XXIII SEMEAD
Seminários em Administração
novembro de 2020
ISSN 2177-3866

# INOVAÇÃO EM TRANSAÇÕES DE PAGAMENTO EM LARGA ESCALA: UMA APLICAÇÃO CONCEITUAL DO SISTEMA BLOCKCHAIN

**FABIO ROMANIN**
FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC (UFABC)

**LEANDRO PETARNELLA**
UNIVERSIDADE NOVE DE JULHO (UNINOVE)

**JULIO FRANCISCO BLUMETTI FACO**
FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC (UFABC)

**ALEXANDRE ACÁCIO DE ANDRADE**
FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC (UFABC)

**SERGIO GOLDMAN**
FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC (UFABC)

Agradecimento à orgão de fomento:
Agradecimento ao Fórum de Pesquisa e Inovação vinculado ao CNPQ.

# INOVAÇÃO EM TRANSAÇÕES DE PAGAMENTO EM LARGA ESCALA: UMA APLICAÇÃO CONCEITUAL DO SISTEMA BLOCKCHAIN.

## 1. INTRODUÇÃO

Na atualidade a hibridização dos meios de comunicação e informação com as ações e a vida cotidiana tem fornecido, ao mesmo tempo, o tom e o desafio de se estabelecer e operar em uma (cada vez mais) nova lógica social. Este desafio se insere em todos os setores que se tornam mais fluídicos e dinâmicos. Em decorrência disso, esta nova ordem social chamada de digital delineia inovações que, muitas vezes, se apresentam como disruptivas e acabam por promover mudanças cuja literatura ainda não se encontra repertoriada para o tratamento do assunto. Uma delas, talvez a mais recente, é o Blockchain e a inserção dos Bitcoins no sistema financeiro mundial que se firma, a partir da necessidade de se refletir e repertoriar as discussões sobre este assunto, como tema do presente trabalho.

O referido tema se mostra como lacunar na medida em que o sistema financeiro mundial ainda se encontra amparado por meios de transações há muito instituído. Um exemplo disso nos remete aos intermediários financeiros que, por sua vez, existem para evitar que ocorra a duplicação ou fraude nas operações de pagamento (NAKAMOTO, 2009). Assim, se atualmente essas entidades garantem a efetivação das transações financeiras mantendo a privacidade, segurança e anonimato dos usuários, pode-se afirmar então que, em tese, são confiáveis e são parte fundamental da estabilidade econômica de muitos países. Entretanto, para manter a credibilidade e a confiança, essas instituições devem seguir normas e controles locais e mundiais de modo a coibir práticas ilegais de movimentações financeiras que patrocinem fraudes, crimes, entre outras ações associadas como tráfico de drogas ou, ainda, a lavagem de dinheiro. Porém, ainda hoje o sistema financeiro mundial sofre com a interferência de indivíduos mal-intencionados obrigando as instituições pertencentes ao sistema financeiro a investir cada vez mais em segurança da informação.

O investimento em sistemas de segurança acaba por gerar a desconfiança sobre a presença de intermediários em transações financeiras. Esta desconfiança, alinhada ao avanço tecnológico e informacional, fez surgir uma solução disruptiva no cenário mundial: a criação de uma criptomoeda denominada Bitcoin. Essa moeda digital surgiu para descentralizar o controle das moedas e a interferência de intermediários nas operações financeiras (GARROD, 2016, p 01) e é justamente esta criptomoeda que se firma como objeto do presente artigo.

Para uma melhor compreensão do assunto se faz importante esclarecer que as criptomoedas necessitam de uma plataforma para a sua operacionalização. Em consequência, a principal inovação dessa invenção é justamente sua plataforma concebida como Blockchain. Esta, por sua vez, surgiu como uma forma de resolver os problemas de duplicação de transações (*double spend*) e foi introduzido por Satoshi Nakamoto, em 2009, por meio da criação do Bitcoin e é nela que os "nós" da rede anexam validações mutuamente acordadas. Essa plataforma abriga as transações no *ledger* (espécie de livro caixa) que estabelece quem possui o que. A tecnologia era apenas um termo computacional para explicar como estruturar e compartilhar dados, mas hoje ela é considerada uma das cinco maiores evoluções da computação (SWAN, 2015).

Todo o dito, em caráter introdutório, nos leva a considerar que o Bitcoin se firma como uma aplicação inovadora para as transações financeiras na atualidade. Entretanto, o Bitcoin tem algumas lacunas que impedem sua adoção em larga escala como, por exemplo, o anonimato das transações (YLI-HUUMO, et al. 2016); (HERRERA, 2014). O referido se firma como um problema já que os usuários podem realizar operações utilizando pseudônimos, e, portanto,

teoricamente garantem o anonimato. Não obstante, o sistema ainda não assegura privacidade total dos dados do usuário, pois há meios de rastrear e identificar o usuário (MOSER; BOHME; BREUKER, 2013, p. 01). Em outras palavras: Se por um lado o Bitcoin se apresenta como uma inovação disruptiva capaz de eliminar os intermediários e deixar as transações financeiras mais seguras, por outro lado, o fato do sistema permitir o registro em pseudônimo abre brechas para circulação ilegal de recursos que financiam práticas criminosas desvelando, desta maneira, um problema que, por sua vez, direcionou a presente pesquisa.

Frente ao problema exposto questionou-se, então: Quais seriam as premissas e/ou os parâmetros para que o Bitcoin pudesse ser adotado em larga escala mas, ao mesmo tempo, garantindo o anonimato do usuário nas transações de pagamento? Para responder esta questão, foi estabelecido, em um primeiro momento, o objetivo de analisar o Bitcoin como fonte de pagamento, em larga escala, dentro da tecnologia Blockchain. Questões relacionadas a preservação do anonimato dos usuários ou, ainda, a compreensão de como as tecnologias privadas do Blockchain (*Hyperledger*) podem se firmar como uma opção em larga escala para operações de pagamento mantendo o anonimato dos usuários também foram consideradas. Já em um segundo momento, objetivou-se verificar se há uma alternativa mais efetiva de preservar o anonimato dos usuários dentro da plataforma pública do Blockchain. Para tanto, alguns estudos sobre plataformas de operação do Blockchain foram realizados para, em um terceiro momento, estabelecer uma matriz de comparação que possa dar a tônica das discussões acerca deste assunto e, ao mesmo tempo, caminhos que possibilitem responder à questão direcionadora anteriormente apresentada. A referida matriz foi delineada a partir da fundamentação teórica a seguir.

## 2 FUNDAMENTAÇÃO TEÓRICA

### 2.1 Bitcoin e Blockchain

Segundo (ZIEGELDORF, 2015) o Bitcoin pode ser descrito como um sistema de contabilidade descentralizado no qual as contas dos usuários estão associadas a chaves públicas de um esquema de criptografia assimétrica. Segundo (KOSHY P., KOSHY D., E MCDANIEL, 2014, p. 02) para evitar que pessoas usem dinheiro que não lhes pertençam, ou reutilizem dinheiro que já gastaram (dupla despesa ou *double spending*), todo o histórico dessas transações deve estar disponível publicamente. Como o Bitcoin não é controlado por nenhuma entidade central, o sistema desafia a regulamentação e os esforços de fiscalização, o que aumenta as preocupações dos reguladores financeiros e dos criminosos do cibercrime. Na verdade, o Bitcoin é muito diferente de muitas outras moedas digitais, foi projetado para uso de identidades pseudônimas (MOSER, 2013, p. 01).

