CONCLUSÃO

Neste trabalho foram analisadas diferentes tipos de abordagens baseadas em blockchain que propõe solucionar a proposta de uma plataforma descentralizada para armazenamento, verificação e compartilhamento de documentos acadêmicos tendo a segurança garantida pelo uso da blockchain. A partir dos trabalhos analisados e dos pontos avaliados, uma proposta de infraestrutura para uso no controle acadêmico seria a união de princípios das abordagens Unicert e GT-RAP. Na primeira, o armazenamento do hash do documento na blockchain e o uso da base de dados local, torna o processo mais semelhante ao atual. Nesse sentido também, a utilização do próprio sistema já utilizado pela instituição para registro, autenticação e validação dos documentos, como visto na solução GT-RAP é a mais indicada visto que, a alteração na ferramenta atualmente utilizada seria mínima. É indicado também a utilização da rede blockchain Ethereum, que permite a implementação de novas abordagens facilmente, descartando a necessidade de uma implementação de uma rede blockchain própria.

Alguns pontos que ameaçam a validade do estudo são a ausência de uma definição mais detalhada da arquitetura proposta com uma simples implementação como prova de conceito, e também de uma análise do custo-benefício da implementação e manutenção da arquitetura a partir do contato com profissionais responsáveis pelo controle acadêmico.

Em possíveis trabalhos futuros recomenda-se a implementação de uma infraestrutura simples como prova de conceito com testes bem definidos, e também uma pesquisa de avaliação com servidores responsáveis pelo controle acadêmico e outros interessados como alunos e servidores da instituição.

6. REFERÊNCIAS

[1] Turkanović, Muhamed & Hölbl, Marko & Košič, Kristjan & Hericko, Marjan & Kamisalic, Aida. (2017). EduCTX: A Blockchain-Based Higher Education Credit Platform. IEEE Access. PP. 10.1109/ACCESS.2018.2789929.

[2] NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em:https://bitcoin.org/bitcoin.pdf. Acesso em: 20 ago. 2022.

[3] Grech, Alex & Camilleri, Anthony. (2017). Blockchain in Education. 10.2760/60649.

[4] Kamisalic, Aida & Turkanović, Muhamed & Mrdovic, Sasa & Hericko, Marjan. (2019). A Preliminary Review of Blockchain-Based Solutions in Higher Education. 10.1007/978-3-030-20798-4_11.

[5] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 10.1109/BigDataCongress.2017.85.

[6] Szabo, Nick. (1997). Formalizing and Securing Relationships on Public Networks. First Monday. 2. 10.5210/fm.v2i9.548.

[7] Melo de Morais, Anderson & Lins, Fernando. (2020). Uso de Blockchain na Educação: Estado da arte e desafios em aberto. Revista Científica Multidisciplinar Núcleo do Conhecimento. 78-100. 10.32749/nucleodoconhecimento.com.br/tecnologia/uso-de-blockchain.

[8] Huynh, Trong & Huynh, Trung & Pham, Dang & Ngo, Anh. (2018). Issuing and Verifying Digital Certificates with Blockchain. 332-336. 10.1109/ATC.2018.8587428.

[9] Arenas, Rodelio & Fernandez, Proceso. (2018). CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. 1-6. 10.1109/ICE.2018.8436324.

[10] Hölbl, Marko & Kamisalic, Aida & Turkanović, Muhamed & Kompara, Marko & Podgorelec, Blaž & Hericko, Marjan. (2018). EduCTX: An Ecosystem for Managing Digital Micro-Credentials. 1-9. 10.1109/EAEEIE.2018.8534284.

[11] Rostand Costa et al. 2018. Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos. In Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações, maio 06, 2018, Campos do Jordão, Brasil. SBC, Porto Alegre, Brasil.

[12] Mateus Pires, Daniel Souza, Rostand Costa, and Guido Lemos. 2018. Uma Abordagem Baseada em Brokers para Registro de Transações em Múltiplos Livros Razão Distribuídos . In Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações, maio 06, 2018, Campos do Jordão, Brasil. SBC, Porto Alegre, Brasil