Carlos Hatus Damasceno Borges

TilliT distribuert: Uma proposta de sistema de vendas digitais *peer to peer* seguras baseada em *blockchain*

Vitória da Conquista/BA

2019

Carlos Hatus Damasceno Borges

TilliT distribuert: Uma proposta de sistema de vendas digitais *peer to peer* seguras baseada em *blockchain*

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Ciência da Computação na Universidade Estadual do Sudoeste da Bahia – UESB.

Universidade Estadual do Sudoeste da Bahia – UESB

Curso de Bacharelado em Ciência da Computação

Departamento de Ciências Exatas e Tecnológicas

Orientador: Prof. Dr. Hélio Lopes dos Santos

Vitória da Conquista/BA

2019

Carlos Hatus Damasceno Borges

TilliT distribuert: Uma proposta de sistema de vendas digitais *peer to peer* seguras baseada em *blockchain*/ Carlos Hatus Damasceno Borges. – Vitória da Conquista/BA, 2019

60 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. Hélio Lopes dos Santos

Trabalho de Conclusão de Curso (Graduação)
Universidade Estadual do Sudoeste da Bahia – UESB
Curso de Bacharelado em Ciência da Computação
Departamento de Ciências Exatas e Tecnológicas, 2019.

1. Blockchain. 2. Ethereum. 3. Smart Contract. I. Prof. Dr. Hélio Lopes dos Santos II. Universidade Estadual do Sudoeste da Bahia. III. Curso de Ciência da Computação. IV. TilliT distribuert: Uma proposta de sistema de vendas digitais *peer to peer* seguras baseada em *blockchain*

Carlos Hatus Damasceno Borges

TilliT distribuert: Uma proposta de sistema de vendas digitais *peer to peer* seguras baseada em *blockchain*

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Ciência da Computação na Universidade Estadual do Sudoeste da Bahia – UESB.

Trabalho aprovado. Vitória da Conquista/BA, 30 de agosto de 2019:

Prof. Dr. Hélio Lopes dos Santos
Orientador

Profa. Dra. Maísa Soares dos Santos Lopes
Convidada

Prof. Dr. Roque Mendes Prado Trindade
Convidado

Vitória da Conquista/BA
2019

Trabalho dedicado a Késsio, Roseleia e Robério.

Agradecimentos

Finalizo mais uma etapa tão sonhada, concluir o curso ao qual passei a admirar desde o ensino médio. Sou grato por todos os momentos que passei desde o dia da minha matrícula, todas as pessoas que conheci, todos os assuntos que tive a oportunidade de estudar, todos os professores que me guiaram neste caminho.

Agradeço primeiramente a Deus, sem o qual não estaria aqui. Ele que esteve comigo e me ajudou em todos os momentos bons ou ruins. Nas dificuldades me fez forte, nas provas difíceis me deu forças para estudar mais, no possível me orientou, no impossível me permitiu enxergar a sua atuação.

Agradeço a minha mãe Roseleia, ela me incentivou a estudar todos os dias de que me lembro até hoje, me ensinou valores e princípios.

Agradeço a meu pai Robério, ele não deixou faltar nada para que eu me preocupasse apenas em estudar, foi uma honra ter trabalhado com ele nas férias do curso.

Agradeço ao meu irmão Carlos Késsio pelo apoio e pela disposição em sempre ajudar. Agradeço aos meus avós Nilton e Cleusa que sempre me apoiaram e colaboraram para que eu estudasse além do suficiente.

Agradeço a todos os professores do do curso de Ciência da Computação da UESB, pessoas que ensinam mais que as aulas ministradas, em especial ao meu orientador o Prof. Dr. Hélio Lopes ao qual admiro a dedicação e o empenho pelo curso e pelos alunos. Agradeço também a profa. Dra. Maísa Soares, profa. Dra. Alzira Ferreira, o prof. Dr. Roque Trindade, o prof. Me. Stênio Longo, a profa. Dra. Cátia Mesquita, o prof. Dr. Marco Antonio, e o prof. Dr. Marlos Marques. Agradeço ao colegiado representado por Celina Pereira que nos ajudou em todos os momentos, e tornou possível este momento.

Agradeço a minha namorada Vanessa pelo apoio, pelos conselhos nas decisões difíceis e por todos os momentos difíceis em que esteve comigo.

Agradeço aos meus amigos Wali Queiroz e Rodrigo Silva que estiveram comigo todo o curso, desde o primeiro dia até hoje, no trabalho e nesta etapa ao qual concluímos juntos.

Agradeço aos meus colegas de curso Yan Kaic, Matheus Thiago, Iago, João Vitor, Leandro, Bruna, e aos demais que conviveram comigo e ajudaram com conselhos e orientações.

Agradeço aos meus colegas de trabalho que conheci no curso, Helber Henrique e Lucas Badaró. Também a toda a equipe do NTI que me ajudou a crescer profissionalmente.

"Qualquer um pode escrever código que um computador pode entender.

Bons programadores escrevem código que seres humanos podem entender."

(Martin Fowler)

Resumo

O e-commerce está em pleno crescimento no mundo, o ramo que se destaca é o do marketplace C2C onde pessoas podem comprar e vender diretamente de/para outras pessoas. Este tipo de comercio enfrenta grandes problemas relacionados a confiança necessária para se realizar uma transação, aos riscos de golpe e a segurança dos dados do usuário. Como alternativa para contornar esta situação as grandes empresas apostam na centralização das operações em um terceiro confiável, geralmente atrelado ao sistema. Essa alternativa gera custos que são repassados aos produtos. Como contra proposta há a alternativa de melhorar o modelo descentralizado que atualmente repassa a responsabilidade da segurança da operação para os usuários envolvidos. Essa melhoria é apresentada através do projeto de um sistema de vendas P2P baseado em Blockchain, no qual as transações ocorrem guiadas por um Smart Contract sob a plataforma Ethereum. O Smart Contract proporciona uma computação multilateral segura e justa na qual o usuário se compromete a agir honestamente ou ser penalizado monetariamente.

Palavras-chave: Blockchain, Ethereum, Smart Contract.

Abstract

E-commerce is growing fast in the world, the branch that stands out is the C2C marketplace where people can buy and sell directly from/to other people. This type of trade faces major issues related to the confidence required to perform a transaction, the scam risks and the security of user data. As an alternative to get around this situation large companies bet on centralizing operations in a reliable third party, usually tied to the system. This alternative generates costs that are passed on to the products. As against proposal there is the alternative of improving the decentralized model that currently passes the responsibility of the operation security to the users involved. This improvement is presented through the project of a Blockchain based P2P sales system, in which transactions take place guided by a Smart Contract under the Ethereum platform. Smart Contract provides safe and fair multilateral computing in which the user commits to act honestly or be penalized monetarily.

Keywords: Blockchain, Ethereum, Smart Contract

Lista de ilustrações

Lista de algoritmos

Lista de abreviaturas e siglas

B2C: *Business to Consumer*

C2C: *Consumer to Consumer*

EVM: *Ethereum virtual machine*

FMCG: *Fast moving consumer goods*

ICO: *Initial Coin Offering*

P2P: *Peer to Peer*

Sumário

Parte I

Preparação da pesquisa

1 Introdução

1.1 Contextualização

O comércio eletrônico, comércio realizado através da internet, tem ganhado cada vez mais espaço no cotidiano das pessoas e tem alcançado números expressivos na movimentação financeira gerada por este setor da economia. Segundo relatório da Ebit e Nielsen (2018b), empresa que certifica a reputação de lojas virtuais e empresa de análise de dados relacionados ao consumo respectivamente, o e-commerce de modo geral "retornou o crescimento de dois dígitos no primeiro semestre de 2018" (EBIT; NIELSEN, 2018b, p. 8).

> Mesmo em um ano turbulento, com eventos como a Copa do Mundo, eleições, alta do dólar e os impactos da Greve dos Caminhoneiros, o comércio eletrônico brasileiro manteve a curva de crescimento em 2018 e registrou faturamento de R$53,2 bilhões, alta nominal de 12%, comparado a 2017. (EBIT; NIELSEN, 2019, p. 17)

O mesmo relatório da Ebit e Nielsen (2018b) afirma que no Brasil em 2017 houve uma alta de 20%, comparado com 2016, no mercado de Digital Commerce que movimentou cerca de R$112,2 bilhões. O termo Digital Commerce refere-se ao comércio eletrônico tradicional acrescido das áreas de serviços e de turismo que também realizam negócios através da internet e que tem alcançado grandes resultados no Brasil. Em um relatório anterior afirmava que "o faturamento do comércio eletrônico foi de R$ 47,7 bilhões em 2017. O número representa um crescimento nominal de 7,5% em relação a 2016, quando foram registrados R$ 44,4 bilhões."(EBIT; NIELSEN, 2018a, p. 16)

> Ao somarmos a esse mercado os outros setores do Digital Commerce, que agrega venda de produtos novos e usados de empresas para consumidores (B2C) e de consumidores para consumidores (C2C), além de serviços (turismo, locação de veículos e Ingressos), verificamos um volume financeiro de R$ 112,19 bilhões. (EBIT; NIELSEN, 2018b, p. 9)

Seguindo as tendências do comércio digital, houve uma popularização de um modelo de negócios chamado marketplace onde vários vendedores menores se juntam em uma única plataforma de vendas pertencente a um grande e-commerce para realizar suas vendas e alcançar um público maior. Sobre isto o relatório da Ebit e Nielsen (2018b) chega a afirmar que "O segmento de marketplaces de produtos novos e usados teve um crescimento nominal de 62,4%, no ano anterior. Ao passo que esse setor em 2016 representava 16,9% do mercado de Digital Commerce, em 2017 sua participação foi correspondente a 22,9%." (EBIT; NIELSEN, 2018b, p. 22) Com ano anterior referindo-se ao ano de 2017.

> Juntos, os marketplaces B2C (apenas de produtos novos) e os que são B2C e C2C (com produtos novos ou usados e artesanato) representam um share de 65,4% do Digital Commerce. E a cada ano, aumenta a lista de e-commerces que migram para o modelo de marketplace, ou seja, sites que permitem a venda de outros lojistas na mesma plataforma. (EBIT; NIELSEN, 2018b, p. 22)

Todo este crescimento evidencia que as negociações na internet têm migrado para ambientes considerados mais seguros e protegidos, como é o caso dos grandes marketplaces (Amazon, eBay, Mercado Livre, Olx e outros). Eles agrupam vários vendedores em suas plataformas, o que garante ao consumidor uma segurança e confiabilidade que não encontraria caso negociasse direto com um dos vendedores sem o ambiente do marketplace. A confiança e a sensação de segurança estão diretamente ligadas ao consumo dos produtos e serviços.

Assim para manter tais aspectos de confiabilidade e segurança nos seus sistemas de vendas as plataformas optam por uma abordagem para prevenir e solucionar os possíveis riscos. Esta abordagem se concentra numa autoridade central (um terceiro confiável), no caso dos grandes marketplaces atrelada ao próprio sistema, que gerencia e faz o intermédio das negociações servindo de mediador entre comprador e vendedor. Recolhendo grande quantidade de informações de ambos para que se possa identificar bem cada parte envolvida com o intuito de minimizar fraudes podendo ser utilizadas no caso de futuras demandas ou como determinarem os termos de uso da plataforma.

Das que utilizam esta abordagem, em sua maioria baseiam-se na confirmação da entrega do produto aliada a retenção do valor pago como medidas de prevenção de golpes. Tais medidas são úteis para mercadorias tangíveis, aquelas que podem ser entregues por uma transportadora ou pelo correio, mas se tornam completamente inúteis quando se trata de produtos digitais intangíveis.

Há uma segunda abordagem utilizada principalmente no seguimento de vendas C2C onde ocorrem vendas de pessoa física para pessoa física. Esta abordagem é marcada pela ausência de uma autoridade central e pela a transferência de responsabilidade pelo sucesso da transação para o usuário. Uma abordagem descentralizada, onde a própria plataforma de vendas dá a liberdade de que o vendedor e o comprador realizem seus negócios sem a supervisão direta do sistema, fazendo apenas a ligação entre quem quer vender com quem deseja comprar.

Para minimizar os possíveis golpes o sistema quantifica uma série de informações sobre cada usuário a fim de avaliar com uma "reputação" boa ou ruim. A reputação por si só não evita golpes, mas dá ao usuário do sistema um parâmetro para decidir se é arriscado ou não para ele entrar em uma negociação com outro usuário. A grande maioria dos sistemas atuais utilizam a primeira abordagem, funcionando como autoridade central e definindo regras rígidas que todos os usuários, tanto vendedores quanto compradores,

devem segui-las a fim de evitar riscos e fraudes. Como exemplos de plataformas de vendas que utilizam esta abordagem temos a Amazon, o eBay, o Mercado Livre, entre outros.

Em contrapartida o Olx (Sistema que lidera o mercado global de marketplace C2C[1]) utiliza o modelo descentralizado apenas parcialmente, retirando a autoridade central da maioria de suas negociações possíveis mediando apenas as que realizarem pagamentos por meio da plataforma, opção ainda em testes que o tornaria uma autoridade central para a mediação das transações. A retirada da autoridade central deixa o sistema à mercê da confiança que o comprador deposita no vendedor e vice-versa, mesmo que esta seja alimentada com a reputação calculada pelo sistema é uma relação frágil que pode facilmente ser quebrada.

> O comércio pela Internet tem se tornado quase exclusivamente construído sobre instituições financeiras servindo como intermediários confiáveis para processar os pagamentos eletrônicos. Enquanto o sistema funciona bem o suficiente para a maioria das transações, ele sofre da fraqueza inerente do modelo baseado em confiança. (NAKAMOTO, 2008)

A tendência da centralização dos negócios em grandes instituições traz questionamentos sobre esta ser a única alternativa para a confiabilidade das relações de compra e venda, mesmo em situações onde a liberdade é essencial e característico como no caso das relações comerciais C2C. Portanto, surge a necessidade de se melhorar o modelo descentralizado sem que este se torne um modelo de autoridade central, mas que tenha uma alta margem de segurança. Suficiente para realizar negociações e onde se possa garantir que na maioria das vezes haverá uma computação justa sem a necessidade de um mediador e que nas demais vezes uma saída será encontrada para que o número de fraudes seja atenuado, mantendo assim a liberdade da negociação direta entre os usuários.