De acordo com (YLI-HUUMO et. al, 2016) o Bitcoin foi a primeira aplicação da tecnologia Blockchain. O Bitcoin criou um ambiente descentralizado para criptomoedas, onde os participantes podem comprar e trocar produtos com uma moeda digital. Segundo (ZIEGELDORF 2015, p. 02), ele é o melhor exemplo de como uma rede P2P descentralizada, que acompanha todas as transferências de dinheiro entre seus usuários, funciona. As transferências são registradas no Blockchain, que são constantemente validadas pelos participantes da rede através de uma prova de trabalho. O gasto duplo (*double spending*) de Bitcoins é eliminado, desde que a maioria dos participantes da rede, com poder computacional, seja formado por endereços honestos sem conluios. Os usuários Bitcoin podem ter uma quantidade praticamente ilimitada de identidades criptográficas, chamadas endereços. Os endereços são usados para armazenar e receber Bitcoins. Um endereço é basicamente o hash de uma chave pública.

Para Ruffing et al (2014, s.n), a rede Bitcoin, que não requer nenhum banco central ou autoridade monetária, está emergindo como uma nova maneira potencial de realizar transações financeiras em todo o mundo. O uso de pseudônimos para proteger a privacidade dos usuários tem sido uma característica atraente para muitos de seus adotantes. Entretanto, apesar de ser uma tecnologia nova e sendo, ainda, pouco conhecido o seu potencial de aplicação no dia-a-dia de empresas, bancos, pessoas físicas, comércio e indústrias, o Bitcoin se apresenta, nesse momento, como uma mudança profunda no cenário tecnológico. Isto porque, ele promove um potencial disruptivo da plataforma de transações financeiras já que, ao transacionar por meio de criptomoedas, o Bitcoin causou euforia e, ao mesmo tempo, muita desconfiança no mercado e nas autoridades reguladoras que, por enquanto, sequer sabem como controlar e fiscalizar tal inovação (SWAN, 2015).

Com a principal característica de eliminar a necessidade de intermediários das transações financeiras, tornando-as mais seguras, confiáveis, eficientes e mais baratas (NAKAMOTO, 2009), algumas plataformas privadas de Blockchain estão surgindo justamente para resolver lacunas que o Bitcoin apresenta. Uma das mais famosas é a *Hyperledger*, desenvolvida por um consórcio de empresas liderado pela IBM. Entretanto, empresas virtuais de *Mixing Service* (serviços de mesclagem) também estão sendo criadas com o objetivo de melhorar a questão do anonimato se firmando, porém, como soluções pagas e que aparentemente não possuem escala suficiente para suportar uma alta demanda de transações. Atualmente, grandes grupos econômicos ou consórcios que, de certa forma, criam seus algoritmos, regras e limitações estão investimento na criação de criptomoedas e, por isso mesmo, a tecnologia Blockchain, com seu potencial disruptivo, se apresenta como uma ameaça e, ao mesmo tempo, como uma oportunidade de mudança para as instituições financeiras globais.

Segundo Christidis & Devetsikiotis (2019), Blockchain é uma estrutura distribuída de dados que é replicada e compartilhada entre os membros de uma rede. O conceito surgiu como uma forma de resolver os problemas de *double spend* e foi introduzido por Satoshi Nakamoto, em 2009, por meio da criação do Bitcoin. Como resultado de como os nós na rede Bitcoin anexam validações, mutuamente acordadas, o Blockchain abriga as transações no *ledger* (espécie de livro caixa) que estabelece quem possui oque. Desta maneira, percebe-se com Laurence (2017), que o Blockchain que, era apenas um termo computacional para explicar como estruturar e compartilhar dados, atualmente é considerada uma das cinco maiores evoluções da computação. A inovação vem da incorporação de velhas tecnologias à novos métodos. Por isso, o Blockchain pode ser pensado como uma base de dados distribuída onde um grupo de pessoas controla, armazena e compartilha informações. Trata-se de uma tecnologia abrangente, de diferentes tipos e aplicações, que é integrada através de plataformas e hardwares em todo o mundo.

Com o objetivo de criar um ambiente descentralizado onde não há a participação de um terceiro no controle das transações e informações (YLI-HUUMO et. al, 2016), o Blockchain permite que qualquer participante de uma rede veja o sistema de registro. Segundo o autor, esta tecnologia terá um impacto significativo em uma grande quantidade de indústrias no futuro, inclusive, nos serviços financeiros.

A ideia central dos Blockchains, segundo Nakamoto (2009), é bastante simples: as transações são agrupadas em blocos com registro de hora e data da transação (*timestamp*). Cada bloco é identificado por seu código criptográfico (*hash*). Cada bloco faz referência ao *hash* do bloco que veio antes dele. Ele estabelece um link entre os blocos criando, assim, uma cadeia de blocos ou Blockchain. Qualquer nó com acesso a esta lista ordenada e ligada a lista de blocos pode lê-lo e descobrir qual é o estado dos dados que estão sendo trocados na rede.

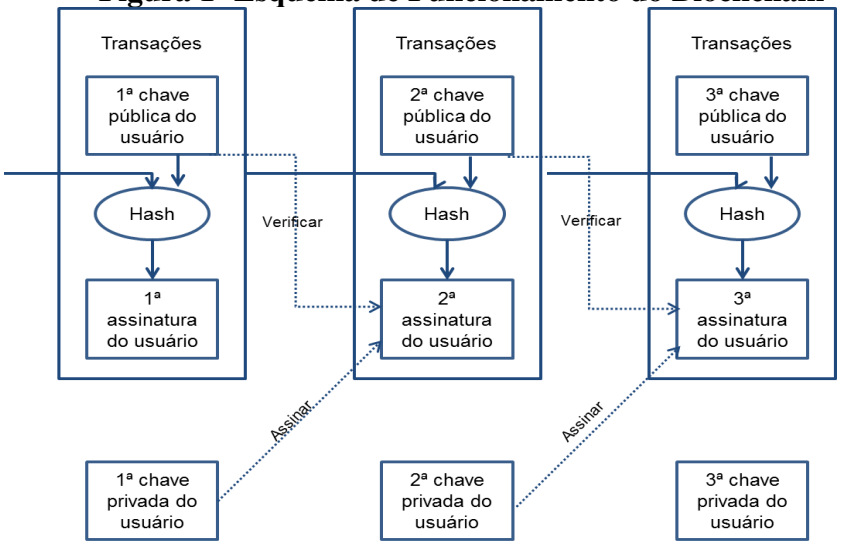
O primeiro bloco da cadeia é denominado gênesis. Conforme Nakamoto (2009), a rede Blockchain é executada quando um conjunto de nós que operam na mesma cadeia de blocos

validam a cópia da transação que cada um detém. Um nó geralmente pode atuar como uma entrada e apontar para vários usuários de blocos diferentes na rede, mas, por simplicidade, assume-se que cada usuário transaciona na rede através de seu próprio nó. Esses nós formam uma rede *peer-to-peer* onde: a) Os usuários usam sua chave privada para assinar suas próprias transações, e são abordáveis na rede através de sua chave pública e b) o uso da criptografia traz autenticação, integridade e não repúdio na rede. Todas as transações assinadas são transmitidas pelo nó de um usuário aos seus pares.

