# JOURNAL

**THE CAPCO INSTITUTE** JOURNAL OF FINANCIAL TRANSFORMATION 04.2017 N°45

FinTech/RegTech

## From “Blockchain Hype” to a Real Business Case for Financial Markets

Massimo Morini

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

TRANSFORMATION

CAPCO

# EMPOWERING THE FINANCIAL WORLD

Pushing the pace of financial technology, we help our clients solve technology challenges for their business – whether it's capital markets in Mumbai or community banking in Macon.

We leverage knowledge and insights from our clients around the world:

**20,000** clients in towns everywhere are becoming more efficient, modern and scalable.

**27 billion** transactions processed help solve clients' challenges – big and small.

**$9 trillion** moved across the globe in a single year empowers our clients' communities to build storefronts, homes and careers.

**55,000** hearts and minds have joined forces to bring you greater capabilities in even the smallest places.

Empowering the Financial World

FISGLOBAL.COM

FIS

// JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

Recipient of the Apex Award for Publication Excellence

# Transformation

## FinTech/RegTech



## Investments



## Banking

# From "Blockchain Hype" to a Real Business Case for Financial Markets

**Massimo Morini** – Head of Interest Rate and Credit Models, IMI Bank - Intesa S.P. Group, and Professor of Fixed Income - Advanced Methods, Bocconi University[1]

**Abstract**

There has been a huge amount of coverage in the press about the great potential uses of bitcoin-related technology for financial markets, such as improvements in efficiency. In addition to the supporters of blockchain, many have been critical of its real-life applications within the business world and suggest that what we are witnessing is nothing short of "blockchain hype," and that this technology can only be applied to bitcoins. This paper will demonstrate that there are real business cases for improving financial markets based on the lessons learned from cryptocurrencies, but, unlike what the hype-enthusiasts suggest, they are not application of a technology to the existing business models within financial markets. They are reforms of the business model itself. What needs to be exported from the world of cryptocurrencies are aspects of the market organization, inspiration for a different accounting and legal system, and some aspects of the technology. These can result in a huge contribution towards more robust, efficient, and stable markets. However, the process cannot be immediate and effortless, and can only be achieved within a market-wide strategic perspective. In this paper, I develop these concepts initially within a parallel analysis of cryptocurrencies and financial markets. Then, I will focus on a specific business case regarding the collateralization of financial derivatives, which will highlight quantifiable benefits in terms of reducing costs, capital, and risk. It is an example of a situation where the use of cryptocurrency technology is not more important than the business ideas developed in the analysis of cryptocurrencies; yet it was inconceivable prior to the advent of distributed ledgers, smart contracts, and oracles.

1 Fruitful conversation with Robert Sams, Giacomo Zucco, and Alex Lipton is gratefully acknowledged. The second part of this paper is just an extension of "Smart derivatives can cure XVA headaches," by Massimo Morini and Robert Sams, Risk Magazine, August 2015. I also thank all those – too many to be mentioned by name – that asked me the questions that form the backbone of this paper. This work expresses the views of its author and does not represent the opinion of his employers, who are not responsible for any use which may be made of its contents.

## INTRODUCTION: BLOCKCHAIN HYPE VERSUS BLOCKCHAIN SECLUSION?

There has been a huge amount of coverage in the press about the great potential uses of bitcoin-related technology for financial markets, such as improvements in efficiency. In addition to the supporters of blockchain, many have been critical of its real-life applications within the business world and suggest that what we are witnessing is nothing short of "blockchain hype," and that this technology can only be applied to bitcoins.

This paper will demonstrate that there are real business cases for improving financial markets based on the lessons learned from cryptocurrencies, but, unlike what the hype-enthusiasts suggest, they are not application of a technology to the existing business models within financial markets. They are reforms of the business model itself. What needs to be exported from the world of cryptocurrencies are aspects of the market organization, inspiration for a different accounting and legal system, and some aspects of the technology. These can result in a huge contribution towards more robust, efficient, and stable markets. However, the process cannot be immediate and effortless, and can only be achieved within a market-wide strategic perspective.

One crucial misunderstanding here is the idea that blockchain technology can be exported to financial markets "as they are" to make them more efficient. This is meaningless, since blockchain technology was created to change some trust-based business processes to make them less reliant on trust. Without structural changes, the best of blockchain technology is lost and we are left with the inefficiencies.

It should be added that suggesting that blockchain technology cannot be used outside of the bitcoin world is also incorrect. Bitcoin was created to create a level of independence from trust sufficient to allow players to be anonymous and do so without any legal protection. Other business solutions based on a level of trust intermediate between bitcoin and traditional finance can use similar technology and yet be very different from bitcoins. But we must ready to use the concept of trust in a totally different manner, as a way to analyze the different parts of a business process and the reasons for its current inefficiencies and risks.

