

04 ottobre 2018 De Cifris incontra Roma

GT 50 改善
VISIONARY INNOVATORS

blockchain
a 1001 obstacle race

Sandro Fontana
sandro.fontana@gt50.org

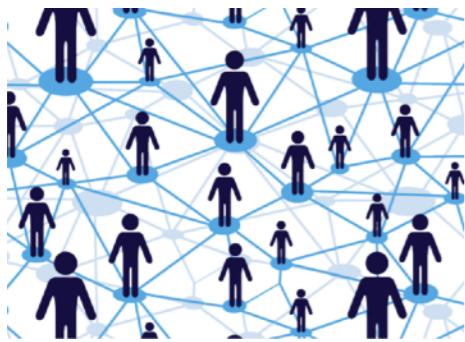
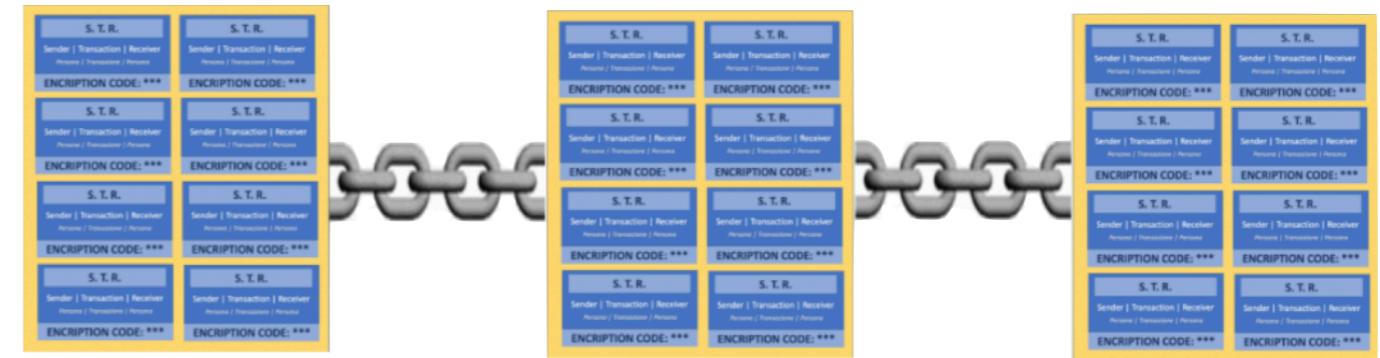
Se i vostri requisiti sono soddisfatti
dalle attuali basi di dati relazionali,
sarebbe folle utilizzare una blockchain
(da Gideon Greenspan, fondatore di Multichain)

Detto tutto ciò cosa capita di frequente?

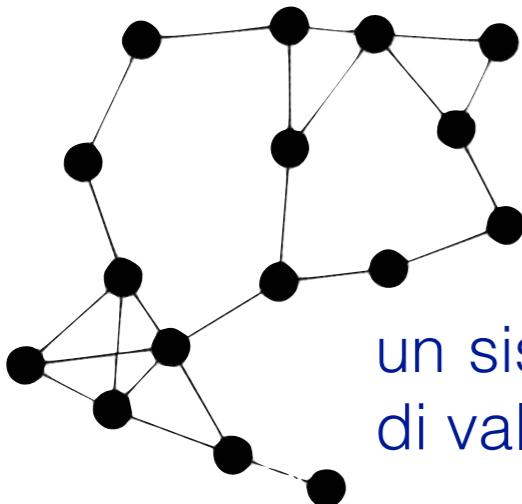


helicopter overview

una lista ordinata di blocchi di dati contenente transazioni applicative



una struttura dati pubblica e decentralizzata: condivisa tramite una rete P2P

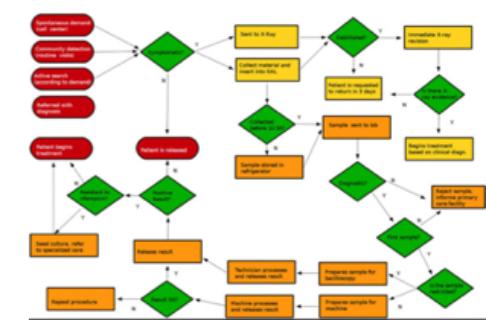


non modificabile;
dimostra autenticità, integrità e non ripudio



un sistema di consenso distribuito che permette di validare e confermare ogni transazione

(in alcune implementazioni) un linguaggio di scripting: permette di scrivere programmi memorizzati ed eseguiti nella blockchain
[smart contract]





1001 Reasons NOT to Start a blockchain project

... maybe a DLT project?

