TECNOLOGIAS DE REGISTROS DISTRIBUÍDOS E SUAS APLICAÇÕES AO MERCADO FINANCEIRO

Raul Baraldi Fernandes Alves (rbaraldi@gmail.com) - Instituto de Ciências Matemáticas e de Computação - ICMC/USP.

Silvia Lenyra Meirelles Campos Titotto (titotto@gmail.com) - Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, Universidade Federal do ABC.

RESUMO

Ao longo dos últimos anos, a tecnologia da informação contribuiu significativamente para a evolução dos mercados financeiros, sem, no entanto, revolucionar a forma como as instituições financeiras interagem uma com as outras. Isso pode começar a mudar, uma vez que alguns participantes do mercado financeito estão prevendo que as novas tecnologias de armazenamento de dados, como o blockchain e outras tecnologias de registros distribuídos (distributed ledger technologies), poderão ser a fonte de uma revolução iminente. Este trabalho analisa as principais características das chamadas DLTs (distributed ledger technologies), a sua relevância para a Internet of Things, os indicativos do seu potencial de adoção pelas instituições financeiras e como o uso dessas tecnologias podem afetar alguns serviços do mercado financeiro.

Palavras chave: blockchain, distributed ledger technologies, smart contracts, registros distribuídos, bitcoin, contratos inteligentes, pós negociação

Área: Potencial da Internet of Things (IoT)

1. INTRODUÇÃO

Dinheiro e os sistemas de pagamento estão intrinsecamente ligados. Para que um bem funcione como um meio de troca, é necessário que haja uma forma segura de transferir esse bem, algo que podemos chamar de um sistema de pagamento. E para qualquer sistema que não seja de troca de notas ou moedas físicas, também é necessário um meio de registrar os valores armazenados, um registrador. Os sistemas modernos de pagamento e demais transações financeiras são totalmente informatizados e a maioria do dinheiro existe apenas como registros digitais em contas digitais dos bancos comerciais.

1.1 A evolução dos sistemas de pós-negociação

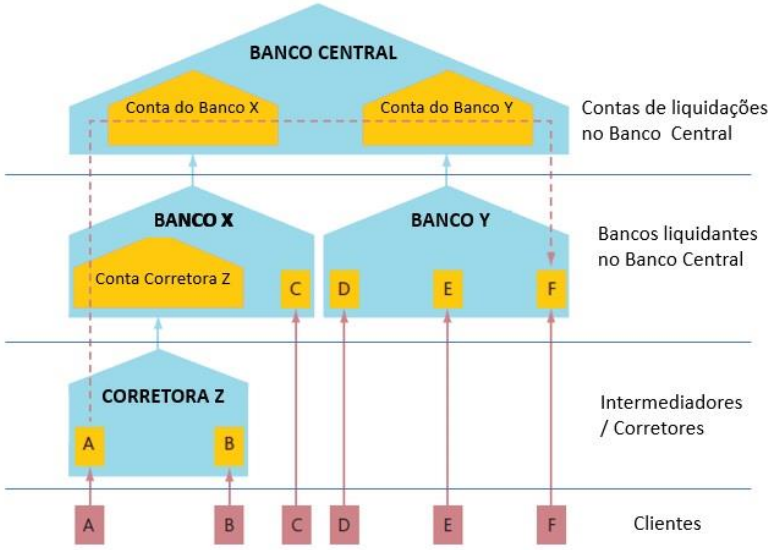
A tecnologia de pagamento utilizada na maioria das economias hoje evoluiu a partir dos primórdios dos sistemas bancários e ainda mantém estruturas características dessas raízes. Inicialmente, pagamentos ou transações eram feitos através da troca de itens intrinsicamente valiosos, como por exemplo, moedas de ouro. Quando os primeiros bancos começaram a surgir no século XVI, eles começaram a utilizar livros contábeis para registrar os débitos e créditos efetuados pelos seus clientes, o que permitiu que os pagamentos fossem feitos apenas realizando alterações nesses livros ao invés de trocar fisicamente os montantes em questão. Porém isso funcionava somente para clientes que compartilhavam do mesmo banco. Ao longo do tempo, a necessidade de fazer pagamentos entre os bancos levou ao surgimento de um banco central, para servir como uma espécie de câmara de liquidação e compensação, no qual todos os bancos membros pudessem manter contas, tornando as transações interbancárias muito mais simples (ALI et al, 2014).

