Massachusetts Institute of Technology

MIT Connection Science

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Blockchain & Transactions, Markets and Marketplaces

PART 2

MAY 2016

David Shrier, Jaclyn Iarossi, Deven Sharma, Alex Pentland
Connection Science & Engineering
Massachusetts Institute of Technology

connection.mit.edu

Massachusetts Institute of Technology

MIT Connection Science

The authors would like to thank the team that helped develop this document, including Jackie Iarossi, German Canale and Weige Wu at MIT Sloan, Michael Casey at the MIT Media Lab Digital Currency Initiative, and Alex Lipton.

This paper is the second of a 4-part series:

- Blockchain & Financial Services: 5th Horizon of Networked Innovation: May 3
- Blockchain & Transactions, Markets and Marketplaces: May 10
- Blockchain & Infrastructure (Identity, Data Security): May 17
- Blockchain & Policy: May 24

I. Introduction

In our May 3 paper in this series, we provided a framework describing blockchain as a "fifth horizon of networked innovation", and outlined basic principles of how the technology operates (both in a technical sense and in a socio-political context). In this installment, we will look at the future impact of blockchain on transactions, markets and marketplaces.

Blockchain technology has the potential to address a number of sectors. We will focus our discussion on:

- **Securities trading:** potential to exceed US$20 billion in cost savings among incumbent financial companies, and possibly drive significant disruption within the existing financial ecosystem.

- **Commercial & Retail Banking:** accessing the US$ 2 trillion credit gap globally.

- **Insurance:** addressing the US$40 billion uninsured in the "protection gap".

Exploiting these opportunities will have profound implications for the numerous intermediaries currently serving these sectors.

Many facets of today's markets and marketplaces are likely to be impacted by large-scale adoption of blockchain technology, creating many new avenues for value creation. Focusing on a few key applications areas for institutional players and Small to Medium-sized Enterprises (SMEs), impact from blockchain technology can range from increasing global access to finance, creating new transaction types and reimagining existing exchange and structural models.

Most transactions are accompanied with data that give them intelligence. For example, data underlying transactions may include information to complete a transaction such as the account and routing number of the payor and payee that identify the source, and receiver and all intermediaries through which the transaction may have passed. Increasingly, transactions also include additional information attributes on participant location and behavior. Data associated with each transaction provides critical information on transaction instruments and the risks associated.

A transaction, such as a typical non-cash payment, can be distilled into elements: Originator, Funding, Instrument, Usage, Processing, Receiver, Confirmation and Settlement. The data attached to transactions raises a fundamental tension: ample data aids in protecting fraud risk, creates opportunity to offer or receive more personalized service, but increases privacy risk. A payment trail, defined as the intermediaries involved and who thus have access to the data on the transaction, also adds to the risk. Cash has no intermediary. Early forms of electronic payment with credit card have six intermediaries: Payor, Website/App Operator, Merchant/Payee, Merchant Bank (Acquirer), Card Network, Customer/Payor Issuer. Different intermediaries have varying practices of capturing, retaining and using the data and as such, the longer the trail the greater the risk.

Fundamentally, advantages that blockchain offers include:

- **Shared ledger:** greater auditability and transparency provides greater trust. Absence of a central intermediary can make micropayments more economical

- **Encryption:** the enhanced security afforded by blockchain provides for more confidence to conduct larger value and riskier transactions

- **Embedding application logic within a transaction:** one can use data attributes embedded in the transaction to make transaction flow conditional on time, location, event, trust level, etc., which creates pathways for automated interactions, eliminating cost and improving speed via vehicles such as smart contracts

Blockchain provides the capability to collapse the transaction trail, and still offer traceability and transparency. Not only can it speed up the process, but also reduce the risk associated with the completion of the transaction and misuse of any data.

II. Commercial & Retail Banking

While approximately 95% of the world's businesses are SMEs, as many as half of them cannot get the financing they need – a credit gap estimated at over $2 trillion across over 200 million businesses[2].

