# Blockchain and "smart contracts": FinTech innovations to reduce the costs of trust

Federico Panisi*

ABSTRACT: Financial technology (FinTech) innovations have the potential to reduce transaction costs. More specifically, blockchain and "smart contracts" aim at decreasing monitoring and enforcement costs (i.e. the "costs of trust"). Thus, blockchain and "smart contracts" can free financial institutions from relying on post-trade financial market infrastructures (FMIs) and improve market efficiency in clearing, settlement and transactions management. However, among others, blockchain and "smart contracts" carry new risks (attributable to operational risk) that require adequate governance systems. Basing its analysis on the MiFID II rules on high-frequency trading (HFT), this article sets the grounds for a new risks governance model specifically addressing "smart contracts". More specifically, this article stresses the necessity that financial institutions develop "internal sandboxes", in which "smart contracts" can be fully tested and monitored before their definitive execution on blockchain platforms.

ABSTRACT ……1

1. FinTech and transaction costs: the revolution of blockchain and "smart contracts" …… 2

2. The benefits of blockchain and "smart contracts" in the current financial markets. From the reduction of "settlement latency" to the automation of transactions management …… 8

3. The need of adequate risk governance models for blockchain and "smart contracts". The high-frequency trading discipline and the grounds for financial institutions "internal sandboxes" ……14

*PhD student, Università degli Studi di Brescia
f.panisi@unibs.it

风向转变时,有人筑墙,有人造风车
(When the wind of change blows, some people build walls,
others build windmills - Chinese proverb)

## 1. FinTech and transaction costs: the revolution of blockchain and "smart contracts"

About ten years after the Global Financial Crisis (GFC) started to shake our worldwide economic certainties, the new financial industry applying technology to improve financial activities[1] (globally known as FinTech) is one of the most disruptive and enthusiastic phenomena that are re-shaping the way any subject (people, enterprises, financial institutions, etc.) financially interact with each other. Indeed, its overwhelming energy has made the financial industry consider it a completely new post-crisis paradigm, revolutionizing the traditional conception of financial services provision and, consequently, its regulation as well[2].

[1] P. SCHUEFFEL, *Taming the Beast: A Scientific Definition of FinTech*, *Journal of Innovation Management* 4, 4, 2016, 32 - 54.

[2] D. W. ARNER, J. BARBERIS, R. P. BUCKLEY, *The Evolution of FinTech: A New Post-Crisis Paradigm?*, in *www.ssrn.com*, 2015. See also D. W. ARNER, J. BARBERIS, R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, in *www.ssrn.com*, 2016. As the Authors clearly explain, the use of technology in finance is anything but new. In our age, this interaction dates back to the laying of the first transatlantic cable in 1866 and has developed through the 20th century due to the IT progress. However, in the aftermath of the GFC, the term FinTech has assumed a new meaning. The main reason of the current evolution can be found in the huge amount of personal data nowadays produced and shared via PCs and other mobile devices on the World Wide Web (WWW), especially on social networks. Thus, words like «*Personal data is the new oil of the internet and the new currency of the digital world*» (M. KUNEVA, *Keynote Speech at Roundtable on Online Data Collection, Targeting and Profiling*, in *www.europa.eu*, March 2009, 2) confirm to be very true. Moreover, this new interaction emerges in a financial context in which trends towards disintermediation are stronger than ever (regarding this, it is worthy to remember the very popular words «*Banking is necessary. Banks are not*» pronounced by the Wells Fargo CEO Dick Kovacevich and reported by J. NOCERA, *"Banking Is Necessary - Banks Are Not". Why has banking become less and less important to America? Let us count the ways*, in *www.archive.fortune.com*, 11 May 1998). In addition, its success takes advantage of the lack of trust that in these times traditional financial institutions suffer from (at least in western countries). Eventually, the need of unbanked (or underbanked) people and enterprises of accessing to finance and that of financial institutions to renovate their business models while reducing the (increasingly) costs of regulation blend with specific political decisions (such as the US Jumpstart Our Business

By benefiting from the new opportunities arising from digital technologies, FinTech is a widespread industry that develops in several different areas, varying from payments, to P2P lending and equity crowdfunding and cybersecurity[3]. However, a deep analysis of the FinTech phenomenon shows that all the research and development areas FinTech is divided into share common basic traits. Among these, one of the most significant is the effort to drastically reduce transaction costs[4]. As clearly pointed out by the economic literature, transaction costs are those intrinsic in any value exchange (or contracting activity) and they might be so high to convince parties to discard the finalization of their original decision. Thus, understandably, the lower they are, the easier transactions are concluded. Moreover, these costs follow transactions for all their lifecycle and are generally distinguished in three general dimensions: (1) definition and manufacturing costs, (2) monitoring costs and (3) costs of enforcement[5].

In the decades within the 20th and 21st centuries, the development of the Internet and the World Wide Web (WWW) have made subjects more interconnected and information more shared. Thus, thanks to these technologies, searching information and finding satisfactory solutions to any need have become much easier. Consequently, costs related to the definition and manufacturing of contracts have substantially decreased; monitoring activities have become simpler

---

Startups Act, or more simply JOBS Act, signed into law on April 5, 2012), boosting the rise of the 21st century wave of FinTech.

[3] To get a very clear idea of the areas of the global FinTech landscape see INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSION, *Research Paper on Financial Technologies (Fintech)*, in *www.iosco.org*, February 2017, 4. In the same research paper it can be easily understood how much FinTech is affecting the post-crisis economy. Indeed, it is reported that since the first 2000s investments have grown dramatically and FinTech has been becoming one of the most important drivers of the current economic progress.

[4] J. HAZARD, O. SCLAVOUNIS, H. STIEBER, *Are Transaction Costs Drivers of Financial Institutions? Contracts Made in Heaven, Hell, and the Cloud in Between*, in P. TASCA, T. ASTE, L. PELIZZON, N. PERONY, *Banking Beyond Banks and Money - A Guide to Banking Services in the Twenty-First Century*, Berlin, 2016, 213 - 235. For further explanations about transaction costs see R. H. COASE, *The Problem of Social Cost*, in *The Journal of Law and Economics*, Vol. 3, 1960, 2 - 44, E. F. FAMA, *Efficient Capital Markets: A Review of Theory and Empirical Work*, *The Journal of Finance*, Vol. 25, No. 2, Papers and Proceedings of Twenty-Eight Annual Meeting of the American Finance Association New York, N.Y. December, 28-30, 1969 (May 1970), 383 - 417, R. J. GILSON, R. H. KRAAKMAN, *The Mechanisms of Market Efficiency*, in *Virginia Law Review*, Vol. 70, No. 4, Fifty Years of Federal Securities Regulation: Symposium on Contemporary Problems in Securities regulation (May 1984), 549 - 644, D. G. NORTH, *Institutions, institutional change and economic performance*, Cambridge, 1991, R. J. GILSON, R. KRAAKMAN, *The Mechanisms of Market Efficiency Twenty Years Later: The Hindsight Bias*, in *The Journal of Corporation Law*, Vol. 28, 2003, 715 - 742.

[5] See J. HAZARD, O. SCLAVOUNIS, H. STIEBER, note 4, 218. As the Authors explain these dimensions correspond to the three stages of modern financial and banking intermediation of (1) underwriting and manufacturing of financial instruments, (2) monitoring and screening credit and market risks to the value of contracts and (3) enforcement and execution of financial contracts. Because of asymmetric information and market imperfections each stage has its own cost that can be borne by institutions in a very efficient way.

as well. For these reasons, even financial activities and institutions have greatly benefited from the worldwide spread of the Internet[6].

