UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

CENTRO DE INFORMÁTICA

2017.1

Trabalho de Graduação

Blockchain para Criação de Novos Modelos de Negócio e Seus Impactos na Indústria de Serviços Financeiros

Juliandson Estanislau Ferreira

Recife

2017

Juliandson Estanislau Ferreira

Blockchain para Criação de Novos Modelos de Negócio e Seus Impactos na Indústria de Serviços Financeiros

Trabalho apresentado ao curso de Sistemas de Informação da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof.° José Carlos Cavalcanti

Recife

2017

Juliandson Estanislau Ferreira

Blockchain para Criação de Novos Modelos de Negócio e Seus Impactos na Indústria de Serviços Financeiros

Trabalho apresentado ao curso de Sistemas de Informação da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof.° José Carlos Cavalcanti

Aprovado em_____de_____de 2017

BANCA EXAMINADORA:

José Carlos Cavalcanti

_____

Vinicius Cardoso Garcia

_____

Recife

2017

“Uma pessoa com um relógio sabe que horas são; uma pessoa com dois relógios nunca está segura”.

Provérbio

Agradecimentos

Primeiramente agradeço a Deus por ter me dado o fôlego de vida e a oportunidade de estudar em uma instituição de ensino superior de qualidade. Em segundo lugar, agradeço aos meus pais, Maria da Conceição, Isael Estanislau e minha irmã Tanize Luana por todo suporte nas horas mais difíceis dessa caminhada.

Gostaria também de expressar minha gratidão a todos os professores que me acompanharam durante minha trajetória para obtenção do título de bacharel em Sistemas de Informação. Graças a vocês o CIn é um centro acadêmico de excelência.

Não poderia deixar de agradecer ao Centro de Informática e Universidade Federal de Pernambuco por todas as oportunidades criadas e por promoverem um ambiente multicultural e de interação social.

Agradeço também a todos os amigos de curso em especial Filipe Gutemberg e Euclides Barbosa por todos os momentos de descontração e pela parceria nos diversos projetos das disciplinas. A minha noiva Grace Suzana por todo seu companheirismo e dedicação.

Por fim, agradeço ao professor José Carlos Cavalcanti pela sua preciosa ajuda paciência e por acreditar no meu trabalho.

Resumo

Blockchain é um banco de dados distribuído, online, público e que pode ser atualizado por qualquer nó participante da rede *peer-to-peer* (P2P) baseado no consenso entre eles e assegurado por um algoritmo de *Proof-of-Work* (PoW). Utiliza-se de técnicas de criptografia para que cada participante possa manipular o *ledger* de forma segura e sem a necessidade de uma autoridade central. Uma vez que um bloco é adicionado ao *blockchain* é extremamente difícil alterar ou remover. Tal conceito foi apresentado em 2008 quando um indivíduo conhecido por Satoshi Nakamoto. Até agora, o *blockchain* tem atraído bastante atenção da indústria de serviços financeiros, mas a tecnologia pode ser adaptada para qualquer indústria onde seja necessário registrar, confirmar e transferir qualquer tipo de contrato ou propriedade. *Blockchain* é uma tecnologia tão disruptiva quanto à máquina a vapor e a eletricidade foram no século XX e espera-se que este novo paradigma seja capaz de modificar profundamente a maneira como a sociedade e a economia funcionam.

Este trabalho investiga como blockchain pode afetar o mercado de ações. Por ser uma tecnologia de registro que fornece um alto grau de segurança e possibilidade de corte de Intermediários, está recebendo bastante atenção do setor financeiro. Atualmente, existem apenas pequenas iniciativas e, por enquanto, ainda não está claro vários aspectos relacionados ao seu futuro.

Palavras-chave: Blockchain, Mercado de ações, Impactos.

Abstract

Blockchain is an online, public distributed database that can be upgraded by any peer-to-peer (P2P) network node based on consensus between them and secured by a Proof-of-Work (PoW) algorithm. Encryption techniques are used so that each participant can manipulate the ledger in a secure manner and without the need for a central authority. Since a block is added to the blockchain it is extremely difficult to change or remove. Such a concept was presented in 2008 when an individual known to Satoshi Nakamoto. So far, the blockchain has attracted much attention from the financial services industry, but the technology can be adapted to any industry where it is necessary to register, confirm and transfer any type of contract or property. Blockchain is as disruptive a technology as the steam engine and electricity were in the twentieth century, and this new paradigm is expected to be able to profoundly change the way society and the economy work.

This work investigates how blockchain can affect the stock market. Because it is a registration technology that provides a high degree of security and the ability to cut Intermediates, it is getting a lot of attention from the financial sector. Currently, there are only small initiatives and for now it is still unclear several aspects related to its future.

Keywords: Blockchain, Stock Market, Impacts.

Lista de Ilustrações

Sumário

1. Introdução

1.1. Contexto

Nos últimos anos a popularidade da tecnologia blockchain cresceu significativamente. O conceito surgiu em 2008 com a ascensão do bitcoin, e já é considerado por vários especialistas como uma ideia com o potencial tão disruptivo quanto a máquina a vapor foi no século XIX.

Blockchain é uma estrutura de dados que faz com que seja possível criar um livro digital das transações e compartilhá-lo entre uma rede de computadores distribuída e descentralizada. Ela permite a realização de autenticações sem a necessidade de uma autoridade central e cada transação é validada pelos nós que compõem a rede. Utiliza-se de criptografia para permitir que cada participante possa manipular o ledger (um livro digital onde informações são registradas regularmente, tais como dinheiro e bens e tem estado no coração do comércio desde tempos antigos) de uma maneira segura. Uma vez que um bloco de dados é gravado no blockchain, é extremamente difícil de alterar ou remover [1].

Tais características melhoram significativamente a segurança dos sistemas, pois a rede mantém de forma transparente um histórico completo de todas as transações que aconteceram desde o seu primeiro dia. Além disso, a tecnologia blockchain pode ser utilizada em qualquer área em que seja necessário registrar, certificar ou transferir uma propriedade representada por um token digital.

Apesar de todos os benefícios provenientes da adoção da tecnologia, os ledgers distribuídos não devem ser vistos como fim em si mesmos, pois somente quando combinados com outras aplicações, tais como, smart contracts, pode-se aproveitar seu verdadeiro potencial [2]. Além disso, seu uso pode também ser adaptado para outras indústrias como: alimentos, energia, saúde e governo.

O sucesso do blockchain tem feito empresas de serviços financeiros se moverem rapidamente para utilizar os seus benefícios ou sistemas semelhantes. Elas veem a oportunidade de se apropriar da tecnologia blockchain para realizar suas próprias transações. A tecnologia também irá impactar os processos de contratos, auditoria e validação de produtos, além disso, em um futuro próximo várias empresas e profissões poderão deixar de existir.

1.2. Motivação

Apesar de todo interesse pela tecnologia, seu processo de desenvolvimento para se adequar ao setor de serviços financeiros ainda está em seu processo inicial, portanto várias questões ainda não foram devidamente respondidas. Quando se implementa uma nova tecnologia nem sempre os seus impactos são conhecidos com antecedência, o que pode tornar os impactos muito mais amplos que o imaginado, e as consequências podem ser diferentes das previstas [1].

O mercado de ações é uma importante indústria em nossa sociedade, e atualmente muitos de seus processos são arcaicos, do ponto de vista digital. O mercado também é altamente regulado o que significa que nenhum tipo de mudança será fácil. A principal motivação deste projeto é uma investigação exploratória para entender como a tecnologia está sendo utilizada para atender às novas necessidades do mercado financeiro.

1.3. Objetivos

A pesquisa desenvolvida visou à realização de um levantamento bibliográfico não extensivo da literatura acadêmica e profissional para identificar e analisar como as empresas do setor financeiro estão adotando a tecnologia, os impactos em sua estrutura, tendências e desafios relacionados. Para alcançar o objetivo geral, os seguintes objetivos específicos foram definidos:

- Descrever as tecnologias descentralizadoras emergentes (blockchain).
- Analisar modelos de negócio de organizações que operam com base nas tecnologias descentralizadoras.
- Identificar os impactos das tecnologias descentralizadoras na estrutura organizacional das organizações modernas.
- Destacar vantagens, desvantagens e o contexto de aplicação dos paradigmas descentralizadores.

1.4. Estrutura do Trabalho

O trabalho encontra-se dividido em seis capítulos, são eles:

1. **Introdução:** Apresenta a motivação da pesquisa, objetivos e sua estrutura do trabalho.
2. **O Mercado de Capitais e o Problema do Modelo Centralizado:** Conceitos básicos relacionados ao mercado de capitais e principais desafios enfrentados para manter a sua estrutura atual.
3. **Distributed Ledgers:** Conceitos relacionados à tecnologia, classificação e exemplos de aplicações.
4. **Distributed Ledgers como plataforma para o mercado de ações:** Apresenta algumas das principais iniciativas do uso dos distributed ledgers no mercado de ações, assim como as plataformas utilizadas e os impactos sob vários pontos de vista.
5. **Considerações Finais:** Conclusão do trabalho e sugestões de temas para possíveis análises no futuro.

1.5. Metodologia

Para que um conhecimento possa ser considerado científico, torna-se necessário identificar as operações mentais e técnicas que possibilitam a sua verificação. Nesse sentido pode-se definir um método científico como um conjunto de procedimentos intelectuais e técnicos adotados para atingir o conhecimento [24]. Sendo assim este capítulo tem o objetivo de classificar esta pesquisa, para os fins pretendidos do trabalho os critérios foram divididos em dois aspectos, são eles:

1.5.1. Tipo da Pesquisa

Esta pesquisa é um estudo exploratório, que de acordo com Hernandez, Fernandez, e Baptista são realizados quando há o objetivo de examinar

um problema ainda pouco discutido [25], a pesquisa também possui um caráter descritivo já que analisa a aplicação do blockchain no contexto organizacional de organizações da indústria de serviços financeiros, e destaca as vantagens e desvantagens do uso da tecnologia.