Os nós sempre consideram a cadeia mais longa como correta e continuará trabalhando para estendê-la. Se dois nós transmitirem diferentes versões do próximo bloco simultaneamente, alguns nós podem receber um ou outro primeiro. Nesse caso, eles trabalham no primeiro que receberam, mas salva o outro, caso fique mais longo. O nó será quebrado quando a próxima prova de trabalho (*proof-of-work*) é encontrada e um nó se torna mais longo; os nós que estavam trabalhando no outro mudarão para o mais longo (NAKAMOTO, 2009).

Novas transmissões de transações não necessitam necessariamente alcançar todos os nós. Enquanto eles alcançarem muitos nós, eles entrarão em um bloco antes disso. As transmissões de blocos também são tolerantes a mensagens descartadas. Se um nó não receber um bloco, ele o solicitará quando receber o próximo bloco e perceberá que perdeu um.

**Figura 1- Esquema de Funcionamento do Blockchain**




**Fonte:** (NAKAMOTO, 2009)

De acordo com Swan (2015), esta tecnologia está dividida em três estágios potenciais, sendo elas, I) Blockchain 1.0 e a criação de criptomoeda, transferência de valores, sistema de pagamento e remessa de dinheiro para o exterior; II) Blockchain 2.0 e o uso de contratos inteligentes e da tecnologia em transações financeiras e III) Blockchain 3.0 utilizada nas áreas governamentais, saúde, ciência, alfabetização, cultura e arte.

Na visão de Swan (2015), as três categorias elencadas têm a função e o potencial de descentralizar e simplificar as operações. A etapa Blockchain 1.0 é para a descentralização de dinheiro e pagamentos, enquanto etapas 2.0 e 3.0 são para descentralizar os mercados de forma geral. Já Delivorias (2016), acredita que o uso desta e de outras metodologias similares pertencentes ao grupo de tecnologias de razão distribuída (*distributed ledger technologies*) poderia se estender aos serviços financeiros tradicionais, ou seja, para além da moeda como tratado a seguir.

## 2.2 Sistema financeiro e Blockchain

Até o surgimento da tecnologia Blockchain, os ativos e transações de valores digitais eram passiveis de infinitas cópias e não havia forma de confirmar que uma transação não teria sido duplicada sem a presença de um intermediário. A participação de um terceiro confiável, como por exemplo, um banco, era uma condição *sine-qua-non* para confirmar que o ativo ou moeda fora transacionado apenas uma vez, que não houve risco de dupla execução da operação. (SWAN, 2015). Nakamoto (2009) propôs uma solução para resolver o problema de "*double spend*" usando uma rede *peer-to-peer* que transcreve data e hora da rede, colocando-as em uma cadeia contínua e validada por um certificado digital ou *hash* (impressão digital da transação), formando um registro que não pode ser alterado sem que tenha de refazer a prova de trabalho. Segundo Yli-Huumo, et. al. (2016), *double spend* é o resultado da duplicação bem sucedida de uma transação envolvendo dinheiro. Em decorrência disso, o Blockchain resolve o problema de duplicação combinando arquivo de tecnologia compartilhada em protocolo de rede *peer-to-peer* com chave pública criptografada para assegurar um novo formato de transferência de moeda ou ativo digital. Dessa forma, o usuário não precisa confiar a um terceiro a concretização de uma transação, basta confiar no sistema. Este sistema pode operar, enquanto exemplo, a partir de variadas classes como apresentado na tabela abaixo:

**Tabela 1 - Aplicação de Blockchain além das moedas**

| CLASSE | EXEMPLO |
|---|---|
| Geral | Contratos de custódia, contratos vinculados, arbitragem de terceiros, transações de assinaturas múltiplas. |
| Transações financeiras | Ações, *private equity* , *crowdfunding, bonds* , fundos mútuos, derivativos, anuidades, fundos de pensão. |
| Registros públicos | Títulos de propriedade de terras, registro de veículos, licenças de negócios, certidões de casamento, certidões de óbito. |
| Identificação | Licença de motorista, identificação do veículo, passaportes, registro de votos. |
| Arquivos pessoais | Empréstimos, contratos, apostas, assinaturas, vontades, documentos de confiança. |
| Atestados | Apólice de seguro, título de propriedade, documentos notariais. |
| Chaves de bens | Imóvel, quartos de hotéis, carros alugados, acesso a veículos. |
| Ativos intangíveis | Patentes, marcas registradas, propriedade intelectual, reservas, domínios. |

**Fonte:** (SWAN, 2015 - adaptado pela lista Ledra Capital Mega Master Blockchain).

É claro que junto às mudanças no modo como as transações de pagamentos são tratadas ou intermediadas, emerge a necessidade de transformação da regulamentação, implementação e disseminação dessa nova tecnologia. Algumas instituições já estão realizando testes de pagamentos e transferências entre contas no padrão Bitcoin (WALCH, 2015), no entanto, a questão do anonimato ainda é um desafio a ser solucionado para que a tecnologia possa ser usada de forma segura, confiável e em larga escala (YLI-HUUMO, et al. 2016); (HERRERA, 2014). Os Bancos Centrais acompanham de perto essa evolução e fazem seus próprios estudos mais relacionados as questões operacionais e regulatórias.

Segundo Swan (2015), a questão da privacidade é muito importante no processo de confiabilidade e autenticidade nas transações de pagamento. Por esse motivo, o uso de intermediários confiáveis garante a credibilidade e autenticidade nas transações financeiras, por outro lado, cria certa dependência dessas instituições. É claro que outras variáveis, além do anonimato, formam o gargalo do Blockchain como, por exemplo, a regulamentação, escalabilidade, privacidade, segurança e riscos. Todavia, esses *gaps* são pontos chave para que

a tecnologia ganhe confiança e, por conseguinte, uso em escala pelas empresas e usuários. Mas é ponto chave, também, para que usuários de Bitcoin, criando contas usando pseudônimos, possam realizar fraudes. Em decorrência disso, as instituições financeiras precisam conhecer seus clientes e, também, serem capazes de identificar potenciais usuários mal intencionados que usam sua estrutura para transformar recursos ilegais em legais (MÖSER; BÖHME; BREUKER, 2013). A solução para estas questões esteja, talvez, na utilização da criptografia alinhada aos sistemas contábeis.

### 2.2.1: Blockchain: criptografia e o modelo disruptivo

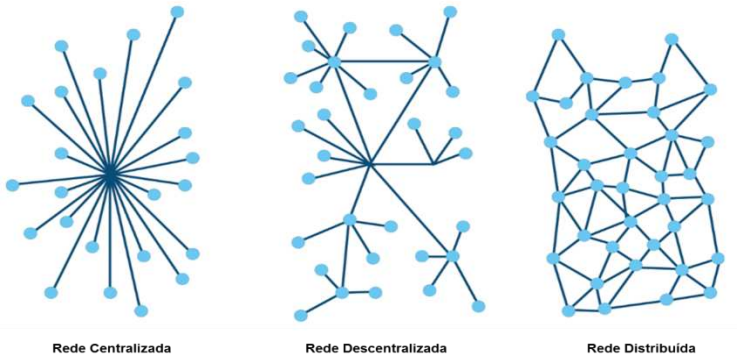
A criptografia tem sido utilizada, em escala global, como meio de garantir a segurança de dados entre seus atores. A rigor, isto implica em dizer que, por meio da criptografia, pode-se enviar uma mensagem através de uma rede aberta e saber que eventualmente chegará ao destinatário com certo grau de confiança e integridade. Com as técnicas de integridade, podemos saber que a informação recebida pelo destinatário estará de acordo com o pretendido. Aliás, usando a criptografia, pode-se preservar a integridade das mensagens ao longo do tempo, diante da falha de software e hardware. Aliás, quando a criptografia começou a ficar mais conhecida e disponível ao final da década de 1980, muitos pesquisadores começaram a usá-la para criar moedas digitais lastreadas em moedas nacionais, metais preciosos e ouro. Esse modelo não funcionou devido a vulnerabilidade a ataques de hackers e governos e ao uso de intermediários para mediar as transações (ANTONOPOULOS, 2017). Em decorrência disso, a complexidade da criptografia financeira exige habilidades derivadas de disciplinas diversas não muito amigáveis, ou seja, os sistemas de criptografia financeira simplificarão ou omitirão disciplinas críticas e é justamente neste ponto que se insere a ideia da contabilidade. Isto porque, são os conceitos de contabilidade que viabilizam os desenvolvedores de sistemas de criptografia financeira a criarem sistemas complexos que garantam não perder valor enquanto todos seguem as regras e para identificar com eficiência onde as regras não são seguidas.

