Fintech Journey, Politecnico di Milano, 2017

Blockchain and Derivatives

Massimo Morini
Banca IMI
Head of Interest Rate and Credit Models
Coordinator of Model Research*

Bitcoin in a world of electronic payments and negative rates

- Why do we have negative rates? Why the players accept them?
- What about corporates and consumers? Why they do not keep all in banknotes? Banknotes have a cost of carry:
  - Storage & Security
  - Difficulty of Payment
- Today, the latter cost is particularly relevant: credit card payments, money transfer, even paypal…all electronic money requires a bank account!
- With **one exception**… cryptocurrencies like Bitcoin. Bitcoin is the first form of electronic money which is not a bank's liability.
- For Central Banks, that's easy: they create money, they want to stimulate consumption and investment. As for banks, they have no choice: they cannot keep everything in banknotes, their official liquidity is at the Central Bank.

Bitcoin in a world of electronic payments and negative rates

- BoE calls *broad money* the money held by households and companies. It is made up of bank deposits and banknotes, with **bank deposits representing 97% of the total**.
- And bank deposits are "**essentially IOUs from commercial banks to households and companies**".
- Investopedia: An IOU is an informal document that acknowledges a debt owed. IOU is an abbreviation, in phonetic terms, of "I owe you."
- Traditionally, banknotes are also considered essentially «IOUs from the central bank», that will redeem them just in case (in gold…).
- From the end of gold standard, banknotes do not fit any more in this meaning. But for bank deposits, this is an exact definition, as confirmed by the existence of a public partial guarantee (From 1 January 2016, the £75,000 limit will apply) when banks default and fail to pay deposits back.
- Bitcoin is first form of electronic money which is not a bank liability.

Conceptually, Bitcoin is web network equipped with:

- A public **Ledger** (or registry, or balance-sheet book) called **Blockchain** that reports a list of wallet indentifiers (*addresses*), each one associate to a number that says how many bitcoins are in each wallet. Wallets can be anonymous.

- A way to make **transactions**: to transfer money you broadcast to a network that the amount on your account should go down, and the amount on a receiver's account up. There are rules for transactions to be **valid**: you must put a *digital signature* in the message that allows everyone in the network to check that you are the owner of that wallet

- All these things must be maintained **without an administrator.** There is a procedure to make some players update the Blockchain after transactions; honesty depends on economic incentives.

- **Smart contracts**, like seen in **Ethereum**, allow the management of the transaction to be done by the network after agreeing on rules.

*

Blockchain Hype vs Blockchain Seclusion

- Some people in finance claimed that Blockchain Technology could be used to make finance faster, more efficient and more secure: "While the Bitcoin hype cycle has gone quiet, Silicon Valley and Wall Street are betting that the underlying technology behind it, the Blockchain, can change... well everything."

  Goldman Sachs, December 2015

- Many Bitcoin leaders answered to this that there is no real Blockchain application when there is «trust». Bitcoin leaders conclude that there are no Blockchain applications in finance other than Bitcoin itself, which is «trustless» finance.

- Let’s see through this…

*

References

Main references:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2760184

http://www.risk.net/risk-magazine/opinion/2422606/-smart-derivatives-can-cure-xva-headaches (with Robert Sams)

SPEEC

Keyno
Before
Decent

"If Allowe

April 12, 2

Introduct

Good morn

Before I be
the Commo
staff.

It is a pleas
currencies
technologi

Notwithsta
Rather, I w
That is the
may have
regulators

Lack of C

To begin, I
markets. A
rife about

I was on V
default sw
floor trying
exposure
the hour. It
that the CD

Now, let's
do not hav

It is not for
crisis was
CFTC, star
complete p
reporting p
impossibili
to recreate

BANKING • NEWS

Banca IMI Researcher: Blockchain Won't Work if Banks Don't Change

Pete Rizzo (@pete_rizzo_) | Published on April 13, 2016 at 16:40 BST

NEWS

The head of interest rate and credit models at Banca IMI, an investment banking and capital markets subsidiary of Intesa Sanpaolo, has penned a new paper on blockchain technology.

Dedicated to spotlighting "real business cases" for the technology, Massimo Morini's report argues that the lesson that should be learned from cryptocurrencies such as bitcoin is that traditional financial business model needs to be reformed, not just improved.

Morini writes:

> *"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; blockchain technology was created to change some trust-based business processes to make them less reliant on trust; without structural changes in*

FEATURES


Winklevoss Brothers Own 'Material' Amount of Ether


Global Expansion is Next

First Misunderstanding

- There are business cases for improving financial markets based on the lesson of cryptocurrencies, but **they are not *applications* of a technology**. They are *reforms*, inspired by cryptocurrencies, of **market organization, accounting and legal system, using some Blockchain technology**.

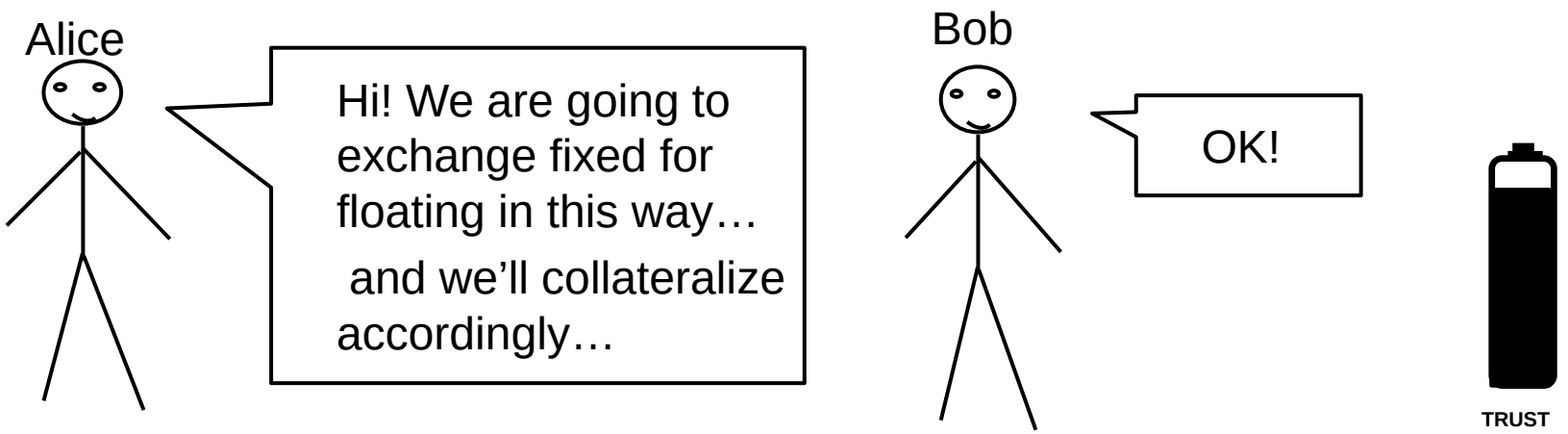
- Blockchain technology was created to **change some trust-based business processes to make them less reliant on trust**; without structural changes in this direction the best of Blockchain technology is lost and just the inefficiencies are left.

Second Misunderstanding

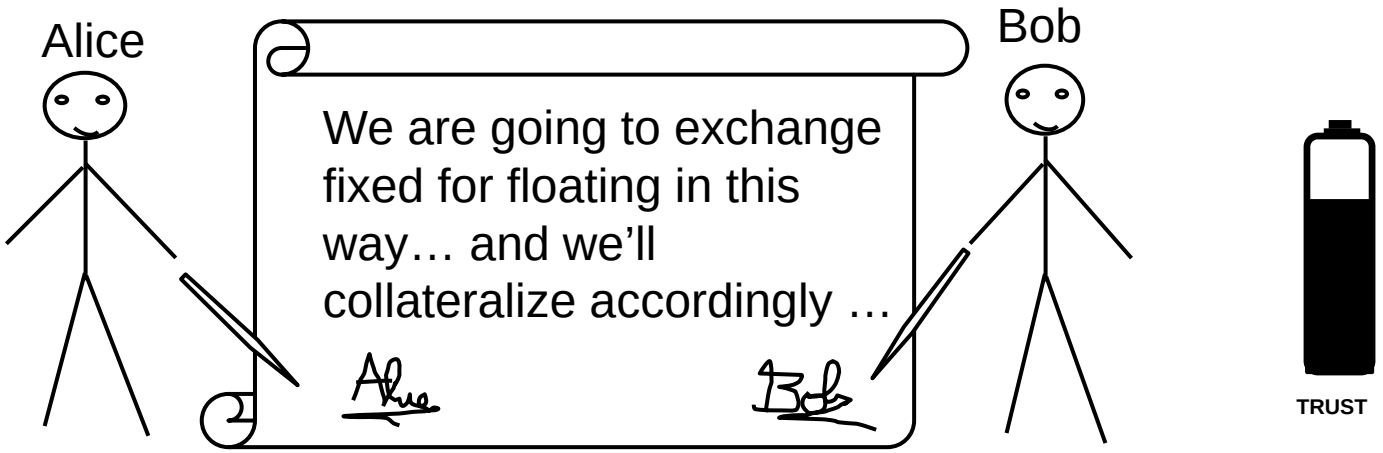
- The idea that Blockchain technology cannot be used outside the Bitcoin world is equally misguided: Bitcoin was created to attempt a level of independence from trust sufficient to allow players to be anonymous and without any legal protection. **Other business solutions based on a level of trust intermediate between Bitcoin and current financial markets can use similar technology and yet be very different from Bitcoins**.

