Escola Nacional de Administração Pública

Programa Cátedras do Brasil

Modalidade Inovação

RELATÓRIO FINAL

CARTEIRA DE CURSOS BASEADA EM TECNOLOGIA BLOCKCHAIN

ROGERIO ATEM DE CARVALHO[1]

Maio de 2019

[1] Este relatório foi elaborado com a direta colaboração de Jean Felippe Dias de Melo (Egresso do SAEG/IFF), que também colaborou no desenvolvimento do software do projeto, com apoio de Galba Arueira (Bolsista Egresso do PICG/IFF) e Helber Cisilio (DTI/IFF).

SUMÁRIO

1. INTRODUÇÃO

1.1. Contextualização

O mundo, hoje, é demasiadamente competitivo e ágil, estando tanto as empresas como os próprios profissionais que nelas atuam ávidos por conhecimento, aprimoramento pessoal e incremento curricular. Uma forma de especialização dos profissionais é através de cursos oferecidos por instituições de ensino, algumas vezes patrocinados pela própria empresa empregadora, mas muitas vezes procurados pelos próprios profissionais que desejam algum tipo de especialização (DUARTE, 2003).

Segundo Børresen et al (2018), a dificuldade de validação de documentos causa uma grande brecha para o mercado de falsificações, o que permite maus profissionais tirarem proveito deste cenário, forjando estudos e formações inexistentes, criando três grandes categorias de documentos falsificados:

- A primeira categoria é o documento que parece ser emitido por uma instituição conhecida, mas ele é produzido ilegalmente, a pessoa que possui o diploma nunca concluiu o curso na instituição.
- Na segunda categoria se enquadram os documentos que realmente são emitidos pelas instituições, mas com informações alteradas.
- A terceira categoria são os documentos emitidos por instituições de fachada, onde nenhum estudo é realmente realizado.

Uma tecnologia se destaca como uma grande candidata à solução dos problemas apresentados, ela é conhecida como Blockchain. Segundo Tapscott et al (2016) Blockchain é um livro digital incorruptível de transações econômicas que pode ser programado para registrar não apenas transações financeiras, mas virtualmente tudo de valor. Apesar da sua primeira e mais conhecida aplicação ser no cenário de movimentações financeiras, o Blockchain pode ser usado em diferentes cenários para aumentar a segurança da informação, e uma dessas aplicação é na emissão de documentos digitais. (VILNER, 2018).

Tecnicamente, nas palavras de seu criador Satoshi Nakamoto (2008), que é um pseudônimo para uma pessoa ou um grupo de pessoas ou empresas (THE ECONOMIST, 2015), o Blockchain consiste em blocos de informação ligados uns aos outros através de *hashcodes* calculados através da *Proof of Work* (Prova de Trabalho)*,* esses *hashcodes* são baseados nas informações já existente no no próprio Blockchain, formando um registro que não pode ser alterado sem refazer a *Proof of Work*. Satoshi Nakamoto apresentou o conceito de Blockchain primeiramente aplicado à transações financeiras, que é a tecnologia que é conhecida hoje como Bitcoin (ACHESON, 2018).

Hooper (2018) cita algumas vantagens no uso do Blockchain para persistência de um registro de dados:

- Transparência: O registro de dados se torna mais transparente com o uso do Blockchain. Por ser um registro distribuído, todos os participantes da rede compartilham a mesma documentação. A versão compartilhada só pode ser atualizada através de um consenso, o que significa que todos os participantes precisam estar de acordo com a mudança. Para alterar uma única transação já persistida, é necessária atualizar todos os registros subsequentes.
- Segurança: O Blockchain*,* de várias formas, se mostra mais seguro que outros sistemas de armazenamento de dados. Quando uma transação é aprovada, ela é criptografada e anexada ao bloco, esse bloco é replicado e armazenado em todos os participantes da rede, tornando praticamente inviável que acessos maliciosos comprometam a integridade da informação.
- Rastreabilidade: Dada a natureza dos dados no Blockchain, a informação é altamente rastreável, sendo que nenhum dado é removido, o que facilita para cenários de auditoria.
- Eficiência e velocidade: Qualquer informação persistida no bloco é considerada verídica, o que torna o processo de validação tão rápido quanto o tempo de processamento de uma nova informação e persistência no Blockchain.
- Redução de custos: O Blockchain torna obsoleto o uso de intermediários para garantir a autenticidade da informação. Outro fator que influencia na redução de

custos é a replicação natural da informação, tornando o uso de uma estrutura de *backup* robusta desnecessária.

1.2. Objetivos

Como objetivo geral, este projeto teve desenvolver uma estrutura para emissão de certificados referentes a cursos oferecidos por instituições de ensino. O objetivo principal é desenvolver esta solução utilizando a tecnologia Blockchain, interligando instituições através de uma rede de comunicação.

Além do objetivo geral, o trabalho possui diferentes objetivos específicos, que são:

- Realizar levantamento sobre as implementações de Blockchain usadas atualmente no mercado.
- Definir a arquitetura do projeto.
- Implementar a solução em ambiente de teste no IFF e na ENAP.
- Possibilitar futuras extensões ao projeto, permitindo criação de novos módulos e de aplicações cliente, além do uso de informações coletadas para análise de dados e tomada de decisão.

1.3. Estrutura do Documento

Este documento se divide em cinco capítulos, enumerados a seguir:

- Após esta Introdução, o segundo capítulo mostra a revisão bibliográfica, com um levantamento do estudo no atual cenário tecnológico e acadêmico.
- No terceiro capítulo é feito um estudo sobre diferentes tecnologias para implementações de redes *Blockchain*, visando escolher a que mais se adequa à proposta deste trabalho.
- O capítulo quatro mostra detalhes do desenvolvimento e da solução, levantando quesitos técnicos e limitações da tecnologia usada.
- O quinto e último capítulo mostra o encerramento do trabalho, nele é feito um levantamento sobre as considerações finais, concluindo o desenvolvimento da

solução. Em seguida, são sugeridas maneiras de dar continuidade ao estudo, mostrando possibilidades de trabalhos futuros.

2. REVISÃO BIBLIOGRÁFICA

Blockchain é uma tecnologia descentralizada de gerenciamento de transações e dados desenvolvida primeiro para a criptomoeda Bitcoin, cujo interesse vem aumentando desde quando a ideia foi cunhada em 2008. A razão para o interesse na Blockchain é sua capacidade de fornecer segurança, anonimato e integridade de dados sem qualquer terceiro no controle das transações. As transações monetárias entre pessoas ou empresas são frequentemente centralizadas e controladas por terceiros. Fazer um pagamento digital ou transferência de moeda requer um banco ou provedor de cartão de crédito como intermediário para concluir a transação. Além disso, uma transação causa uma taxa de um banco ou de uma empresa de cartão de crédito. O mesmo processo também se aplica em vários outros domínios, como jogos, música, *software* etc. O sistema de transações e todos os dados e informações são controlados e gerenciados por uma organização terceirizada, em vez das duas principais entidades envolvidas na transação (YLI-HUUMO et al, 2016).

O objetivo da tecnologia Blockchain é criar um ambiente descentralizado onde nenhum terceiro esteja no controle das transações e dos dados. Cabe observar que no caso dos governos, embora haja distribuição de processamento e armazenamento entre os nós da rede, é possível que isso seja feito em uma rede privada controlada por um órgão governamental.

O Blockchain é uma solução de banco de dados distribuída que mantém uma lista crescente de registros de dados que são confirmados pelos nós participantes. Os dados são registrados em um registro público, incluindo informações de todas as transações já concluídas (YLI-HUUMO et al., op. Cit.). Alta integridade de transações e segurança, bem como a privacidade dos nós, são necessários para evitar ataques e tentativas de perturbar transações no Blockchain e adicionalmente, as transações distribuídas exigem poder computacional (SWAN, 2015). Prototipar soluções e testar sua segurança e escalabilidade colaboram no entendimento destas questões.

Atualmente, a Bitcoin, criptomoeda mais conhecida, é também a aplicação mais comum de Blockchain (COINMARKETCAP, 2016), e o número de transferências nesta moeda cresce constantemente (KONDOR et al., 2014). O Bitcoin usa o mecanismo de infra-estrutura de chave

pública (*Public Key Infrastructure*, PKI). Neste mecanismo, o usuário tem um par de chaves públicas e privadas. A chave pública é usada no endereço da carteira do usuário Bitcoin, e a chave privada é para a autenticação do usuário. A transação do Bitcoin consiste na chave pública do remetente, múltiplas chaves públicas do receptor e o valor transferido. Em cerca de dez minutos, a transação será gravada em um bloco. Este novo bloco é então vinculado a um bloco previamente escrito. Todos os blocos, incluindo informações sobre cada transação feita, são armazenados em disco dos usuários, chamados nós. Todos os nós armazenam informações sobre todas as transações gravadas da rede *Bitcoin* e verificam a exatidão de cada nova transação feita usando blocos anteriores. Os nós são recompensados, verificando a exatidão das transações. Este método é chamado de mineração, e é confirmado com *Proof of Work*, que é um dos os principais conceitos da tecnologia Blockchain. Quando todas as transações são confirmadas com sucesso, existe um consenso entre todos os nós. Os novos blocos estão ligados aos blocos anteriores e todos os blocos estão alinhados em uma cadeia contínua (HOUSLEY, 2004)

Para o entendimento da aplicação do Blockchain, o seu uso será analisado no cenário de implantação proposto por este estudo, uma explicação mais abstrata será usada, evidenciando somente pontos cruciais para esta implementação e omitindo detalhes não cruciais para o entendimento da tecnologia.

Dada uma transação, que neste cenário é a emissão de um certificado, um novo bloco é criado com os detalhes do certificado e um cabeçalho, esse cabeçalho possui o *hashcode* do bloco atual, do anterior e do próximo, formando uma lista encadeada e também possui um elemento chamado *Nonce*, que é utilizado na *Proof of Work*, e será detalhado na continuação deste texto.

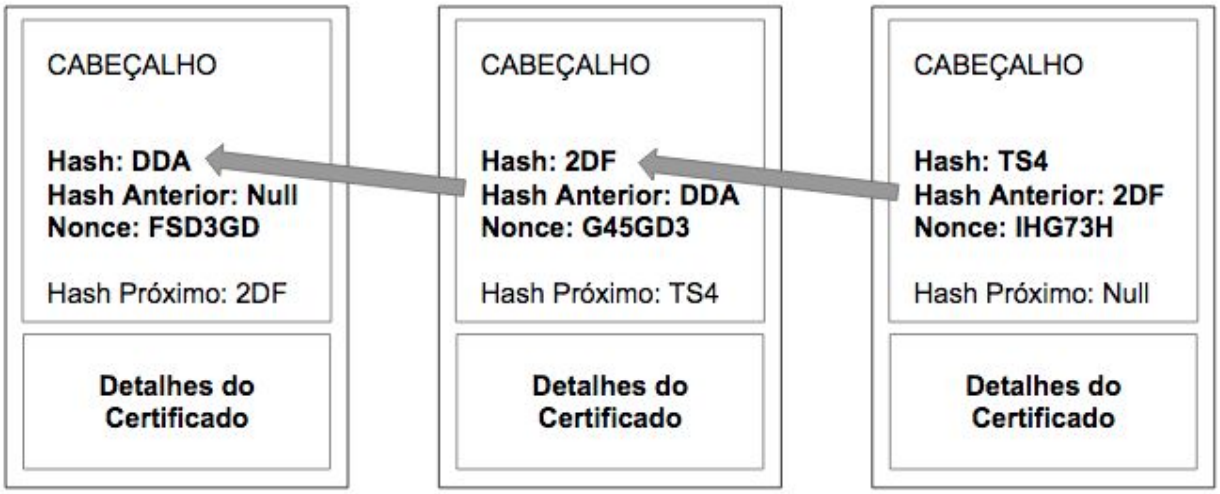

Figura 1 - Blocos do Blockchain. Fonte: (Elaboração Própria, 2018).

O *hashcode* do novo bloco a ser inserido no Blockchain é calculado baseado nos detalhes do certificado, e na informação do bloco anterior, porém, a proposta do Blockchain é que o cálculo desse novo *hashcode* exija um poder computacional grande para ser calculado, sendo que para alterar um bloco no meio da corrente seria preciso calcular o *hashcode* de todos os blocos subsequentes novamente, algo que se torna inviável dada a tecnologia de processamento atual dos computadores mais modernos.

