Spunti di ricerca in CifrisChain

Norberto Gavioli
Università dell'Aquila

CifrisChain 2019
Roma 9 maggio 2019

Alcuni progetti aziendali attivi in De Cifris

- Parcel delivery - DCOT
- EUSTEMA
  - Trusted Data Sharing
  - Gestione consensi GDPR
  - Blockchain4doc
- Bit4Id
  - KONFIDO
  - EUCLID
- Cherry-Chain
- Armundia Group

Parcel delivery

- DCOT (Digital Chain of Trust) è un progetto EIT (European Institute of Innovation & Technology)
- Consorzio tra INNOPAY, Poste Italiane, FBK Engineering, Fraunhofer Institute, Systematic

Parcel delivery

- A fronte di un'enorme crescita del commercio elettronico vi è l'esigenza di uniformare il sistema di tracciamento per lo stato di consegna dei colli.
- Un sistema di E-Commerce affidabile ha numerosi benefici:
  1. efficienza,
  2. capillarità nella distribuzione
  3. competitività e contenimento dei prezzi
- Richiede peraltro fiducia nel sistema da parte dei consumatori, sia per quanto riguarda le transazioni economiche, che nei sistemi di consegna che sono in gran parte frammentati.

Parcel delivery

- La principale difficoltà nei sistemi di consegna è il tracciamento della custodia delle merci quando sono coinvolti numerosi attori e processi (trasporto, verifica, smistamento, ecc…)

- Possibili rischi in questo processo sono
  1. Esposizione dei dati personali
  2. Difficoltà di controllo/correzione/integrazione dei dati necessari alla spedizione durante la consegna
  3. Difficoltà a ricostruire i singoli passaggi della spedizione

Parcel delivery

- La tecnologia blockchain permette una soluzione

- Il sistema
  - traccia la catena di custodia dei colli in ogni stadio
  - garantisce provenienza, stato attuale della spedizione e immutabilità
  - è accessibile da tutte le parti interessate
  - permette l'integrazione delle informazioni di spedizione da parte di mittenti e destinatari
  - permette il controllo dei dati personali e ne garantisce la protezione

Trusted Data Sharing

Progetto di EUSTEMA

- Il progetto propone una metodologia basata su blockchain per l'interoperabilità tra pubbliche amministrazioni europee.
- Direttive e normativa

  Digital Single Market, eIDAS, GDPR, PSD2, SPID, EIF

Trusted Data Sharing

- **eIDAS** (**electronic IDentification Authentication and Signature**) stabilisce l'interoperabilità tra gli stati Membro Europei per i sistemi di identificazione e stabilisce le regole ed un framework legale per i servizi fiduciari
- **GDPR (General Data Protection Regulation)** stabilisce regole specifiche per la protezione dei dati individuali ed il loro libero movimento, abrogando le precedenti direttive europee e nazionali
- **PSD2 (Payment Service Directive 2)** dispone norme tecniche sulla Strong Authentication per i clienti per disporre operazioni di pagamento. Introduce nuovi attori quali i Third Party Providers (TPP) che possono offrire servizi a partire dai dati di pagamento dei clienti (PISP, Payment Initiation Service Provider e AISP, Access Information Service Provider).
- **SPID (Sistema Pubblico di Identità Digitale)** è il sistema previsto dall'Italia per l'identificazione e l'autenticazione a livello nazionale.
- **EIF (European Interoperability Framework)** è il framework per promuovere e supportare il delivery di servizi pubblici interoperabili in modo cross-nazionale e cross-settoriale.

Trusted Data Sharing

- In particolare l'EIF è un framework di interoperabilità

- L'interoperabilità facilita la:
  - Cooperazione tra le pubbliche amministrazioni con lo scopo di fornire servizi pubblici;
  - Lo scambio di informazioni tra le pubbliche amministrazioni per soddisfare requisiti legali o impegni politici
  - Condivisione ed il riuso di informazioni tra le pubbliche amministrazioni per migliorare l'efficienza ed abbattere la burocrazia per I cittadini e le imprese

Trusted Data Sharing

- Principali obiettivi del progetto
  - Sperimentare una piattaforma digitale per abilitare un modello standard di interoperabilità
  - Utilizzare la piattaforma digitale per consentire ai service provider di certificare l'anagrafica dell'utente (titolo di studio, stato di famiglia, domicilio digitale, vaccinazioni, ecc.)
  - Utilizzare la piattaforma per disassociare i dati dell'utente dall'erogatore di servizi in modo «trusted»
  - Costruire un Personal Data Store che permette all'utente di memorizzare i propri dati in modo sicuro e controllato dall'utente stesso.
  - Avere un ambiente che permette all'utente di verificare e revocare i consensi prestati circa i dati personali

Trusted Data Sharing

- Esempi di applicazioni
  - Sistema federato di certificazione titoli di studio
  - Sistema federato di certificazione stato di famiglia
  - Gestione delle iscrizioni all'A.I.R.E. (Anagrafe Italiani residenti all'estero)
  - Gestione federata delle carte d'identità
  - Gestione federata delle firme digitali
  - Certificazione titolo Universitario ed iscrizione transfrontaliera

Gestione dei consensi in conformità al regolamento GDPR

Progetto EUSTEMA

Caratteristiche principali

- L'accesso al Registro Consensi è associato all'identità SPID
- I cittadini potranno fruire di un'unica interfaccia per consultare e gestire tutti i consensi al trattamento espressi verso le amministrazioni compreso il loro ciclo di vita
- le amministrazioni, vengono sollevate da una serie di impegni inerenti la gestione del consenso
- la gestione del consenso è trasparente
- il consenso è memorizzato in un registro uniforme ed indipendente dal singolo ente facilitando l'interoperabilità

Gestione dei consensi in conformità al regolamento GDPR

Spunti per altri sviluppi

- estensione della piattaforma consensi anche ai Service Provider privati
- verifica dei consensi ed esecuzione automatica dei permessi tramite Smart Contract
- utilizzo della blockchain come piattaforma di trasparenza e affidabilità: infrastruttura di certificazione dati (es. pagamento tasse, posizione pensionistica), ecc.
- autocertificazione degli attributi qualificati
- interoperabilità con ANPR

Blockchain4doc

Progetto EUSTEMA

- sistema di protezione di repository documentale con utilizzo in ambito aziendale; blockchain privata.
- sicurezza assicurata utilizzando una blockchain privata e di end-to-end encryption
- controllo capillare da parte degli utenti sul versionamento di ogni file
- evita il fork nell'edizione condivisa di documenti
- sulla blockchain vengono salvati i digest di documenti residenti in un repository privato
- sono possibili alcune funzionalità di flusso documentale
- i metadati (es: versionamento) dei documenti sono pubblicati in forma cifrata sulla blockchain
- Gli utenti autorizzati possono seguire l'intero ciclo di vita dei documenti

KONFIDO

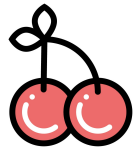
- Progetto Bit4Id
  - Blockchain based logging, progetto finanziato dal programma Horizon 2020
  - Sviluppo di una soluzione che garantisce:
    - origine ed integrità dei log
    - privacy degli utenti
    - immutabilità e accesso distribuito ai dati

EUCLID

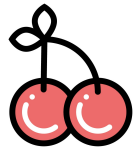
- EU Computing services Leveraging digital Identity
- Progetto Bit4Id, finanziato nell'ambito del bando Grandi Progetti R&S - PON 2014/2020
- Principali obiettivi

  - identità digitale a supporto delle applicazioni su cloud per l'autenticazione, la tracciabilità e la sicurezza delle informazioni, di persone, di beni e prodotti.
  - sistema per la tracciatura di filiera e di autenticità sia per beni di valore (es. opere d'arte) sia per prodotti di largo consumo, basato su blockchain, chip NFC e tecniche spettrometriche

CherryChain



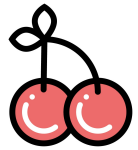
- Blockchain privata
- Interoperabiltà nei sistemi di pagamento tra banche, pagatori, beneficiari e PISP/ AISP con fatturazione e conciliazione del pagamento
- Utilizza un sistema di consenso basato sul protocollo Raft e garantisce performance nelle transazioni
- Basso consumo nelle operazioni di mining (consenso).
- Supporta nativamente gli smart contract

CherryChain 

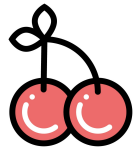
- Processi di filiera nella **distribuzione dell'energia elettrica**

  Benefici della tecnologia blockchain

  - Produzione: facile accesso al mercato all'ingrosso
  - Vendita all'ingrosso: processi di clearing automatizzati, scambi senza intermediari, accesso agli scambi da parte degli enti regolatori
  - Contratti e pagamenti tramite smart contracts (es. mercato all'ingrosso dell'energia)
  - Gestione automatizzata di trasmissione, distribuzione e misura
  - Vendita al dettaglio: automazione pagamenti e accesso diretto al mercato all'ingrosso, maggior trasparenza
  - Bilanciamento automatico P2P tra consumer e prosumer senza intermediari

CherryChain 

- Generazione nuova offerta digitale
  - si può sottoscrivere rapidamente il contratto attraverso canale digitale; si possono attivare nuove formule di gestione come pre-pagati, stabilire degli importi fissi alle proprie fatture, modalità di dilazione o rateizzazione.
- Gestione dei processi
  - Orchestrazione processi dal contratto all'incasso, pagamenti e riconciliazioni per renderli meno onerosi in termini di rischi e costi.
- Smart Device & Community
  - Smart meter/IoT per lo scambio dei dati, dal trading energetico alla mobilità elettrica e gestione di comunità energetiche di utenti prosumer.

CherryChain 

- Sicurezza basata su
  - Identity Management;
  - Strong Authentication;
  - Crittografia;
  - Security;
- Compliance & Privacy (Psd2, AML, GDPR);

Armundia Group

- Attività: soluzioni software banking/finance/insurance
- Attività di ricerca con l'Università dell'Aquila
- Tavolo di lavoro su tecnologie DLT e smart contracts per l'automazione e la trasparenza dei processi/contratti bancari e assicurativi e per l'accesso agevolato al mercato dei prodotti da parte dei broker

Martedì 14 maggio a L'Aquila

Nel corso di **combinatoria e crittografia** ci saranno presentazioni a cura di EUSTEMA e GT50 con le quali sono in corso contatti per future collaborazioni (non necessariamente su blockchain).

Grazie per l’attenzione