- But we must use the concept of ***trust*** differently, as **a way to analyze the different parts of a business process and the reasons for its current inefficiencies and risks.**

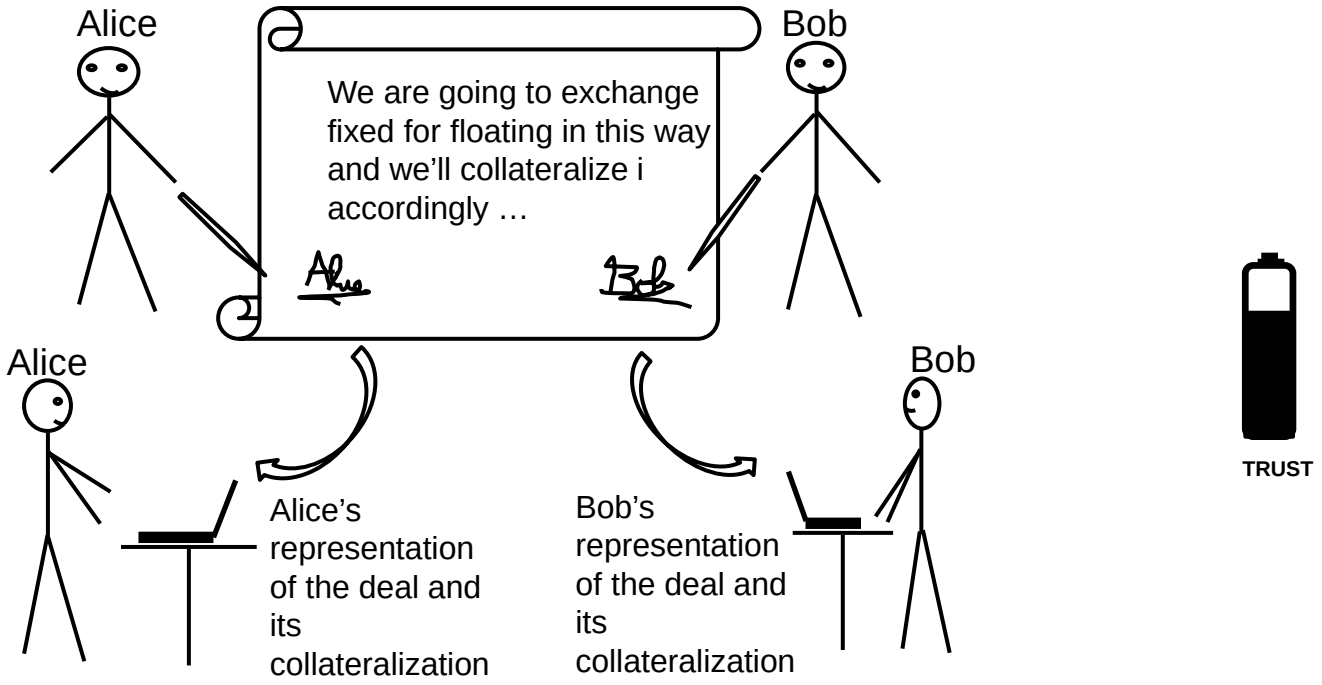
Different Levels of Trust



- A pure **«hand shake »** model is certainly characterized by a very high level of trust… current financial markets do something better, having **contracts, master agreements and CSAs protected by the law**…