Os desenvolvimentos tecnológicos nos últimos 40 anos afetaram os sitemas de transferências bancárias de duas formas principais (ALI et al, 2014). Primeiro, os registro contábeis foram convertidos para o formato eletrônico, o que aumentou a velocidade de conclusão de transações e reduziu os riscos operacionais. Em segundo lugar, o surgimento de tecnologias de baixo custo permitiu que surgissem novos esquemas de pagamento, como os feitos via aplicativos de *smartphones* ou via portais de acesso proprietário dos bancos na internet.

Apesar da utilização de novas tecnologias, a estrutura básica dos sistemas de transações bancárias centralizada parmaneceu inalterada. No centro encontra-se um registrador central, no qual as liquidações das transações são feitas por uma autoridade, agindo como um banco de compensação (normalmente atribuído a um banco central da respectiva economia, ou a câmara de liquidações regulamentadas pelo banco central). Cada participante, normalmente uma instituição financeira, mantém um saldo no banco central, registrado no livro contábil do banco central, mas por sua vez também registrado no livro contábil da própria instituição financeira. Clientes (pessoa física), empresas ou até mesmo outros bancos manteriam o seu

balanço financeiro diretamente na instiuição financeira, que por sua vez refletiria no balanço da respectiva instituição no banco no central.

Figure 1. Exemplo de estrutura cetralizada, Fonte: autor



Nos últimos anos, foram surgindo uma variaedade de desenvolvimentos em novas tecnologias de pagamentos, transações bancárias e até mesmo moedas alternativas. Algumas dessas inovações se concentram em tornar as transações mais acessíveis a uma ampla gama de usuários, como por exemplo os pagamentos via aplicaticos de *smatphones*, mesmo ainda estando associados a uma instituição financeira por trás e entidades centralizadoras.

Inovações ainda mais recentes introduziram uma estrutura fundamentalmente diferente e descentralizada para os sistemas de pós-negociação (responsáveis pela liquidação e registros efetivos das transações), utilizando-se da criptografia para garantir unicidade e legitimidade, ao invés da confirmação de uma autoridade central. O grande exemplo de nova estrutura foi introduzida pelo moeda digital mais proeminente no momento - o Bitcoin. Criada em 2009 por um engenheiro de computação sob o nome de Satoshi Nakamoto. Além da moeda, nos apresentou também o conceito de DLT para o gerenciamento das transações feitas nesta moeda digital, o qual é amplamente conhecido pelo nome de *blockchain*.

2. MOEDAS CRIPTOGRAFADAS E O BITCOIN

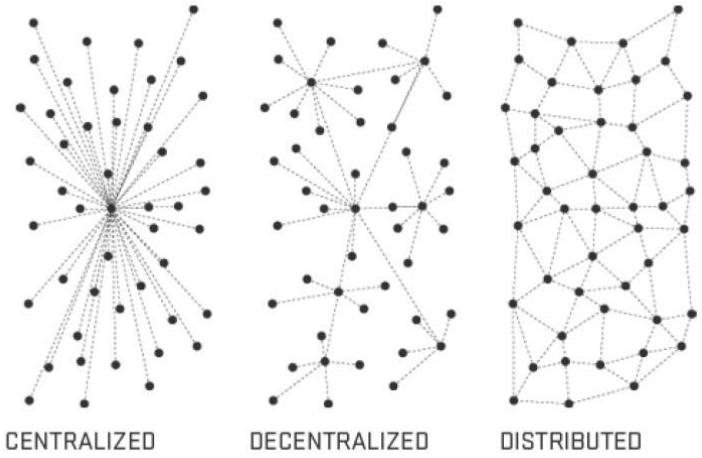
Bitcoin foi a primeira e ainda se mantem como a maior moeda digital. Foi lançada em janeiro de 2009 e é uma moeda desenvolvida de forma privada, independente de instituições reguladoras, focada na arquitetura da internet e que também não requer intermediários (como bancos) para a processamento de transações financeiras. Além disso, o fornecimento de bitcoins é não controlado por um banco central. (1) É comumente referido como uma "*cryptocurrency*", pois depende de técnicas de criptografia para garantir a validação segura das transações. Atualmente existem várias centenas de *cryptocurrencies*, tal como Litecoin e Peercoin. A maioria destes foram inspiradas, ou explicitamente baseadas em Bitcoin.

