Politecnico di Milano, May 10, 2018

Smart Contracts for Derivatives and DvP

Massimo Morini
Head of Interest Rate and Credit Models
Banca IMI – Intesa San Paolo Group

The current state of blockchain

"DLT will likely develop hand-in-hand with new smart contracts that can value themselves in real-time, report themselves to data repositories, automatically calculate and perform margin payments and even terminate themselves in the event of counterparty default, see Massimo Morini & Robert Sams, Smart Derivatives Can Cure XVA Headaches, Risk Magazine (2015)."

WRITTEN TESTIMONY OF J. CHRISTOPHER GIANCARLO CHAIRMAN, COMMODITY FUTURES TRADING COMMISSION BEFORE THE SENATE BANKING COMMITTEE WASHINGTON, D.C. FEBRUARY 6, 2018

The current state of blockchain

Despite optimism…

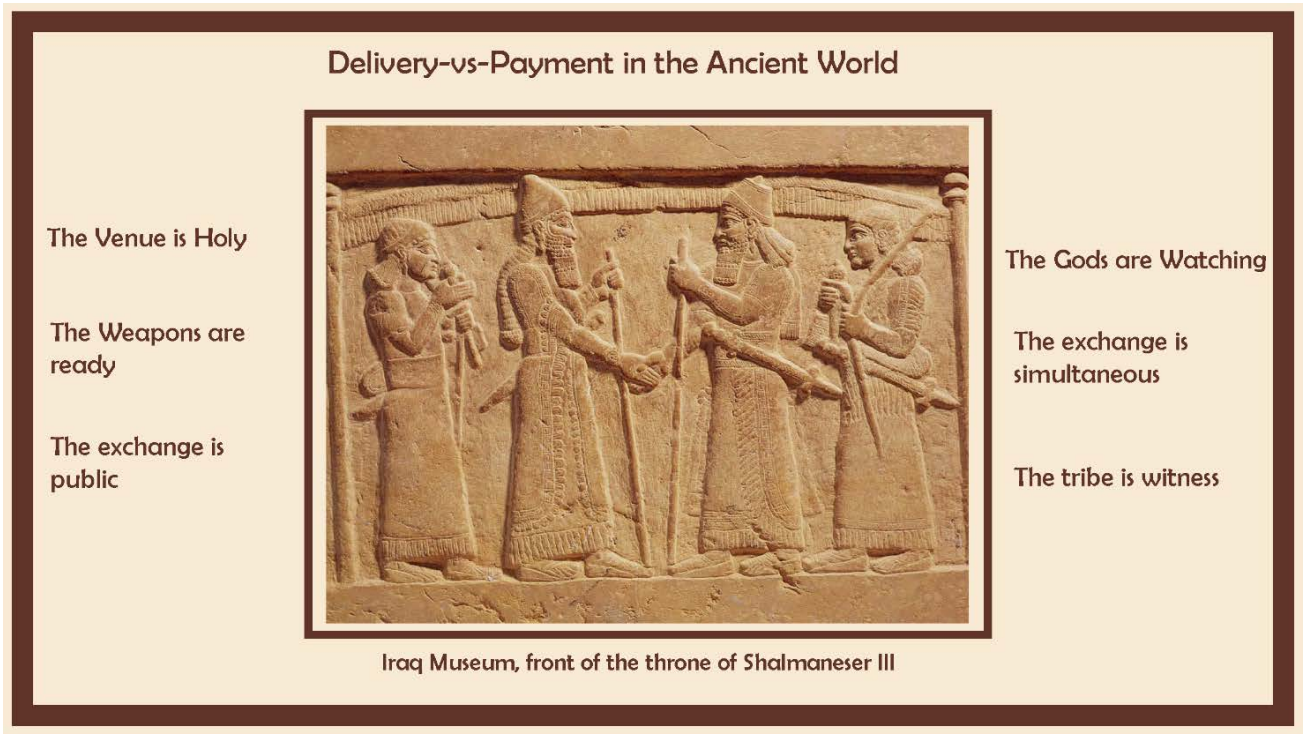
- 1988: Tim Berners-Lee invents the Word Wide Web in 1988.
- 1999: the future Nobel Prize Paul Krugman could still predict a negligible impact of the Internet on future economy
- How was that possible? In the first 10 years of the internet that fantastic idea was visible already, but a good deal of the tech and the services that could make it the revolution it promised to be were not there yet! Too slow. Not enough people were connected. Services like google search already invented but not widespread.
- In spite of above optimism, in part we are in a similar situation for blockchains. The only application which is driving real billions are cryptocurrencies on public blockchains, with first basic smart contracts and creation of project-specific tokens, seen as ways to have a stake in separate economic and technological environments.
- Applications in the regulated world are only at the level of proof-of-concept. Why?

The current state of blockchain

- All blockchain applications require a fullly digitized representation of value (money). Despite experiments (Central Bank Digital money, USC, RIPPLE) only public cryptos already exist
- Blockchains have a peculiar governance, the «consensus». Public blockchains use proof-of-work, those that should be regulated (private) are still researching, only bilateral available.
- Applications like smart contracts, decentralized settlement, issuance of digital value, are at odds with current regulations, even if they are in line with regulatory principles. Among the issues to tackle:
  - Legal Status of Cryptos and Tokens
  - Legal status of smart contracts
  - Specific impact on the regulation of financial markets
  - Privacy, Identity, Finality
- In the public Blockchain, however, we can undestand the potential of Smart Contracts, see next applications.

DvP: a historical problem

Within a single tribe, economic needs were satisfied via gifts and sharing, without explicit exchanges (Humphrey, 1985). As if trading was not needed where there was mutual *trust*. But people from different tribes did not trust each other. In the moment of the exchange, one of the two parties could try to take the other party's asset and run away before doing their own side of the exchange.

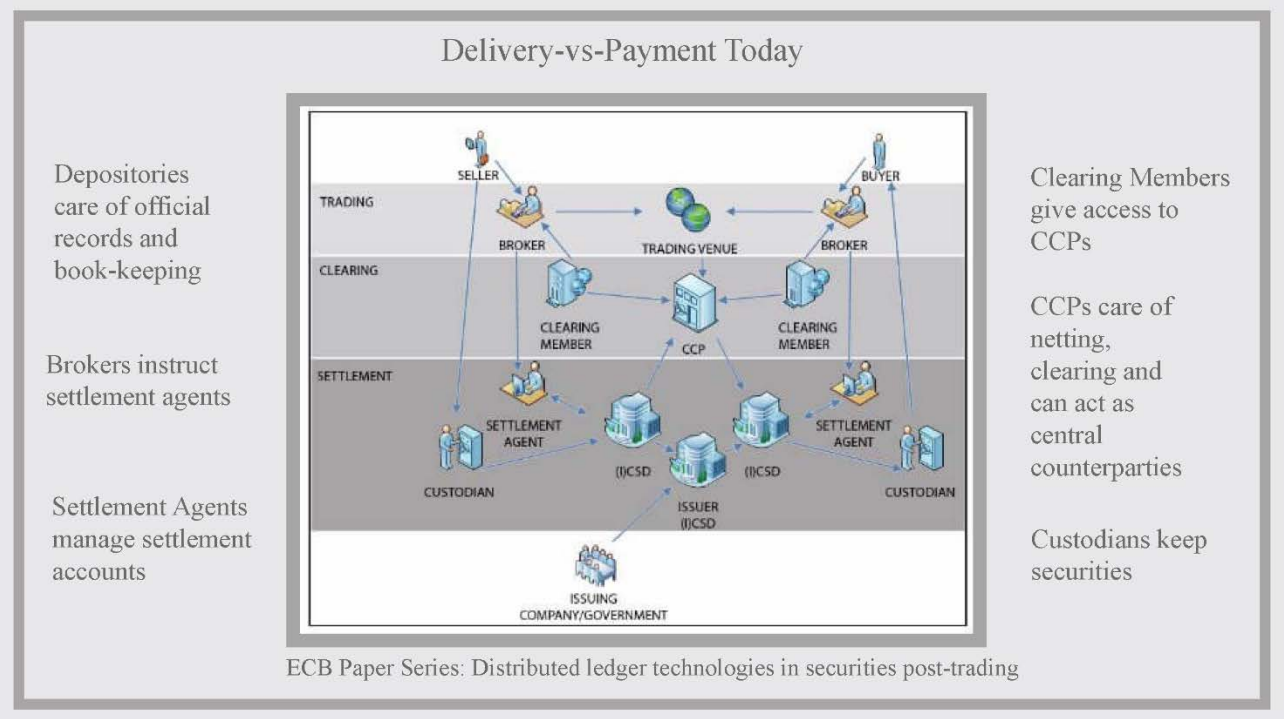


The issue of Delivery-versus-Payment resurfaced after the great explorations of 16th and 17th centuries, when it happened that merchants had to arrange trades which were not for now and face-to-face, but between counterparties living on either side of oceans, and for future delivery.

