

Um framework para interoperabilidade de instituições heterogêneas de ensino utilizando Blockchain

Rodrigo Pennella Cardoso¹, Denise Goya²

¹Programa de Pós-Graduação em Ciência da Computação, ²Centro de Matemática, Computação e Cognição
Universidade Federal do ABC (UFABC)
Caixa Postal 09210-580 Av. dos Estados, 5001 - Bangú, Santo André – SP - Brazil

rodrigo.pennella@aluno.ufabc.edu.br, denise.goya@ufabc.edu.br

Abstract:

O Blockchain é uma tecnologia que tem recebido grande atenção recentemente devido às suas características principais, como a descentralização, a persistência, a auditabilidade com alta proteção contra adulterações, mesmo trabalhando com redes *peer-to-peer* em nós não confiáveis. Estas peculiaridades a tornam uma importante ferramenta para ser utilizada para a interoperabilidade de instituições heterogêneas de ensino. Neste trabalho são apresentadas as características que sustentam o uso do Blockchain nesse contexto e é definido um modelo para a interoperabilidade de instituições heterogêneas de ensino, baseado no Blockchain do Ethereum.

1. Introdução

Criado em 2008, o Bitcoin é uma criptomoeda que surgiu como alternativa aos meios de pagamentos eletrônicos tradicionais, eliminando a necessidade da figura de um banco como entidade central responsável por realizar e manter os registros de todas as transações financeiras, permitindo trocas irreversíveis diretamente entre duas pessoas [Nakamoto 2008].

O triunfo do Bitcoin se dá principalmente devido à tecnologia desenvolvida para ser seu livro-razão. Conhecida como Blockchain, essa tecnologia permite a criação de um banco de dados descentralizado, robusto e encadeado [Buterin et al. 2014], o que proporciona a operação do Bitcoin com integridade, autenticidade e disponibilidade, ainda que seus dados estejam distribuídos em nós que não possuem confiança entre si.

O Blockchain mantém seus registros de maneira sequencial, encadeada e partilhada em todos os nós da rede *peer-to-peer*, de tal forma que a alteração de uma transferência já processada só possa ser feita com a alteração dos registros subsequentes no mesmo momento em mais da metade dos nós da rede [Armstrong 2016], o que mantém seus registros auditáveis e não suscetíveis a alterações. Essas características permitem que o Blockchain possa ser utilizado em outros contextos além das criptomoedas.

2. Motivação

A interoperabilização de registros de ensino é uma das áreas que podem obter grandes avanços através do uso do Blockchain. O modelo atual de certificação de cursos por certificados impressos possui diversas limitações e problemas. Um certificado impresso, mesmo com as mais sofisticadas técnicas de impressão, é passivo de falsificações. [Ezell and Bear 2005] discutem sobre o mercado bilionário por trás da falsificação e adulteração de certificados educacionais por todo o mundo.

Além do evidente problema com falsificações, os certificados impressos possuem a limitação quanto a dificuldade que uma empresa tem em verificar a autenticidade da informação. Atualmente, confirmar as informações contidas em um certificado é uma tarefa manual, distinta para cada instituição e que pode ser em muitos casos demorada e custosa.

Adicionalmente, tem-se o problema de manter os registros por um período de tempo longo e indeterminado já que a qualquer momento pode ser necessária a confirmação de algum certificado emitido. Ademais, manter esses registros

é uma tarefa custosa e que pode resultar na adulteração de informações com problemas de segurança ou mesmo com a perda da possibilidade de confirmação da autenticidade com o fechamento da instituição de ensino.

Por fim, as informações contidas em um certificado impresso no geral são muito restritas, resumindo-se a uma titulação, data e identificação dos envolvidos, o que torna demasiadamente vago quais são exatamente os conhecimentos que estão sendo comprovados, uma vez que, mesmo cursos com o mesmo título podem possuir características diferentes dependendo da instituição de ensino.

3. Considerações Preliminares

Algumas plataformas como a *BlockCerts* e *Blockchain for Education* conseguem resolver parcialmente os problemas citados anteriormente através da modelagem de plataformas distribuídas em Blockchain, trazendo melhorias na forma de consulta e validação em relação ao modelo atual, contudo, o conteúdo da certificação continua sendo o tradicional, contendo apenas informações básicas e vagas sobre o título obtido naquela instituição [Media Lab Learning Initiative 2017] [Gräther et al. 2018].

Para solucionar de maneira mais abrangente, propomos um framework baseado na tecnologia Blockchain que seja capaz não somente de armazenar diplomas, mas também, de armazenar de maneira online e confiável, a comprovação de cada um dos conhecimentos específicos adquiridos pelo aluno, ou seja, suas novas competências, de forma a permitir que empresas e instituições de ensino possam tirar melhor proveito dessas informações.

