COMMITTEE ON CAPITAL MARKETS REGULATION

Blockchain and Securities Clearing and Settlement

April 2019

COMMITTEE ON CAPITAL MARKETS REGULATION

Blockchain and Securities

Clearing and Settlement

April 2019

Table of Contents

Introduction

Blockchain technology – the technology underpinning Bitcoin and other cryptocurrencies – may have the potential to revolutionize several areas of our economic markets, including payment systems, banking, and real estate transactions, to name a few. For financial markets specifically, blockchain and distributed ledger technology or DLT (a more generalized version of blockchain) has recently been considered for use in securities clearing and settlement systems.[1] Stock exchanges in countries including Australia and Switzerland have announced plans to implement blockchain technology in securities trading over the next couple of years,[2] while other jurisdictions (e.g. Singapore and Canada) have also studied similar uses for blockchain.[3] Financial market participants have also begun experimenting with the use of blockchain in capital markets more generally, including the issuance of securities.[4] However, despite blockchain's potential, to date its practical use in these areas has yet to fully materialize[5] and it remains unclear whether blockchain can be useful in securities clearing and settlement. This brief report provides an overview of the relevant blockchain technologies and examines several of the issues that arise when attempting to integrate blockchain into clearing and settlement systems.

In improving securities clearing and settlement systems, several objectives must be considered, including settlement speeds, integration (i.e. delivery-versus-payment), security (e.g. resistance to hacking or other manipulations), operational resilience (i.e. avoiding operational failures), and mutability. At the same time, overall costs should always be factored as well, including the costs of designing, operating, and maintaining the system. It may be the case that blockchain technology proves to be useful in achieving the five primary objectives, but at such a high cost as to be much less efficient than alternative system designs.

[1] A recent report by IHS Markit estimates that if blockchain could eliminate all frictions in securities and clearing settlement, then securities market participants could save up to $12 billion in aggregate; *see* IHS Markit, *Blockchain in Finance Report*, 2019.

[2] *See Stock Exchanges Find Novel Uses for Blockchain*, The Economist, Nov. 15, 2018.

[3] *See MAS and SGX apply blockchain tech for settlement of tokenized assets*, Finextra, Nov. 12, 2018; *also see Bank of Canada, TMX say blockchain feasible for securities settlement,* Reuters, May 11, 2018.

[4] *See JPMorgan, National Bank of Canada, others test debt issuance on blockchain*, Reuters, Apr. 20, 2018.

[5] *See e.g.* J.P. Morgan Perspectives, *Blockchain and Cryptocurrencies 2019*, Jan. 24, 2019 at 6 (noting that "despite all the promises and potential of [distributed ledger technology] in making the world more efficient, its actual uptake has been quite limited…").

The specific design of the blockchain for use in clearing and settlement must also be carefully considered. The original value of blockchain for Bitcoin's purposes was to create a payment system that was completely decentralized, removing intermediaries entirely (such as financial institutions or central banks), while also eliminating any need for counterparties to trust each other. To achieve this, the Bitcoin blockchain sacrifices speed and efficiency in order to promote the security of the decentralized network. However, for blockchain to be useful in clearing and settlement, where speed and efficiency are paramount, modifications to the original Bitcoin blockchain must be made.

Part I of this report begins with a description of the relevant technologies, followed by a discussion of the security concerns associated with blockchain and an outline of alternative blockchain designs. Part II then discusses the specific application of blockchain technology to securities clearing and settlement, focusing on delivery versus payment objectives and concerns surrounding the immutability of blockchains. Part III then concludes with our general recommendation that further research into improving clearing and settlement systems not be focused exclusively on blockchain as part of the solution.