However, in the last years, digital technologies have been constantly progressing, opening new opportunities and reducing other costs human activities are inevitably tied to. In this context, a new technology aims at revolutionizing the next world economy and at becoming the new transaction costs saver. Its name is Distributed Ledger Technology (DLT) or, as it is more popularly known, blockchain[7].

This technology was originally invented in 2009 by the (still) mysterious author of the first cryptocurrency *Bitcoin* (Sathoshi Nakamoto)[8], to allow people to make secure payments through a trustless-trust and peer-to-peer electronic system, in which it is possible to trust the outputs of the system itself without the need to trust any actor within it[9]. In the following years, blockchain has become a worldwide mania, gaining a lot of attention by start-ups, industries, academics, financial supervisors, regulators and politicians. Nowadays, its non-stop developments and studies have radically exceeded its original intentions[10].

---

[6] The interaction between the Internet and the financial services industry is only one of the sides of a wider reciprocal contamination between technological progress and the evolution of finance within the last centuries. As D. W. ARNER, J. BARBERIS, R. P. BUCKLEY, note 2, 6 and following clearly explains, within 1997 and 2007 the financial markets have become interconnected as never in history thanks to the Internet; in these ten years, transaction costs were reduced and consequently the financial economy lived a period of extraordinarily expansion.

[7] For a general point of view about the expectations of how blockchain (and related "smart contracts", whose it is furtherly explained below) can improve financial services and the whole market see, among others, D. TAPSCOTT, A. TAPSCOTT, *Blockchain Revolution - How the Technology Behind Bitcoin is Changing Money, Business, And the World*, New York, 2016 and W. MOUGAYAR, *The Business Blockchain - Promise, Practice, and Application of the Next Internet Technology*, Hoboken, 2016. Moreover, in its report, SANTANDER INNOVENTURES, *The Fintech 2.0 Paper: rebooting financial services*, in *www.santanderinnoventures.com*, 2015, 15 writes that «distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15 - 20 billion per annum by 2022».

Regarding the terminology used, there is still a lot of confusion. However, as clearly indicated by BANK FOR INTERNATIONAL SETTLEMENTS - COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES, *Distributed ledger technology in payment, clearing and settlement - An analytical framework*, in *www.bis.org*, February 2017, from a general point of view, it can be stated that blockchain is a type of distributed ledger technology. Another type of distributed ledger technologies is consensus ledgers. Moreover, attempts of clarifying the blockchain lexicon (that is still rapidly evolving) have been becoming more frequent (see, for instance, A. WALCH, *The Path of the Blockchain Lexicon (and the Law)*, in *www.ssrn.com*, 2017).

[8] See S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, in *www.bitcoin.org*, 2009.

[9] K. WERBACH, *Trustless Trust*, in *www.ssrn.com*, 2016.

[10] To understand all the potential areas where blockchain could be used see, for instance, C. CATALINI, *How Blockchain Applications Will Move Beyond Finance*, in *www.hbr.org*, March 2017 or BLOCKGEEKS, *17 Applications That Are Transforming Society*, in *www.blockgeeks.com*, March 2017 or CB INSIGHTS, *Banking Is Only The Start: 27 Big Industries Where Blockchain Could Be Used*, in *www.cbinsights.com*, February 2017.

Briefly speaking, blockchain is a computer protocol that allows many participants of a same network (the so-called nodes) to record information on a single shared ledger, so everyone can see the same data. The ledger's key benefit is that users do not need trusted third parties to guard against double-spending risks or expensive processes to reconcile information between ledgers[11]. Thus, due to a system that combines cryptography, game theory and distributed consensus principles, blockchain technologies aim at offering a new solution to the never-ending human problem of trust[12].

As it is easily understandable, trust (i.e. the combination of rational risk assessment and disposition towards any other agent - person, institution, etc.) is an essential factor in the success of societies. In fact, a culture of trust can be compared to an economic lubricant able to reduce the transaction costs inherent in every economic activity and is so important that recent studies have shown that high-trust countries create more wealth than others do[13]. However, due to its limits and the difficulty to extend it beyond the borders of small simple communities (such as families), trust works best in informal societies.

Therefore, in the modern world - where human certainties are reduced because of society complexities and asymmetric information, high-trust communities have developed methods to extend trust to strangers as well, allowing individuals to contract and exchange value on a large scale[14]. All these methods can be traced back to the idea of relying on third-party agents, which lower all transaction costs, including those of monitoring and enforcement. Indeed, once contracts are signed, intermediaries can monitor their execution more easily than

---

[11] C. A. WILKINS, *Fintech and the Financial Ecosystem: Evolution or Revolution?*, in *www.bankofcanada.ca*, June 2016, 4. See also FINANCIAL CONDUCT AUTHORITY, *Discussion Paper on distributed ledger technology*, in *www.fca.org.uk*, April 2017, FINANCIAL INDUSTRY REGULATION AUTHORITY, *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*, in *www.finra.org*, January 2017, EUROPEAN SECURITIES AND MARKETS AUTHORITY, *Discussion Paper - The Distributed Ledger Technology Applied to Securities Markets*, in *www.esma.europa.eu*, June 2016, 8, A. PINNA, W. RUTTENBERG, *Distributed ledger technologies in securities post-trading - Revolution or evolution?*, in *www.ecb.europa.eu*, April 2016 and EUROPEAN CENTRAL BANK, *In Focus, Issue 1 - Distributed Ledger Technology*, in *www.ecb.europa.eu*, April 2016.

[12] K. WERBACH, note 9, 2.

[13] K. WERBACH, note 9, 8. For a very interesting study on science-backed insights of human trust and how it affects every complex organization see also P. J. ZAK, *Trust Factor - The Science of Creating High-Performance Companies*, New York, 2017.

[14] K. WERBACH, note 9, 8 and J. HAZARD, O. SCLAVOUNIS, H. STIEBER, note 4, 220, who highlight that the difference between contracting in very simple (informal) and complex (formal) societies is ultimately a matter of combination between flows of information and "cooperation-*vs*-defection" choices of their members. Indeed, they write that «[i]n groups, individuals have information about the other members of the group based on past interactions. The smaller, denser and more homogenous the group, the faster information related to reputation travels. This enables individuals to ascertain the risk of dealing with another individual. Defection from the accepted institution is dis-incentivized by damaging the reputation of the offender (thus making it harder for her to find other trading partners) and by the resultant ostracism from other members».

each single individual and have even the power to force any party to meet their obligations, if necessary. However, although essential for any complex society, from an economic point of view, intermediary-based trust is a cost that is reasonably accepted by agents because it is generally lower than the sum of all transaction costs if third-party agents missed[15]. Moreover, third-party agents are a cost-efficient solution for the system depending on whether they perform their function impartially and consistently and to the extent their actions are trusted to be fair[16].

However, what if technology can overtake this "trust dilemma"? Since its invention, blockchain has appeared able to overcome the dilemma between the necessity of intermediaries and the trust-related costs, enabling any subject to exchange value both without worrying about the risk of the other party's defection (that is what Nakamoto originally identifies as "double-spending risk") and the need to rely on third-party agents[17]. In a nutshell, the core of the blockchain idea is to substitute third-party agents with a system of validation of any change of state, which ultimately is a process that updates data (information or records) throughout the entire distributed ledger in a trustworthy, secure and efficient way[18]. Thus, on blockchain platforms value can be exchanged by parties only after the validation mechanism has correctly processed.