- 0001) difficoltà ad adeguare la tecnologia ai cambiamenti (business, compliance ...)
- 0010) completa trasparenza VS necessità di riservatezza
- 0011) incapacità di scalare e spreco energetico: PoW
- 0100) dove mettiamo i dati?
- 0101) nulla è gratis ... ed in alcuni casi costa molto
- 0110) che succederà nel futuro di alcune (tutte) le blockchain
- 0111) i rischio per gli utilizzatori, in particolare per gli utenti finali
- 1000) nel business la mancanza di una autorità garante non sembra accettabile
- 1001) siamo certi di voler unire A.I. con un sistema che nessuno può bloccare?

la gran parte di questi spunti di riflessione, sono sicuramente gestibili in una DLT (blockchain permissioned); sarà comunque necessario ripensare a come disegnare le applicazioni e per questo, sviluppare/imparare altri strumenti.

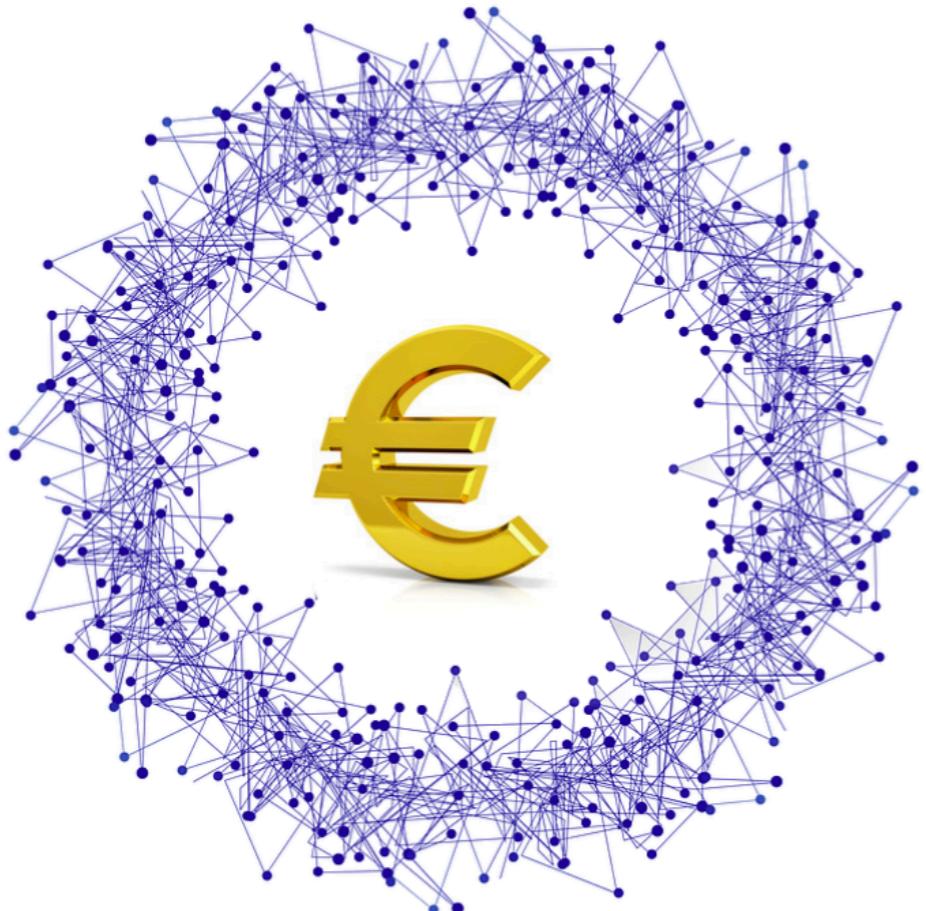
(by courtesy of myself <https://www.linkedin.com/pulse/1001-reasons-start-blockchain-project-maybe-dlt-sandro-fontana/>)





Don't smart contract me, bro!

