Ferdinando M. Ametrano (ferdinando@ametrano.net)
Emilio Barucci (emilio.barucci@polimi.it)
Daniele Marazzina (daniele.marazzina@polimi.it)
Stefano Zanero (stefano.zanero@polimi.it)
Politecnico di Milano
Piazza Leonardo da Vinci, 32
20133 Milano – Italy

European Securities and Markets Authority
103 rue de Grenelle
75007 Paris
France

September 2, 2016

Response[1] to ESMA/2016/773[2]
The Distributed Ledger Technology Applied to Securities Markets

Distributed Ledger Technology (DLT) is in a very early stage of development. Sometimes confused with the blockchain technology underlying bitcoin, it is supposed to be its evolution designed to avoid the architectural choices that make bitcoin and blockchain unsuitable for securities settlement [1] and financial applications [2]. DLT is enjoying the blockchain hype originating from the resiliency of bitcoin operations, but it still lacks a reference implementation or strict technical specifications, beyond being a shared ledger using cryptographic tools (e.g. Corda [3, 4]). As such, it is difficult to discuss its promises and limitations. Nonetheless, some considerations are possible starting from the existing market infrastructure, the experience with operational blockchains, and the available elements of the public debate about DLT.

For a broader context supporting the following answers, the reader is referred to Ametrano [5], Ammous [6], and Mainelli and Milne [7].

[1] This document is available at https://drive.google.com/drive/folders/0B8tGDTaBY4-Nb3ZuRmgzRXJXOUk. The official response is available, among others, at https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets. This version just avoids ESMA format for a more readable one.

[2] The public consultation page is at https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies, with the discussion paper being https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf.

Q1: Do you agree with the list of possible benefits of the DLT for securities markets? Please explain, e.g., are these benefits unique to the DLT, are some more important than others, are some irrelevant?

Most of the benefits associated to the DLT are not really peculiar to this technology.

Instant clearing and settlement is probably the most appealing promise of DLT: however, in the current infrastructure allowing nanosecond financial transactions, this feature is not blocked by technological limitations. Instant clearing and settlement is hard to obtain mainly because of the "consensus by reconciliation" process that financial markets have elected as their "checks and balances" system: the independent reconciliation of multiple self-reliant ledgers allows for all the prescriptions, corrections, and restrictions required by the regulatory framework. In order to shorten the time span of the compliance processes, progress could be obtained augmenting the existing database technology and automation practices with cryptographic tools. Anyway, so far the analysis of the regulatory and operational feasibility of alternatives to "consensus by reconciliation" has been neglected. The only widely accepted opinion is that any forms of alternative "*decentralized* consensus" must provide a recourse mechanism and rules subject to the review, management, and approval of some intrinsically *centralized* higher court: an oxymoron which does not exist yet.

For instant clearing and settlement of spot transactions it would be crucial the existence of cash on the ledger to implement effective "Delivery versus Payment". Such a facility is not available yet, and it is absent from the agenda of prominent players promising DLT solutions. Notice that providing access to central bank money on a ledger might be distressing for the retail banking system: as pointed out by Mark Carney, Governor of the Bank of England, "*it would mean people have direct access to the ultimate risk-free asset. In its extreme form, it could fundamentally and perhaps abruptly re-shape banking. However, were it to co-exist with the current banking model, it could exacerbate liquidity risk by lowering the frictions involved in running to central bank money*" [8]. In other words, everybody would prefer to own central bank instead of commercial bank money. As far as cash on a ledger is concerned, it will be interesting to follow the diffusion of the Ripple protocol, the development of the Utility Settlement Coin proposed by Clearmatics and its five-member consortium (UBS, BNY Mellon, Deutsche Bank, ICAP, and Santander) [9] and the possibly related evolution of the SETLcoin, the "Cryptographic Currency For Securities Settlement" patent filed by Goldman Sachs [10].

In case of derivative transactions with maturity beyond the spot date, there are difficulties that make the application of DLT implausible; therefore, the claimed efficiency in collateral management and reduction of counterparty risk are not realistic. The collateral amount is correlated to the risk of the outstanding portfolio between two counterparties, generally proportional to the portfolio sensitivities. This risk calculation is computationally intensive: in a DLT environment it is not clear which agent would perform it, and its economic incentive. Additionally, different counterparties often disagree on the models to be used for such computations. How to automate the payment of variation margins should be specified with a programmatic access to payment funds, which entails a huge operational risk. Last but not least, whatever automation is evoked for frequent payment of variation margins, the default of counterparty would leave the other party exposed to the market risks usually covered by initial margin: i.e. initial margin would still be required. Even automated prompt detection of the default would not help significantly in reducing the initial margin amount, as it is basically tied to the time required to find a new counterparty replacing the defaulted one. Operational glitches in automated payments would even trigger automated defaults, being a huge operational risk.