Essa descentralização, de modo geral, ocasionaria uma série de vantagens econômicas aos usuários. Além de permitir uma maior variedade de produtos que por serem classificados como intangíveis não podem ser legalmente comercializados na maioria dos ambientes tradicionais. Como é o caso de serviços, softwares, streams, moedas digitais, arquivos de mídia, projetos digitais, documentos, imagens, cursos, shows, etc. Tais produtos poderiam ser comercializados em uma rede descentralizada além dos produtos tradicionais.

A confiança está virando um produto caro com o modelo centralizador, o custo agregado de cada transação intermediada pela autoridade central mais a margem de lucro pela intermediação é muitas vezes repassada pelo vendedor em busca de uma maior porcentagem de lucro sobre o produto. Os custos repassados ao consumidor pela confiança agregada pela autoridade central praticamente inexistem com um modelo de negócios distribuído onde, no lugar de uma autoridade central, a comunidade de usuários atesta e agrega a confiabilidade do sistema. No lugar de uma série de informações pessoais uma

[1] https://portalolx.olx.com.br/quem-somos/

reputação construída pelas ações dentro da rede e que quanto maior, melhores as chances de se realizar um bom negócio. E se mesmo assim ocorrer algum contratempo a comunidade pode apontar uma solução.

1.2 Objetivos

Observa-se os avanços do e-commerce no Brasil e no mundo, o surgimento a cada dia de novos marketplaces, a tendência crescente de centralização inclusive para as transações C2C, as notícias cada vez mais repetidas de vazamentos de dados de clientes e de golpes através de vendas realizadas pela internet, a popularização das criptomoedas e os indícios da popularização eminente do seu uso comercial. Todos esses pontos desenham a necessidade de se propor formas alternativas a centralização da confiança em grandes empresas e instituições fechadas, formas de comprar e vender sem expor os seus dados e uma forma de se garantir que a negociação será justa para todos os envolvidos.

A segurança dos dados é algo que tem estado no foco dos usuários. Mas além disso a confiança centralizada tem sido um atrativo para os grandes marketplaces que continuam a cobrar altas taxas pelo seu uso. Neste cenário há espaço para uma solução descentralizada, que ofereça a oportunidade de pessoas negociarem diretamente entre si com segurança sem a necessidade de intermediários.

1.2.1 Objetivo geral

Apresentar a problemática da segurança e da confiança nas vendas online de consumidor para consumidor e propor uma solução descentralizada baseada na tecnologia blockchain que implemente a justiça computacional como alternativa a relação de confiança centralizada.

1.2.2 Objetivos específicos

Apresentar o projeto de um sistema de e-commerce descentralizado que implementa o conceito de confiança distribuída.

Definir as principais funções necessárias para um Smart Contract que implemente o conceito de justiça computacional.

1.3 Metodologia

A metodologia adotada neste trabalho é a pesquisa exploratória, onde o objetivo é alcançar uma maior familiaridade com o tema abordado, tal objetivo foi atingido através

do estudo de publicações relacionadas ao tema e da análise e observação dos modelos de vendas atuais.

1.4 Organização do trabalho

Este trabalho vem dividido em capítulos para uma melhor apresentação do conteúdo e está organizado da seguinte forma: O capítulo 1 apresenta a contextualização do tema e as bases para a idealização deste trabalho; O capítulo 2 apresenta os conceitos e as definições que serão utilizadas ao longo do trabalho; O capítulo 3 apresenta as características principais do projeto da plataforma de vendas apresentada como tema central deste trabalho; O capítulo 4 encerra as considerações do trabalho, apresentando as possibilidades de trabalhos futuros.

Parte II

Referenciais teóricos

2 Referenciais teóricos

2.1 Considerações Iniciais

Este capítulo apresenta as bases teóricas para este trabalho e os principais assuntos relacionados ao seu desenvolvimento, com o objetivo de compreender os pontos principais abordados pelo projeto proposto no capítulo 3.

2.2 Comércio eletrônico

O comércio eletrônico tem se expandido ao longo dos anos junto com o acesso á internet e hoje já ocupa um importante espaço na economia mundial. Não está limitado apenas a compra e venda de produtos, ele abrange também os pagamentos através de meios eletrônicos e os serviços prestados através da internet, como por exemplo pagamento pelos serviços de stream de músicas ou filmes.

O avanço significativo do comércio eletrônico traz diversas vantagens e comodidades. Seus benefícios para os usuários são vários, dentre eles citamos alguns como a comodidade de realizar suas atividades (compras, vendas, pagamentos, trocas) sem ter de se deslocar de seu ambiente; com um maior poder de comparação e de escolha para o cliente que pode verificar os preços em concorrentes antes de fechar um negócio. Disponibilidade de horário ilimitada para as compras (útil para quem não tem tempo de ir as lojas físicas). Acesso a inúmeras informações antes de se decidir pela compra. Entre outras vantagens.

Uma fatia importante deste setor da economia é o Digital Commerce que, segundo Ebit e Nielsen (2018b), movimentou R$112,2 bilhões em 2017, alta de 20% ante 2016. Este termo inclui os "setores online de turismo; ingressos (de shows, cinema e eventos esportivos); e marketplaces de produtos novos e usados entre empresas e consumidores (B2C) e de consumidores para consumidores (C2C)." (EBIT; NIELSEN, 2018b, p. 20), já o termo e-commerce se refere aos negócios entre empresas e consumidores (B2C) com foco nas vendas de bens de consumo.

2.2.1 B2C (Business-to-consumer)

Modelo de negócios tradicional entre empresas e consumidores, "este modelo envolve as operações de varejo entre empresas e consumidores individuais, a empresa disponibiliza aos consumidores seus bens, produtos e serviços sendo o pagamento feito eletronicamente." (SOARES; SOUSA, 2018)

O modelo é utilizado pela maioria dos compradores, um ambiente dominado pelas grandes empresas do setor devido a sensação de confiança gerada pela possibilidade de saber com quem se está negociando realmente, a possibilidade de pesquisar informações da empresa e saber como foi avaliada anteriormente por outros clientes que realizaram negócios com esta empresa.

> Neste tipo de comércio eletrônico, a troca de informações é essencial para criar um relacionamento entre consumidor e o varejista eletrônico, sendo necessário capturar as informações do consumidor desde o acesso inicial até o momento que deixa o site da loja virtual, independente de concluir a compra ou não. (CORDEIRO, 2016, p. 27)

Os negócios são centralizados de maneira que a empresa recolhe informações de cada usuário para se proteger de possíveis golpes e fraudes que eventualmente possam ser realizados por clientes. Estes por sua vez buscam realizar negócios em sites que confiam por terem recebido boas recomendações ou por experiências anteriores, deixando de lado sites menos conhecidos.

Na busca por espaço nas vendas e com a possibilidade de se apresentarem ao cliente sob a imagem de uma grande empresa os marketplaces tem avançado sobre o e-commerce mundial. Segundo Ebit e Nielsen (2018b) a concentração de vendas nos marketplaces é uma tendência mundial principalmente nos Estados Unidos, China e Europa.

2.2.2 C2C (Consumer-to-consumer)

Modelo de negócios de consumidores para consumidores. Os produtos não são vendidos por empresas registradas mas sim diretamente por outros consumidores que anunciam nos marketplaces ou redes sociais.

> O C2C consiste nas vendas realizadas entre indivíduos que ora são compradores, ora vendedores, intermediados por plataformas virtuais que promovem essas interações e que podem, ou não, lucrar através delas. (KOHN; KRUEL, 2016)

Considerado mercado informal por, em sua maioria, serem produtos sem emissão de nota fiscal pelo vendedor por se tratar de uma pessoa física sem CNPJ. Este modelo ganha espaço a medida que os empregos formais se tornam escassos se tornando até a única fonte de renda de várias pessoas. De acordo com este ponto de vista Kohn e Kruel (2016) afirmam que:

> Apesar da sua informalidade, uma vez que ocorre entre pessoas físicas, vem crescendo exponencialmente e ganhando espaço em novos canais de comunicação, especialmente nas mídias sociais, de forma acelerada e conquistando muitos adeptos, tanto vendedores como compradores. (KOHN; KRUEL, 2016)

Apesar do grande crescimento deste mercado, não são todos os marketplaces que aceitam vendedores pessoa física. A grande maioria exige CNPJ para realizar vendas, algumas exceções são, Mercado Livre, eBay, Amazon, Olx, etc.

2.2.3 Marketplaces

Um modelo de negócios onde um site maior abre espaço para agrupar lojas menores e até vendedores do tipo pessoa física em sua própria plataforma de vendas, segundo Cordeiro (2016, p. 34) uma plataforma de comércio eletrônico consiste num sistema responsável por gerenciar e pela visualização dos itens da loja virtual na internet. não se limitando apenas ao site mas expandindo sua atuação para muito além do que é visível ao consumidor. O Marketplace permite que outras lojas, sellers, realizem vendas em seu site recebendo uma participação e oferecendo em troca além da marca, a confiança que os clientes já possuem em comprar nesta loja virtual.

> O modelo, que está em franca expansão, tem sua popularidade atrelada especialmente a três fatores principais: A crise político-econômica brasileira impulsionou a busca por alternativas de consumo, como os marketplaces. E à medida que esse tipo de e-commerce oferece uma gama maior de fornecedores e produtos, os preços tornam-se mais competitivos e oferecem mais vantagens e variedades para os consumidores. (EBIT; NIELSEN, 2018b)

Assim tanto clientes como vendedores conseguem vantagens. Os vendedores ganham a confiança dos clientes de maneira mais fácil graças ao marketplace e os clientes conseguem uma variedade maior de ofertas sem ter que procurar muito ou se arriscar em sites desconhecidos.

> Marketplace fornece as ferramentas necessárias para os sellers, o modelo igualmente mostrou-se vantajoso para novos vendedores formais e informais para venda de produtos novos ou usados. Desta forma, não necessariamente o vendedor precisa despender esforço e investimento para estruturar seu próprio e-commerce com maior escalabilidade. (EBIT; NIELSEN, 2018b)

Alguns exemplos de marketplaces são: Amazon[1], B2W[2] (responsável pelos sites Americanas[3], Shoptime[4] e Submarino[5]), Magazine Luiza[6], Netshoes[7], Mercado Livre[8], OLX[9] entre inúmeros outros.

[1] https://www.amazon.com.br/
[2] https://www.b2wmarketplace.com.br/v3/
[3] https://www.americanas.com.br/
[4] https://www.shoptime.com.br/
[5] https://www.submarino.com.br/
[6] https://marketplace-vendamais.magazineluiza.com.br/
[7] https://www.netshoes.com.br/marketplace
[8] https://www.mercadolivre.com.br/
[9] https://www.olx.com.br/

2.3 Breve análise dos marketplaces C2C atuais

Existem atualmente vários sistemas que atuam com o modelo de negócios C2C proporcionando liberdade aos usuários de realizarem suas transações, com ou sem mediador, dentre eles destacamos apenas alguns.

2.3.1 eBay e Mercado Livre

O eBay é considerado o primeiro site de leilões na internet que iniciou suas atividades no ano de 1995[10]. Sendo um site de leilões, os interessados em comprar algum produto anunciado por outro usuário faziam um lance, ou seja, uma proposta de preço para o produto e o vendedor selecionava a melhor. No entanto, com o passar do tempo se tornou popular uma nova forma de precificação, o preço passou a ser fixo e determinado previamente pelo vendedor do produto.

Semelhante ao eBay, o Mercado livre iniciou no ano de 1999 na Argentina com o objetivo de ser também um site de leilões na internet. Hoje ele é o maior da américa latina[11]. Atualmente conta com a maioria dos seus anúncios com preço fixo, mas ainda mantém o sistema de leilão. E tem alcançado cada vez mais resultados no mercado brasileiro que "Impulsionado pela expansão do Mercado Livre, o faturamento proveniente das vendas via marketplaces, incluindo produtos novos e usados, atingiu R$ 73,4 bilhões em 2017, alta de 21,9%."(EBIT; NIELSEN, 2018a).

Ambos os sistemas têm a possibilidade de vendas sem intermédio da plataforma. Mas recomendam o uso da plataforma para mediar tanto as negociações quanto o pagamento, e ainda a entrega do produto, como medidas para agregar segurança e confiabilidade aos usuários. Quando a plataforma intermedia o pagamento ela realiza a retenção do valor até que seja constatada a entrega do produto ao comprador, só então o vendedor recebe o valor pago pelo produto.

O eBay cobra uma taxa de 10% sobre o valor final de cada venda[12]. Já o Mercado livre possui um plano gratuito de 5 vendas por ano para produtos novos ou 20 vendas anuais de produtos usados, nos demais casos as tarifas vão de 11% a 16%[13].

2.3.2 Amazon

A Amazon, empresa criada no ano de 1994, desde o início se desenvolveu para o comércio eletrônico, ela se auto denomina criadora do conceito de marketplace[14] que

[10] https://www.ebayinc.com/company/our-history/
[11] https://ideias.mercadolivre.com.br/sobre-mercado-livre/tudo-o-que-voce-precisa-saber-sobre-o-mercado-livre/
[12] https://www.ebay.com/pages/br/help/sell/fees.html#totalamount
[13] https://www.mercadolivre.com.br/ajuda/quanto-custa-vender-um-produto_1338
[14] https://services.amazon.com.br/

foi iniciado no ano 2000. Nesta época a empresa passou a permitir que lojas menores anunciassem e realizassem vendas através do seu site pagando uma taxa por cada venda realizada.