I. Distributed ledgers, blockchain and cryptocurrencies

(a) Descriptions of relevant technologies

Distributed ledgers and blockchain are distinct concepts. *Distributed ledger technology* refers to a database that is stored across multiple sites in a continuous record book, as opposed to a centralized database that is stored and maintained in a single location.[6] A main benefit of a distributed ledger is that the lack of a central entity mitigates the threat of a single point of failure. In addition, since no central entity can alter the ledger, the ledger is considered to be immutable.[7] The network of those holding copies of the ledger must agree through consensus (often a majority of nodes) to any changes or else the change is disregarded.[8] *Blockchain* is a subset of distributed ledger technology in which digital transactions are grouped and recorded on the shared ledger in "blocks," resulting in a ledger that consists of a complete history of transactions.[9] Importantly, blockchain uses cryptography to verify the identity of the parties to a transaction – through a *digital signature* – and to ensure that only valid transactions are written to the blockchain – through *cryptographic hash functions*.[10] Blockchains generally share certain characteristics, including: (i) encrypted data, (ii) encrypted access to data, (iii) distributed copies of the current state of the ledger with built-in redundancy, and (iv) an immutable log of transactions that is (effectively) impossible to alter.[11]

Cryptocurrencies are virtual currencies that are "created, stored and governed electronically by an open, decentralized, cryptography system,"[12] and reside on a blockchain. Bitcoin is the dominant cryptocurrency globally, constituting approximately 53% of the cryptocurrency market as of January 2019.[13] Bitcoin are created through a process known as *mining*, which is the act of grouping transactions into a block and adding the block to the

[6] Mark Walport, *Distributed Ledger Technology: beyond block chain*, A report by the UK Government Chief Scientific Adviser, Government Office for Science, December 2015.

[7] The definition of "immutable" can be debated, since technically a ledger can be altered by consensus. However, in discussions of blockchain and distributed ledger technology, this is considered immutability.

[8] In the case of the Bitcoin blockchain, a majority of the nodes must agree to changes.

[9] *See* Bank for International Settlements, *Distributed ledger technology in payment clearing and settlement: An analytical framework*, Feb. 2017, at 2.

[10] *See* Reade Ryan & Mayne Donohue, *Securities on Blockchain*, The Business Lawyer, Vol. 73, Winter 2017-2018 at 89-90.

[11] *See supra* n. 5 at 8-9.

[12] *See supra* n. 5 at 18.

[13] *See* CoinMarketCap, *Total Market Capitalization*, Global Charts https://coinmarketcap.com/charts/

blockchain.[14] The miner is rewarded with newly created units of the cryptocurrency upon successfully adding a block to the blockchain.[15] To add a block to the blockchain, the miner must first solve a computationally-intensive cryptographic puzzle. Computers, not humans, conduct the mining and verification of transactions and require an immense amount of energy to do so.[16] While the solution to the cryptographic puzzle serves no practical purpose in itself, the substantial resources required (i.e. energy and computing power) serve as a "proof-of-work" on the part of the miner. The *proof-of-work* is what ensures that only valid transactions are written to blockchain, thus establishing an impenetrably secure network. Mining is also the process used to transfer *existing* crypto units on the blockchain. Cryptocurrencies, therefore, can neither be double spent nor misappropriated from the blockchain, since every transfer of crypto units requires proof-of-work.

Proof-of-work secures the blockchain through the combination of the resource-intensive cryptographic puzzles and the economic incentives (i.e. the cryptocurrency reward for solving the puzzle) inherent in the blockchain structure. Since the blockchain is decentralized, the current "true" state of the ledger must be consistently agreed upon by the network participants (there is no single entity holding the "true" state). The process for ensuring agreement is known as a *consensus algorithm* or *consensus protocol*. When a miner adds a block to the blockchain, he initially is adding the block only to his own copy of the ledger. The rest of the nodes in the network will only adopt that updated version of the ledger (now including the miner's new block) if the block contains only valid transactions. If the block contains invalid transactions or if the miner has attempted to fraudulently alter a transaction, this will be easily identified by the network and the miner's updated version of the ledger, i.e. the new block, will be rejected. If the miner's block is rejected, he will not receive his cryptocurrency reward and all the resources expended to solve the cryptographic puzzle will have been wasted. Therefore, knowing that an invalid or fraudulent block will be rejected, it is unlikely that any miner will even attempt to fraudulently alter the

[14] *See supra* n. 5 at 18.

[15] In cases where the total supply of crypto units is capped, miners are rewarded with new crypto units only until the aggregate supply cap has been reached. For e.g., Bitcoin has a cap of 21 million bitcoin.

[16] *See Why Bitcoin Uses so Much Energy*, The Economist, Jul. 9, 2018 (noting that the computer power used to mine bitcoin is equivalent to the energy consumption of Ireland).

blockchain since it will only result in wasted computational resources, thus ensuring the security of the blockchain.

