Condividere informazioni in modo sicuro combinando Git e Blockchain

Paolo Speziali

Università degli Studi di Perugia - Dipartimento di Ingegneria

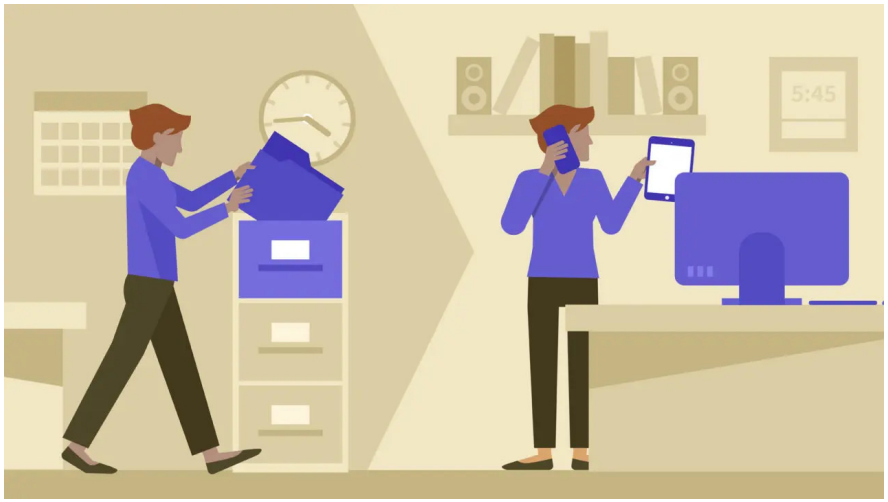
A.D. 1308
unipg
DIPARTIMENTO
DI INGEGNERIA

A.A. 2020/2021

Indice

La digitalizzazione

È in atto, negli ultimi anni, un piano di **digitalizzazione** delle PA. Esso mira all'evoluzione tecnologica di tutte le sue mansioni e alla creazione di portali web per il cittadino. L'esigenza di questa trasformazione si è fatta sentire anche da parte dell'Unione Europea, che con il Recovery Fund ci sta fornendo i fondi per attuarla.

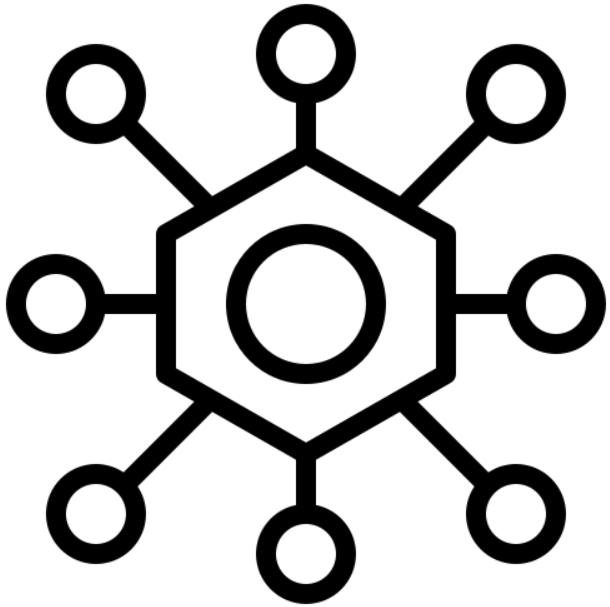


Il problema della burocrazia

Tuttavia, anche avendo i fondi necessari, sono molti i problemi che non permettono una digitalizzazione totale delle PA, tra cui la lenta e farraginosa macchina della burocrazia. Sembra necessario un processo di **sburocratizzazione** grazie a degli strumenti digitali che permettano di salvare, validare e condividere documenti in maniera sicura.

