Torino, FPDapp, August 28, 2018

Decentralized Financial Markets

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…

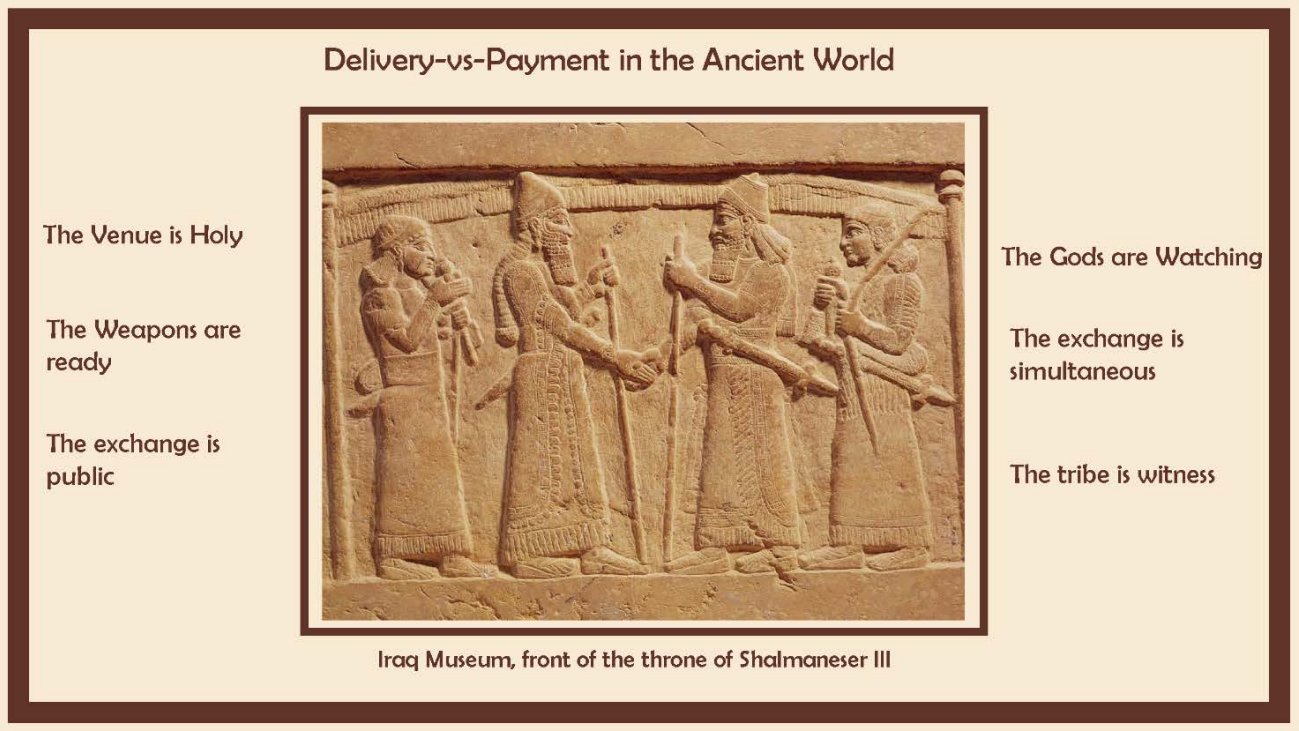
- 1988: Tim Berners-Lee invents the Word Wide Web in 1988.
- 1999: the future Nobel Prize Paul Krugman could still predict a negligible impact of the Internet on future economy
- How was that possible? In the first 10 years of the internet that fantastic idea was already on display, but a good deal of 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, 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 and consensus. Large public blockchains use proof-of-work, unfit for the regulated world, those that should be regulated (private) are still researching.
- Public Blockchains work because even if they lack privacy, you can work around the problem hiding your legal identity. In a regulated environment this is inacceptable, so you need privacy to have the identities. And privacy should cohexist with decentralized validation… some good solutions seen only short ago...
- Scalability: the tech setup, with all nodes keeping a version of the blockchain and in principle verifying all of it is not very efficient, let alone the overhead of proof-of-work. Solutions under development.
- Removing intermediaries is at odds with current regulations of markets, that give specific roles to middlemen which are no more necessary in blockchain. Regulators must understand and update.

From the fundamental problem of trading…

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.

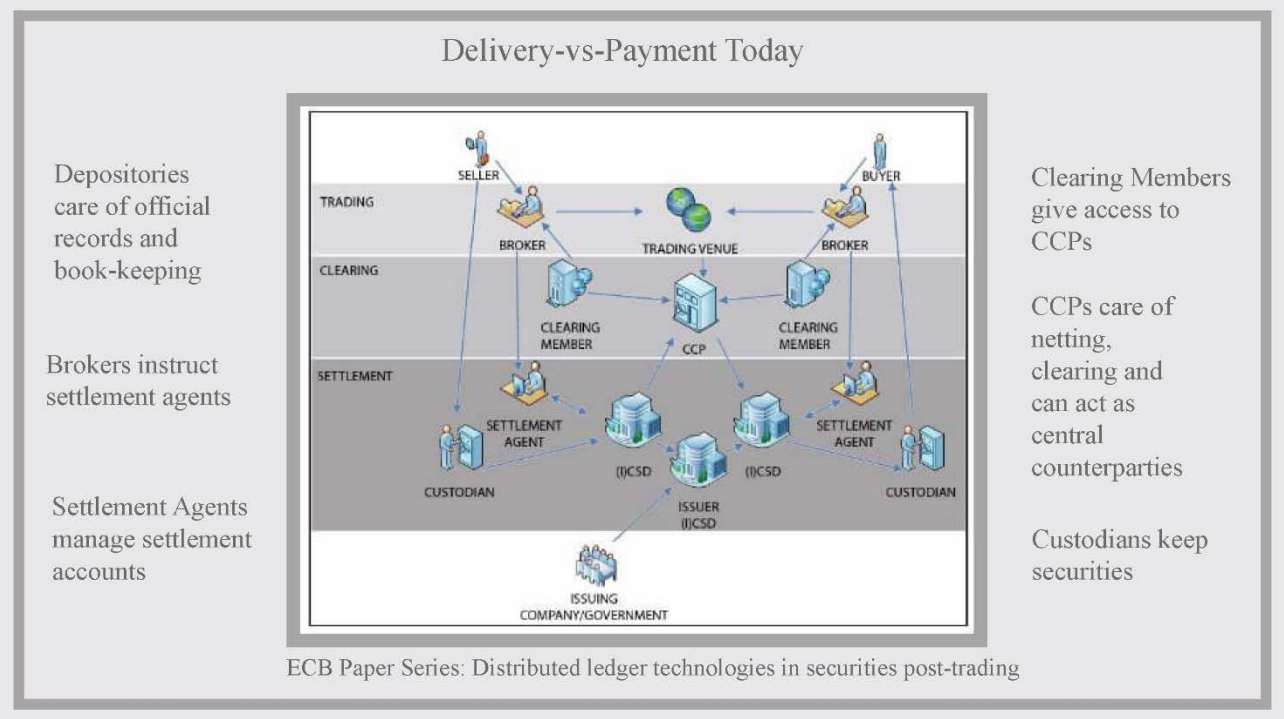


The issue of Delivery-versus-Payment resurfaced after the great explorations of 16th and 17th centuries, when it happened that merchants had to arrange trades which were not for now and face-to-face, but between counterparties living on either side of oceans, and for future delivery.

