UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA

BLOCKCHAIN NA GESTÃO DO ACERVO ACADÊMICO DE INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR. UMA PROPOSTA DE IMPLEMENTAÇÃO.

THIAGO MARQUES FERNANDES DE MELLO

JUIZ DE FORA
2023

THIAGO MARQUES FERNANDES DE MELLO

Thiago Marques Fernandes de Mello

BLOCKCHAIN NA GESTÃO DO ACERVO ACADÊMICO DE INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR. UMA PROPOSTA DE IMPLEMENTAÇÃO.

Projeto de dissertação apresentado como requisito parcial para a conclusão do Mestrado Profissional em Administração Pública, da Faculdade de Administração e Ciências Contábeis, Universidade Federal de Juiz de Fora.

Professor orientador:
Prof. Dr. Marcos Tanure Sanábio

JUIZ DE FORA
2023

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Mello, Thiago Marques Fernandes de.
BLOCKCHAIN NA GESTÃO DO ACERVO ACADÊMICO DE INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR: UMA PROPOSTA DE IMPLEMENTAÇÃO. / Thiago Marques Fernandes de Mello. -- 2023.
128 f.

Orientador: Marcos Tanure Sanábio
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Administração e Ciências Contábeis. Programa de Pós-Graduação em Administração Pública em Rede Nacional - PROFIAP, 2023.

1. Admnistração Pública. 2. Blockchain. 3. Documentos. 4. Autenticação. 5. Validação. I. Sanábio, Marcos Tanure, orient. II. Título.

Thiago Marques Fernandes de Mello

Blockchain na Gestão do Acervo Acadêmico de Instituições Federais de Ensino Superior: uma proposta de implementação

Dissertação apresentada ao Mestrado Profissional em Administração Pública da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Administração Pública. Área de concentração: Administração Pública

Aprovada em 29 de agosto de 2023.

BANCA EXAMINADORA

Prof. Dr. Marcos Tanure Sanábio - Orientador
Universidade Federal de Juiz de Fora

Prof. Dr. Fernando Marques de Almeida Nogueira
Universidade Federal de Juiz de Fora

Prof. Dr. Geraldo Magela Jardim Barra
Universidade Federal de São João del-Rei

Juiz de Fora, 31/08/2023.

Documento assinado eletronicamente por **Geraldo Magela Jardim Barra**, **Usuário Externo**, em 31/08/2023, às 13:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcos Tanure Sanabio**, **Professor(a)**, em 01/09/2023, às 06:46, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fernando Marques de Almeida Nogueira**, **Professor(a)**, em 01/09/2023, às 20:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf (www2.ufjf.br/SEI) através do ícone Conferência de Documentos, informando o código verificador **1445170** e o código CRC **D2A1F760**.

RESUMO

O Ministério da Educação (MEC) tem empreendido esforços para aprimorar a eficiência e segurança no processo de emissão de diplomas, certificados e documentos oficiais, incentivando a pesquisa e desenvolvimento de soluções nesse contexto. A tecnologia *blockchain* tem sido cada vez mais mencionada pelo Governo Federal como uma possível ferramenta para modernizar e aperfeiçoar os processos na esfera pública. Essa tecnologia pode ser compreendida como um registro distribuído capaz de garantir a imutabilidade e autenticidade de dados, sem depender de uma autoridade central, e é considerada por muitos autores como uma tecnologia disruptiva, capaz de gerar inovação ao romper com modelos antigos e introduzir novos padrões. Impulsionado por essas premissas, o presente trabalho desenvolveu e implementou uma aplicação que utiliza a blockchain da rede Ethereum para assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico originado de uma Instituição Federal de Ensino Superior (IFES). Foram empregadas as linguagens de programação PHP e Javascript, com auxílio de bibliotecas e ferramentas específicas para a programação de Contratos Inteligentes (*smart contracts*) e conexão com a *blockchain* Ethereum. A eficácia da aplicação foi confirmada por meio da avaliação dos resultados utilizando ferramentas como exploradores de nós. No entanto, os resultados também revelaram que os custos associados à operação podem representar um desafio para a escalabilidade do projeto, o que torna o desenvolvimento de redes *blockchain* privadas *(permissioned blockchains)* pelas organizações públicas uma solução potencialmente mais viável.

Palavras-chaves: Blockchain; Documentos; IFES; Autenticação; Validação.

ABSTRACT

The Ministry of Education (MEC) has made efforts to improve efficiency and security in the process of issuing diplomas, certificates and official documents, encouraging research and development of solutions in this context. Blockchain technology has been increasingly mentioned by the Federal Government as a possible tool to modernize and improve processes in the public sphere. This technology can be understood as a distributed registry capable of guaranteeing the immutability and authenticity of data, without depending on a central authority, and is considered by many authors as a disruptive technology, capable of generating innovation by breaking with old models and introducing new standards. . Driven by these assumptions, this work developed and implemented an application that uses the Ethereum blockchain to ensure the immutability, integrity and availability of an academic collection item originating from a Federal Institution of Higher Education (IFES). The programming languages PHP and Javascript were used, with the help of libraries and specific tools for programming Smart Contracts (smart contracts) and connection with the Ethereum blockchain. The effectiveness of the application was confirmed by evaluating the results using tools such as Node Explorers. However, the results also revealed that the costs associated with the operation can pose a challenge to the project's scalability, which makes the development of private blockchain networks (permissioned blockchains) by public organizations a potentially more viable solution.

Keywords: Blockchain; Documents; IFES; Authentication; Validation.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

BCB	Banco Central do Brasil
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
dApps	Aplicações Descentralizadas
DSR	Design Science Research
DS	Design Science
DETIC	Departamento de Políticas e Programas Setoriais em Tecnologia da Informação
DLT	Distributed Ledger Technology
EVM	*Ethereum Virtual Machine*
FGV	Fundação Getúlio Vargas
ICE	Instituições de Ciências Exatas.
IFES	Instituições Federais de Ensino Superior
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
ITS Rio	Instituto de Tecnologia e Sociedade do Rio.
MEC	Ministério de Educação e Cultura
MD5	Message Digest 5
PF	Polícia Federal
NRC	Núcleo de Recursos Computacionais.
PoS	Proof of Stake
PoW	Proof of Work
RBB	Rede Blockchain Brasil
RNP	Rede Nacional de Ensino e Pesquisa

SEDGG	Secretaria Especial de Desburocratização, Gestão e Governo Digital
SERPRO	Serviço Federal de Processamento de Dados –
SHA-2	*Secure Hash Algorithm* 2
TCU	Tribunal de Contas da União

SUMÁRIO

1. INTRODUÇÃO

Segundo o Censo da Educação Superior do Brasil, organizado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), as instituições de ensino brasileiras possuem anualmente, mais de três milhões de estudantes ingressantes no ensino superior, contabilizando o total de oito milhões de estudantes matriculados nesta modalidade (COSTA *et al*, 2018), por trás desses números existe uma complexa estrutura administrativa, responsável por gerir as atividades de suporte ligadas a docentes e alunos, uma dessas demandas é a emissão e autenticação do acervo acadêmico. As Instituições Federais de Ensino Superior (IFES), bem como todas as Autarquias Federais possuem autonomia no que diz respeito à emissão e autenticação dos seus diplomas e certificados, tal qual está definido na Portaria. Nº 1.095, de 25 de outubro de 2018, e essa natureza distribuída, somado à ausência de normalização dos mecanismos de verificação de validade, acabam gerando problemas de segurança que são explorados por entes mal intencionados.

Outra questão igualmente ligada a segurança, diz respeito à manutenção de forma permanente dos registros, que também é responsabilidade das próprias entidades, desastres naturais ou mesmo a execução errada das rotinas administrativas ou técnicas podem acarretar falhas na conservação desses dados (LEPIANE *et al*, 2019).

O Ministério da Educação (MEC), entendendo a necessidade de modernização das suas rotinas de validação e autenticação do seu acervo acadêmico, e através dos meios que lhe são pertinentes, vem lançando ofensivas que estipulam novas diretrizes, processos e estruturas ligadas aos procedimentos de distribuição e verificação de autenticidade dessas certidões. A principal medida foi a descrita na Portaria Nº 1095, de 25 de outubro de 2018, que dispõe sobre a expedição e o registro de diplomas de cursos superiores de graduação no âmbito do sistema federal de ensino. De acordo com a portaria acima mencionada, a partir de 1º de janeiro de 2022, todas as universidades federais brasileiras precisam emitir diplomas de graduação de forma digital. Essa mudança vem sendo construída desde o ano de 2017, com as diretrizes que estipulavam ambientes de desenvolvimento e testes, além de etapas que deveriam ser cumpridas até o momento da implantação final em ambiente de produção. Nas definições estabelecidas pelo MEC sobre os Diploma Digital, temos que os documentos emitidos pelo sistema deverão ser nato-digitais, ou seja, serão emitidos em ambiente virtual, sem a necessidade da sua versão

impressa, esses documentos serão assinados e validados através da assinatura digital pelo padrão ICP-Brasil com carimbo de tempo. Cada Instituição de Ensino deverá desenvolver um ambiente acessível a qualquer interessado em conferir os dados do diploma, e a sua validação (MEC, 2022).

Os esforços feitos pelo MEC na construção de parâmetros mais maduros e seguros para a emissão do acervo acadêmico pelas IFES, são claramente um passo para a consolidação de uma estrutura mais sólida no combate às fraudes, mas alguns pontos continuam de certa forma descobertos. Como mencionado anteriormente por (LEPIANE *et al*, 2019), a natureza distribuída do processo ainda persiste, já que cada Instituição deve manter um repositório com os dados de cada diploma, essas informações ainda estão suscetíveis a incidentes técnicos ou a desastres naturais que podem causar perda de dados. Um outro detalhe ainda presente no conceito do Diploma Digital, é a presença de uma autoridade central certificadora, intermediando o processo, o tornando mais burocrático e dependente. A adoção da tecnologia conhecida como *blockchain* poderia ser usada para preencher essas lacunas garantindo um processo mais seguro e prático (TCU, 2020).

Segundo Mendanha (2017), a *blockchain* é descrita como um grande livro razão[1], responsável por manter um histórico completo de todas as transações, com data e hora. A informação é replicada e distribuída através dos computadores ligados à rede, portanto, não há um ponto central de controle ou falha. Por meio da criptografia e do poder computacional dos membros da rede, toda transação antes de ser incluída é verificada pelos mesmos participantes, com o objetivo de reconhecer se uma informação maliciosa está sendo transferida. Essa verificação é realizada por meio de provas de consenso, permitindo que as transações sejam feitas de forma segura e rápida.

A utilização da *blockchain* como ferramenta auxiliadora na inovação e melhoria dos processos públicos já é uma premissa do governo federal. De acordo com o Tribunal de Contas da União (TCU), o serviço *blockchain* tem a capacidade de transformar, bem como acelerar uma parcela significativa das atividades desenvolvidas pelo Poder Público. Tais progressos podem ser efetivados pelo fato de que o livro-razão compreende uma estrutura de dados que não é passível de modificação, de maneira que transações são registradas e mantidas de forma permanente e imutável (TCU, 2020). Em 18 de abril de 2022 o Banco Nacional de

[1] O termo livro razão, está ligado à área das ciências contábeis, e é definido como um registro que contém todos os lançamentos contábeis de uma determinada conta patrimonial (Marion, J.C., 1998).

Desenvolvimento Econômico e Social (BNDES) e o TCU assinam acordo de cooperação técnica para criação da Rede Blockchain Brasil (RBB), publicado no Diário Oficial da União, edição de 18 de abril de 2022. De acordo com o TCU, o compromisso é mais uma medida para estimular a tecnologia na administração pública e inicia uma preparação para o uso futuro da tecnologia *blockchain* em ações de controle externo, com o objetivo de trazer mais segurança para atos e contratos da administração pública (TCU, 2022). Ainda sobre a utilização de *blockchain*, mas agora de forma pontual nas IFES, em 14 de fevereiro de 2022, foi assinado entre a Rede Nacional de Ensino e Pesquisa (RNP) e os países membros da Cooperação Latino-Americana de Redes Avançadas, (Equador, México, Guatemala, Uruguai, Costa Rica, Chile, Colômbia, Honduras, Nicarágua) um acordo para o desenvolvimento de um ecossistema *blockchain*, interligando a América Latina (RNP, 2022). De acordo com Andrés Moya, pesquisador de Informática e Computação da Universidade de la Serena, no Chile:

> *Blockchain* irá permitir que as universidades consigam cuidar da identidade digital dos membros de sua comunidade. Ou seja, teremos a segurança e a certeza de que o que estamos construindo tenha validade ou certificação em algum lugar (RNP, 2022).

1.1 Problema de Pesquisa

"O suspeito que promoveu a falsificação utilizou-se de carimbos e assinaturas do Reitor, bem como do Diretor da Universidade Federal de Pernambuco" (BRASIL, 2022a). Essa declaração está incluída em nota disponível no site da Polícia Federal, no portal do Governo Federal, disponibilizada no dia 22 de fevereiro de 2022, e trata-se da venda de diplomas e a falsificação de documentos emitidos por Universidades Federais e privadas.

A informação contida no parágrafo acima representa uma realidade. Em apenas uma operação da Polícia Federal, realizada em abril de 2021, foram presas mais de sete pessoas ligadas à falsificação de diplomas e documentos de universidades públicas e privadas, a autoridade federal estima que milhares de diplomas foram distribuídos pela quadrilha (BRASIL, 2021a).

De fato, mesmo após todas as implementações recentes por parte do MEC, emitir e consultar a autenticidade de um documento ou diploma é um processo por vezes custoso e lento, utilizando um exemplo específico, alunos ou empregadores que estão no exterior e que precisam

verificar a validade de um diploma, seja para a admissão em um cargo de trabalho, ou seja para um processo seletivo, precisam passar por procedimentos que variam conforme o curso ou país, entretanto, de forma geral, devem requerer uma tradução e posteriormente a autenticação e legalização, dessa tradução, geralmente através de um serviço notarial pago, como medida para provar a autenticidade dos seus documentos (BRASIL, 2022b). Porém, com os recentes avanços ligados a ciências da computação e com o desenvolvimento da tecnologia *blockchain*, dotada de características como imutabilidade, descentralização, segurança e rastreabilidade, a sua adoção pode ser uma excelente escolha que vai de encontro às necessidades de incremento dos aspectos de segurança e acessibilidade, permitindo que um diploma ou documento possa ser verificado por qualquer parte interessada, a partir de qualquer lugar do globo, sem a necessidade de um intermediário ou de uma autoridade certificadora (CASTRO, 2021).

Frente ao exposto, entendemos que desenvolver meios para aumentar a segurança, facilitar a autenticidade e disponibilidade de documentos que fazem parte do acervo acadêmico emitidos por IFES, através do desenvolvimento de soluções tecnológicas como, softwares, aplicativos ou outros tipos de sistemas informatizados que adotam a tecnologia blockchain como estrutura de armazenamento e distribuição de dados, é um senso comum por parte do governo federal. A necessidade de modelos de confiança que possam ser desenvolvidos e utilizados como ferramentas práticas de estudo também é uma realidade.

1.2 Objetivo

Nesta seção será apresentado o objetivo geral e quais são os objetivos específicos o qual este Trabalho propõe-se a atingir.

1.2.1 Objetivo Geral

Desenvolver e implementar uma aplicação que utiliza a *blockchain* Ethereum[2] para assegurar a imutabilidade, garantir a integridade, autenticidade e disponibilidade de um documento nato-digital, originado de uma IFES.

[2] A Ethereum é a blockchain utilizada pela criptomoeda Ether. Ela possui características específicas que facilitam a sua adoção para projetos em áreas diferentes às das moedas digitais.

1.2.2 Objetivos Específicos.

1. Descrever a tecnologia blockchain e suas vertentes, listando os principais modelos adotados atualmente.
2. Analisar a trajetória da tecnologia blockchain no governo federal.
3. Analisar os métodos atuais de validação, autenticação e publicidade dos documentos emitidos nas Instituições Federais de Ensino.
4. Descrever as soluções em Blockchain já desenvolvidas ou em desenvolvimento pelas organizações públicas brasileiras.

1.2 Justificativa

Propõe-se a implantação de um sistema de autenticação e disponibilidade de documentos utilizando a tecnologia *blockchain* por meio da construção de uma aplicação descentralizada com a capacidade de fornecer autenticação e publicidade a documentos de IFES. Explorando as principais características da tecnologia: sua existência descentralizada, sua independência da uma autoridade central e sua imutabilidade. Nessa perspectiva, a pesquisa a ser realizada é relevante pelos seguintes aspectos:

1. Devido às suas principais características, a utilização da *blockchain* pode aumentar a eficiência e transparência de sistemas governamentais, se transformando numa ferramenta no combate à corrupção e ineficiência da Administração Pública. É o que afirma o artigo: "*How blockchain can help dismantle corruption in government services"* publicado no Fórum Econômico Mundial (WEF, 2021).
2. Existe um evidente movimento do Governo Federal no sentido de se adotar soluções em Blockchain na Administração Pública. O decreto nº 10.332, assinado pelo presidente da República em abril de 2021 estabelece a criação de uma rede em Blockchain oficial para o Governo Federal, até o final de 2022.
3. Pesquisas e experimentos utilizando Blockchain, são estimuladas pelo Governo Federal. Como exemplo temos o acórdão 1613/2020 do Tribunal de Contas União (TCU), que determinou à Secretaria Especial de Desburocratização,

Gestão e Governo Digital (SEDGG) do Ministério da Economia e a outros órgãos que atentem para a necessidade de realizar estudo de viabilidade e de verificar desafios, riscos e oportunidades das Tecnologias Blockchain.

4. A adoção do Governo Federal da utilização de Blockchain nas soluções de demandas de controle e disponibilidade de informações já se iniciou, porém, a quantidade de ferramentas implementadas e disponíveis à sociedade ainda são tímidas, atualmente o Governo Brasileiro possui apenas duas aplicações oficiais que utilizam a tecnologia blockchain, a bConnect e a b-CNPJ.

1.3 Organização do Texto

O primeiro capítulo tem como foco apresentar uma contextualização do tema de pesquisa, situar a problematização e o problema de pesquisa da investigação, apontar os objetivos do estudo bem como a justificativa e relevância da realização deste projeto de mestrado. Sendo assim, trata-se da introdução do estudo. O segundo capítulo corresponde à fundamentação teórica. Neste capítulo, serão apresentados autores que definem, caracterizam e discutem temas relevantes para o objeto do estudo a partir do enquadramento teórico-conceitual determinado para compor esta etapa da pesquisa.

No terceiro capítulo ocorre a apresentação do método de pesquisa, nele serão explicados as metodologias e técnicas utilizados para o desenvolvimento da pesquisa. O *Design Science* foi escolhido como paradigma epistemológico para a condução do nosso trabalho e como a sua utilização ainda não é amplamente conhecida, alguns conceitos sobre a metodologia serão apresentados. Posteriormente, são descritas as etapas da pesquisa, utilizando o *Design Science Resource* como método discorrendo acerca dos instrumentos e técnicas utilizadas para coletar, analisar e produzir os resultados.

No quarto capítulo, abordaremos o procedimento de desenvolvimento do artefato, as ferramentas empregadas nesse processo, bem como a simulação e a coleta de dados relacionados à utilização do referido artefato. Além disso, serão discutidos e apresentados os resultados obtidos nessa etapa.

Por fim, no capítulo final, serão apresentadas as conclusões alcançadas por meio da análise dos resultados, com a compilação e apresentação do conhecimento gerado durante o

processo de criação da ferramenta. Ainda, compõe o trabalho o Referencial e Apêndices anexados ao final.

REFERENCIAL TEÓRICO

Com o intuito de fundamentar a presente pesquisa, o referencial teórico foi estruturado de forma segmentada. O tópico 2.1 diz respeito às definições e diretrizes do MEC com relação a emissão e manutenção do acervo acadêmico pelas Instituições de Ensino Superior (IES), no tópico 2.2 um estudo sobre os eventos e citações ligadas à *blockchain* feitas pelo Governo Federal é apresentado, e a partir do tópico 2.3 vão ser demonstrados os conceitos ligados à tecnologia *blockchain*, como criptográfica, funções *hash*, certificado digital, provas de consenso entre outros.

2.1. Acervo Acadêmico

De acordo com a portaria MEC nº 315, de 4 de abril de 2018, o acervo acadêmico é composto pelo conjunto de documentos produzidos e recebidos por instituições de ensino superior públicas e privadas, ligadas ao sistema federal de ensino, referentes à vida acadêmica do estudante.

Esse acervo engloba qualquer documento que gere um rastro do aluno, não só os que se relacionam à parte pedagógica, a documentação relativa ao FIES, ou mesmo atestados médicos apresentados pelo estudante são exemplares que fazem parte do acervo. A tabela contendo todos os documentos e outras informações como o tempo de armazenamento de cada item pela instituição de ensino, podem ser encontradas no apêndice A, do presente trabalho.

A construção do conceito de acervo acadêmico, vem sendo pavimento pelo Governo Federal nas últimas décadas, nos próximos parágrafos faremos uma breve análise sobre esse processo.

Embora o termo acervo acadêmico não seja encontrado explicitamente no texto, podemos afirmar que o seu conceito está identificado na portaria nº 255 de 20 de dezembro de 1990, nela o Governo Federal, após o questionamento por parte de Instituições de Ensino Superior, públicas e privadas, sobre os procedimentos ligados ao arquivamento e inutilização de documentos, estabelece uma série de critérios que precisavam ser observados. Esses critérios formavam uma um conjunto de normas básicas e delimitavam de forma nominal explicita

apenas alguns itens, utilizando termos generalistas como “documentação do aluno” para todos os outros.

Em 2011, através da portaria AN/MJ nº 92, de 23 de setembro, foi estabelecida a Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos às Atividades-Fim das Instituições Federais de Ensino Superior (IFES), essa tabela contém uma relação de cerca de 500 tipos de documentos ligados à atividade fim das Instituições de Ensino Superior, cada item representa um tipo de documento, e o período o qual ele deverá ser mantido pela instituição. A criação da Tabela de Temporalidade e Destinação de Documentos relativos às Atividades-Fim das IFES, foi um passo relevante na formação de políticas mais consistentes ligadas à gestão do acervo acadêmico. A Tabela se encontra no APÊNDICE A, deste trabalho

Em 2013, o Governo Federal delibera a portaria 1.224/2013 contendo inúmeros avanços ligados à gestão do acervo acadêmico: a ampliação da classificação e destinação de documentos, à definição de sanções pelo não cumprimento das normas, a criação da figura do Depositário do Acervo Acadêmico (DAA) que junto ao representante legal da instituição, são responsáveis pela manutenção e guarda do acervo, são algumas dessas inovações.

Em análise feita através nota técnica conjunta, a Secretaria de Regulação e Supervisão do Educação Superior (SERES) e o Instituto Nacional de Estudos e Pesquisa Educacionais Anísio Teixeira INEP/MEC foi concluído que implementação da Portaria nº 1.224/2013 busca, atender aos imperativos constitucionais de melhoria dos padrões de qualidade da educação, em benefício dos alunos e da sociedade em geral, em cumprimento à missão do Ministério da Educação como órgão público responsável pela educação superior.

> A Portaria nº 1.224/2013 procurou sanar uma lacuna de vinte e três anos sem orientações específicas quanto à gestão do acervo acadêmico das IES, desde que havia sido publicada a Portaria nº 255 do MEC, de 20 de dezembro de 1990, que disponibiliza orientações básicas para o arquivamento de documentos referentes às atividades dos estabelecimentos de ensino. Tais orientações, com o passar dos anos, tornaram-se ultrapassadas, uma vez que foram elaboradas antes mesmo da Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos), que cunhou o conceito de gestão de documentos na legislação brasileira. (LIMA; SEIFFERT; SCHÄFER, 2019)

O Decreto Nº 9.235, de 15 de dezembro de 2017 é o considerado o novo marco regulatório da educação superior e dispõe sobre o exercício das funções de regulação,

supervisão e avaliação das instituições de educação superior e dos cursos superiores de graduação e de pós-graduação no sistema federal de ensino, o decreto traz uma série de mudanças alterando antigas diretrizes e acrescentando uma série de novas medidas referente ao Ensino Superior no Brasil.

De acordo com análise conduzida pelo Sindicato das Mantenedoras de Ensino Superior, o decreto Nº 9.235, carrega na sua essência a preocupação de se utilizar de artifícios tecnológicos durante os processos (SEMESP, 2018).

Com relação ao acervo acadêmico, tema dessa sessão, é possível identificar no texto um item relevante, no seu Art. 104 está definido que os documentos que compõem o acervo acadêmico das IES na data de publicação deste Decreto serão convertidos para o meio digital, mediante a utilização de métodos que garantam a integridade e a autenticidade de todas as informações contidas nos documentos originais, nos termos da legislação. O prazo para e as condições para que as IES e suas mantenedoras convertam os seus acervos será definido em regulamento a ser editado pelo MEC. A Portaria também estabelece que essa transição seja feita a partir do uso de tecnologias que garantam a integridade, a autenticidade, a confiabilidade e a duração da informação no meio digital

No ano de 2020, a Portaria Nº 332, os documentos e as informações que compõem o acervo acadêmico, independente da fase em que se encontrem ou de sua destinação final, conforme Código e Tabela aprovados pela Portaria AN/MJ nº 92, de 2011, deverão ser convertidos para o meio digital, no prazo de quarenta e oito meses,

Em 2022, o Governo Federal através da portaria nº 360 que está em vigor desde o dia 18 de maio instituiu que a partir de 1º de agosto de 2022, nenhuma Instituição de Ensino Superior pertencente ao Sistema Federal de Ensino, poderá produzir material integrante do acervo acadêmico de forma física. A mudança pode ser compreendida como a peça final no processo de digitalização do acervo acadêmico, pois a partir da data estabelecida no decreto, além da obrigatoriedade de digitalização de todos os documentos do acervo, fica vedado a produção de material físico, ou seja, todos os próximos documentos gerados pelas IES, deverão ser do tipo nato-digital.

Através da análise feita a partir dos dados detalhados acima, é possível reconhecer um padrão de amadurecimento dos processos ligados à Gestão de Documentos, com estímulo evidente à adoção de novas tecnologias e da utilização de sistemas de informação.

É interessante salientar que os procedimentos de conservação e preservação do acervo digital ainda serão regulamentado em ato específico ainda não definidos pelo Governo Federal (BRASIL, 2022c), e portanto a experimentações de novas técnicas e metodologias ligadas à conservação e preservação dos documentos digitais do acervo acadêmico, e com a observância dos princípios de integridade, a autenticidade, a confiabilidade dispostos no Art. 104 podem indicar a melhor solução a ser adotada na regulamentação.

2.2. Blockchain e sua trajetória no Governo Federal.

De acordo com as pesquisas realizadas em ferramentas de busca externas e internas do Governo Federal, as primeiras manifestações do Governo relacionadas à tecnologia blockchain aconteceram em 2016. Neste ano, o Banco Central do Brasil (BCB) criou um Grupo de Trabalho Interdepartamental com o objetivo de acompanhar inovações tecnológicas digitais e seus impactos nos sistemas financeiro e de pagamentos. Uma das tecnologias digitais acompanhadas é a *blockchain.*

Em 2017, foi possível identificar três referências, a primeira se encontra no Relatório de gestão do exercício de 2017 do Ministério da Ciência, Tecnologia e Inovações, mais especificamente das atribuições do Departamento de Políticas e Programas Setoriais em Tecnologia da Informação (DETIC).

> Especificamente quanto a temas cibernéticos, o DETIC dedicou-se ao acompanhamento de tecnologias digitais e análise de seus impactos, tais como inteligência artificial, blockchain, algoritmos, big data, entre outros, bem como à formulação de proposta de visão estratégica para lidar com a economia digital, promovendo inclusive cooperação internacional quanto a esses tópicos (MCTI, 2018 pag. 79)

Ainda em 2017, o Banco Central confecciona o estudo: "*Distributed Ledger Technical Research in Central Bank of Brazil"*, o documento explora a capacidade do blockchain na emissão de moedas eletrônicas nacionais, plataformas de gerenciamento de identidades e sistemas de transações capazes de substituir os atuais, de acordo Dubard (2021), desde 2016 o Banco Central do Brasil analisa o potencial da tecnologia blockchain, desse modo, o documento desenvolvido é produto desses estudos.

Um artigo disponibilizado pela Serpro[3] detalha o sucesso de alguns países como a Estônia e Dubai na utilização da tecnologia blockchain. Ele lista também alguns pontos que podem ser beneficiar com a implementação da blockchain:

1. Criar identidades digitais on-line para realização de serviços públicos na modalidade de autosserviço.
2. Desenvolver plataformas digitais de votação que possibilitaram o voto em trânsito para todos os cargos ou mesmo o voto por meio de um smartphone.
3. Desburocratizar serviços de registros públicos (certidão de nascimento, patente, registro de veículo etc.) e do sistema notarial brasileiro.
4. Dar transparência e rastreabilidade aos processos licitatórios.
5. Agregar segurança a novos serviços baseados em Internet das Coisas.
6. Automatizar a operação aduaneira, dando mais agilidade aos portos brasileiros.
7. Promover inovações no agronegócio por meio de certificados e rastreabilidade ao longo de toda cadeia produtiva.
8. Permitir que dados médicos como prontuários, receitas, cartão de vacinas, entre outros, sejam digitalizados e fiquem disponíveis para toda rede, mas com o acesso controlado pelo paciente (LIMA, 2017).