Moreover, thanks to the progress that blockchain technologies have made in less than ten years, new blockchain protocols have been developed and new blockchain-based ideas have been rapidly invented and tested[19]. Consequently,

---

[15] J. HAZARD, O. SCLAVOUNIS, H. STIEBER, note 4, 221. Even S. NAKAMOTO, note 8, 1 is completely conscious about this problem when, regarding payments, he explains that «[t]he cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party».

[16] J. HAZARD, O. SCLAVOUNIS, H. STIEBER, note 4, 221.

[17] S. NAKAMOTO, note 8, 1 and following.

[18] See HONG KONG APPLIED SCIENCE AND TECHNOLOGY RESEARCH INSTITUTE, *Whitepaper on Distributed Ledger Technology*, in *www.hkma.gov*, November 2016, 3.

[19] Indeed, in the aftermath of the spread of the Bitcoin blockchain new protocols have been invented and nowadays there are other several major platforms, such as *Ethereum*, *Ripple*, *Hyperledger*, *Corda* etc. (among the others see EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *Distributed Ledger Technology & Cybersecurity - Improving Information Security in the Financial Sector*, in *www.enisa.europa.eu*, December 2016 or B. NIELSON, *Review of the 6 Major Blockchain Protocols*, in *www.richtopia.com*) and each of one has its own characteristics. Indeed, blockchains can be permissionless (or public, such as *Bitcoin* or *Ethereum*) or permissioned (or private). Permissionless blockchains are open systems and do not have any restriction on participation and are secured only by mechanisms based on cryptoeconomies. In public blockchain each participant of the network functions as its node, has the right to access data stored in the ledger, to add to the ledger and to participate in the validation process. Differently, permissioned

blockchain has gone beyond its original borders and have spread into other areas different from payments, such as legal agreements. Therefore, a second layer of blockchain technologies has received attention and is represented by the so-called "smart contracts".

Notwithstanding the misleading terminology, "smart contracts" are new automatable software programs running on blockchain platforms and made by computer modules programmed to transfer tokens of value, enable access to different resources or automate condition-based functions[20]. "Smart contracts" essential and most exciting characteristic is that they are self-executing and self-enforcing, ideally nullifying the enforcement costs by eliminating the risk of breach of contract between parties[21]. The idea of "smart contracts" is older than the blockchain popularization but it is only thanks to blockchain that "smart contracts"

---

blockchains are distributed ledgers shared by trusted parties that are permitted to access the system. For this reason, private blockchains are more attractive to the financial services industry. Moreover, in permissioned blockchains there are governing entities that approve admissions of new participants under certain predefined criteria and specific nodes are responsible for the validation process. Thus, permissioned blockchains are only partially decentralized.

Blockchains also differentiate one from the other on the consensus protocol that is the mechanism by which the nodes within a distributed ledger agree on the validity of the underlying data. The most commonly used consensus protocols are proof-of-work (PoW) and proof-of-stake (PoS). The former is usually used in permissionless blockchains and it is characterized for the presence of some "full nodes" that voluntarily validate data by using computational power, generally in exchange of digital rewards. The latter instead requires specific nodes collecting ("bonding") a certain number of digital assets as collateral to validate and add new blocks on blockchain.

[20] INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSION, note 3, 51, C. D. CLACK, V. A BAKSHI, L. BRAINE, *Smart Contract Templates: foundations, design landscape and research directions*, in *www.arxiv.org*, August 2016 (revised March 2017), 2 and P. DE FILIPPI, S. HASSAN, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, in *First Monday - Peer-reviewed Journal on the Internet*, Vol. 21, No. 12, December 2016. Regarding the terminology used, although law and software must be kept separated (see J. HAZARD, O. SCLAVOUNIS, H. STIEBER, note 4, 225 peremptorily writing that "smart contracts" «are automation, not law») "smart contracts" determine a mixture of them. Indeed, P. DE FILIPPI, S. HASSAN explain that "smart contracts" represent the fourth phase of the permanently evolving relationship between law and technology. After the period of the digitizing information process (first phase), of the automation of decision-making process (second phase) and the years of the incorporation of legal rules into codes and the emergence of regulation by code (that is the third phase or the rise of *Lex Informatica*) we are now witnessing the beginning of the «code-ification of law, which entails an increasing reliance on code not only to enforce legal rules, but also to draft and elaborate these rules. As a result of these technological advances, the lines between what constitutes a legal or technical rule becomes more blurred, since smart contracts can be used as both a support and as a replacement to legal contracts».

[21] Of course, "smart contracts" can be distinguished into different categories on the basis of their degree of immutability and their proneness to be altered and modified through modification or revocation. For further explanations, it is worthy to read M. RASKIN, *The Law and Legality of Smart Contracts*, in *Georgetown Law Technology Review*, Vol. 1:2, 2017, in which the Author distinguishes between "strong smart contracts" and "weak smart contracts" (depending on whether the cost to alter the contract is prohibitive or not) to clarify that «technology and societies are far away from […] pure strong smart contract[s]». Both are more comfortable with "weak smart contracts", such as «an easily revocable money transfer between two large financial institutions where a court could simply order the transfer undone or modified if necessary».

supporters can anchor their hopes of realization, because blockchain finally offers a reliable value-transfer and enforcement underlying mechanism[22].

2. The benefits of blockchain and "smart contracts" in the current financial markets. From the reduction of "settlement latency" to the automation of transactions management

In the last years, blockchain and "smart contracts" have gained a lot of attention, especially in the financial world, in which different institutions aspire to become "frontrunners" for their next implementation. To financial institutions blockchain and "smart contracts" are highly attractive. On the one hand, blockchain deeply addresses the issue of asymmetric information among financial players, while "smart contracts" are considered (as any other computer or algorithmic machine) faster, more efficient and more reliable compared to mistake-prone and biased human actions, especially in case of high repetitive works[23]. Thus, it is widely thought they can both consistently reduce costs and improve market efficiency[24].

[22] K. WERBACH, N. CORNELL, *Contracts* Ex Machina, in *www.ssrn.com*, 2017. As clearly pointed out by the Authors, embodying legal agreements in software code is not new. In fact, we have already known electronic contracts (contracts whose form is written in digital costume, but the execution still relies on human activities), data-oriented contracts (contracts in which parties express one or more terms or conditions of their agreements in a designed manner that can be processed by computer systems - for example, a financial option contract granting the right to purchase a stock at a given price and expiring on a certain date, so that a broker, if conditions are met, orders its computer system to transfer the security to the buyer's account and debit the correct amount of money) and computable contracts (where computer systems implementing data-oriented contracts have also the power to make automated, *prima-facie* assessments about the parties compliance or performances - in the previous financial option example, the broker's computer evaluates if price and timing of a proposed purchase meet the terms of the agreement). However, these are not "smart contracts" as the inventor of this concept, the cryptographer Nick Szabo, intended. Indeed, when in 1996 -1997 he published some articles about his ideas, he suggested to embed all the contractual phases in hardware and software, in a way that it alone handles the full lifecycle of the contractual activity. His very simple example of "smart contract" is the vending machine, that directly effectuates its performance (it takes money and dispends product) making for the buyer the cost of defection (to destroy the machine itself to get the product) higher than the potential reward.

[23] K. WERBACH, N. CORNELL, note 22, 56.