A. Collateral Registries

Often a lack of sufficient collateral serves as a limiting factor on the ability of SMEs to secure a loan, particularly in developing countries. According to the World Bank globally almost 80% of all enterprise loans require collateral, which on average needs to be valued at 202.7% of the loan amount.[3]

While property is internationally accepted as a form of collateral, moveable assets such as receivables or inventory frequently are not, and yet comprise the majority of SME value. Wider use of movable assets as collateral is limited by a lack of trusted, central collateral registries which currently require government support and funding.

How impactful is a trusted movable assets registry? In a 2013 study of over a 100 countries, those that implemented collateral registry reform saw an 8% increase in access to credit for SMEs.[4] Further work by the IMF saw significant increases to access to credit and lower costs of credit. "In countries where security interests are perfected and there is a predictable priority system for creditors in case of default, credit to GDP averages 60 percent, compared with 30 percent to 32 percent of average for countries without a clear creditor protection system. In industrial countries, borrowers using collateral get nine times the level of credit, repayment periods up to eleven times longer, and interest rates 50 percent lower than borrowers without collateral." Systemically, it also reduces financial institutional risk by increasing diversification of assets, offering opportunities to lenders to increase market share and short-term liquidity of those assets.[5]

Despite overwhelmingly positive benefits many countries have yet to implement collateral registries and inconsistent standards exist globally. Blockchain technology means that creation of these registries will no longer depend on government sponsorship. Using best practices already established by international agencies such as the IMF, SMEs could register their assets and grant access to potential lenders offering better information to make credit decisions.

An added benefit for SMEs to register their goods: fraud reduction. According to Sylvain Theveniaud, managing director of Allianz Accelerator "a definitive registry to trace ownership and certify provenance of big-ticket items would root out illegal goods and decrease fraud worldwide."[6] The value of blockchain is significant in potentially mitigating the $1.77 trillion cross-border counterfeit goods market.[7]

B. Smart Property

In September 2014, China and Hong Kong had amassed a $13.5 billion commodity trade discrepancy in just 9 months. It is believed that to circumvent Chinese capital import laws, fake commodity invoices were created leading to manipulation of export numbers as well as the yuan.[8] If the trades represented by these disputed invoices were required to share one ledger there would be no way to arrive at any settlement differences.

The diamond industry derives a lot of its value based on provenance. To combat blood diamonds and prove the value of the stone there is an industry-wide initiative to implement Everledger, a distributed platform that creates a unique digital fingerprint for each diamond so it can be tracked through all borrowers straight to its origin.[9]

But what if we could move one step further in validating underlying collateral or commodities are where and what was promised? Combining blockchain with another growing technological force, the Internet of Things, could unleash a powerful new idea, smart property. If a physical asset was embedded with sensors, the property would record any transaction where ownership changed hands or alert parties that terms of a contract may not be satisfied. Using oil as an example, before agreeing to the terms of a deal, the exact chemical composition and weight of a barrel of oil would be known. If a storm disrupted shipping times, a cargo ship could trigger contingency clauses of a contract and alert impacted parties.

Collateral management could be even more streamlined. If a business puts its inventory up as collateral, the collateral value could dynamically update improving the risk and collateral management teams supporting the loan more like a securities-backed loan. For any type of collateral utilizing a collateral ledger and smart contracts, the parties could agree upfront on specific reference data, be it information within the company or external macro data, automatically triggering and either satisfy or alert all parties to a collateral call. Closing the gap on collateral management could have a huge net effect, inefficiencies in the global collateral management market are estimated to cost banks up to $4 billion annually.[10]

C. Commercial Payments / New SME Opportunities

There has been a question around blockchain technology of what is the real use case? Is this just a solution in search of a problem? Micropayments are an example of a problem-space suitable for a peer-to-peer low cost value transfer method. Poised to help redefine many business models, micropayments are transactions less than $10. The idea of online micropayments were championed by IBM and Netscape so much so that they lobbied the World Wide Web Consortium (W3C) to develop universal micropayment standards - there is even an error code 402 built into the web for require payment[11, 12].