É certo que o domínio científico da criptografia permite a resolução de problemas a partir da paridade e da logica matemática. Entretanto, é importante ressaltar que é justamente este domínio que garante, por exemplo, a confidencialidade (através de algoritmos de criptografia), a integridade (com a possibilidade de *hashes* e digestões de mensagens) e a autenticação (por meio de assinaturas digitais e cadeias de *hash*) das informações. Em decorrência disso, ao associar a criptografia á informação contábil, cria-se a possibilidade de se obter registros e realizar a mensuração, a avaliação, a análise e a demonstração da informação contábil do mesmo modo no qual se realiza os registros das operações convencionais.

Sobre a segurança e a integridade das informações, o sistema pode ser eficiente a partir da utilização do que Dapp e Karollus (2016), enumerou como sendo as sete características disruptivas do Blockchain para o setor financeiro, sendo elas, 1) apresentar todo o histórico das transações realizadas; 2) possuir várias cópias idênticas, já que não há um único ponto de ruptura; 3) tornar a informação disponível ao público, ou seja, todos podem procurar o conteúdo dos blocos, porém podem ver ou não na íntegra; 4) pode haver múltiplos Blockchains vinculados as mais diversas transações; 5) a informação é criptograficamente assegurada para ser inviolável; 6) as informações armazenadas podem representar outros ativos, não apenas moeda e 7) podem ser construídos programas que aproveitam as informações no Blockchain.

Aqui, vale ressaltar que a tecnologia Blockchain efetivamente remove a necessidade de uma câmara de compensação ou estabelecimento financeiro para atuar como intermediário de uma transação de pagamento transferindo o controle e o poder de uma autoridade central para muitas, facilitando trocas de valor rápidas, seguras e de baixo custo (FERENZY et al., 2015). Na figura 2 exemplifica-se as três formas de tratamento da transação, com a participação de intermediário (rede centralizada ou rede descentralizada) e sem a participação de intermediário (rede distribuída):

**Figura 2 - Diferentes formatos de rede**




**Fonte:** https://forum.bitcoin.pl

Como se visualiza na figura acima, a tecnologia utilizada pelos Blockchain pode ser tão disruptiva quanto a internet graças ao seu potencial de uso de dados transparentes em tempo real, na liquidação imediata de transações e no uso de contratos inteligentes que podem ser auto executados, simplificando a automação de todo tipo de processo, sem intermediários, com transparência, segurança e baixo custo. Segundo Swan (2015), a tecnologia Blockchain poderia, ainda, ser implementada e adotada muito mais rapidamente do que a Internet, tendo em vista os efeitos de rede de internet de alcance global e conectividade celular.

No cerne de toda a questão apresentada, encontra-se a recompensa oferecida ao trabalho de processamento computacional. É neste ponto que, de acordo com Swan (2015, p. 12), enredam-se o Bitcoin que, por sua vez, é conhecido como o processo de mineração de dados no qual os usuários oferecem seu poder de computação para verificar e registrar pagamentos no livro de contas público. Em outras palavras: indivíduos ou empresas se envolvem em mineração em troca de taxas de transação de Bitcoins recém-criados e, desta maneira, além da mineração, como qualquer moeda, os Bitcoins podem ser obtidos em troca de dinheiro fiduciário, produtos e serviços. Os usuários podem enviar e receber Bitcoins eletronicamente por uma taxa de transação opcional usando carteira de software em um computador pessoal, dispositivo móvel ou aplicativo web.

É certa, concordando com Antonopoulos (2017), a possibilidade de se verificar pagamentos sem executar um nó de rede completo. Isto porque, um usuário só precisa manter uma cópia dos cabeçalhos dos blocos da prova mais longa da cadeia de trabalho e obter a árvore Merkle conectando a transação e o bloco que contém o registro (*timestamped*). Entretanto, mesmo não sendo possível verificar a transação si, a segurança se estabelece na medida na qual o bloco é vinculado em um lugar na cadeia onde o usuário pode ver que um nó de rede aceitou, e os blocos foram adicionados depois que ela ainda confirmou que a rede aceitou. Por consequência, conforme Nakamoto (2009) constatou, a verificação se firma como confiável já que os nós honestos controlam a rede, mas se tornam mais vulneráveis se a rede for dominada por um nó invasor. Enquanto os nós de rede podem verificar suas próprias transações, o método simplificado pode ser enganado por transações desenvolvidas por um hacker. Uma estratégia para proteger o sistema contra esta invasão, seria aceitar alertas de nós de rede quando eles detectarem um bloco inválido, solicitando que o software do usuário baixe o bloco completo e as transações alertadas para confirmar a inconsistência.

Frente às possibilidades que se descortinam por meio da verificabilidade e confiabilidade das transações em Blockchain e dor processos de mineração, é muito provável que as empresas que recebem pagamentos frequentes queiram executar seus próprios nós para uma segurança mais independente e uma verificação mais rápida. Por outro lado, as entidades públicas e reguladoras se vêm obrigadas a entender, normatizar e possibilitar os negócios, a esta rede, associados. Em consequência, diferentes modelos de Blockchain podem ser

concebidos, mas sempre respeitando a sua natureza de ser público ou privado. Para entender a diferença entre Blockchain público e privado, considere a diferença entre a Internet, que é pública e disponível para todos, e intranets, que são criadas por entidades específicas e apenas disponíveis para determinadas pessoas com permissão. Aqui se visualiza uma forma que o criador da tecnologia desenvolveu para garantir a integridade do sistema e validar as transações, ou seja, ocorre a criação de mecanismos de incentivo financeiro e consenso incorporado ao sistema. As transações são transparentes, no entanto, são anônimas.

A rigor, qualquer pessoa pode baixar o software e começar a executar um nó público em seu dispositivo local e começar a validar transações na rede, participando, dessa forma, do processo de consenso. Não obstante, qualquer individuo em qualquer parte do mundo pode enviar transações através da rede e esperar que sejam incluídas no Blockchain. Assim como qualquer pessoa pode ter acesso a leitura das transações no explorador de blocos públicos (VOSHMGIR E KALINOV, 2017). O bloco público requer esforços de programadores de software usando computadores potentes para implementar os protocolos, tais esforços devem ser recompensados. O protocolo fornece um conjunto de regras para o uso de técnicas criptográficas para enviar e receber transações usando uma rede distribuída para registrar e validar transações (EVANS, 2014, p.11). Ainda a este respeito, de acordo com Voshmgir & Kalinov (2017), as permissões de leitura podem ser públicas ou restritas de forma arbitrária. Os aplicativos, por exemplo, incluem o gerenciamento de banco de dados e auditoria que são de uso interno de uma única empresa e, portanto, a legibilidade pública pode, em muitos casos, não ser necessária.