Figura 2. Exemplo de *cryptcurrencies*. Fonte: PluralSight

Os usuários do Bitcoin não precisam divulgar quem são, eles mantem uma "carteira" digital em seus computadores e, por meio de softwares e aplicativos específicos, negociam a moeda entre si em troca de moeda tradicionais ou bens e serviços. Várias milhares de empresas no mundo aceitam atualmente Bitcoins em pagamento por qualquer coisa, desde pizza até hospedagem de sites. Os pagamentos podem ser feitos a qualquer momento e entre qualquer par de usuários em qualquer lugar do mundo.

A chave da inovação destas moedas digitais é a utilização de registros distribuídos, o que permite pagamentos serem realizados de formas decentralizada. Como isso funciona, e como ele é a chave da inovação para transações financeiras, veremos adiante neste trabalho.

Figura 3. Estruturas centralizadas, descentralizadas e distribuídas. Fonte: R3 Consortium



3. TECNOLOGIA DE REGISTROS DISTRIBUÍDOS

A chave da inovação técnica das moedas digitais é o registro distribuido e seu poder de solução do problema de *double spend* em um sistema de pagamentos decentralizados. O registro distribuído (*blockchain* no caso das *cryptocurrencies*) foi possível graças ao surgimento de várias inovações anteriores, incluindo a internet. Baseia-se em conceitos de criptografia, teoria dos jogos e redes *peer-to-peer* (TAPSCOTT et al 2016).

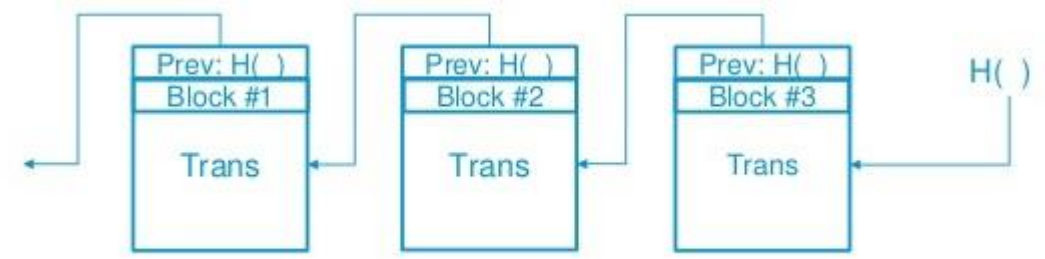
A tecnologia *blockchain* fornece uma alternativa que permite que qualquer participante único essencialmente "terceirizassem" os problemas de gerenciamento, comunicações e escalabilidade da rede *peer-to-peer* que mantém a cadeia de blocos. Em vez de usar um servidor central, um registro público distribuido será mantido para armazenar os registros de transações de "coisas" (neste caso estamos focando em transações financeiras) e cada nó possuirá uma cópia deste registro público imutável.

O uso de DLT fornece a capacidade de redistribuir os custos em todos os participantes da rede *peer-to-peer* e dar a cada par uma motivação econômica para fornecer sua (pequena) parte da infra-estrutura necessária para permitir o bem maior. Isso reduz o fardo para qualquer pessoa individualmente, ao mesmo tempo em que permite aproveitar os recursos de todos. O custo para adicionar uma mensagem à cadeia é uma pequena "taxa de transação", de modo que uma mensagem de transmissão pode ser adicionada à cadeia de blocos e ser recebida literalmente por um bilhão ou mais de dispositivos por muito pouco custo direto relativo para o remetente. Isso não é muito possível com uma abordagem centralizada.

3.1. Blockchain – a estrutura do registro distribuído

Conforme já mencionamos, *Blockchain* é basicamente uma cadeia de blocos conectados sequencialmente. Nesta cadeia de blocos, os dados ordenados cronologicamente são agrupados em unidades de armazenamento individuais denominadas blocos. Esses blocos são então ordenados sequencialmente e armazenados de forma descentralizada em todos os nós participantes para formar o *blockchain*. Cada vez que um bloco é concluído, um novo bloco é gerado. A tecnologia é altamente apreciada por ter o conceito de "armazenamento de dados imutáveis", que foi um sonho no mundo da computação por muitas décadas. A técnica de mapeamento de dados (*hashing*) desempenha um papel vital no armazenamento de dados imutáveis. Para conferir imutabilidade à cadeia de blocos, um valor de *hash* é computado e armazenado localmente dentro de cada bloco usando seu conteúdo e o valor de *hash* de seu antecessor imediato. A função *hash* é projetada de forma que seja muito complexa para calcular, porém fácil de verificar. Esta seqüência de funções de *hash* para os blocos cronologicamente ordenados formam assim um mecanismo público disponível e fácil de verificar para proteger o conteúdo da cadeia. Devido à dependência cronológica do bloco anterior, o valor *hash* armazenado em cada nó não pode ser adulterado. A seqüência pública verificável de funções de *hash* associadas ao bloco de cadeias torna qualquer modificação ilegal facilmente identificável. Além disso, qualquer adulteração exigiria a re-computação de toda a cadeia de *hash*, o que é computacionalmente muito custoso e isso faz do *blockchain* um "registro de dados imutável". Simplesmente, esta tecnologia pode ser vista como uma abordagem inovadora da criação de um registro público seguro que aproveita o potencial de redes *peer-to-peer*, *hash* criptográfico e abordagem de consenso distribuída em um enigma matemático complexo (Nakamoto,S. 2009).