In the next section, I will develop these concepts initially within a parallel analysis of cryptocurrencies and financial markets. Then I will focus on a specific business case regarding the collateralization of financial derivatives, which will highlight quantifiable benefits in terms of reducing costs, capital, and risk. It is an example of a situation where the use of cryptocurrency technology is not more important than the business ideas developed in the analysis of cryptocurrencies; yet it was inconceivable prior to the advent of distributed ledgers, smart contracts, and oracles. In fact, it was first presented in Morini and Sams (2015), in an introduction to the blockchain innovation for the derivatives world.

## THE MISUNDERSTANDING ABOUT "TRUST"

Notice that the term "trust" is often used in the bitcoin debate in a radical way, moving from a totally trustless anarchist model to a cooperative model based on absolute trust. None of them really exists. Even bitcoin has created peculiar elements of trust in some players, like a stable group of core developers or miners. And, financial markets have never been based on absolute trust in counterparties or central bodies. The radicalism of the debate has hidden the fact that different business models are associated with different levels of trust. Trust can be hidden in many passages in the working of a market, and can be eliminated or reduced in some without disappearing from others. More than a generic term for ideological debate, trust can be used as a precise concept to understand the features of a business model, and how that model can be positively reformed; without forgetting that any removal of trust creates some form of disintermediation, of some institutions or of some functions within institutions, and in this way it requires changes to the business model, and often to the legal, regulatory, and accounting frameworks.

An example of an unnecessary element of trust is the reliance on the agreement between two counterparties about the exact representation of a deal without any automation enforcing this agreement, not even in critical cases. Many markets are still crippled by this feature. This can be addressed with elements of distributed automation similar to those seen in cryptocurrencies.

## WHAT ARE THE PROBLEMS OF FINANCIAL MARKETS THAT WE WANT TO SOLVE?

Financial market transactions are still based on the logic of "consensus-by-reconciliation." Every player gives its own representation of a transaction in its own accounting systems (ledger) and its own IT systems. The only proof that this representation is correct is coincidence with the representation given by the counterparties. The confidence in the legal validity of the contract in all its aspects is crucially dependent on trust in this coincidence, which in practice needs to be verified more than once. This verification requires a number of steps, such as confirmation, affirmation, communication to central bodies, and other reconciliation passages along clearing and settlement.

This is an objective bottle-neck towards more efficient and reliable markets. Current reconciliation steps slow the process down, even if the technology enables very fast communication. They also drive up costs.

Furthermore, the need for this kind of reconciliation leaves open the risk of disagreement and litigation, making the process uncertain and increasing the capital requirements for members. It is a system intrinsically inefficient that has not been seriously reformed in decades, for lack of incentives and no visibility of a technological and organizational stack suitable for a change. Even if many bits of the fundamental technology to solve it were already available in the past decades, just think of the internet giving a shared information platform, this had never been applied to changing the foundations of some transactions. Now there is visibility of a different business model in the cryptocurrency example, together with a full technology package enabling it.

## WHAT EXACTLY ARE THE SOLUTIONS THAT MAY COME OUT OF THE BITCOIN EXPERIENCE?

Bitcoin and the other experiments of cryptocurrencies or crypto-transactions are based on a single accounting and reporting system, a distributed ledger (DL). With a DL, the reconciliation bottleneck is avoided since there is a consensus algorithm that verifies transactions and gives to them a unique representation on the ledger, collapsing all reconciliation steps into a a single initial passage. Further reconciliation steps are unnecessary when there is a single authoritative deal representation for all the parties. It is this business model that makes transactions so fast for bitcoins, more generally than any specific piece of technology. This insight is useful for the use of ledgers in financial markets too, even if financial players may need DLs that are different from the blockchain, which is a peculiar implementation where all transactions are reported together, visible to all, and their time-order is defined through a sequence of blocks.

For advanced financial markets, distributed consensus can be applied also to a deal made up of many payments, like a derivative or a bond, through the concept of a Smart Contract, which is a piece of program code, in a given computer language, executing the transaction agreed at inception between the parties. This guarantees the enforcement of consensus, namely that the deal will follow the agreement taken at inception between the parties. Bitcoin has only basic smart contracts, but other cryptocurrencies like Ethereum have smart contracts written in a Turing-complete language, which means it can do everything that a normal computer does.

Notice that this is a further step towards a different and more advanced model of the market. Not only do the accounting/reporting of the transaction move from individual representation to an authoritative distributed representation, but also the contract stops being two pieces of papers to be implemented and represented in separate ways but becomes a unique manager of the transaction signed (cryptographically) by the interested parties. Financial contracts are already translated by parties into software running on IT systems. What was missing were working examples of a technology where the piece of code could become the contract itself and not one of the many representations of it given by the parties. When the unique smart contract signed by the parties manages directly the flow of the transaction, there is a further reduction of delays and risks of disagreements and misalignments.