Para melhor entendimento, será usado o seguinte cenário: o *hashcode* de cada bloco deve começar com uma sequência pré estabelecida de caracteres para ele ser incluído no Blockchain e esse *hashcode* é alterado modificando o conteúdo do bloco, neste caso o *Nonce*. Um cálculo em uma abordagem de tentativa e erro precisa ser feito até que o *Nonce* tenha uma valor que faça o *hashcode* do bloco atender ao pré-requisito. O trabalho computacional necessário para calcular o *Nonce* é que é chamado de *Proof of Work*.

A forma de validação de um novo bloco através da *Proof of Work* possui uma grande desvantagem, que é o desperdício de energia, pois um grande poder de processamento é exigido para o cálculo do *Nonce* e todo o trabalho efetuado pelos nós não vencedores é totalmente descartado. Uma forma alternativa à *Proof of Work* para validação de um novo bloco, é a *Proof of Stake*, que em um Blockchain que armazena registros de movimentação financeira, como o

Bitcoin, ao invés de cálculo de hashing, as próprias moedas são utilizadas para a validação (KHATWANI, 2018).

Em um Blockchain que faz uso do *Proof of Stake*, Khatwani (op. cit.) define o seguinte funcionamento: o validador do próximo bloco é determinado aleatoriamente, e para se tornar um validador, o participante precisa depositar uma quantidade de moedas que é chamada de *stake*, que funciona como um depósito caução. O tamanho do stake determinar a probabilidade do participante de ser escolhido como o validador do próximo bloco. Quando um participante é escolhido para validar o novo bloco, ele confere se todas as informações no bloco são válidas, em seguida adiciona o bloco ao Blockchain e recebe a recompensa da transação. Caso um validador valide uma transação fraudulenta, ele perderá parte do seu *stake* maior do que a quantia ganha como recompensa.

A vantagem do Blockchain é que o livro público não pode ser modificado ou excluído depois que os dados foram aprovados por todos os nós. É por isso que o Blockchain é bem conhecido por suas características de integridade e segurança de dados. A tecnologia Blockchain também pode ser aplicada a outros tipos de uso. Pode, por exemplo, criar um ambiente para contratos digitais e compartilhamento de dados peer-to-peer em um serviço de nuvem. O ponto forte da técnica Blockchain, integridade de dados, é a razão pela qual seu uso se estende também a outros serviços e aplicações, embora apresente alguns desafios (SWAN, op. Cit.):

- Taxa de transferência: O rendimento potencial de problemas na rede Bitcoin é atualmente maximizado para 7 transações por segundo. Outras redes de processamento de transações como a VISA e o Twitter apresentam 2.000 transações por segundo e o 5.000 transações por segundo respectivamente. Quando a frequência das transações no Blockchain aumenta para níveis semelhantes, a taxa de transferência da rede Blockchain precisa ser melhorada.
- Latência: Para criar segurança suficiente para um bloco de transação Bitcoin, é necessário cerca de 10 minutos para concluir uma transação. Para obter eficiência na segurança, é preciso gastar mais tempo em um bloco, porque ele tem que compensar o custo de ataques com gastos duplos. O gasto duplo é o resultado de gastos bem-sucedidos de dinheiro mais de uma vez. O Bitcoin protege contra o

gasto duplo, verificando cada transação adicionada à cadeia de blocos, para garantir que as entradas para a transação não tenham sido gastas anteriormente (BITCOIN, 2016a). Isso torna a latência um grande problema no Blockchain atualmente. Fazer um bloqueio e confirmar a transação deve acontecer em segundos, mantendo a segurança. Para concluir uma transação, por exemplo na VISA leva apenas alguns segundos, o que é uma enorme vantagem em relação ao Blockchain.

- Tamanho e largura de banda: No momento, o tamanho de um Blockchain na rede Bitcoin é de mais de 50.000 MB (MegaBytes) (fevereiro de 2016). Quando a taxa de transferência aumenta para os níveis da VISA, Blockchain pode crescer 214 PB (PetaBytes) em cada ano. A comunidade Bitcoin assume que o tamanho de um bloco é de 1 MB e um bloco é criado a cada dez minutos (BITCOIN, 2015). Portanto, há uma limitação no número de transações que podem ser manipuladas (em média 500 transações em um bloco) (ANTONOPOULOS, 2014). Se o Blockchain precisar controlar mais transações, os problemas de tamanho e largura de banda precisam ser resolvidos.
- Segurança: O Blockchain atual tem a possibilidade de um ataque de 51%. Em um ataque de 51%, uma única entidade teria controle total da maior parte da taxa de *hash* de mineração da rede e seria capaz de manipular o Blockchain. Para superar esse problema, mais pesquisas sobre segurança são necessárias.
- Recursos desperdiçados: a mineração de Bitcoins emprega enormes quantidades de energia. O gasto energético no Bitcoin é causado pelo esforço de *Proof of Work*. Existem algumas alternativas nos campos da indústria, como prova de participação. Com a *Proof of Work,* a probabilidade de mineração de um bloco depende do trabalho realizado pelo minerador. No entanto, na Prova de Aposta, o recurso que é comparado é a quantidade de Bitcoin que um minerador detém. Por exemplo, alguém que detenha 1% do Bitcoin pode extrair 1% dos “blocos de prova de aposta” (BITCOIN, 2016b). A questão com recursos despendidos precisa ser resolvida para ter uma mineração mais eficiente no Blockchain.

- Versionamento, *hard forks* e cadeias múltiplas: uma pequena cadeia que consiste em um pequeno número de nós tem uma maior possibilidade de um ataque de 51%. Outro problema surge quando as cadeias são divididas para fins administrativos ou de versão.

Ponto importante a considerar em aplicações Blockchain é se a rede formada deve ser pública ou privada. Segundo a ComputerWorld (2018), no Blockchain público todos podem ler e enviar transações ou participar do processo de consenso no Blockchain, pois não é requerida permissão. Todas as transações são públicas e os usuários podem permanecer anônimos. Já os privados são controlados por uma única organização que determina quem pode ler e enviar transações e participar do processo de consenso. Ainda segunda a ComputerWorld (op. cit.) há ainda outros dois tipos de redes de Blockchain. O consórcio de Blockchain, que é controlado por um grupo predefinido e onde o direito de ler e enviar transações para o Blockchain pode ser público ou restrito aos participantes. Os consórcios de Blockchain são considerados "com permissão" e são os mais indicados para a maioria das empresas. Já os Blockchains semi privados são administrados por uma única organização que concede acesso a qualquer usuário que atenda aos critérios preestabelecidos. Embora não seja realmente descentralizado, este tipo de Blockchain com permissão é mais interessante para casos de uso de B2B (Business to Business) e aplicações governamentais. A principal diferença entre público e privado é o mecanismo de consenso. No público, os usuários não se conhecem, portanto o nível de confiança é baixo, necessitando uma sobrecarga computacional maior. Assim, a validação de cada transação é bastante demorada. Já na conexão privada, a confiança é maior, pois é baseada na permissão de acesso. Assim, é possível fazer uso de algoritmos compartilhados mais simples e rápidos como alternativa aos previamente demonstrados *Proof of Work* e *Proof of Stake*, resultando, em vez de algumas, milhares de transações por segundo. Além disso, em *Blockchains* privados, os registros das transações podem ser criptografados e estão disponíveis apenas para as partes autorizadas, o que, por sua vez, ajuda a satisfazer os requisitos de privacidade dos participantes.

O modelo de consórcio parece ser o mais adequado para o estudo de caso, onde diferentes instituições participariam do Blockchain, compartilhando certificados, o que diminuiria o volume de processamento na autenticação de transações, sem porém impedir o acesso de leitura aos registros, posto que existem soluções para tanto, como por exemplo, a proposta por Júnior et al. (2018).

Em relação à temática específica deste projeto, a ideia de empregar Blockchain para emitir diplomas já vem sendo implantada há algum tempo por instituições no Brasil e no exterior. Uma das primeiras iniciativas foi a do MIT (Massachusetts Institute of Technology), como relata Sá (2017), que já em Outubro de 2017 emitiu seus primeiros diplomas empregando a técnica. Várias instituições a seguiram no mundo como a Escola de Finanças e Administração de Frankfurt, na Alemanha, Universidade de Cagliari na Itália, e a Impacta no Brasil. Neste ponto, Cardoso e Goya (2018) identificam os problemas dos certificados de cursos impressos:

- Falsificação, que envolve um mercado bilionário mundial;
- Confirmação manual das informações contidas no certificado;
- Custos de Manutenção dos registros por tempo às vezes indeterminado, que pode ainda gerar adulterações nas informações durante este armazenamento, bem como acessos indevidos à informação;
- Limitação das informações contidas em um certificado a um conjunto restrito de metadados.

Cardoso e Goya (op. cit.) propõem um modelo conceitual de framework onde as instituições de ensino mantém os registros (escrita) e os disponibilizam para consulta (leitura), disponibilizando um interface comum de acesso para os participantes da rede. Costa et al. (2018) chegam a conclusão similar, citando que o Blockchain pode fornecer Prova de Propriedade/Autoria, Prova de Integridade e Prova de Existência, as três dimensões principais da certificação de documentos, e apresentam estudo de caso na implementação de plataforma agnóstica em termos tecnológicos para a proteção de documentos acadêmicos, como na solução de Cardoso e Goya, esta proposta oferece uma forma de acesso em comum para interação com o Blockchain através de aplicações *Desktop*, *Mobile* e via *Browser*. As Figuras 2 e 3 a seguir, ilustram as soluções propostas por Cardoso e Goya e Costa et al.

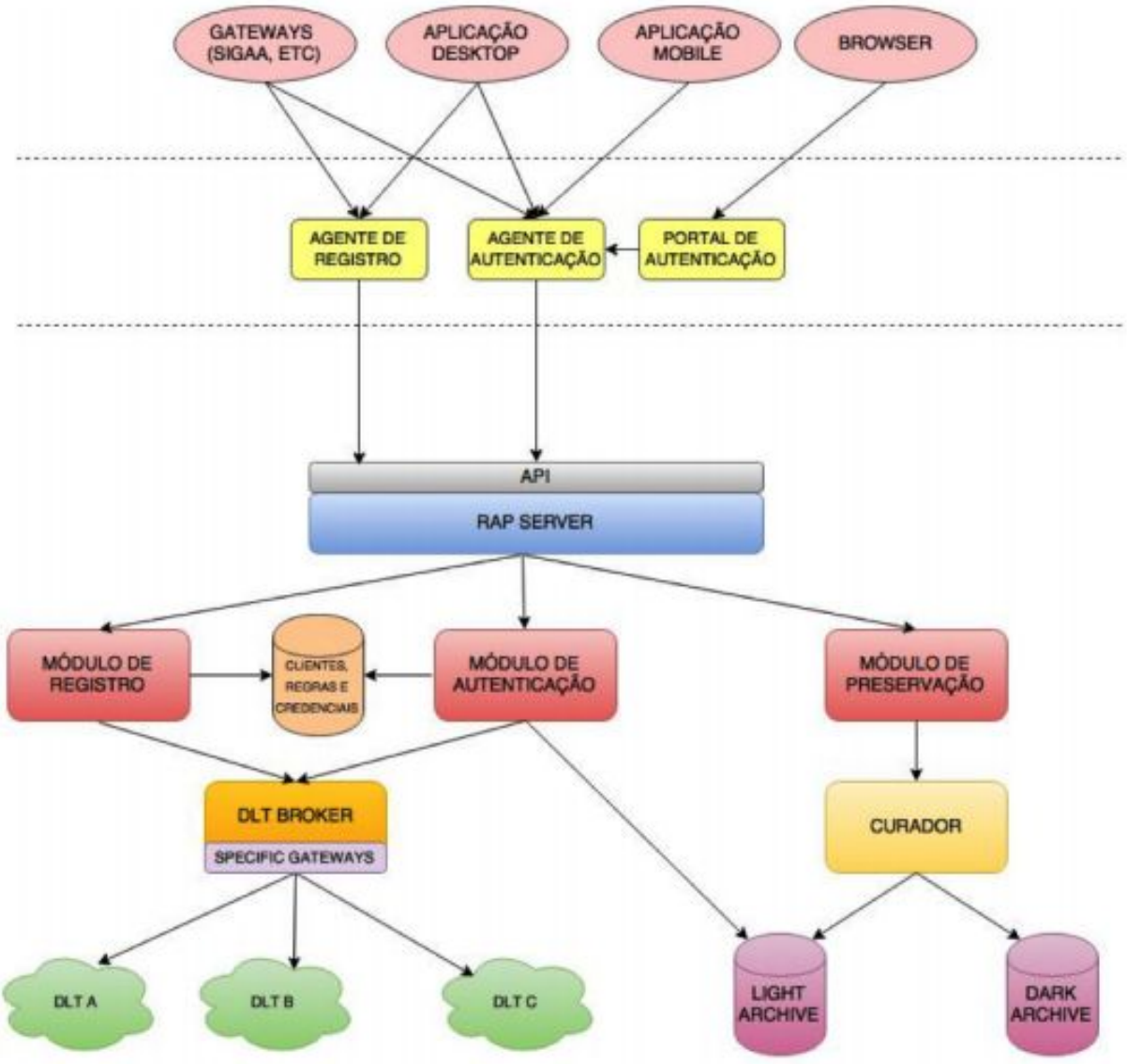

Figura 2 - Arquitetura do Protótipo. Fonte: (Costa, R. et al., 2018).