*

DvP: a historical problem

The Philadelphia Stock Exchange, founded in 1790, began using a clearing house as early as 1870
Later, it put itself in the middle of the trade. CCPs were born, and then other institutions followed…

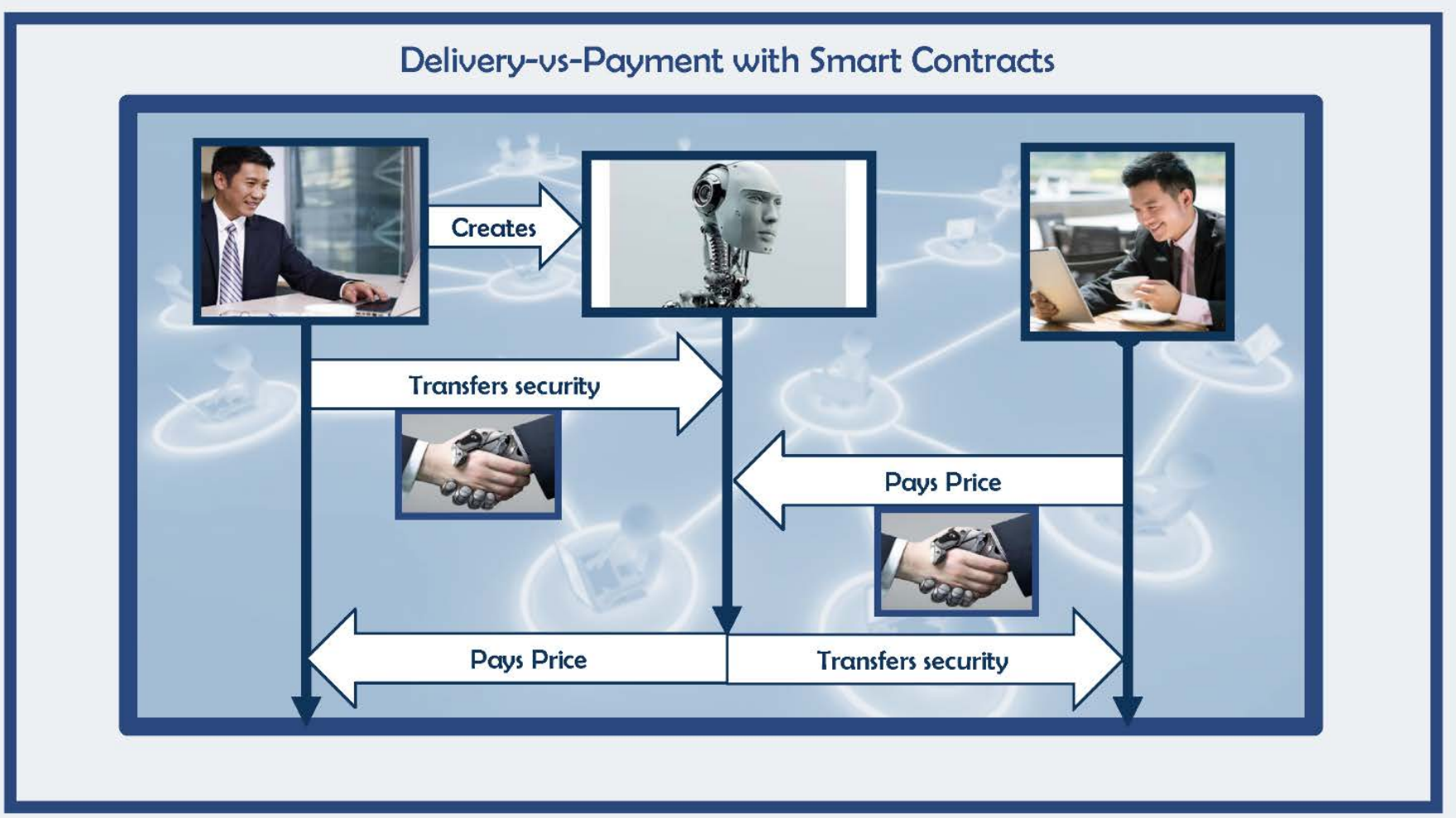


1. There are Registrars and Depositors who perform the notary function of keeping an official record of who owns each security.
2. Depositors together with Custodian banks provide securities accounts and custody services.
3. Then there are Securities Settlements Systems, that make DvP possible.
4. Central Security Depositories (CSDs) that may take many of the above roles and operate on a centralized database transferring the security through double-entry book-keeping.
5. In the European Union there is a further layer: Target2 Securities, a central platform for local CSDs to meet10 years to complete.

*

DvP: current issues and opportunities

Today, DvP and counterparty risk appear in a rather different form. The internet brought this transformation, by replacing face-to-face relations with web connections.



*

ISSUERS and REGULATORS

1. A smart contract allows the issuance of digital assets, such as ERC20. A contract X can create, in his own storage, a new digital asset X, by creating a list that records how much every address in Ethereum owns of the digital asset X. At creation, all the Xs will be listed at the address of the issuer, that usually is the person who created contract X (the *message sender* in X creation). By trading, assets X will spread to other addresses, under the rules written in contract X that maintains the list after creating it.
2. In case of issuance via smart contracts, the list is visible to everyone in the blockchain, and can be altered only following the rule that everyone can see in the associated contract.
3. You may have already noticed that, for the whole life of a digital asset, the associated contract not only makes the issuance possible, but also takes the **role of custodian and depositor**, giving a complete, unforgeable and unmistakable view of who owns what, and keeping assets safe under the rules written in his code. Such a concentration of roles happens at times also in traditional markets, for example at CSDs, for efficiency reasons. Here it is native, and additionally it is not a real concentration, since the contract is stored and managed by all computers in the network. It is only a specialized, digital issuance document, held in a distributed database, that thanks to distributed automation also executes the tasks of a CSD.

DvP or Atomic Swaps

With the toolbox of smart contracts and tokens, it is not difficult to create an escrow contract for decentralized DvP exchanges.

Compared to the example above, we can even simplify: the seller can avoid sending the token to the escrow contract since he can just give the escrow contract the authorization to move the agreed number of tokens. The escrow contract will ensure that, if any of the two legs of the exchange is not executed, for example because the seller withdraws his allowance, all the changes to the state of the blockchain are reverted so that no leg can go through without the other leg.

This is easily obtained with Ethereum exception handling tools like the *revert()* instruction.

*

INTEROPERABILITY: Cross-chain Atomic Swap

Consider blockchain A where party Alice holds some value and blockchain B where party Bob holds some value. They want to exchange their values.

1. Alice thinks of a *secret sentence*, whose hash is 17ae36b … .(see below)
2. On blockchain A, Alice hands the asset to a smart contract that has the order to give it to Bob as soon as Bob shows the *secret sentence* whose hash is 17ae36b …
3. On blockchain B, Bob does the same thing, handing the asset to a smart contract that has the order to give it to Alice as soon as Alice shows the *secret sentence* whose hash is 17ae36b …
4. Now, if Alice wants to get Bob's asset, she must show the *secret sentence* on the public blockchain…
5. Bob sees the *secret sentence* shown by Alice. With that he gets Alice's asset.

17ae36b9635ade01e7b47ea9d3e65b3e9922d5a5b570d6d943d27b588e5db24f. This the SHA256 hash of the sentence "this is a secret sentence".

In the above description, both parties get the asset they want; there must also be a provision for the possible failure, through a time condition that unlocks the assets returning them to the owners after a given time (that will be slightly longer for Bob, since he can only act after Alice).

*

EXCHANGES: Decentralized Price Discovery

Projects like (Warren & Bandeali, 2017) or (etherdelta.github.io, 2016) try to build not only decentralized DvP, but also decentralized exchanges.

A party gives authorization to the exchange contract to move a given amount of his tokens, the he writes an order to exchange Token A for Token B (or for ethers), specifying a desired exchange rate, expiration time beyond which the order cannot be filled, and finally signs the order with his private key. Then he sends the order to a liquidity pool. Even if the liquidity pool is held offchain, an observer can pick up the order and, if he has the right assets to fulfil it, he also signs the order and sends it to the blockchain.

The exchange smart contract will settle the trade on the blockchain if the signatures are valid. This is an evolving field and technology is perfecting, but it is interesting to notice that in this business model *contract execution* happens offchain avoiding any latency issues, while settlement will happen in minutes on the blockchain

Finance - Derivatives

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.**

Variation Margin

- The derivative portfolio is revaluated *every day* by party A using its pricing model f^A that takes in 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 positive to A, which means that A is a net creditor, A will make a margin call for a cash amount V_t^A to B.

- Party B does the same thing but with its model f^B and its data M_t^B. If

$$V_t^A \approx -V_t^B$$

(or if $V_t^A \leq -V_t^B$) the process proceeds smoothly and B provides the required amount to A in form of collateral. If $V_t^A \geq -V_t^B$, B only provides the amount $-V_t^B$.

- When there is a remarkable difference between V_t^A and $-V_t^B$, the two counterparties talk to each other for a reconciliation.

Derivatives. The problems.