## BUT ALL THESE GOALS CAN BE OBTAINED JUST VIA A CENTRAL DATABASE AND COMPUTING GRID ON ONE SERVER

For many of the above goals, the answer is: of course. But a computer/database shared among all the players of a market is a centralized solution, with all the well-known limits of centralization. These limits are a central topic in the state machine replication approach: centralized systems are usually more efficient from a technological point of view, but they are not fault-tolerant. In abstract terms, this means that failure of the central server is failure of the entire system. In economic terms, this unpleasant fact has additional consequences. In case of centralization, there will be an administrator of the database/hardware, and this institution would bear a great operational risk, the risk of the entire network, thus demanding an equally great power on controlling and unilaterally changing the rules. Centralized solutions create monopolies that drive the business costs up because the monopolist does not have the right incentives to contain them. Additionally, in finance centralized solutions also generate a concentration of financial risk that drives up – correctly – both the regulatory burden and the amount of risk-management provisions, such as collateral.

A centralized database also raises the likelihood of legal disputes; it would be easy to accuse the administrator of tampering with the ledger. Since the ledger must report the situation of everyone and yet belong to no one, a DL appears a more natural solution. It avoids the need for a central body and also reduces the legal uncertainties. The ledger downloaded by one party is the official ledger as much as the version downloaded by someone else. They are all replications of the ledger, there is not one central database and many duplications, which is a lays the groundwork for uncertainty, reconciliation delays, and legal disputes.

## AND WHAT IF THE DATABASE WAS "FULLY REPLICATED AND DISTRIBUTED"?

The technology of "distributed services" (DS) (and the state machine replication approach) that developed in the last decades are certainly a crucial part of the solution. There exist database technologies that try to keep away from the risks of centralization and predate DL technology. One can find works on fully replicated distributed databases that date back to the early 1990s, such as the evolution of the technology that has helped bring about well-known distributed solutions like DVCS (distributed version control systems), of which Linus Torvalds' Git is the best known.

The bitcoin blockchain evolved in the same stream of technological advances, partially based on the same cryptographic solutions. It is a relevant example of radical economic application of this form of technology, and in this way it showed how this technology applied logically to a market brings about a fundamental change in market organization.

Bitcoin found a decentralized solution for chronological tracking and time-stamping that was suitable for its peculiar context of building a market from scratch based on pseudonymous players. Even if this solution cannot be exported rigidly to different contexts, like current and foreseeable financial markets, blockchain is the natural turning point of distributed technology to take inspiration from when building DLs for financial markets, without ideological distinctions between distributed ledgers with blocks and proof-of-work, and distributed ledgers that may be different in these respects. An additional reason to keep more than an eye on blockchain in evolving existing financial markets is to keep a standard compatible with other DL solutions that have different privacy and validation requirements, cryptocurrencies included.

## WOULD THE CURRENT TECHNOLOGY FOR DLS BE READY TO PROVIDE THIS?

No. First of all, there is a scalability issue. The logic of distributed consensus across the entire network limits the amount of transactions that can be managed in a block. Solutions can exist for financial markets, but they are not tested yet.

Furthermore, the most tested market, bitcoin, has only basic smart contracts. Large-scale application of smart contracts is exactly the test that DLs for financial markets need to perform.

Finally, neither bitcoin nor other solutions like Ethereum have a focus on privacy and identity, as needed for financial markets. Identity is an unavoidable issue for any legal recognition. Privacy is a concept that is evolving in financial markets, with regulators demanding increasing transparency. These privacy challenges might be solvable with solutions such as complex data-encryption, interlinked bilateral ledgers, or regulated exploiting of pseudonymity. However, it should be noted that these are all elements that prove that the process will take time.

## SO FAR ONLY THE LEDGER, THE BLOCKCHAIN, IS USED FROM THE BITCOIN STACK. WHAT ELSE IS USEFUL?

In bitcoin there is also a fundamental use of cryptographic techniques, such as asymmetric cryptography and hashing, both for ledger management and inside the incentive/selection method called proof-of-work. Asymmetric public-private key cryptography is important also for extension to financial markets, as it is already in many fields. This form of cryptography can be used to eliminate a level of intermediation, for example bitcoin use it to disintermediate the role of banks as providers of cash deposits. In financial markets, the main players, including banks, have a different role as structurers, traders, issuers of deals and securities, lenders, and managers of credit and market risks. There is less fear of cryptographic disintermediation here, since the layers that can be eliminated or disintermediated in financial markets with no loss of security and a gain of efficiency and transparency are mostly not banks or their business counterparties.

Furthermore, cryptography may enable both identity and privacy at the same time. Other applications of cryptography are emerging now. For example, the use of cryptography by Oraclize[2] is interesting. They apply cryptography in order to provide a cryptographic guarantee that an operation has been executed. It is a way to enforce a contract with a computer or website and being guaranteed the contract has been executed exactly. That is another bit of technology, related to the concept of Oracles, that was developed around blockchain even if it is not part of it. This can be used, for example, to secure the process of importing data from outside the DL for internal use, something very common in financial markets. Excessive reliance on trust here would create a single point of failure outside the control of those that have a stake on the ledger. A similar logic is also behind the Intel Software Guard Extensions,[3] with the additional feature that the logic is embedded in the hardware itself and not only in the software.