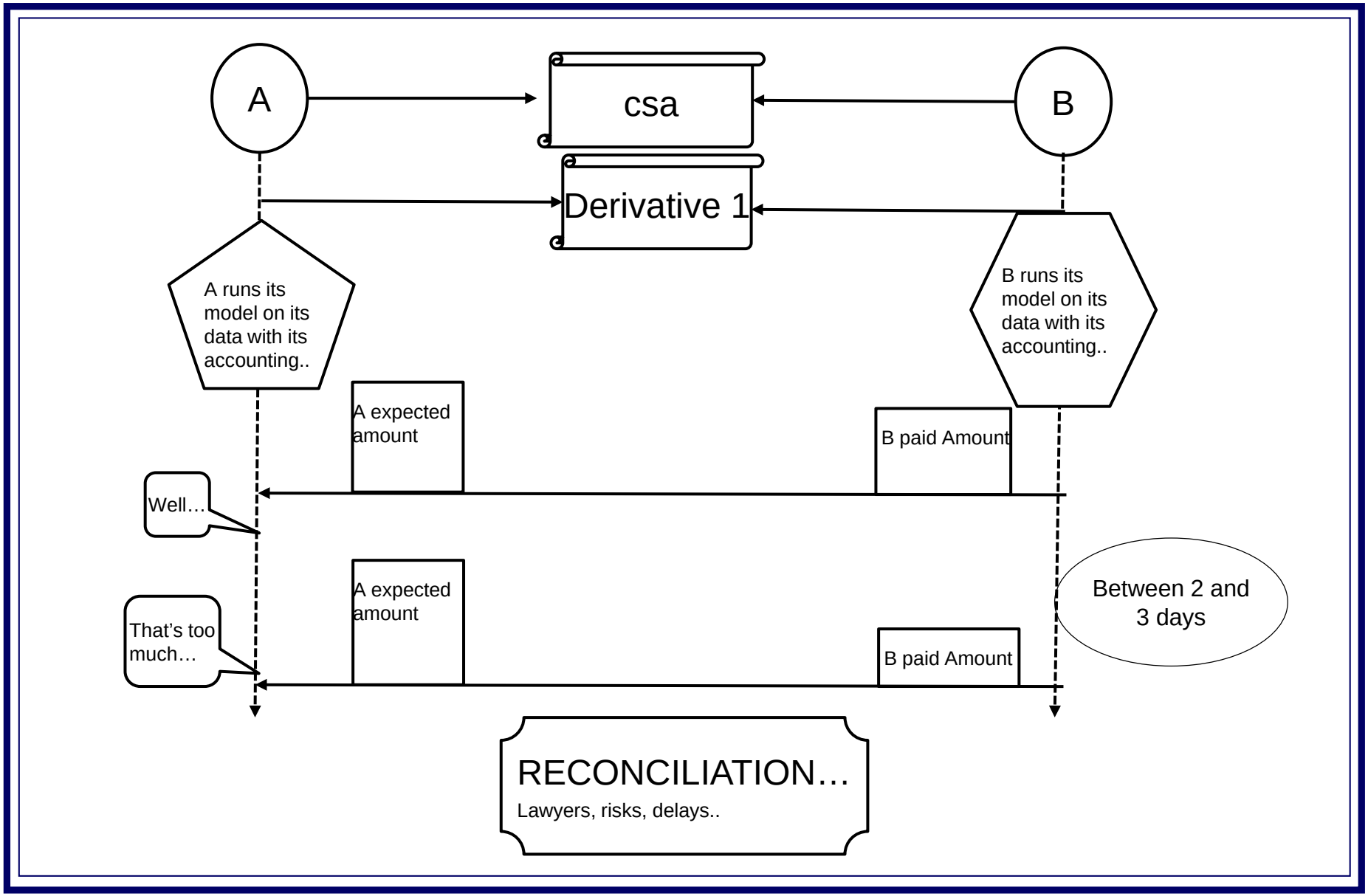


Yet… Consensus by Reconciliation

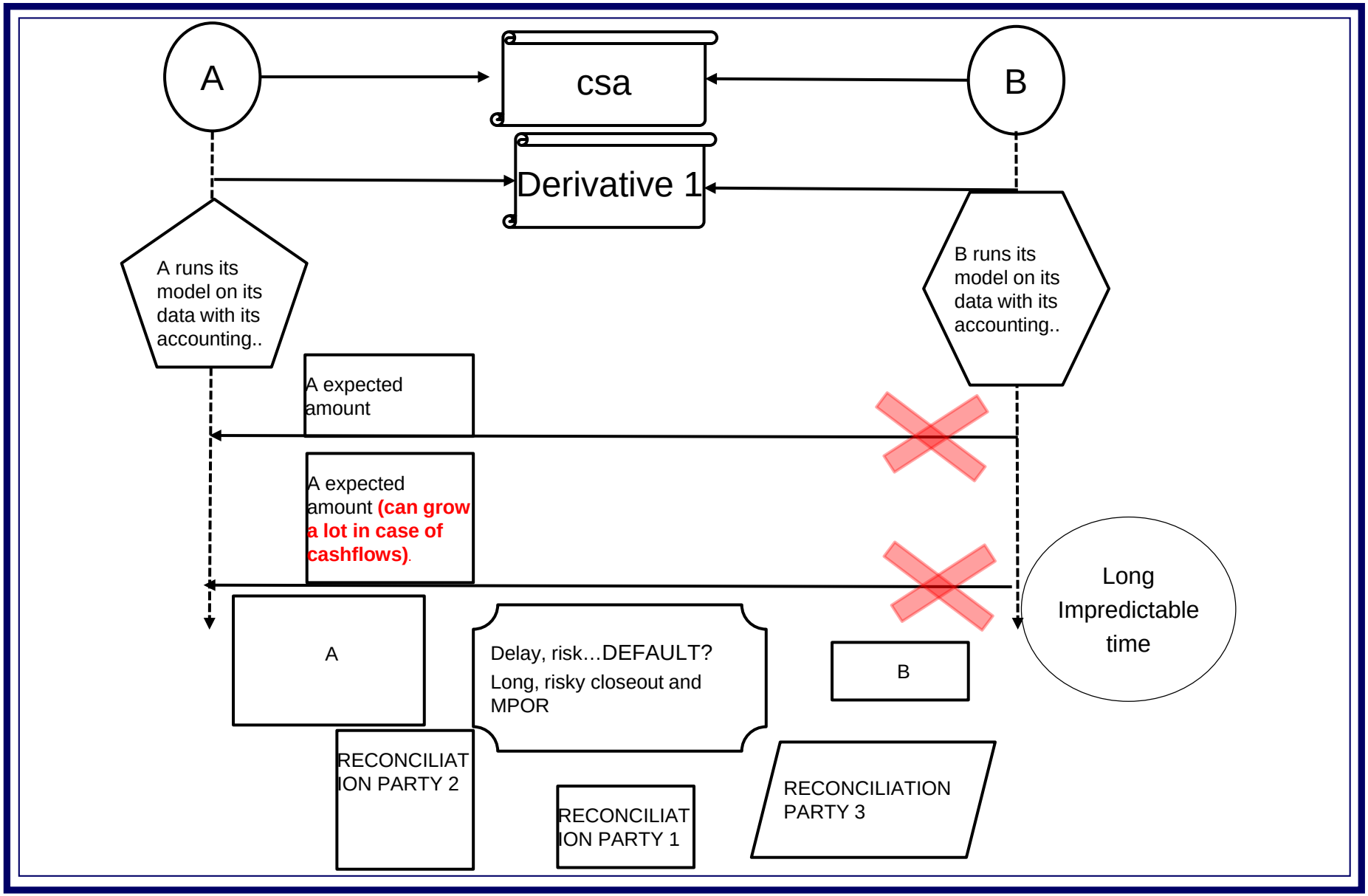


- In the current model, after paper contract every player gives **its own representation of a transaction in its own accounting systems (ledger) and its own IT systems, with its own models**. The confidence in smooth execution of all aspects is crucially dependent on **trust on representation coincidence, to be verified more than once**. This is the logic of **"consensus-by-reconciliation", a bottle-neck** preventing efficiency and reliability. Derivatives collateral is a perfect example…

Derivatives Collateral exchange process



What if there are serious problems?



Consensus by Reconciliation: delays, costs, risk, capital

- Current reconciliation and settlement steps slow the process down even if the technology enables very fast communication. They also drive costs up.

- The need for reconciliation and lack of automation leaves open the risk of disagreement and litigation, making the process uncertain and increasing risks and consequently the capital requirements for members.

- It is a system intrinsically inefficient that has never 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, 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.

- **How do Cryptocurrencies avoid the above bottle-neck?**

Consensus by Reconciliation: delays, costs, risk, capital

■ Crypto-currencies are based on **a single accounting and reporting system, a *Distributed Ledger***. With a Distributed Ledger, the reconciliation bottleneck is avoided since there is **at inception 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, coinciding with settlement**. Further reconciliation steps are much more unlikely when there is a single authoritative deal representation for all the parties. It is this business model that makes transactions so fast for Bitcoin, more generally than any specific piece of technology.

■For advanced financial markets, distributed consensus can be extended 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, managing (executing direcly or driving the execution) the transaction agreed at inception between the parties.** This guarantees the **enforcement of consensus**, namely that the deal will respect the agreement taken at inception between the parties.

Smart Contracts (Ethereum example)

This seems the end of counterparty risk. One can even create contracts that collect money from different investors and then allocate them following agreed rules. These are the DAOs, decentralized, autonomous organizations…

We will see later example, potential problems (The_DAO), and solutions.

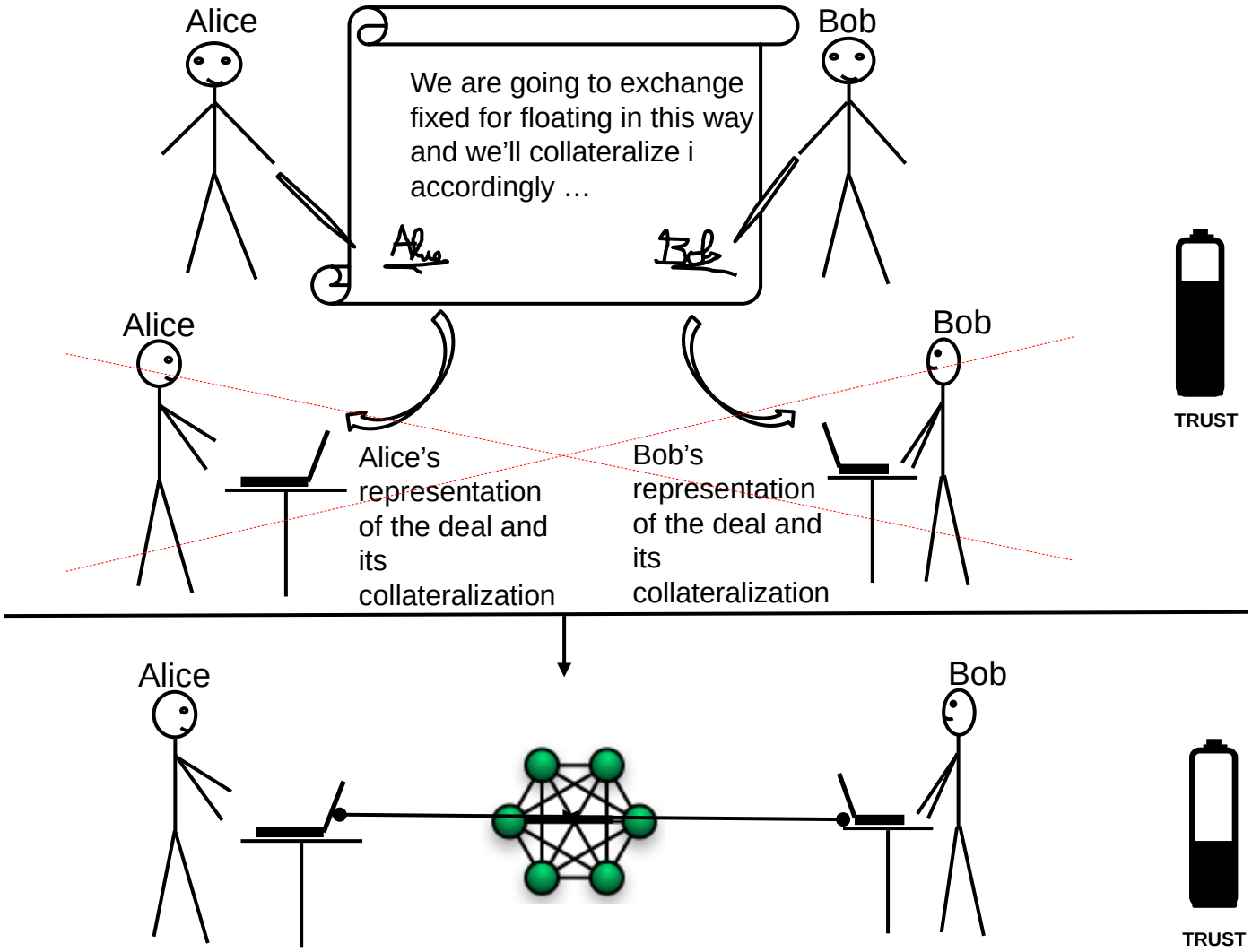
Smart Contracts

An obvious application of smart contracts and distributed ledger technology would be securities settlement, and in particular derivatives. A derivatives deal can be smart contract cryptographically signed by both counterparts. As a standard cryptocurrency transaction can command to move X units of money from wallet A to wallet B now (ten minutes in practice), a Smart Contract transaction can for example move

$$\max(S_{1Y} - X, 0)$$

from wallet A to wallet B in 1 year from now, where S_{1Y} is the price of a given stock in 1 year, provided that an amount of money (the value of this contract) is transferred, say by ten minutes from now, from wallet B to wallet A. This is clearly a sketch of the implementation of a call option transaction, where A is the option seller and B is the option buyer.