Today collateral agreements are very far from this ideal situation:

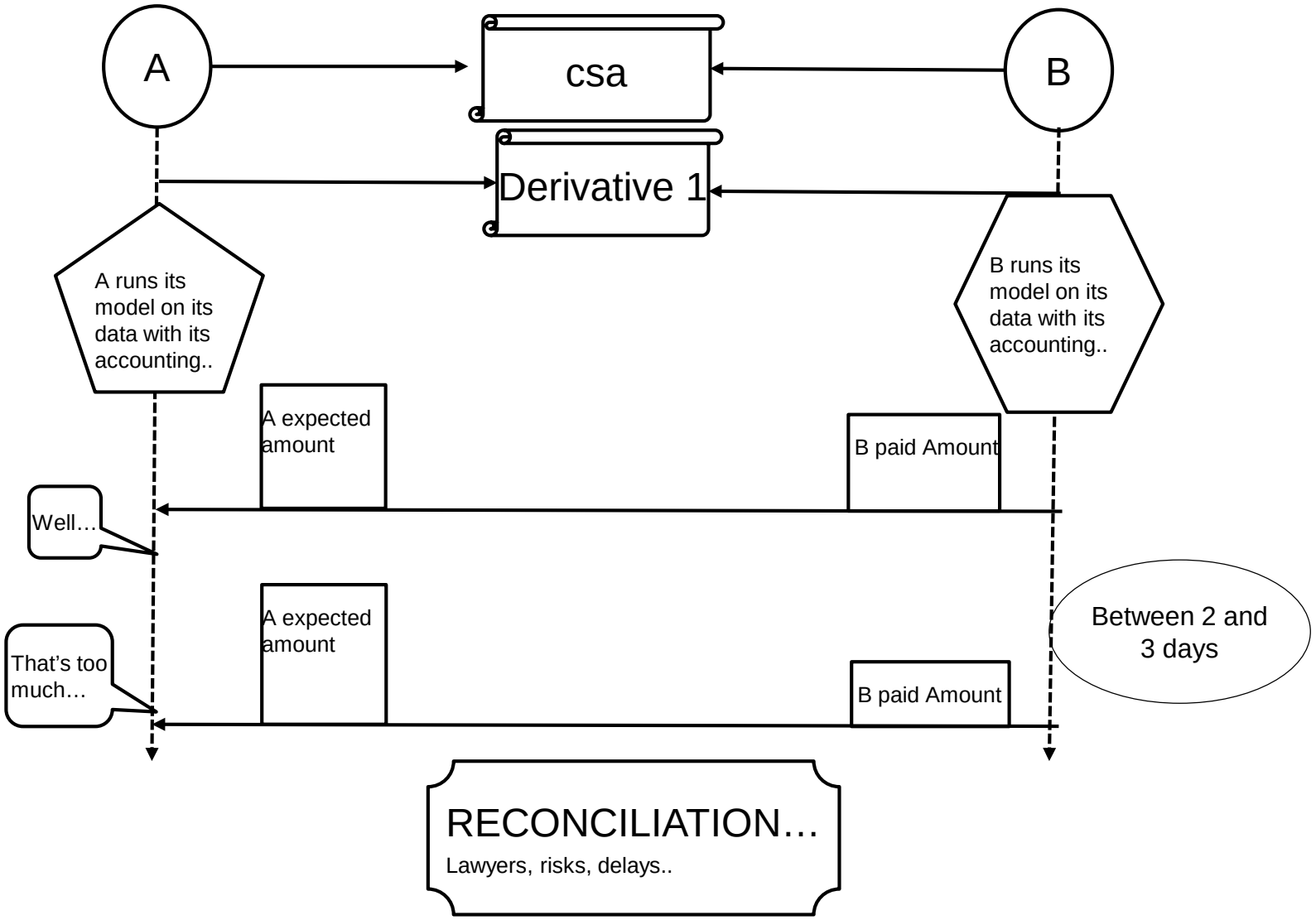
- ***Technical Complexity*.** It requires the capability to transfer liquidity easily across accounts with particular features, access a variety of input market data, and use properly valuation/risk models to compute the amount of variation margin. Corporates and funds usually do not have such capabilities, only banks have good agreements.
- ***Collateral Misalignments***. Even banks do not get Variation Margin with features A and B, since in every trade *the two banks still use very different data and models*. This leads to the margin payer sending variation margin amounts that for the margin receiver are often misaligned compared to the mark-to-market of the option. This leaves risks open and can also lead to costly reconciliation processes.
- ***Settlement Delays***. Even if data and models were the same, collateral would not match the option mark-to-market simply because collateral settles in a time that goes from 1 to 3 days. The collateral received is in the best case aligned with the mark-to-market of 1-to-3 days ago, not with current mark-to-market.

Derivatives. The problems.

■***Asynchronous Cash-flows versus Collateral***. In many derivatives there are various cash-flows to be paid regularly from one party to the other. Every time there is a cash-flow payment, the mark-to-market of the derivative jumps by an amount equal to the cashflow payment. Collateral should have a simultaneous jump to avoid risks to jump up instead, but cash-flows and collateral payments are far from simultaneous.

■***Default Uncertainty and Delays***: if a counterparty stops paying collateral, it is not immediately declared to be in default. The process takes several days, and this delay will add to the ones seen above. To make matters worse, after a default is declared, collateral and exposures are not immediately quantified and made available for netting: a complex valuation procedure, called default *closeout* process, is started, adding additional delay and uncertainty.

Derivatives Collateral exchange process



Derivatives. The problems.

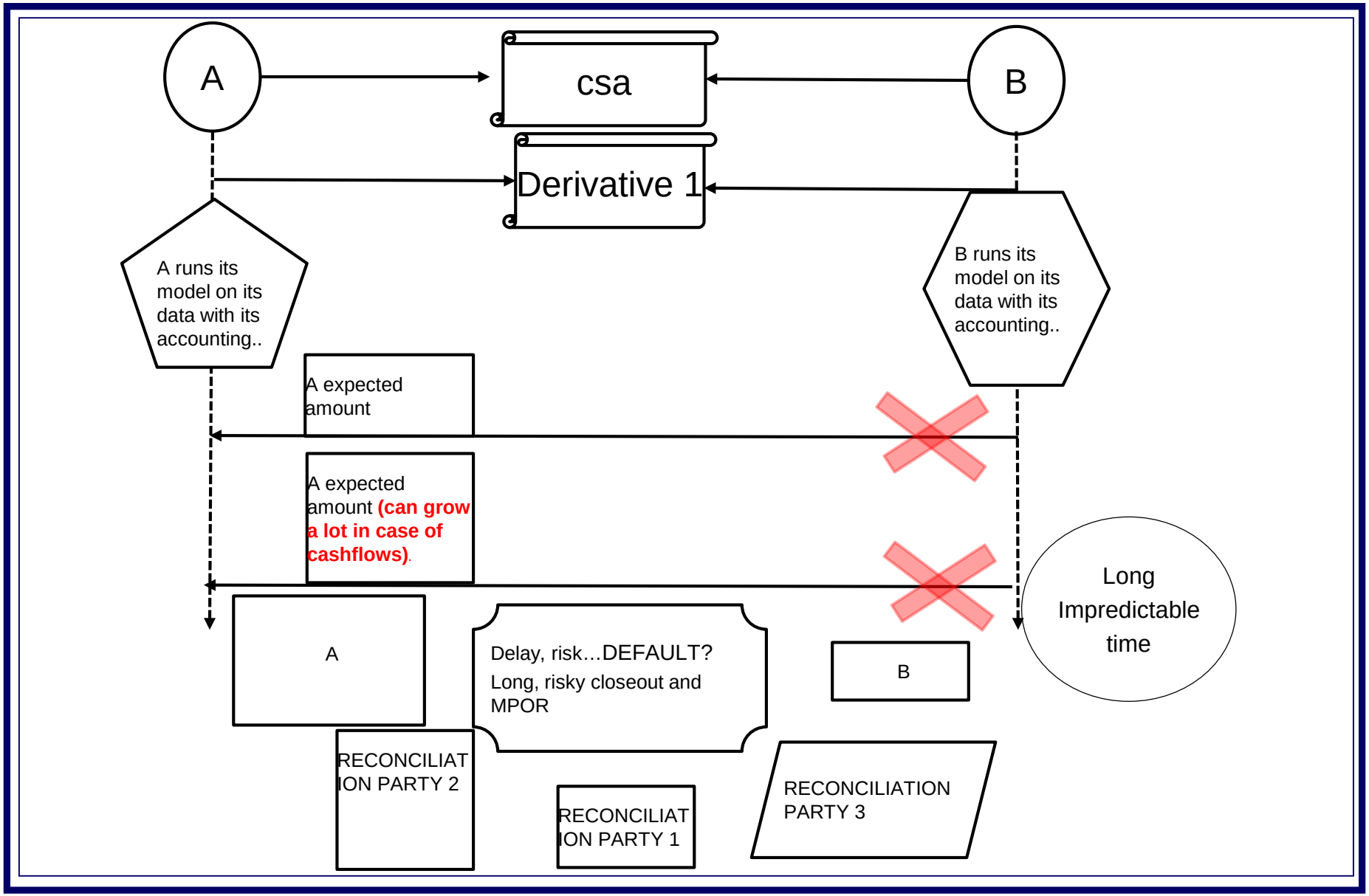
- **From Andersen, Pytkin and Sokol 2015**

Event	Date type	Notation
Observation date for the last margin flow by C	Observation	$t_C = t - \delta_C$
Observation date for the last margin flow by B	Observation	$t_B = t - \delta_B$
Date of last trade flow payment by C	Settlement	$t'_C = t - \delta'_C$
Date of last trade flow payment by B	Settlement	$t'_B = t - \delta'_B$
ETD	Observation	t

Parameter	Conservative	Aggressive	Classical+	Classical−
δ_C	15bd	7bd	10bd	10bd
δ_B	9bd	6bd	10bd	10bd
δ'_C	8bd	4bd	0bd	10bd
δ'_B	3bd	4bd	0bd	10bd

Table 2: MPR Periods for CSAs with Daily Re-margining

What if there are serious problems?