Micropayments never gained critical mass before as they were not financially feasible and many businesses saw no need for revenue streams beyond advertising and subscriptions. The normal business model of taking a small percentage of each transaction is prohibitively expensive for high volume low value payments.[13] The exorbitant expense comes from transmitting the data associated with transaction and processing to complete the transaction. The world of ecommerce looks very different now, with diminishing advertising margins and subscription models still proving difficult.

Other SME micropayment opportunities are additionally emerging. Gyft provides gift cards to SMEs who previously were not large enough to support the necessary payment infrastructure, a nice boon since 65% of consumers spend 38% more than the face value of their gift cards according to CEB. Gyft ultimately wants to fundamentally change gift cards by creating a standardized trading platform for gift cards and see their issuance through blockchain to reduce issuance costs. Consumers could easily exchange gift cards and never lose the card value.[14]

III. Securities & Trading

Trade and collateral finance are one of many financial spaces that startups and incumbent players are creating new solutions underpinned by blockchain technology. Ideas covering commercial payments, capital markets and beyond are all receiving attention and funding.

A. Capital Markets / Institutional Changes

Today's capital markets infrastructure, systems, processes and regulation are overly complex and built when the financial world looked very different from today. Looking through the entire lifecycle of a trade, there are a number of significant areas that in an ideal state, is implemented as the underlying infrastructure, shown in this exhibit[15]:

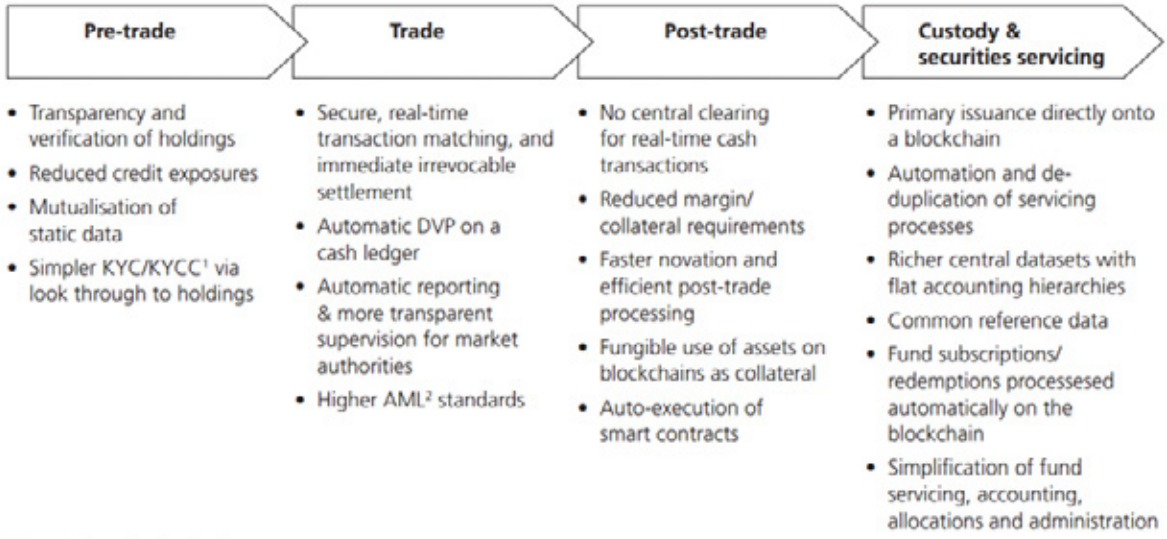

Figure 4 – benefits of adoption

[1] KYC – Know Your Customer, KYCC – Know Your Customer's Customer
[2] AML – Anti-Money Laundering

Some of the areas with the greatest promise for improvement over the current state include asset ownership, new financial instruments and settlement.