What do we get from this new business model?



Unique, distributed representation & management of the deal

Derivatives. The problems.

Many problems of derivatives come from **credit risk**:

- Credit risk of the counterparty: CVA cost for bank
- Credit risk of the bank: DVA cost for counterparty
- Credit risk increases the **funding** spread: FVA cost for the bank
- Credit risk requires more **capital**: KVA cost for the bank

Collateral is the solution, and should kill them all. Why it does not happen?

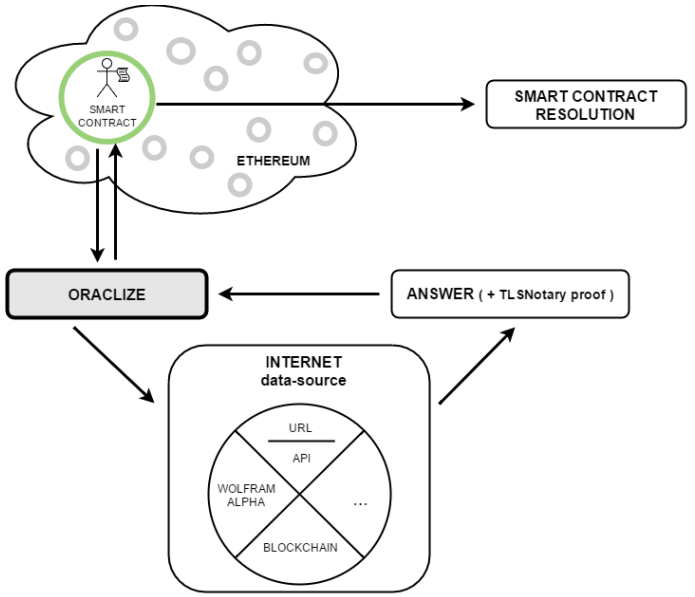
- **Lack of automation**: first-class collateral agreements embed a valuation/risk models, fast liquidity management, **not easy for many parties**.
- **Need of reconciliation in collateral exchange:** different data, different models, different implementations, different system representations for the two parties, with no mutual visibility. **Risk of litigation. Even when daily, 2-3 days for settlement. Risk of big misalignments around cash-flow times.**
- Need for reconciliation (liquidiators, third parties…) for valuation at default: closeout amount. **Very long margin period of risk (time) for lack of shared termination and determination process.**

Extra-collateral (initial margin) is added, high cost and yet not closing risks.

Detailed problems and possible solutions for derivatives collateral

- Collateral management is not so easy for non-financial players
  - ☼ Smart contracts and digital cash/transactions to make it easier. **Smart contracts can implement derivatives payoff, trusted valuation with an agreed algorithm deployed in the cloud, requirements of ISDA Master and CSA agreement, and automatic transfer of collateral from a digital (multisig) wallet with automatic breakup in case of problems.**

Oraclize acts as a node that receives a query from the smart contract, fetches data from the trusted data sources indicated in the query, process them through agreed software deployed on Amazon web services, and provides the desired result together with cryptographic proof of its honesty (the so called "honesty proof") based on TLS-notary. Proof of honesty means proof of no manipulation beside the requests made by the smart contract in the query code.



Detailed problems and possible solutions for derivatives collateral

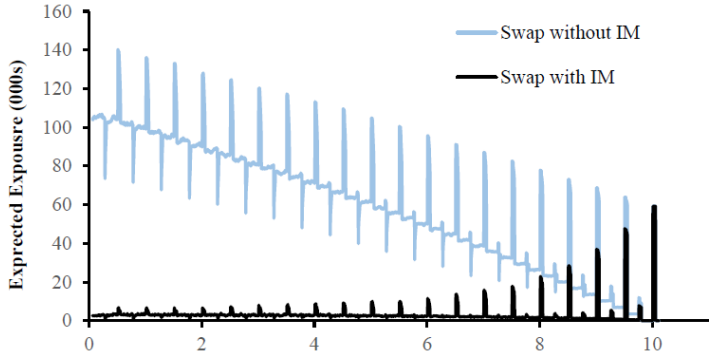
- Variation Margin based on different models and market data and computations and accounting representations, with reconciliation and litigation
  - **There can be no differences due to the model or the data or the computation or the accounting rules if the agreement is taken not on a generic paper contract, 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. So collateral can match exposures much more precisely**

- Variation Margin slow settlement with big misalignments around cashflow times
  - **Much faster collateral update (mins or hours) becomes possible on single ledger. Smart contract can retain cashflows until also updated collateral is available, and release them simultaneously.**

- When a party pays a cashflow, its exposure to the counterparty can raise dramatically. If collateral is not updated swifly, one party will find itself with a large open risk. A smart contract can make the cashflow payment and the corresponding collateral exchange to happen simultaneously, preventing big misalignments between collateral and exposures, like in the Ethereum bond example.

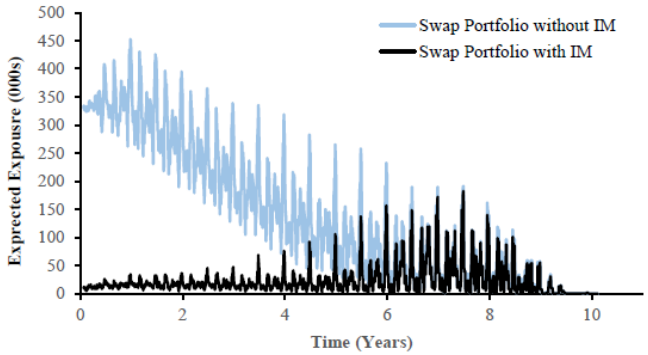
MPOR and Cashflow-Collateral Mismatch

Figure 10: Expected Exposure for 10-Year Vanilla Swap

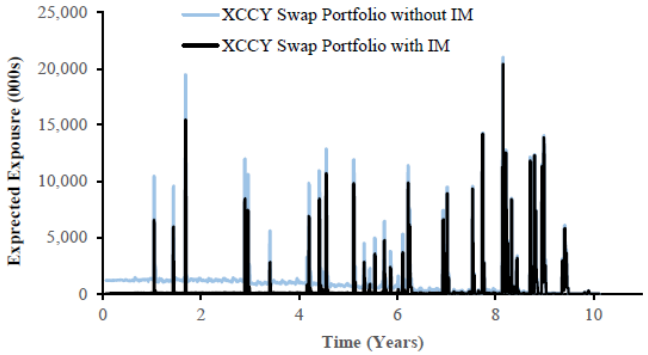


- **One relevant feature of cashflow/collateral misalignment risk is that standard Initial Margin does not close it.**