MPOR and Initial Margin

Variation Margin leaves delay between the **last collateral update** and the **closeout for liquidation** of a defaulting counterparty's positions. This delay is called **Margin Period of Risk (MPOR).**

MPOR is large since, when a default happens, there is no guarantee that the valuation of the residual derivatives, V_τ^A and $-V_\tau^B$, with τ being the default time, coincide for the two parties. The current process assume 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.

Detailed problems and possible solutions for derivatives collateral

The effect of the current state of affairs is that a large counterparty risk remains open even in interbank markets. This requires banks to keep large amounts of capital. This has led regulators to require counterparties to add an additional amount of margin, called *Initial Margin*, that is meant to cover the misalignment between variation margin and mark-to-market. Since misalignments are large, the Initial Margin is also large.

This amount strains the liquidity resources of banks; and it is still to be seen if this additional requirement will reduce risk effectively.

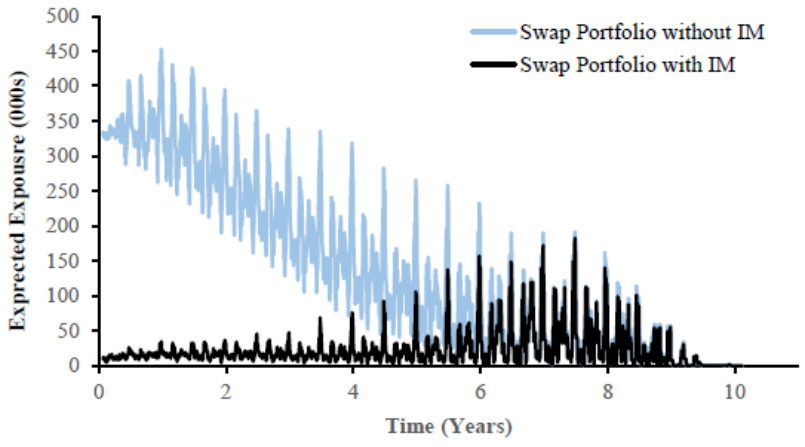
The recent paper (Andersen, et al., 2017), that got the Quant of the Year 2017 prize, computes that it does not, because it does not solve the crucial problem 4 of *Asynchronous Cash-flows versus Collateral.*

As a more radical solution, for many derivatives regulators have prevented market participants to trade directly with each other, requiring the presence of a central counterparty (CCP) in the middle of the two parties.

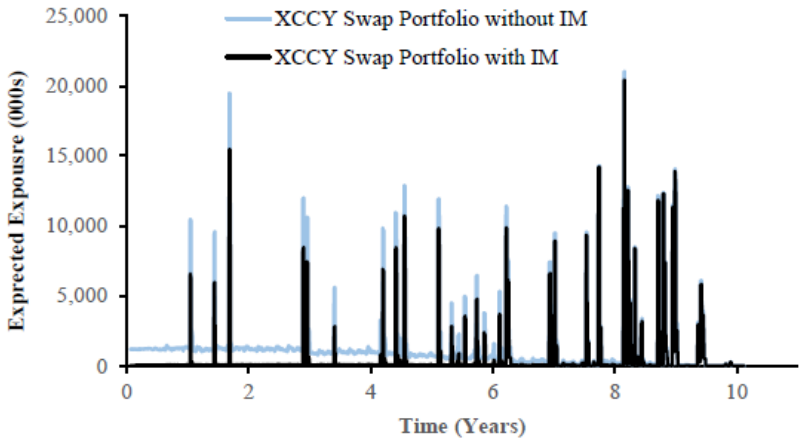
Detailed problems and possible solutions for derivatives collateral

- 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. **Andersen, Pytkin and Sokol 2015 find this is the dominant driver of counterparty risk and that standard Initial Margin does not cover it.**

(a) Regular Interest Rate Swaps

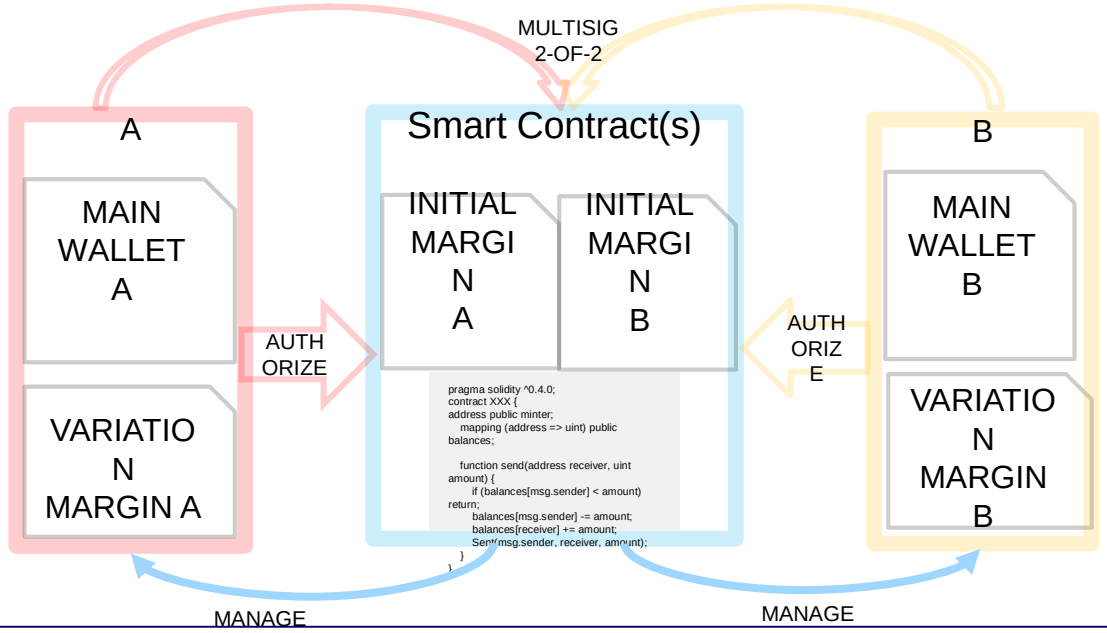


(b) Cross Currency Swaps



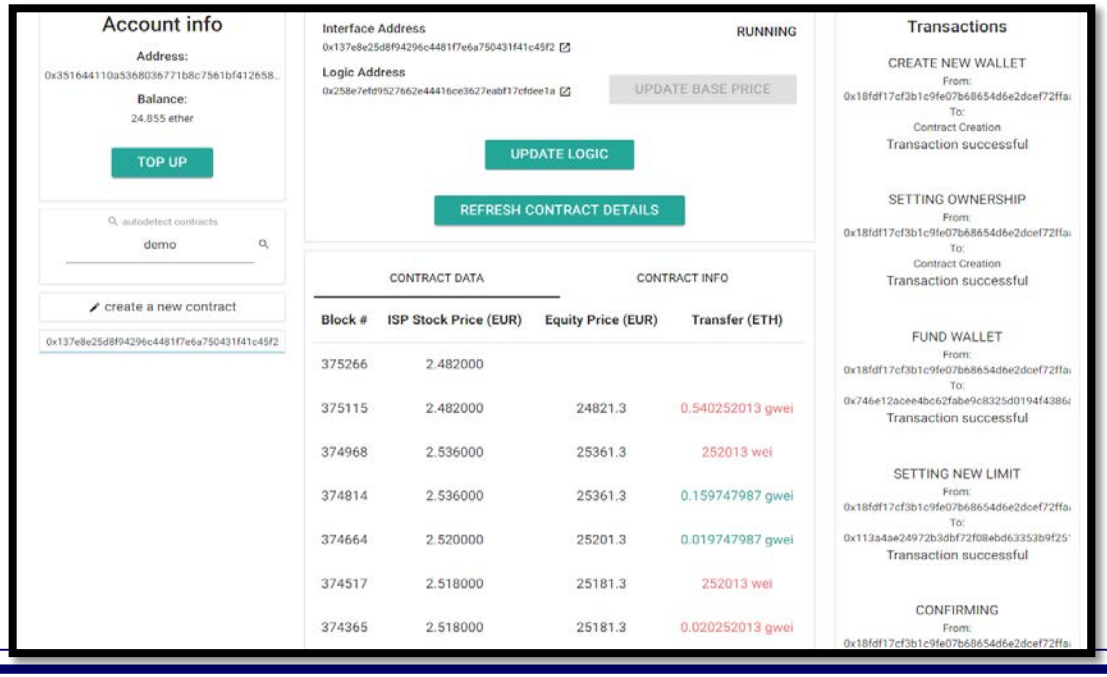
Detailed problems and possible solutions for derivatives collateral

- A DAPP (Decentralized Application) is built based on *multisig* wallets and smart contracts. A multisig structure uses cryptography to make wallets and contracts controlled by more than one private key. In the multisig used here, two private keys allow the two parties, if they agree, to fully modify and maintain the smart contracts. Lacking agreement, the smart contracts are fully autonomous. In the DAPP the management of the collateral flow is delegated to one such smart contract.