[24] To CAPGEMINI CONSULTING, *Smart Contracts in Financial Services: Getting from Hype to Reality*, in *www.capgemini-consulting.com*, October 2016, 2, the potential benefits of "smart contracts" for financial institutions and their customers are huge. Indeed, Capgemini estimates that "smart contracts" would shorten the settlement cycles of syndicated loans, leading to an additional 5% to 6% growth in demand in the future and to additional income of between US $2 billion and $7 billion annually. Moreover, the paper reports that investment banks in the US and Europe would also see lower operational costs. Retail banking and insurance would significantly benefit from

Because of the attention gained by financial institutions, many efforts have been put in the last years in developing these technologies and important experimentations are spreading very quickly in financial markets, such as the project aimed at developing a blockchain-based market for repurchase agreements (or, as more commonly known, repos)[25].

Before having a look at blockchain and "smart contracts" in financial markets, it must be considered that repos and, more in general, any other financial contract originally developed in their simplest structure, which is bilateral. Bilateral financial contracts are usually characterised by a "delivery versus payment" (or DVP) settlement system.

In the DVP settlement system, the transfer of securities and payment is simultaneous and follows the specific settlement required by the securities transacted. DVP settlement systems are very beneficial for the buyer, entrusting the same with direct operational control on securities. However, in this settlement model, transactions are burdened by expensive fees. In addition, bilateral financial contracts can turn out to be very high complex operations for some financial players (especially for those that do not deal daily with securities management[26]). Consequently, the lack of expertise in management activities that are essential for their financial goals (including, for instance, tracking the securities to be received, evaluating their adequacy and the correct value, ensuring that proper margins have been applied, etc.) makes these contracts too expensive[27].

---

adopting "smart contracts" too. For example, banking consumers could save from US $480 to US $960 per loan and banks would be able to reduce costs in the range of US $3 billion to $11 billion annually by lowering processing costs in the origination process in the US and European markets. Similarly, and regarding the insurance sector, the usage of "smart contracts" in the personal motor insurance industry could result in US $21 billion annual cost savings and consumers could also expect lower premiums as insurers potentially pass on a portion of their annual savings to them.

[25] For further statements about the last steps of the current experimentation see DTCC, *DTCC & Digital Asset Move to Next Phase After Successful Proof-Of-Concept for Repo Transactions Using Distributed Ledger Technology - Press Release*, in *www.dtcc.com*, February 2017 and A. IRREA, *DTCC Completes Blockchain Repo Test*, in *www.reuters.com*, February 2017, reporting that «Post-trade provider Depository Trust & Clearing Corporation, or DTCC, has successfully completed testing of blockchain-based technology for the clearing and settlement of repurchase, or repo, agreement transactions». Other statements about the launch of the project can be found in DTCC & DIGITAL ASSET HOLDING, *DTCC and Digital Asset to Develop Distributed Ledger Solution to Drive Improvements in Repo Clearing - Press Release*, in *www.dtcc.com*, March 2016 and K. BURNE, T. DEMOS, *Repurchase Agreements: Digital-Ledger Test Set for Repos - Bitcoin technology blockchain might help smooth over problems in $2.6 trillion market*, in *Wall Street Journal - Eastern edition*, March 30th 2016.

[26] Considering the above-mentioned repo transactions is worthy to better understand these problems. In fact, buyers in repos (the so-called "cash providers") can be easily included in this category of financial players.

[27] A. COPELAND, D. DUFFIE, A. MARTIN, S. MCLAUGHLIN, *Key Mechanics of the U.S. Tri-Party Repo Market*, in *FRBNY Economic Policy Review*, November 2012, 19 and EUROCLEAR, *Understanding repos and the repo markets*, in *www.theotcspace.com*, March 2009, 30.

Therefore, more articulated versions of financial transactions have been developed, such as those in which the seller of securities offers to hold them into specific and segregated accounts[28]. In this case, the settlement of the whole operation becomes much easier (i.e. more cost-efficient compared to DVP contracts) because of the lack of operational movement of securities during the transaction lifecycle. However, the segregation of assets does not sufficiently safeguard against the difficulties to achieve the securities if the seller defaults. Moreover, this model is not considered trustworthy anymore, because it suffers from the potential risk of fraud, such as "double dipping" (generally considered as the risk that financial professionals operate in a way enabling them to receive two incomes from the same financial source)[29]. As a consequence, the segregation of assets model is not very popular in finance anymore.

To overtake such problems, financial practice has moved towards transaction models characterized by the presence of third-party agents (the so-called Financial Market Infrastructures - FMIs) aimed at facilitating the operations that contracts lifecycle inevitably requires (such as clearing of data coming from contracting parties and settlement functions). While easing transactions, third-party agents also safeguard confidence and trust among market players. In addition, third-party agents also provide complex operational services, including the custody of assets, their revaluation and the margining of securities that are pledged as collateral (that is the so-called "collateral management")[30].

---

[28] Repurchase agreements can be considered a good example of this trend. Indeed, due to the complexities related to the management of securities (such as their tracking, evaluating their adequacy and the correct value, ensuring that proper margins have been applied etc.), very soon bilateral repos evolved in Hold-In-Custody (HIC) repos, in which the seller also offers to hold the securities as a custodian.

[29] A. COPELAND, D. DUFFIE, A. MARTIN, S. MCLAUGHLIN, note 27, 18. See also EUROCLEAR, note 27, 30 stating that «Double dipping was a serious problem in the US market in the 1980s». For instance, "double dipping" in repo transactions realizes if the seller borrows money from different cash providers by pledging the same securities.

[30] Once again, mentioning repos is very helpful to understand it. Indeed, nowadays, repo transactions are based whether on central counterparty clearing houses (CCPs) or clearing banks depending on whether the third-party agent assumes or not the counterparty risk (for further details see A. COPELAND, D. DUFFIE, A. MARTIN, S. MCLAUGHLIN, note 27, 19). In addition to this, a consequential trait of CCP-based repos directly linked to the assumption of counterparty risk by the central counterparty clearing house is anonymity between securities dealers and cash providers. As reported by DE NEDERLANSCHE BANK, *All the Ins & Outs of CCPs - The central counterparty: a pivotal player in the financial network*, in *www.dnb.nl*, October 2013, financial players consider anonymity as a very important advantage. Indeed, «[a]s the CCP becomes the counterparty of both trading participants [i.e. the CCP becomes the "buyer to every seller and seller to every buyer"], they remain anonymous to their counterparty. The advantage of anonymity is that trading participants need not worry about the counterparty's creditworthiness. They can trade with any other trading members. In addition, anonymity is extremely desirable in certain situations, for instance if a party suddenly needs to borrow a large sum of money or sell a large investment portfolio. This prevents a party who is already in a difficult position being hit harder due to the market getting wind of its predicament and turning against it».

If contractual structures based on third-party agents are compared to the first two models, the analysis leads to the following statement: third-party agent models offer both the safety of DVP transactions (since operational as well as legal control is transferred to the buyer) and the cost-efficiency of transactions relying on segregated accounts of the seller (indeed, collateral moves within the custodian rather than across settlement systems)[31].

However, despite such benefits both for the contracting parties and the whole market, relying on third-party agents is costly and highly time-consuming. Therefore, it is inevitable that a "settlement latency" between the opening and the final settlement of financial operations arises. The longer this latency is, the higher is for both parties the "settlement risk", which is the risk each party fails to fulfil the terms of the contract by the settlement date. Financial players are always very careful in considering this risk while negotiating, because its realization can even lead to other (and more dangerous) risks, such as credit and liquidity risks[32].

All this considered, repurchase agreements can better clarify the reason of this latency in financial operations and how the implementation of blockchain can radically disrupt the current *status quo*. More specifically, next focus will be on those repurchase agreements with the shortest term commonly signed by financial institutions: "overnight repos".