Hoje está entre as maiores empresas do mundo, dominando grande parte da movimentação do comércio eletrônico. Segundo Ebit e Nielsen (2018b) "Nos EUA a participação da Amazon no total das vendas virtuais é superior a 40%". Seu sistema de vendas é completamente centralizado, a plataforma gerencia cada negociação proporcionando aos usuários e vendedores uma maior segurança. Possui regras rígidas quanto aos produtos que podem ser comercializados e ao cadastro de vendedores, que também podem ser pessoa física. Na Amazon os vendedores pagam uma comissão por cada item vendido, comissões que variam de 11% a 20% a depender da categoria do item[15].

2.3.3 Olx

A plataforma Olx afirma ser um ambiente de vendas online onde "Comprador e vendedor têm total controle em suas transações, decidindo juntos a melhor forma de fechar negócio."[16]. Neste modelo há uma completa liberdade de negociação e pagamento que não é intermediada pelo sistema, afirmando que qualquer transação e comunicação é de exclusiva responsabilidade das partes e não é da competência da plataforma sugerir qualquer vendedor ou meio de pagamento, recomendando apenas que o usuário sempre analise o anúncio do produto/serviço em que está interessado, assim como a descrição.[17]

Dessa forma o sistema apenas apresenta os anúncios, deixa a cargo do comprador escolher aquele que mais despertou a sua atenção. A confiança é mantida através do cadastro único de cada usuário, que tem seus dados verificados pelo sistema antes de iniciar sua utilização, e também da penalização dos usuários que tiverem conduta inadequada no sistema.

> Apesar de permitir que se desenrolem negócios de compra e venda online, o OLX não detém "um carácter mediador de transações, (...) não se responsabiliza por qualquer eventualidade resultante da falta de capacidade jurídica dos utilizadores" e, muito importante para a confiança dos clientes, garantem que "os registos no OLX são pessoais e intransmissíveis, sendo o titular do mesmo o único responsável pelas ações efetuadas com o seu registo". (SILVA, 2016 apud OLX, 2016, p. 45)

No Olx não há cobrança de taxas sobre anúncios ou sobre as vendas, mas limita o número de anúncios grátis por mês[18]. Com todas estas características o Olx é, dentre

[15] https://sellercentral.amazon.com.br/gp/help/external/200336920/
[16] https://olxbrasil.zendesk.com/hc/pt-br/articles/211994645-Quem-Somos
[17] https://olxbrasil.zendesk.com/hc/pt-br/articles/211376849-A-OLX-pode-interferir-na-minha-negocia%C3%A7%C3%A3o-
[18] https://olxbrasil.zendesk.com/hc/pt-br/articles/115004581225

os sistemas analisados, o que mais se assemelha a proposta deste trabalho, com uma abordagem de anúncios classificados e que não interfere nas negociações realizadas pelos usuários do sistema. Serve como exemplo para a área de aplicação do projeto apresentado no capítulo 3.

2.4 Problemas relacionados ao comércio eletrônico atual

Mesmo com as muitas vantagens do comercio eletrônico há alguns pontos que preocupam qualquer comprador quando se trata de um e-commerce: a confiança necessária para realizar uma negociação (compra, venda, etc.), a possibilidade eminente de um golpe, a incerteza sobre a segurança dos seus dados (principalmente bancários e de crédito).

> Um dos maiores desafios do e-commerce é questão da segurança, pois ao realizar uma compra, o cliente precisa informar seus dados pessoais, números de cartões de crédito e até senhas, fazendo com que o cliente tenha medo de efetuar a compra pela internet, pois infelizmente existem muitos casos de golpes virtuais. (COELHO; OLIVEIRA; ALMÉRI, 2013)

Os riscos ao consumidor nas compras online são muitos, principalmente devido a troca de informações entre comprador e vendedor que por vezes não conseguem verificar se são verídicas, para Andrade e Silva (2017) "a troca de informações entre fornecedores e compradores torna-se mais vulnerável por terceiros, que podem utilizá-las para outras finalidades, sem autorização."

> mesmo com as Vendas online crescendo a cada ano, ainda há muito medo por parte das pessoas, as quais utilizam a Internet somente como forma de consulta e não para a compra. Isso por insegurança, já que são muitas as informações que disponibilizam ao efetuar as compras. Vale ressaltar que os sistemas de criptografia estão reduzindo esse problema, de forma significativa. (ANDRADE; SILVA, 2017)

Portanto, mesmo com grandes avanços o comércio eletrônico ainda é um ambiente em construção e com grandes espaços para inovação, ainda há algumas brechas a serem solucionadas, principalmente no modelo C2C. Este modelo de comércio é recente na internet, embora já exista desde os primórdios da humanidade quando as trocas de mercadorias eram o único meio de comércio existente.

Hoje com os marketplaces, o C2C encontrou uma forma de se expandir online, mas com este avanço tem se perdido uma das essências deste comércio. O modelo centralizado da maioria dos ambientes de vendas trava as negociações que só podem ser realizadas nos moldes da plataforma para que esta garanta a segurança da transação. Por outro lado, nos moldes descentralizados a total liberdade de negociação perde em segurança sendo mais propício a fraudes.

2.5 Computação multilateral segura e justa

Em um ambiente de vendas online descentralizado há uma grande incidência de fraudes e golpes realizados pelos usuários, tanto clientes como vendedores. Pensando na possibilidade de prevenção de tais atos ilícitos nos deparamos com o seguinte problema computacional: Como fazer uma computação justa na qual nenhuma das partes envolvidas seja prejudicada por uma ação ilícita da outra e, como esta ação pode ser punida.

Neste contexto chegamos ao dilema de que "a justiça não pode ser alcançada de maneira geral. Entende-se por justiça a garantia de que, no final de uma computação, ou todos os participantes recebem suas respostas ou nenhum deles recebe." (OLIVEIRA FILHO, 2016). Desta forma buscamos alcançar o máximo possível de justiça para a negociações online.

Há diversas formas de se alcançar a justiça em operações multilaterais, considerando justiça não a ausência de fraudes mas abrangendo a reparação pelos danos causados. Oliveira Filho (2016) destaca a justiça através de sistemas de reputação, que podem ser encarados como a probabilidade de agir honestamente em uma negociação. E a justiça monetária, na qual uma multa é paga pelo participante desonesto ao participante honesto.

Por definição Oliveira Filho (2016) afirma que "qualquer funcionalidade multilateral pode ser computada de forma segura através de um protocolo distribuído."

2.6 Modelo Peer to Peer

O termo Peer to Peer foi importado do ambiente de redes por muito se assemelhar com o conceito do modelo de negócios C2C. Sobre tal termo Righi, Pellissari e Westphall (2004) afirma que "as redes Peer-to-Peer são sistemas distribuídos sem controle centralizado [...]. Esses sistemas possibilitam que os usuários sejam, além de consumidores de recursos, os próprios responsáveis por disponibilizá-los.".

O Peer-to-Peer, ou P2P, como é conhecido, já existe há algum tempo. Ele se tornou popular com Napster, que teve seu auge por volta do ano 2000 com mais de 500 milhões de usuários segundo Tanenbaum (2003, p. 7). O Napster era um aplicativo de compartilhamento de arquivos com um conjunto de servidores centrais que listavam quais pessoas tinham os arquivos, e que eram verificados por pessoas que queriam os arquivos, para poderem acessar diretamente quem os possuía.

No caso do Napster, o conteúdo compartilhado eram arquivos música. Assim quando alguém procurava um arquivo, o servidor pesquisava todas as cópias disponíveis desse arquivo e as apresentava ao usuário. Então o usuário abria uma conexão direta com quem possuía o arquivo de música desejado, e as músicas eram transferidas diretamente entre os dois computadores. Apesar desse processo não ocorrer em um servidor central, o Napster

ainda foi responsabilizado por violação de direitos autorais e encerrado posteriormente.

O conceito de rede P2P não morreu com o fim do Napster, o P2P agora implica em você estar se conectando diretamente. Tanenbaum (2003, p. 8) chama este relacionamento P2P de comunicação não-hierárquica porque cada participante do grupo pode se comunicar diretamente com os outros participantes do grupo.

Certamente aplicando este conceito ao modelo de vendas C2C concluímos que qualquer usuário dentro do sistema pode exercer tanto o papel de vendedor como o de comprador sem restrições. Esta liberdade é característica do modelo Peer to Peer.

2.7 Blockchain

Uma cadeia de blocos, como o próprio nome diz, "A blockchain é uma estrutura de dados pública que armazena, em blocos inalteráveis, todas as transações que já ocorreram. Uma transação só é considerada válida se estiver na blockchain."(OLIVEIRA FILHO, 2016). Uma tecnologia considerada relativamente amadurecida já que surgiu em meados de 2008 com a publicação do bitcoin por Nakamoto (2008). Desde então diversas funcionalidades e formas de utilização tem sido descobertas e aplicadas para a solução de problemas computacionais.

> O blokchain surgiu com a criptomoeda Bitcoin e tinha por objetivo ser um livro-razão em que todas as transações financeiras de todos os usuários de Bitcoin ficassem armazenadas de forma a não ocorrer o problema de gasto duplo (utilizacão de uma mesma quantia monetária em transações financeiras diferentes) e não ser necessário um órgão centralizador para validar as transações financeiras efetuadas. (LUCENA; HENRIQUES, 2016)

"A tecnologia desenvolvida na blockchain surgiu, inicialmente, para ser um sistema capaz de registrar e armazenar a escrituração das transações realizadas com a moeda virtual bitcoin."(ROCHA, 2018). Embora atrelado ao lado financeiro uma blockchain faz mais que simplesmente armazenar transações de criptomoedas. Utilizar a blockchain como livro caixa é apenas uma possibilidade dentre as suas incontáveis utilidades.

> (...) poderia ser interessante em outras aplicações em que adulterações não são desejadas: contratos e eleições digitais; em aplicações em que há elevada necessidade de garantia contra erros e modificações: armazenamento de dados; em aplicações com o objetivo de garantir propriedade: distribuição de mídias; e em aplicações em que é importante garantir se determinado elemento pertence a um conjunto: identificadores pessoais. (LUCENA; HENRIQUES, 2016)

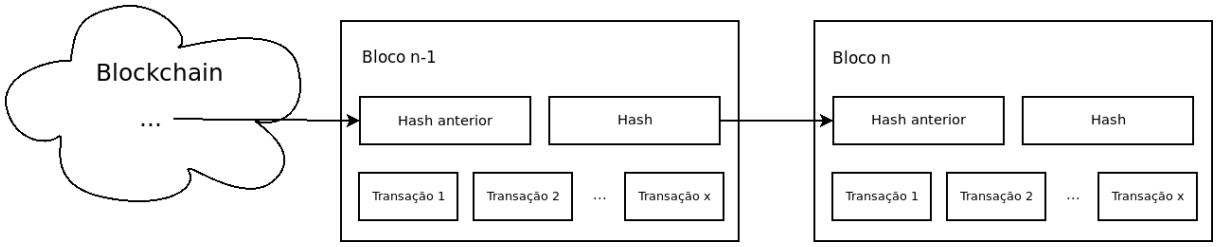
Estruturalmente uma blockchain é composta por uma cadeia de blocos (Figura 1) que só pode ser alterada no final onde um novo bloco é criado a medida que uma

determinada quantidade de transações ocorre. Cada bloco faz referência ao seu antecessor formando uma sequência de forma que para alterar um bloco seria necessário alterar todos os seus sucessores. Quanto mais antigo for o bloco mais imutável seus valores são. Seus dados não ficam em um só lugar mas são distribuídos através dos nós participantes dificultando ainda mais alterar um valor já confirmado pelo consenso.

> Assim, pode-se definir o blockchain como uma base distribuída de dados que mantém uma lista encadeada com todos os registros dos elementos de uma rede, bem como registros de qualquer criação de novos elementos e modificação destes, impossibilitando revisão e adulteração dos mesmos. (LUCENA; HENRIQUES, 2016)

> Cada Blockchain é criptografado e organizado em um conjunto de dados menores denominados blocks. Cada block contém uma informação sobre um certo número de transações, uma referência ao block anterior da cadeia (chain), e a solução para um algoritmo matemático (hash), que será usado para validação das informações incrementadas e associadas àquele bloco. Uma cópia do Blockchain será salva em cada computador que fizer parte dessa rede P2P e periodicamente sincronizados entre si para manter o mesmo e atualizado banco de dados. (DIVINO, 2018)

Figura 1 – Diagrama simplificado da estrutura blockchain



Fonte: Autor

2.7.1 Criptomoedas

Segundo Nakamoto (2008) as moedas digitais descentralizadas baseadas em criptografia, conhecidas como criptomoedas, tem como objetivo facilitar o envio de pagamentos online de pessoa para pessoa (Peer to Peer) sem o intermédio de uma instituição financeira.

> Nós definimos uma moeda eletrônica como uma cadeia de assinaturas digitais. Cada proprietário transfere a moeda para o próximo assinando digitalmente uma codificação com as transações anteriores e a chave pública do próximo proprietário e adicionando estas ao fim da moeda. Um recebedor pode verificar as assinaturas para verificar a cadeia de propriedade. (NAKAMOTO, 2008)

Através das criptomoedas é possível fazer transações financeiras irreversível, ou seja, sem estorno para serviços onde não há possibilidade de devolução. Um exemplo

superficial de serviço sem estorno pode ser uma corrida de táxi, pois depois de transportar o passageiro o taxista não tem como desfazer o serviço prestado. Porém o passageiro pode tentar solicitar a instituição financeira o estorno do pagamento feito com cartão de crédito, caracterizando um golpe, já que o serviço foi prestado. Esta situação não aconteceria com um pagamento à vista, em dinheiro físico, ou seja, o pagamento não seria estornado, devolvido.

Atualmente os pagamentos intermediados por instituições financeiras, principalmente as que utilizam os cartões de crédito, geram um alto custo operacional, que é embutido no valor da transação para manter a possibilidade do estorno através da instituição financeira.