Detailed problems and possible solutions for derivatives collateral

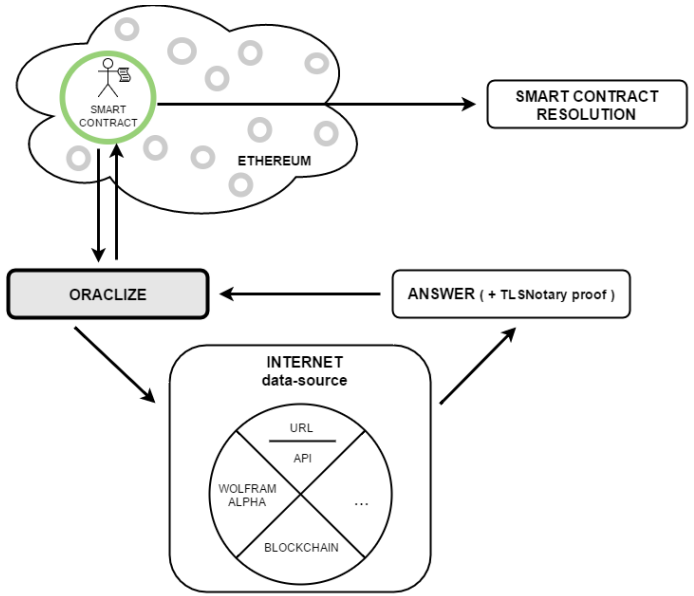
The contract keeps Initial Margin in direct custody within his own storage, since the financial logic of Initial Margin requires it to be used only at default and to be kept segregated and not accessible by the parties. The contract also receives an authorization from the two parties (that can withdraw the authorization at any time) to move the parties' Variation Margin payments, to and from specialized accounts, and takes charge of computing and transferring the due collateral amount based on an agreed algorithm. Variation Margin is akin to anticipated transfer of value, and needs not to be segregated, it can even be spent.



Detailed problems and possible solutions for derivatives collateral

- The smart contract implements the rules chosen jointly by the parties to collateralize the derivative, and incorporates a unique reference (a hash) to the algorithm required to compute mark-to-market. Computation of variation margin can for some derivatives become too heavy/specialized for Ethereum. In this case the contracts use a computation service provided by Oraclize, one of the most popular oracle services in the Ethereum ecosystem, that also provides the data required for computation.

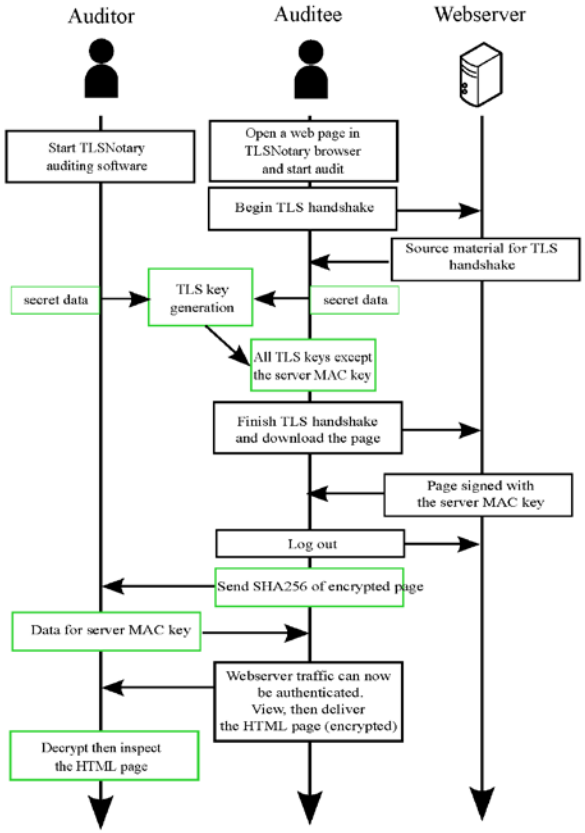
Oraclize acts as a node that receives a query from the smart contract, fetches data from the trusted data sources indicated in the query, process them through agreed software deployed on Amazon web services, and provides the desired result together with cryptographic proof of its honesty (the so called "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.



Oraclize – TLS notary

The smart contract includes an automatic rule, set at the moment of contract creation, in case of insufficient funds in the variation margin accounts.

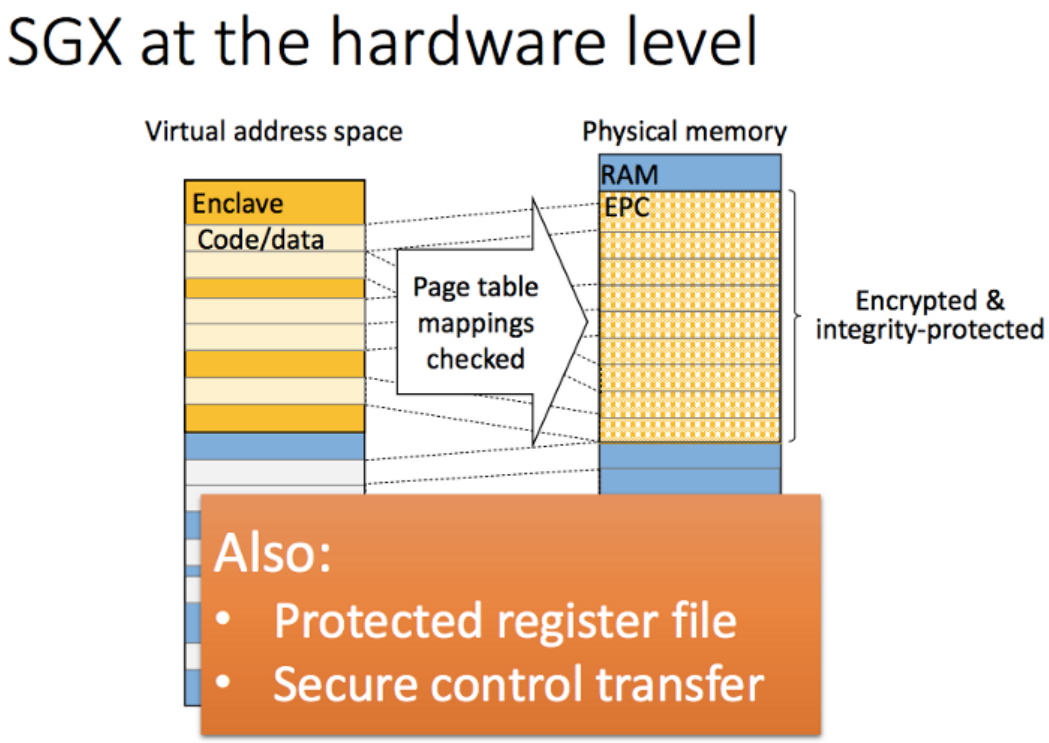
Oraclize on Ethereum provides Oracle services by acting as an intermediary between contract and external web source. Instead of provider co-signing you get data and a proof of honesty. It uses a modification of the TLS protocol (TLS-notary) that makes the communication server-client auditable and authenticated, with no need for the server application to provide any blockchain-specific integration; by splitting some of the cryptographic keys between auditor and auditee, it makes the session not forgeable by the auditee.



SGX

Similar services are probably sufficiently safe for many financial applications – in the sense that the credibility of the data provider is taken for granted and guaranteed communication with the chain is the issue. One can implement here algorithm selecting provider or other. It can also be used for “guaranteed” computation from clouds such as AWS or MS Azure.

