UNIVERSIDADE
FEDERAL RURAL
DE PERNAMBUCO

Saulo Gomes da Silva

Uma metodologia para suporte à tomada de decisão quanto ao uso de blockchain na área de registros públicos

Recife

2021

Saulo Gomes da Silva

Uma metodologia para suporte à tomada de decisão quanto ao uso de blockchain na área de registros públicos

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação da Universidade Federal Rural de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Universidade Federal Rural de Pernambuco – UFRPE

Departamento de Computação

Curso de Bacharelado em Ciência da Computação

Orientador: Prof. Dr. Fernando Antonio Aires Lins

Recife

2021

Foi pensando nas pessoas que este trababalho foi feito, por isso dedico este trabalho a todos aqueles a quem esta pesquisa possa ajudar de alguma forma.

Agradecimentos

À minha mãe, Maricélia Gomes da Silva, por desde sempre me mostrar o valor do conhecimento, da ética e do pensamento a longo prazo. Também agradeço por todos os sacrifícios feitos para que eu obtivesse o máximo de educação possível.

À Sarah Maria Moura por estar ao meu lado nos momentos bons e ruins, compartilhando a vida e apoiando o meu crescimento, assim como eu apoio o crescimento dela.

Ao meu professor e orientador, Fernando Antônio Aires, pela paciência, calma e disponibilidade ao me conduzir no desenvolvimento deste trabalho.

Aos professores Péricles Miranda, Andrêza Leite, Marcelo Marinho, Suzana Sampaio, Erica Souza, Julian Menezes, Abner Barros, Rinaldo Lima, Obionor Nóbrega, Jeísa Domingues, Robson Medeiros, Ricardo Souza, Rafael Dueire e Marcos Cardoso. Professores que eu possuo carinho e admiração, que me acompanharam nesta jornada e espero poder novamente trabalhar ao lado deles no futuro.

Aos meus amigos Allyson Almeida, Ikaro Alef, Eduardo Silva, Tayane Miranda, Welton Santos, Allan Moura, André Lins, Victor Alexandre, Maik Paixão, Ranniery Dias, Raylison Nunes, Mércio Andrade, Matheus Agostinho, André de Andrade, Ana Juriti e Marcos Lira. Alunos da universidade, que me acompanharam durante a trajetória, compartilhando as vitórias e os momentos de superação.

Por fim, mas não menos importante, à Sandra Xavier, secretária do curso de Bacharelado em Ciência da Computação na UFRPE, ela foi a primeira pessoa, relacionada ao curso, que tive contato ao chegar na universidade e seu apoio, dedicação e carinho para comigo e demais alunos é algo para ser guardado no coração.

“A persistência é o caminho do êxito.”
(Charles Chaplin)

Resumo

O surgimento do Bitcoin e da tecnologia Blockchain mudou o mundo do comércio eletrônico. Essas tecnologias possuem potencial para se tornar um dia o padrão para aplicações Web, por meio de aplicações descentralizadas. As aplicações descentralizadas são aplicações flexíveis, transparentes, distribuídas, resilientes e possuem poder de crescimento maior, em termos de escalabilidade e disponibilidade, se compararmos ao modelo atual de software (arquitetura cliente-servidor). Há limitações que impedem o uso da tecnologia Blockchain para solução de problemas envolvendo dados e distribuição da informação. Por haver limitações, projetistas e entusiastas que não estejam bem instruídos sobre a tecnologia podem cometer equívocos e usar a mesma de forma a prejudicar a solução ao qual ela faz parte, além de impedir o alcance de sua plenitude. Devido às possibilidades que a tecnologia Blochchain e aplicações descentralizadas trazem, este trabalho tem como objetivo a concepção de uma metodologia para auxiliar na tomada de decisão quanto ao uso de Blockchain para o ambiente governamental, especificamente na área de registros públicos. Para exemplificar a aplicação da metodologia foi realizado um estudo de caso utilizando o serviço de cadastro e consulta de registros em cartórios, serviço esse que é apoiado por um sistema fornecido pelo Conselho Nacional de Justiça. Como resultado, foi possível demonstrar que o processo da metodologia cria um perfil de implementação da tecnologia Blockchain, perfil este que possibilita ao projetista de sistemas escolher e configurar plataformas Blockchain para a finalidade desejada. O resultado do processo indica que a tecnologia Blockchain é adequada para o propósito do serviço dos cartórios, garantindo o uso adequado da tecnologia e evitando possíveis perdas.

Palavras-chave: blockchain, aplicações descentralizadas, metodologia, tomada de decisão, registro público.

Abstract

The emergence of Bitcoin and Blockchain technology has changed the world of e-commerce. These technologies have the potential to one day become the standard for Web applications, through decentralized applications. Decentralized applications are flexible, transparent, distributed, resilient applications and have greater growth power, in terms of scalability and availability, when compared to the current software model (client-server architecture). There are limitations that prevent the use of Blockchain technology for solving problems involving data and information distribution. Because there are limitations, designers and enthusiasts who are not well educated about the technology can make mistakes and use it in a way that damages the solution to which it belongs, in addition to preventing it from reaching its fullness. Due to the possibilities that Blockchain technology and decentralized applications bring, this work aims to design a methodology to assist in decision making regarding the use of Blockchain for the government environment, specifically in the area of public records. To exemplify the application of the methodology, a case study was carried out using the service of registration and consultation of registries in notaries, which service is supported by a system provided by the National Council of Justice. As a result, it was possible to demonstrate that the methodology process creates an implementation profile for Blockchain technology, a profile that allows the system designer to choose and configure Blockchain platforms for the desired purpose. The process result indicates that the Blockchain technology is suitable for the purpose of notary service, ensuring the proper use of technology and avoiding possible losses.

Keywords: blockchain, decentralized applications, methodology, decision making, public record.

Lista de ilustrações

Lista de abreviaturas e siglas

BFT	Byzantine Fault Tolerance
BPMN	Business Process Model and Notation
CNJ	Conselho Nacional de Justiça
DAPPS	Decentralized Applications
IOT	Internet Of Things
NTP	Network Time Protocol
P2P	Peer-to-Peer
PBFT	Pratical Byzantine Fault Tolerance
PC	Personal Computer
PeA	Privacidade e Anonimato
PoA	Proof of Authority also Proof of Activity
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
RBFT	Randomized Byzantine Fault Tolerance
RG	Registro Geral
SAD	Sistema de Arquivos Descentralizados
TTP	Trusted Third Party
XFT	Cross-Fault Tolerance

Sumário

1 Introdução

1.1 Contexto

Desde 2008, após o surgimento da moeda virtual Bitcoin e da tecnologia Blockchain, ambos definidos pelo trabalho de Satoshi Nakamoto (NAKAMOTO, 2008), o mundo do comércio eletrônico mudou. Um novo paradigma para registro de transações havia sido criado, onde duas partes são suficientes para a realização de uma transação financeira, dispensando a necessidade de terceiros no processo de troca de valores e registro de operação. Assim podemos definir o objetivo inicial da tecnologia Blockchain.

Segundo Junior (2017), é possível definir Blockchain como o livro de registros público onde ficam armazenadas todas as transações efetuadas utilizando criptomoedas. Reduzir custo e tempo sem perder as características de segurança necessárias para operações monetárias também são intenções iniciais deste novo paradigma.

Registros armazenados criptograficamente unidos à tecnologia de arquitetura ***Peer-to-Peer*** (P2P) provê um ponto de partida para um novo tipo de software chamado **Aplicação(es) Descentralizada(s)** (*Decentralized Applications* – DAPPS) (TANENBAUM; STEEN, 2006) (RAVAL, 2016).

Com potencial para se tornar um dia o padrão para aplicações Web, as DAPPS vêm ganhando mais espaço na mídia especializada e contando com um crescimento considerável de soluções baseadas nesta abordagem. São aplicações flexíveis, transparentes, distribuídas, resilientes e que possuem poder de crescimento maior, em termos de escalabilidade e disponibilidade, se compararmos ao modelo atual de software para a Web (RAVAL, 2016).

Segundo Swan (2016), podemos dividir o amadurecimento, em relação ao uso, da Blockchain em três fases: na primeira (1.0) temos as aplicações financeiras, a criação de **criptomoedas** e o uso do registro descentralizado das operações. A segunda (2.0) traz o conceito de contratos inteligentes (***smart contracts***). A terceira fase (3.0) vai **além de aplicações monetárias** e inclui áreas como Saúde, Ciência, Plataformas Governamentais, Literatura, Cultura, Artes etc. (SWAN, 2016).

No âmbito governamental há iniciativas que visam a utilização da tecnologia Blockchain no fornecimento de serviços à população. Segundo Lima (2017), há diversas possibilidades de emprego da tecnologia dentre elas a desburocratização de serviços de registros públicos como certidão de nascimento, patente, registro de veículo e do sistema notarial brasileiro, formado pelos cartórios de ofícios.

Ainda no contexto governamental, Lima (2017) descreve um problema existente e que com a adoção da tecnologia Blockchain não mais existiria, o problema da emissão de Registro Geral (RG).

Hoje nada impede que um cidadão tenha 27 carteiras de identidades diferentes, uma em cada unidade da federação. Haver um único registro geral para cada cidadão seria a melhor opção, porém centralizar os dados criaria o problema de haver um ponto único de falha (LIMA, 2017).

Com a adoção da Blockchain ambos os problemas seriam sanados, pois não se trata de uma base centralizada, mas sim de uma rede compartilhada por todos (LIMA, 2017).

Desde o seu surgimento, a Blockchain traz a transparência de transações como ponto forte, além da capacidade de evitar que o dado seja copiado de forma que seja utilizado em outros lugares da mesma rede, nós (*node*) ou blocos da rede.

Características como confidencialidade, integridade e disponibilidade são necessárias para a viabilidade do uso da cadeia de blocos. Estas três características também são conceitos que permeiam o assunto de segurança da informação, conhecidas como a tríade CIA (do acrônimo em inglês para *confidentiality, integrity and availability*).

A Blockchain traz estes conceitos em sua concepção, garantindo a confidencialidade por utilizar *hash* criptográfico e chaves (criptografia assimétrica) (STALLINGS, 2014) (COULOURIS et al., 2013), para garantir que somente o dono da informação possa ver seu conteúdo. A integridade e disponibilidade se dá por meio da rede de computadores que além de ter uma cópia dos dados também possui um mecanismo de consenso (NAKAMOTO, 2008) (RAVAL, 2016) (SWAN, 2016).

Nem sempre descentralizar os dados é a melhor solução para todos os cenários. Bancos de dados tradicionais, microsserviços e outras soluções para fornecimento de dados em rede podem ser soluções mais adequadas.

Há limitações que impedem o uso de uma arquitetura descentralizada para solução de problemas envolvendo dados e distribuição da informação. Algumas limitações são diretamente consequência das características técnicas necessárias, como: (I) a vazão da quantidade de transações por segundo, se comparada aos sistemas de processamento e registro de transações de empresas de cartão de crédito; (II) latência da comunicação; (III) tamanho da cadeia de blocos após milhares de operações serem registradas e (IV) largura de banda necessária para o ingresso de novos nós na rede, valores que estão na proporção de gigabytes no caso da moeda Bitcoin (SWAN, 2016).

Devido às possibilidades que a tecnologia Blochchain e aplicações descentralizadas podem trazer, a concepção de uma metodologia para auxiliar na tomada de deci-

são quanto ao uso de Blockchain para o ambiente governamental, especificamente na área de registros públicos, contribui para que a tecnologia possa ser utilizada em sua plenitude de maneira consciente, sem prejuízos aos que disponibilizarem seus dados.

1.2 Problema e Contribuição Principal

A tecnologia Blockchain é reconhecida por ser uma revolução em como a sociedade faz comércio e interage entre si. A reputação é dada devido às suas propriedades: ser descentralizada, permitindo que haja uma comunicação e troca de bens ponto a ponto sem a necessidade de um banco ou agência reguladora para o registro da transação; ter um bom nível de segurança trazendo confidencialidade, integridade e disponibilidade como características essenciais na sua concepção.

O sucesso da moeda virtual Bitcoin (NAKAMOTO, 2008) trouxe, além de um conjunto de outras criptomoedas propostas para fins similares, um caminho para aplicações descentralizadas. De forma comparativa, havendo tanta exposição das possibilidades e interesse do público tecnológico quanto o surgimento do BitTorrent (COULOURIS et al., 2013).

A tecnologia Blockchain faz parte de um novo paradigma computacional disruptivo, assim como foi o surgimento dos computadores pessoais (*Personal Computer* - PC), da Internet nos anos 1990 e dos aparelhos *Smartphones* e Redes Sociais, nos anos 2000 (SWAN, 2016).

Porém, assim como todo novo paradigma, há um certo grau de desconhecimento por parte das pessoas, mesmo pessoas da área de computação, que muitas vezes não conseguem desassociar a tecnologia Blockchain da moeda virtual. Consequentemente, também não compreendendo os pontos positivos e negativos da tecnologia.

Saber o quando, como e onde é importante utilizar tal tecnologia e padrão de arquitetura descentralizada, saber se as limitações conhecidas hoje podem trazer futuros prejuízos financeiros, além de saber se realmente é necessário para uma nova ideia de negócio, solução ou serviço são questões relevantes para a adoção da tecnologia.

Assim sendo, a questão da pesquisa é: como determinar se o uso da tecnologia Blockchain é indicada como solução em um projeto que envolve o uso de registros públicos?

Determinar se existe a necessidade de usar ou não uma Blockchain, como parte de uma solução, é uma tarefa tão importante quanto o levantamento e análise de requisitos em um projeto de software.

Uma contribuição esperada deste projeto é apresentar uma metodologia para

auxiliar na tomada de decisão sobre o uso de Blockchain, estendendo os métodos já apresentados no meio acadêmico.

1.3 Objetivos

1.3.1 Objetivo Geral

Propor uma metodologia para auxiliar na tomada de decisão quanto ao uso de Blockchain na área de registros públicos.

1.3.2 Objetivos Específicos

a) Apresentar o fluxo de decisões seguindo a notação *Business Process Model and Notation* (BPMN), notação comum em ambientes de gestão de processos;

b) Demonstrar o uso da metodologia proposta através de um estudo de caso representativo;

c) Servir como um método para facilitar a adoção em maior escala da tecnologia Blockchain e aplicações descentralizadas na área de registros públicos.

1.4 Estruturação do Trabalho

Este documento está estruturado da forma que se segue.

O Capítulo 2 discorre sobre os conceitos básicos necessários para compreender o contexto da pesquisa. Neste capítulo, serão apresentados conceitos sobre Criptografia, Blockchain e outros conceitos que ajudam o entendimento do trabalho proposto.

O Capítulo 3 apresenta os principais trabalhos relacionados a esta pesquisa, os quais foram utilizados como referência para o entendimento do estado da arte, construir a contextualização do trabalho e identificar a problemática que deve ser tratada neste trabalho de pesquisa.

O Capítulo 4 é dedicado à metodologia proposta neste trabalho. Este capítulo apresentará o processo utilizado para o uso desta metodologia e a visão geral de sua estrutura. O capítulo também discorrerá sobre a especificação de cada atividade definida como parte do processo da modelagem proposta.

Por sua vez, o Capítulo 5 busca ilustrar e avaliar a metodologia proposta, para isso apresenta um estudo de caso representativo da área.

Por fim, o Capítulo 6 discorre sobre as conclusões deste trabalho e possibilidades de trabalhos futuros.

2 Conceitos Básicos

Neste capítulo, serão apresentados os principais conceitos necessários para o entendimento deste trabalho. Dentre os fundamentos conceituais, serão apresentados conceitos sobre Criptografia, Blockchain e outros conceitos que ajudam o entendimento do trabalho proposto.

2.1 Registro Público

Registro público é o nome dado ao(s) documento(s) que possuem a finalidade de dar publicidade formal a determinados fatos, circunstancias ou direitos, que operam sob a regulamentação e o controle da administração pública nacional, local ou institucional, para assim prestar um serviço de transparência legal. Os registros públicos são postos em prática para substituir, mesmo formalmente, outros meios de publicidade relevante de fatos e direitos.

> ”A necessidade de se fazer publicidade de atos e negócios jurídicos vem de muito tempo. No direito da Babilônia, por exemplo, por meio do Código de Hamurabi, a propriedade imobiliária era objeto de proteção especial dos homens e dos deuses. Há inscrições em pedras, com figuras e divindades ou nomes tutelares e, embaixo, atos reais de doação de terras, especificando-lhe os limites.”(NASCIMENTO, 2019, p. 1).

No Brasil os registros públicos são regulamentados pela Lei 6.015, de 31 de dezembro de 1973 (BRASIL, 1973) e pelo artigo 236 da Constituição Federal de 1988 (BRASIL, 2017). Dentre os tipos de registros referidos pela lei estão o registro civil de pessoas naturais, o registro civil de pessoas jurídicas, o registro de títulos e documentos e o registro de imóveis.

Os demais registros públicos do governo Brasileiro são regidos por leis próprias, como por exemplo o Código Eleitoral, Lei 4.737, de 15 de julho de 1965 (TSE, 1965), que contém normas destinadas a assegurar a organização e o exercício de direitos políticos principalmente os de votar e ser votado.

2.2 Criptografia

A criptografia é um termo que atualmente é muito relacionado com a segurança em rede, mas é conhecida desde os tempos antigos. Marques (2013) define a cripto-

grafia como a ocultação, por meio de códigos, do real significado de uma informação, garantindo que somente o remetente e o destinatário entendam o seu conteúdo. Amaro (2007) ainda é mais abrangente quanto à sua conceituação:

> ”Um processo pelo qual um texto puro (normal) é convertido em uma mensagem codificada (texto cifrado), através da aplicação de um algoritmo (...), de forma a ser possível retornar a mensagem à sua forma original.”(AMARO, 2007, p. 1).

Na Ciência da Computação, a criptografia é categorizada em dois tipos: simétrica (de chave única) ou assimétrica (de chave pública e privada).

A criptografia simétrica é utilizada para ocultar o conteúdo dos blocos ou fluxos contínuos de dados de qualquer tamanho, incluindo mensagens, arquivos, chaves de encriptação e senhas (STALLINGS, 2014).

A criptografia assimétrica é usada para ocultar pequenos blocos de dados, como valores de função de hash e chaves de encriptação, que são usados em assinaturas digitais (STALLINGS, 2014).

Aqui vale destacar que a criptografia simétrica é baseada em chave única, a chave precisa ser compartilhada entre as partes que precisam cifrar e decifrar dados (senhas, assinaturas etc.). Já a criptografia assimétrica utiliza um par de chaves, pública e privada, para as operações de criptografia.

2.2.1 Função *Hash*

A função hash é uma função matemática que é utilizada na Blockchain para a construção dos registros. Segundo Narayanan et al. (2016), essa função possui três propriedades:

- Entrada é constituída por uma sequência de caracteres de qualquer tamanho.
- Como saída, uma série de caracteres que possuem tamanho fixo.
- Sua eficiência é computável. Isso quer dizer que, ao introduzir uma determinada entrada, é possível descobrir a correspondente saída em um período de tempo razoável.