É claro que ao contrário do Blockchain público, os consórcios operam sob a liderança de um grupo não sendo permitido que qualquer pessoa com acesso à Internet participe do processo de verificação das transações. Os consórcios são mais rápidos, têm maior escalabilidade e oferecem mais privacidade de transações. Essa estrutura é usada principalmente no setor bancário. Alguns especialistas dizem que esse sistema não é um Blockchain. Aqui, ressalta-se que muitos argumentam que o Blockchain privado ou consórcio pode sofrer o destino das Intranets na década de 1990, quando as empresas privadas construíram suas LANs particulares ou WANs em vez de usar a Internet pública, mas se tornou obsoleta, especialmente com o advento de SAAS na Web2 (VOSHMGIR e KALINOV, 2017).

O Blockchain público apresenta atualmente um problema de escalabilidade, o que significa que a rede só pode lidar com poucas transações por segundo, tornando-o inviável para grandes volumes. Tanto o Bitcoin quanto o Ethereum só podem lidar com menos de uma dúzia de transações por segundo, enquanto que a Visa sozinha exigiria 100k transações por segundo em horários de pico (VOSHMGIR e KALINOV, 2017). Uma solução criada pela BigchainDB para resolver essa deficiência, foi combinar o poder de escalabilidade do banco de dados distribuído com elementos imutáveis de Blockchains.

**Tabela 2 - Descrição sintetizada de acesso às transações - REDE P2P Pública, Privada e Consórcio**

| | PÚBLICO | PRIVADO | CONSÓRCIO |
|---|---|---|---|
| **ACESSO** | Aberto para leitura e escrita | Permissão para leitura e ou escrita | Permissão para leitura e ou escrita |
| **PARTICIPAÇÃO** | Pública | Organização ou grupo | Organizações ou grupos específicos |
| **AGILIDADE** | Mais lento | Mais rápido | Mais rápido |
| **SEGURANÇA** | Prova de trabalho<br>Prova de participação<br>Outros mecanismos | Participação pré-aprovada | Participação pré-aprovada |
| **IDENTIDADE USUÁRIO** | Anônimo / Pseudônimo | Conhecimento do usuário | Conhecimento do usuário |
| **ATIVO** | Nativo | Qualquer ativo | Qualquer ativo |

**Fonte:** Estudo Blockchain - Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation – Nov/2016 e Chris Skinner´s blog (Adaptado pelo autor).

### 2.3 Regulamentação do Blockchain

As leis, os regulamentos e as políticas de supervisão relevantes visam alcançar objetivos amplos, como a transparência do mercado, a segurança, a solidez das instituições financeiras e o funcionamento eficiente e efetivo do sistema financeiro. Geralmente não visam favorecer uma tecnologia eletrônica específica (FEDERAL RESERVE, 2016). Neste sentido, a tecnologia Blockchain tem implicações sobre o modo como transacionamos ativos, e o seu potencial de inovação é difícil de mensurar. Os reguladores financeiros devem desenvolver uma melhor compreensão do potencial de impacto da tecnologia Blockchain à medida que continuam a envolver-se em sua regulação pragmática (KIVIAT, 2015).

No que concerne a questão da regulamentação da tecnologia Blockchain nos EUA, o Federal Reserve diz que dependendo da época, da jurisdição e do problema abordado, algumas organizações multilaterais receberam papéis como intermediários financeiros. A necessidade fundamental de coordenação muitas vezes exigiu ação conjunta através de entidades jurídicas novas ou existentes para, no mínimo, fornecer organização e governança.

O risco regulatório é inerente às tecnologias disruptivas. Embora nos países do Leste os reguladores tenham adotado uma linha relativamente rígida em criptografia (figura 6), a posição mais frouxa do Ocidente significa que, em equilíbrio, o clima regulatório é relativamente benigno, afirmam (BRENNAN e LUNN, 2016). No Brasil, já se discute a regulamentação do uso do Bitcoin como moeda eletrônica através do projeto de Lei nº 48 de 2015 de autoria do deputado Reginaldo Lopes - PT/MG, que está sendo debatido na Câmara dos Deputados por meio da Comissão de Defesa do Consumidor. Essa discussão pode ter efeito direto na regulamentação da tecnologia Blockchain.

Internacionalmente, o Bitcoin ainda está em uma área cinzenta – as regulamentações sobre a criptomoeda não estão claras internacionalmente. Algumas nações como China, Rússia e Índia proibiram as transações em Bitcoin em graus variados. Essas diferenças regulatórias são problemáticas para o desenvolvimento da tecnologia porque o cumprimento de regras diferentes pode tornar-se excessivamente onerosa (HOROWITZ, 2016).

Delivorias (2016) reconhece que a tecnologia Blockchain tem o potencial de contribuir positivamente para o bem-estar e o desenvolvimento econômico dos cidadãos, mas enfatiza que tais tecnologias envolvem riscos que precisam ser abordados de forma adequada para aumentar sua confiabilidade. Abordar esses riscos exigirá o desenvolvimento de um quadro legal sólido

que acompanhe a inovação, mas observa que, se um regulamento for adotado em uma fase muito precoce, pode não estar bem adaptado a um estado de coisas que ainda está em fluxo e, portanto, pode transmitir a mensagem incorreta ao público sobre as vantagens ou a segurança de tais tecnologias. É certo que a tecnologia poderia reduzir a incerteza relacionada aos termos do contrato e ajudar a tornar o processamento das ações corporativas mais automatizadas através do uso de contratos inteligentes. Embora os bancos possam ver os benefícios, eles ainda não se comprometeram com um sistema em que os concorrentes possam acessar os dados uns dos outros e, assim, reunir informações sobre as transações de cada um (DELIVORIAS, 2016).

A partir do exposto percebe-se, então, que trazer à luz sobre esta área cinzenta na qual toda a discussão, até o presente, realizada se faz tão importante quanto necessária. Para tanto, buscou-se responder a questão de pesquisa apresentada em caráter introdutório, ou seja, sobre quais seriam as premissas e/ou os parâmetros para que o Bitcoin pudesse ser adotado em larga escala mas, ao mesmo tempo, garantindo o anonimato do usuário nas transações de pagamento, a partir da metodologia que se descreve a seguir.

## 3. METODOLOGIA

A partir da fundamentação teoria apresentada, para este trabalho, optou-se por constituir uma matriz linear para comparar as variáveis mais importantes de acordo com as características de funcionamento de cada plataforma as quais se apresentaram como necessárias para simular o funcionamento das operações de pagamento. A matriz linear foi escolhida pela objetividade dos resultados de uma tecnologia pouco conhecida e carente de resultados práticos.

A matriz contempla as tecnologias utilizadas de maneira pública (no formato Bitcoin) comparada a tecnologia privada *(Hyperledger).* A tecnologia *Hyperledger* foi escolhida considerando os avanços tecnológicos, investimentos em pesquisas e, principalmente, pela constituição de um consorcio formado por mais de 250 empresas de vários setores, destacando-se, entre eles, o setor financeiro. Aqui, vale lembrar quer o *Hyperledger* utiliza o Blockchain como plataforma tecnológica para criar seus produtos e serviços.