## IS PROOF-OF-WORK TO BE EXPORTED TO FINANCIAL MARKETS?

Proof-of-work, as we see it in bitcoins, may not be applicable to financial market because it is designed to solve a specific problem: finding a way to make players update the blockchain in an honest way even if they are not forced to either by a reputation incentive (because they can be anonymous) or by any legal framework. This is a very extreme concept of disintermediation and lack of trust that does not apply in a context where players are not anonymous and where fraud is legally prosecuted. This is an important reason why proof-of-work might not be used in advanced financial markets: the core motivation for its use is missing.

But there is another reason why it makes sense for us to look at proof-of-work in more detail. The clever idea behind the mechanism is that it requires the participants that wish to receive remuneration for updating the blockchain (miners) to solve a complex computational problem. This forces them to make an off-ledger investment in energy and computational power that makes it uneconomical to fraud the system. In fact, double spending is the only fraud that miners could implement easily in bitcoins, since asymmetric cryptography and the public ledger protects, in its own peculiar way, past transactions and possessions. The loss of credibility of the network coming from a fraud would be, for those who have made the off-ledger investment in energy and computational power, greater than the easy gain from double spending. It is important here to understand a practical point not enough stated in theoretical analyses: that the investment in computational power is dominant over the investment in energy, and that the former is more relevant also because it is a long-lasting one. Mining technology is very expensive and difficult to reuse for other purposes. This is crucial in helping explain why it makes frauds uneconomical, and also why alternatives like proof-of-stake did not work: they did not guarantee an off-chain, long-lasting, capital investment.

Retruning to today's financial markets, it should be stated that while proof-of-work is not a waste of resources in bitcoin, since it is the only off-chain long-lasting investment of the crucial players, in financial markets it would be a real waste since the existence of off-chain economic commitment for crucial players is already proved; they already have a strong incentive to maintain the credibility of the whole financial system. This state of affairs may not last for ever, but it is the reality we start from.

## SO, SHOULD TRANSACTION VISIBILITY AND VALIDATION BE LEFT TO THE COUNTERPARTIES ONLY?

In principle, a basic extension of the current reality is a consensus algorithm where only the two parties involved sign the smart contract and validate the transaction, potentially on a private DL. This is already an improvement in terms of efficiency and finality of financial markets, removing some of the need for reconciliation and the risk of litigation. Considering also that currently visibility and some aspects of validation of a trade would involve a number of regulators, introducing a role for reliable third parties, this could be sufficient for most goals of the practical business case described.

Yet, it would be shortsighted to depart from the cryptocurrency experience to such an extent as to use a bilateral solution. The business case described below would work easily, from a technological point of view, in a multilateral public blockchain. From a financial point of view, a multilateral setting would pose some issues, but there are also many services benefiting from multilateral reliable and efficient distributed transaction validation and recording. For example, in some extensions of the business case described below, collateral may be provided or guaranteed by a third party. In this case, consensus, speed,

2 http://bit.ly/2mdCJ0M
3 http://intel.ly/2k9mUYr

and transparency, like those allowed by a multiplayer ledger, are particularly useful. Other examples are the use of the techniques for compression of exposures that are possible on a network, see, for example, TriOptima,[4] or the possibility to give regulators a broader and deeper vision of the market.

This can lead to a range of possible consensus algorithms, not excluding something more similar to what we have seen for cryptocurrencies. In fact, we can add that the validation algorithm used in the bitcoin world is mainly required to avoid double spending. This possibility might seem to be of marginal importance in financial markets with trusted, or at least known, members. But, in fact, the same economic problems take on a different appearance. Double spending, or spending of non-existing resources, also takes place in financial markets too and is considered the main risk by market participants and regulators: except that its called default.

Default risk is where we clearly see that trust is not unlimited in financial markets. Financial markets are made up of trustworthy parties, but none is completely riskless, since even the largest institutions/governments can default, as history shows.[5] And, default is by definition a form of double spending, where a counterparty undertakes commitments that are greater than the funds they actually have available. Thus, thinking of methods for assessing fund availability within the network, beyond pure unilateral confirmation, is relevant, and this may support the case for more advanced validation, involving regulators or custodians or some other players not directly related to the transaction.

But a similar business case is still out-of-sight. Still difficult, but nearer, are solutions to some credit-related issues that can be solved using some aspects of the DL model that we discussed above, and that are robust enough for different choices about consensus and ledger visibility.

## OK. CAN WE MOVE FROM GENERAL PROBLEMS TO A SPECIFIC ONE?

It is about time. Simply saying that a business reform might eliminate reconciliation or make settlement faster is not enough. There can be cases in which reconciliation steps are a real business need or faster settlement is prevented by regulators for good reasons. One also needs to demonstrate business cases for when these sorts of worries are outweighed by the risk and cost savings coming from less reconciliation and faster settlement.