(a) Regular Interest Rate Swaps



(b) Cross Currency Swaps



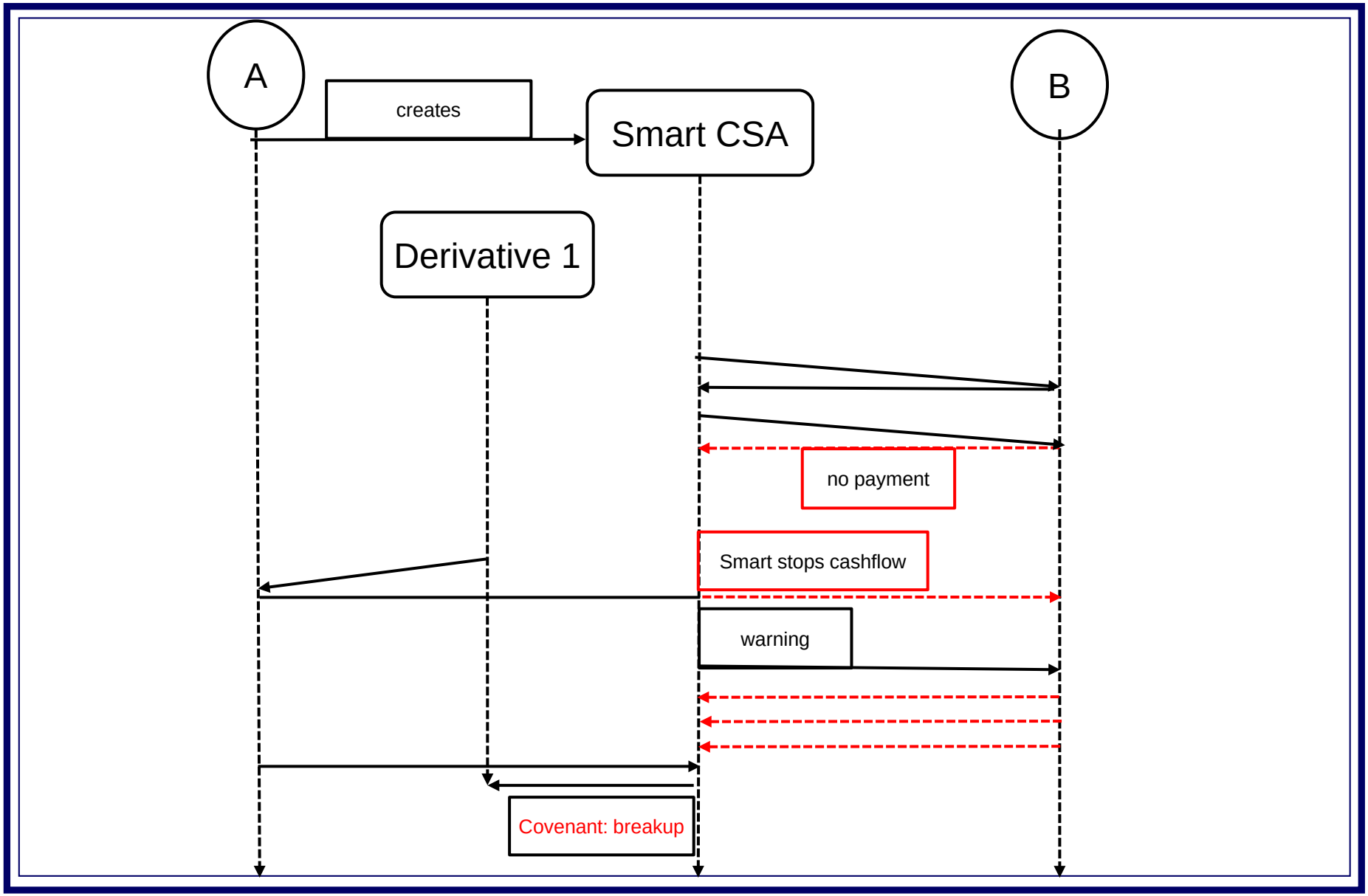
Using a smart contract to close the gap

- Smart contracts can also provide for various automatic actions in case a counterparty does not fulfill its obligations, avoiding to enter in a long and uncertain default closeout procedure.
- **Margin period of risk too long** summing collateral frequency and the period for the agreement on closeout, **still remarkable credit risk and capital cost (KVA). When this is addressed via Initial Margin in the currente model, there are high liquidity and funding costs.** Initial Margin stays in a secluded account and due to its size, that in turn depends on the length of the MPOR, it drains a large amount of liquidity from institutions.

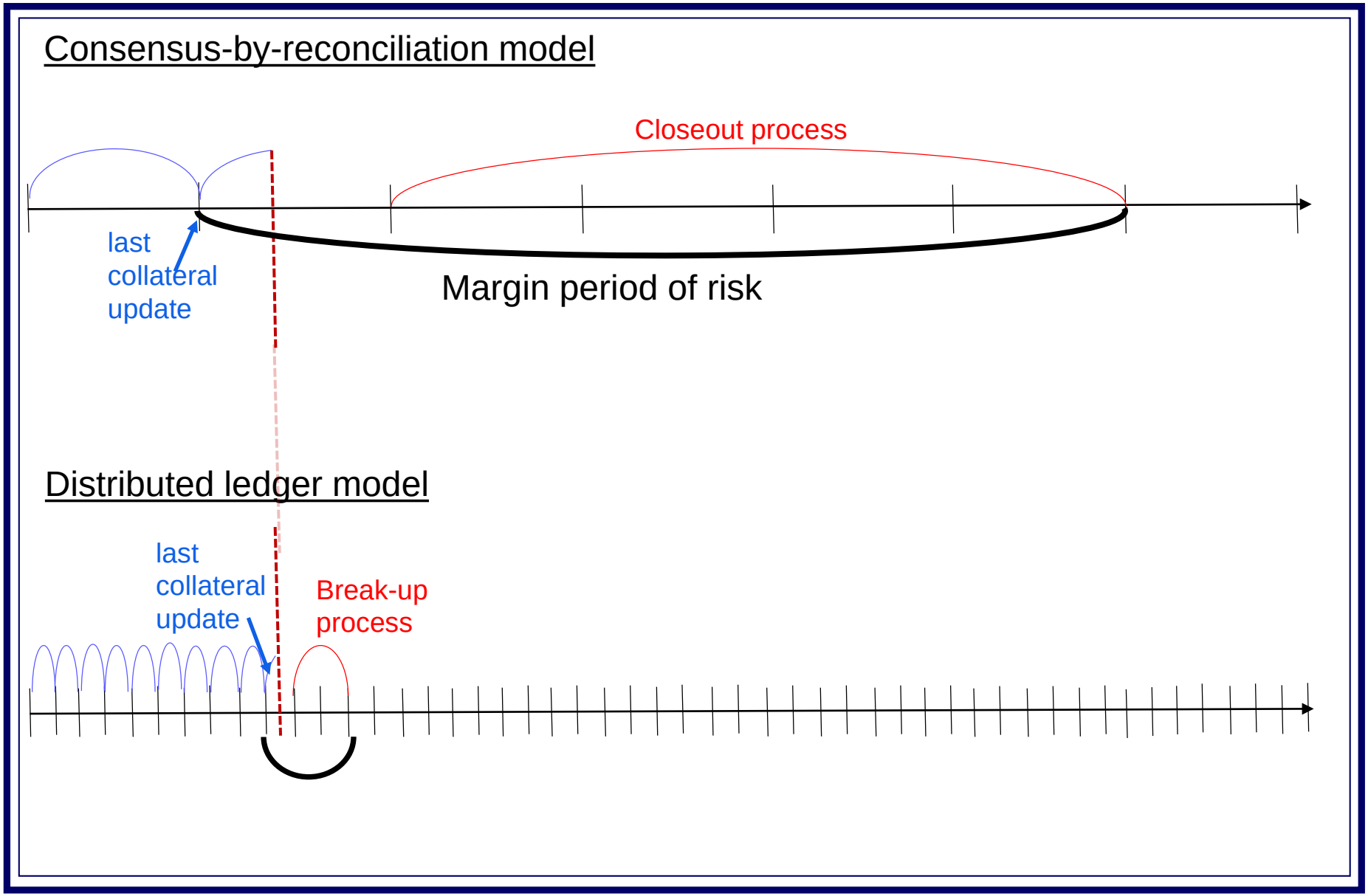
  - With collateral on a ledger, a missed collateral update is detected in real time. **We can design the smart contract to contractually breakup and provide closeout on the ledger based on the agreed model. Small Initial Margin held by contract automatically employed.**

  - **This can reduce the gap between collateral and close-out amounts to levels sufficiently small to allow to exclude «on-chain» default: a missed collateral payment can be treated as a contractual breakup.**

Dummy Collateral Workflow on dummy DL – Problematic status



Margin Period of Risk ($\propto Credit, Funding, Capital$)



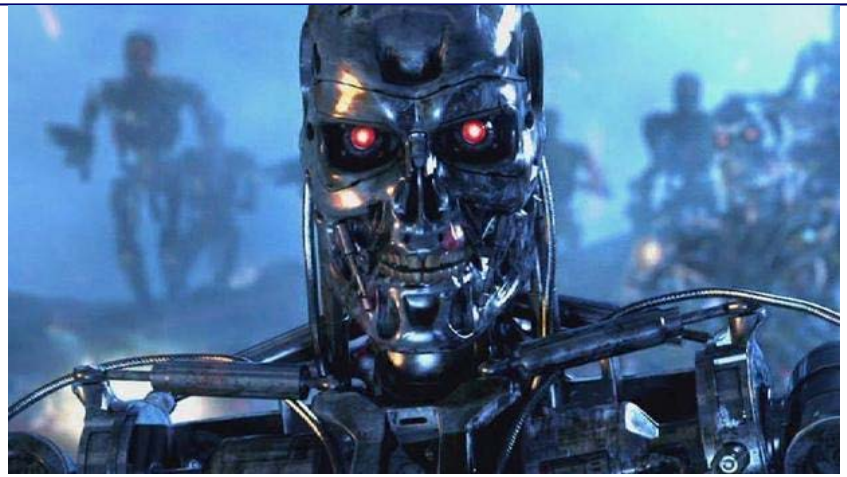
Other non-technical issues; to be studied and addressed

- This can be set on public chain (Ethereum, Oraclize) or regulated bodies can set it on private chain: there an overseeing regulatory node in the network can replace global visibility.