Figura 4. Estrutura do blockchain. Fonte: Princeton University Press



Uma vez que um bloco é adicionado ao registro público distribuído, é extremamente difícil modificá-lo ou removê-lo. Sempre que um nó quer adicionar conteúdos à cadeia, cada nó em questão executa o algoritmo de consenso para avaliar e verificar a transação e todo o histórico do nó. O nó pode ser um indivíduo, um grupo de *miners* ou somente uma máquina equipada com *smart contracts*. Se a maioria dos nós concordar com a validade da transação, então será aprovada e será adicionada ao novo bloco na cadeia. Geralmente, os critérios para a maioria e o número de confirmações necessárias serão incorporados ao primeiro bloco (bloco gênese) da cadeia de bloco (SWANSON, 2015). Dentre as características do *blockchain* que são altamente bem vidas pelo mundo da computação, podemos citar:

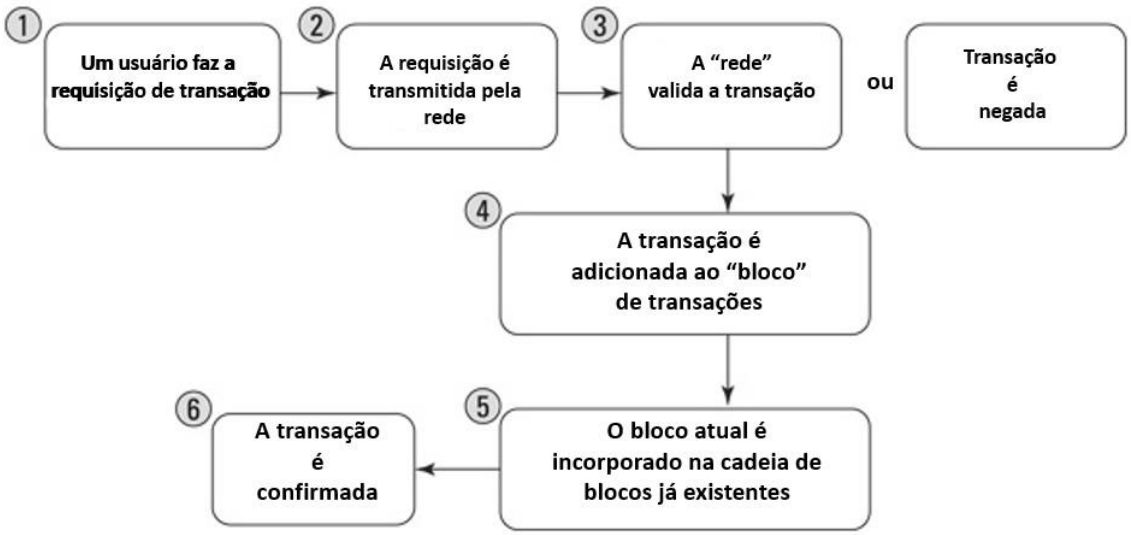
• Cada nó na rede de cadeias de blocos pode convergir em uma estratégia de consenso da última versão do registro público distribuído, mesmo com nós "desonestos" e anônimos para garantir que nenhum ataque ocorra na cadeia.

• Todo nó válido que participa na rede do *blockchain* tem a capacidade de determinar a validade de uma transação e ganha recompensa na conclusão bem-sucedida do consenso.

• *Blockchains* facilita a transação eficiente entre entidades desconhecidas sem a ajuda de intermediários confiáveis . Também podem eliminar o problema *double-spend* e as transações conflitantes da rede.

• A rede *Blockchain* cobra custos extremamente elevados para modificar ou reescrever uma transação.