Para atingir o objetivo citado, será realizada uma modelagem de dados visando a padronização das informações de conhecimento, levando em conta os aspectos mais importantes de cada tipo de curso.

A interoperabilidade das informações proporcionará benefícios a todos os envolvidos no processo, sendo eles:

Instituições de ensino: com as informações salvas no Blockchain, as instituições de ensino não terão de se preocupar com infraestruturas para armazenamento das informações, além de automatizarem o processo de atendimento a terceiros que desejam confirmar a autenticidade, tornando-o online. Pretende-se com esse novo modelo, reduzir os custos com infraestrutura e aumentar a segurança das informações.

Alunos: os alunos poderão acompanhar e utilizar as informações de forma rápida e prática, usando os dados dos conhecimentos adquiridos de forma a solicitar equivalências de cursos ou disciplinas, ou mesmo facilitar a candidatura em vagas de emprego com pré-requisitos.

Empresas e Recrutadores: os recrutadores terão maior facilidade em confirmar a veracidade das informações dos candidatos, além de poderem filtrar aqueles que possuem comprovadamente os pré-requisitos solicitados para a vaga. Também será possível comparar detalhadamente a formação de cada candidato, não apenas levando em conta a instituição de ensino e o curso concluído, mas sim, os conhecimentos e habilidades adquiridos.

4. Objetivos

O objetivo principal deste trabalho consiste na proposição e criação de um modelo para a interoperabilidade de instituições de ensino através da tecnologia descentralizadora do Blockchain. O objetivo secundário é superar limitações que a tecnologia do Blockchain atualmente enfrenta, especificamente com relação a seu uso como plataforma de interoperabilidade de instituições heterogêneas, e modelagem de um framework abrangendo instituições de ensino, pessoas e empresas interessadas na confirmação de informações registradas.

5. Arquitetura Proposta

O escopo da Arquitetura do framework engloba a interoperabilização não apenas dos diplomas emitidos por cada instituição de ensino, mas sim das competências e conhecimentos específicos obtidos por cada discente, permitindo que empresas e instituições de ensino tenham acesso detalhado a cada uma das habilidades de um indivíduo.

A arquitetura proposta considera como necessidades fundamentais:

- Armazenamento seguro, com garantia de disponibilidade e escalabilidade.
- Possibilidade de revogação das informações por órgãos reguladores e instituições de ensino.
- Acesso a dados privados apenas a pessoas autorizadas.
- Inclusão de informações com garantia de autenticidade do emissor dos dados.
- Compartilhamento das informações com terceiros autorizados.

5.1. Atores

A arquitetura conta com 4 atores fundamentais: órgãos reguladores, instituições de ensino, alunos e recrutadores, sendo suas funções discriminadas abaixo.

Instituições de Ensino: as instituições de ensino possuem um papel fundamental no contexto do framework, sendo a principal responsável pela inclusão das informações inseridas na base de dados. As funcionalidades para esse grupo de usuário englobam: inserção de conhecimentos adquiridos pelos alunos da instituição, além de consulta e revogação dos certificados.

Alunos: são responsáveis por criar perfis de acesso, criando links de acesso agrupando determinados certificados.

Recrutadores: exemplo de classe usuária da plataforma para visualização de informações e verificação de autenticidade das mesmas.

Órgãos Reguladores: são responsáveis por regular atuação das instituições de ensino e emissões de certificados.

5.2. Camadas

A arquitetura é dividida em 4 camadas, sendo elas: Dados, Aplicação, Integração e Usuários. A imagem da Figura 1, ilustra de maneira simplificada as camadas e suas relações na arquitetura proposta.

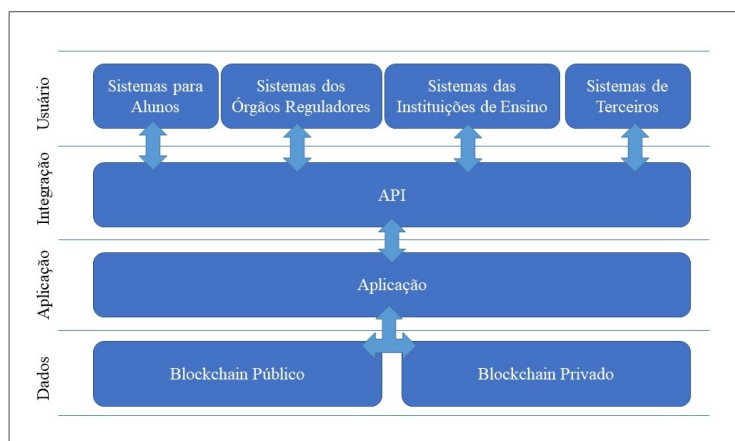


Figura 1. Diagrama de Camadas da Arquitetura

A camada de dados, consiste no conjunto de ferramentas utilizadas para armazenar e consultar as informações de todo o sistema. Devido ao grande volume de dados que podem ser inseridos e a questão da privacidade das informações, a arquitetura proposta baseia-se na utilização de não apenas um Blockchain público para armazenamento, mas sim, na utilização conjunta de dois Blockchains, um público e outro privado.