"Overnight repos" are repurchase agreements through which financial players buy securities under the agreement that they are repurchased by the seller the following day. In "overnight repos" the "opening leg" (which is the allocation and the purchase of collateral) is generally settled as an ordinary transaction in the late afternoon of day "T". Consequently, the transaction is cleared in day "T + 1" and, only when clearing is fully completed, the "closing leg" is finally settled. In addition, because of this time lag, solely the repurchase transaction is settled through netting (differently from the "opening leg" that is settled as a normal transaction), ensuring only for the "closing leg" aggregation of cash amounts and fewer payments for parties[33].

As mentioned above, blockchain essentially consists in a shared distributed ledger in which data can be seen simultaneously by every member of the same network. Once encrypted through specific validation protocols, data stored on blockchain platforms cannot be modified anymore and are added to the previous blocks, building the chain. Consequently, thanks to chains of immutable and accessible data, financial institutions must not heavily rely on post-trade processes

[31] EUROCLEAR, note 27, 30.

[32] Among different definitions of settlement risk see, for instance, BANK FOR INTERNATIONAL SETTLEMENTS - COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES, *A glossary of terms used in payments and settlement systems*, in *www.bis.org*, March 2003, 45.

[33] For further explanations about the different settlement systems of the "opening" and the "closing leg" of repurchase agreements see *www.dtcc.com*.

of data reconciliation as they currently do. Indeed, the trustworthy "pre-trade transparency", on which the blockchain proof-of-concept is based, leads negotiating parties (and the whole blockchain financial network as well) to have more information about the capacity of each counterparty to meet its own obligations, even before each transaction is signed[34].

Thus, because of this "transparency revolution", blockchain technologies reduce the need of clearing and allow faster - or even "near-real time" - settlements of contracts[35]. Therefore, and with more specific regard to the previous example, blockchain is potentially able to reduce the current overnight repos "settlement latency" from T + 1 to T + < 1 or, as just mentioned, even to T + "near-real T". Of course, financial markets (such as the repo markets) can highly benefit from blockchain, because it can both save post-trade FMIs-related costs, drastically reduce the "settlement risk" and shorten the current "settlement latency" even by intra-day time, speeding financial transactions up.

Benefits of blockchain technologies are even more evident when considering the automation of transactions management through "smart contracts" that they allow.

As it can be easily understood, financial transactions always require different management activities during their lifecycle. Proper management is considered essential to retain their economic benefits. For this reason, risks related to these management activities are generally governed by specialized third-party agents that make use of trustworthy operational mechanisms. However, as already pointed out, relying on these agents turns out to be a cost for financial players. "Smart contracts" aims to radically reduce this cost, creating the opportunity to code transactions management directions into self-enforcing software running on blockchain platforms.

Therefore, thanks to "smart contracts", transactions management is radically simplified because any variation of the initial contractual details is constantly updated and immediately executed by the code into which the contractual clauses have been "translated"[36]. Moreover, thanks to the distributed

[34] It is important to remind that blockchain is a "transactional technology", which means that any change in the ledger (i.e. a transaction) is possible because it is either not done at all or already completed (see Introduction to Smart Contracts available at *www.solidity.readthedocs.io*). After the validation of the transaction, everyone can read the updated and immutable entries in the database just by participating in the network. Thus, transparency within the network is much higher.

[35] EUROCLEAR, OLIVER WYMAN, *Blockchain in Capital Markets - The Prize and the Journey*, in *www.dltmarket.com*, February 2016, 12 - 13. To further understand the impact of blockchain technologies in the post-trade financial market infrastructures and processes see also Digital Asset Holding - Frequently Asked Questions available at *www.digitalasset.com*.

[36] For instance, in repo transactions, the automated management achieved by "smart contracts" can refer both to the maintenance of initial haircut through "margin calls", the claim of rights of direct substitution of securities and payments of incomes on pledged collateral.

validation system characterizing blockchain technologies, management activities cannot be neither altered nor modified. The expectations they can be fairly unwound all along the transaction lifecycle seem to be finally fulfilled. Eventually, due to "smart contracts" (as a rule) cannot be stopped while they execute[37], settlement risk is furtherly reduced. Consequently, even counterparty risk is resized, although only partially[38].

---

Regarding the contractual clauses that are translated into code, it must be remembered that «[n]*ot all clauses are susceptible to automation and self-execution*» (ISDA, LINKLATERS, *Whitepaper Smart Contracts and Distributed Ledger - A Legal Perspective*, in *www.linklaters.com*, August 2017, 10). Indeed, as the White Paper explains contractual clauses can be divided into "operational" and "non-operational". The former clauses are usually written in some form of conditional statements (such as "if-then-else" sentences stating, "if X happens, do Y, else do Z") and constitute the main part of financial contracts. To the White Paper examples of "operational" clauses are those «that [require] an amount to be payable on a payment date equal to the product of a calculation amount, a floating rate (plus or minus a spread) and a day count fraction» or «that [require] a party to transfer assets on a particular date that have a value equal to the amount by which a required credit support amount is less than the value of collateral provided, subject to certain formulaic haircuts and adjustments». Differently, "non-operational" clauses relate to the wider legal relationship between the parties, although they are not embedded in conditional logic. Translating these clauses into "smart contracts" code is less achievable and needs more steps. However, due to the necessity of this translation activity, in both cases there is a split into a "dumb contract" written in human-readable language (or "wet code", which is inherently ambiguous and flexible and that can be applied on a case-by-case basis to an indefinite number of situations that might not have been precisely foreseen) and a "smart contract" written in "dry code", made of computer codes and computer-readable files. Differently from the "wet code", the latter is made of a strict and formalized language, which requires well defined categories and the precise stipulation of methods and conditions that need to be defined in advance (for deeper analyses see P. DE FILIPPI, S. HASSAN, note 20, 7). Due to the obvious discrepancies that subsist between these two different types of language, translation errors might arise. Therefore, it is worthy to highlight that an appropriate model for designing and implementing "smart contracts" is to sign a "dumb contract" in the form of a «legal wrapper which sets out terms of the contract which are not deterministic and not suitable for execution through smart contract [and that] should incorporate the smart contract code by reference into the contract, but […] should take priority over the code if there was some conflict between the two» (see C. LIM, TJ SAW, C. SARGEANT, *Smart Contracts: Bridging the Gap Between Expectation and Reality*, in *www.law.ox.ac.uk*, July 2016).

[37] M. RASKIN, note 21, 7 and K. WERBACH, note 9, 27. Of course, the fact that "smart contracts" are unstoppable while executing can be also counter-beneficial. This is the reason why C. LIM, TJ SAW, C. SARGEANT, note 36, proposes to provide "smart contracts" with a "kill-switch" or a "fail-safe" to empower parties to terminate the code in certain agreed circumstances. If controversies arise from the "fail-safe" adoption they can be resolved by the parties in accordance with the original legal agreement and within the framework of the law. Moreover, the Authors think that adding a "fail-safe" «could also allow parties to amend the smart contract code when there is a contract variation, or where a party chooses to waive certain rights under the contract».