Figura 5. Ciclo de vida de uma transação via blockchain. Fonte: autor



3.2. Blockchain – confiabilidade e segurança contra ataques

O esqueleto do *blockchain* existe em torno de um grande número de nós conectados para formar uma rede distribuída. Cada único nó na rede tem uma cópia de toda a cadeia de blocos, e ao mesmo tempo que torna o ataque / *hacking* extremamente difícil, também o torna fácil de ser detectado e eliminado. Supondo que um invasor tente alterar as transações em um bloco intermediário, então ele deve fazer as mudanças nesse bloco e refazer todos os blocos sucessivos até o bloco atual dentro de um curto período de tempo em que todos os nós válidos funcionam no consenso para criar o bloco atual. Mesmo que um hacker tenha sucesso em qualquer tentativa, a mudança será refletida para apenas um nó e o conteúdo das cadeias em todos os outros nós não serão afetados. Cada nó na cadeia ajuda no desenvolvimento de um ambiente distribuído e confiável através da rede de consenso *peer-to-peer*. Esta propriedade dos nós melhora a confiabilidade da rede *blockchain*.

Uma das principais propriedados do *blockchain* para assegurar esta dinâmica é o chamado *proof-of-work* (POW), o qual pode ser definido como um *puzzle* que pode ser resolvido apenas computacionalmente. Este potencial do POW foi utilizado para estabelecer um paradigma de computação assimétrica, de modo que a computação deve ser desafiadora (mas viável) no lado do solicitante, e ao mesmo tempo fácil de verificar para o provedor de serviços (Asharaf et al., 2017). O conceito do POW é utilizado para resolver o problema do *double-spend* e criar uma plataforma de consenso livre de confiança distribuída. Para perceber este mecanismo de consenso distribuído.

4. VIABILIDADE PARA O MERCADO FINANCEIRO

Atualmente, todos os bancos e instituições financeiras estão mantendo grandes bancos de dados individualmente, isso resulta em alto consumo de energia, mão de obra e plataformas de segurança sofisticadas. Com o *blockchain*, a necessidade de um banco de dados centralizado e de alta disponibilidade pode ser completamente eliminada e cada banco pode fazer transações em uma única cadeia, o que colocaria em cheque até mesmo a necessidade da existência física de um banco. O tempo de liquidação entre os bancos e as câmaras de compensação poderia ser reduzidos de vários dias úteis para até alguns minutos, ou mesmo segundos, com possibilidade literalmente nula para transações duplicadas ou falsas.

No futuro, os bancos poderiam cobrir os clientes globalmente sem a necessidade de um escritório em todos os locais, mas apenas virtualmente através de uma rede *blockchain*. Isso reduziria o custo operacional, a taxa de transação e a necessidade de funcionários, tornando o negócio altamente lucrativo. O Blockchain também exploraria o potencial de ligação com outros paradigmas de negócios que poderiam criar oportunidades para melhorar os modelos de negócios das instituições financeiras (Moody’s, 2016).

Instituições financeiras estão cada vez mais confiaando em *smart contracts* como uma solução prática para reduzir os custos indiretos e acelerar a negociação e a liquidação. Grandes bancos como Citi e J.P. Morgan (SWIFT, 2016), juntamente com câmaras de compensação como a Depository Trust & Clearing Corporation, estão no processo de construir e testar *smart contracts* para negociar swaps de inadimplência de crédito.

4.1 RESISTÊNCIAS E DIFICULDADES

Alguns estudos porém apontam que este processo não necessariamente seria algo simples de ser implementado de forma a estabelecer uma nova dinâmica no mercado (MAINELLI et al, 2015). Muito disso também se deve ao fato de que a tecnologia ainda não é totalmente compreendida e, ao mesmo tempo, não existem ainda casos de sucesso bem consolidados no mercado, mesmo com do sucesso e do crescimento que as negociações de Bitcoin vem apresentando ao longo da última decada.

Representantes técnicos de participantes ativos do mercado também levantaram questionamentos pertinentes nos últimos anos, porém não necessariamente consistentes com as premissas básicas do *blockchain*.