Mais duas propriedades asseguram a confiabilidade dessa função (NARAYANAN et al., 2016) (STALLINGS, 2014):

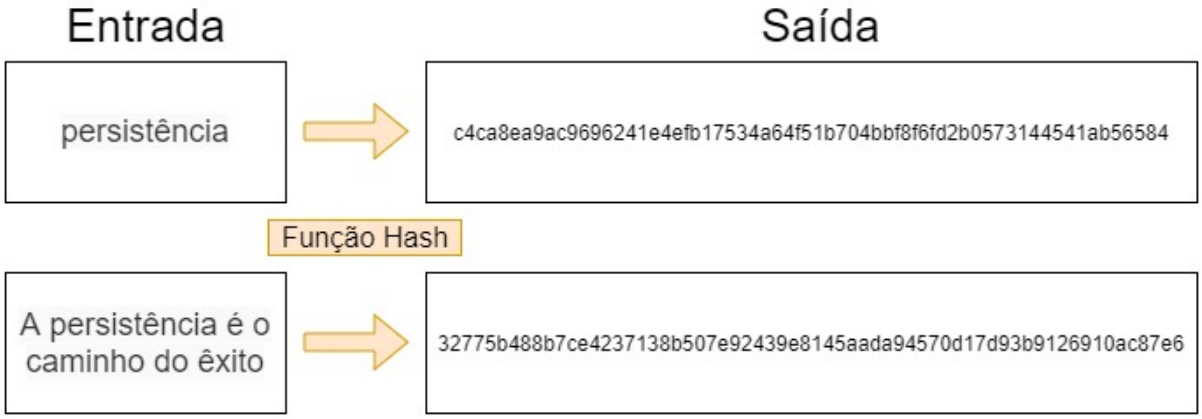
- Resistência à colisão: uma colisão acontece quando duas ou mais entradas diferentes produzem o mesmo *hash* de saída. Desse modo, a resistência à colisão

tem a finalidade de certificar que essa ação indesejável tenha uma probabilidade pequena de acontecer.

- Anti-reversão: é a sua unidirecionalidade, pois, uma vez aplicada, não é reversível. Sendo assim, não é possível a recuperação da entrada original a partir da sequência *hash* de saída.

A Figura 1 apresenta dois exemplos de entrada e saída da função *hash*.

Figura 1 – Exemplo da função hash



Fonte: Produzido pelo autor.

Devido a essas características, a função *hash*, conforme Stallings (2014), é um meio frequentemente utilizado para indicar se determinados dados foram ou não modificados. Um receptor da mensagem, ciente do conteúdo da mesma, pode utilizar a função *hash* e confirmar se a saída se mantêm igual ao *hash* recebido.

2.3 Blockchain

O conceito de Blockchain foi definido pela primeira vez em 2008 com a publicação do artigo ”**Bitcoin: A Peer-to-Peer Electronic Cash System**”, publicado por uma pessoa ou grupo sob o pseudônimo de **Satoshi Nakamoto** (cuja real identidade permanece um mistério até o corrente ano de 2021) (NAKAMOTO, 2008).

Segundo Junior (2017), um somatório de características compõe a tecnologia Blockchain. As características são: (I) Livro razão que armazena todos os registros de transações que acontecem; (II) Descentralizado, não depende de uma entidade central para funcionar, gerir ou definir regras; (III) Distribuído, espalhado por todo o planeta, por milhares de computadores, como a Internet.

De acordo com Ferreira et al. (2017), podemos entender Blockchain (também conhecido como protocolo de confiança) como bases de dados distribuídas e criptogra-

fadas que funcionam como um livro razão, que serve para registrar todas as transações que ocorrem em uma determinada rede.

A Figura 2 mostra de forma resumida as principais características que formam a Blockchain.

Figura 2 – As principais características que compõem uma Blockchain

Fonte: Junior (2017).

O livro razão mantem os registros e cada registro se dá de forma pública e compartilhada, através de protocolos de consenso e confiança entre as partes envolvidas, sem a necessidade do intermédio de terceiros. As operações para calcular os dados necessários para que os registros possam ser salvos são chamadas de **mineração**.

2.3.1 Mineração

As transações que ocorrem na rede vão sendo agrupadas e armazenadas em blocos, cada novo bloco precisa ser validado para saber se este atende aos requisitos definidos pela rede. Essa validação, conhecida popularmente como mineração, consiste em um custoso procedimento computacional que busca encontrar um *hash* válido para o bloco (NAKAMOTO, 2008).

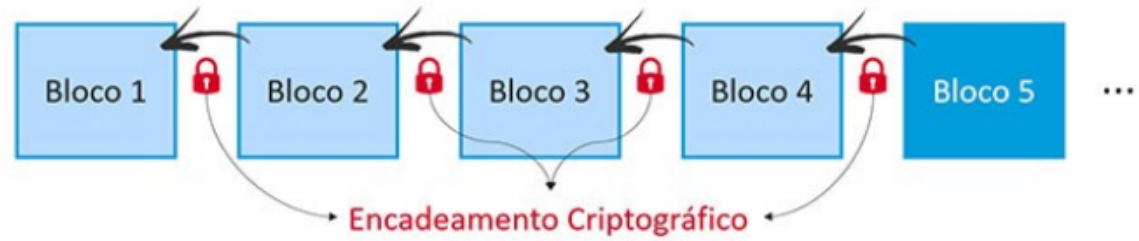
O *hash* trata-se de um código composto por números encriptados que serve como um “protocolo” que garante que aquela transação é válida. Ao ser encontrado o *hash*, o bloco pode ser adicionado a rede (NAKAMOTO, 2008).

Cada computador (também conhecido como nó) conectado à rede Blockchain guarda uma cópia do “livro razão”, que armazena o registro de todas as transações.

Quando um novo bloco é validado e adicionado à rede todos os nós são atualizados para receber os novos valores e, assim, garantir a integridade da rede. Isso assegura que novos blocos não possam ser inseridos ou modificados no meio da cadeia sem que isso seja imediatamente percebido pelos demais.

Na Figura 3, é apresentada uma representação que como se dá a estruturação da cadeia de blocos.

Figura 3 – Estrutura da organização da rede Blockchain



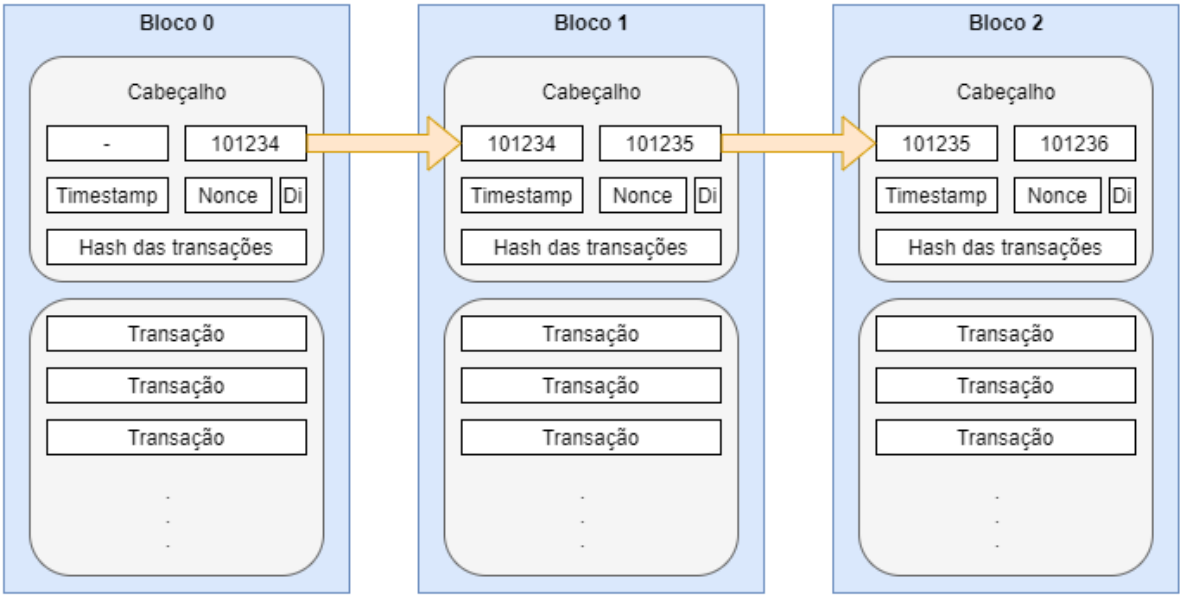
Fonte: Proof (2019).

2.3.2 Estrutura do Bloco

Segundo Ferreira et al. (2017), um bloco é composto por duas partes principais que são o cabeçalho e as transações. As transações são o agrupamento dos dados que são armazenados no bloco. O cabeçalho, por sua vez, possui diversos campos, sendo os mais importantes para seu funcionamento: o *hash* do bloco anterior, dificuldade e nonce, conforme será explicado posteriormente.

Na Figura 4, é apresentada uma representação mais detalhada da estrutura dos blocos e dos principais campos contidos neles.

Figura 4 – Estrutura dos blocos da Blockchain



Fonte: Produzido pelo autor.

No retângulo inferior de cada bloco na Figura 4, estão as transações que vão sendo adicionadas uma a uma até que o limite do bloco seja atingido.

No retângulo superior de cada bloco na Figura 4, estão as representações dos cabeçalhos. O cabeçalho é composto por campos contendo: (I) *Hash* das transações; (II) *Hash* do bloco anterior; (III) *Hash* do bloco que é o seu identificador, é ele que é enviado ao bloco seguinte; (IV) *Timestamp* registrando o momento em que aquele bloco foi gerado; (V) *Nonce* que é utilizado para a validação do bloco e (VI) Valor de dificuldade para se gerar o hash do bloco.

2.3.3 Consenso Descentralizado

Antes da Blockchain, consenso na validação de uma transação sempre requisitava algum nível de centralização (RAVAL, 2016) (FERREIRA et al., 2017).

Ao fazer um pagamento por meios atualmente tradicionais, a transação precisa ser informada e registrada por uma terceira organização, ação feita por entidades financeiras como operadoras de cartão de crédito e bancos. O consenso descentralizado é uma inovação que a tecnologia Blockchain traz.

Para alcançar consenso descentralizado, é necessário o uso de algoritmos para essa finalidade, como os apresentados abaixo:

- ***Proof of Work* (Pow)**: é o primeiro e mais popular algoritmo de consenso para Blockchain, apresentado por Nakamoto (2008). Possui o princípio de resolver um problema matemático complexo de forma que possa validar que o minerador trabalhou para encontrar a solução para um tipo de quebra-cabeça criptográfico.
- ***Proof of Stake* (Pos)**: nasceu como uma alternativa ao PoW. No algoritmo de PoS quem tem criptomoedas em seu poder é recompensado e ter criptomoedas no seu endereço é a prova de que está a participar na rede descentralizada. As carteiras dos usuários são responsáveis por armazenar e validar blocos. Os blocos são gerados de forma semi-aleatória, tendo prioridade, quem tem mais moedas armazenadas e por mais tempo. Todos aqueles que têm moedas na carteira receberão uma recompensa, mas aqueles que tiverem mais moedas receberão uma recompensa maior.
- ***Proof of Elapsed Time* (PoET)**: este algoritmo específico é usado principalmente em redes Blockchain de acesso restrito (Privadas, Consorcio e Permissionárias). Essas redes de permissões precisam decidir sobre os direitos de mineração e princípios de votação. Para garantir que tudo ocorra bem, os algoritmos PoET usam uma tática específica para cobrir a transparência em toda a rede. Cada indivíduo da rede tem que esperar por um período de tempo; no entanto, o limite de tempo será totalmente aleatório. O participante que tiver terminado seu com-

partilhamento de tempo de espera chegará ao livro de registro para criar um novo bloco.

- ***Byzantine Fault Tolerance* (BFT)**: também aplicável ao *Practical Byzantine Fault Tolerance* (PBFT). Nós em uma rede habilitada PBFT são ordenados de forma sequencial, com um nó sendo o líder e os outros nós secundários (nós *backup*). Neste esquema qualquer nó pode ser eleito como líder, inclusive em caso de falha do líder atual. O objetivo é que todos os nós honestos ajudem a alcançar um consenso a respei-to do estado do sistema.

- ***Proof of Authority* (PoA)**: é um algoritmo de consenso que dá a um pequeno e definido número de atores na rede o poder para validar transações e interações com a rede. De acordo com o esquema escolhido, uma ou mais máquinas validadoras são responsáveis por gerar cada novo bloco de transações que serão incluídas na Blockchain. O novo bloco pode ser aceito diretamente sem verificação ou por votação unanime dos geradores dos blocos ou por votação da maioria, dependendo da configuração escolhida para a Blockchain.

- ***Cross-Fault Tolerance* (XFT)**: baseado no consenso BFT, combina protocolos de comunicação síncronos e assíncronos, uma evolução dentro dos algoritmos BFT. Segundo a IBM, responsável pelo desenvolvimento do XFT, este algoritmo possui inteligência para usar menores caminhos e também ignora possíveis ataques que hoje são muito caros (computacionalmente) e extremamente improváveis.

2.3.4 Plataformas e Ferramentas

Implementar uma rede Blockchain não é algo trivial, é necessário o conhecimento em diversos assuntos e tecnologias, além da compreensão de como uma rede blockchain funciona.

Aqui são apresentadas algumas plataformas e ferramentas que auxiliam na atividade de implementar a tecnologia Blockchain.

Neste contexto, plataforma é um conjunto de software que implemente quase que em sua totalidade as características da tecnologia Blockchain. Ferramentas são componentes de software que possuam quantidade e capacidade limitada de participação na tarefa de implementar a rede descentralizada com cadeia de blocos.

Também é importante entender que *Frameworks* são estruturas de software, compostos por um conjunto de *scripts* e ferramentas para a criação de aplicações.

2.3.4.1 Ethereum

Ethereum é uma plataforma de computação distribuída baseada em Blockchain e de código aberto que fornece uma máquina virtual descentralizada (COINBR, 2020).

A plataforma Ethereum possui um conjunto de ferramentas e frameworks para a implementação, dentre eles podemos citar a Truffle Suite (2020), que auxilia na implementação de contratos inteligentes usando a linguagem de programação Solidity (2020), linguagem especifica para contratos em uma rede Ethereum.

2.3.4.2 Hyperledger

A plataforma Hyperledger é resultado de um esforço colaborativo entre indústrias de diversas áreas para criar um registro distribuído de código aberto (The Linux Foundation, 2015).

De maneira geral seu objetivo é promover a adoção em massa da tecnologia Blockchain, reutilizando recursos em comum para acelerar o processo de inovação (HYPERLEDGER, 2020).

Dentre os cinco frameworks, o que mais chama atenção é o **Hyperledger Fabric**. O **Fabric** foi projetado para o desenvolvimento de aplicações com uma arquitetura modular, permitindo que serviços sejam associados utilizando o método *plug-and-play* (conectar e usar).

2.4 Considerações Finais

Neste capítulo é apresentado um conjunto de conceitos básicos como Criptografia e Blockchain, sua estrutura e funcionamento. Conceitos essenciais para a o entendimento da proposta desta pesquisa e compreensão do método de tomada de decisão apresentado no Capítulo 4.

A não compreensão destes tópicos dificultará o entendimento do leitor nos demais capítulos, principalmente nos quesitos de configurações avançadas que a metodologia aborda.

O Capitulo 3 apresenta trabalhos relacionados com a proposta da pesquisa, descrevendo os mesmos e o porque deles serem relevantes para o estado atual do método proposto.

3 Trabalhos Relacionados

Neste capítulo, serão apresentados os principais trabalhos relacionados à temática associada a esta pesquisa.

Para um melhor entendimento, este capítulo foi dividido em três seções: a seção 3.1 discorre sobre trabalhos de contexto geral que dão suporte à escolha e uso da Blockchain como solução, apresentando algumas propostas de metodologias em contextos variados. A seção 3.2 apresenta contribuições mais próximas do objetivo deste trabalho, levando em consideração avaliação de riscos, modelos de maturação e abordagem orientada a requisitos. A seção 3.3 discorre sobre o que está faltando no estado da arte no que se refere aos modelos e metodologias relacionadas com o trabalho.

Alguns dos trabalhos aqui citados podem ser encontrados nos portais de periódicos (XPLORER, 2020), (ACM, 2020) e (SPRINGER, 2020), utilizando o termo de pesquisa ”Blockchain Methodology” (sem aspas). No caso do (XPLORER, 2020), até o momento de escrita deste trabalho, a pesquisa retorna 160 publicações. Dentro do conjunto de publicações, os títulos e resumos foram avaliados, levando em consideração os objetivos da pesquisa (metodologia para tomada de decisão quanto ao uso de Blockchain). Outros trabalhos são referências citadas em trabalhos anteriormente feitos pelo autor da pesquisa e referências de referências.

3.1 Propostas que dão suporte à escolha e uso da Blockchain

Visando um contexto geral, no sentido de não haver área de aplicação definida, Wüst e Gervais (2018) apresentam uma análise sobre quando o uso de Blockchain é de fato uma solução técnica apropriada, segundo as características do problema em questão.

Apresentando um fluxograma para auxiliar os leitores, Wüst e Gervais (2018) traçam um caminho baseado em perguntas sobre características do problema a ser resolvido. Exemplo de perguntas: múltiplas entidades escreverão no livro razão? A aplicação será baseada em estados e os mesmos precisam ser armazenados? Todos que criarão registros são confiáveis? Tais perguntam guiam o leitor para uma resposta positiva ou negativa quanto ao uso de Blockchain.

Os trabalhos de Pahl, Ioini e Helmer (2018) e Caramés e Lamas (2018), apresentam as categorias de Blockchain divididas em: (I) pública e privada e (II) com e sem permissão, provendo uma estrutura sistematizada para determinar qual modelo deve

ser seguido e desta forma contribuir para o sucesso da aplicação e do projeto.

Uma taxonomia de sistemas baseados em Blockchain é apresentada por Xu et al. (2017), expondo questões mais internas de como é uma implementação da tecnologia. Tal trabalho mostra características técnicas, como a forma de lidar com mecanismos de consenso e tratamento do anonimato nos registros.

A tecnologia Blockchain possui muitas configurações possíveis e variantes, por exemplo: a escolha do mecanismo de consenso, o que torna o trabalho de arquitetar uma solução complexo, sem um mapeamento da visão de arquitetura de software (XU et al., 2017).

No contexto de registros públicos e cidades inteligentes, Ibba et al. (2017) propõem o monitoramento da qualidade de ambientes urbanos através de uma rede descentralizada de sensores móveis, que são dispositivos de Internet das Coisas (do inglês ***Internet of Things* - IoT**).

Sensores que produzem medições digitais, úteis para investigar e estudar a qualidade de vida em cada parte da cidade. Na visão proposta, os dados do ambiente precisam estar disponíveis e compartilhados para todos os cidadãos, tais dados precisam ser não modificáveis (IBBA et al., 2017).