The proof-of-work concept in the Bitcoin blockchain is precisely what makes Bitcoin mining so resource intensive and what contributes to the relative slowness and inefficiency of Bitcoin transactions. Bitcoin can only process seven transactions per second, while VISA, for example, can process 24,000 transactions per second.[17] Other prominent cryptocurrencies offer slightly better transactions speeds – Ethereum handles 20 per second and Litecoin handles 56 per second – but are still relatively slow and inefficient.[18] However, while inefficient, proof-of-work is also what allows the blockchain to be decentralized and available for use by anyone, which was the primary goal for Bitcoin.[19] Some experts argue that it is the proof-of-work mining component of the Bitcoin blockchain that makes it so revolutionary.[20]

An alternative to the proof-of-work protocol that has been utilized by other cryptocurrencies is the *proof-of-stake* protocol. Whereas in the proof-of-work system the creator of a new block of transactions is whomever first solves a resource-intensive cryptographic puzzle, in the proof-of-stake system the creator of a new block of transactions is chosen by an algorithm based on the total wealth of each network participant, i.e. their stake.[21] The higher the stake, the greater the chance of being chosen as the creator of a new block and, thus, receiving a reward of newly created coins, similar to the reward in proof-of-work systems. However, unlike the proof-of-work protocol, proof-of-stake allows for validation of transactions without consuming the massive amounts of energy currently required through the proof-of-work process.

[17] *See Transaction Speeds: How Do Cryptocurrencies Stack Up to Visa or PayPal?* howmuch, Understanding Money, Jan. 10, 2018. https://howmuch.net/articles/crypto-transaction-speeds-compared
[18] Id. Note that Ripple can handle 1,500 transactions per second, but Ripple does not rely on blockchain and is not widely considered as a cryptocurrency.
[19] Other cryptocurrencies have attempted alternatives to proof-of-work, including proof-of-stake and proof-of-activity. *See* Amy Castor, *A (Short) Guide to Blockchain Consensus Protocols*, Mar. 4, 2017. https://www.coindesk.com/short-guide-blockchain-consensus-protocols/
[20] Arvind Narayan, *"Private blockchain" is just a confusing name for a shared database*, Sept. 18, 2015, https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/
[21] *See* Cryptocurrency Facts, *Proof of Stake (PoS)*, https://cryptocurrencyfacts.com/proof-of-stake-pos/.

Smart contracts are another important feature of blockchains that are not components of the Bitcoin blockchain.[22] Smart contracts are digital contracts written in code directly on the blockchain that automatically execute when the defined underlying terms are triggered.[23] The Ethereum network is the most prominent example of a blockchain design that supports the use of smart contracts.[24] For example, a smart contract could be coded to transfer cryptocurrency units between parties in the case that a stock price closes above a specified level on a given day. Smart contracts would be important components of a blockchain designed for securities clearing and settlement.

(b) Security on the blockchain

The combination of the distributed nature of DLT and the cryptographic encoding ensure the security of blockchains and their resistance to hacking. However, widespread concerns have arisen in the security of *cryptocurrencies*, which would potentially be indicative of broader security concerns about blockchains. Theft of cryptocurrencies were estimated at $1.1 billion stolen globally in the first half of 2018 alone.[25] However, the theft of cryptocurrencies is not the result of vulnerabilities of the blockchain technology *per se*, but rather is due to cybersecurity problems at third-party entities who hold cryptocurrencies on behalf of clients (e.g. cryptocurrency exchanges). For example, Bitcoin owners verify ownership on the Bitcoin blockchain by use of a private key that only they possess. Effectively, the private key is a 64-character password that must be used to access the Bitcoin. So long as the Bitcoin owner secures the private key, then the underlying Bitcoin can never be stolen. However, if the Bitcoin owner loses the private key, then those Bitcoin are lost forever. Moreover, if the Bitcoin owner stores the private key with an outside vendor (e.g. a broker), which is often done by individuals seeking to buy and sell Bitcoin for U.S. dollars or other real currencies, then the Bitcoins are only as secure as the outside vendor. If the

[22] Alternatively, some may consider Bitcoin transactions to be the simplest of smart contracts, albeit in a very limited context.