[38] As N. BEIER, H. HARREIS, T. POPPENSIEKER, D. SOJKA, M. THATEN, *Getting to grips with counterparty risk - McKinsey Working Papers on Risk, Number 20*, in *www.mckinsey.com*, June 2010, 2 clearly explains, settlement risk is only one version of the wider concept of counterparty risk, which is one of two areas of credit risk. The other versions of counterparty risk are default risk (the risk that counterparty defaults and transaction fails to pay) and replacement risk (the risk that, after the counterparty's default, replacing the same deal is not possible anymore). Although "smart contracts" reduce settlement risk, they cannot reduce default risk. In fact, the idea that "smart contracts" are software programs able to self-enforce legal agreements does not mean that default risks are avoided. As ISDA, LINKLATERS, note 36, 9 points out, the self-execution characteristic of

3. The need of adequate risk governance models for blockchain and "smart contracts". The high-frequency trading discipline and the grounds for financial institutions "internal sandboxes"

Although law and software codes have been interacting and reciprocally evolving for some decades[39], both blockchain and "smart contracts" already witness that we have just entered a new phase of the knitting between finance and technology; in this new "financial era", both might be the next true "game changer" of our markets[40]. In this new context, automation and (systemic) software dependence get always more importance. As a consequence, further technological complexity overlaps the high level of sophistication financial markets are already deeply characterized. Because of this, additional new risks can arise and easily spread.

Of course, blockchain and "smart contracts" can be very potential drivers of these new risks. Indeed, as any other software program also blockchain and "smart contracts" are human creations and, like those who program them, they are inherently imperfect. Therefore, they might suffer from glitches and bugs and show all their vulnerability[41].

Of course, the reliance of contemporary finance on information and digital technologies is high beneficial and, most of all, is a one-way path which started to proceed many years ago. This is why financial markets have already got accustomed to technological vulnerability and wisely consider it as a main risk category, which is "operational risk"[42]. In fact, as it is well known, "operational

"smart contracts" is «subject to the obvious qualification that the party making the payment needs to have sufficient funds to make such payment and those funds need to have been made available to the smart contract». Due to self-execution essentially means that pre-specified actions are enforced automatically, it might also happen that the payment has been enforced by the software on insolvency grounds. This is the main reason why legal actions between parties might be still required although they decided to automate the execution of transactions through "smart contracts".

[39] P. DE FILIPPI, S. HASSAN, note 20.

[40] Indeed, as D. W. ARNER, J. BARBERIS, R. P. BUCKLEY, note 2, 15 and following explains, currently we are in the «*FinTech 3.0 era*», that will be increasingly characterized both by the massive use of digital technologies in financial services and by the rise of new technological players which traditional banking institutions might not be able to compete with.

[41] A. WALCH, *The Bitcoin blockchain as financial market infrastructure: A Consideration of Operational Risk*, in *New York University Journal of Legislation and Public Policy*, Vol. 18:837, 2015, 856.

[42] N. BEIER, H. HARREIS, T. POPPENSIEKER, D. SOJKA, M. THATEN, note 38, 2.

risk" is generally defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events[43].

However, recent events clearly help to better understand the operational risks of these very new technologies and what kind of financial outcomes imperceptible software bugs can have towards investors and financial markets. More specifically, it is worthy to remember that the glitch that the American global financial services firm *Knight Capital Group* experienced in summer 2012 in its high-frequency trading (HFT) computers easily turned out to be a technology breakdown, which led to a financial meltdown with considerable losses both for the firm (about $460 million) and the stock markets as well[44].

Similarly, the vulnerability affecting the code *The DAO* (a distributed autonomous organization[45]) relied on for its investment vehicle running on *Ethereum* blockchain was essential to allow, in summer 2016, one (or more) *The DAO* token holders[46] to exploit a bug in the code, to siphon off one-third of the

---

[43] BASEL COMMITTEE ON BANKING SUPERVISION, *International Convergence of Capital Measurement and Capital Standards - A Revised Framework*, in *www.bis.org*, June 2004, 137. This definition includes legal risk, but excludes strategic and reputational risk.

[44] As clearly explained by P. CONAC, *Algorithmic Trading and High-frequency Trading (HFT)*, in *Regulation of the EU Financial Markets - MiFID II and MiFIR (edited by Danny Busch and Guido Ferrarini)*, Oxford, 2017, 469 and following high-frequency trading (HFT) is a subcategory of algorithmic trading, referring to automated trading conducted at millisecond or microsecond speeds throughout the trading day. Regarding the Knight Capital Group HFT software failure, U.S. SECURITIES AND EXCHANGE COMMISSION, *Order Instituting Administrative and Cease-and-desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-desist Order*, in *www.sec.gov*, January 2015 reports that in that summer Knight Capital Group made some changes to the software code of its HFT servers to enable customers to participate to a new convenient program. However, due to a copying mistake and a lack of adequate double-check internal procedure, the update did not remove an unwanted unused code (the "Power Peg" functionality) that on August 1st 2012 was accidentally triggered. The result was 4 million executions in 154 stocks for more than 397 million shares in approximately 45 minutes that made Knight assume an approximately $3.5 billion net long position in 80 stocks and an approximately $3.15 billion net short position in 74 stocks. The millions of shares bought and sold pushed the value of many stocks up and the company borne many losses when it had to sell the overvalued shares back into the market at a lower price. Of course, financial disorders were not limited to Knight Capital but inevitably affected other stock trading firms.

[45] As explained by K. WERBACH, note 9, 53, distributed autonomous organizations are business firms conceived as nexuses of contracts and built entirely in software programs, by encoding the standard corporate arrangements of equity, debt and corporate governance. On the one hand, investors contribute funds through cryptocurrencies (such as *Bitcoin* or *Ether*, like it was in *The DAO* case); on the other, the distributed application handles payments of salaries, dividends, proxy vote and so on.

[46] The word "token" refers to the digital representation of real-world assets like currencies, commodities, securities or properties. For instance, a share token is a digital version of a share certificate. Rather than owning a paper certificate specifying ownership of shares, a shareholder owns digital tokens, representing the equivalent of shares. Moreover, due to "smart contracts" are legal contracts embedded into codes, it is possible to assign the attached rights to various classes of shares to these tokens. Tokens can also refer to more complex financial instruments such as derivatives, whose settlement execution follows external events (see EUROPEAN UNION AGENCY

value held in the application (roughly $50 million) and to move it to their own accounts. This software vulnerability was so irremediable that the so-called "recursive attack"[47] was stopped only through a bailout of the original *The DAO* investors by setting a new protocol that enabled investors to withdraw their own funds[48].

Both episodes have a very strong pedagogic power. Indeed, in addition to highlight the possible *cons* inevitably brought by these new technologies, they also help to elaborate the awareness that these risks must be managed with new adequate firewalls that protect from further financial disorders and instability spreading throughout markets[49].

Before reasoning about which firewalls might be appropriate, a preliminary consideration must be underlined. The last financial crises taught us that the first safeguards helping the system to withstand the force of severe financial storms are internal to financial institutions. This is the reason why in its aftermath, regulators and supervisors have been stressing the necessity that financial institutions have adequate capital buffers that avoid them to be overleveraged[50]. Similarly, to prevent that software errors can cause dangerous meltdowns in the next hyper-technologized financial networks, financial institutions must equip themselves with adequate internal risk governance models, specifically addressing the new digital technologies they are going to adopt.

In this attempt, the efforts of legal scholars reveal very important. Indeed, both blockchain and "smart contracts" technologies are still underway; thus, while

---

FOR NETWORK AND INFORMATION SECURITY, note 19, 25). Related to tokens are the cryptocurrency projects financing tools called ICOs (Initial Coin Offerings). Through ICOs new cryptocurrency projects sell part of their cryptocurrency tokens in exchange of fiat money. ICOs can raise *Bitcoin*, *Ether* or other cryptocurrencies.