1.5.2. Procedimento Técnico

O procedimento utilizado neste trabalho é o documental, segundo Melvin Campo. Esse tipo de pesquisa utiliza como principal fonte de informação diversos tipos textos como livros, revistas, jornais e artigos provenientes das bases da IEEE, Springer e Science Direct.

Além das fontes formais, as informações foram coletadas de páginas da internet, blogs e sites de empresas que já adotam a tecnologia, como por exemplo, a Ethereum, que é uma plataforma descentralizada que executa contratos inteligentes, aplicações que funcionam exatamente como programados, sem qualquer possibilidade de tempo de inatividade, censura, fraude ou interferência de terceiros.

Após a revisão das informações houve o processo de análise e interpretação dos documentos. A análise foi feita de acordo com a perspectiva do autor com base em experiências prévias do mercado financeiro. Nesse processo também se levou em consideração a opinião do orientador e dos grandes especialistas em blockchain. Após a análise a informação foi organizada em diferentes grupos que, por sua vez, foi dividido em tópicos de acordo com o conteúdo. A abordagem utilizada é de natureza qualitativa, uma vez que se utiliza um conjunto de técnicas interpretativas para descrever significados dos termos relacionados a uma área específica do conhecimento.

2. O Paradigma Centralizado

2.1. O Mercado de Capitais

O mercado de capitais, muito embora secular, teve desenvolvimento mais dinâmico em meados do século XIX, permitindo a transferência de bens acumulados por pessoas físicas para as empresas, que por sua vez emitem ações aos investidores. Sendo assim, uma ação representa uma participação de propriedade em uma determinada corporação. Uma empresa é dita privada quanto uma pessoa ou família detém todas as ações da empresa. Se as ações podem ser negociadas em bolsas de valores, a empresa é chamada de empresa pública [3].

O mercado de capitais é composto por bolsa de valores, corretoras, e órgãos reguladores. Sua principal função é mediar transações entre aqueles que têm um excedente de dinheiro e aqueles que têm um déficit, da forma mais eficiente e barata possível. Seu papel é fundamental para uma sociedade desenvolvida, pois permite que as pessoas distribuam seus ganhos ao longo do tempo e ao mesmo tempo permite que as empresas obtenham recursos para se financiarem [4].

O mercado de capitais apresenta dois segmentos:

Mercado Primário: Provê um canal para venda de novos valores mobiliários que são negociados diretamente entre a empresa e os investidores. Os recursos levantados normalmente são destinados para projetos de modernização da empresa ou para o caixa.

Mercado Secundário: A maioria das transações é realizada nesse mercado. Os investidores negociam as ações diretamente entre si e a empresa que inicialmente as ofereceu não tem participação alguma. Esse mercado permite que os participantes possam ajustar suas ações de acordo com suas perspectivas de custo e benefício.

As compras e vendas de ações acontecem nas bolsas de valores, que basicamente são mercados que provêm estrutura adequada e um ambiente

regulamentado para tal prática. Na maioria das vezes o comprador não tem contato direto com vendedor, nesses casos a transação normalmente é intermediada por bancos e corretoras. Para o bom andamento das atividades, faz-se necessário um órgão supervisor, que em conjunto com o banco central do país, deve monitorar as operações ocorridas e assegurar que tudo está acontecendo de acordo com as leis estabelecidas [3].

2.1.1. Atividades

No mercado de capitais há várias atividades que precisam ser executadas para que uma transação seja totalmente concluída. Elas podem ser classificadas em atividades de negociação e pós-negociação.

Negócio

Os negócios são solicitações feitas por um indivíduo com o auxílio de um agente, essas ordens e incluem a quantidade do número de ações a serem compradas e o preço. Quando a solicitação é recebida pelo agente, ele a envia para a bolsa de valores, que por sua vez retorna algum tipo de recibo para o investidor [5].

O grande papel da bolsa de valores é prover confiança às partes, e isso é feito provando a autenticidade e precisão de seus registros. Essa instituição deve ainda estabelecer meios de rastrear cada ação que será recebida pelos envolvidos [5].

Pós - Negócio

Depois que uma transação é realizada, ainda existe muito tempo de trabalho administrativo para confirmar os seus detalhes. Umas das primeiras operações é o book, onde se registra a data e hora da transação, e atribuem-se responsabilidades sobre a transação. Esse passo é necessário para o cálculo do ciclo de vida de liquidação, que é o período entre a emissão da ordem de venda até a conclusão de

todo processo [5]. Quanto maior o ciclo de vida, mais arriscado para uma das partes. Um comprador poderia emitir uma ordem de compra e não pagar por vários dias; além disso, nesse período o preço da ação pode variar fazendo com que uma das partes desista para pegar um melhor preço.

Assim que o backoffice recebe uma transação, a validação deve ser realizada para confirmar que os dados necessários são conhecidos e válidos. O processo pode ser feito manualmente ou automaticamente dependendo das ferramentas disponíveis. Uma vez finalizado o processo de liquidação é importante que organizações envolvidas atualizem suas bases de dados com todos os dados gerados no processo.

2.2. Bancos de Dados Relacionais

A história do blockchain começa no início dos anos 70 do século passado, quando os bancos de dados foram desenvolvidos, e foi criado o modelo relacional. Tal modelo é subjacente a um Sistema Gerenciador de Banco de Dados (SGBD), e se baseia no princípio em que todos os dados estão guardados em tabelas. Toda sua definição é teórica e baseada na lógica de predicados e na teoria dos conjuntos. O conceito foi criado por Edgar Frank Codd em 1970, sendo descrito no artigo "***Relational Model of Data for Large Shared Data Banks***" [6].

A linguagem padrão e utilizada na maioria dos bancos de dados relacionais é a Structured Query Language (SQL). Essa linguagem dá suporte à grande maioria dos sistemas de gerenciamento de conteúdo que são executados na web, mas originalmente era uma linguagem de comando para unidades de fita. Os bancos relacionais eram bastante inflexíveis em termos de capacidade de armazenamento, o que, por sua vez, no nível semântico, provocam distorções na forma como percebemos o mundo. Tudo que era difícil de ser representado nos bancos relacionais era simplesmente desvalorizado ou descartado.

A segunda fase se inicia quando Tim Berners-Lee cria a Web (World Wide Web) no fim dos anos 80. Para viabilizar esse projeto foi necessário criar protocolos que serviriam para estabelecer padrões de comunicação dentro da rede, e, ao mesmo tempo, forneceriam interfaces amigáveis para os usuários. No início dos anos 90 várias redes estavam em operação, mas funcionavam de forma isolada ou

conectada a poucos computadores dentro de uma universidade [7]. O processo de consolidação da web pode ser dividido em duas fases, a saber:

Web 1.0: é considerada estática, e seus conteúdos não podem ser alterados pelos usuários finais. Todo o conteúdo da página é somente leitura para leitura. Na web 1.0, não existia qualquer tipo interatividade do usuário com a página e somente o programador podia realizar alterações ou atualizações [8].

Web 2.0: é a que utilizada atualmente, destaca-se por ser dinâmica. Essa dinamicidade indica a interatividade e participação do usuário final com a estrutura e conteúdo da página. Nela, o usuário final pode postar comentários, enviar imagens, compartilhar arquivos e fazer milhares de outras coisas que a web 1.0 não permitia [8].

Apesar dos grandes avanços tecnológicos presenciados nos últimos anos, ainda existe o grande desafio de encontrar um modelo que faça com que os computadores que compõem a web, e os bancos de dados se comuniquem com facilidade. O principal problema é fazer com que os bancos de dados trabalhem em conjunto de forma invisível ou fazer com que eles se comuniquem com processos do usuário final. Esse problema, de natureza técnica, geralmente é traduzido em processos mais caros e burocráticos [7].

Para os bancos comerciais é praticamente impossível atuarem em um ambiente muito burocrático, e para minimizar o problema todos acabam se ligando a uma rede operada por apenas um intermediário. O cartão Visa seria um típico exemplo de intermediário, por fornecer uma interface padrão para essa finalidade.

Isso acontece porque cada instituição constrói seus sistemas de acordo com suas necessidades, e quando se precisa de comunicação entre dois modelos, utilizam-se humanos nos processos, o que por sua vez impede uma cooperação genuinamente digital. Diante desses grandes desafios, desenvolveram-se alguns modelos que visam facilitar a cooperação entre a rede de computadores e os bancos de dados.

2.3. Modelo Hub and Spoke

O modelo hub and spoke (figura 01) surgiu como uma alternativa à grande complexidade de gerenciar as várias conexões do modelo peer to peer. Nesse caso todo o controle da rede é transferido para um intermediário [9].

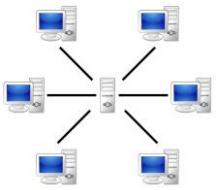

Figura 1: Modelo Hub and Spoke
Fonte: A cliente-server model[11].

Esse tipo de rede reduz e simplifica os seus custos de manutenção e construção, e centraliza o seu controle em pontos específicos. Além disso, os custos de operação e instalação são fixos, novos nós são fáceis de serem adicionados, e operações com alto custo de processamento podem ser realizadas no hub ao invés dos nós da rede.

Apesar de todas as vantagens o modelo apresenta sérias limitações, na maioria dos casos ocorre um monopólio da rede por parte da instituição gerenciadora do hub; o cartão Visa, por exemplo, ganha certa porcentagem de todas as transações que ocorrem na rede que ela administra. A censura e falta de transparência das informações também são problemas comuns deste tipo de rede.