Em 2018, a regulamentação da tecnologia blockchain para certificar transações virtuais começa a ser discutida pela Comissão de Ciência e Tecnologia, Comunicação e Informática na Câmara dos Deputados, especialistas ligados ao Serpro, e ao Instituto Nacional de Tecnologia da Informação (ITI), participaram das discussões (BRASIL, 2018). Neste mesmo ano aconteceu a primeira edição do Fórum BlockchainGov promovido pelo BNDES com o tema: Contribuições da blockchain para a transformação digital dos governos (BLOCKCHAINGOV, 2018).

Já no ano 2019, o Serpro junto à Receita Federal do Brasil desenvolve o primeiro protótipo de blockchain do governo federal, ela recebe o nome de bConnect solução que utiliza tecnologia blockchain para garantir a autenticidade das informações compartilhadas entre

[3] O Serviço Federal de Processamento de Dados - Serpro é uma empresa pública vinculada ao Ministério da Fazenda. Foi criada no dia 1º de dezembro de 1964, pela Lei nº 4.516, com o objetivo de modernizar e dar agilidade a setores estratégicos da Administração Pública brasileira (SERPRO, 2018).

Brasil e países parceiros, neste mesmo ano o bConnect inicia a sua fase de testes (BCONNECT, 2019).

Também em 2019 aconteceu o II Fórum BlockchainGov, um evento sobre a tecnologia *blockchain* promovido pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) em parceria com o Instituto de Tecnologia e Sociedade do Rio (ITS Rio). De acordo com a organização, o evento é focado nos principais desafios para que a tecnologia *blockchain* passe a ser um dos pilares de aceleração da transformação digital dos governos. (BLOCKCHAINGOV, 2019).

O ano de 2020 foi marcado por manifestações mais consistentes do Governo Federal relativas à blockchain, no Decreto Nª 10.332, de 28 de abril de 2020, onde se instituiu a Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal, o termo *blockchain* aparece pela primeira vez, e é listado como um dos objetivos que irão nortear a transformação do governo por meio do uso de tecnologias digitais, de acordo com ANEXO do Decreto N° 10.332 fica definido:

> Objetivo 8 - Serviços públicos do futuro e tecnologias emergentes 8.3. Disponibilizar, pelo menos, nove conjuntos de dados por meio de soluções de blockchain na administração pública federal, até 2022.8.4. Implementar recursos para criação de uma rede blockchain do Governo federal interoperável, com uso de identificação confiável e de algoritmos seguros (BRASIL, 2020).

Em agosto de 2020 e estimuladas pelo Decreto Nº 10.332 o Governo Federal lança uma página exclusiva no portal do Governo Digital, sobre *blockchain*, contendo algumas informações básicas sobre a tecnologia, e listando as suas possibilidades de aplicação e casos de uso. Em novembro foi publicado no Diário Oficial da União (DOU) o Decreto 10.550/2020, que altera o regulamento aduaneiro e inclui a hipótese de utilização da tecnologia de *blockchain* nas operações de comércio exterior, pavimento o caminho legal para que o bConnect comece a validar documentos de importação e exportação. No mesmo ano o TCU publica o documento intitulado Levantamento da Tecnologia Blockchain, a publicação de acordo com o TCU (TCU, 2020), tem o intuito de compreender o que são as tecnologias *blockchain* e de livros-razão distribuídos (*Distributed Ledger Technology* - DLT), assim como analisar o potencial e as incertezas dessas tecnologias para os serviços digitais do governo.

No início de 2021, o governo federal anunciou a adoção completa da tecnologia blockchain no Portal Único de Comércio Exterior, o Siscomex, por meio do sistema bConnect, desenvolvido pela Serpro. De acordo com o Governo o bConnect será o espaço de armazenamento de procedimentos, normas e estatísticas sobre transações internacionais de bens e prestações de serviço (THOMSONREUTERS, 2021). Em abril de 2021 o Governo Federal lança o sistema baseado em blockchain b-CNPJ, desenvolvido pela Empresa de Tecnologia e Informações da Previdência (Dataprev) com objetivo de simplificar o processo de fornecimento dos dados armazenados na base de dados do Cadastro Nacional da Pessoa Jurídica (CNPJ) (BRASIL, 2021b).

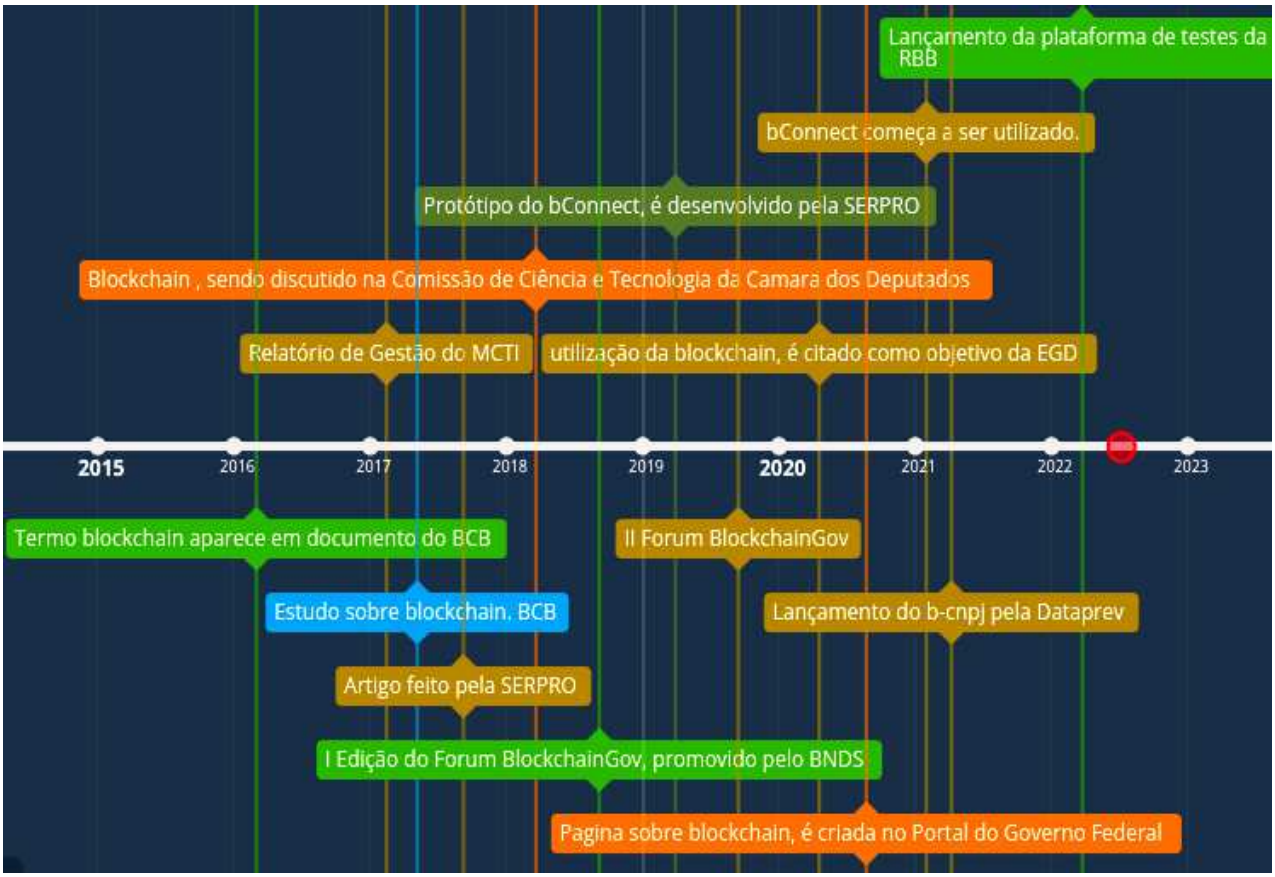
O lançamento em caráter experimental da chamada Rede Blockchain Brasil (RBB), em 2022, uma rede pública sem fins lucrativos, com previsão de implantação efetiva em 2023. De acordo com o TCU:

> A Rede Blockchain Brasil (RBB) funcionará como uma base de dados pública, com o armazenamento de informações em blocos encadeados de forma sequencial. Para que os documentos sejam aceitos na rede, deve haver consenso entre as partes e, uma vez publicados, não podem ser modificados nem deletados, garantindo segurança e integridade dos dados. (TCU, 2022)

Uma observação interessante é que a declaração do TCU sobre a RBB, se confunde com a própria definição original da tecnologia *blockchain*.

Os dados expostos nesta seção, mostram que o Governo Federal a partir de 2016 começou a demonstrar interesse e se aproximar de forma mais efetiva da tecnologia blockchain, e que a participação de empresas estatais como a Serpro e a Dataprev, são de fundamental importância no fomento da utilização e desenvolvimento de tecnologias. O lançamento experimental da RBB também merece destaque, mas a aceitação e utilidade só poderá ser avaliada a partir da sua implantação em ambiente de produção, anunciado para 2023. Os eventos relevantes ligados à tecnologia blockchain no governo federal estão representados através da linha de tempo da Figura 1.

Figura 1: Trajetória da blockchain no governo federal.



Fonte: Autor

2.3 Conceitos e Técnicas

A partir deste item, são apresentadas a definição da tecnologia blockchain, e a história do seu desenvolvimento. Além disso, serão expostos os conceitos e métodos que compõem a sua estrutura.

2.3.1 Blockchain

De acordo com Nofer *et al* (2017), no seu artigo "*Blockchain* A *Disruptive Technology"*, a tecnologia *blockchain* vem atraindo a atenção de forma massiva da comunidade

acadêmica tal como do setor industrial, e o seu advento vem fomentando o desenvolvimento de novos projetos nas mais diversas áreas.

Diversos autores definem e categorizam a *blockchain* como uma tecnologia disruptiva, com a capacidade de causar alterações substanciais nos processos, nas tecnologias e nos modos pelos quais realizamos atividades em nosso dia a dia (REYNA *et al*, 2018).

Em seu trabalho, o pesquisador da Fundação Getúlio Vargas (FGV) Eduardo Henrique Diniz afirma:

> Dado o envolvimento de pessoas e empresas de vários segmentos e o leque de possibilidades, não há como não considerar que a tecnologia blockchain tem elementos para provocar o maior impacto na sociedade e no mundo dos negócios desde o aparecimento da World Wide Web no início dos anos 1990. Assim sendo, estamos assistindo à emergência de uma nova tecnologia disruptiva que, como a web, transformou o mundo de modo irreversível (DINIZ, 2017, p.50).

A *blockchain* é descrita como um grande livro registro[4] por Satoshi Nakamoto, no seu icônico e único trabalho *A Peer-to-Peer Electronic Cash System,* o *White Paper* do Bitcoin. Este livro registro pode ser compreendido como uma estrutura de banco de dados com características particulares, e sua inovação fundamental reside no fato de que tais registros possuem uma natureza descentralizada, ou seja, várias instâncias interligadas dessa estrutura estão dispersas em diferentes localidades (HABER, STORNETTA, 1991).

Ainda sobre a característica descentralizada, temos que sistemas que são baseados em *blockchain* são capazes de trabalhar de maneira distribuída envolvendo múltiplos agentes de forma independente, e se estruturando de forma coletiva em uma grande rede cooperada e compartilhada, sem uma autoridade ou hierarquia definida, essa seria a grande diferença entre uma estrutura baseada em *blockchain*, com os modelos do tipo cliente-servidor já consolidados e utilizados em grande escala atualmente (NAKAMOTO, 2008).

Um outro ponto presente na tecnologia *blockchain* diz respeito à imutabilidade de informações registradas. Os registros adicionados a uma *blockchain*, não podem ser modificados ou apagados. Através de uma cadeia de blocos que são ligados entre si por meio

[4] A palavra "ledger" foi utilizada por Nakamoto no seu artigo que popularizou a blockchain (NAKAMOTO, 2008), esse termo é encontrado em trabalhos em língua portuguesa como livro razão, livro registro, ou por vezes a palavra original no inglês é utilizada.

de chaves criptográficas que são calculadas utilizando o próprio conteúdo da informação a ser adicionada concatenada à informação contida no bloco anterior, cada nova informação é adicionada ao final do bloco e recebem um carimbo temporal. Esses imensos blocos são armazenados de forma distribuída e descentralizada sem uma autoridade ou estrutura hierárquica definida (NAKAMOTO, 2008).

Quanto a autenticidade das informações, temos que a confirmação de que cada inclusão de dados dentro do bloco só pode ser realizada por um usuário possuidor de uma chave privada, partindo de um endereço público para outro, o que garante a autenticidade da informação. (NOFER *et al*, 2017).

Se faz interessante notar que não existe um tipo específico de dados a ser persistido em uma blockchain, a adoção da tecnologia pelo setor financeiro, podem levar-nos à crença de que apenas dados ligados a transações monetárias podem ser guardados em uma *blockchain*, porém compartilhamento de qualquer tipo de informação, textos, imagens, sons e vídeos, podem ser armazenados na sua estrutura.

2.3.2. Uma breve história da blockchain

Satoshi Nakamoto, em 2008, publicou um trabalho intitulado "*Bitcoin: A Peer-To-Peer Electronic Cash System*", em tradução livre: "Bitcoin: Um sistema de pagamentos ponto a ponto", o trabalho de Nakamoto, possui apenas oito páginas e foi escrito seguindo o rigor acadêmico exigido para a publicação de artigos, entretanto ele foi distribuído através de uma lista de e-mail de discussões sobre criptografia. O seu conteúdo descreve um sistema de pagamento por meio eletrônico que podia ser implementado sem a intermediação ou interferência de uma instituição financeira, ou seja, as remessas de valores poderiam seguir diretamente de um usuário a outro (NAKAMOTO, 2008).

A criptomoeda mais conhecida hoje, a Bitcoin, foi a primeira implementação do conceito descrito por Nakamoto, após isso o termo criptomoeda acabou sendo usado para definir todas as redes e sistema de transferências de valores que utilizam esse esquema de criptografia para assegurar as transações, se diferenciando das moedas corriqueiras que utilizam uma instituição financeira centralizada para confirmar as operações (IANSITI e KARIM, 2017).

O Bitcoin popularizou a *blockchain*, gerando a alguns, a sensação de que a tecnologia havia sido desenvolvida pelo mesmo criador do Bitcoin (NOFER *et al*. 2017), mas a verdade é que o desenvolvimento do conceito *blockchain* remete aos anos 70 (ASTE *et al*, 2017).

Merkle elaborou no final dos anos 70 um conceito de estrutura de dados através do uso de códigos criptografados conhecidos como *hashes*, concatenados em um arranjo em formato de árvore, que tinham como objetivo, realizar uma espécie de assinatura digital que foram nominados como *Merkle Tree,* ou em português Árvore de Merkle, (MERKLE, 1987). A árvore de Merkel é um dos principais componentes da estrutura de uma *blockchain*. (NAKAMOTO, 2008);

No ano de 1991, dois pesquisadores, Stuart Haber e W. Scott Stornetta. no seu trabalho "*How to Timestamp a digital Document*", com o objetivo de evitar que documentos digitais fossem alterados ao longo do tempo (PADMAVATHI, 2021), desenvolveram uma estrutura em formato de cadeias de blocos, essa estrutura é o que nós conhecemos atualmente por blockchain, sua relevância é tamanha no trabalho de Nakamoto, que três das dez referências bibliográficas utilizadas, estão ligadas aos trabalhos de Haber e Stornetta (NOFER *et a*l. 2017).

Em 1992, o matemático Dave Bayer se juntou a Haber e Stornetta e incorporaram as árvores Merkle ao projeto inicial de 1991, o que melhorou sua eficiência ao permitir que vários documentos fossem coletados em um único bloco. (BAYER *et al*, 1993)

Em 2008, Satoshi Nakamoto tornou público o *White Paper* do Bitcoin, utilizando os conceitos de Haber, Stornetta e Bayer, como base para o seu projeto, e trazendo aplicação prática às construções teóricas ligadas ao *blockchain* e a colocando em destaque.

2.3.3. Tipos De Blockchain

De acordo com Turkanovic *et al*, (2018) existem três tipos diferentes de redes Blockchain: pública (*permissionless*), privada (*permissioned*) ou consórcio, também chamada de híbrida.

Nas redes públicas qualquer ente pode se ligar a rede e através da sua chave privada, sendo possível enviar ou verificar as informações contidas nos blocos, o número de nós conectados à rede não pode ser definido com exatidão e sua estrutura é dinâmica, ou seja, um nó pode se ligar ou desligar a rede sem nenhum tipo de autorização ou manifesto. Exemplos

clássicos de redes *blockchain* públicas são as redes Bitcoin e a Ethereum. (BELOTTI *et al*, 2019).

Uma blockchain privada (*permissioned*), possui regras que são implementadas de acordo com a necessidade e interesse do negócio, dispositivos de controles sobre quem pode se conectar à rede e se tornar um nó podem ser implementados, informações podem ser enviadas ou consultadas por usuários específicos, e mecanismo de consenso para controle da rede podem ser implantados ou modificados, essas são redes indicadas para uso corporativo ou governamental, um exemplo de rede privada é a RBB em desenvolvimento pelo Governo Brasileiro (BASHIR, 2017).

E, por fim, temos as redes híbridas que propõem oferecer propriedades da rede pública e da rede privada ao mesmo tempo (TURKANOVIC *et al*, 2018).

2.3.4. Criptografia

De acordo com Simmons (1979), o objetivo fundamental da criptografia, palavra derivada do grego que significa "Escrita Oculta" é fazer com que duas ou mais entidades possam se comunicar através de um canal seguro de uma maneira em que um terceiro indivíduo não consiga entender ou decifrar a mensagem que foi transmitida. Essa definição, ainda de acordo com o autor, está ligada ao conceito clássico de criptografia.

Francese (2008), afirma que a criptografia é historicamente dividida em dois períodos: a clássica, intervalada entre 100 a.c. e a Segunda Guerra Mundial; e a criptografia moderna, compreendida desde o período pós-guerra até os dias atuais.

A criptografia moderna trabalha com objetivos mais sofisticados do que a criptografia clássica, que para alguns autores é considerada uma arte (DENNING, 1982). Hoje, o grande foco da criptografia além de obviamente "esconder" informações nas comunicações entre entes é garantir a integridade dos dados e garantir também o intercâmbio seguro de chaves secretas, públicas e privadas entre os envolvidos.

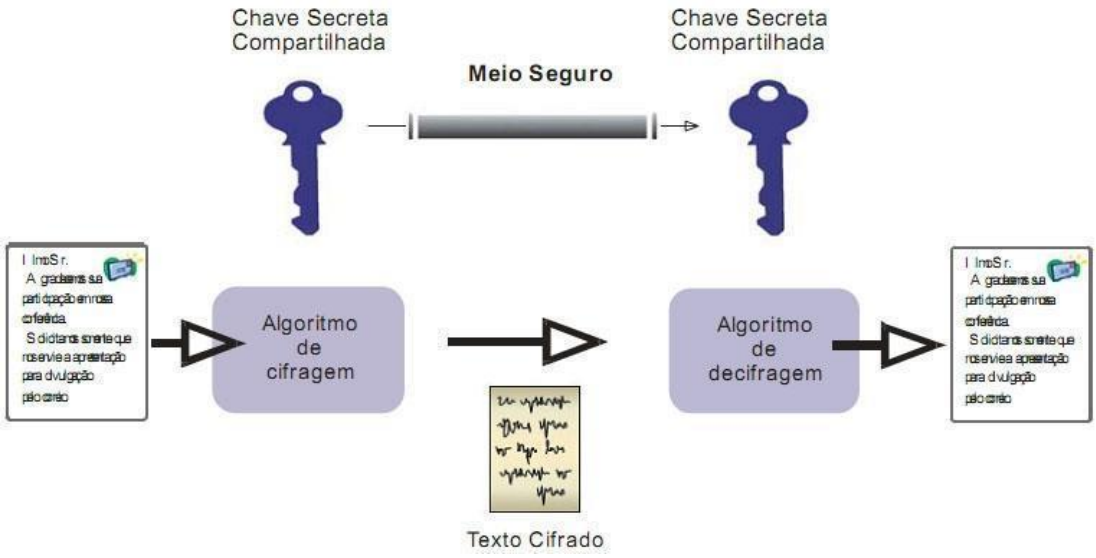
De acordo com Cohen (1995), existem dois tipos de algoritmos criptográficos: a simétrica e a assimétrica.

Na criptografia simétrica, uma mesma chave é utilizada para criptografar e descriptografar uma mensagem, portanto tanto o emissor quanto o destinatário precisam

conhecer essa chave, o que nos leva a conclusão de que assegurar que essa chave não foi comprometida é extremamente importante para a segurança do processo (FAULKNER, 2016). O tamanho da chave usada pode variar de acordo com o sistema utilizado, e a mensagem pode ser criptografada *bit* a *bit*, ou em blocos de *bits*, na maioria das vezes em blocos de 64 bits por vez (FRANCESE, 2008).

O Processo de criptografia utilizando chave simétrica, é representado na Figura 2.

Figura 2: Processo de criptografia com chave simétrica.



Fonte: Alcarás (2010)

De acordo com Oliveira (2012), um dos principais pontos a serem observados nos algoritmos de chaves simétricas, é que a sua implementação não é capaz de preencher algumas lacunas:

1. Como cada par necessita de uma chave para se comunicar de forma segura, para um uma rede de n usuários precisaríamos de algo da ordem de n2 chaves, quantidade esta que dificulta a gerência das chaves;
2. A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido;
3. A criptografia simétrica não garante os princípios de autenticidade e não-repudiação.

Ainda no seu trabalho, Oliveira (2012) afirma também que os principais sistemas de criptografia simétrica utilizados são: AES, Blowfish, DES, IDEA, RC4, Skipjack e o DES.

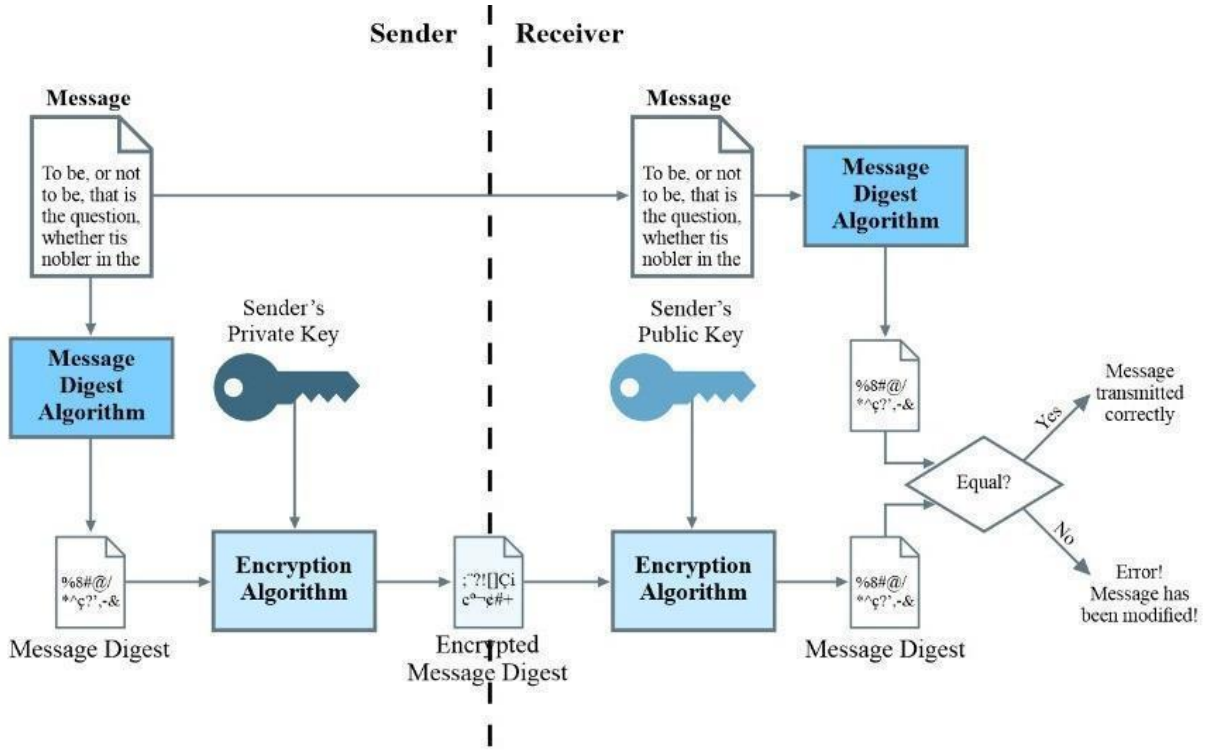
O comprimento da chave utilizada exerce um impacto direto na segurança de um sistema criptográfico simétrico. É incontestável que quanto mais extensa a dimensão da chave, maior será o conjunto de senhas distintas admitidas. Por conseguinte, a segurança é substancialmente ampliada. Essa ampliação se justifica pelo fato de que os ataques dirigidos aos algoritmos simétricos, em sua maioria, se valem da abordagem de força bruta. Em outras palavras, múltiplas combinações de chaves são exaustivamente testadas até que a chave correta seja identificada e, consequentemente, a mensagem cifrada seja desvelada. (COHEN, 1995)

Por ser mais intuitiva, a criptografia simétrica era a única forma conhecida até meados da década de 1970. Ela possui vantagens que ainda a fazem ser utilizada até hoje, como a velocidade na codificação e decodificação. Ela também é vantajosa quando a troca de chaves secretas não é um problema (FRANCESE, 2008).

Já os algoritmos de chaves assimétricas também conhecido como algoritmos de chave pública, foram propostos em 1976 por Diffie e Hellman, causando uma revolução no campo da criptografia, a proposta era utilizar um par de chaves para cifrar e decifrar uma mensagem, uma chave seria pública, que poderia ser distribuída livremente e outra privada que deveria ser mantida em segredo. O funcionamento é de fácil entendimento, uma mensagem cifrada pela chave privada pode ser decifrada pela pública e uma mensagem cifrada pela pública pode ser decifrada pela privada.

Na Figura 3, podemos observar como as chaves assimétricas podem ser usadas para garantir a integridade e a autenticidade de uma mensagem.

Figura 3: Garantindo a integridade de uma mensagem utilizando chaves assimétricas.



Fonte: Adaptada com base em Sotomayor (2005)

A chave pública é gerada utilizando-se a chave privada, e o processo inverso, ou seja, obter uma chave privada através da sua chave pública é computacionalmente inviável até o presente momento (MARTINS, 2018).

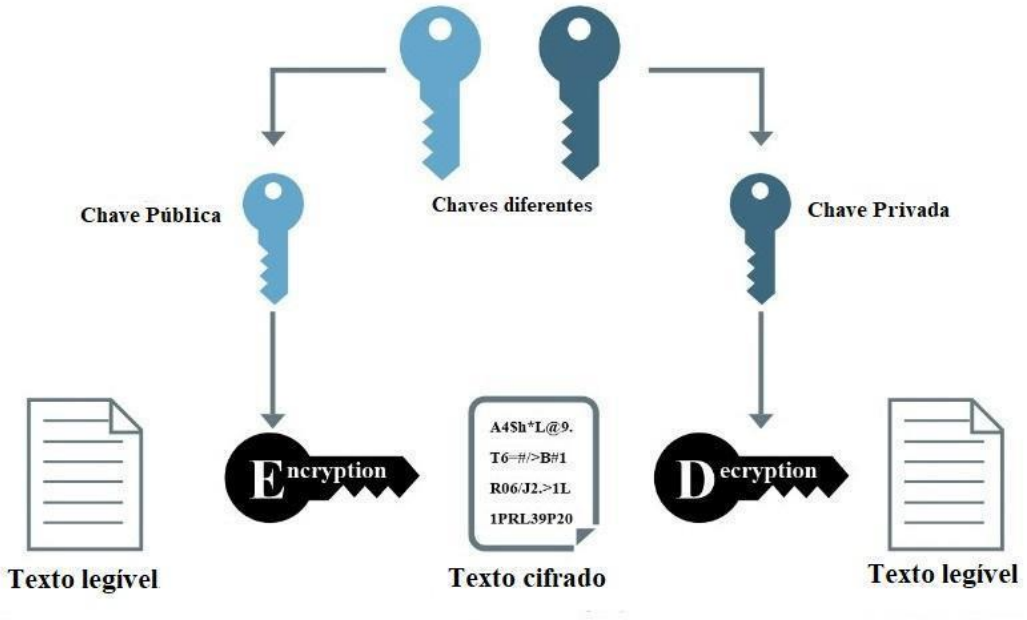
De acordo com Meyer (2011), um dos pontos interessantes do algoritmo de criptografia assimétrica é que uma chave pública pode ser distribuída livremente, e uma comunicação segura pode ser estabelecida entre um par apenas utilizando essa chave pública.

Oliveira detalha de forma resumida e bastante lúdica como se dá a utilização da criptografia assimétrica com o objetivo de proteger uma mensagem que será enviada pela internet.

> *A chave privada deve ficar em posse de cada indivíduo, em segredo. Já a chave pública, deve ser disponibilizada na Internet. É através da chave pública que o indivíduo recebe a mensagem, e a partir de sua chave privada, a mensagem é descriptografada. Portanto, qualquer pessoa que possuir a chave privada de uma chave pública será capaz de ler a mensagem enviada ao endereço público (OLIVEIRA, 2012.).*

Na Figura 4, temos a ilustração do processo descrito por Oliveira (2012).