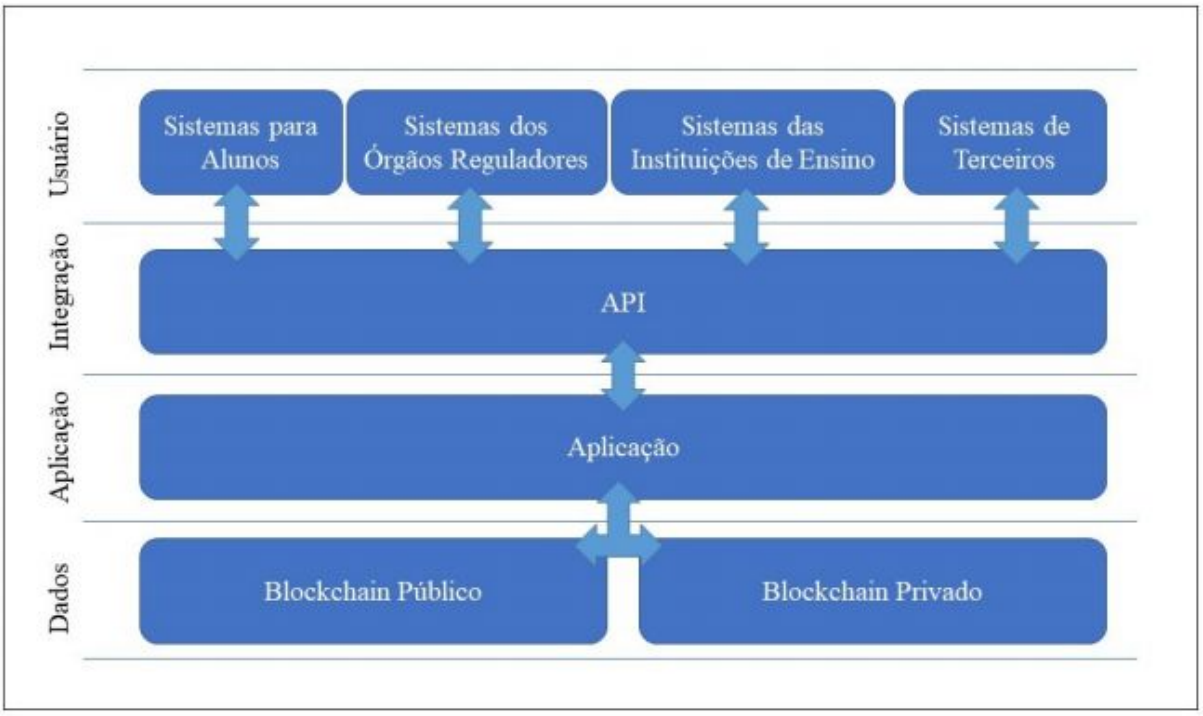

Figura 3 - Diagrama de Camadas da Arquitetura. Fonte: (Cardoso e Goya, 2018).

Em relação à discussão sobre Blockchain *versus* certificação digital, uma breve e objetiva abordagem é dada pela empresa Link Certificação Digital (2018), que lista os prós e contras de cada tecnologia. Blockchain é segura e barata, mas relativamente de difícil acesso e pouco prática, além de presumir o anonimato. Já o certificado digital é mais prático, acessível e permite identificar as pessoas quando utilizado, mas possui uma estrutura mais onerosa e centralizada. Assim, a empresa indica que o caminho mais viável parece ser fazer com que as duas tecnologias se encontrem em um mesmo ponto, fazendo com que as falhas sejam preenchidas pelas qualidades que uma tecnologia oferece a outra. Mesma conclusão chegaram Costa et al (op. cit.), que integram *Blockchain*, certificação digital e preservação de documentos para implementar um serviço de registro capaz, segundo os autores, de interferir ao mínimo nos processos correntes de emissão de documentos acadêmicos. Este serviço de registro possui módulos cliente e módulos servidor, permitindo as funcionalidades tanto de leitura quanto de escrita de dados, dependendo do papel que o usuário tem no serviço. A plataforma oferece uma API (*Application*

Programming Interface) REST (Representational State Transfer) e um *broker* para as tecnologias Bitcoin e Ethereum, embora outras possam ser incorporadas no futuro.

Cabe ainda ressaltar a existência de um conceito mais genérico, porém de menor granularidade, os *badges* (medalhas), que são reconhecimentos de mérito eletrônicos. A ideia de usar Blockchain para autenticar mérito deu origem ao Open Badge, uma sistemática de emissão de certificados digitais com o padrão de autenticação Blockchain, que visa dar reconhecimento profissional às pessoas de forma transparente e auditável (Brasil Open Badge, 2018). Um badge, ou "medalha", possui uma imagem, um nome que identifique rapidamente a capacitação relativa, a descrição desta capacitação, os critérios que indicam o por que o ganhador recebeu o *badge*, validade e o emissor. Estes metadados de um badge podem ser empregados como base os metadados para certificados, faltando referências legais da certificação.

3. DEFINIÇÃO DA TECNOLOGIA

Com a publicação do artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" por Satoshi Nakamoto no ano de dois mil e oito, e consequentemente o sucesso do Bitcoin, várias outras tecnologias começaram a aparecer no mercado. De acordo com Marr (2018), o uso do Blockchain depois do Bitcoin foi somente para implementações de soluções similares, como o Ethereum, mas com o tempo, surgiram outras soluções que não tinham como seu principal *asset* uma moeda.

Karthik (2018) define seis soluções de Blockchain como as maiores e mais usadas no mercado, são elas:

- Eris Industries
- Ethereum
- HyperLedger
- Multichain
- Openblockchain
- R3 Corda

Essas seis tecnologias citadas por Karthik como as principais no atual mercado, foram analisadas para a implementação deste projeto, tendo como requisito algumas características como: distribuição gratuita; não voltada à monetização como o Bitcoin; rede privada, já que as primeiras tecnologias tinham como premissa o uso de um rede pública; e suporte à autorização, ou seja, os nós da rede e usuários do Blockchain precisam ser identificáveis.

A primeira analisada e descartada foi a Ethereum, pois sua proposta é a mesma do Bitcoin, oferecer um Blockchain para suportar movimentações financeiras. A R3 Corda que é projetada especificamente para aplicação de Blockchain em um determinado domínio, especializada para a indústria BFSI (*Bank, Financial Service and Insurance*), também foi descartada. Outra solução disponível no mercado é a Openblockchain, desenvolvida pela IBM, porém esta veio a se tornar parte da Hyperledger (IBM, 2018), outra tecnologia que será analisada neste estudo, portanto, a análise da Openblockchain se tornou desnecessária. Também

excluída deste trabalho, mas por um motivo diferente, foi a solução Eris Industries. Seu *website* e documentação se mostrou instável e inacessível durante o levantamento das tecnologias realizado neste capítulo.

As duas tecnologias que atenderam a todos os requisitos foram Multichain e HyperLedger. O Quadro 1 mostra o resumo do levantamento das seis tecnologias analisadas e o motivo pelo qual não foram selecionadas.

TECNOLOGIA	SELECIONADA	MOTIVO (CASO NÃO SELECIONADA)
Eris Industries	Não	*Website* fora do ar durante o levantamento.
Ethereum	Não	Especializada para movimentações financeiras.
HyperLedger	Sim	
Multichain	Sim	
Openblockchain	Não	Foi incorporada a outra tecnologia da lista.
R3 Corda	Não	Especializada para um ramo diferente.

Quadro 1 - Tecnologias selecionadas e eliminadas. Fonte: (Elaboração Própria, 2019).

3.1. Tecnologias Candidatas

O HyperLedger surgiu de um esforço colaborativo para para evoluir o uso de Blockchains na indústria. É uma colaboração global, na qual a *The Linux Foundation* é a anfitriã e grandes empresas também fazem parte, como líderes na área de finanças, bancos, internet das coisas, manufatura e tecnologia, de acordo com a documentação oficial do produto em seu *website* (2016).

O MultiChain, segundo Greenspan (2015) no *blog* oficial da tecnologia, é uma plataforma para criação de Blockchains privados com o objetivo de oferecer segurança e controle através dessa privacidade. Tanto o HyperLedger quanto o MultiChain, ainda se encontram em constantes atualizações, sendo assim, as informações fornecidas neste estudo são baseadas nas funcionalidades oferecidas pelas tecnologias nas versões oferecidas nas versões HyperLedger

1.3.0 e MultiChain 1.0. O Multichain já disponibilizou uma versão 2.0, mas ainda se encontra na sua fase beta.

3.2. Comparação das Tecnologias

Alguns quesitos foram levados em consideração para a escolha da tecnologia que seria usada para a aplicação projeto, o primeiro desses quesitos foi como cada tecnologia suporta a estruturação dos dados da aplicação, ou seja, se é oferecido uma forma de mapear o modelo da do Blockchain. O HyperLedger oferece um mapeamento orientado a objetos em JavaScript, enquanto o MultiChain trata o asset como uma descrição em JSON (*JavaScript Object Notation*). Para os propósitos deste projeto, ambas soluções, apesar de diferentes, são viáveis e oferecem vantagens e desvantagens. A vantagem do HyperLedger é uma estrutura mais robusta, podendo ter validações dos dados inseridos no Blockchain, porém, uma atualização no modelo é mais trabalhosa, necessitando uma criação de uma nova versão para qualquer mudança realizada. As vantagens do HyperLedger são justamente as desvantagens do MultiChain, por falta de um modelo pré definido, uma validação de dados teria que ser feita por um intermediário entre o nó e o Blockchain. E pelo fato de não haver validação do modelo, diferentemente do HyperLedger, uma atualização não implicaria na necessidade de uma nova versão da rede.

O segundo quesito analisado foi o suporte à autorização. O MultiChain trabalha com um conceito de *Streams*, que nada mais é do que rotular alguns blocos do Blockchain como pertencentes a uma *Stream*, podendo aplicar diferentes permissões de leitura e escrita para cada um desses *Streams*. Esse conceito poderia ser usado, por exemplo, criando um *Stream* para cada uma das instituições emissoras de certificados, garantido direito de escrita somente para a instituição detentora do *Stream*. O HyperLedger oferece uma validação baseada em certificados digitais, podendo ser aplicada uma hierarquia de permissões, como exemplo neste projeto, essa hierarquia poderia ser usada para cada instituição ter suas permissões, porém, podendo ainda dar permissões diferentes para cada funcionário. Nesse quesito o HyperLedger se mostrou mais completo e com uma maior escalabilidade.

Como uma das propostas deste projeto é a componentização do Blockchain, oferecendo-o como um serviço para diferentes implementações como aplicações cliente, o terceiro quesito

analisado foi se a tecnologia oferece uma API. Ambas disponibilizam acesso ao Blockchain através de uma API REST, porém o HyperLedger oferece um maior grau de customização desta API, o que não teria muito impacto para cumprir os requisitos deste projeto, porém, poderia ser útil em uma futura atualização.

O quarto e último quesito é o uso de *Smart Contracts* pelas tecnologias, que segundo Chandler (2017) são códigos que são executados no BlockChain para aplicação de regras, lógicas de negócio, e outros variados usos. Nesse quesito o HyperLedger se destaca, pois ele oferece suporte ao desenvolvimento de *Smart Contracts*, que nessa tecnologia são chamados de *Chain Code*, enquanto o Multichain não oferece esse suporte até a sua versão 1.0.

O Quadro 2 mostra um resumo dos quesitos mais importantes na escolha do HyperLedger sobre o Multichain para a implementação da solução proposta.