[23] K, Lucas, "What is Blockchain and Smart Contracts? Brief Introduction", *Medium*, May 31, 2017, Accessed 2/12/2018.

[24] Alyssa Hertig, *How Do Ethereum Smart Contracts Work?, Coindesk*. https://www.coindesk.com/information/ethereum-smart-contracts-work

[25] Kate Rooney, *$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do*, CNBC, Jun. 7, 2018.

vendor is hacked and the private key stolen, then the Bitcoin can be stolen as well. This is a security issue with the vendor, not the blockchain itself.

(c) The Bitcoin blockchain versus alternative blockchain designs

While the public openness of the Bitcoin blockchain was a key aspect of the design, abstractions from that original blockchain structure have led to a more generalized definition of blockchain that allows for both private blockchains and permissioned blockchains. The following are working definitions of these blockchain structures:[26]

(1) *Public blockchains* offer unrestricted access to view the blockchain and transact with others on the blockchain. Consent of the blockchain operator, if one exists for the particular blockchain, is unnecessary.

(2) *Private blockchains* restrict viewing access to a designated list of approved users. Transactions can only occur through interfaces offered by the operator.

(3) *Permissioned blockchains* limit the ability to add blocks to the blockchain to a set of known entities. The permissioned entities can control the access of end users.

(4) *Permissionless blockchains* do not restrict the set of entities that can add blocks. Any entity can add blocks to the blockchain and users can freely enter and exit the network.

The Bitcoin blockchain is a public, permissionless blockchain. Blockchain theists consider the public and permissionless characteristics to be defining features of any blockchain.[27] But this is not always the case. This is important when considering specific applications of blockchain technology beyond cryptocurrencies, such as in the context of securities clearing and settlement.

Private, permissioned blockchains offer many advantages as a blockchain design. For example, a private blockchain can vary the levels of access to network participants. Regulators and key financial institutions may have the highest level of access to the data, while network users and support service providers may only have access to lower levels of data. Permissions to write blocks to the blockchain can vary in similar manners, whereby a strict set of permissions may be necessary for high-value transactions conducted among a smaller group of financial institutions.

[26] As defined in J.P. Morgan Perspectives. *See supra* n. 5.

[27] Bailey Reutzel, *A Very Public Conflict Over Private Blockchains*, Payments Source, Jul. 13, 2015. https://www.paymentssource.com/news/a-very-public-conflict-over-private-blockchains

The result is a blockchain design that can both facilitate transactions by financial market participants, while also improving the efficiency of regulation.

II. Blockchain and securities clearing and settlement

Securities clearing and settlement systems in the United States are potential candidates for utilization of blockchain technology. While the current settlement system handles a large volume of activity – the two main actors, the Depository Trust Company and National Securities Clearing Corporation, process 300 million shares per second during peak trading[28] – settlement times can be improved. Currently, most transactions are required to settle within two days of the transaction date (T+2),[29] which is an improvement over the T+5 standard that was applicable until 1995[30] and the T+3 standard that applied from 1995 to 2017.[31] However, even with the recent improvement, the DTCC estimates that the relatively lengthy settlement period forces system participants to hold over $5 billion collectively, on average, in risk margin to manage counterparty default risk.[32] If a clearing and settlement system using blockchain can be designed to allow for real-time settlement, then settlement speeds can be greatly improved, thus reducing counterparty risk, freeing up capital and making the financial system more dynamic, more automated and more resilient. Blockchain and DLT can also improve the transparency and verification of asset ownership, while also reducing operational costs of a trade, particularly in cross-border transactions.[33] The distributed nature of DLT also mitigates the single-point-of-failure problems of more centralized systems. Since copies of the ledger are distributed among network participants, the failure of any one entity will not disrupt the rest of the system, unlike in centralized systems that must rely on back-up systems in the case of failure (which are themselves always at risk of failure).