> Um certo percentual de fraude é aceito como inevitável. Estes custos e incerteza de pagamentos podem ser evitados com uma pessoa usando uma moeda física, mas não existe mecanismo que faça pagamentos sobre canais de comunicação sem um intermediário confiável. (NAKAMOTO, 2008)

O custo operacional é repassado ao usuário, aumentando o custo da transação e estabelecendo valores mínimos para as transações, além de exigir inúmeras medidas de segurança para garantir o mínimo de confiança na realização destas operações.

> Vendedores devem tentar se proteger de seus clientes, obrigando-os a fornecer mais informações do que seriam necessárias de outra forma, pois os mesmos podem comprar produtos e serviços, pagar eletronicamente, e logo após estornar o pagamento. (NAKAMOTO, 2008)

Além de ser utilizado para compras de produtos e serviços, as criptomoedas também são comercializadas livremente, sejam vendidas por moedas físicas ou trocadas por outras moedas virtuais. Elas se diferem não só no nome, mas também no valor, na abrangência de mercado e na estrutura de geração e armazenamento.

Tais trocas e negociações são realizadas em sua maioria através das Exchanges que são centralizadoras de transações, que permitem a troca de criptomoedas por outros tipos de moedas digitais, cobrando uma taxa sobre cada movimentação realizada. Funcionando também como corretoras da bolsa de valores no mercado de ações, as Exchanges permitem acompanhar a cotação atual de cada criptomoeda, calculada em relação as últimas vendas.

As Exchanges não são obrigatórias para a realização de uma transação com criptomoeda, já que as transações são sempre Peer to Peer. Isso impede que o sistema de criptomoedas se torne como uma instituição financeira centralizada, o que fugiria do escopo da autoridade distribuída.

Atualmente existem várias criptomoedas em circulação e cada uma delas possui uma funcionalidade diferente que pode estar associada a uma tecnologia de blockchain diferente.

Essa diversidade ocorre devido ao desenvolvimento das tecnologias e funcionalidades atreladas as necessidades da comunidade de usuários. A pesar de hoje serem bastante valorizadas, apenas algumas possuem valor real, ou seja, estão atreladas ao valor de uma reserva financeira em moeda física ou posses materiais, como o ouro por exemplo.

2.7.2 Smart Contract

"Smart Contracts são contratos digitais construídos em um código de computador e armazenados no blockchain, auto executáveis, de caráter descentralizado, e que prezam pela praticidade, redução de custos e pelo anonimato."(DIVINO, 2018) Os contratos inteligentes, como são chamados, são programas que rodam sob a blockchain e utilizam de suas propriedades.

Os Smart Contracts são inalteraveis depois de publicados na blockchain, o que permite que eles sejam executados exatamente como foram programados independente de fatores externos. Devido a isso é atribuído um alto grau de confiança aos Smart Contracts sendo até comparados e apontados como possíveis substitutos dos contratos de papel.

Não há limitações para o seu uso, pois eles podem realizar transações com criptomoedas, como pagamentos automáticos, distribuição de valores, venda de itens, pagamento de salario, premiação automática, licitações, leilões, entre outros. Juristas tem estudado suas possibilidades de substituir contratos físicos em algumas situações. Rocha (2018) complementa afirmando que os contratos inteligentes permitem a realização de negócios com qualquer coisa que seja livre de conflito sem intervenção de nenhum intermediário.

> Uma das diferenças substanciais, se comparado ao contrato tradicional, é a possibilidade de cumprimento e execução forçados da obrigação em caso de adimplemento ou inadimplemento de uma determinada condição pré-estabelecida. Após realizadas as tratativas iniciais com a eventual transcrição do pacto em linguagem da computação, a execução desse negócio jurídico independe da vontade das partes e dispensará posteriores verificações, aprovações ou ações dos envolvidos ou de terceiros. (DIVINO, 2018)

> Dentre as principais características dos Smart Contracts podemos destacar: são contratos autoexecutáveis, pois não dependem da intervenção das partes. Assim, quando os termos fixados no contrato são alcançados a ação seguinte é liberada automaticamente; são também seguros e imutáveis, de modo que, há uma segurança e imutabilidade de todas as ações do contrato, sendo imodificáveis as cláusulas fixadas pelas partes; e transparência, onde cada um que participa deste tipo de contrato pode acompanhar em qual estágio se encontra a transação, assim como todas as ações que foram realizadas neste percurso. (ROCHA, 2018)

2.8 Ethereum

Dentre as principais tecnologias de blockchain, a que melhor atende as necessidades deste trabalho é a Ethereum, por ser open source e possuir integradas todas as funcionalidades necessárias como a possibilidade de implementar um Smart Contract.

> A intenção da Ethereum é criar um protocolo alternativo para a criação de aplicativos descentralizados, fornecendo um conjunto diferente de compensações que acreditamos ser muito úteis para uma grande classe de aplicativos descentralizados, com ênfase particular em situações em que o tempo de desenvolvimento rápido, segurança para pequenas e aplicações raramente utilizadas e a capacidade de diferentes aplicações interagirem de forma muito eficiente são importantes. (BUTERIN et al., 2013)

Em comparação com outras blockchains como a do Biticoin idealizada por Nakamoto (2008) fica claro que o objetivo do Ethereum é bem diferente, o Bitcoin foi criado para ser um "um sistema de pagamentos eletrônicos baseado em provas criptográficas"(NAKAMOTO, 2008). Tendo como principal foco a utilidade monetária, posteriormente o Ethereum "foi concebido para ser uma rede peer-to-peer de máquinas virtuais e foi criado como uma plataforma para criar e executar Smart Contracts ou aplicações descentralizadas sobre blockchain."(LUCENA; HENRIQUES, 2016)

A tecnologia utilizada pelo Ethereum consiste em "um blockchain com uma linguagem de programação Turing-completa integrada"(BUTERIN et al., 2013) que ainda segundo Buterin et al. (2013) permite que qualquer pessoa possa escrever contratos inteligentes e aplicativos descentralizados e que também possam criar suas próprias regras arbitrárias de propriedade, formatos de transação e funções de transição de estado.

> A rede Ethereum inclui sua própria moeda embutida, o ether, que serve ao propósito duplo de fornecer uma camada de liquidez primária para permitir a troca eficiente entre vários tipos de ativos digitais e, mais importante, fornecer um mecanismo para pagamento de taxas de transação. (BUTERIN et al., 2013)

Segundo Buterin et al. (2013) o ether é o principal (não é o único) combustível interno do Ethereum, ele é usado para pagar as taxas de transação, chamadas de *gas* (combustível em inglês). As taxas são utilizadas para recompensar os mineradores que dispõem do poder de processamento da rede ethereum.

> A unidade fundamental de computação é "gas"; Normalmente, uma etapa computacional custa 1 gas, mas algumas operações custam quantidades maiores de gas porque são computacionalmente mais caras ou aumentam a quantidade de dados que devem ser armazenados como parte do estado.

O Ethereum não é exclusivamente financeiro, é uma plataforma aberta para o desenvolvimento de novas aplicações, inclusive outras moedas digitais baseadas no ether regradas a partir de um Smart Contract.

> O que é mais interessante sobre o Ethereum, no entanto, é que o protocolo Ethereum se move muito além da moeda. Protocolos em torno de armazenamento de arquivos descentralizado, computação descentralizada e mercados de previsão descentralizada, entre dezenas de outros conceitos, tem o potencial de aumentar substancialmente a eficiência da indústria computacional e fornecer um grande impulso a outros protocolos peer-to-peer, adicionando pela primeira vez uma camada econômica. Finalmente, há também um conjunto substancial de aplicativos que nada têm a ver com dinheiro. (BUTERIN et al., 2013)

2.9 Considerações finais

Este capítulo apresentou os principais assuntos relacionados ao desenvolvimento do trabalho, foram definidos pontos que serão utilizados para esclarecer a proposta de solução e suas características já no próximo.

Parte III

Proposta de solução

3 Proposta de solução

3.1 Considerações Iniciais

Este capítulo apresenta como proposta de solução para um método seguro de se realizar compras de produtos digitais online P2P baseado em blockchain. Este capítulo trará uma compreensão mais detalhada a respeito do projeto TilliT distribuert.

3.2 O desafio

Comprar e vender na internet nem sempre é uma tarefa tão simples quanto parece, exige atenção, pesquisa e uma grande parte de confiança naquele que está disposto a negociar o produto. Tudo isso pode ser simplificado caso o personagem da ação escolha um grande marketplace que ofereça vantagens que serão um consolo caso ocorra algum problema e a compra não seja realizada ou não atenda as suas expectativas. Segundo a Ebit e Nielsen (2019) cerca de 56% dos brasileiros comprariam online se tivessem uma garantia de devolução do dinheiro como segurança para o caso de algo dar errado.

Essa tem sido a estratégia usada por grandes marketplaces para inspirar confiança nos compradores, mas esta confiança não é grátis, os custos para mantê-la são bastante altos e são repassados ou ao consumidor final ou ao vendedor do marketplace ou a ambos.

Os pequenos vendedores, fugindo das taxas cobradas pelos marketplaces encontram as redes sociais como forma de anunciar seus produtos para garantir suas vendas. Os grupos de compra e venda se popularizaram. Neles, há um contato mais direto do vendedor com o comprador, mas sem nenhuma garantia. O comércio C2C, como é conhecido, se distribui entre os marketplaces mais liberais (aqueles que não obrigam o vendedor a ter uma empresa registrada) as plataformas de interligação entre compradores e vendedores e as redes sociais "visto que por si só já promovem a interação entre as pessoas e derrubam algumas das barreiras negativas, como as taxas dos sites, por exemplo, pois as mídias, em sua maioria, são de adesão gratuita."(KOHN; KRUEL, 2016)

Ainda segundo Kohn e Kruel (2016) "Os sites intermediadores, que embora representem segurança por um lado, cobram por esse serviço e limitam um relacionamento mais direto entre os negociantes.". Para os autores, a cobrança de taxas é a principal justificativa para o "social commerce"(KOHN; KRUEL, 2016), comércio através das redes sociais, ter se popularizado. Embora haja grandes vantagens para os vendedores e compradores com relação as taxas os mesmos autores relatam como desvantagens deste tipo de comércio "a ausência de garantia de pagamento, o uso fraudulento de nomes e websites conhecidos e

falhas de controle de qualidade dos produtos."(KOHN; KRUEL, 2016)

Na tentativa de solucionar tais dificuldades surge a possibilidade de se utilizar do modelo blockchain para alcançar altos níveis de segurança e confiabilidade. "O conceito de blockchain representa uma área muito atraente para pesquisas e novas aplicações, prometendo uma vasta gama de possibilidades."(LUCENA; HENRIQUES, 2016) Uma delas é a de gerir a relação entre comprador e vendedor sem um intermediário.

O grande desafio é encontrar uma forma de conciliar a comodidade das compras online com a liberdade do modelo P2P e com a segurança dos dados da blockchain com o objetivo de tornar mais segura a comercialização de produtos e mídias digitais. Tais mídias que não podem ser comercializadas nos grandes marketplaces por serem contrários aos seus termos de uso.

Um dos principais motivos para a não comercialização de produtos digitais é a possibilidade da pirataria já que não é possível controlar a distribuição de tais mídias. A princípio pode-se imaginar que tal forma de comercialização favoreceria a pirataria e criaria diversos outros problemas legais. Mas o que realmente ocorre é que há como solucionar este primeiro impasse.

> O uso de blockchain na distribuição de conteúdo multimídia poderá fazer com que qualquer arquivo de música ou filme possa ser utilizado apenas pelo dono de determinado nó, impossibilitando a cópia e distribuição gratuita do arquivo para outras pessoas. A venda de um arquivo de mídia seria a transferência do mesmo para o domínio de outra chave pública pertencente a outro usuário dentro da rede blockchain, de forma similar ao que ocorre com a transferência de uma criptomoeda. (LUCENA; HENRIQUES, 2016)

3.3 TilliT distribuert - White paper

O nome do projeto da plataforma de vendas P2P vem do norueguês *tillit distribuert* e significa confiança distribuída que é um dos principais pontos defendidos para a sua idealização. Um sistema que permita vendas de artigos tanto digitais quanto físicos e que permita uma computação multilateral justa, sem a existência de um centralizador. Para uma computação multilateral justa são necessárias algumas garantias, entendendo por justiça a afirmação de Oliveira Filho (2016) onde estabelece que participantes desonestos sejam monetariamente penalizados por causarem dano ao processo natural da computação. Aliado com um decréscimo na reputação do participante desonesto.

> Um exemplo de garantia naturalmente desejável é a da correção, ou seja, a de que, ao final da computação, cada participante receberá uma resposta coerente com a execução de f sobre as entradas dadas. Outra garantia importante é a privacidade das entradas. Ela pode ser vista como a impossibilidade de um participante ter acesso a qualquer informação

> sobre uma entrada, ou saída, que não a sua própria. (OLIVEIRA FILHO, 2016)

Sendo f uma computação multilateral. Pensando em atender tais garantias a tecnologia blockchain escolhida para o projeto é a Ethereum, desenvolvida pela Fundação Ethereum a partir de 2013, buscando melhorar pontos da arquitetura Bitcoin proposta por Nakamoto (2008) e adicionar novas funcionalidades

> O blockchain Ethereum é em muitos aspectos semelhante ao blockchain Bitcoin, embora tenha algumas diferenças. A principal diferença entre o Ethereum e o Bitcoin em relação à arquitetura blockchain é que, diferentemente do Bitcoin (que contém apenas uma cópia da lista de transações), os blocos Ethereum contêm uma cópia da lista de transações e do estado mais recente. Além disso, dois outros valores, o número do bloco e a dificuldade, também são armazenados no bloco. (BUTERIN et al., 2013)

A proposta principal do Ethereum é ser uma plataforma de desenvolvimento e um ambiente de execução de aplicações descentralizadas de alta confiabilidade, chamadas de *Smart Contracts*. O seu uso não se limita apenas ao financeiro mas em geral, existem três tipos básicos de aplicações Ethereum.