- Regulators could see advantages in an architecture which is more **transparent and creates less risk** than most of the current solutions**. Not immediate process.** There can be fear that a market that is faster/more automatic creates more «**technical defaults,» due to temporary lack of digital cash. We suggest missed payment is treated contractually as an unwinding** (balance covered by small Initial Margin or set to be settled in a longer term).

- **Regulators and market players can be wary of a technology that just eliminates reconciliation or gives immediate settlement**; in fact, this may increase risks. A great example is The_Dao hack in Ethereum: a smart contract can raise up to $150mn in few weeks, but a careless design can be exploited by good programmers to drive the contract to personal interest.

We all know that robots, if given too much power…



TheDAOwas a decentralized crowd-funding application where participant contributed digital money which was then allocated to funding investments chosen through a complex voting procedure, a process fully administered by the code of a smart contract. In few weeks in spring 2016, this amazing idea collected over $150 million. Yet on June 17 2016, about $45 million were drained by an unknown attacker who exploited a code weakness allowing him to withdraw money that was not his own…

Yet money was 90% recovered and 10% given to hacker via a hard fork.

*

Other non-technical issues; to be studied and addressed

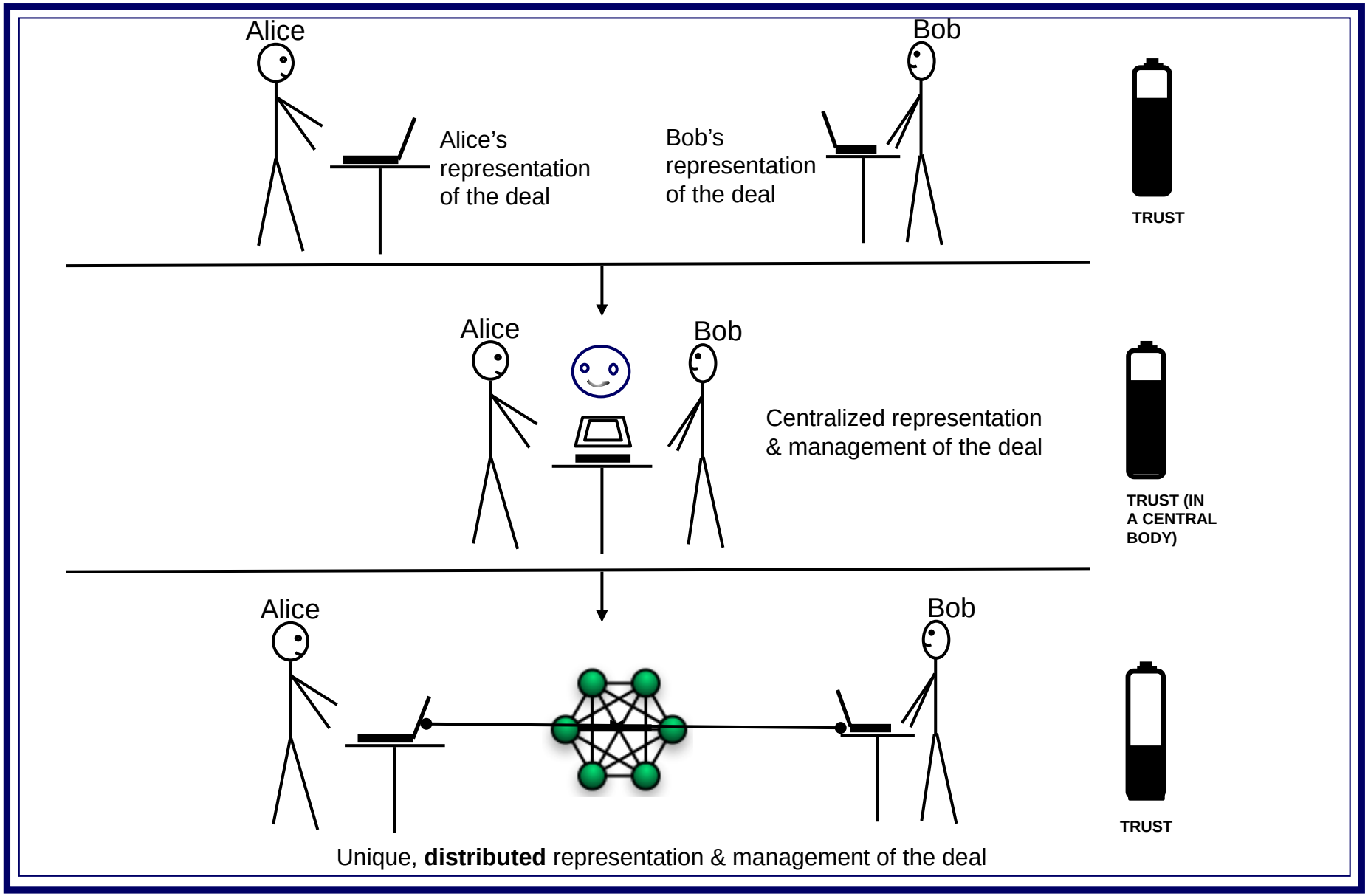
- Solutions for financial markets: legal prose delegates part of the contract to smart contract, but gives a **legal setting to frame its execution**, so that legal system keeps proof of authority in case of errors. Absence of a legal system is impossible chimera of cryptoword. See Lee Braine (2015).

- Technically, Smart Contracts can have different design. In Ethereum they are **«robot counterparties»** that own money and make transactions. But, more in Bitcoin style, they can be **«digital referees»** that allow players to execute only transactions allowed by smart contract, with no direct execution power. In this case automation is matched with accountability of non-anonymous players. See CORDA smart contracts:

  - SIMILARITIES TO ETHEREUM:
    - Contracts are fully Turing complete and can implement complex logic, they are created and used with transactions
    - Logic is apps over platform
  - DIFFERENCES FROM ETHEREUM:
    - Contract is not a robot counterparty: every object is associated to a signed contract that gives rights and prevents actions, but players own their money and make their own transactions
    - The contract is not the law: legal prose delegates to code when appropriate (giving also legal support to «distributed court decisions» like ethereum TheDao fork…)

Centralization and Decentralization

From Consensus by Reconciliation to Automated Consensus



From Consensus by Reconciliation to Distributed Consensus

■ These goals can be reached also with centralized solutions. Centralized systems are not *fault-tolerant*. A fault of the central body is failure of the whole system.

■ In economic terms, this means that an administrator institution would bear the network operational risk, thus demanding an equally great power on changing unilaterally the rules and applying them arbitrarily. Centralized solutions can be technically efficient but drive the business costs up (monopoly/oligopoly). In finance centralized solutions also generate a concentration of financial risk that drives up the regulatory burden and the amount of risk-management provisions such as collateral.

■Since the ledger must report the situation of everyone and yet belong to no-one, a distributed ledger can appear a natural solution. It avoids the need for a central body and also reduces the legal uncertainties. Agreement must be bilateral and not a one-fits-all rule. The protocol manages the network in a deterministic (predictable) way. Yet, in the current environment, we may choose a hybrid model where a legal entity remains accountable for the market: the CCP.

■This may help CCPs to meet the concerns raised in **IOSCO-BIS 2016 and ISDA 2016.**

Few more words on CCPs

- IOSCO and Basel recently published a paper where they point out gaps and shortcomings in CCP recovery planning and in credit/liquidity management. They strentghten further the requirements.