Os dados são armazenados em uma Blockchain, que possui disponibilidade, capacidade e integridade compatíveis com o desejado para a proposta de visão. Unida com a possibilidade de uso de contratos inteligentes (*smart contracts*), faz com que seja possível alcançar o nível de gerenciamento e controle lógico desejado (IBBA et al., 2017).

Novos riscos surgem ao adotar tecnologias disruptivas, a Blockchain não está livre desta afirmação. Morganti, Schiavone e Bondavalli (2018) identificam as ameaças mais relevantes e avaliam os impactos relativos as mesmas.

Para cada ameaça, executam uma avaliação qualitativa de riscos. Com os objetivos: (I) dar uma visão ampla para usuários e projetistas sobre os possíveis riscos ao adotar a tecnologia Blockchain; (II) Compreender as forças e fraquezas da Blockchain e como ela pode ser atacada; (III) Tornar a Blockchain mais segura e resiliente, explorando soluções e contramedidas.

3.2 Modelo de Maturação e Metodologia para Blockckain

Um modelo de maturação para adoção de Blockchain é proposto por Wang, Chen e Xu (2016), utilizando um modelo de quatro indicadores: (i) Redes; (ii) Sistemas de informação; (iii) Metodologias computacionais e (iv) Segurança e Privacidade.

O estudo de Wang, Chen e Xu (2016) serve como um guia para instituições ado-

tarem a Blockchain de forma sistematizada, observando aspectos internos (requisitos e recursos) e externos (equipe, organizações relacionadas e impacto nos resultados do negócio).

A proposta de metodologia apresentada por Staderini, Schiavone e Bondavalli (2018), possui como objetivo auxiliar projetistas em determinar quando uma Blockchain é ou não a solução mais apropriada para um problema específico, dados os requisitos.

Além de saber se Blockchain é uma solução adequada ou não, saber a categoria apropriada de implementação é tão importante quanto. Esta decisão não é trivial, visto que há várias formas de combinar as características da Blockchain e ainda manter as características principais da definição.

A metodologia proposta por Staderini, Schiavone e Bondavalli (2018) consiste de partes e guias para configuração e seleção da Blockchain. Considerando critérios relacionados aos algoritmos de consenso, suporte a contratos inteligentes, medidas de segurança, privacidade, anonimato, computação de dados e armazenamento.

A Figura 5 apresenta um fluxograma criado para representar o processo proposto por Staderini, Schiavone e Bondavalli (2018). O fluxo na Figura 5 possui 3 atividades principais que são: (I) Análise de requisitos do projeto, (II) Escolha da Categoria da Blockchain e (III) Configuração Específica.

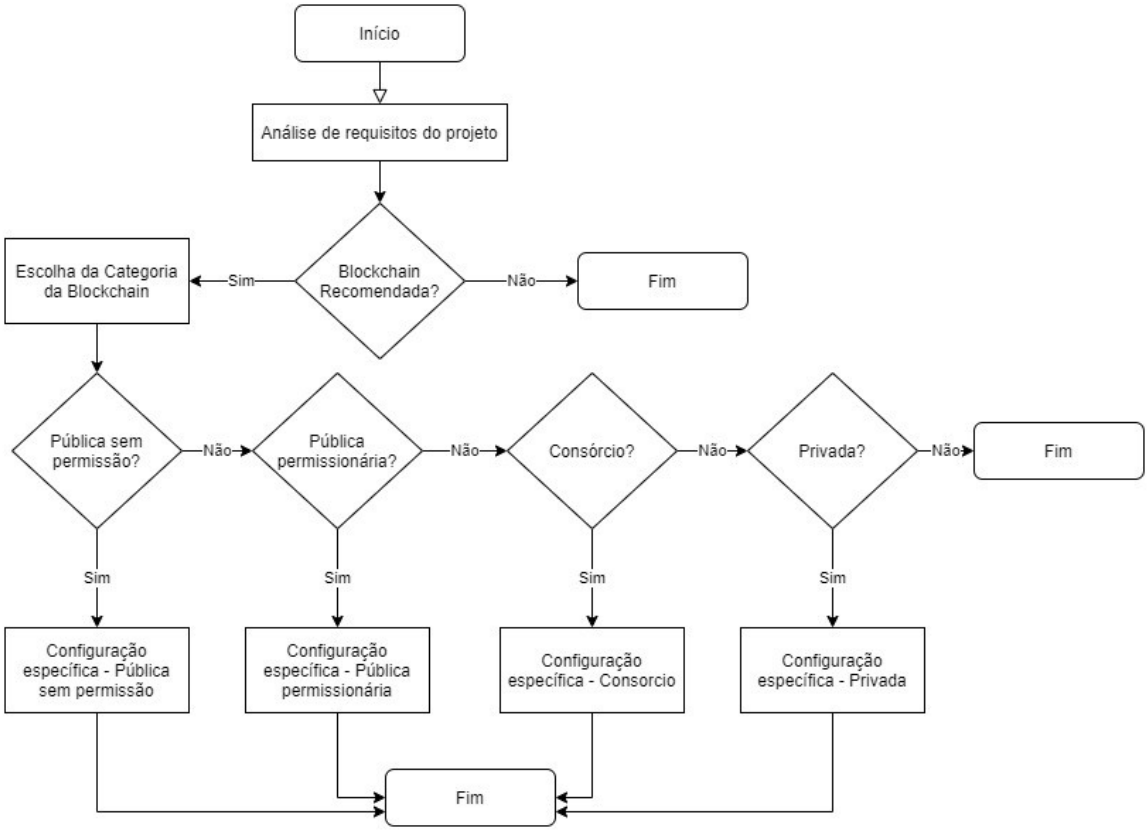
3.3 Discussão

Dentre os trabalhos relacionados, o apresentado por Staderini, Schiavone e Bondavalli (2018) é o mais próximo do que é esperado para uma proposta de metodologia que leva em consideração o uso de dados de registros públicos, pois não somente basta saber que serão fornecidos dados de cidadãos que podem ser acessíveis aos mesmos, mas também como esses dados serão disponibilizados.

Porém, a proposta de Staderini, Schiavone e Bondavalli (2018) presume que os riscos de segurança da informação já são conhecidos e também presume que a implementação será utilizando soluções baseadas em um único fornecedor de produtos (*hardware* e *software*).

Da forma que está o trabalho de Staderini, Schiavone e Bondavalli (2018) não poderia ser utilizado por organizações que não possuam o mesmo contexto apresentado na proposta. Como exemplo, Staderini, Schiavone e Bondavalli (2018) apresentam uma implementação de Categoria Privada para a implementação Blockchain. Ao tentar utilizar o método proposto por Staderini, Schiavone e Bondavalli (2018) é possível notar que há fluxos que levam a caminhos vázios.

Figura 5 – Visão geral da Metodologia baseada em Requisitos para seleção e configuração de Blockchains



Fonte: Produzido pelo autor.

Organizações, sejam elas públicas ou privadas, possuem contextos, equipes e necessidades diversas; logo uma metodologia que possa ser aplicada levando em consideração as características da organização seria o ideal, para um processo que realize a projeção e uso da tecnologia Blockchain.

4 Uma metodologia para suporte à tomada de decisão quanto ao uso de blockchain na área de registros públicos

Este capítulo apresenta a proposta de metodologia em resposta ao problema de pesquisa definido neste trabalho. A principal questão que a pesquisa se propõe a responder é: como determinar se o uso da tecnologia Blockchain é indicada como solução em um projeto que envolve o uso de registros públicos?

Para auxiliar a responder a pergunta da pesquisa, é utilizada a *Business Process Model and Notation* (BPMN), notação comum em diversos ambientes de gestão de processos (OMG, 2013). A BPMN possui quase todos os recursos necessários para a representação do processo da metodologia. Além dos conceitos de atividades e subprocessos, neste trabalho é usado o conceito de macroatividade.

No contexto deste trabalho, uma macroatividade é uma atividade que pode ser dividida em várias outras menores, difere do conceito de subprocesso da notação BPMN pois uma macroatividade pode conter subprocessos dentro de subprocessos, situação não definida pela notação BPMN.

A metodologia proposta é dividida em 3 (três) marcos (do inglês *milestone*, termo usado para indicar um momento chave na linha do tempo de um processo), onde cada marco é composto por um conjunto de atividades que são necessárias para selecionar e decidir sobre as configurações de implementação da tecnologia a fim de alcançar a finalidade proposta por este trabalho.

Na subseção 4.1 - é fornecida uma visão geral da metodologia proposta e também são apresentadas as definições de cada macroatividade envolvida nas etapas do processo de decisão sobre o uso de Blockchain.

Na subseção 4.2 - são apresentados os subprocessos da metodologia, de forma que o leitor possa ter uma visão detalhada das atividades por meio de diagramas baseados na notação BPMN.

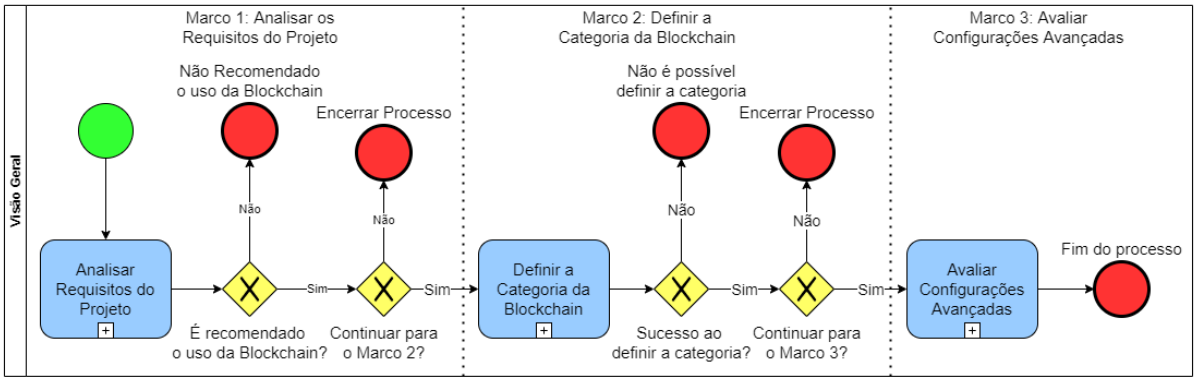
4.1 Visão Geral da Metodologia Proposta

A abordagem proposta neste trabalho tem como objetivo apoiar o(s) projetista(s) de sistemas no que se refere a como decidir e planejar a implementação da tecnologia blockchain para soluções que envolvam registros públicos. Respondendo perguntas

como: (I) Devemos usar blockchain como solução? (II) Em qual categoria a blockchain que será usada está? (III) Quais aspectos de configurações e segurança devem ser observados?

A Figura 6 apresenta uma visão geral do fluxo completo da metodologia, que é dividida em 3 (três) marcos.

Figura 6 – Visão geral da Metodologia Proposta



Fonte: Produzido pelo autor.

Os marcos estão divididos em:

1) **Analisar os Requisitos do Projeto**: Neste momento, o projetista avalia as características do problema que será resolvido com a finalidade de saber se o uso da tecnologia Blockchain é adequado ou não como solução. Havendo a recomendação de uso da tecnologia Blockchain, o processo segue perguntando se o projetista deseja prosseguir para o Marco 2. Não havendo a recomendação, o processo encerra com a saída “Não recomendado o uso da Blockchain”.

2) **Definir a Categoria da Blockchain**: Nesta fase, o projetista, baseado nos requisitos do projeto, analisa a categoria da blockchain que deve ser usada, seguindo a classificação apresentada por Xu et al. (2017) somada a apresentada por Wüst e Gervais (2018). As categorias presentes hoje na metodologia são: (a) pública sem permissão, (b) pública permissionária, (c) consórcio e (d) privada. Saber a categoria da Blockchain possibilita uma melhor escolha das ferramentas e plataformas que serão usadas na implementação.

3) **Avaliar Configurações Avançadas**: Para dar embasamento ao projetista sobre quais características de configuração adotar, esta etapa segue os mesmos passos apresentados por Staderini, Schiavone e Bondavalli (2018), sendo composta por 5 (cinco) subprocessos: (I) Mecanismo/Algoritmo de Consenso, (II) Contrato Inteligente, (III) Medidas de Segurança, (IV) Privacidade e Anonimato e (V) Processamento dos Dados e Armazenamento. A configuração avançada não é obri-

gatória para todos os casos, visto que ferramentas e plataformas já oferecem os aspectos apresentados no marco 3 definidos por padrão. Em casos onde detalhes de comportamento do algoritmo de consenso, contratos inteligentes, processamento das transações e/ou o armazenamento de dados são pontos importantes, para o sucesso da solução, é necessário o aprofundamento nas configurações avançadas da tecnologia.

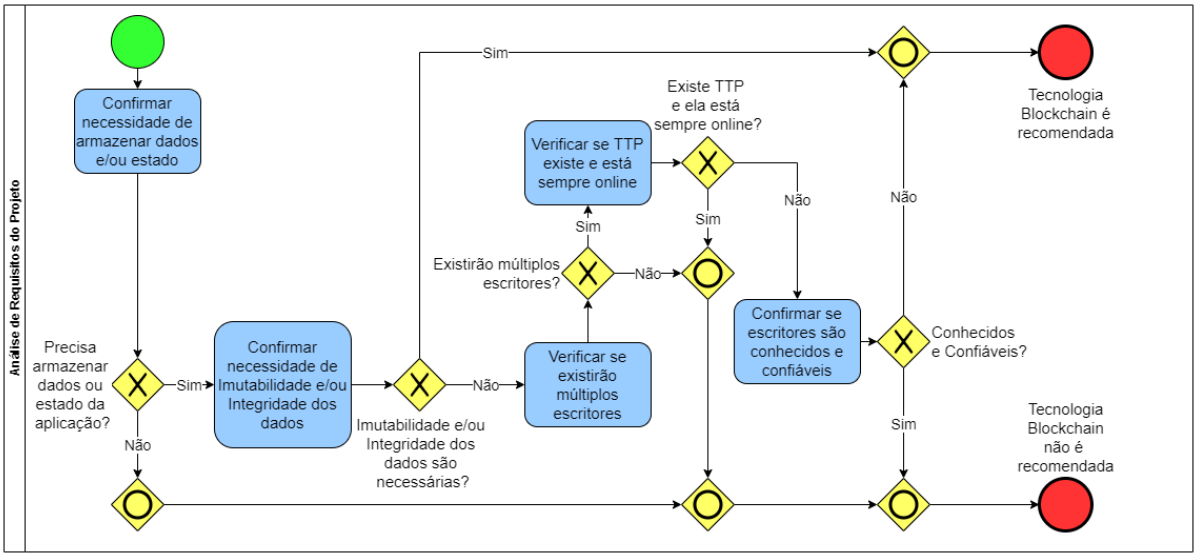
4.2 Detalhamento da Metodologia

4.2.1 Analisar os requisitos do projeto

Esta seção descreve os primeiros passos da metodologia proposta, os quais consistem em determinar se usar a Blockchain como solução é apropriada ou não, considerando as características do problema. Em outras palavras, se deve responder a seguinte questão: “Devemos usar blockchain como solução?”.

Em um projeto de software, primeiros entendemos o problema que será resolvido para depois escolhermos quais tecnologias serão usadas. Após compreender o problema, é possível escolher como será resolvido e decidir quais tecnologias serão usadas. Estas decisões são baseadas nos requisitos do projeto. A Figura 7 apresenta o processo referente a análise de requisitos do projeto.

Figura 7 – Processo de análise de requisitos do projeto



Fonte: Produzido pelo autor.

O processo de análise de requisitos do projeto é uma extensão de Wüst e Gervais (2018), incluindo a questão sobre imutabilidade e/ou integridade dos dados como critério adicional. Alguns critérios incidem diretamente no resultado de recomendar a tecnologia Blockchain ou indicar o não uso da tecnologia.

As atividades deste marco são:

- **Confirmar necessidade de armazenar dados ou estado**. A primeira atividade é confirmar a necessidade de armazenar dados ou estado da aplicação. Se no projeto não houver a necessidade de armazenar nenhum deles, não é necessário o uso da Blockchain. Logo, se este não for um requisito, o processo encerra com a resposta "Tecnologia Blockchain não é recomendada".

- **Confirmar necessidade de Imutabilidade e/ou Integridade dos dados**. Se imutabilidade é um requisito, então é possível considerar o uso da Blockchain, pois esta é uma propriedade forte da tecnologia. A integridade também é avaliada neste mesmo bloco. Se um projeto necessita que os dados sejam protegidos contra alterações não autorizadas, então pode ser alcançado com o uso da Blockchain.

  Os termos imutabilidade e integridade podem parecer sinônimos em muitos casos, porém neste contexto imutabilidade é a impossibilidade de se alterar algum registro. Imutabilidade é regra de negócio. A integridade, segundo Stallings (2014), é a capacidade de prevenir-se contra a modificação ou destruição imprópria de informação.

- **Verificar se existirão Múltiplos Escritores**. Esta atividade do processo está relacionada com a decisão de armazenamento de dados ou estado, considerando a multiplicidade de entidades encarregadas de escrever. Se apenas uma entidade escreve, uma base de dados comum é mais apropriada que uma Blockchain.

  A vazão de dados e latência de rede são pontos importantes e que em um ambiente com apenas um escritor causariam custos de processamento e comunicação desnecessários.

- **Verificar se existe TTP e se o mesmo está sempre online**. Uma terceira parte confiável, do inglês *Trusted Third Party* (TTP), é uma entidade que facilita as interações entre entidades que não possuem confiança umas nas outras. Neste ponto temos 3 (três) possíveis cenários, que são:

  (i) Se no sistema uma TTP é necessária e está planejada para sempre estar online, as entidades podem delegar para ela as operações de escrita de transações ou mudanças de estado. Portanto, a TTP possui um papel de confiança no ambiente para entrega e verificação de registros, dados e demais informações relevantes ao contexto. Neste caso, a Blockchain, conhecida por ser uma tecnologia para ambiente em que os participantes não confiam entre si, se torna desnecessária e a metodologia retorna o resultado "Tecnologia Blockchain não é recomendada".

(ii) Em um segundo cenário temos a existência de uma TTP, porém a mesma não está sempre online. Neste caso, ela se torna uma entidade que dá autorizações em uma Blockchain permissionária (*permissioned blockchain*).

(iii) Como terceiro cenário, uma TTP pode não existir. Em ambos os cenários II e III não se pode excluir a recomendação de usar a tecnologia Blockchain. A Blockchcain exercerá um papel próximo ao que a TTP teria se existisse e estivesse sempre online, sendo o ponto de confiança entre as partes envolvidas.

- **Confirmar se Escritores são conhecidos e confiáveis**. Se todas as entidades envolvidas na escrita são conhecidas e há confiança nos dados fornecidos entre elas, significando que são mutualmente confiáveis, então uma Blockchain não é necessária. Uma base de dados tradicional compartilhada entre as entidades é uma solução mais adequada.

