ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO

GERALDO JOSE DOLCE UZUM MARTINS

**Avaliação do blockchain aplicado no processo de compras de uma
organização**

São Paulo

2019

GERALDO JOSÉ DOLCE UZUM MARTINS

**Avaliação do blockchain aplicado no processo de compras de uma
organização**

Dissertação apresentada ao Departamento de Engenharia de Produção da Escola Politécnica da Universidade de São Paulo para a obtenção do título de mestre em Ciências.

Orientador: Prof. Dr. Rodrigo Franco Gonçalves.

São Paulo

2019

Autorizo a reprodução e divulgação total ou parcial deste trabalho, por qualquer meio convencional ou eletrônico, para fins de estudo e pesquisa, desde que citada a fonte.

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 19 de abril de 2019

Assinatura do autor: _____

Assinatura do orientador: _____

Martins, Geraldo José Dolce Uzum

Avaliação do blockchain aplicado no processo de compras de uma organização / G. J. D. U. Martins -- versão corr. -- São Paulo, 2019.

84 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Produção.

1.BLOCKCHAIN 2.COMPRA E VENDA 3.TECNOLOGIA DA INFORMAÇÃO I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Produção II.t.

MARTINS, Geraldo Jose Dolce Uzum. **Avaliação do blockchain aplicado no processo de compras de uma organização**. 2019. 84f. Dissertação (Mestrado em Engenharia de Produção) – Departamento de Engenharia de Produção, Escola Politécnica da Universidade de São Paulo, São Paulo, 2019.

Aprovado em:

Banca Examinadora

Prof. Dr. _____

Instituição: _____

Julgamento: _____

Prof. Dr. _____

Instituição: _____

Julgamento: _____

Prof. Dr. _____

Instituição: _____

Julgamento _____

RESUMO

MARTINS, Geraldo Jose Dolce Uzum. **Avaliação do blockchain aplicado no processo de compras de uma organização**. 2019. 84f. Dissertação (Mestrado em Engenharia de Produção) – Departamento de Engenharia de Produção, Escola Politécnica da Universidade de São Paulo, São Paulo, 2019.

O trabalho tem como objetivo realizar uma prova de conceito que reproduza a rotina de compras entre empresas com a utilização da tecnologia blockchain. A prova de conceito será executada por meio da construção de dois artefatos. O primeiro artefato foi a modelagem e simulação dos processos de compras na sua forma tradicional (*As-Is*) e com o uso blockchain (*To-Be*) expandido para transação máquina a máquina (M2M). O segundo artefato foi a implantação de um contrato inteligente no blockchain público do *Ethereum*, que retratou o processo *To-Be*. Foi sugerida a proposição de que uma base de dados distribuída como o blockchain tenha um desempenho operacional superior ao de uma base de dados tradicional. Para tanto, comparou-se os custos transacionais de duas variáveis obtidas como resultados da simulação: tempos de execução da tarefa de geração de pedidos e número de postos de atendimentos necessários. Pode-se comprovar o desempenho superior do blockchain, mas dependente da arquitetura selecionada. No presente estudo, o blockchain privado com prova de trabalho ajustada para descobrir o *hash* iniciado com dois zeros consecutivos teve o melhor desempenho.

Palavras-chave: Blockchain. Processo de compra; Sistemas de informação.

ABSTRACT

MARTINS, Geraldo Jose Dolce Uzum. **Evaluation of the blockchain technology applied in the purchasing process of an organization.** 2019. 84f. Dissertation (Master in Production Engineering) – Department of Production Engineering, Escola Politécnica of the University of the University of São Paulo, São Paulo, 2019.

The aim of this work is to build two artifacts as a proof of concept of a procurement management that makes use of blockchain technology in order to demonstrate its feasibility. The first artifact was the modeling and simulation of a traditional (*As-Is*) purchasing process and other with the use of expanded blockchain (*To-Be*) for machine-to-machine (M2M) transactions. The second artifact was the implementation of a smart contract in the public blockchain of Ethereum, which portrayed the *To-Be* process. It was suggested that a distributed system of registries presents a more efficient operational performance than the conventional one. The output of the simulations was used to compare the transactional costs of each model measured through two variables: the execution time of placing orders and the number of service stations required. It could be verified that the blockchain alternative had a superior performance according to the type of architecture employed. In this present study, the private blockchain with proof of work adjusted to seek hashes that begins with two consecutive zeros had the best achievement.

Keywords: Blockchain. Purchasing process. Information systems.

LISTA DE FIGURAS

Figura 1 – Fluxo do processo de compras entre duas organizações.....	14
Figura 2 – Estrutura da dissertação	15
Figura 3 – Estrutura da cadeia de blocos.....	23
Figura 4 – Processo de compras <i>As-Is</i>	37
Figura 5 – Processo de compras <i>To-Be</i>	37
Figura 6 – Modelo gráfico da simulação no AnyLogic.....	39
Figura 7 – Blocos Source, Queue, Delay e Sink	39
Figura 8 – Parâmetros utilizados na simulação.....	40
Figura 9 – Dados do pedido de compra	45
Figura 10 – Gráfico com distribuição acumulada ajustada do blockchain público	46
Figura 11 – Gráfico com distribuição acumulada ajustada – privado – <i>hash</i> com dois zeros.....	47
Figura 12 – Gráfico com distribuição acumulada ajustada – privado – <i>hash</i> com três zeros	47
Figura 13 – Configuração de propriedades do Gerar_Pedido.....	48
Figura 14 – Histograma de quant. produzida no processo <i>As-Is</i>	51
Figura 15 – Histograma de quant. produzida no processo <i>To-Be</i> (privado – <i>hash</i> com 2 zeros iniciais)	51
Figura 16 – Histograma de quant. produzida no processo <i>To-Be</i> (público)	51
Figura 17 – Histograma de quant. produzida no processo <i>To-Be</i> (privado – <i>hash</i> com 3 zeros iniciais)	51
Figura 18 – Histograma de fila média no sistema no processo <i>As-Is</i>	51
Figura 19 – Histograma de fila média no sistema no processo <i>To-Be</i> (privado – <i>hash</i> com 2 zeros iniciais)	51
Figura 20 – Histograma de fila média no sistema no processo <i>To-Be</i> (público)	51
Figura 21 – Histograma de fila média no sistema no processo <i>To-Be</i> (privado – <i>hash</i> com 3 zeros iniciais	51
Figura 22 – Hist. de tempo de espera no sistema no processo <i>As-Is</i>	52
Figura 23 – Hist. de tempo de espera no sistema no processo <i>To-Be</i> (privado – <i>hash</i> com 2 zeros iniciais)	52
Figura 24 – Hist. de tempo de espera no sistema no processo <i>To-Be</i> (público)	52
Figura 25 – Hist. de tempo de espera no sistema no processo <i>To-Be</i> (privado – <i>hash</i> com 3 zeros iniciais)	52
Figura 26 – Metamask aberto na página do Remix	55
Figura 27 – Contrato em atividade no Remix.....	56
Figura 28 – Fluxograma do pseudocódigo do processo	57

LISTA DE TABELAS

Tabela 1 - Roteiro de condução do <i>Design-Science Research</i>	33
Tabela 2 -Elementos output utilizados na simulação.....	41
Tabela 3– Elementos do pedido de compra.....	44
Tabela 4– Auto ajuste das distribuições do blockchain público.....	46
Tabela 5 - Auto ajuste das distribuições– privado – <i>hash</i> com dois zeros	47
Tabela 6 - Auto ajuste das distribuições– privado – <i>hash</i> com três zeros	47
Tabela 7– Resumo dos cenários simulados	49
Tabela 8 - Resumo dos resultados das simulações.....	50

SUMÁRIO

1	INTRODUÇÃO	10
1.1	Contexto	10
1.2	Problema.....	11
1.3	Objeto de Pesquisa	13
1.4	Estrutura da dissertação e questão da pesquisa.....	15
1.5	Objetivo.....	16
1.6	Justificativa	17
1.7	Organização do Trabalho	18
2	REVISÃO DA LITERATURA.....	20
2.1	Blockchain.....	20
2.1.1	Funcionamento do blockchain.....	22
2.1.2	Validação	23
2.1.3	Aplicações do blockchain	26
2.1.4	Evolução das tecnologias de informação e comunicação e a futura integração com o blockchain.....	30
3	METODOLOGIA.....	33
3.1	Primeiro Artefato	35
3.1.1	Processos simulados.....	36
3.1.2	Elementos do AnyLogic.....	38
3.2	Segundo Artefato	41
4	RESULTADOS E DISCUSSÃO	43
4.1	Primeiro Artefato	43
4.2	Segundo Artefato	53
5	CONCLUSÕES	58
	REFERÊNCIAS.....	62
	APÊNDICE A – Código VBA para cálculo do <i>hash</i> SHA-256	68
	APÊNDICE B – Macro para simular a mineração do blockchain.....	82
	APÊNDICE C – Código do contrato inteligente escrito em <i>Solidity</i>.....	84

1 INTRODUÇÃO

1.1 Contexto

Na década de 1970, nascia uma rede de computadores usada exclusivamente por pesquisadores e profissionais de tecnologia. Três décadas depois, a Internet torna-se uma realidade cotidiana para o público em geral, mudando a maneira de trabalhar, socializar, criar e dividir informações, além de organizar globalmente o fluxo de pessoas, ideias e bens..

Relatório da *Mckinsey Global Institute* mostrou que 2 bilhões de pessoas estavam conectadas à Internet no ano de 2011, e que transacionaram cerca de US\$ 8 trilhões por meio do comércio eletrônico, respondendo por 21% do crescimento do Produto Interno Bruto (PIB) mundial nas economias maduras nos cinco anos anteriores. Os autores argumentam que, apesar de sua magnitude e alcance, a Internet está numa fase de amadurecimento (MANYIKA; ROXBURGH, 2011).

Grande parte da economia mundial, em especial o setor financeiro, está sustentada por uma infraestrutura rígida e complexa. Riscos crescentes da centralização das organizações foram evidenciados com a crise econômica de 2008, na qual toda a credibilidade do sistema político e financeiro foi colocada à prova. Além disso, o comércio eletrônico convencional resolveu parcialmente a questão de troca de ativos digitais e dinheiro, pois a rede possui fragilidades relacionadas à estabilidade e segurança, visto que algumas aplicações na Internet funcionam em redes descentralizadas.

A troca de informações valorizadas economicamente necessita de um intermediário de confiança para validar a transação. A função dos intermediários é confirmar a identidade das partes, registrar e validar a transação e garantir e proteger a propriedade dos dados para fins de auditoria e conciliação de possíveis divergências no cumprimento dos acordos. Entidades governamentais, por meio de seus órgãos reguladores e do sistema judiciário, cartórios de registros e os bancos comerciais são os principais agentes nessa estrutura. A dificuldade é que esse modelo é ineficiente, burocrático, custoso e vulnerável a irregularidades e corrupção. E mais, custos transacionais associados a terceiros reduzem a eficiência

operacional do processo. Inúmeras tecnologias foram desenvolvidas para resolver essa questão de confiança de modo a automatizar, consolidar e conectar tarefas tradicionalmente executadas por pessoas individualmente ou em grupos (GLASER; BEZZENBERGER, 2015).

1.2 Problema

A capacidade de conectar pessoas em qualquer lugar do planeta e o acesso sob demanda de todo conhecimento humano impactou profundamente as relações econômicas e sociais, seja pela ótica da produção, seja pela ótica do consumo. A conectividade permitiu melhorar o fluxo de informações dentro e fora das empresas que fazem uso dos Sistemas de Informação (SI). Esses sistemas são implementados dentro de uma organização com o objetivo de ampliar a eficácia e a eficiência de seus processos e do planejamento de seus recursos.

O aumento da produtividade e melhor alocação dos recursos na produção é decorrente da implantação de inúmeras tecnologias baseadas em SI, dentre as quais pode-se destacar a conectividade entre as máquinas. As máquinas deixaram de se conectar apenas com pessoas, podendo agora ser programadas para se conectarem diretamente entre si, permitindo a coleta e o processamento de dados numa escala sem precedentes (CULLINEN, 2013). Isso trouxe e ainda traz inúmeras implicações na produtividade, visto que muitas linhas de produção em massa podem se tornar customizadas ao cliente.

Essa conectividade foi resultado de um conjunto inovações associado ao aprimoramento dos sensores, que se tornaram menores e mais potentes, criando o conceito de Internet das Coisas (IoT). A ideia do IoT é estabelecer um sistema de componentes físicos dotados de elementos eletrônicos (como sensores ou etiquetas de identificação por rádio frequência), um endereço de protocolo de Internet (IP) e uma conexão com a rede Internet. Os objetos materiais se tornam participantes nos processos de negócios, visto que estão integrados na rede de informações e podem transmitir dados sobre suas situações, ambientes adjacentes, processos de produção, manutenção programada, dentre outros. A utilização das informações do

IoT contribui para um melhor desenvolvimento cognitivo do ambiente humano. Entretanto, muitas dessas informações não são gratuitas.

Para aplicações profissionais, em especial na área de produção, o conceito é ampliado para Internet das Coisas Industriais (IIoT), cujos dispositivos desempenham um papel significativo nos medidores e redes inteligentes, habilitando a captura de variáveis de consumo em tempos reais (SHROUF; ORDIERES; MIRAGLIOTTA, 2014).

Nas aplicações de comunicação máquina a máquina (M2M), os benefícios dos objetos inteligentes não estão limitados somente à manufatura de produtos individuais, cujos dados de fabricação são propagados por uma rede de equipamentos, mas também pode haver benefícios para todas as etapas de produção sujeitas a uma melhoria contínua. Para esse fim, o IIoT permite atingir o potencial máximo na contribuição para o desempenho operacional como um todo, considerando objetos inteligentes, equipamentos de fabricação e colaboradores que apenas desempenham o papel de supervisão (CHAMBERS; JOHNSTON; SLACK, 2002).

Em sistemas M2M, com destaque para a área de manufatura, o registro de dados históricos é fundamental. Por meio da análise de dados, podem-se identificar os principais fatores que influenciam a qualidade do produto. Consequentemente, o processo pode ser melhorado por meio de otimizações, identificação de gargalos e eliminação de tarefas desnecessárias. Espera-se que essas ações impactem nos custos da cadeia de suprimentos e reduzam os custos de produção (YIN, 2017).

Porém a principal preocupação que fazem os sistemas de IIoT pouco atrativos ao segmento industrial é a questão da segurança dos dados. Por exemplo, em aplicações de IIoT na indústria, o risco de uma invasão fatal com efeitos danosos à produção, à infraestrutura energética ou à saúde pública é muito alto para uma completa aceitação desse sistema inteligente pelas organizações.

Outra dificuldade é a necessidade de um sistema de transação conveniente, seguro e estável para a troca de informações e valores monetários. O sistema de comércio eletrônico não resolveu totalmente essa questão, visto que a obrigatoriedade de um terceiro não permite o aproveitamento de todo o potencial de

uma rede IoT e, conseqüentemente, custos adicionais são introduzidos, o que reduz a eficiência da operação.

O blockchain pode ser utilizado para garantir a segurança da rede por meio de um protocolo leve, especialmente desenhado para uma taxa de transmissão de dados baixa e com pouca demanda dos processadores. Seus princípios de base de dados distribuída, assinatura digital e mecanismo de consenso representam um esforço demasiado para invasores terem acesso ao processo de comunicação e infiltrarem informações falsas (SKWAREK, 2017). E com o surgimento do Bitcoin tornou-se possível o pagamento e a obtenção de dinheiro diretamente entre pares de pessoas sem a interferência de um terceiro.

1.3 Objeto de Pesquisa

O objeto de pesquisa é o blockchain empregado no processo de compras entre empresas. Os sistemas de informações aplicados à cadeia de suprimentos são incapazes de fornecer dados de rastreamento validados e em tempo real durante a etapa de distribuição. A informação geralmente é disponibilizada por uma fonte única e compartilhada com as partes interessadas na medida em que é necessária. A privacidade dos dados também é uma questão estratégica quando se trata da comercialização de produtos acabados, principalmente os químicos e farmacêuticos (WU, 2017). A inteligência desse modelo é administrada por regras comerciais reguladas por regras consensuais entre as partes envolvidas, de modo que elas se obrigam a cumprir o que foi regrado sob determinadas condições. Pode-se pensar na extensão desse uso do blockchain na área de produção onde as máquinas assumem as funções de compras ao se comunicarem entre si.