Intel SGX extends this logic to a contract with a machine; providing prooof that exactly a given process has been executed in an aerea of memory, and nothing else. Application to finance beyond Blockchain…



Using a smart contract to close the gap

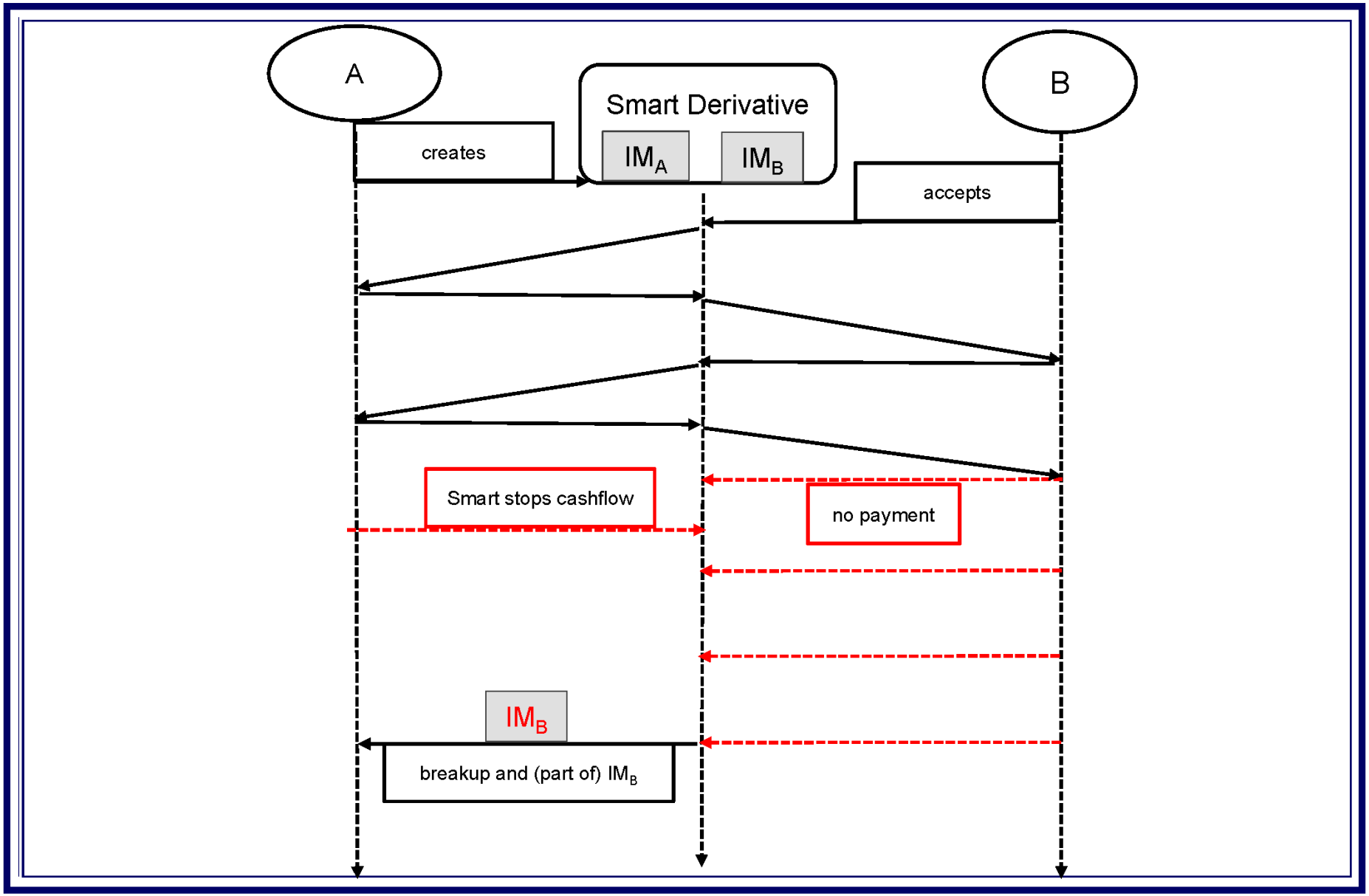
- ***Technical Complexity:*** blockchains level the playing field, eliminating the limits that currently some players have in managing fast liquidity transfers and a multiplicity of depository account. **As nodes of the same blockchain, banks, corporations, funds and households have all access to the same payment and account technology**
- ***Collateral Misalignments***: the technology for calculating collateral amount, that cannot be incorporated in traditional paper contracts, can be incorporated in a digital smart contract. Once the parties have agreed on the smart contract code**, the same algorithms will be executed for both parties, eliminating by design the asymmetry** that currently prevents many players to access state-of-the-art collateral practices. **Moreover, having agreed on a detailed piece of code, misalignments between two parties are ruled out by design.**
- ***Settlement Delays***: The experiment brought the time between exposure measurement and blockchain settlement **from the few days of the traditional business model to few minutes**, although costs (Gas, Fees, Oracle, Cloud) suggest few hours are a reasonable timing.

Using a smart contract to close the gap

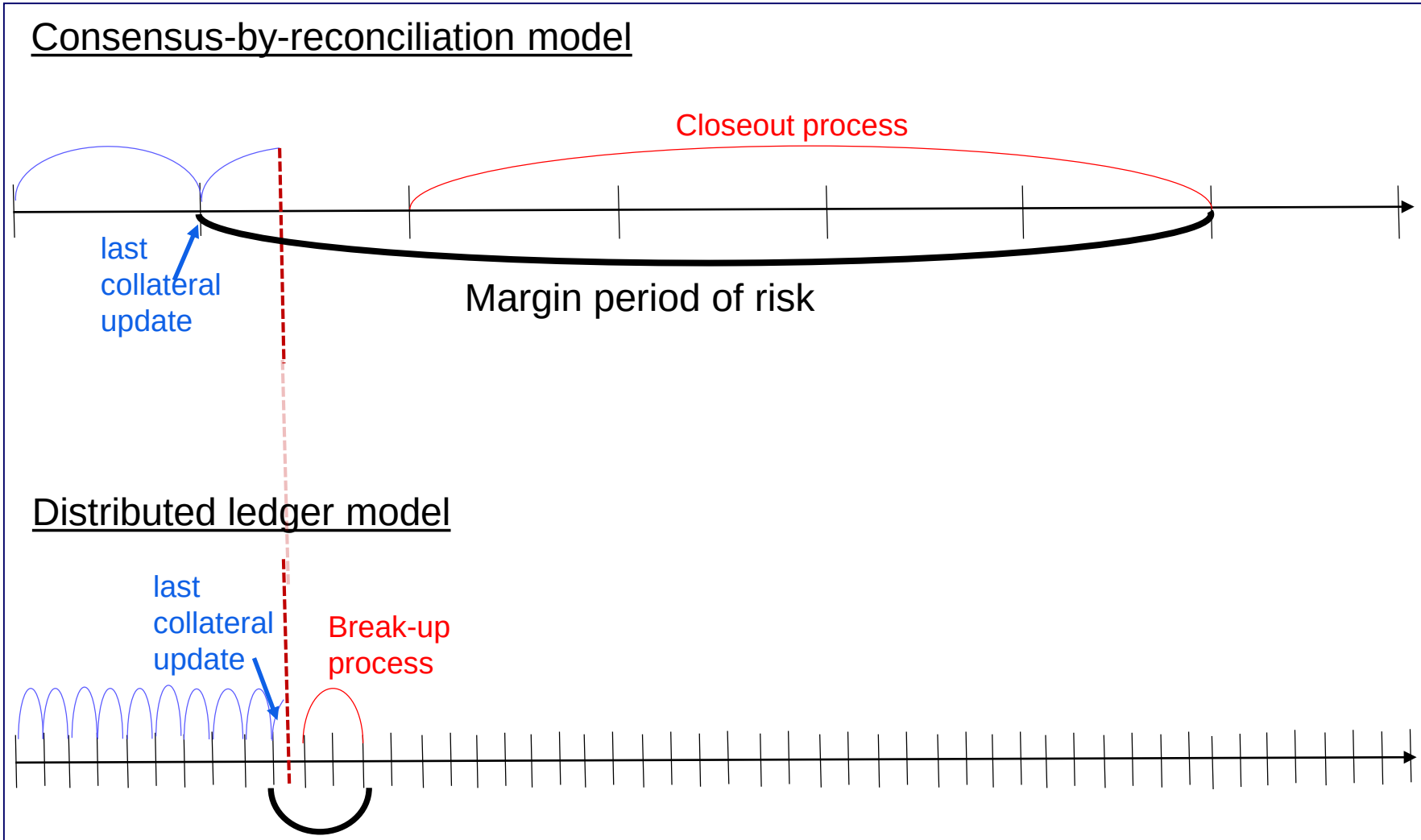
- *Asynchronous Cash-flows versus Collateral*: **the smart contracts can act as an escrow and withhold cash-flows until collateral is available, and make the two payments simultaneous like the DvP example**.

- *Default Uncertainty and Delays*: Smart contracts can incorporate automatic covenants when there are signs of counterparty credit problems. A smart contract can intervene, with a procedure pre-agreed and pre-signed by the parties, if a counterparty delays its payments, with no need to wait for long legal processes. **The covenant in (Morini, 2017) unwinds the contract when one party delays its payments by more than a pre-agreed grace period. The Initial Margin is used by the smart contract to cover the possible shortage of Variation Margin upon unwinding, as prescribed by current regulations**. The Margin left after this in the smart contract storage is returned to the parties.

Collateral Workflow on Blockchain



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



Centralization and Decentralization

Few 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.