	HYPERLEDGER	**MULTICHAIN**
Estrutura de Dados	Estrutura Orientada a Objetos	Representação JSON
Suporte a Autorização	*Roles* (Multi-hierarquia)	*Stream* (por Instituição)
API	REST	REST
Smart Contracts	*Chain Code*	-

Quadro 2 - Comparação entre tecnologias. Fonte: (Elaboração Própria, 2019)

3.3. Tecnologia Selecionada

Para os propósitos deste projeto, o HyperLedger se mostrou mais robusto para atender os requisitos iniciais, se destacando no suporte à autenticação, oferecendo vários níveis de permissões. Outro característica do HyperLedger que se destaca é a capacidade de validação dos dados inseridos, não sendo necessário o desenvolvimento de um projeto intermediário, isso é facilitado pelo mapeamento orientado a objetos, que como já citado, também traz desvantagens, como a necessidade de atualização da versão do modelo em qualquer mudança no mesmo.

Outro requisito que teve grande influência na escolha do HyperLedger foi a possibilidade de uso de *Smart Contracts*, o que o Multichain não oferece. Tendo essa análise sido feita,

HyperLedger foi a tecnologia escolhida para a implementação do projeto, pois atende às características dos requisitos. O próximo capítulo mostrará em como essa implementação foi realizada, descrevendo detalhes técnicos da tecnologia, assim como detalhes do desenvolvimento e também dificuldades encontradas.

4. DESENVOLVIMENTO E IMPLANTAÇÃO

A rede que compõe a comunicação dos participantes do Blockchain é formada por nós que representam as instituições emissoras de certificado. Cada nó, ou cada instituição, possui sua própria e exclusiva réplica do Blockchain. A Figura 4 a seguir, ilustra uma possível rede de comunicação do *Blockchain*, onde os nós representados por pontos e as linhas de comunicação, são representadas por linhas. As instituições de ensino mostradas, além do IFF e da ENAP são meramente ilustrativas.

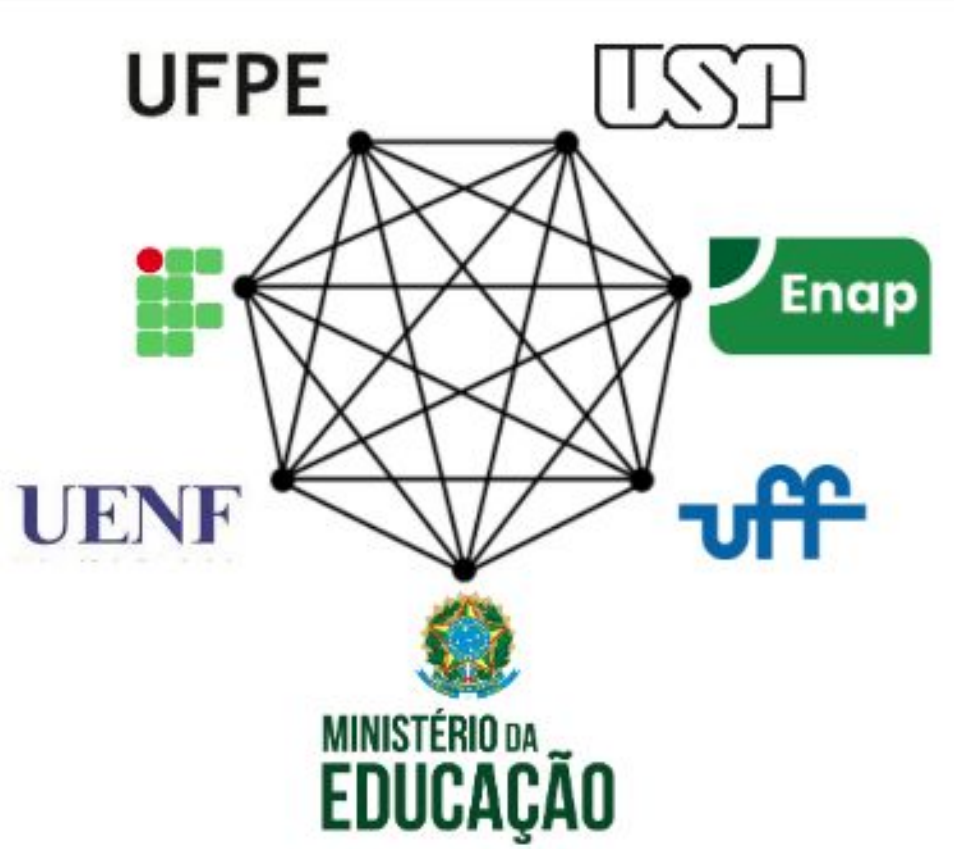

Figura 4 - Uma possível rede de Instituições como nós do Blockchain. Fonte: (Elaboração Própria, 2018).

A ideia principal para que o Ministério da Educação faça parte da rede, é para que ele possa oferecer um mecanismo de leitura do Blockchain, funcionando como um centralizador de informação. A funcionalidade de leitura continuaria disponível em cada um dos nós, podendo

cada instituição escolher exibir os dados somente dos certificados emitidos por ela, ou ainda exibir todos os certificados persistidos no Blockchain. A proposta deste projeto, é tornar a leitura do Blockchain altamente flexível.

4.1. Arquitetura Funcional

A arquitetura funcional do projeto se divide em três partes, que serão detalhadas após a seguinte breve descrição sobre elas:

- Criação, leitura, edição e deleção dos dados do Blockchain realizadas pelas instituições de ensino.
- Pesquisa sobre os dados do Blockchain disponibilizada pelas instituições de ensino e pelo Ministério da Educação.
- Disponibilização de uma carteira de certificados pelo Ministério da Educação e pelas instituições de ensino para acesso individual do estudante.

4.1.1. Caso de Uso: Leitura e Escrita

A primeira parte da arquitetura funcional é relativa ao acesso de leitura e escrita (criação, edição e deleção) no Blockchain, realizadas pelas instituições de ensino e pelo Ministério da Educação. Toda instituição de ensino participante da rede tem o direito total de leitura e direito parcial de escrita, incluindo somente os certificados emitidos por ela. Este controle de escrita é providenciado através de mecanismos de autenticação e autorização que serão detalhados ainda neste capítulo. A Figura 5 mostra o caso de uso de leitura e escrita no Blockchain pelas instituições de ensino e pelo Ministério da Educação

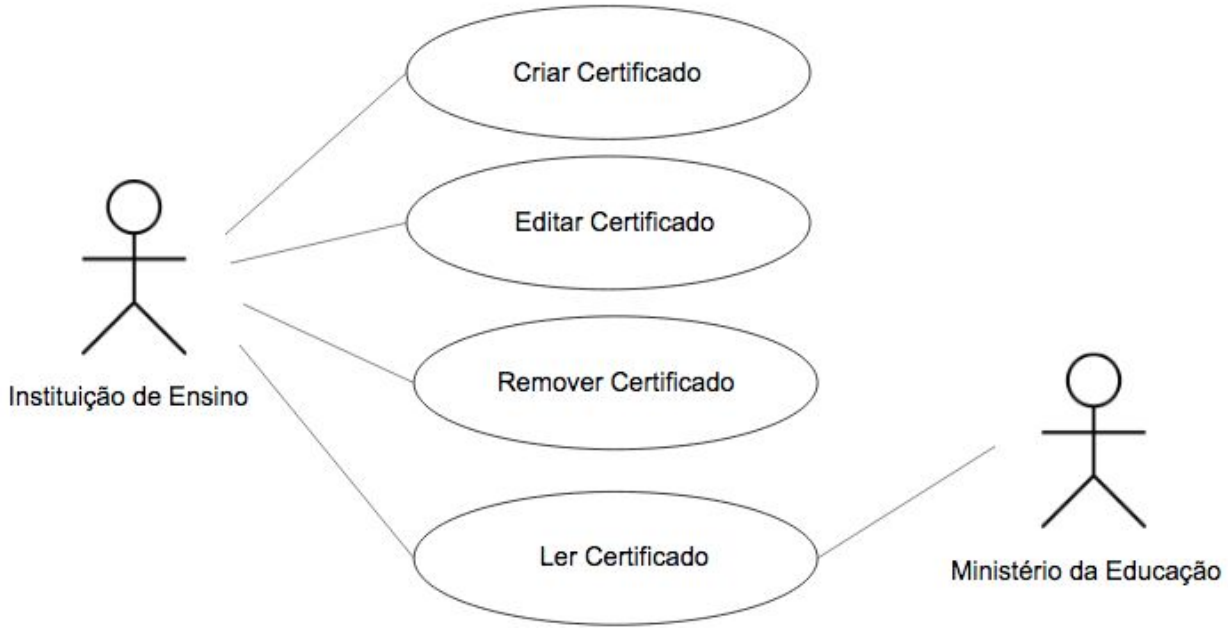

Figura 5 - Caso de uso de leitura e escrita no Blockchain: (Elaboração Própria, 2018).

O diagrama mostra a instituição de ensino e o Ministério da Educação como atores do caso de uso, sendo que enquanto as instituições possuem acesso de leitura e escrita, o Ministério da Educação possui somente acesso à leitura, pois não emite certificados.

4.1.2. Caso de Uso: Pesquisa

A segunda parte da arquitetura funcional é a disponibilização de pesquisa sobre os dados do Blockchain, esta é uma funcionalidade para tornar os dados do Blockchain disponíveis para consulta pública. A proposta principal deste projeto é que o Ministério da Educação disponibilize esta funcionalidade para pesquisa pública incluindo todo o conteúdo persistido no Blockchain, enquanto as instituições de ensino também possam oferecer uma pesquisa limitada aos certificados emitidos por elas. A Figura 6 mostra o diagrama de caso de uso da disponibilização da pesquisa pública da informação contida no Blockchain sobre os certificados emitidos, as instituições de ensino e o Ministério da Educação são exibidos como atores no diagrama responsáveis por disponibilizar a pesquisa, e o público em geral é representado por um ator responsável por realizar a pesquisa.

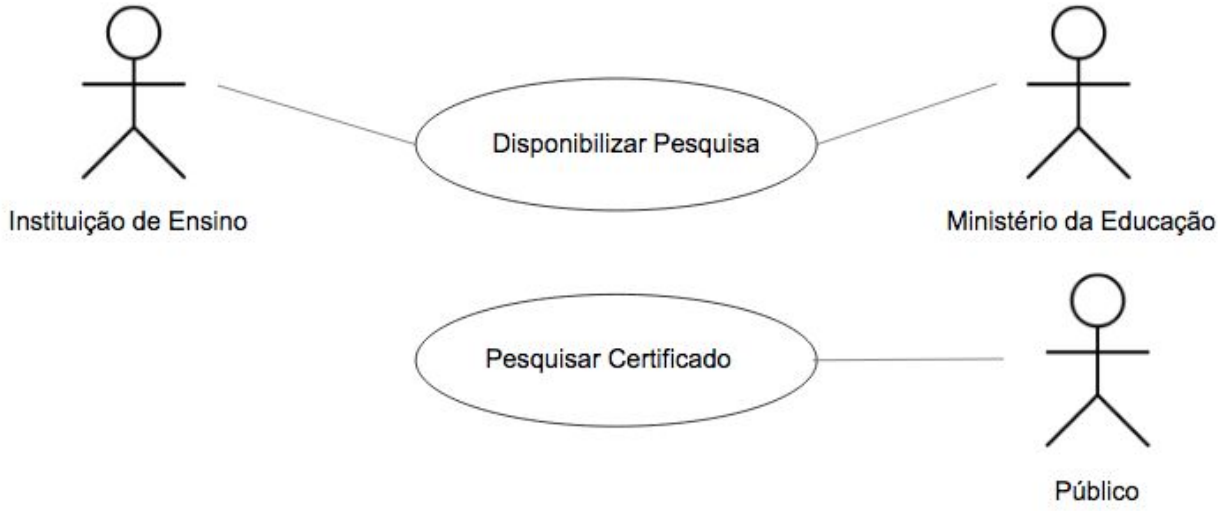

Figura 6 - Caso de uso de pesquisa no Blockchain: (Elaboração Própria, 2018).

As instituições possuem acesso irrestrito de leitura, cabendo a cada uma implementar a pesquisa de forma mais adequada. Este projeto oferece uma aplicação cliente como exemplo, nessa implementação, a leitura do Blockchain é implementada na visão de um funcionário autenticado no sistema e oferece a visão de todos os certificados no nome do estudante filtrado através do CPF, porém, fornecendo as opções de remoção e edição somente para os certificados emitidos para instituição responsável pela emissão dos mesmos.