> A primeira categoria é de aplicativos financeiros, oferecendo aos usuários maneiras mais poderosas de gerenciar e entrar em contratos usando seu dinheiro. Isso inclui sub-moedas, derivativos financeiros, contratos de hedge, carteiras de poupança, testamentos e até mesmo algumas classes de contratos de trabalho em larga escala. A segunda categoria é a aplicação semi-financeira, onde o dinheiro está envolvido, mas há também um lado pesado não monetário para o que está sendo feito; Um exemplo perfeito são recompensas auto-executivas para soluções de problemas computacionais. Finalmente, há aplicações como votação online e governança descentralizada que não são financeiras. (BUTERIN et al., 2013)

Para este projeto definiremos um *Smart Contract* modelo de compra e venda atendendo as garantias necessárias para uma computação multilateral segura e justa. Mas inicialmente vamos entender como funciona o modelo de vendas do projeto TilliT.

3.3.1 O modelo de vendas virtuais TilliT

Quais os diferenciais de uma loja virtual? O preço, a comodidade, os melhores produtos, ou até a melhor forma de pagamento. Não há muito no que se inovar a respeito de um e-commerce, o fluxo quase sempre segue da mesma forma. O usuário encontra um produto, se interessa, pesquisa, cadastra-se no site onde vendem o produto, realiza a compra e paga pelo produto para então receber uma confirmação e aguardar a chegada do produto no seu endereço.

A proposta do TilliT distribuert é conectar interessados em fechar negócios. Um ambiente virtual onde qualquer usuário possa anunciar seu produto, inclusive mídias digitais, e aguardar o contato de um possível comprador. Para evitar spans e outros tipos de ações indesejadas, apenas o comprador pode iniciar a negociação. Todo o processo é conduzido através de mensagens P2P entre o comprador e o vendedor, não existem intermediários nem mediadores.

Ao iniciar a transação, ambos os participantes podem negociar e definir como serão os passos para realizar a compra/venda. Após os acertos iniciais onde podem ser discutidos preços, formas de pagamento, formas de entrega e garantias. Entrando em acordo, o sistema sugere a adoção de um Smart Contract para prevenir possíveis riscos. O Smart Contract é facultativo para manter o princípio da liberdade de negociação entre vendedor e comprador mas é altamente recomendado para a segurança e confiabilidade da operação.

Após o passo da negociação, caso definido, o Smart Contract servirá para gerir tanto as multas (garantias) quanto as licenças, direitos autorais e os artigos digitais. Ambos os usuários devem estar de acordo com os termos (funções) do Smart Contract para poder iniciar depositando o valor das garantias. O valor depositado servirá uma pequena parte para custear o contrato (gas no ethereum) e o restante será devolvido ao final caso a operação ocorra dentro da normalidade.

3.3.2 Detalhando o modelo de Smart Contract TilliT

Um acordo de compra e venda pode ser simplesmente fechado entre duas pessoas sem que haja a necessidade de um contrato formal como é feito nas compras em lojas físicas. Apesar de não haver um contrato explícito, o ato de comprar ou vender estabelece uma relação contratual na qual o vendedor se compromete a entregar o produto em bom estado mediante o pagamento feito pelo comprador. Em contrapartida o comprador se compromete a entregar o pagamento nas devidas condições acertadas previamente sob risco de não receber o produto caso não efetue o pagamento.

Este contrato implícito é valido para todos os tipos de compras. Há ainda o caso de compras que envolvem um volume financeiro maior onde são celebrados contratos com valor jurídico. Independente da situação não há como comprar e vender sem um contrato. Sem algo que defina as regras da operação e as penalidades possíveis para os casos que ocorrerem fora do esperado. Para as compras online também existem contratos implícitos e explícitos. Os grandes marketplaces e as demais lojas virtuais definem seus contratos nos termos de uso da sua plataforma.

Além dos contratos há uma regulamentação sobre as vendas, o código de defesa do consumidor, que regulamenta inclusive os contratos de compra e venda. Aplicar as

sanções previstas no código de defesa do consumidor é algo relativamente fácil quando o vendedor é uma pessoa jurídica, seja ela uma loja física ou virtual. Mas quando as vendas são praticadas por uma pessoa física, para usar o termo adequado, o quadro muda completamente. Os riscos de se sofrer um golpe comprando ou vendendo de pessoas físicas é inumeravelmente maior.

Segundo Kohn e Kruel (2016) a maioria dos relatos de problemas relacionados a compras virtuais são relacionados a negociação, como pessoas que não comparecem ao local marcado para a venda, ou que desaparecem assim que o negócio é fechado ou quando recebem uma parte ou todo o pagamento. Ainda segundo os autores o comércio C2C não possui garantias, seja de qualidade do produto ou de que a entrega será realizada ou nem mesmo de que o pagamento ocorrerá como o previsto.

É notável o motivo pelo qual se faz necessária uma alternativa segura para compras e vendas entre pessoas físicas, o comércio C2C, ou P2P que são tratados como sinônimos neste trabalho. Para solucionar tal questão de maneira justa temos a proposta de firmar um contrato entre o vendedor e o comprador, no qual eles se comprometem a, depois de negociada a venda, cumprir cada um a sua parte ou pagar uma multa.

Como fazer isso dar certo quando vendedor e comprador não se conhecem e estão distantes demais para assinar um contrato? A solução encontrada foi criar um Smart Contract personalizado para cada venda. "Os contratos inteligentes permitem aos que aderem esse modelo negocial trocar dinheiro, propriedades, compartilhamentos ou outra coisa qualquer que seja livre de conflito sem intervenção de nenhum intermediário."(ROCHA, 2018)

> Para seu funcionamento, as partes devem acordar as condições que deverão ser adimplidas para a realização do negócio. As regras definidas serão inseridas no sistema operacional e deverão ser programadas em um código autoexecutável que, após a “assinatura” e cumprimento das disposições contratuais, cumprir-se-á de forma irreversível e automática. (ROCHA, 2018)

O Ethereum permite a criação de Smart Contracts elaborados pois eles são executados sob a máquina virtual Ethereum (EVM), pois ela é Turing-complete. "Isso significa que o código EVM pode codificar qualquer cálculo que possa ser realizado, incluindo loops infinitos."(BUTERIN et al., 2013). Ou seja pode executar praticamente qualquer algoritmo desde que este possa ser reduzido a um problema solucionável por uma máquina de Turing.

3.3.2.1 Adicionar garantias

O algoritmo base para os Smart Contracts que serão utilizados para as vendas foi pensado para atender as necessidades de segurança permitindo que cada usuário tenha acesso a personalizá-lo através do sistema de vendas P2P mas só será aceito caso ambos os

envolvidos aceitem os termos de cada venda. Um Smart Contract é composto por funções auto executáveis que são chamadas através do endereço do contrato publicado na blockchain. O algoritmo 1 apresenta o método ***AdicionaGarantias(valor, gas, usuario, papel)***, que receberá os depósitos das garantias para a realização da venda e inicializará o Smart Contract.

Algoritmo 1: Adicionar garantias

Dados: O valor a ser depositado acrescido da parte correspondente ao usuário do valor do *gas* calculado previamente e que manterá o contrato ativo, o Usuário que está realizando o depósito e o papel desempenhado pelo usuário na negociação.

Resultado: Continua aguardando por um tempo determinado ou avança para o próximo passo.

```
1  AdicionaGarantias(valor, gas, usuario, papel) início
2      se VerificaUsuario(usuario) e valor == GetValorDefinido(usuario) então
3          AceitaValor(valor, gas);
4          AdicionaUsuario(usuario, papel);
5      senão
6          RejeitaValor(valor, gas);
7      fim
8      se GetUsuariosAceitos() == GetUsuariosEsperados() então
9          ProximoPasso();
10     senão
11         AguardeNovoUsuario(tempo);
12     fim
13 fim
```

Fonte: Autor

Caso tudo ocorra bem, todos os usuários envolvidos na transação vão conseguir depositar o valor correspondente a garantia (ou multa para melhor entendimento). A seguir uma descrição mais detalhada dos métodos utilizados:

- ***VerificaUsuario(usuario)*** é utilizado para definir se o depósito vem de um dos usuários envolvidos na transação, para evitar a inclusão de terceiros em uma transação já iniciada.
- ***GetValorDefinido(usuario)*** retorna o valor que foi proposto para que cada participante deposite como garantia de que agirá honestamente durante a transação acrescida da parte correspondente ao *gas* que manterá o Smart Contract ativo.
- ***AceitaValor(valor, gas)*** registra o valor recebido relacionado ao usuário e destina o *gas* ao contract.

- ***AdicionaUsuario(usuario, papel)*** adiciona o usuário com seu respectivo papel na transação para a lista de usuários aceitos.
- ***RejeitaValor(valor, gas)*** disponibiliza o valor e o *gas* depositados para que seja pedido o reembolso. Não é uma boa prática num Smart Contract devolver o valor ao remetente, por segurança este deve solicitar sua restituição chamando o método de reembolso.
- ***GetUsuariosAceitos()*** retorna a lista de todos os usuários que já realizaram seu depósito.
- ***GetUsuariosEsperados()*** retorna a lista de usuários que foram definidos inicialmente para participar da transação.
- ***ProximoPasso()*** segue o fluxo do sistema, o contrato continua aguardando a próxima ação ou o final do tempo definido.
- ***AguardeNovoUsuario(tempo)*** espera, pelo tempo determinado inicialmente, o depósito dos usuários restantes. Caso o tempo finalize o contrato também é finalizado e o valor arrecadado é disponibilizado para restituição aos seus respectivos usuários, que devem solicitar o reembolso. O usuário faltante é penalizado com decréscimo na sua reputação.

3.3.2.2 Os envios de itens

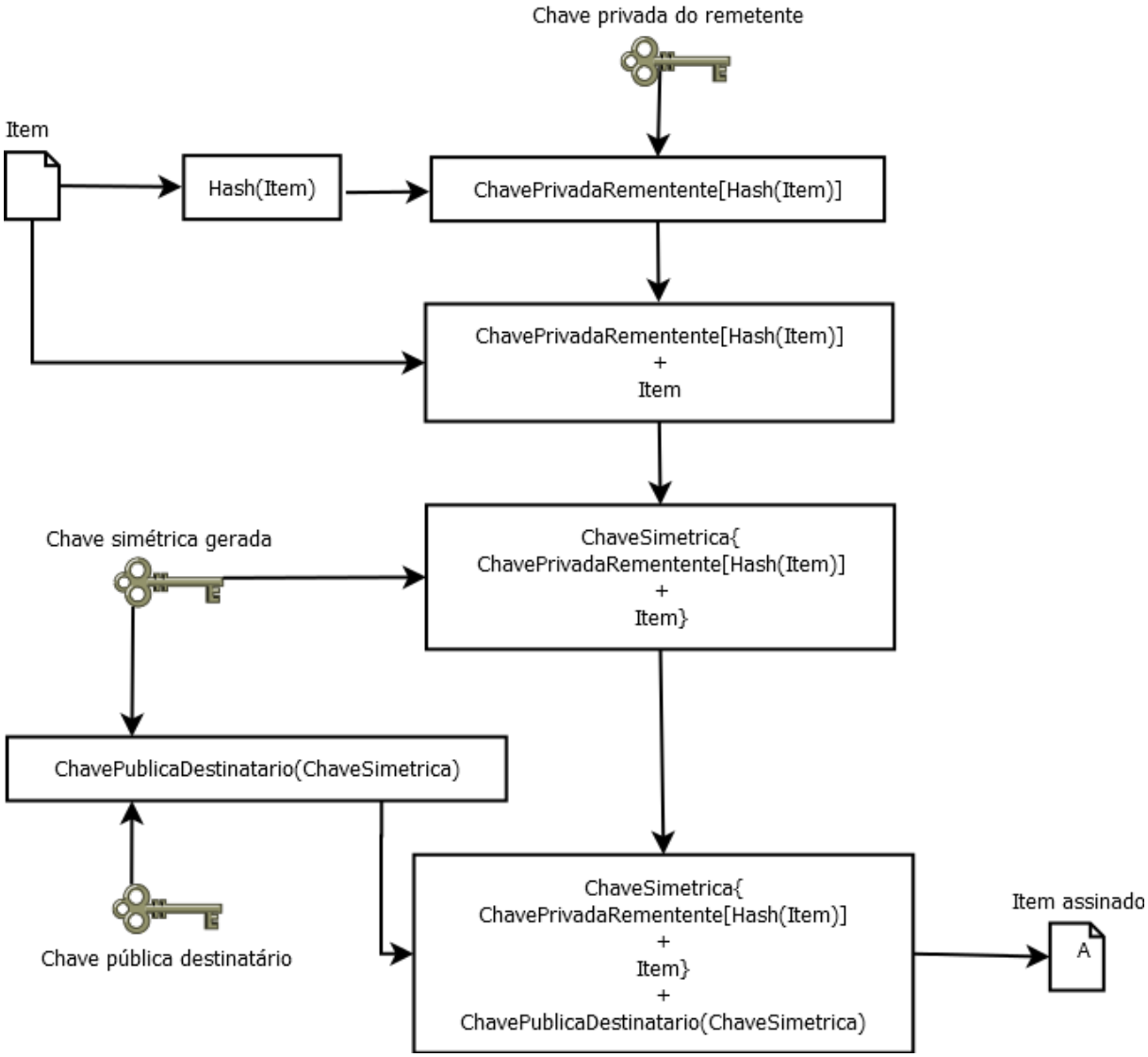
Caso seja necessário e seja da opção dos usuários envolvidos, é possível o envio de artigos digitais através do Smart Contract e também gerenciar o pagamento através do ether ou qualquer outra sub moeda ethereum, ou o TilliT (moeda digital baseada em ethereum que acompanha o TilliT ditribuert em seu projeto). É possível além do envio do artigo comercializado o envio dos comprovantes tanto de envio como de pagamento, sendo estes também obrigatórios para a restituição da garantia a partir deste passo caso a operação não seja inteiramente controlada pelo Smart Contract.