Como técnica de pesquisa, a partir do arcabouço apresentado, optou-se pela pesquisa exploratória e documental. O objetivo da escolha desse tipo de pesquisa foi determinado pela complexidade de um tema recente, não repertoriado. A mesma foi realizada no período entre 20 de fevereiro e 30 de agosto de 2019, utilizando-se, para tanto, dos trabalhos científicos depositados nas bases de dados portal Capes de periódicos, base Scopus e Google Acadêmico. Excluindo-se as duplicidades e os temas não vinculados a especificidade do assunto aqui tratado, foram selecionados 70 documentos relacionados ao tema Blockchain, Bitcoin, Pagamentos e Anonimato. A partir destes documentos, a matriz apresentada na figura 3, a seguir, pode ser constituída:

**Figura 03- Matriz comparativa rede privada versus rede pública**

| | | Anonimato | Segurança | Tempo de Processamento | Escalabilidade | Consumo de Energia | Validação da Transação | Ataque de Hackers | Acesso à Tecnologia | Smartcontract | Pagamentos |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Bitcoin | MÉDIO | MÉDIO | 10 minutos por operação | 100k transações/ dia | ALTO | ALTO | BAIXO | ALTO | NA | SIM |
| | Hyperledger | ALTO | ALTO | Assíncrono | 10k transações/ segundo | BAIXO | ALTO | NA | BAIXO | SIM | SIM |
| Protocolos mistos | Chipmixer.com | ALTO | ALTO | 10 min – 24 hrs | NA | NA | NA | NA | NA | NA | SIM |
| | Cryptomixer.io | ALTO | ALTO | 0 - 48 horas | 2000 Coins | NA | NA | NA | NA | NA | SIM |
| | Bitcoinmix.org | ALTO | ALTO | 0 - 48 horas | NA | NA | NA | NA | NA | NA | SIM |

**Fonte:** Dos autores

Os itens avaliados na matriz foram definidos de acordo com as principais características disruptivas da tecnologia e respectivos problemas ainda não solucionados, principalmente na solução do formato Bitcoin.

A tecnologia Blockchain é caracterizada como disruptiva porque representa as realizações de transações de pagamento sem a participação de um intermediário confiável que garanta a validação e não duplicação da operação. Adicionalmente, agrega-se à inovação o fato de o Blockchain ser uma plataforma de uso público e imutável. Para cada variável da matriz foram considerados os níveis de escala básica de três pontos (baixo, médio e alto). Estes, por sua vez, foram associados e apresentados com escalas de tempo e quantidade para mostrar as distorções entre a plataforma pública versus a plataforma privada tornado capaz a construção de três constructos, sendo eles, o de tempo, de processamento e o de escalabilidade. Ainda sobre a matriz, um último item – o de pagamentos, foi incluído para reforçar quais redes têm a condição de realizar estas transações de pagamento.

Ainda na construção da matriz, estabeleceu-se os seguintes conceitos para o entendimento de cada relação estabelecida:

**Anonimato:** é um dos principais objetos desse estudo, nele são considerados os níveis de confiança que o usuário pode ter que sua identidade não será ameaçada quando vier a realizar transações de pagamento utilizando umas dessas redes. Vale ressaltar que o anonimato é um dos principais entraves do Bitcoin. É claro que é possível rastrear uma operação pelo valor transacionado, pelo IP da máquina, etc. Entretanto, no caso do *Hyperledger*, por se tratar de uma plataforma privada, ele pode perfeitamente ser programado para manter a confidencialidade dos usuários de acordo com o tipo de negócio e a escolha da empresa que utilizará a tecnologia através dos contratos inteligentes.

**Segurança:** nível de segurança que usuário tem que seus dados pessoais não serão desvendados por hackers durante a realização de uma transação.

**Tempo de processamento:** apresenta as escalas de tempo para medir quanto leva para que uma transação seja 100% concluída. Cabe ressaltar que as operações de mixagem são consideradas dependentes do tempo de processamento na rede Bitcoin, portanto, os tempos deverão ser somados.

**Escalabilidade:** são consideradas as quantidades de operações que cada rede pode executar em seu limite. A escalabilidade dos protocolos mistos será afetada pela limitação da escalabilidade da rede Bitcoin.

**Consumo de Energia:** na rede Bitcoin para que um novo bloco seja minerado há um consumo elevado de energia ao passo que na rede privada os blocos já são constituídos e validados por meio de uma rede própria. Os protocolos mistos (serviço de mesclagem) não tem medida expressiva de consumo de energia, pois sua função é apenas misturar os valores já validados dentro do bloco público.

**Validação da Transação**: a validação das transações tanto da rede pública quanto da privada apresenta bons níveis de confiabilidade. A rede pública é mais contundente, devido a quantidade de validadores a nível global. Já a rede privada tem validadores próprios indicados pelos detentores da plataforma, diminuindo o nível de credibilidade da validação.

**Ataque de Hackers:** A rede bitcoin possui um elevado nível de proteção contra ataques de hackers. Quanto mais longa for a cadeia de blocos, mais segura estará a transação. A proporção aumentará conforme forem aumentando o volume de transações. Para a rede privada não foram encontrados dados na academia que registrem ou não ataques de hackers.

**Acesso à tecnologia:** o Bitcoin por ser público é amplamente acessível, basta que o usuário tenha acesso a uma boa conexão de internet. Já para a rede privada, será necessário um desembolso muito grande para criar a própria plataforma.

**Smartcontracts:** somente podem ter acesso usuários da rede *Hyperledger*, trata-se de uma característica própria da plataforma.

A partir da compreensão teórica e da metodologia estabelecida e, neste momento apresentada, tornou-se possível, então, proceder as análises dos resultados apresentados para, posteriormente, encaminhá-lo às vias de conclusão. Dada a tipologia da pesquisa, os resultados não estão dissociados de suas análises sendo apresentados, portanto, de maneira uníssona característica das pesquisas exploratórias.

## 4 RESULTADOS E ANÁLISES

Apesar de ser uma tecnologia recente (NAKAMOTO, 2008) e inovadora, por dispensar a utilização de intermediários confiáveis que evitam a duplicação do pagamento, a velocidade de processamento das transações é um dos fatores limitantes do Blockchain para adoção em larga escala. Isto porque se, por um lado, o custo por transação é totalmente benéfico, por outro, perde-se muito em termos de tempo de processamento, inviabilizando qualquer tentativa de implementação para operações que exijam a referida larga escala. Apesar disso, analisando a alternativa privada de pagamento, é possível constatar que o *Hyperledger* pode se tornar viável do ponto de vista da segurança, escalabilidade, tempo de processamento e validação. No entanto, cabe ressaltar que a tecnologia *Hyperledger* é uma plataforma privada, portanto, de alto custo de implementação e adoção. Aliás, conceitualmente, a plataforma *Hyperledger* não contempla uma das principais características disruptivas do Bitcoin que é a possibilidade de democratização de acesso por meio de uma rede pública mundial e imutável.

Um outro fator importante a ser analisado, se refere ao anonimato. Considerando que os resultados aqui apresentados foram extraídos de uma pesquisa bibliográfica, deve-se aportar no entendimento de Conoscenti, Vetro e de Martin (2016), para quem no Blockchain apenas o pseudônimo é garantido. A rigor, isto implica em dizer que em relação a adaptabilidade e a integridade, no Blockchain, dependem da alta dificuldade da prova de trabalho e do grande número de mineiros honestos e, ao mesmo tempo, também se constitui como uma prova de trabalho difícil limitada justamente pela referida adaptabilidade. Não obstante, quando se reflete sobre os benefícios oferecidos por esses serviços emergem-se críticas em relação a privacidade. Isso ocorre porque os dispositivos conectados espalham dados pessoais sensíveis e revelam comportamentos e preferências de seus proprietários. Em outras palavras: a privacidade das pessoas é particularmente vulnerável quando esses dados confidenciais são geridos por empresas centralizadas, o que pode fazer uso ilegítimo delas.