4.1.3. Caso de Uso: Carteira de Certificados

A terceira e última parte da arquitetura funcional é a parte dedicada à carteira de certificados do estudante. Assim como na pesquisa pública, a ideia principal é que esta carteira de certificados abranja todos os certificados conquistados pelo estudante, não dependendo da instituição emissora. A maneira mais intuitiva de alcançar esse objetivo é o Ministério da Educação disponibilizar tal funcionalidade, agindo como um integrador e centralizador da informação, possibilitando às instituições de disponibilizarem uma carteira de certificados específica para os cursos oferecidos pela própria instituição. Como o acesso a leitura é livre, nada impede as instituições que também tenham acesso de leitura aos certificados emitidos por outras, mantendo a proposta de flexibilidade deste projeto. Na aplicação demonstrativa que será

apresentada neste capítulo, a instituição exibe ao estudante todos seus certificados emitidos, concretizando a flexibilidade da arquitetura deste projeto.

A Figura 7 detalha a interação do estudante com a sua carteira de certificados. No diagrama as instituições de ensino e o Ministério da Educação são exibidos como atores responsáveis pela disponibilização da carteira de certificados, e o estudante é representado como um ator que pode acessar a sua própria carteira.

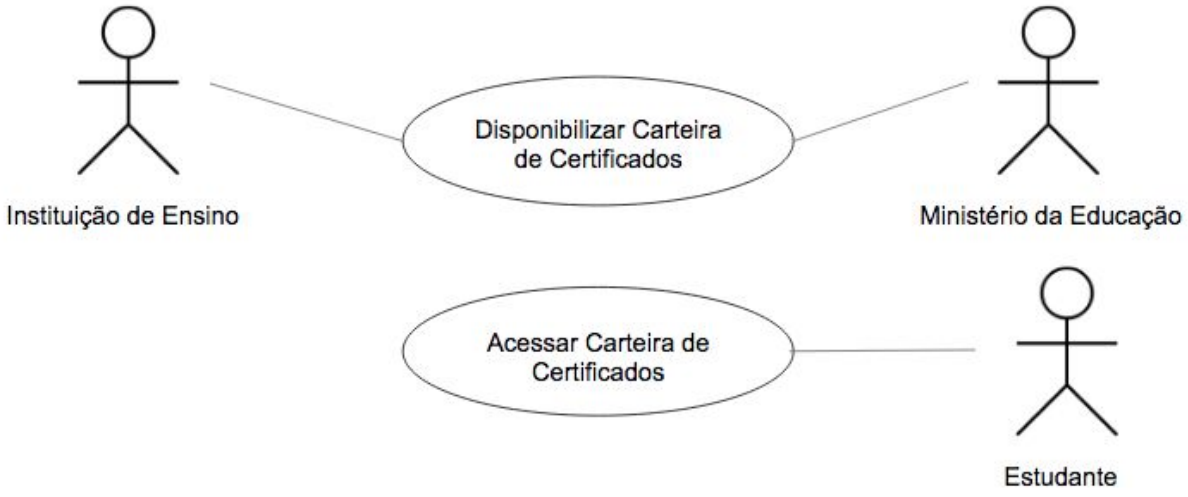

Figura 7 - Caso de uso carteira de certificados: (Elaboração Própria, 2018).

4.2. Componentes

Cada nó da rede consiste em três componentes. O primeiro é o próprio Blockchain desenvolvido no HyperLedger Fabric, o acesso ao Blockchain é feito através do segundo componente, um servidor que disponibiliza uma API REST. O terceiro componente é a aplicação cliente que as instituições emissoras de certificado usarão para acessar o Blockchain através do Servidor REST. Esta aplicação cliente será altamente customizável, permitindo que qualquer instituição desenvolva sua tecnologia, sendo necessário somente usar a API disponibilizada para acesso. A Figura 8 a seguir, ilustra o relacionamento dos três componentes do nó.

Figura 8 - Componentes do nó Blockchain. Fonte: (Elaboração Própria, 2018).

4.3. Arquitetura Cliente Servidor

Os três elementos de cada nó do Blockchain são separados em uma arquitetura Cliente Servidor, a aplicação cliente corresponde à parte Cliente e O Servidor REST e a réplica do Blockchain de cada nó se entendem pela parte do Servidor.

A proposta do projeto é disponibilizar toda a arquitetura entendida como Servidor através de plataformas IaaS (*Infrastructure as a Service*), o que pode-se chamar de nuvem para esse cenário, termo utilizado na área de Tecnologia da Informação para definir a distribuição de serviços de computação – servidores, armazenamento, bancos de dados, redes, software, análises, inteligência e muito mais pela Internet, proporcionando inovações mais rápidas, recursos flexíveis e economia na escala (MICROSOFT, 2010). O Blockchain é replicado para cada instituição devido à característica padrão do protocolo, o que leva também a necessidade de replicar o Servidor REST, em um relacionamento de um-para-um com a réplica do Blockchain. O uso de instâncias exclusivas do Servidor REST para cada nó também tem ligação com o suporte à autorização, que será discutido em detalhes nos capítulos seguintes.

4.4. Modelo

A seguir, será discutido o modelo da da aplicação e as decisões tomadas para se chegar ao resultado final.

4.4.1. Terminologia

A tecnologia HyperLedger oferece uma estrutura robusta para criação de um modelo de dados, e é preciso estar habituado com sua terminologia para compreender a capacidade e limitações da plataforma. A seguir são descritos os principais conceitos usados pelo projeto para a criação de um modelo. Os nomes foram mantidos em inglês, já que são usados como palavras chaves no código:

- *Asset* - É o elemento principal do Blockchain, no caso do projeto sendo apresentado é o certificado.
- *Participant* - São elementos que apresentam uma relação de cliente no Blockchain.
- *Transaction* - Operações realizadas no Blockchain que alteram sua estrutura, geralmente inserindo um novo bloco.
- *Concept* - São usadas para definir um tipo complexo de dados, formado pela composição de informações simples.

O HyperLedger ainda oferece outros elementos para a criação do modelo, mas pela simplicidade da explicação e pelo fato desses elementos não serem usados no projeto, eles não foram mencionados.

4.4.2. Modelo Relacional

No Blockchain, é preciso somente armazenar as informações pertinentes ao certificado e outras para controle de segurança e auditoria, por exemplo, para o estudante que conquistou o certificado, é preciso somente seu nome e um identificador único, que nesse caso foi usado o CPF (Cadastro de Pessoa Física), os outros dados cadastrais do estudante que a instituição possui não são necessários para o certificado. Caso haja uma futura necessidade de persistir outros dados, pode-se enriquecer o modelo. A Figura 9 mostra o modelo relacional.

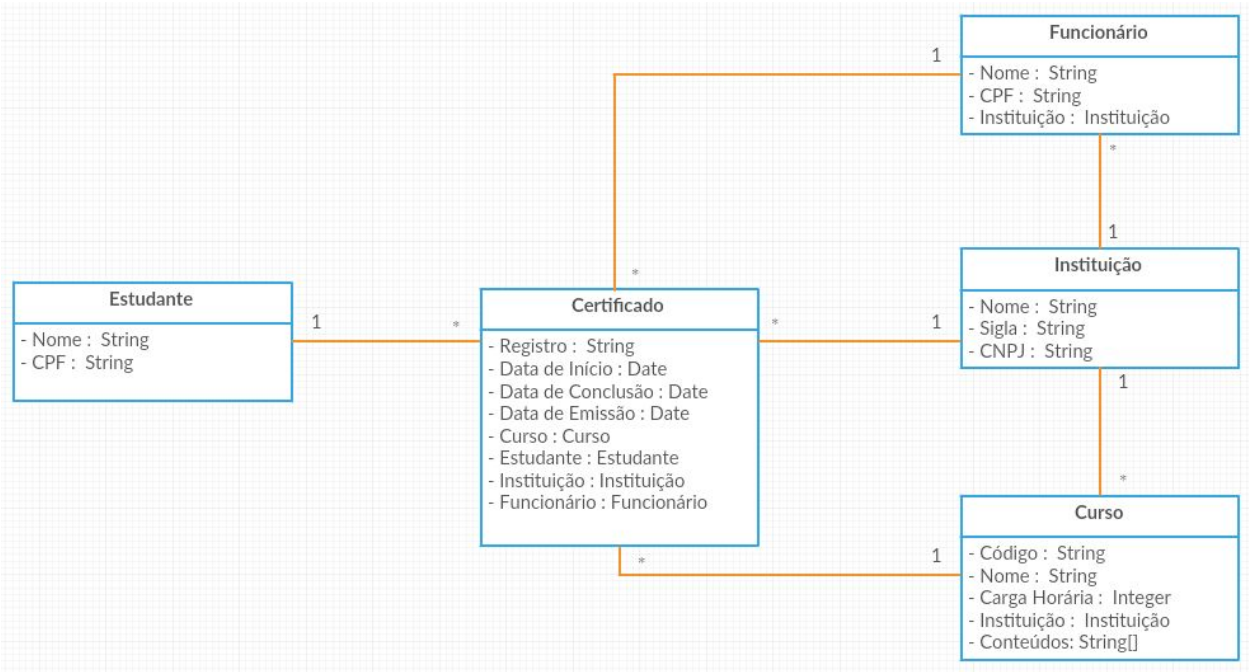

Figura 9 - Modelo Relacional adaptado do Blockchain. Fonte: (Elaboração Própria, 2018).

Esse modelo relacional foi criado devido ao fato do HyperLedger trabalhar com um mapeamento Orientado a Objetos, mas pode-se notar claramente que o *asset* da transação, que é o certificado, é a peça principal que será persistida no bloco do Blockchain. Os outros componentes, além de serem referenciados pelo certificado, possuem relacionamentos que facilitam a segurança e a auditoria, como o relacionamento entre Funcionário e Instituição assim como Instituição e Curso.

De acordo com os componentes do HyperLedger mostrado no capítulo anterior (*Asset*, *Participant* e *Concept*), cada classe do diagrama é representada por um tipo de elemento. Primeiramente, tem o certificado como o *Asset*, que é o elemento principal no Blockchain. As classes Instituição, Estudante e Funcionário, três das quatro classes restantes, são definidas como *Participant*, esse elemento representa entidades que possuem um relacionamento de cliente com o Blockchain, o que significa que quando um aluno ou funcionário interagir com a API REST, o HyperLedger os reconhecerá e aplicará as devidas abordagens de segurança. A Instituição também é definida como *Participant*, pois regras de segurança podem ser aplicadas a nível de instituição ou a nível de funcionário.

O último elemento é o Curso, que é definido como um *Concept*. Ele é somente um tipo complexo do certificado, possuindo suas propriedades. Durante o desenvolvimento foi encontrado um comportamento inesperado no acesso à API REST devido ao uso do Curso como um *Concept*, e por isso no modelo ele foi definido como *Participant*. Este mesmo problema também impactou na propriedade Registro do certificado, qual a princípio seria um *Concept* contendo três valores: Número, Registro e Folha. Até a conclusão do desenvolvimento do modelo, este problema do HyperLedger não tinha sido resolvido.

4.5. Interface

O servidor REST é o único ponto de interação do cliente com o Blockchain, e ele cumpre esse papel oferecendo uma API que pode ser acessada pelas aplicações clientes. Essa API providencia seis formas de interação com o Blockchain através de cinco verbos HTTP (*Hypertext Transfer Protocol*). O Quadro 3 informa o modo de interação com a API REST a partir dos métodos HTTP e URLs (*Universal Resource Locator*).

HTTP	URL	DESCRIÇÃO
GET	/Certificado	Retorna todos os certificados, possibilitando filtragem..
GET	/Certificado/{id}	Retorna o certificado representado pelo identificador {id}.
POST	/Certificado	Cria um novo certificado.
PUT	/Certificado/{id}	Atualiza o certificado representado pelo identificador {id}.
DELETE	/Certificado/{id}	Remove o certificado representado pelo identificador {id}.
HEAD	/Certificado/{id}	Consulta se o certificado representado pelo identificador {id} existe.

Quadro 3 - API REST. Fonte: (Elaboração Própria, 2019).