O envio de itens é realizado através do método ***AdicionaEnvio(item, remetente, descricao, destinatario)*** descrito pelo algoritmo 2 e que utiliza os seguintes métodos:

- ***VerificaUsuario(remetente)*** é utilizado para definir se o item vem de um dos usuários envolvidos na transação, para evitar a inclusão de terceiros em uma transação já iniciada.
- ***VerificaItem(item)*** é utilizado para definir se o item enviado é válido, possível realizar nesta etapa verificação automatizada de conteúdo sensível e de direitos autorais.

- ***AssinaItem(item, remetente, destinatario)*** retorna o item incrementado de sigilo, autenticação do remetente, e de integridade da mensagem através de criptografia de chave assimétrica e de chave simétrica com uma chave gerada aleatóriamente de acordo com a figura 2.
- ***EnviaItem(itemAssinado, remetente, descricaoAssinada, destinatario)*** registra o envio do item no Smart Contract com acesso apenas pelo destinatário e pelo remetente.

Figura 2 – Esquema do processo de assinatura digital com chaves assimétricas



Fonte: Autor

A figura 2 apresenta o fluxograma do processo de assinatura digital do item que será enviado a Blockchain. A assinatura digital com a chave privada do remetente, por si, só garante a autenticação do remetente, esta assinatura é feita na hash(resumo) do item para garantir também a verificação da integridade da mensagem.

Para garantir o sigilo uma chave simétrica é gerada para garantir o acesso ao item para todos os usuários envolvidos na transação. Para cada usuário o sistema envia a chave simétrica cifrada com a chave pública do destinatário.

Algoritmo 2: Adicionar envios

Dados: O item/arquivo a ser enviado para a transação, o usuário que está enviando, uma descrição obrigatória do item a ser enviado e o usuário destinatário.

Resultado: Caso o item seja válido aceita e o armazena vinculado ao seu respectivo usuário.

```
1 AdicionaEnvio(item, remetente, descricao, destinatario) início
2     se VerificaUsuario(remetente) e VerificaItem(item) então
3         itemAssinado = AssinaItem(item, remetente, destinatario);
4         descricaoAssinada = AssinaItem(descricao, remetente, destinatario);
5         EnviaItem(itemAssinado, remetente, descricaoAssinada, destinatario);
6     fim
7 fim
```

Fonte: Autor

3.3.2.3 O resgate das garantias

Ao fim da transação, ocorrendo tudo da melhor forma possível (situação em que todos os envolvidos na transação agiram de forma honesta e não houveram outros problemas), cada usuário tem o direito de solicitar o resgate da sua garantia depositada descontada a parte do *gas* utilizado pelo Smart Contract que é dividida para todos os usuários envolvidos. O *gas* necessário é calculado antes mesmo de iniciar o Smart Contract a partir do tempo de vida estipulado para o contrato e seu valor é acrescentado ao valor inicial da garantia. Ao fim do resgate o Smart Contract é desativado, ele não pode ser apagado da blockchain, o histórico e os dados permanecerão enquanto a blockchain existir.

O resgate das garantias só pode ser realizado após cada um dos envolvidos confirmar que tudo está correto, tanto o produto quanto o pagamento realizado, veja no algoritmo 3. No melhor caso ambos poderão retirar o seu valor e terão sua reputação incrementada. Este é o ponto crucial do modelo de confiança, neste ponto deverá existir justiça computacional. Segundo Oliveira Filho (2016) a justiça computacional é a garantia de que, concluída a computação, ou todos os participantes recebem suas respostas ou nenhum deles deve receber.

Utilizaremos a definição de justiça monetária de Oliveira Filho (2016) que afirma que todo participante que abortar, agir desonestamente (no caso da venda) paga uma multa aos participantes honestos. Assim, se por ventura a justiça for quebrada, ou um dos participantes agir de forma desonesta para tentar obter uma vantagem indevida,

os participantes honestos não recuperam suas saídas, mas recebem uma compensação monetária.

Em outras palavras, o valor depositado como garantia no início da transação de compra/venda será utilizado para restituir o participante que permanecer honesto ou a ambos caso todos tenham atitudes honestas relacionadas a transação. Além da penalidade monetária ainda há o decréscimo na reputação do participante desonesto e ainda a sua negativação perante a comunidade de usuários como já ocorre atualmente no comércio C2C.

> Quando esse tipo de coisa acontece, as pessoas que se sentem lesadas costumam publicar dentro do grupo a experiência, alertando para que não se façam negócios com o indivíduo. Já outros grupos permitem a "denúncia", que acarreta a expulsão de quem não cumpre com o que é combinado. (KOHN; KRUEL, 2016)

O algoritmo 3 apresenta o método ***ResgateGarantias(usuario, confirma)*** que verificará a forma de restituição do valor depositado como garantia. A seguir uma descrição mais detalhada dos métodos utilizados:

- ***VerificaUsuario(usuario)*** é utilizado para definir se a solicitação de resgate vem de um dos usuários envolvidos na transação, para evitar a inclusão de terceiros em uma transação já iniciada.
- ***GetComprovanteEnviado(usuario)*** retorna o comprovante de envio/pagamento obrigatório enviado pelo usuário ou gerado pelo sistema no caso de envio de produto e pagamento realizados dentro do contract.
- ***ConfirmaRecebimento(usuario)*** registra o usuário na lista dos usuários confirmados e na lista dos usuários que responderam.
- ***GetUsuariosAceitos()*** retorna a lista de todos os usuários que realizaram o depósito inicial, veja no algoritmo 1.
- ***DisponibilizaValor(usuario)*** disponibiliza o valor da restituição para o método de reembolso. Não é uma boa prática num Smart Contract devolver o valor ao remetente, por segurança este deve solicitar sua restituição chamando o método de reembolso.
- ***GetUsuariosResponderam()*** retorna a lista de todos os usuários que responderam a confirmação de recebimento.
- ***IniciaJulgamento(transacao)*** este passo é iniciado caso os envolvidos na transação não entrem em acordo a respeito do recebimento, ambos se tornam suspeitos de

ação desonesta. Mas cabe ao primeiro a negar apresentar prova de que diz a verdade, veja mais na seção 3.3.4.

- ***AguardeOutroUsuario(tempo)*** espera, pelo tempo determinado inicialmente, a resposta dos usuários restantes. Caso o tempo finalize o contrato também é finalizado e o valor arrecadado é disponibilizado para restituição conforme os seguintes casos:
  - **Nenhum dos usuários confirmou ou contestou seu recebimento**, neste caso o Smart Contract entende que a operação foi concluída e prorroga o tempo de vida do contrato por igual período descontando da restituição de todos os usuários o valor que custeará o *gas* para manutenção do contrato, há decremento na reputação dos envolvidos. Após este período caso não haja resgate dos recursos estes serão destinados a manutenção do sistema.
  - **Apenas um dos usuários contestou o seu recebimento**, neste caso o Smart Contract entende que houve uma fuga da responsabilidade de se defender. Como não houve julgamento, veja na seção 3.3.4, 75% do valor do usuário ausente é destinado ao usuário que contestou dentro do tempo, este por sua vez não sofre alteração na reputação enquanto o outro envolvido sofre um decréscimo. Lembrando que nenhum dos envolvidos tem ciência das ações do outro antes do fim do contract. O valor restante é destinado a manutenção do sistema.
  - **Apenas um dos usuários confirmou o seu recebimento**, neste caso o Smart Contract entende que a operação foi concluída com sucesso, o usuário presente tem sua reputação incrementada e tem seu valor disponibilizado para reembolso, enquanto o outro envolvido sofre um decréscimo. O valor referente ao usuário ausente custeará o *gas* para manutenção do contrato por igual período de tempo. Após este período caso não haja resgate dos recursos estes serão destinados a manutenção do sistema.
- ***ContestaRecebimento(usuario)*** registra o usuário na lista dos usuários que contestaram e na lista dos usuários que responderam habilitando o contract para julgamento, veja na seção 3.3.4.

Algoritmo 3: Resgatar garantias

Dados: O Usuário que está realizando a solicitação de resgate e a confirmação do recebimento, seja do produto ou pagamento.

Resultado: Registra a solicitação de resgate e caso haja consenso afirmativo disponibiliza o valor de cada usuário para reembolso.

```
1  ResgateGarantias(usuario, confirma) início
2      se VerificaUsuario(usuario) e GetComprovanteEnviado(usuario) != vazio então
3          se confirma então
4              ConfirmaRecebimento(usuario);
5              se GetUsuariosConfirmados() == GetUsuariosAceitos() então
6                  para cada usuarioConfirmado => GetUsuariosConfirmados() faça
7                      DisponibilizaValor(usuarioConfirmado);
8                  fim
9              senão se GetUsuariosResponderam() == GetUsuariosAceitos() então
10                 IniciaJulgamento(transacao);
11             senão
12                 AguardeOutroUsuario(tempo);
13             fim
14         senão
15             ContestaRecebimento(usuario);
16             se GetUsuariosResponderam() == GetUsuariosAceitos() então
17                 IniciaJulgamento(transacao);
18             senão
19                 AguardeOutroUsuario(tempo);
20             fim
21         fim
22     fim
23 fim
```

Fonte: Autor

3.3.3 O sistema de vendas TilliT

A plataforma TilliT tem como objetivo conectar interessados em fechar negócios de maneira segura. Para isso, além do Smart Contract que poderá ser criado para atender os requisitos de computação justa, o sistema precisa oferecer um ambiente para o cadastro de usuários, divulgação dos produtos e negociação até o encerramento da venda.

O cadastro de usuários deve conter o mínimo de informações dos usuários, isso é possível devido ao modelo de vendas baseado em blockchain que permite que pessoas totalmente anônimas possam negociar sem a necessidade de se conhecerem previamente e

nem também posteriormente.

Com o intuito de proporcionar a comunidade e-commerce uma plataforma de anúncios classificados que não limite os usuários interessados em comprar apenas aos anúncios melhor patrocinados e que permita um relacionamento direto com o vendedor. O contato inicial é feito pelo comprador que escolhe o produto e inicia uma transação com o vendedor. Esta transação é representada na forma de troca de mensagens P2P criptografadas de ponta a ponta (no caso de aplicativos mobile e desktop) em ambientes que não permitem ainda uma criptografia de ponta a ponta de maneira eficiente como um navegador web a opção de mensagens criptografadas via servidor. As mensagens são armazenadas no contract.

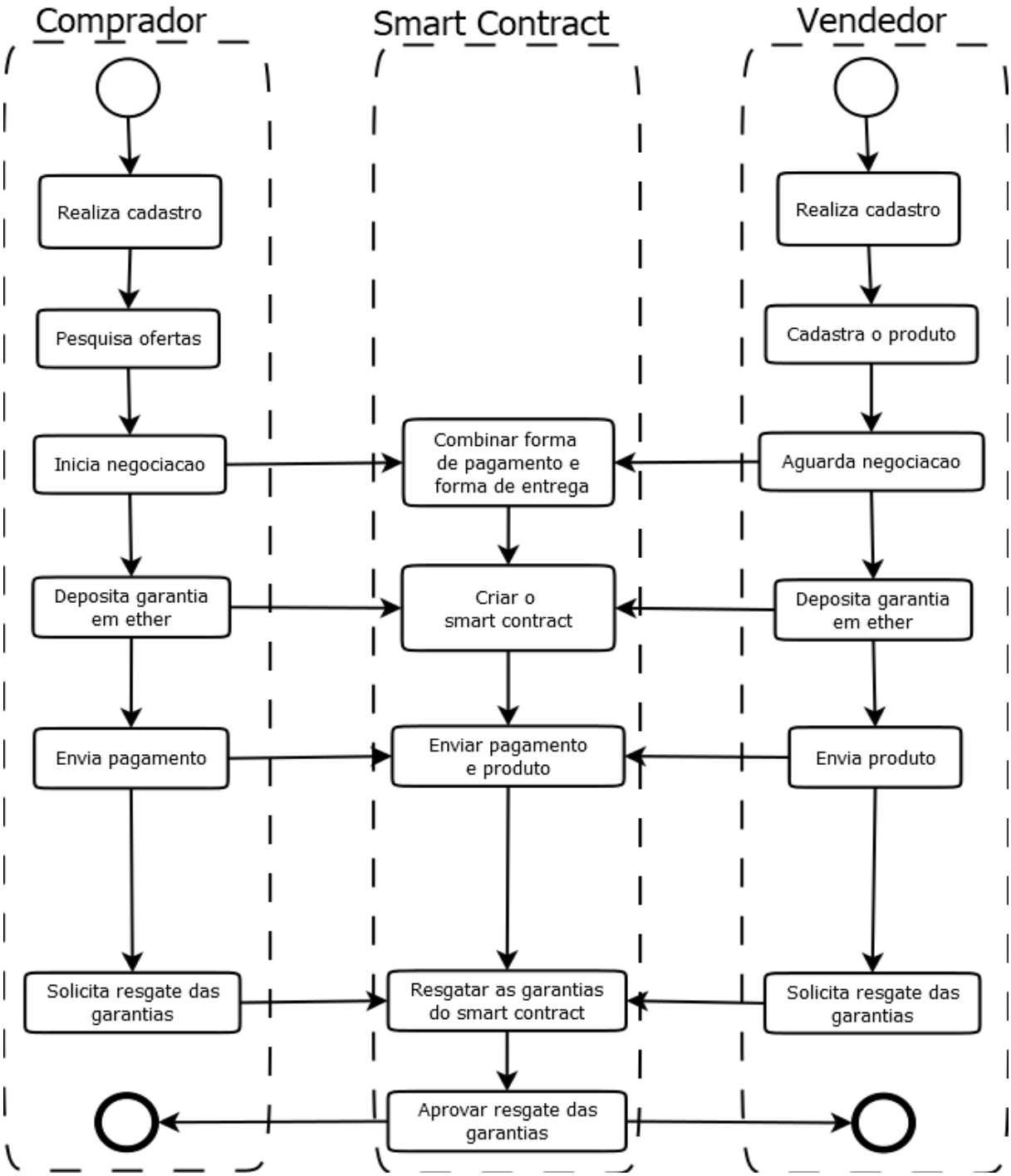
É possível vender sem o Smart Contract, os usuários tem toda a liberdade, mas as vendas sem o contract não tem ligação com o sistema. As mensagens não podem ser armazenadas em blockchain nem pode ser oferecida nenhuma garantia de uma computação justa. A liberdade do usuário é outro ponto marcante do sistema, pode se vender praticamente qualquer produto desde que não fira as leis internacionais ou locais. Um filtro de anúncios para conteúdos sensíveis e ilegais terá um amplo trabalho a ser realizado, além de regras claras e compreensíveis nos termos de uso, punições tanto monetárias quanto de reputação ou até o banimento são aplicáveis para manter a ordem.