A cadeia de suprimentos inicia-se com a demanda de um material que desencadeia o processo de compras entre empresas. Esse processo implica em transações que compreendem registros fiscais, contábeis e financeiros, atribuindo um valor monetário para os produtos ou serviços negociados. Esses números comprovam a veracidade das operações de compra e venda para todos os agentes relacionados.

O processo inicia-se com o reconhecimento de uma insuficiência de insumos para continuar a produção, assumindo que o estoque mínimo de segurança tenha sido atingido. O setor de compras recebe essa demanda e elabora um pedido de compra ao fornecedor dessa matéria-prima. O fornecedor recebe o pedido e lança uma ordem de produção. Uma vez concluída a fabricação, emite-se a nota fiscal e o material segue para expedição. O material é recebido e conferido de acordo com o pedido. Em caso de concordância, o recebimento lança os dados do material no sistema de controle de estoque. Em paralelo, o setor fiscal recebe a nota fiscal e efetua os lançamentos contábeis para posterior execução do pagamento. A **Figura 1** ilustra o fluxo do processo de compras entre duas organizações.

Figura 1 – Fluxo do processo de compras entre duas organizações

Fonte: Elaborado pelo autor.

1.4 Estrutura da dissertação e questão da pesquisa

Atualmente, a tecnologia blockchain é utilizada em inúmeras aplicações independentemente se ela é a mais apropriada ou não e, podem ser listadas mais de 80 funcionalidades derivadas do blockchain em 20 diferentes setores (ZANINOTTO, 2016). Todavia, nem todas as aplicações são aceitáveis, pois potencializam desvantagens como: alta redundância, isto é, o esforço de cálculo desnecessário, capacidade exigida da rede de dados, consumo energético e mecanismos de consensos.

Na opção de uso do blockchain ao invés de uma base de dados clássica devem ser considerados os atributos que lhe tragam as seguintes vantagens: armazenamento de dados de forma imutável e permanente, distribuição independente das informações e transações entre todos os parceiros e execução segura das transações ou aplicações. Pode-se presumir que essas são características desejadas no fluxo de informações do processo de compras entre empresas. Assim, origina-se a questão de pesquisa sobre a viabilidade operacional do blockchain em substituir uma base de dados desenvolvida em plataformas disponíveis atualmente no mercado. A **Figura 2** descreve, de forma resumida, a estrutura de pesquisa da dissertação.

Figura 2 – Estrutura da dissertação

Fonte: Elaborado pelo autor.

1.5 Objetivo

O objetivo da pesquisa é avaliar a viabilidade do blockchain como um potencial substituto de um sistema integrado de informação aplicado a um processo de compras entre organizações. A efetividade dessa proposição será efetuada pela comparação dos custos transacionais associados aos tempos operacionais nas condições atuais e na qual o blockchain é empregado.

Na teoria econômica clássica, assume-se que a informação é simétrica no mercado. Isto é, uma vez suposto que os compradores e os vendedores tenham as mesmas informações, a transação pode ser efetuada sem qualquer custo. Porém, na prática, os mercados são ineficientes, pois os agentes devem executar tarefas como buscar a informação, negociar condições comerciais e acompanhar passo a passo todo o processo de modo a garantir que todos os requisitos sejam cumpridos. Os custos dessas atividades adjacentes são conhecidos como custos de transação (WILLIAMSON, 2007).

A mesma teoria ajuda a explicar a razão de escolha dos agentes de uma forma particular de transação em detrimento de outras. O princípio básico é o de que os agentes preferem conduzir transações de uma forma que seus custos transacionais sejam mínimos. Dentre os mais conhecidos exemplos de aplicação dessa teoria estão o modo decisório entre fazer ou comprar e integrações de negócios (LIANG; HUANG, 1998).

Uma forma de diminuir as incertezas e os custos transacionais de coletar dados, negociar e controlar os agentes incluídos nas transações, além de dar garantias legais aos negócios, resolvendo as questões pertinentes à assimetria de informações, seria a adoção de contratos (NORTH, 1981). Nessa perspectiva, contratos inteligentes desenvolvidos no blockchain poderiam ser usados no processo de compras entre empresas para reduzir as intervenções humanas no fluxo de informações.

Visto que a aplicação do blockchain na indústria é uma alternativa para aumentar a automação dos processos, a economia do custo transacional é um incentivo válido para explicar a sua possível adoção. Essa teoria estuda a estrutura de governança mais adequada para a condução das transações. O custo de

transação é a principal variável avaliada pelas empresas no momento em que precisam definir entre a produção interna e a compra do produto ou serviço diretamente no mercado (COASE, 1937).

É importante destacar que o escopo dessa pesquisa é restrito a avaliação de um processo comercial particular, que é fluxo de compras entre empresas. E mais, limita-se a análise comparativa do blockchain contra um modo de operação comumente empregado e não contra uma solução alternativa de base de dados integradas. E por último, os custos econômicos relativos às transações não foram estudados.

1.6 Justificativa

As transações comerciais entre empresas compreendem a emissão de registros fiscais, contábeis e financeiros que atribuem valores monetários para os produtos ou serviços negociados em todas as etapas do processo de compras. Os números traduzem com precisão a veracidade das operações de compra e venda para todos os agentes relacionados. A gestão desse sistema pode ser resumida em três principais atividades: faturamento, arrecadação e cobrança. O faturamento consiste no processamento de informações relacionadas aos produtos e serviços, considerando todas as peculiaridades cadastrais existentes, tarifas, impostos e preços previamente acordados entre as empresas. Os resultados dessa rotina incluem a emissão de documentos fiscais, apontamento de valores à contabilidade, cálculo de impostos e tributos inerentes à operação, atualizações cadastrais dos clientes e relatórios de desempenhos operacionais.

O faturamento é a conexão entre a prestação do serviço ou venda de um produto ao cliente e a sua contrapartida financeira à empresa. As rotinas de arrecadação contemplam a coordenação dos recebimentos financeiros decorrentes dos pagamentos efetuados pelos clientes. Mais do que controle sobre os recebimentos, elas permitem a atualização do fluxo de caixa, dada a visualização dos valores a receber num horizonte de tempo e consequente programação dos desembolsos financeiros pela empresa. Adicionalmente, as práticas de arrecadação incluem tanto a execução das políticas de cobrança quanto os clientes que se

tornam inadimplentes. No âmbito legal e em relação aos acordos contratuais específicos firmados entre as partes, o credor define a elaboração de regras de parcelamentos, descontos, devoluções e cancelamentos de dívidas. Estão incluídas as suspensões de negócio entre a empresa e o cliente, a comunicação da dívida aos órgãos de proteção ao crédito e a possibilidade de acionar o devedor judicialmente.

Dadas as inúmeras etapas e complexidade existentes hoje na geração de dados no processo de compras, é predominante o interesse de uso do blockchain na simplificação e automação desse processo com segurança, ao possibilitar que as transações ocorram diretamente entre os agentes, com o propósito de reduzir estágios e consequentemente a sua duração (PETRE & HAÏ, 2018). Christidis; Devetsikiotis (2016) é favorável à automação com o blockchain de fluxos de trabalho que despendam muito tempo para execução.

1.7 Organização do Trabalho

Este trabalho está organizado em seis capítulos. Na presente introdução é definido o contexto no qual o objeto de estudo, o blockchain, está inserido. A partir do apontamento do problema foi identificada a lacuna de conhecimento na literatura e a justificativa indica a importância desse estudo no preenchimento desse hiato. Apresenta-se nesse momento a estrutura da dissertação. O capítulo seguinte trata a revisão da literatura de tópicos relacionados ao tema deste estudo. A análise crítica de relacionamento com a corrente pesquisa segue a explicação de funcionamento do blockchain e validação dos dados por meio de funções *hash* unidirecionais e da prova de trabalho. Além disso, o capítulo aborda o estado-da-arte da tecnologia blockchain fazendo um resumo das suas potenciais aplicações no mercado associadas à evolução das tecnologias de informação e comunicação. Na sequência, discute-se o método de pesquisa utilizado, os detalhes de cada artefato construído. No Capítulo 4 são apresentados os resultados e discussões de cada artefato construído: o primeiro, a modelagem e simulação do processo de compras entre organizações; e o segundo, a implantação de um contrato inteligente no blockchain do *Ethereum*. Ambos são provas de conceito da aplicabilidade do

blockchain. Por fim, são discutidas as conclusões e as principais limitações da pesquisa e apresentadas as referências bibliográficas.

2 REVISÃO DA LITERATURA

A concepção de uma rede de comunicação de dados distribuída foi apresentada pela primeira vez no trabalho de Paul Baran (1964). No contexto da Guerra Fria, esse estudo propõe avaliar o desempenho de uma rede na qual cada estação conecta-se com todas as estações e adjacentes em vez de poucas, como num sistema centralizado. Demonstra-se, por meio de simulação, que a configuração distribuída possui uma capacidade de sobrevivência a ataques inimigos muito maior do que uma rede centralizada. Discute-se também a necessidade de ter um formato de mensagem padronizado que use um mecanismo adaptativo de armazenamento e distribuição de informação de qualquer tipo de dado digital. E mais, prova-se que irregularidades no tráfego na rede são respondidas de forma mais eficiente pela estação local, dispensando o controle central, que é um ponto de vulnerabilidade. Quarenta anos depois, verifica-se que todos esses conceitos, além de manifestados na Internet, constituem a ideia central do blockchain.

2.1 Blockchain

Os avanços na tecnologia de registros distribuída no campo de criptografia em moedas digitais, sistemas descentralizados de consenso, baseado nas concepções de uma rede ponto a ponto começam a se difundir, contrariamente a uma autoridade centralizada. Conhecida como blockchain, ela promete modificar a maneira de registrar ativos, transações e simplificar processos nas organizações.

Nos últimos três anos, o blockchain obteve um reconhecimento amplo, o que levou a um aumento significativo nas propostas de aplicações de software, serviços e novos modelos de negócios baseados no blockchain. Comumente nos estágios iniciais de adoção de uma nova tecnologia, apresentam-se inúmeras propostas irrealistas e expectativas inflacionadas e por essa razão, é importante entender as limitações do blockchain, seus potenciais uso e benefícios. A maioria das tentativas focam em bancos e serviços financeiros, mas se destacam as aplicações no setor público e inclusão social como a transferência de recursos a refugiados sírios, o registro de propriedades em Honduras e no Estado da Geórgia nos Estados Unidos

da América, processo eleitoral no parlamento europeu, emissão de moeda fiduciária na Suécia e registros públicos na Estônia. Há também exemplos no setor privado como o serviço de transferência de dinheiro *Ripple*, fechaduras eletrônicas Slock.it e a plataforma de veículos compartilhados Arcade City (ZĪLE & STRAZDIŅA, 2018).

E mais do que um sistema de pagamento criptografado, o blockchain possui potencial de aplicação em cadeias de valores que demandem a gravação de dados operacionais ou financeiros autênticos e íntegros. Sugere-se que a automação com o blockchain possa ser viável em fluxos de trabalho que consumam muito tempo para execução (CHRISTIDIS; DEVETSIKIOTIS, 2016).

Na sua concepção original, blockchain é uma base de dados distribuída numa rede de computadores, com todos os registros de endereços e saldos gravados cronologicamente, onde alguns participantes ofertam esforços computacionais para gravação de um novo bloco em troca de uma parte do valor transacionado (NAKAMOTO, 2008). Literalmente, é uma enorme planilha que arquiva todas as movimentações contábeis das transações irreversivelmente. Pode ser usado também como um sistema de inventário com gravação, rastreamento, monitoramento e transferência de ativos. Isso significa que qualquer ativo tangível ou digital pode ser armazenado no blockchain (SWAN, 2015). A primeira aplicação real do blockchain foi a moeda digital Bitcoin.

De acordo com as definições de SAP Brasil (2018) existem dois tipos de blockchain: o público e o privado. No blockchain público, todos os participantes podem ler, enviar transações ou cooperar no processo de consenso, pois esse tipo de blockchain não necessita de autorização. Todas as transações são públicas e os usuários permanecem anônimos. O *Bitcoin* e *Ethereum* são os exemplos mais conhecidos de blockchains públicos. Já os blockchains privados são dirigidos por uma única entidade, que libera acesso a qualquer usuário que respeite os critérios predeterminados. Apesar de não ser, de fato, descentralizado, esse tipo de blockchain com concessões de permissão é mais proveitoso para os casos de uso de B2B (*business to business*) e administrações governamentais. O esforço computacional para criação de um novo bloco (mineração) é feito exclusivamente por cada computador conectado.

Redes de blockchain como *Ethereum* são estruturas que permitem o desenvolvimento de um sistema econômico dentro do software, com contas de gestão e uma unidade nativa de troca entre as contas (moeda), conhecida como *token*. O *token* é uma forma de ativo digital usada exclusivamente dentro do sistema. O *Ether* é o *token* utilizado como combustível dentro da plataforma do *Ethereum* para rodar os contratos inteligentes, serviços computacionais dentro da rede e para pagar taxas aos mineradores. Porém novos *tokens*, lastreados no *Ether*, podem ser criados para rodar um sistema de contas acessível a um grupo de usuários em especial.

O blockchain é desenvolvido numa arquitetura de blocos de dados conectados por criptografia. Cada bloco contém os dados de todas as transações do sistema desde sua origem e pode criar uma impressão digital única, utilizada para confirmar a validade da informação. Os blocos estão conectados linear e cronologicamente (como uma corrente) com o próximo bloco através de um *hash*. Um alto padrão de privacidade é alcançado, pois a identidade de cada usuário faz uso de uma chave de acesso pública e variável. A criação de um novo bloco depende de provas de consenso, que são problemas matemáticos que demandam certo poder computacional para resolução.

2.1.1 Funcionamento do blockchain

2.1.1.1 Estrutura do blockchain

Conforme explicado anteriormente, o blockchain é uma cadeia de blocos ordenados de forma temporal e validados por meio de um algoritmo para resolver um problema matemático que envolve funções *hash* unidirecionais. O tamanho do blockchain aumenta conforme cresce o número de transações. Cada bloco contém um *hash* exclusivo (assinatura digital única), lote das transações mais recentes e o *hash* do bloco anterior. A geração de cada bloco acontece no momento em que ele é validado. O *hash* do bloco anterior garante a união dos blocos e previne que qualquer bloco seja alterado ou outro bloco seja inserido entre dois blocos existentes. A alteração em qualquer uma das operações de um bloco já validado invalida todo o restante da cadeia a sua frente, dado que as autenticações dos

blocos à frente não são mais válidas. Assim, cada bloco subsequente fortalece a checagem do bloco anterior e, conseqüentemente, de todo blockchain. A estrutura da cadeia e dos blocos é representada na **Figura 3**.

Figura 3 – Estrutura da cadeia de blocos

Fonte: GUPTA (2017).

2.1.2 Validação

2.1.2.1 Funções de hash unidirecionais

Para entender a validação de um bloco da cadeia é preciso discutir o conceito de funções *hash*, mais especificamente as unidirecionais. As funções de *hash* são pequenos programas de computador que transformam qualquer classe de dado em um número de tamanho fixo, independentemente do tamanho de entrada. Existem muitas funções de *hash* diferentes entre si no que tange ao tamanho do valor de *hash* gerado. Um grupo importante de funções de hash chama-se funções de *hash* criptográficas, que criam impressões digitais singulares para qualquer tipo de dado. A mais utilizada no blockchain é a SHA-256, que produz uma *string* de saída de 256 bits. A classificação unidirecional impossibilita que seus valores de entrada sejam rastreados com base nas saídas. Esse tipo de função é muito utilizado no campo da criptografia, uma vez que é fácil de computar o resultado da função, mas o inverso não é válido. Isso significa que é impossível recuperar os dados de entrada originais baseado no valor de *hash* (BUCHMANN, 2013).