As far as the availability, security, and resilience of the trading environment is concerned, notice that the conditions have improved in recent years through execution facilities, central clearing counterparties and a push toward the collateralization and margining of bilateral (non-centrally cleared) transactions. Instead, it is not clear how availability, security and resilience can be granted by private distributed ledgers that cannot pay the cost for reaching consensus with seigniorage revenues, as it happens in the case of bitcoin's blockchain. The mirage of low operational costs derives from the false impression of free blockchain transactions: if one takes into account the seigniorage revenues invested, each transaction on the bitcoin blockchain has a cost of about 5-10USD. Cheaper forms of consensus have not been proven yet, and even if one can imagine resorting to basic bilateral consensus through digital signatures (something hardly innovative or disruptive…) the integration cost in the existing infrastructure is not going to be irrelevant. Moreover, if trading is suspended overnight, this is an operational safety choice, not a technological constraint to be solved with DLT; on the contrary, it should be proved how to enforce closing time for DLT operations with clear cut-off times.

Reporting and oversight, which should be easy because of the blockchain transparency, become cumbersome again once it is accepted that DLT must grant privacy, providing access only to relevant parties; even if auditors and regulators were granted access to the data, the burden of generating reports would be shifted to them, something they might not be keen about.

Other benefits, such as pre-trade information, matching of buyers and sellers, etc. have not been presented as key DLT features so far; in addition, in some trading environments the service of human brokers is considered flexible and efficient to the point of not pursuing possible automated alternatives.

"*Current interest in mutual distributed ledgers has established significant momentum, but there is a danger of building unrealistic expectations […] achieving all the potential benefits from mutual distributed ledgers will require board level buy-in to a substantial commitment of time and resource, and active regulatory support for process reform, with relatively little short term pay-off*" [7].

Q2: Do you see any other potential benefits of the DLT for securities markets? If yes, please explain.

Notarization services are a very promising blockchain application [11]: the bitcoin blockchain (the most secure one, since the effort/cost for its manipulation is prohibitive) can be used for the trustless time-stamping of documents and the anchoring of arbitrarily large data set. A generic data file can be hashed to producing a short unique identifier, equivalent to its digital fingerprint. Such a fingerprint can be associated to a bitcoin transaction, the bitcoin amount being irrelevant, and hence registered on the blockchain: the blockchain immutability then provides robust non-repudiable time-stamping that can always prove without doubt the existence of that data file in that specific status at that precise moment in time. This generic process is even undergoing some standardization to achieve third party auditable verification [12]. Broker-dealers could use it to satisfy the regulatory prescriptions [13] for storing required records exclusively in non-rewriteable and non-erasable electronic storage media. WORM (write once read many) optical media has been used so far, but it is quite impractical, especially for large data set; instead, compliance could be easily achieved anchoring rewritable data sources to the blockchain, providing accurate and secure time-stamping resilient to manipulation.

In general, applications based on cryptographic proofs and digital IDs are promising, even if there is no explicit evidence of relevant use cases for the securities markets so far. Moreover, such applications often use only the cryptographic tools popularized by bitcoin, not really requiring a blockchain or a DLT at all.

Q3: How would the benefits of the technology be affected, in the case where the DLT is not applied across the entire lifecycle of securities (i.e., issuance, trading, clearing and settlement, safekeeping of assets and record of ownership) but rather to some activities only?

The incremental adoption of DLT, often suggested to ease integration while speeding up its adoption, would be problematic: if not applied across the entire lifecycle of securities, then DLT would just become another silo which needs to be integrated in an increasingly heterogeneous stack of technologies, with relevant costs and operational risks.

Q4: Which activities (e.g., post-trading, other activities), market segments and types of assets in the securities markets are likely to be impacted the most by the DLT in your opinion? How is the DLT likely to modify the way securities markets operate? Please explain.

Even assuming that the key challenges and main risks discussed later can be solved, we have very limited evidence of activities, market segments and types of assets in the securities markets that are likely to be significantly impacted by the DLT. The less unlikely candidates would be simple fungible assets in spot transactions. What blockchain technology is really suited for are cash-like fungible bearer assets like bitcoin.

Q5: According to which timeframe, is the DLT likely to be applied to securities markets in your view? Please distinguish by type of activities, market segments and assets if relevant.

