



USO DE BLOCKCHAIN NA EDUCAÇÃO: ESTADO DA ARTE E DESAFIOS EM ABERTO

ESTADO DA ARTE

MORAIS, Anderson Melo de ¹

LINS, Fernando Antonio Aires ²

MORAIS, Anderson Melo de. LINS, Fernando Antonio Aires. **Uso de Blockchain na Educação: Estado da arte e desafios em aberto**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 05, Ed. 10, Vol. 22, pp. 78-100. Outubro de 2020. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/tecnologia/uso-de-blockchain>

RESUMO

A educação é uma das áreas mais importantes da sociedade e gera constantemente grandes quantidades de informação. Gerenciar essas informações, e assegurar o seu armazenamento com segurança, disponibilidade e imutabilidade, é um desafio relevante. Considerando esse contexto, muitas soluções tecnológicas foram propostas nos últimos anos, incluindo aplicações baseadas em Blockchain. O uso de Blockchain voltado para a informática na educação pode garantir segurança e confiabilidade por meio da descentralização de dados. Este artigo apresenta uma revisão de literatura contendo as principais pesquisas relacionadas ao uso do Blockchain em instituições de ensino. Entre as principais possibilidades de aplicação está o registro de diplomas e certificados, garantindo a sua autenticidade e evitando falsificações. Também é possível registrar outros documentos importantes, como históricos escolares. O uso de contratos inteligentes em ambientes acadêmicos e o

¹ Mestrando em Informática Aplicada, bacharel em Ciência da Computação.

² Orientador. Doutor em Ciência da Computação, mestre em Ciência da Computação, bacharel em Engenharia da Computação.



registro de conhecimentos na Blockchain também são tópicos de pesquisa relevantes. Por fim, este artigo apresenta e discute os atuais desafios em aberto a serem resolvidos na área.

Palavras-Chave: Blockchain, informática na educação, segurança, privacidade.

1. INTRODUÇÃO

No contexto atual, novas tecnologias têm surgido para facilitar a maneira como as pessoas se relacionam. Adicionalmente, grandes quantidades de informações educacionais são geradas pelas instituições de ensino. No entanto, em meio a tantas inovações surgem também novos desafios relacionados à segurança e privacidade dos dados, confiabilidade, imutabilidade de registro, dentre outros. Diante disso, surge a necessidade de se investir em tecnologias e metodologias que assegurem a integridade dos dados educacionais.

Os avanços científicos decorrentes da indústria 4.0 vêm trazendo como resultado progressos para os diversos setores da sociedade, dentre eles a educação (NGUYEN e DANG, 2018). Um dos conceitos tecnológicos emergentes é o de Blockchain, que tem potencial para revolucionar a maneira como a informática é utilizada na educação, pois tal tecnologia visa conferir mais segurança e confiabilidade aos processos educacionais (WATTERS, 2016).

O conceito de Blockchain foi apresentado ao mundo em 2008 e tinha como principal propósito dar suporte à criação da criptomoeda Bitcoin (NAKAMOTO, 2008). Naquele ano, muitos países viviam uma severa crise financeira, a qual ocasionou instabilidades econômicas e enfraqueceu a economia mundial. Em meio a este cenário, a rede Blockchain surgiu com a proposta de levar as transações financeiras para o meio digital e tornar possível a sua execução de forma descentralizada, sem a necessidade do intermédio de bancos ou instituições reguladoras.

A Blockchain é constituída por bases de dados distribuídas e criptografadas, onde as mesmas visam garantir um alto nível de segurança através da descentralização dos



dados (CHICARINO *et al.*, 2017). Todas as transações que ocorrem entre os usuários são agrupadas em blocos e estes, por sua vez, são distribuídos entre os computadores conectados à rede. Quando um novo bloco é gerado e validado, ele é adicionado à cadeia e todos os demais são atualizados para receberem os novos dados. O registro dos blocos ocorre de forma encadeada, onde cada um guarda uma referência para o seu anterior, o que impossibilita que novos dados sejam inseridos ou modificados sem que isso altere o encadeamento de todos os demais blocos da cadeia.

Devido ao alto nível de segurança observado no uso da Blockchain, surgiram então várias propostas de aplicação da tecnologia em outras áreas. Dentre estas áreas está o uso da informática na educação. Atualmente, muitos problemas são enfrentados por instituições de ensino, como por exemplo o gerenciamento da vida escolar dos alunos e a ocorrência de falsificação de diplomas e certificados. O aluno, por sua vez, ao necessitar mudar de instituição, ou mesmo de curso, passa por inúmeros processos burocráticos para a realização de uma nova matrícula. Além disso, ao tentar ingressar no mercado de trabalho, o aluno necessita apresentar comprovações da formação recebida e das competências adquiridas, o que nem sempre se mostra uma tarefa simples (HARTHY; SHUHAIMI e ISMAILY, 2019).

Neste contexto, estão surgindo várias propostas para o uso de Blockchain em ambientes educacionais com o intuito de solucionar diversas problemáticas relacionadas a Informática na Educação. Desta forma, este trabalho tem como objetivo fazer um levantamento do atual estado da arte da utilização de Blockchain em contextos educacionais, assim como identificar os desafios científicos ainda existentes nesta área.

Este artigo está organizado de acordo com as seções a seguir. A Seção II apresenta os conceitos básicos fundamentais para o entendimento deste artigo. A Seção III descreve a metodologia utilizada para a realização deste trabalho. A Seção IV apresenta as principais pesquisas relacionadas a Blockchain em contextos educacionais existentes atualmente. A Seção V apresenta os desafios de pesquisa



que se encontram em abertos na área deste artigo. Por fim, a Seção VI apresenta as conclusões do trabalho e indica os trabalhos futuros.

2. CONCEITOS BÁSICOS

Esta seção apresenta os principais conceitos e terminologias necessárias para a compreensão deste trabalho.

2.1 BLOCKCHAIN

A rede Blockchain busca garantir segurança através da descentralização dos dados. São bases de dados distribuídas, criptografadas e compartilhadas que armazenam informações sobre todas as transações que ocorrem entre os usuários da rede (CHICARINO *et al.*, 2017). Todos os nós da rede devem conter as mesmas informações; desta forma, quando um novo bloco é inserido, todos os nós são atualizados para receber as novas informações e desta forma voltarem a conter o mesmo conteúdo.

Os blocos são estruturas que armazenam as informações contidas na rede e são organizados em cadeia (WATTERS, 2016). Cada bloco guarda uma referência para o seu anterior; desta forma, é possível percorrer toda a cadeia até chegar ao bloco zero, também chamado bloco gênese. Tal bloco é codificado pelo software no momento em que a rede é criada e serve como o estado inicial do sistema, guardando informações sobre como a rede deve se comportar durante o seu funcionamento. Devido ao encadeamento dos blocos, não é possível que um deles seja alterado sem que isso seja percebido pelos demais da rede. Para realizar uma alteração seria necessário gerar novamente todos os blocos posteriores da cadeia, o que em uma rede de grandes proporções se tornaria inviável do ponto de vista computacional.

Cada bloco é composto por duas partes principais: o cabeçalho, onde são guardadas as informações de identificação do bloco como o *hash[i]* do bloco anterior e o *nonce*, e as transações, que consistem no agrupamento dos dados que estão armazenados no bloco.

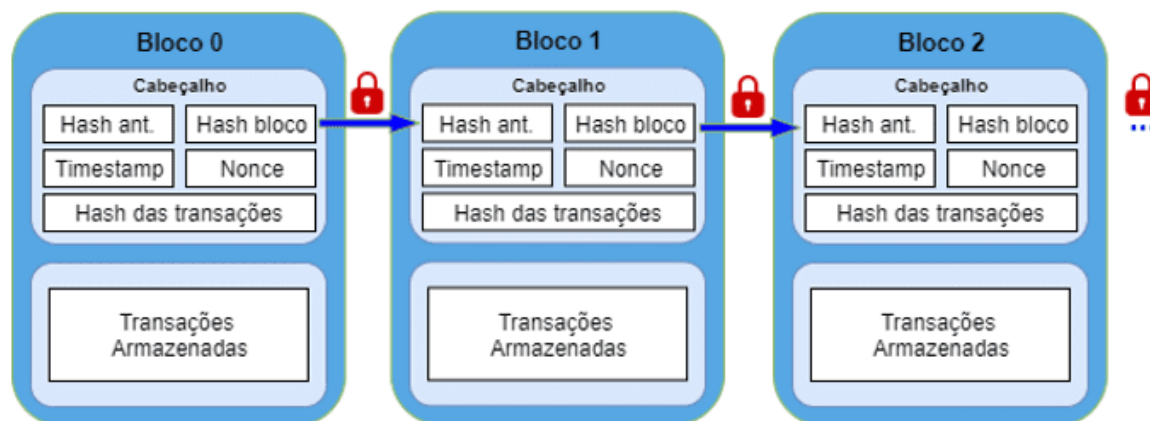


A seguir são destacados outros conceitos importantes na área de Blockchain (CHICARINO *et al.*, 2017):

- **Transações.** São o conjunto de dados que estão armazenados em cada bloco. Quando um nó recebe uma nova transação, ele a reenvia aos demais para que toda a rede contenha o mesmo conteúdo. Após um novo bloco ser validado e incluído na cadeia, as transações nele contidas se tornam públicas e inalteráveis.
- **Hash do cabeçalho.** É um número que tem a função de identificar o bloco dentro da cadeia. Após todas as transações terem sido validadas e incluídas no bloco, o *hash* do cabeçalho é gerado. Este dado é incluído no bloco posterior para garantir o encadeamento dos blocos.
- **Hash do bloco anterior.** No cabeçalho de cada bloco é armazenado o *hash* de identificação do bloco anterior; isto permite o encadeamento sucessivo dos blocos. Desta forma, é possível percorrer toda a cadeia até alcançar o bloco gênese que, por sua vez, possui o campo *hash* do bloco anterior preenchido com zero por inexistir blocos anteriores a ele.
- **Nonce.** Consiste em uma variável usada para alterar o resultado gerado pelo cabeçalho. É utilizado para provar que um bloco foi validado e que atende aos critérios estabelecidos pela rede.
- **Altura do bloco.** Os blocos são incluídos na cadeia de forma sequencial. A diferença entre a posição de um bloco e o bloco gênese da cadeia é denominada altura do bloco.
- **Timestamp.** Junto a cada bloco é armazenado o momento em que ele foi gerado. Este registro se dá através de um número que representa a data e a hora exata da criação do mesmo.

A Figura 1 apresenta uma visão geral da estrutura dos blocos e dos principais campos contidos neles. No retângulo superior de cada bloco está representado o seu cabeçalho, com os campos descritos anteriormente, e no retângulo inferior as transações que o bloco armazena.

Figura 1 - Estruturas dos blocos da Blockchain



Fonte: Autoria própria

2.2 SMART CONTRACTS

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.

O conceito de *Smart Contracts* surgiu na década de 90, antes mesmo da existência das criptomoedas e das Blockchains, com o propósito de utilizar softwares para executar contratos (SZABO, 1994). Os contratos inteligentes recebem como entrada uma série de condições que permanecem sendo constantemente monitoradas e ao serem satisfeitas o contrato se auto executa. Todo o processo é automatizado e pode se dar de maneira totalmente virtual ou mista, como um complemento a contratos feitos no papel. A segurança da transação é garantida pela Blockchain.

O funcionamento dos *Smart Contracts* é dividido em três etapas (TEIXEIRA e TAVARES, 2018), as quais são apresentadas abaixo:

- **Codificação.** Inicialmente é realizada a codificação do contrato em alguma linguagem de programação. No código são definidas com exatidão as



instruções que o contrato deve executar e que devem estar de acordo com o interesse das partes.

- **Envio à Blockchain.** Após a codificação, o código é criptografado e enviado para outros computadores por meio da Blockchain. Isto ocorre de forma semelhante ao que é realizado nas transações das criptomoedas.
- **Execução.** A Blockchain recebe o código e o processa em um de seus nós. Em seguida a rede atualiza os registros para que todos os nós contenham os resultados do processamento dos contratos. O contrato passa então a ser monitorado pela rede.

Smart Contracts oferecem um alto nível de confiabilidade e segurança, pois não há como controlar a execução do código, já que ela se dá de maneira distribuída e descentralizada. Também não é possível alterar os resultados da execução, porque os dados estão gravados de forma imutável nos blocos da Blockchain.

3. METODOLOGIA

Esta seção descreve a metodologia utilizada para a realização deste trabalho. O levantamento bibliográfico do estado da arte é realizado através de um mapeamento sistemático da literatura, que tem como objetivo detectar evidências sobre o problema, identificar as principais fontes de informação a partir de conceitos-chave da área de pesquisa e descobrir lacunas e oportunidades de pesquisa na área (ARKSEY, 2005).

Para a realização do mapeamento foram definidos os critérios da pesquisa, mediante a elaboração de um protocolo. Informações essenciais deste protocolo se encontram apresentadas a seguir.

- **Questão de pesquisa:** como garantir integridade, autenticidade e imutabilidade aos dados e documentos acadêmicos?
- **Bases científicas consultadas:** IEEE Xplore Digital Library; Springer Link; ACM Digital Library; Scielo; Google Scholar;
- **Palavras chave:** "Blockchain", "education", "data security";



- **Crítérios de inclusão:** artigos publicados após 2015 e que apresentam conteúdo relacionado a questão de pesquisa;
- **Crítérios de exclusão:** trabalhos publicados antes de 2015 ou que apresentem conteúdo não relacionado ao tema de pesquisa;
- **Strings de busca:** "Blockchain AND Education", "data security AND education", "Blockchain AND Education AND data security";

4. MAPEAMENTO SISTEMÁTICO SOBRE O USO DE BLOCKCHAIN NA ÁREA DE EDUCAÇÃO

Esta seção descreve as principais iniciativas de pesquisa relacionadas ao uso de Blockchain para a Informática na Educação. O estudo foi dividido em quatro áreas principais: registro e validação de diplomas, registro de documentos acadêmicos, uso de *Smart Contracts* por instituições de ensino e registro de conhecimento em Blockchain.