Em outros trabalhos, como o de Wüst e Gervais (2018) e Staderini, Schiavone e Bondavalli (2018), é recomendada a atividade de verificação de não repúdio. Nessa atividade, o projetista é perguntado sobre a necessidade de haver ou não a possibilidade de não repúdio sobre os registras na Blockchain. Ao responder sim para a necessidade de haver não repúdio, é indicado ao projetista utilizar a tecnologia Blockchain, sem a realização de mais perguntas.

Vimos que a atividade de verificação de não repúdio se torna opcional devido às possibilidades de resposta positiva ou negativa. Haver não repúdio significa que uma entidade não pode se livrar da responsabilidade por um registro ou ação na rede. Para esse tópico temos dois cenários:

(i) É necessário garantir o não repúdio. Com apenas isto, não é possível recomendarmos o uso da tecnologia Blockchain, pois o não repúdio pode ser alcançado de outras formas, sem Blockchain. Usar assinatura digital e par de chaves de criptografia é uma forma alcançar não repúdio.

(ii) Não é necessário garantir o não repúdio. Também não podemos responder se a tecnologia Blockchain é ou não recomendada apenas baseado neste ponto. Outras características da tecnologia também podem ser relevantes para a solução do problema alvo do projeto, como no caso da imutabilidade de registros e terceira parte confiável.

4.2.2 Definir a categoria da Blockchain

Neste marco, as atividades guiarão o projetista para responder questões que traçam um perfil de implementação e assim poder categorizar entre as possíveis alter-

nativas hoje existentes.

As categorias são: Blockchain Pública sem permissão; Blockchain Pública Permissionária, Blockchain Consórcio e Blockchain Privada. Podemos definir cada categoria como segue:

- **Pública sem permissão**. Permite que todos os usuários possam criar contas pessoais e interajam com a rede, submetendo transações e adicionando blocos ao livro razão. Todas as partes possuem a opção de se tornar um nó do sistema, empregando protocolos de mineração para ajudar na verificação de transações e registro das mesmas.
- **Pública Permissionária**. São ecossistemas fechados para quem registra os dados, porém aberto para a leitura dos registros. Os usuários não são livres para ingressar na rede, é necessário haver um grupo de usuários que decidem sobre a entrada e saída de nós na rede, assim como o controle do processo de autenticação.
- **Privada**. Atua como sistema fechado, onde os usuários não são livres para ingressar na rede, a leitura dos registros não é aberta, assim como o registro de transações na cadeia de blocos. São voltadas para organizações que precisam do poder da tecnologia blockchain para seus próprios processos de negócio.
- **Consórcio (ou Comunitária)**. É "semiprivada", controlada por um grupo de usuários, mas funciona por meio de organizações diferentes. Por definição, a finalidade das organizações não é fator determinante para a classificação na categoria, as organizações podem ou não ter fins lucrativos, como também podem ou não ser públicas e/ou privadas.

Primeiro, para ser possível definir a categoria da Blockchain, é necessário considerar as operações de leitura e escrita. Como descrito por Wüst e Gervais (2018), estes termos indicam múltiplas operações, sendo a escrita o ato de registrar na cadeia de blocos transações (dados) e a leitura a ação de recuperar transações nos blocos.

No diagrama apresentado na Figura 8, as operações de leitura e escrita são divididas em duas ações na rede, separadamente considerando: (I) Consultar o estado do livro razão e (II) Criar transações.

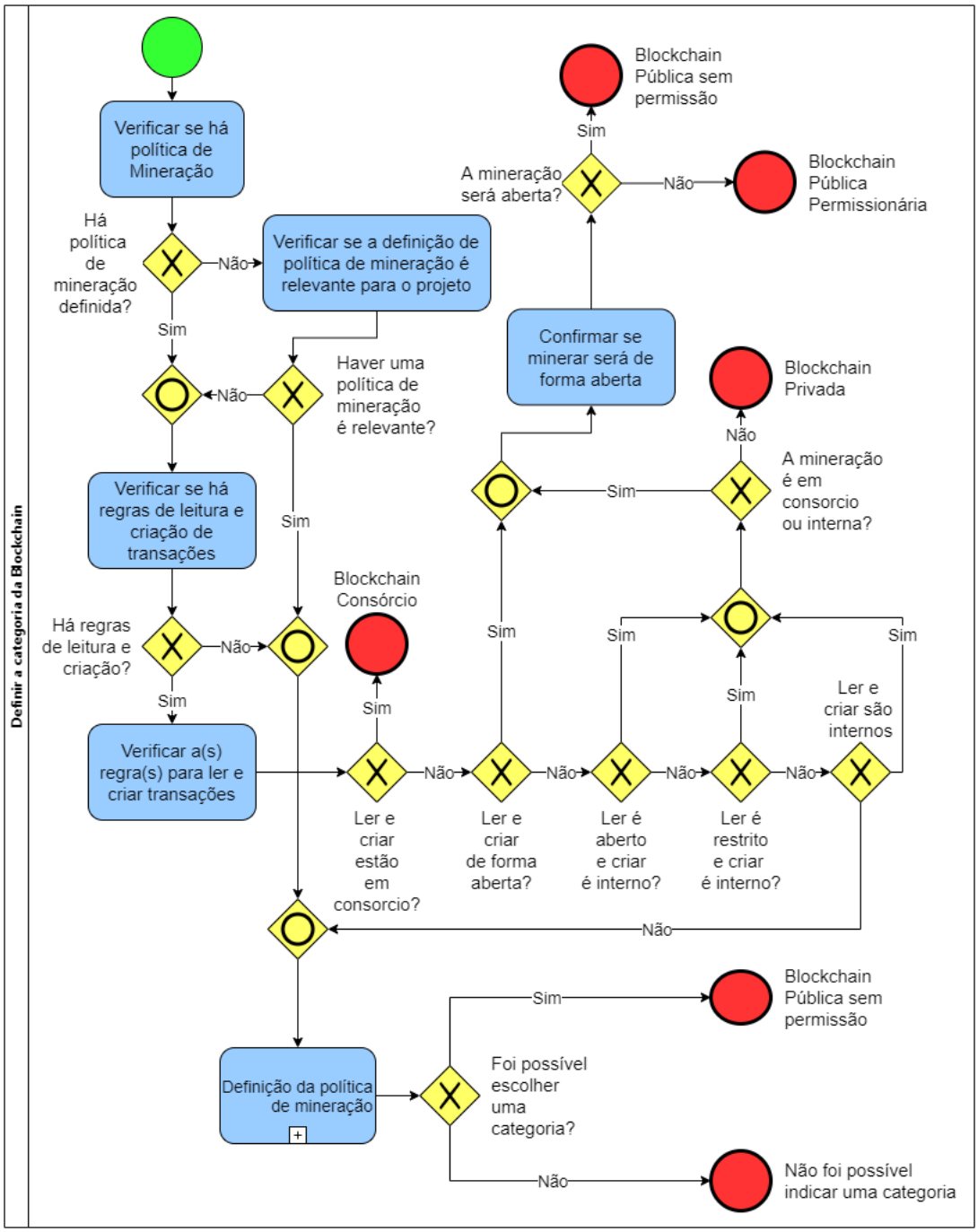
As possíveis configurações para as duas operações na rede são: Aberto, restrito e interno, significando respectivamente que a operação é permitida por qualquer nó, permitida para alguns nós privilegiados apenas, e permitida para alguns nós privilegiados pertencentes a uma única organização apenas.

A política de mineração é um requisito de projeto que estabelece as entidades permitidas para executar operações de escrita de blocos (WüST; GERVAIS, 2018).

As possibilidades apresentadas no diagrama são: Mineração Aberta, significa que todos os nós podem escrever; Mineração consórcio, onde apenas alguns nós são permitidos escrever, mas eles podem ser entidades pertencentes à diferentes organizações ou mineração interna, onde os mineradores são apenas um subconjunto de nós da mesma organização.

Para situações onde a política de mineração não está definida e a existência da mesma é um ponto importante para o projeto, Staderini, Schiavone e Bondavalli (2018) sugerem um subprocesso separado que leva em consideração 10 (dez) características, onde se não for possível definir uma política de escrita baseada nos aspectos questionados, não será possível para a metodologia sugerir uma categoria.

Figura 8 – Processo para definir a categoria da Blockchain



Fonte: Produzido pelo autor.

As características consideradas para a definição de uma política de mineração são:

- **Escalabilidade**: característica que indica a possibilidade de aumento nas taxas de processamento de transações, aumento do número de nós e latência de comunicação estável com o aumento da rede.
- **Custo de transação**: refere ao custo computacional para que novos blocos sejam criados, registrados e recuperados na cadeia.
- **Desempenho**: característica que indica o quão rápido a rede deve responder às requisições.
- **Descentralização**: indica o quão importante é que a aplicação não possua pontos de responsabilidade centralizados.
- **Disponibilidade**: refere-se sobre o quão disponíveis são os nós para que as operações de leitura e escrita possam ser realizadas sem perda de dados ou demora para resposta.
- **Anonimidade**: indica a possibilidade de não registrar o autor de ações tomadas na rede, isso é uma característica forte em redes públicas sem permissão, onde não é necessário haver uma identificação de quem usa a rede.
- **Privacidade**: o quão é possível manter informações em sigilo, sobre o dono de algum ativo registrado na rede ou até a identificação de informações do ativo em si.
- **Confidencialidade**: refere-se à possibilidade de manter informações sigilosas somente acessíveis aos respectivos usuários detentores dos direitos sobre as informações, podendo ser um dono de ativo, grupo de pessoas ou organizações detentoras de propriedade intelectual, por exemplo.
- **Transparência**: característica que indica que transações e registros de blocos são de conhecimento da rede, ou sua maior parte.
- **Não confiança entre as partes**: principal característica da tecnologia Blockchain, as partes envolvidas em uma operação de troca de ativos ou bens, não precisa confiar entre eles para que a transação possua garantia de que obedecerá às regras de negócio. Com o uso de contratos inteligentes essa característica ganha ainda mais força, sendo algo muito relevante na definição da categoria da Blockchain.

Na subseção 4.2.2.1, o subprocesso de definição da política de mineração é detalhado.

4.2.2.1 Definição da Política de mineração para a Blockchain

Conforme descrito na subseção 4.2.2, se não houver uma política de mineração definida para o projeto e a existência da mesma é um ponto importante, não será possível para a metodologia indicar uma categoria de Blockchain.

Caso o projetista precise definir uma política de mineração, pode usar o subprocesso descrito nesta subseção. A visão deste subprocesso pode ser vista na Figura 9 e Figura 10, onde cada parte será explicada.

O projetista terá que avaliar, dentre as características apresentadas, qual delas possui mais relevância para o projeto. As características são: Escalabilidade, Custo de transação, Desempenho, Descentralização, Disponibilidade, Anonimidade, Privacidade, Confidencialidade, Transparência e Não confiança entre as partes.

Segundo Staderini, Schiavone e Bondavalli (2018), o projetista precisa ter o entendimento claro sobre o quão importante são essas características para que ele possa responder adequadamente as perguntas do subprocesso. Caso não exista correlação entre as características apresentadas e o projeto destino, não será possível sugerir uma categoria e o processo termina.

Dependendo da resposta sobre qual característica é a mais relevante, é necessário ao projetista responder perguntas sobre o quesito interoperabilidade.

Interoperabilidade, neste escopo, é definida como a necessidade de cooperação entre diferentes organizações compartilhando um único livro razão.

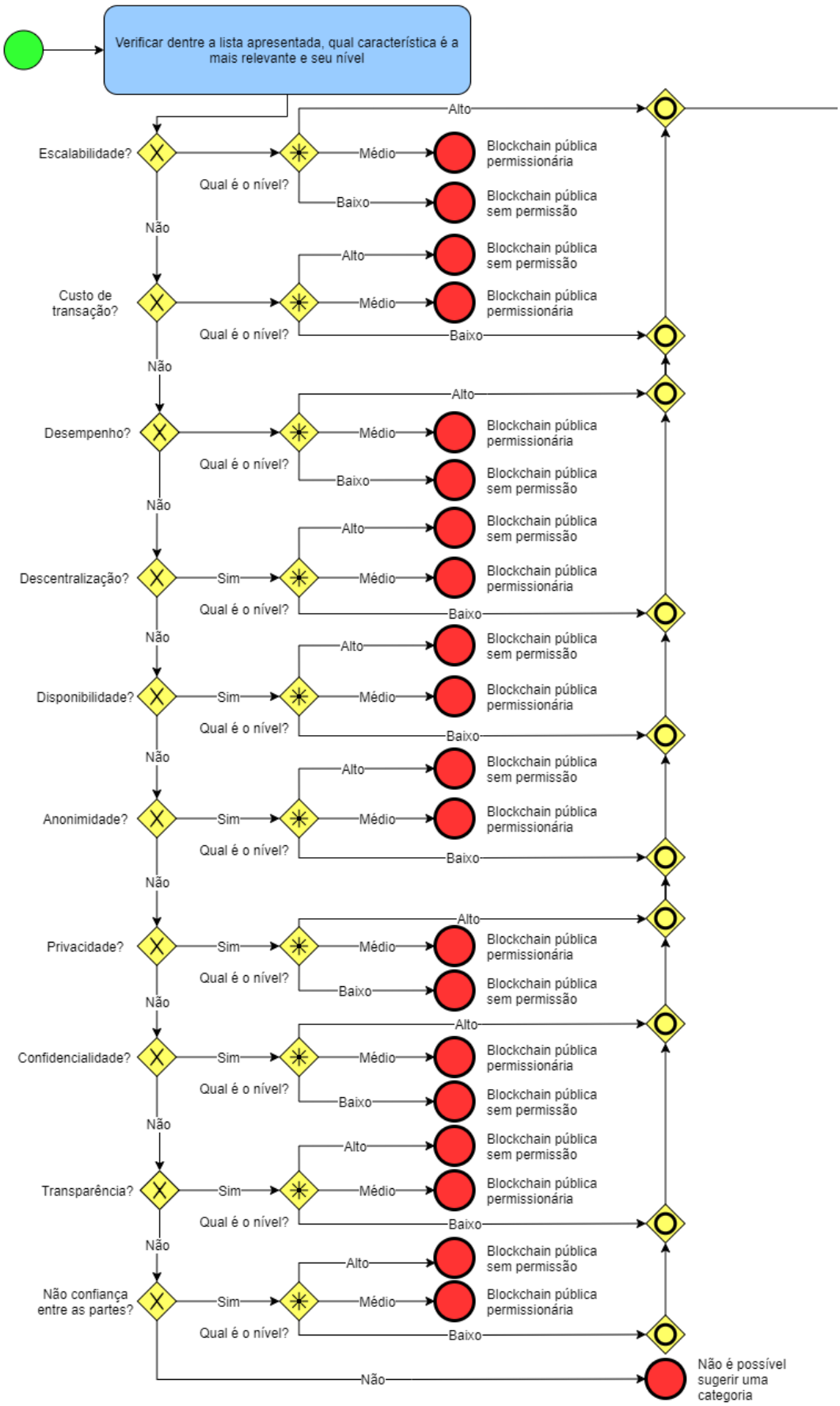
Compartilhar um livro razão entre diferentes organizações é típico de Blockchains consórcio e, portanto, pode servir como critério determinante para a escolha da categoria da Blockchain. Se interoperabilidade não for um ponto importante, o subprocesso considera a flexibilidade.

A flexibilidade está relacionada às alterações de configuração e permissões. A maior flexibilidade possível é encontrada em organizações privadas, que são gerenciadas e controladas por um único grupo de indivíduos.

Em uma implementação que não é privada, alterações de configurações e/ou permissões ocasionarão problemas como a inconsistência de comportamento, como no caso de uma alteração de chaves de criptografia de uma cadeia. Por consequência os registros antigos terão que ser reinseridos com novos *hashes* criptográficos, o que em um ambiente que não é privado, ocasionará inconsistência entre nós que ainda não possuem ou não estão fazendo uso da nova chave.

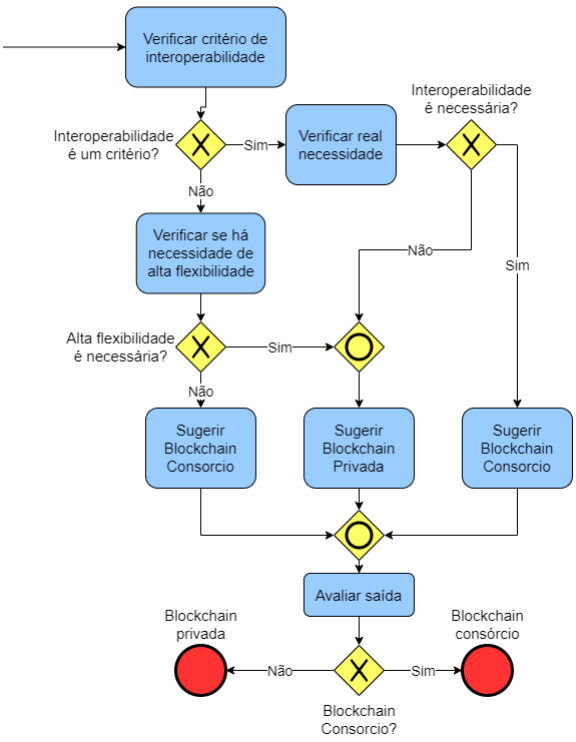
No caso de uma implementação de consórcio, deve ser acordado entre todas as partes os parâmetros para tais alterações.

Figura 9 – Subprocesso de definição da política de mineração - parte 1 de 2



Fonte: Produzido pelo autor.

Figura 10 – Subprocesso de definição da política de mineração - parte 2 de 2

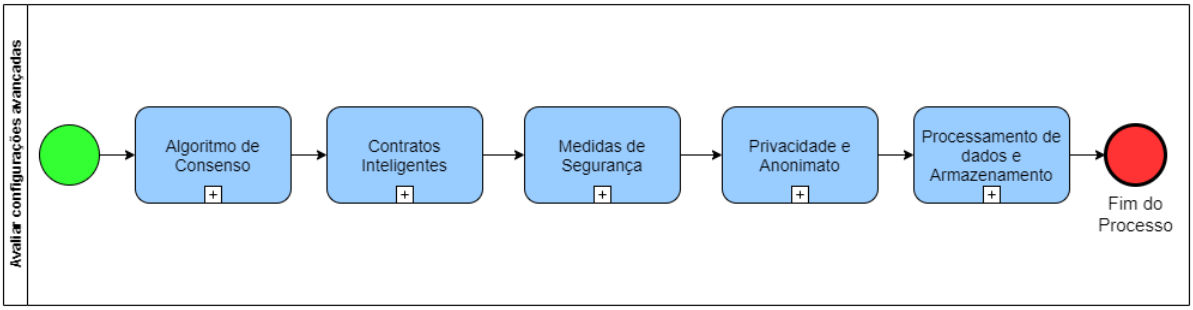


Fonte: Produzido pelo autor.