Figura 4: Confiabilidade no envio de mensagens utilizando chaves assimétricas.



Fonte: Adaptado com base em Jallouli (2017).

Os algoritmos de criptografia assimétrica na maioria das vezes são mais lentos do que os algoritmos simétricos, porém eles são utilizados em conjunto com a técnica de algoritmo simétrico. Essa técnica combinada funciona da seguinte forma: O remetente gera uma chave simétrica, que é criptografada pela chave pública do destinatário e a envia, portanto apenas o portador da chave privada do destinatário poderá decifrar a mensagem e recuperar a chave simétrica utilizada inicialmente, a partir desse momento a comunicação e cifrada e decifrada utilizando a chave simétrica gerada inicialmente (FRANCESE, 2008)

O principal algoritmo de criptografia utilizando chaves públicas foi desenvolvido em 1977 e foi nominada como RSA, nome criado a partir das iniciais dos seus desenvolvedores Rives, Shamir e Adleman, suas chaves possuem 512 a 2048 bits. O algoritmo RSA é a base para a maioria dos sistemas que utilizam criptografia assimétrica na atualidade (MAHTO; KHAN; YADAV; 2016).

2.3.5. Função Hash

Os algoritmos de função *hash* possuem uma relação importante com a tecnologia *blockchain*, de forma objetiva, podemos dizer que o componente *hash* está envolvido no processo de junção e mineração dos blocos que formam sua estrutura, e são responsáveis por garantir a integridade dos dados (BELOTTI *et al*, 2019).

Uma função *hash*, também conhecida como função de resumo, é um tipo de algoritmo que recebe um determinado conjunto de caracteres de tamanho variável e entrega como saída um conjunto alfanumérico sempre com o mesmo tamanho, essa saída é conhecida *como hash-code* (SOBTI; GEETHA, 2012).

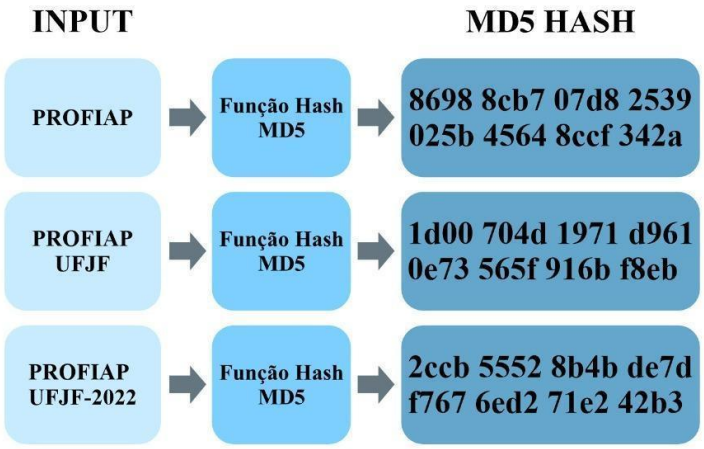
As funções *hashes* podem ser usadas para resumir dados, verificar a integridade de arquivos e garantir a segurança de senhas.

Uma das principais características da função de *hash*, é entregar sempre o mesmo resumo (saída), ou seja, sempre o mesmo texto, quando a sua entrada for a mesma. Caso qualquer alteração seja feita no texto de entrada, mesmo que uma simples vírgula seja adicionada, toda a saída será modificada. (SILVA, 2003).

Podemos fazer uma analogia com a impressão digital, uma função *hash* pode ser entendida como a impressão digital de um determinado dado, essa entrada pode ser, um número, um texto, ou mesmo um arquivo, e enquanto não houver modificações no arquivo de entrada a função hash sempre entregará a mesma saída.

O funcionamento de uma função hash pode ser mais facilmente compreendido através da representação na Figura 5, observe que independentemente do tamanho da entrada o tamanho da saída sempre será o mesmo.

Figura 5: Funcionamento de uma função hash.



Fonte: Autor.

Conforme exposto por Ralph Merkle em sua tese de doutorado intitulada "*Secrecy, Authentication and Public Key*" (1979), a fim de que uma função seja classificada como uma função *hash*, esta deve satisfazer os seguintes critérios:

1. Capacidade: Pode ser aplicada a uma entrada de qualquer tamanho.
2. Padronização: Uma função *hash*, deverá sempre entregar um resumo com o mesmo tamanho, independentemente do tamanho da entrada
3. Unidirecional: Estamos falando da não invertibilidade de uma função, para que essa propriedade seja atendida deve ser impossível através da saída de uma função hash encontramos a entrada.
4. Resistência a segunda pré-imagem: A resistência à segunda pré-imagem significa que não podem existir dois valores de entrada com a mesma saída.
5. Resistência a colisão: Essa propriedade se comporta como uma redundância anterior, e é uma das mais importantes. A colisão acontece quando duas entradas diferentes possuem um *hash-code* de saída igual.

De acordo com Mathew e Jacob (2010), as três funções *hashes* mais utilizadas estão descritas abaixo:

1. *Message Digest* 5 (MD5): Essa função é utilizada principalmente no processo de investigação de integridade de arquivos, porém ela possui vulnerabilidades que a impedem de ter seu uso mais amplo, sua principal vulnerabilidade é quanto a resistência a colisões, é relativamente fácil encontrar duas entradas distintas com uma mesma saída de hash. Durante muito tempo o MD5 foi largamente usado, chegando a ser considerado quase um sinônimo de função de resumo. No entanto, devido aos ataques, esta função tem caído em desuso, sendo substituída por outras que têm tamanhos de resumo maiores, como o SHA-1.
2. Família SHA-2 (*Secure Hash Algorithm* 2), A família SHA-2 é a sucessora do SHA-1 e ao contrário do SHA-1 e do MD5, sua resistência a colisões ainda não foi comprometida. O SHA-2 possui algumas variantes, todas elas utilizam o mesmo algoritmo, com diferença em algumas constantes. Os membros mais famosos do grupo são o SHA-256 (com tamanho de saída de 256 *bits*) e o SHA-512 (com tamanho de saída de 512 bits). O SHA-2 é hoje a função mais robusta em termos de resistência a colisão, e essa característica somada a flexibilização do tamanho das suas saídas são o que tornam o SHA-2 como o algoritmo de função hash mais popular, a sua ampla utilização nas tecnologias de blockchain ajudam a aumentar a sua visibilidade.
3. RIPEMD é uma versão melhorada das funções MD. As saídas do RIPEMD possuem 160 bits de tamanho, enquanto as saídas MD possuem 128 bits

2.3.6. Certificado Digital

Já de posse do conceito de chave assimétrica vamos detalhar o funcionamento do Certificado Digital. Para o melhor entendimento da ideia, vamos nos utilizar do recurso de se recriar uma situação específica.

João precisa acessar um site de e-commerce para realizar uma compra através do seu cartão de crédito, no primeiro acesso, o site envia para o João sua chave pública, para que ele lhe envie de volta uma chave simétrica (chave de sessão gerada a cada acesso), criptografada

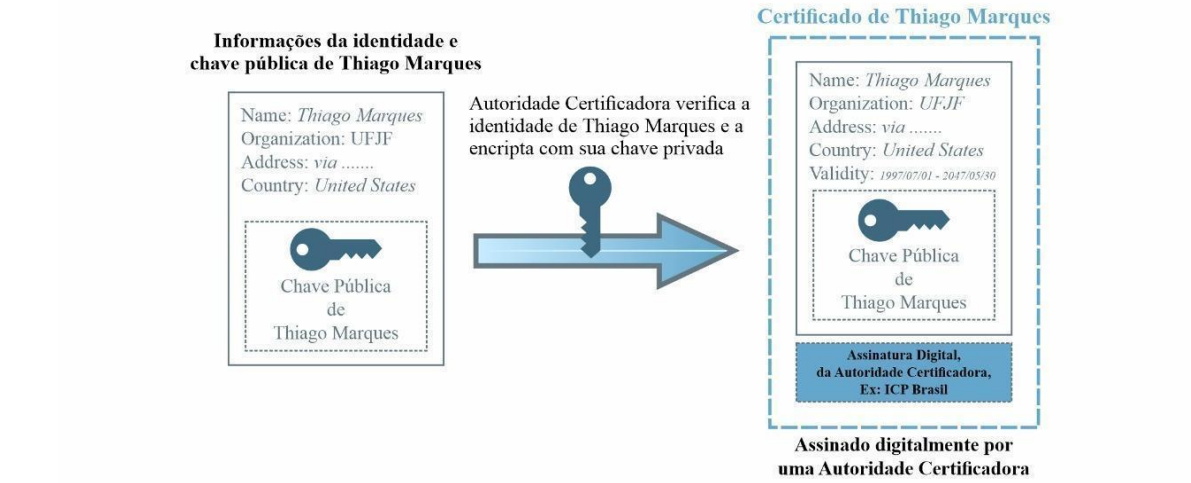
com a chave pública do site, e assim, somente o site poderá ter acesso a chave simétrica e iniciar uma comunicação criptografada e segura entre as partes.

Mas, a grande questão nesse momento é: Quem garante que aquela chave pública pertence realmente ao site de e-commerce solicitado?

Um certificado digital válido garante a veracidade da identidade e consequentemente a transição segura dos dados com destinatários e remetentes corretos, vinculando uma pessoa física ou jurídica a uma determinada chave pública, essa é a sua principal função. Ele é um arquivo distribuído em qualquer tipo de mídia, (*pen drives*, cartões de memória, ou mesmo baixado do site emissor).

O certificado digital é um documento eletrônico que é assinado digitalmente por uma autoridade certificadora e pode conter diversos dados sobre o emissor e o proprietário, como CPF, CNPJ, nome ou razão social. No Brasil, o órgão responsável por fazer a gestão das chaves públicas é o ICP-Brasil (CORRÊA, 2017). A criação de um certificado digital é exemplificada na Figura 6

Figura 6 - Criando um certificado digital.



Fonte. Adaptado com base em Silva, (2020).

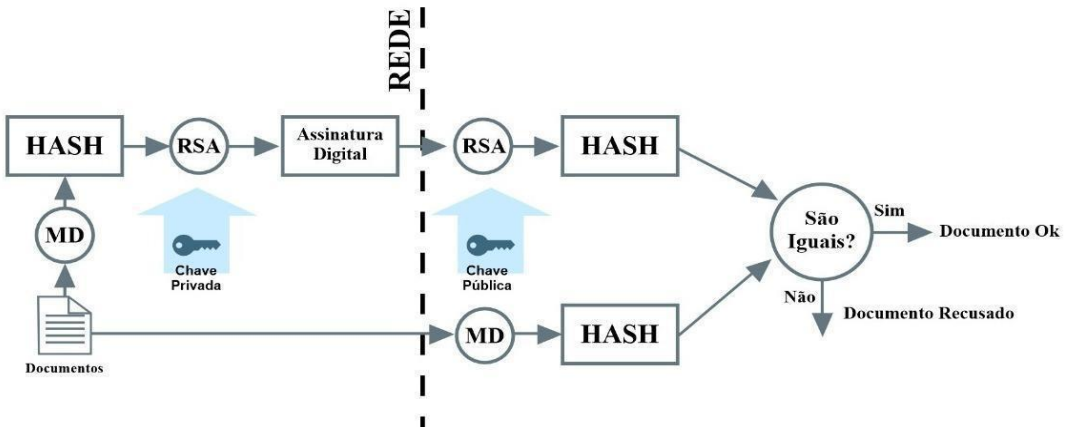
2.3.7 Assinatura Digital

Durante o processo de assinatura convencional (manuscrita) de um documento, é possível garantir a autenticidade do assinante, porém a integridade do documento não pode ser verificada. Na assinatura digital, tanto a autenticidade do assinante quanto a integridade do documento são garantidas (SOUZA, 2019).

A técnica de assinatura digital pode ser detalhada da seguinte forma: o usuário emissor portando sua chave privada criptografa o resultado da função hash da mensagem/documento a ser enviado, geralmente se usa a função MD5 como função hash e RSA como algoritmo para a criptografia assimétrica, essa informação é a assinatura digital, que é anexada ao documento original e enviada ao receptor. O receptor utilizando a chave pública do remetente, fornecida por um certificado digital válido, descriptografa a assinatura digital recebida, e caso o resultado produzido seja idêntico ao *hash-code* do documento original, nós acabamos de provar que o documento foi assinado pelo remetente e manteve a sua integridade, ou seja, não sofreu mudanças durante o processo de transmissão.

Conforme representado na Figura 7, as partes interessadas do documento podem verificar sua autenticidade encontrando a hash do documento obtido através de um algoritmo de resumo da família MD, para descriptografar a assinatura digital, é utilizada a chave pública do emissor da mensagem, caso a *hash* do documento original for igual a assinatura descriptografada pela chave pública, a mensagem é de fato do emissor e não houve nenhuma ação fraudulenta, conseguimos assim verificar a autenticidade e integridade da informação.

Figura 7: Assinatura digital e conferência da autenticidade e integridade de um documento enviado através da rede.



Fonte: Trinta (1998)

2.3.8. Estrutura Funcional Blockchain

Uma rede *blockchain* é essencialmente uma base de dados descentralizada como já foi citado nos capítulos introdutórios, sua existência é perpetuada através dos participantes da rede, conhecidos como nós (BELOTTI, 2019), outra importante característica da rede *blockchain* é a imutabilidade dos dados, ou seja, uma vez uma informação adicionada a rede, ela não pode ser mais apagada ou modificada (MENDANHA, 2017).

A tradução literal de *blockchain* é "corrente de blocos" e a tecnologia recebeu esse nome em razão da maneira com que os dados são gravados e ligados (acorrentados) a outros blocos, como já foi esclarecido, outra nomenclatura encontrada é livro-razão, ou livro-registro.

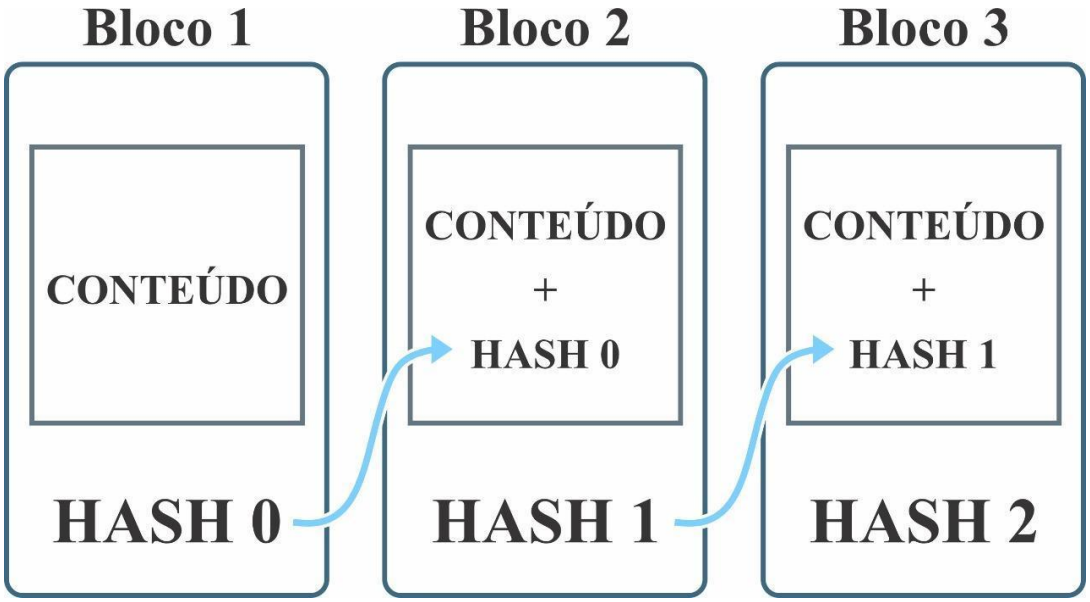
Uma das grandes revoluções na tecnologia *blockchain* está no processo de inclusão de dados, para que uma informação possa ser incluída no bloco, é necessário que a maioria dos participantes da rede confirme e valide esses dados, isso é chamado de prova de consenso.

De acordo com Silva, (2019) a operação lógica e a dinâmica de funcionamento da tecnologia blockchain são sustentadas por tecnologias subjacentes como assinaturas digitais, criptografia e algoritmos de consenso, garantindo especialmente descentralização de gerência e integridade da base de dados.

Quando um dado é inserido em uma *blockchain*, uma série de processos são iniciados, e uma das etapas iniciais e a inserção da informação à estrutura, cada bloco de informação está ligado a outro bloco contendo o dado anterior através de códigos criptografados, e assim sucessivamente, ou seja, para que um bloco de informação seja alterado, o bloco anterior precisa ser alterado, e todos os outros blocos anteriores também seriam alterados (CORREA, 2017) o que é computacionalmente impossível, já que cópias da blockchain estarão espalhadas através de vários nós na rede (BELOTTI et al, 2019).

Na Figura 8 temos uma representação simplificada da "amarração" existente entres os blocos de uma blockchain.

Figura 8: Representação simplificada de blocos de uma blockchain.

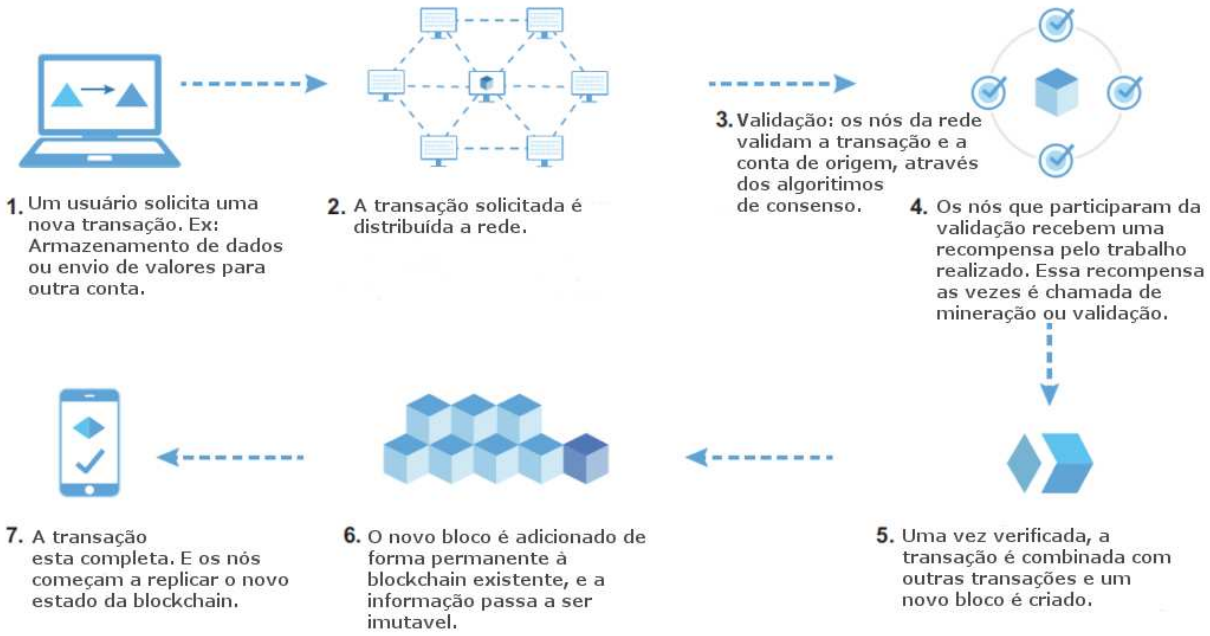


Fonte: Autor.

Após esse bloco ser validado por vários nós e ser inserido esse processo começa a se espalhar por outros integrantes da rede e o banco de dados começa a ser replicado, gerando novas cópias da blockchain atualizada (NAKAMOTO, 2008). Um detalhe importante precisa ser observado, para que essa replicação possa acontecer, os outros nós que irão receber as novas informações, precisam concordar com a informação nova, através dos mecanismos de consenso (MENDANHA, 2017), conceito que será melhor detalhado adiante.

A Figura 9 demonstra os passos existentes no procedimento de inclusão de um novo bloco a uma blockchain.

Figura 9: Como uma informação é incluída na blockchain.



Fonte: Adaptado de cloudcredential.org, (2023)

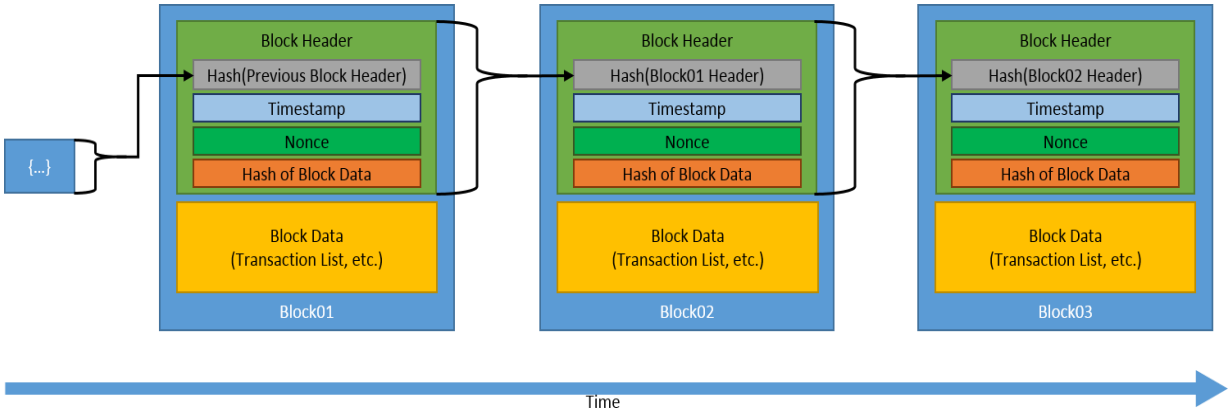
2.3.9. Blocos

Cada bloco de uma *blockchain* é uma estrutura de dados que contém várias informações encapsulados no seu corpo. Ele é composto de um cabeçalho formado por metadados, informações que são utilizadas para resumir e facilitar o acesso e busca dos dados armazenados (MENDANHA, 2017*)*. Os primeiros metadados do cabeçalho fazem referência aos códigos *hashes* do bloco anterior, e a versão do protocolo utilizado (a versão utilizada neste estudo é a 2.0, que introduz o conceito de *smart contracts*), o segundo conjunto de metadados estão relacionados a mineração dos blocos, como a dificuldade, o carimbo de tempo e o *nonce* e por último na terceira parte dos metadados está a raiz da árvore de Merkle, uma estrutura usada para resumir todas as transações do bloco de maneira eficiente, ainda dentro do cabeçalho existe a referência ao hash do bloco anterior, portanto através desses hashes podemos percorrer o caminho até o bloco inicial da cadeia, o bloco gênesis (ZHENG et al, 2018), uma representação da sua estrutura esta apresentada na figura 10.

Um bloco pode ser identificado pela sua posição dentro da cadeia de blocos ou pelo resultado da função hash (SHA256) do seu próprio cabeçalho.

No corpo do bloco encontramos as informações que estão sendo armazenadas, na literatura ela é muitas vezes chamada de transações, pois na sua utilização mais popular, a *blockchain* é utilizada para armazenar transações financeiras, como a venda e compra de criptomoedas (BELOTTI *et al*. 2019).

Figura 10: Estrutura dos blocos de uma blockchain.



Fonte: NIST, (2021)

2.3.10. Árvore De Merkle

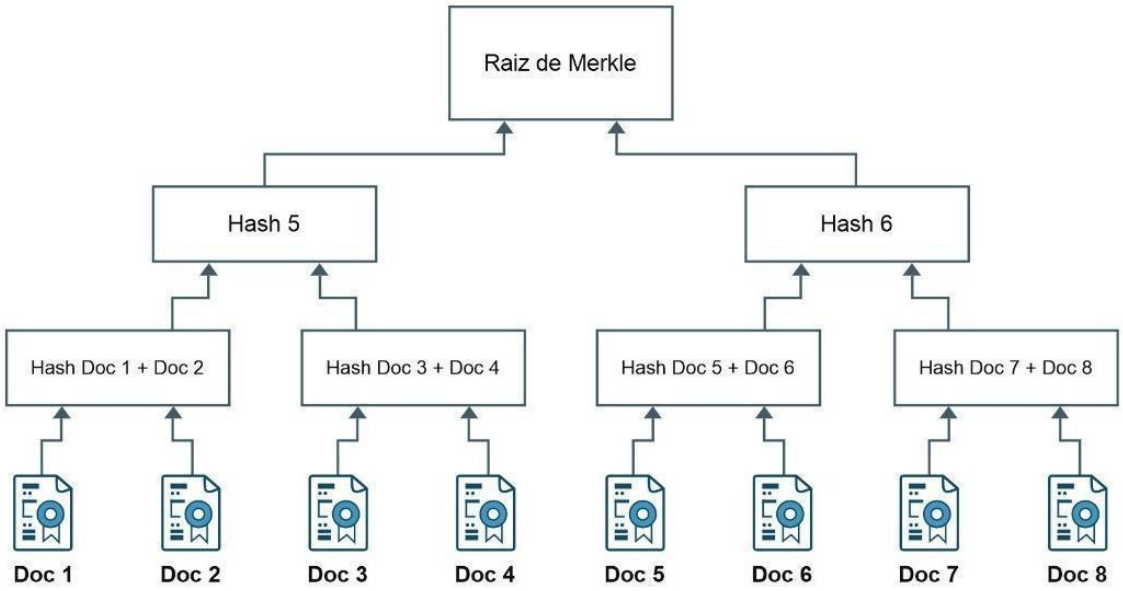
A Árvore de Merkle, também conhecida como Árvore de Dispersão, foi desenvolvida em 1979, por Ralph Merkle, o cientista já foi citado no item 2.3.4 do presente estudo como um dos envolvidos na criação do algoritmo de criptografia assimétrica RSA. As Árvores de Merkle são estruturas de dados do tipo árvore binária que podem ser utilizadas para resumir e agrupar uma grande quantidade de informações de forma eficiente e simples. Uma das características mais interessantes da árvore de Merkel é a possibilidade de se verificar a existência de qualquer documento que compõem a estrutura, sem a necessidade de se possuir ou registrar todo o seu conteúdo na árvore (MERKLE, 1979).

Podemos explicar o seu funcionamento da seguinte forma: uma função *hash*, geralmente a SHA-256 é aplicada em cada documento formador da estrutura, o resultado dessa função conforme já foi descrito, é uma *hashcode*/resumo com tamanho fixo. Cada resumo é concatenado, com o *hashcode* de outro documento, sempre em pares, essa ação vai se repetindo

até que se chegue a apenas um *hashcode* final, conhecido como raiz da árvore de Merkle (SILVA, 2020).

A Figura 11 pode nos ajudar a entender o seu funcionamento. Nesse exemplo um par é formado pelo resumo *hash* do documento 1 e pelo resumo do documento 2, produzindo a hash concatenada Hash Doc 1 + Doc 2 (A), no par ao lado, a *hash* Hash Doc 3 + Doc 4 (B), foi formada pela concatenação do resumo destes dois documentos, a *hash* 5, é obtida através da concatenação da hash A + B, um processo semelhante ocorre do "outro lado da estrutura", onde obtivemos a *Hash* 6, finalmente no processo de concatenação entre a *Hash* 6 e 5 obtivemos a hash final, conhecida como a raiz da árvore de Merkle, explicada na Figura 11.

Figura 11: Exemplo de Árvore de Merkle.



Fonte: Silva, (2020).

2.3.11. Mineração

O processo conhecido como mineração em *blockchain*, é um processo computacional que tem como objetivo adicionar e validar um novo bloco de informação na rede. Esse processo de inserção é composto basicamente por transações matemáticas, pois quando um usuário

consegue realizar todos os cálculos necessários para inserção e consequentemente a validação do bloco ele é recompensado financeiramente pela rede, na grande maioria das vezes pela criptomoeda corrente da *blockchain* utilizada.

2.3.12. Prova de Consenso

Um dos grandes pilares das estruturas de *blockchain* são os mecanismos de consenso conhecidos também como algoritmos de consenso ou provas de consenso. De acordo com Swanson (2015)**,** um mecanismo de consenso pode ser definido como o movimento de validação e confirmação da maioria ou às vezes de todos os nós de uma rede quanto a determinada ação ou transação inserida na blockchain, ainda de acordo com Swanson, um algoritmo de consenso é um conjunto de regras e procedimentos que permitem manter um conjunto coeso de fatos entre vários entes participantes de um grupo.

Em um contexto mais prático, adaptado a realidade das blockchain, é através da prova de consenso que os nós da rede conseguem definir se a informação recebida por eles realmente deve ser inserida na cadeia, ou é um dado errático que foi inserido por um nó malicioso. Através desses mecanismos todo o ambiente pode se manter estável, sem informações desencontradas ou invalidadas, e com a principal vantagem de não ser necessário o uso de um mecanismo de auditoria externo (SILVA, 2020). Mesmo que um ativo da rede tente enviar uma informação forjada, e tente invalidar uma informação correta, se pelo menos 51% dos nós da rede entrarem em concordância, a informação é considerada verdadeira. Esse problema já foi descrito antes mesmo do desenvolvimento dos sistemas distribuídos, e foram expostos através da história conhecida como o Problema dos Generais Bizantinos[5] (LAMPORT *et al,* 1982).