using blockchain for a common benefit



alterEuro:
a parallel coin to
improve the economy

without impacting on EU Growth and Stability Pact

using blockchain for a common benefit

grant of asylum
“refugees&immigrants in EU:
identification and tracking challenge”

without impacting on National Identity Standards
and their implementation

Test Field for a Future EU Identity Standard

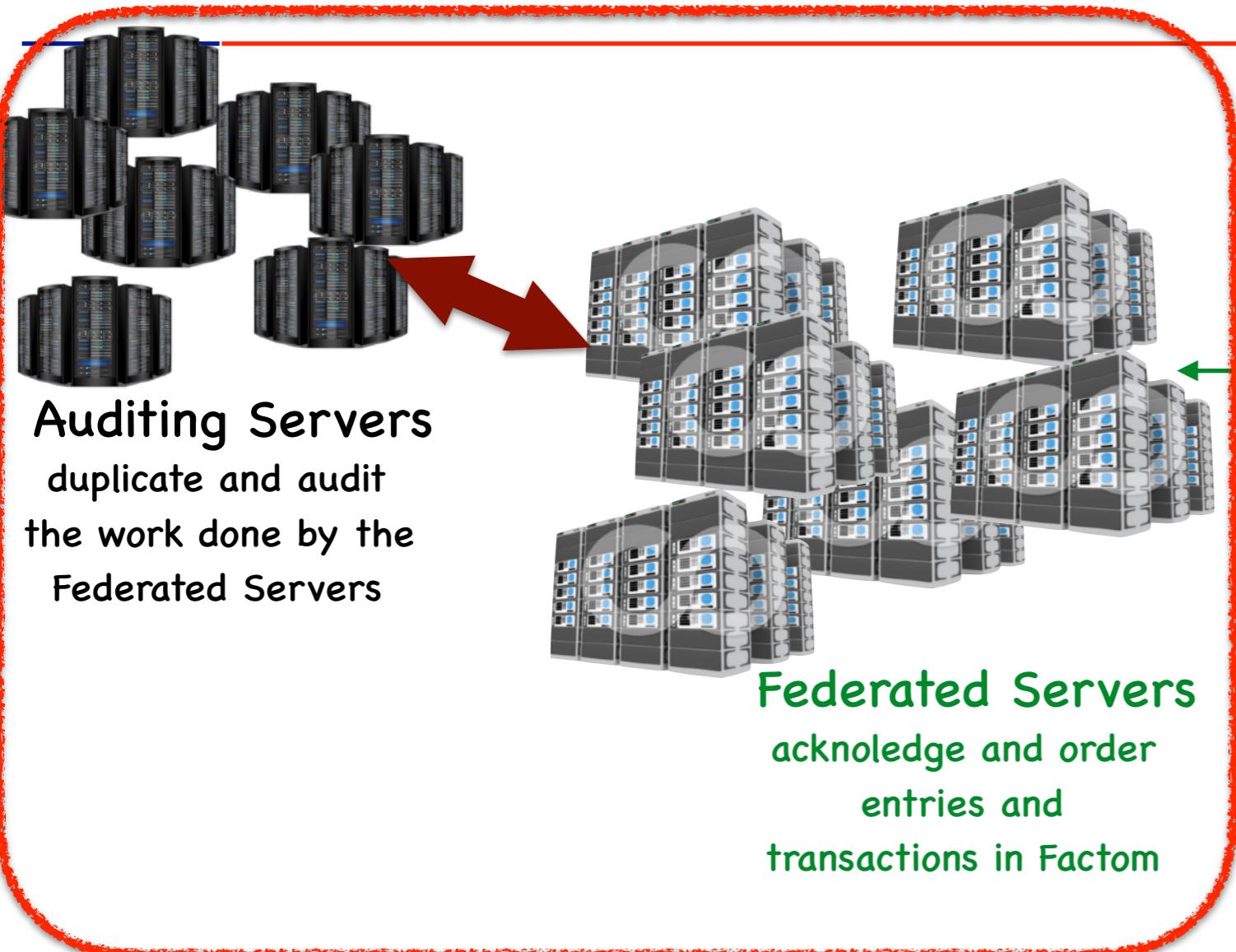


FACTOM™

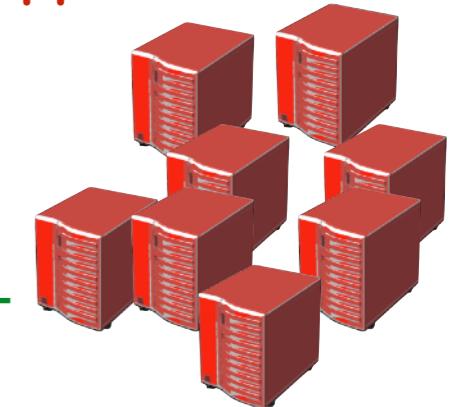
“... quello che ho capito”
(Sandro Fontana)