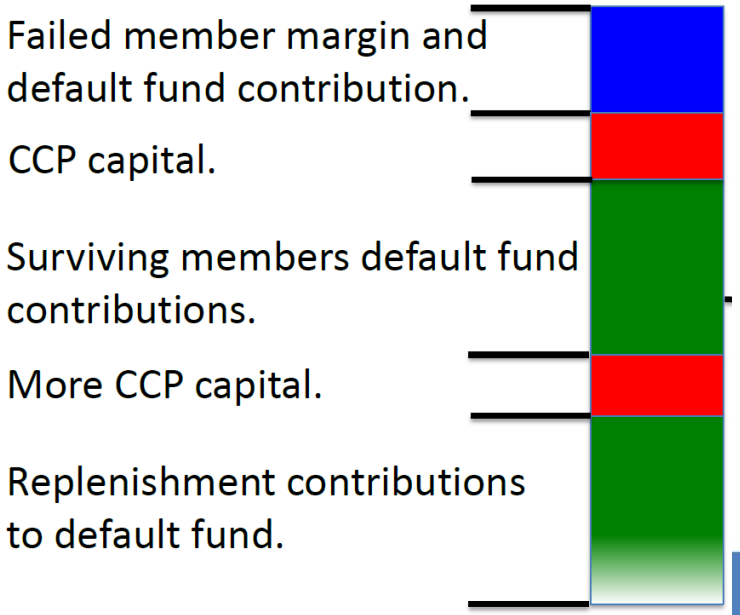
- CCPs have become “increasingly crucial” due to mandatory clearing regulations, so much that is “imperative” that they are resilient to stress events to “ a very high probability”, which means a very low probability of default for any of them.

- Same view, also very recent, was expressed by the Financial Stability Forum, whose chairman is now Mark Carney, governor of the boE http://www.fsb.org/2016/07/meeting-of-the-financial-stability-board-in-chengdu-on-21-july/

- The real point is that, with CCPs so crucial, no probability can be sufficiently low, considering that, with a handful of CCPs around the world, default of a single one would be a catastrophe. That is why now regulators feel compelled practically revise/strenghten (making “more granular”) the new standards for CCPS they just introduced in 2012.

*

Few more words on CCPs



In theory, CCP Capital very important. In practice, it is very small compared to the pooled resources posted by client banks (see below in bn's).

In case of trouble CCPcan stop paying variation margin to clients (but this increases the risk for clients), and they can early terminate their contracts (but in this way clients lose a hedge).

	Initial Margin	Operator Capital	Default Fund
CME Clearing U.S.	133 USD	0.150 USD	2.37 USD
LCH.Clearnet Ltd.	89 EUR	0.046 EUR	3.62 EUR

*

Few more words on CCPs

- It is natural to wonder if these roles could not be played by a “distributed consortium” rather than a “central counterparty”. In the end, the real resources used are initial margin, which provided by each counterparty, and a default fund pooled by counterparties. This could be managed with a smart contract logic. Regulators may end up thinking that such a model makes a better risk balance… so far, however, they support CCPs that granted standardization and transparency.

- **Here comes the other side of the coin.** : if a CCPs have operational weaknesses and high costs, that could be diminished by DLT, even replacing CCPs, and yet there is need of manual control and of a legal entity managing it and accountable for it, why not merging DLT with CCP services, without replacing CCPs but improving them? There is even more:

https://isda.derivativiews.org/ say that in case of serious stress for a CCP it would be crucial to maximize certainty and predictability by following a precise sequence of loss allocation and position allocation tools, already defined by ISDA. Transparency, with indicators defined upfront and followed strictly by regulators, can help maintain market confidence and avoid disruption.

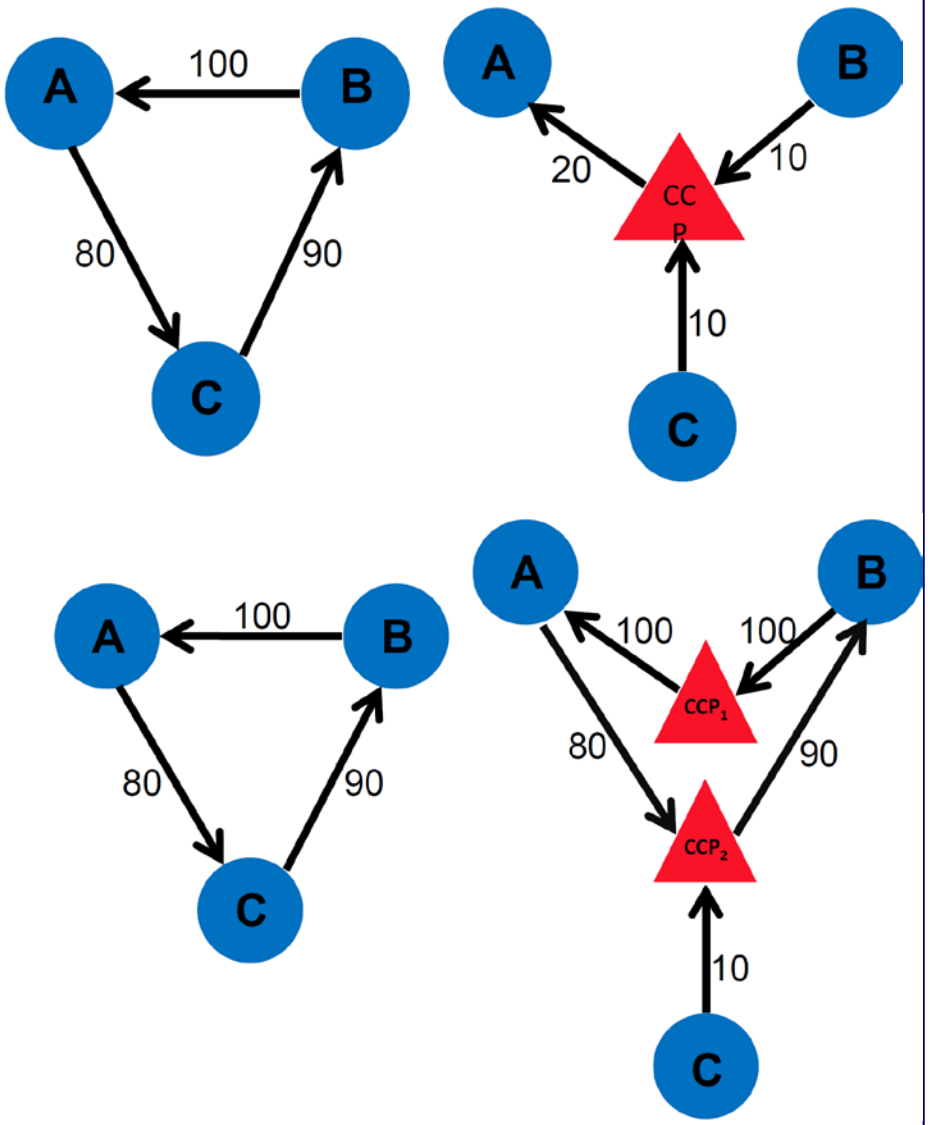
*

Few more words on CCPs

There is even more…One central counterparty reduces risk a lot… But two central counterparties can spoil the benefit! (Duffie 2015, Basel).

Blockchain can provide visibility/ netting across CCPs, and availability of IM and DF where it is needed across CCPs.

The business model can change even with CCPs. Then, their exact role will be a matter of choice.



Few more words on CCPs

- DTCC is now working with Axoni Blockchain and R3, LCH may work with R3 and D-Pactum. This opens up to other business models for CCPs. From counterparties of all deals when things go well, and potential systemic points of failure when there is a trouble, they may become counterparties of last resort. If this is coupled with CCPs providing for portfolio valuation during normal business, the risk they would bear could be accounted for in their valuation for collateral.

- This technology opens up to more mutualization of services among banks: we can mutualize data, computations, collateral, ratings… without having to rely on one central counterparty.

- In a world where banks may face the competition of unregulated internet giants, each one dominating its own market, a technology for mutualization of processes, resources and risk management through distributed automation beyond centralized exchanges/CCPs or custodians is interesting for all.

- Yet it's a long way forward: it shakes the foundations of regulatory frameworks and business models; it creates risks we are learning to manage only now.