2.3.12.1. Problema Do Gasto Duplo

Outro problema que precisava ser resolvido para que a segurança descentralizada das redes *blockchain* continuassem funcionais, é a questão do gasto duplo, pois um indivíduo mal

[5] O general do exército bizantino deseja atacar seu inimigo, mas para que o ataque seja bem-sucedido, todos os comandantes do seu exército precisam entrar em consenso entre atacar, ou bater em retirada. O problema surge, quando existe a necessidade de enviar a mensagem do general aos comandantes, mas pode haver um comandante traidor, que para sabotar o ataque, repassa a mensagem errada para os demais comandantes (MONTEZANO,2018)

intencionado pode tentar repetir uma transação de mesmo valor, para dois destinatários diferentes, possuindo em sua posse o valor suficiente para honrar apenas uma transação.

Para solucionar esses problemas os nós da rede precisam entrar em consenso para homologar qual das duas transações deve ser efetivada e qual deve ser excluída.

Atualmente esse é um problema que já está solucionado pela maioria dos algoritmos de consenso adotados (ANTONOPOULOS, 2014).

Devido aos problemas apresentados acima e as suas respectivas soluções, as provas de consenso não permitem que uma nova informação seja adicionada a uma *blockchain* de forma automática e instantânea, tomamos como exemplo a *blockchain* do Bitcoin, as novas transações antes de serem adicionadas permanentemente a cadeia da Blockchain, são movidas temporariamente para um bloco, enquanto a maioria dos nós da rede conferem a veracidade das informações que deverão ser incluídas (BELOTTI et al, 2019).

Cada *blockchain* é capaz de escolher qual o tipo de algoritmos de consenso vai ser implementado, porém, após essa definição, todos os nós dessa rede deverão seguir as mesmas regras impostas pelo mecanismo escolhido.

De acordo com David Schwartz *et al*. (2014), três problemas devem ser solucionados com relação à conferência dos dados utilizando uma prova de consenso, o primeiro é a corretude. A corretude é a capacidade dos nós diferenciarem uma transação legítima de uma transação incorreta. O segundo problema a ser solucionado por um mecanismo de consenso é o acordo, que é a capacidade do sistema se manter integro e único, o terceiro e última característica a ser perseguida por um algoritmo de consenso é a utilidade, que indica a capacidade de implementação e utilização real de determinado tipo de consenso, por exemplo, um algoritmo que consegue entregar corretude e acordo, porém demora um período extremamente longo para entregar a confirmação, não atende o princípio da utilidade.

2.3.12.2 Algoritmos De Consenso Probabilísticos

Os mecanismos de consenso mais conhecidos e implementados em redes Blockchain atualmente são do tipo probabilísticos, esse tipo de algoritmo assume que uma rodada de consenso entre nós, pode obter um valor com alguma probabilidade. Eles geralmente se baseiam em recursos de processamento computacional para se obter o consenso, gerando uma prova que

é distribuída aos participantes da rede, o participante que encontrar sua solução primeiro pode decidir qual informação deve ser adicionada a cadeia, ou seja, apenas um nó na rede é suficiente capaz de gerar provas que lhe dá o direito de inserir uma informação correta. Essa prova, assim como a confirmação de que a formação do bloco de dados está correta, é verificada pelos outros indivíduos que formam a cadeia (CARRARA, 2018).

O mecanismo Prova de Trabalho, ou *Proof of Work* (PoW) do inglês é o mais famoso dos algoritmos de consenso e atualmente é utilizado na rede Bitcoin (NAKAMOTO, 2008), ele utiliza o recurso de desafios criptográficos para garantir a integridade dos blocos de uma *blockchain*.

O ativo da rede precisa demonstrar que foi utilizado certo tempo no processo de resolução do desafio, e que a resposta encontrada vai de encontro ao que foi solicitado pelo algoritmo, esse processo deve ser difícil e trabalhoso, mas não pode ser impossível, de forma contrária, a verificação da solução deve ser rápida e fácil de ser realizada pelos outros nós (JAKOBSSON, 1999).

Os problemas são resolvidos através de força bruta, o que acaba gerando uma grande demanda de recursos computacionais, tornando a prova de trabalho um mecanismo caro na sua execução (CARRARA, 2018).

No anseio de mitigar problemas conhecidos na utilização da PoW implementado na rede Bitcoin, como o alto consumo de processamento e consequentemente energia, o nível baixo de escalabilidade já que a cada n blocos o protocolo diminui o incentivo entregue aos usuários no momento da resolução do problema, e principalmente para evitar o ataque dos 51%, quando se tem um grupo de usuários que possuem o controle de 51% da rede é possível efetuar um gasto duplo (ELROM, 2019), foi criado em 2012 o algoritmo de consenso *Proof of Stake* (PoS), ele foi desenvolvido por Sunny King e Scott Nadal.

O *proof of stake* utiliza um processo de seleção pseudo-aleatória, para escolher o nó que irá validar o próximo bloco, esse processo de seleção se baseia em algumas características, como a idade e riqueza do nó, entende-se por riqueza, a quantidade da moeda[6] que o nó possui. Nos sistemas PoS, utiliza-se taxas de transação como recompensa ao nó que irá validar e fazer

[6] A moeda é a unidade monetária definida no momento de criação da estrutura de uma rede do tipo blockchain, geralmente são criptomoedas, ex: a rede Ethereum utiliza a sua moeda ether, para compensar os seus nós validadores. Mas nada impede que uma nova rede blockchain seja criada, que utilize os reais brasileiro como pagamento aos seus membros.

o trabalho de inclusão do novo bloco, já no PoW novas quantidades de moeda são criadas para compensar os blocos que trabalharam no processo de validação e inclusão, conhecido como mineração.

2.3.13. Blockchain e Criptomoedas

O conceito de criptomoedas se confunde às vezes com a própria definição de *blockchain*, porém é necessário ressaltar que apesar de conectadas, essas duas ideias são diferentes e precisam ser esclarecidas. De fato, uma criptomoeda é formada por uma coleção de tecnologias, e a *blockchain* é uma dessas tecnologias.

Nos itens anteriores trabalhamos a definição de *blockchain*, e abordamos as principais tecnologias que fazem parte da sua concepção, nos próximos parágrafos iremos abordar o assunto criptomoedas e as suas principais instâncias.

Desde os anos 80 quando as pesquisas ligadas a criptografia começaram a ficar mais robustas e também mais populares, muitos pesquisadores tentaram implementar algum tipo de moeda digital ou moeda virtual, utilizando a criptografia, porém essas primeiras moedas virtuais necessitavam de um lastro, geralmente ouro, e também precisavam ter as suas transações centralizadas em alguma instituição, o processo de contabilização e validação dessas atividades era muito parecido com o que é utilizado em instituições financeiras tradicionais. Muitas dessas moedas virtuais foram vistas com maus olhos por alguns governos e foram banidas e seus projetos encerrados (ANTONOPOULOS, 2014).

As criptomoedas são categorizadas na literatura acadêmica como um subtipo de moedas virtual, o conceito que não é novo, e frequentemente é assunto de trabalhos acadêmicos que com alguma regularidade geram significativas mudanças na dinâmica da economia mundial (HILEMAN, 2014).

A principal diferença entre uma criptomoeda e uma outra moeda virtual é a não necessidade de se ter uma autoridade centralizadora ou uma instituição governamental, validando e auditando as transações (MENDOZA-TELLO, 2019). Toda essa descentralização só é possível graças à implementação de técnicas de criptografias que se encontram nas blockchain utilizadas pelas mesmas, e na validação e autenticação dos usuários utilizando os conceitos de assinatura digital e certificados digitais (BALCERZAK et al, 2022).

2.3.14. Bitcoin

É praticamente impossível falar sobre Blockchain sem falarmos sobre Bitcoin. A mais conhecida das criptomoedas foi responsável por popularizar a tecnologia do Blockchain e também de trazer à tona, para o público leigo, assuntos que até então eram apenas discutidos em nichos acadêmicos restritos, como criptografia e processamento descentralizado (NAKAMOTO 2008).

Em 31 de outubro de 2008 um documento chamado "Bitcoin: *A Peer-to-Peer Electronic Cash System*", elaborado no formato de *white paper*, ou seja, um documento que aprofunda determinado problema, suas causas, conceitos e sua solução, contendo todas as especificações técnicas e instruções de implementação da criptomoeda surgiu. Satoshi Nakamoto é o pseudônimo por trás da elaboração deste trabalho, porém até hoje o seu verdadeiro nome é desconhecido, e muitas pessoas reivindicam a autoria do trabalho.

O Bitcoin é uma criptomoeda formada por uma coleção de tecnologias e conceitos que já existiam anteriormente, mas não foram exploradas com tamanho pragmatismo. Cada unidade dessa moeda pode ser transmitida de um usuário a outro, pode ser usada para fazer compras, ser utilizada como garantia em operações de crédito e pagar contas, assim como uma moeda convencional (ANTONOPOULOS, 2014).

A grande inovação na sua concepção, está ligada à utilização da tecnologia blockchain e da criptografia como base estrutural do seu funcionamento. Através do *blockchain* as transações são praticamente irreversível, o que evita fraudes, além disso, todo o processo acontece de forma descentralizada e é checada e validada por múltiplos participantes da rede, através da utilização da criptografia substituímos o modelo mais comum de confiança, onde é necessário um terceiro para certificar de que o valor realmente existia e poderia ser transferido para outro portador, conhecida como prova de confiança, no Bitcoin utilizamos a para a prova de criptografia, que permite duas partes possam realizar transações livremente, sem uma terceira parte confiável (NAKAMOTO, 2008).

2.3.15. Ethereum

A Ethereum assim como o Bitcoin, é uma rede do tipo *blockchain*, seu surgimento se deu através das pesquisas de Vitalik Buterin um programador e pesquisador russo-canadense, envolvido em pesquisas relacionadas ao Bitcoin e fundador de uma das mais famosas publicações ligadas ao meio, a Bitcoin Magazine.

A criação do Ethereum surgiu com o objetivo de expandir as capacidades da rede Bitcoin. Na visão de Buterin a rede *blockchain* poderia se tornar muito mais útil se além de movimentações financeiras ela pudesse realizar qualquer tipo de processamento. Vitalik Buterin tentou angariar outros pesquisadores no desenvolvimento de sua plataforma, porém a ideia não foi muito bem aceita. Diante desse fato, em 2014 ele resolveu embarcar por conta própria nesse novo projeto, que foi lançado ao público em 2015. Atualmente a Ethereum é a segunda rede blockchain mais utilizada, possui uma extensa documentação e uma comunidade extremamente ativa de desenvolvedores com inúmeros aplicativos descentralizados construídos e disponíveis em sua plataforma (RANGANTHAN, 2018).

A documentação oficial da Ethereum traz uma definição lúdica que nos ajuda a entender melhor o seu conceito, "O Ethereum é uma *blockchain* com um computador embutido, ela é a base para a criação de aplicativos e organizações de maneira descentralizada, autônoma e resistente à censura" (WACKEROW, 2023).

O computador apontado no parágrafo anterior se chama Ethereum *Virtual Machine* (EVM). A EVM é uma máquina virtual, que permite aos desenvolvedores escreverem espécies de programas conhecidos como contratos inteligentes (*smart contracts),* utilizando linguagens de programação completas contendo todos os recursos encontrados em linguagens de programação convencionais como Java e C++, esses contratos são então implantados na rede Ethereum e interpretados pela EVM. Cada participante da rede possui uma réplica da EVM em conjunto com sua respectiva *blockchain*, o que lhes confere a habilidade de enviar solicitações para que sejam realizadas, por exemplo, operações de cálculo ou armazenamento de informações na cadeia de blocos. Essas solicitações são transmitidas aos demais nós da rede que validam e executam o código causando assim uma alteração de estado na EVM que é propagada aos demais participantes (BUTERIN, 2013).

A rede Ethereum assim como a rede Bitcoin, possui um sistema de recompensa para os participantes que realizarem o trabalho de validar e adicionar nós à rede, portanto, quando uma nova informação é adicionada, um valor em Ether, (a moeda utilizada na Ethereum) é cobrado

da conta que deseja realizar operação e é entregue como pagamento aos usuários que realizarem a tarefa de validação e implantação das informações. Esses custos podem variar de acordo com a demanda da rede e tipo de operação realizada, e são medidos através de um termo chamado Gas. Cada operação consome um valor fixo de Gas que está ligado à medição do trabalho realizado para a interação na rede, porém o valor de cada unidade de Gas varia conforme a demanda e disponibilidade dos nós. (WACKEROW, 2023).

Por fim, Antonopoulos e Wood (2019) enfatizam a existência de ambientes oficiais destinados a testes nos quais os desenvolvedores podem avaliar suas aplicações antes de implantá-las definitivamente na Mainnet nome dado ao ambiente de produção e rede principal da Ethereum. Esses ambientes de testes são conhecidos como testnets, e de acordo com a documentação oficial, atualmente existem duas testnets disponíveis denominadas Sepolia e Goerli. Para este trabalho iremos adotar a rede Sepolia, o qual oferece um ambiente bastante semelhante ao da Mainnet.

2.3.15.1. Ether

Assim como a rede Bitcoin, possui uma criptomoeda, a Ethereum implementou o Ether (ETH) como moeda oficial, além de ser utilizada para transações financeiras entres os usuários ela também fornece incentivo econômico para os participantes verificarem ou executarem solicitações de transação e fornecerem recursos computacionais para a blockchain Ethereum. Portanto, reforçando o que foi exposto no item 2.3.15, qualquer participante que transmita uma solicitação de transação também deve oferecer alguma quantidade de ETH à rede como pagamento pela atividade. A rede concederá essa recompensa a quem eventualmente fizer o trabalho de verificar a transação, executando-a, confirmando-a na cadeia de blocos e propagando-a para o resto da blockchain (WOOD, 2014).

2.3.15.2. Aplicações Descentralizadas (dApps)

As Aplicações Descentralizadas (dApps), são programas de computador que foram desenvolvidos em uma rede descentralizada como a blockchain da Ethereum e utilizam os contratos inteligentes como código fonte. No modelo tradicional de desenvolvimento de

software, o sistema criado é executado em um local centralizado como um computador pessoal ou um servidor na Internet, nos dApps, esses sistemas estão rodando de forma descentralizadas e uma cópia da aplicação se encontra em cada nó da rede. Abaixo citamos os maiores benefícios dos dApps:

1. Zero tempo de inatividade: uma vez que a aplicação é implementada na blockchain, a rede como um todo sempre será capaz de atender clientes que procuram interagir com o contrato. Os atores mal-intencionados, portanto, não podem lançar ataques de negação de serviço direcionados a dApps individuais.
2. Privacidade: você não precisa fornecer identidade real para implantar ou interagir com um dApp.
3. Resistência à censura: nenhuma entidade na rede pode impedir que os usuários enviem transações, implantem dApps ou leiam dados da blockchain.
4. Integridade dos dados: os dados armazenados na blockchain são imutáveis e indiscutíveis graças aos princípios criptográficos. Atores mal-intencionados não podem forjar transações ou outros dados que já foram tornados públicos.
5. Independência de uma autoridade central: as dApps possuem a garantia de execução de maneiras previsíveis, sem a necessidade da chancela por parte de uma autoridade central; por exemplo, quando usamos sistemas bancários on-line, temos que confiar que as instituições financeiras não usaram indevidamente nossos dados pessoais, adulteraram registros ou mesmo se foram hackeadas (WACKEROW, 2023).

Os dApps representam uma abordagem revolucionária para a descentralização e autonomia do usuário. Sua utilização abrange diversos setores trazendo maior segurança, transparência e eficiência nas transações e interações. Embora existam desafios a serem enfrentados, como escalabilidade e usabilidade, o potencial transformador dos dApps é inegável (ANTONOPOULOS; WOOD, 2019).

Além do próprio artefato desenvolvido nesse trabalho, alguns dApps elaborados pelo governo federal, já foram citados, como por exemplo, o bConnect e o b-CNPJ criados pela Serpro, e à medida que a tecnologia *blockchain* continua a evoluir, é provável que vejamos um aumento na adoção e no desenvolvimento de dApps.

2.3.15.3. *Smart Contracts* (Contratos Inteligentes)

O conceito de smart contracts (contratos inteligentes) foi introduzido em 1997 por Nick Szabo através do seu trabalho "*Formalizing and securing relationships on public networks",* Szabo define contratos inteligentes como sendo um protocolo de computação descentralizada que executa os termos de um conjunto de regras pré-definidas (SZABO, 1997). Em outras palavras, são instruções computacionais que rodam em uma *blockchain* e executam automaticamente as ações pré-definidas (termos) quando determinadas condições são satisfeitas, essas condições também são nomeadas em alguns textos como eventos ou gatilhos, as ações podem incluir o envio de criptomoedas, o armazenamento de dados em um registro público, ou até mesmo a execução de outros *smart contracts*. Podemos exemplificar o seu funcionamento através de do seguinte modelo hipotético, imagine o seguinte cenário onde determinada informação é enviada para ser registrada em blockchain através de um contrato inteligente, no momento em que a informação é enviada, o código do contrato pode analisar o endereço de origem da informação e caso ele seja diferente de uma lista pré-armazenada no próprio contrato, a operação será cancelada e um aviso de erro pode ser mostrado para os usuários envolvidos. Um outro exemplo, mas agora de implementação real de *smart contracts* e dApp é o caso da plataforma de empréstimos descentralizados (DeFi) MakerDAO. A MakerDAO usa *smart contracts* para permitir que usuários emprestem e peçam emprestado a criptomoeda DAI, que é indexada ao dólar americano. Os *smart contracts* gerenciam automaticamente as taxas de juros, a avaliação de risco, e a execução do empréstimo, tornando o processo mais rápido, eficiente e transparente quando comparadas aos empréstimos tradicionais (BRENNECKE, 2022).

Embora os *smart contracts* sejam frequentemente comparados a programas de computador, há algumas diferenças fundamentais entre eles, a principal é que os *smart contracts* são executados em uma *blockchain*, enquanto os programas de computador podem ser executados em um sistema operacional ou plataforma de computação, outro ponto são que os *smart contracts* são projetados para serem autônomos, enquanto os programas de computador geralmente dependem de um intermediário, como um servidor centralizado para executar suas funções, essas características tornam os smart contracts mais estáveis e resistentes a fraudes e falhas, quando comparados aos programas de computadores convencionais (KHAN

et al, 2021). Um diagrama simplificado representando o funcionamento dos smart contracts pode ser visto na figura 12.

Figura 12: Como os contratos inteligentes funcionam.

Fonte: Adaptado de ideausher.com, 2023.

Contratos inteligentes na rede Ethereum são escritos em linguagens de alto nível, ou seja, linguagens de programação com sintaxe de fácil entendimento ao ser humano, os códigos escritos em linguagens de alto nível necessitam ser convertidas em linguagem de baixo nível que podem ser interpretadas pelos computadores (OLIVEIRA, 1999), na rede Ethereum o responsável por fazer essa transcrição é a EVM. As linguagens disponíveis para serem utilizadas pelos desenvolvedores no processo de criação de *smart contracts* são a *Serpent* a Viper, e a Solidity as duas primeiras possuem sintaxes semelhantes ao Python, linguagem amplamente utilizada pelos cientistas de dados e acadêmicos, já a *Solidity* possui uma sintaxe semelhante a outras linguagens mais tradicionais, como o Javascript e o C++, dentre as três linguagens a Solidity é a mais popular e esse fato somada à grande disponibilidade de documentação foram o que a levaram a ser utilizada em nosso projeto (WOHRER; ZDUN, 2018).

A popularidade dos *smart contracts* tem crescido rapidamente, e se tornaram uma peça fundamental no processo de desenvolvimento e implantação de aplicações descentralizadas (dApps). De acordo com o Aran Davies no seu artigo "*Why Blockchain Developers Use*

Ethereum?”, eles são um dos grandes motivos da popularização do Ethereum e da sua adoção para o desenvolvimento de aplicações descentralizadas (DAVIES, 2023).

3. PROCEDIMENTOS METODOLÓGICOS

As ciências tradicionais como exemplo as naturais e as sociais, quando utilizadas como paradigmas norteadores de pesquisas científicas tem como resultado estudos que estão comprometidos em explicar, descrever, explorar, ou predizer fenômenos e suas relações. Entretanto, quando o objetivo do pesquisador é o estudo da construção de um novo artefato, ou realizar pesquisas orientadas à solução de problemas, às ciências naturais podem apresentar limitações. Uma alternativa capaz de superar essas limitações seria a adoção do Design Science, um novo paradigma epistemológico para a condução de pesquisas (DRESCH, LACERDA, ANTUNES, 2020). Como o nosso objetivo é a construção de um novo artefato, escolhemos o Design Science (DS) como metodologia e vamos utilizar o Design Science Research (DSR) como processo metodológico para a condução do desenvolvimento do presente estudo e consequentemente da construção do artefato.

Através deste capítulo serão explicados alguns conceitos ligados à DS e DSR, e serão descritos os procedimentos metodológicos adotados ao longo da pesquisa, ao final, o cronograma da nossa pesquisa será apresentado.

3.1. Design Science e Design Science Resource

Herbert Alexander Simon, foi um notável pesquisador na área da economia, computação, e psicologia, com contribuições pródigas que lhe renderam uma medalha Alan Turian[7] em ciência da computação, e um prêmio Nobel em economia, além de outros relevantes prêmios e homenagens (LARKEY,2002).

A sua obra As Ciências do Artificial de 1996, introduziu o conceito *da science of design* que posteriormente foi chamado de *design science,* nela Simon diferencia o artificial do natural. Conforme o pesquisador, o artificial é algo que foi produzido ou inventado pelo homem, como exemplo as máquinas organizações, a economia e até a sociedade. Pimentel, Filippo e Santoro,

[7] A medalha Alan Turing é frequentemente referenciada como o Prêmio Nobel da Computação concedido anualmente pela Association for Computing Machinery para uma pessoa selecionada por suas contribuições à ciência da computação. (AMTURING.ACM.ORG,2020)

(2018) afirmam que o *design science* é visto por Simon como uma ciência sobre o desenvolvimento de artefatos sociotécnicos. Ele também a caracteriza como paradigma epistemológico, apontando a necessidade de se produzir conhecimento sobre os artefatos.

Os artefatos, de acordo com Peffers et al (2007), não são exclusivamente objetos físicos, eles podem ser qualquer coisa projetada para se alcançar um objetivo, inclusive abstrações. Na tabela 1, é apresentado alguns exemplos de artefatos mais comumente utilizados nas pesquisas ligadas à ciência da computação.

Tabela 1: Tipos de Artefatos

Tipo de Artefato	Descrição
Constructo	Vocabulário conceitual de um domínio
Modelo	Proposições que expressam relacionamentos entre os constructos
Framework	Guia, conceitual ou real, que serve como suporte ou guia
Arquitetura	Sistemas de estrutura de alto nível
Princípio de Projeto	Princípios-chave e conceitos para guiar o projeto
Método	Princípios-chave e conceitos para guiar o projeto
Instanciação	Implementações em ambientes que operacionalizam constructos, modelos, métodos e outros artefatos abstratos
Teorias de Projeto	Conjunto prescritivo de instruções sobre como fazer algo para alcançar determinado objetivo. Uma teoria geralmente inclui outros artefatos abstratos, tais como constructos, modelos, frameworks, arquiteturas, princípios de design e métodos.

Fonte: PIMENTEL, FILIPPO E SANTORO, (2018)

O processo de criação de um artefato e o estudo sobre o seu uso num dado contexto se caracterizam como um meio para produzir conhecimento, o que faz do artefato um elemento central nas pesquisas científicas concebidas no paradigma epistemológico do Design Science (LIMA *et al*, 2014).

Um ponto que precisa ser esclarecido é sobre as terminologias envolvidas com o *design science*, o termo *design science* (DS) constitui a base epistemológica, ou seja, se configura como

metodologia, e com o objetivo de conduzir as pesquisas fundamentadas no design science, vários métodos foram propostos por diversos autores das mais diferentes áreas, com predominância da área de sistemas de informação, os nomes dados a esses métodos também variam, de *design science research*, *design science research methodology*, *design cycle*, *design research* entre outros (DRESCH, LACERDA, ANTUNES, 2020). Por tanto para esse trabalho adotamos o termo design science research (DSR) como o método, que será capaz de operacionalizar a construção de nosso artefato (REIS, 2019).

Como método de pesquisa objetivando solução de problemas, o DSR tendo como ponto de partida o entendimento do problema, procura desenvolver e avaliar artefatos que permitam modificar situações, transformando suas condições para estados melhores ou desejáveis. A DSR é utilizada nas pesquisas como forma de diminuir a lacuna existente entre teoria e prática (LIMA *et al*, 2014), Dresch (2013) ainda afirma que a DSR busca a solução de problemas específicos de forma satisfatória e não necessariamente ótima.

3.2. Procedimentos Metodológicos

Alan Hevner *et al* (2004) definiu sete critérios a serem considerados por pesquisadores durante a condução do design science research, na Tabela 2, constam essas diretrizes aplicadas à presente pesquisa.

Tabela 2: Critérios do DSR, aplicados ao presente trabalho.

Critério	Aplicação do Critério à pesquisa
Relevância do Problema	A blockchain, tem sido apontada pelo Governo Federal, como ferramenta inovadora, capaz de aumentar a segurança e eficiência dos processos ligados à administração pública, entretanto ainda são poucos os projetos implementados.
Artefato	Instanciação de um sistema para garantir a existência e autenticidade de um documento, através da blockchain da rede Ethereum

Processo de Busca da Solução	Guiado pelo método de pesquisa Design Science Research.
Rigor da Pesquisa	Para cada ciclo de conhecimento da pesquisa um ou mais conceitos foram utilizados para garantir o rigor da pesquisa.
Avaliação	Utilização da simulação como método de avaliação. A simulação faz parte metodologia experimental e é caracterizada pela execução do artefato utilizando dados artificiais (HEVNER et al., 2004).
Contribuições da Pesquisa	A solução poderá ser utilizada como modelo para novos projetos, ligados à utilização da blockchain para a gestão de documentos da administração pública.
Comunicação da Pesquisa	As pesquisas que utilizam o design science como método de condução, devem ser apresentadas tanto para o público mais orientado a tecnologia quanto para aqueles mais orientados à gestão. (DRESCH, LACERDA, ANTUNES, 2020). Para o corrente trabalho entendemos que a formação de uma banca de defesa multidisciplinar e a disponibilidade do texto em plataformas online de acesso amplo, atendem a esse critério.

Fonte: Adaptado de Hevner et al. (2004)

Para este trabalho vamos adotar a metodologia de DSR sugerida por Vaishnavi e Kuechler (2004), o método proposto pelos dois pesquisadores é uma variação do método de DSR proposto em 1990 pelo professor da Universidade de Tóquio, Hideaki Takeda.

De acordo com Vaishnavi e Kuechler o método DSR é composto por cinco fases de condução, cada qual com uma sua respectiva saída ou produto conforme representado na Tabela 3.

Tabela 3: Fases da DSR e suas respectivas saídas.

Fase	**Nome da Fase**	**Saída da DSR**
Primeira	Conscientização	Proposta
Segunda	Sugestão	Tentativa
Terceira	Desenvolvimento	Artefato
Quarta	Avaliação	Medidas de Desempenho
Quinta	Conclusão	Resultados

Fonte: Lacerda et al. (2013)

Durante a Conscientização do Problema, o pesquisador deve identificar e compreender o problema que deseja estudar e solucionar, para isso se planeja realizar uma análise de dados secundários através da revisão bibliográfica da literatura relacionada a:

1. Gestão de documentos e do acervo acadêmico na administração pública brasileira.
2. Conceitos e fundamentos sobre a tecnologia blockchain.
3. Ferramentas utilizadas para o desenvolvimento do artefato
4. Trajetória da tecnologia blockchain na administração pública brasileira

Durante a fase de Sugestão, são listadas possíveis soluções para o problema que está sendo estudado. Através do método abdutivo, iremos sugerir como solução para o nosso problema, a criação de uma ferramenta capaz de persistir dados de documentos advindos do acervo acadêmico de uma IF em uma blockchain. Abaixo temos uma descrição sobre o método abdutivo.

> O método abdutivo consiste em estudar fatos e propor uma teoria para explicá-los. Logo, a abdução é um processo de criar hipóteses explicativas para determinado fenômeno/situação. Posteriormente, no momento de colocar as hipóteses à prova, outros métodos científicos podem ser utilizados. A abdução é considerada um processo, acima de tudo, criativo, por isso é o mais indicado para compreender uma situação ou problema, justamente em função do processo criativo intrínseco a esse tipo de raciocínio. Ademais, é o único

> método científico que permite a introdução de uma nova ideia (Fischer; Gregor, 2011). Peirce (1975) ressalta ainda que o raciocínio abdutivo é característico de descobertas científicas revolucionárias. (Dresch et al., 2015, p. 62-63)

Na etapa de Desenvolvimento, tem-se a documentação e implementação do artefato. O artefato é construído no formato de um sistema informatizado, caracterizado por uma interface onde o usuário poderá enviar um documento pertencentes ao acervo acadêmico. Alguns dados dos documentos serão persistidos na rede *blockchain* da Ethereum, a linguagem PHP será utilizada no *back-end*[8], e utilizaremos um aplicativo para dispositivos móveis desenvolvido na linguagem Flutter no *frontend*[9].