As seen in Morini and Sams (2015)[6] and later in AssiomForex,[7] a relevant case concerns collateral and default management in the derivatives market, a market 7-8 times the GDP of the world in notional terms, and as large as the U.S. GDP or the global bond market in terms of value.

Credit risk is a central issue for over-the-counter (not listed) derivatives, which are the dominant part of the market. The issue reached dramatic levels after the financial crisis started in 2008. The Lehman Brothers' default marked a crucial change in the derivatives markets. From an aggressive market with high leverage, little attention to risk, and a disordered multiplication of complex payoffs, we moved to a market with strong standardization, heavy regulations, and potentially excessive attention to risks. This has made the financial world a safer place from the perspectives of many, but certain negative side effects are also becoming clear. Firstly, derivatives users, such as funds and corporates, are increasingly unhappy with a market in which prices do not express the intrinsic market risk of a financial product (interest rate risk, commodity risk, etc.), but are skewed by charges that are more or less related to default risk.

This includes credit valuation adjustment (CVA), a valuation adjustment made by financial dealers for the risk of default by banks' counterparties, an adjustment called FVA (funding value adjustment), which accounts for the funding cost of banks, which increased when the banks' default risk increased, and KVA (capital value adjustment), an adjustment for the amount of extra capital that banks need to hold to account for the increased default risk. Additional costs to users of derivatives come from the recent increase of the margin requirements for market players (these are part of funding costs and generate another value adjustment, the MVA (margin value adjustment), which is also in response to increased default risk).

Buy-side clients still need financial markets and derivatives for their investment and diversification needs, as well as for hedging their costs and risks, in terms of cashflows and from an accounting perspective. For these clients, the above transformation meant a sharp increase in costs.

4 http://bit.ly/2ldvcPE
5 Defaults by the likes of Latin American governments, Enron and Parmalat, and partially Lehman, illustrate this fact clearly.
6 Morini, M., and R. Sams, 2015, "'Smart' derivatives can cure XVA headaches," Risk Magazine, August 27, http://bit.ly/2mf2XjB
7 http://bit.ly/2mVzJU2

## IN THE CURRENT MARKET SITUATION, WHAT IS USED TO REDUCE CREDIT RISK? COLLATERAL?

The mainstream approach for reducing the size of these charges is to mitigate the losses in case of default, of banks or their counterparties, through collateralization.

Collateral for derivatives comes in two forms. First, we have the variation margin, which requires that the derivative is revaluated every day by party A using its pricing model $f^A$. It takes as input the current value $M_t^A$ of the relevant market variables from the info provider chosen by A, and gives current derivative value $V_t^A = f^A(M_t^A)$

If $V_t^A$ is negative for A, which means that A expects to pay to party B in the transaction more than what it will receive, so that A is a net debtor, A will ensure that an amount in cash (and sometimes using other assets, bonds or equities, with a haircut rule) equal to $V_t^A$ is available for counterparty B in a collateral account. Party B does the same thing but with its model $f^B$ and its data $M_t^B$. Hopefully $V_t^A \approx -V_t^B$ and the process proceeds smoothly. When there is a remarkable difference between $V_t^A$ and $-V_t^B$, the two counterparties talk to each other for a reconciliation. In some cases, it is the net creditor that makes a margin call, but this does not change the general picture.

In many cases, particularly when a party is a non-financial corporate that has difficulties in moving cash quickly or computing quickly the right amount of collateral, this process of collateral update happens less often than daily. It may be that longer period is stated in the agreements, or that the agreements accept explicitly to leave a part of the exposure not collateralized (via defining thresholds or a minimum transfer amount). These are inferior variation margin agreements that contrast with the top-class agreements between banks, characterized by daily updates, no minimum transfer amounts, and zero threshold.

## IS THIS ALL WE NEED AS MARGIN? OR ADDITIONAL MARGIN, SUCH AS THE INITIAL MARGIN, CAN BE USEFUL?

Even in case of variation margin, there is always an expected delay between the last collateral update and the closeout for liquidation of a defaulting counterparty's positions, leaving risk of default still open. This delay is called "margin period of risk" (MPOR), and comes from combining the collateral frequency with the delay between default time and the computation of a closeout amount. The total delay is estimated to be rather large by regulators since, when a default happens, there is no guarantee that the valuation of the residual derivatives, $V_\tau^A$ and $-V_\tau^B$, with $\tau$ being the default time, coincide for the two parties. The current process assumes disagreement and potential litigation, and a reconciliation procedure driven by the liquidators that involve asking various third parties to give a valuation of the residual deal before arriving at a closeout amount. This pushes MPOR to range from 5 to 40 days.

Thus, on top of variation margin, there can be an additional amount of collateral called initial margin to cover the risks due to the length of the MPOR. In an initial margin agreement, counterparties use their risk models to make a conservative estimate (worst case scenario or Value at Risk computation) of the difference between the amount of collateral available at the beginning of the MPOR (last collateral update) and the actual default closeout amount computed at the end of MPOR (closeout day). This computation needs to take into account the impredictability of market movements along the MPOR and the uncertainties concerning how the closeout amount will be computed. Under a long MPOR, initial margin can be very high.