- No contexto do mundo real do mercado financeiro, registros distribuídos não necessariamente removem totalmente a necessidade de entidades centrais participando das transações (MAINELLI et al, 2015). Neste caso o papel da entidade central seria limitado apenas a asegurar a identidade das partes, assim como a existência dos saldos a serem transitados de uma parte para a outra (MAINELLI et al, 2015). No entanto, foi descrito nas seções acima deste trabalho, que o *blockchain* justamente é utilizado para tornar desnecessário qualquer controle de indentidade ou de recurso, uma vez que o histórico da cadeia de blocos já traz uma identificação forte e também garante a existência do recurso financeiro (MOUGAYAR et al, 2016).
- Uma outra observação levantada foi que, uma vez que o registro distribuído se comporta como um grande banco de dados distribuído, seria pertinente avaliar esta estrutura sob a ótica da estrutura tradicional de banco de dados relacional adotada amplamente há mais de três décadas (PINNA et al, 2016). Novamente não aparenta ser algo que se aplique na discussão, uma vez que a premissa e o principal benefício do *blockchain* é justamente a independência de cada transação e a arquitetura estrutural da cadeia de blocos (MOUGAYAR et al, 2016).

5. CONCLUSÃO

Em geral, as negociações realizadas sobre uma estrutura de cadeia de blocos com registros distribuídos apresentam benefícios técnicos importantes quando comparados aos sistemas tradicionais. As partes podem desfrutar de mais privacidade, segurança, monitoramento e controle sem complicações sobre seus ativos financeiros a um custo razoável. Pensando nas empresas, esta tecnologia pode cortar as taxas de processamento, permitir um pagamento global mais rápido e reduzir o risco de fraude drasticamente. Porém mantendo como grande desafio o movimento que tome a frente e inicie a mudança de paradigma em escalas globais.

Um grande consórcio de empresas e bancos, chamado R3, foi criado com o obejtivo de ser o agente desta mudança. Empresas como IBM e a Samsung apresentaram nos últimos meses provas de conceito com *blockchain* feito através de um sistema chamado ADEPT. E começaram a integrar esta tecnologia em diversas soluções de softwares e aplicativos que já existiam. Como por exemplo a plataforma Watson da IBM, um dos grande símbolos da internet das coisas (IoT) e de soluções envolvendo inteligência artificial.

Podemos tentar ir um pouco além e pensar também que as informações sobre o bem-estar financeiro de uma empresa muda o tempo todo. Quando você pesquisa na web os dados

financeiros de uma empresa, você procura em duas dimensões: horizontal (na web) e vertical (em sites específicos). O que você achou pode estar desatualizado ou impreciso.

Em uma cadeia de blocos, porém, há uma terceira dimensão: a seqüência. Além de poder obter uma imagem histórica da empresa desde que foi incorporada, você pode ver o que ocorreu nos últimos minutos. A oportunidade de pesquisar o registro completo de valor de uma empresa terá implicações profundas para a transparência da mesma, pois traz à luz transações off-book e contas ocultas. As pessoas responsáveis por registros e relatórios serão capazes de criar filtros que permitam aos interessados encontrar o que estão procurando por meio de um simples clique em um botão.

6. BIBLIOGRAFIA

ALI, R., BARRDEAR, J., CLEWS, R., SOUTHGATE, J. 2014. *Innovations in payment technologies and the emergence of digital currencies*. Bank of England, Quarterly Bulletin, Q3.http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q301.pdf

ASHARAF, S.,ADARSH, S. 2017. *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities*, IGI Global.

CHRISTIDIS, K, DEVETSIKIOTIS, M. 2016. *Blockchains and Smart Contracts for the Internet of Things*, IEEE Access

MOUGAYAR, W., BUTERIN, V. 2016. *The Business Blockchain*. Jonh Wiley & Sons

MOODY'S. 2016. *Robust, Cost-effective Applications Key to Unlocking Blockchain's Potential Credit Benefits*.

NAKAMOTO, S. 2009, *Bitcoin: A peer-to-peer electronic cash system*, manuscript

https://bitcoin.org/bitcoin.pdf

PINNA, A., RUTTENBERG, W. 2016. *Distributed ledger technologies in securities post-trading*, Occasional Paper Series, European Central Bank.

SWANSON, T. 2015. *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*. R3 CEV

SWIFT, 2016 *Swift on Distributed Ledger Technologies*, Position Paper https://www.swift.com/sites/default/files/resources/swift_position_pape_dlts.pdf

MAINELLI, M., MILNE, A., 2016. *The Impact and Potential of Blockchain on Securities Transaction Lifecycle*. SWIFT Institute Working Paper No. 2015-007

https://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf

TAPSCOTT, D., TAPSCOTT, A., PILGRIM, J. 2016. *How Blockchain will change organizations*. MIT Sloan Management Review.