[47] The attack has been called "recursive" because it blocked the function that updated every user's token balance, allowing the attacker (or attackers) to withdraw more funds than they were entitled to.

[48] P. MURCK, *Who Controls the Blockchain?*, in *www.hbr.org*, April 2017. This operation is technically called "hard fork" and it is a protocol change of the underlying blockchain that creates a new path (a new chain of blocks, indeed) and nodes running the previous blockchain protocol are not accepted by the new version anymore. Luckily, thanks to this "hard fork", nearly half of the original investors have been able to recover their investments within a day (EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, note 19, 29.). However, because of it, the *Ethereum* blockchain was split and now there are two different blockchains: *Ethereum* and *Ethereum Classic*, which is the continuation of the original hacked blockchain and does not recognise the reversion of the attack as valid.

[49] For a similar idea see the Securities and Exchange Commission Chairman Schapiro Statement on Knight Capital Group Trading Issue, released on August 3rd 2012, a few days after the Knight HFT system failure: «the error reflects the type of event that can raise concerns for investors about […] equity markets […]. Reliance on computer is a fact of life not only in markets everywhere, but in virtually every facet of business. That doesn't mean we should not endeavor to reduce the likelihood of technology errors and limit their impact when they occur» (the Statement of Mrs. Schapiro is available at *www.sec.gov*).

[50] T. F. GEITHNER, *Stress Test - Reflections on Financial Crises*, New York, 2014, 115.

they get further maturity to prove their estimated benefits, questions about understanding which regulation might fit best naturally arise. Answering these questions must first take into consideration that blockchain financial networks cannot remain outside the regulatory perimeter and that law and distributed ledgers need to cooperate with each other to move ahead[51]. In addition, legal scholars have the task to help finding a balance that does not harm the potentialities of these technologies while safeguarding markets[52]. Thus, the first step to do is to wonder about which regulation might address financial institutions implementing "smart contracts" on blockchain financial networks. The effort to identify the best regulation for blockchain and smart contracts should start from looking at the regulation of those activities and financial firms that strongly rely on technology and software-based automation. Once again, focusing on high frequency trading (HFT) can be very useful for the further reasoning.

As briefly explained while mentioning what happened to *Knight Capital*, HFT is a form of algorithmic trading in which algorithms replicate human decisions, automatically determining individual parameters of orders such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission[53]. Thus, similarly to blockchain-based "smart contracts", in HFT, technology surrogates what is traditionally entrusted to humans. In both cases, execution (of orders, the former, of contracts, the latter) is completely automated.

Due to the risks related to this automation process, HFT has been punctually regulated. In the European Union, its discipline is in the recent Directive 2014/65 EU (MiFID II), coming into force soon. More specifically, article 17 paragraph (1) Directive 2014/65 EU states that «[a]n investment firm that engages in algorithmic trading shall have in place effective systems and risk controls suitable to the business it operates to ensure that its trading systems are resilient and have sufficient capacity, are subject to appropriate trading thresholds and limits and prevent the sending of erroneous orders or the systems otherwise functioning in a way that may create or contribute to a disorderly market. […] The investment firm shall have in place effective business continuity arrangements to deal with any failure of its trading systems and shall ensure its systems are fully tested and properly monitored to ensure that they meet the requirements laid down in this

[51] See P. PAECH, *The Governance of Blockchain Financial Networks*, in *www.ssrn.com*, 2016, 6 and K. WERBACH, note 9, 73 and following.

[52] Requests not to harm the current blockchain evolution comes from the industry but also from advocates of some government agencies like J. Christopher Giancarlo, Commissioner of the United States Commodity Futures Trading Commission (CFTC). See J. C. GIANCARLO, *Regulators and the Blockchain: First, Do No Harm - Special Address before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium*, in *www.cftc.gov*, March 2016.

[53] See P. CONAC, note 44, 470 and article 4(1) (39) of Directive 2014/65 EU (MiFID II).

paragraph»[54]. It is important to underline that the paragraph highlights the direct correlation between the correct functioning of HFT systems and the market price stability[55]. For this reason, it imposes to HFT firms to set effective and suitable systems and risk controls, whose requirements are set out in detail in the ESMA complementary regulatory technical standard 6 (RTS 6). RTS 6 contains different dispositions focusing on «the organisational requirements of investment firms engaged in algorithmic trading», including those related to the resilience of trading systems of these firms[56]. These dispositions establish that HFT firms must comply with the MiFID discipline carrying out the following activities: (a) testing the algorithms, (b) monitoring and, where necessary, changing the algorithms used, (c) annual stress testing, (d) incorporating a kill functionality so that all resting orders can be cancelled in the event of an emergency, (e) monitoring for the prevention and identification of potential market abuse, (f) carrying out pre-trade controls on order entry, (g) carrying out post-trade controls[57]. In addition, RTS 6 imposes on HFT firms to self-assess the specific organizational requirements regarding the minimum required parameters set out in the regulation itself[58].

---

[54] Similarly, in the USA, the new Rule15c3-5 under the Securities and Exchange Act of 1934 identifies a risk governance framework for brokers or dealers with market access. The rule states that « (b) A broker or dealer with market access, or that provides a customer or any other person with access to an exchange or alternative trading system through use of its market participant identifier or otherwise, shall establish, document, and maintain a system of risk management controls and supervisory procedures reasonably designed to manage the financial, regulatory, and other risks of this business activity. Such broker or dealer shall preserve a copy of its supervisory procedures and a written description of its risk management controls as part of its books and records […]. (c) The risk management controls and supervisory procedures required by paragraph (b) of this section shall include the following elements: (1) Financial risk management controls and supervisory procedures. The risk management controls and supervisory procedures shall be reasonably designed to systematically limit the financial exposure of the broker or dealer that could arise as a result of market access, including being reasonably designed to: (i) Prevent the entry of orders that exceed appropriate pre-set credit or capital thresholds in the aggregate for each customer and the broker or dealer and, where appropriate, more finely-tuned by sector, security, or otherwise by rejecting orders if such orders would exceed the applicable credit or capital thresholds; and (ii) Prevent the entry of erroneous orders, by rejecting orders that exceed appropriate price or size parameters, on an order-by-order basis or over a short period of time, or that indicate duplicative orders. […]».

[55] Likewise, see D. BUSCH, *MiFID II: regulating high frequency trading, other forms of algorithmic trading and direct electronic market access*, in *Law and Financial Markets Review*, 10:2, 2016, 73, balancing the benefits and risks of flash trading and other forms of algorithmic trading. The Author explains that MiFID II considers this technology beneficial for market and market participants (due to, for example, wider participation in markets, increased liquidity, narrower spreads, reduced short-term volatility and better execution of orders for clients) but also a source of potential risks, including those of «algorithmic trading generating duplicative or erroneous orders or otherwise malfunctioning in a way that may create a disorderly market».

[56] See EUROPEAN SECURITIES AND MARKETS AUTHORITY, *Regulatory Technical and Implementing Standards - Annex I MiFID II/MiFIR*, in *www.esma.europa.eu*, 2015, 201 and D. BUSCH, note 55, 76.

[57] D. BUSCH, note 55, 76.

[58] EUROPEAN SECURITIES AND MARKETS AUTHORITY, note 56, 203 (11).

As it can be easily seen, EU HFT discipline stresses the importance of well-articulated internal risk governance models that can ensure the resiliency of the systems, to assure that algorithms work properly, and investment orders are executed correctly. By doing this, both dispositions get one of the essential traits of software-based technologies, that is the necessity algorithms and software programs are constantly tested - before and while their adoption. Moreover, they mirror a new major trend of our software-driven societies, in which testing rooms (or, technically speaking, "sandboxes") have been becoming increasingly important elements to safeguard not only the resiliency of high-digitalized and complex systems but also the stability of human organizations[59].