## IS THIS SOLUTION FULLY SATISFACTORY TO MARKET PLAYERS?

It has some very relevant limits.

1. First of all, collateral management is not, in the current market, so easy for non-financial players. Computing, finding, and moving the necessary margin liquidity can be an obstacle even for agreeing on the valuation margin procedure.
2. Secondly, even a top-cass variation margin procedure is tampered by uncertainty on the different valuation models, market data, computations, and accounting representations from the two parties, an uncertainty that can create misalignments and make the process never faster than daily.
3. Thirdly, the margin period of risk is very long. Combining collateral frequency and the period for the agreement on closeout can take as long as 10 days. It is a delay sufficiently long to result in high levels of credit risk and capital costs (KVA), even in the presence of VM.
4. Finally, initial margin on top of the variation margin can reduce these costs dramatically, but only at the cost of a fourth problem: setting up a conservative initial margin agreement is expensive. Initial margin stays in a secluded account and due to its size, which in turn depends on the length of the MPOR, drains a large amount of liquidity from institutions.

## ANY ADDITIONAL SOLUTION IN PLACE TOWARDS A REDUCTION OF CREDIT RISK? WHAT ABOUT CCPS?

One solution is trading through central counterparties (CCPs), which can reduce credit risk through trade compression. Consider a situation where bank A owes 100 to bank B, bank B owes 100 to C, C owes 100 to A. If all the players trade through a central counterparty, the three above payments cancel out with each other, reducing settlement and credit risk.

CCPs do something even more important beyond compression. By pooling risks together, they reduce the size of potential losses through the netting effects. When a bank defaults, its obligations towards a counterparty are usually netted with those of the counterparty towards the bank. This reduces the closeout amount to be paid, thus reducing potential losses. When there is a unique counterparty like the CCP, this netting effect is stronger.

CCPs, however, are an intrinsically centralized solution. Centralization has the advantages just mentioned, but also symmetric disadvantages like creating a central institution whose default, however unlikely, would spread losses to the entire market at an unprecedented speed and scale[8,9]. This also means that the regulatory burden is particularly high on such institutions, also increasing collateral cost and demand, since a CCP is such a single point of failure that it needs to be massively overcollateralized.

We also have to remember that a centralized body lacks some of the competitive pressures to optimize collateral costs to members. Excessive collateral demand does worry regulators, since it can strain the market's liquidity conditions.

Finally, CCPs, as a natural corollary to this business, decide unilaterally the rules for variation and initial margins. The rules are also changed unilaterally quite often, particularly for Initial Margin.

## CAN WE THINK OF AN ALTERNATIVE OR COMPLEMENTARY SOLUTION WITHOUT THE COSTS OF CENTRALIZATION?

This is where DLs come into play, but they can be useful only if we are eager to take from cryptocurrencies not only some of the technology but also inspiration on how the process can be designed, making a change that needs to be technological, regulatory, legal, and organizational. DLs can be designed to be an independent solution, or a solution to be adopted by a body like a CCP, as long as the CCP is eager, while reducing some of the possible shortcomings seen above. In order to achieve that, it needs to change its own business model and decentralize some of the actions and decisions that now are centralized, while remaining the facilitator of the smooth working of the market, and a possible counterparty of last resort in times of crisis.

On the technology side, smart contracts suitable for derivatives can be implemented within a DL system if the consensus algorithm contains what is known as a Turing-complete state-transition function – for example, it must support if-then-else-branching, enabling the conditional features of a derivative to be executed.

A smart contract transaction might, for example, instruct the network to transfer: $\max(S_{1Y} - X, 0)$ from account A to account B a year from now, where $S_{1Y}$ is the price of a given security one year later, provided a certain sum – the value of the contract – is transferred from account B to account A of the distributed ledger now. This is a sketch of the implementation for a cash-settled call option.

Once knowledge of $S_{1Y}$ is provided in real time to the smart contract through an oracle managing access to trusted data providers, the contract can take care of the terminal settlement, transferring the right amount of money automatically. The smart contract can be much more detailed than the simple example provided above, incorporating more complex contractual features such as breakups, American exercise, legal requirements, and International Swaps and Derivatives Association standards. And the smart contract can take care of collateral regulation.

8 Gregory, J., 2014, Central counterparties: mandatory clearing and bilateral margin requirements for OTC derivatives, John Wiley & Sons, Ltd
9 Duffie, D., and H. Zhu, 2011, "Does a central clearing counterparty reduce counterparty risk?," Review of Asset Pricing Studies 1:1, 74-95

## WHAT ARE THE REAL SAVINGS OF SMART DERIVATIVE CONTRACTS ON A DL?

The main savings are seen when we consider collateral. The smart contract can include the implementation of a model that computes the amount of collateral to exchange, as a subroutine or from an external source communicating with the network through a precise, cryptographically signed agreement with the contract itself (an Oracle in the extended sense of Oraclize).