Disclaimer

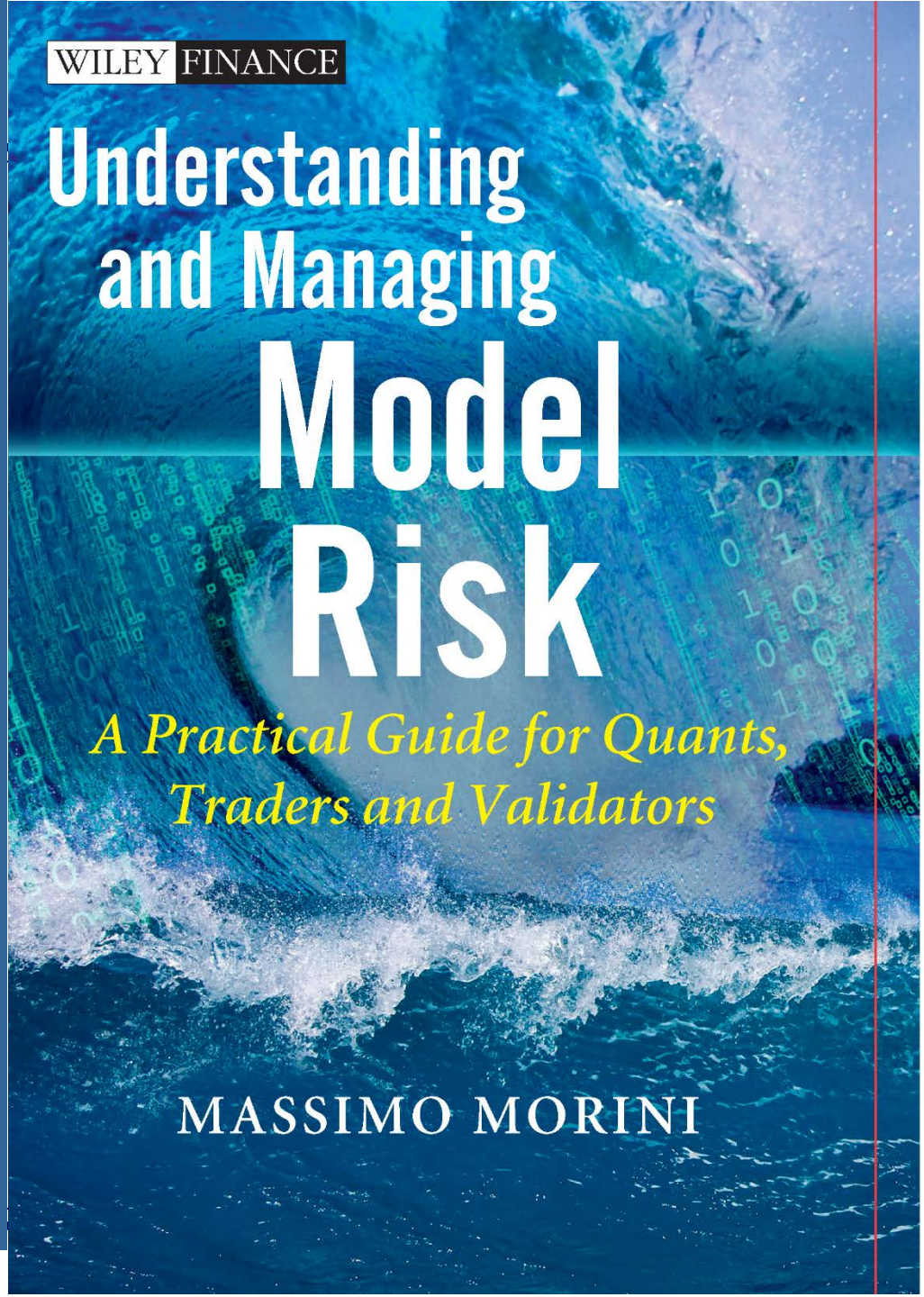
Thank you!

Main references:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2760184

http://www.risk.net/risk-magazine/opinion/2422606/-smart-derivatives-can-cure-xva-headaches (with Robert Sams)

* This presentation expresses the views of its authors and does not represent the opinion of its employers, which are not responsible for any use which may be made of its contents.



"The most thoughtful and yet practical book I've seen on dealing with model risk."

Emanuel Derman, Professor at Columbia University, former Head of Quantitative Risk Management at Goldman Sachs, and author of *Models.Behaving.Badly*

"Massimo Morini has provided a comprehensive and practical book on model risk that well covers the practitioner's needs in these post-credit-crisis times. The various applications are woven together by a strong conceptual underpinning that provides unity and coherence to the book. Traders, product controllers, regulators, accountants and, in general, students of the reality of financial modelling will greatly benefit from this high-quality work."

Riccardo Rebonato, Head of Front Office Risk Management and Quantitative Analytics, RBS Global Banking & Markets, Visiting Lecturer, Mathematical Finance, Oxford University, and member of the Board of Directors of ISDA and GARP.

"At last, a book (other than my own obviously!) that takes model risk seriously. And does so by hitting the "maths sweet spot," not dumbed down and not trying to impress with complexity. I wish more finance books were this sensible."

Paul Wilmott, Founder of the CQF, the world's largest quant education program.

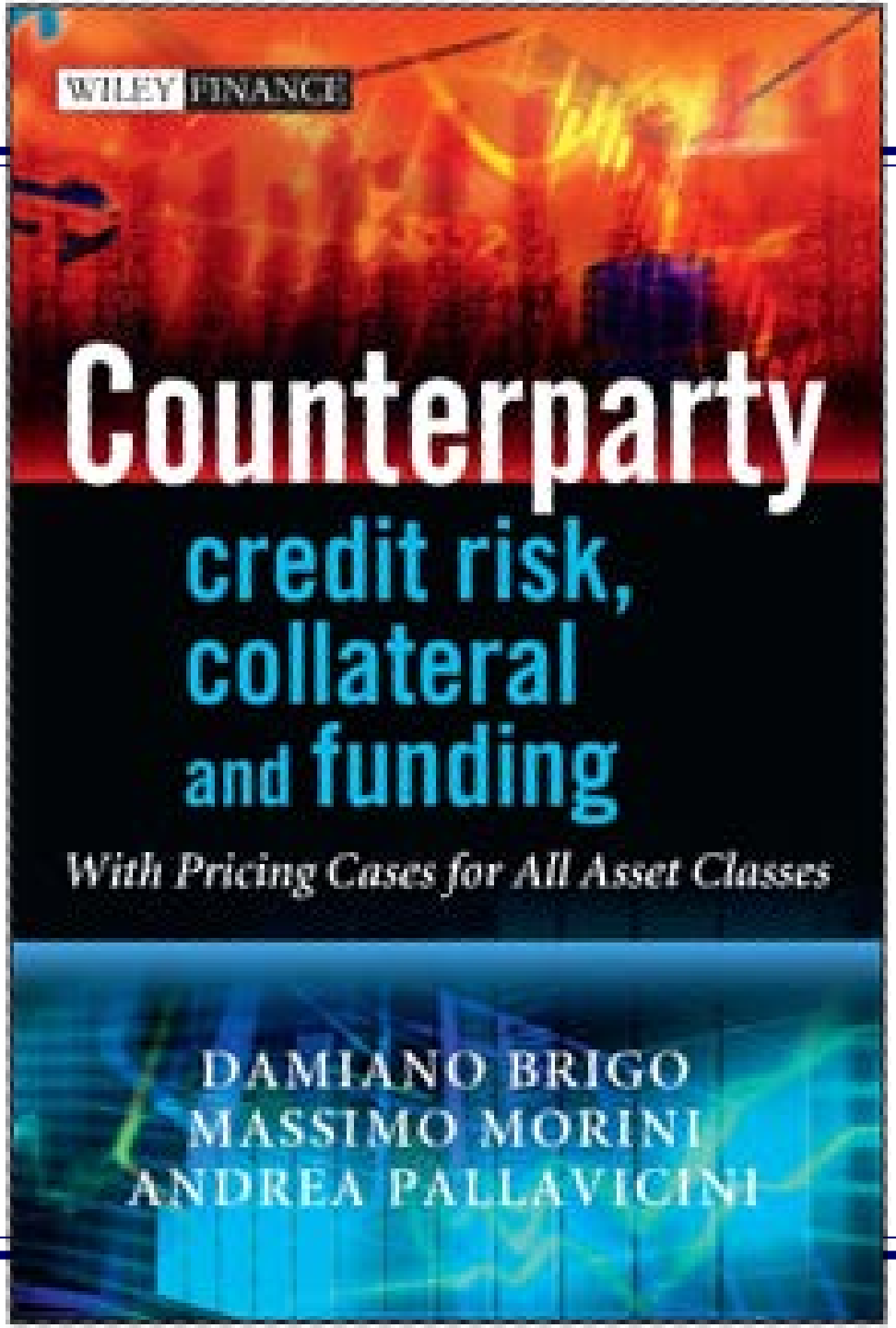
"The recent credit crisis taught us that model risk can have disastrous consequences if not properly accounted for. This timely contribution by Massimo Morini presents thorough studies on the types of risk that arise when modeling and pricing derivatives across different asset classes. The perfect blend of rigorous modeling and market wisdom makes this excellent book a must have for quants and risk managers: model risk at no book risk."

Fabio Mercurio, Quant Business Manager, Bloomberg L.P., New York.

"Long-neglected by risk managers and regulators, model risk was shown to be a major component of the risk of derivatives portfolios during the recent financial crisis. Massimo Morini's book offers a much-needed resource for practitioners who want to deal with the "invisible" risks associated with the widespread use of quantitative models in finance."

Rama Cont, Columbia University, New York, and CNRS, Paris

continued on back flap


WILEY FINANCE
Counterparty
credit risk,
collateral
and funding
With Pricing Cases for All Asset Classes
DAMIANO BRIGO
MASSIMO MORINI
ANDREA PALLAVICINI