4.2.3 Avaliar configurações avançadas

O último marco da metodologia proposta consiste em avaliar configurações avançadas para a Blockchain. Este marco é composto por 5 (cinco) subprocessos: (I) Avaliar Algoritmo de Consenso, (II) Avaliar Contratos Inteligentes, (III) Avaliar Medidas de Segurança, (IV) Avaliar Privacidade e Anonimato, e (V) Avaliar Processamento de dados e Armazenamento. A Figura 11 apresenta o fluxo geral do marco 3 (três).

Figura 11 – Visão Geral do Marco 3: Avaliar configurações avançadas.



Fonte: Produzido pelo autor.

Os aspectos de configuração avançada dependem do nível de exigência do

projeto, experiência do(s) projetista(s) e também da categoria da Blockchain, resultado do marco 2 (dois) da metodologia.

Conforme dito anteriormente, a categoria da Blockchain ajudará o projetista na escolha das ferramentas e/ou plataformas que serão usadas para a implementação da Blockchain. Os subprocessos do marco 3 (três) possuem questionamentos técnicos sobre a implementação, levando em consideração o que é esperado e planejado para a rede do projeto.

Como primeiro subprocesso temos a avaliação do algoritmo de consenso, que traz questionamentos sobre como é esperado que a rede se comporte sobre o consenso entre os nós para aceitação do registro dos blocos. O diagrama apresentado na Figura 12 descreve o primeiro subprocesso do marco 3 (três).

4.2.3.1 Algoritmos de Consenso

Os algoritmos considerados neste trabalho constituem a seleção dos mais amplamente adotados, segundo Staderini, Schiavone e Bondavalli (2018), e os quais possuem dados suficientes quanto a suas propriedades e desempenho.

Conforme é mostrado pela Figura 12, o primeiro aspecto avaliado é a finalidade das transações. Dependendo do algoritmo, uma transação que é incluída em um bloco pode ser considerada imediatamente ou probabilisticamente final.

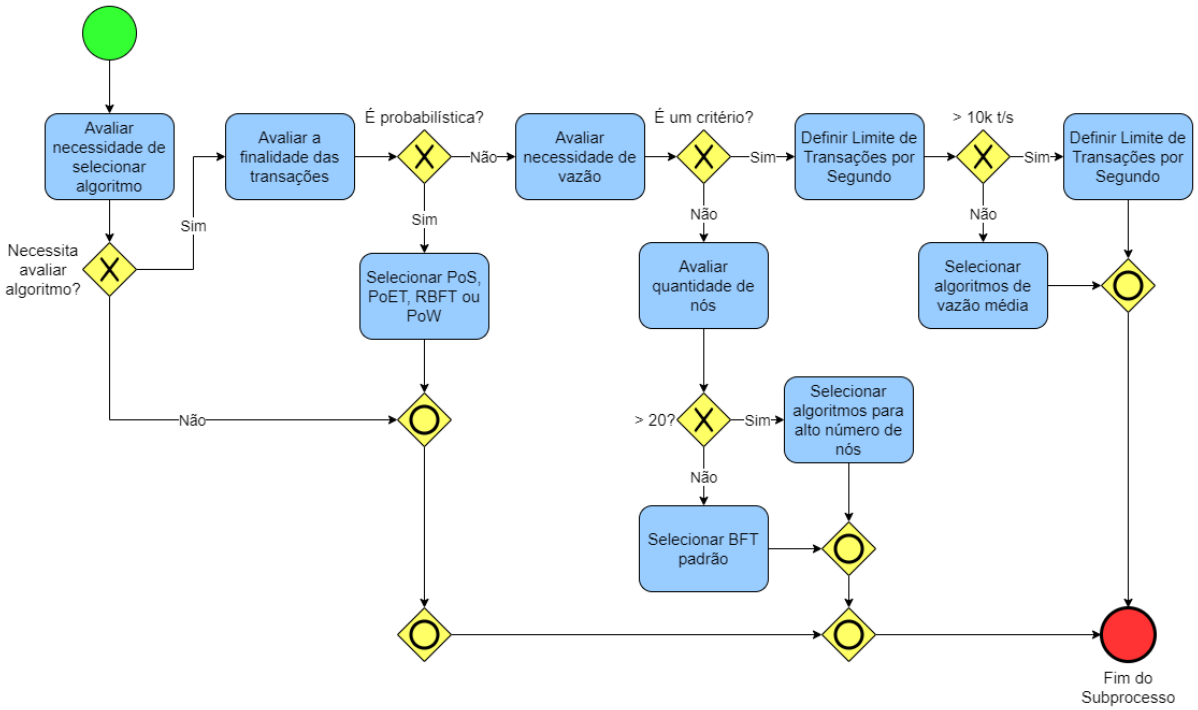
O algoritmo Proof of Work (PoW), proposto por Nakamoto (2008), é um algoritmo probabilístico. Ao utilizar PoW, é necessário que seja apresentada uma prova de trabalho e a mesma deve ser válida para que os nós na rede cheguem ao consenso sobre o registro do bloco, se o bloco deve ou não ser aceito.

Diferente do modelo de consenso probabilístico, existe o modelo de consenso determinístico. O modelo determinístico é tolerante a falhas de parada (*crash*) ou bizantinas (referente ao problema dos generais bizantinos) (REBELLO et al., 2019). Em uma implementação de Blockchain privada faz sentido existir algoritmos determinísticos, já que é apenas uma organização que é responsável pelos dados.

Supondo que este é um parâmetro presente na lista de requisitos do sistema, o projetista pode fazer uso da metodologia para obter um conjunto de algoritmos sugeridos. Se a escolha é probabilística, a possibilidade de saída é um algoritmo entre *Proof of Stake* (PoS), *Proof of Elapsed Time* (PoET) (BALIGA, 2017), *Randomized Byzantine Fault Tolerance* (RBFT) (VUKOLIć, 2016) e *Proof of Work* (PoW) (NAKAMOTO, 2008). Desta forma, o alcance de possíveis saídas é reduzido a quatro algoritmos de consenso. O fluxo continua considerando o próximo estágio, a configuração dos contratos inteligentes.

Se a transação é determinística, assim como se o critério não é indicado como

Figura 12 – Escolha do algoritmo de Consenso.



Fonte: Produzido pelo autor.

um requisito de projeto, é possível seguir o fluxo alternativo, o qual traz o seguinte aspecto para ser analisado: a vazão. Baseado na vazão, é possível distinguir duas classes de algoritmos apropriados.

A primeira classe é a de algoritmos capazes de processar entre 100 e 10^4 transações por segundo, o qual podemos chamar de Algoritmos de Vazão Média. São eles: *Randomized* BFT, *Hybrid* BFT, *Scalable* BFT, Kafka e Tendermint (CACHIN; VUKOLIC, 2017).

A segunda classe são dos algoritmos capazes de processar mais que 10^4 transações por segundo, que podemos chamar de Algoritmos de Vazão Alta, são eles: *Optimistic* BFT, BFT, *Pratical* BFT (PBFT), *Cross-Fault Tolerance* (XFT), BFT-SMaRT, *Proof of Authority* (PoA) (CACHIN; VUKOLIC, 2017).

Se a vazão não for considerada como um requisito importante do projeto, o número de nós para o consenso pode servir como um critério guiando a escolha do algoritmo. Este número não deve ser confundido com o número total de nós na rede Blockchain.

Uma escolha adequada, caso o número não seja superior a 20 (vinte), é o algoritmo BFT. O primeiro algoritmo da família BFT, referenciado como *Standard* BFT, tem limitação de escalabilidade, foi testado com um máximo de 20 (vinte) nós (VUKOLIć, 2016). Para mais de 20 (vinte) nós envolvidos no mecanismo de consenso, Staderini,

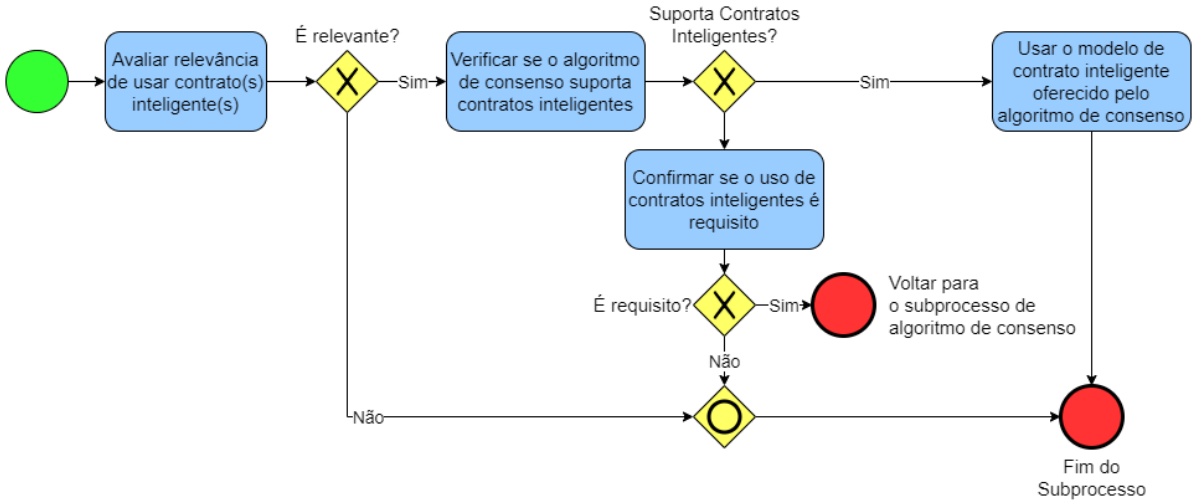
Schiavone e Bondavalli (2018) sugerem: XFT, *Optimistic* BFT, PBFT, *Hybrid* BFT, *Randomized* BFT, e *Scalable* BFT.

4.2.3.2 Contratos Inteligentes

Conforme mostrado na Figura 12, após a escolha do algoritmo de consenso, o fluxo segue para a configuração dos contratos inteligentes. Se o suporte a contratos inteligentes não for um requisito do projeto, este estágio pode ser pulado. Caso contrário, a configuração continua considerando o uso de contratos integrantes.

A Figura 13 mostra o fluxo deste estágio. Se o algoritmo de consenso não suportar o uso de contratos, o projetista precisará voltar para o subprocesso de escolha do algoritmo de consenso e escolher outro algoritmo, algoritmo este que ditará as regras para uso de contratos.

Figura 13 – Configuração de contratos Inteligentes.



Fonte: Produzido pelo autor.

4.2.3.3 Medidas de Segurança

Este subprocesso considera os possíveis problemas de segurança, guiando o projetista em direção a contramedidas baseadas na categoria do problema.

Staderini, Schiavone e Bondavalli (2018) optaram por dividir os problemas de segurança em níveis, utilizando o nível do risco como meio para dirigir as ações de projetistas, usando etiquetas como nível baixo (L, *Low*), médio (M, *Medium*) e alto (*High*).

Porém, Morganti, Schiavone e Bondavalli (2018) apresentam um sistema de categorias para ameaças de segurança, que melhor se adequa para este subprocesso.

Um sistema de categorias para ameaças é adequado para este subprocesso. Esta abordagem possibilita ao projetista não apenas planejar a implementação para os problemas conhecidos hoje. A abordagem também possibilita a tomada de ações rápidas para ameaças novas, onde o risco ainda não é totalmente conhecido.

Morganti, Schiavone e Bondavalli (2018) classificam as ameaças em 4 (quatro) categorias, que são:

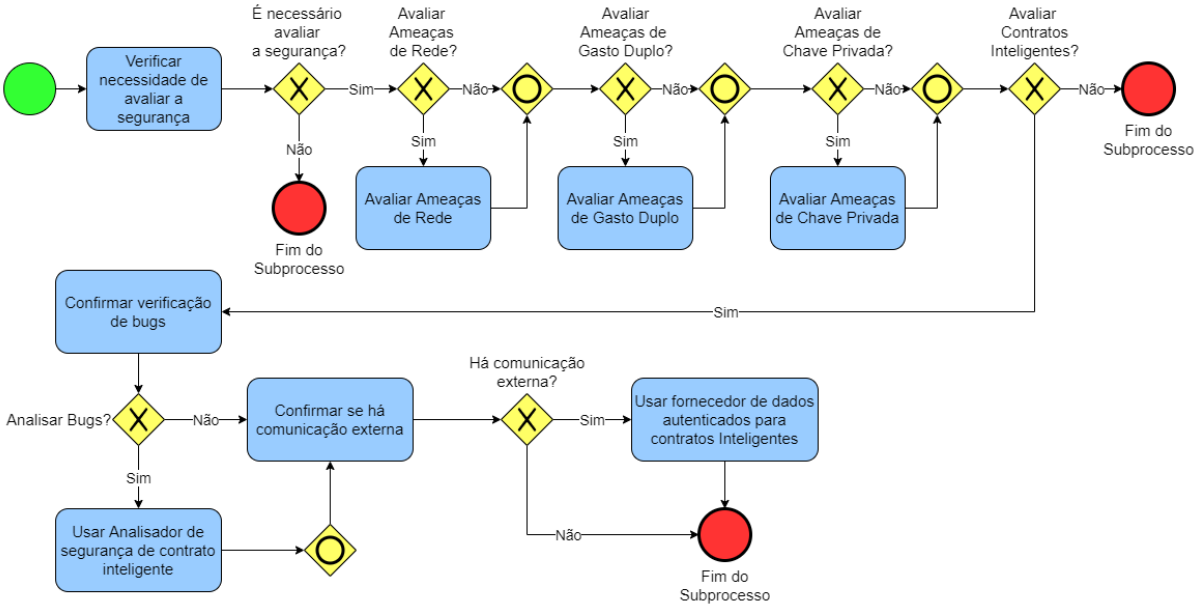
- **Ameaças de Rede**: ameaças que exploram os protocolos de comunicação, seus projetos e implementações. Tais como ataques de negação de serviço, envenenamento de tabelas de roteamento e resolução de nomes e data e hora na rede, protocolo *Network Time Protocol* (NTP).
- **Ameaças de Gasto Duplo**: ameaças baseadas na criação de duas ou mais transações conflitantes, que tentam gastar o mesmo recurso (fundos financeiros) com o objetivo de prejudicar uma terceira parte.
- **Ameaças de Chave Privada**: uma identidade pode ser roubada em uma rede Blockchain, mesmo havendo mecanismos de autenticação forte para evitar alguém se passar por outra pessoa. Ao utilizar chaves públicas e privadas, se uma chave privada for roubada, será difícil impedir o uso malicioso e/ou se recuperar dos possíveis prejuízos que podem ser causados pelo atacante utilizando a chave roubada.
- **Ameaças de Contratos Inteligentes**: contratos são aplicações dentro de Blockchains. Da mesma forma que as aplicações tradicionais estes estão sujeitas a problemas como bugs e brechas de segurança, contratos inteligentes também estão sujeitos a tais problemas. Analisar os contratos utilizando alguma ferramenta ou procedimento é importante para garantir um bom nível de segurança em uma implementação Blockchain 2.0 ou maior.

Basear-se nas categorias de ameaças é uma forma de evitar que alguma ameaça ainda não medida fique de fora da avaliação. Se a ameaça for conhecida então ela pode ser categorizada, o que já a inclui no processo apresentado na Figura 14.

Primeiro, o projetista precisa questionar se é necessário realizar a avaliação de segurança para a aplicação/projeto em questão, caso a resposta seja negativa o subprocesso termina. Durante todo o subprocesso é possível encerrar o mesmo sem precisar passar pelas atividades seguintes, basta o projetista escolher não prosseguir após o encerramento de cada avaliação.

Caso a resposta seja positiva, é necessário realizar a avaliação de segurança, o fluxo segue para a atividade Avaliar Ameaças de Rede, Avaliar Ameaças de Gasto

Figura 14 – Medidas de Segurança.



Fonte: Produzido pelo autor.

Duplo, Avaliar Ameaças de Chave Privada e avaliações de ameaças em Contratos Inteligentes.

Para as vulnerabilidades em contratos inteligentes, já existem soluções bem aceitas no mercado e meio acadêmico que dão suporte para o processo de avaliação de segurança. Para o bloco de análise de bug, o uso de uma ferramenta como Oyente (Melon Project, 2016) para contratos que usam a linguagem *solidity* ou abordagem similar é sugerido, enquanto a solução Town Crier é adequada se há a necessidade de comunicação externa (LI et al., 2017), já que a solução atua como fornecedor de dados autenticados para contratos inteligentes.

Ao final do subprocesso Medidas de Segurança, o projetista possuirá conhecimento suficiente para poder lidar com as ameaças conhecidas e as suas respectivas contramedidas.

4.2.3.4 Privacidade e Anonimato

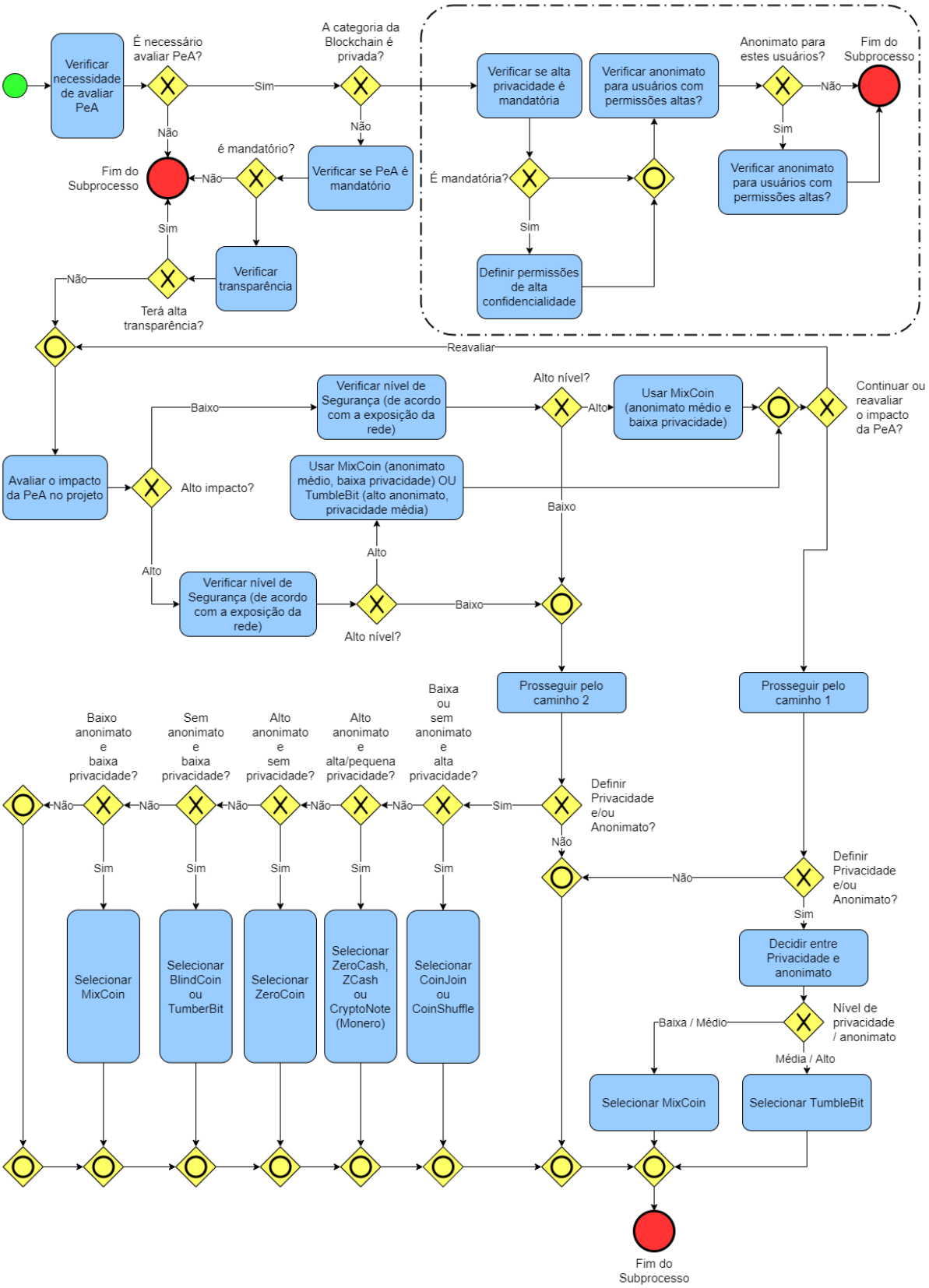
Neste subprocesso são apresentados protocolos que reforçam a camada de privacidade e anonimato, protocolos estes que são usados em redes Blockchain amplamente difundidas, como por exemplo o Bitcoin.