Authority Servers

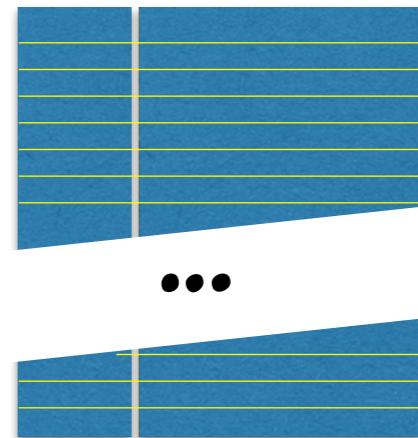
Factom's characters



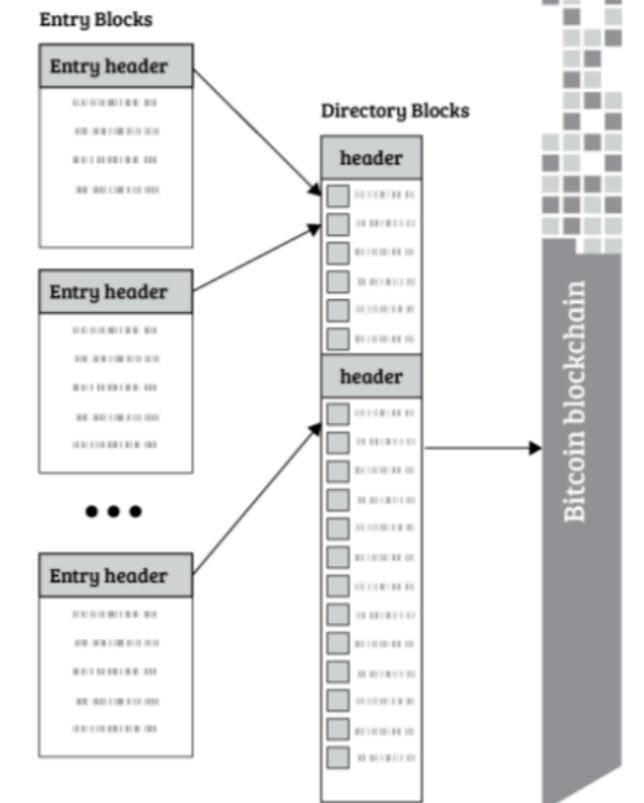
Application Servers



Distributed Hash Table



How Entry Blocks are Written to Directory Blocks



- 1) **Directory Layer** -- Organizes the Merkle Roots of Entry Blocks
- 2) **Entry Block Layer** -- Organizes references to Entries
- 3) **Entries** -- Contains an Application's raw data or a hash of its private data
- 4) **Chains** -- Grouping of Entries specific to an Application

Sicurezza ICT

architetture, policy, procedure



Progettazione di reti e sistemi, hardening, security assessment

Crittografia e sicurezza documentale

protocolli, strutture dati, firma [digitale&non]



Librerie di firma digitale
Codice 2D-Plus
Codice SQCode

OTP OATH Time/Event based

Prodotti Software

App Android/iOS, Linux



Timbro Digitale 2D-Plus
Digital Seal & Lambda Service
Q-ID (mobile OTP)
Factom's Blockchain

Timbro Digitale 2D-Plus



UFFICIO DELLO STATO CIVILE

CERTIFICATO di NASCITA

Questo certificato ha valore legale per 6 mesi a partire dalla data di emissione.

L'UFFICIALE DELLO STATO CIVILE

In base alle ristrettezze amministrative (Art. 108 comma 2 D.P.R. 396/2000)
Certifica che:

FONTANA SANDRO
Cod.Fis.: FNTSDR55B13H501Y
E' NATO il 13/02/1955 a ROMA (RM)
nato N. 00612 parte 1 serie A05 del comune di ROMA (RM)

L'UFFICIALE DI STATO CIVILE Angelo Ottavianielli

Roma, 21/11/2016

Il presente certificato non può essere prodotto agli organi della pubblica amministrazione nei privati gestori di pubblici servizi.