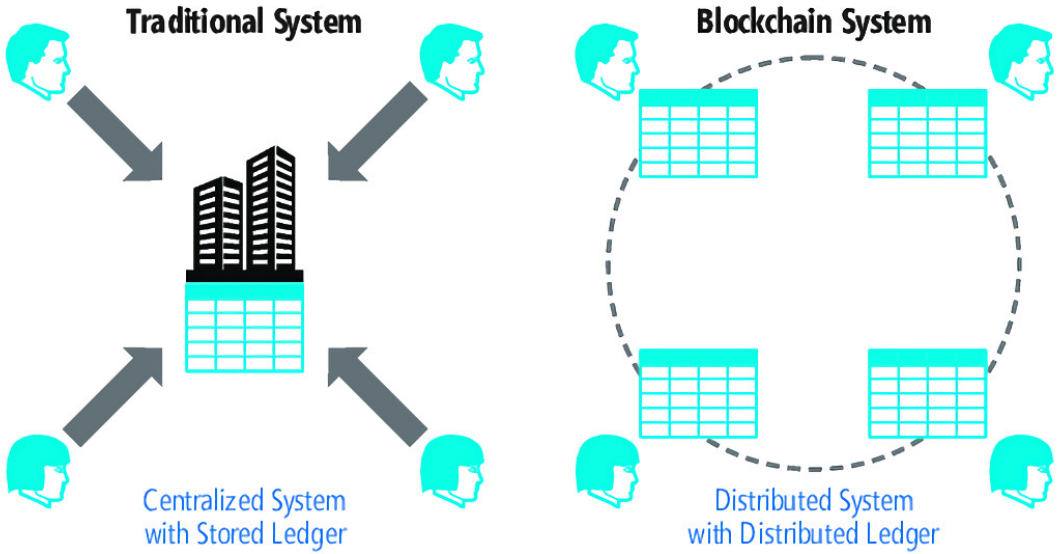
Gli strumenti attuali

Gli strumenti attualmente in utilizzo hanno un'architettura centralizzata: un'entità centrale si occupa dell'immagazzinamento e della verifica dei dati degli utenti. Ciò è potenzialmente rischioso, sia perché potrebbero verificarsi attacchi alle unità centrali, sia perché mettiamo in mano di un'azienda esterna i nostri dati.



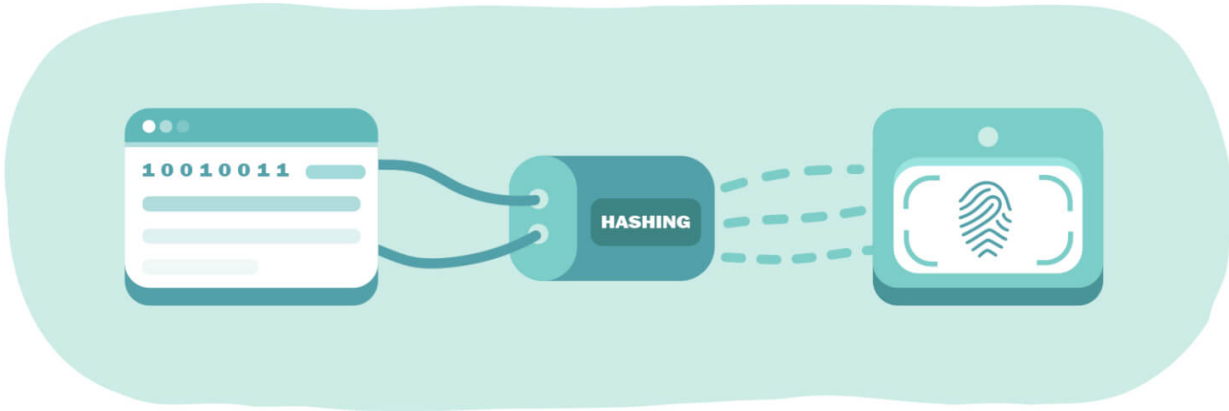
Strumenti decentralizzati

Usando invece strumenti decentralizzati, sia per la gestione dei file, per cui utilizzeremo **Git**, sia per la verifica delle informazioni, per cui useremo la **blockchain**, saremo in grado costruire uno strumento che può affidarsi alla parola di una moltitudine di entità, rendendo molto più complicati e rilevabili attacchi e manomissioni.