3.3.3.1 Vendas de artigos digitais

Artigos digitais são os mais fáceis de se comercializar através de um Smart Contract, embora não seja pelos meios de e-commerce tradicionais. Estes podem ser enviados através do próprio contrato que realizará um gerenciamento de entrega bem mais simplificado. A figura 3 apresenta o fluxo do sistema desde o cadastro até a venda de um artigo digital. Caso seja a opção dos usuários, o envio de pagamento e de produto por outros meios seguirá o modelo da seção 3.3.3.2.

Cada passo é coordenado através do envio de mensagens ao contract, proporcionando uma maior comodidade ao usuário. Ao final o usuário comprador confirma no recebimento se o produto é o que foi acordado com o vendedor, estando tudo certo as garantias são reembolsadas. Estes contratos podem ter um tempo de vida bem reduzido pois as operações são bem rápidas, podendo a transação ser finalizada em poucas horas ou até minutos.

Figura 3 – Fluxo de vendas de um artigo digital entregue via blockchain



Fonte: Autor

3.3.3.2 Vendas de artigos físicos

A venda de artigos físicos representa o maior desafio. Como negociar algo na internet que terá de ser entregue a alguém que você não conhece? Muitos diriam que esta é uma pergunta do século passado. Pois nas últimas décadas o comércio digital cresceu em grandes proporções e hoje é responsável por movimentar trilhões de dólares por ano,

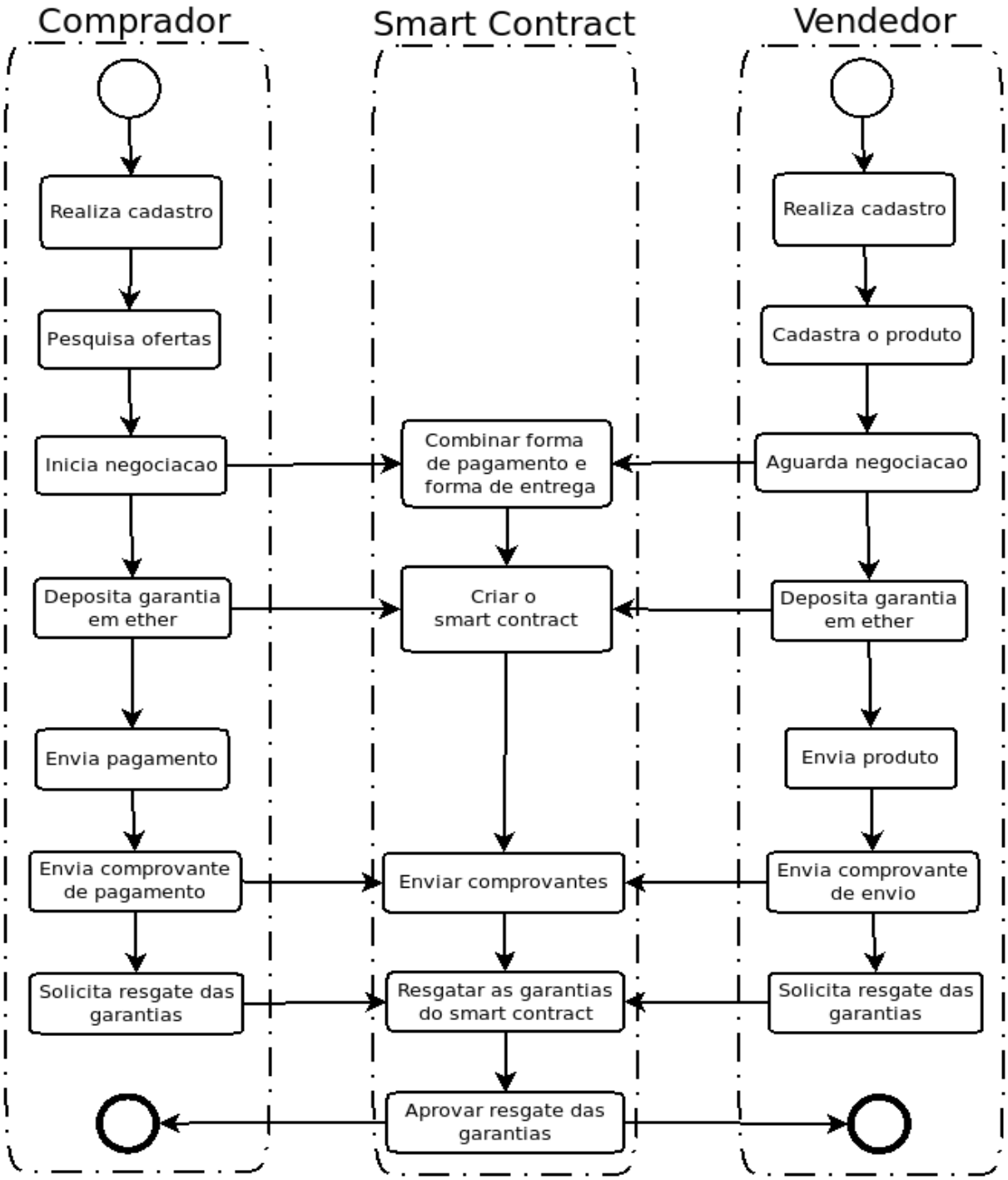
"o e-commerce apresentou 24% de crescimento no mundo todo em 2018, atingindo uma marca de 2,9 trilhões de dólares em vendas. Na América Latina o crescimento foi de 17,9% com relação ao mesmo período de 2017."(EBIT; NIELSEN, 2019)

> As vendas online apresentam crescimento maior que o varejo tradicional em praticamente todos os países que já operam o comércio eletrônico. Isto se torna ainda mais evidente para as vendas de FMCG, que globalmente cresceram 5 vezes mais no e-commerce, quando comparado ao offline.
>
> O volume do e-commerce representa um share de vendas de 12% para o varejo de todo o mundo. Os números mostram que a América Latina tem uma grande oportunidade, pois apenas 2,7% do total consumido é feito pelo online. Concentrando, assim, boas oportunidades para investidores. (EBIT; NIELSEN, 2019)

O mercado mundial está cada vez mais informatizado, e comprar pela internet passou a fazer parte da rotina das pessoas. "Perguntas por exemplo: "Como comprar cosméticos sem sentir o cheiro?"ou "Como comprar uma roupa ou calçado sem experimentar?"já não são as principais preocupações dos mais de 58 milhões de consumidores do comércio eletrônico."(EBIT; NIELSEN, 2019).

O projeto TilliT distribuert consegue englobar as vendas de bens tangíveis entre consumidores, o C2C. A diferença está na maior duração dos contratos que devem abranger todo o tempo de envio até o recebimento do produto pelo consumidor, este ponto deve ser levado em consideração ao inicializar o Smart Contract. As transações podem durar de dias a semanas e o envio dos comprovantes passa por um processo mais rigoroso de verificação para que a confirmação ou a rejeição possam ser comprovadas caso necessário. A figura 4 apresenta o fluxo para as vendas de bens tangíveis ou intangíveis entregues fora do contract.

Figura 4 – Fluxo de vendas de um artigo digital ou físico entregue de forma externa



Fonte: Autor

3.3.4 Solucionando os problemas

Numa venda online, nem sempre ocorre tudo bem, seja por um produto entregue diferente da descrição, ou um produto não entregue por falha no serviço postal. São inúmeras as possibilidades de algo acontecer. Sejam bem ou mal intencionadas, todas as situações adversas podem ter uma solução justa. A solução proposta tem como base o

sistema de júri popular utilizado pela justiça brasileira.

O acordo entre os usuários é a primeira opção, até este ponto não houve nenhuma interferência do sistema ou externa com relação a transação. Caso não cheguem a um acordo, uma interferência externa pode ser solicitada e a transação passa ao estado de julgamento. Um quórum de usuários da comunidade é escolhido aleatoriamente dentre os usuários de maior reputação que autorizaram a possibilidade de ser jurado na resolução de conflitos.

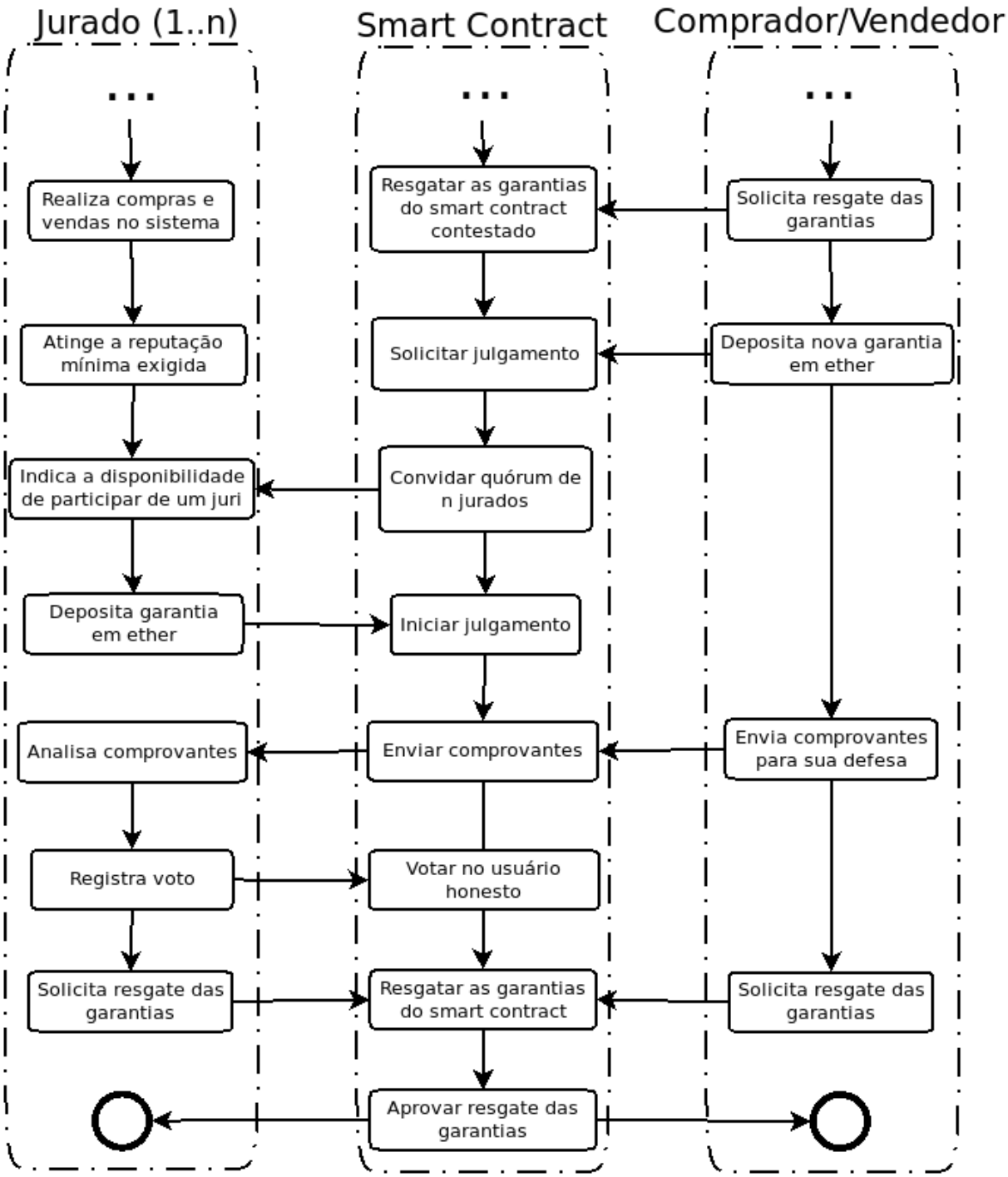
Para iniciar o julgamento, cada usuário deve depositar novas garantias proporcionais ao valor em disputa, veja melhor no algoritmo 1. Ao final, no caso de um dos usuários ser considerado desonesto o seu valor depositado servirá para remunerar os jurados. A reputação serve como indicador da probabilidade de um usuário agir honestamente, mas há ainda a possibilidade de penalização financeira para os jurados. Cada um dos jurados deve se comprometer com um valor definido com base no valor em disputa.

Cada jurado desconhece os outros jurados e vota por suas próprias convicções. Os usuários originais da transação devem providenciar provas e comprovantes da sua defesa e enviar ao Smart Contract através do algoritmo 2, estes novos envios serão destinados ao quórum, o que permitirá que cada um dos jurados tenha acesso. O tempo de vida do julgamento é definido com base na transação inicial e ao fim cada jurado deverá confirmar seu voto.