Como o modelo é centralizado, as operações do dia-a-dia podem ser relativamente inflexíveis e as mudanças no hub, mesmo em uma única rota, podem ter consequências inesperadas em toda a rede. Pode ser difícil, ou mesmo impossível, lidar com períodos ocasionais de alta demanda entre as rotas [10]. A capacidade de carga total da rede é limitada pela capacidade do hub, e os problemas que ocorrem no hub podem afetar toda a rede; além disso, toda carga deve passar pelo hub antes de chegar ao seu destino o que geralmente causa gargalos na rede e torna o hub um único ponto de falha.

2.4. Modelo Peer-to-Peer

Peer-to-peer (P2P) (figura 02) é um modelo de comunicação descentralizado onde cada membro tem as mesmas capacidades e qualquer parte pode iniciar uma sessão. Podem ser classificadas em duas categorias: P2P puras e híbridas.

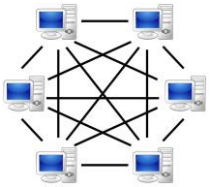

Figura 2: Modelo Peer-to-Peer.

Fonte: A peer-to-peer network[11].

Em uma rede P2P pura, todos os participantes são iguais, e cada peer desempenha o papel de cliente e de servidor. O sistema não depende de um servidor central para ajudar a controlar, coordenar ou gerenciar as trocas entre os pares. Em uma rede P2P híbrida, existe um servidor central para executar certas funções "administrativas" para facilitar os serviços [11].

Nesse modelo cada máquina registra suas transações em seu próprio banco de dados, o por sua vez dificulta bastante o processo de recuperação e backup de dados, além disso, nesse processo frequentemente aparecem inconsistências quando os dados fluem das fronteiras de uma organização para outra.

Supondo que uma pessoa resolva fazer compras on-line, sua compra só deve ser finalizada quando houver a confirmação do pagamento. Até que chegue a confirmação do pagamento, a empresa só pode especular sobre o status da transação. Caso haja algum erro, todo processo precisa ser redefinido.

O segundo problema das conexões P2P é a instabilidade. Uma pequena mudança no software em qualquer um dos nós pode levar a bugs que em alguns casos passam muito tempo despercebidos. Esse sistema também apresenta graves falhas de segurança, uma vez que vírus, spywares e malwares podem ser transmitidos facilmente através da rede. Além disso, o fato do sistema ser descentralizado torna-o muito difícil de administrar, já que uma pessoa não consegue determinar a configuração de toda rede [12]. Por último, há o problema da

escalabilidade, que em termos gerais pode ser definida como a adaptabilidade a mudanças de tamanho do sistema. Em uma rede com cinco nós haveria 13 conexões para gerenciar, com dez seriam 45. O custo de manutenção cresce exponencialmente a cada novo participante que entra na rede.

3. Blockchain

Blockchain é um ledger distribuído, e é bastante conhecido por ser a tecnologia que tornou viável a rede da criptomoeda bitcoin. Seu conceito foi apresentado em novembro de 2008 com a publicação do artigo ***Bitcoin: A Peer-to-Peer Electronic Cash System*** por um indivíduo com o pseudônimo de Satoshi Nakamoto. A grande importância do bitcoin está no fato de ser o primeiro sistema puramente peer-to-peer a permitir o envio e recebimento de dinheiro eletrônico sem a necessidade de uma instituição intermediadora (third party), e que evita o problema do double-spending. Esse problema acontece quando um peer utiliza o mesmo token digital mais de uma vez. É um problema quase que exclusivo dos ativos digitais devido a sua facilidade de reprodução.

Blockchain é um banco de dados confiável que é mantido coletivamente de maneira descentralizada. Como o nome indica, o banco de dados é composto por uma cadeia de blocos ordenados, que por sua vez, são protegidos por criptografia. O encadeamento é feito adicionando o hash do bloco anterior ao bloco atual, o hash do bloco atual com o do próximo bloco, e assim por diante. Os blocos aninhados garantem que as transações sejam organizadas em ordem cronológica; portanto, um bloco específico não pode ser alterado sem alterar os blocos antecedentes e subsequentes [13].

Todos os blocos, incluindo informações sobre cada transação feita, são armazenados em disco dos usuários, chamados nós. Todos os nós armazenam informações sobre todas as transações da rede, e verificam cada nova transação usando blocos anteriores; o nó que consegue vencer a corrida e adicionar primeiro o novo bloco à cadeia é recompensado. Este método é chamado de mineração, e é confirmado com proof of work, que é um dos principais conceitos da tecnologia Blockchain [14].

Os registros do blockchain são visíveis para todos os usuários da rede, mas pessoas de fora também podem visualizá-los através da Internet. Geralmente é referido como um ledger "compartilhado" ou "distribuído", uma vez que todos os participantes da rede têm uma cópia e compartilham a responsabilidade de mantê-lo atualizado. Essa ampla distribuição é a principal diferença entre blockchain e um registro clássico, que normalmente é feito em um ledger central sob o controle de um único banco, corporação ou autoridade governamental [15]. Além disso, com o blockchain pode-se definir regras (lógica de negócio) que estão ligadas a transação, diferente dos bancos de dados convencionais, nos quais as regras geralmente são definidas no nível do banco de dados, ou na aplicação, mas não na transação.

Como observa Satoshi Nakamoto, muitos problemas podem surgir quando apenas uma entidade tem acesso ao ledger e permissão para modificá-lo. Estes problemas potenciais vão desde o pagamento de pesadas taxas para a entidade controladora à corrupção e falhas técnicas.

3.1. Ledger

Os Ledgers estão presentes no comércio desde os tempos antigos, e podem ser vistos como um banco de dados onde são registrados ativos, que são classificados como *tangíveis*, como imóveis e máquinas, ou *intangíveis,* como marcas e direitos autorais. No ledger também são registradas informações sobre a quem pertence os ativos, que por sua vez podem ser transferidos. Esse processo é conhecido como transação, que normalmente envolve três participantes: compradores, vendedores, e uma terceira parte (bancos, cartórios e etc..), que intermediará a troca e executará o contrato.

Os ledgers atuais são deficientes em muitos aspectos. Eles são ineficientes, caros, não transparentes e sujeitos a fraude e uso indevido. Esses problemas são típicos de sistemas centralizados e baseados em confiança e de terceiros. Esses tipos de sistemas levam a gargalos e dificultam acordos de transação. A falta de transparência, bem como a suscetibilidade à corrupção e à fraude, levam a disputas [16]. Tentar criar soluções para resolver todos esses problemas e disputas ainda é uma atividade bastante custosa.

Nesse contexto o blockchain surge como uma resposta a esses desafios, pois é um banco de dados que junta vários registros em um bloco e posteriormente os liga usando uma assinatura criptográfica. Isso permite que o blockchain seja usado como um ledger, que pode ser compartilhado e modificado por qualquer pessoa com as permissões apropriadas. Se os participantes do processo forem pré-selecionados é um permissioned ledger, caso contrário é um unpermissioned ledger [17].

- **Unpermissioned ledgers:** Esse tipo de ledger não possui um dono específico e permite que qualquer pessoa que queria participar da rede tenha uma cópia idêntica dos dados e permissão para modificá-los. Os participantes mantêm a integridade dos dados através de um consenso sobre o estado do ledger. Nenhum participante pode impedir que transações sejam adicionadas no ledger e uma vez que elas são inseridas não podem ser editadas.
- **Permissioned ledgers:** Possuem um ou mais donos e a integridade de seus dados é verificada por uma instituição confiável, o que torna o processo bem mais simples. Esta solução tem se mostrado bastante efetiva, já que eles são mais rápidos que os unpermissioned ledgers e o processo de criação de um consenso cria uma assinatura digital que pode ser verificada por todos os interessados.

Embora a tecnologia tenha sido inventada para satisfazer um objetivo (dinheiro digital), empresas e outras instituições atualmente estão explorando como pode ser aplicado à solução de outros problemas. Isso deu origem a vários tipos de ledgers (figura 03) que são utilizados a depender das necessidades de negócio.

Figura 3: Grau de Centralização dos Ledgers

Fonte: Distributed Ledger Technology: beyond block chain[17].

3.2. Distributed ledgers

Um ledger distribuído é um banco de dados de ativos que pode ser compartilhado através de uma rede para vários locais e instituições. Todos os participantes da uma rede podem ter sua própria cópia do ledger. Quaisquer alterações no ledger são refletidas em todas as outras cópias em minutos ou, em alguns casos, em segundos. A segurança e a precisão das informações armazenadas são mantidas com o auxílio de criptografia através do uso de chaves e assinaturas para controlar quem pode fazer o que no ledger. As informações que entram também podem ser inseridas por um, alguns ou todos os participantes, de acordo com regras estabelecidas pela rede [17]. O valor dos ledgers compartilhados pode ser verificado através de suas quatro principais características:

1. **Reconciliação Através da Criptografia**. Atualmente diversas instituições fazem transações umas com as outras, e para todas transações realizadas cada instituição atualiza seu banco de dados. Tal prática pode levar a graves inconsistências, pois não existe uma maneira simples de verificar se as cópias são correspondentes. Com os ledgers distribuídos é possível compartilhar os mesmos dados com várias instituições ou provendo ‘proof points’ para verificar os dados.
2. **Replicado a muitas instituições**. As instituições que assim desejarem poderão ter uma cópia dos dados, evitando que haja um ponto único de falha. A réplica dos dados é um desafio para as tecnologias atuais, pois cria grande complexidade e custos para os projetos de TI.
3. **Controle de Acesso**. Os ledgers distribuídos usam chaves para controlar quem pode fazer o que dentro do ledger compartilhado. Com essas chaves pode-se também atribuir permissões específicas para serem usadas somente sob certas condições.
4. **Transparência e Auditabilidade.** As informações armazenadas nos ledgers são completamente transparentes, pois todos usuários podem ter acesso acesso aos dados coletados e como eles são acessados. Isso permitirá auditorias mais confiáveis uma vez que é possível verificar os estados do

conteúdo do ledger.