4.1 USO DE BLOCKCHAIN PARA REGISTRO E VALIDAÇÃO DE DIPLOMAS

Uma das principais discussões sobre a utilidade de Blockchain para a educação recai sobre o registro de diplomas. O diploma é considerado um dos documentos mais importantes emitidos pelas instituições de ensino (GRECH e CAMILLERI, 2017). O diploma serve como um documento comprobatório da formação recebida pelo aluno e lhe confere a autorização necessária para exercer a sua profissão.

Atualmente há uma busca crescente por curso na modalidade de Educação a Distância (EAD), para que tais cursos possam ser ofertados se faz necessário uma ampla utilização de recursos de Informática na Educação (PAULA *et al.*, 2018). Todo o processo da EAD se dá através de ambientes virtuais de aprendizagem (AVA), inclusive a disponibilização do diploma do aluno ao final do curso. Contudo, existem diversos casos de falsificação de diplomas e isso pode comprometer a credibilidade de instituições de ensino e até mesmo pôr a vida de pessoas em risco, ao inserir profissionais não qualificados no mercado. Neste contexto, é necessária a



implementação de mecanismos de segurança mais robustos para conferir uma maior confiabilidade ao processo de emissão e validação de diplomas (GALLARDO; BAZAN e VENOSA, 2019).

Segundo Harthy; Shuhaimi e Ismaily (2019) é possível utilizar Blockchain para assegurar uma melhor segurança à emissão de diplomas, garantido que eles possam ser validados por qualquer interessado, a qualquer hora. Os autores apresentam quatro recomendações, que segundo eles, devem ser consideradas de forma geral ao utilizar Blockchain em instituições de ensino:

- **Definir as condições para execução da Blockchain.** É necessário que os nós sejam executados em máquinas que garantam um adequado poder de processamento à aplicação.
- **Definir qual método criptográfico será utilizado.** Deve-se conhecer o algoritmo que realizará o cálculo do *hash* dos blocos. O mais utilizado é o SHA256, que transforma um grande número de informações em uma sequência numérica hexadecimal de tamanho fixo.
- **Definir as regras de utilização de *Smart Contracts*.** Caso a aplicação faça uso de *Smart Contract*, é necessário definir suas regras de implementação e execução com clareza.
- **Rastreamento das transações.** É preciso garantir a rastreabilidade de todas as transações que ocorreram na rede e de todos os nós que foram minerados. Contudo, o trabalho não apresenta implementações ilustrando a viabilidade de uso de Blockchain, o que reduz o entendimento sobre como esta solução poderia ser usada na prática.

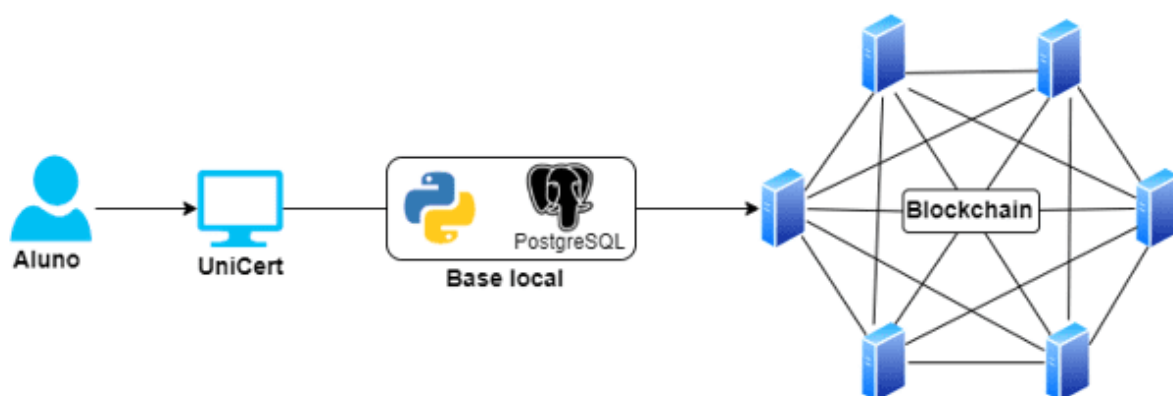
Para Kolvenbach; Ruland e Grather (2018) é possível desenvolver uma plataforma baseada em Blockchain para controlar a emissão e validação de diplomas e certificados devido ao alto nível de segurança apresentado pela rede. O trabalho menciona ferramentas baseadas em Blockchain já existentes voltadas para este propósito: a Blockcerts (MIT, 2016), desenvolvida pelo MIT, e a TrueRec (BOESER, 2017), criada pelo grupo SAP.

Os autores descrevem ainda a criação de uma nova plataforma, baseada em Ethereum, onde os diplomas podem ser registrados através de *Smart Contracts*. A instituição de ensino registra os dados do aluno no contrato. Estes dados, por sua vez, serão validados por outras entidades de certificação. Após este processo, o diploma ou certificado poderá ser emitido e gravado na Blockchain, sendo possível a sua consulta por qualquer interessado, como empregadores ou outras instituições de ensino.

Uma proposta semelhante é apresentada por Huynh *et al.* (2018), onde os autores abordam a possibilidade de uso de Blockchain para a emissão e validação de certificados digitais visando garantir segurança e evitar falsificações. É proposta a criação do UniCert (Figura 2), uma aplicação que irá receber os dados dos certificados, realizar o seu registo em um banco de dados local PostgreSQL e envia o *hash* do documento para os nós da rede Blockchain.

Esta proposta apresenta um nível de segurança ainda maior em relação a outras propostas de uso de Blockchain, pois o registro é realizado em múltiplos níveis, na base de dados local e na Blockchain, o que torna ainda mais difícil a possibilidade de sucesso de ataques aos dados.

Figura 2 - Visão geral do funcionamento da Unicert.



Fonte: Autoria própria



Kanan; Obaidat e Al-Lahham (2019) descrevem a modelagem e implementação do SmartCert, um sistema para emissão e validação de certificados, que realiza o registro dos mesmos em uma Blockchain Ethereum. A aplicação foi desenvolvida na Universidade de *Al-Zaytoonah* na Jordânia utilizando dados reais dos estudantes.

Após o planejamento e definição dos requisitos, o SmartCert foi implementado tendo dois módulos principais: um que permite a universidade realizar a inserção dos dados do aluno e de seus respectivos cursos e outro que permite ao estudante consultar os seus certificados. No entanto, os autores não apresentam testes de segurança e disponibilidade, que seriam importantes para assegurar a o nível de segurança da aplicação.

Arenas e Fernandez (2018) apresenta o CredenceLedger, uma aplicação para verificação de credenciais acadêmicas. Ela realiza o acesso a uma rede Blockchain Ethereum, onde estarão armazenadas diversas informações sobre a trajetórias acadêmicas do aluno. Ao finalizar o curso, o estudante recebe uma cópia dos seus dados acadêmicos e o seu histórico em uma versão impressa e outra digital, autenticada pela plataforma. Futuramente, terceiros interessados poderão verificar a autenticidade destes documentos através da Blockchain.