O Blockchain privado é formado por todas as instituições de ensino, que funcionam como um nó da rede Blockchain em execução. Por ser uma rede privada, tanto a participação como um nó quanto o acesso aos dados acontece de maneira restrita, cabendo aos órgãos reguladores controlarem esse acesso. Nesse Blockchain todas as informações dos certificados emitidos e revogados pelas instituições são armazenados e ficam disponíveis para consulta pelos órgãos reguladores e pelas instituições de ensino, bem como todos os detalhes previstos para cada certificado.

Já no Blockchain público, as instituições de ensino atuam como usuários, e utilizam-se do Blockchain em execução de forma a registrar imediatamente após a emissão do certificado, o valor Hash calculado com base nas informações salvas, de forma a garantir a verificação posterior, atuando como uma forma pública de segurança de todas as informações salvas. Dessa forma, qualquer indivíduo de posse de um certificado pode facilmente verificar sua autenticidade de forma online realizando uma consulta ao Blockchain público.

A camada de aplicação é composta pelos componentes lógicos, que são formados pelo conjunto de classes e métodos que controlam todas as operações realizadas na camada de dados.

A camada de integração é constituída por uma API (*Application Programming Interface*) que funciona de forma a prover um conjunto de métodos que tem por objetivo prover o acesso aos dados de maneira simplificada, sem a necessidade de um amplo conhecimento na plataforma ou sua arquitetura. Essa camada é responsável por permitir a integração com sistemas externos, como por exemplo: sistemas de empresas de recrutação, aplicações que desejam realizar a conferência de certificados recebidos de forma automática, sistemas próprios das instituições de ensino, entre outros.

Por fim, a camada de usuário, é constituída pelas aplicações desenvolvidas para interagir diretamente com o usuário, sendo uma forma de acesso intuitiva às funções providas pelas camadas inferiores, permitindo a execução de funções como: emissão de certificados, consultas e revogações.

Ademais, planeja-se implementar uma aplicação com o intuito de testar o modelo proposto e identificar possíveis melhorias futuras a serem adicionadas ao modelo.

6. Conclusão

O Blockchain tem se mostrado uma importante alternativa às tecnologias tradicionais utilizadas em interoperabilidade de informações, impulsionada pelos ganhos em segurança, disponibilidade e até mesmo custos operacionais em relação as estruturas tradicionais de armazenamento.

Em se tratando especificamente de informações de conhecimentos, a utilização do Blockchain pode trazer benefícios a todos os envolvidos, garantindo um maior nível de segurança contra fraudes, maior agilidade na emissão, verificação e revogação dos certificados, além de permitir o compartilhamento das informações de forma detalhada e com a possibilidade de verificação de sua autenticidade de forma online.

Neste trabalho, foi apresentado um modelo conceitual baseado em Blockchain que possibilita que instituições de ensino que atuam em diferentes ramos e níveis de conhecimento possam compartilhar registros em uma plataforma descentralizada, preservando aspectos de sigilo, integridade e autenticidade que instituições, estudantes e órgãos reguladores exigem.

Durante o desenvolvimento do modelo, observou-se que, apesar dos avanços, muitas barreiras técnicas devem ser superadas para sua ampla utilização. Entre os principais desafios, a necessidade de padronização das informações compartilhadas se mostrou essencial para a evolução de sua utilização, de forma a garantir não apenas o acesso as informações de forma rápida e segura, mas também sua interoperabilização entre as mais diversas instituições de ensino por todo o país. Além da padronização das informações, é essencial que se defina também uma arquitetura e implementação a ser utilizada por todas as instituições, de forma a assegurar que todas as informações sejam armazenadas e acessadas por todos de maneira unificada.

Por fim, existem também barreiras operacionais, como a necessidade de adaptação de todas as instituições de ensino para a utilização de uma plataforma única global, o que implica em investimentos em adaptações dos sistemas já existentes.

Referências

- Armstrong, S. (2016). Move over bitcoin, the blockchain is only just getting started. Acessado em: 10 de Março de 2018.
- Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *white paper*. Acessado em: 30 de Março de 2018.
- Ezell, A. and Bear, J. (2005). *Degree mills: The billion-dollar industry that has sold over a million fake diplomas*. Pyr Books.
- Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., and Wendland, F. (2018). Blockchain for education: Lifelong learning passport. In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET).
- Media Lab Learning Initiative, L. M. (2017). Digital certificates project.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.