*

From the fundamental problem of trading…

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…

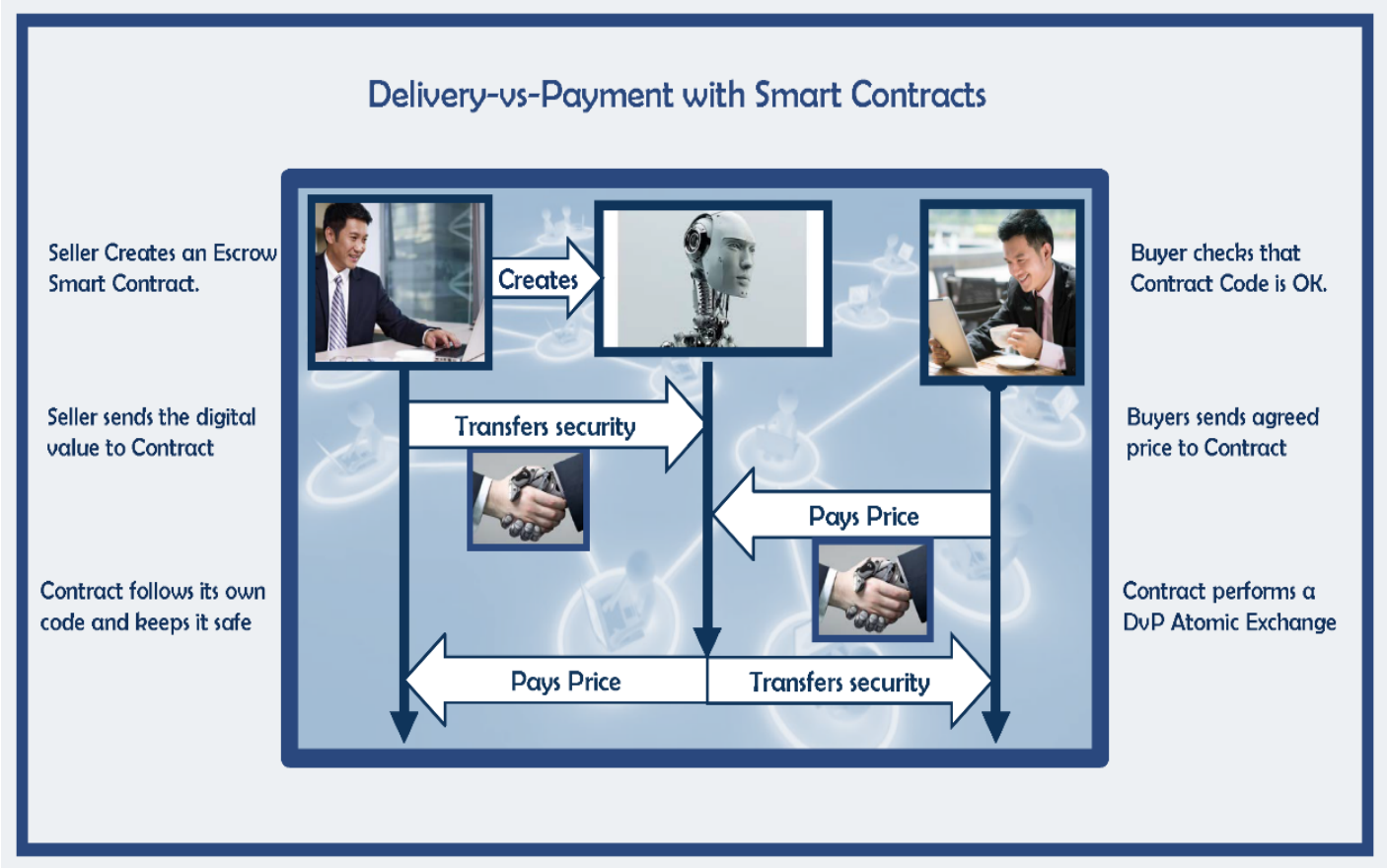


1. Registrars and Depositors perform the notary function: keep official record of who owns each security.
2. Depositors together with Custodian banks provide securities accounts and custody services.
3. Then there are Securities Settlements Systems, that make DvP possible.
4. Central Security Depositories (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 integrate, it took 10 years to complete.

*

Transforming Securities Markets

Smart contracts could change the game. They issue tokens, maintain a public immutable registry, custody is in the firm of private keys, and arrange DvP working as escrows.



Ethereum

Let’s make an example of how a smart contract is useful. Party A can create a smart contract SC that works like that:

«Hi, I’m Robot escrow (RE2016), a smart contract of the last generation. I have just been created, and I have been created with an Intesa bond in my possession. I execute this operation: if whithin 24h I receive 100 ethers from a sender, I will transfer the bond to the sender and 100 ethers to my creator. Otherwise in 24h I will send the bond back to my creator, Mr A.»

Notice that, even if Mr. A is the creator of the contract, as duly recognized by RE2016, a normal contract has no owner. A cannot modify the contract after creating it or destroy it or get money back.*

There is an instruction the creator can later destroy the contract and get money back, but not very much used in the Main network: «Build unstoppable applications» is the motto.

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…

This has shown weaknesses of smart contracts, and hinted at governance solutions...

*

We know the robots…

On June 17 2016, about $45 million were drained by an unknown attacker from one of the largest pools of money on the Ethereum blockchain, TheDAO. It was a decentralized crowd-funding application where participant contributed digital money to be 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, this amazing idea collected over $150 million, until someone found a «bug»…

*

TheDAO…

- The bug allowed a smart contract to withdraw his money from TheDao with a transaction and then, before the first transaction was closed and the balance updated, make another transaction to withdraw his money again, in a loop…Loops are dangerous, as Satoshi knew…
- There are solution, but bug was natural in Ethereum design: the fact that sending money in Ethereum also makes the recipient run arbitrary code that can send further messages. This is the flaw exploited by the hacker.
- Hacker could not withdraw money before a 27 day grace period (the smart contract was doing his job) and this gaver Ethereum community time for debate:
  - For the majority, a decision of the majority of nodes had to subvert the «thief» transactions… like a high court!
  - For purist, contract code is law! What code allows, must be immutable. They use now old chain with hacker money.
- There was a hard fork. 90% changed client version and erased «stolen» money, 10% remained on original chain. Through market forces, value distributed proportionally to the two chains!

*

Public Blockchain Tech: Issuers

1. A smart contract allows the issuance of digital assets. A contract X can create a new digital asset X, by creating a list that records how much every address owns of the digital asset X. At creation, all the Xs will be listed at the address of the issuer(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 rules in the contract.

3. For the life of a digital asset, the associated contract 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 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.

*

The technical form of Tokens:

The current standard is called ERC20, and it was introduced to make it simple to manage tokens for decentralized applications like exchanges, escrows, and the thousands of other applications under development. It defines all the functions a smart contract must implement to create a token. They are

1. The notary function, represented by the list of owners mentioned above, and the functionalities to query it.
2. The function to allow an owner to transfer part of his tokens to someone else. When the owner is happy to execute this single leg, he does not even need any exchange, neither traditional nor decentralized, he just does it from his wallet using ERC20 functionality..
3. A set of functions to allow an owner to give to a third party the right to handle his own tokens up to a given allowance. This is a functionality that can be used to create transparent and controlled escrow or exchange services.

*

Public Blockchain Tech: DvP or Atomic Swaps

With the toolbox of smart contracts and tokens, it is possible 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.

Public Blockchain Tech: Interoperability

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).

*

Public Blockchain Tech: : Exchanges

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

*

The current Derivatives Market

A bit of history…

RSS Feeds | Email Subscriptions | Plugins | Glossary | Forms & Submissions | Careers | Contact Us

U.S. COMMODITY FUTURES TRADING COMMISSION

ENSURING THE INTEGRITY OF THE FUTURES & SWAPS MARKETS

Go

Advanced Search | Search Tips | Site Map

ABOUT THE CFTC | PRESS ROOM | MARKET REPORTS | CONSUMER | INDUSTRY | INTERNATIONAL | LAW & | TRANSPARENCY

Home // Press Room // Speeches & Testimony

PRESS ROOM

- Press Releases
- In the News
- Speeches & Testimony
- Events
- Press Room Archive

Speeches & Testimony

- Chairman Timothy G. Massad
- Commissioner Sharon Y. Bowen
- Commissioner J. Christopher Giancarlo

SPEECHES & T

Keynote Addre
Before the Cat
Decentralized F

"If Allowed to Thrive

April 12, 2016

Introduction

Good morning, ladies ar

Before I begin, let me sa
the Commodity Futures
staff.

It is a pleasure to be he
currencies, one of the r
technologies.

Notwithstanding today's
Rather, I want to focus
That is the technology c
may have enormous imp
regulators.

Lack of Counterparty

To begin, I want to take
markets. An enormous
rife about imminent inve

I was on Wall Street, se
default swaps (CDS), th
floor trying to maintain c
exposure of several ma
the hour. It was clear th
that the CDS markets w

Now, let's fast forward
do not have full visibility

It is not for lack of hard
crisis was the reporting
CFTC, started that initiat
complete picture of glob
reporting protocols and
impossibility of a single
to recreate a real-time l

CoinDesk

TRENDING
Consensus 2016 Live Stream

BITCOIN PRICE INDEX (24H)
$452
$449
$445

USD 0.59% ▲ $451.19
EUR €395.21

CNY 0.75% ▲ ¥2,925.13
GBP £311.80

NEWS | PRICE & DATA | GUIDES | EVENTS | RESEARCH | PRESS RELEASES | CONSENSUS 2016 | Search

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

241 | 57 | 7 | 46 | 1

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*

DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

Email Address SUBSCRIBE

FEATURES

Winklevoss Brothers Own 'Material' Amount of Ether

Derivatives. The problems, today.

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

Derivatives are agreements for future payments whose value (mark-to-market) changes every time the underlyings move. Default of one party can be loss of the market-to-market. The most popular way to address credit risk has been **collateral**. If Variation Margin was

A. equal in every moment to the mark-to-market of a derivative, through frequent collateral exchange.
B. paid in liquid assets and made immediately available to the counterparty as soon as a party defaults

the product would be virtually risk-free. Unfortunately, today collateral agreements are very far from this ideal situation.