4.2 USO DE BLOCKCHAIN PARA GARANTIA DE AUTENTICIDADE, INTEGRIDADE E IMUTABILIDADE DE DOCUMENTOS ACADÊMICOS

Além dos diplomas e certificados abordados na seção anterior, existem vários outros documentos acadêmicos que precisam ser emitidos e armazenados com segurança. Tais documentos servem, por exemplo, como prova da formação recebida pelo aluno e de sua trajetória acadêmica. Exemplos destes documentos incluem provas, históricos, dentre outros. Segurança é importante neste contexto porque, por exemplo, informações como notas em disciplinas cursadas podem ser alvo de adulterações para se aumentar as chances de contratação em um determinado emprego.

Srivastava *et al.* (2018) sugerem a criação de uma plataforma para registro de dados baseada em Blockchain que registra, através de *tokens*, todos os créditos adquiridos



pelo estudante ao longo da sua trajetória acadêmica. Cada universidade integrante do sistema possui um nó na Blockchain e é responsável por gerar credenciais de identificação dos seus alunos mediante a verificação de autenticidade dos seus documentos pessoais.

Cada aluno possui a sua carteira digital, onde são registrados os *tokens* referentes a cada curso concluído na instituição. Isto permite ao aluno comprovar de maneira confiável a formação recebida, e reduzirá os procedimentos burocráticos existentes caso o mesmo necessite mudar de instituição de ensino, pois os dados poderão ser consultados na própria Blockchain. O trabalho descreve a implementação da Blockchain utilizada no projeto e apresenta os principais algoritmos desenvolvidos. Estes algoritmos têm como propósito cadastrar o aluno, cadastrar a instituição de ensino, realizar o consenso da rede, dentre outras funções.

Atualmente grande parte dos documentos acadêmicos são impressos em papel e armazenados em arquivos físicos. As bases de dados digitais existentes são, em sua maioria, centralizadas e de acesso restrito. Ao se transferir para uma nova escola o aluno precisa refazer todo o seu cadastro, não havendo facilidade para se reutilizar os dados da instituição anterior. Diante disso, Bore *et al.* (2017), em seu trabalho, tratam da falta de bases de dados educacionais completas, acessíveis e atualizadas. Isso dificulta a análise de dados e as tomadas de decisão pelos gestores das instituições e pelo governo.

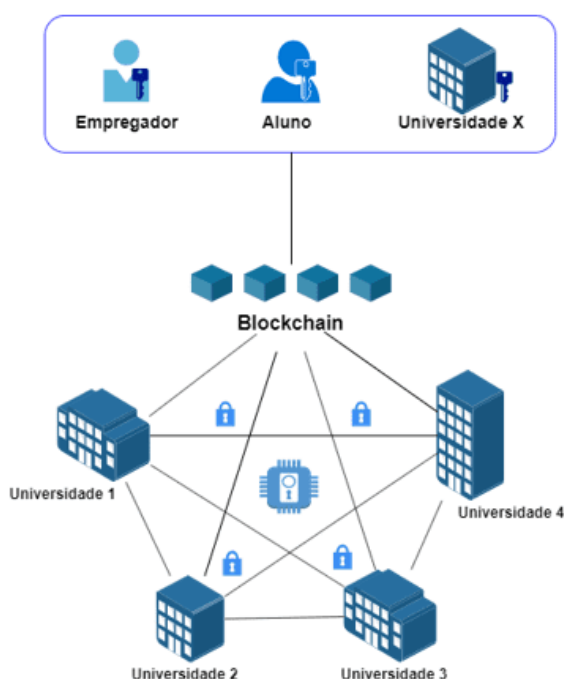
O trabalho proposto por Bore *et al.* (2017) apresenta o projeto, implementação e avaliação de um Hub de Informações Escolares integrado a uma Blockchain com o objetivo de descentralizar os dados e os manter seguros e acessíveis. Na proposta, todas as atividades e ocorrências escolares seriam registradas na forma de transações na Blockchain. Exemplos de transações incluem: cadastro de novos alunos, matrícula ou rematrícula em disciplinas, atualização da identidade do usuário, registro de frequência do aluno, etc.

Os autores apresentam um protótipo de implementação utilizando a rede Hyperledger Fabric[i], onde é possível realizar o cadastro de alunos e professores, gerar

identificadores (*hashs*) de documentos digitais e os inserir na rede. Por fim, os autores realizam um estudo de caso em uma escola do Quênia, utilizando dados reais de estudantes e professores.

Uma outra proposta inovadora é a plataforma EduCTX, apresentada por Holbl *et al.* (2018), que permite atribuir e gerenciar credenciais de indivíduos e instituições de ensino, bem como outras potenciais partes interessadas, como empresas. Uma visão geral desta plataforma é ilustrada na Figura 3. Na plataforma são registrados *tokens* que comprovam as capacidades de indivíduos, quais cursos o indivíduo já realizou, onde estudou, quais experiências profissionais possuem, dentre outras informações. Todas estas informações podem ser consultadas por possíveis interessados, como empresas empregadoras ou instituições de ensino, o que inclusive ajuda a evitar falsificações de documentos. De acordo com os autores, a plataforma encontra-se em fase de implementação, sendo desenvolvida para a rede Ethereum. A plataforma faz uso de Smart Contracts para realizar o registro das informações dos indivíduos e das transações ocorridas na rede.

Figura 3 - Visão geral da plataforma EduCTX.



Fonte: Autoria própria

RC: 63856

Disponível em: <https://www.nucleodoconhecimento.com.br/tecnologia/uso-de-blockchain>



Turknovic *et al.* (2018), em seu trabalho, também fazem referência a EduCTX. De acordo com os autores, trata-se de uma plataforma de crédito estudantil global baseada em Blockchain que visa evitar barreiras linguísticas e administrativas na hora de reconhecer a formação acadêmica de estudantes. Nela o estudante tem a vantagem de manter todo o seu histórico sempre acessível. De acordo com os autores, a Universidade Nacional de La Plata (2020) e a Faculdade CESYT (AMATI, 2015) da Argentina já utilizam outras soluções baseadas em Blockchain para registro de dados acadêmicos e emissão de diplomas. Na plataforma EduCTX, cada universidade é um nó na Blockchain, e armazena uma cópia da base de dados. Desta forma, as informações permanecem continuamente disponíveis para consulta por alunos, empregadores ou outras instituições de ensino interessadas mediante o uso de uma chave de acesso que funciona como identificador.

Em outra pesquisa relevante na área, Mikroyannidis *et al.* (2019) propõem a utilização de Blockchain para auxiliar pesquisadores da área de ciência de dados. Em seu trabalho é descrita a criação de uma base de registro de alunos, onde são armazenadas as suas habilidades, cursos e conquistas profissionais.