After the above reasoning, there is not much to say about which changes are brought about by a DL logic coupled with a smart contract that uses a single cryptographically secure implementation of a model.

All the uncertainties we have seen before are eliminated. There can be no differences because of the model, the data, the computation, or the accounting rules. The agreement was taken not on a generic paper contract, but on a single smart contract managing the quantification of the payments through a single model implementation, and recording the exchanges on a single ledger.

Since precise rules for collateral payments have been agreed and validated from the start on a DL, and then managed by a digital contract, the need for reconciliations and the risk of litigation are minimized. This reduces credit risk in two ways. Firstly, collateral can match exposures much more precisely than currently. Secondly, slashing the time required for reconciliation means that much faster collateral update becomes possible. Collateral exchange frequency can be reduced from the current 1-day delay to a fraction of an hour. This, eventually, makes collateral a real-time guarantee and eliminates problem 2) seen above.

Additionally, in an environment where transactions are naturally automated, and collateral is quantified and managed by the smart contract, problem 1) can also be reduced.

## BUT THIS MEANS COUNTERPARTIES SHOULD AGREE ON A VALUATION MODEL, MOVING FROM $f^A$, $f^B$ TO $f$

Extending the range of what is contractually agreed and validated at the beginning, reducing the scope for trust and future reconciliation, is a core point of this possible business evolution. It is the price to pay for efficiency, risk-reduction, and cost saving. But this specific price may not be seen as too high these days.

First of all, banks are already accepting, and in some cases they are even seeking, more consensus about models. Before the crisis, private valuation models were regularly used for complex payoffs, and valuation differences could be seen as drivers of value, as much as of risk. Today, the stress in regulations, margins, and credit risk has changed the picture, making risk the dominant effect, and valuation differences have already been minimized in many contexts. In the post-crisis years, regulations regarding CCPs have already led the market to accept external standardized valuations for margin purposes (initial and variation margin), and ISDA/IOSCO have led the market to agree on a common model for part of the margin (the initial margin), even for non-cleared products. However, this trend towards sharing calculation logic is not only regulations-led, and goes beyond the margins issue. Services, such as Markit Totem,[10] are used by banks to also indirectly reach a general consensus on the pricing logic of complex, non-cleared products, that have gained importance in recent years.

Secondly, what would happen on a DL is much less restrictive than the model standardization banks are already accepting. This is because it is in principle a bilateral agreement between the same parties that have just agreed on a price (valuation model at time zero) and on a future collateral exchange (valuation model in future times); they do not need to accept the one-size-fits-all model of current CCPs or regulatory intervention.

Finally, we get the majority of benefits even if the counterparties just agree on a valuation model for all those cases where valuation becomes a payment in the contract, like collateral regulation (and potentially anticipated closeout, a topic addressed below). If the ledger is used just as a transaction report but is not the only accounting report, players can be left free to keep private models for valuation in their own accounting systems, while binding them to smart contract agreement when valuation is used to quantify payments with the original counterparty. Misalignments between the private accounting valuation model and the agreed collateral valuation model already exist in dealing with CCPs.

10 http://bit.ly/2ldFYp4

## CAN WE DO SOMETHING MORE TO REDUCE CREDIT RISK IN COLLATERALIZED DERIVATIVES?

Faster and precise collateral would already reduce risks and associated costs, however, the full benefit would derive from extending the agreement on the revaluation model from collateral to default closeout. A mutually agreed valuation model can change the closeout process completely – reducing the MPOR to a few hours.

With collateral on a ledger, a missed collateral update (a default warning) is detected in real time, and can trigger the smart contract to terminate itself and provide immediately closeout valuation based on the agreed model. Suppose party B misses a collateral payment at t. We can agree on the smart contract that there is a grace period $\delta$, say $\delta$ = few hours, during which the contract waits for a collateral payment from B. At the end, the difference between deal value and collateral from A's point of view is computed with the agreed model $\Delta = f(M_{t+\delta}) - f(M_{t-\varepsilon})$, where $\varepsilon$ is the interval between two collateral payments, so that $t - \varepsilon$ is (conservatively) the time of the last collateral update. Party A becomes owner of the collateral, already in his/her possession, with only $\Delta$ to be paid by A to B if $\Delta < 0$ to A. Party B is left with the residual obligation, apart from $\Delta$ to be paid by B to A if $\Delta > 0$ to A.

In this way, the closeout amount is promptly computed in the network using the agreed bilateral model $f(M_{t+\delta})$, and the margin period of risk is slashed to the short $\varepsilon + \delta$ time, that can realistically be few hours, an order of magnitude smaller than the current MPOR of several days. The discrepancy between the last collateral update and the closeout amount, $\Delta$, will be as small as the change in few hours of a net present value, computed with a single model.