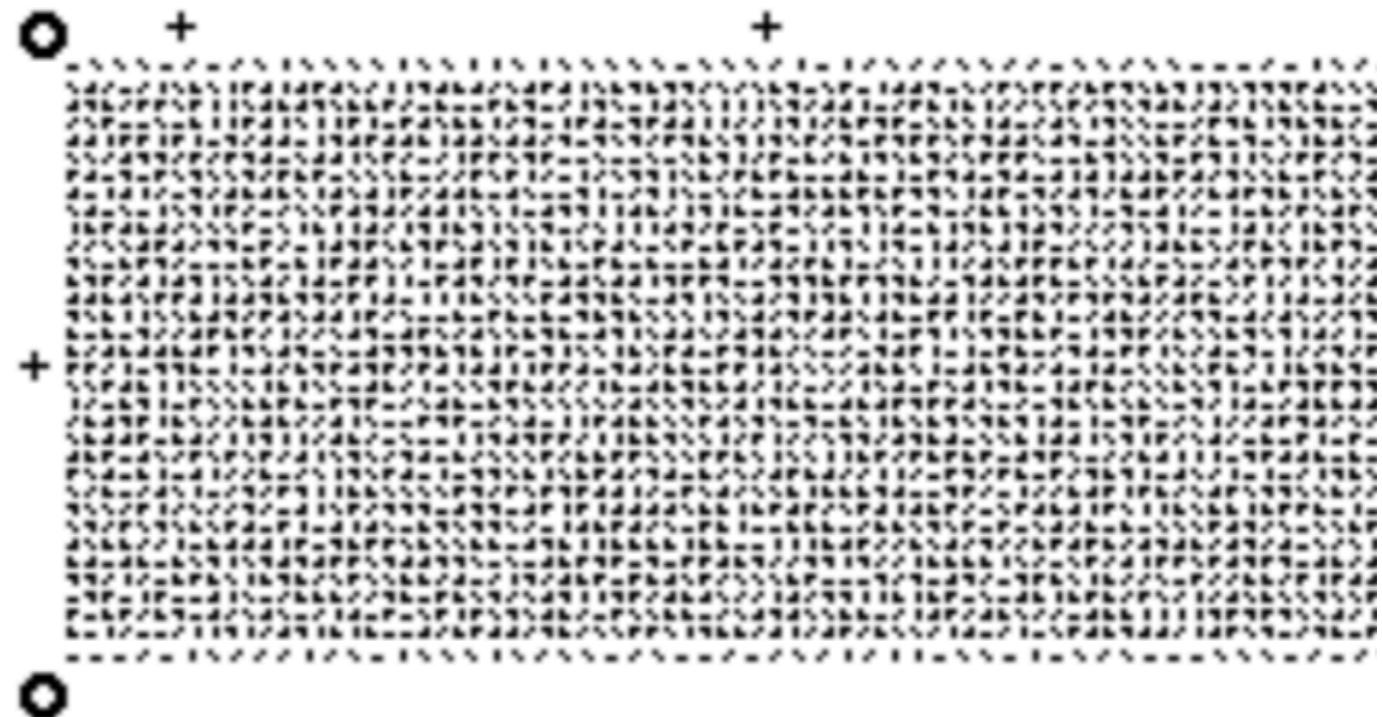
E' possibile incupire il certificato all'indirizzo: <https://www.comune.roma.it/bewiz/certificati/recupero>