In considering the application of blockchain to securities clearing and settlement, it is important to recognize that the purpose of a securities settlement blockchain differs significantly from the purpose of the original Bitcoin blockchain design. The primary goal of the original Bitcoin blockchain was not to improve the speed and efficiency of transactions, but rather to create

[28] *Modernizing the US Equity Markets Post-Trade Infrastructure* A White Paper to the Industry, DTCC, Jan. 2018. http://www.dtcc.com/news/2018/march/14/creating-an-alternate-settlement-model-with-settlement-optimization
[29] Legal Information Institute [LII], *17 CFR 240.15c6-1 – Settlement cycle.*, Cornell Law School.
[30] Federal Register, *17 CFR 202, 228, 229, 230, 232, 239, 240, 270, and 274,* Vol. 60, No. 95, May 17, 1995, at 26604.
[31] Federal Register, *17 CFR Part 240 Securities Transaction Settlement Cycle,* Vol 82, No 59, Mar. 29, 2017, at 15564.
[32] *See supra* n. 28.
[33] *See* Report from MAS, SGX, Anquan Capital, Deloitte and Nasdaq, *Delivery versus Payment on Distributed Ledger Technologies*.

a payment system that was completely decentralized, removing intermediaries entirely (such as financial institutions or central banks), while also eliminating any need for counterparties to trust each other. To achieve this, the Bitcoin blockchain imposed features that sacrifice speed and efficiency in order to promote the security of the decentralized network.

The primary objectives in applying blockchain to securities clearing and settlement are not the removal of trusted intermediaries (such as a central counterparty) for the sake of removing the intermediary, but rather, to speed up and improve the efficiency of the settlement process.[34] If transacting through a trusted intermediary were the fastest and safest means of settling securities transactions, there would be no need to employ blockchain technology. However, to the extent that intermediaries slow down or pose risk to the settlement process, there is a role for blockchain's ability to decentralize the process. In that pursuit, a private permissioned blockchain would be the optimal design for a securities blockchain, which strikes the appropriate balance between the benefits provided by the distributed nature of the blockchain, while also ensuring that transactions are added to the blockchain by known, entrusted entities. The permissioned nature of the blockchain allow transactions to be validated without the need for proof-of-work or any other inefficient consensus protocol. This would enable the blockchain to handle the high volumes of transactions inherent in securities markets, as illustrated in a recent study by the DTCC.[35] However, even with a private permissioned blockchain, two key challenges arise that must be considered when applying blockchain technology to clearing and settlement: (i) delivery versus payment and (ii) immutability.

(a) Delivery versus Payment

Delivery versus payment (DvP) is a settlement procedure in securities transactions whereby the buyer must make payment for the securities at the time that securities are delivered from the seller. Settlement systems that rely on DvP link the transfer of assets and cash (or two assets) in a manner that ensures that one side of the transaction executes only if the other side executes

[34] For example, one factor that could improve the speed and efficiency of the settlement process is the shared nature of the distributed ledger, which could reduce or eliminate entirely reconciliation and confirmation inefficiencies.

[35] *See DTCC Announces Study Results Demonstrating that DLT Can Support Trading Volumes in the US Equity Markets,* DTCC Press Release, Oct. 16, 2018.

simultaneously.[36] DvP on a blockchain presents a challenge: how can securities be transferred on a blockchain, while ensuring that cash payments are made simultaneously? In order for the securities leg of a transaction to be validated by the network, confirmation of the cash leg of the transaction must also be verified. However, if the cash transfer were to occur off the blockchain, then settlement may be delayed as the cash leg is verified, thus slowing down transaction speeds and reducing efficiency. Therefore, the cash leg of a securities transaction must also be represented on the blockchain, in addition to the securities leg of the transaction, to solve the DvP issue.[37]

Digitalization and tokenization of the currency, such as through the use of *stablecoin*, can help solve the DvP issue by allowing the currency and the security to be represented on the blockchain. *Stablecoin* are a variant of cryptocurrencies in which the digital currency is collateralized by other assets, such as U.S. dollars.[38] For example, recently two stablecoins collateralized by the U.S. dollar (i.e. can be redeemed one-for-one for U.S. dollars) have been approved by the state of New York - the Paxos Standard and Gemini Dollar,[39] while JP Morgan has also introduced a stablecoin, JPM Coin, pegged to the U.S. dollar.[40] With both the security and currency represented on the same blockchain system, transactions on the blockchain can account for both simultaneously. The transaction written into the block will consist of the security being transferred from A to B and the stablecoin (or other digital currency) being transferred from B to A. Since the transaction consists of both transfers, either both transfers are added to the blockchain or neither of them are. The cash leg of the securities transaction would not delay the settlement of the securities leg in this case, which would be the case if the currency were not tokenized. As a result, securities transactions on the blockchain could be settled continuously in real-time, rather than T+2.[41] However, settlement would occur in stablecoin, rather than U.S. dollars, potentially

[36] European Central Bank & Bank of Japan, *Securities settlement systems: delivery-versus-payment in a distributed ledger environment*, Mar. 2018.