2.1.2.2 Prova de Trabalho (Proof of Work)

Um elemento central na validação dos blocos é a verificação da prova de trabalho (*proof of work*), isso é, o quebra-cabeça de *hash*. Somente os blocos que contenham uma solução precisa de seu quebra-cabeça de *hash* individual serão processados. Essa validação é, essencialmente, a resolução de um problema matemático envolvendo funções *hash* unidirecionais. De forma simplificada, o problema a ser resolvido é determinar uma variável que, quando combinada com dados do bloco anterior e de bloco atual e processada por uma função *hash* unidirecional, produza um resultado cujo início seja uma sequência específica predeterminada (TAPSCOTT; TAPSCOTT, 2016).

A ação de resolver esse problema é popularmente conhecida como mineração, ao passo que o computador que executou a rotina é chamado de minerador. A criação de blocos válidos custa energia, tempo e dinheiro, pois exige a resolução de um problema de adivinhação de *hash* único para cada bloco, dispendioso do ponto de vista de processamento. A resolução de um bloco gera uma recompensa para o usuário que a realizou primeiro. Dessa forma, a rede remunera pelo seu funcionamento e os usuários são incentivados a minerar mais, aumentando a eficiência da rede. Pode-se afirmar que a recompensa é o ônus relacionado à obtenção e à manutenção da integridade de todo o sistema (DRESCHER, 2018). Basicamente, o processo de mineração consiste em resolver o seguinte problema:

$$H(\text{Hash}_{\text{anterior}} + \text{Bloco}_{\text{transações}} + \text{PoW}) = 000\text{AAAAAAAAA}$$

Fonte: Adaptado de *IBM Blockchain: Proof of Technology Workshop* (IBM CORPORATION, 2016).

No qual:

H (...) representa a função *hash* e, nessa equação, o esforço reside na determinação do valor de PoW de modo que o resultado final se inicie, por exemplo, com três zeros à esquerda. Uma vez que essa função é unidirecional, tal resolução somente pode ser realizada por tentativa e erro, à medida que a rede se expande, o sistema efetua uma calibração da dificuldade de obtenção da resposta do problema, aumentando a quantidade de zeros.

Entretanto, esse método implica no consumo energético crescente, limitando a escalabilidade da rede, de forma que, em algum instante, o custo transacional (que deverá cobrir o custo da infraestrutura computacional e de consumo energético) será tão alto que a rede se tornará cara demais para ser usada. A rede do Bitcoin, por exemplo, poderá consumir em um futuro próximo, 7.7 gigawatt de eletricidade, consumo comparável ao de países como Irlanda (3.1 gigawatt) e Áustria (8.2 gigawatt) (DE VRIES, 2018).

Algoritmos alternativos à prova de trabalho estão sendo desenvolvido no momento. O principal destaque é o *proof-of-stake*, que seleciona o minerador do bloco de forma aleatória e restrita. Apenas mineradores que depositem uma garantia na rede podem participar da mineração. Porém, caso os outros participantes da rede entrem em consenso de que a validação do bloco não foi realizada de forma adequada, o minerador perde seu depósito. Posto que o valor em risco de perda é maior do que a remuneração recebida pelo bloco validado, autenticações fraudulentas não são atrativas, garantindo a segurança da rede (SIIM, 2017).

2.1.2.3 Distribuição da informação na rede

Após a resolução do problema de criação do bloco, é necessário compartilhar essa informação com toda a rede por meio da Internet. Em virtude das adversidades nas redes e limitações no seu acesso, a comunicação é marcada pelos seguintes fatos: não há garantia de recepção das mensagens pelo destinatário, mensagens podem chegar repetidas vezes ao destino e ainda surgirem em ordens distintas daquelas em que foram enviadas. O blockchain se defende desses contratemplos na comunicação por meio de um algoritmo de consenso, que é uma série de regras que governa o modo como os dados de transação são processados e adicionados ao sistema. Em linhas gerais, todos os usuários devem trabalhar com a mesma e mais atualizada versão da cadeia. Para tanto, a informação de que um novo bloco acabou de ser criado é tratada de forma semelhante por cada usuário, encaminhando aos pares com quem se comunica após validação. Duplicatas de transações ou de blocos são identificadas e filtradas com base em seus valores de *hash* criptográficos. E todo usuário é habilitado a ordenar as informações recebidas, pois os dados de transações e cabeçalhos dos blocos contêm marcadores de data.

Uma vez que essa validação é executada pela maioria dos mineradores, os mesmos abandonam o trabalho no bloco atual e iniciam os esforços no bloco seguinte. Eventualmente, devido ao tamanho da rede e a possibilidade de validações simultâneas ocorrerem, existe a possibilidade de uma bifurcação na cadeia. O mesmo algoritmo de consenso resolve essa questão, determinando que a sequência mais longa criada após a bifurcação será a sobrevivente. A bifurcação mais curta é excluída e seus blocos retornam para a fila de processamento.

2.1.3 Aplicações do blockchain

O banco suíço *Credit Suisse* elaborou um relatório para os seus clientes sobre as potenciais aplicações da tecnologia blockchain em inúmeras indústrias. Para tanto, classificou os seus benefícios em três categorias: desintermediação de terceiros, imutabilidade de registros e contratos inteligentes (BRENNAN, 2016).

A desintermediação de terceiros trata da irrelevância da participação de um terceiro para validar uma operação. Do ponto de vista de custos transacionais, organizações e mercados são as instituições que coordenam a economia, dado que elas são responsáveis por organizar e regular as transações. Portanto, baixos custos estão diretamente relacionados à combinação eficiente de instituições. A economia nos custos de transação leva a uma estrutura institucional eficiente de organização econômica e governança. Por outro lado, blockchains não são organizações formais nem mercados. São organizações espontâneas que competem com as demais empresas e possuem propriedades de mercado. Seu papel é ser um facilitador de transações e não apenas executar a troca. Basicamente, blockchains coordenam grupos distribuídos de indivíduos, permitindo sua aproximação de maneira a criar um ambiente econômico (MCDONALD; ALLEN; POTTS, 2016).

A imutabilidade de registros aborda a criação de um livro-razão com dados auditáveis para descrever e proteger a posse de ativos. O blockchain protege o histórico de dados de transação para que não seja manipulado ou adulterado, armazenando-os em um repositório imutável por meio de dois artifícios: a exigência de se reescrever a estrutura de dados desde o ponto que causou a mudança até o fim da cadeia e a obrigatoriedade de uma solução de um quebra-cabeça de *hash*.

Contratos inteligentes são algoritmos de comunicação entre dois ou mais computadores, com interfaces de usuários. São programas automatizados que transferem ativos dentro do blockchain, depois que ações específicas são acionadas. Utilizam criptografia e outros mecanismos de segurança para estabelecer relações por meio de algoritmos, sem a interferência dos atores principais no processo e com ausência de terceiros para validar regras ou resolver disputas. Considera-se que eles possam reduzir custos de transação mental e computacional exigidos pelas partes envolvidas, terceiros e suas ferramentas (SZABO, 1997).

2.1.3.1 Desintermediação de terceiros

Na categoria de desintermediação de terceiros, Sikorski, Haughton e Kraft (2017) realizam uma prova de conceito de aplicação do blockchain na interação entre máquinas no setor elétrico. A simulação consiste na relação entre dois geradores e um consumidor representado por uma máquina. Os dois geradores registram suas ofertas de venda de energia no blockchain e a máquina analisa e escolhe a oferta que melhor satisfaz sua demanda a um menor custo. O processo operacional ocorre simultaneamente ao registro da transação financeira. A Câmara de Comercialização de Energia Elétrica seria um agente dispensável nesse processo. Hardjono e Smith (2016) apresentam um modelo de comissionamento de dispositivos IOT numa plataforma em nuvem. A proposta é utilizar o blockchain para estabelecer uma conexão para troca de dados de forma segura e anônima entre os fabricantes e os proprietários dos dispositivos. O artigo destaca a concepção de comissionamento em que os detentores dos dispositivos pudessem ser remunerados por permitir o seu uso e dividir os dados coletados. Preferências dos consumidores não precisariam ser detectadas por agências de pesquisas e campanhas de marketing poderiam ser direcionadas diretamente ao público-alvo. No setor financeiro, tem-se a análise de MacDonald, Allen e Potts (2016) sobre as implicações do blockchain no setor bancário do ponto de vista tecnológico e de governança. Em teoria, inúmeros processos bancários são passíveis de desintermediação, porém, questões regulatórias necessitam de mais discussões.

Goertzel, B.; Goertzel, T.; Goertzel, Z. (2017) discorrem sobre economia colaborativa e mutualismo. Em oposição a economias capitalistas em que rege a lei

do livre mercado, apresenta-se de maneira fantasiosa uma nova organização da sociedade com base nos conceitos dos Estados Socialistas, porém controlada não por comitês políticos, e sim por uma inteligência artificial. Esse sistema centralizado atuaria no planejamento de produção conforme a oferta de trabalho e demandas individuais de cada pessoa. Todas as transações financeiras decorrentes desse sistema seriam liquidadas numa moeda digital no blockchain para dar transparência e evitar especulações com a moeda.

2.1.3.2 Imutabilidade de dados

Na qualidade da imutabilidade de dados, confiabilidade, privacidade e anonimato são fatores importantes no blockchain e tratados recentemente no meio acadêmico. Hashemi *et al.* (2016) sugerem a criação de um mecanismo baseado em blockchain com o objetivo de compartilhar dados entre dispositivos, pessoas e organizações, centrado no usuário, em diferentes níveis e com granularidade. Tian (2016) propõe o uso de sensores dotados com radiofrequência para coletar, transmitir e compartilhar dados de todas as fases da cadeia de suprimentos do setor agropecuário, que incluem: produção (plantação e alimentação), colheita e abate, processamento, estocagem, distribuição e vendas. A ideia é que os dados armazenados no blockchain não sejam usados apenas por cada empresa na cadeia, mas também pelos clientes finais e órgãos reguladores. Além de melhorar o processo de rastreabilidade, a credibilidade em se consumir alimentos seguros aumenta, combatendo, ao mesmo tempo, produtos falsificados. São citados como entraves o alto custo dos dispositivos de radiofrequência e a imaturidade do blockchain. Todavia, não há dúvidas de que esse sistema aumentaria a qualidade e a segurança dos produtos alimentares.

Shrestha e Vassileva (2016) tratam do uso de dispositivos inteligentes ancorados em plataformas na nuvem para oferecer serviços ao usuário, tais como celulares smartphones, sensores sem fio, veículos e roupas inteligentes. Com o intuito de personalizar os serviços, os dados armazenados na nuvem são analisados e combinados para gerar uma informação relevante ao usuário. Geralmente, cada fabricante detém sua própria plataforma conectada com os produtos exclusivamente desenvolvidos por ela. O compartilhamento de dados com outras plataformas é

dificultado por questões de segurança e privacidade em relação aos dados do usuário. A proposta do trabalho é descentralizar o armazenamento dos dados numa plataforma em nuvem comum a todos os dispositivos utilizando o blockchain.

2.1.3.3 Contratos inteligentes

O blockchain viabiliza a automatização de processos que funcionam de forma ineficiente em redes centralizadas e permite a criação e a comercialização de inúmeros tipos de ativos, que possuem características e dinâmicas distintas quando comparados à dimensionalidade única das moedas digitais. E quanto mais intensa as propriedades do ativo, mais próximo da ideia de contrato inteligente ele se identifica. A criação de contratos inteligentes no blockchain é feita pela combinação de protocolos, que são algoritmos de comunicação entre dois ou mais computadores, com interfaces de usuários. Huckle *et al.* (2016) exploraram o uso combinado de contratos inteligentes no blockchain com o IOT no mercado de compartilhamento, ilustrado por três exemplos práticos: sistema autônomo de aluguel de veículos, contratos no mercado de câmbio e automatização do processo de pagamento de direitos autorais. Huh, Cho e Kim, (2017) propõem um modelo de IOT construído no blockchain para avaliar a limitação do atual modelo cliente-servidor, relacionado à sincronização de um número elevado de dispositivos. A simulação faz uso dos contratos inteligentes do blockchain *Ethereum*, onde são estabelecidas regras de funcionamento de três dispositivos IOT conectados a esse arranjo.

Biswas e Muthukkumarasamy (2017) definem um modelo de plataforma de cidade inteligente baseado em contratos no blockchain, em que dispositivos se comunicam de forma segura e privativa. O intento é permitir a integração e a gestão da infraestrutura física, social e de negócios de uma cidade, de maneira que as entidades governamentais façam uma utilização mais eficiente dos recursos públicos. Christidis e Devetsikiotis (2016) examinam a funcionalidade de contratos inteligentes do blockchain, especificamente no ambiente de IOT. Exploram detalhadamente características técnicas do blockchain, bem como explicitam suas limitações no contexto de automação de processos operacionais morosos. Eles estimulam, ainda, o emprego de uma moeda digital na rede blockchain numa

camada de pagamentos, preparando toda uma estrutura de ambiente de negócios de produtos e serviços entre máquinas.

Xu *et al.* (2017) incitam o desenvolvimento de uma plataforma de aplicações de economia colaborativa num blockchain público. Sugerem um modelo, ilustrado pelo aluguel de um imóvel, onde o contrato foi estabelecido diretamente entre proprietário e locador. O artigo foca em ferramentas para preservar a privacidade dos usuários, respeitando as regras contratuais. Zhang e Wen (2015) introduzem o conceito de empresas autônomas e distribuídas dentro de modelos de negócios digitais no IOT. O artigo discute com detalhes todas as etapas tradicionais de um negócio digital (etapa pré-transacional, negociação, assinatura e cumprimento do contrato) e as adequações necessárias no IOT e no ambiente descentralizado do blockchain.

Uma das aplicações específicas e mais populares dos contratos inteligentes é a criação de ativos digitais definidos como *tokens*. Os *tokens* podem representar qualquer tipo de recurso que possua uma expectativa de geração de benefício ou valor no futuro dentro de uma comunidade. Pode-se pensar no seu uso potencial na comprovação de procedência, características e direitos de propriedade de bens com alto valor agregado e abstrato como obras de arte, joias e colecionáveis. As propriedades e funções de cada token estão condicionadas a finalidade que se estabeleça para eles. Eles podem ser utilizados como meio de pagamento para acessar uma rede ou para a formação de uma governança descentralizada sobre uma organização (Dannen, 2017).

2.1.4 Evolução das tecnologias de informação e comunicação e a futura integração com o blockchain

A evolução das tecnologias de informação e comunicação na indústria e economia está associada diretamente às transições para novos processos de manufatura conhecidas como revoluções industriais. Uma revolução industrial é reconhecida por mudanças abruptas e radicais, motivadas pela incorporação de tecnologias, tendo implicações nos âmbitos econômico, social e político. Na maioria das vezes, a inovação tecnológica começa com uma simples ideia testada inúmeras

vezes e frequentemente abandonada após fracassos consecutivos. Algum tempo mais tarde, outra pessoa resgata essa ideia e, com persistência e determinação, consegue um resultado conclusivo. Essa é a melhor descrição do processo de invenção das diversas máquinas nas linhas de produção nos dias atuais (GOMBRICH, 2008).

Há um entendimento entre historiadores sobre a ocorrência de três revoluções industriais. A primeira acontece entre 1760 e 1840, com o aparecimento das máquinas a vapor e linhas férreas. A segunda ocorre entre o final do século XIX e início do século XX, tendo como principais inovações a eletricidade, a linha de montagem e a difusão da produção em massa. A terceira, que se iniciou na década de 1960, rompeu paradigmas por meio do desenvolvimento dos semicondutores e tecnologias como mainframes, computadores pessoais e, mais tarde, nos anos 1990, a Internet.

Todavia, com um grande progresso e difusão de algumas tecnologias da terceira revolução, assim como o advento e incorporação de outras, alguns autores sugerem que, no começo do século XXI, houve o início de uma quarta revolução industrial (SANTOS, 2016). Schwab (2017) sugere que a quarta revolução industrial é caracterizada pela transformação digital. Essa mudança seria motivada por tecnologias como internet móvel, inteligência artificial, automação, robótica, veículos autônomos, impressão em 3D, nanotecnologia, biotecnologia, além do aperfeiçoamento de sensores, tornando-os menores e mais potentes possibilitando, assim, a internet das coisas (IoT).

O processamento de transações não teria alcançado os atuais patamares sem o conceito da computação distribuída. Esse tipo de arranjo já existe há algum tempo, como em redes ponto a ponto como *Napster* ou *Torrent*. Porém avanços recentes revelam sua aderência à Lei de Moore e a performance da computação distribuída duplica a cada ano (THOMPSON; PARTHASARATHY, 2006). Logo, será possível aproveitar o poder computacional, *terabytes* de armazenamento e a capacidade de transferência de dados disponíveis em bilhões de dispositivos que estão ociosos na maior parte do tempo. A adoção em massa da computação distribuída processada em dispositivos remotos poderia reduzir significativamente os

custos associados à instalação e à manutenção de enormes centros de processamento de dados centralizados.

A ideia do IoT é estabelecer um sistema de componentes físicos dotados de elementos eletrônicos (como sensores ou etiquetas de identificação por radiofrequência), um endereço de protocolo de Internet (IP) e uma conexão com a rede Internet. Os objetos materiais se tornam participantes nos processos de negócios, visto que estão integrados na rede de informações. Podem transmitir dados sobre suas situações, ambientes adjacentes, processos de produção, manutenção programada, dentre outros. No cenário da Indústria 4.0, IoT desempenha um papel significativo nos medidores inteligente, habilitando a captura de variáveis de consumo em tempo real (SHROUF; ORDIERES; MIRAGLIOTTA, 2014).

Uma descentralização bem-sucedida por meio do IoT reside não somente na inserção em uma rede ponto a ponto, mas também na questão de confiabilidade: um ambiente no qual não há necessidade de os participantes serem confiáveis e no qual não haja um único ponto de falha decorrente da centralização. Enquanto o blockchain possui riscos regulatórios e econômicos na função de reserva de valor, ele pode ser revolucionário como uma ferramenta transacional. O blockchain pode ser visto como uma estrutura facilitadora no processo transacional e na coordenação das iterações entre os dispositivos (PURESWARAN, 2014). Ademais, a comunicação entre máquinas viabiliza a automação de processos de maneira flexível, permitindo que as empresas consigam entregar a esperada customização com o menor desembolso.

A literatura trata a IoT suportada pelo blockchain como uma conexão entre o meio físico e o digital. Os dispositivos seriam habilitados para executar de forma independente contratos digitais, como pagamentos, permutas e convênios, trocando recursos e serviços. Explora-se também o conceito de empresa autônoma e descentralizada, onde cada equipamento seria capaz de gerenciar suas próprias funções e comportamento. Por outro lado, muitos desafios técnicos e paradigmas, precisam ser superados para que o blockchain não tenha o seu uso restrito a poucas atividades.

3 METODOLOGIA

A construção dos protótipos empregará a metodologia do *Design Science Research* (DSR). Esse método busca ampliar os limites das capacidades humanas e organizacionais por meio de criação de artefatos inovadores para solucionar uma dificuldade organizacional (HEVNER; CHATTERJEE, 2010).

Artefatos funcionais são produzidos para tratar de problemas não resolvidos e sua utilidade para solucioná-los é avaliada. Será adotado o roteiro adaptado de Hevner *et al.* (2004) para condução dessa pesquisa de acordo com as diretrizes apresentadas no **Tabela 1**.

Tabela 1 - Roteiro de condução do *Design-Science Research*

Diretriz	Contribuição
Projeto do artefato	O resultado é a validação de uma prova de conceito por meio de um protótipo implementado no blockchain.
Relevância do problema	A transferência de créditos entre empresas representa mais da metade do volume de recursos financeiros movimentados no mundo. O protótipo em blockchain visa simular e provar a viabilidade de um sistema baseado nessa tecnologia.
Avaliação do projeto	Testes estruturais e funcionais serão conduzidos para avaliar e demonstrar a utilidade, qualidade e eficácia do protótipo. E mais, será conduzida modelagem e simulação da arquitetura do blockchain para avaliar o desempenho de um cenário sem blockchain e outro com.
Contribuição esperada	As contribuições esperadas desse protótipo são: revelar a viabilidade do blockchain na função de uma base de dados distribuída, aumentar a eficiência no processo de compras entre organizações e reduzir custos com intermediários.

Rigor científico	De modo a garantir o rigor científico, serão utilizadas as diretrizes legitimadas de Hevner <i>et al.</i> (2004) e March e Smith (1995) para direcionar a criação e a construção do artefato.
Projeto como um processo de escolha	Com o intuito de alcançar uma solução justificada para as questões de pesquisa, o projeto foi fundamentado na literatura existente, tais como Nakamoto (2008); Brennan (2016); Glaser e Bezzenberger (2015). Trabalhos similares também foram considerados: Burgos <i>et al.</i> (2017); Notheisen, Cholewa e Shanmugan (2017); Sharma, Moon e Park (2017); Turkanović (2018); Sikorski, Haughton e Kraft (2017); e Pop <i>et al.</i> (2018).
Comunicação da pesquisa	O trabalho será estruturado de acordo com Gregor e Hevner (2013) de modo a potencializar os resultados dessa pesquisa no meio acadêmico e profissional. Para o público com viés acadêmico, serão fornecidas: uma descrição pormenorizada da arquitetura de protótipo, o código de programação, a lógica de implantação e descrição de suas características de modo que o experimento possa ser reproduzido por outro pesquisador. No entanto, para a audiência profissional, serão discutidas a eficácia do protótipo no contexto da aplicação, aspectos operacionais e propostas de soluções para as limitações identificadas.

Fonte: Adaptado de Hevner *et al.* (2004).

As atividades de pesquisa no DSR podem ser divididas em duas partes: criação e avaliação. A criação refere-se à construção do artefato, demonstrando de fato que ele pode ser fabricado para executar determinada tarefa. Avaliar envolve o desenvolvimento de critérios e análise do desempenho do artefato em relação aos

padrões definidos. A avaliação determina se a tecnologia progrediu, substituindo a atual por uma mais efetiva (MARCH; SMITH, 1995).

3.1 Primeiro Artefato

O primeiro artefato consistirá na modelagem e simulação do processo de compras entre organizações. Será feita uma análise comparativa entre a situação atual do processo (*As-Is*) e o cenário hipotético com a aplicação do blockchain (*To-Be*). A simulação pode ser definida como uma tentativa de representação de sistemas reais, a partir da construção de modelos computacionais de simulação. Ela é uma das técnicas mais usadas em Pesquisa Operacional (PO), que permite a formação de cenários onde, através destes, pode-se orientar o processo de tomada de decisão, preceder análises e avaliações de sistemas e propor soluções para a melhoria de desempenho (PEREIRA, 2015).

A modelagem é uma forma pela qual podemos solucionar problemas do mundo real. Na maioria das vezes, não é possível arcar com experimentos com objetos reais para encontrar as soluções corretas: construir, destruir e fazer alterações pode ser muito oneroso, perigoso ou meramente impossível. Nesse caso, pode-se construir um modelo que use uma linguagem de modelagem para representar o sistema real. Esse processo assume abstrações onde são incluídos detalhes julgados importantes e excluídos aqueles que não. O modelo sempre será menos complexo do que o sistema original (GRIGORYEV, 2018).

Um modelo é um conjunto de proposições ou afirmações que expressam relacionamentos entre construtos. Nas atividades de projeto, modelos representam situações como demonstrações de problemas e soluções. Um modelo pode ser simplesmente visto como uma descrição de como o sistema funciona. A modelagem é útil para estudos de viabilidade em que o propósito é obter uma ordem de grandeza aproximada sobre o desempenho do sistema. No caso de modelos, eles são avaliados em relação a sua exatidão com o fenômeno no mundo real, integridade, nível de detalhe, robustez e consistência interna (MARCH; SMITH, 1995).

Essa abordagem foi adotada por Sabounchi e Wei (2017), cujo trabalho avaliou por simulações um modelo de comercialização de energia elétrica distribuída ponto a ponto, baseado no blockchain do *Ethereum*. Engelmann *et al.* (2017) também utilizaram a simulação para avaliar o desempenho financeiro de conexões adjacentes entre pares de computadores e a rede blockchain, com o objetivo de armazenar transações de pagamentos bilaterais fora da rede. A ideia é aumentar o número de transações por segundo no sistema, registrando na cadeia principal apenas o saldo final confirmado entre as duas partes.

Nessa pesquisa, foi utilizado o software *AnyLogic 7* para reproduzir os processos de compras *As-Is* e o *To-Be*. Esse simulador permite a construção de modelos complexos e contém uma variedade grande de funções. Também possui flexibilidade para a produzir os três métodos de simulação modernos: eventos discretos, modelagem baseada em agentes e dinâmica de sistemas. Além disso, o programa permite realizar análises de sensibilidade e de variação de parâmetros, que são muito importantes e úteis para o presente trabalho. O código fonte dos modelos pode ser encontrado em <https://github.com/gdolce/blockchain>.

3.1.1 Processos simulados

No processo *As-Is*, os dados transacionais são registrados manualmente em quatro diferentes bancos de dados. Mesmo com uma programação de controle de produção e uma automação M2M mínimas, o sistema é vulnerável à lançamentos imprecisos, integrações deficientes e inúmeras inconsistências na conciliação de dados, o que gera atrasos na produção e na execução de pedidos de forma incorreta.

Em contrapartida, no *To-Be* tem-se os dados de produção gravados unicamente na base de dados do blockchain, que é acessível tanto ao comprador quanto ao vendedor. Cabe a cada agente executar as consultas necessárias e efetuar as devidas confirmações das transações nos blocos. Será presumido nesse modelo que os agentes serão as máquinas, cujas interações se darão exclusivamente pelo blockchain. Os processos de compras *As-Is* e *To-Be* são apresentados nos fluxogramas detalhados nas **Figura 4 e 5**.

Figura 4 – Processo de compras As-Is

Fonte: Elaborado pelo autor no Bizagi.

Figura 5 – Processo de compras To-Be

Fonte: Elaborado pelo autor no Bizagi.

O custo transacional é aquele gasto embutido no processo transacional. No processo de compras *As-Is*, esses custos podem ser associados às seguintes atividades: identificação da demanda pelo operador da máquina; elaboração do pedido de compra pelo comprador; lançamento do pedido pelo vendedor; emissão da nota fiscal pelo responsável da expedição; registro manual da entrada do produto no estoque pelo responsável do recebimento; e registro da nota fiscal no sistema contábil pelo contador. No processo *To-Be*, esses custos são referentes à gravação dos dados de produção no blockchain pelo equipamento do comprador e as posteriores consultas aos blocos para verificar a situação do processo. Nas duas condições, os esforços transacionais terão seus desempenhos analisados estatisticamente por meio de duas variáveis: tempo de execução de cada tarefa e número de colaboradores envolvidos.

3.1.2 Elementos do AnyLogic

Ambos os modelos serão simulados por modelagem de eventos discretos, pois o objetivo é modelar um processo, ou seja, uma sequência de operações que os agentes executam. Os agentes são entidades presentes nos softwares de simulação que representam desde objetos físicos nos modelos mais gerais, até o comportamento de empresas e governos em modelos mais abstratos. No exemplo, são representados pelas ordens de compra e pelo produto ou serviço em trânsito nos processos *As-Is* e *To-Be*. As operações de um modelo podem incluir atrasos, serviços de múltiplos recursos, seleções de ramificações de processos, separações, dentre outros. Uma vez que os agentes disputem recursos limitados e possam se atrasar, a geração de filas é inerente a quase todos os modelos de eventos discretos.

Os modelos de eventos discretos são estocásticos, visto que os tempos de chegada de agentes e os tempos de serviço são comumente estocásticos, ou seja, eles são resultados de uma distribuição de probabilidade. Isso representa que um modelo deve ser executado por um tempo específico ou realizar um número particular de replicações antes de gerar uma saída relevante. As saídas mais comuns de um modelo de eventos discretos são: utilização de recursos, tempo gasto no sistema ou em parte dele, tempos de espera, filas, desempenho do sistema e

identificação de gargalos. As atividades do processo de compras modeladas no *AnyLogic* foram consolidadas em três etapas sequenciais: geração de pedido de compra, fabricação e recebimento. A representação gráfica dos elementos simulados é apresentada na **Figura 6**.

Figura 6 – Modelo gráfico da simulação no AnyLogic

Fonte: Elaborado pelo autor no *AnyLogic*.

Esse processo fez uso de quatro blocos no simulador, o *Source*, o *Queue*, o *Delay* e o *Sink*, conforme ilustrado na **Figura 7**. O *Source* é responsável pela criação dos agentes. Nesse bloco, deve ser especificada a ação e a quantidade de agentes a serem criados. O *Queue* é uma fila (um buffer) de agentes aguardando serem aceitos pelo próximo objeto no fluxo do processo ou um armazenamento de uso geral para os agentes. O modo de enfileiramento usado foi o padrão FIFO (*First In First Out*). Por sua vez, o *Delay* faz a retenção dos agentes numa determinada quantidade de tempo. Uma vez que os agentes competem por recursos limitados e estão condicionados ao atraso, as filas fazem parte de quase todos os modelos de eventos discretos.

Figura 7 – Blocos Source, Queue, Delay e Sink

Fonte: Extraído da biblioteca de processos do *AnyLogic*.

A fila ocorre sempre que a procura por um determinado serviço é maior que a capacidade do sistema de prover este serviço. O tempo de espera é avaliado dinamicamente, pode ser estocástico e pode depender do agente, bem como quaisquer outras condições. Foram criados três blocos *Delay* no modelo:

Gerar_Pedido, *Fabricar* e *Receber*. Por último, o *Sink* é onde os agentes são destruídos após o término do processo.

Para a simulação, foram usadas quatro variáveis atribuídas para cada bloco *Delay*: quantidade demandada, tempo de operação para gerar o pedido, tempo de operação para a fabricação e tempo de operação para o recebimento. A **Figura 8** mostra os parâmetros utilizados nas simulações dos processos de compras.

Figura 8 – Parâmetros utilizados na simulação

Fonte: Elaborado pelo autor no *AnyLogic*.

As variáveis frequentemente representam algumas características do objeto modelado como por exemplo: tempo, velocidade, quantidade, aceleração, comprimento, área etc. Elas são úteis quando as instâncias de objeto têm o mesmo comportamento descrito na classe e são comumente utilizadas para descrever os objetos de forma estática.

Um parâmetro, normalmente, é uma constante em uma única simulação, e é alterado somente quando você precisa ajustar o comportamento do seu modelo. Todos os parâmetros são visíveis durante a execução do modelo. Assim, pode-se simplesmente ajustar o modelo mudando os parâmetros das variáveis no tempo de execução. A ação a ser executada pode ser definida na mudança de parâmetro.

Para avaliar o funcionamento do modelo, fez-se uso de elementos de análise, usados para coletar, visualizar e analisar os dados de saída. Esses elementos podem carregar as estatísticas de uma rede de filas, tais como: tamanho da fila, tempo de fila, número médio de clientes no sistema, número médio de clientes em atendimento, tempo médio de permanência no sistema e tempo de atendimento. Os principais elementos usados são o *output*, gráfico de barras e histograma.

O elemento *output* é usado para armazenar um único valor de dados escalares e exibi-lo após (ou durante) o modelo executado. Exemplos de tais valores incluem indicadores quantitativos importantes (tempo médio no sistema, lucro, despesas, nível de satisfação do cliente etc.), que fornecem uma visão dos resultados da simulação.