Todas as informações enviadas pelas aplicações clientes através dos métodos HTTP Get, Delete e Head são passadas unicamente pela URL, somente o Post e o Put necessitam passar informações no corpo do protocolo. A API REST aceita tanto informações em formato JSON ou

em formato XML (*eXtensible Markup Language*). A seguir no Quadro 4 pode-se ver lado a lado uma representação da mesma requisição de criação de um novo elemento feita através do método POST em formato JSON e a mesma requisição em XML.

JSON	XML

[
  {
  "id": "string",
  "registro": "string",
  "inicio": "2019-01-06T09:41:20.617Z",
  "fim": "2019-01-06T09:41:20.617Z",
  "emissao": "2019-01-06T09:41:20.617Z",
  "curso": {},
  "estudante": {},
  "instituicao": {},
  "funcionario": {}
  }
]
	<?xml version="1.0"?>
	<Inline Model>
	  <id>string</id>
	  <registro>string</registro>
	
	<inicio>1970-01-01T00:00:00.001Z</inicio>
	  <fim>1970-01-01T00:00:00.001Z</fim>
	
	<emissao>1970-01-01T00:00:00.001Z</emissao>
	  <curso></curso>
	  <estudante></estudante>
	  <instituicao></instituicao>
	  <funcionario></funcionario>
	</Inline Model>

Quadro 4 - Requisição JSON e XML. Fonte: (Elaboração Própria, 2019).

Os elementos que são definidos como *Participant*, são referenciados na requisição de criação do certificado através de seus identificadores, isso significa que esses elementos precisam antes já estarem criados no Blockchain. A API REST fornece as mesmas formas de interação relativas ao certificado para os elementos *Participant*, isso significa que também pode-se pesquisar, criar deletar e atualizar dados desses elementos. Então, na criação do certificado é necessário pesquisar se suas dependências já estão criadas no Blockchain, caso

alguma não exista, estas precisam ser criadas antes do envio da requisição de criação do certificado.

Para a consistência do modelo, o HyperLedger oferece, além de tipagem das propriedades, o uso de validações através restrições como tamanho de campo, limite mínimo e máximo para propriedades numéricas e também oferece o uso de expressões regulares. Essas expressões regulares podem ser usadas por exemplo para validar um formato de CPF ou do número do registro do certificado.

4.6. Segurança (Rede Privada e Suporte a Autorização)

Um dos quesitos na escolha da tecnologia para a implementação deste projeto foi o oferecimento de uma rede permissionada, já que a proposta original da tecnologia Blockchain era propor uma rede onde seus nós sejam anônimos (Sharma, 2018). O HyperLedger oferece uma rede onde não há anonimato entre seus nós, isto é alcançado através do uso de certificados digitais de chave pública baseados no protocolo X.509.

Para melhor entendimento de como o HyperLedger suporta a autorização, primeiramente é preciso entender o papel desempenhado pelo MSP (*Membership Service Provider*), que segundo a documentação oficial da tecnologia é responsável por abstrair todos os mecanismos criptográficos e protocolos por trás da criação e validação de certificados. Em um nível de abstração maior, para a proposta deste projeto, o MSP pode ser entendido como o conjunto de três funções. A primeira é a de CA (*Certificate Authority*) responsável por emitir certificados digitais no Blockchain, a segunda função é a de VA (*Validation Authority*), responsável pela validação dos certificados e a terceira e última função é a de RA (*Registration Authority*), que é responsável por verificar a requisição de um novo certificado e enviar para o CA (Rouse, 2006).

A proposta deste projeto é que cada nó possua seu MSP exclusivo, responsável pelo gerenciamento de protocolos locais, podendo ser aplicadas vários níveis de autenticação, como a nível de departamento da instituição ou até a nível de funcionário.

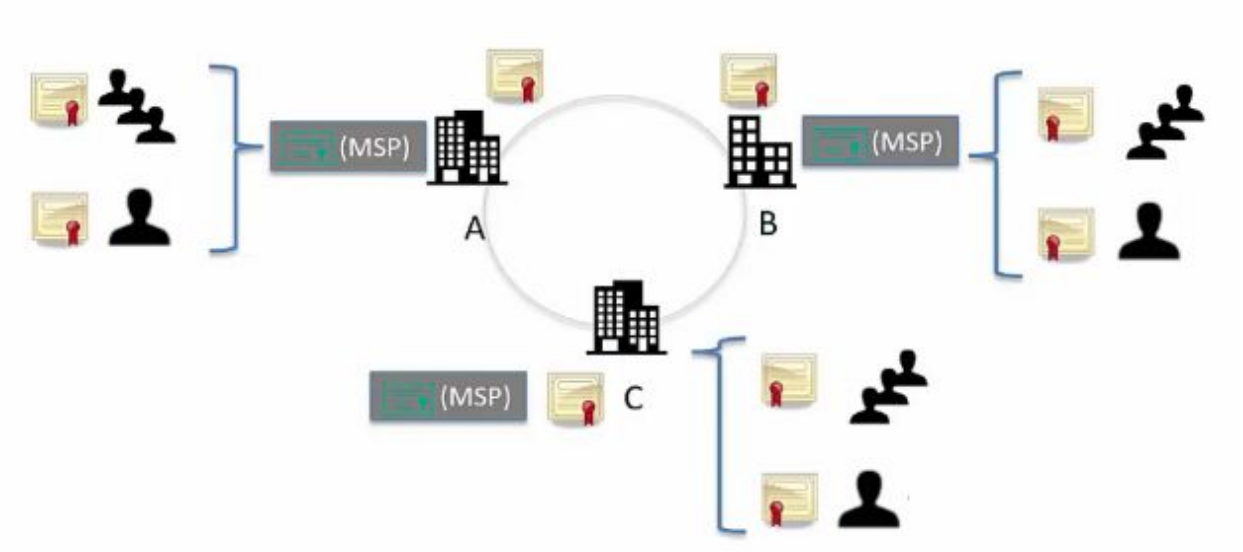

Figura 10 - Membership Service Provider. Fonte: Sakhuja (2017).

Na Figura 10 é exibida a integração das instituições com o MSP, sugerindo uma hierarquia de permissões baseadas em certificados digitais de chave pública. A figura mostra três instituições representadas pelas letras A, B e C, cada uma com um MSP exclusivo com um certificado digital de chave pública que garante o acesso da instituição ao Blockchain. No contexto dentro da instituição, a hierarquia de permissões fica a cargo na mesma, a figura sugere níveis de permissões individuais, representados pela silhueta de uma pessoa e departamentais, representados pelo conjunto silhuetas.

4.7. Auditoria

A principal característica de um Blockchain é ser um modelo *append-only*, isso significa que cada nova informação é registrada no banco como um novo registro, nenhuma atualização sobrescreve outra já existente com o novo valor (CROOK, 2014). Isso permite rever todo histórico de edições. O HyperLedger otimiza a ideia inicial do conceito Blockchain dividindo a informação em dois registros distintos. O primeiro registra todos as transações realizadas em ordem cronológica e o segundo registra o estado atual do *asset*.

Neste projeto, qualquer informação de emissão de certificado ficará persistida nesse registro, facilitando a inspeção do histórico, e como é característico do Blockchain, esse histórico de registro ficará replicado em cada nó por toda a rede.

4.8. Aplicação Cliente Demonstrativa

A solução foi desenvolvida para ser altamente customizável no quesito de aceitação de aplicações clientes, e por isso foi facilmente acoplada ao SUAP, plataforma administrativa utilizada pelo IFF, esta integração será abordada no próximo tópico. Durante o desenvolvimento foi criada uma aplicação cliente demonstrativa, simulando um conjunto de operações denominado CRUD (*Create Read Update Delete*), que são as operações comum de leitura e escrita, incluindo: criação, leitura, atualização e remoção de dados. Essa aplicação se divide em dois cenários, o primeiro é a visão do estudante sobre sua carteira de certificados.

Figura 11 - Carteira de Certificado na aplicação cliente. Fonte: (Elaboração Própria, 2019).

Quando o estudante se encontra autenticado no sistema, ele tem acesso a todos seus certificados emitidos por diferentes instituições. Também cabe a instituição oferecer acesso de

pesquisa mesmo para usuários que não fazem parte da instituição, ou seja, pessoas e instituições que não possuem acesso ao sistema através de autenticação.

O próximo cenário é a visão de um funcionário da instituição com permissão de criação e atualização de dados no Blockchain. No seu acesso ao sistema, depois de autenticado, ele tem acesso completo à funcionalidade de leitura de todos os certificados do Blockchain, porém, as permissões de criação, atualização e remoção de dados, são limitadas somente aos certificados emitidos pela própria instituição, permissões que o HyperLedger também permite limitar a nível departamental. É válido relembrar que mesmo as informações de atualização e remoção dos dados são realizadas em um modelo *Append-Only*, sendo que nenhuma informação já persistida no Blockchain é perdida.

As próximas três figuras mostram detalhes da interface da aplicação cliente na visão de um funcionário autenticado no sistema. A Figura 12 ilustra a visão de um funcionário do IFF autenticado no sistema, este possui permissão de visualização de todos os certificados criados no Blockchain, porém só possui a permissão de escrita para os certificados emitidos pelo IFF, isso fica claro na coluna "Ação" onde os certificados emitidos pelo ENAP não exibem a opção "Remover".

Figura 12 - Funcionário autenticado na aplicação cliente. Fonte: (Elaboração Própria, 2019).

A Figura 13 exibe um formulário para emissão de um novo certificado, este formulário permite o preenchimento de dados importantes do certificado como: nome do estudante, nome do curso, data de início e conclusão do curso, data de emissão do certificado e dados relativos ao número de registro do certificado. A Figura 14 exibe dados de um certificado já criado, na aplicação demonstrativa, esses dados são exibidos ao clicar na ação "Ver" na lista apresentada na Figura 12.

Figura 13 - Formulário de emissão na aplicação cliente. Fonte: (Elaboração Própria, 2019).

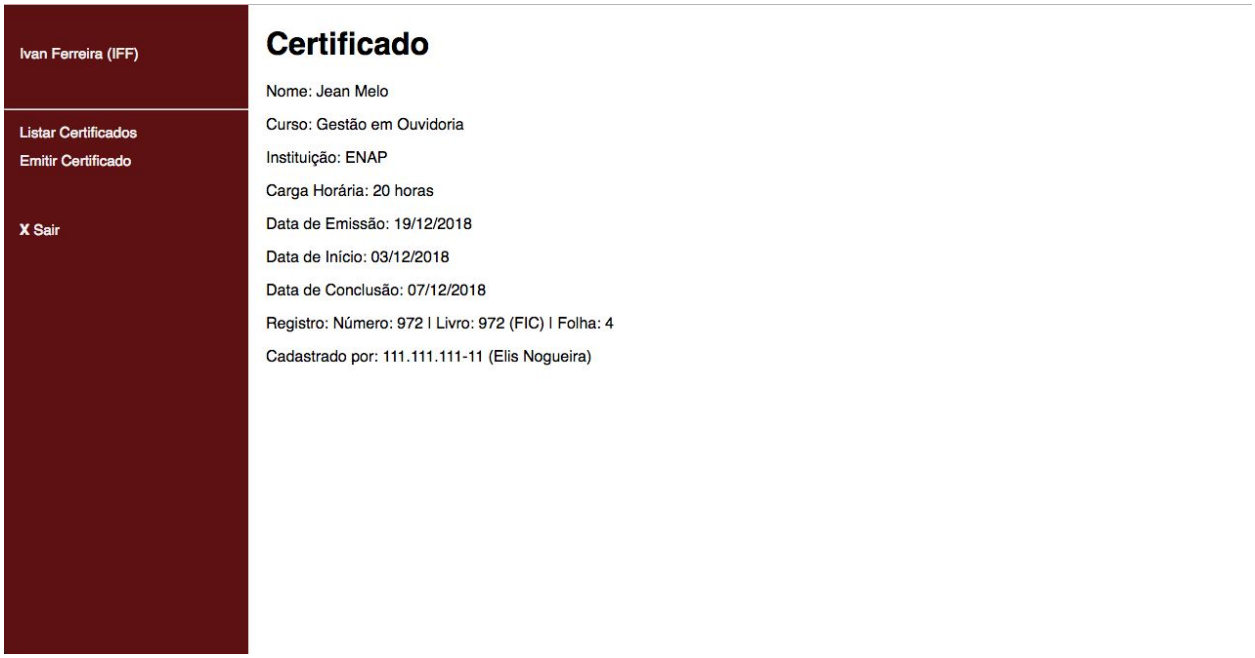

Figura 14 - Visualização de certificado aplicação cliente. Fonte: (Elaboração Própria, 2018).