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.

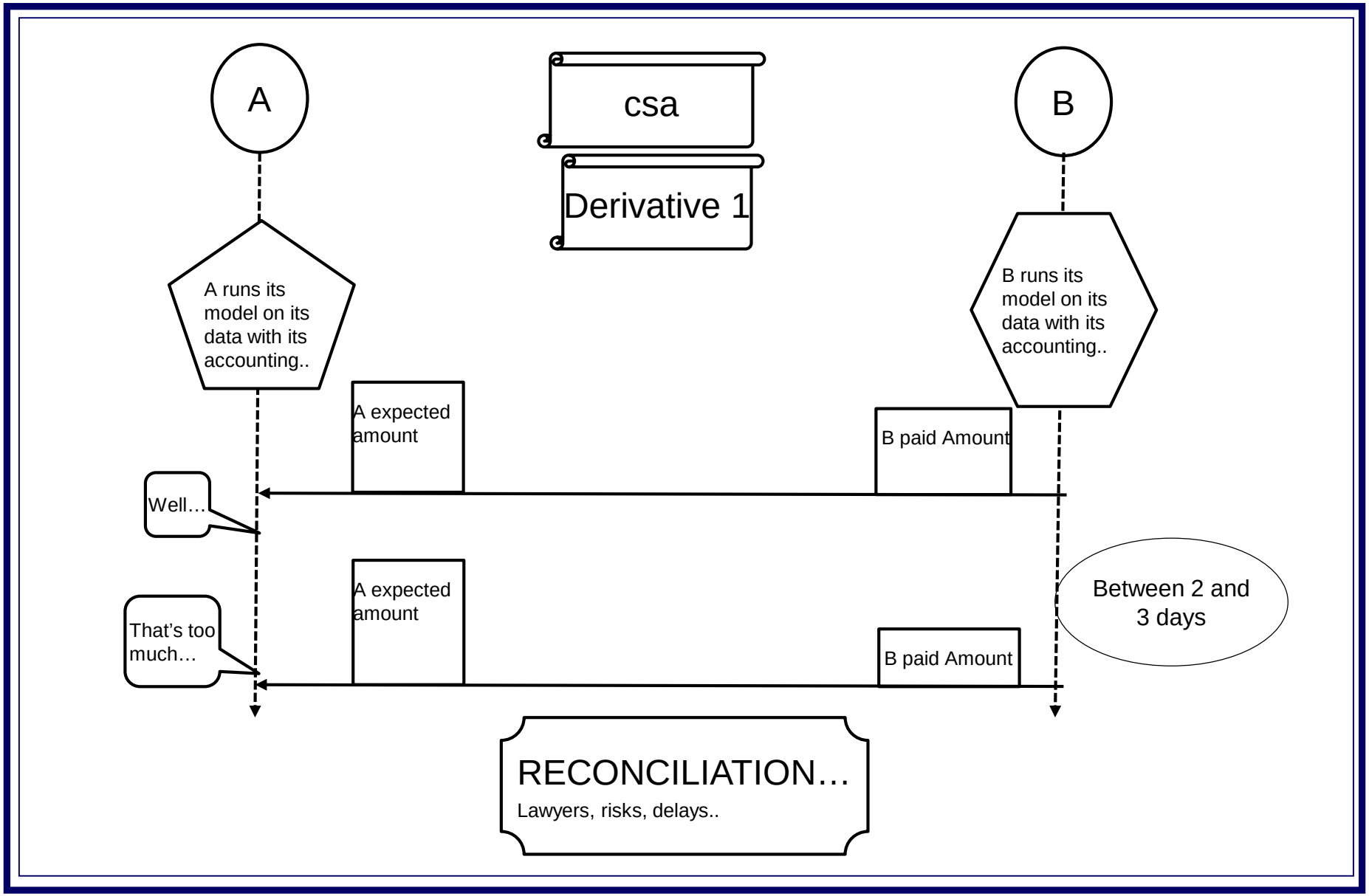
Derivatives. The problems.

- ***Technical Complexity*** Top collateral agreement requires the capability ansfer liquidity easily across accounts with particular features, access a variety of input market data, and use properly valuation/risk models. Corporates and funds usually do not have such capabilities, only banks have good agreements.

- ***Collateral Misalignments***. Even banks do not get perfect risk protection, mainly because *the two banks still use very different data and models,* so for a party variation margin can be 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.

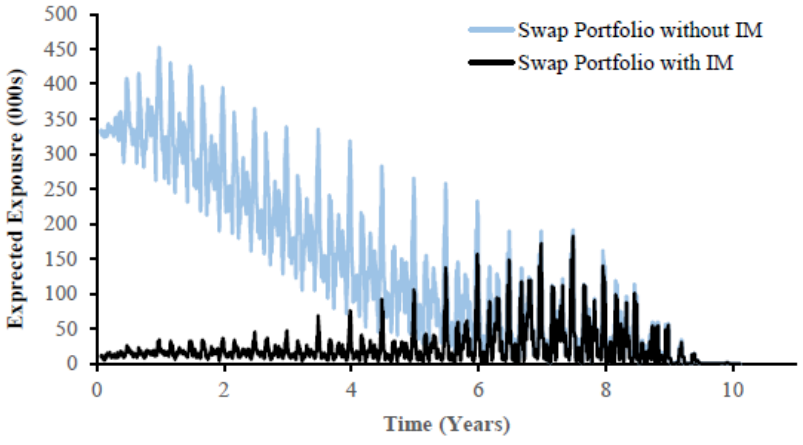
Derivatives Collateral exchange process



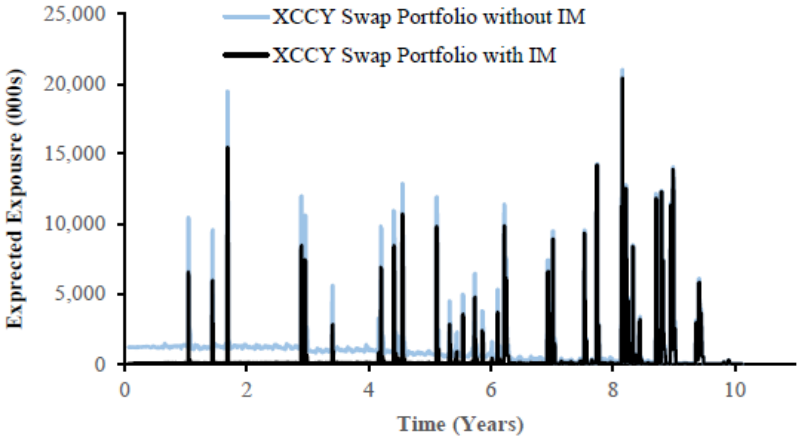
Collateral and Cashflows misalignment

▪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



Derivatives. The problems.

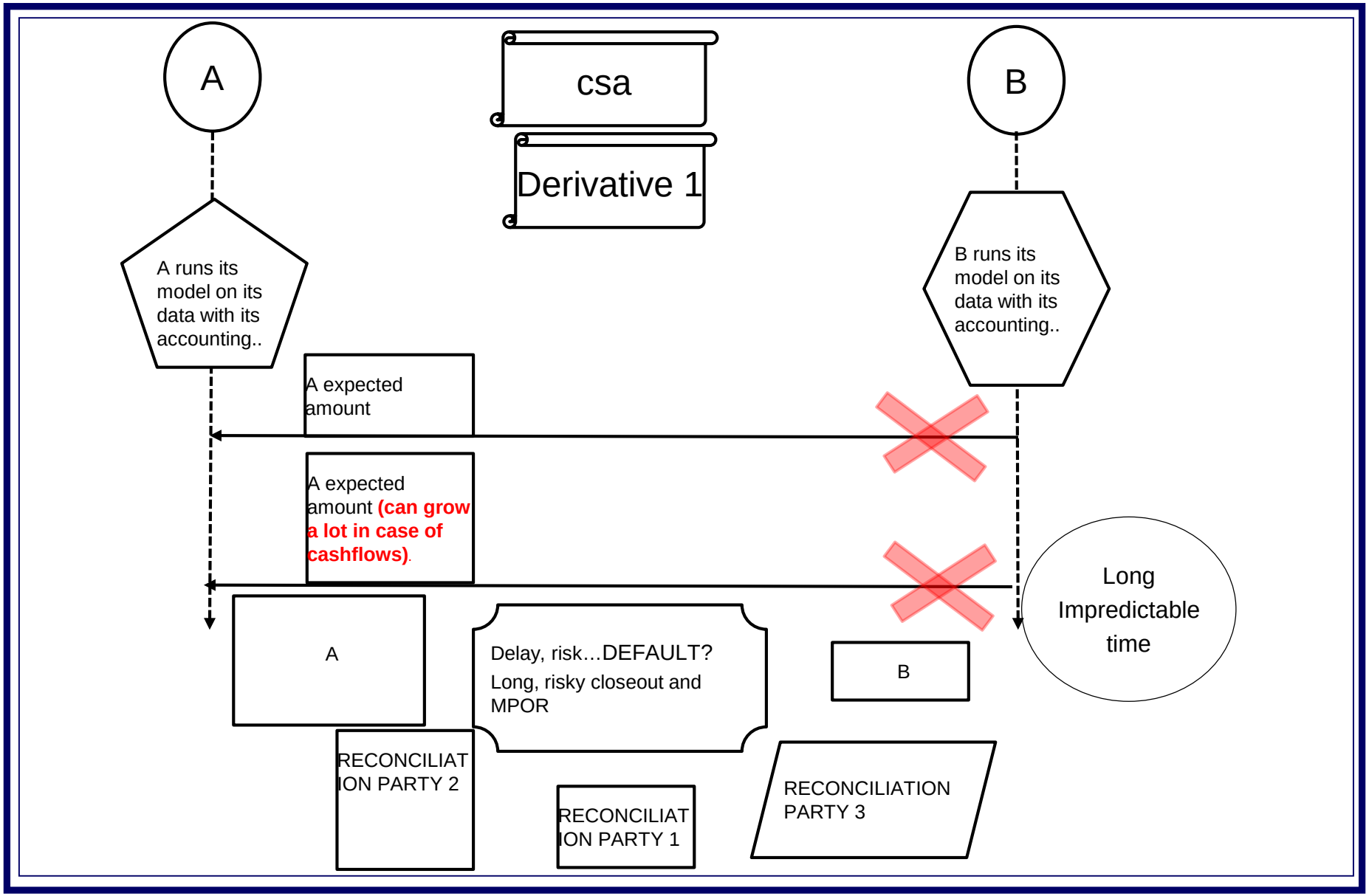
■***Asynchronous Cash-flows versus Collateral***. In many derivatives there are various cash-flows to be paid regularly from one party to the other. Every time there is a cash-flow payment, the mark-to-market of the derivative jumps by an amount equal to the cashflow payment. Collateral should have a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

This leads to long *Margin Period of Risk* and expensive, and not fully efficient *Initial Margin (regulatory excess collateral)* requirements.

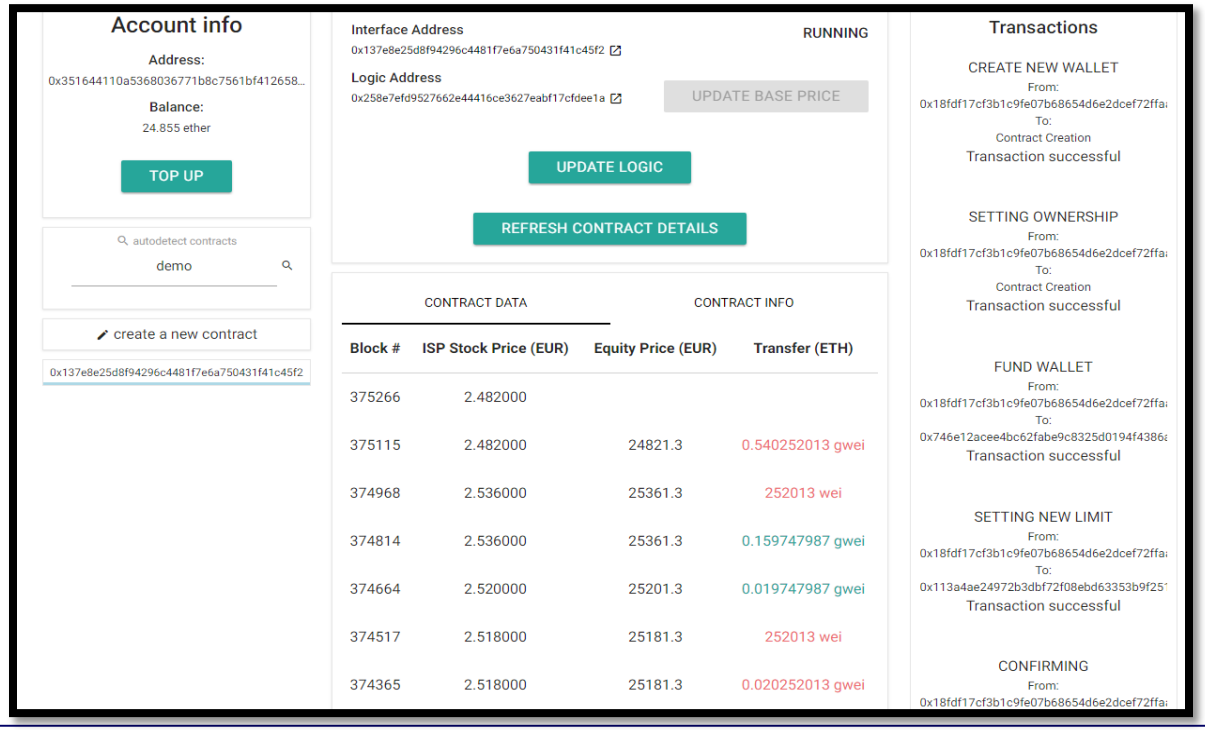
What if there are serious problems?



How Derivatives may look like in the future

Derivatives… the future?

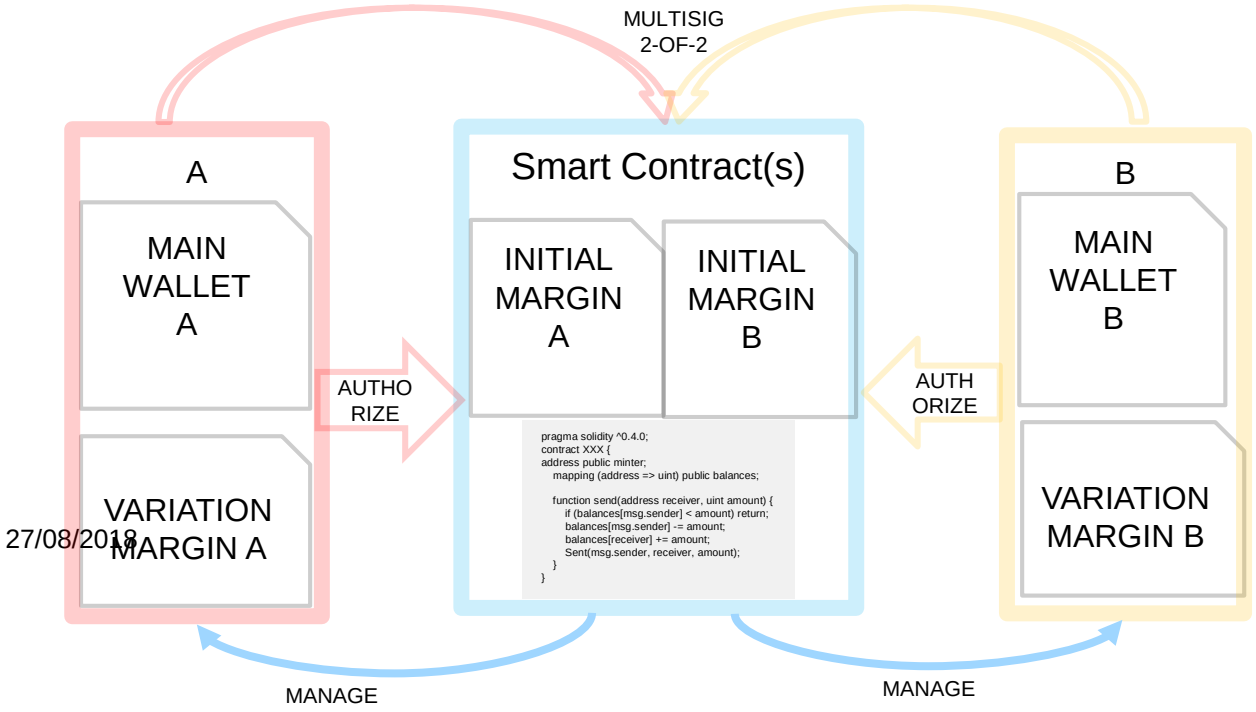
- Why looking at blockchain technology? For its features of autonomous execution of **digital smart contracts, settlement by consensus, and decentralization.**
- We developed a Decentralized Application based on *multisig* smart contracts that two parties, if they agree, can control. Lacking agreement, the smart contracts are autonomous. They manage collateral.



Smart contracts for collateral on Ethereum Testnet

The contract keeps **Initial Margin** in direct custody within his own storage, since the financial logic of Initial Margin requires it to be kept segregated and not accessible by the parties.

The contract receives an authorization from the two parties 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.