A grande novidade do blockchain está no fato de que ele é mais que um banco de dados; é possível também definir regras de negócio que estão diretamente ligadas às suas transações. Portanto seu verdadeiro potencial só é aproveitado quando combinado com smart contracts. Nesse sentido, já surgiram várias ideias inovadoras que aproveitam o melhor das duas tecnologias. Pode-se criar aplicações de registros públicos descentralizados, como títulos de terra, emissão de passaportes, votação e antecedentes criminais ou registros privados, como testamentos e trusts.

3.3. Smart contracts

Smart contract é um termo usado para descrever um programa de computador que é capaz de facilitar, executar e negociação ou desempenho de um contrato. Todo processo é automático e pode ser utilizado com um complemento, ou substitutos para os contratos legais, onde os termos seriam escritos como um conjunto de instruções. O seu principal objetivo é permitir que duas partes anônimas façam transações, geralmente através da Internet, sem a necessidade de um intermediário [18]. O conceito se popularizou no início de 1996 com a publicação do artigo ***Smart Contracts*** na revista Extropy, por um dos supostos criadores do sistema bitcoin, Nick Szabo.

Em seu artigo, Szabo previu que a revolução digital mudaria drasticamente a forma como as pessoas fazem contratos, e que os smart contracts melhoram significativamente quatro aspectos básicos dos contratos, descritos como: observabilidade, verificabilidade, privacidade e exigibilidade. Além disso, questionou se os tradicionais contratos continuariam a ter espaço na era digital [19].

Em um futuro muito próximo os smart contracts serão essenciais para a economia e poderão ser utilizados para realizar transações financeiras, propriedade ou qualquer outra coisa de valor. Mais ainda, os contratos inteligentes definem regras e penalidades em torno de um acordo da mesma forma que um contrato tradicional, e executam automaticamente as obrigações.

Para entender como os smart contracts funcionam é preciso analisar a

questão sob três aspectos fundamentais:

Codificação: (O que acontece em um smart contract?)

Smart contracts são como qualquer outro programa, então é importante que eles atendam as necessidades dos atores envolvidos. Sendo assim o código deve ter um comportamento pré-definido e não possuir as ambiguidades da linguagem natural.

Distributed Ledgers: (Como o contrato inteligente é disponibilizado?)

O contrato é criptografado e disponibilizado para outros computadores através de uma rede de ledgers. Esse processo pode ocorrer utilizando-se plataformas públicas, privadas ou híbridas.

Execução: (Como é processado?)

Cada computador recebe o código e processa de forma individual para chegar a um acordo sobre o resultado. O papel da rede é atualizar o ledger para armazenar a execução e checar se tudo ocorreu de acordo com os termos do contrato. Fraudes são extremamente difíceis de ocorrer, pois o processo não está em controle de um ator específico.

O blockchain possibilitou o surgimento de novos tipos de plataformas digitais e ecossistemas ao seu redor. Nos últimos anos várias indústrias, especialmente a de serviços financeiros, estão tentando adaptar a tecnologia a seus negócios para aumentar a eficiência de seus processos. Em outros setores o uso do blockchain ainda está em fase inicial [20]. Dentre as principais vantagens oferecidas pelas novas plataformas, pode-se destacar:

Autonomia – Não é mais necessário o uso de intermediários para confirmar a transação, o que por consequência torna o processo muito mais barato e menos burocrático. Além disso, elimina o risco de manipulação, já que a execução é gerenciada automaticamente pela rede.

Backup – No blockchain, qualquer membro da rede pode ter uma cópia do banco de dados, esse fator dificulta bastante qualquer perda de dados. Além disso, não existe um ponto único de falha, ou seja caso um nó da rede esteja inoperante outros podem assumir sem problemas.

Segurança – As transações no blockchain acontecem de forma muito segura, pois todas as informações são protegidas por criptografia, e um hacker levaria um tempo considerável para quebrá-la. Além do mais, qualquer alteração em um bloco teria que ser aceita por todos os outros da rede, ou seja o ataque deveria ser simultâneo, isso é algo extremamente difícil atualmente.

Smart contracts podem ser usados de várias formas. Szabo acreditava que se poderia incorporar smart contracts em nossa propriedade física, o que ele descreveu como "smart property". Esses contratos garantiriam automaticamente o acesso ao legítimo proprietário do ativo ou convidado, dependendo dos seus parâmetros [19]. Por exemplo, um carro alugado, poderia automaticamente retornar o controle do carro ao seu dono original se o locatário não fizesse pagamentos a tempo. A aplicação mais inovadora são as ***Decentralised Autonomous Organisations (DAO's)***, que basicamente é uma rede de smart contracts interconectados, que são capazes de executar as mesmas funções que organizações tradicionais. As DAO's possuem um alto grau de independência e os humanos não ocupam o papel principal na organização, já que o sistema é projetado para organizar transações por meio de algoritmos [20].

3.4. Como Blockchain funciona

Blockchain é um ledger onde são armazenadas todas as transações que são executadas na rede. Esse ledger é composto por blocos que por sua vez são identificados por um código hash. Uma função hash é um processo matemático que recebe dados de qualquer tamanho executa uma operação sobre eles e retorna dados de saída de um tamanho fixo [21]. O hash representa o conteúdo exato do arquivo original. Sempre que o conteúdo precisa ser checado, a mesma função é

executada sobre o arquivo original e o resultado deve ser o mesmo, caso contrário é um indicativo que o arquivo foi alterado.

No caso do bitcoin, para cada bloco é gerado um hash com 77 dígitos. Os blocos são então ligados ao seu anterior da cadeia através de seu código hash, que ainda contém a quantidade de transações incluídas no bloco, número do bloco atual e o número do próximo bloco da cadeia. Chaves públicas e privadas são utilizadas para identificar os remetentes e destinatários de cada transação (figura 4).

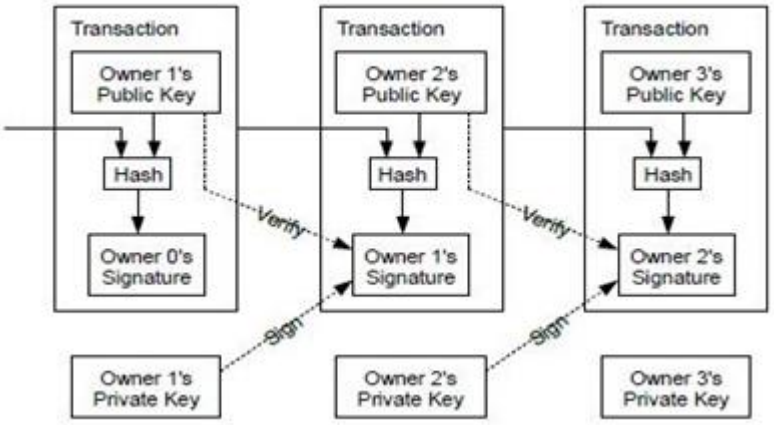

Figura 4: Estrutura do blockchain.
Fonte: Bitcoin: A Peer-to-Peer Electronic Cash System[45].

O fato dos blocos serem encadeados faz com que as transações sejam organizadas de forma cronológica, sendo assim é possível navegar até o bloco gênese e nenhum bloco pode ser modificado sem que se modifique todos os subsequentes. O blockchain é totalmente distribuído e depende uma rede de voluntários que o mantêm coletivamente e verificam as transações. Esses nós são chamados de mineradores. Minerar é o processo de adicionar blocos ao ledger e o este processo é projetado para ser difícil de ser executado de forma que mantenha estável o número de blocos adicionados todos os dias. Cada bloco deve conter uma quantidade proof of work para ser considerado válido.

Proof of work (Pow) consiste em um sistema que com um certo esforço para a realização de uma tarefa. Tal método é utilizado para evitar desperdício de poder computacional com tarefas fúteis ou evitar ataques maliciosos, como por exemplo Denial of Service (DoS) ou spam [22]. Para que o sistema funcione a prova deve ser difícil de ser criada e facilmente verificada pelo avaliador. O conceito foi adaptado a transações financeiras por Hal Finney em 2004 e a rede bitcoin foi o primeiro caso

de sucesso. Atualmente essa proposta é utilizada em quase todas criptomoedas. Produzir proof of work, na maioria dos casos, é um processo aleatório, de modo que uma grande quantidade de tentativas e erros acontecem, antes que uma prova de trabalho válida seja gerada [23].

Cada nó da rede possui sua cópia do blockchain e todos modificam suas cópias. Após a modificação de uma cópia local é necessário que haja um acordo com o resto da rede para se chegar a um consenso sobre o estado do ledger. Todo esse trabalho provê proteção a ataques do tipo double-spending, além disso hackers que atacarem o blockchain necessitarão ter controle de 51% da rede, o que seria altamente custoso [23].

4. Distributed Ledgers como Plataforma para o Mercado de Ações

No capítulo 3 foram apresentados os principais conceitos relacionados aos ledgers distribuídos, bem como seu funcionamento e alguns exemplos de aplicação. Este capítulo tem como principal objetivo identificar as principais estratégias que instituições financeiras, que atuam no mercado de capital, estão desenvolvendo para adaptar a tecnologia aos seus modelos de negócio, e analisar os impactos na estrutura organizacional dessas empresas, e no mercado com um todo.

De acordo com relatório ***Leading the Pack in Blockchain Banking: Trailblazers Set the Pace,*** publicado em 2016 pela IBM:

> *“Banking and financial markets are adopting the technology "dramatically faster than initially expected””.*

O relatório ainda aponta que atualmente a maioria das instituições está imaginando como adaptar a tecnologia a seus modelos de negócio, porém espera-se que em quatro anos 66% dos bancos usarão ledgers distribuídos em escala comercial [26]. Estas informações apontam o quanto à tecnologia será essencial

para o setor financeiro em um futuro próximo.