[37] *See* Andrea Pinna & Weibe Ruttenberg, *Distributed Ledger Technologies in Securities Post-Trading: Revolution or evolution?* European Central Bank Occasional Paper Series, no 172, April 2016.

[38] CB Insights, *What Are Stablecoins?*, https://www.cbinsights.com/research/report/what-are-stablecoins/?

[39] Id.

[40] *J.P. Morgan Creates Digital Coin for Payments*, https://www.jpmorgan.com/global/news/digital-coin-payments.

[41] The cash leg of the securities transaction does raise potential issues under securities laws if the transaction entails tokenized or digital currency. A question arises as to the legal standing of the tokenized currency (i.e. do securities laws treat it as cash or as a security itself?).

introducing delays and counterparty risk during the redemption process (i.e. redeeming stablecoin for dollars). For example, Paxos does not offer instantaneous redemption, promising redemption within one business day.[42] However, the dollars that collateralize the Paxos stablecoin are held in custody by FDIC-insured institutions, thus reducing counterparty risk during the redemption process.[43]

Smart contracts can be employed to facilitate the DvP, while also ensuring that any other necessary pre-conditions for the trade are met.[44] The use of smart contracts to automate the DvP settlement process has been successfully demonstrated in a joint project by the Monetary Authority of Singapore and the Singapore Exchange, which developed technology to carry out the exchange of securities and tokenized currency simultaneously using blockchains.[45] In this project, automated DvP was successfully achieved in the trading of Singapore government securities (the security leg) for central bank-issued cash-depository receipts or CDR (the cash leg), each of which were represented on separate distributed ledgers.[46] The CDR is a tokenized form of the Singapore Dollar issued by the Singapore Monetary Authority in which "participant banks pledge cash into a custody account held at the central bank" in return for a CDR represented on a distributed ledger.[47]

The most appropriate blockchain design for securities clearing and settlement would entail a private permissioned blockchain with the permissioned parties (nodes) consisting of a known consortium of financial institutions. These institutions, tasked with validating the securities transactions, would be highly motivated to ensure that the integrity of the blockchain is not compromised. Therefore, whereas a permissionless blockchain (such as Bitcoin) requires proof-of-work (or alternative protocol) to ensure that only valid transactions are added to the blockchain, the permissioned blockchain can rely solely on the motivations of the permissioned nodes to add only valid transactions. Otherwise, financial market participants would be reluctant to transact on

[42] *See* Paxos Standard, *Transact at the Speed of the Internet*, https://www.paxos.com/standard/ (last accessed 2/15/19).

[43] *See* Chad Cascarilla, I*ntroduciung Paxos Standard (PAX), the new digital dollar*, Paxos, News and Blogs, Sep. 10, 2018. https://www.paxos.com/repository/introducing-paxos-standard-pax-the-new-digital-dollar-2/ (last accessed 2/15/19).

[44] In addition to DvP, smart contracts can also be used to handle other aspects of securities ownership, including dividend distribution, proxy voting, and interest payments.

[45] *See supra* n. 3.

[46] *See supra* n. 33.

[47] Id at 11.

the securities blockchain. In addition, reputational concerns for each individual institution and the threat of legal liability would also ensure that only valid transactions are verified and manipulation of the blockchain is avoided. Members of the permissioned network can also engage in a degree of self-regulation by disciplining any bad actors, potentially by revoking permission to the network.