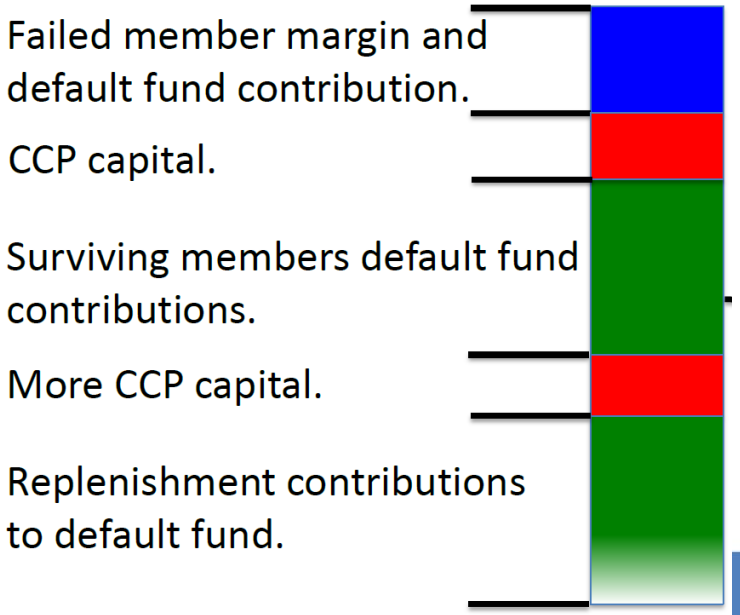
- CCPs have become “increasingly crucial” due to mandatory clearing regulations, so much that is “imperative” that they are resilient to stress events to “ a very high probability”, which means a very low probability of default for any of them.

- 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 the existenc of such model makes a better risk balance… so far, however, they will stand for CCPs, that granted standardization and transparency for them.

- **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.

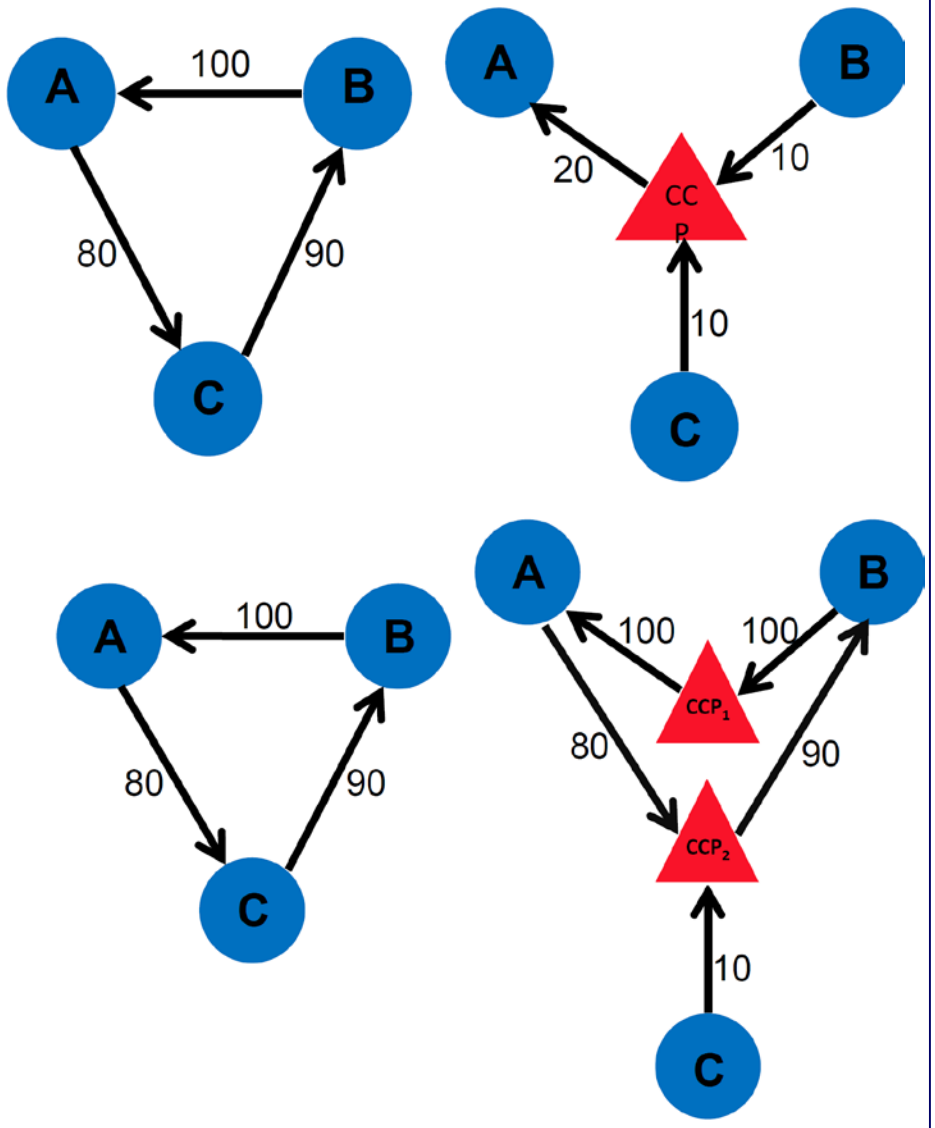
https://isda.derivativiews.org/ say that in case of serious stress for a CCP it would be crucial to maximize certainty and predictability by following a precise sequence of loss allocation and position allocation tools, already defined by ISDA. Transparency, with indicators defined upfront and followed 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 a lot benefit! (Duffie 2015, Basel).

Some proposed Blockchain for netting across different CCP, and availability of IM and DF where it is needed across CCPs.



Few more words on CCPs

- CCPs may adopt private forms of blockchain technology. They may take three approaches, in increasing order of disruption.
  - A CCP may use financial cryptography tools like hashing, digital receipts and smart contracts to make its business process more streamlined and auditable.
  - Alternatively, a CCP may keep its business model but try to get savings through tokenization of collateral and faster blockchain settlement.
  - This is mutualization technology: we can mutualize capital, data, computations, collateral, ratings… in a world where banks may face the competition of internet giants, each one dominating its own market, a technology for mutualization of processes, resources and risk management through distributed automation rather than centralized exchanges/CCPs or custodians is interesting for banks. Yet…

Few more words on CCPs

- We are not yet ready to imagine a business like central clearing managed as a DAO: the fear that this DAO could behave in an uncontrolled way would cloud any prospective advantage. Yet, there would be a simple way to address such a fear.

- The institution that today runs a CCP could transform its role into the one of institutional “guardian” of a DAO CCPs. It would give away the massive operational risk of being the counterparty of all trade, but would remain, thanks to the appropriate keys and cryptographic rights, ready to act effectively when signals are given of credit risk and automated recipe is deemed not appropriate or not sufficient. This way the CCP would take the more natural role of a veritable counterparty of last resort.

Privacy solutions for Public and Private Blockchains

Homomorphic Encryption. The RSA example.

Zero-knowledge proof is the possibility to prove the truth of a statement without revealing it.

It often uses the fact that some forms of encryption are homomorphic to some operations, f(ENC(x))=ENC(f(x)).

For example, with RSA the product of the encryptions of two messages is equal (modulo n) to the encryption of the product of the messages, since, using $\left[.\right]_n$ to indicate MOD n, we have

$$\left[a * b\right]_n = \left[\left[a^k\right]_n * \left[b^k\right]_n\right]_n$$

For example, if a=3 and b=2, with the above encryption with public key (n=77,k=17), we have that ENC(a)=75 and ENC(b)=18. We know a*b=6, and we can compute ENC(6)=41. We also know that ENC(a)* ENC(b)=75*18=1350.

Notice that in fact 41 MOD 77=41, and 1350 MOD 77=41.

Look at zk-snarks for generalization, and more interestingly to Pedersen commitments for additive homomorphic encryption.