De acordo com os autores, a principal finalidade da plataforma é garantir a veracidade do histórico de formação do aluno e evitar falsificações. O sistema realiza recomendações de novos cursos de acordo com as áreas de interesse do estudante. A plataforma serve ainda como um sistema de recomendações de empregos, tomando como base as qualificações do aluno, recomendando as vagas que lhes são mais indicadas. De acordo com os autores a aplicação, que faz uso da rede Ethereum, se encontra em fase de prototipação e ainda não faz uso de dados reais de estudantes.

Duan; Zhong e Liu (2018), por sua vez, propõem o uso de Blockchain para registrar toda a trajetória educacional dos alunos, tendo como base o modelo de Educação Baseada em Resultados, onde os estudantes são avaliados de acordo com as metas atingidas e a qualidade das atividades realizadas. É realizada a implementação de uma versão inicial da aplicação, onde são registrados dados sobre as turmas, número de alunos, cursos, indicadores de desempenho, graus de desempenho e outras



informações. Contudo, não são apresentados detalhes sobre a Blockchain utilizada no projeto.

De acordo com Bai *et al.* (2019) é possível ocorrer problemas como falsificações de documentos e adulterações de informações em documentos de projetos de pesquisa. Os autores propõem a criação de uma solução baseada em Blockchain para o gerenciamento e registro de todas as etapas de projetos de pesquisas. Nesta solução, cada agente envolvido na pesquisa possui um nó na Blockchain. Exemplos de agente incluem a agência financiadora, os pesquisadores, os auditores financeiros, dentre outros. Assim, todas as atividades desenvolvidas são registradas na Blockchain, passando pela validação do nó da agência financiadora. Dessa forma, descentralizando os dados, torna-se possível assegurar a sua imutabilidade e preservação. O trabalho se mostra interessante e promissor, contudo descreve apenas a modelagem da aplicação, não apresentando detalhes específicos acerca da sua implementação.

4.3 UTILIZANDO *SMART CONTRACTS* EM AMBIENTES ACADÊMICOS

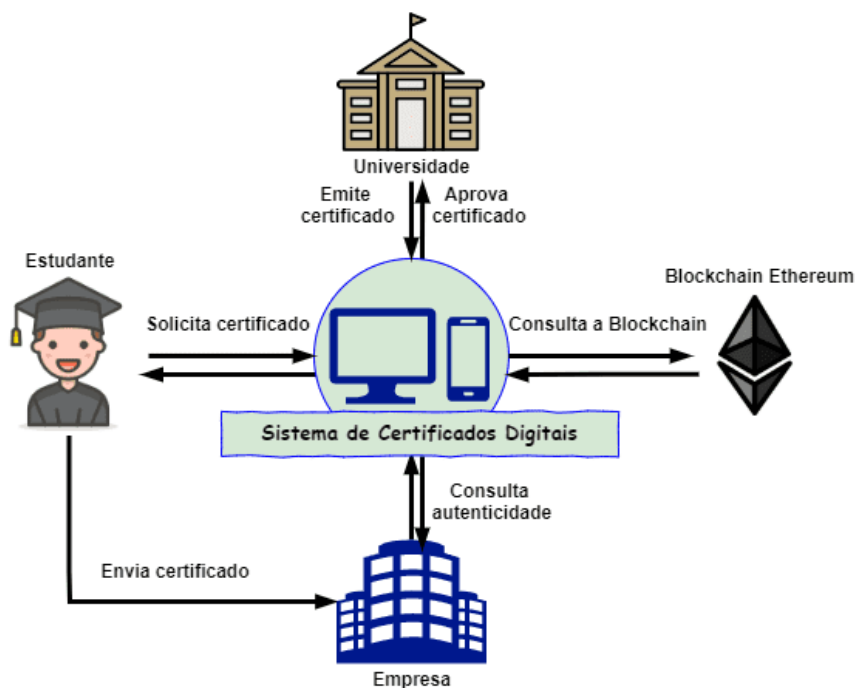
Cheng *et al.* (2018) propõem o uso de *Smart Contracts* registrados em Blockchain para a emissão e validação de diplomas. No contrato serão definidas as condições necessárias para a conclusão do curso, o prazo disponível e outras informações. Quando o aluno cumprir todas as especificações, o contrato se auto executa e o diploma poderá ser emitido.

O trabalho descreve a modelagem e implementação de um sistema desenvolvido para a plataforma Ethereum utilizando a linguagem Solidity. O trabalho apresenta também um exemplo de geração de um certificado e o seu registro na rede Ethereum mediante a criação de um *Smart Contract* contendo as suas informações. O sistema proporciona economia de papel, reduz custos de gerenciamento, evita a falsificação de documentos e fornece informações precisas e confiáveis sobre os certificados digitais emitidos.

A Figura 4 apresenta o fluxo de emissão de um certificado digital através da plataforma. A universidade tem a função de inserir os dados do estudante no sistema e também de realizar a validação dos certificados emitidos. O aluno pode realizar a solicitação do seu certificado através da plataforma. Uma vez que o arquivo é gerado, o seu *hash* é calculado e registrado na Blockchain, ficando o seu número impresso em uma etiqueta que será afixada na versão impressa do documento, caso esta seja solicitada pelo aluno. Desta forma, o sistema não apenas aumenta a credibilidade dos certificados que são emitidos em papel como também reduz eletronicamente os riscos de perda ou dano destes documentos.

De posse do seu certificado, o aluno poderá enviá-lo a outras entidades, como empresas empregadoras, que poderão, por sua vez, consultar a autenticidade das informações descritas no documento.

Figura 4 - Fluxo de emissão de um certificado digital utilizando Blockchain Ethereum



Fonte: Autoria própria

Ocheja; Flanagan e Ogata (2018) propõe a criação de um sistema de avaliação de aprendizagem baseado em Blockchain. A aplicação proposta realiza o acesso as



bases de dados dos alunos, reúne suas principais informações (ex.: notas, avaliações, dados comportamentais, etc.) e organiza tais informações na forma de *Smart Contracts*, que serão enviadas a rede Blockchain Ethereum. Tais contratos se auto executarão na medida em que o aluno progride no curso, garantindo assim o registro de todas as suas atividades e interações na cadeia de blocos. Tudo isso permite uma maior interoperabilidade entre as bases de dados educacionais, garantindo o registro de dados de forma imutável e fará com que o acesso às informações ocorra de forma segura.

Também é possível a utilização de *Smart Contracts* para a realização de pagamentos. Rooksby e Dimitrov (2017) propõe a criação de uma plataforma baseada em Blockchain Ethereum para utilização em ambientes universitários. Esta proposta permite o registro de alunos e de suas respectivas notas nos cursos. Na plataforma também existe uma criptomoeda, chamada Kelvin Coin, que o estudante recebe como recompensa mediante o bom desempenho nas atividades acadêmicas. Com a moeda o aluno poderá pagar por seus novos cursos mediante a execução de *Smart Contracts*.