B. Asset Issuance and ownership

Assets would be issued directly into the blockchain ledger. When transactions take place to buy or sell it would simply involve entries being matched in a peer to peer method, with clear ownership based on identify or in the case of a broker someone with clear permission acting on someone else's behalf. This collapses many layers of intermediaries and complexity required under the current system.

For example, shares would be issued digitally via the blockchain and tied to the owners' and/or brokers' identity not an intermediary or custodian as they are today. This is a powerful change for several reasons, because the settlement of cash and the securities exchange could be simultaneous. Faster settlement and elimination of paper certificates would reduce costs. Most importantly share owners would be able to ensure all the rights granted by ownership, which are not always guaranteed by today's system. Today as a cost reduction initiative almost all shares are technically owned by a subsidiary of the Depository Trust & Clearing Corporation (DTCC), so that paper stock transfers are kept in one place and accounted for by one entity.

As recent as a 2015 ruling on the Dell acquisition some shareholders lost their appraisal rights in Delaware court simply because shares had to be retitled in order for the physical paper to be stored without an additional fee, meaning that there was not continuous ownership.[16] While there are several compounding factors in this case, the issue here is that there are broader issues with the system which could be addressed with a digital, secure asset. Going even further would to have all shareholder votes recorded directly on the asset, which means the entire voting history of that share could be attached to the share, regardless of ownership change.

Several companies have started playing with this type of asset issuance today. The most prominent took place in December 2015. Created by a partnership between Nasdaq and Chain, the Linq platform issued and settled the first securities transaction using blockchain backed technology. This was a private equity issuance to a US investor for a private amount.[17]

C. Settlement & Reconciliation

As shown with the collateral trade differences, having only one version of the truth is extremely beneficial to a settlement and reconciliation process. With reducing the number of parties required to execute one transaction and working off a shared ledger has the ability to greatly reduce reconciliation process both with external parties and for internal systems. Distributed ledger technology is projected to reduce costs associated with cross-border payments, securities trading and regulatory compliance by $15-20 billion per year by 2022.[18]

What does this mean in practice for post-trade settlement? First ownership transfer and payment could be simultaneous, cutting counterparty risk down from T+3 to minutes, or whatever timeframe is deemed ideal for the security type. Counterparty risk is further decreased with significant reduction in asymmetric information through counterparty transaction history, immediate collateral information updates, full asset title records and more. Implementing robust smart contracts means that parts of deals could be settled machine to machine rather than requiring significant manual confirms. Lastly, monitoring parties, regulatory or agreed third-party, could be granted access to have complete transaction details and be able to real-time monitor.

Yet, at the same time, instantaneous settlement (or even settlement in a few minutes) will eliminate some of the flexibility inherent in the current system. For example, T+3 allows for borrowing against and lending of shares purely as a broker-based transaction, allowing greater speculation capabilities on the part of rapid traders – something that will be lost in a world with no float. Should a market be constructed only for long-term holders, or should it also facilitate high frequency traders and short-term speculators? Do those short-term players provide for greater liquidity and price flexibility in a dynamic market environment?

Execution errors are another issue that blockchain complicates. The BATS exchange had to withdraw its 2012 IPO due to a programming error, requiring a 4-year wait until it could finally go public in 2016. While current settlement systems allow for a voiding and reconciliation process, imagine the challenges of "rollback" in a blockchain world: by definition, blockchain is an irrevocable record. Furthermore, an automated series of "irrevocable" trades using blockchain could create a cascading series of errors that become difficult to unwind – without the simplicity of a database rollback, the dependent nature of the "chain" creates a new kind of complexity on resolving errors. The so-called "Lehman Hairball" (of interdependent derivatives contracts) still hasn't been resolved six years later. If not proactively designed, a blockchain-based market might be even more opaque.

D. Financial Instruments and Smart Contracts

With more information (i.e. decreased asymmetric information), property and digital IP more publically available new niche derivatives will become possible as underlying assets are more transparent and secondary markets significantly easier to create. Going a step further, needs of company could be broken down to individual cash flows, then bundled to create all new swaps.