The European Central Bank and the Bank of Japan recently engaged in joint research studying the feasibility of DvP on distributed ledgers, exploring "how the settlement of two linked obligations, such as the delivery of securities against the payment of cash, could be conceptually designed and operated in an environment based on [distributed ledger technology]."[48] The joint project concluded that DvP could indeed be achieved on a distributed ledger through multiple implementation designs. The securities blockchain could host cash and securities together on the same ledger (i.e. a single-ledger DvP) or it could host cash and securities each on separate ledgers (i.e. a cross-ledger DvP).[49] The report notes that the single-ledger DvP concept is similar to "the 'integrated model' in existing securities settlement mechanism (such as TARGET2-Securities and BOJ-Net JGB Services…) in which securities and cash are processed on a single integrated platform."[50] Such a system for government securities also exists in the United States, the book-entry program, as provided through the Federal Reserve, the U.S. Treasury and other federal agencies.[51] The cross-ledger DvP concept is similar to "the 'interfaced model' in existing securities settlement systems in which securities and cash are settled on two difference systems and the two systems coordinate to facilitate DvP by blocking assets (such as the DvP link between BOJ-NET Funds Transfer Service and Japan Securities Depository Center…)."[52] Applying blockchain to settlement of *private* securities can therefore be achieved through the ECB-BOJ design, but with private control of the settlement system (as opposed to a government-run system). The digitization

[48] *See supra* n. 36.

[49]*Id.*

[50] *Id* at 5.

[51] Federal Reserve Bank of New York, *Book-Entry Procedure*. https://www.newyorkfed.org/aboutthefed/fedpoint/fed05.html

[52] *See* ECB and BoJ, *supra* note 33 at 5. The report further explains that in this model the "securities settlement system first blocks the securities to be delivered by either earmarking balances or transferring the securities to an escrow account. Based on the confirmation from the securities settlement system, the payment system processes the transfer of cash and informs the securities settlement system to release the securities. After receiving this confirmation from the payment system, the securities settlement system releases the block and processes the transfer of securities..." at 5.

of central bank-issued cash, as is being explored by a consortium of the largest banks in the world through the Utility Settlement Coin project, could also prove useful in such a system.[53] Such tokenization of central bank cash could facilitate cross border transactions.

In the context of payment systems, however, the ECB has concluded that blockchain is not necessary for real-time settlement of payments, evidenced by its upcoming implementation of the TARGET instant payment settlement (TIPS) service that will allow for real-time settlement of payments without relying on blockchain technology.[54] While the TIPS service is not contemplated for use in securities clearing and settlement, TIPS will "offer final and irrevocable settlement for instant payments in central bank money on a 24/7/365 basis."[55] Unlike settlement on a blockchain, TIPS will be a centralized system for payments settlement, not relying on distributed ledger technology. While payment systems and clearing and settlement systems are fundamentally different and should not be directly compared, the ECB's approach is instructive in as much as it highlights the central bank's general view that blockchain is not necessarily the best technology for making significant improvements to financial systems.

Based on the projected transactions speeds and costs, an ECB executive board member has suggested that the TIPS system is superior to blockchain technology, offering faster transaction speeds at lower costs.[56] However, blockchain proponents contend that while the TIPS system may offer improved speeds over the old payments system, it does not provide the same level of security as distributed ledger technology.[57] Since the TIPS system is centralized, it inherently has a single point of failure, making the system more vulnerable than decentralized blockchain systems in this respect.[58] Going forward, the goal for improved blockchain technology is to offer both speed *and*

[53] *See Why ICAP Believes Central Banks Could Adopt Digital Currency*, https://www.coindesk.com/icap-leads-the-way-for-central-bank-adoption-of-a-new-digital-currency.

[54] *See ECB finalizes pricing for settlement of instant payments*" Finextra, Aug. 6, 2018. https://www.finextra.com/pressarticle/74982/ecb-finalises-pricing-for-settlement-of-instant-payments

[55] European Central Bank, *The new TARGET instant payment settlement (TIPS) service*, June 2017.

[56] Carolynn Look & Piotr Skolimowski, *ECB's Mersch Says His Payment System Is Better Than Blockchain*, Bloomberg, Feb. 8, 2018.

[57] Simon Chandler, *No, Yves Mersch, the ECB's System is Not 'Better' than the Blockchain*, Cryptonews, Feb. 12, 2018,https://cryptonews.com/exclusives/no-yves-mersch-the-ecb-s-system-is-not-better-than-the-block-1195.htm.