A hint at zero-knowledge SNARKS

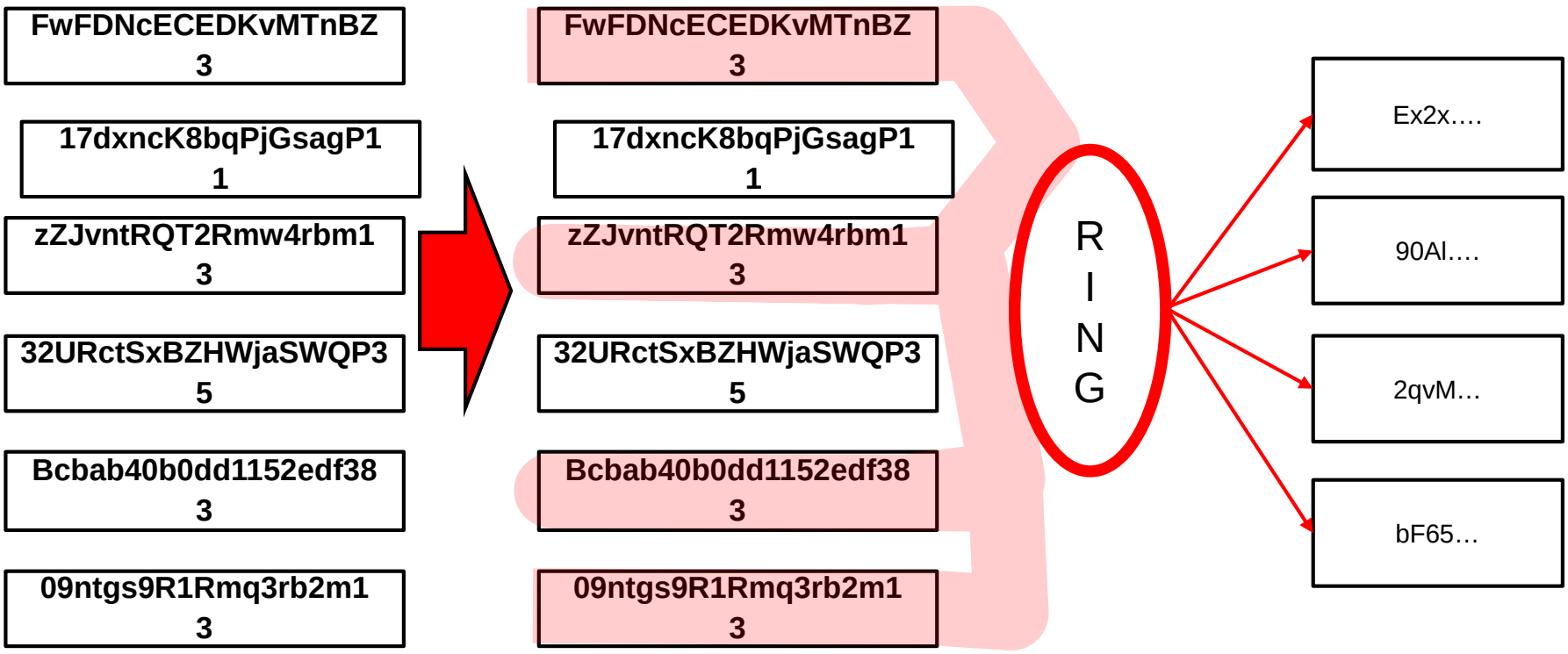
In the so-called zk-snarks (Zero-Knowledge Succinct Non-interactive Arguments of Knowledge), **one can prove that a given transaction is valid (public key A is moving an amount X which belongs to A and is not double spent to B) without knowing A or B or X.** It is still a complex procedure, based on fact that *transaction verification can be simulated by* an NP-complete problem, for example *proving one knows t,h,w,v polynomials such that t(x)h(x)=w(x)v(x), without revealing t,h,w,v.*

This translates into the following zero-knowledge verification:

- the verifier (the validator of a cryptocurrency) chooses two secret points to verify, so truth to prove reduces to t(s1)h(s1)=w(s1)v(s1) and t(s2)h(s2)=w(s2)v(s2).
- with encryption algorithm E homomorphic to the above f(s) functions, the verifier can give to prover only E(s), which allows prover compute E(f(s)) as f(E(s)), since they are equal. So he gives to prover E(s1), E(s2).
- the prover gives E(f(s1)), E(f(s2)) for all fs. The verifier can check, also on the encrypyted version, that in fact t(s1)h(s1)=w(s1)v(s1), t(s2)h(s2)=w(s2)v(s2), and also that in fact f(s1), f(s2) come from the same polynomia function f's with the above properties, without knowing the f's themselves…
- …and actually there is more!!

There also computationally lighter alternatives.

A hint at Ring Signatures



Bitcoin is organized via Unspent Transaction Outputs (UTXOs).

All those with same amount (3 in example) become part of a RING. Rather than individual signatures, now these UTXOs are given RING SIGNATURES, that only prove that someone in the RING has signed.

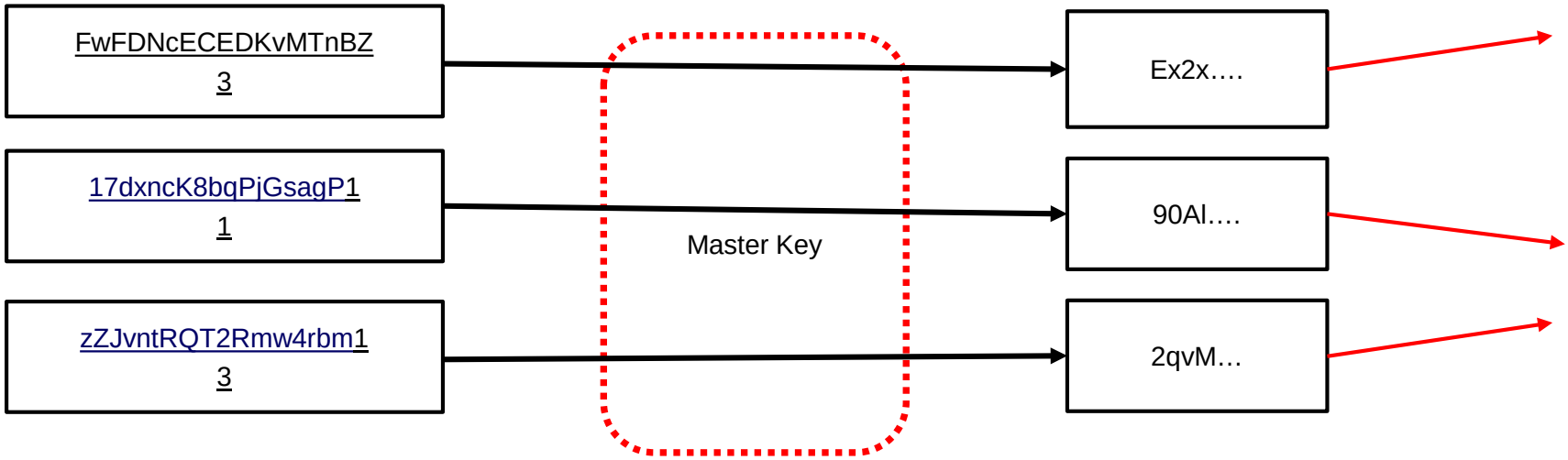
Thanks to Linkability, one can verify that each signature is used only one. Once they have all been used, the RING is empty and there is no more to spend. This obfuscates sender.

A hint at Stealth Addresses

What about the RECEIVER? Is there a way to hide it too?

Yes. The RECEIVER can identify itself by a STEALTH ADDRESS. Stealth addresses are identified by a MASTER public key to which one cannot send money directly. Yet the MASTER key allows that payer to generate ADDRESSES that can actually then be spent by the RECEIVER.

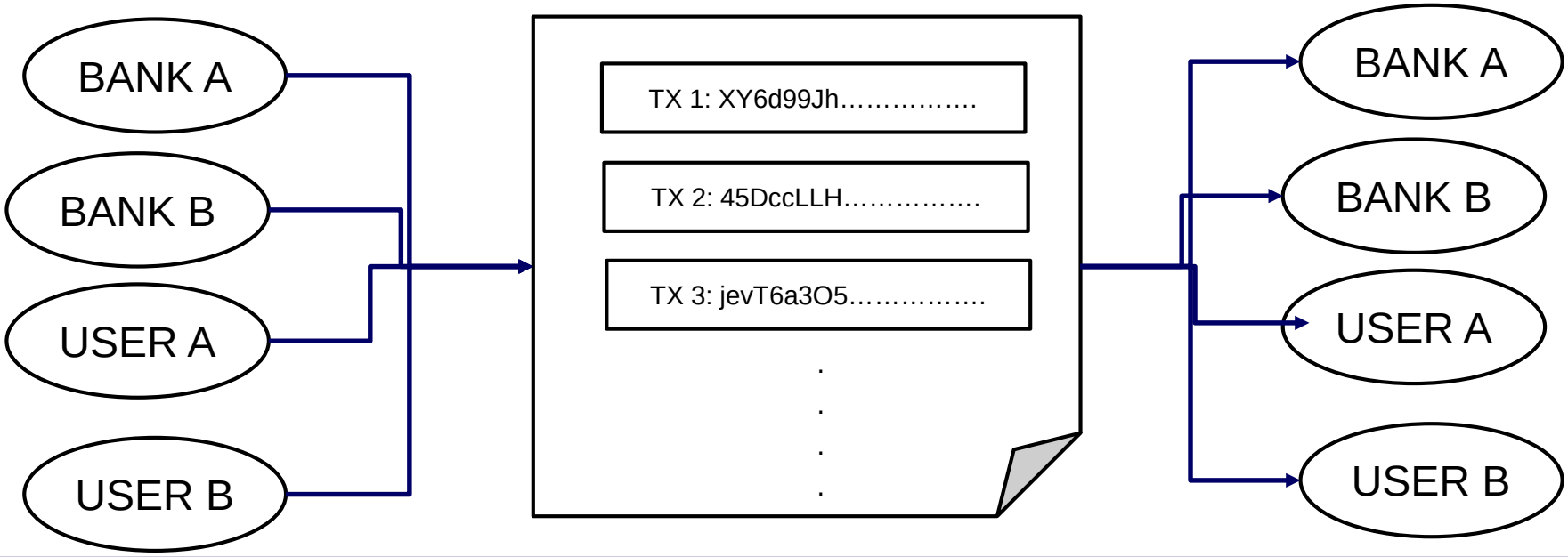
All the payments below are addressed to the same receiver, but payers have used the receiver's master key (and a secret) to create addresses that are controlled by the receiver, in the sense that he is the only one who can spend them (master private key), while no one else can recognize they are associated to the receiver.



A private public chain

The final purpose is to have a blockchain where identities are visible and unencrypted, while transactions are visible but encrypted. They can be verified without breaking privacy, unless one is a regulator that has been given a key to see transactions unencrypted.

Privacy can coexist with decentralization.



Disclaimer

Thank you!

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