Concluída a implementação do artefato, realiza-se a etapa de avaliação. A qualidade, eficácia e a utilidade do artefato podem ser avaliadas em termos de funcionalidade, completude, consistência, acurácia, performance, confiabilidade, usabilidade (Mullarkey *et al,* 2019). De acordo com Hevner *et al* (2004). a seleção da metodologia utilizada para a avaliação deve estar alinhada com o artefato desenhado e as métricas selecionadas, as principais metodologias de avaliação utilizadas nos DSR, estão listadas na Tabela 4.

Tabela 4: Métodos de Avaliação do DS.

Métodos de Avaliação do design	
Observacional	Estudo de Caso: Estudo em profundidade de um artefato em um ambiente de negócio
	Estudo de Campo: Monitorar o uso de um artefato em múltiplos projetos
Analítico	Análise Estática: Examinar a estrutura de um artefato para qualidades estáticas

[8] O Back-End fica responsável pelos bastidores de uma aplicação, ou seja, os códigos que permitem a parte visual funcionar corretamente ANHANGUERA, 2022

[9] Front-End é tudo que envolve a parte visível de um site ou aplicação, com a qual os usuários podem interagir. ANHANGUERA,2022

	Análise de Arquitetura: Estudo de compatibilidade de um artefato em uma arquitetura técnica de TI
	Otimização: Demonstração inerente de propriedade ótimas de um artefato ou identificar margens de otimização no comportamento de um artefato
	Análise Dinâmica: Estudo do artefato em uso para qualidades dinâmicas
Experimental	Experimento controlado: Estudo do artefato em um ambiente controlado
	Simulação: Execução do artefato com dados artificiais
Teste	Teste Funcional (Caixa Preta): Executar a interface de um artefato para descobrir falhas e identificar defeitos
	Teste Estrutural (Caixa Branca): Performar um teste de acordo com métricas na implementação de um artefato
Descritivo	Argumentação: Uso de informações de pesquisas para construir um argumento da utilidade do artefato
	Cenários: A construção detalhada de cenários em torno do artefato para demonstrar sua utilidade

Fonte: HEVNER et al., 2004.

Para o presente trabalho vamos escolher a simulação como metodologia de avaliação, com o objetivo de identificar se a ferramenta é capaz de atender os seguintes pontos: a) garantir que os dados dos documentos estão persistidos na blockchain, b) garantir que esses dados não podem ser alterados, c) garantir que as informações estarão distribuídas de forma descentralizadas.

Por fim, na Conclusão, dar-se prosseguimento à discussão dos resultados obtidos por meio da apresentação do conhecimento adquirido após as fases anteriores, incluindo a análise de potencialidades e desafios atrelados à solução aqui proposta.

4. RESULTADOS E DISCUSSÕES

Através deste capítulo serão apresentadas as discussões que envolvem o desenvolvimento do artefato, bem como os resultados obtidos e a verificação da eficácia da ferramenta.

No item 4.1 vamos expor de forma detalhada cada tecnologia e ferramenta auxiliar utilizada na criação do nosso artefato. No item 4.2 vamos descrever o processo de desenvolvimento com a apresentação e análise de alguns códigos implementados pelo autor, e por fim no item 4.3 iremos apresentar os resultados obtidos após a execução do nosso experimento.

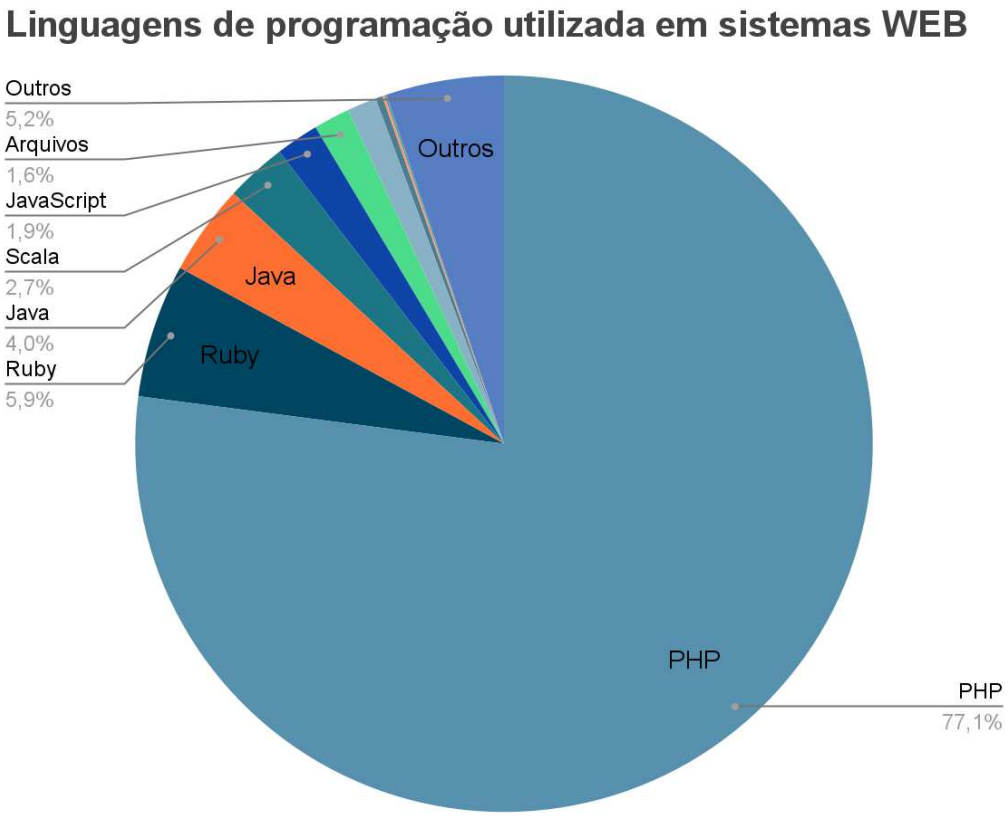
4.1. Tecnologias

Nesta seção serão detalhadas as tecnologias e ferramentas adotadas e utilizadas no desenvolvimento da solução.

4.1.1. PHP

A linguagem escolhida para o desenvolvimento da nossa aplicação *back-end* foi o PHP. O PHP é uma linguagem de código aberto (*open source)* utilizada para a criação de aplicações WEB e sites, foi apresentada à comunidade de desenvolvedores em 1994, e rapidamente se tornou a linguagem mais utilizada para a criação de sistemas WEB. Desde o seu surgimento foi se aprimorando e ganhando novas funcionalidades e dispositivos de segurança, que foram responsáveis por manter a sua popularidade até os dias atuais, dados levantados pela W3Techs, organização responsável por prover informação sobre a utilização de tecnologias na WEB, demonstram que cerca de 77% dos sistemas WEB utilizados atualmente foram escritos em linguagem PHP, mais informações relativas a esse levantamento podem ser observadas no gráfico 1.

Gráfico 1: Utilização de linguagens em sistemas WEB



Fonte: W3TECH, 2023

O PHP é a linguagem utilizada na construção de várias aplicações e sistemas adotadas pelo poder público, um dos mais conhecidos é o Sistema Eletrônico de Informações (SEI), ferramenta utilizada amplamente por várias autarquias e instituições públicas (FONSECA, 2022).

A sua facilidade de integração com outras linguagens e ferramentas, sua robusta documentação oriunda de uma comunidade de usuários bem atuantes, e o seu nível de maturidade alcançado através dos mais de 25 anos de utilização, foram os principais motivadores de sua adoção.

4.1.2. Remix

O Remix IDE pode ser descrita como um ambiente de desenvolvimento integrado (IDE)

para contratos inteligentes, escritos na linguagem *Solidity,* De acordo com Latif (2020), a Remix IDE é a maneira mais fácil de se construir contratos inteligentes para Ethereum, e através dela, todo o ciclo de trabalho envolvendo o desenvolvimento funciona de forma intuitiva, interativa e inteligente. Sua interface apesar de simples possui todos os recursos necessários para que os *smart contracts* possam ser escritos e enviados às blockchain. Ela possui também interação com outras ferramentas ligadas ao desenvolvimento de aplicações descentralizadas, como carteiras virtuais, sistemas de virtualização de blockchain e sistemas de versionamento.

A sua facilidade de operação a não necessidade de instalação, além de todos os aspectos da construção de contratos estarem cobertos pela ferramenta, foram os motivos que embasaram a sua escolha neste projeto

4.1.3. *Simple* WEB3 PHP

Para a interação com as redes blockchain Ethereum, foi utilizada a biblioteca *Simple* WEB3 PHP, essa biblioteca foi criada em 2022 pelo desenvolvedor espanhol Alex Cabrera. A Simple WEB3 PHP possibilita a execução de chamadas do tipo *Remote Procedure Call* (RPC), a um provedor de acesso à rede Ethereum. Através dessa ferramenta também é possível executar funções de determinados contratos inteligentes, e realizar chamadas utilizando a assinatura digital de uma carteira. Não foram encontradas muitas opções de bibliotecas de interação com blockchains Ethereum para a linguagem PHP, porém a escolha por essa ferramenta se deu à sua simplicidade de implementação e atualizações mais recentes por parte do desenvolvedor.

4.1.4. Infura

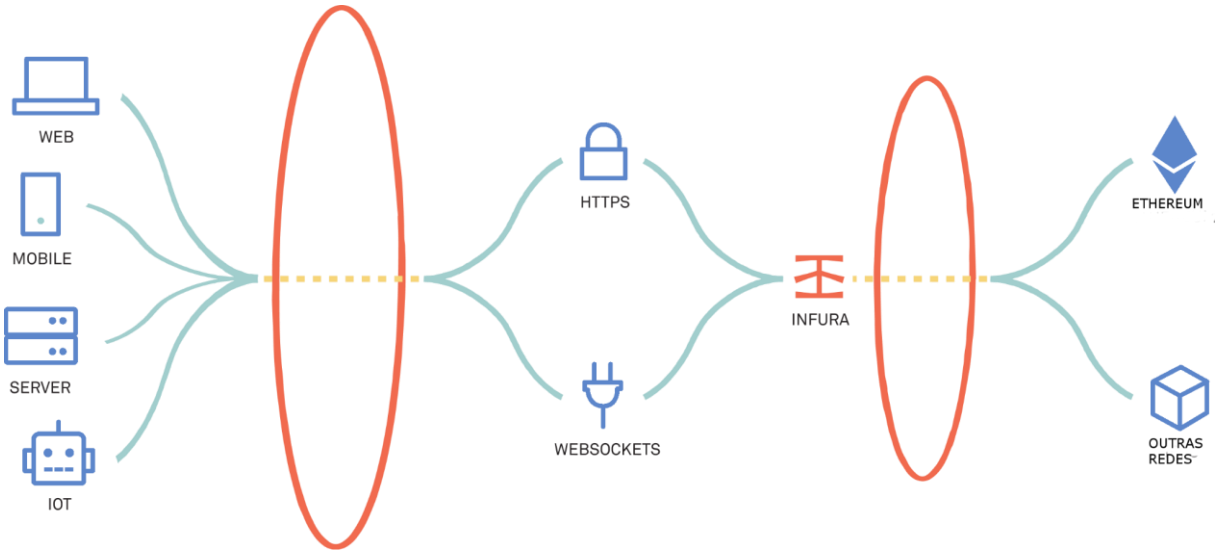
Cada nó de uma blockchain, possui uma cópia de toda a cadeia de registros da rede, e a cada interação é necessário que o nó se comunique, e em seguida aceite ou rejeite a nova informação, e em caso de aceite, replique esses dados para os outros pontos da rede. A Infura é um serviço conhecido em inglês como *Node Provider*, que funciona como um canal de acesso entre aplicações e nós das redes, sem essa ferramenta para fazer o envio dos contratos inteligentes para a rede, seria necessário se tornar um nó da blockchain Ethereum, demandando o download de uma quantidade enorme de dados, e consumo de tempo visto que existe um

processo recorrente de sincronização sempre que novas informações são adicionadas aos blocos (ALNUAIMI *et al*, 2022). Além de fornecer o acesso a rede Ethereum, a Infura fornece acesso a outras redes blockchain, e fornece também uma gama de serviços para os desenvolvedores, como a gerência de projetos e acesso seguro aos recursos da rede através de conexões criptografadas.

A escolha da Infura como ponto de acesso, se baseou na sua confiabilidade e extensa documentação disponível, visto que mais de 50% de todas as transações da rede Ethereum passam pela infraestrutura da Infura (KHARIF, 2022).

Na figura 13, podemos exemplificar o funcionamento do Infura, intermediando o tráfego de informações entre aplicações e a rede Ethereum

Figura 13: Funcionamento do Infura



Fonte: Adaptado de consensys.net (2018)

4.1.4. Etherscan

A fim de se provar a capacidade do nosso experimento em atingir o objetivo desejado, precisamos verificar se os contratos inteligentes foram realmente enviados à blockchain e se encontram funcionais, posteriormente, devemos assegurar a correta integração dos dados provenientes do item do acervo acadêmico à blockchain. Para esse fim iremos utilizar o

Etherscan, uma ferramenta do tipo explorador de blocos, capaz de rastrear de forma detalhada as informações e transações efetivadas em uma blockchain.

O Etherscan é a mais popular e conceituada ferramenta para o monitoramento de redes blockchain Ethereum, estando integrada oficialmente ao Google e recentemente ao Chat Gpt (SALVO, 2022). Sua operação é viabilizada através de inúmeras instâncias em nós da rede, que juntas são capazes de capturar o estado atualizado da blockchain, listando as transações que são enviadas assim como os blocos que são criados (OLIVA, 2022).

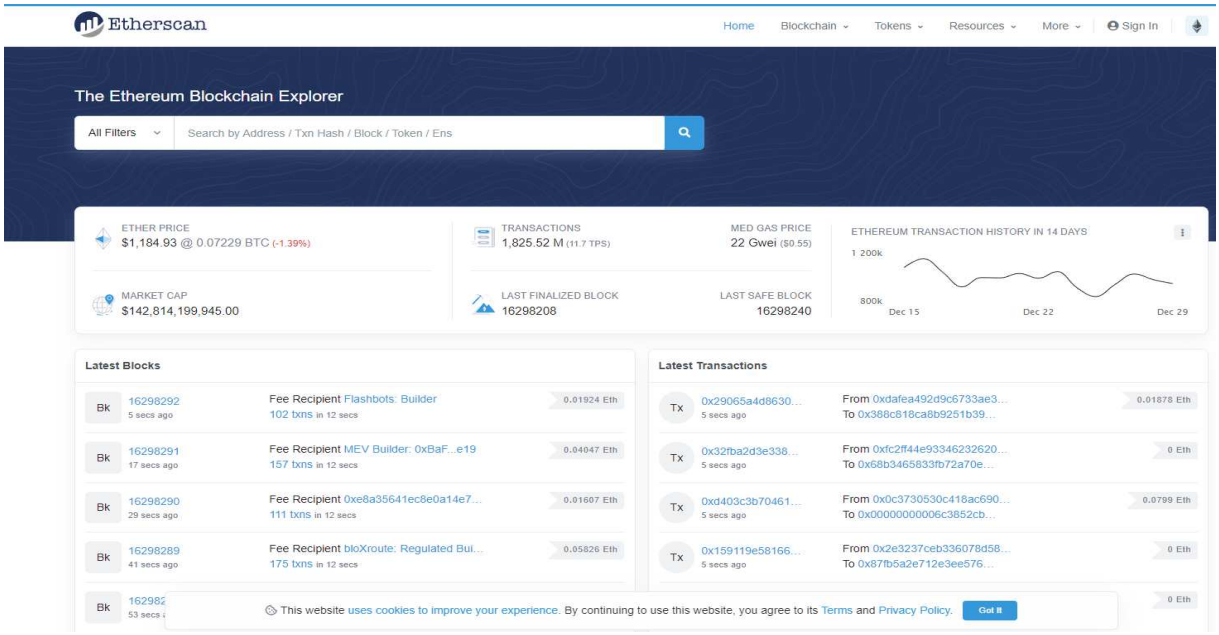
Todas essas informações são compiladas e apresentadas através de uma plataforma WEB, o que permite que qualquer usuário possa explorar a rede da Etherium, sem necessariamente estar ligado a ela. Abaixo, listamos os principais recursos da Etherscan:

1. Pesquisa por endereços: A ferramenta permite que os utilizadores pesquisem por qualquer endereço Ethereum, visualizando todas as transações que foram feitas por aquele endereço, assim como o saldo disponível de Ether para o mesmo.
2. Pesquisa por transações: Através do código hash de uma transação, é possível recuperar todos os detalhes envolvidos na operação, como por exemplo, o endereço de quem executou a transação, a quantidade de ether envolvida, gas utilizado, e informações de data e hora da efetivação.
3. Pesquisa por blocos: As informações incluídas em determinado bloco, assim como outros dados ligados a ele, também podem ser acessadas através da Etherscan.
4. Pesquisa por contratos inteligentes: Umas das características mais interessantes da Etherscan, é a sua capacidade de interação com os contratos que estão armazenados na rede, além de detalhar os dados de implementação do contrato, como a conta de origem, custos envolvidos, data e hora da transação, nós podemos interagir com os contratos, verificando as suas funções e variáveis. Por fim todas as transações que utilizaram o contrato alvo, também podem ser listadas (PERRYMAN, 2019).

O alto nível de detalhamento das informações apresentadas, a popularidade da ferramenta e a sua adoção por parte de grandes companhias de tecnologia, foram os atrativos para a sua utilização neste trabalho.

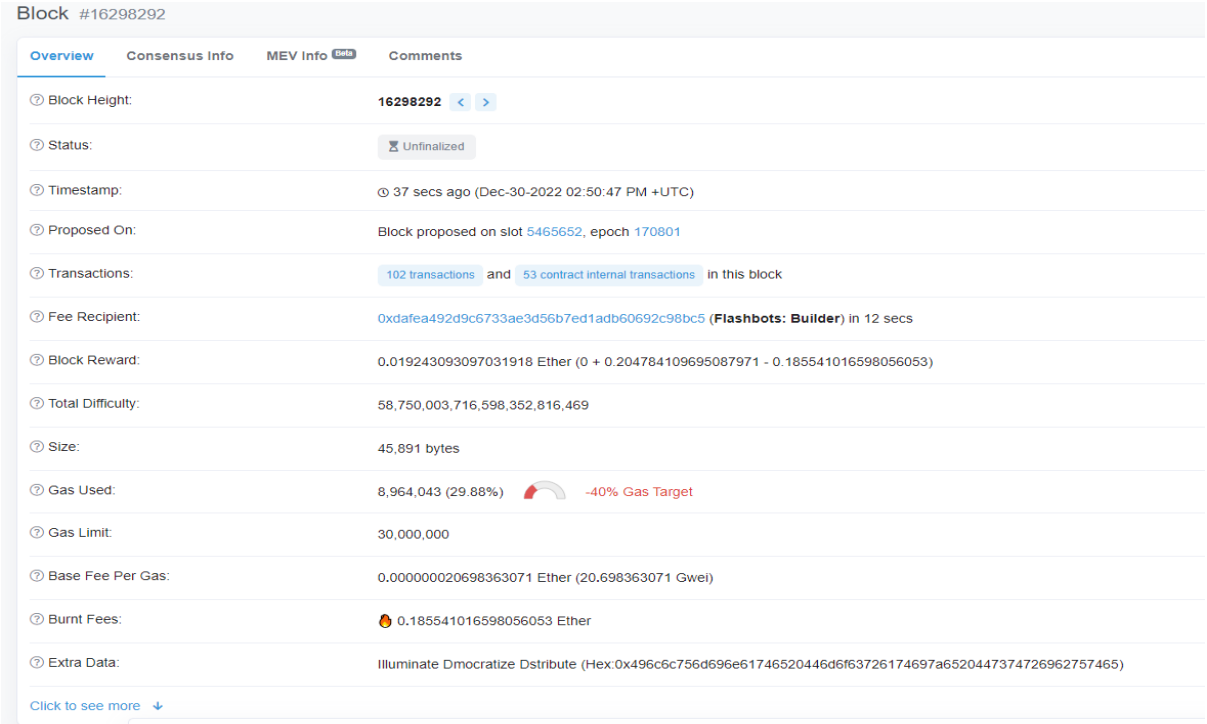
Na figura 14 e 15, podemos observar de forma sequencial o dashboard inicial da ferramenta, e as informações de um determinado bloco escolhido de forma aleatória.

Figura 14: Painel principal do Etherscan



Fonte: Etherscan, 2023

Figura 15: Informações sobre um bloco específico na blockchain



Fonte: Etherscan, 2023

4.2. Desenvolvimento

No presente item serão descritos os processos envolvidos na construção da nossa aplicação e experimento, além de uma sucinta demonstração sobre como funcionará a dinâmica de interação entre todos os sistemas envolvidos.

A intenção inicial seria utilizar a linguagem de programação Java como base para o desenvolvimento do sistema, porém durante o processo de escrita do código resolvemos alterar a linguagem adotada para o PHP devido a sua maior flexibilidade, facilidade de desenvolvimento, extensa comunidade ativa de programadores e analistas, e da sua maior preferência em termos de utilização na construção de sistemas WEB conforme visto no Gráfico 1.

O processo de desenvolvimento pode ser desmembrado através dos seguintes passos:

1. Desenvolvimento do contrato inteligente.

2. Processo de implementação do contrato inteligente em uma das redes de testes da Etherium, processo conhecido como *smart contract deployment.*
3. Codificação do *back-end* utilizando a linguagem PHP, e a biblioteca Simple_web3_php.
4. Integração da *back-end* como uma das aplicações já existentes capazes de manipular um ou vários itens do acervo acadêmico.

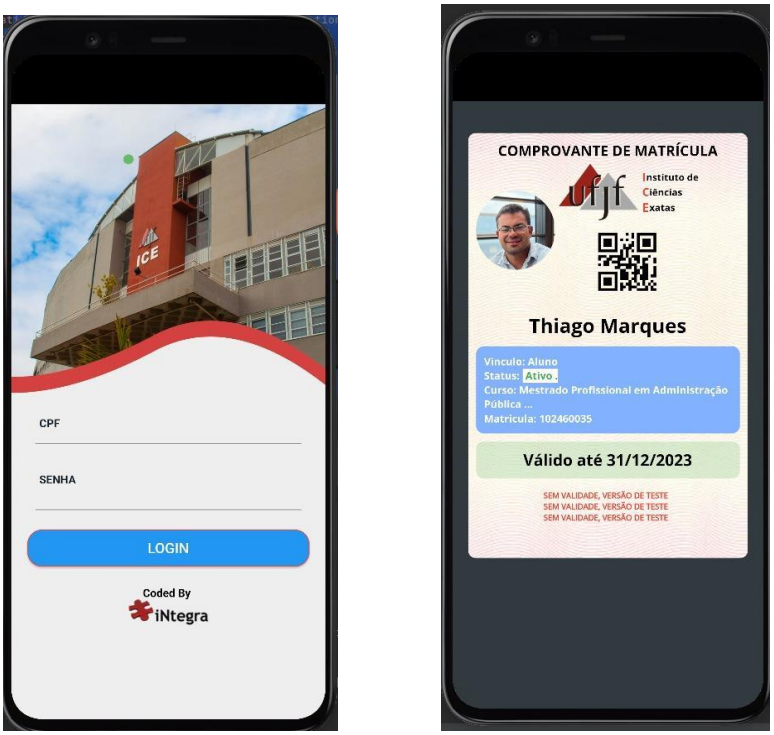
4.2.1. Dinâmica de interação entre os sistemas.

Nosso objetivo é garantir e assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico, utilizando a tecnologia *blockchain* como base, e para isso vamos utilizar o aplicativo ICEapp como aplicação que fará a interface entre o nosso sistema e o usuário final.

O ICEapp é um aplicativo para dispositivos móveis (Android e iOS), que está sendo desenvolvido pelo Instituto de Ciências Exatas (ICE) através do Núcleo de Recursos Computacionais (NRC), ele tem como finalidade fornecer um conjunto de recursos e facilidades para servidores e alunos. Uma versão inicial já se encontra disponível nas plataformas de instalação, porém apenas alguns módulos estão disponíveis aos usuários finais. A expectativa é de que novas funcionalidades sejam adicionadas nos próximos meses.

Um dos recursos que será disponibilizado é o comprovante de matrícula do aluno, e é através dessa funcionalidade já disponível nas versões de testes, que iremos realizar a integração, testes e a avaliação do nosso trabalho, conforme ilustrado na figura 16.

Figura 16: ICEapp - Comprovante de matrícula.



Fonte: Autor

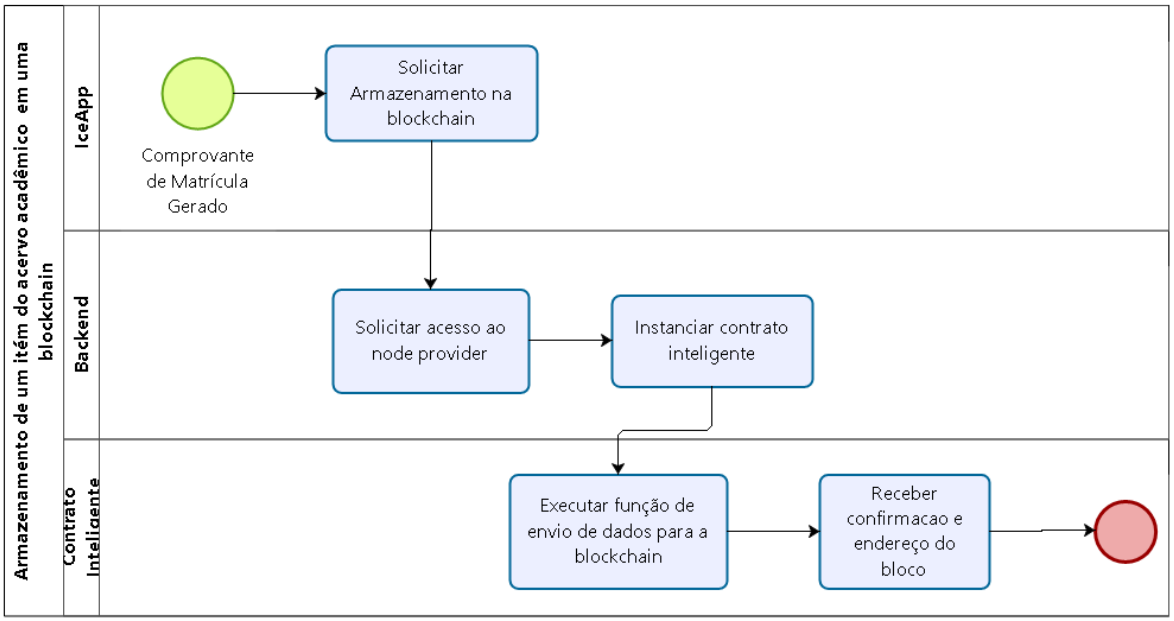
Ao receber uma solicitação de geração de comprovante de matrícula o aplicativo consulta a API ou banco de dados da instituição, e caso o aluno esteja devidamente matriculado, a instituição de ensino informa os dados ao aplicativo que posteriormente envia essas informações através de uma requisição HTTP segura até o servidor onde se encontra o nosso *back-end*.

O *back-end* recebe essa conexão, confirma as credenciais de acesso, e inicia o processo de envio desses dados até a rede *blockchain* Ethereum. A transmissão destes dados do *back-end* até a rede blockchain é feita através da biblioteca *Simple* Web3 PHP, descrita no item 4.1.3 deste trabalho, ela requisita acesso a rede blockchain através da *node provider* Infura utilizando a os dados de acesso da plataforma, assim que o *back-end* estabelece uma conexão com o Infura, os dados do contrato inteligente que foi desenvolvido e implementado pela instituição são carregados.

De posse da instância do contrato inteligente, o *back-end*, realiza uma chamada à função que irá persistir as informações do estudante na *blockchain*, caso a operação seja concluída com sucesso, uma mensagem contendo o endereço do bloco que armazena a informação é

apresentada, esse endereço pode ser utilizado para resgatar esses dados sempre que for necessário. Um diagrama representando a dinâmica de interação do sistema é apresentado na figura 17.

Figura 17: Diagrama de Funcionamento



Fonte: Autor

4.2.2. Desenvolvimento do Contrato Inteligente.

O Primeiro passo do nosso processo de desenvolvimento consiste na elaboração do código do contrato inteligente, o conceito de *smart contracts* já foi abordado na seção 2.3.15.3 do presente trabalho, portanto não iremos nos delongar em definições e conceitos.

Vamos começar criando a estrutura de dados que irá armazenar as informações do item do acervo acadêmico. Como pretendemos armazenar dados de documentos diversos, ou seja, de forma generalista, optamos por criar apenas quatro campos, que poderão ser utilizados de forma flexível por várias aplicações.

O Solidity, linguagem utilizada para se programar contratos inteligentes possui um recurso chamado de *struct*, uma *struct* é um tipo de dados que diferente dos tipos primitivos mais conhecidos como inteiro, texto, decimal, pode ser construído para representar os atributos de classes de objetos da vida real (MODI, 2018), por exemplo: através do *struct*, poderíamos

construir o tipo de dados aluno, que possuiria os seguintes campos nome, matrícula, CPF, curso, data de ingresso conforme demonstrado na figura 18.