A metodologia leva em consideração as prováveis condições que a aplicação terá que lidar em relação ao trato dos dados das transações e dados dos usuários, problemas relativos à privacidade e anonimato, levando em conta características da categoria da blockchain, selecionada no marco 2 (dois).

Neste contexto é possível definir Privacidade como a capacidade da rede em prover dados e informações somente aos usuários que possuírem direito sobre a mesma, de forma homóloga à confidencialidade na tríade de segurança da informação. Anonimato, pode ser definido como a capacidade da rede em fornecer meios para que algum dado ou usuário não possa ser identificado por outros usuários da rede ou fora dela (STADERINI; SCHIAVONE; BONDAVALLI, 2018).

A Figura 15, mostra uma visão geral do subprocesso.

Figura 15 – Privacidade e Anonimato (PeA) visão geral.

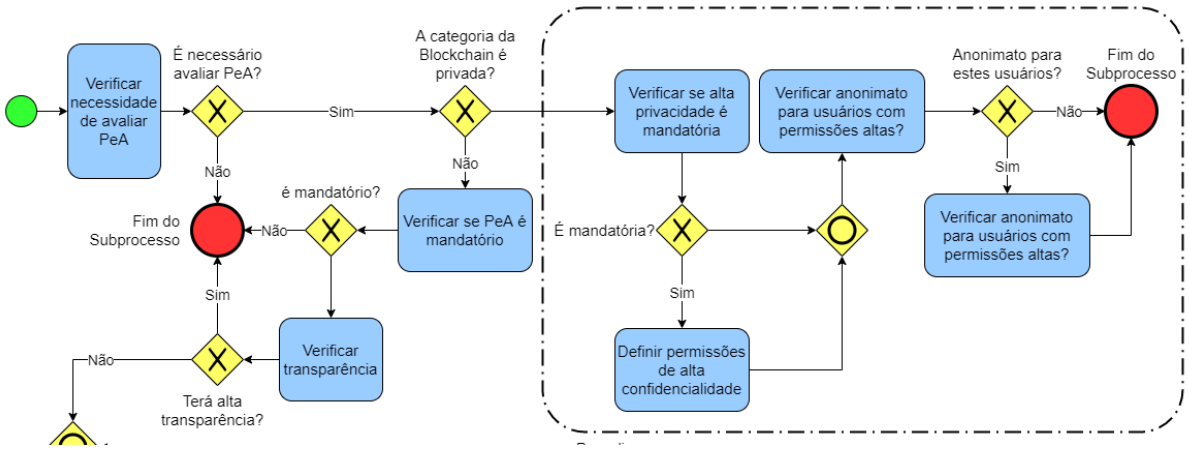


Fonte: Produzido pelo autor.

Assim como os subprocessos anteriores, primeiro é necessário que o projetista responda se há a necessidade de avaliar as configurações de privacidade e anonimato no projeto em questão. Caso não haja necessidade ou este ponto não possua relevância para o projeto, o projetista é direcionado para um evento de fim do subprocesso.

O início do subprocesso pode ser visto na Figura 16.

Figura 16 – Privacidade e Anonimato (PeA) - parte 1 de 3.



Fonte: Produzido pelo autor.

Havendo a necessidade de avaliar a Privacidade e Anonimato (PeA), o projetista precisa verificar a categoria da Blockchain, obtida no Marco 2 (dois), e responder se a categoria é privada ou não. Em uma Blockchain de categoria privada, as permissões de leitura e escrita são restritas e o nível da privacidade envolvida é mais alto que as outras categorias de Blockchains.

Neste momento, dentro do grupo de atividades para a categoria privada, as ações podem ser realizadas fixando permissões que reflitam a realidade do ambiente. Podendo ou não ter alta confidencialidade e também ocultar dados e usuários com altos privilégios.

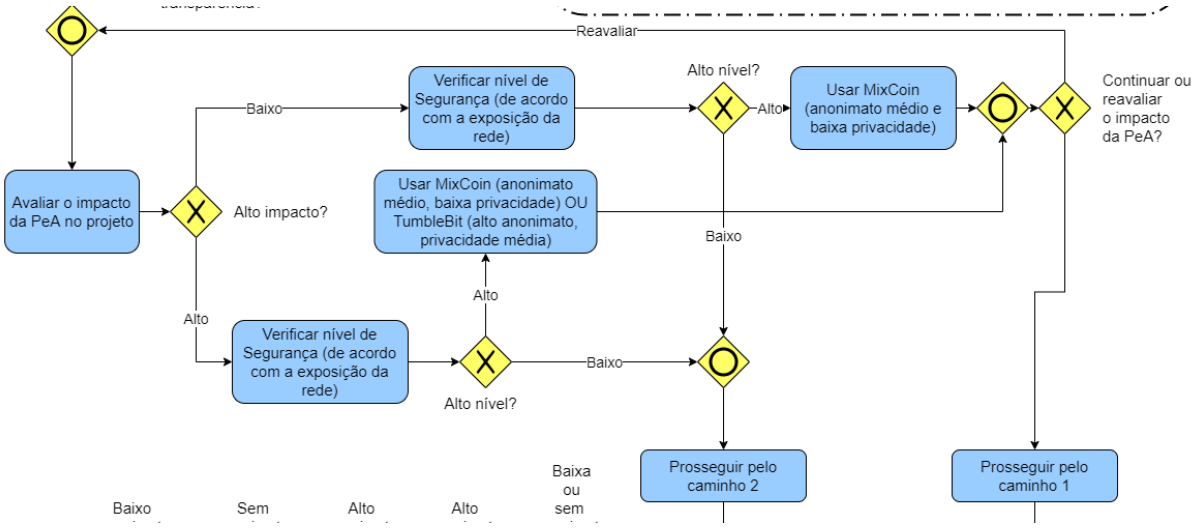
Se a categoria não for privada, o fluxo segue para a atividade Verificar se PeA é mandatório. Assim como na primeira atividade que verifica a necessidade de avaliar PeA, o projetista também precisa responder aqui se é um requisito obrigatório ao projeto, não sendo mandatório, o fluxo segue para o evento fim do subprocesso.

Se configurações avançadas de PeA for mandatório, o fluxo segue para a atividade verificar transparência da rede, quanto mais alta a transparência da rede menor é a capacidade de privacidade e anonimato. Isso se dá pela falta de alta transparência significar que todos os usuários sabem sobre os dados e usuários presentes na cadeia de blocos, não havendo necessidade de implementar protocolos avançados de PeA.

Se o projetista responder que a implementação não terá alta transparência, o mesmo é direcionado para a avaliação do impacto da PeA no projeto. Na Figura 17, é

apresentado o fragmento do subprocesso responsável pela avaliação do impacto da PeA.

Figura 17 – Privacidade e Anonimato (PeA) - parte 2 de 3.



Fonte: Produzido pelo autor.

O impacto da existência da PeA na rede pode ser de **alto impacto**, que significa ser de grande importância para o sucesso do projeto, ou **baixo impacto**, que denota não ser de extrema necessidade a presença nas transações nem nos dados dos usuários.

Neste momento é importante que o projetista conheça os protocolos mais comuns para a tarefa de implementar PeA. Abaixo segue uma lista dos protocolos que aparecem nesta versão da metodologia:

- **TumbleBit**: é um protocolo de pagamento unidirecional e não associável, compatível com o protocolo Bitcoin atual, no qual é possível fazer pagamentos rápidos, anônimos e fora da Blockchain através de um intermediário que não precisa ser confiado chamado *Tumbler* (HEILMAN et al., 2020a).
- **CryptoNote**: é um protocolo da camada de aplicação que possui o objetivo de resolver problemas descritos no **Bitcoin Core**, o protocolo por trás do Bitcoin. O protocolo é usado por várias criptomoedas descentralizadas orientadas a privacidade (HEILMAN et al., 2020b).
- **MixCoin**: é um protocolo que facilita pagamentos anônimos no Bitcoin e criptomoedas similares (BONNEAU et al., 2020).
- **CoinJoin**: é um método confiável para combinar vários pagamentos Bitcoin de vários usuários em uma única transação para tornar mais difícil para terceiros determinar qual usuário pagou qual destinatário ou destinatários. Ao contrário de

muitas outras soluções de privacidade, as transações com coinjoin não exigem uma modificação no protocolo bitcoin (MAXWELL, 2020).

- **CoinShuffle**: um protocolo completamente descentralizado que permite usuários utilizar Bitcoin em uma maneira verdadeiramente anônima. CoinShuffle é baseado em outros protocolos já presentes no Bitcoin (RUFFING; MORENO-SANCHEZ; KATE, 2014).

- **ZeroCash**: é um protocolo que fornece uma versão do Bitcoin que preserva a privacidade. Zerocash é uma melhoria do protocolo Zerocoin, desenvolvido por alguns dos mesmos autores, ambos funcionais e eficientes (BEN-SASSON et al., 2020a).

- **Zcash**: é uma moeda digital que protege a privacidade. Transaciona com eficiência e segurança com taxas baixas, garantindo que as transações digitais permaneçam privadas. Possibilita o compartilhamento seletivo das informações de endereço e transação para auditoria ou conformidade regulamentar (ZCASH, 2020).

- **Zerocoin**: um protocolo projetado como uma extensão do protocolo Bitcoin objetiva melhorar o anonimato das transações com a mistura de moedas, recurso nativamente incorporado ao protocolo (BEN-SASSON et al., 2020b).

- **BlindCoin**: é uma modificação do protocolo MixCoin, que provê garantias que os endereços de entrada e saída mapeados para qualquer usuário estão mantidos ocultos, utilizando o esquema de assinatura cega. O esquema é totalmente compatível com o Bitcoin e preserva o anonimato do usuário (VALENTA; ROWAN, 2020).

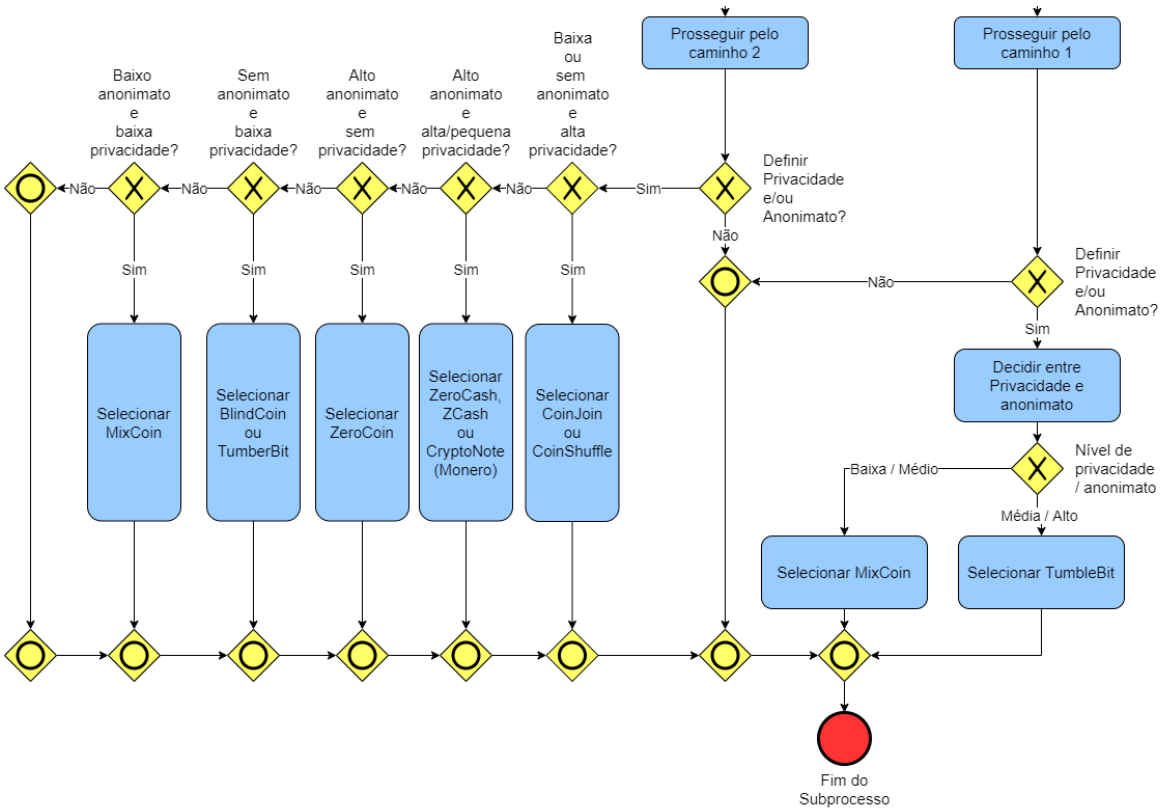
A atividade de verificar o nível de segurança servirá para indicar qual dos caminhos do processo é o melhor para o caso em questão. Este nível depende do quão exposta é a rede, redes públicas possuem um nível de exposição maior do que redes consórcio, já que as redes consórcio possuem características da categoria privada.

Antes de seguir pelo caminho 1 (um), é possível que o projetista queira reavaliar o impacto dos recursos de PeA, esta opção é possível no fluxo do subprocesso.

No caminho do alto impacto, a atividade de verificar o nível de segurança é apresentada e a resposta da mesma servirá para guiar o projetista entre os caminhos do subprocesso. Caso a resposta seja nível alto, o fluxo será direcionado para o caminho 1. Caso a resposta seja nível baixo, o fluxo será direcionado para o caminho 2 (dois).

A Figura 18, apresenta os caminhos finais do subprocesso.

Figura 18 – Privacidade e Anonimato (PeA) - parte 3 de 3.



Fonte: Produzido pelo autor.

Neste momento do subprocesso, existem dois caminhos. No caminho 1, a segurança necessária é de nível alto, neste momento o protocolo MixCoin é indicado pela metodologia para ser implementado na rede, porém o projetista ainda pode mudar caso queria dar prioridade maior ao Anonimato ou a Privacidade. Ao escolher não definir entre Privacidade e/ou Anonimato, o subprocesso chega ao evento fim.

Caso o projetista deseje balancear entre Privacidade e/ou Anonimato, são apresentadas duas opções: Privacidade média e Anonimato alto ou Privacidade baixa e Anonimato Médio. Nestas configurações os protocolos são sugeridos respectivamente TumbleBit e MixCoin e assim é alcançado o evento fim do subprocesso.

No caminho 2 (dois), o nível de segurança é baixo, e há uma série de combinações para a seleção do protocolo de PeA. Neste momento o projetista define as combinações de níveis de privacidade e anonimato, conforme segue:

- Não definir PeA: o fluxo segue para o evento fim do subprocesso.
- PeA baixa ou sem anonimato e baixa privacidade: é sugerido o uso de CoinJoin ou CoinShuffle.
- PeA de Alto anonimato e alta ou pequena privacidade: os protocolos Zcash, ZeroCash ou CryptoNote são sugeridos.

- Pea com alto anonimato e sem privacidade: Zerocoin é sugerido.
- PeA sem anonimato e baixa privacidade: BlindCoin ou TumbleBit.
- PeA de baixo anonimato e baixa privacidade: MixCoin.
- Nenhuma das opções anteriores: o fluxo segue para o evento fim do subprocesso.

Ao final do subprocesso, o projetista terá informações importantes sobre o quesito Privacidade e Anonimato, e qual das opções de protocolos ele poderá usar na implementação.

Este subprocesso do Marco 3 difere entre o apresentado por Staderini, Schiavone e Bondavalli (2018) quanto a atividade avaliação de segurança. No trabalho apresentado aqui é avaliado o quão exposta a rede será; já no trabalho de Staderini, Schiavone e Bondavalli (2018) a segurança é avaliada baseada no nível de ameaça de segurança, são maneiras diferentes para abordar as Medidas de Segurança.

Exceto o ponto de avaliação de segurança todo o subprocesso sobre Privacidade e Anonimato é compatível com o apresentado no trabalho de Staderini, Schiavone e Bondavalli (2018).

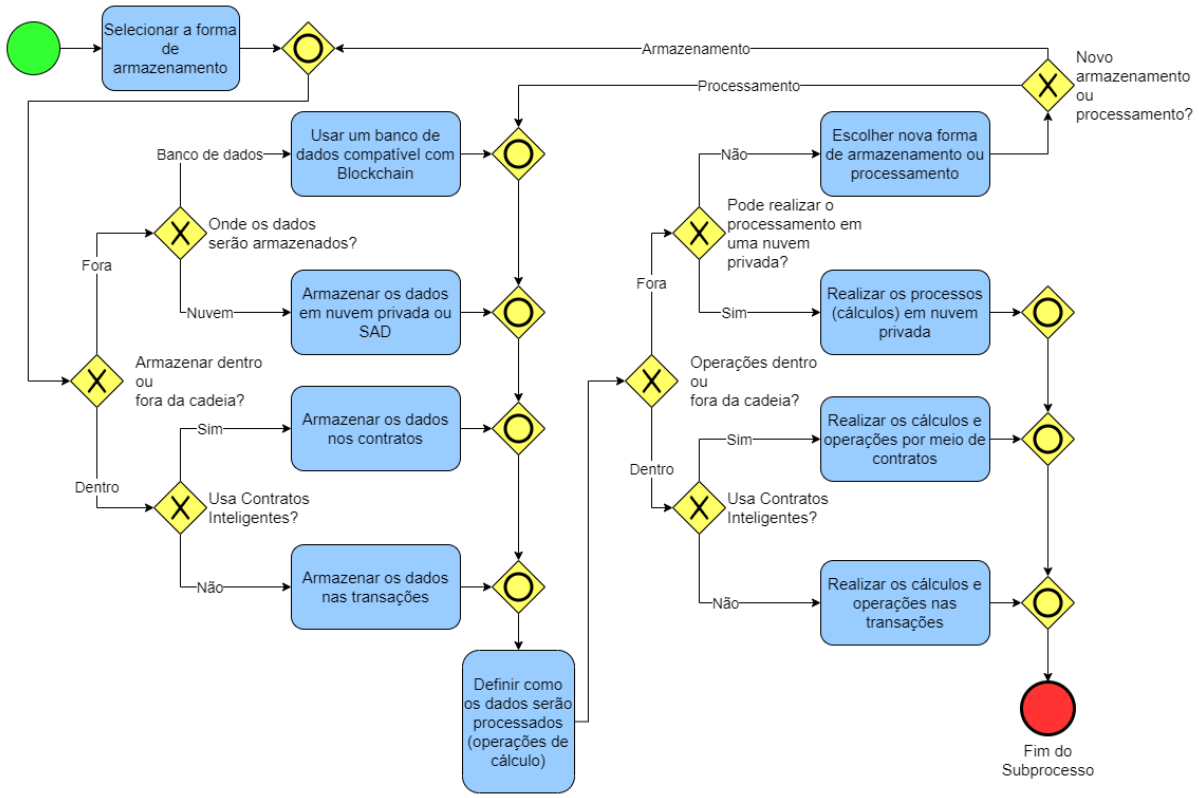
4.2.3.5 Processamento de dados e Armazenamento

Este é o último subprocesso do Marco 3 (três) e o seu papel é guiar o projetista em alcançar o melhor custo-benefício entre processamento e armazenamento de dados dentro e fora da cadeia de blocos. Isto é relevante porque o espaço disponível na cadeia para processamento e armazenamento é limitado.

Por exemplo, considere uma situação onde será preciso armazenar um arquivo grande, algo maior que 1 Gigabyte (1.000.000.000 de bytes, ou ainda 10^9 bytes). Dividir o arquivo em blocos e transações seria muito custoso, no sentido computacional; logo ao invés de armazenar em blocos na cadeia, é possível utilizar sistemas de arquivos descentralizados, como o InterPlanetary FileSystem (IPFS, 2019) ou o Decentralized Cloud Storage (STORJ, 2019). Estes sistemas de arquivos poderão armazenar o arquivo, ficando a cargo da Blockchain armazenar a referência para o arquivo que foi adicionado ao sistema de arquivos descentralizado.

Além disso, o custo de usar Blockchains públicas pode ser realmente considerável, já que a leitura de dados pode atingir uma larga escala, como em um cenário onde é necessário consultar centenas ou milhares de blocos por segundo. Dentre as características, para o processamento, é importante observar a existência de suporte a contratos inteligentes e eficiência de custo. A Figura 19 apresenta o fluxo do subprocesso.

Figura 19 – Configuração do processamento e armazenamento de dados



Fonte: Produzido pelo autor.

A primeira atividade é selecionar a forma de armazenamento. O projetista deve levar em consideração o volume de dados que será armazenado por vez. Se a natureza da aplicação exigir o armazenamento de grandes volumes de dados, armazenar os dados fora da Blockchain é o melhor a se fazer. Caso sejam registros pequenos, armazenar os dados nos blocos da rede é aceitável, assim como no caso de armazenar registros de operações ou ações em um sistema.

No cenário em que é escolhido armazenar internamente na Blockchain, o suporte a contratos inteligentes é verificado. Os contratos podem possuir coleções de dados (listas) em sua composição, ficando a cargo do processador do contrato (isso é implementado pela plataforma de blockchain usada) a gestão de armazenamento e recuperação destes dados.

Se a rede não fizer uso de contratos inteligentes, o projetista é direcionado para a atividade armazenar os dados nas transações, como é no caso de redes blockchain de implementação simples; por exemplo, o projeto NaiveChain (HARTIKKA, 2018).

No cenário em que é escolhido armazenar externamente à Blockchain, o projetista deve observar se os dados utilizados na aplicação seguem um modelo que pode ser estruturado, como com os dados utilizados em bancos de dados tradicionais. Desta forma, será possível armazenar estes dados em uma base de dados que também pos-

sua alguma interface de comunicação compatível com a Blockchain implementada.

Usar um banco de dados possui a consequência de trazer um ponto de centralização ao projeto, podendo ser algo não desejado para a finalidade da aplicação de responsabilidade do projetista.

Caso o projetista compreenda que o uso de um banco de dados não se aplica ao projeto, pode fazer uso de armazenamento em nuvem privada. Neste contexto o termo privado indica que a blockchain deve possuir acesso aos dados porém o mesmo não deve, necessariamente, estar disponível diretamente aos usuários da aplicação. Aqui existe a opção de usar alguma solução de Sistema de Arquivos Descentralizados (SAD).

O IPFS pode ser utilizado neste contexto, em redes de categoria pública, no lugar de uma solução de nuvem privada, trazendo o armazenamento descentralizado para a aplicação.

Após as atividades que envolvem o armazenamento, temos as atividades sobre o processamento. Neste momento é importante que o projetista entenda que os recursos de processamento podem, e devem, mudar com o passar do tempo. Iniciar com uma forma de processar os dados e depois muda-la para algo mais robusto, completo e complexo é esperado em qualquer aplicação que possua escalabilidade.

O projetista primeiro deve responder se o processamento será realizado dentro ou fora da Blockchain. Caso seja definido fora, a cadeia de blocos servirá para armazenar o estado e referências nas transações e o processamento poderá ser por um grupo de computadores em uma nuvem privada, assim como na atividade de armazenamento, deixando um ponto de processamento não distribuído. Se não for possível ou viável o uso de uma nuvem privada, o projetista é direcionado de volta para escolher se o processamento será dentro ou fora da Blockchain.

Ao optar por realizar o processamento dentro da blockchain, o uso de contratos inteligentes é questionado. Existindo o suporte ao uso de contratos é recomendado o uso dos mesmos para realizar o processamento dos dados.

Por definição, os contratos trazem as regras de negócios para a Blockchain. Caso não exista o suporte a contratos inteligentes, as operações deverão ser feitas pelas transações, realizando comparações e demais operações necessárias no momento de criação dos *hashes* e concepção das transações e blocos.

4.3 Considerações Finais

Ao encerrar o quinto subprocesso do marco 3, o projetista chega ao estado final da metodologia. Como resultado, o projetista deve ter sido assistido pelo processo de

tomada de decisão, estando capaz de fazer escolhas a respeito da configuração da Blockchain de acordo com os requisitos do projeto.

É importante notar que o projetista precisa ter conhecimento acerca do problema que será resolvido assim como compreender o ambiente e a relação entre organizações e indivíduos do contexto. Assim, muitas das perguntas levantadas pela metodologia poderão ser respondidas com assertividade, garantindo saídas adequadas nos subprocessos e marcos.

A seguir, o Capítulo 5 apresenta um estudo de caso, onde a metodologia é aplicada. Ao passar pelo processo da metodologia, é criado um perfil de implementação da tecnologia Blockchain, perfil esse que auxilia o projetista durante a implementação da tecnologia.

5 Estudo de Caso

Com o intuito de avaliar a metodologia proposta, este trabalho realizou um estudo de caso, onde buscou-se aplicar o processo de suporte à tomada de decisão quanto ao uso de Blockchains na área de registros públicos.

O ambiente utilizado para o estudo de caso escolhido é o serviço de cadastro e consulta de registros em cartórios, que se enquadram na definição de registros públicos e possuem a capacidade para um dia estarem disponíveis em todo o território nacional.

5.1 Sistema de Registro Eletrônico de Imóveis - SREI

O Conselho Nacional de Justiça (CNJ) fornece um sistema para o cadastro e consulta de registros em cartórios.

O Sistema de Registro Eletrônico de Imóveis (SREI) tem como objetivo facilitar o intercâmbio de informações entre os ofícios de registro de imóveis, o Poder Judiciário, a administração pública e o público em geral (CNJ, 2015).

A documentação do sistema inclui o mapeamento dos processos de trabalho adotados em vários cartórios em território nacional e este mapeamento é disponibilizado por Unger et al. (2011). Este mapeamento é apresentado na seção 5.1.1.

5.1.1 Visão Geral do Processo dos Cartórios

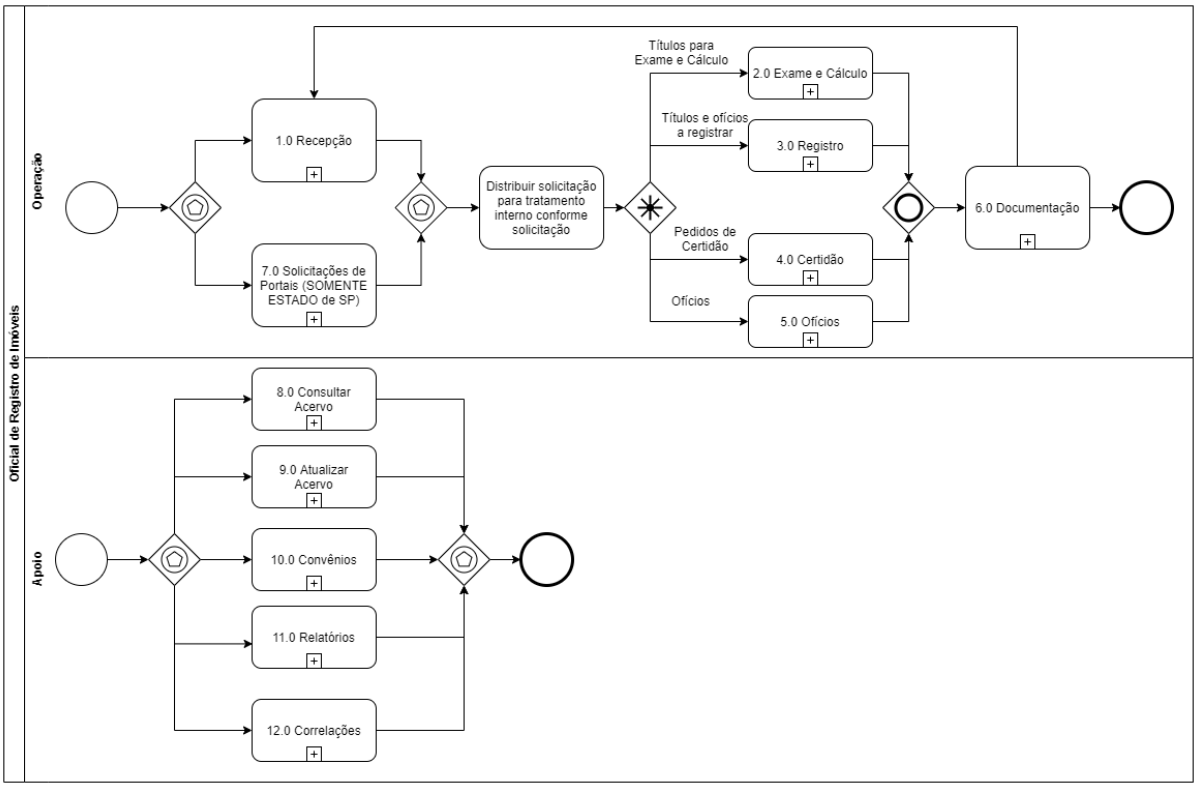
O diagrama que apresenta as principais atividades realizadas por cartórios está apresentado na Figura 20.

Os cartórios possuem dois tipos de processos iniciais de operação:

- Atendimento presencial na recepção;
- Atendimento de solicitações provenientes de portais eletrônicos.

Os processos tanto no atendimento presencial da recepção quanto no atendimento de solicitações provenientes dos portais possuem a mesma finalidade, que é o encaminhamento da solicitação para o tratamento em um dos seguintes processos: Exame e Cálculo, Registro, Certidão ou Ofícios (UNGER et al., 2011).

Figura 20 – Visão geral da modelagem do processo atual dos Cartórios Brasileiros.



Fonte: Unger et al. (2011).

5.2 Aplicação da Metodologia Proposta

Com o conhecimento da visão geral das atividades desenvolvidas por cartórios e serviços oferecidos pelos mesmos, é possível aplicar a metodologia proposta no processo atual dos Cartórios Brasileiros.

5.2.1 Analisar os Requisitos do Projeto

Seguindo o fluxo de atividades apresentadas para o marco 1 da metodologia, será preciso responder perguntas sobre o objetivo do sistema que será construído e o ambiente em que o mesmo será usado.

Assim sendo, as atividades são seguidas de perguntas que o projetista deve responder para que a metodologia possa indicar se a tecnologia Blockchain é indicada como solução.

A seguir serão descritas as perguntas e respostas.

- **Precisa armazenar dados ou estado da aplicação?** Sim, cartórios armazenam dados em diversos formados de documentos. Por exemplo: certidões de nasci-

mento, certidões de óbito, registro de imóveis, reconhecimento de assinaturas. Cada documento possui sua própria estrutura.

- **Imutabilidade e/ou integridade dos dados são necessárias?** Sim, os dados fornecidos por cartórios precisam ser íntegros e imutáveis, no sentido de não podem ser alterados sem o consentimento das partes envolvidas.

Nesse ponto a metodologia indica o uso da tecnologia Blockchain. O marco 1 é finalizado e fica a cargo do projetista continuar para o marco 2, Definir a Categoria da Blockchain.

Se a resposta para a pergunta sobre imutabilidade fosse não, o projetista teria que responder as seguintes outras perguntas:

- **Existirão múltiplos escritores nos registros?** Sim, a ideia de disponibilizar um sistema único para todos os cartórios em âmbito nacional deve prever que vários cartórios agirão como nós na rede e realizarão a mineração dos blocos.
- **Existe TTP e ela está sempre online?** Não, uma terceira parte seria uma entidade validadora do trabalho dos cartórios. O CNJ serve em parte para isso, mas cada cartório possui um certo nível de independência.
- **Escritores são conhecidos e confiáveis?** Não, pois é desejável que um sistema de registros de cartórios possua a característica de não repúdio por parte dos nós da rede.

Ao final deste marco, a metodologia retorna com a saída “Tecnologia Blockchain é Recomendada”.

5.2.2 Definir a Categoria da Blockchain

O projetista precisa definir a categoria da blockchain que será utilizada, saber isso facilitará a adoção de alguma plataforma que implementa a tecnologia, além de trazer a compreensão da escolha da plataforma.

As perguntas deste marco são:

- **Há política de mineração definida?** Sim, os nós poderão criar blocos (minerar) e a inclusão de novos nós pode ser decidida pelo CNJ, que é hoje quem toma essa decisão e fornece o atual sistema dos cartórios.
- **Há regras para leitura e criação?** Sim, cada cartório pode ser representado por um nó na rede e cada nó na rede ter o poder de criar blocos e consultar dados na rede. Isso é representado na metodologia como ler e criar de forma aberta.

- **Ler e criar estão em consórcio?** Não, todos os nós no caso proposto poderão ler e criar.
- **Ler e criar de forma aberta?** Sim, cada nó é a representação de um cartório e todos os cartórios possuem os mesmos privilégios.
- **A mineração será aberta?** Não, todos os nós são vistos como iguais na rede, porém a entrada de novos nós deverá ser controlada pelo CNJ.

Ao final deste marco a metodologia retorna com a saída “Blockchain Pública Permissionária”.

Com este resultado em mãos o projetista pode decidir a implementação de Blockchain adequada à finalidade do projeto.

O próximo marco, avaliar configurações avançadas, apresenta configurações técnicas para a implementação da Blockchain.

5.2.3 Avaliar configurações avançadas

Neste momento, o projetista possui os resultados dos marcos anteriores. Estes resultados fornecem uma visão de implementação para a Blockchain. Este é o momento para analisar mais detalhes das possibilidades com a tecnologia e traçar um perfil completo da implementação.

As perguntas deste marco estão divididas pelos subprocessos apresentados pela metodologia. Todos os subprocessos neste marco são opcionais. O projetista pode no início de todos os subprocesso optar por não avaliar a configuração proposta pelo subprocesso.

Algoritmos de Consenso: neste momento o projetista responderá perguntas sobre como deve ser o processo de consenso para o registro de blocos na rede.

As perguntas deste subprocesso são:

- **Necessita avaliar algoritmo?** Sim, com o intuito de criar uma rede para os cartórios em todo o território nacional, é importante que o algoritmo de consenso seja adequado ao cenário.
- **A avaliação das transações deve ser probabilística?** Não, os cartórios já passam por um crivo do CNJ. Então, é de se esperar que a cada registro de transação a mesma seja considerada imediatamente.
- **A vazão é um critério importante?** Não, seria se o caso fosse, por exemplo, o fornecimento de recursos financeiros, como o caso de uma criptomoeda ou operadora de cartão de crédito.

- **É esperada uma quantidade de nós maior que 20?** Sim, no caso será uma rede de abrangência nacional, independentemente da localização geográfica do cartório.

O subprocesso indica a atividade de “Selecionar algoritmos para alto número de nós”. Dentro da lista de algoritmos temos XFT, Optimistic BFT, PBFT, Hybrid BFT, Randomized BFT e Scalable BFT, conforme é apresentado pela metodologia.

Contratos Inteligentes: a implementação de contrato inteligente (smart contract) é totalmente consequência da escolha do algoritmo de consenso utilizado pela rede.

No caso apresentado, ao utilizar um algoritmo da família BFT é possível utilizar smart contracts, escritos em diversas linguagens de programação, pois o algoritmo suporte a inclusão de lógica na rede.

Medidas de Segurança: este subprocesso, diferente dos outros, é cíclico. A cada entrada de um novo nó a medição deve ser realizada novamente. A avaliação depende da exposição da rede, pois quanto maior é a exposição maior são as possibilidades de ataques e ameaças surgirem. Em uma rede como a do Bitcoin, onde novos nós podem entrar sem a aceitação de uma organização ou entidade, há mais riscos de segurança.

No caso apresentado, uma rede de cartórios que estão utilizando um sistema fornecido pelo CNJ, não há vários dos riscos que uma rede pública sem permissão possui.

As avaliações de ameaças podem ser puladas nesse momento para este caso.

A avaliação de defeitos em contratos inteligentes é feita por meio de ferramentas como Oyente e Town Crier.

O objetivo desse subprocesso é fornecer um caminho para que os projetistas possam compreender que há ameaças de segurança e que as mesmas precisam de analise frequênte e periódica.

Privacidade e Anonimato: em uma rede formada por cartórios onde os mesmos assinam os registros e disponibilizam para que outros cartórios na rede possam consultar, é possível encarar como uma implementação de alta transparência.

Diferente de uma implementação de categoria privada, onde o projetista teria que responder questões como garantir anonimato para usuários com muitos privilégios na rede e a utilizações de protocolos de anonimato e privacidade, o caso da rede de cartórios não demanda esse tipo de recurso.

Ao existir uma criptomoeda na rede, essa configuração se torna muito impor-

tante para garantir a segurança de quem possui um bem financeiro no livro razão, o que não é o caso proposto.

Processamento de dados e Armazenamento: ao receber um documento para registro, como o cadastro de uma assinatura (reconhecimento de firma), é necessário armazenar a assinatura cursiva de forma virtual e assim garantir a integridade da mesma.

Segundo Unger et al. (2011), digitalização e arquivamento são atividades comuns em cartórios, logo o armazenamento de dados é algo importante em um sistema para cartórios.

O subprocesso apresenta as seguintes perguntas:

- **O armazenamento será dentro ou fora da cadeia de blocos?** Fora, pois não existe limite para a quantidade de páginas ou itens que um serviço de cartório pode precisar digitalizar e arquivar. Logo, a utilização de armazenamento dentro dos blocos da rede não é uma opção interessante.
- **Onde os dados serão armazenados?** O ideal é armazenar em uma nuvem privada, ou em um sistema de arquivos descentralizado (SAD). No caso de uma nuvem de armazenamento, a mesma deve possuir mecanismos de garantia de integridade própria.
- **Operações de cálculo serão efetuadas dentro ou fora da cadeia?** Dentro da cadeia, o cálculo dos hashes e endereçamento podem ser realizados por meio da Blockchain.
- **Usa contratos Inteligentes?** Sim, ao utilizar algum algoritmo da família BFT o suporte a contratos inteligentes é garantido.

A metodologia indica como armazenar de dados (artefatos) e como realizar o processamento em que eles estarão envolvidos.

5.3 Resultados e Discussão

Esta seção visa ressaltar os principais resultados obtidos com a aplicação da metodologia proposta aplicada ao caso de criação de uma rede de cartórios.

É importante compreender que a metodologia proposta é uma ferramenta de auxilio e serve como um guia para o projetista, apresentando opções ao uso da Blockchain, categorizando e indicando configurações avançadas para a mesma.

Através da aplicação desta metodologia ao cenário estudado, buscou-se verificar a sua adequabilidade ao contexto de projetos de registros públicos, de forma a

ser aplicável em contextos diversos como organizações públicas ou privadas, considerando as propriedades inerentes a este paradigma.

Nos dois primeiros marcos da metodologia é possível notar que um caminho para a resposta é facilmente encontrado se houver conhecimento suficiente sobre o objetivo e contexto do projeto em questão.

O terceiro marco depende do conhecimento do projetista. A avaliação de configurações avançadas exige um certo grau de conhecimento em protocolos, comunicação e segurança em ambientes blockchain. Os subprocessos que compõem o terceiro marco são opcionais, ficando a cargo do projetista a utilização ou não dele.

Um resumo das saídas da metodologia é apresentado a seguir:

- **Analisar os Requisitos do Projeto**: Tecnologia Blockchain é Recomendada.
- **Definir a Categoria da Blockchain**: Blockchain Pública Permissionária.
- **Avaliar configurações avançadas**
  - **Algoritmos de Consenso**: XFT, família BFT, Optimistic, PBFT, Hybrid, Randomized e Scalable.
  - **Contratos Inteligentes**: compatível com a família BFT.
  - **Medidas de Segurança**: ameaças externas são de baixo nível, é recomendado o uso de ferramentas para avaliação de defeitos em contratos inteligentes.
  - **Privacidade e Anonimato**: não é mandatório.
  - **Processamento de dados e Armazenamento**: a utilização de Nuvem privada ou Sistema de Arquivos Descentralizado é uma recomendação, os contratos inteligentes podem ser responsáveis por mapear os arquivos armazenados e demais cálculos necessários.

Com estes resultados, o projetista pode realizar a implementação da Blockchain de forma a garantir que a tecnologia será utilizada de forma adequada às necessidades do projeto.

Em suma, este estudo de caso demonstra que a metodologia proposta cumpre com seus objetivos. Ou seja, serve como ferramenta para facilitar a adoção e implementação da tecnologia Blockchain em aplicações que utilizam registros públicos.

6 Conclusão e Trabalhos Futuros

6.1 Conclusões

Este trabalho objetivou a proposta de uma metodologia para auxiliar na tomada de decisão quanto ao uso de Blockchain na área de registros públicos. Esta metodologia apresentou um conjunto de atividades que percorrem o ciclo de tomada de decisão necessário para a escolha da tecnologia, assim como recursos avançados possíveis com a adoção da mesma.

O processo da metodologia é representado utilizando a notação *Bussiness Process Management Notation* (BPMN), dividido em 3 (três) marcos.

O primeiro marco é composto por atividades que ajudam o projetista de sistemas a saber se a tecnologia é adequada ao propósito desejado, levando em consideração o ambiente em que o problema será tratado.

O segundo marco busca definir qual a categoria da Blockchain que será implementada, já que a tecnologia é flexível de tal forma que categorizar é um passo importante no processo de implementação. De acordo com o comportamento dos membros da rede para as operações de leitura e escrita de blocos a categoria pode ser definida.

O terceiro marco do processo apresenta opções de configurações avançadas para a implementação da Blockchain. Neste marco, o projetista é apresentado a conceitos técnicos de implementação, desde a possibilidade de adicionar lógica de negócio na rede até a inclusão de uma criptomoeda para retribuir o processamento de indivíduos participantes.

Como exemplo de aplicação da metodologia é apresentado um estudo de caso utilizando serviços oferecidos por cartórios, em âmbito nacional. O Conselho Nacional de Justiça (CNJ), atualmente, fornece um sistema para cartórios e a possível implementação de Blockchain para este sistema foi ilustrada com a metodologia proposta neste trabalho.

Ao seguir a metodologia foi possível traçar um perfil de implementação para o caso dos cartórios nacionais. O perfil resultante mostra que a metodologia cumpre o objetivo para o qual foi criada, ainda havendo a possibilidade de ser utilizada em diversos cenários de organizações públicas e/ou privadas.

Com isso, é esperado que este trabalho seja utilizado como um método para facilitar a adoção em maior escala da tecnologia Blockchain e aplicações descentralizadas. A área de registros públicos foi escolhida como foco do trabalho devido as

necessidades reportadas pelas organizações tecnológicas do governo federal, porém, nada impede que o presente trabalho possa ser utilizado em áreas distintas.

6.2 Trabalhos Futuros

Como trabalhos futuros, espera-se que a metodologia seja aprimorada com mais estudos de casos e atinja um nível de maturação e aceitação por parte da comunidade de projetistas de sistemas descentralizados.

Há limitações na metodologia, como o fato de o projetista precisar compreender as partes avançadas da tecnologia para poder tirar real proveito das configurações avançadas. Tais configurações não são possíveis de serem analisadas sem a experiência do projetista.

Facilitar o entendimento e planejamento das configurações avançadas também é uma proposta interessante como continuação deste trabalho. Tornar natural o processo de escolha das configurações avançadas trará maturidade tanto para a tecnologia quanto para a metodologia apresentada.

A possibilidade de utilizar a metodologia de forma reversa também é uma opção interessante. Sistemas que atualmente funcionam sobre a Blockchain poderão utilizar a metodologia como forma de avaliar e validar as decisões anteriormente tomadas e com isso melhorar implementações futuras.

Avaliar o impacto de desempenho e financeiro no uso da tecnologia Blockchain, no contexto de sistemas de registros públicos, contribui para a evolução do estado da arte. Um método para mensurar desempenho, custos, riscos e ganhos (financeiros) trará mais segurança e maturidade aos que utilizam ou planejam utilizar a tecnologia.

Referências

ACM. *ACM Digital Library*. 2020. <https://dl.acm.org/>. Acesso em 30 Dez. 2020. Citado na página 23.

AMARO, G. Criptografia simétrica e criptografia de chaves públicas: vantagens e desvantagens. *Revista Negócios e Tecnologia da Informação, Volume 2 n1*, 1 2007. Citado na página 16.

BALIGA, A. Understanding blockchain consensus models. In: . [S.l.: s.n.], 2017. Citado na página 39.

BEN-SASSON, E. et al. *ZeroCash*. 2020. <http://zerocash-project.org/>. Acesso em 30 Dez. 2020. Citado na página 48.

BEN-SASSON, E. et al. *Zerocoin*. 2020. <http://zerocoin.org/>. Acesso em 30 Dez. 2020. Citado na página 48.

BONNEAU, J. et al. *Mixcoin - Anonymity for Bitcoin with accountable mixes*. 2020. <https://eprint.iacr.org/2014/077.pdf>. Acesso em 30 Dez. 2020. Citado na página 47.

BRASIL. *Lei Nº 6.015, DE 31 DE DEZEMBRO DE 1973.* 1973. <http://www.planalto.gov.br/ccivil_03/leis/L6015compilada.htm>. Acesso em 17 Mar. 2020. Citado na página 15.

BRASIL. *Art. 236 - Título IX. Das Disposições Constitucionais Gerais*. 2017. <https://www.senado.leg.br/atividade/const/con1988/con1988_14.12.2017/art_236_.asp>. Acesso em 17 Mar. 2020. Citado na página 15.

CACHIN, C.; VUKOLIC, M. Blockchain consensus protocols in the wild. *CoRR*, abs/1707.01873, 2017. Disponível em: <http://arxiv.org/abs/1707.01873>. Citado na página 40.

CARAMéS, T. M. F.; LAMAS, P. F. Uma revisão sobre o uso de blockchain para a internet das coisas. *IEEE Access*, v. 6, p. 32979 – 33001, 5 2018. DOI: 10.1109/ACCESS.2018.2842685. Citado na página 23.

CNJ. *Sistema de Registro Eletrônico de Imóveis (SREI)*. 2015. <https://www.cnj.jus.br/sistemas/srei/>. Acesso em 24 Nov. 2020. Citado na página 54.

COINBR. *Guia Básico sobre o Etherum*. 2020. <https://www.coinpy.net/assets/docs/eth-guide-pt.pdf>. Acesso em 21 Mar. 2020. Citado na página 22.

COULOURIS, G. et al. *Sistemas Distribuídos: Conceitos e Projeto*. 5. ed. [S.l.]: Bookman Editora Ltda, 2013. ISBN 978-85-8260-054-2. Citado 2 vezes nas páginas 12 e 13.

FERREIRA, E. et al. Uso de blockchain para privacidade e segurança em internet das coisas. In: ____. [S.l.: s.n.], 2017. p. 51. ISBN 9788576694106. Citado 3 vezes nas páginas 17, 19 e 20.

HARTIKKA, L. *Naivechain - a blockchain implementation in 200 lines of code*. 2018. <https://github.com/lhartikk/naivechain>. Acesso em 22 Mar. 2020. Citado na página 51.

HEILMAN, E. et al. *TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub*. 2020. <https://cs-people.bu.edu/heilman/tumblebit/>. Acesso em 30 Dez. 2020. Citado na página 47.

HEILMAN, E. et al. *TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub*. 2020. <https://cryptonote.org/>. Acesso em 30 Dez. 2020. Citado na página 47.

HYPERLEDGER. *About Hyperledger*. 2020. <https://www.hyperledger.org/about>. Acesso em 21 Mar. 2020. Citado na página 22.

IBBA, S. et al. Citysense: blockchain-oriented smart cities. In: . [S.l.: s.n.], 2017. p. 1–5. Citado na página 24.

IPFS. *InterPlanetary File System*. 2019. <https://ipfs.io>. Acesso em 21 Set. 2019. Citado na página 50.

JUNIOR, E. O. *Blockchain e Aplicações Descentralizadas*. 2017. <http://irib.org.br/files/palestra/blockchain-02.pdf>. Acesso em 03 Jun. 2019. Citado 3 vezes nas páginas 11, 17 e 18.

LI, X. et al. A survey on the security of blockchain systems. *Future Generation Computer Systems*, 08 2017. Citado na página 43.

LIMA, M. T. da S. *Como utilizar a tecnologia blockchain no governo?* 2017. <https://www.serpro.gov.br/menu/noticias/noticias-2017/como-utilizar-a-tecnologia-blockchain-no-governo>. Acesso em 16 Nov. 2020. Citado 2 vezes nas páginas 11 e 12.

MARQUES, T. V. *Criptografia: Uma abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula*. Dissertação (Mestrado) — Universidade Federal da Paraíba, João Pessoa, 4 2013. Citado na página 15.

MAXWELL, G. *CoinJoin: Bitcoin privacy for the real world*. 2020. <https://bitcointalk.org/?topic=279249>. Acesso em 30 Dez. 2020. Citado na página 48.

Melon Project. *Oyente - An Analysis Tool for Smart Contracts*. 2016. <https://github.com/melonproject/oyente>. Acesso em 21 Set. 2019. Citado na página 43.

MORGANTI, G.; SCHIAVONE, E.; BONDAVALLI, A. Risk assessment of blockchain technology. In: . [S.l.: s.n.], 2018. p. 87–96. Citado 3 vezes nas páginas 24, 41 e 42.

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. <https://bitcoin.org/bitcoin.pdf>. Acesso em Janeiro 2019. Citado 7 vezes nas páginas 11, 12, 13, 17, 18, 20 e 39.

NARAYANAN, A. et al. *Bitcoin and Cryptocurrency Technologies – A Comprehensive Introduction*. 1. ed. [S.l.]: Princeton University Press, 2016. ISBN 978-0691171692. Citado na página 16.

NASCIMENTO, A. L. *História do Registro Civil*. 2019. <http://www.arpensp.org.br/?pG=X19wYWdpbmFz&idPagina=176>. Acesso em 12 Mai. 2019. Citado na página 15.

OMG. *Business Process Model and Notation (BPMN)*. 2013. <https://www.omg.org/spec/BPMN/2.0.2/PDF>. Acesso em 12 Mai. 2019. Citado na página 27.

PAHL, C.; IOINI, N. E.; HELMER, S. A decision framework for blockchain platforms for iot and edge computing. *3rd International Confernce on Internet of Things, Big Data and Security*, 3 2018. DOI: 10.5220/0006688601050113. Citado na página 23.

PROOF. *Entenda blockchain em menos de 15 minutos*. 2019. <https://www.proof.com.br/blog/blockchain/>. Acesso em 9 Set. 2019. Citado na página 19.

RAVAL, S. *Decentralizaed Applications: Harnessing Bitcoin's Blockchain Technology*. 1. ed. [S.l.]: O'Reilly Media., 2016. ISBN 978-1-491-92454-9. Citado 3 vezes nas páginas 11, 12 e 20.

REBELLO, G. A. F. et al. *Correntes de Blocos: Algoritmos de Consenso e Implementação na Plataforma Hyperledger Fabric*. 2019. <https://www.gta.ufrj.br/ftp/gta/TechReports/RCS19c.pdf>. Acesso em 18 Jan. 2021. Citado na página 39.

RUFFING, T.; MORENO-SANCHEZ, P.; KATE, A. Coinshuffle: Practical decentralized coin mixing for bitcoin. In: . [S.l.: s.n.], 2014. v. 8713. ISBN 978-3-319-11211-4. Citado na página 48.

SOLIDITY. *Solidity documentation page*. 2020. <https://solidity.readthedocs.io/>. Acesso em 21 Mar. 2020. Citado na página 22.

SPRINGER. *SPRINGER Link*. 2020. <https://link.springer.com/>. Acesso em 30 Dez. 2020. Citado na página 23.

STADERINI, M.; SCHIAVONE, E.; BONDAVALLI, A. A requirements-driven methodology for the proper selection and configuration of blockchains. In: . [S.l.: s.n.], 2018. p. 201–206. Citado 9 vezes nas páginas 25, 28, 31, 33, 36, 39, 41, 44 e 50.

STALLINGS, W. *Criptografia e Segurança de Redes: Princípios e Práticas*. 6. ed. [S.l.]: Pearson Education do Brasil., 2014. ISBN 978-85-430-1450-0. Citado 4 vezes nas páginas 12, 16, 17 e 30.

STORJ. *Decentralized Cloud Storage*. 2019. <https://storj.io/>. Acesso em 21 Set. 2019. Citado na página 50.

SWAN, M. *Blockchain: Blueprint for a new Economy*. 1. ed. [S.l.]: O'Reilly Media., 2016. ISBN 978-1-491-92049-7. Citado 3 vezes nas páginas 11, 12 e 13.

TANENBAUM, A. S.; STEEN, M. V. *Distributed Systems: Principles and Paradigms*. 2. ed. [S.l.]: Pearson Education Inc., 2006. ISBN 0-13-239227-5. Citado na página 11.

The Linux Foundation. *Linux Foundation Unites Industry Leaders to Advance Blockchain Technology*. 2015. <https://www.linuxfoundation.org/press-release/2015/12/linux-foundation-unites-industry-leaders-to-advance-blockchain-technology/>. Acesso em 21 Mar. 2020. Citado na página 22.

Truffle Suite. *Truffle Suite - Sweet Tools for Smart Contracts*. 2020. <https://truffleframework.com/>. Acesso em 21 Mar. 2020. Citado na página 22.

TSE. *Código Eleitoral - Lei nº 4.737, de 15 de julho de 1965*. 1965. <http://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965>. Acesso em 17 Mar. 2020. Citado na página 15.

UNGER, A. et al. *Sistema de Registro Eletrônico de Imóveis (SREI) - A1 Modelagem do processo atual*. 2011. <https://folivm.files.wordpress.com/2011/04/srei_p5a1_modelagemdoprocessoatual_v1-1-r-2.pdf>. Acesso em 24 Nov. 2020. Citado 3 vezes nas páginas 54, 55 e 59.

VALENTA, L.; ROWAN, B. *Blindcoin - Blinded, Accountable Mixes for Bitcoin*. 2020. <https://fc15.ifca.ai/preproceedings/bitcoin/paper_3.pdf>. Acesso em 30 Dez. 2020. Citado na página 48.

VUKOLIć, M. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: . [S.l.: s.n.], 2016. p. 112–125. ISBN 978-3-319-39027-7. Citado 2 vezes nas páginas 39 e 40.

WANG, H.; CHEN, K. H.; XU, D. A maturity model for blockchain adoption. *Financial Innovation*, v. 2, p. 1–5, 2016. Citado na página 24.

WüST, K.; GERVAIS, A. Do you need a blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 6 2018. DOI: 10.1109/CVCBT.2018.00011. Citado 6 vezes nas páginas 23, 28, 29, 31, 32 e 33.

XPLORER, I. *IEEE Xplorer*. 2020. <https://ieeexplore.ieee.org/>. Acesso em 30 Dez. 2020. Citado na página 23.

XU, X. et al. A taxonomy of blockchain-based systems for architecture design. In: . [S.l.: s.n.], 2017. Citado 2 vezes nas páginas 24 e 28.

ZCASH. *Zcash*. 2020. <https://z.cash/pt/technology/>. Acesso em 30 Dez. 2020. Citado na página 48.