No reference implementation of DLT has emerged yet, and there is no complete technical description of its underlying assumptions. As such, it is difficult to provide an informed opinion.

Q8: Do you agree with the analysis of the potential challenges? Please explain, e.g., are some more important than others, are some irrelevant in your view.

The ESMA listing of key challenges for DLT is very thorough: unproven ability to operate on a large scale, the need to achieve interoperability between different ledgers and with legacy systems, the need to settle in central bank money, the lack of a recourse mechanism, the inability to efficiently net derivative transactions, the impossibility of short-selling and the difficulty of margin finance, the unspecified governance process for permissioned network nodes, the lack of privacy and anonymity, the uncertainty of legality and enforceability of DLT records.

Another main challenge is the type of consensus processes that would be adopted by DLT, bitcoin's proof-of-work being very costly and basically rejected by all promised DLT solutions. How to reach consensus in a distributed network is a very complex computer science problem: progress beyond proof-of-work has been scarce; shortcuts to forms of bilateral consensus would easily negate the distributed nature of a ledger.

Lack of a reliable consensus algorithm and of central bank money are the most relevant challenges, followed by inability to efficiently net, unspecified governance process and recourse mechanism, and interoperability.

The inability to fit into existing regulatory framework does not appear to be a crucial challenge: public permissionless blockchains are not aiming for that, private permissioned DLTs are supposedly being built from the ground up according to regulatory compliance guidelines. See also our answer to Q24.

Q10: Which solutions do you envisage for these challenges and where do the current initiatives stand in terms of practical achievements to overcome them?

No easy or clear solutions have been proposed so far, and for the major problems listed above some DLT proponents make a point of not tackling them at all. If major DLT players will submit their answers to ESMA, it will be interesting to analyse their suggestions about how to deal with these challenges.

Q11: Do you agree with the analysis of the key risks? Please explain, e.g., are some risks more important than others, are some irrelevant in your view.

Cybersecurity risk is the most relevant. In the current market infrastructure (e.g. stock exchanges) governance and operations are usually centralized, but all players keep their own self-reliant ledger for tracking transactions; in the bitcoin network governance and operations are decentralized, all nodes being equal (besides their characterization as mining or non-mining), with one single authoritative ledger massively duplicated among network nodes. In the current financial markets a cyber-attack to the central governance and operations can disrupt the ability to transact, but the independence of multiple ledgers preserves the ability to restore the network status. In the case of bitcoin's blockchain, the distributed nature of its operations makes it harder for a cyber-attacker to halt the network transaction ability, but the single authoritative ledger is a potential weak point, defended by the fact that proof-of-work implies huge costs for an attacker. In the case of DLT, there is the risk of combining together the worst of the two scenarios: the central governance necessary for accountability and recourse system could be attacked, and the single authoritative ledger could be hacked, with any appeal to alternative independent data source being invalid for the agreed protocol.

In the case of bitcoin, if fraudulent transactions are technically valid, they are technically irreversible, as expected because of bitcoin being a bearer asset. There are no attempts to solve this problem, which is intrinsic for bearer instruments even in the physical world. When it comes to registered assets the use of cryptographic tools like private keys is problematic, and so far nobody has proposed a robust governance framework able to revert fraudulent technically valid transactions. Fraudulent transactions of this sort have plagued home banking systems for years [14] and have recently become an issue for backbone services such as SWIFT [15].

Automation is an incremental innovation driver which can reduce the likelihood of human errors. But taken to extreme disruptive limits, as it might happen in the so-called code-is-law smart-contract approach, it can trigger new error classes of potentially humongous consequences. The reader is referred to the Ethereum TheDAO incident [16]: an unknown attacker drained about $60m worth of the digital currency ether from TheDAO's $150m pool, just exploiting a flaw (undocumented feature?) in TheDAO's smart contract. Subsequent attempts to fix the incident failed and required the last-resort measure of rewriting the blockchain transaction history; the betrayal of blockchain immutability and code-is-law paradigm resulted in network-wide controversies and overall confusion: in the end, ether has forked in two independent distinct instances. Since even this sub-optimal solution would be unfeasible for registered assets, the operational risks of smart-contracts should not be underestimated.

Instead, volatility risk should not increase significantly because of technological choices. Volatility is the measure of the intrinsic uncertainty associated to the expected future value of an asset: if nanosecond algorithmic trading is considered a legitimate practice, DLT is not expected to pose peculiar new challenges.

Finally, fair competition and orderly markets do not seem to be too problematic in a financial regulated environment.

Q13: How could these risks be addressed? Please explain by providing concrete examples, especially for the risks potentially affecting your organisation.