Figura 18: Struct Aluno, código fonte em *Solidity*

```
8   struct Aluno{
9       uint matricula;
10      string nome;
11      uint cpf;
12      uint dataIngresso;
13  }
```

fonte: Autor

Em nossa aplicação, vamos construir uma estrutura semelhante ao exemplo da figura acima, utilizando cinco campos para armazenar os dados providos pelo utilizador. Os campos são: nome da pessoa; tipo de acervo; tipo de documento; número do documento; dados extras, este último poderá ser utilizado, quando necessário, para armazenar qualquer conjunto de informações adicionais, incluindo dados binários como imagens ou outros arquivos, sua implementação está exposta na figura 19. É importante salientar que a intenção do presente estudo não é buscar a modelagem conceitual perfeita, portanto, a formulação da estrutura de dados e seleção das informações que deverão ser armazenados, serão tratadas de forma superficial e os nossos esforços se voltaram ao processo de envio e recuperação segura dos dados à blockchain da Ethereum.

Figura 19: *Struct* documento, código fonte em *Solidity*

```
8   address private owner;
9       struct Documento{
10          uint id;
11          string tipoAcervo;
12          string nomePessoa;
13          string tipoDocumento;
14          string numeroDocumento;
15          string dados;
16      }
```

Fonte: Autor

Em seguida, precisamos montar a estrutura que vai conter, organizar e sequenciar cada objeto do tipo documento, o Solidity, possui a instrução *map*, que possibilita a criação de uma espécie de dicionário contendo informações que possam ser acessadas e pesquisadas através de uma indexação. Sua implementação é mostrada na figura 20.

Figura 20: *Mapping*, código fonte em *Solidity*

```
15    mapping (uint => Documento) public documentos;
```

Fonte: Autor

Antes de prosseguirmos com as funcionalidades que viabilizarão a inserção e busca de conteúdo na blockchain, vamos escrever o código que será responsável por garantir que apenas uma determinada conta possa utilizar a nossa aplicação para armazenar as informações na blockchain, ou seja, queremos que qualquer conta possa consultar os dados ligados aos nossos documentos, porém apenas a conta da instituição de ensino vai estar autorizada a manter esses dados.

Portanto, como visto nas figuras 21 e 22 no método *constructor*, (um método especial que é executado uma única vez, apenas quando o contrato é enviado para blockchain), nós armazenamos o endereço da conta que está fazendo o *deploy* do contrato, e depois, através do recurso conhecido como modificador, utilizamos essa informação para que se alguma outra conta realize a tentativa de inserir uma informação, ela seja impedida e seja alertada através de uma mensagem de erro.

Figura 21: Método constructor, código fonte em *Solidity*.

```
31    constructor() public {
32        console.log("Proprietario do contrato deployed by: ", msg.sender);
33        owner = msg.sender; // 'msg.sender' is sender of current call,
34                            // contract deployer for a constructor
35        emit OwnerSet(address(0), owner);
36      memberCount = 0;
37    }
```

Fonte: Autor.

Figura 22: Modificador isOwner, código fonte em *Solidity*.

```
// modificador para conferir se quem esta utilizando a conta é o proprietario
modifier isOwner() {
    // If the first argument of 'require' evaluates to 'false', execution terminates and all
    // changes to the state and to Ether balances are reverted.
    // This used to consume all gas in old EVM versions, but not anymore.
    // It is often a good idea to use 'require' to check if functions are called correctly.
    // As a second argument, you can also provide an explanation about what went wrong.
    require(msg.sender == owner, "Caller is not owner");
    _;
}
```

Fonte: Autor.

Após criarmos a estrutura de dados que receberá as informações oriundas das Instituições de Ensino, vamos construir a função que efetivamente as enviará para blockchain. Nomeamos a função como addDados. Essa função está demonstrada na figura 23 e recebe como parâmetro as informações que foram enviados através da aplicação externa, é uma função relativamente simples que basicamente atribui as informações recebidas ao *map* criado anteriormente no código, no momento em que esses dados são colocados no *map*, os próprios mecanismos internos da linguagem se encarregam de armazenar as novas informações de forma persistente na *blockchain*.

Figura 23: Função addDados, código fonte em *Solidity*.

```
53    function addDados(string memory _tipoDocumento,uint  _codTipo,str
    memory _nomePessoa,string memory _dados, uint  _validade) public {
54      documentos[memberCount] = Documento(memberCount,_codTipo,_tipoD
    _nomePessoa,_dados,_validade);
55      memberCount++;
56    }
```

Fonte: Autor

Agora precisamos recuperar os dados que foram armazenados dentro da *blockchain*, para isso criamos a função getDados, apresentada na figura 24, essa função recebe como parâmetro o código identificador do registro, e retorna os dados referentes ao mesmo. Ao ser invocada, a referida função realiza uma iteração na *blockchain* a fim de localizar as informações requisitadas. Assim que essas informações são encontradas, a função procede à devolução de

uma instância da estrutura de dados previamente estabelecida no início do código populada com os dados do documento.

Figura 24: Função getDados, código fonte em *Solidity*.

```
65    //return Array of structure Value
66    function getDados() public view returns (uint[] memory, string[]
    memory,string[] memory,string[] memory){
67        uint[]    memory id = new uint[](memberCount);
68        string[]  memory tipoDocumento = new string[](memberCount);
69        string[]  memory nomePessoa = new string[](memberCount);
70        string[]  memory dados = new string[](memberCount);
71
72        for (uint i = 0; i < memberCount; i++) {
73            Documento storage member = documentos[i];
74            id[i] = member.id;
75            tipoDocumento[i] = member.tipoDocumento;
76            nomePessoa[i] = member.nomePessoa;
77            dados[i] = member.dados;
78        }
79
```

Fonte: Autor.

É possível observar que as funções apresentam uma relativa simplicidade e são desenvolvidas com uma quantidade reduzida de linhas de código, isso se deve a utilização da linguagem Solidity para a manipulação de contratos inteligentes. Essa linguagem estabelece uma camada de abstração altamente eficiente entre a rede blockchain e o programador (HEGEDŰS, 2018), em outras palavras, muitos dos recursos complexos, como a criação de blocos, a validação e a busca de informações em uma blockchain, são encapsulados na linguagem e realizados de maneira transparente e automática.

4.2.3. Implantação do Contrato Inteligente

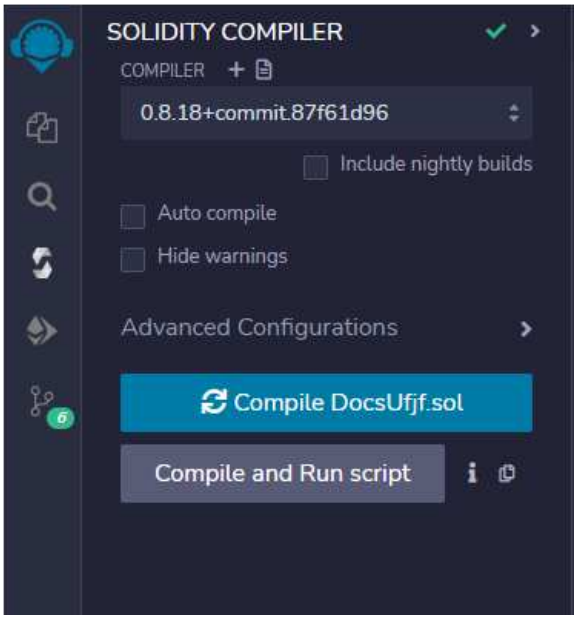
Uma vez que o código do nosso contrato inteligente é escrito, nós precisamos enviá-lo e implanta-lo na rede *blockchain*, etapa conhecida como *deployment*. O processo de *deployment* consistem na compilação do código escrito em Solidity para *bytecodes,* que são interpretados pela EVM (Etherium Virtual Machine), posteriormente uma instância desse contrato é criada e

enviada para a rede *blockchain* escolhida, assim que ele é alocado em um bloco, o usuário recebe um endereço que aponta para a instância do contrato. Conforme GÓRSKI (2021), é por meio deste endereço que podemos realizar consultas e alocar novas informações na blockchain.

Para realizar o nosso *deployment*, utilizaremos a ferramenta REMIX, a mesma ferramenta utilizada para escrever o código do nosso contrato inteligente.

Inicialmente iremos realizar a compilação, ao ser solicitada, a ferramenta verifica o código fonte escrito e procura por erros de sintaxe, uma vez que o código se encontre sem erros ele é transformado em linguagem de máquina (*bytecodes*), que pode ser interpretada pelo emulador da Ethereum. Na figura 25 podemos observar a interface do REMIX responsável pelo início do processo de compilação do contrato inteligente.

Figura 25: Compilação do contrato inteligente.



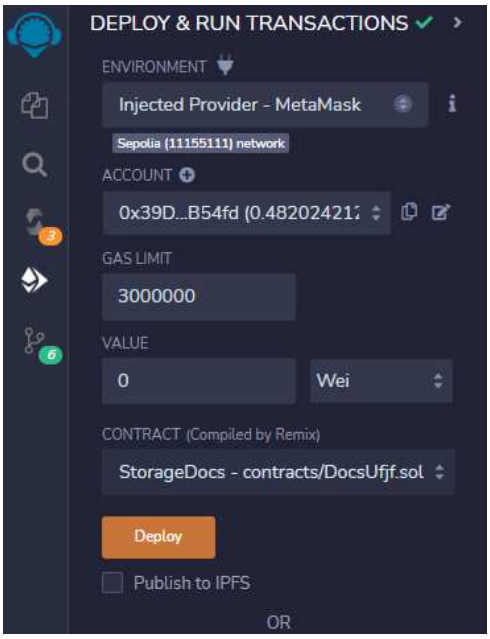
Fonte: Autor.

Após o processo de compilação vamos efetivamente enviar o nosso contrato inteligente para a *blockchain*. Nesse instante algumas informações precisam ser declaradas previamente: o endereço da nossa carteira virtual, o limite máximo de custos que estamos dispostos a pagar pela operação, e a rede Ethereum para qual gostaríamos de implementar o contrato. Conforme visto no item 2.3.15 deste trabalho, a Ethereum possui algumas redes de testes, e durante o desenvolvimento foi necessário realizar por duas vezes a migração do projeto para outras redes,

pois aquelas que vieram a ser escolhidas foram colocadas em estado de obsoletas pelos responsáveis pela tecnologia e consequentemente pararam de receber atualizações por parte da equipe de desenvolvedores do Ethereum.

Na figura 26 podemos observar a área responsável pelo *deployment* dentro do REMIX Após enviar o comando de *deploy*, uma instância do nosso contrato inteligente é enviada à rede.

Figura 26: *Deploy* do contrato inteligente.



Fonte: Autor.

Observe que após o envio para a *blockchain*, o processo de *deployment* está concluído. Nesse momento recebemos o endereço que identifica a instância do contrato, conforme evidenciado na imagem 27.

Figura 27: Conclusão do *deployment* e recebimento do endereço do contrato.

Fonte: Autor.

Um ponto importante nesse processo *deployment*, é o seu custo. Para que o contrato seja inserido na *blockchain*, existe um trabalho computacional que foi executado por outros nós da rede, esse trabalho é recompensado através de uma taxa paga pelo utilizador, nas próximas sessões nós iremos avaliar todos os custos envolvidos nas operações.

4.2.4. Codificação do *back-end*

Agora que já possuímos uma instância do nosso contrato inteligente persistida na blockchain, vamos proceder a codificação do sistema que irá fazer a ponte entre o contrato que está na rede e nossa aplicação disponível ao usuário final,

Para isso nós vamos utilizar a "Simple-Web3-Php", biblioteca já descrita no item 4.1.3 deste trabalho.

A primeira parte do código, como visto nas figuras 28 e 29, consiste em carregar a biblioteca Simple Web3 Php, e atribuir as informações relativas à nossa conta ethereum, endereço do contrato, chaves de acesso e endereços de pontos de acesso.

Figura 28: Atribuindo as informações às variáveis, código fonte escrito em PHP

```php
// DADOS DO INFURA
define('INFURA_PROJECT_ID', '2ed5a6862d094462b80099336832982f');
define('INFURA_PROJECT_SECRET', '[illegible]');
//NOME DA REDE ETHEREUM UTILIZADA
define('ETHEREUM_NET_NAME', 'sepolia'); //ropsten , mainnet
//ENDEREÇO DA INSTANCIA DO CONTRATO
define('SWP_Contract_Address','0x63e25adFD6a6e0D374d9111FdEe6fF2Af61fE709');


//REAL endpoint, this is what is really used internally
define('ETHEREUM_NET_ENDPOINT', 'https://'.ETHEREUM_NET_NAME.'.infura.io/v3/'.INFURA_PROJECT_ID);
```

Fonte: Autor.

Figura 29: Carregando a biblioteca *Simple* Web, código fonte em PHP

```php
//Carregando a biblioteca Sweb3,
use SWeb3\SWeb3;
$sweb3 = new SWeb3(ETHEREUM_NET_ENDPOINT);

//Atribuindo informações às variaveis

//Endereço da carteira
$from_address = '0x39D1275cd84F8dA04808D0d9F6EbbB1e804B54fd';
//Chave privada relativa a carteira
$from_address_private_key = '[illegible]
$sweb3->setPersonalData($from_address, $from_address_private_key);
$sweb3->chainId = '11155111 ';//Sepolia
```

Fonte: Autor.

Na segunda parte (figura 30), vamos carregar as variáveis com os dados que vieram da aplicação final e que serão enviadas à blockchain.

Figura 30: Carregando as variáveis oriundas do ICEapp, código fonte em PHP

```php
$send_data = new stdClass();
    $send_data->id = $_POST['id'];
    $send_data->tipoDocumento =  $_POST['tipoDocumento'];
    $send_data->dados =  $_POST['dados'];
    $send_data->nomePessoa = $_POST['nomePessoa'];
```

Fonte: Autor.

Por fim, vamos inicializar a instância do contrato inteligente que já está armazenada na blockchain e utilizar a função addDados para efetivamente alocar as informações que recebemos do acervo acadêmico, através da aplicação final, podemos observar a estrutura é conteúdo da função através da figura 31.

Figura 31: Inicializando a instância do contrato inteligente e chamando a função addDados

```php
//Inicializando a instancia do contrato
$contract = new SWeb3_contract($sweb3, SWP_Contract_Address, $SWP_Contract_ABI);

//get the nonce
 $extra_data = ['nonce' => $sweb3->personal->getNonce()];

 //Chamando a função do contrato inteligente
$res = $contract->send('addDados',$send_data,$extra_data);
```

Fonte: Autor

O resultado da operação de envio é armazenado na variável denominada "$res". Essa variável é responsável por indicar se o processo ocorreu conforme o esperado, confirmando assim que as informações foram adequadamente registradas na blockchain. Nesse contexto, além do endereço do bloco onde as informações foram armazenadas, uma chave exclusiva que identifica a transação também é retornada. Por outro lado, caso algum erro seja encontrado durante o processo, a variável "$res" irá conter um código de erro específico, juntamente com uma descrição detalhada do problema ocorrido.

Uma vez mais, podemos observar a simplicidade do código, a qual é atribuída, em grande parte, à utilização da biblioteca Simple Web3 PHP. Essa biblioteca abstrai a maioria das operações complexas por meio de funções simplificadas, proporcionando maior praticidade e rapidez no desenvolvimento e maior facilidade de manutenção do código quando necessário.

4.3. Teste e Avaliação

Conforme mencionado no item 3.2 do presente estudo, os testes e avaliações serão realizados por meio de simulações, com o intuito de comprovar a capacidade da ferramenta em cumprir os objetivos propostos. As simulações utilizarão o ICEapp como interface com o usuário, reproduzindo a dinâmica habitual de geração do comprovante de matrícula por meio do aplicativo. Todas as simulações serão conduzidas na rede de testes Ethereum Sepolia. A Sepolia é uma das redes de testes oficiais existentes no ecossistema do Ethereum, e é utilizada pelos desenvolvedores a testarem os seus aplicativos antes de enviá-los à principal rede de produção (WACKEROW, 2023). Além de determinar a eficácia da ferramenta, neste tópico também realizaremos uma análise dos recursos consumidos em cada interação.

4.3.1. Geração do comprovante de matrícula via aplicativo.

Como a parte que engloba a comunicação entre o aplicativo e a Instituição, assim como sua comunicação com o *back-end* não se enquadram dentro do escopo do nosso trabalho, nossa avaliação se inicia a partir da interação entre o *back-end* e a rede *blockchain*.

Neste cenário encontramos a situação típica de utilização da ferramenta, o usuário através do aplicativo realiza a solicitação do seu comprovante de matrícula, quando a sua emissão é autorizada pela instituição, o aplicativo se comunica com o *back-end* da ferramenta que por sua vez realiza a interação com o contrato inteligente e com a *blockchain*, em casa de sucesso, o *hash* de identificação da transação assim como o código identificador do registro é retornado através dos sistemas até chegar ao usuário final, de posse desse código é possível realizar a consulta do registro da blockchain.

A versão utilizada do aplicativo é uma versão de testes não disponível aos usuários finais, nossa *back-end*, também foi desenvolvido em uma plataforma externa e não possui

qualquer tipo de interação com a base de dados oficial da Instituição, e por fim, toda a comunicação realizada com a *blockchain* implementada em umas das redes de testes disponibilizada pelos próprios desenvolvedores do Ethereum, a rede Sepolia, portanto, conforme as informações expostas, podemos afirmar que toda a simulação foi realizada em ambiente controlado e não implica em qualquer tipo de interação com os ambientes de produção da Instituição de Ensino ou da rede *blockchain* Mainnet utilizada nas transações reais.

4.3.1.1. - Conta/Endereço da Carteira

Um endereço/conta de carteira digital foi criado através do Metamask aplicativo que permite criar e manter endereços de carteiras de Ethereum, além da criação, através do Metamask é possível acompanhar todas as interações que envolvem a sua conta.

A conta que foi criada e que será utilizada para enviar os dados à blockchain é identificada pelo seguinte endereço: 0x39D1275cd84F8dA04808D0d9F6EbbB1e804B54fd, esse mesmo endereço foi utilizado para realizar o *deployment* do contrato inteligente. Durante a programação do nosso código definimos que somente a carteira que responsável pelo *deployment* do contrato está autorizada a utilizá-lo para enviar as informações à blockchain. Em outras palavras, apenas a instituição poderá armazenar os dados do item do acervo acadêmico na *blockchain*

4.3.1.2. Faucets

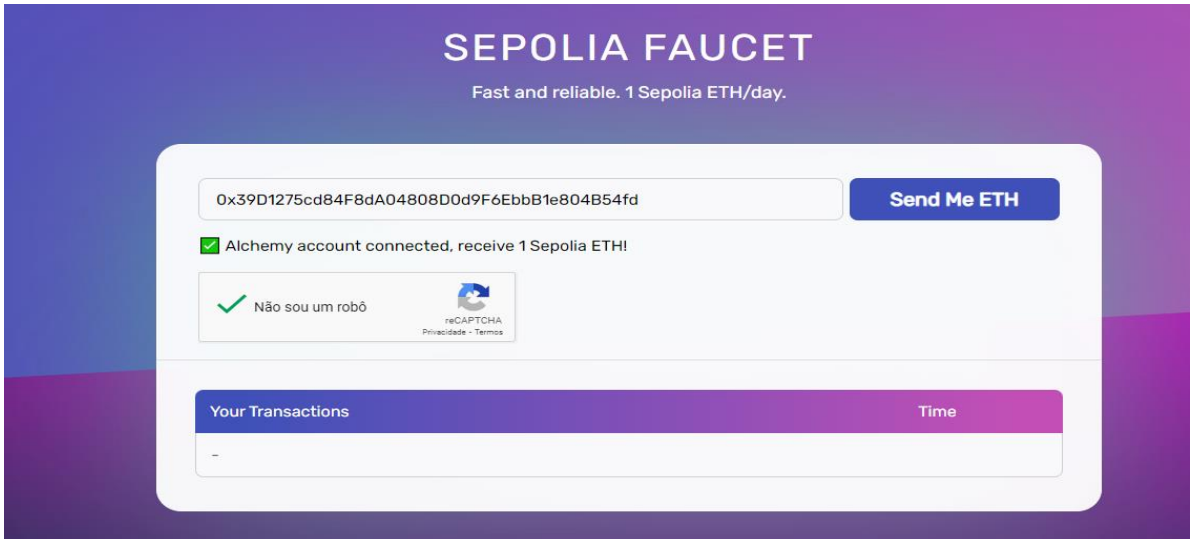
Quando uma informação é adicionada a uma rede blockchain, uma série de trabalhos computacionais e matemáticos são realizados, de forma geral essas operações são executadas por nós da rede que são recompensados de alguma forma, no caso das redes Ethereum essa recompensa se dá através do pagamento de criptomoedas conforme visto nas seções 2.3.15. Nas redes de testes como a Sepolia, essa dinâmica é a mesma, e portanto, além das taxas envolvidas, todos os nós que participam da interação devem ser recompensados através do pagamento de *Ether*. É importante ressaltar que, embora o consumo de Gas de cada operação seja o mesmo na Mainnet e nas redes de teste, o preço de cada unidade de Gas varia entre as redes, visto que

a demanda, tamanho da blockchain, e quantidade de nós ativos determinam o seu valor (COOK, 2023).

Como estamos utilizando uma rede de testes não faria sentido utilizarmos dinheiro real. Por isso utilizamos os Faucets, que são sites que disponibilizam de forma gratuitamente Ether que pode ser utilizado apenas em redes de testes.

Para a execução dessa simulação utilizaremos o *faucet* em https://sepoliafaucet.com/, após realizarmos um cadastro simplificado, adicionamos o endereço da nossa carteira no campo relacionado, e solicitamos o envio do valor de 1 ether. A interface do Faucet, pode ser vista na figura 32.

Figura 32: Sepolia Faucet

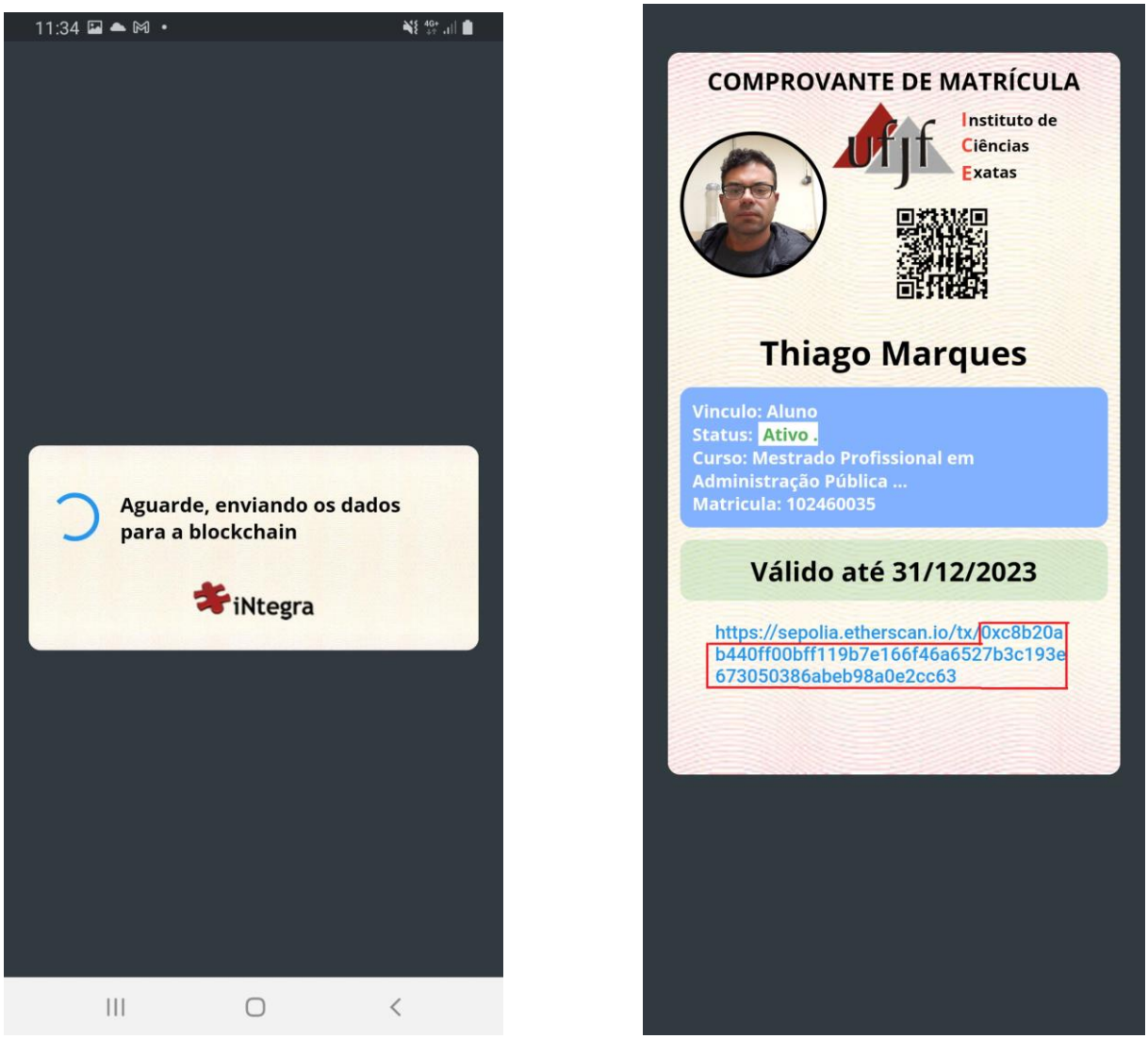


Fonte: sepoliafaucet.com, (2023).

4.3.1.3. Armazenando as Informações na blockchain

Por meio da versão de testes do ICEapp, o usuário requisitou a emissão do comprovante de matrícula. Após a autorização da instituição e o envio das informações para o aplicativo, foi realizado de maneira transparente uma solicitação ao back-end para que este enviasse os dados à blockchain. Somente após esse processo, o aplicativo apresentou os dados do estudante na tela. Uma captura de tela dessa operação está evidenciada na figura 33.

Figura 33: ICEapp, enviando os dados à blockchain.



Fonte: Autor.

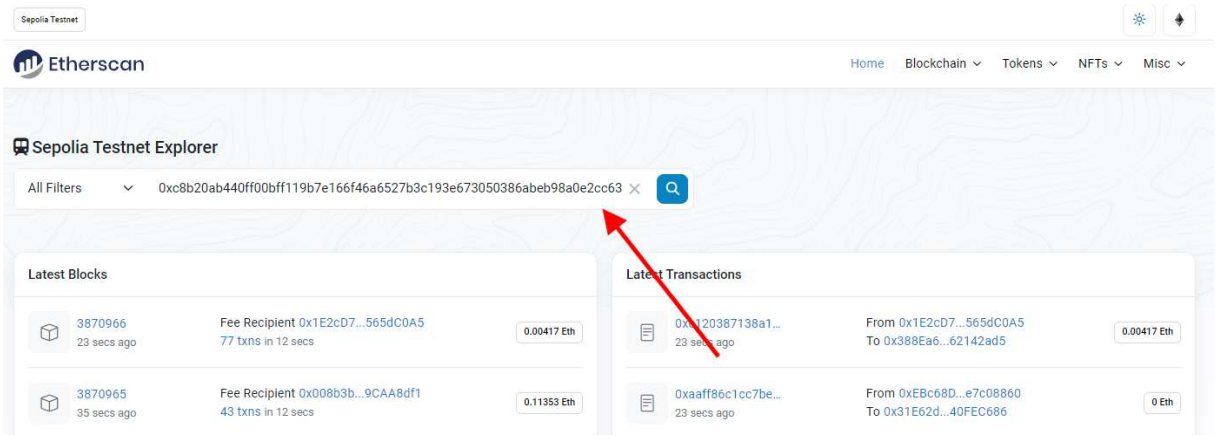
A operação foi completada em 5 segundos e ao final, o *back-end* apresentou a mensagem informando que a operação havia sido bem sucedida, o código *hash* da transição "0xc8b20ab440ff00bff119b7e166f46a6527b3c193e673050386abeb98a0e2cc63" foi exibido ao usuário.

4.3.1.4. Informações da Transação

De posse do código hash da transição, vamos utilizar a ferramenta Etherscan, apresentada na seção 4.1.4 deste trabalho, para proceder com as análises.

Para isso vamos acessar a ferramenta através do seu endereço WEB https://sepolia.etherscan.io/ e utilizar o endereço *hash* recebido através do *backend* e exposto no ICEapp para realizar a busca do recibo da transação através do campo em destaque na figura 34.