Em outro trabalho de pesquisa, Gilda e Mehrotra (2018) afirma ser possível utilizar *Smart Contracts* para gravar as informações de consentimento dos envolvidos em uma pesquisa e permitir que essas informações sejam monitoradas com facilidade e transparência e possam ser revogadas caso necessário.

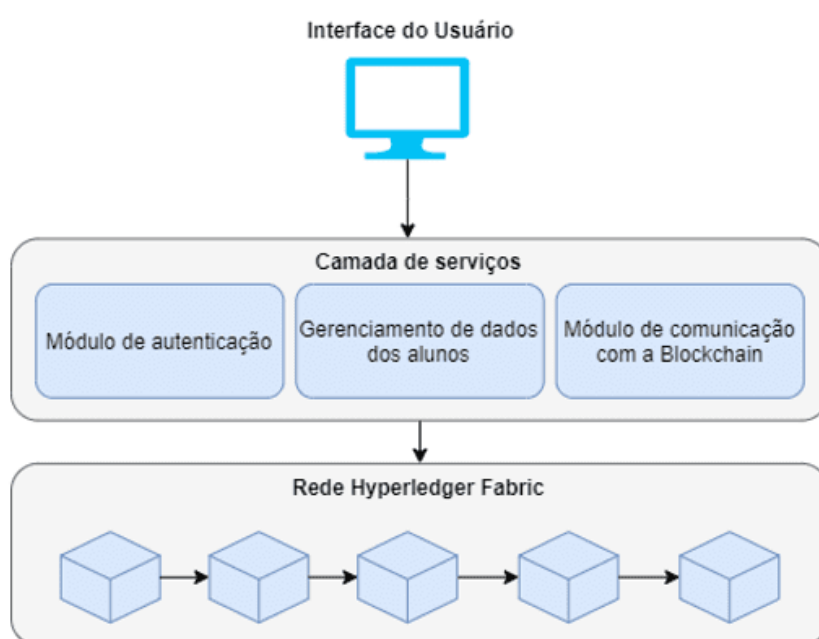
Os autores descrevem a modelagem de um sistema, implementado na plataforma Hyperledger Fabric, para a criação e gravação destes registros na Blockchain. Os dados dos estudantes são adquiridos por meio de voluntários, que se reúnem pessoalmente com eles e, através do preenchimento de formulários, obtêm as informações. Em seguida, são registrados na Blockchain, permitindo assim o seu acesso por todos os envolvidos na pesquisa mediante a utilização de suas credenciais de acesso.

4.4 REGISTRANDO CONHECIMENTO EM BLOCKCHAIN

Liu *et al.* (2018) sugere o uso de Blockchain para o registro de informações geradas pelos estudantes, através da criação de uma plataforma distribuída que trará transparência, segurança e integridade aos dados. O trabalho apresenta a modelagem da solução fazendo uso da plataforma Hyperledger Fabric.

O protótipo do sistema utiliza dois nós de Hyperledger e serve para registrar as diferentes informações relacionadas a cada aluno, suas notas, histórico escolar, atividades desenvolvidas, dentre outras informações. São armazenadas informações não apenas da instituição de ensino atual onde o aluno se encontra, mas também de todos os demais lugares por onde ele passou, devido a interoperabilidade permitida pela Blockchain. A Figura 5 apresenta a arquitetura da aplicação e suas diferentes camadas. O sistema possui diversos módulos com finalidades específicas, como autenticação, gerenciamento dos dados dos alunos, acesso aos nós da Blockchain, dentre outros.

Figura 5 - Visão geral da proposta descrita por Liu et al (2018)



Fonte: Autoria própria



Sharples (2016), por sua vez, propõe um sistema de reputação acadêmica, fazendo uso de uma Blockchain privada baseada em Ethereum. Nesta Blockchain os alunos recebem uma moeda virtual chamada Kudos como prova dos créditos, trabalhos desenvolvidos ou conquistas obtidas. Os Kudos podem ser negociados, vendidos e trocados dentro das instituições de ensino. Tal sistema de reputação apresenta benefícios para as instituições, como por exemplo, fornece um registro seguro, acessível e distribuído da escolaridade dos alunos. Através da utilização de uma Blockchain educacional, os indivíduos e instituições poderão armazenar registros públicos de realizações pessoais de forma confiável e facilmente verificável.

Em seu trabalho, Zhong *et al.* (2018) apresentam a modelagem de uma plataforma que serve para registrar os alunos e armazenar as informações de todas as suas atividades acadêmico/escolares. O sistema possui mecanismos de recompensa que premiam o aluno, em criptomoedas, pelas conquistas alcançadas. Essas moedas podem ser usadas para compra de materiais de estudo, o que ajuda inclusive a evitar plágio e proteger a propriedade intelectual dos proprietários.

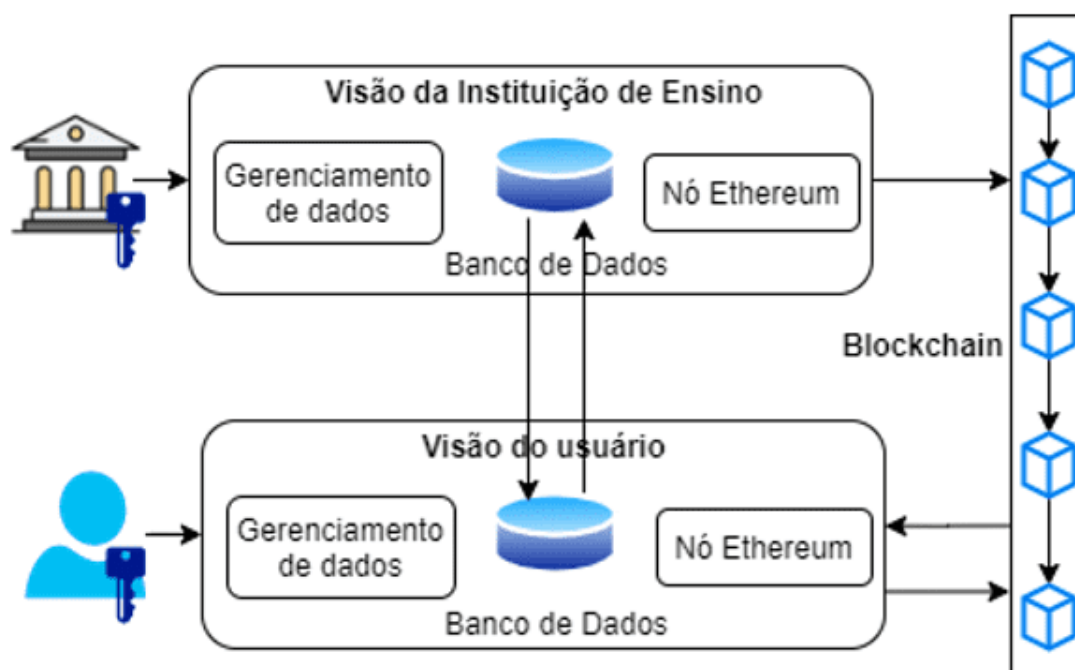
A plataforma é desenvolvida em NodeJs e realiza o registro dos dados em um banco de dados MongoDB, a partir de onde são enviados à Blockchain. A cadeia de blocos permanece sendo constantemente monitorada, assim é feito o acompanhamento do progresso de aprendizagem do aluno até que este chegue ao término do curso e o seu certificado possa ser gerado.