4.1. Instituições

4.1.1. National Association of Securities Dealers Automated Quotations (NASDAQ)

Fundada em 1971 nos EUA, foi o primeiro mercado de ações eletrônico do mundo. Atualmente é a segunda maior bolsa do mundo em termos de capitalização. Atualmente há cerca de 50 pessoas na Nasdaq que trabalham exclusivamente com a tecnologia blockchain. Toda pesquisa é desenvolvida em um departamento central de desenvolvimento. O trabalho é então enviado às unidades que devem utilizá-lo da forma mais adequada a suas necessidades de negócio [27].

Em dezembro de 2015 a companhia ficou conhecida por ser a primeira a realizar uma transação de ações com a tecnologia blockchain. A companhia também já lançou o Nasdaq Linq. Na ocasião Bob Greifeld o CEO da Nasdaq afirmou:

> *"Blockchain applied to the private market is innovation built on top of innovation, and carries with it the opportunity to forever alter the future of financial services infrastructure."*

Este produto foi direcionado às empresas privadas que desejam registrar e acompanhar o histórico de suas ações.

4.1.2. Japan Exchange Group (JPX)

Está localizada em Tóquio e possui mais de cem anos de existência, sendo uma das empresas mais antigas ainda operantes no mercado de ações. Ao longo dos anos sofreu várias mudanças em sua estrutura, porém a mais importante foi a informatização completa das transações em 1999 [28]. Visando dar mais um passo em sua evolução tecnológica, o JPX montou uma equipe interna de profissionais

dedicados à pesquisa e desenvolvimento para a aplicabilidade das DLTs no mercado financeiro.

Em 2016 o JPX realizou dois experimentos. No primeiro, utilizou-se a plataforma Ethereum para descentralização das informações das contas dos investidores e verificação do grau de resistência a fraudes. Para o segundo experimento, firmou-se uma parceria com a IBM para testar o potencial uso da tecnologia em mercados com baixo volume de transações, desta vez foi utilizado o framework disponibilizado pelo projeto Hyperledger.

Nos experimentos foi identificado que as DLTs podem tornar os processos pós-transação bem mais eficientes no futuro. A solução também foi muito bem avaliada no critério de disponibilidade, já que a rede opera com vários nós simultaneamente, evitando que haja o um único ponto de falha. Um dos desafios encontrados está relacionado a baixa taxa de processamento da rede, já que houve uma grande oscilação a depender da quantidade de transações e do algoritmo de consenso escolhido. De maneira geral os experimentos apresentaram avanços bastante significativos. Em um relatório sobre o tema, intitulado ***Applicability of Distributed Ledger Technology to Capital Market Infrastructure,*** o JPX afirmou:

> *"We have tested whether a streamlined process on securities market, security issuance, trading, settlement, clearing, and ownership registry, could be realised in a blockchain environment. Through our research, we have concluded that blockchain has the potential to transform capital market structure by encouraging new business development, improving operation efficiency, and contributing to cost reduction."*

4.1.3. Brasil Bolsa Balcão (B3)

É a maior bolsa de valores da América latina e está situada no estado de São Paulo. No fim de 2011 figurava como uma das 13 maiores bolsas de valores do mundo. No ano de 2016, juntou-se ao consórcio liderado pela R3CEV na busca de soluções baseadas na tecnologia blockchain que possam ser aplicadas às suas

necessidades. De acordo com uma nota oficial emitida por Fábio Dutra, Diretor Comercial e de Desenvolvimento de Mercado [29].

> *"A inovação com supervisão regulatória apropriada é de suprema importância para tornar os mercados brasileiros ainda mais eficientes e confiáveis. A DLT poderá desempenhar um papel importante aqui."*

Ainda não ficou claro como a tecnologia será adotada, porém espera-se que o principal foco seja a criação de novos modelos de negócio. Segundo as notícias, a instituição estaria se esforçando para melhorar a transparência e fiscalização do mercado. Segundo Jochen Mielke, Diretor de Sistemas de Negociação e Arquitetura:

> *"A B3 está pesquisando soluções baseadas em blockchain sob a ótica de negócios e TI, na busca de inovações para o mercado de capitais. A DLT tem um grande potencial de ganhos de eficiência nos processos atuais e queremos trabalhar com os nossos clientes para avaliar casos de uso.*"

4.1.4. London Stock Exchange (LSE)

Foi fundada em 1881 e está localizada no Reino Unido. Atualmente possui outras instituições ligadas ao setor financeiro como: Borsa Italiana, MillenniumIT e Russell Investments. Em 2015 ficou conhecida por ser uma das principais fundadoras do Post-Trade Distributed Ledger Working Group (PTDL), é também uma das instituições que mais experimentos com o blockchain.

O PTDL conecta vários profissionais, reguladores e bancos centrais, atualmente é formado por 37 membros de todos os lugares do mundo e é um dos primeiros consórcios a seguir os passos do R3. Seu principal objetivo é prover um ambiente para que os participantes possam compartilhar informações sobre as atividades pós-transação. Assim o PTDL realiza pesquisas para descobrir como o blockchain transformará esse cenário.

Sua criação é um grande marco do novo ciclo tecnológico que está nascendo. Muitas instituições financeiras que possuem longa tradição no mercado

tentarão alavancar modelos colaborativos que ultrapassaram o escopo proposto pela R3 [30].

Uma pesquisa realizada entre os membros PTDL para classificar os principais benefícios da tecnologia descobriu que 81% acreditam que as DLTs podem reduzir custos operacionais, 67% o aumento da eficiência / redução dos ciclos de liquidação e 43% que trarão mais transparência aos processos. A pesquisa mostrou ainda que 20% afirma que a prioridade do blockchain possui uma alta prioridade para seus negócios [31].

Apesar de toda empolgação ainda há algumas barreiras para uma ampla adoção das DLTs. Isso se deve em grande parte a questões relacionadas à falta de padronização, e questões relacionadas à confidencialidade das informações.

De acordo com uma nota oficial de Sandra Ro, membro do comitê organizador do PTDL:

> *The potential impact of blockchain and distributed ledger technology on the post-trade industry is huge, and as with all pioneering developments there is great excitement but also uncertainty.*

4.2. Plataformas

O conceito do Blockchain foi introduzido em 2008, por um grande motivo: afastar-se de um sistema centralizado onde as instituições financeiras, o estado e os reguladores não eram confiáveis [1]. Conforme discutido anteriormente, o paradigma centralizador é inadequado para lidar com dinamismo, complexidade e rapidez do mundo contemporâneo. No mercado de ações há uma grande quantidade de atores envolvidos na execução de cada transação (figura 5), isso por sua vez o torna o processo muito mais burocrático que o necessário e eleva seus os custos de manutenção da estrutura do mercado como um todo.

Figura 5: Mercado de ações atual.
Fonte: The potential of Blockchain in the Public Sector.

Os Blockchains são destinados a descentralizar, aplicativos como o Bitcoin, minam a necessidade de qualquer instituição financeira central. Atualmente quase todos os bancos estão fazendo experimentos com essa tecnologia, com o objetivo de encontrar novas oportunidades de negócios e reduzir seus custos operacionais. A exploração acontece várias maneiras, através de parcerias com fintechs, adesão a consórcios globais e construção de suas próprias soluções internas [1]. Apesar de haver diversas iniciativas, elas possuem um único propósito, simplificar os processos através da criação de um único ledger que seja compartilhado por todos os participantes da rede (figura 6).

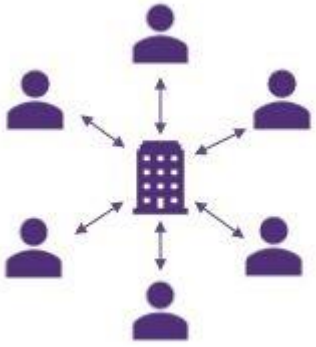

Figura 6: Mercado de ações com blockchain.
Fonte: The potential of Blockchain in the Public Sector[44].

4.2.1. Corda

Corda é um ledger distribuído para processamento e registro de transações financeiras. Seu principal objetivo é fornecer uma plataforma com serviços comuns para garantir que todas as aplicações criadas no topo sejam compatíveis entre si, enquanto ainda promovem a inovação em um tempo de mercado mais rápido, uma vez que a infraestrutura subjacente será aceita pelos participantes da rede [33].

A plataforma faz um amplo uso de smart contracts para ligar a lógica de negócio aos dados do negócio. Isso assegura que as transações estejam em conformidade coma lei, o que ajuda a evitar ambiguidade, incerteza ou disputa. Ela foi inspirada no blockchain e projetada especificamente para atender as necessidades das instituições financeiras.

Dentre as principais funcionalidades contidas na plataforma estão:

- Gerenciamento das transações entre duas partes.
- Uso ferramentas padrão do setor financeiro.
- Suporte a uma variedade de mecanismos de consenso.
- Restrição do acesso aos dados dentro de um contrato apenas para os que têm o direito.

Diferente do Bitcoin, Corda não possui um banco de dados central. Cada nó mantém um subconjunto das informações, sendo assim nenhum peer conhece o ledger como um todo. Em Corda as transações não são ordenadas em bloco como ocorre no bitcoin, consequentemente não necessita-se de miners ou proof-of-work. Para que uma transação ocorra na plataforma é necessário haver a entrada de ao menos um estado, e não será permitido que nenhuma transação use estados que já foram consumidos previamente.

Os estados são imutáveis e representam um fato conhecido por um ou mais nós em um momento específico. Eles podem conter qualquer tipo de dados (ações, títulos, empréstimos, informações de identidade), permitindo que representem fatos de qualquer natureza. Por serem imutáveis eles não podem ser modificados diretamente, quando um estado precisa ser atualizado cria-se uma nova versão e

marca-se o anterior como histórico. Isso permite o acompanhamento da evolução dos estados. Cada estado aponta para um notário, que basicamente é serviço que provê consenso na rede, além disso, garante que uma transação só será concluída caso todos os estados de entrada forem válidos.