Aqui, há de se concordar com Ziegeldorf et al. (2015, p. 01) que os Bitcoins são armazenados e transferidos entre endereços e identidades criptográficas correspondentes às chaves públicas de algoritmo de assinatura digital. Os endereços e, portanto, as transações são anônimas, desde que os endereços não possam ser vinculados aos seus proprietários. Mas, se o número da conta ou a chave pública está associado à sua verdadeira identidade, a implementação não pode ser garantida como anônima como bem informa Möser, Böhme e Breuker (2013, p. 01). Em decorrência disso, o entrave está justamente na possibilidade de atividades criminosas quando o anonimato é pensado sob a ótica da integridade ou da reprodução de sistemas de pagamento já instituídos quando pensados sob o prisma da adaptabilidade. Logo, com Koshy, P.; Koshy D. e P. McDaniel (2014), pode-se afirmar que essa tensão entre a crescente popularidade das moedas virtuais e seu anonimato percebido fornece um problema único para os usuários dessas moedas e para os reguladores que procuram compreender os verdadeiros riscos que eles colocam.

Ao avançar a presente análise rumo às implicações dos Bitcoins na ordem social, percebe-se que os Bitcoins foram, indiscutivelmente, associados ao mercado informal *Silk Road* (onde os Bitcoins poderiam ser trocados por produtos como drogas, revólveres e assassinos). Neste mercado, a honestidade é colocada em dúvida já que, como bem diz Ziegeldorf et al (2015), um invasor pode tentar adivinhar o endereço de entrada e o endereço de saída de um participante e, desta maneira, ampliar o tamanho do nível de anonimato alcançado. Em

consequência, um conjunto de anonimato maior leva a uma menor probabilidade de um acerto e, portanto, mais anonimato provocando ameaças, inclusive, ao valor de uma transação.

O valor da transação, em um sistema de transações como o Bitcoin, pode servir como uma impressão digital, revelando a origem de uma operação. Enquanto exemplo: se um invasor monitora os endereços de um usuário e sabe quantos Bitcoins ele transferiu para o serviço, ele tentaria procurar uma transação de saída de igual tamanho (menos a taxa previsível) nos blocos subsequentes. Desta maneira, poderia gerar ameaças à transação de forma anônima, manipulando os endereços da operação. Como todas as transações na rede são armazenadas publicamente no Blockchain, permitindo que qualquer um as inspecione e as análise, o sistema não oferece anonimato real, mas pseudônimos. Além disso, os usuários podem ser rastreados por casas de câmbio ou lojas de Bitcoins, onde eles devem fornecer informações pessoais que podem ser vinculadas aos seus endereços de Bitcoin (MÖSER, 2013, p. 01).

A própria comunidade Bitcoin afirma que a implementação atual não é muito anônima. Geralmente, as pessoas devem fornecer informações pessoais para comprar Bitcoins. Qualquer pessoa que pretenda depositar ou retirar moedas diferentes da BTC deve fornecer sua identidade. Além disto, um procedimento formal que o sistema financeiro utiliza hoje para garantir que os usuários não estejam envolvidos em práticas ilegais é o KYC (*Know Your Customer* ou Conheça Seu Cliente). Através dele, as instituições colhem dados e informações dos clientes e as mantém em sigilo em um sistema interno. Em princípio, se o KYC pudesse ser aplicado nas margens do sistema Bitcoin, ou seja, no momento em que os Bitcoins são trocados por moedas convencionais ou produtos e serviços, tornar-se-ia possível identificar atividades suspeitas no Blockchain e, consequentemente responsabilizar os perpetradores quando e onde eles interagem com o mundo real, Möser, Böhme e Breuker (2013, p. 01).

O KYC poderia ser apenas um primeiro passo que permitiria atividades posteriores, como a lista negra de titulares de contas suspeitas. Considerando que as contas Bitcoin têm identidades fracas, mas todos os registros de transações são públicos, na melhor das hipóteses, para que o combate à lavagem de dinheiro seja efetivo, deve-se listar os históricos das transações ao contrário de contas ou detentores de contas. Uma boa analogia off-line é registrar números de série de notas de banco usadas para pagar resgates Möser, Böhme e Breuker (2013, p. 11).

Enquanto não há uma forma mais eficiente de garantir o anonimato no Bitcoin a proposta seria a adoção de um sistema de pagamentos utilizando uma das plataformas de *Mixer Service* para melhorar a exposição de dados dos usuários durante a realização das operações de pagamento. No entanto, o uso desse serviço inviabilizaria tanto financeiramente quanto em termos de escalabilidade as transações de pagamento.

Todo o dito, implica no entendimento de que a matriz elaborada a partir da fundamentação teórica e a análise de seus elementos permitiu compreender como tem se estabelecido as relações teóricas e, também, empírica sobre este tema ainda latente. Desta maneira, responder à questão introdutória sobre quais seriam as premissas e/ou os parâmetros para que o Bitcoin pudesse ser adotado em larga escala mas, ao mesmo tempo, garantindo o anonimato do usuário nas transações de pagamento? tornou-se possível, ainda que de maneira provisória. A rigor, isto implica em dizer que, ao levar o presente trabalho para as vias de conclusão, a resposta à referida questão possibilitou a abertura de outras possibilidades investigativas que se apresentam após a conclusão a seguir.

## 5 CONCLUSÃO

É possível inferir que o Blockchain pode assumir um papel importante na democratização das transações de pagamento a nível global. Todavia, seu potencial de uso é totalmente questionável, principalmente em transações que exijam agilidade no processamento

e garantia do anonimato. Ademais, o custo de mineração ainda é alto e exige muito esforço computacional. Aqui, há de se considerar também, com Yli-Huumo et al. (2016), que a mineração de Bitcoin envolve altos custos em energia elétrica, embora a redução de custo nas operações e a melhoria da eficiência produtiva sejam evidentes. Estabelecer relações entre o custo energético e a viabilidade do processo se firma, então, como um viés para futuras pesquisas.

Além da relação entre os esforços e os dispêndios atribuídos à mineração, conclui-se também que o anonimato é um dos principais gargalos da tecnologia, principalmente no que tange o Bitcoin. Esse conceito de criptomoeda, que deu origem a tecnologia Blockchain, é imutável e público garantido confiabilidade nas transações de pagamento, mas, o anonimato, que no início era um atrativo para práticas criminais usando a moeda, se tornou um novo desafio para adoção em larga escala. Logo, apesar do usuário se registrar na rede usando pseudônimos é possível rastrear operações de diversas formas como aqui apresentadas. Ainda: É certo que algumas opções de ferramentas estão surgindo para melhorar a questão do anonimato, mas elas não garantem a total privacidade do usuário dentro dos limites das regras de combate a lavagem de dinheiro. Aqui, se estabelece uma outra questão a ser enfrentada a título de pesquisas futuras.