Thus, testing is becoming increasingly important also in finance, in which risks must be never underestimated or easy managed[60]. If in the past this could appear crystal clear for some risks (especially credit, market and liquidity risks), nowadays neither must be done with those regarding new digital technologies with high destabilizing potentiality, like "smart contracts". Indeed, their failure or mis-execution could reveal a real threat for financial players and, more generally, for the stability of financial markets[61]. Therefore, due to its attention to «effective

[59] In computer sciences, the term "sandbox" refers to «a type of software testing environment that enables the isolated execution of software or programs for independent evaluation, monitoring or testing» (see *www.techopedia.com*).
An enlightening prove of how software-related concepts are affecting our traditional mind-set is the regulatory strategy innovation, specifically addressing FinTech, known as "regulatory sandbox" (that some countries have already set up or are going to. For a detailed review of which countries are orientating their regulatory efforts of FinTech towards "regulatory sandbox" solutions see D. W. ARNER, J. BARBERIS, R. P. BUCKLEY, note 2, 45 and following and E. VERMEULEN, M. FENWICK, W. A. KAAL, *Regulation Tomorrow: What Happens when Technology is Faster than the Law?*, in *TILEC Discussion Paper*, October 2016, 27). More specifically, the UK Financial Conduct Authority defines the "regulatory sandbox" as «a "safe space" in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question» (see FINANCIAL CONDUCT AUTHORITY, *Regulatory sandbox*, in *www.fca.org.uk*, November 2015, 1). To E. VERMEULEN, M. FENWICK, W. A. KAAL the "regulatory sandbox" is one of the principles of a new proactive, dynamic and responsive regulation able to balance the need to foster innovation in a cost-efficient environment and to limit the downsides for consumers. The Authors highlight that the most interesting aspect of "regulatory sandboxes" is the idea of testing in a «"live" environment» where technological developments are open to discussion and democratic supervision and control.
[60] Although this might be considered banal, it cannot be taken for granted. One of the major lessons of the Global Financial Crisis is that risk-underestimation is very common in finance. In fact, it is now well known that, in the years before the financial turmoil, even the most consolidated financial institutions were prone to underestimate risks related to high-engineered financial securities (such as CDOs) and did not have adequate, firm-wide consolidated understanding of the risk factor sensitivities. For example, regarding the American TBTF bank Citigroup T. F. GEITHNER, note 50, 135 states that the FRBNY «supervisors always considered it a laggard in risk management».
[61] This is reported also by important MIT computer scientists like David Shrier, Deven Sharma and Alex Pentland. Indeed in D. SHRIER, A. PENTLAND, *Frontiers of Financial Technology: Expeditions in future commerce, from blockchain and digital banking to prediction markets and beyond*, Visionary Future, 2016, 25 the Authors write that «[i]n strategic discussions with regulators, [they] were invited to contemplate not only the positive potential of blockchain, but also the inverse, where

systems and risk controls», HFT regulation must be considered good grounds to step towards a legal framework specifically addressing blockchain-oriented financial institutions[62] and leads to think about internal risk governance models for "smart contracts" as well.

Of course, blockchain platforms create distributed networks; consequently, the distinction between internal effective systems and risk controls and those regarding the network itself might be a little more indefinite. However, it is reasonable to think that each financial institution belonging to the network should provide its internal governance model with a testing room (a "sandbox", more precisely) in which specific systems and risk controls for "smart contracts" can be fully realized. It is thought that within these "internal sandboxes", "smart contracts" can be carefully tested and monitored through appropriate systems[63]. For example, both contracting financial institutions can double-check the translation of their legal agreements into the software language, work on the codes of "smart contracts" and freely modify them in a safe environment before their final execution on blockchain platforms[64].

"Internal sandboxes" for "smart contracts" are considered both cost-efficient for contracting financial institutions and highly beneficial for the market.

---

the promise of blockchain failed to materialize» and invite to «imagine a world where five of the largest banks collapse due to coding errors that result in hundreds of thousands of smart contracts mis-executing. It's possible […] shifting the decimal a few places to the right could have a systemic impact on the global financial system». As clearly pointed out by these words, although the risks might be close to any other IT system currently used in financial markets, "smart contracts" emphasize the reasoning on operational risks because of the unimaginable number that might be executed throughout future global blockchain financial networks. From the regulators' point of view, correspondingly, EUROPEAN SECURITIES AND MARKETS AUTHORITY, *Report - The Distributed Ledger Technology Applied to Securities Markets*, in *www.esma.europa.eu*, February 2017, 12 stresses that «a mistake in the coding of smart contracts or reference data might affect a greater number of participants, not to forget the additional time that might be needed to correct a mistake once identified. Similarly, a glitch or failure might have wide consequences with DLT as many parties would share the same tools».

[62] This is what also P. PAECH, note 51, 26 thinks when he writes that «there is a need to assess blockchain financial networks and the potential of smart contracts in the light of rules addressing flash crashes and algorithmic trading».

[63] Along these lines see also ISDA, LINKLATERS, note 36, 17, regarding the following questions: «"how do I know the effect of the code, when executed by a machine, will be what I intend?" In other words, what if there is a glitch somewhere in or between the high-level programming language and the executable machine code that means the code does not do what it was intended to do when executed? What if the high-level programming language coding was accurate in the sense that it was written in the way that should have produced a given effect, but something has gone wrong somewhere down the line?» Here is the answer: «To help guard against this, simulations can be run to observe whether the code produces the expected outputs». To mitigate the realization and dissemination of errors also EUROPEAN SECURITIES AND MARKETS AUTHORITY, note 61, 12 highlights the necessity that «a number of checks [must be] implemented».

[64] Indeed, it is worthy thinking that, during the "internal sandbox" the execution of dumb contracts is suspended and that the only obligation arising from the contract that binds parties is coding it and engaging the following testing activities.

Indeed, the former can develop correct and resilient "smart contracts", avoiding the (not easy) task to try to interrupt the software execution when huge amount of money is already involved. The latter is better safeguarded from the risks that dangerous glitches or bugs are discovered when "smart contracts" are already operating among financial players. Consequently, technology breakdowns can be prevented more frequently, capital shortfalls avoided, and the stability of financial markets better preserved.

Lastly, of course, the need that financial institutions are provided with "internal sandboxes" specifically addressing "smart contracts" must be further stressed for those markets in which both manias and panics can easily spread (including the already mentioned repo markets)[65], due to the inevitable interaction between two financial layers of fragility: high short-term liabilities (that inevitably expose debtors to "bank-runs") and articulated interconnections within the financial players. Indeed, although their benefits, blockchain and "smart contracts" add a new fragility layer to such markets, that is immutable automation and its correlated effects, (such as the increase of herding behaviours and the consequential rise of still unknown risks pockets[66]). For sure, new and unstoppable drivers of financial instability must be averted; thus, counteracting measures specifically addressing "smart contracts" (like the here suggested "internal sandboxes" for financial institutions) become imperative. Otherwise, the risks that blockchain and "smart contracts" entail can turn out to be unmanageable and their downsides higher than the benefits they promise. But this is not what our financial markets are calling for.

[65] T. F. GEITHNER, note 50, 68.
[66] To further understand how the risks of these technologies can origin wider financial risk see also EUROPEAN SECURITIES AND MARKETS AUTHORITY, note 11, 18.