No modelo em questão, 21 elementos *output* foram usados e são apresentados na **Tabela 2**:

Tabela 2 -Elementos output utilizados na simulação

LQ1	fila média em Fila_M1
LQ2	fila média em Fila_M2
LQ3	fila média em Fila_M3
LS1	fila média em Gerar_Pedido
LS2	fila média em Fabricar
LS3	fila média em Receber
WQ1	tempo médio de espera em Fila_M1
WQ2	tempo médio de espera em Fila_M2
WQ3	tempo médio de espera em Fila_M3
WS1	tempo médio de espera em Gerar_Pedido
WS2	tempo médio de espera em Fabricar
WS3	tempo médio de espera em Receber
L1	LQ1+LS1: fila média na saída de Gerar_Pedido
L2	LQ2+LS2: fila média na saída de Fabricar
L3	LQ3+LS3: fila média na saída de Receber
L	L1+L2+L3: fila média no sistema
W1	WQ1+WS1: tempo médio de espera na saída de Gerar_Pedido
W2	WQ2+WS2: tempo médio de espera na saída de Fabricar
W3	WQ3+WS3: tempo médio de espera na saída de Receber
W	W1+W2+W3: tempo médio de espera no sistema
Output	quantidade de produtos entregues
Utilização_Gerar_Pedido	nível de utilização / ociosidade da atividade de geração de pedido
Utilização_Fabricar	nível de utilização / ociosidade da atividade da fabricação
Utilização_Receber	nível de utilização / ociosidade da atividade de recebimento

Fonte: Elaborado pelo autor no *AnyLogic*.

3.2 Segundo Artefato

O segundo artefato será a implantação de um contrato inteligente no blockchain público do *Ethereum*, que retratará o processo *To-Be*. O pedido de compra será registrado pelo comprador no blockchain e os eventos posteriores (emissão da nota fiscal, recebimento e fechamento da fatura) acionados após

consulta e confirmação da informação pelo responsável. Os dados do pedido de compra registrados no blockchain serão: número sequencial único (NSU), identificação do comprado, identificador do vendedor, quantidade, unidade, preço unitário e imposto. O *hash* da etapa de fabricação será o identificador único da nota fiscal.

A aplicação desse artefato permitirá a redução das interações sistêmicas que se dão hoje entre os departamentos comerciais das empresas, transferindo-as às linhas produtivas, o que propiciará a transação direta entre as máquinas ou equipamentos de diferentes empresas. O processo foi executado com dados de demanda gerados de forma arbitrária e o blockchain foi usado para validar e controlar o fluxo produtivo da operação. A utilização das características essenciais do blockchain acarreta na geração de um banco de dados seguro, transparente e validado pelas partes, reduzindo a assimetria de informações e eventuais disputas (NOTHEISEN; CHOLEWA; SHANMUGAN, 2017).

4 RESULTADOS E DISCUSSÃO

4.1 Primeiro Artefato

O modelo conceitual do artefato é análogo a um sistema de filas, caracterizado por um regime de chegada, um regime de serviço e disciplina da fila. A fila é um processo estocástico, isto é, desenvolve-se no tempo e no espaço conforme leis de probabilidade. O seu estado num instante t (número de pedidos, tamanho da fila, tempo de atendimento etc.) é uma variável aleatória, cuja probabilidade nesse instante t depende do valor da probabilidade no instante inicial t_0 (TÔRRES, 1966).

Em muitos casos essa dependência do estado inicial se encerra depois de certo tempo, ou seja, o sistema atinge um estágio de equilíbrio em que as probabilidades independem do estado inicial e do tempo decorrido, chamado de padrão de chegada estacionário. Assim, é necessário conhecer a distribuição de probabilidade descrevendo os tempos entre as sucessivas chegadas dos clientes, bem como os tempos de serviços. Para determinação de qual distribuição de probabilidade conhecida melhor se ajusta aos dados coletados, foi usado o utilitário de análise estatística *Statfit 3*.

O processo de chegada aponta o padrão de chegada de ordens no sistema. Apresenta comportamento estocástico, o sistema cuja chegadas no espaço e tempo acontecem segundo as leis de probabilidade. Os modelos de filas estocásticos mais frequentes assumem que os tempos de chegada e serviço obedecem a uma distribuição exponencial. Considerou-se que as unidades das operações de *Gerar_Pedido*, *Fabricar* e *Receber* fossem inicialmente de capacidades unitárias, ou seja, os pedidos são atendidos individualmente e não simultaneamente.

Com intuito de obter resultados consistentes com a realidade, buscou-se um referencial que disponibilizasse dados de volume de compras para a simulação. O relatório de estatísticas da Organização das Nações Unidas apresenta um volume de compras na ordem de 18.6 bilhões de dólares no ano de 2017, que correspondem a 715 mil ordens de compra (UNITED NATIONS GLOBAL MARKETPLACE, 2018). Com base nessa referência, foi arbitrada uma demanda de 82 pedidos a cada hora, considerando o ano base de 365 dias e 24 horas de

trabalho ao dia. Os tempos de operação e as capacidades de fabricação e recebimento foram determinados de modo que o trânsito de produtos nas filas anteriores a esses processos não fosse obstáculo ao sistema. Desse modo, a taxa de fabricação foi definido em 1,36 minuto por pedido e o tempo de recebimento em 1,36 minuto por pedido.

Na análise comparativa entre a situação atual do processo (*As-Is*) e o cenário hipotético (*To-Be*), foi adotada a premissa de que somente o tempo de operação para gerar o pedido seria afetado pela aplicação do blockchain. Na primeira situação, atribuiu-se ao tempo de geração do pedido a duração média de digitação manual de um pedido de compra contendo entre 106 e 108 caracteres, contendo os dados exibidos na **Tabela 3**:

Tabela 3– Elementos do pedido de compra

Informação	Tipo	Tamanho
ID	identidade única do pedido	3 caracteres
Endereço do comprador	<i>hash</i> único	42 caracteres
Endereço do vendedor	<i>hash</i> único	42 caracteres
NSU	número sequencial único do produto	3 - 4 caracteres
Quantidade do produto	<i>string</i>	3 caracteres
Unidade	<i>string</i>	7 caracteres
Preço total	<i>string</i>	2 -3 caracteres
Impostos	<i>string</i>	4 caracteres

Fonte: Elaborado pelo autor.

A amostra de 50 tomadas de tempo revelou um tempo mínimo de 0,54 minuto e o máximo de 0,90 minuto para o término da tarefa. Visto que a probabilidade de ocorrência de duração da atividade é igual em qualquer tempo dentro desse intervalo, adotou-se uma distribuição uniforme para o tempo de geração do pedido no *As-Is*. No modelo uniforme, a probabilidade de gerar qualquer ponto em um intervalo contido no espaço amostral é proporcional ao tamanho do intervalo, por essa razão a necessidade de se definir os pontos máximo e mínimo. A **Figura 9** exibe alguns exemplos de dados do pedido de compra.

Figura 9 – Dados do pedido de compra

ID	address comprador	address vendedor	NSU	Quantidade	Unidade	Preço	Tax
100	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1700	236	unidade	R\$ 138,00	27%
101	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1866	498	unidade	R\$ 139,00	27%
102	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1313	433	unidade	R\$ 150,00	27%
103	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1705	256	unidade	R\$ 250,00	27%
104	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1766	476	unidade	R\$ 125,00	27%
105	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1586	290	unidade	R\$ 96,00	27%
106	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1183	106	unidade	R\$ 142,00	27%
107	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1851	182	unidade	R\$ 238,00	27%
108	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1158	485	unidade	R\$ 106,00	27%
109	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1299	447	unidade	R\$ 164,00	27%
110	0x85185fe3A4e36079818Ba1d12705A9B689899658	0xa60AdD2af71a4f50b3F94509E71a1e9DbDeA5dDa	1998	175	unidade	R\$ 96,00	27%

Fonte: Elaborado pelo autor.

No segundo caso admitiu-se que o tempo de operação para gerar o pedido fosse o ciclo de gravação de um novo bloco no blockchain, correspondente à duração da busca de uma solução para o algoritmo de prova de trabalho, que torna a base de dados imutável. O tempo de criação de um novo bloco depende do tipo de blockchain usado e da dificuldade empregada no algoritmo de consenso para calibração da oferta de processamento computacional.

No cenário *To-Be*, foram testados o blockchain público e o privado. Para obtenção do tempo de criação no blockchain público do *Ethereum*, foram empregados os dados históricos de tempo de geração de blocos de 12/11/2017 a 18/11/2018, obtidos em *Etherscan* (2018). A amostra exibiu uma média de 14,35 segundo por bloco com desvio-padrão de 0,39 segundo. O gráfico de distribuição acumulado, como ilustrado na **Figura 10**, é a curva dos dados versus as distribuições de probabilidades ajustadas.

A análise de aderência no software *Statfit3*, para descobrir a distribuição de probabilidade mais aderente a amostra, revelou que a curva lognormal é a que melhor se ajusta aos dados reais do tempo de criação do bloco no *Ethereum* público. A **Tabela 4** exibem o auto ajuste das distribuições do blockchain público.

Figura 10 – Gráfico com distribuição acumulada ajustada do blockchain público

Fonte: Extraído do Statfit 3 pelo autor.

Tabela 4– Auto ajuste das distribuições do blockchain público

autofit of distributions		
distribution	rank	acceptance
Lognormal(13, 0.16, 0.408)	100	do not reject
Uniform(13, 15.4)	0.247	reject
Exponential(13, 1.27)	0	reject

Fonte: Extraído do Statfit 3 pelo autor.

No exemplo do blockchain privado, foram desenvolvidos dois algoritmos escritos na linguagem *VBA Excel*. O primeiro foi uma função *hash* que transforma qualquer dado de uma célula em uma *string* com tamanho fixo de 64 caracteres. O segundo código foi uma rotina que simulou a construção do bloco e mediu o intervalo de tempo de criação de cada um. A construção do bloco finaliza-se no instante em que uma solução para a prova de trabalho for encontrada. A prova de trabalho foi ajustada para se descobrir *hashes* finais que se iniciassem com dois ou três zeros consecutivos.

Os dados usados foram pedidos de compra de 106 a 108 caracteres cada um, com campos de informação similares aos utilizados no processo *As-Is*. A criação de um novo bloco consiste na junção dos dados com o *hash* do bloco anterior e uma variável aleatória que precisa ser descoberta, de modo que atenda a condições de se iniciar com o número estabelecido de zeros. A macro e a função que calcula o *hash* de uma célula são apresentadas no **Apêndice**. Para o artefato em questão, foi utilizado um computador dotado de um processador Intel Core i7-4500U CPU @ 2,70 GHz, 16,00 GB de RAM e sistema operacional *Windows 10 Home Single Language*.

A macro executou duas amostras de 500 blocos cada com erros amostrais aproximados de 4,5%. Foram obtidos o tempo médio de 6 segundos e desvio-padrão de 6 segundos para a obtenção de *hashes* com dois zeros consecutivos; e o tempo médio de 1,13 minuto e desvio-padrão de 1,23 minuto para a obtenção de

hashes com três zeros consecutivos. Os testes de aderência mostraram que o tempo de obtenção de *hashes* com dois zeros consecutivos ajusta-se melhor à uma distribuição exponencial enquanto, o tempo de obtenção de *hashes* com três zeros consecutivos à uma distribuição lognormal conforme **Figuras 11 e 12**. As **Tabelas 5 e 6** apresentam os autos ajustes das distribuições do blockchains privados.

Figura 11 – Gráfico com distribuição acumulada ajustada – privado – hash com dois zeros

Fonte: Extraído do Statfit 3 pelo autor.

Tabela 5 - Auto ajuste das distribuições– privado – hash com dois zeros

autofit of distributions		
distribution	rank	acceptance
Exponential(0, 0.000146)	100	do not reject
Lognormal(0, -9.38, 1.14)	50.4	do not reject
Uniform(0, 0.000706)	0	reject

Fonte: Extraído do Statfit 3 pelo autor.

Figura 12 – Gráfico com distribuição acumulada ajustada – privado – hash com três zeros

Fonte: Extraído do Statfit 3 pelo autor.

Tabela 6 - Auto ajuste das distribuições– privado – hash com três zeros

autofit of distributions		
distribution	rank	acceptance
Lognormal(0, -7.41, 1.09)	100	do not reject
Exponential(0, 0.001)	86.8	do not reject
Uniform(0, 0.00363)	0	reject

Fonte: Extraído do Statfit 3 pelo autor.

Os tempos de criação distintos no público e no privado são explicados pelo tipo de hardware empregado no processamento. É esperado que a velocidade com que os blocos são criados seja proporcional a capacidade do processador empregado. No caso da rede pública, são utilizados equipamentos mais potentes,

como placas de processamento gráfico dedicadas (*GPUs*); e outras mais sofisticados, como o *ASIC (Application-Specific Integrated Circuit)*, que são máquinas desenvolvidas exclusivamente para essa função e que facilitam a escala industrial do segmento.

Os tempos obtidos foram aplicados como parâmetro de entrada no modelo de simulação de modo a alterar a propriedade de atuação do bloco *Gerar_Pedido*, conforme mostra a **Figura 13**.

Figura 13 – Configuração de propriedades do Gerar_Pedido

Fonte: Extraído pelo autor do *AnyLogic*.

De modo a ter uma avaliação completa do desempenho dos quatro cenários, utilizou-se a simulação de Monte Carlo. Essa metodologia efetua a análise de risco através de modelos de resultados prováveis, mudando todo fator com incerteza intrínseca por uma distribuição de probabilidade. Posteriormente, calculam-se os resultados continuamente com outro conjunto distinto de valores aleatórios gerados pelas funções probabilísticas. Nas simulações, os cálculos foram repetidos mil vezes em cada cenário com horizontes de tempo de 1 ano.

A resposta da simulação de Monte Carlo é uma distribuição de valores dos possíveis resultados. Ao usar as distribuições de probabilidade para definição dos valores de entrada, as variáveis de saída podem apresentar diferentes probabilidades de ocorrência de inúmeros resultados. As distribuições de probabilidade representam uma forma realista de detalhar a incerteza em variáveis.

A simulação de Monte Carlo oferece ao tomador de decisão um conjunto de possíveis resultados e suas respectivas probabilidades de ocorrências, de acordo com a ação estabelecida como decisão. Ela revela também as possibilidades extremas, ou seja, os resultados das decisões mais ousadas e das menos arriscadas e, todas as prováveis implicações das decisões tomadas. A **Tabela 7** apresenta o resumo dos cenários simulados.

Tabela 7– Resumo dos cenários simulados

Tipo de Simulação	Tipo de distribuição de probabilidade	Tempo do Gerar_Pedido
As-Is		
Digitação manual	Uniforme	32.00 e 54.00 segundos
To-Be		
Blockchain público	Lognormal	14.35 ± 0.39 segundos
Blockchain privado		
Hash de 2 zeros consecutivos	Exponencial	6.00 ± 6.00 segundos
Hash de 3 zeros consecutivos	Lognormal	73.00 ± 83.00 segundos

Fonte: Elaborado pelo autor.

Na comparação entre os quatro cenários, pode-se observar que o blockchain privado, com a prova de trabalho ajustada para encontrar *hashes* iniciados por dois zeros consecutivos, apresentou desempenho superior aos demais cenários *To-Be*. Em virtude do maior tempo médio de criação do bloco, no caso do privado com prova de trabalho na busca de três zeros consecutivos, o nível de utilização da atividade de geração de pedido foi de 100%, originando uma fila média elevada e tempo de espera superior às demais condições. Em relação ao *As-Is*, essa configuração possui comportamento similar em relação ao melhor cenário *To-Be* quanto às variáveis: quantidade entregue, fila média no sistema e tempo de espera no sistema. Entretanto, o *As-Is* precisa de uma capacidade de atendimento de 5 unidades, enquanto o melhor cenário do *To-Be*, apenas uma. A capacidade de atendimento é definida como o número máximo de pedidos que podem ser processados por uma máquina ou por um trabalhador simultaneamente. Os resultados são apresentados de forma sintética na **Tabela 8**. Geralmente, quanto maior a capacidade de serviço, pior a eficiência do sistema.

Tabela 8 - Resumo dos resultados das simulações

	As-Is		To-Be (Blockchain)	
Tipo de gravação	Manual	Privado hash 2 zeros	Público	Privado hash 3 zeros
Tempo médio de criação do bloco (seg)	não aplicável	6,0	14,0	71,0
Distribuição de probabilidade	Uniforme	Exponencial	Lognormal	Lognormal
Quantidade entregue (mil)	718,3	718,3	717,3	445,4
Fila média no sistema (unid)	29,4	29,1	1.150	136.470
Tempo de espera no sistema (min)	24,0	22,7	820	99.828
% Utilização do bloco Gerar_Pedido	40,5%	13,6%	65,2%	100,0%
Capacidade na geração do pedido (unid)	5	1	1	1

Fonte: Elaborado pelo autor.

Os resultados no formato gráfico são apresentados nas **Figuras 14 a 25**, a seguir. Nos histogramas as frequências relativas são exibidas no eixo y e o intervalo da quantidade de produtos entregues no eixo x. A análise gráfica das variáveis aleatórias medidas nos cenários *As-Is* e *To-Be* dos blockchains privados permite concluir que as distribuições de frequências seguem uma curva normal de probabilidades, visto que graficamente representam curvas simétricas, no formato de sinos, em torno de um ponto central médio. Por outro lado, no blockchain público, a distribuição de frequência da quantidade entregue segue a curva normal, enquanto a fila média e o tempo de espera no sistema se assemelham a uma curva lognormal.

Na distribuição lognormal, os valores são positivamente assimétricos ou distorcidos e é utilizada para representar valores que não passam abaixo de zero, mas que têm um potencial positivo ilimitado. Dada a particularidade de ser um banco de dados único, não há possibilidade de aumento de capacidade operacional, tanto no cenário do blockchain público quanto no privado com a prova de trabalho ajustada para encontrar *hashes* iniciados por três zeros. Desse modo, é improvável que esses dois cenários alcancem produtividades similares ao cenário *As-Is* e ao privado com prova de trabalho especificada para encontrar *hashes* iniciados por dois zeros.

Figura 14 – Histograma de quant. produzida no processo As-Is

Fonte: Elaborado pelo autor.

Figura 15 – Histograma de quant. produzida no processo To-Be (privado – hash com 2 zeros iniciais)

Fonte: Elaborado pelo autor.

Figura 16 – Histograma de quant. produzida no processo To-Be (público)

Fonte: Elaborado pelo autor.

Figura 17 – Histograma de quant. produzida no processo To-Be (privado – hash com 3 zeros iniciais)

Fonte: Elaborado pelo autor.

Figura 18 – Histograma de fila média no sistema no processo As-Is

Fonte: Elaborado pelo autor.

Figura 19 – Histograma de fila média no sistema no processo To-Be (privado – hash com 2 zeros iniciais)

Fonte: Elaborado pelo autor.

Figura 20 – Histograma de fila média no sistema no processo To-Be (público)

Fonte: Elaborado pelo autor.

Figura 21 – Histograma de fila média no sistema no processo To-Be (privado – hash com 3 zeros iniciais)

Fonte: Elaborado pelo autor.

Figura 22 – Hist. de tempo de espera no sistema no processo As-Is

Fonte: Elaborado pelo autor.

Figura 23 – Hist. de tempo de espera no sistema no processo To-Be (privado – hash com 2 zeros iniciais)

Fonte: Elaborado pelo autor.

Figura 24 – Hist. de tempo de espera no sistema no processo To-Be (público)

Fonte: Elaborado pelo autor.

Figura 25 – Hist. de tempo de espera no sistema no processo To-Be (privado – hash com 3 zeros iniciais)

Fonte: Elaborado pelo autor.

4.2 Segundo Artefato

Com o objetivo de representar o processo *To-Be*, o segundo artefato consistiu na criação e lançamento de um contrato inteligente no blockchain público do *Ethereum*, em que o comprador e o fornecedor atuariam como clientes da rede, utilizando a Internet como infraestrutura de comunicação, dada a sua resiliência. Optou-se pelo desenvolvimento do artefato no blockchain público, pois seu funcionamento é similar ao privado.

A plataforma *Ethereum* é um projeto de código aberto, fundado no início de 2014 por Vitalik Buterin, financiado como um projeto de financiamento coletivo e lançado oficialmente em julho de 2015. O *Ethereum* é um blockchain capaz de armazenar registros de transações num arquivo, que é um tipo de planilha pública, distribuída e de segurança garantida por criptografia. As transações publicadas são verificadas e validadas pelos próprios usuários num processo conhecido como mineração, que ocorre via execução de códigos de natureza criptográfica, sendo assim, o sistema pode funcionar num protocolo distribuído recompensando seus usuários pelo poder computacional empregado por eles.

No *Ethereum*, além da rede oficial, existem outras duas redes para homologação e testes, a *Ropsten* e a *Rinkeby*. O objetivo das redes de teste é simular o contrato como se fosse no ambiente oficial, utilizando o *ether* nas transações sem qualquer custo. E mais, a plataforma permite a criação de redes semiprivadas ou públicas de blockchain com acesso restrito a um limitado número de participantes.

A comunicação com o blockchain *Ethereum* requer o uso de ferramentas específicas que depende do nível de conhecimento de cada usuário. Para os iniciantes, recomenda-se a extensão *Chrome Metamask*, que é a maneira mais simples de se navegar pelo *Ethereum*, permitindo a criação de contas, realização de transferências de *ether* e lançamento de contratos na rede. Ela pode ser encontrada no endereço: <https://metamask.io/>.

Outra forma é por meio do navegador *Mist*, que é um tipo de carteira virtual que desempenha as mesmas funções do *Metamask*, exceto pelo fato de que necessita fazer download de todo o bloco para o seu funcionamento. Para usuários

intermediários, há a possibilidade de acessar o blockchain diretamente no *prompt* de comando do sistema operacional, utilizando interfaces de comandos escritas em Go e C++, chamadas de *Geth* e *Eth* (Dannen, 2017).

Em conjunto com as ferramentas de acesso, foi desenvolvido um editor e compilador de programas chamado *Remix Solidity*. Sobretudo, ele é um navegador utilizado para escrever o código dos contratos inteligentes exclusivamente na linguagem nativa do *Ethereum*, o *Solidity*.

Na construção do protótipo, o primeiro passo foi escrever o contrato inteligente. Optou-se pela utilização do *Solidity*, mas a plataforma permite a programação em outras linguagens como *Go*, *JavaScript*, *Java*, *Python*, *node.js* e *C++*, além de rodar em diversos sistemas operacionais como Windows, Linux e OS X. O contrato é composto basicamente de eventos e funções. Os eventos são os registros no bloco que são usados por desenvolvedores e provedores externos de interface com usuários para rastrear as ações do contrato e para fins de auditoria.

Foram definidos cinco eventos nesse contrato: pedido de compra, fabricação, emissão de nota fiscal de saída, recebimento do produto e recebimento da nota fiscal. Os dados brutos gravados foram os mesmos usados na construção do primeiro artefato e apresentados anteriormente na **Tabela 3**: ID, endereço do comprador, endereço do vendedor, NSU, quantidade do produto, unidade, preço total e impostos.

As funções são operações que alteram o estado do sistema e garantem a sua dinâmica. Três funções foram estabelecidas no contrato: comprar, produzir e receber. O código completo do contrato inteligente é apresentado no **Apêndice**.

O estágio seguinte foi a distribuição desse contrato na rede de teste *Ropsten*, escolhida de forma circunstancial. Primeiramente, o código do contrato é transcrito no compilador Remix, acessado no endereço <https://remix.ethereum.org/>, e aberto no navegador Google Chrome. Ao mesmo tempo, efetuou-se o acesso à extensão *Metamask* e criou-se uma conta para executar as operações. A **Figura 26** ilustra o *Metamask* aberto na página do editor Remix.

Figura 26 – Metamask aberto na página do Remix

Fonte: Elaborado pelo autor.

Para ser possível executar operações na rede, foi necessário o acúmulo de *ethers* nessa conta para custear as transações. Esses *ethers* não possuem valor econômico e podem ser obtidos em <http://faucet.ropsten.be:3001/>, bastando indicar o endereço da conta receptora.

Uma vez compilado no Remix, o contrato é compartilhado na rede. No próprio Remix, podem-se acessar as funções do contrato, que ficam disponíveis na parte inferior direita da tela. O passo adiante é lançar os dados dos pedidos em formato texto ou numérico e confirmar o registro no bloco. A **Figura 27** expõe a tela do Remix com o contrato em atividade.

Figura 27 – Contrato em atividade no Remix

Fonte: Elaborado pelo autor.

Em resumo, a criação do protótipo foi feita na rede de testes *Ropsten*, utilizando o Remix para escrever o código do protótipo e o *Metamask* para gerenciar as transações na rede. O *hash* do endereço do contrato é *0xa60add2af71a4f50b3f94509e71a1e9dbdea5dda*. Por fim, para se ter acesso aos registros gravados no blockchain, utilizou-se a ferramenta de consulta *Etherscan*, disponível em <https://ropsten.etherscan.io/address/> (ETHERSCAN, 2018).

Nesse local, é possível confirmar e validar transações, checar a data de gravação, número do bloco e o montante de *ether* gasto no registro. No exemplo, realizou-se uma busca pelo endereço do contrato e, ao acessar o campo eventos, os dados de cada transação são evidenciados no formato hexadecimal, mas podem ser convertidos nos formatos texto ou numérico.

No caso concreto, as etapas processuais seriam executadas manualmente ou por meio de sistemas comerciais integrados ao blockchain conforme o pseudocódigo ilustrado na **Figura 28**. A demanda de sistemas é diretamente proporcional ao consumo computacional e a quantidade de dados a serem atualizados.

Figura 28 – Fluxograma do pseudocódigo do processo

Processo	Integração	Base de dados
<u>Plataforma</u> SAP, Oracle, TOTVS, Web, ERP, Controle manual, etc	<u>API</u> (Application Programming Interface)	<u>Blockchain</u> Contrato inteligente
Pedido de compra		
Emissão de documento fiscal		
Registro de entrada do produto		

Fonte: Elaborado pelo autor.

5 CONCLUSÕES

A pesquisa analisou dois artefatos para verificar a viabilidade de uso do blockchain no processo de compras entre organizações. O primeiro artefato foi a modelagem e simulação desse processo numa situação atual (*As-Is*) e em outra que faria uso do blockchain (*To-Be*). O segundo artefato consistiu na implantação e manipulação de um contrato inteligente no blockchain do *Ethereum*. Pode-se comprovar o desempenho operacional superior da alternativa com o blockchain, medido por meio de duas variáveis: tempos de execução da tarefa de geração de pedidos e número de postos de atendimentos necessários. Ainda que as simplificações do modelo tornem a simulação dos processos distantes da realidade nas empresas, o mérito dessa pesquisa está na avaliação do modo de operação do blockchain na criação de uma base de dados. Desse modo, os resultados obtidos permitem concluir que o blockchain é uma alternativa viável como substituto de uma base de dados tradicional. Entretanto, é importante destacar as limitações dessa pesquisa em relação aos desafios técnicos do blockchain indicados por Swan (2015).

O primeiro desafio é relacionado à taxa de transações processadas. A arquitetura descentralizada do blockchain necessita que em toda aplicação de prova de trabalho, cada participante da rede seja obrigado a processar a transação. Isso implica numa restrição temporal em razão do processamento de cada transação. Adicionalmente, à medida que a rede blockchain cresce, haverá mais competição por uma capacidade limitada de transações e, conseqüentemente, as confirmações levarão mais tempo para serem concluídas e comissões maiores serão cobradas. Hoje, blockchains públicos como *Bitcoin* e *Ethereum* processam entre 3 e 30 transações por segundo. Mas para serem capazes de sustentar processos mais robustos, elas teriam que processar milhares de transações por segundo. Como exemplo, a bandeira de cartão de crédito Visa realiza em média 60.000 transações por segundo, o Twitter faz em média 5.000 transações por segundo e essa pesquisa fez uso de uma taxa real arbitrada em 2×10^{-2} transações por segundo (82 transações por hora).

O segundo problema refere-se ao tamanho do blockchain e à amplitude de acesso à Internet. O blockchain do Bitcoin, por exemplo, ultrapassou 140 GB e

cresceu a uma taxa de 52 GB no último ano. Nas condições padrões atuais, o download de todo o bloco pode demorar até 24 horas. Se o desempenho crescesse a um fator de 2.000 tps (referencial bandeira de cartão de crédito VISA), o bloco cresceria a uma taxa de 1,42 PB/ano ou 3,9 GB/dia. Processar um volume de dados imenso não é tarefa trivial, tanto que hoje apenas 10 mil servidores ao redor do mundo rodam o blockchain do Bitcoin completo, motivando um risco de centralização no processamento. Por outro lado, 140 GB é um volume de dados usual em muitas áreas de análise de dados. A compactação de dados hoje não seria adequada ao blockchain por questões de acessibilidade e segurança. Porém existe aqui uma oportunidade de inovação em novos tipos de algoritmos de compressão que aumentem a usabilidade e o armazenamento do blockchain, mantendo sua integridade e acessibilidade, além do desenvolvimento de artifícios para limitar o número de participantes necessários para validar cada transação, sem perder a confiança de que cada transação é verdadeira.

A terceira dificuldade é a segurança do blockchain em razão de se acreditar que um de seus atributos essenciais é a sua suposta resistência a ataques cibernéticos em função da sua complexa criptografia e da natureza distribuída do seu banco de dados. O número de participantes da rede blockchain compartilhando dados entre si é superior aos dos bancos de dados tradicionais, uma vez que a toda a informação precisa ser distribuída igualmente entre todos. Todavia, empresas não podem permitir que informação privada se torne pública por questões comerciais ou legais. E, de modo a superar essa contradição, o acesso à maioria dos blockchains demanda uma chave pública e outra privada. Isso representa um ponto forte do sistema, uma vez que é praticamente impossível o acesso aos dados sem uma combinação perfeita de chaves. Por outro lado, a proteção dessas chaves é crucial para evitar que hackers tenham acesso a elas e consigam acessar os dados e refazer transações. Existe também o risco de que 51% do poder computacional concentre-se em um único participante, o que possibilitaria que um servidor minerador transferisse todas as moedas digitais para sua própria carteira. O mecanismo que inibe essa prática é a recompensa do minerador, que é calibrada para incentivá-lo a ser um servidor honesto, visto que o preço da moeda é superior ao custo energético do processamento e remunera o capital investido em equipamentos.

A quarta adversidade trata dos recursos energéticos desperdiçados, pois a mineração consome uma quantidade enorme de energia, visto que inúmeros servidores competem ao mesmo tempo na criação do próximo bloco. Por um lado, esse desperdício é o que faz o sistema ser confiável, onde agentes racionais participam de uma competição sem utilidade para decifrar o *hash* do bloco em busca de uma recompensa. Por outro lado, os recursos gastos não trazem qualquer benefício a não ser a mineração. A demanda energética do *Ethereum* estimada em novembro de 2018 é de 9,87 TWh, ou seja, aproximadamente 2% da energia consumida no Brasil no ano de 2016. (DIGICONOMIST, 2018).

O quinto obstáculo é a usabilidade e a integração do blockchain com outros sistemas de tecnologia de informação (TI). A facilidade de uso em trabalhar com o blockchain é uma barreira de entrada crucial para a adoção da tecnologia. No estágio atual, são necessárias melhorias na interface com os usuários, na velocidade do sistema e na definição de normas oficiais entre os blockchains. Enquanto padrões estão sendo estabelecidos isoladamente em cada blockchain, a interoperabilidade entre essas plataformas e outros sistemas de TI é limitada e quase inexistente. Esse fato aumenta os custos operacionais, dada a necessidade de incorporação de novas autenticações e protocolos de comunicação aos novos processos de negócios baseados no blockchain.

O último ponto trata da possibilidade da bifurcação forçada do blockchain em múltiplas cadeias por razões administrativas ou de versão, impossibilitando a futura fusão dos dados. O próprio blockchain do *Ethereum* se dividiu em duas partes em junho de 2016: clássico e tradicional. A decisão de ramificação foi majoritária entre os participantes e decorreu após ataque de *hackers* ao maior financiamento coletivo e descentralizado da história, The DAO (*The Decentralized Autonomous Organization*), que levantou na ocasião cerca de 150 milhões de dólares. De modo a recuperar os tokens furtados, a ação tomada foi reverter todas as transações até o momento anterior ao lançamento da empreitada, ocasionando a criação de um novo ramo do bloco nesse ponto. Evidentemente que essa decisão, apesar de ajudar na recuperação dos valores, prejudicou outros clientes cujas transações não estavam relacionadas com o problema (FALKON, 2017).