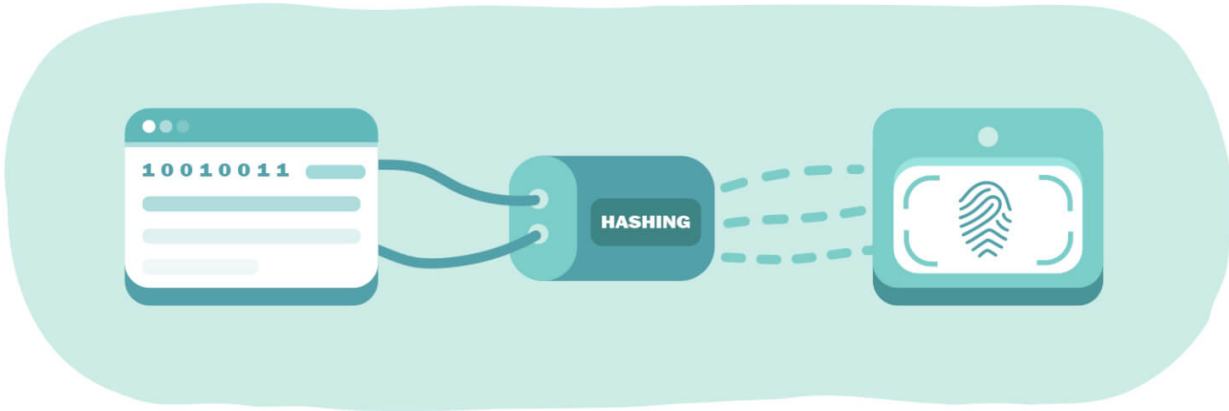
Funzioni crittografiche di hashing

Una funzione crittografica di hashing è una funzione di hashing, ovvero una funzione che permette di associare, a una qualsiasi sequenza m di lunghezza arbitraria in input, una sequenza in output $h(m)$ di lunghezza costante, con alcune proprietà aggiunte che deve seguire per poter essere considerata *crittograficamente sicura*. Esse impediscono di risalire all'input originale e facilitano i **controlli di integrità sui file**.



Il Problema

Una funzione crittografica di hashing è una funzione di hashing, ovvero una funzione che permette di associare, a una qualsiasi sequenza m di lunghezza arbitraria in input, una sequenza in output $h(m)$ di lunghezza costante, con alcune proprietà aggiunte che deve seguire per poter essere considerata *crittograficamente sicura*. Esse impediscono di risalire all'input originale e facilitano i **controlli di integrità sui file**.



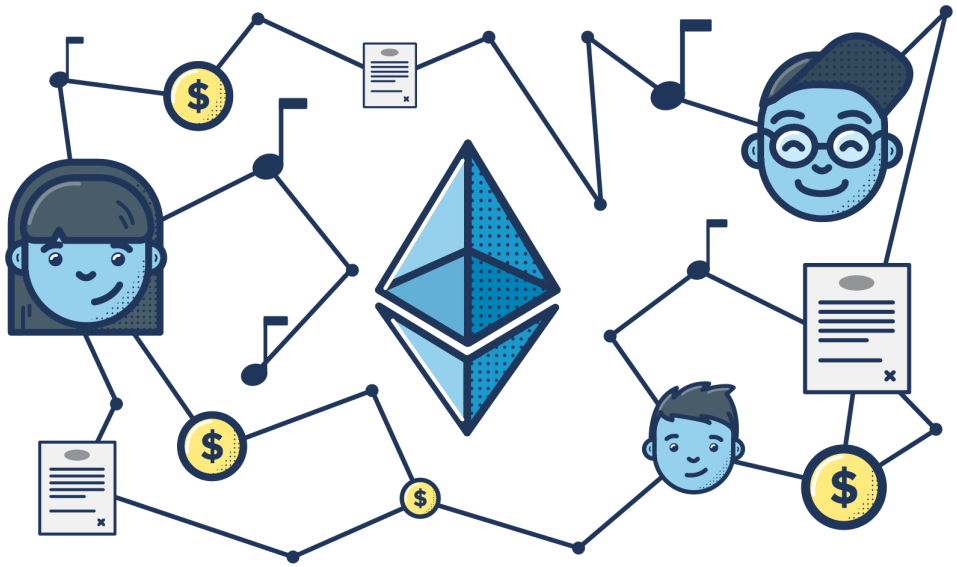
Fase 2: Specifica dei requisiti

L'applicazione avrebbe dovuto quindi fornire all'utilizzatore le funzionalità del software Git corredando il tutto con la possibilità di registrare e, successivamente, verificare l'integrità delle Storage Unit. Una volta creata una Storage Unit essa deve essere immutabile, dando tuttavia la possibilità di esportarne singoli file dotandoli sempre di meccanismi di controllo.

Figura: Il logo dell'applicazione

Excursus su Ethereum e Blockchain

La tecnologia di Ethereum permette la creazione di una rete distribuita e decentralizzata finanziata e incentivata ad operare e rimanere attiva mediante la creazione, lo scambio e l'utilizzo dell'omonima criptovaluta.