Sendo unânime, a decisão não cabe recurso, todos os jurados recebem sua recompensa e incremento na reputação, veja na figura 5. Caso um jurado não vote em tempo hábil ele perde o valor depositado e tem um decréscimo na sua reputação. Caso a decisão não seja unânime, cada usuário pode pedir mais um recurso, totalizando no máximo três julgamentos (O inicial, o primeiro recurso e o segundo recurso). Para cada recurso novos valores são depositados pelos usuários originais, um novo quórum é escolhido aleatoriamente e os novos jurados não conhecem a fase atual do processo ou os jurados que participaram de fases anteriores. Julgam e votam como se fosse a primeira fase.

Finalizado o julgamento, são feitos os pagamentos e aplicadas as penalidades aos usuários considerados desonestos (perca dos valores depositados e decréscimo na reputação). O voto de cada jurado e o resultado de cada julgamento é registrado pelo sistema para comparações de desempenho dos jurados que podem perder reputação caso falhem em julgamentos. São consideradas falhas votar contrário a maioria absoluta repetidas vezes, lembrando que cada jurado não sabe nem mesmo após o julgamento quem eram os outros jurados ou o que eles votaram, nada além do resultado final, veja no algoritmo 4.

Figura 5 – Fluxo da solução por jurados



Fonte: Autor

O algoritmo 4 apresenta o método ***ResgateGarantiasJulgamento(usuario, voto)*** que verificará a forma de restituição do valor depositado como garantia por cada jurado.

Algoritmo 4: Resgatar garantias após um julgamento

Dados: O Usuário que foi jurado e que está realizando a solicitação de resgate e o voto registrado.

Resultado: Registra a solicitação de resgate e caso haja consenso afirmativo disponibiliza o valor de cada usuário para reembolso

```
1  ResgateGarantiasJulgamento(usuario, voto) início
2      se VerificaJurado(usuario) e voto != vazio então
3          se GetComprovantesEnviados() != vazio então
4              RegistraVoto(voto, usuario);
5              se GetVotosRegistradosIguais() >= GetQuorumMinimo() então
6                  PublicaResultado();
7                  CalculaRestituicoes();
8                  se GetVotosRegistradosIguais() == GetQuorumTotal() então
9                      para cada juradoConfirmado => GetJuradosConfirmados() faça
10                         DisponibilizaValor(juradoConfirmado);
11                     fim
12                 senão
13                     AguardeOutroJurado(tempo);
14                 fim
15             senão
16                 AguardeOutroJurado(tempo);
17             fim
18         senão
19             AguardeUsuarios(tempo);
20         fim
21     fim
22 fim
```

Fonte: Autor

A seguir uma descrição mais detalhada dos métodos utilizados:

- ***VerificaJurado(usuario)*** é utilizado para definir se o voto vem de um dos jurados envolvidos na transação, para evitar a inclusão de terceiros em uma transação já iniciada.
- ***GetComprovantesEnviados()*** retorna a lista de comprovantes enviados pelos usuários aos jurados para o julgamento, caso nenhum comprovante tenha sido enviado não será possível votar ainda. Os jurados aguardarão o tempo do Smart Contract e ao fim deste receberão seus valores e o pagamento pelo julgamento depositado pelos usuários.

- ***RegistraVoto(voto, usuario)*** registra o voto de um jurado a favor de um dos usuários.
- ***GetVotosRegistradosIguais()*** retorna a maior quantidade de votos alcançada até o momento.
- ***GetQuorumMinimo*** retorna a quantidade mínima de votos para definir o resultado final.
- ***PublicaResultado()*** disponibilia o resultado aos usuários mas não aos outros jurados, cada usuário se não tiver usado sua oportunidade antes, poderá contestar o resultado reiniciando o fluxo com novos jurados.
- ***CalculaRestituicoes()*** define os valores que serão retornados para cada participante da transação.
- ***GetQuorumTotal()*** retorna a quantidade total de votos possíveis, jurados aptos a votar na transação.
- ***GetJuradosConfirmados()*** retorna a lista dos jurados que já votaram.
- ***AguardeOutroJurado(tempo)*** espera, pelo tempo determinado inicialmente, o voto dos jurados restantes.
- ***AguardeUsuarios(tempo)*** espera, pelo tempo determinado inicialmente, o envio dos comprovantes pelos usuários, caso o tempo finalize sem que qualquer dos usuários envie um comprovante os jurados serão restituídos e recompensados.

3.4 Considerações finais

Este trabalho não é suficiente para abranger todos os detalhes de um projeto desta grandeza, alguns dos pontos citados neste trabalho necessitam ser melhor detalhados em outros trabalhos.

A reputação como um quantitativo calculado através do histórico de transações realisadas pelo usuário não é a única opção existente, de acordo com Gomes (2009), Mamani e Gerosa (2011), Hinz (2018) esta é a forma mais simples de se computar uma reputação de um usuário dentro do sistema, mas há uma vasta gama de possibilidades e melhorias abordadas por estes autores que podem ser analisadas fora do contexto deste trabalho.

Algoritmos de detecção de conteúdo sensível e algoritmos para análise de direitos autorais são importantes para a implementação deste projeto mas também estão além dos limites da proposta deste trabalho, que foi a de apresentar uma solução viável para

a centralização das operações comerciais. Segundo Ghellere (2015) pode se utilizar visão computacional e aprendizagem de máquina para detecção de objetos em imagens e vídeos, incluindo conteúdo sensível. Cunha (2018) destaca a possibilidade de se utilizar da tecnologia Blockchain e Smart Contracts para solucionar a problemática dos direitos autorais na internet.

Parte IV

Considerações finais

4 Conclusão

O modelo de vendas C2C preza pela liberdade dos usuários comprarem e venderem sem restrições injustas ou as altas taxas cobradas pelos grandes marketplaces. A centralização dos negócios em um terceiro confiável restringe e gera custos desnecessários para as transações. Um modelo descentralizado é uma alternativa viável para alcançar altos níveis de confiança em operações, sem intermediários.

O projeto proposto trouxe um ponto de vista diferente dos atuais sintemas de vendas onde quanto menos interferência da plataforma significa passar toda a responsabilidade da segurança da transação para os usuários envolvidos. As vendas e pagamentos online podem ser seguras sem sacrificar a liberdade, elas podem ser justas sem necessitar conhecer com quem se está negociando.

A problemática da confiança necessária para realizar compras online no modelo C2C ou até mesmo no modelo B2C e a problemática da supervalorização da confiança enquanto produto comercializado pelos centralizadores, conhecidos como terceiros confiáveis, podem ter solução através de uma rede de usuários que tem muito mais vantagem em agir honestamente atrelada a um modelo personalizável de Smart Contract. As características destes contratos garantem um grande nível de confiabilidade a transação devido as propriedades de imutabilidade da Blockchain.

Para o desenvolvimento deste sistema são necessários recursos que podem ser obtidos através de um ICO (Oferta inicial de criptomoedas), um modelo de patrocínio onde integrantes da futura comunidade de usuários financiam o projeto visando receber benefícios do seu desenvolvimento no futuro, para projetos baseados em blockchain os ICOs estão atrelados ao desenvolvimento de uma nova moeda digital distribuída aos patrocinadores proporcionalmente ao valor da sua contribuição. No caso deste projeto, a moeda se chamaria TilliT em referência ao titintar das moedas reais.

4.1 Contribuições

O modelo de vendas TilliT traz como grande contribuição a proposta de uma resolução de conflitos numa venda C2C baseada num quórum distribuído com votação de jurados aleatórios de alta reputação na rede de usuários. Assim como acontece na rede blockchain com os mineradores, a honestidade dos jurados é recompensada financeiramente enquanto a sua desonestidade é punida de forma semelhante.

A proposta de atrelar um contrato a venda online garante que esta ocorrerá conforme o planejado ou então serão aplicadas as penalidades impostas. Um Smart Contract que tem

por característica a sua imutabilidade tem uma importante contribuição na manutenção da confiança já que este não poderá ser alterado para beneficiar nenhum dos lados envolvidos. Sendo aplicável a qualquer sistema de vendas C2C e não somente a modelo TilliT.

O uso de criptomoedas para o comércio de produtos e de serviços ainda está em fase inicial, este trabalho apontou como podemos utilizar moedas digitais para a compra e venda de produtos de maneira bem mais facilitada através de um Smart Contract.

4.2 Trabalhos futuros

Este trabalho não é uma obra acabada onde não se possa fazer mais nada, pelo contrário, há ainda diversas formas de se expandir este tema, como trabalhos futuros surgem como possibilidades:

1. Desenvolver um protótipo funcional do Sistema de vendas proposto;
2. Desenvolver uma moeda digital própria para o sistema de vendas distribuídas;
3. Analisar o impacto de uma alternativa segura de vendas C2C;
4. Aplicar um Smart Contract a uma venda no sistema Olx;
5. Analisar os diversos tipos e formas de determinar a reputação de um usuário num sistema P2P;
6. Desenvolver um algoritmo para filtro de conteúdo sensível;
7. Desenvolver um algoritmo para análise de direitos autorais.

Referências

ANDRADE, M. C. F. de; SILVA, N. G. O comércio eletrônico (e-commerce): Um estudo com consumidores. *Perspectivas em Gestão & Conhecimento*, Centro de Ciências Sociais Aplicadas, v. 7, n. 1, p. 98–111, 2017. Citado na página 26.

BUTERIN, V. et al. Ethereum white paper. *GitHub repository*, p. 22–23, 2013. Citado 4 vezes nas páginas 32, 33, 37 e 39.

COELHO, L. da S.; OLIVEIRA, R. C.; ALMÉRI, T. M. O crescimento do e-commerce e os problemas que o acompanham: a identificação da oportunidade de melhoria em uma rede de comercio eletrônico na visão do cliente. *Revista de Administração do UNISAL*, v. 3, n. 3, 2013. Citado na página 26.

CORDEIRO, D. A. Desafios de segurança para o comércio eletrônico. Niterói, 2016. Citado 2 vezes nas páginas 22 e 23.

CUNHA, R. M. R. da. Uma análise histórica da proteção do direito de autor e os novos mecanismos de proteção de obras musicais na era digital. *Revista da Esmam*, v. 12, n. 13, p. 241–255, 2018. Citado na página 55.

DIVINO, S. B. S. Smart contracts: Conceitos, limitações, aplicabilidade e desafios. *RJLB–Revista Jurídica Luso-Brasileira*, v. 4, p. 2771–2808, 2018. Citado 2 vezes nas páginas 29 e 31.

EBIT; NIELSEN. *Webshoppers 37*. 2018. Disponível em: <https://www.ebit.com.br/webshoppers>. Citado 2 vezes nas páginas 15 e 24.

EBIT; NIELSEN. *Webshoppers 38*. 2018. Disponível em: <https://www.ebit.com.br/webshoppers>. Citado 6 vezes nas páginas 15, 16, 21, 22, 23 e 25.

EBIT; NIELSEN. *Webshoppers 39*. 2019. Disponível em: <https://www.ebit.com.br/webshoppers>. Citado 3 vezes nas páginas 15, 35 e 49.

GHELLERE, J. S. *Detecção de objetos em imagens por meio da combinação de descritores locais e classificadores*. Dissertação (B.S. thesis) — Universidade Tecnológica Federal do Paraná, 2015. Citado na página 55.

GOMES, E. A. Segurança em aplicações p2p através de reputação inferida de redes sociais. *UFBA: Bahia*, 2009. Citado na página 54.

HINZ, V. T. Integrando reputação às técnicas de recomendação de objetos de aprendizagem em ambientes de e-learning. 2018. Citado na página 54.

KOHN, V. H.; KRUEL, A. J. O comércio c2c nas redes sociais: Uma análise de grupos no facebook. *Desenvolve Revista de Gestão do Unilasalle*, v. 5, n. 2, p. 97–125, 2016. Citado 5 vezes nas páginas 22, 35, 36, 39 e 44.

LUCENA, A. U. d.; HENRIQUES, M. A. A. Estudo de arquiteturas dos blockchains de bitcoin e ethereum. *São Paulo*, 2016. Citado 4 vezes nas páginas 28, 29, 32 e 36.

MAMANI, E. Z. S.; GEROSA, M. A. Cálculo de reputação em redes sociais. *VIII Simpósio Brasileiro de Sistemas Colaborativos*, p. 202–207, 2011. Citado na página 54.

NAKAMOTO, S. Bitcoin: Um sistema de dinheiro eletrônico ponto-a-ponto. *The Cryptography Mailing List*, v. 31, 2008. Tradução Daniel Ribeiro. Citado 6 vezes nas páginas 17, 28, 29, 30, 32 e 37.

OLIVEIRA FILHO, M. B. d. *Utilizando o protocolo Bitcoin para condução de computações multilaterais seguras e justas*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2016. Citado 5 vezes nas páginas 27, 28, 36, 37 e 43.

RIGHI, R. R.; PELLISSARI, F. R.; WESTPHALL, C. M. Escambo: um modelo de reputação e micropagamentos para sistemas peer-to-peer. In: *IV Congresso Brasileiro de Computação-CBComp*. [S.l.: s.n.], 2004. Citado na página 27.

ROCHA, R. V. da F. Blockchain e smart contracts: Como a tecnologia está mudando a intermediação e o direito empresarial. *Cadernos de Direito-UNIFESO*, v. 1, n. 2, 2018. Citado 3 vezes nas páginas 28, 31 e 39.

SILVA, H. C. S. *Estudo da experiência da marca OLX na internet: qual o impacto da confiança e do risco percebido na experiência da marca*. Dissertação (Mestrado) — Universidades Lusíada, 2016. Citado na página 25.

SOARES, M. C. G.; SOUSA, C. V. Comércio eletrônico: Motivações e hábitos de consumo. *REUNIR: Revista de Administração, Contabilidade e Sustentabilidade*, v. 8, n. 1, 2018. Citado na página 21.

TANENBAUM, A. S. Redes de computadores quarta edição. *Editora Campus*, p. 6–8, 2003. Citado 2 vezes nas páginas 27 e 28.