BLOCKCHAIN
PER
PROCESSI AZIENDALI

Alessio Meneghetti
CifrisChain 2018 ROMA - DE CIFRIS

PON MIUR inizio luglio 2018

CryptoLabTN ha presentato una domanda vincente di finanziamento al PON MIUR, per un progetto di valore complessivo di circa **9 milioni di euro** (su 30 mesi), con partner principale **Poste Italiane**.

Il progetto ha come tematica unificante le applicazioni della blockchain.

Nel suo complesso, il progetto coinvolge i seguenti partner:

Accademia: CNR-, UNITN, UNIRC, UNICAL,

Aziende: Poste, Alkemy Tech, OKT, BV Tech, SUBCOM,

Obiettivi generali PON lato UNITN

All'interno del progetto, il CryptoLabTN individua soluzioni tecnologiche capaci di raggiungere i seguenti obiettivi di carattere generale:

1. migliorare i processi aziendali connessi all’uso di dati personali di utenti, da un punto di vista sia della sicurezza, sia della tracciabilità: confidenzialità, integrità e disponibilità;

2. abilitare processi automatici di verifica della compliance normativa, in particolare sulla gestione dei dati personali, viste anche le nuove norme europee e la complessità della loro attuazione.

Caso d'uso: i permessi della privacy

La piattaforma che il CryptoLabTN progetterà assieme a Poste Italiane avrà come caso d'uso immediato la gestione del

ciclo di vita dei consensi privacy e dei processi collegati,

preservandone le caratteristiche di sicurezza in termini di

confidenzialità, integrità e disponibilità,

abilitando al tempo stesso attività di analisi, monitoraggio e verifica di compliance normativa.

PRIVACY PRESERVING BLOCKCHAIN

Una **blockchain** per sua natura conserva **dati accessibili** a tutti i partecipanti, se non addirittura a chiunque sia connesso su Internet.

Vi è talvolta la necessità di proteggere **specifiche informazioni** conservate su una blockchain da accessi indesiderati. Per realizzare questo, è necessario introdurre **primitive crittografiche sofisticate** che mascherano in qualche modo le informazioni non divulgabili.

In generale, si parla di PRIVACY PRESERVING BLOCKCHAIN.

Approccio al problema

Nella proposta progettuale si prevede esplicitamente di avvalersi di tecnologia blockchain.

PRO

Immutabilità, verifica automatica, disponibilità

CONTRO

Apparente perdita di confidenzialità -> risolvibile con una

privacy-preserving blockchain progettata ad hoc dal **CryptoLabTN**

Approfondimento tecnico I

Nella tesi di dottorato di Riccardo Longo, 2018, seguita dal prof. M. Sala (UNITN), viene affrontato il problema della privacy-preserving blockchain da un punto di vista protocollare e crittografico.

- Ad ogni persona vengono associate **transazioni** che riguardano i propri dati e documenti.

- Il contenuto delle transazioni è cifrato con un sistema a chiave simmetrica, nota solo all'utente.

- La blockchain similmente a Ethereum viene accompagnata da uno **stato**

Approfondimento tecnico II

- Lo **stato** contiene solo alcune informazioni necessarie per decifrare il contenuto delle transazioni.

- Poniamo che Alice voglia accedere al contenuto di una transazione di Bob e che Bob sia consenziente:
  Bob invia ad Alice un token autorizzativo, col quale Alice riesce a ottenere dallo **stato** la chiave simmetrica della transazione in questione.

- Lo **stato** viene aggiornato periodicamente da un processo automatico chiamato **StateKeeper**

Approfondimento tecnico III

- Al primo aggiornamento dello **stato** successivo al token di Alice, lo stesso token diventa inutilizzabile

- Naturalmente Alice potrebbe salvarsi la **chiave simmetrica**, ma **si dimostra** che non ne avrebbe vantaggio

- Inoltre **si dimostra** che lo **StateKeeper** non può violare la confidenzialità del contenuto delle transazioni: anzi non ha nessuna informazioni addizionale rispetto a un utente qualunque del sistema.
  L'unico problema è se lo **StateKeeper** si impossessa di un token.

Grazie dell'attenzione!