Coelho e Brandão (2019) busca solucionar problemas que existem em bases de registro de pesquisa científica, como por exemplo falsificações, adulterações e plágios. O trabalho propõe a criação de uma solução baseada em Blockchain para o gerenciamento e registro de todas as etapas dos projetos de pesquisas, especialmente as publicações. Nela, os autores podem submeter os seus trabalhos de forma gratuita, e com a garantia de autenticidade fornecida pela Blockchain. Os revisores receberão os trabalhos e os avaliarão, de forma anônima e descentralizada. Por se tratar de um sistema descentralizado, não poderão ocorrer monopólios ou qualquer outra forma de controle por grupos de indivíduos com interesses especiais.

A aplicação proposta recompensa os autores e revisores dos periódicos com um *token* digital que eventualmente pode ser trocado por criptomoedas.

Han *et al.* (2018) propõem a criação de uma plataforma baseada em Ethereum que permite a instituição de ensino registrar todos os seus alunos e suas trajetórias acadêmicas, assim como o conhecimento produzido por cada indivíduo. Esta plataforma viabiliza também o registro de diplomas e certificados, que poderão ser validados sempre que necessário, por qualquer interessado, seja outra instituição de ensino ou empregadores. A Figura 6 apresenta a arquitetura da aplicação. Na parte superior está representado o módulo de visão da instituição, onde é possível realizar a inserção e atualização dos dados dos estudantes, que serão gravados na rede Ethereum. Na parte inferior da figura, encontra-se o módulo do usuário, onde é possível acessar os dados.

Figura 6 - Representação do funcionamento da aplicação



Fonte: Autoria própria



5. DESAFIOS DE PESQUISA EM ABERTO

Após a avaliação dos trabalhos apresentados na seção anterior, foi possível identificar pontos que ainda precisam ser melhor aprofundados pela comunidade científica. São eles:

- **Avaliação da melhor arquitetura a ser usada para Blockchains com fins educacionais.** Ao optar por uma solução de Blockchain pública tem-se acesso a uma rede verdadeiramente descentralizada, onde todos os nós, além de armazenarem uma cópia da cadeia de blocos, podem também atuarem como mineradores, realizando a validação dos novos nós. Em uma rede privada, tem-se a presença de um órgão regulamentador, seja uma pessoa ou um grupo, o que torna a rede centralizada ou permissionada. Para participar da rede é necessário obter um convite ou autorização, e cumprir todas as regras, condições e políticas definidas pelo órgão regulador. Todos estes fatores devem ser avaliados quando da escolha de uma Blockchain ou Privada, e um estudo mais aprofundado sobre esta temática se faz necessário considerando as peculiaridades da área da Informática na Educação;
- **Avaliação de desempenho de Blockchains com fins educacionais.** Caso a instituição de ensino opte por implementar uma rede Blockchain local, dentro da infraestrutura do campus, é necessário avaliar se essa nova camada de segurança irá ocasionar alterações significativas no desempenho da rede e do sistema educacional em si. Também é importante analisar se o nível de segurança apresentado por tal aplicação será satisfatório. Faz-se necessária a realização de uma avaliação de segurança, levando em consideração todas as variantes envolvidas;
- **Integração a sistemas legados.** É preciso avaliar maneiras de integrar as redes Blockchain aos sistemas legados e bases de dados já existentes e em uso nas universidades e instituições de ensino. Atualmente a maioria das instituições já fazem uso de plataformas de registro, onde são armazenados os dados dos alunos. No entanto, integrar tais sistemas com uma rede Blockchain



pode ser um desafio devido a diversidade de tecnologias utilizadas em cada caso;

- **Ferramentas de suporte à integração de Blockchains com ferramentas da área de Informática na Educação.** Atualmente, os avanços da Informática na Educação são muito relevantes e vêm sendo amplamente adotados pela comunidade. O uso de tecnologias de suporte ao Ensino a Distância (como Ambientes Virtuais de Aprendizagem e ferramentas de videoconferência) se tornam cada vez mais frequentes. Neste contexto, existe o desejo que determinados requisitos de segurança sejam garantidos. Por exemplo, como verificar se uma atividade realmente foi entregue pelo aluno? Ou como garantir que os alunos em um vídeo chamada são efetivamente eles? Para isso, a integração destas ferramentas da Informática na Educação com Blockchain se mostra muito útil pois aumentará a confiabilidade das interações entre alunos e professores. No entanto, tal integração se mostra como um problema pertinente, pois demandará a integração de múltiplos tipos de tecnologias e bases de dados diferentes.

6. CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho teve como objetivo reunir os principais trabalhos científicos relacionados ao uso de Blockchain no contexto da Informática na Educação e avaliar o estado da arte desta área. Foram identificadas quatro principais aplicações de Blockchain na educação: registro e validação de diplomas, registro de documentos acadêmicos, utilização de *Smart Contracts* por instituições de ensino e registro de conhecimento.

No registro de diplomas faz-se necessário garantir a sua autenticidade e permitir que ela seja verificada sempre que necessário. Também é possível realizar o registro de outros documentos educacionais em Blockchain, como o histórico do aluno, provas e atividades, para assegurar dessa forma que estes dados permaneçam sempre acessíveis e acompanhem o estudante durante toda a sua vida. Através dos *Smart Contracts* é possível a realização de acordos entre alunos e professores, ou ainda a realização de pagamentos à instituição pelos cursos ofertados, tudo isso de forma automática e descentralizada através da Blockchain. É possível também registrar uma



série de outros conhecimentos em Blockchain, integrando-o às bases de dados e sistemas já existentes; desta forma, o aluno possa ter todas as suas informações registradas de forma segura e acessíveis sempre que se fizer necessário.

Através deste trabalho foi possível também encontrar e tornar disponível desafios atuais de pesquisa na área. Esses desafios precisarão ser melhor abordados para que o uso de Blockchain em Informática na Educação possa ter maior sucesso. Como trabalhos futuros pretende-se avaliar qual a melhor arquitetura de Blockchain a ser utilizada em ambiente educacionais. Outra linha de trabalho futuro busca propor soluções integradoras para a interconexão entre Blockchain a sistemas legados; para isto, serão pesquisados os sistemas acadêmicos mais utilizados atualmente e serão propostos módulos de integração específicos para cada um destes sistemas.

REFERÊNCIAS

AMATI, F. First official career diplomas on bitcoin's Blockchain. Disponível em: <<https://blog.signatura.co/first-official-career-diplomas-on-bitcoin-s-blockchain-69311acb544d>>. Acesso em: 21/07/2020.

ARENAS, R.; FERNANDEZ, P. CredenceLedger: a permissioned blockchain for verifiable academic credentials. In **2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)** (pp. 1-6). IEEE. 2018.