[58] Id.

security concurrently, without sacrificing one for the other. While such as system does not exist, blockchain optimists foresee its development in the next couple of years.[59]

The Bank of Canada along with the Toronto Stock Exchange also recently tested a securities settlement platform based on blockchain technology that allows for instantaneous securities settlement through tokenization of both the currency and the security.[60] However, a Bank of Canada official noted that it was not certain that the use of blockchain would reduce costs and, moreover, it is "not clear that all the participant dealers and banks are going to get a significant benefit out of this settlement system."[61] Therefore, while blockchain technology may be feasible for use in securities clearing and settlement, it is not necessarily efficient.

(b) Immutability

Another fundamental challenge that arises with the application of blockchain technology to securities transactions is how to deal with the immutability of blockchain records. It is effectively impossible to void or reverse a transaction on the Bitcoin blockchain without mutual agreement by both transacting parties.[62] However, this extreme degree of immutability is not necessarily desired in the context of securities transactions.[63] The need to reverse or void securities transactions is most prominently evident in the "clearly erroneous" rule, whereby a trade is voided due to an obvious error in price, number of shares, or identification of the security.[64] The need for reversing clearly erroneous trades became even more apparent following the 2010 flash crash.

The concern about the immutability for securities transactions can be mitigated through a permissioned blockchain structure in which the trusted permissioned nodes can be tasked with voiding or reversing trades under clearly defined rules. Other circumstances that would necessitate a revision to the blockchain can also be achieved in a similar manner, either by prescribed rules or through consensus among the permissioned nodes. Reputational concerns and legal liability can

[59] Id.

[60] *See Bank of Canada, TMX say blockchain feasible for securities settlement,* Reuters, May 11, 2018.

[61] Id.

[62] A transaction can be reversed by both parties agreeing to enter into a new transaction that effectively reverses the original transaction.

[63] Immutability is desirable, however, in the context of blockchain providing an immutable audit trail of transactions, including voided transactions.

[64] *See Clearly Erroneous Transactions Policy*,,NASDAQ. https://www.nasdaqtrader.com/Trader.aspx?id=ClearlyErroneous

again serve to discipline the permissioned entities to enforce the rules appropriately. To the extent that prescribed rules are employed, the blockchain design can use smart contracts to carry out any necessary revisions to a trade. In the case of clearly erroneous trades, the conditions for voiding the transaction can be written into smart contracts, which will automatically reverse any trades if necessary or simply reject the trade as invalid without ever executing it.

Whether private permissioned nodes or smart contracts (or a combination of the two) are used in the blockchain design, the immutability of blockchain is not an insurmountable hurdle in the context of securities settlement. The process by which transactions can be revised by the permissioned nodes must be carefully considered, however. Some financial market participants may prefer a relatively more immutable blockchain, giving transacting parties more certainty that a validated trade is permanent. While others may prefer more leeway for subsequent revisions. Striking the appropriate balance on the immutability issue is a key concern for an effective clearing and settlement system.

III. Conclusion

Blockchain technology has been touted for its potential to revolutionize many aspects of financial markets, including securities clearing and settlement systems. But the optimal blockchain design for securities transactions differs significantly from the original blockchain designed for Bitcoin and other cryptocurrencies. While Bitcoin's blockchain intentionally introduces speed bumps to ensure the security of its ledger, such features are not necessarily appropriate for securities settlement, where real-time settlement of transactions is the ultimate goal. The joint study by the ECB and Bank of Japan serves as a roadmap in this respect, illustrating how delivery versus payment can be achieved on a distributed ledger. But the realization of blockchain's potential for optimizing both speed *and* security of securities transactions at low cost remains unclear. The Committee on Capital Markets Regulation is encouraged by the general focus on improving clearing and settlement systems, but believes the question remains open as to whether blockchain technology provides the best framework for doing so. We strongly recommend that securities regulators and policymakers collaborate with market participants (broker-dealers, exchanges, and clearinghouses) and continue to push the research forward in how to improve the existing securities clearing and settlement system, considering blockchain but also recognizing that blockchain technology may not be necessary to do so.

COMMITTEE ON CAPITAL MARKETS REGULATION

134 Mount Auburn Street, Cambridge, MA 02138
www.capmktsreg.org