Somente após a assinatura do notário pode-se ter certeza sobre a validade da transação, sendo assim é o ponto de finalidade do ciclo. A plataforma também suporta vários tipos de algoritmos de consenso, permitindo às instituições escolherem o que melhor se adaptam aos seus requisitos de privacidade, legais e escalabilidade. Para um bom algoritmo de consenso duas propriedades devem ser levadas em consideração:

- **Validade**: As partes podem ter certeza de que uma transação foi válida se o contrato associado é executado com êxito e possui todas as assinaturas necessárias.
- **Singularidade**: As partes podem ter certeza de que a transação em questão é única se todos os seus estados de entrada forem consumidos. Ou seja não houve nenhuma outra transação anterior que alcançou consenso utilizado qualquer um dos mesmos dados.

Embora a plataforma Corda tenha sido criada tendo como inspiração o blockchain, ela possui algumas diferenças que a tornam vantajosa para o uso no mercado financeiro.

- As transações podem ser executadas em paralelo, em diferentes nós, sem que nenhum dos dois esteja ciente das transações do outro.
- Por permitir o processamento paralelo diminui consideravelmente a energia gasta no processo.
- Dados são compartilhados somente quando necessário.
- Transações são validadas através dos notários, e cada um pode ter seu próprio algoritmo de consenso.

4.2.2. Etherum

Ethereum é uma plataforma de computação distribuída baseada em blockchain e de código aberto que fornece uma máquina virtual descentralizada. Foi proposta em 2013 pelo jovem Vitalik Buterin, fruto de uma pesquisa realizada na comunidade Bitcoin. No mesmo ano, ele publicou o Ethereum white paper, no qual ele descreve em detalhes o protocolo por trás do Ethereum, além da arquitetura dos smart contracts. Em abril de 2014, em parceria com o Dr. Gavin Wood, publicou o Ethereum Yellow Paper onde continha especificações técnicas para a Ethereum Virtual Machine (EVM). A partir disso, o Ethereum passou a ter a possibilidade de ser implementado em várias linguagens de programação [34].

Essa plataforma foi criada para facilitar a vida de desenvolvedores que desejam criar aplicações que possuem as propriedades do blockchain, evitando ter que criar um novo blockchain para cada aplicação. Embora seja uma plataforma genérica a maioria das aplicações testadas atualmente estão voltadas para o setor financeiro.

Assim como o blockchain o Ethereum opera um ledger global e utiliza um protocolo PoW para atingir o consenso, apesar de ser parecida com o bitcoin em vários aspectos o ethereum apresenta algumas diferenças, a principal é que os blocos ethereum contém uma cópia da lista de transação e do estado mais recente [35]. Além disso, ethereum permite que você a criação de tokens digitais que podem ser usados para representar partes virtuais, ativos, comprovante de associação entre outros.

No início deste ano foi anunciada uma parceria entre 30 das maiores empresas mundo, entre elas destacam-se JPMorgan Chase, Microsoft e Intel. Ao grupo foi dado o nome de Enterprise Ethereum Alliance, cujo principal objetivo é criar uma versão da plataforma onde empresas de todo o mundo possam usar para rastrear dados e contratos. Em maio 86 novas empresas provenientes de várias de indústrias se juntaram ao consórcio, isso mostra que a solução proposta vai muito além do mercado financeiro. A iniciativa foi criada para prover alternativas ao uso das plataformas corda e hyperledger, e até agora vários bancos já realizaram testes em ambientes controlados com essa plataforma.

4.2.3. Hyperledger

A plataforma Hyperledger é resultado de um esforço colaborativo entre indústrias de diversas áreas para criar um ledger distribuído de código aberto. Ela incorpora tecnologias, incluindo frameworks, smart contract, interfaces gráficas e amostras de aplicações. Atualmente o projeto conta com 130 membros e 5 frameworks, hyperledger Burrow, Fabric, Iroha, Sawtooth e Indy. De maneira geral seu objetivo é promover a adoção em massa da tecnologia blockchain, reutilizando recursos em comum para acelerar processo de inovação [36].

Dentre os cinco frameworks o que mais chama atenção é o hyperledger fabric que foi projetado para o desenvolvimento de aplicações com uma arquitetura modular, permitindo que serviços sejam associados utilizando o método plug-and-play. Foi observado que redes do tipo permissioned que exigem que todos os nós mantenham o ledger e rodem o algoritmo de consenso não são altamente escaláveis. Sendo assim, para resolver esse problema no hyperledger os peers são separados em três funções Endorser, Committer, e Consenter.

O Hyperledger baseia-se na expectativa de que no futuro haverá várias redes blockchain, cada uma servindo a um objetivo diferente. Embora ainda possa haver uma instância de uso geral, não deve haver nada que faça com que uma rede confie em outra para desempenhar suas funcionalidades básicas.

Por isso entre suas principais características estão:

- **Gerenciamento de Identidade**: Fornece um serviço que gerencia as identidades dos usuários e autêntica os participantes da rede. As listas de controle de acesso podem ser usadas para fornecer camadas adicionais de permissão através da autorização de operações de rede específicas.

- **Privacidade**: permite que os interesses comerciais concorrentes e quaisquer grupos que exijam transações confidenciais e confidenciais coexistam na mesma rede de permissões. Os canais privados são caminhos de mensagens restritas que podem ser usados para fornecer privacidade e confidencialidade de transações para subconjuntos específicos de membros

da rede. Todos os dados, incluindo informações sobre transações, membros e canais, em um canal são invisíveis e inacessíveis para qualquer membro da rede que não tenha concedido explicitamente o acesso a esse canal.

- **Eficiência**: Para proporcionar paralelismo à rede, a execução é separada do pedido de transação. A execução de transações antes de ordená-las permite que cada nó processe várias transações simultaneamente, o que aumenta a eficiência de processamento em cada ponto e acelera a entrega de transações para o serviço de pedidos.

Em maio deste ano foi revelado que a IBM está desenvolvendo um projeto em conjunto com a bolsa de valores de Santiago, a terceira maior da América Latina. A solução desenvolvida permitirá a troca de informações entre os participantes do mercado e ao mesmo tempo reduzirá o tempo dos os processos em até 40%. Segundo Andrés Araya, CIO da bolsa de Santiago, não é se trata de um PoC, a ideia é rodar o sistema em paralelo com os já existentes nos próximos meses e migrar completamente para os ledgers distribuídos no próximo ano. O próximo objetivo é escalar o projeto permitindo comunicação dessa bolsa com a de países vizinhos [37].

4.2.4. Comparação Hyperledger, Corda e Ethereum

As plataformas Hyperledger, Corda e Ethereum possuem objetivos e campos de aplicação bastante distintos, apesar pertencerem ao mesmo grupo (DLT's). Corda está sendo desenvolvida para atender especificamente aos anseios do mercado financeiro, diferente do hyperledger que visa fornecer uma arquitetura modular onde uma ampla gama de serviços podem ser a acoplados. A ethereum se apresenta como uma plataforma de transações genérica e assim como a hyperledger pode ser empregada em qualquer indústria onde seja necessário registrar, confirmar e transferir qualquer tipo de propriedade [46].

O modo de operação do ledeger (permissionless ou permissioned) impacta significativamente a forma como se chega ao consenso na rede. O ethereum por ser um blockchain do tipo público, todos os participantes devem estar cientes de todas as transações realizadas, independente de ter participado. Já que a transação pode ocorrer entre partes anônimas é preciso um algoritmo de consenso que proteja o ledger contra ataques e fraudes. No caso do ethereum isso é feito utilizando as

técnicas de mineração e proof-of-work. Esse tipo de técnica por sua vez, afeta negativamente o desempenho do processamento de transações, além disso não é adequado para aplicações onde os usuários precisem de um alto nível de privacidade.

O hyperledger possui um conceito de consenso mais amplo, os nós possuem papéis diferentes e podem ser classificados em: clientes, peers ou ordenadores. Os clientes se comunicam com os peers e ordenadores e invocam transações em nome dos usuários finais. Os peers são responsáveis por manter a integridade do ledger e recebem as transações dos ordenadores em uma ordem lógica para o registro no ledger.

Com o hyperledger, o algoritmo consenso empregado é conectável e depende dos requisitos específicos da aplicação, portanto vários algoritmos podem ser usados. A solução ainda permite um maior controle sobre o consenso e o acesso restrito às transações, o que resulta em uma melhor escalabilidade e privacidade e desempenho.

No caso da Corda o consenso é feito de forma bem parecida ao hyperledger, em nível de transação e envolvendo apenas as partes. Avalia-se a validade e singularidade da transação. A validade é assegurada quando verifica-se que todas as assinaturas necessárias são válidas, enquanto que a singularidade diz respeito aos estados de entrada de uma transação. Nesse caso deve-se assegurar que nenhum dado de entrada tenha sido consumido previamente. Diferente do bitcoin, corda não usa os conceitos de mineração e proof-of-work.

Outra importante diferença entre as três e que ethereum opera a criptomoeda ether. Além disso, pode-se criar tokens digitais para representação de ativos. No hyperledger, é possível desenvolver uma moeda nativa ou um token digital com chaincode, na corda não é possível a criação de tokens.

4.3. Impactos

4.3.1. O mercado de ações

Apesar da tecnologia blockchain impactar praticamente todos os setores da economia, espera-se que o setor mais afetado por essas mudanças seja o mercado de ações, porém não se espera grandes mudanças em um período curto prazo. De acordo com o relatório ***The Blockchain: Capital Markets Use Cases,*** produzido em 2016 pela empresa de consultoria GreySpark Partners, a disrupção ocorrerá dentro

de um período de dez anos. Uma mudança na base desse mercado exigirá tempo para uma redefinição de todos os processos, além disso, as empresas que já participam podem criar obstáculos para esse tipo de mudança [27].