No longer will derivative users have to endure litigation and lengthy procedures involving multiple third parties to arrive at a closeout amount, solving problem 3) and reducing risk and associated regulatory capital. The gap $\Delta$ between collateral and close-out amounts can be reduced to much smaller levels. If we want to minimize even this risk, we can think of initial margin here too. It will have to cover $\Delta$, and will be much smaller than it is now, creating less strain on the liquidity of financial players, which solves problem 4).

## COULD FAST REACTION TO MISSED PAYMENTS CREATE MORE DEFAULTS FOR TEMPORARY LIQUIDITY PROBLEMS?

Not necessarily, because on a ledger we can reduce the gap between collateral and close-out amounts to levels sufficiently small to allow us to exclude "on-chain" default. A missed collateral payment can be treated as an unwinding that generates a small balance to be settled in the longer term, when temporary problems, if they were really the issue, will surely be over. Let us see how this can be done.

It is reasonable to worry that a market where everything is faster or more automatic creates more technical defaults, due to problems like a temporary lack of digital cash. But the procedure above for the case of a missed collateral payment need not be considered a default in the usual legal sense, since we can design it contractually. We increase the risk of "technical" defaults only if we ask B to pay $\Delta$ immediately after the grace period. However, since the payment is now determined by a precise contractual agreement and is likely to be small, being based on a MPOR of few hours rather than 10 days, we can postpone this payment to a later time, to allow the counterparty to get the necessary liquidity. Default in the legal sense is thus driven out of the ledger. If this happens, it will be driven by external reasons, and will affect the network only for the precomputed amount $\Delta$.

The participants will still be unhappy when a counterparty defaults and, for example, a hedge is lost. But, at least players now have as soon as possible as much cash as possible to

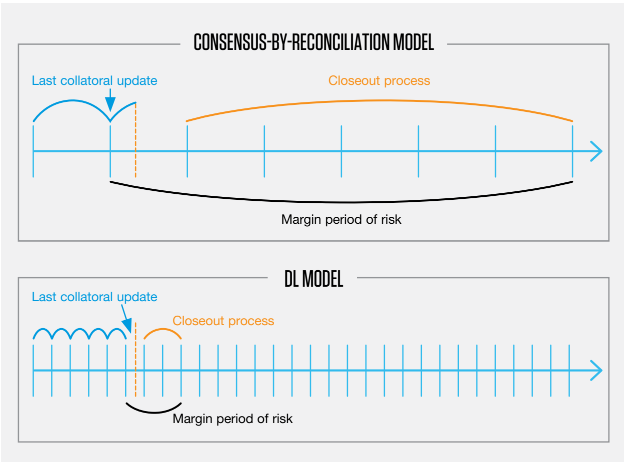


**Figure 1 – Margin period of risk**

find a new counterparty for the same deal. The long waiting times and discrepancies are cut out by design. The role of providing a counterparty in case of a crisis could be one of the roles that a CCP can take up if it reduces its direct exposure as counterparty of all trades in non-crisis times.

## IT SEEMS MANY THINGS HAVE TO CHANGE TO ALLOW THIS: NEW (SMART) CONTRACTS, NEW (DISTRIBUTED) ACCOUNTING…

A lot of things have been to be made consistent with such a framework, including the regulatory framework. We also need money with digital representation, which can be a digital currency fully convertible in central bank accounts, an independent cryptocurrency, or just one or more currencies issued by banks redeemable with fiat currencies or other assets. The first choice is preferable, the other two choices have their own limitations, such as too much market risk, or volatility risk, for current cryptocurrencies,[11] too much credit risk, or default risk, for banks' money. The network needs to receive a number of inputs from outside, such calendar changes, fixings, data for valuation, and potentially valuation from an external engine. The technology for communication between ledger and the external world is the technology of Oracles. Standard contract specifications, including ISDA standards, will have to be expressed as template code.

DL technology is the natural way to get the cost and risk savings seen above for derivatives, not only because they enable faster clearing and settlement, but more importantly because they require first to move the market logic towards putting the on-ledger smart contract at the center of the transaction, as opposed to the current approach based on two different implementations and two different reports of a paper contract.

Legal and regulatory status could come earlier than expected if regulators see advantages in an architecture that is more transparent and creates less risk than most of the current solutions. This is why I think it useful that we continue with the analysis of advanced business cases: to show the possible advantages for financial markets, and to clarify the hard, but necessary, journey, moving once and for all beyond the false dichotomy between "blockchain hype" and "blockchain seclusion."

11 Morini, M., 2014, "Inv/Sav wallets and the role of financial intermediaries in a digital currency," working paper, http://bit.ly/2ldUqh2

Layout, production and coordination:
Cypres – Daniel Brandt, Kris Van de Vijver and Pieter Vereertbrugghen

BANGALORE
BRATISLAVA
BRUSSELS
CHICAGO
DALLAS
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
KUALA LUMPUR
LONDON
NEW YORK
ORLANDO
PARIS
SINGAPORE
TORONTO
VIENNA
WASHINGTON D.C.
ZURICH

**CAPCO.COM**