4.9. Integração com o SUAP

A primeira integração da solução proposta com uma instituição de ensino foi feita no próprio IFF através do SUAP. Foi criado um novo módulo na interface do sistema administrativo e um servidor com a API REST e o Blockchain. Todo o processo, desde preparação do servidor para a API REST e o desenvolvimento do módulo no SUAP durou aproximadamente duas semanas, sendo dois profissionais responsáveis pela integração, totalizando cento e sessenta homem / hora. Testes foram utilizados durante o desenvolvimento, seguindo uma abordagem BDD (*Behaviour Driven Development*), e comprovaram a natural integração entre o novo módulo e o Blockchain.

Com somente o IFF compondo a rede, o Blockchain pode ser visto como apenas um banco de dados *Append-Only*, já que as principais propostas do Blockchain incluem a integração entre os nós da rede. O segundo nó da rede é o ENAP, sua integração com o Blockchain será detalhada no próximo tópico.

As Figuras 15, 16 e 17 mostram telas do módulo do SUAP desenvolvidas para integração com o Blockchain. A Figura 15 mostra a tela de criação de um certificado na visão de um funcionário autenticado no sistema com as devidas permissões. A Figura 15 exibe, também na

visão do funcionário, uma lista com os certificados, no caso do exemplo, exibe o certificado criado. A Figura 17 mostra a visualização dos dados do certificado emitido.

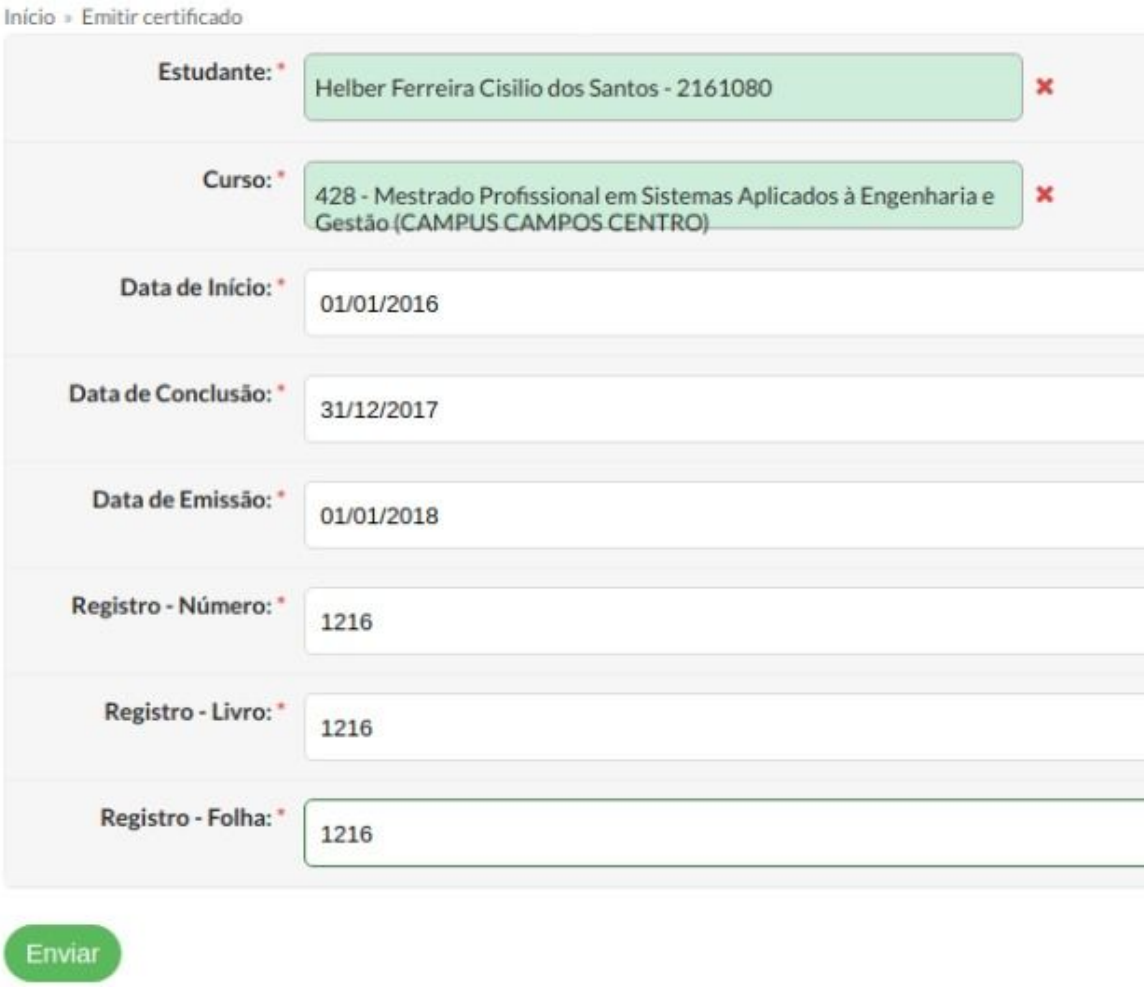

Figura 15 - Visualização de certificado aplicação cliente.. Fonte: (Elaboração Própria, 2018).

Figura 16 - Visualização de certificado aplicação cliente.. Fonte: (Elaboração Própria, 2018).

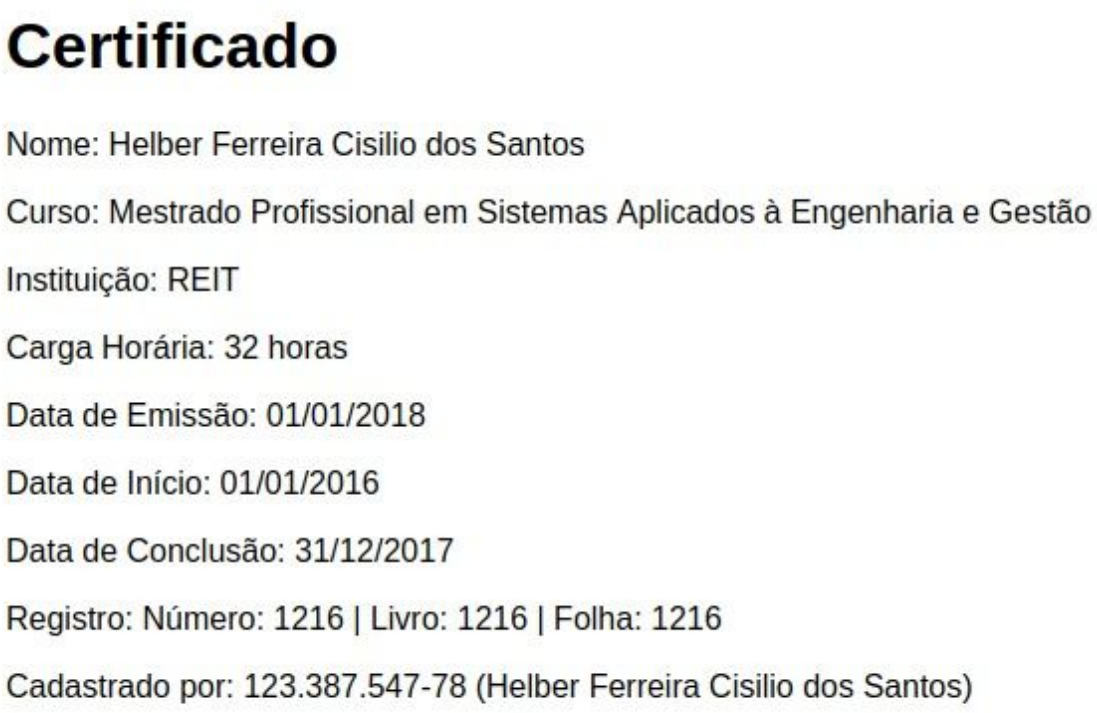

Figura 17 - Visualização de certificado aplicação cliente.. Fonte: (Elaboração Própria, 2018).

4.10. Base para Solução ENAP

Durante o mês de Fevereiro de 2019 foi iniciada a integração do código desenvolvido neste projeto com a versão do SUAP empregada pela ENAP. No momento de entrega deste relatório, a Coordenadoria de Gestão da Tecnologia da Informação (CGTI) da ENAP está adaptando a instância da solução aqui apresentada para que seja empregada na geração de

certificados digitais desta Escola, em fase de testes. Serão necessárias adaptações que foram discutidas com membros das equipes de Gestão da Inovação, documentação acadêmica, Desenvolvimento de Sistemas e Infraestrutura de Tecnologia da Informação da ENAP.

Estas adaptações foram discutidas em reuniões presenciais realizadas nos dias 12 e 13 de fevereiro e 06 de maio de 2019, na sede da ENAP em Brasília/DF, e foram definidas como as seguintes, todas a serem realizadas no SUAP-ENAP:

- Adaptação do Módulo de Geração de Certificados para ler das Tabelas de Cursos, Diários e Alunos e gerar os dados, que serão enviados utilizando a interface REST definida pelo plugin Python. Este plugin é independente de plataforma e envia um request para o Blockchain, criando o bloco que representa o certificado;
- Alterar o código desenvolvido no Hyperledger para retornar uma chave única, que identifique o bloco e será devolvida para o plugin e deste para o Módulo de Geração de Certificados, que finalmente armazenará esta chave numa tabela do SUAP.
- O plugin será empregado também para fornecer, via REST, dados para qualquer aplicação que deseje acessar a base de certificados da ENAP, devendo ainda serem analisadas as questões referentes à segurança, em especial quanto a ataques do tipo *Denial of Service* (DoS).
- Criar e documentar um sistema de versionamento das templates de certificados, o número da versão do certificado deve ser também armazenado como metadado deste certificado. Isso se mostra necessário para emitir segundas-vias de certificados, onde é necessário resgatar o mesmo padrão do certificado, bem como a assinatura da autoridade competente que o assinou à época da conclusão do curso pelo egresso.

A Figura 18 mostra esquematicamente como deve funcionar a solução aqui descrita. Deve ser salientado que as imagens dos certificados em PDF não serão armazenadas na Blockchain a princípio, posto que com os metadados e as templates dos certificados, é sempre possível reconstruir essas imagens, evitando assim o uso excessivo de armazenamento nos nós da rede.

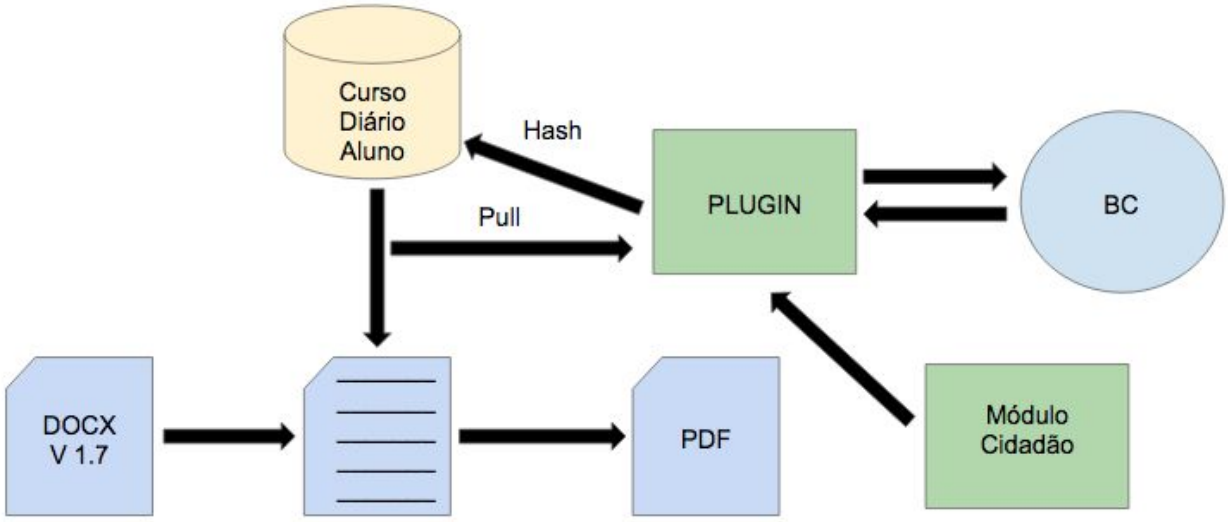

Figura 18 - Arquitetura da Solução ENAP. Fonte: (Elaboração Própria, 2018).