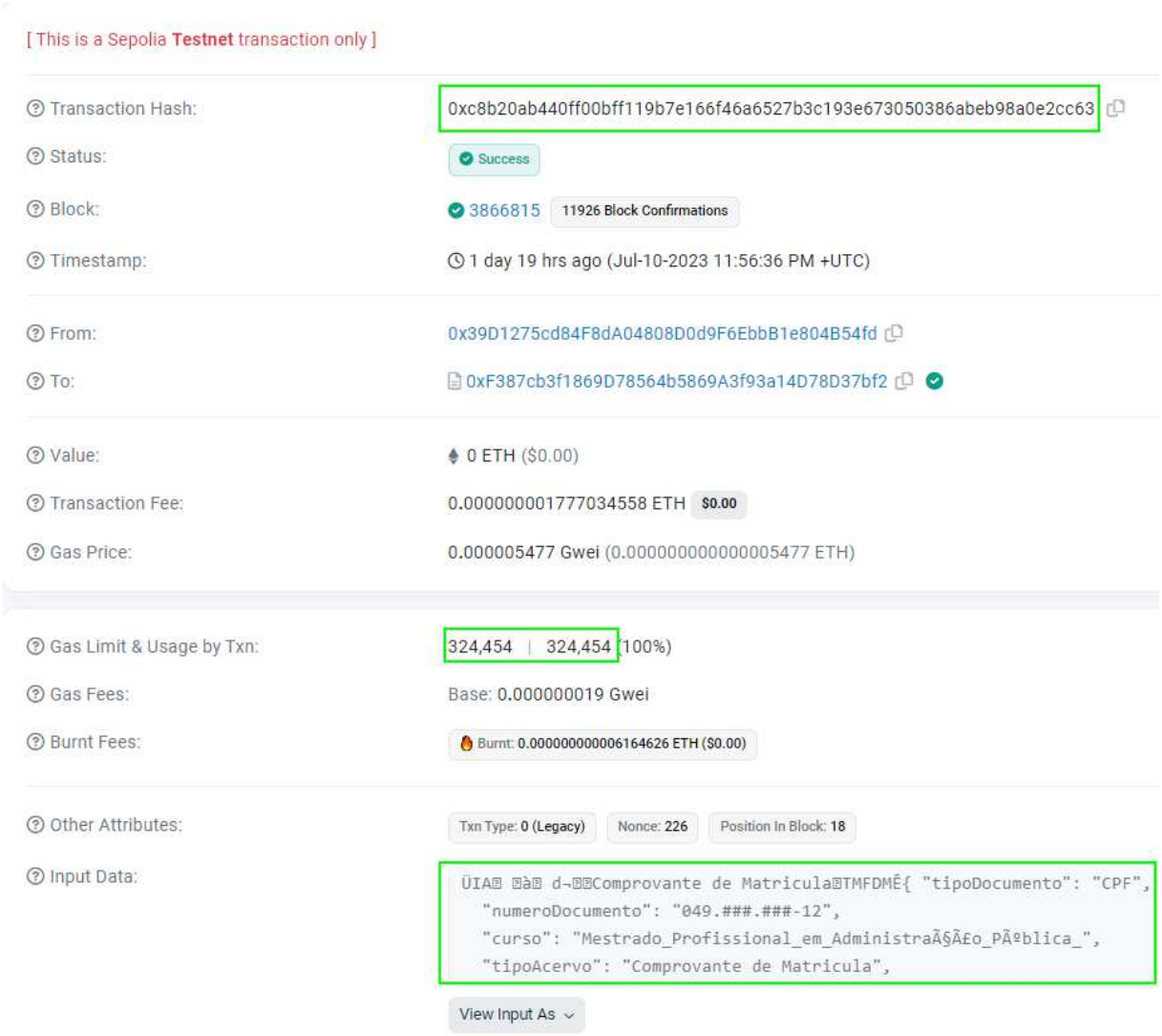
Figura 34: Busca de informações através do código hash da transação.



Fonte: Adaptado de Etherscan, 2023.

Em caso de sucesso na busca, a ferramenta no retorna todas as informações referentes a transação, na nossa simulação os dados foram resgatados corretamente e foi apresentado o recibo da transação conforme demonstrados na figura 35:

Figura 35: Comprovante de registro da transação da rede Ethereum



Fonte: Adaptado de Etherscan, 2023.

O recibo exibido na figura 35, é capaz de nos fornecer informações relevantes relacionadas à nossa transação.

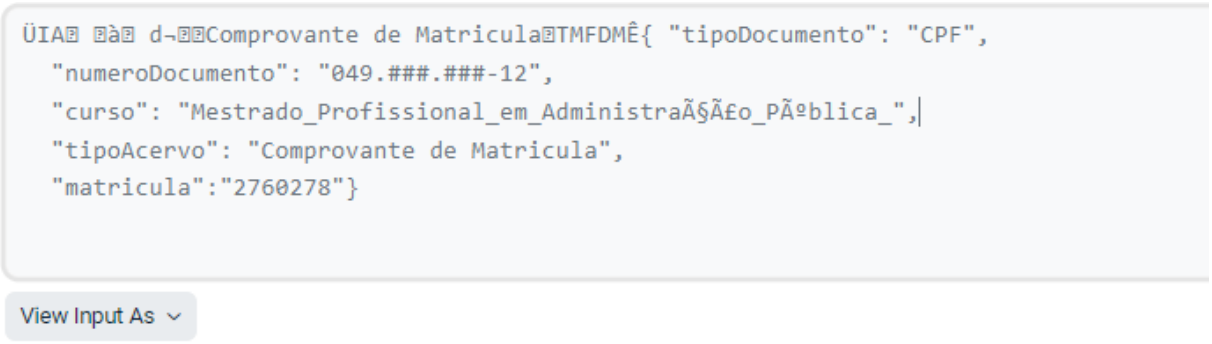
O primeiro campo é o "*Transaction Hash"*, ele é o identificador único de cada transação ocorrida na *blockchain*, o segundo campo é "*status"*, ele nos mostra se a operação foi bem sucedida ou não, nesse caso o status está apresentando a palavra "*Success",* ou seja, as informações enviadas foram corretamente mineradas/validadas e já se encontram persistidas na blockchain.

O instante exato em que os dados foram registrados está indicado no campo "*timestamp"*. O campo "*block"* faz referência a qual bloco da *blockchain* as informações foram armazenadas.

Os campos "*from"* e "*to"*, se referem respectivamente ao endereço da conta/carteira utilizada para enviar os dados: 0x39D1275cd84F8dA04808D0d9F6EbbB1e804B54fd; e ao código hash que faz referência ao deploy do contrato inteligente: 0xF387cb3f1869D78564b5869A3f93a14D78D37bf2.

No campo denominado "Input Data", encontram-se todas as informações enviadas pelo contrato inteligente com o intuito de serem armazenadas, ou seja, os dados relativos ao item do acervo acadêmico estão presentes nesse campo.

Figura 36: Informações relativas ao acervo acadêmico, na *blockchain*.



Fonte: Adaptado de Etherscan, 2023.

Como podemos ver na figura 36, os dados do comprovante de matrícula estão organizados através de uma estrutura conhecida com json[10], essa estrutura pode ser convertida para qualquer tipo de arranjo de dados, como tabelas ou textos corridos.

4.3.1.4.1. Custo da Operação

[10]Json é uma estrutura ou formato de dados utilizado quando se deseja trocar informações entre sistemas computacionais diferentes, ele é de fácil leitura tanto para máquina quanto para humanos e representação textual respeita um pequeno conjunto de regras. Um exemplo de informação em formato json seria: {"nome":"João","idade":18} (SMITH, 2020)

Os próximos campos a serem analisados estão relacionados ao custo da operação. No campo "*Gas Limit* & *Usage by* Txn", encontramos, em sequência, o limite de Gas a ser utilizado e o Gas efetivamente consumido durante a interação. Conforme mencionado nas seções 2.3.15 e 4.3.1.2, o Gas é uma unidade de medida que representa o trabalho realizado. O valor de Gas consumido em cada operação permanece o mesmo em todas as redes, porém o preço associado a cada unidade de Gas varia entre a Mainnet e a Sepolia.

Através das declarações anteriores, podemos inferir que, a fim de determinar o custo real de nossa operação, é necessário multiplicar o consumo de Gas da operação pelo preço atual do Gas e, em seguida, pela taxa de câmbio entre o real (BRL) e o Ether (ETH). Essa operação é expressa pela fórmula (1):

$$\mathbf{C = (G \,.\, p).\, e}$$

Onde:
C = custo da operação;
G = consumo de Gas;
p = preço do Gas na Mainnet;
e = cotação do ether (ETH) em real (BRL);

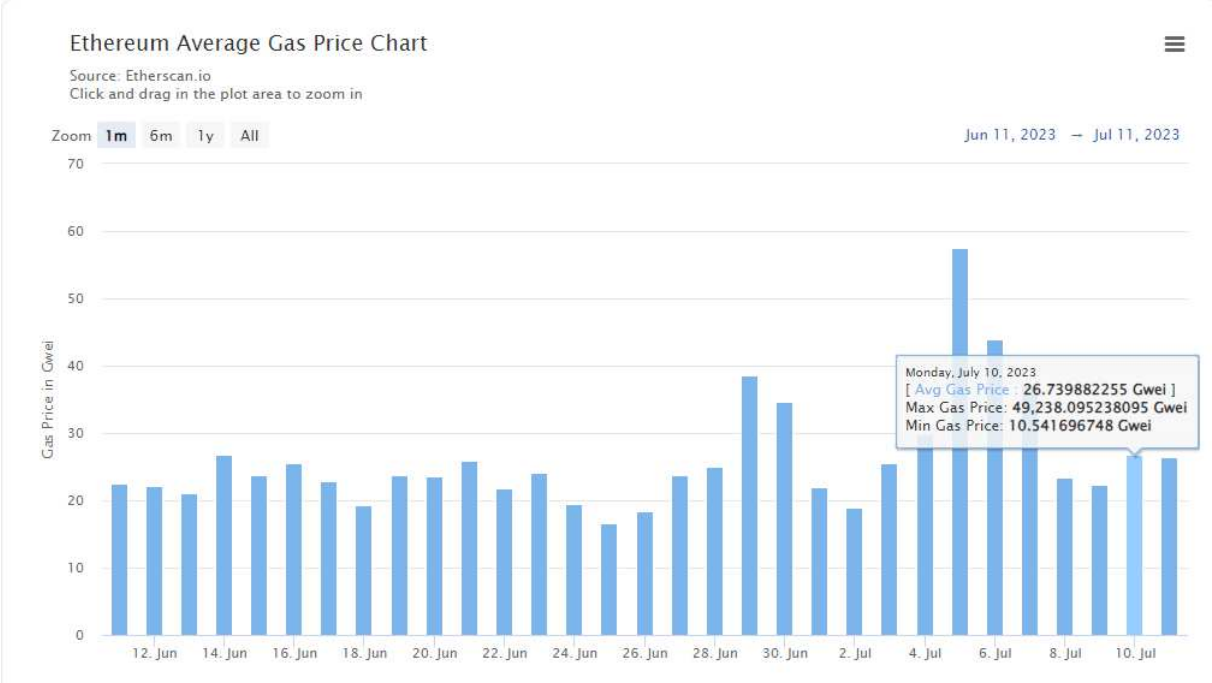
Para que possamos encontrar o custo da operação através da fórmula 1 utilizaremos o valor exposto no campo “Usage by Txn”, que é de 323192, e representa o Gas consumido para armazenar os dados da blockchain. Em seguida iremos buscar o preço do Gas, no entanto, nesse ponto cabe uma ressalva, toda nossa operação foi executada na rede de teste, e portanto o preço do Gas exibido no recibo de transação (figura 35) se refere a essa rede, entendendo que o nosso objetivo é obter o custo da operação em ambiente real, ou seja, na Mainnet, foi necessário encontrar o preço do Gas referente à Mainnet no dia 10 de julho de 2023 neste dia cada Gas possuía o custo médio de 26,74 Gwei, conforme evidenciado no gráfico 2, sabendo que cada Gwei equivale a 0,000000001 de Ether (COOK, 2023), chegamos ao valor de 0,000000027 ether. Por fim, a cotação do ether em real no dia 10 de julho de 2023 foi de R$ 9.276,59 como podemos observar no Gráfico 3. Finalmente, aplicando os valores às variáveis da fórmula 1 temos:

C = 323.192 . 0,000000027 ETH . 9.276,59 BRL/ETH

C= R$80,94

Logo, o custo da nossa operação foi de R$80,94 oitenta reais e noventa e quatro centavos.

Gráfico 2 - Preço médio do Gas



Fonte: Etherscan.io

Gráfico 3 - Preço do ether (ETH) em reais (BRL)

Fonte: Google e Coinmarketcap (2023)

4.3.1.5. Validação da ferramenta

Nesse tópico procederemos à validação da nossa ferramenta a fim de verificar sua capacidade de atingir os objetivos elencados na seção 3.2.

4.3.1.5.1 Garantir que os dados dos documentos estão persistidos na blockchain.

Para conferir esse item, vamos utilizar o código hash que representa o recibo de transação coletado através do *Etherscan* apresentado no item 4.3.1.4 deste trabalho e exposto através da figura 37, e o código hash que foi retornado pelo back-end apresentado na figura 34 do item 4.3.1.3. Inicialmente podemos observar através da figura 34 e 35 que a busca utilizando o código fornecido pelo ICEapp encontrou resultado consistente no Etherscan indicando que a transação foi enviada à blockchain. Podemos fazer uma conferência adicional com objetivo de verificar se os *hashes* possuem o mesmo conteúdo, através da análise do campo "*transaction hash"* do recibo de transação e comparando-o com o hash apresentado no aplicativo.

Figura 37: Retorno do código de transação pela *blockchain*

Fonte: Autor.

Figura 38: Código de transação no Etherscan.

Fonte: Adaptado de Etherscan, 2023.

É possível constatar nas figuras 37 e 38 que o código de transação proveniente do back-end e apresentado ao usuário no aplicativo ICEapp são idênticos. Consequentemente, podemos assegurar que o recibo emitido pelo Etherscan é autenticamente vinculado à operação de emissão do comprovante de matrícula iniciada no ICEapp.

Passemos agora ao campo denominado "*status*", cujo o conteúdo apresentado é: "*success*", evidenciando que a transação foi verificada por um nó minerador e transcorreu conforme o esperado. Consequentemente, todas as informações estão devidamente armazenadas na blockchain (AMIR, 2020). No campo denominado "*input text*", conforme já detalhado na seção 4.3.1.4, encontram-se todas as informações pertinentes ao comprovante de matrícula gerado.

Considerando os fatos assinalados e expostos no último parágrafo, podemos assegurar que os dados referentes ao item do acervo acadêmico foram efetivamente persistidos na blockchain.

4.3.1.5.2 Garantir que os dados não podem ser alterados, e estarão distribuídos de forma descentralizada.

A propriedade da imutabilidade e da descentralização, são características intrínsecas do conceito de blockchain, portanto, uma vez que as informações referentes ao item do acervo acadêmico foram corretamente alocadas na blockchain da Ethereum, conforme vimos na seção 4.3.1.5.1, podemos afirmar que os dados não podem ser alterados e estão distribuídos de forma descentralizada.

5. CONCLUSÃO

O objetivo principal deste trabalho consistiu no desenvolvimento de uma solução apta a armazenar com sucesso as informações relativas a um item do acervo acadêmico em uma rede blockchain pública Ethereum, valendo-se das características mais relevantes dessa tecnologia, como imutabilidade e descentralização. O item selecionado para esse propósito foi o comprovante de matrícula, embora o projeto permita a persistência e recuperação de qualquer documento. Podemos afirmar que esse objetivo foi alcançado de maneira satisfatória, uma vez que os testes e avaliações realizados ao final do experimento confirmaram que as informações enviadas foram devidamente armazenadas na blockchain e, quando solicitadas, puderam ser recuperadas de maneira precisa, sem comprometer a integridade dos dados. Ademais, a adoção de ferramentas *open source* disponíveis surpreendeu de forma positiva a implementação do projeto, agilizando o processo de programação e resultando em um código mais conciso e compreensível.

Apesar do sucesso obtido no experimento, o custo associado às operações pode representar um desafio para a escalabilidade do projeto. Para o envio de um documento contendo aproximadamente 300 caracteres, foram gastos cerca de R$ 80,94 (oitenta reais e noventa e quatro centavos) em taxas relacionadas à interação na blockchain Ethereum. Uma vez que os custos envolvidos nas operações possuem uma relação diretamente proporcional à quantidade de informações manipuladas (ALBERT, 2020), é possível afirmar que valores ainda mais expressivos serão necessários ao enviar documentos mais complexos, com maior volume de dados.

Outro ponto a ser observado ainda relacionado aos custos, diz respeito a volatilidade do preço do Gas, podemos observar no gráfico 2 que variações superiores a 200% podem acontecer em intervalo de dias, levando a uma imprevisibilidade nos custos da operação. Nesse sentido, a adoção de uma estratégia baseada na criação de uma blockchain privada (*permissioned*), compartilhada entre entidades governamentais ou até mesmo organizações internacionais, como tem sido feito no desenvolvimento da Rede Blockchain Brasil (RBB) e pelo CNPQ, parece ser a abordagem mais adequada para a introdução da tecnologia blockchain no setor público.

Por meio do uso de ferramentas *open source* como o Hyperledger Besu, é possível criar redes *blockchain* fundamentadas na tecnologia Ethereum, aproveitando sua capacidade de manipular contratos inteligentes e, consequentemente, seu suporte ao desenvolvimento de dApps, sem necessariamente vincular as interações entre nós e a validação de blocos a taxas atreladas à criptomoeda Ether (GARCIA; RAMACHANDRAN; UEYAMA, 2022).

Seguindo os princípios do design science, compreendemos que o processo de elaboração de nosso artefato, frequentemente referido como "ferramenta" ao longo do texto, pode ser considerado um meio pelo qual o conhecimento foi construído. Isso ocorreu por meio da documentação do código do artefato, do desenvolvimento do referencial teórico, que aborda os conceitos essenciais da tecnologia, e dos estudos relacionados à gestão de documentos na administração pública e sua relação com a tecnologia blockchain, como abordado na seção 2.2. do presente documento.

No que diz respeito a esse último aspecto, podemos afirmar que os governos já deram início às suas jornadas em busca de estudar e implementar soluções que tragam melhorias às rotinas administrativas públicas. No contexto específico do Governo Federal, observamos um movimento de amadurecimento que se iniciou em 2016 e que já resultou em numerosos estudos e ferramentas que adotam a blockchain. Destaca-se o lançamento da Rede Blockchain Brasil (RBB), uma infraestrutura que poderá ser utilizada pelos órgãos da administração pública para implementar soluções que se beneficiam dessa tecnologia, sem depender exclusivamente de redes públicas como a Bitcoin e a Ethereum.

5.1. Limitações

A fim de manter o foco deste trabalho no desenvolvimento da aplicação e sua integração com a blockchain, questões legais, como a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), que aborda os direitos fundamentais de liberdade e privacidade de cada indivíduo (BRASIL, 2018), não foram abordadas. No entanto, caso ocorra uma implementação em um ambiente produtivo de forma escalonada, todas as questões relacionadas à LGPD devem ser devidamente consideradas.

5.2. Trabalhos futuros

No decorrer do processo de elaboração deste trabalho, foram surgindo possíveis direções para o desenvolvimento, sendo a primeira delas relacionada à preservação da privacidade dos dados dos usuários. Em uma blockchain pública, os dados inseridos estão intrinsecamente acessíveis a qualquer pessoa ou algoritmo que deseje consultá-los (ZHENG, 2020). Consequentemente, informações pessoais e sensíveis, como números de documentos oficiais, ficariam expostas e poderiam ser utilizadas de maneira prejudicial aos seus proprietários.

Uma solução viável, que poderia ser elaborada e implementada por meio de um trabalho futuro, consistiria na adoção de uma interface capaz de gerar uma chave criptográfica simétrica. Essa chave seria empregada para criptografar os dados antes de serem armazenados na blockchain. A chave estaria disponível para os usuários ou responsáveis pelos dados e poderia ser fornecida aos terceiros que necessitassem verificar as informações na blockchain. A chave criptográfica e o endereço de acesso à interface poderiam ser representados por um código QR, facilitando sua distribuição.

Considerando os elevados custos envolvidos no armazenamento de documentos na blockchain da Ethereum, seria proveitoso desenvolver um estudo que abordasse e descrevesse o processo de criação de uma blockchain pública/privada. Alternativamente, seria interessante explorar o desenvolvimento de aplicações utilizando a rede de testes da Rede Blockchain Brasil, que já se encontra disponível para experimentação e pode ser utilizada por parceiros interessados em criar soluções relacionadas ao setor público ou de interesse coletivo (TCU, 2022).

REFERÊNCIAS

ALBERT, Elvira et al. Gasol: Gas analysis and optimization for ethereum smart contracts. In: Tools and Algorithms for the Construction and Analysis of Systems: 26th International Conference, TACAS 2020, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020, Dublin, Ireland, April 25–30, 2020, Proceedings, Part II. Cham: Springer International Publishing, 2020. p. 118-125.

ALCARÁS, Bruno. Métodos de Criptografia. Revista The Club. 2010. Disponível em: <http://theclub.com.br/Restrito/Revistas/201011/meto1011.aspx> Acesso em 22 de junho. de 2022

ALNUAIMI, Eiman et al. Blockchain-based system for tracking and rewarding recyclable plastic waste. Peer-to-Peer Networking and Applications, p. 1-19, 2022.

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

ANTONOPOULOS, Andreas M.; WOOD, Gavin. Mastering ethereum: building smart contracts and dApps. O'reilly Media, 2019.

ASTE, Tomaso; TASCA, Paolo; DI MATTEO, Tiziana. Blockchain technologies: The foreseeable impact on society and industry. 2017.

BALCERZAK, Adam P. et al. Blockchain technology and smart contracts in decentralized governance systems. Administrative Sciences, v. 12, n. 3, p. 96, 2022.

BARDIN, Laurence. Análise de conteúdo. São Paulo: Edições 70. 2011

BASHIR, Imran. Mastering blockchain. Packt Publishing Ltd, 2017

BAYER, Dave; HABER, Stuart; STORNETTA, W. Scott. Improving the efficiency and reliability of digital time-stamping. In: Sequences Ii. Springer, New York, NY, 1993. p. 329-334.

BCONNECT entra em uso no início de 2020. 12 dez. 2019. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2019/bconnect-uso-inicio-2020-blockchain-serpro. Acesso em: 26 jul. 2023.

BELOTTI, Marianna. et al. A vademecum on blockchain technologies: When, which, and how. IEEE Communications Surveys & Tutorials, v. 21, n. 4, p. 3796-3838, 2019.

BLOCKCHAINGOV - Forum Blockchaingov Contribuições da blockchain para a transformação digital dos governos. 1 dez. 2018. Disponível em:

https://www.bndes.gov.br/wps/portal/site/home/conhecimento/seminarios/blockchaingov. Acesso em: 26 jul. 2023.

BLOCKCHAINGOV - II Forum BlockchainGov Contribuições da blockchain para a transformação digital dos governos. 29 out. 2019. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/seminarios/II-forum-blockchaingov. Acesso em: 26 jul. 2023.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.303, de 08 de julho de 2015. Dispõe sobre a prestadora de serviços de ativos virtuais; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições

BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasil. Brasília, DF, Edição: 81, Seção: 1, Página: 6.

BRASIL. Lei nº 13.709, de 11 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, ano 130, n. 8, p. 1-74, 14 ago. 2018

BRASIL. Polícia Federal investiga grupo suspeito de falsificação de diplomas de Universidades Federais. Brasília, 31, jan, 2022. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/noticias/2022/02/policia-federal-investiga-grupo-suspeito-de-falsificacao-de-diplomas-de-universidades-federais>. Acesso em: 16 maio. 2022.

BRASIL. Serviços e informações do Brasil. Ferramenta simplifica fornecimento de dados do CNP. 31 fev. 2021. Disponível em: https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/03/ferramenta-simplifica-fornecimento-de-dados-do-cnpj. Acesso em: 6 ago. 2023.

BRASIL. Ministério das Relações Exteriores. Revalidação e reconhecimento de títulos e diplomas. 17 fev. 2022. Disponível em: https://www.gov.br/mre/pt-br/assuntos/cultura-e-educacao/temas-educacionais/revalidacao-e-reconhecimento-de-titulos-e-diplomas. Acesso em: 6 ago. 2023.

BRASIL. Serviços e informações do Brasil. Governo Federal define prazos para conversão de acervo acadêmico para o meio digital. 31 out. 2022. Disponível em: https://www.gov.br/pt-br/noticias/educacao-e-pesquisa/2022/05/governo-federal-define-prazos-para-conversao-de-acervo-academico-para-o-meio-digital#:~:text=A%20Portaria%20nº%20360%20está,1º%20de%20agosto%20de%202022. Acesso em: 6 ago. 2023.

BRASIL. PF desarticula esquema de fraudes de emissões de diplomas de ensino superior no Ceará. Brasília, 30, abr, 2021. Disponível em: <https://www.gov.br/pf/pt-

br/assuntos/noticias/2021/05/pf-desarticula-esquema-de-fraudes-de-emissoes-de-diplomas-de-ensino-superior-no-ceara>. Acesso em: 20 maio. 2022.

BRENNECKE, Martin et al. The de-central bank in decentralized finance: a case study of Maker DAO. In: Proceedings of the 55th Hawaii International Conference on System Sciences. 2022.

BUTERIN, Vitalik et al. A next-generation smart contract and decentralized application platform. white paper, v. 3, n. 37, p. 2-1, 2014

CARDOSO, João Antonio Aparecido; DE SOUZA PINTO, Jefferson. Blockchain e Smart Contracts: Um Estudo Sobre Soluções para Seguradoras. In: Congresso de Gestão, Negócios e Tecnologia da Informação–CONGENTI. 2018

CARRARA, Gabriel R.; MATTOS, Diogo MF; ALBUQUERQUE, Célio VN. Consenso por Localidade: Um Mecanismo de Consenso Leve com Convergência por Vizinhanças para Cadeia de Blocos. In: Anais do IV Workshop em Blockchain: Teoria, Tecnologias e Aplicações. SBC, 2021. p. 13-26.

CASTRO, Renato Q.; AU-YONG-OLIVEIRA, Manuel. Blockchain and higher education diplomas. European Journal of Investigation in Health, Psychology and Education, v. 11, n. 1, p. 154-167, 2021.

COHEN, Fred. Introductory Information Protection, 1995. Disponível em: <http://all.net/edu/curr/ip/>. Acesso em 22 de junho. de 2022.

COOK, Joseph. Gas and fees | ethereum.org. 11 jul. 2023. Disponível em: https://ethereum.org/en/developers/docs/gas/. Acesso em: 14 jul. 2023.

CORRÊA, Otávio Augusto. Estudo da aplicação de estrutura blockchain com proof of stake para arquivamento de documentos com registro no Tempo. - Universidade Federal De Santa Catarina. 2017.

COSTA, Rostand; FAUSTINO, Daniel; LEMOS, Guido; QUEIROGA, Ademir;

DJOHNNATHA, Cláudio; ALVES, Felipe; LIRA, Jordan; PIRES, Mateus. Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos. In: WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES (WBLOCKCHAIN), 1. , 2018, Campos do Jordão. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018.

DAVIES, A. Why Blockchain Developers Use Ethereum? Disponível em: <https://www.devteam.space/blog/blockchain-developers-use-ethereum/>. Acesso em: 26 jun. 2023.

DENNING, Dorothy Elizabeth Robling. Cryptography and data security. Reading: Addison-Wesley, 1982.

DINIZ, Eduardo Henrique. Emerge uma nova tecnologia disruptiva. GV-executivo, v. 16, n. 2, p. 46-50, 2017.

Diploma Digital. Disponível em: <http://portal.mec.gov.br/diplomadigital/?pagina=faq-sociedade>. Acesso em: 20 maio. 2022.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES, José Antônio Valle. Design science research. In: Design science research. Springer, Cham, 2020.

DRESCH, Aline. Design science e design science research como artefatos metodológicos para engenharia de produção. 2013.

DUBARD, Caroline. Blockchain: o que é e qual a sua importância para o futuro do mercado financeiro. Disponível em: https://blog.magnetis.com.br/blockchain/. Acesso em; 01 de Mar. de 2022.

ELROM, Elad. The Blockchain Developer - A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchainbased Projects. Apress, Julho de 2019. ISBN: 978-1-4842-4847-8. Disponível em: https://www.researchgate.net/publication/334652142_The_Blockchain_Developer_A_Practical_Guide_for_Designing_Implementing_Publishing_Testing_and_Securing_Distributed_Blockchain-based_Projects.

EUROMONEY, How does a transaction get into the blockchain, Euromoney Learning, 2022 Disponível em: <https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain > Acesso em 26 de junho de 2022.

FONSECA, Eliane Andrea Barbosa. O Sistema Eletrônico de Informações (SEI) no âmbito do governo do estado de Minas Gerais: estudo de suas principais propriedades, aspectos de sua operacionalidade e benefícios. 2022.

FAULKNER, Jonh. Getting Started with Cryptography in .NET - 2016. Disponível em: https://books.google.com.br/books?id=rH6CCwAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false. Acesso em 19 mai de 2022.

GARCIA, Rodrigo D.; RAMACHANDRAN, Gowri; UEYAMA, Jó. Exploiting smart contracts in PBFT-based blockchains: A case study in medical prescription system. Computer Networks, v. 211, p. 109003, 2022.

GIL, A. C. Métodos e técnicas de pesquisa social. São Paulo: Atlas, 1992.

GÓRSKI, Tomasz. Towards continuous deployment for blockchain. Applied Sciences, v. 11, n. 24, p. 11745, 2021.

HABER, Stuart; STORNETTA, W. Scott. How to time-stamp a digital document. Springer Berlin Heidelberg, 1991.

HEGEDŰS, Péter. Towards analyzing the complexity landscape of solidity based ethereum smart contracts. In: Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain. 2018. p. 35-39.

HEVNER, Alan R. et al. Design science in information systems research. MIS Quarterly, 28(1), 75-105. 2004.

IANSITI, Marco; LAKHANI, Karim R. The truth about blockchain. Harvard business review, v. 95, n. 1, p. 118-127, 2017.