ARKSEY, H.; O'MALLEY, L. (2005). Scoping studies: towards a methodological framework. *International journal of social research methodology*, 8(1), 19-32. Disponível em: <<https://core.ac.uk/download/pdf/56237.pdf>>. Acesso em: 15/03/2020.

BAI, Y. et al. Researchchain: union blockchain based scientific research project management system. In **2018 Chinese Automation Congress (CAC)** (pp. 4206-4209). IEEE. 2018.

BOESER B. (2017) Meet truered by sap: Trusted digital credentials powered by blockchain. Disponível em: <<https://news.sap.com/2017/07/meet-truered-by-sap-trusted-digital-credentials-powered-by-blockchain>>. Acesso em: 11/03/2020.



BORE, N. et al. Towards blockchain-enabled school information hub. In **Proceedings of the Ninth International Conference on Information and Communication Technologies and Development** (pp. 1-4). 2017.

CHENG, J. C. et al. Blockchain and smart contract for digital certificate. In **2018 IEEE international conference on applied system invention (ICASI)** (pp. 1046-1051). IEEE. 2018.

CHICARINO, V. R. et al. Uso de Blockchain para privacidade e segurança em internet das coisas. **Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. Brasília: SBC, 28. 2017.

COELHO, F. C.; BRANDÃO, A. Decentralising scientific publishing: can the Blockchain improve science communication?. **Memórias do Instituto Oswaldo Cruz**, vol. 114, no. July, pp. 1–4, 2019.

DUAN, B.; ZHONG, Y.; LIU, D. Education application of Blockchain technology: Learning outcome and meta-diploma. In **2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)** (pp. 814-817). IEEE. 2017.

GALLARDO, I.; BAZAN, P.; VENOSA, P. Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada. **RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação**, (32), 49-66. 2019.

GILDA, S.; MEHROTRA, M. Blockchain for Student Data Privacy and Consent. In **2018 International Conference on Computer Communication and Informatics (ICCCI)** (pp. 1-5). IEEE. 2018.

GRECH A.; CAMILLERI A. F. **Blockchain in Education** – European Commission, 2017. Disponível em: <<https://ec.europa.eu/jrc/en/publication/>>. Acesso 19/02/2020.

HAN, M. et al. A novel Blockchain-based education records verification solution. In **Proceedings of the 19th Annual SIG Conference on Information Technology Education** (pp. 178-183). 2018.



HARTHY, K. A.; SHUHAIMI, F. A.; ISMAILY, K. K. J. The upcoming Blockchain adoption in Higher education: requirements and process. In **2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)** (pp. 1-5). IEEE. 2019.

HÖLBL, M., et al. EduCTX: an ecosystem for managing digital micro-credentials. In **2018 28th EAEEIE Annual Conference (EAEEIE)** (pp. 1-9). IEEE. 2018.

HUYNH, T. T. et al. Issuing and Verifying Digital Certificates with Blockchain. In **2018 International Conference on Advanced Technologies for Communications (ATC)** (pp. 332-336). IEEE. 2018.

KANAN, T.; OBAIDAT, A. T.; AL-LAHHAM, M. SmartCert BlockChain Imperative for Educational Certificates. In **2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)** (pp. 629-633). IEEE. 2019.

KOLVENBACH, S., et al. Blockchain 4 education. In **Proceedings of 16th European Conference on Computer-Supported Cooperative Work-Panels, Posters and Demos**. European Society for Socially Embedded Technologies (EUSSET). 2018.

LIU, Q., et al. Education-Industry Cooperative System Based on Blockchain. In **2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)** (pp. 207-211). IEEE. 2018.

MIKROYANNIDIS, A. et al. Smart Blockchain badges for data science education. In **2018 IEEE Frontiers in Education Conference (FIE)** (pp. 1-5). IEEE. 2018.

MIT Initiative (2016). *Digital certificates project*. [Online]. Available: <http://certificates.media.mit.edu/>

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. **Journal for general Philosophy of Science**, vol. 39, no. 1, pp. 53–67, 2008. doi:10.1007/s10838-008-9062-0. 2008;



NGUYEN, Q. K.; DANG, Q. V. Blockchain Technology for the Advancement of the Future. In 2018 **4th International Conference on Green Technology and Sustainable Development** (GTSD) (pp. 483-486). IEEE. 2018.

OCHEJA, P.; FLANAGAN, B.; OGATA, H. Connecting decentralized learning records: a blockchain based learning analytics platform. In **Proceedings of the 8th international conference on learning analytics and knowledge** (pp. 265-269). 2018.

PAULA, M. T. D.; et al. Desafios na implementação de cursos a distância no ensino superior. In **I CONEFEA-Tecnologia, Pesquisa e Desafios na Educação Brasileira**. 2018.

ROOKSBY, J.; DIMITROV, K. Trustless education? A blockchain system for university grades. **Ubiquity: The Journal of Pervasive Media**, 6(1), 83-88. 2019.

SHARPLES M. Adaptive and Adaptable Learning, vol. 9891, no. September, 2016. Disponível em: <<http://link.springer.com/10.1007/978-3-319-45153-4>>. Acesso em 04 jun. 2020.

SRIVASTAVA, A., et al. A distributed credit transfer educational framework based on blockchain. In 2018 **Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T)** (pp. 54-59). IEEE. 2018.

TEIXEIRA L. F.; TAVARES J. F. C, Blockchain: Dos conceitos as possíveis aplicações, pp. 4–10, mar 2018. Disponível em: <<https://www.researchgate.net/publication/327161498>>. Acesso em: 14/05/2020.

Turkanović, M., et al. EduCTX: A blockchain-based higher education credit platform. **IEEE access**, 6, 5112-5127. 2018.

UNIVERSIDAD NACIONAL DE LA PLATA. Disponível em: <<https://unlp.edu.ar/>>. Acesso em: 11/04/2020



WATTERS A. Blockchain for Education: A Research Project, **Hack Education**, pp. 2016–2017, 2016. Disponível em: <<https://medium.com/@audreywatters/blockchain-for-education-a-research-project-a09fd4338622>>. Acesso em 19/12/2019.

WATTERS A. The Blockchain for Education: An Introduction, **Hack Education**, pp. 1–12, 2016. Disponível em: <<http://hackeducation.com/2016/04/07/blockchain-education-guide>>. Acesso em 19/12/2019.

ZHONG, J et al. A Blockchain Model for Word-Learning Systems. In 2018 **5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC)** (pp. 130-131). IEEE. 2018.

APÊNDICE - REFERÊNCIAS DE NOTA DE RODAPÉ

i. Cadeias de caracteres que servem como identificadores de dados que se encontram armazenados em um determinado local. O bloco gênese possui o campo hash do bloco anterior preenchido com zero, por inexistir blocos anteriores a ele.

ii. Trata-se de um projeto colaborativo desenvolvido em parceria com várias indústrias, iniciado em dezembro de 2015 pela Linux Foundation. Tem como principal objetivo desenvolver a tecnologia de registro distribuído Blockchain em múltiplos segmentos da indústria.

Enviado: Outubro, 2020.

Aprovado: Outubro, 2020.