Em outro trecho o relatório afirma:

> *"DLT's has the potential to reduce operational costs and counterparty and settlement risk, while also impacting payments and remittances, among other financial sectors."*

Com a redução dos custos de negociação e segurança os clientes serão os principais beneficiados e espera-se que um aumento no número de transações. No mercado de ações os processos realizados para confirmação da transação serão os mais impactados. Nos últimos houve um grande aumento na velocidade com que as transações são executadas, porém os processos pós-transações pouco foram alterados. Atualmente ainda se usa sistemas legados ou processos manuais para dar suporte a essa atividade, portanto a ineficiência, risco e altos custos afetam a lucratividade das organizações. Com os DLT's é possível reduzir o ciclo de vida dos processos pós-transação de dias para minutos, o que por sua vez reduzirá os riscos para as pessoas e empresas envolvidas nas transações.

4.3.2. Participantes

A tecnologia blockchain diminuirá drasticamente a razão de existência dos intermediadores. Os intermediadores são instituições ou pessoas que a facilitam a transação e confiança entre as partes envolvidas ou regulam o mercado de forma geral. Eles também são responsáveis por gerenciar o histórico de propriedade e transações.

As DLT's mudam essa lógica, pois permitem que os contratos sejam incorporados no código e armazenados em bancos de dados compartilhados de forma transparente e protegidos contra qualquer tipo de adulteração. Cada transação teria um registro digital que poderia ser identificado, validado, armazenado e compartilhado [38].

Estima-se que o processo de substituição dos intermediários não acontecerá em curto prazo. Esse processo requer uma grande quantidade de esforço para ser concluído. Praticamente todos os participantes serão afetados de alguma maneira. As empresas existentes provavelmente serão forçadas a mudar a forma como conduzem suas operações e novas oportunidades de negócios podem surgir junto com as novas necessidades trazidas pela tecnologia blockchain [27].

4.3.3. Regulação

Regulação tem um papel muito importante em um setor tão complexo quanto o mercado de ações. Como qualquer nova tecnologia, os ledgers distribuídos vêm acompanhados de importantes desafios que irão influenciar sua adoção. Alguns dos mais relevantes têm que ver com a forma como eles vão ser regulados, tendo em mente que uma tecnologia, por definição, não é objeto de regulação, mas sim seus os diferentes usos. O fato do blockchain estar em sua fase exploratória dificulta ainda mais a sua regulamentação, já que muitas perguntas ainda não foram respondidas como: o que deve ser regulado? Deve-se regular as criptomoedas? Quem deve ser o responsável por verificar a conformidade dos processos?

Um relatório apresentado em 2016 pelo Banco Bilbao Vizcaya Argentaria (BBVA) intitulado ***Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*** apresenta três modelos para lidar com essa questão:

- **Supra regulador**: Nesse modelo haveria um único regulador a nível global, que teria acesso ilimitado a informações relevantes de todos os consórcios da indústria financeira. Essa hipótese é bastante remota, visto que diferentes regiões têm especificidades que devem ser levadas em consideração.

- **Regulador DL**: A segunda opção seria a criação de consórcios regionais, onde haveria um regulador para cada consórcio. Os reguladores regionais poderiam compartilhar informações entre si em tempo real através de seus próprios ledgers distribuídos.

- **Regulador DL em Níveis**: No terceiro modelo, reguladores de diferentes regiões participam em todos os consórcios existentes, porém eles só têm acesso às informações necessárias para supervisionar as atividades relacionadas às instituições sob sua jurisdição. Entre os três modelos apresentados, esse tem a maior probabilidade de se tornar realidade.

4.3.4. Economia

A centralização tem sido um princípio organizador central para a economia e a sociedade desde a revolução agrícola, sendo o princípio de organização mais eficaz quando os custos de comunicação e transação são elevados. Nesse contexto, blockchain tem o potencial de ser a força democratizadora mais importante da história porque nenhuma autoridade central é necessária [39]. Além disso, blockchain pode ajudar a democratizar a economia compartilhada, tornando mais barato criar e operar uma plataforma online. Por exemplo, as transações podem ser coordenadas por contratos inteligentes ou realizadas a um menor custo por outros pequenos fornecedores.

A tecnologia Blockchain facilita assim o surgimento de novas formas de organizações, que além de não ter estrutura física, são descentralizadas. Essas organizações não têm diretor ou CEO, nem qualquer tipo de estrutura hierárquica e são administradas, coletivamente, por todos os indivíduos que interagem cooperam com o blockchain. Uma vez que não existe um operador intermediário, o valor produzido nessas plataformas pode ser mais distribuído entre aqueles que contribuíram para a sua criação [40].

Já existem várias aplicações que promovem a economia compartilhada como o La'zooz, que funciona como a Uber, mas sem um operador centralizado. Essa aplicação é regida apenas pelo código implantado em uma infraestrutura baseada em blockchain, que é projetado para governar interações entre motoristas e usuários. Esse aplicativo recompensa os motoristas que contribuem para a plataforma com tokens especialmente projetados que representam uma participação na aplicação. Da mesma forma, o OpenBazaar é um mercado descentralizado, como Amazon, mas que opera de forma independentemente. A ideia baseia-se na tecnologia blockchain para garantir que compradores e vendedores possam interagir diretamente entre si, sem passar por qualquer intermediário centralizado.

4.3.5. Efeitos Técnicos

Atualmente existem duas alternativas para implementar blockchain: *permissionless* e *permissioned*. O permissionless é atualmente o mais popular devido ao grande interesse no desenvolvimento de aplicações de código aberto [27]. Mas esse tipo de ledger consome muita energia em seu processo de consenso, estima-se que a rede bitcoin, por exemplo, consumirá a mesma quantidade de energia que a Dinamarca no ano de 2020. Além disso, não é recomendado quando precisa-se processar um alto número de transações. A plataforma Ethereum é capaz de executar 8 transações por segundo, o que é muito pouco quando comparado a Visa que consegue executar até 56000 transações [41].

Os permissioned ledgers são mais adequados ao mercado de ações, pois o custo do processo de consenso é menor, e ainda assim consegue assegurar que as transações entre os participantes ocorrerão de forma segura. Essa solução elimina a necessidade de uma autoridade central para validação de transações quando os participantes concordam sobre como a validação deve ser conduzida [27].

A tecnologia blockchain será usada em conjunto com sistemas que operam hoje, e muitos deles estão bastante ultrapassados. Ainda há um longo caminho para uma adaptação desses sistemas a essa nova tecnologia e provavelmente nem todos os sistemas que surgirão no futuro se integrarão com o blockchain.

4.3.6. Inovação

As DLT’s estimulam a cooperação entre as empresas e seus competidores. Na verdade o grande segredo para a consolidação dessa tecnologia é a cooperação, que tem por objetivo criar uma solução global e processos padrão para alinhar todos os participantes da rede. Além disso, é mais lucrativo para as empresas, pois a acelera o tempo de chegada ao mercado do produto ou serviço, cria novas oportunidades e reduz custos com pesquisa e desenvolvimento. Este processo também é conhecido como Inovação aberta. Tal conceito foi criado pelo professor Henry Chesbrough e publicado em seu livro ***Open Innovation***. Trata-se de uma abordagem mais distribuída, participativa e descentralizada da inovação, com base no fato de que o conhecimento útil hoje não está amplamente distribuído

dentro de nenhuma empresa, independente de quão capaz ou grande, ela possa inovar por conta própria [42].

Atualmente essa abordagem apresenta algumas limitações, há uma grande dificuldade em estabelecer rastreabilidade e capitalização de ideias e conhecimentos. Isso pode causar desconfiança entre os participantes e causar desmotivação o que por sua vez tornaria a abordagem ineficaz [43].

Para esse desafio as DLT's oferecem uma solução, elas possibilitam a rastreabilidade, segurança e até uma medição das trocas de conhecimento ocorridas na rede. Pela primeira vez será possível ignorar os intermediários e permitir que os indivíduos sejam reconhecidos e até pagos pela sua criação.

5. Conclusão

A presente pesquisa buscou esclarecer os conceitos relacionados às tecnologias descentralizadoras, assim como seus impactos e contexto de aplicação. Com base em toda discussão apresentada é possível concluir que o blockchain provê respostas para antigos problemas do setor financeiro. Seu paradigma descentralizador, aberto e acessível permite que os dados ali contidos sejam altamente confiáveis, tendo grande relevância no registro de transações, rastreabilidade e comprovação de propriedade.

No mercado de ações os processos pós-transação sofrerão os maiores impactos. Isso se deve a grande quantidade de burocracia e processos manuais que existem atualmente. Os smarts contracts também terão um papel crucial no sentido de conduzir as organizações a um nível mais alto de autonomia. Espera-se ainda que surjam novos modelos de governança corporativa e a legislação deverá evoluir para dar resposta às novas questões legais que surgirão.

Apesar de toda expectativa em relação ao impacto que esta tecnologia causará nos próximos anos, ela ainda possui um baixo nível de maturação, portanto há um longo caminho para que o blockchain chegue ao seu último estágio de desenvolvimento e se consolide como uma tecnologia que atenda a todas questões tecnológicas, legais e econômicas.

Ainda existem muitos desafios para implantação das soluções, porém o blockchain é um tema que cada dia atrai a atenção de mais pesquisadores, portanto, suas falhas tendem a ser mitigadas à medida que sua aplicação se tornar mais difundida.

