INTESA SANPAOLO

Intesa Sanpaolo Blockchain/DL Technology approach

Savino Damico – Head of Digital Payments and Biometrics

Blockchain for social good - Turin, December, 15th 2017

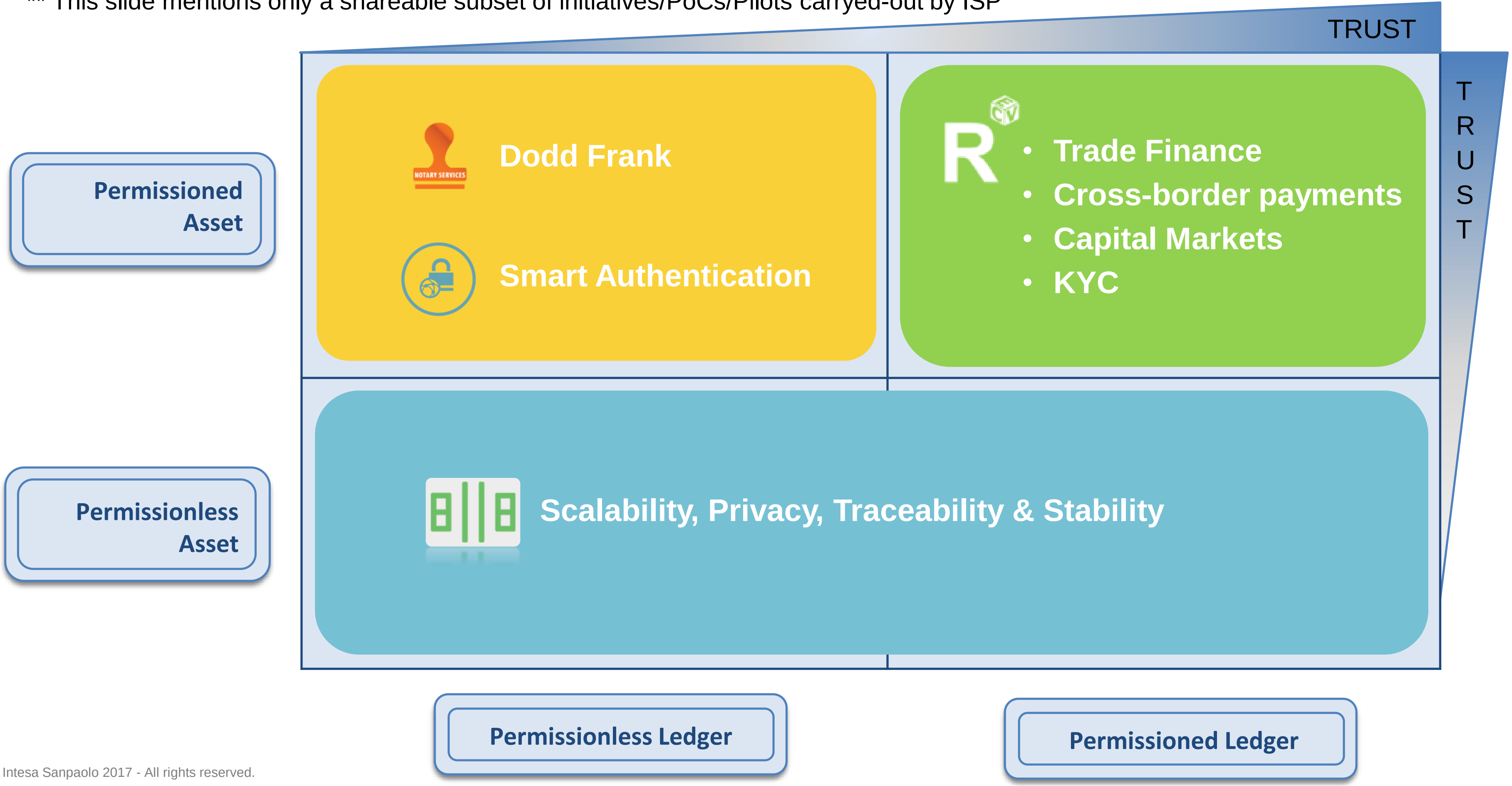
innovation center
INTESA SANPAOLO

Agenda

- **ISP approach for blockchain/DL Technologies: a holistic approach**
- Timestamping and notarization

Premessa: a holistic approach**

** This slide mentions only a shareable subset of initiatives/PoCs/Pilots carryed-out by ISP



TRUST

TRUST

Permissioned Asset

Permissionless Asset

Dodd Frank

Smart Authentication

- Trade Finance
- Cross-border payments
- Capital Markets
- KYC

Scalability, Privacy, Traceability & Stability

Permissionless Ledger

Permissioned Ledger

Agenda

- ISP approach for blockchain/DL Technologies: a holistic apprach
- **Timestamping and notarization**

Timestamping and notarization

Blockchain opportunities

Which opportunities from bitcoin permissionless ledger?

How to leverage security and transparency of permissionless ledger?

Compared to traditional **information and data management systems**, blockchain offer interesting opportunities regarding

Auditability

Accessibility enables to easily verify the timestamp data any time is needed

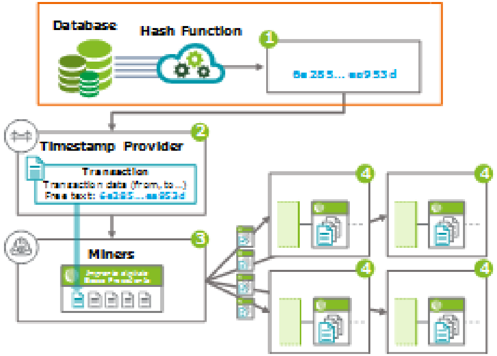
Immutability

Information stored in blocks is not alterable after a new block is added

The blockchain could be used in all contexts requiring a guarantee of data immutability

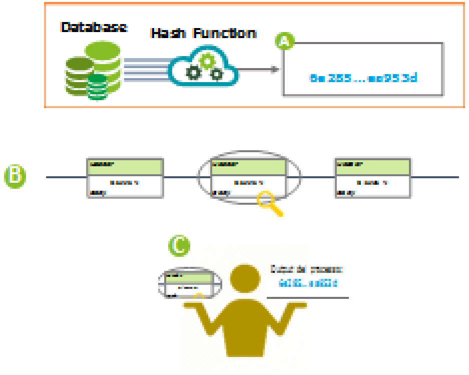
USE CASE: TIMESTAMPING

Step 1: the certification process



The hash generated on the document, needed to ensure the immutability over time, is published in a non-editable and non-erasable public blockchain

Step 2: verification process



Anyone with the document and the hash algorithm can check the consistency with what previously published on public blockchain

Timestamping and notarization

Use for Dodd-Frank Act compliance purposes

Dodd-Frank Act Title VII

23.202 Daily trading records
Each swap dealer and major swap participant shall make and ***keep daily trading records*** *of all swaps it executes, including* [..] ***Pre-execution*** *trade information,* [..] ***Execution*** *trade information,* [..] ***Post-execution*** *trade information*

23.203 Records; retention and inspection
[..] *the swap dealer or major swap participant must provide* [required] *records* [..] ***within 72 hours*** *after receiving the request*

1.31 Books and records; keeping and inspection
[All books and records required shall be kept by means of an "electronic storage media".]…*"electronic storage media" means any digital storage medium or system that preserves the records exclusively in a* ***non-rewritable, non-erasable format***

DFA requirements
Trade Reconstruction

- **Collect and store trade data,** including pre and post execution information
- **Reconstruct trades, on demand, within the 72h** required by CFTC
- **Prove that data storage is immutable**

