# Studio tecnologico Identity Trust Fabric

## Diario delle modifiche

|  |  |  |
| --- | --- | --- |
| Data | Descrizione | Autore |
| 12/06/18 | Creazione documento. Scrittura dei capitoli Descrizione prodotto, scopo del documento e ITF, Permissionless e Permissioned blockchain, Ethereum | Simone Ballarin |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Scopo del documento

Nell’ottica di un prossimo sviluppo di un’estensione basata su blockchain dell’attuale servizio ora in produzione MonoKee, questo documento intende valutare in termini di benefici tecnici e tecnologici l’uso della tecnologia Ethereum quale base dell’Identity Trust Fabric (ITF).

## Riferimenti

1. Blockchain: The Dawn of Decentralized Identity (G00303143), Homan Farahmand per Gartner
2. Sito ufficiale Ethereum, [www.ethereum.org](http://www.ethereum.org)
3. bornonjuly4.me/2017/01/10/blockchain-what-is-permissioned-vs-permissionless

## Descrizione prodotto

Il progetto ha come scopo la creazione di un’estensione del servizio MonoKee basato su blockchain. L’estensione offre un sistema di Identity Access Management (IAM) composto da quattro principali fattori:

1. Identity Wallet (IW)
2. Service Provider (SP)
3. Identity Trust Fabric (ITF)
4. Trusted Third Party (TTP)

In sintesi l’estensione dovrà operare al fine di fornire la possibilità ad un utente di registrare e gestire la propria identità tramite l’IW autonomamente, mandare i propri dati (IPP) all’ITF la quale custodirà la sua identità e farà da garante per le asserzioni proveniente dai TTP. Inoltre il SP dovrà essere in grado con le informazioni provenienti da IW e ITF di verificare o meno l’accesso ai propri servizi.

## ITF – Identity Trust Fabric

Sulla base di un primo studio di fattibilità l’unico componente coinvolto nell’uso blockchain è l’Identity Trust Fabric. La sua principale funzione è quella di poter permettere ai vari Service Provider aderenti al servizio di poter verificare le informazioni rilasciate dai vari utenti tramite l’utilizzo del loro personale Identity Wallet (IW). Il componente mantiene al suo interno l’hash della chiave pubblica degli utenti (che rappresenta la loro identità) e le asserzioni fornite dai vari IW che possono essere potenzialmente certificate da una TTP (tramite una firma con la loro chiave privata). Le asserzioni devono poter essere modificate o eliminate in ogni momento, ovviamente ogni alterazione deve essere ogni volta certificata nuovamente. Anche da parte del TTP ci dev’essere la possibilità di revocare la certificazione di un’asserzione.

Una buona implementazione di una ITF deve possedere le seguenti caratteristiche:

* Fiducia: il contenuto presente nella ITF deve essere solo quello autorizzato, non ci devono poter essere manomissioni malevoli da parte degli utilizzatori della rete. Ogni componente deve potere aver fiducia nella veridicità dei dati.
* Garanzia: le regole logiche della ITF non devono poter essere manomesse. Deve essere possibile applicare le varie policy aziendali in ambito di gestione dei rischi.
* Tracciabilità: ogni informazione e cambio di stato relativo alle identità e alle asserzioni deve poter essere tracciato e verificabile sia in termini cronologici sia in termini di provenienza.
* Sicurezza: intesa come CIA. L’ITF deve rispettare i vincoli di confidenzialità, inalterabilità e disponibilità delle informazioni dentro lei contenute.
* Scalabilità: l’ITF deve fornire un elevato grado di scalabilità soprattutto in un’ottica in cui il prodotto potrebbe essere reso disponibile ad un uso Consumer.
* Efficienza: il funzionamento dell’ITF deve richiedere la minima quantità di risorse possibili.

## Permissionless e Permissioned blockchain

Al fine di poter valutare la fattibilità dell’utilizzo di Ethereum quale blockchain sottostante all’ITF è necessario avere in mente le due principali categorie di blockchain: **permissionless** e **permissioned**.

### Permissioned blockchain

Una permissioned blockchain pone dei vincoli sulla partecipazione alla rete. Soli i nodi autorizzati possono partecipare all’algoritmo di consenso dei blocchi. Le autorizzazioni possono essere date singolarmente, quindi i vari nodi possono avere o meno le seguenti possibilità:

* lettura dei blocchi;
* scrittura dei blocchi;
* esecuzione di codice;
* verifica dei nodi.

### Permissionless blockchain

Una permissionless blockchain è una rete in cui qualsiasi nodo può partecipare al processo di verifica dei blocchi. Ogni nodo ha tutte le precedenti quattro proprietà.

## Ethereum

Ethereum è una rete blockchain **permissionless** con la principale caratteristica di poter eseguire codice. L’uso di questa tecnologia presenta

## 