5. CONCLUSÃO

Este projeto propôs uma aplicação baseada na tecnologia Blockchain na emissão de certificados acadêmicos. A proposta contempla aspectos técnicos e do domínio específico, mostrando como característica a escalabilidade e componentização do sistema, permitindo qualquer instituição desenvolver seu próprio módulo cliente em sistemas já usados por esta, e como exemplo, foi desenvolvido um módulo do SUAP, sistema administrativo utilizado pelo IFF.

As tecnologias Eris Industries, Ethereum, Hyperledger, Multichain, Openblockchain e R3 Corda foram estudadas antes do desenvolvimento do protótipo, com uma preocupação maior a respeito do quesito segurança, principalmente abordando detalhamento como suporte à autorização e auditoria. Duas das tecnologias citadas foram escolhidas para a implementação de um protótipo, foram elas: HyperLedger e MultiChain, as outras foram descartadas por diferentes motivos detalhados no capítulo 3 deste trabalho. O desenvolvimento dos protótipos mostrou que a tecnologia HyperLedger seria a mais adequada para atingir os propósitos deste projeto, e uma solução foi desenvolvida baseada nesta tecnologia. Este trabalho detalhou as características e limitações do HyperLedger aplicado ao domínio de interesse, tratando de tópicos como arquitetura do projeto, criação de um modelo, segurança, auditoria, API e integração com uma aplicação cliente demonstrativa.

Integrações do projeto com o IFF e o ENAP foram realizadas, sendo que a integração do IFF atingiu um nível funcional, e a integração com o ENAP se encontra em andamento.

5.1 Limitações

O estudo destacou algumas limitações tecnológicas, alguns pequenos problemas técnicos foram encontrados, mas devido à tecnologia usada estar em constante atualização, os problemas técnicos apresentados neste trabalho se tornam completamente irrelevantes. Outras limitações, referentes ao modelo da tecnologia, como a característica que esta lida com o seu suporte à segurança, foram apresentadas, analisadas, discutidas e finalmente foram encontradas alternativas e soluções para adequamento do projeto baseado nessas limitações.

Cabe dizer, que mesmo este estudo tendo sido focado em duas diferentes implementações de Blockchain, suas características, qualidades, pontos fortes e pontos fracos, o conceito de aplicação da emissão de certificados via Blockchain é mais abrangente do que uma tecnologia escolhida. O conceito de Blockchain é relativamente novo, ainda existem muitas implementações surgindo no mercado e as existentes continuam em constante evolução, assim como o próprio estudo sobre as capacidades e possibilidades de aplicação do Blockchain no cenário acadêmico e em outras inúmeras diferentes áreas.

5.2 Trabalhos Atuais e Futuros

Um possível trabalho futuro é a integração com Certificação Digital e Preservação de Documentos Digitais, cuja aplicação teve discussão iniciada entre ENAP, IFF e UFPB, tendo este trabalho e a proposta apresentada por Costa et al. (2018) como bases para implementação.

Uma recomendação seria experimentar uma abordagem diferente usada neste projeto, isto é, ao invés de oferecer somente uma interface REST para integração com aplicações clientes, estudar se é viável e mais adaptável o desenvolvimento de uma aplicação cliente em comum. Isso pode trazer algumas vantagens como a não necessidade de desenvolvimento de uma aplicação cliente pela instituição, agilizando a implantação do sistema, mas também traz algumas desvantagens, como a falta de customização da solução, sendo necessário os funcionários responsáveis por emitir o certificado usarem uma segunda aplicação administrativa. No caso do IFF, como exemplo, os servidores não poderiam emitir o certificado pelo SUAP, sendo necessário conectar-se a uma outra aplicação.

Outra recomendação de trabalho futuro, já baseada na existência do Blockchain com uma carga de informação considerável, seria a aplicação de técnicas de mineração. Através da informação sobre emissão de certificados de diferentes instituições concentrada em um mesmo repositório de dados, seria possível a aplicação desta técnica, utilizando a informação coletada, possibilitando diferentes estudos e análises que podem ajudar na concepção de diferentes relatórios e na tomada de decisão.

REFERÊNCIAS BIBLIOGRÁFICAS

ACHESON, N. **What is bitcoin?** CoinDesk, 26 jan. 2018. Disponível em: <https://www.coindesk.com/information/what-is-bitcoin>. Acesso em: 2 mar. 2019.

ANTONOPOULOS, A. M. **Mastering Bitcoin: unlocking digital cryptocurrencies**. O'Reilly Media, Inc., 2014.

BITCOIN. **Bitcoinwiki**. Disponível em: <https://en.bitcoin.it>, 2015. Acesso em: 21 mar. 2018.

BITCOIN. **Double-spending**. Disponível em: <https://en.bitcoin.it/wiki/Double-spending>, 2016a. Acesso em: 21 mar. 2018.

BITCOIN. **Proof-of-Stake**. Disponível em: <https://en.bitcoin.it/wiki/Proof_of_Stake>, 2016b. Acesso em: 21 mar. 2018.

BØRRESEN, L.; SKJERVEN, S. **Detecting fake university degrees in a digital world**, 2018. Disponível em: <https://www.universityworldnews.com/post.php?story=20180911120249317>. Acesso em: 2 abr. 2019.

BRASIL OPEN BADGE. **Brasil Open Badge**. Disponível em: <https://www.brasilopenbadge.com.br/site> Acesso em: 28 dez. 2018.

CARDOSO, R.P.; GOYA, D. **Um framework para interoperabilidade de instituições heterogêneas de ensino utilizando Blockchain**. Anais do II Workshop @NUVEM, Universidade Federal do ABC, 2018.

CHANDLER, R. **Smart Contracts: How To Understand Smart Contracts And Be Ahead Of Competition - Learn About The Future Of Blockchain Technology**. Wroclaw: CreateSpace Independent Publishing Platform, 2017.

CHENG, S.; DAUB, M.; DOMEYER, A.; LUNDQVIST, M. **Using Blockchain to Improve Data Management in the Public Sector**. Disponível em <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector>, 2017. Acesso em 15 mar. 2018.

COINMARKETCAP. **Cryptocurrency Market Capitalizations**. Disponível em: <https://coinmarketcap.com>, 2016. Acesso em 22 mar. 2018.

COMPUTERWORLD. **Blockchain privado e público: entenda as principais diferenças.** Disponível em: <https://computerworld.com.br/2018/03/01/blockchain-privado-e-publico-entenda-principais-diferencas/>. Acesso em: 30 out. 2018.

COSTA, R. et al. **Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos.** Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain_SBRC), [S.l.], v. 1, n. 1/2018.

CRANE, F. B. **Proof of Work, Proof of Stake and the Consensus Debate**. Disponível em: <https://cointelegraph.com/news/proof-of-work-proof-of-stake-and-the-consensus-debate>. Acesso em: 2 abr. 2019.

CROOK, P. **Append-only Data Store - FAIMS Mobile Platform User Guide - FAIMS Wiki**. Disponível em: <https://faimsproject.atlassian.net/wiki/spaces/MobileUser/pages/5865632/Append-only+Data+Store>. Acesso em: 13 jan. 2019.

DUARTE, J. **Artigo: A empresa que investe no aprimoramento pessoal de seu empregado**., 2003. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI3115,91041-A+empresa+que+investe+no+aprimoramento+pessoal+de+seu+empregado>. Acesso em: 2 abr. 2019.

GREENSPAN, G. **Private blockchains are more than "just" shared databases | MultiChain**. Disponível em: <https://www.multichain.com/blog/2015/10/private-blockchains-shared-databases/>. Acesso em: 2 mar. 2019.

HOOPER, M. **Top five blockchain benefits transforming your industry**, 2018 Disponível em: <https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/>. Acesso em: 2 abr. 2019.

HOUSLEY R. **Public Key Infrastructure (PKI)**. Disponível em: <http://dx.doi.org/10.1002/047148296X.tie149> John Wiley & Sons, Inc., 2004. Acesso em 22 mar. 2018.

HYPERLEDGER DOCUMENTATION. **About Hyperledger**, 16 set. 2016a. Disponível em: <https://www.hyperledger.org/about>. Acesso em: 20 jan. 2019

HYPERLEDGER DOCUMENTATION. **Introduction — hyperledger-fabric docs master documentation**. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/whatis.html#permissioned-vs-permissionless-blockchains>. Acesso em: 13 jan. 2019b.

HYPERLEDGER DOCUMENTATION. **Membership Service Providers (MSP) — hyperledger-fabricdocs master documentation**. Disponível em: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/msp.html>. Acesso em: 24 fev. 2019c.

IBM. **Open BlockchainIBM Developer**, [s.d.]., 2018 Disponível em: <https://developer.ibm.com/open/projects/open-blockchain/>. Acesso em: 2 abr. 2019

JUNIOR, G. M. A. et al. **BNDES Token: Uma Proposta para Rastrear o Caminho de Recursos do BNDES**. Workshop em Blockchain: Teoria, Tecnologias e Aplicações, (WBlockchain_SBRC), [S.l.], v.1, n.1/2018. Disponível em: <https://portaldeconteudo.sbc.org.br/index.php/wblockchain/article/view/2355>. Acesso em: 30 out. 2018.

KARTHIK, K. **6 Blockchain frameworks to build Enterprise Blockchain & how to choose them? Medium**, 21 jan. 2018. Disponível em: <https://medium.com/hyperlegendary/6-blockchain-frameworks-to-build-enterprise-blockchain-how-to-choose-them-2b7d50ba275c>. Acesso em: 3 abr. 2019

KHATWANI, S. **What is Proof-Of-Work & Proof-Of-Stake?**, 2018. Disponível em: <https://coinsutra.com/proof-of-work-vs-proof-of-stake-pow-vs-pos>. Acesso em: 2 abr. 2019.

KISHIGAMI J., FUJIMURA S., WATANABE H., NAKADAIRA A., AKUTSU A. **The Blockchain-Based Digital Content Distribution System**. IEEE Fifth International Conference on Big Data and Cloud Computing (BDCloud); p. 187–190, 2015.

KONDOR D., PÓSFAI M., CSABAI I., VATTAY G. **Do the rich get richer? An empirical analysis of the Bitcoin transaction network**. PloS one, 9(2):e86197, 2014.

LINK CERTIFICAÇÃO, **Digital. Blockchain x Certificado Digital: Quem vence essa briga?** Disponível em: <https://www.linkcertificacao.com.br/blockchain-e-certificado-digital>. Acesso em 29 dez. 2018.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**, 2008. Disponível em: <http://bitcoin.con/bitcoin.pdf>. Acesso em: 22 mar. 2018.

MARR, B. **A Very Brief History Of Blockchain Technology Everyone Should Read**. Disponível em: <https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/>. Acesso em: 20 jan. 2019.

MICROSOFT AZURE DOCUMENTATION. **O que é computação em nuvem? Um guia para iniciantes | Microsoft Azure**. Disponível em: <https://azure.microsoft.com/pt-br/overview/what-is-cloud-computing/>. Acesso em: 6 jan. 2019.

ROUSE, M. **What is registration authority (RA)? - Definition from WhatIs.com**. Disponível em: <https://searchsecurity.techtarget.com/definition/registration-authority>. Acesso em: 24 fev. 2019.

SÁ, V. **MIT Emite Diplomas na Blockchain**. Disponível em: <https://portaldobitcoin.com/mit-emite-diplomas-na-blockchain-do-bitcoin>. Acesso em: 20 dez. 2018.

SAKHUJA, R. **Hyperledger Fabric & Composer for Blockchain Development**. Disponível em: <https://www.udemy.com/hyperledger/>. Acesso em: 2 mar. 2019.

SHARMA, T. K. **How is Blockchain verifiable by public and yet anonymous?**, 10 jul. 2018. Disponível em: <https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/>. Acesso em: 24 fev. 2019.

SWAN, M. **Blockchain: Blueprint for a New Economy**. O'Reilly Media, Inc., 2015.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World**. [s.l.] Penguin UK, 2016.

THE ECONOMIST. Who is Satoshi Nakamoto? **The Economist**, 2 nov. 2015.

VILNER, Y. **5 Blockchain Product Use Cases To Follow This Year**., 2018. Disponível em: <https://www.forbes.com/sites/yoavvilner/2018/06/27/5-blockchain-product-use-cases-to-follow-this-year/#74506df21b60>. Acesso em: 2 abr. 2019.

YLI-HUUMO, J; KO, D; CHOI, S; PARK, S; SMOLANDER, K. **Where Is Current Research on Blockchain Technology?** A Systematic Review. PLoS ONE, 11(10), 2016.