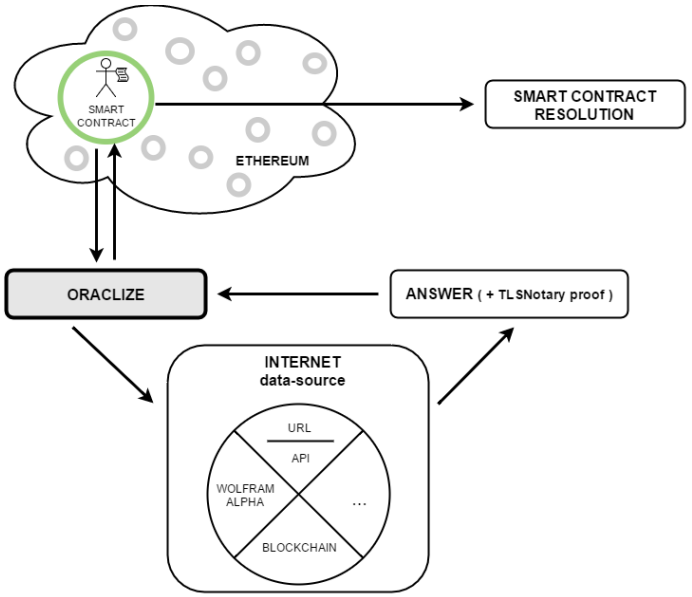


Trusted Execution Engines

■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. The smart contract includes an automatic rule, set at the moment of contract creation, in case of insufficient funds in the variation margin accounts: **it terminates the contract and uses Initial Margin to cover the gap**.

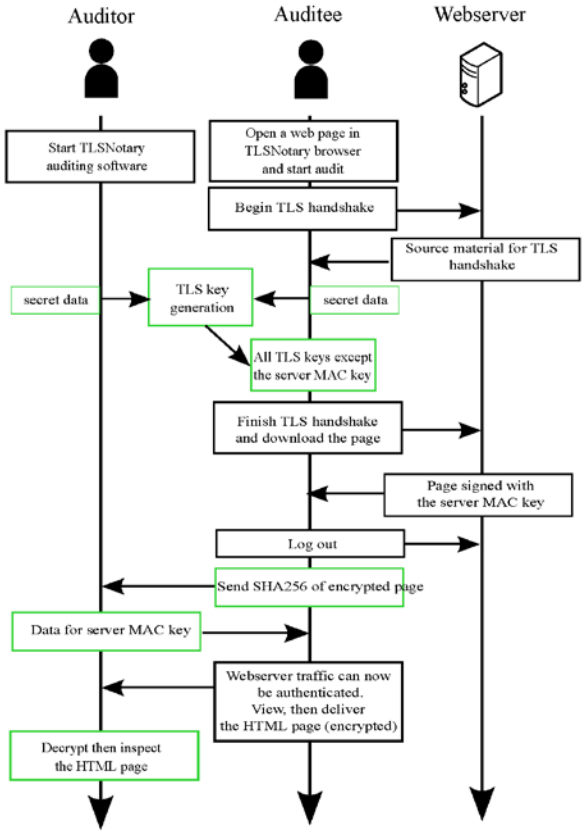
■Computation of variation margin can for some derivatives become too heavy/specialized for Ethereum.

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.



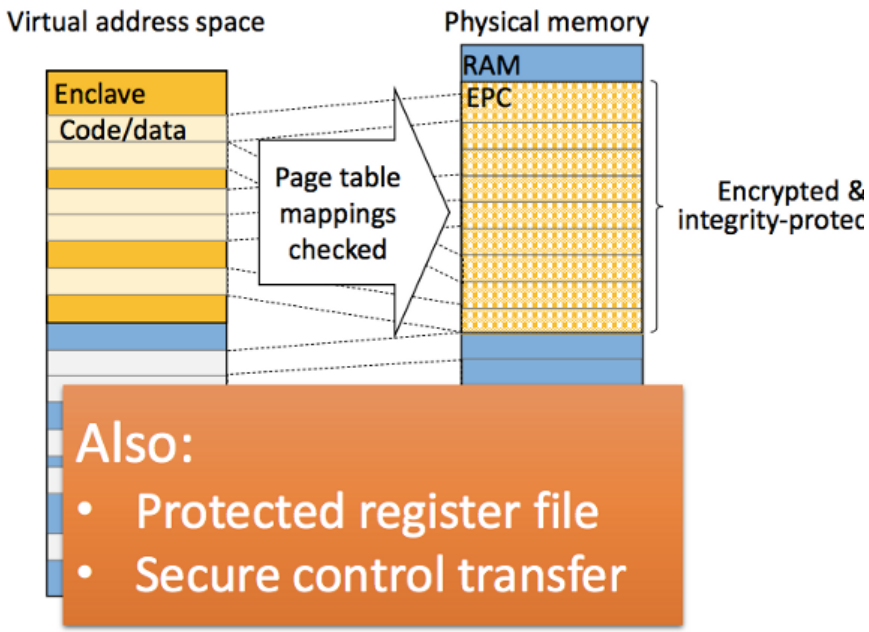
Oraclize – TLS notary

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. We extended this to auditable computations. Severak auditors reduce need to trust one entity.



SGX

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, with digital signature from hardware. Application to finance beyond Blockchain…



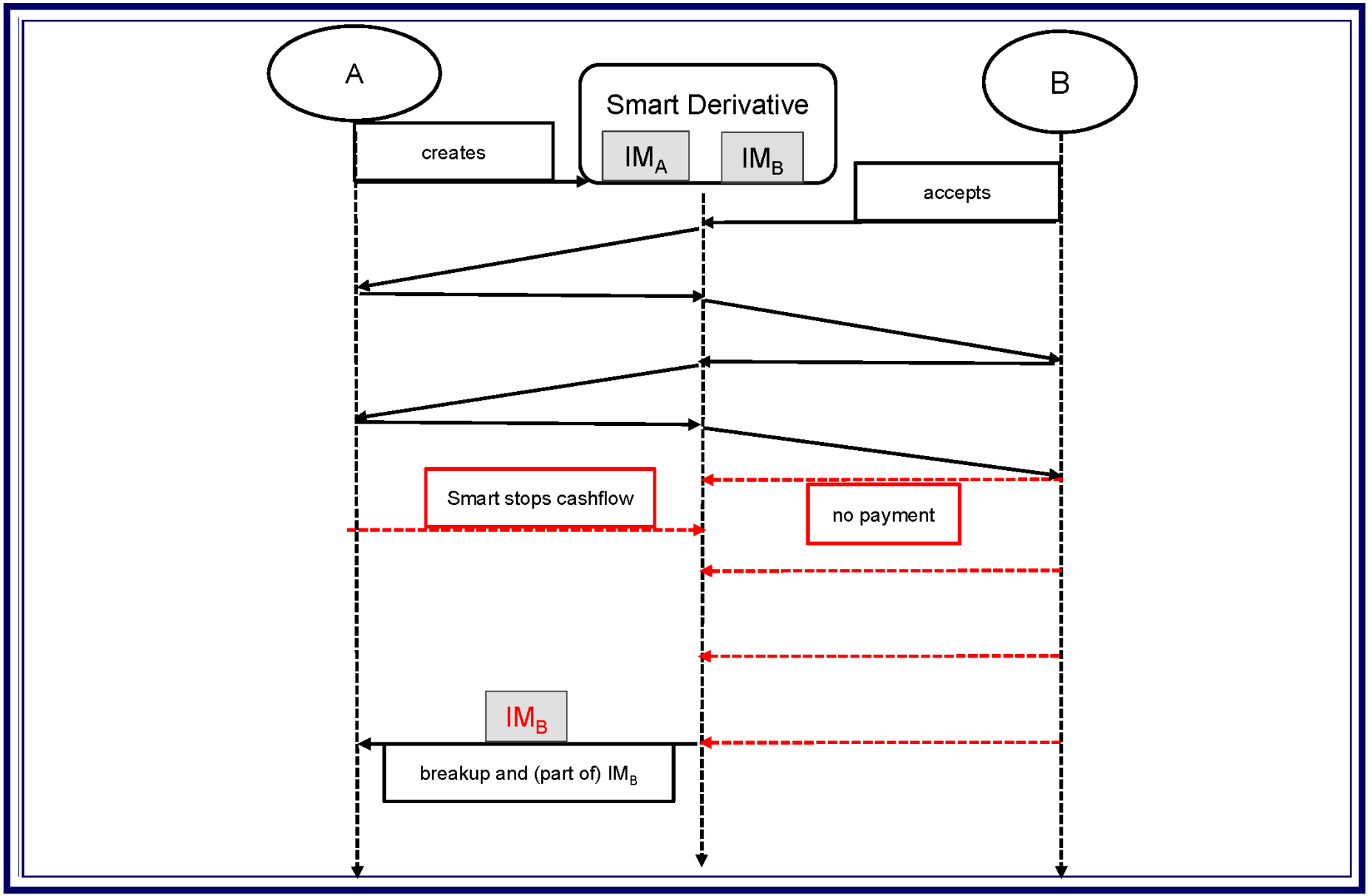
Using a smart contract to close the gap

- ***Technical Complexity:*** blockchains level the playing field. **As nodes of the same blockchain, banks, corporations, funds and households have all access to the same payment and account technology**

- ***Collateral Misalignments***: 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. **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.

Collateral Workflow on Blockchain



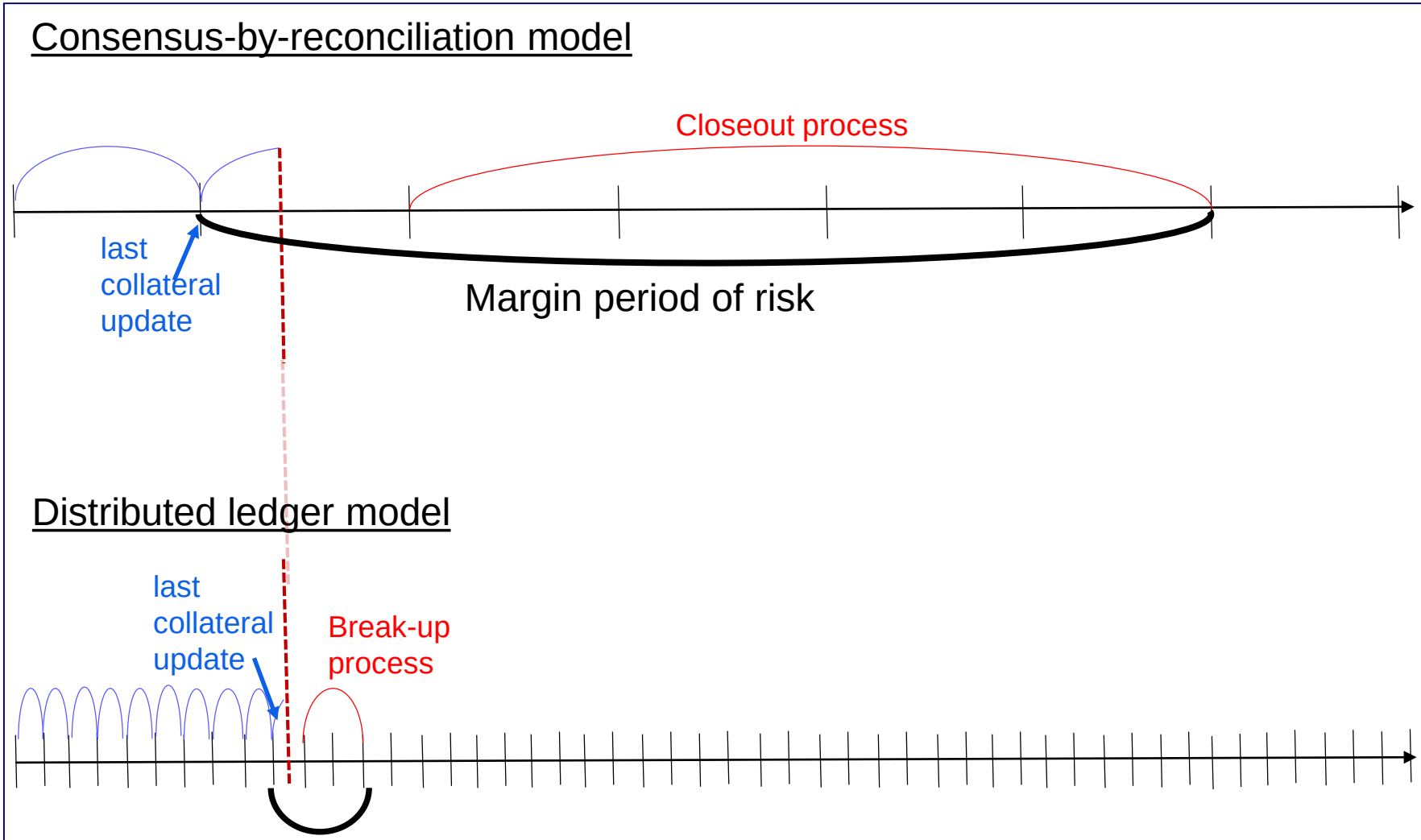
Using a smart contract to close the gap

- *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. **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.

- Much smaller amount of Initial Margin required to avoid losses. Works (only small potential losses) even with lack of legal recourse.

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



Centralization and Decentralization

Few words on CCPs

- CCP have been the other strategy against default risk. One entity puts itself in the middle of all trades; and we make it so big and over-regulated and over-collateralized that then we assume «it cannot default». It was the main solution after the credit crunch.

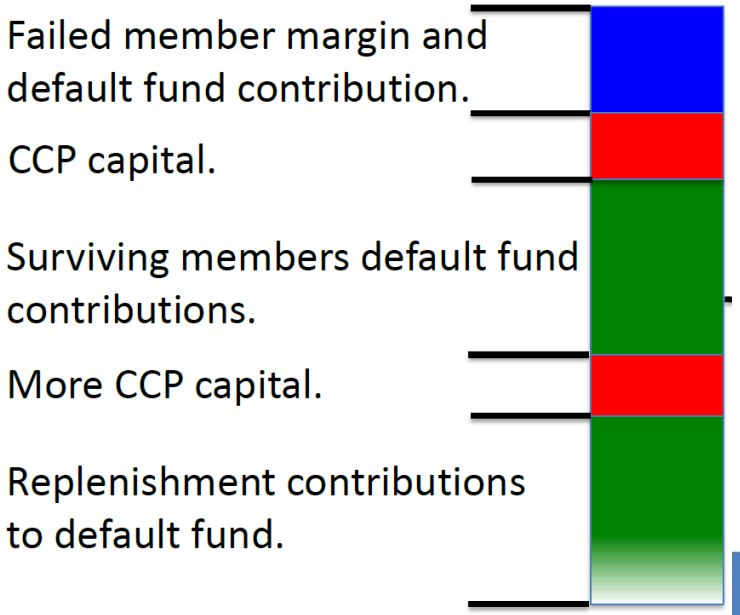
- IOSCO and Basel recently published a paper where they point out gaps and shortcomings in CCP recovery planning and in credit/liquidity management. They strentghten further the requirements.

- 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.

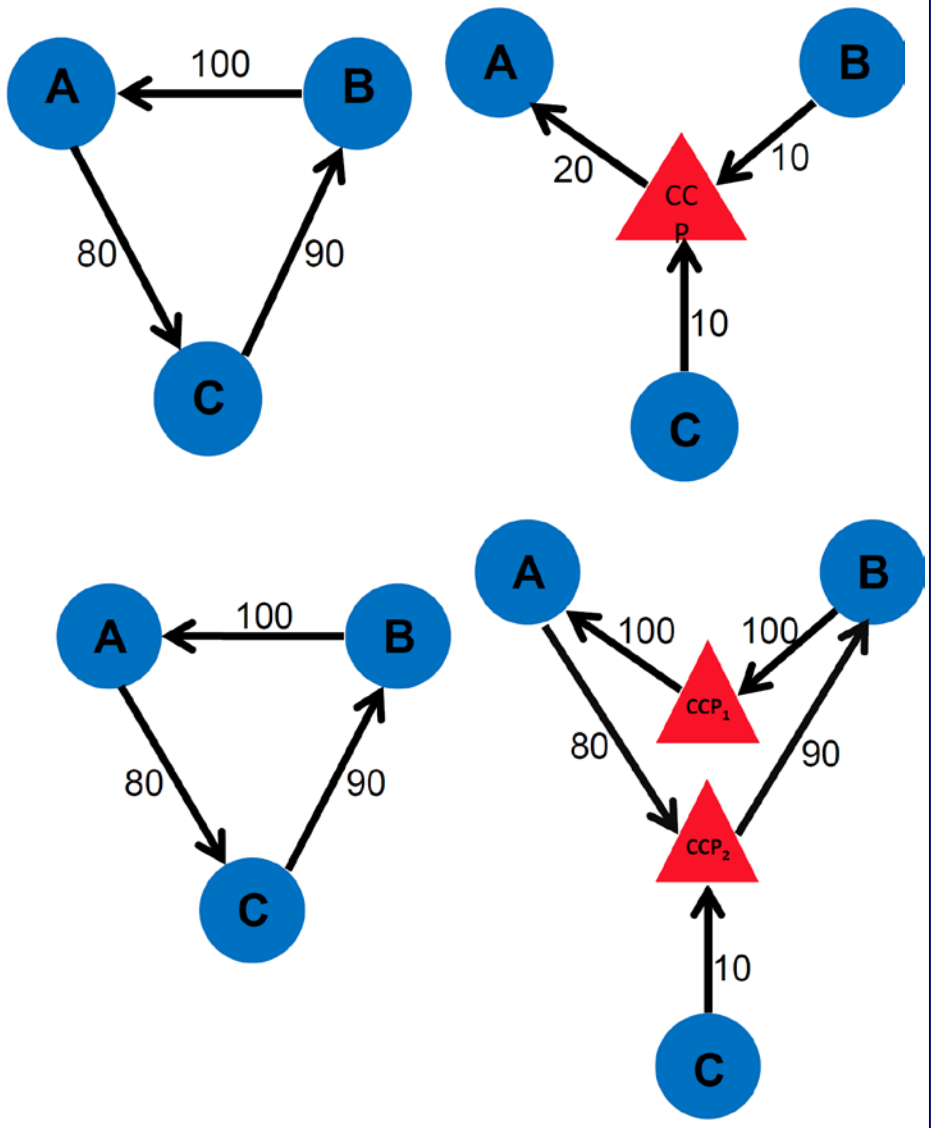
https://isda.derivativiews.org/ say that in case of serious stress for a CCP it would be crucial to maximize certainty and predictability by following a precise sequence of loss allocation and position allocation tools, already defined by ISDA. Transparency, with indicators defined upfront and followed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

Financial Markets: Regulatory Principles and the Blockchain

Blockchain and Principles for FMIs

CCPS and IOSCO principles for FMIs, 2012 and 2016:	ETHEREUM Functionality, 2018
• Transparency • Monitoring & Recording • Fair and Open Access	• Native in Blockchain
• Realtime settlement • Resilience & Business Continuity	• Achieved by Decentralized Consensus
• Dematerialized Securities • Efficient Margin	• Easier with Tokens
• Delivery vs Payment • Objective rules • Netting Effect, Fund Mutualization...	• Possible with Smart Contracts

*

Regulatory principles and the Blockchain

There is one first point to consider when discussing Blockchain regulations.

Blockchains are designed to be much more self-regulated than traditional systems.

The consensus algorithm run by the network ensures the respect of the fundamental rules of the network. The architecture of digital signatures ensures a very effective way to give self-executable rights.

But there is more. **Various regulatory principles, for example transparency and resiliency are satisfied by construction, but in a way that is different from the current standard.**

Regulating blockchain requires first of all to understand these aspects to exploit them for effective regulations, and to avoid regulations that actually stifle innovative solutions.

Let us see a very precise example analysing the regulatory principles of financial market infrastructures.

*

Blockchain and Principles for FMIs

In 2012, the International Organization of Securities Commissions (IOSCO) and the Basel Committee on Payments and Market Infrastructures (CPMI) of the Bank for International Settlement (BIS) issued a foundational regulatory document that gives the cardinal rules and standards for Financial Market Infrastructures (FMIs), that are payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories. It is called the *Principles for financial market infrastructures* and suggests application of similar principles also for infrastructures not formally covered by this report" such as "*trading exchanges, trade execution facilities,* or *multilateral trade-compression systems*". Nine areas are covered:

Transparency (principles 23 and 24)
Organization (principles 1-3)
Access (principles 18-20)
Efficiency (principles 21 and 22)
Settlement (principles 8-10)
Business & Operational Risk Management (principles 15-17)
Credit and Liquidity Management (principles 4-7)
Default Management (principles 13 and 14)
Depositories and exchange systems (principles 11 and 12)

Clarity and Transparency

Transparency: the need for a FMI that provides "timely and accurate data to relevant authorities and the public in line with their respective needs". A *blockchain is natively made up by all the data relative to a market,* so their immediate availability and absolute accuracy is intrinsic to any blockchain. In a basic public blockchain all market data are visible to everyone. Nowadays, we can modulate their provision to the relevant authority and the public via cryptography. No need for the FMI to provide data with a plethora of inefficient, corruptible and difficult-to-reconcile reports.

Organization: the need for clear rules and responsibilities. FMI have made a large effort to increase the clarity of their rules. Yet, being paper-based and subject to very large areas of interpretation, judgement, and variations, massive areas of uncertainty and arbitrariness still exist.

Blockchains work by applying precisely the rules of their protocol, which is public and translated in the software that all computers run. In Blockchains like Ethereum, this applies also to the agreements that go beyond the fundamental protocol rules, due to the smart contracts. Clarity and transparency of the rules are native in blockchains; they can give this property to FMIs more easily than any previous technology.

*

Efficiency and Open Access

Fair and Open Access: A peer-to-peer network where *everyone* can be a node, as long as he accepts to *follow the rules* by running a protocol software, *is suitable to provide fair and open access even beyond what regulators could expect in 2012* when decentralized technology was not yet part of the public debate. Here the Identity developments can be useful to keep the open access principle within the right requirements.

The fourth general area is *Efficiency*. In particular Principle 22 mentions the need for *efficient payments*, *clearing*, *settlement* and *recording*. On a blockchain, payments can be executed directly by the parties with no need for layers of intermediaries. As we have seen in Section 2 and 3, payments can even be automatic thanks to smart contracts, with native DvP. Settlement can be few orders of magnitude faster than it is today. Recording is also native and comes for free for each payment or agreement. Blockchain operates 24h with no national barriers.

Settlement. The specific principle 9 suggests that "an FMI should conduct its money settlements in central bank money where practical and available". We saw already that digital currencies have features similar to central bank money: both dematerialized, both are no risky debt of private banks, and both can settle instantaneously. Notice: for settlement finality, Byzantine agreements required.

*

Risk, Credit and Liquidity Management

Risk Management. Principle 17 stresses the need for *operational reliability* and *business continuity management*. Here again current decentralized technology may surpass the expectation of 2012's regulators on system resilience. Regulators require critical FMIs guarantee "reliability and resilience", in particular "each site should have robust resilience based on the duplication of software and hardware, and the technology in place to replicate data between the various sites should be consistent with the chosen recovery-point objective". These are natural features when all users are network nodes, and all, or a part of them, replicate the entire database, as it is the case in current blockchains.

The next group of principles regards *Credit and Liquidity Management*. Principles 4 and 7 require explicitly an FMI to have the best tools and practices for effectively managing and monitoring credit and liquidity risk. We have seen a range of applications where smart contracts implement automatic credit risk management covenants, that intervene when there are signs of credit problems, and the use of different wallets to ease and regulate the liquidity flow. Notice that, if financial obligations are codified and evaluated via smart contracts, credit and liquidity risk is not only automatically monitored, but can also be simulated, running the smart contracts on different scenarios. The importance of evaluating FMI resources under stress scenarios is underlined in principle 4, with particular emphasis on CCPs.

*

Default, Depositories and Settlement

Default Management. Regulators require in principle 13 that "an FMI should have effective and clearly defined rules and procedures to manage a participant default". When speaking of CCPs we mentioned similar more recent requirements from other regulators, see (BoE, 2016) and (ISDA, 2016), confirming the issues is still burning. Regulators would like the CCP default process to be more predictable and detailed. Indeed, smart contracts and other blockchain-related technologies like provably-honest computations we mentioned earlier can be a natural tool for this.

The final area, encompassing principles 11 and 12, regards *depositories and settlement systems*, and gives indications "to maintain securities in an immobilised or dematerialised form for their transfer by book entry" and to "eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other". This brings us back to Delivery versus Payment. We have seen in how the management of dematerialized securities is the strongest application of smart contracts, with growing standardization and the development of a range of native tools where transactions are atomically linked, so that no DvP failure is possible.

Traditional institutional intermediaries often work to keep old roles. Yet some think there are roles for institutions even in a more decentralized regulated setting...