6. Trabalhos Futuros

Este trabalho foca no uso do blockchain no setor de serviços financeiros e suas consequências. Porém é um assunto bastante novo e complexo; portanto ainda há muitos temas que merecem ser explorados a partir das ideias aqui apresentadas. Um tema que têm chamado muita atenção dos pesquisadores nos últimos meses são as Decentralized Autonomous Corporations (DACs), que basicamente são uma estrutura organizacional totalmente baseada em smart contracts, opera exclusivamente na nuvem e provêm valor para seus consumidores. Nesse sentido, seria importante investigar novos modelos de governança corporativa que atenda a essas novas estruturas organizacionais.

Vários bancos centrais ao redor do mundo já admitem a possibilidade de emitir suas próprias criptomoedas. No Brasil já existe o projeto de lei 48/2015 proposto pelo deputado Reginaldo Lopes com o objetivo de proibir a circulação de cédulas de dinheiro. A principal justificativa para o projeto é a de que transações digitais são mais seguras. Nesse contexto, seria um grande avanço científico uma análise para verificar a viabilidade de um projeto de emissão de criptomoedas pelo Banco Central do Brasil.

Nos últimos anos muitas pessoas se questionam sobre a validade do processo eleitoral brasileiro. Dentre as principais críticas estão a falta de transparência e auditabilidade. Uma proposta de um novo modelo eleitoral com base na tecnologia blockchain poderia aumentar significativamente a confiança e segurança do processo eleitoral.

Por último, ressalta-se que o blockchain é uma tecnologia de grande importância para a área médica e direito. Um estudo feito colaborativo entre pesquisadores da área de tecnologia com pesquisadores destas duas áreas poderia contribuir para manter a privacidade dos pacientes no que diz respeito a seu prontuário médico.

7. Referências

[1] CIO Explainer: What is Blockchain? Disponível em<http://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/> Acesso em: 25 de março de 2017.

[2] Etherum e o movimento da descentralização/upgrading da internet. Disponível em: <http://www.creativante.com/new/index.php/2013-02-03-19-36-05/2016/305-ethereu_m-e-o-movimento-da-descentralizacao-upgrading-da-internet> Acesso em: 21 de março de 2017.

[3] Byström, H. (2014). “Finance: markets, instruments & investments”. 3., edn. Lund: Studentlitteratur.

[4] Andersson, L. (2010). “Värdepapper: en genomgång av kapitalmarknaden och skattereglerna: aktier, obligationer, optioner, fonder, konvertibler”. 8., edn. Näsviken: Björn Lundén information.

[5] Simmons, M. (2002). “Securities Operations: A Guide to Trade and Position Management”. Sussex: John Wiley & Sons.

[6] Modelo Relacional. Disponível em:<https://pt.wikipedia.org/wiki/Modelo_relacional> Acesso em: 02 de abril de 2017.

[7] Programmable blockchains in context ethereum future. Disponível em:<https://media.consensys.net/programmable-blockchains-in-context-ethereum-s-future-cd8451eb421e> Acesso em: 10 de abril de 2017.

[8] World Wide Web. Disponível em:<https://pt.wikipedia.org/wiki/World_Wide_Web#Web_1.0> Acesso em 10 de abril de 2017.

[9] Spoke–hub Distribution Paradigm. Disponível em:<https://en.wikipedia.org/wiki/Spoke%E2%80%93hub_distribution_paradigm> Acesso em: 12 de abril de 2017.

[10] Carlsson, J. G.; and Fan J. Euclidean hub-and-spoke networks. Disponível em: <http://www-bcf.usc.edu/~jcarlsso/hub-and-spoke-rev2-raster.pdf> Acesso: 21 de maio de 2017.

[11] Peer-to-Peer Network Disponível: <https://www.infosec.gov.hk/english/technical/files/peer.pdf> Acesso: 25 de maio de 2017.

[12] Advantages of Peer-to-Peer Networking. Disponível em: <http://www.ianswer4u.com/2011/05/peer-to-peer-network-p2p-advantages-and.html#axzz4iPulNggh> Acesso: 25 de maio de 2017.

[13] Tian, F. An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology. Kunming 2016

[14] Yli-Huumo, J.; Ko, D.; Choi, S; Park, S.; Smolander K. Where is the current research in blockchain technology? – A systematic review. Virginia, 2016.

[15] Yermack, D. Coorporare Governance and Blockchian. Cambrige 2015.

[16] Blockchain basics: Introduction to business ledgers. Disponível em:<http://www.finyear.com/Blockchain-basics-Introduction-to-business ledgersa36159.html> Acesso em: 20 de abril de 2017.

[17] Walport; Walport, Mark. (2016) —Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser. Information Policy Team, The National Archives, Kew, London TW9 4DU. 65-71.

[18] What is a Smart Contract? Disponível em:<http://www.blockchaintechnologies.com/blockchain-smart-contracts#smart-contract-definition> Acesso em: 25 de abril de 2017.

[19] Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality. Disponível em:<https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/> Acesso em: 01 de maio de 2017.

[20] A Beginner's Guide to Smart Contracts. Disponível em: <https://blockgeeks.com/guides/smart-contracts/> Acesso em: 03 de maio de 2017.

[21] Bitcoin Hash Functions Explained. Disponível em:<http://www.coindesk.com/bitcoin-hash-functions-explained/> Acesso em: 05 de maio de 2017.

[22] Mining. Disponível em: <https://en.bitcoin.it/wiki/Mining> Acesso em: 08 de maio de 2017.

[23] Proof of Work. Disponível em: <http://www.investopedia.com/terms/p/proof-work.asp> Acesso em: 08 de maio de 2017.

[24] GIL, Antonio Carlos. Métodos e Técnicas de Pesquisa Social. 6. ed. São Paulo: Atlas, 2008.

[25] Sampieri, R; C. Collado; P. Lucio (2006), "Metodologia de Pesquisa", Mc Graw-Hill, S. Paulo.

[26] Blockchain Will Be Used By 15% of Big Banks By 2017. Disponível em:<http://fortune.com/2016/09/28/blockchain-banks-2017/> Acesso em: 12 de maio de 2017.

[27] Lundström, V. K. Impact from the blockchain technology on the Nordic capital market. Uppsala, 2016.

[28] Santo, A.; Minowa, I.; Hosaka G.; Kondo, M.; Hayakawa, S.; Ichiki, S.; Kaneko, Y.

Applicability of Distributed Ledger Technology to Capital Market Infrastructure. Tóquio 2016.

[29] BM&FBOVESPA becomes first exchange to join R3 distributed ledger consortium. Disponível em: <http://www.bmfbovespa.com.br/en_us/about/press/recent-releases/bm-fbovespa-becomes-first-exchange-to-join-r3-distributed-ledger-consortium.htm> Acesso em 12 de junho de 2017.

[30] 10 Stock and Commodities Exchanges Investigating Blockchain Tech. Disponível em: <http://www.coindesk.com/10-stock-exchanges-blockchain/ > Acesso em: 14 de junho de 2017.

[31] Post-trade Distributed ledger Group sees bright future for blockchain. Disponível em: <https://www.finextra.com/pressarticle/68000/post-trade-distributed-ledger-group-s ees-bright-future-for-blockchain> Acesso em: 16 de junho de 2017.

[32] Why banks are using blockchain? Disponível em:<http://www.oneglobeforum.com/blog/why-banks-are-using-blockchain> Acesso em: 16 de junho de 2017.

[33] Hearn, M. Corda: A distributed ledger. Disponível em: <https://docs.corda.net/_static/corda-technical-whitepaper.pdf> Acesso em: 17 junho de 2017.

[34] Guia Básico sobre o Etherum. Disponível em: <https://coinbr.net/media/pdfs/eth-guide-pt.pdf> Acesso: 17 de junho de 2017.

[35] Ethereum: A Secure Decentralised Generalised Transaction Ledger, Disponível em: <http://gavwood.com/paper.pdf >Acesso: 20 de junho de 2017.

[36] About Hyperledger. Disponível em: <https://www.hyperledger.org/about> Acesso em: 20 de junho de 2017.

[37] Chile's Largest Stock Exchange Plans to Implement IBM Blockchain Tech. Disponível em:<http://www.coindesk.com/chiles-largest-stock-exchange-plans-implement-ibm-blockc hain-tech/> Acesso em: 23 de junho de 2017.

[38] The Truth About Blockchain. Disponível em:<https://hbr.org/2017/01/the-truth-about-blockchain> Acesso em: 25 de junho de 2017.

[39] Blockchain and the sharing economy 2.0. Disponível em:<https://www.ibm.com/developerworks/library/iot-blockchain-sharing-economy/index.html> Acesso em 25 de junho de 2017.

[40] What Blockchain means for the Sharing Economy. Disponível em: <https://hbr.org/2017/03/what-blockchain-means-for-the-sharing-economy> Acesso em: 28 de junho de 2017.

[41] What is the Blockchain – part 3 – Blockchain Startups and Five Challenges to Overcome. Disponível em: <https://dataflog.com/read/what-is-blockchain-part-3-startups-

five-challenges/2381> Acesso em 28 de junho de 2017.

[42] Everything you need to know about open innovation. Disponível em: <https://www.forbes.com/sites/henrychesbrough/2011/03/21/everything-you-need- to-know-about-open-innovation/#5474935875f4 > Acesso em: 28 de junho de 2017.

[43] Why is blockchain a small revolution? Disponível em: <https://medium.com/@ericseulliet/open-innovation-co-creation-why-blockchain-is-a-small-revolution-73e7d0b480d5> Acesso em 29 de junho de 2017.

[44] The potencial use of blockchain in the public sector. Disponível em: <http://wavestone-advisors.co.uk/potential-blockchain-public-sector/> Acesso em 05 de julho de 2017.

[45] Bitcoin: A Peer-to-Peer Electronic Cash System Disponível. em: <https://bitcoin.org/bitcoin.pdf> Acesso em: 05 de julho de 2017.

[46] Comparasion of Ethereum, Hyperledger and Corda <https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6> Acesso em: 06 de julho de 2017.