Como essa pesquisa era orientada para solução de um problema específico, pode-se considerar a viabilidade do blockchain para registro de pedidos de compras entre empresas conforme evidenciado na prova de conceito realizado no *Ethereum*. No entanto, as aplicações do blockchain não estão restritas à indústria. Por exemplo, contratos inteligentes podem ser capazes de gerenciar sistemas de registros privados nos setores de saúde e financeiro; certificação de origem de produtos agrícolas, de documentos públicos (como registros de veículos, passaportes, licenças governamentais e escrituras de imóveis) e de registros pessoais (como diplomas, certificados, histórico profissional); e, por fim, registros de rastreabilidade de ativos (como carros, chaves, celulares e computadores) (ASTE; TASCA; MATTEO, 2017).

A indústria do blockchain ainda está nos estágios iniciais de desenvolvimento e, conseqüentemente, limitações potenciais são identificadas, mas nada que atrapalhe a difusão da tecnologia. Após superadas essas barreiras, os blockchains poderão se reproduzir repetidamente em grande quantidade com ganho de produtividade. As propriedades apresentadas pelo blockchain de conhecimentos disseminados há anos, porém a combinação de todos esses recursos o torna atrativo para várias indústrias. É notável a recomendação predominante de uso de blockchain com uma alternativa para banco de dados. Entretanto, existem muitos cenários em que será mais vantajosa a utilização de um banco de dados tradicional. É fundamental que na escolha do blockchain, as suas propriedades sejam avaliadas de modo a responder as reais necessidades da sua aplicação (CASINO, DASAKLIS, & PATSAKIS, 2018). Desse modo, esse trabalho contribuiu para mostrar a compreensibilidade da tecnologia de maneira simplista, carecendo de uma prova de conceito mais elaborada e acoplada nos sistemas legados de empresas.

REFERÊNCIAS

ASTE, T.; TASCA, P.; MATTEO, T. D. Blockchain technologies: the foreseeable impact on society and industry. **Computer**, v. 50, n. 9, p. 18 - 28. Sept. 2017.

BANCO CENTRAL DO BRASIL. **Diagnóstico do Sistema de Pagamentos de Varejo do Brasil**. Brasília, 2015. Disponível em:

<<https://www.bcb.gov.br/htms/novaPaginaSPB/Diagnostico%20do%20Sistema%20de%20Pagamentos%20de%20Varejo%20no%20Brasil.pdf>>. Acesso em: 15 maio 2018.

BARAN, P. **On distributed communications networks**. California: The Rand Corporation, 1964.

BISWAS, K.; MUTHUKKUMARASAMY, V. Securing smart cities using blockchain technology. In: INTERNATIONAL CONFERENCE ON HIGH PERFORMANCE COMPUTING AND COMMUNICATIONS, 18.; INTERNATIONAL CONFERENCE ON SMART CITY, 14.; INTERNATIONAL CONFERENCE ON DATA SCIENCE AND SYSTEMS, 2., 2016, Sydney. **Proceedings...** IEEE: Sydney, 2017.

BRENNAN, C. **Blockchain: the trust disrupt** Credit Suisse. [s.l.], 2016. Disponível em: <<http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf>>. Acesso em: 05 de nov. 2017.

BUCHMANN, J. **Introduction to cryptography**. [s.l.]: Springer Science & Business Media, 2013.

BURGOS, A. et al. **Distributed ledger technical research in Central Bank of Brazil**. Brasília: Banco Central do Brasil, 2017. Disponível em: <https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf>. Acesso em: 12 jan. 2019.

CASINO, F., DASAKLIS, T. K., & PATSAKIS, C. (2018). **A systematic literature review of blockchain-based applications: current status, classification and open issues**. Telematics and Informatics.

CHAMBERS, S.; JOHNSTON, R.; SLACK, N. **Administração da produção**. São Paulo: Atlas, 2002.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. **IEEE Access**, [s.l.], v. 4, p. 2292-2303, May, 2016.

COASE, R. H. The nature of the firm. **Economica**, v. 4, n. 16, p. 386-405, Nov. 1937.

CULLINEN, M. **Machine to machine technologies: unlocking the potential of a \$1 trillion industry**. Washington: Carbon War Room Research & Intelligence Group, 2013.

DANNEN, C. **Introducing Ethereum and solidity: foundations of cryptocurrency and blockchain programming for beginners**. California: Apress Berkely, 2017.

DE VRIES, A. Bitcoin's growing energy problem. **Joule**, [s.l.], v. 2, n. 5, p. 801-805, May, 2018.

DIGICONOMIST. **Ethereum Energy Consumption Index (beta)**. [s.l.], 2018. Disponível em: <<https://digiconomist.net/ethereum-energy-consumption>>. Acesso em: 12 jan. 2019.

DRESCHER, D. **Blockchain básico: uma introdução não técnica em 25 passos**. São Paulo: Novatec, 2018.

ENGELMANN, F. et al. Towards an economic analysis of routing in payment channel networks. In: WORKSHOP ON SCALABLE AND RESILIENT INFRASTRUCTURES FOR DISTRIBUTED LEDGERS, 1., 2017, Las Vegas. **Proceedings...** Las Vegas, 2017.

ETHERSCAN. **Ethereum token market capitalization**. [s.l.], 2018. Disponível em: <<https://etherscan.io/tokens>>. Acesso em: 12 jan. 2019.

FALKON, S. (24 de 12 de 2017). **The Story of the DAO—Its History and Consequences**. Acesso em 15 de 12 de 2018, disponível em <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>

GLASER, F.; BEZZENBERGER, L. Beyond cryptocurrencies—a taxonomy of decentralized consensus systems. **ECIS Completed Research Papers**, [s.l.], n. 57, p. 1-18, 2015.

GOERTZEL, B.; GOERTZEL, T.; GOERTZEL, Z. The global brain and the emerging economy of abundance: mutualism, open collaboration, exchange networks and the automated commons. **Technological Forecasting and Social Change**, v. 114, p. 65-73, Jan. 2017.

GOMBRICH, E. H. **A little history of the world**. Londres: Yale University Press, 2008

GREGOR, S.; HEVNER, A. R. Positioning and presenting design science research for maximum impact. **MIS quarterly**, v. 37, n. 2, p. 337-355, Jun. 2013.

GRIGORYEV, I. **AnyLogic 7 em três dias: um curso rápido de modelagem de simulação**. Tradução de Phillipe Cavalcante. [s.l.]: The AnyLogic Company, 2018. Disponível em: <<https://www.anylogic.com/resources/books/material-de-aprendizado-em-portugues>>. Acesso em: 01 out. 2018.

GUPTA, M. **Blockchain for dummies**. [s.l.]: IBM Limited Edition, 2017.

HARDJONO, T.; SMITH, N. Cloud-based commissioning of constrained devices using permissioned blockchains. ACM INTERNATIONAL WORKSHOP ON IOT PRIVACY, TRUST, AND SECURITY, 2., 2016, Xi'an. **Proceedings...** Xi'an, 2016. p. 29-36.

HASHEMI, S. H. et al. World of empowered IoT users. In: INTERNATIONAL CONFERENCE ON INTERNET-OF-THINGS DESIGN AND IMPLEMENTATION, 1., 2016, Berlim. **Proceedings...** Berlim: IEEE Xplore, 2016. p. 13-24.

HEVNER, A. et al. Design science in information systems research. **MIS Quarterly**, v. 28, n. 1, p. 75-105, Mar. 2004.

HEVNER, A.; CHATTERJEE, S. Design science research in information systems. **Springer Science**, [s.l.], v. 28, p. 9-22, 2010.

HUCKLE, S. et al. Internet of Things, Blockchain and Shared Economy Applications. **Procedia Computer Science**, [s.l.], v. 98, p. 461-466, Sept. 2016.

HUH, S.; CHO, S.; KIM, S. Managing IoT devices using blockchain platform. INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION TECHNOLOGY (ICACT), 19., 2017, Bongpyeong. **Proceedings...** Bongpyeong, 2017.

IBM CORPORATION. **IBM blockchain proof of technology workshop**: a deeper view of blockchain technology. [s.l.:s.n.], 2016. Disponível em: < [https://www-01.ibm.com/events/www/grp/grp308.nsf/vLookupPDFs/14673529/\\$file/14673529.pdf](https://www-01.ibm.com/events/www/grp/grp308.nsf/vLookupPDFs/14673529/$file/14673529.pdf) > . Acesso em: 12 jan. 19.

LIANG, T. P.; HUANG, J. S. An empirical study on consumer acceptance of products in electronic markets: a transaction cost model. **Decision Support Systems**, v. 24, n. 1, p. 29-43, nov. 1998.

MACDONALD, T. J.; ALLEN, D. W.; POTTS, J. **Blockchains and the boundaries of self-organized economies**: predictions for the future of banking. [s.l.]: Banking Beyond Banks and Money, 2016. p. 279-296.

MANYIKA, J.; ROXBURGH, C. **The great transformer: the impact of Internet on economic growth and prosperity**. [s.l.]: McKinsey Global Institute, 2011. Disponível em: <https://www.mckinsey.com/~media/McKinsey/Industries/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.aspx>. Acesso em: 12 jan. 2019.

MARCH, S. T.; SMITH, G. F. Design and natural science research on information technology. **Decision Support Systems**, [s.l.], v. 15, n. 4, p. 251-266, Dec. 1995.

NAKAMOTO, S. **Bitcoin**: a peer-to-peer electronic cash system. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 01 dez. 2017.

NORTH, D. C. **Structure and change in economic history**. New York: W. W. Norton & Company, 1981.

NOTHEISEN, B.; CHOLEWA, J. B.; SHANMUGAM, A. P. Trading Real-World Assets on Blockchain. **Business & Information Systems Engineering**, v. 59, n. 6, p. 425-440, Dec. 2017.

OPC UNIFIED ARCHITECTURE. **Interoperability for industrie 4.0 and the internet of things**. [s.l.]: OPC Foundation, [s.d.]. Disponível em: <<https://opcfoundation.org/wp-content/uploads/2016/05/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN-v5.pdf>>. Acesso em: 16 maio 2017.

PEREIRA, C. D. A simulação na pesquisa operacional: uma revisão literária. IX EEPA - Encontro de Engenharia de Produção Agroindustrial, 9., 2015, Campo Mourão. **Anais...** Campo Mourão, 2015. Disponível em: <http://www.fecilcam.br/anais/ix_eeпа/data/uploads/3-pesquisa-operacional/3-03.pdf>. Acesso em: 24 ago. 2018.

PETRE, A., & HAI, N. (2018). **Opportunities and challenges of blockchain technology in the healthcare industry**. *Medecine sciences: M/S*, 34(10), 852-856.

POP, C. et al. Blockchain based decentralized management of demand response programs in smart energy grids. **Sensors**, [s.l.], v. 18, n. 1, E162, Jan. 2018.

PURESWARAN, V. **More than a billion intelligent, connected devices already comprise today's "Internet of Things (IoT)"**. IBM Institute for Business Value, 2014. Disponível em: <<http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings>>. Acesso em: 12 jan. 2019.

SABOUNCHI, M.; WEI, J. Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism. **IEEE Conference on Energy Internet and Energy System Integration (EI2)**, Beijing, nov. 2017.

SANTOS, E. S. **Digitalização, inovação e desigualdade: pesquisa sobre digitalização**. Rio de Janeiro: Fundação Dom Cabral, 2016. Disponível em: <https://www.fdc.org.br/professorespesquisa/nucleos/Documents/inovacao/digitalizacao/boletim_digitalizacao_fevereiro2016.pdf>. Acesso em: 16 out. 2017.

SAP BRASIL. **O que é blockchain?** [s.l.], 2018. Disponível em: <<https://www.sap.com/brazil/products/leonardo/blockchain/what-is-blockchain.html>>. Acesso em: 12 jan. 2019.

SCHWAB, K. **The fourth industrial revolution**. Crown Business, 2017.

SHARMA, P. K.; MOON, S. Y. PARK, J. H. Block-VN: a distributed blockchain based vehicular network architecture in smart city. **Journal of Information Processing Systems**, [s.l.], n. 13, p. 184-195, 2017.

SHRESTHA, A. K.; VASSILEVA, J. Towards decentralized data storage in general cloud platform for meta-products. In: INTERNATIONAL CONFERENCE ON BIG DATA AND ADVANCED WIRELESS TECHNOLOGIES, 16., 2016, Blagoevgrad. **Proceedings...** New York: Association for Computing Machinery, 2016.

SHROUF, F.; ORDIERES, J.; MIRAGLIOTTA, G. Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In: INTERNATIONAL CONFERENCE ON INDUSTRIAL ENGINEERING AND ENGINEERING MANAGEMENT, 2014, Bandar Sunway, **Proceedings...** New Jersey: IEEE, 2014.

SIIM, J. **Proof-of-Stake**: research seminar in cryptograph. 2017. Disponível em: <https://courses.cs.ut.ee/MTAT.07.022/2017_fall/uploads/Main/janno-report-f17.pdf>. Acesso em: 12 jan. 2019.

SIKORSKI, J. J.; HAUGHTON, J.; KRAFT, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. **Applied Energy**, v. 195, p. 234-246, Jun. 2017.

SKWAREK, V. Blockchains as security-enabler for industrial IoT-applications. **Asia Pacific Journal of Innovation and Entrepreneurship**, v. 11, n. 3, p. 301-311, Oct. 2017.

SWAN, M. **Blockchain**: blueprint for a new economy. Boston: O'Reilly Media, 2015.

SZABO, N. Formalizing and Securing relationships on Public Networks. **Peer-Reviewed Journal on the Internet**, Chicago, v. 2, n. 9, Sept. 1997.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain revolution**: how the technology behind bitcoin is changing money, business, and the world. New York: Penguin., 2016.

TAYLOR, S. **Agent-based modeling and simulation**. [s.l.]: Springer, 2014.

THE WORLD BANK. **Global Payment Systems Survey (GPSS)**. [s.l.], 2018. Disponível em: <<http://www.worldbank.org/en/topic/financialinclusion/brief/gpss>>. Acesso em: 12 jan. 2019.

THOMPSON, S. E.; PARTHASARATHY, S. (2006). Moore's law: the future of Si microelectronics. **Materials Today**, [s.l.], v. 9, n. 6, p. 20-25, Jun. 2006.

Tian, F. An Agri-food Supply Chain Traceability System for China Based on RFID \&Blockchain Technology. In: INTERNATIONAL CONFERENCE ON SERVICE SYSTEMS AND SERVICE MANAGEMENT, 13., 2016, Kunming. **Proceedings...** Kunming: IEEE, 2016.

TÔRRES, O. F. Elementos da teoria das filas. **Revista de Administração de Empresas**, São Paulo, v. 6, n. 20, p. 111-127, jul./set. 1996.

TURKANOVIĆ, et al. **EduCTX**: a blockchain-based higher education credit platform. [s.l.]: IEEE Access, 2018.

UNITED NATIONS GLOBAL MARKETPLACE. **Annual statistical report on UN procurement**. 2018. Disponível em: <<https://www.ungm.org/Public/ASR>>. Acesso em: 12 jan. 2019.

WILLIAMSON, O. E. The economic institutions of capitalism: firms, markets, relational contracting. In: BOERSCH, B.; ESCHEN, R. **Das summa summarum des management**: die 25 wichtigsten werke für strategie, führung und veränderung. Wiesbaden: Gabler Verlag, 2007. p. 61-75.

WU, H. et al. A distributed ledger for supply chain physical distribution visibility. **Information**, Basel, Switzerland, v. 8, n. 4, E137, nov. 2017.

XU, L. et al. Enabling the sharing economy: privacy respecting contract based on public blockchain. In: ACM WORKSHOP ON BLOCKCHAIN, CRYPTOCURRENCIES AND CONTRACTS, 17., 2017, Abu Dhabi. **Proceedings...** New York: ACM, 2017. p. 15-21.

YIN, S. et al. M2M security technology of cps based on blockchains. **Symmetry**, v. 9, n. 9, E193, Sept. 2017.