The biggest boon to financial engineering comes in the form of Smart Contracts – computer programmable contracts that are verified and enforced electronically. Chris DeRose, community director of the Counterparty Foundation believes that smart contracts create risk reduction through non-discriminatory execution.[19] It creates a cheap, previously agreed method to ensure that all parts of a contract are fulfilled without interference.

IV. Insurance

The global insurance industry is acutely aware of the "insurance protection gap" – the idea that there are a large number of people who should have insurance but don't. According to industry trade group The Geneva Association, the emerging markets comprise 40% of the world's GDP but only 17% of its insured population. Globally, 4 billion people are uninsured, representing notional premiums of US$40 billion annually[20].

Blockchain-based smart contracts could provide for automated claims handling and processing, making for a cost-effective microinsurance solution. When combined with other solutions, such as machine learning systems and pattern recognition technology, one could imagine a property & casualty world in which auto claims, for example, could be assessed via an automated system analyzing images captured via a mobile phone, and a claim could be adjudicated in a matter of minutes instead of days or weeks.

An even more disruptive application of blockchain is in the area of peer-to-peer insurance, circumventing established companies (if the regulatory issues are addressed). For example, Uber or Lyft drivers, who currently rely mainly on their personal auto policies, could pool their money on a blockchain and create a smart contract to insure each other, DeRose says. "That's what insurance companies do now, only they govern the pool and take money off the top," he says. "If you have an unbreakable chain of identity to issue an insurance policy, why do you need an insurance company at all?"[21]

As with other intermediated markets, new technology such as distributed cryptographic ledgers could reduce cost and improve access in insurance.

V. Privacy

We will get into greater detail on questions of privacy in our next paper about Infrastructure. However, it is worth noting that transparency on transactions may have the unintended consequence of revealing proprietary trading strategies that financial investors have developed – making it less attractive for them to participate in a market. How can privacy of individuals and firms be appropriately managed in a system that is fundamentally designed for transparency? Zero-knowledge proofs may be a partial answer, where critical or relevant information can be queried (such as: does this entity have enough funds to cover the margin call?) without revealing other data (such as: what is this entity's total portfolio value?).

VI. Rethinking Intermediaries and Other Market Participants

One of the biggest systemic questions for the mass implementation of blockchain in financial markets centers on the role of counterparties and intermediaries. The current system of intermediation arose out of needs to manage risk, particularly when securities were transacted using paper instruments. While intermediaries have adapted somewhat to digital environments, they have no incentives to reduce margin or eliminate their roles entirely.

When envisioning the future state for capital markets, it is important to remember that technology introduction has previously created opportunity to reduce the number of intermediaries. Computing technology, and later the internet, helped lead to disintermediation and ultimately the creation of the DTCC. This paradigm shift created efficiency savings as well as reducing risk for a system too complex for the new technical realities of finance.

A significant market benefit of blockchain is the collapsing of additional custodial layers, achievable through use of a single ledger and transparent audit. Retrofitting the technology to current processes will inevitably limit how far forward capital markets can be developed, and how many layers of intermediation can be removed. Rethinking the entire transaction system would allow for more profound efficiencies to be introduced, but also creates transition risk.

So what do the future intermediaries look like? Focusing on the core functions that intermediaries play today, there are several roles that will need to be considered.

While who or what performs these functions may differ on based on the asset class, these functions are still required for a properly functioning market:

IMPACT OF BLOCKCHAIN ON DIFFERENT MARKET PARTICIPANTS

DIMENSION	COMMENTS
Financial Guarantor	If the transaction is allowed to be T+0, as in no delay between the transaction confirmed to the chain and settlement of the transaction there is no timing risk thus no intermediary, other than the market itself, is required. However, in the US capital markets today there are legal mandates, not technological limitations, which set many settlement periods, such as the US equity market convention of T+3 which is set to move to T+2 by 3Q 2017[22]. If those settlement requirements remain then counterparties would be exposed to some risk. In these scenarios there is an opportunity to create some kind of holding account or have a clearing party serve the guarantor function.
Security Register and/or Transfer Agent	**Embedded Asset:** If the asset is embedded, for example through a digital equity issuance, then the marketplace will record and transfer the asset. A regulatory body could additionally receive information of the transaction directly to hold a consolidated, centralized view, to foster risk management. **External Asset:** If the asset is not built into the blockchain, then the record of the transaction will still be recorded. However, the transfer agent mechanism will need to be determined. The counterparties may decide where appropriate to transfer assets on their own, meeting agreed standards, or an intermediary could fill that role[23].

DIMENSION	COMMENTS
Technology Governing Body	The need for standards and protection of the blockchain infrastructure may dictate the need for its own oversight. Just as the internet saw the formation of such consortiums like ARIN (American Registry for Internet Numbers), IETF (Internet Engineering Task Force) and ICANN (Internet Corporation for Assigned Names and Numbers), an independent group of experts could help ensure stability, continued open source nature, and agree wider standards or changes.
Regulatory Oversight	While regulation and ensuring lawful compliance will still be a core concern to any market, blockchain could change the nature of regulatory oversight. This is because regulators will have greater transparency through the public nature of nodes within the network. The transparency blockchain has the ability to provide gives regulators a much clearer picture of what is going on in the markets on a close-to-real-time basis.

As some of these intermediary functions illustrate, the marketplace itself will absorb some of the roles currently. This adds a new dynamic to the idea of a market itself as an avenue for value creation. “Activity around blockchain technology is creating energy for further improvements to the system. A common barrier cited for some innovations is how to agree on a lead provider to hold central responsibility and power in an essentially monopolistic position. Perhaps the only way for the industry as a whole to agree who should develop such solutions is if they all collectively develop and own it together as in the case of blockchain.”

An ability to unlock new business models also gives rise to the idea of a market on demand. As consumers have proven the value of the new shared economy model, an ability to build a market where trust, infrastructure costs and potentially geopolitical stability is not a roadblock means a big opportunity to design even more shared solutions. Markets could be thoughtfully designed with self-enforcing rules created through smart contracts, in areas where it wasn't possible before. One example would be to create a pool for individuals forced to self-insure. The question around markets may no longer be which market but rather what are the minimum viable characteristics for there to be a market.

Potential on-demand markets does not mean that traditional existing markets will have the same freedom to appear instantly. The minimum viable requirements for capital markets not only includes regulatory oversight but a significant pool of participants operating in the same space. Adam Ludwin at Chain estimates that despite many networks looking to launch, the lead institutions need others to join to stay viable. "I think there's a very real probability that only a handful of meaningful blockchain networks ultimately come to market and gain network effects, but that there are many, many participants on those networks."[24]

Massachusetts Institute of Technology

MIT Connection Science

REFERENCES

[1] Santander InnoVentures, Oliver Wyman, Anthemis Group (2015) "The Fintech 2.0 Paper: rebooting financial services"

[2] Stein, P (2015) "5 steps to closing the $2 trillion credit gap" World Economic Forum https://www.weforum.org/agenda/2015/10/5-steps-to-closing-the-2-trillion-credit-gap/

[3] The World Bank. Enterprise Surveys. (http://www.enterprisesurveys.org). 2010-2016.

[4] Love, Inessa, Sandeep Singh, and Maria Soledad Martínez Pería. "Collateral Registries for Movable Assets: Does Their Introduction Spur Firms' Access to Bank Finance?" January 2013. http://www.ifc.org/wps/wcm/connect/8891c280415edb709ba3bb9e78015671/Collateral+Registries+for+Movable+Assets++Does+Their+Introduction+Spu+Firms+Access+to+Bank+Finance.pdf?MOD=AJPERES.