ID Certificato: VGO-DGF-VTD-211-116

ID Ufficio: Portale Comunale

Documento generato il 21/11/2016

Pagina 1



il servizio λPeS : funzionamento /1

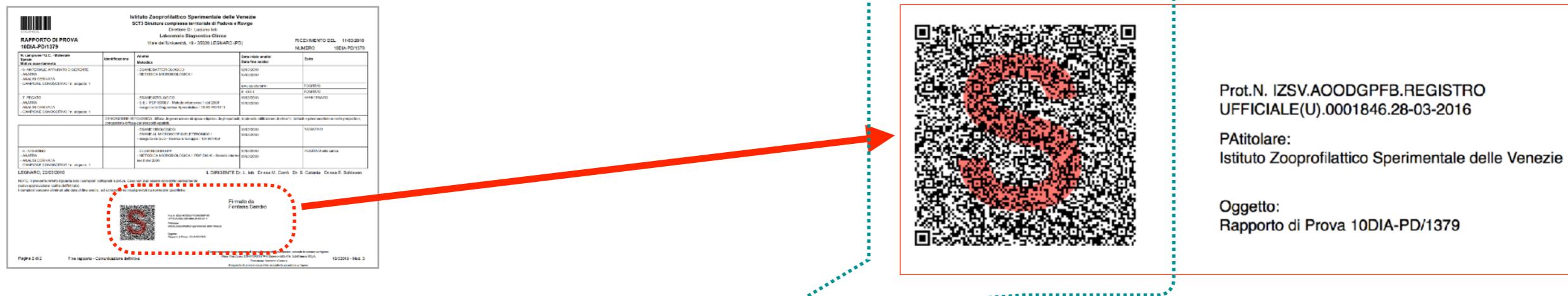


λPeS è un servizio tipicamente presente nella lan aziendale, che permette di applicare una firma PAdES su documenti PDF garantendo la validità del documento anche se stampato.

I software documentali aziendali inviano i file PDF da firmare^(*) in modo automatico, ad un apparato di firma, precedentemente attivato dal Titolare

I documenti PDF vengono firmati dal servizio λPeS: il file elettronico (PAdES) potrà essere verificabile nella sua Integrità, Autenticità e Non Ripudio grazie alla firma.

Il sistema λPeS aggiunge, nell'area grafica della firma, il contrassegno elettronico **Lambda Seal**

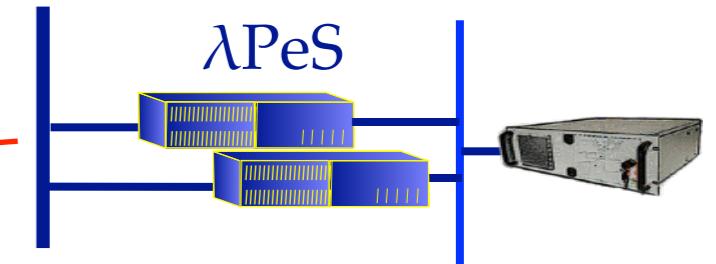


(*) Firma PAdES a norma eIDAS

il servizio λPeS : funzionamento/2



restituzione file PDF firmati



Dopo la firma i file PDF vengono restituiti all'Utente; una loro copia codificata verrà inoltre inserita nel repository on-line λStore. La chiave di icodifica è random ed unica per documento.

Anche in caso di violazione del server λStore, nessuno potra' accedere ai dati in chiaro.

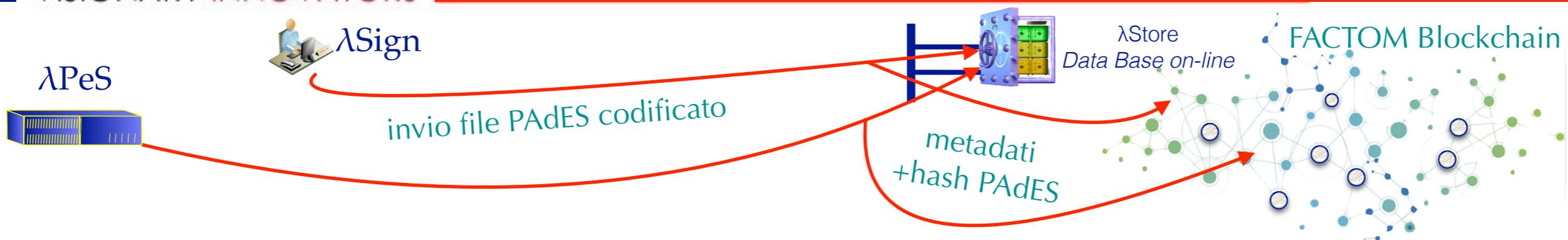
λStore
Data Base on-line



Da un documento stampato, si potrà leggere il codice *Lambda Seal*, per recuperare immediatamente la copia elettronica firmata del documento stesso.

Lambda Seal contiene tutte le informazioni necessarie a recuperare in modo trasparente e sicuro, il documento elettronico firmato, compresa la chiave di decodifica specifica per ogni documento.

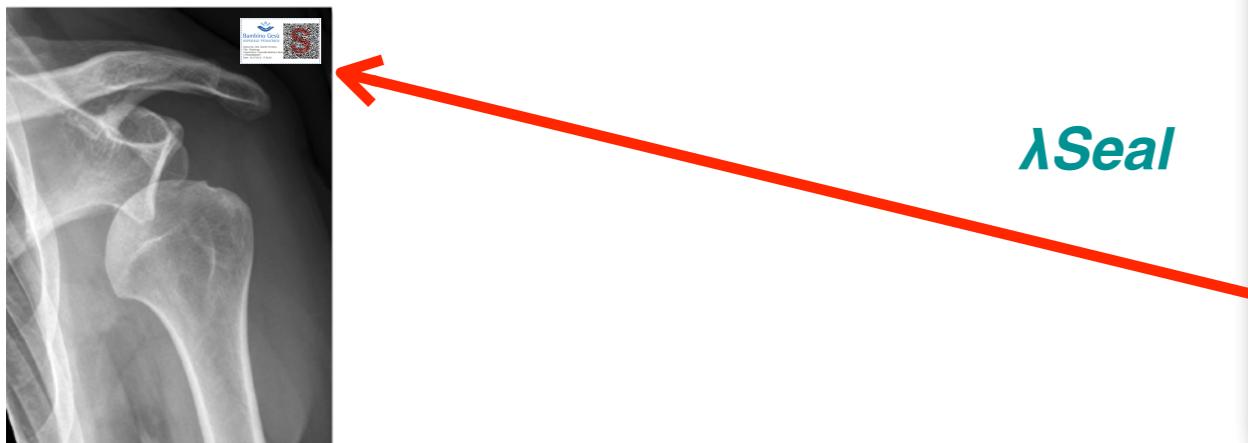
λSign: StoreFunct in blockchain



λPeS e λSign accettano anche documenti PDF/immagine di qualsiasi tipo; anche in questo caso per ogni file viene generata una chiave di crittografia (AES256) ed il corrispondente λSeal.

I file vengono codificati all'origine ed inviati su λStore; l'hash del documento, insieme ad una serie di metadati, compongono un messaggio che viene inserito nella blockchain FACTOM; questo prova con data certa l'esistenza del file (timestamp)

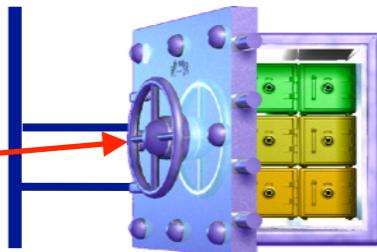
λPeS e λSign permettono di inserire il λSeal all'interno del documento (PDF, immagine JPG, TIFF, PNG) ovvero di stampare λSeal su una etichetta autoadesiva da applicare al documento cartaceo



λSign: uso per professionisti



invio file PAdES codificato



λStore
Data Base on-line

λSign è un software Windows/Mac gratuito, che permette di applicare una firma digitale su documenti PDF.

Tramite questo software l'utente seleziona il/i file PDF da firmare; quindi attiva la firma^(*) sul token locale in modo automatico, fornendo una sola volta il PIN di attivazione per tutti i file selezionati.

Il sistema λSign aggiunge inoltre, nell'area grafica della firma, il contrassegno elettronico **λSeal**.

Dopo aver creato il file PAdES, λSign codifica il file e lo invia al servizio λStore, per renderlo disponibile anche a partire da una copia cartacea.



Lambda Seal

(*) Firma PAdES a norma eIDAS

Secure Link SQCode: App

La verifica della integrità ed autenticità è quindi l'utilizzo dei dati contenuti nel Lambda Seal, avviene tramite l'uso di **Universal QReader™** una App per smartphone/tablet gratuita, scaricabile da PlayStore(Android) ed AppStore(iOS).



L'App Universal QReader™ può interpretare tutti i codici SQCode.

Lambda Seal contiene tutte le informazioni necessarie sia a recuperare in modo trasparente e sicuro la copia codificata del documento elettronico firmato, sia la chiave di decodifica, permettendo così alla App di restituire all'utente il PDF firmato

Se letto da diversa applicazione, un Lambda Seal informa l'utente della necessità di utilizzare

Universal QReader™
fornendo un link allo store per il download dell'App.



Thank you for your attention

Sandro Fontana, sandro.fontana@gt50.org
CISSP, ISO27001 L.A., CISM, CISA, C|CISO
skype/twitter: sinetqnlap
<http://sandrofontana.com>