ZANINOTTO, F. (2016) The blockchain explained to web developers, part 1: the theory. Disponível em: <http://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html>. Acesso em: 12 jan. 2019.

ZHANG, Y.; WEN, J. An IoT electric business model based on the protocol of bitcoin. In: INTERNATIONAL CONFERENCE ON INTELLIGENCE IN NEXT GENERATION NETWORKS, 18., 2015, Paris. **Proceedings...** Paris: IEEE, 2015.

ZĪLE, K., & STRAZDIŅA, R. (2018). Blockchain use cases and their feasibility. *Applied Computer Systems*, 23(1), 12-20.

APÊNDICE A – Código VBA para cálculo do *hash* SHA-256

Private m_IOnBits(30)
Private m_I2Power(30)
Private K(63)
Private Const BITS_TO_A_BYTE = 8
Private Const BYTES_TO_A_WORD = 4
Private Const BITS_TO_A_WORD = 32
Sub initial()
m_IOnBits(0) = CLng(1)
m_IOnBits(1) = CLng(3)
m_IOnBits(2) = CLng(7)
m_IOnBits(3) = CLng(15)
m_IOnBits(4) = CLng(31)
m_IOnBits(5) = CLng(63)
m_IOnBits(6) = CLng(127)
m_IOnBits(7) = CLng(255)
m_IOnBits(8) = CLng(511)
m_IOnBits(9) = CLng(1023)
m_IOnBits(10) = CLng(2047)
m_IOnBits(11) = CLng(4095)
m_IOnBits(12) = CLng(8191)
m_IOnBits(13) = CLng(16383)
m_IOnBits(14) = CLng(32767)
m_IOnBits(15) = CLng(65535)

m_lOnBits(16) = CLng(131071)
m_lOnBits(17) = CLng(262143)
m_lOnBits(18) = CLng(524287)
m_lOnBits(19) = CLng(1048575)
m_lOnBits(20) = CLng(2097151)
m_lOnBits(21) = CLng(4194303)
m_lOnBits(22) = CLng(8388607)
m_lOnBits(23) = CLng(16777215)
m_lOnBits(24) = CLng(33554431)
m_lOnBits(25) = CLng(67108863)
m_lOnBits(26) = CLng(134217727)
m_lOnBits(27) = CLng(268435455)
m_lOnBits(28) = CLng(536870911)
m_lOnBits(29) = CLng(1073741823)
m_lOnBits(30) = CLng(2147483647)
m_l2Power(0) = CLng(1)
m_l2Power(1) = CLng(2)
m_l2Power(2) = CLng(4)
m_l2Power(3) = CLng(8)
m_l2Power(4) = CLng(16)
m_l2Power(5) = CLng(32)
m_l2Power(6) = CLng(64)
m_l2Power(7) = CLng(128)
m_l2Power(8) = CLng(256)
m_l2Power(9) = CLng(512)
m_l2Power(10) = CLng(1024)
m_l2Power(11) = CLng(2048)
m_l2Power(12) = CLng(4096)

m_I2Power(13) = CLng(8192)
m_I2Power(14) = CLng(16384)
m_I2Power(15) = CLng(32768)
m_I2Power(16) = CLng(65536)
m_I2Power(17) = CLng(131072)
m_I2Power(18) = CLng(262144)
m_I2Power(19) = CLng(524288)
m_I2Power(20) = CLng(1048576)
m_I2Power(21) = CLng(2097152)
m_I2Power(22) = CLng(4194304)
m_I2Power(23) = CLng(8388608)
m_I2Power(24) = CLng(16777216)
m_I2Power(25) = CLng(33554432)
m_I2Power(26) = CLng(67108864)
m_I2Power(27) = CLng(134217728)
m_I2Power(28) = CLng(268435456)
m_I2Power(29) = CLng(536870912)
m_I2Power(30) = CLng(1073741824)
K(0) = &H428A2F98
K(1) = &H71374491
K(2) = &HB5C0FBCF
K(3) = &HE9B5DBA5
K(4) = &H3956C25B
K(5) = &H59F111F1
K(6) = &H923F82A4
K(7) = &HAB1C5ED5
K(8) = &HD807AA98
K(9) = &H12835B01

K(10) = &H243185BE
K(11) = &H550C7DC3
K(12) = &H72BE5D74
K(13) = &H80DEB1FE
K(14) = &H9BDC06A7
K(15) = &HC19BF174
K(16) = &HE49B69C1
K(17) = &HEFBE4786
K(18) = &HFC19DC6
K(19) = &H240CA1CC
K(20) = &H2DE92C6F
K(21) = &H4A7484AA
K(22) = &H5CB0A9DC
K(23) = &H76F988DA
K(24) = &H983E5152
K(25) = &HA831C66D
K(26) = &HB00327C8
K(27) = &HBF597FC7
K(28) = &HC6E00BF3
K(29) = &HD5A79147
K(30) = &H6CA6351
K(31) = &H14292967
K(32) = &H27B70A85
K(33) = &H2E1B2138
K(34) = &H4D2C6DFC
K(35) = &H53380D13
K(36) = &H650A7354
K(37) = &H766A0ABB
K(38) = &H81C2C92E

K(39) = &H92722C85
K(40) = &HA2BFE8A1
K(41) = &HA81A664B
K(42) = &HC24B8B70
K(43) = &HC76C51A3
K(44) = &HD192E819
K(45) = &HD6990624
K(46) = &HF40E3585
K(47) = &H106AA070
K(48) = &H19A4C116
K(49) = &H1E376C08
K(50) = &H2748774C
K(51) = &H34B0BCB5
K(52) = &H391C0CB3
K(53) = &H4ED8AA4A
K(54) = &H5B9CCA4F
K(55) = &H682E6FF3
K(56) = &H748F82EE
K(57) = &H78A5636F
K(58) = &H84C87814
K(59) = &H8CC70208
K(60) = &H90BEFFFA
K(61) = &HA4506CEB
K(62) = &HBEF9A3F7
K(63) = &HC67178F2
End Sub
Private Function LShift(IValue, iShiftBits)

If iShiftBits = 0 Then
LShift = IValue
Exit Function
Elseif iShiftBits = 31 Then
If IValue And 1 Then
LShift = &H80000000
Else
LShift = 0
End If
Exit Function
Elseif iShiftBits < 0 Or iShiftBits > 31 Then
Err.Raise 6
End If
If (IValue And m_I2Power(31 - iShiftBits)) Then
LShift = ((IValue And m_IOnBits(31 - (iShiftBits + 1))) * m_I2Power(iShiftBits)) Or &H80000000
Else
LShift = ((IValue And m_IOnBits(31 - iShiftBits)) * m_I2Power(iShiftBits))
End If
End Function
Private Function RShift(IValue, iShiftBits)
If iShiftBits = 0 Then
RShift = IValue
Exit Function
Elseif iShiftBits = 31 Then
If IValue And &H80000000 Then
RShift = 1

Else
RShift = 0
End If
Exit Function
Elseif iShiftBits < 0 Or iShiftBits > 31 Then
Err.Raise 6
End If
RShift = (IValue And &H7FFFFFFE) \ m_I2Power(iShiftBits)
If (IValue And &H80000000) Then
RShift = (RShift Or (&H40000000 \ m_I2Power(iShiftBits - 1)))
End If
End Function
Private Function AddUnsigned(IX, IY)
Dim IX4
Dim IY4
Dim IX8
Dim IY8
Dim IResult
IX8 = IX And &H80000000
IY8 = IY And &H80000000
IX4 = IX And &H40000000
IY4 = IY And &H40000000
IResult = (IX And &H3FFFFFFF) + (IY And &H3FFFFFFF)

If IX4 And IY4 Then
IResult = IResult Xor &H80000000 Xor IX8 Xor IY8
Elseif IX4 Or IY4 Then
If IResult And &H40000000 Then
IResult = IResult Xor &HC0000000 Xor IX8 Xor IY8
Else
IResult = IResult Xor &H40000000 Xor IX8 Xor IY8
End If
Else
IResult = IResult Xor IX8 Xor IY8
End If
AddUnsigned = IResult
End Function
Private Function Ch(x, y, z)
Ch = ((x And y) Xor ((Not x) And z))
End Function
Private Function Maj(x, y, z)
Maj = ((x And y) Xor (x And z) Xor (y And z))
End Function
Private Function S(x, n)
S = (RShift(x, (n And m_IOnBits(4))) Or LShift(x, (32 - (n And m_IOnBits(4)))))
End Function
Private Function R(x, n)

R = RShift(x, CInt(n And m_IOnBits(4)))
End Function
Private Function Sigma0(x)
Sigma0 = (S(x, 2) Xor S(x, 13) Xor S(x, 22))
End Function
Private Function Sigma1(x)
Sigma1 = (S(x, 6) Xor S(x, 11) Xor S(x, 25))
End Function
Private Function Gamma0(x)
Gamma0 = (S(x, 7) Xor S(x, 18) Xor R(x, 3))
End Function
Private Function Gamma1(x)
Gamma1 = (S(x, 17) Xor S(x, 19) Xor R(x, 10))
End Function
Private Function ConvertToWordArray(sMessage)
Dim IMessageLength
Dim INumberOfWords
Dim IWordArray()
Dim IBytePosition
Dim IByteCount
Dim IWordCount
Dim IByte
Const MODULUS_BITS = 512

Const CONGRUENT_BITS = 448
IMessageLength = Len(sMessage)
$\text{INumberOfWords} = (((\text{IMessageLength} + ((\text{MODULUS\_BITS} - \text{CONGRUENT\_BITS}) \setminus \text{BITS\_TO\_A\_BYTE})) \setminus (\text{MODULUS\_BITS} \setminus \text{BITS\_TO\_A\_BYTE})) + 1) * (\text{MODULUS\_BITS} \setminus \text{BITS\_TO\_A\_WORD}))$
ReDim IWordArray(INumberOfWords - 1)
IBytePosition = 0
IByteCount = 0
Do Until IByteCount >= IMessageLength
IWordCount = IByteCount \ BYTES_TO_A_WORD
$\text{IBytePosition} = (3 - (\text{IByteCount} \bmod \text{BYTES\_TO\_A\_WORD})) * \text{BITS\_TO\_A\_BYTE}$
IByte = AscB(Mid(sMessage, IByteCount + 1, 1))
$\text{IWordArray}(\text{IWordCount}) = \text{IWordArray}(\text{IWordCount}) \text{ Or } \text{LShift}(\text{IByte}, \text{IBytePosition})$
IByteCount = IByteCount + 1
Loop
IWordCount = IByteCount \ BYTES_TO_A_WORD
$\text{IBytePosition} = (3 - (\text{IByteCount} \bmod \text{BYTES\_TO\_A\_WORD})) * \text{BITS\_TO\_A\_BYTE}$

IWordArray(IWordCount) = IWordArray(IWordCount) Or LShift(&H80, IBytePosition)
IWordArray(INumberOfWords - 1) = LShift(IMessageLength, 3)
IWordArray(INumberOfWords - 2) = RShift(IMessageLength, 29)
ConvertToWordArray = IWordArray
End Function
Public Function SHA256(sMessage)
Dim HASH(7)
Dim M
Dim W(63)
Dim a
Dim b
Dim c
Dim d
Dim e
Dim f
Dim g
Dim h
Dim i
Dim j
Dim T1
Dim T2
Call initial
HASH(0) = &H6A09E667
HASH(1) = &HBB67AE85
HASH(2) = &H3C6EF372

HASH(3) = &HA54FF53A
HASH(4) = &H510E527F
HASH(5) = &H9B05688C
HASH(6) = &H1F83D9AB
HASH(7) = &H5BE0CD19
M = ConvertToWordArray(sMessage)
For i = 0 To UBound(M) Step 16
a = HASH(0)
b = HASH(1)
c = HASH(2)
d = HASH(3)
e = HASH(4)
f = HASH(5)
g = HASH(6)
h = HASH(7)
For j = 0 To 63
If j < 16 Then
W(j) = M(j + i)
Else
W(j) = AddUnsigned(AddUnsigned(AddUnsigned(Gamma1(W(j - 2)), W(j - 7)), Gamma0(W(j - 15))), W(j - 16))
End If
T1 = AddUnsigned(AddUnsigned(AddUnsigned(AddUnsigned(h, Sigma1(e)), Ch(e, f, g)), K(j)), W(j))
T2 = AddUnsigned(Sigma0(a), Maj(a, b, c))

h = g
g = f
f = e
e = AddUnsigned(d, T1)
d = c
c = b
b = a
a = AddUnsigned(T1, T2)
Next
HASH(0) = AddUnsigned(a, HASH(0))
HASH(1) = AddUnsigned(b, HASH(1))
HASH(2) = AddUnsigned(c, HASH(2))
HASH(3) = AddUnsigned(d, HASH(3))
HASH(4) = AddUnsigned(e, HASH(4))
HASH(5) = AddUnsigned(f, HASH(5))
HASH(6) = AddUnsigned(g, HASH(6))
HASH(7) = AddUnsigned(h, HASH(7))
Next
SHA256 = LCase(Right("00000000" & Hex(HASH(0)), 8) & Right("00000000" & Hex(HASH(1)), 8) & Right("00000000" & Hex(HASH(2)), 8) & Right("00000000" & Hex(HASH(3)), 8) & Right("00000000" & Hex(HASH(4)), 8) & Right("00000000" & Hex(HASH(5)), 8) & Right("00000000" & Hex(HASH(6)), 8) & Right("00000000" & Hex(HASH(7)), 8))
End Function
Public Function encrypt(x, Optional fmt As String) As String

Dim x1 As String
x1 = WorksheetFunction.Text(x, fmt)
encrypt = SHA256(x1)
End Function

APÊNDICE B – Macro para simular a mineração do blockchain

Sub Mining()
tempo = Now()
Cells(2, 2) = 0
Do While Cells(2, 10) <> 0
Cells(2, 2) = Cells(2, 2) + 1
Loop
Cells(2, 11) = Now() - tempo
End Sub
Sub Rodar()
For i = 400 To 500
Cells(2, 1) = i

$\text{Cells}(2, 3) = \text{Cells}(i + 5, 3)$
$\text{Cells}(2, 4) = \text{Cells}(i + 5, 4)$
Call Mining
$\text{Cells}(i + 5, 2) = \text{Cells}(2, 2)$
$\text{Cells}(i + 5, 5) = \text{Cells}(2, 5)$
$\text{Cells}(i + 5, 11) = \text{Cells}(2, 11)$
Next i
End Sub

APÊNDICE C – Código do contrato inteligente escrito em *Solidity*

```
pragma solidity ^0.4.18;

contract compra {

    event PedidoCompra (address vendedor, int256 NSU, int256 Quantidade, int256 Unidade,
int256 Preco, int256 Tax);

    event Fabricar (int256 NSU, int256 Quantidade, int256 Unidade);

    event EmitirNota (address comprador, int256 NSU, int256 Quantidade, int256 Unidade,
int256 Preco, int256 Tax);

    event ReceberProduto (string hash);

    event ReceberNota (address vendedor, int256 NSU, int256 Quantidade, int256 Unidade,
int256 Preco, int256 Tax);

    function comprar (address vendedor, int256 NSU, int256 Quantidade, int256 Unidade,
int256 Preco, int256 Tax) public {

        emit PedidoCompra (vendedor, NSU, Quantidade, Unidade, Preco,Tax);}

    function produzir (address comprador, int256 NSU, int256 Quantidade, int256 Unidade,
int256 Preco, int256 Tax) public {

        emit Fabricar (NSU, Quantidade, Unidade);

        emit EmitirNota (comprador, NSU, Quantidade, Unidade, Preco,Tax);}

    function receber (address vendedor, string hash, int256 NSU, int256 Quantidade, int256
Unidade, int256 Preco, int256 Tax, int256 NSU_recebido, int256 Quantidade_recebida)
public{

        emit ReceberProduto (hash);

        assert (NSU_recebido==NSU);

        assert (Quantidade_recebida==Quantidade);

        emit ReceberNota (vendedor, NSU, Quantidade, Unidade, Preco,Tax);

    }}
}
```