[5] International Finance Corporation. Secured Transactions and Collateral Registries (http://www.ifc.org/wps/wcm/connect/793e79804ac10fff9ea69e4220e715ad/Secured+Transactions+and+Collateral+Registries+Brochure-English.pdf?MOD=AJPERES).

[6] Nash, Kim S. "Blockchain: Catalyst for Massive Change Across Industries." Wall Street Journal. February 2, 2016. http://blogs.wsj.com/cio/2016/02/02/blockchain-catalyst-for-massive-change-across-industries/.

[7] http://www.iacc.org/resources/about/statistics accessed 07 May 2016.

[8] Bloomberg News. "China Fake Invoice Evidence Mounts as HK Figures Diverge." Bloomberg. October 27, 2014. http://www.bloomberg.com/news/articles/2014-10-27/china-fake-invoice-evidence-mounts-as-hong-kong-figures-diverge.

[9] UK Government Chief Scientific Advisor. "Distributed Ledger Technology: beyond Blockchain." Government Office for Science. 2016

[10] "Collateral Management – Unlocking the Potential in Collateral." Accenture and Clearstream, 2011.

[11] Metz, Cade. "Coinbase Is Out to Build Payments Right Into Browsers." Wired. Nov. 13, 2015. http://www.wired.com/2015/11/coinbase-is-bringing-back-the-webs-long-lost-payment-code/

[12] W3C. "Common Markup for micropayment per-fee-links" Aug. 25, 1999. https://www.w3.org/TR/WD-Micropayment-Markup/#origin-goals

[13] Kaufman, Stacy, Ramani, Abhinav, Luciano, Dave, Zou, Long and Fosco, James. "Micropayments: A Viable Business Model?" Stanford University. June 2, 2011. http://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/MicropaymentsAndTheNet/index.html.

[14] Lebleu, G. "Building Gift Cards 2.0 on the Blockchain an overview." June 16th, 2015. https://medium.com/@giyom/building-gift-cards-2-0-on-the-block-chain-3ae9e7cf4152#.1zeoabmly.

[15] Oliver Wyman and Euroclear. "Blockchain in Capital Markets: the prize and the journey." Feb. 2016.

[16] Levine, Matt. "Banks Forgot Who Was Supposed to Own Dell Shares." Bloomberg View. Jul. 14th, 2015. http://www.bloombergview.com/articles/2015-07-14/banks-forgot-who-was-supposed-to-own-dell-shares.

[17] Vigna, Paul. "Nasdaq's Blockchain-Based Securities Platform Records First Transaction." Wall Street Journal. Dec 20th, 2015. http://blogs.wsj.com/moneybeat/2015/12/30/nasdaqs-blockchain-based-securities-platform-records-first-transaction/.

[18] "The Fintech 2.0 Paper: rebooting financial services." Santander InnoVentures, Oliver Wyman and Anthemis Group.

2016. http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf.

[19] DeRose, Chris. "Smart Contracts are the Future of Blockchain." Jan. 11th, 2016. http://www.paymentssource.com/news/paythink/smart-contracts-are-the-future-of-blockchain-3023206-1.html

[20] Schanz Kai-Uwe and Wang S, "The Global Insurance Protection Gap Assessment and Recommendations" (2014), The Geneva Association. https://www.genevaassociation.org/media/909569/ga2014-the_global_insurance_protection_gap.pdf

[21] http://blogs.wsj.com/cio/2016/02/02/blockchain-catalyst-for-massive-change-across-industries/

[22] Kentouris, C (2015) "US T+2 Settlement: The Long Journey Officially Begins" FinOps Report. http://finops.co/investments/us-t2-settlement-the-long-journey-officially-begins/

[23] CFTC. "CFTC Tackles the What Ifs of Blockchain."

[24] Shin L "How Will Bitcoin Technology Go Mainstream? An Analysis Of 5 Strategies" (2016) Forbes http://www.forbes.com/sites/laurashin/2016/01/26/how-will-bitcoin-technology-go-mainstream-an-analysis-of-5-strategies/#47767db63c31