- The **Proof of Concept** (PoC) has been focused on the **possibility** of **using hashing** and **timestamping** on the **bitcoin blockchain** to **ensure data immutability,** potentially absolving the DFA requirements. In particular, the study has been focused on:
  - **considering** the **opportunity** to implement the use case
  - **analyzing** all the **requirements** and verifying the technical design of the model
  - **defining** a potential **implementative roadmap**

Timestamping and notarization

Use for Dodd-Frank Act compliance purposes

SOME INFORMATION ON THE ARCHITECTURE

- The hashing system had been handled by Intesa Sanpaolo
- The management of transactions within bitcoin network had been outsourced to a Third Party
- The Third Party provided Intesa Sanpaolo with all needed information to identify the blockchain transaction where the hash had been included

SOME OF THE TESTS EXECUTED

- We published on the public blockchain the hashes of some operational working days
- We connected the hash of each day to that of the previous one by creating a «hash chain» with all the transactional history
- In order to ensure to store the hash on the bitcoin blockchain, we included eac hash in more than one transaction
- We tested also a data tampering, by modifying 1 byte of a document and by comparing the difference in the relevant produced hashes

Timestamping and notarization

Some considerations and next steps

SOME LESSONS LEARNED

- The kind of experimentation was deemed effective for Dodd-Frank Act compliance purposes
- The same model can be used for a number of different use cases anytime it is needed to proof «data immutability» both within financial services and for non–financial ones (refer for instance to the land building register)
- As such a proof is not formally accepted by Regulators, we're using it as an «add-on» to standard compliance tools

THE WAY FORWARD

- To convince Regulators to allow banks/financial institutions to use blockchain/DL technologies for complying to data immutability requirements
- To start analysis to apply the same model to other use cases, both within Intesa Sanpaolo and within national/international communities using blockchain technology
- To carry out an analysis for reaching the same objectives by using different ledgers, e.g. private/permissioned ledgers (both within Intesa Sanpaolo and within national/international communities using blockchain technology)
- To identify, if any, the consequences of the new Final Rule on the PoC executed (refer to next slide for the new Final Rule)

Timestamping and notarization

PoC evolution: the new Final Rule

New version of Dodd-Frank Act Title VII

The latest version of the **Final Rule** (FR, Vol. 82, No. 102, May 30, 2017):

- **cancelled** the **requirements** to maintain:
  - records in their native electronic format
  - any record in a non re-writable, non-erasable format (‘‘write once, read many’’ or ‘‘WORM’’ requirement’);
- Set **new rules** for **keeping “regulatory records”** as follows: *“Each records entity maintaining electronic regulatory records* ***shall establish appropriate systems*** *and* ***controls*** *that* ***ensure*** *the* ***authenticity*** *and* ***reliability*** *of* ***electronic regulatory records****, including, without limitation:*
  - *systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*
  - *systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity’s electronic record retention systems;*
  - *the creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records”*

- The new version of **Final Rule** sets new rules **for keeping information over time**
- A relevant **analysis** is **ongoing** to **verify impacts** on the previous Proof-of-Concept

THANK YOU

GRACIAS

ARIGATO

SHUKURIA

DANKSCHEEN

SPASSIBO

SNACHALHUYA

NUHUN

CHALTU

YAQHANYELAY

TASHAKKUR ATU

YUSPAGARATAM

TINGKI

BÏYAN

SHUKRIA

MABEEJA

MAITEKA

HUI

SUKSAMA

DHANYAVAAD

AWHA

MEHRBANI

EKHMET

MERSI

SPASIBO

DENKAUJA

NENACHALHYA

UNALCHEESH

ATTO

GUI

MATUR

EKOJU

SIKONO

SANCO

MAAKE

GRAZIE

MERASTAWHY

GAEJTHO

KOMAPSUMNIDA

LAH

HAKETAI

TAVTAPUCH

MEDAMAGSE

GOZAIMASHITA

JUSPAXAR

DANKA

EFCHARISTO

AGUYJE

FAKAAUE

PALDIES

BOLZÏN

MERCI

MINMONCHAR