Quando pensada sob a ótica da escalabilidade, uma solução que é usada pelos bancos e que pode se tornar viável, desde que haja um consenso de adoção entre os usuários, é o *Know Your Customer* (Conheça Seu Cliente). Esta opção, no formato Bitcoin, ainda não se encontra testada e/ou estabelecida na literatura indicando, em decorrência disso mesmo, a necessidade de se ampliar o escopo da pesquisa para o referido viés. Não obstante, dada a necessidade do envolvimento de profissionais de outras áreas, tais como, programadores e desenvolvedores de plataformas, sugere-se a respectiva abordagem sob uma ótica multidisciplinar.

Aqui, cabe destacar ainda que a rede *Hyperledger* se mostrou totalmente viável no que diz respeito a maioria dos itens avaliados, principalmente na questão do anonimato. Entretanto, em se tratando de uma tecnologia nova e pouco explorada, ainda há muito a evoluir. Isto porque, é este tipo de rede que se apresentou como caminho para soluções que contribuem para o aprimoramento da rede Blockchain e a criação de novas ramificações da tecnologia.

Ao fornecer organicidade ao presente, é possível concluir, a partir do que foi delineado, que as transações de pagamento dentro do formato Bitcoin ainda não pode ser implementada em larga escala levando em conta a baixa escalabilidade e o tempo de processamento. É possível concluir também, que a adoção de empresas de mesclagem pode ser uma solução paliativa para esta questão, haja vista a necessidade de recursos suficientes que garantam a viabilidade do negócio para um grande grupo de usuários o que, por sua vez, faria com que os custos exigidos pelas plataformas deixasse o processo inviável e semelhante ao que já se existe tradicionalmente no mercado. É claro que, superada essas barreiras, torna-se factível e vantajosa a adoção dessa nova tecnologia nos sistemas de pagamento. Aliás, o avanço nos estudos sobre este tema, a partir das sugestões apresentadas nas vias desta conclusão, se firma como condição *sine qua non* para o aprimoramento dos sistemas de pagamento baseado na tecnologia Blockchain.

## REFERÊNCIAS

ANTONOPOULOS, Andreas M. **Mastering Bitcoin - Programming the Open Blockchain.** New York, O´Reilly Media: 2017.

BROWN, Richard G.; CARLYLE, James.; GRIGG, Mike; HEARN, August. **Corda: An Introduction**, 2016. Disponível em < DOI: 10.13140/RG.2.2.30487.37284>. Acesso em : 12. Set. 2019.

BRASIL, Conselho Federal de Contabilidade. **Normas Brasileiras de Contabilidade**. Conselho Federal de Contabilidade. Brasília, 2019. Disponível em: www.cfc.org.br. Acesso em: 30 set. 2019.

BRENNAN, Charles; LUNN, William. Blockchain: The trust disrupter. **Research Analysts**, Credit Suisse, ago. 2016.
CONOSCENTI, Marco; VETRO, Antonio; DE-MARTIN, Juan C., Blockchain for the Internet of Things: a Systematic Literature Review. **Nexa-Center for Internet & Society**, DAUIN-Politecnico di Torino, Italy, set., 2016.
CHRISTIDIS, Konstantino; DEVETSIKOTIS, Michael., **Blockchains and Smart Contracts for the Internet of Things**. Department of Electrical and Computer Engineering: North Carolina, 2019.
DELIVORIAS, Angelos. Distributed ledger technology and financial markets-EPRS. **European Parliamentary Research Service**, nov., 2016.
DAPP, Thomas F. Deutsche Bank - Blockchain – attack is probably the best form of defence. **Fintech**, n2, v. 28, jul.,2016.
EVANS, David S. **Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms:** University of Chicago Law School, 2014.
FERENZY, Dennis; TRAN, Herman; GIBBS, Sans; FRENCH, Conan. **The Internet of Finance Unleashing the Potential of Blockchain Technology.** IIF, 2015. Disponívelem: < https://www.iif.com/Publications/ID/582/Getting-Smart-Contracts-on-the-Blockchain>. Acesso em: 16. Set. 2019.
GARROD, Jonas Z. The real world of the decentralized autonomous society. **Triple C,** n. 14, v 1, pp. 62-77, 2016.
HERRERA, Jordi; JOANCOMART, Ian. Pesquisa e Desafios sobre o Anonimato Bitcoin. **Computer Science**. London: Springer, 2014.
HOROWITZ, Keyth; COBART, Mike; GERSPACH, Jonh. Us Digital Banking Could The Bitcoin Blockchain Disrupt Payments? **CITIBANKGROUP**: Junho. 2016.
KIVIAT, Trevor I. Beyond Bitcoin: Issues in regulating Blockchain transactions. **Duke Law Journal,**, n. 65, v. 3, s.n., 2015.
KOSHY, Phillip; KOSHY, Dianna; MCDANIEL, Patrick. "Uma análise do anonimato na Bitcoin usando o tráfego de rede P2P". **Computer Science**. London: Springer, 2014.
LAURENCE, Tiana**. Blockchain for Dummies.** John Wiley & Sons: White Paper, 2017.
FEDERAL RESERVE, Service. Distributed ledger technology in payments, clearing, and settlement**. Finance and Economics Discussion Series 2016-095**. Washington: Board of Governors of the Federal Reserve System, 2016.
MOSER, Malte. Anonymity of Bitcoin Transactions: An Analysis of Mixing Services. **University of Münster**, Münster, Germany, jun., 2013.

MOSER, Malte; BOHME, Robert; BREUKER, Dominic., **Um inquérito sobre ferramentas de lavagem de dinheiro no ecossistema Bitcoin.** Disponível em: https://maltemoeser.de/paper/money-laundering.pdf. Acesso em 20 ago. 2019.
NAKAMOTO, Satoshi. **Bitcoin: A peer-to-peer electronic cash System.** White paper, 2009. Disponível em: < www.bitcoin.org.>. Acesso em: 16 jun 2019.
RUFFING, Tim; MORENO-SANCHEZ, Pedro; KATE, Annicat. **CoinShuffle: Practical Decentralized - Coin Mixing for Bitcoin?** MMCI: Saarland University, 2014.
SWAN, Melanie. Blockchain Thinking: the Brain as a Decentralized Autonomous Corporation. **IEEE Technology and Society Magazine**, n. 34, v. 4, art. no. 7360255, 2015.
VALENTA, Luke; ROWAN, Brendan., **Blindcoin: Meias Responsáveis para Bitcoin. Computer Science**: Springer, 2015.
VOSHMGIR, Shermin; KALINOV, Valentine. **Blockchain A Beginners Guide**. BlockchainHub, 2017. Disponível em: < https://s3.eu-west-2.amazonaws.com/blockchainhub.media/Blockchain+Technology+Handbook.pdf>. Acesso em 14 mar. 2019.

WALCH , Angela. The bitcoin Blockchain as financial market infrastructure: a consideration of operational risk. **18 NYU Journal of Legislation and Public Policy** , n. 837, 2015.
YLI-HUUMO, Jesse; DEOKYOON, Ko; CHOI, Sujin; SOOYONG, Pio; SMOLANDER, Kevin. Where Is Current Research On Blockchain Technology? A Systematic Review. **Journals Plo**, n. 3, out., 2016. Disponível em: < https://doi.org/10.1371/journal.pone.0163477>. Acesso em: 16 jun. 2019.
ZIEGELDORF, Jan H; GROSSMANN, Fred; HENZE, Martin; INDEN, Nicolas; WEHRLE, Klaus, CoinParty: Secure Multi-Party Mixing of Bitcoins, Communication and Distributed Systems (COMSYS). **RWTH**. Aachen University: Germany, 2015.