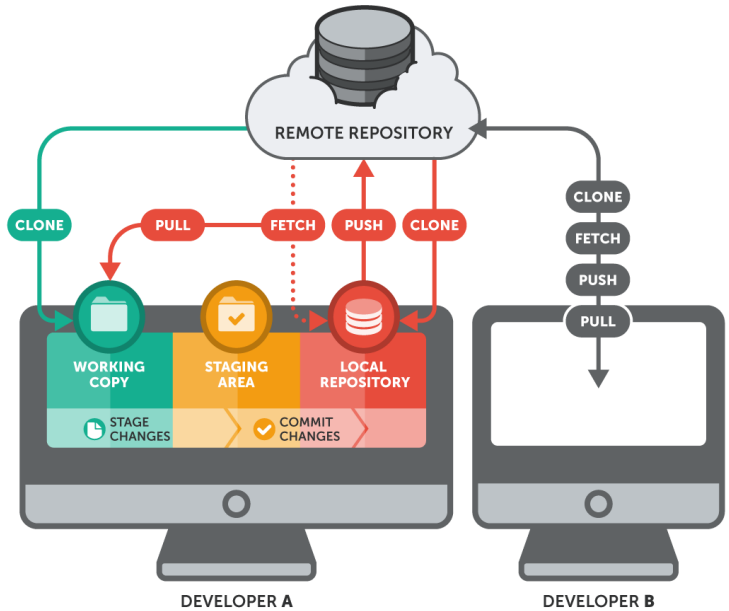


Excursus sulle Applicazioni Distribuite

Su tale rete è possibile mettere a disposizione delle applicazioni che chiunque può utilizzare dietro pagamento di una piccola commissione. Queste applicazioni sono realizzabili dagli sviluppatori interessati tramite vari framework e suite di applicativi, il più celebre è **Truffle**.

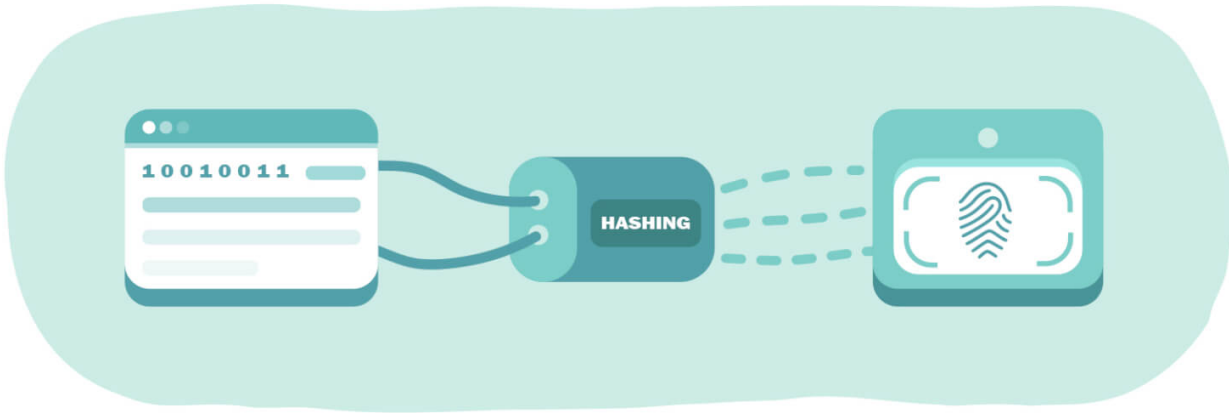
Excursus su Git

Git è un software che permette in maniera semplice di gestire insiemi di file tramite un sistema di controllo di versione, una grande risorsa per gli sviluppatori che devono contribuire in maniera condivisa ad uno stesso progetto o che devono tenere sotto controllo i vari cambiamenti che sono stati apportati ai vari file e documenti.



Excursus sulle funzioni di hashing

Le funzioni di hashing sono funzioni non invertibili che permettono di associare in maniera univoca (o quasi) stringhe di caratteri (e quindi anche documenti di varia natura tradotti in stringhe) a delle stringhe alfanumeriche di lunghezza fissa.



Fonti

- Strumenti Ethereum per sviluppatori
- Tutorial Truffle DAPPs - Pet Shop
- Build a JavaScript CLI with Node.js
- Tutorial di Mozilla su async / await
- Immagini reperite dai siti ufficiali degli strumenti eccetto per alcune scaricate da queste pagine web:
  - Funzioni di Hashing
  - Concorso pubblico
  - Ethereum Blockchain
  - Git repository
  - async / await
  - Merkle Tree
- Strumento di upscaling delle immagini