*

What will happen in regulated space…

TODAY, Several intermediaries guarantee safe and transparent trading in financial markets…	A ROAD TO EVOLUTION	TOMORROW, blockchain and smart contracts require capital-ligher, narrower roles, but crucial services are still needed…
REGISTRARs now keep records of legal ownership of securities	ownerhip of securities is natively mapped by the issuing smart contract, but map is with public keys…	REGISTRAR roles needed to establish and maintain the association of legal identities with public keys. A KYC/AML role to share with CUSTODIANs in a narrow banking approach…
CUSTODIANs now administer securities accounts, services…	smart contract storage takes autonomous care of securities, but users interact with private keys…	CUSTODIAN roles will help manage private keys, from key generation services to multisig to protect from theft or loss, or cold storage… a capital-lighter, tailor-made service
TRADE REPOSITORIEs now record reports of transaction data	all transactions are automatically recorded on the blockchain, no need to send reports, yet…	TRs roles will maintain block viewers for regulatory representation. Plus, a modern blockchain is encrypted by zk proof or ring sigs…who keep keys to grant view to regs or authorities?
CENTRAL DEPOSITORIEs or CENTRAL COUNTERPARTIEs now hold all securities or are even parties to all trades	in far future all members could interact directly via smart contracts, slashing counterparty risk, but…	…not only some will be in charge for contract maintenance, but even with reduced counterparty risk there will be a need for counterparties of last resort to ensure business continuity…

Privacy solutions for Public and Private Blockchains

Homomorphic Encryption

Zero-knowledge proof (Goldwasser, Micali, and Rackoff 1985) 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

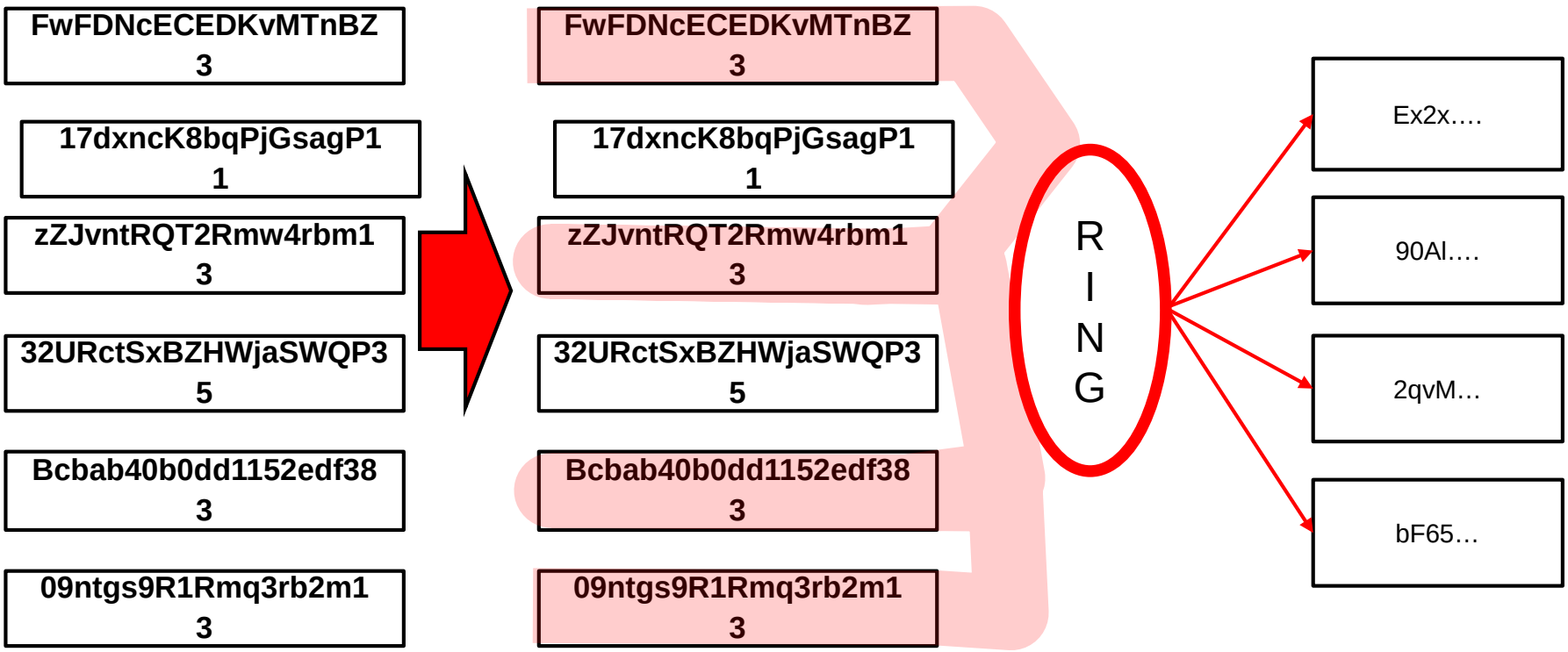
$$\left[a * b\right]_n = \left[\left[a^k\right]_n * \left[b^k\right]_n\right]_n$$

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 41 MOD 77=41, and 1350 MOD 77=41.

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

A hint at Ring Signatures



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.

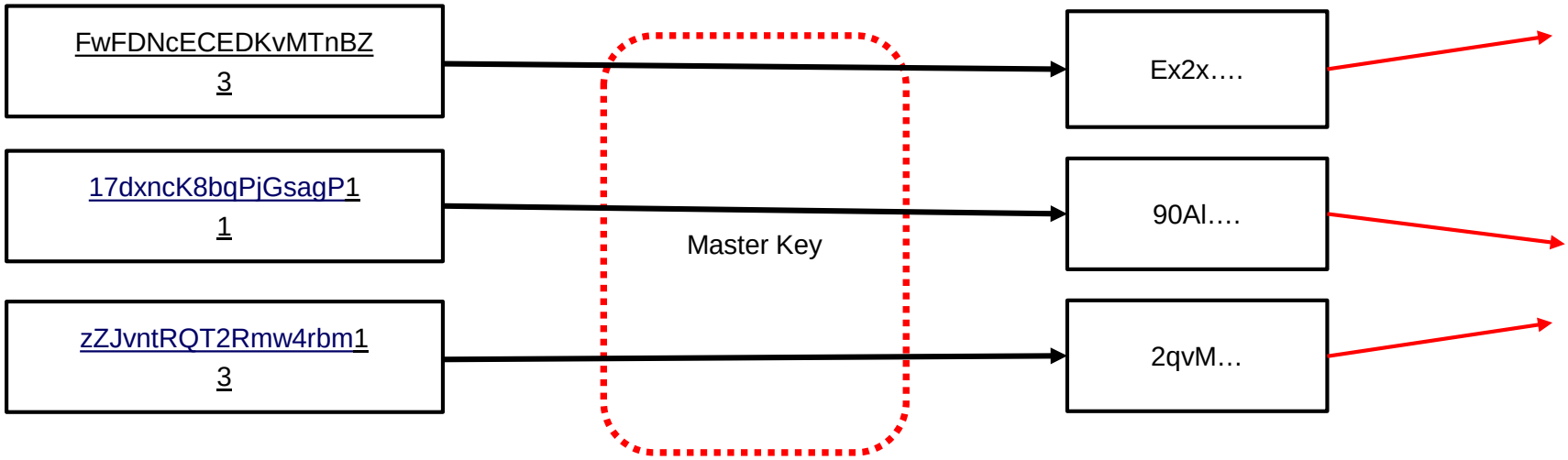
Thanks to Linkability, one can verify that each signature is used only one. Once they have all been used, the RING is empty and there is no more to spend. This obfuscates sender.

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

Such techniques give rise to interesting, and feasible, models for regulated markets.

We can imagine a market with legal identities where all transactions among all parties are fully identifiable, but all amounts are private. Homomorphic Encryption may allow this.

We can imagine a market with legal identities where all amounts are visible, but the identity of transactions, senders and receivers are obfuscated. Ring signatures and Stealth addresses may allow this.

Different techniques can also be used jointly.

Blockchain extensions for the regulated world: first hints

In some blockchains, with *zk-snarks* even if the registry is publicly visible, private information is shielded via encryption. See Section 4.

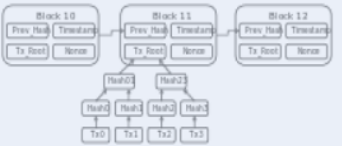
In some blockchains, with *ring signature* and *stealth address*, keys associated uniquely to a wallet are never used, for maximum privacy

In Ethereum, the signed message can be addressed to a smart contract, or can even be creating a contract. See Section 2.

In Ethereum, in case the transaction is addressed to a smart contract, block producers run the contract code and act accordingly. See Section 2.

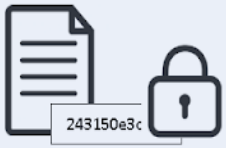
In Ethereum, in case the transaction is addressed to a smart contract, also validators run the contract code to verify blockchain. See Section 2.

1: Download the Blockchain

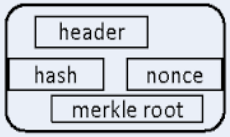


2: Create Public-Private Key

3: Send a signed message



4: A block-producer puts it in a block



5: The network validates

Research on Sharding is aimed to allow different nodes to keep just relevant partition of the Blockchain, to increase scalability.

If one of the privacy techniques above is used, the blockchain can features explicit legal identities given by an authority

Research on State Channels to make transactions go only to counterparty except a final one going to blockchain, to increase scalability. See Section 4

Different blockchains have different ways to choose block-producer: proof-of-work or proof-of-stake or random selected members. See Section 3.

Different consensus algorithms in different blockchains mean different criteria, including checking a majority of votes for finality. See Section 4.

at the next download, the blockchain will include this transaction

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.