JAKOBSSON, Markus; JUELS, Ari. Proofs of work and bread pudding protocols. In: Secure Information Networks: Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99) September 20–21, 1999, Leuven, Belgium. Boston, MA: Springer US, 1999. p. 258-272.

KHARIF, Olga. Key Player In Ethereum Infrastructure Infura Rejects Centralization Claim. 16 set. 2022. Disponível em: https://www.bloomberg.com/news/articles/2022-09-16/ethereum-infrastructure-firm-infura-plans-decentralized-service?in_source=embedded-checkout-banner. Acesso em: 7 ago. 2023.

KHAN, Shafaq Naheed et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications, v. 14, p. 2901-2925, 2021.

LACERDA, Daniel Pacheco et al. Design Science Research: método de pesquisa para a engenharia de produção. Gestão & produção, v. 20, p. 741-761, 2013.

LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. The Byzantine Generals

LARKEY, Patrick D. Ask a simple question: a retrospective on Herbert Alexander Simon. Policy Sciences, v. 35, n. 3, p. 239-268, 2002.

LATIF, Raja. Understanding an Ethereum Transaction. 24 ago. 2020. Disponível em: https://info.etherscan.com/understanding-an-ethereum-transaction/. Acesso em: 29 jun. 2023.

LEPIANE, Cristiane Dias et al. Digital Degree Certificates for Higher Education inBrazil: A Technical Policy Specification. In: Proceedings of the ACM Symposium on Document Engineering 2019. 2019. p. 1-10

LIMA, Eliseu dos Santos; SEIFFERT, Claudineli Carin; SCHÄFER, Murilo Billig. ACERVO ACADÊMICO DAS IES PERTENCENTES AO SISTEMA FEDERAL DE ENSINO: MANUTENÇÃO, GUARDA E CONVERSÃO PARA O MEIO DIGITAL CONFORME A LEGISLAÇÃO BRASILEIRA. REVISTA SOCIAIS & HUMANAS, Santa Maria - RS, ano 2019, n. 2, 9 jan. 2019. Semestral.

LIMA, Marco Túlio da Silva Como utilizar a tecnologia blockchain no governo?. SERPRO 2017. Disponível em < https://www.serpro.gov.br/menu/noticias/noticias-2017/como-utilizar-a-tecnologia-blockchain-no-governo acesso em 26/06/2022 >

LIMA, T. C. S. MIOTO, R. C. T. Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica. Rev. Katál. Florianópolis v. 10 n. esp. p. 37-45 2007. Acesso em: abr. 2022.

MACHADO, Maria Aglaê de Medeiros. Desafios a Serem Enfrentados na Capacitação de Gestores Escolares. **Em Aberto**, Brasília, v. 17, n. 72, fev./jun. 2000, p. 97-112.

MAHTO, Dindayal; KHAN, Danish Ali; YADAV, Dilip Kumar. Security analysis of elliptic curve cryptography and RSA. In: Proceedings of the world congress on engineering. 2016. p. 419-422.

MATHEW, Sheena; JACOB, K. Poulose. Performance evaluation of popular hash functions. International Journal of Computer and Information Engineering, v. 4, n. 1, p. 65-68, 2010.

MCTI - Ministério da Ciência, Tecnologia, Inovações e Comunicações. Relatório de gestão do exercício de 2017. 2018

MEC. Diretores terão programa de formação continuada e extensão. Sexta-feira, 04 de dezembro de 2015 (Última atualização). Disponível em: <http://portal.mec.gov.br/component/tags/tag/36237>. Acesso em: 01 out. 2022.

MENDANHA, Gabriel Oliveira. Assegurando a propriedade e imutabilidade de documentos digitais : uma prova de conceito utilizando blockchain. 2017. TCC (Graduação em Engenharia de Software) Universidade Federal do Ceará, Campus Quixadá, Quixadá, 2017.

MENDOZA-TELLO, Julio C. et al. Disruptive innovation of cryptocurrencies in consumer acceptance and trust. Information Systems and e-Business Management, v. 17, n. 2, p. 195-222, 2019.

MERKLE, Ralph C. A digital signature based on a conventional encryption function. In: Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1987. p. 369-378

MINAS GERAIS. Decreto nº 45.849, de 27 de dezembro de 2011. Dispõe sobre a organização da Secretaria de Estado de Educação. **Imprensa Oficial de Minas Gerais,** Minas Gerais, MG, 28 dez. 2015. p. 06-13

MODI, Ritesh. Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain. Packt Publishing Ltd, 2018.

MONTEZANO, Pablo Rinco et al. Sistema Digital para Notificações Baseado em Blockchain. 2018

MULLARKEY, Matthew T. et al. Citizen data scientist: a design science research method for the conduct of data science projects. In: International conference on design science research in information systems and technology. Springer, Cham, 2019. p. 191-205.

NAKAMOTO, Satoshi; BITCOIN, A. A peer-to-peer electronic cash system. Disponível em: https://bitcoin. org/bitcoin. pdf, v. 4, p. 2, 2008.

NOFER, Michael et al. Blockchain. Bus Inf Syst Eng 59, 183–187 (2017). https://doi.org/10.1007/s12599-017-0467-3

OLIVA, Gustavo A. Mining the ethereum blockchain platform: best practices and pitfalls (MSR 2022 tutorial). In: Proceedings of the 19th International Conference on Mining Software Repositories. 2022. p. 201-202.

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica - os principais algoritmos de cifragem. Segurança Digital [Revista online], v. 31, p. 11-15, 2012.

OLIVEIRA, R. da S. Minidicionário compacto de Informática. 2. ed. atual. São Paulo: Editora Rideel, 1999.

PADMAVATHI, U.; RAJAGOPALAN, Narendran. Concept of blockchain technology and its emergence. In: Blockchain Applications in IoT Security. IGI global, 2021. p. 1-20

PEFFERS, Ken et al. A design science research methodology for information systems research. Journal of management information systems, v. 24, n. 3, p. 45-77, 2007.

PERRYMAN, Emily. What is Etherscan? 28 out. 2019. Disponível em: https://finance.yahoo.com/news/etherscan-080428243.html. Acesso em: 29 jun. 2023.

RANGANTHAN, Vishnu Prasad et al. A decentralized marketplace application on the ethereum blockchain. In: 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC). IEEE, 2018. p. 90-97.

REIS, Paulo. Ciência do Artificial e Design Science Research.2019

REYNA, Ana et al. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, v. 88, p. 173-190, 2018.

RNP. Redes acadêmicas assinam acordo para criação de rede de Blockchain na América Latina. Brasília, 14, fev, 2022. Disponível em: <https://www.rnp.br/noticias/redes-academicas-assinam-acordo-para-criacao-de-rede-de-blockchain-na-america-latina>. Acesso em: 17 maio. 2022.

SALVO, Mathew Di. You Can Now Google the Balances of Ethereum Addresses. 11 out. 2022. Disponível em: https://finance.yahoo.com/news/now-google-balances-ethereum-addresses-193132945.html. Acesso em: 29 jun. 2023.

SCHWARTZ, David. et al. The Ripple Protocol Consensus Algorithm. 2012. Disponível em: <https://ripple.com/consensus-whitepaper/>. Acesso em: 01 jan. 2022

SEMESP. Resultados dos processos de avaliação institucional podem ser melhorados. 2018. Disponível em: Disponível em: https://www.semesp.org.br/wp-content/uploads/2018/01/Resultados-processos-avaliacao-institucional-melhorados-1.pdf Acesso em: 04 out. 2019.

SILVA, Carlo Kleber; CAETANO DA SILVA, Paulo. Uma Análise De Algoritmos De Consenso Para Blockchain Visando À Implementação De Sistemas De Informação Distribuídos Transparentes. Revista de Sistemas e Computação-RSC, v. 9, n. 1, 2019.

SILVA, John Edward. An overview of cryptographic hash functions and their uses. GIAC, v. 6, 2003.

SILVA, Rafael Rodrigues da. Utilizando a Blockchain como modelo de confiança para comprovar a existência e imutabilidade de um arquivo digital. 2020. Trabalho de Conclusão de Curso.

SIMMONS, Gustavus J. Symmetric and asymmetric encryption. ACM Computing Surveys (CSUR), v. 11, n. 4, p. 305-330, 1979.

SMITH, Ben. JSON básico: conheça o formato de dados preferido da web. Novatec Editora, 2020.

SOBTI, Rajeev; GEETHA, Ganesan. Cryptographic hash functions: a review. International Journal of Computer Science Issues (IJCSI), v. 9, n. 2, p. 461, 2012.
Solidity Documentation by Solidity Team (2021). This is the official documentation for Solidity, the programming language for writing smart contracts on Ethereum. It includes a tutorial, reference manual, and other resources for learning Solidity.

SOTOMAYOR, Borja. The globus toolkit 3 programmer's tutorial. University of Chicago, Department of Computer Science, 2005

TCU. Rede Blockchain Brasil vai garantir mais segurança a atos e contratos públicos | Portal TCU. 05 de maio de 2022. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/rede-blockchain-brasil-vai-garantir-mais-seguranca-a-atos-e-contratos-publicos.htm>. Acesso em: 14 jul. 2022.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. TCU avalia tecnologias da informação blockchain e livros-razão distribuídos para o setor público. Por Secom TCU: 03/07/2020. 2020. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-avalia-tecnologias-da-informacao-blockchain-e-livros-razao-distribuidos-para-o-setorpublico.htm#:~:text=O%20relator%20do%20processo%2C%20ministro,central%20facilita%20a%20implementa%C3%A7%C3%A3o%20de Acesso em: 09 mai. 2022.

THOMSONREUTERS, Governo federal adota blockchain no Portal Único de comércio exterior. Disponível em: https://www.thomsonreuters.com.br/pt/tax-accounting/comercio-exterior/blog/governo-federal-adota-blockchain-no-portal-unico-de-comercio-exterior.html>. Acesso em: 14 jul. 2022.

TRINTA, Fernando Antonio Mota; MACÊDO, Rodrigo Cavalcanti de. Um estudo sobre criptografia e assinatura digital. Pernambuco: DI/UFPE, 1998.

TURKANOVIĆ, Muhamed et al. EduCTX: A blockchain-based higher education credit platform. IEEE access, v. 6, p. 5112-5127, 2018.
Understanding an Ethereum Transaction. Disponível em: <https://info.etherscan.com/understanding-an-ethereum-transaction/>.

VAISHNAVI, Vijay; KUECHLER, William; PETTER, Stacie. Design science research in information systems. January, v. 20, p. 2004, 2004.
W3tech. USAGE Statistics and Market Share of PHP for Websites, July 2023. Disponível em: https://w3techs.com/technologies/details/pl-php#:~:text=PHP%20is%20used%20by%2077.4,side%20programming%20language%20we%20know. Acesso em: 10 jul. 2023.

WHITAKER, Amy. Art and blockchain: A primer, history, and taxonomy of blockchain use cases in the arts. Artivate, v. 8, n. 2, p. 21-46, 2019.

WEF. Blockchain could dismantle corruption in government services. 2021. Disponível em: <https://www.weforum.org/agenda/2021/07/blockchain-for-government-systems-anti-corruption/#:~:text=Blockchain%20could%20improve%20the%20transparency>.

WOOD, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Disponível em: https://ethereum.org/pdfs/EthereumYellowPaper.pdf

WOHRER, Maximilian; ZDUN, Uwe. Smart contracts: security patterns in the ethereum ecosystem and solidity. In: 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2018. p. 2-8.

WACKEROW, Paul. Redes | ethereum.org. 7 jun. 2023. Disponível em: https://ethereum.org/pt-br/developers/docs/networks/. Acesso em: 10 jul. 2023.

ZHENG, Peilin et al. Xblock-eth: Extracting and exploring blockchain data from ethereum. IEEE Open Journal of the Computer Society, v. 1, p. 95-106, 2020.

ZHENG, Zibin et al. Blockchain challenges and opportunities: A survey. International journal of web and grid services, v. 14, n. 4, p. 352-375, 2018.

APÊNDICE A – TABELA RELATIVOS ÀS ATIVIDADES-FIM DAS INSTITUIÇÕES DE ENSINO SUPERIOR

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

CÓDIGO	ASSUNTO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		Fase Corrente	Fase Intermediária		
100 ENSINO SUPERIOR					
110	Normatização. Regulamentação	Enquanto vigora	-	Guarda Permanente	
120 Cursos de graduação (inclusive na modalidade a distância)					
121 Concepção, organização e funcionamento dos cursos de graduação					
121.1	Projeto pedagógico dos cursos	Enquanto vigora	-	Guarda Permanente	
121.2	Criação de cursos. Conversão de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
121.21	Autorização. Reconhecimento. Renovação de reconhecimento	Até a homologação do ato	5 anos	Guarda Permanente	
121.3	Desativação de cursos. Extinção de cursos	Até a homologação do ato	5 anos	Guarda Permanente	
122 Planejamento e organização curricular					
122.1	Estrutura do currículo (grade ou matriz curricular)	Enquanto vigora	-	Guarda Permanente	
122.2	Reformulação curricular	Enquanto vigora	-	Guarda Permanente	
122.3	Disciplinas: programas didáticos	Enquanto vigora	-	Guarda Permanente	
122.31	Oferta de disciplinas	2 anos	-	Eliminação	
122.32	Atividades complementares	Enquanto vigora	-	Guarda Permanente	

APÊNDICE B – RELATÓRIO TÉCNICO CONCLUSIVO.

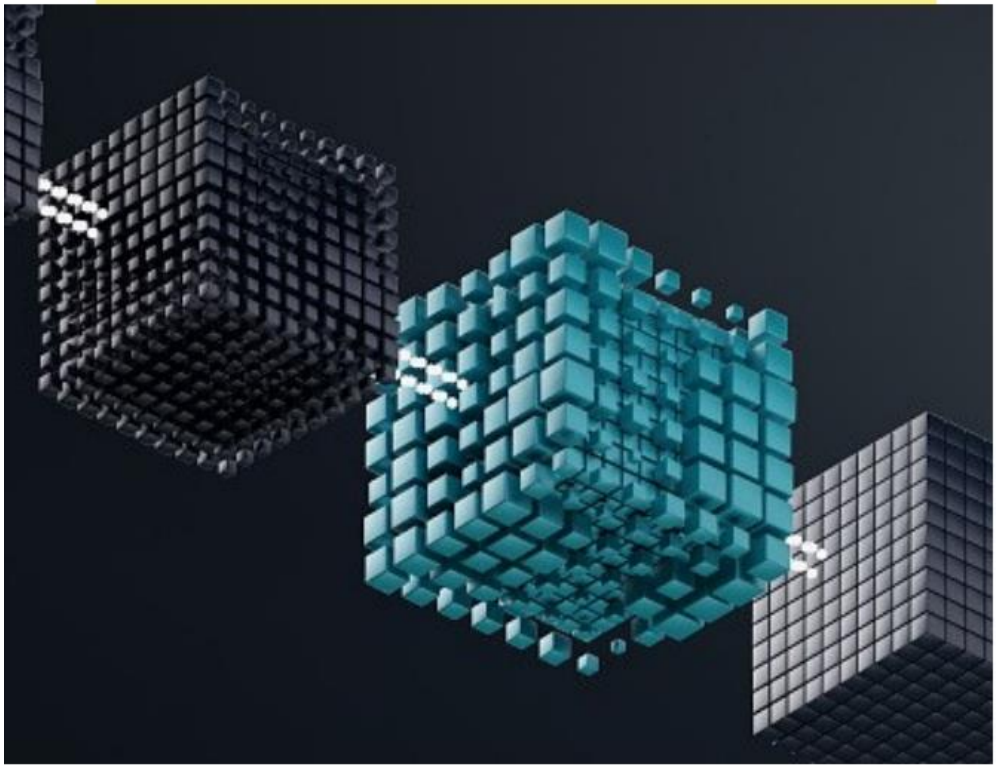
PROFIAP
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA

RELATÓRIO TÉCNICO CONCLUSIVO

UFJF
UNIVERSIDADE FEDERAL DE JUIZ DE FORA

APLIVATIVO PARA ENVIO DE DADOS A BLOCKCHAIN

RELATÓRIO TÉCNICO & INSTRUÇÕES DE IMPLEMENTAÇÃO



SUMÁRIO

RESUMO

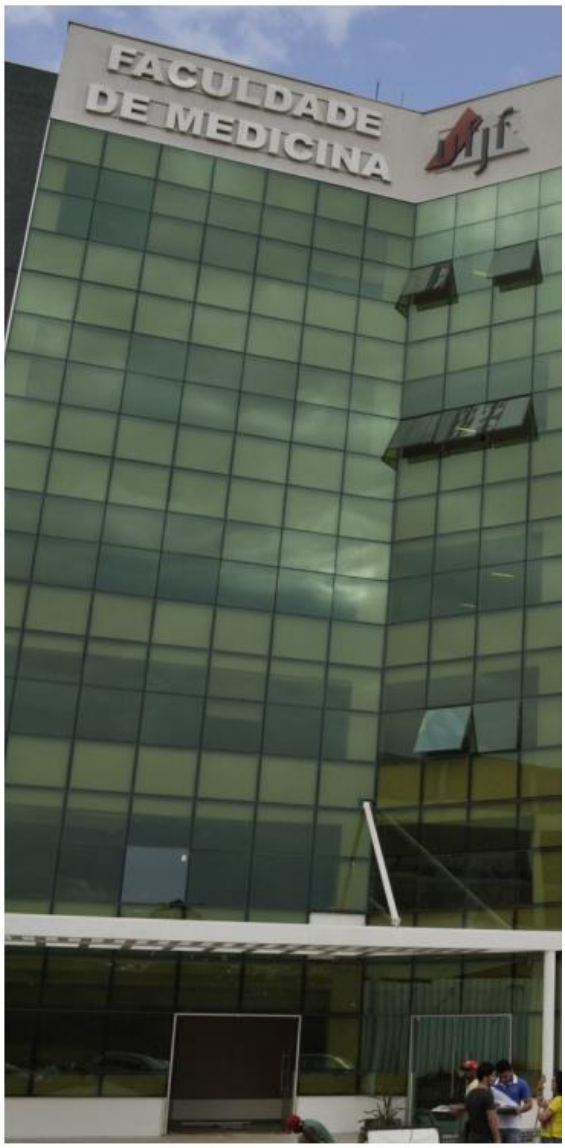
A tecnologia blockchain tem sido cada vez mais mencionada pelo Governo Federal como uma possível ferramenta para modernizar e aperfeiçoar os processos na esfera pública. Essa tecnologia pode ser compreendida como um registro distribuído capaz de garantir a imutabilidade e autenticidade de dados, sem depender de uma autoridade central, e é considerada por muitos autores como uma tecnologia disruptiva, capaz de gerar inovação ao romper com modelos antigos e introduzir novos padrões. Impulsionado por essas premissas, foi proposto e executado, o desenvolvimento uma aplicação que utiliza a blockchain da rede Ethereum para assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico originado de uma Instituição Federal de Ensino Superior (IFES), mas que pode ser utilizada para o envio de qualquer tipo de documento. Em nossa proposta utilizamos a aplicação *back-end* desenvolvida pelo autor para enviar à blockchain um comprovante de matrícula gerado pelo aplicativo móvel para estudantes e servidores desenvolvido pelo Instituto de Ciências Exatas (ICE) da Universidade Federal de Juiz de Fora (UFJF).

A adoção da tecnologia blockchain poderia ser usada para garantir uma gestão pública mais segura e prática (PORTAL TCU, 2020)

CONTEXTO

A proposta de intervenção foi concebida no ICE da UFJF durante o desenvolvimento do aplicativo que será utilizado para fornecer serviços aos alunos e servidores da unidade.

Pautada no estímulo feito pelo MEC, na busca de novas tecnologias para a gestão de documentos como diplomas e certificados (MEC, 2022), além das iniciativas do Governo Federal, ligadas ao desenvolvimentos de estudos e aplicações utilizando a tecnologia blockchain (TCU, 2022), a idéia de desenvolvimento de uma solução capaz de unir esses dois temas surgiu.



PÚBLICO ALVO

A implementação da ferramenta "aplicação back-end para envio de documentos à blockchain" pode beneficiar de forma direta alunos e usuários externos à comunidade acadêmica. A utilização de uma rede blockchain para armazenar documentos oficiais como comprovantes de matrículas, certificados e diplomas, representa uma série de vantagens quando comparado aos métodos tradicionais, essas vantagens serão apresentadas nos próximos tópicos público alvo

DESCRIÇÃO DA SITUAÇÃO-PROBLEMA

Emitir e consultar a autenticidade de um documento ou diploma é um processo por vezes custoso e lento. Utilizando um exemplo específico: alunos ou empregadores que estão no exterior e que precisam verificar a validade de um diploma, seja para a admissão em um cargo de trabalho, ou seja para um processo seletivo, devem requerer uma tradução e posteriormente a autenticação e legalização, dessa tradução, geralmente através de um serviço notarial pago, como medida para provar a autenticidade dos seus documentos. Porém, com os recentes avanços ligados a ciências da computação e com o desenvolvimento da tecnologia blockchain, dotada de características como imutabilidade, descentralização, segurança e rastreabilidade, a sua adoção pode ser uma excelente escolha que vai de encontro às necessidades de incremento dos aspectos de segurança e acessibilidade, permitindo que um diploma ou documento possa ser verificado por qualquer parte interessada, a partir de qualquer lugar do globo, sem a necessidade de um intermediário ou de uma autoridade certificadora (CASTRO,2021).

"A tecnologia blockchain pode aumentar a eficiência e transparência de sistemas governamentais." (WEF, 2021)

OBJETIVOS

Através do desenvolvimento e implementação de aplicação que utiliza a blockchain Ethereum para assegurar a imutabilidade, garantir a integridade, autenticidade e disponibilidade de um documento nato-digital, originado de uma IFES, pretendemos atingir os seguintes objetivos específicos:

01. Possibilitar a submissão de um documento do acervo acadêmico à blockchain da rede Ethereum.

02. Possibilitar o acesso ao documento por qualquer cidadão ou instituição quando se fizer necessário

03. Permitir o armazenamento de forma descentralizada e distribuída, diminuindo assim a incidência de eventos adversos ligados a perda de dados

04. Diminuir a incidência de fraudes se valendo da característica de imutabilidade inerente à tecnologia blockchain.

05. Criar um modelo de segurança capaz de ser reproduzido e aperfeiçoado por outras instituições

DIAGNÓSTICO E ANÁLISE DA SITUAÇÃO-PROBLEMA

Os esforços feitos pelo MEC na construção de parâmetros mais maduros e seguros para a emissão do acervo acadêmico pelas IFES, são claramente um passo para a consolidação de uma estrutura mais sólida no combate às fraudes, mas alguns pontos continuam de certa forma descobertos.

De acordo com Lepiane *et al*, (2019), mesmo após mudanças recentes na questão da emissão e autenticação de itens do acervo acadêmico, a natureza distribuída do processo ainda persiste, já que cada Instituição deve manter um repositório com os dados de cada documento, essas informações ainda estão suscetíveis a incidentes técnicos ou a desastres naturais que podem causar perda de dados. Um outro detalhe ainda presente é a presença de uma autoridade central certificadora, intermediando o processo, o tornando mais burocrático e dependente. Porém, com o desenvolvimento da tecnologia blockchain, dotada de características como imutabilidade, descentralização, segurança e rastreabilidade, a sua adoção pode ser uma excelente escolha que vai de encontro às necessidades de incremento dos aspectos de segurança e acessibilidade, permitindo que um diploma ou documento possa ser verificado por qualquer parte interessada, a partir de qualquer lugar do globo, sem a necessidade de um intermediário ou de uma autoridade certificadora (CASTRO,2021).

Frente ao exposto, entendemos que desenvolver meios para aumentar a segurança, facilitar a autenticidade e disponibilidade de documentos que fazem parte do acervo acadêmico emitidos por IFES, através do desenvolvimento de soluções tecnológicas como, softwares, aplicativos ou outros tipos de sistemas informatizados que adotam a tecnologia blockchain como estrutura de armazenamento e distribuição de dados, é um senso comum por parte do governo federal, e a necessidade de modelos de confiança que possam ser desenvolvidos e utilizados como ferramentas práticas de estudo também é uma realidade

OBJETIVOS DA PROPOSTA

Nosso objetivo é garantir e assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico, utilizando a tecnologia blockchain e conforme apresentado nos tópicos anteriores, para atingir este objetivo a nossa proposta de intervenção se apresenta através da construção e implementação de um sistema back-end. Back-ends, são sistemas que não interagem diretamente com os usuários, eles são integrados a outros sistemas que são responsáveis por "conversar" com o usuário final. O diagrama apresentado na figura X, apresenta um pouco dessa dinâmica.

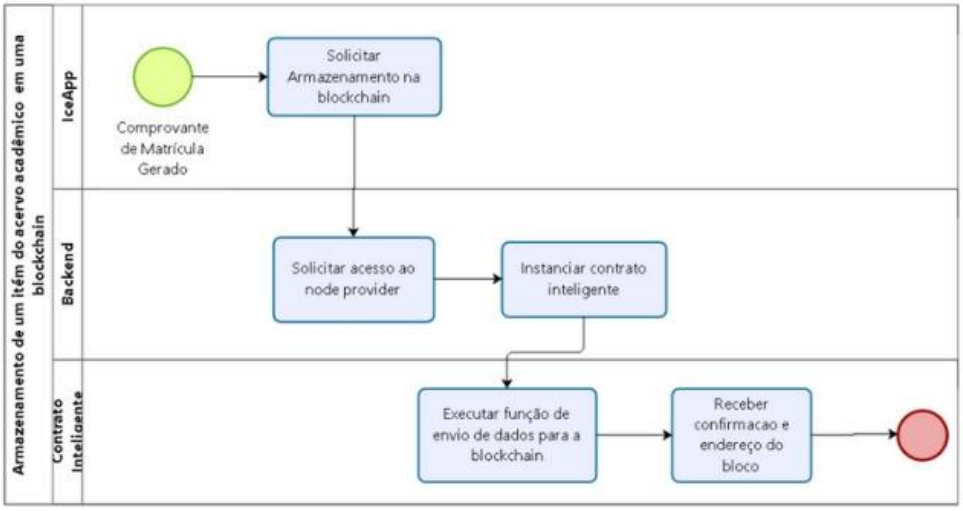
Vamos nos valer dos recursos do 5W2H, para que possamos entender melhor como implementar a nossa proposta de Intervenção

- **O que (What) ?** Realizar a implementação do nosso sistema back-end
- **Quem (Who) ?** Técnicos e analistas de TI.
- **Onde (Where) ?** Qualquer instituição pública.
- **Quando (When) ?** Após a criação de contrato inteligente e da obtenção das credenciais necessárias.
- **Porque (Por que) ?** Para garantir e assegurar a imutabilidade, integridade e disponibilidade de um item do acervo acadêmico, utilizando a tecnologia blockchain
- **Como (How) ?** Através de codificação necessária à integração, entre o back-end e a interface previamente existente
- **Quanto (How much) ?** Nenhum custo.

Conforme demonstrado no figura 5W2H, e nos parágrafos anteriores, nosso back-end, precisa ser conectado a outra aplicação ou sistema que faça a interação com o usuário final.
E essa integração precisa ser construída por técnicos ou analistas de TI,
com alguma experiência na área de integração de sistemas.
Portanto as próximas instruções serão direcionadas a esse grupo de profissionais.

INFORMAÇÕES TÉCNICAS PARA A INTEGRAÇÃO

Na figura abaixo, podemos observar a dinâmica de funcionamento do nosso artefato integrado a um sistema de interface ja existente (ICEapp)



URL do projeto no GitHub
https://github.com/thiagom10/backendDocToEthereum.git

A seguir serão listadas informações e instruções importantes aos integradores que irão utilizar o back-end.

O Sistema back-end foi construído em linguagem PHP, e possui apenas uma dependência, o pacote web3, conhecido como simple-web3-php, as informações são enviadas a ele através de requisições do tipo GET, mas podem ser facilmente substituídas por requisições POST.

Não existe qualquer camada de autenticação no nosso código, portanto, é importante que ele seja implementado junto a algum tipo de sistema de autenticação como por exemplo: Oauth 2.0.

Toda a comunicação é feito através do Node Provider Infura, por tanto é necessário que a instituição possua uma conta no serviço. Todo projeto foi constituido para utilizar o Infura. Portanto uma inegração com outro Node Provider ou mesmo diretamente a um nó da rede é possível mas vai requerer conhecimento técnico especializado e algum tempo para que seja realizado a alteração no código.

Por fim, as variáveis contendo informações essenciais precisam ser setadas, elas se encontram nas parte inicial do código fonte e são as seguintes:

1. Hash referente a conta/caretira virtual da instituição
2. Hash referente à instância do smart contratct
3. Chave de acesso a carteira da instituição
4. Credenciais de acesso ao infura.

RESPONSÁVEIS

Thiago Marques Fernandes de Mello
Bacharel em sistemas de Computação, Pós-graduado em Redes de Computadores
Servidor Técnico Administrativo na universidade Federal de Juiz de Fora, no cargo de Analista de Tecnologia da Informação
E-mail: thiago.marques@ice.ufjf.br

Marcos Tanure Sanábio
Graduado em Administração, Mestre em Administração Pública, Doutor em Administração
Docente do Programa do Mestrado Profissional em Administração Pública da Universidade Federal de Juiz de Fora

ELABORADO EM 27/07/2023