Even assuming that the introduction of these risks would be compensated by relevant benefits, in the absence of a reference implementation or clear technical specifications it is very hard to provide suggestions to mitigate risks. One might be tempted to just define DLT a chimera, or at least something unfit for financial markets in the near future. Again, it would be interesting to read the suggestions coming from the DLT proponents.

Q14-Q21 […]

In the absence of a DLT reference implementation and/or of clear technical specifications, it is difficult to provide an informed opinion.

Q22: Do you think that the DLT could be used for other securities-related services than those already discussed, in particular trading and issuance?

See our answer to Q2 about notarization services.

Q23: Do you see potential regulatory impediments to the deployment of the DLT in securities markets?

No real impediments for the security markets. Anyway, the suggestion from EBA to national supervisory authorities on discouraging "*credit institutions, payment institutions and e-money institutions from buying, holding or selling VCs*" [17] might hamper the possible use of VCs as a form of cash-on-ledger for the cash leg of a security transaction.

Q24: Should regulators react to the deployment of the DLT in securities markets and if yes how? If you think they should not do so please justify your answer.

In the case of a real DLT application, regulators should examine it under the light of the existing regulatory framework. To regulate in advance on the basis of vague ephemeral discussions about DLT would be problematic and might stifle innovation. Notice that the necessity for ad-hoc regulation is not evident yet, and there has not been a motivated explicit request for it.

Bibliography

[1] Sams, Robert, “No, Bitcoin is not the future of securities settlement” (May 18, 2015). Available at http://www.clearmatics.com/2015/05/no-bitcoin-is-not-the-future-of-securities-settlement/

[2] Walch, Angela, “The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk” (March 16, 2015). 18 NYU Journal of Legislation and Public Policy 837 (2015). Available at SSRN: http://ssrn.com/abstract=2579482

[3] Gendal Brown, Richard, “Introducing R3 CORDA™: a distributed ledger designed for financial services” (April 5, 2016). Available at https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/

[4] Gendal Brown, Richard and Carlyle, James and Gregg, Ian and Hearn, Mike, “Corda: An Introduction” (August 2016). Available at http://r3cev.com/s/corda-introductory-whitepaper-final.pdf

[5] Ametrano, Ferdinando M., “Bitcoin, Blockchain, and Distributed Ledger Technology” (2016). Available at SSRN: http://ssrn.com/abstract=2832249

[6] Ammous, Saifedean, “Blockchain Technology: What is it good for?” (August 8, 2016). Available at the Columbia Center on Capitalism and Society: http://capitalism.columbia.edu/files/ccs/workingpage/2016/ammous_blockchain_technology_.pdf

[7] Mainelli, Michael and Milne, Alistair, “The Impact and Potential of Blockchain on Securities Transaction Lifecycle” (May 9, 2016). SWIFT Institute Working Paper No. 2015-007. Available at SSRN: http://ssrn.com/abstract=2777404

[8] Carney, Mark, “Enabling the FinTech transformation: Revolution, Restoration, or Reformation?” (June 16, 2016). Available at http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf

[9] “Settlement Coin Creators Seek to 'Liberalize' Central Banks With Blockchain”, Coindesk (August 24, 2016). http://www.coindesk.com/ubs-clearmatics-bny-icap-deutsche-liberalize-central-banks-settlement-coin/

[10] “Goldman Sachs Seeking Crypto Trade Settlement Patent”, Coindesk (December 1, 2015). http://www.coindesk.com/goldman-sachs-crypto-patent/

[11] https://eternitywall.it/notarize, https://stampery.com/, https://tierion.com/

[12] http://blog.eternitywall.it/2016/06/24/announcing-opentimestamps-support/, https://github.com/opentimestamps/python-opentimestamps

[13] Rule 17a-4 of the Securities Exchange Act (Broker Dealers). See also http://www.17a-4.com/regulations-summary/

[14] M. Carminati, R. Caron, F. Maggi, I. Epifani, S. Zanero, “BankSealer: A decision support system for online banking fraud analysis and investigation”, Computers & Security 53, 175-186, http://www.sciencedirect.com/science/article/pii/S0167404815000437

[15] “2016 Bangladesh Bank Heist”. Available at https://en.wikipedia.org/wiki/2016_Bangladesh_Bank_heist

[16] “The Hard Fork: What's About to Happen to Ethereum and The DAO”, Coindesk (July 18, 2016). http://www.coindesk.com/hard-fork-ethereum-dao/

[17] “EBA Opinion on ‘virtual currencies’” (July 4, 2014). Available at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf