CifrisChain 2018

Panoramica su alcuni progetti industriali in CifrisChain

Andrea VISCONTI

Dipartimento di Informatica "Giovanni degli Antoni"
Università degli Studi di Milano

Progetto KONFIDO (Bit4id)

KONFIDO

Di cosa si tratta:

É un progetto H2020 sviluppato in un consorzio di 15 partner che vuole migliorare l'interscambio di dati sanitari tra i paesi UE.

Un possibile scenario:

- Un cittadino danese che soffre di una malattia cronica ha in programma di trascorrere una decina di giorni a Barcellona, ma è preoccupato per una potenziale esacerbazione della sua malattia.
- Il suo medico lo informa che, grazie alla tecnologia sviluppata in KONFIDO, è possibile gestire in modo sicuro l'accesso alla sua cartella clinica.
- Utilizzando i meccanismi di sicurezza di KONFIDO, il cittadino danese può dormire sonni tranquilli. I dati generati da un ipotetico intervento clinico a Barcellona saranno registrati e visualizzati in modo sicuro e corretto anche nel suo paese d'origine.

KONFIDO

L'approccio basato su blockchain garantisce, per esempio, che:

- tutte le parti interessate abbiano la **stessa copia dei dati**;
- ogni volta che si vuole accedere a un "dato paziente", l'accesso viene gestito automaticamente attraverso l'uso di uno smart contract;
- ...

In questo contesto Bit4id ha concepito, progettato e sviluppato il sistema di logging delle transazioni tra differenti paesi UE basato su tecnologia blockchain (Hyperledger Fabric) e cifratura dei dati.

Progetto EUCLID (Bit4id)

EUCLID

Di cosa si tratta:

EUCLID è un progetto di ricerca finanziato dal Ministero dello Sviluppo Economico che ha lo **scopo di sviluppare nuove soluzioni per l'identità digitale**, combinando tecnologie innovative come blockchain, funzioni omomorfiche, etc.

Nell'ambito di questa attività progettuale Bit4id, assieme ai partener del progetto, svilupperà una serie di prototipi quali:

- Tracciamento di filiera per beni di largo consumo;
- Tracciamento e verifica di autenticità di beni di grande valore;
- Voto elettronico per assemblee societarie e organizzazioni professionali;
- Gestione di dati sensibili (cloud) in ambito sanitario e contrattualistica del lavoro.

Trusted Data Sharing tra le PA Nazionali, Europee e i Cittadini (Eustema)

Trusted Data Sharing tra PA Nazionali/Europee e Cittadini

Contesto:

Digital Single Market (DSM): La Commissione europea indica chiaramente la **strategia per garantire l'accesso alle attività online** per privati e imprese in condizioni di concorrenza leale, protezione dei consumatori, protezione dei dati, etc.

A favore del DSM sono stati istituiti una serie di **regolamenti nazionali o comunitari**:

- protezione dei dati individuali (GDPR),
- normativa sui pagamenti (PSD2),
- riconoscimento dell'identità digitale per l'accesso ai servizi delle PA degli Stati membri (eIDAS),
- Sistema Pubblico di Identità Digitale (SPID),
- ...

Trusted Data Sharing tra PA Nazionali/Europee e Cittadini

Motivazioni:

In questo contesto, l'idea progettuale di Eustema si basa sull'utilizzo della tecnologia blockchain come piattaforma per **abilitare la condivisione certificata dei dati** degli utenti tra le PA e favorire l'**interoperabilità tra i fornitori di servizi**, garantendo così la **sicurezza** e la **trasparenza**.

La blockchain può essere sfruttata perchè garantisce *privacy-by-design*, per

- il tracciamento dei consensi
- il tracciamento dei dati richiesti (dai prestatori di servizi) e concessi (dall'utente) per effettuare una transazione.

Possibili casi d'uso:

- sistemi federati di certificazione di titoli di studio o di stato di famiglia;
- gestione delle iscrizioni all'anagrafe degli italiani residenti all'estero;
- gestione federata di carte di identità;

Blockchain e Gestione Consensi del GDPR (Eustema)

Blockchain e Gestione Consensi del GDPR

Contesto:

L'idea progettuale si sviluppa attorno alla **gestione dei consensi in conformità al regolamento GDPR**.

Eustema propone la realizzazione di un *registro consensi*, certificato e protetto, e basato su **tecnologia blockchain per memorizzare i consensi al trattamento dei dati del cittadino** per l'accesso ai servizi della PA.

Possibili vantaggi di questo approccio sono:

- **gestione del consenso sicura e trasparente** (si riducono i ricorsi al garante)
- memorizzazione del consenso in un **registro indipendente dal singolo Ente** (si facilita l'interoperabilità)

Blockchain4doc (Eustema)

Blockchain4doc

Di cosa si tratta:

Blockchain4doc è un sistema di protezione di **repository documentale** pensato per un utilizzo in **ambito aziendale**.

La sua sicurezza risiede nell'utilizzo di una **blockchain privata** e di tecniche di **end-to-end encryption**.

Come viene utilizzata la blockchain?

- per il **controllo dell'integrità** dei documenti;
- per il **controllo degli accessi** al singolo documento — per esempio utilizzando gli **smart contracts** per negare la lettura di un documento protetto da password per un certo lasso di tempo.

.

Obiettivo immagine: Estetica della fotografia e cultura del territorio (UniMI + Brera)

Obiettivo immagine

Di cosa si tratta:

- Valorizzazione del percorso artistico dei giovani fotografi dell'accademia di Brera (la loro **storia**);
- Tutela del **diritto d'autore** delle loro opere;

Questi artisti potrebbero avere interessi contrastanti con

- le case d'asta,
- le gallerie,
- i collezionisti di opere d'arte,
- ...

Obiettivo immagine

Un semplice esempio:

Queste fotografie sono valutate approssivamente 1.000 $ la prima (Vibeke Tandberg), 300-400 mila $ la seconda (Jeffrey Wall) e nulla la terza (una collega @UniMI).

Obiettivo immagine

Obiettivi

- la sperimentazione di un **modello inedito di certificazione estetica**;
- la **tutela del diritto d'autore** attraverso l'utilizzo della **blockchain**;
- la **valorizzazione di nuovi talenti artistici**.

La blockchain è utilizzata per memorizzare

- il fingerprint di un'immagine/archivio fotografico
- la storia dell'artista, le tecniche fotografiche utilizzate, il suo stile, ...
- la storia di quello scatto, dove è stato esposto, il suo valore economico, ...

Obiettivo immagine

Il progetto prende forma...

Nel 2017 ha vinto un **bando regionale**.

A novembre 2018 ha vinto il **concorso nazionale *Idee Vincenti*** ideato da **Lottomatica** e sviluppato in collaborazione con l'incubatore di imprese del Politecnico di Milano.
L'iniziativa è finalizzata a incentivare nuove idee d'impresa basate su tecnologie avanzate per sostenere la **promozione e lo sviluppo innovativo del patrimonio artistico e culturale** del nostro Paese.

Da gennaio 2019 questa idea diventerà una startup UniMI: **Authclick**.

Solo, open source security key & wallet (SoloKeys)

Solo, open source security key & wallet

Di cosa si tratta:

HW per memorizzare le chiavi private, fornendo un dispositivo entry level anche a quelle persone che non hanno familiarità con i concetti crittografici

Solo, open source security key & wallet

Obiettivi:

- Costruire un dispositivo **sicuro**, **economico** e **open source**.
- Implementare una *strong two-factor authentication*
- Supporta il nuovo standard FIDO2
- Creazione di un portafoglio hardware a basso costo.

- Campagna di lancio del prodotto: 2795 sostenitori e 125 mila $ per avviare la produzione
- Certificazione FIDO2
- ETH wallet in versione alpha

Digital Chain of Trust (FBK)

Digital Chain of Trust

Di cosa si tratta:

É un progetto EIT sviluppato da un consorzio internazionale (FBK, Poste Italiane, Systematic, INNOPAY, ...)

Contesto:

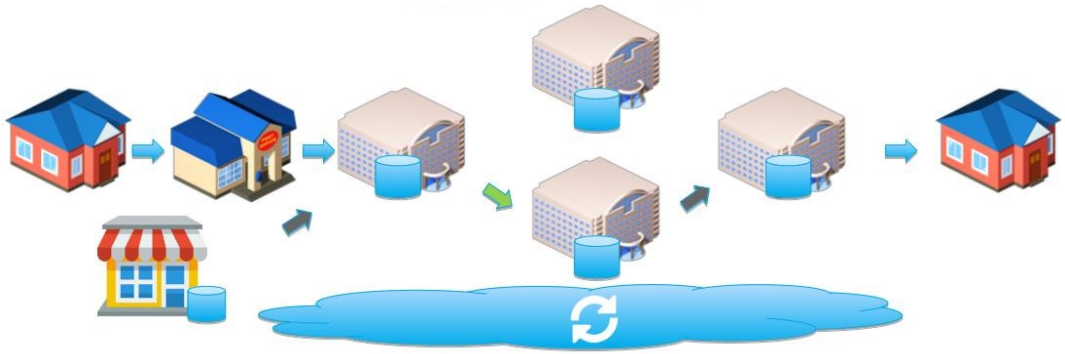
L'economia europea beneficia di una **solida infrastruttura di consegna pacchi** come fattore abilitante per la crescita nell'e-commerce. In che modo questa infrastruttura può beneficiare dell'uso delle nuove tecnologie?

Obiettivi del progetto:

- Realizzazione di una soluzione commerciale per il **tracciamento della custodia di oggetti importanti**
- Confidenzialità dei dati (Attribute-based Encryption)
- Log immutabile dei **passaggi di custodia** (blockchain – Hyperledger Fabric)

Digital Chain of Trust

La mancanza di informazioni di controllo può introdurre una serie di rischi. É evidente la difficoltà nel tracciare un pacco in un sistema complesso.



In questi casi la blockchain può essere utilizzata per **tracciare la provenienza**, l'**immutabilità** e la **disponibilità** di un bene.

Cherrychain (FBK)

Cherrychain

Descrizione:

CherryChain è un start-up che lavora con nuove tecnologie quali Distributed Ledger Technology (DLT) e Smart Contract. Obiettivo di R&D è lo sviluppo del protocollo CherryChain aderente alle normative GDPR, PSD2, 4AML e ai nuovi sistemi di autenticazione Mobile.

Ricerca Industriale e Sviluppo sperimentale

- **Ricerca e sviluppo** con FBK (Identity Management, Strong Authentication, Compliance & Privacy, etc.) tramite la legge provinciale sugli incentivi alle imprese (Legge 6/99);
- Partecipazione di alcuni attori in **fase di sperimentazione** quali Banca Popolare dell'Alto Adige, Dolomiti Energia e Conad cooperative DAO.

Progetto SecureOpenNets – Distributed Ledgers for Secure Open Communities (UniTN)

SecureOpenNets

Di cosa si tratta:

É un progetto PON - Ricerca e Innovazione sviluppato in un consorzio di 9 partner che vuole ottenere **soluzioni blockchain** per le **smart communities**

Tre linee di Ricerca e Sviluppo

- Blockchain per la Privacy (CryptoLab di UniTN)
- Blockchain per la Sharing Economy
- Blockchain per i Digital Rights

Blockchain, DLTs e standardizzazione

Di cosa si tratta:

Attività di standardizzazione su blockchain e distributed ledger tecnologies (Dott. P.Campegiani, Bit4id)

Borsa di dottorato industriale

Borsa di dottorato industriale

Di cosa si tratta:

- di una opportunità sottoutilizzata dalle industrie;
- al sud ci sono borse gratis POR e PON per dottorati industriali;

Bit4id e Dottorato di Ricerca in Ingegneria dell'Informazione

- Titolo: Tecnologia Blockchain: Dati Privati e Applicazioni Industriali
- Responsabile del progetto: Prof. Ivan Visconti, Università degli Studi di Salerno
- Periodo in Azienda: 12 mesi, presso Bit4id, referente Dott. Paolo Campegiani
- Periodo all'estero: 6 mesi, presso University of Edinburgh, referente Prof. Vassilis Zikas

Grazie per l'attenzione!