

PROGETTO BLOCKCHAIN



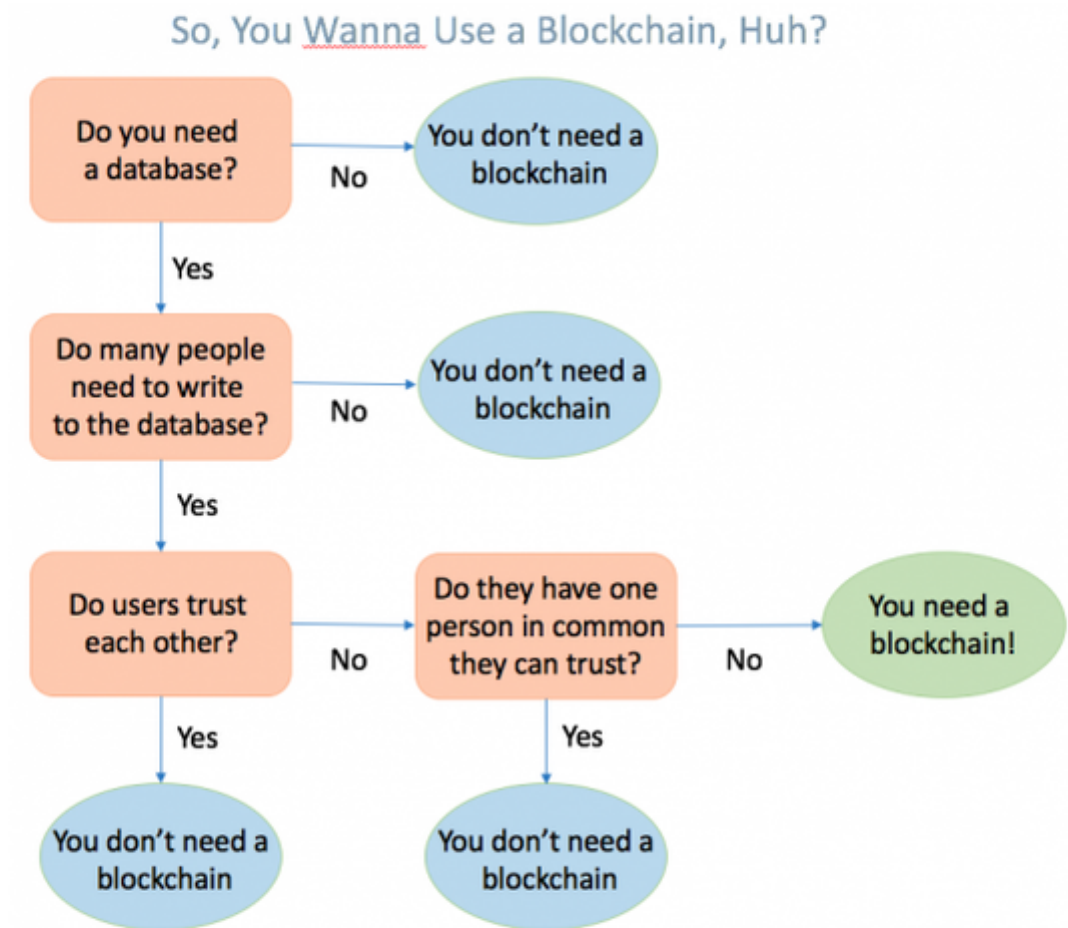
ASPETTI PRINCIPALI

La **BLOCKCHAIN** è una struttura dati **condivisa** e **immutabile**. Questi due aspetti fanno sì che, questa tecnologia sia parte dei **Distributed Ledger**, ossia sistemi che si basano su un registro distribuito, che può essere letto (e in determinati casi modificato) da più nodi di una rete.

Un primo utilizzo della blockchain è stato sul fronte **cryptovalute** (Bitcoin, Ethereum ecc. ecc.) e successivamente, grazie all'avvento degli **smart contract**, si è iniziato ad adottare questa tecnologia su diversi fronti.

JENIA, seguendo questo semplice processo decisionale, realizzato da Tom Davies, ha **identificato** e **realizzato** alcuni casi d'uso della blockchain:

- Notarizzazione di documenti
- Gestione licenze software mediante smart contract



da Tom Davies - So, You Wanna Use a Blockchain, Huh?

CASO D'USO NOTARIZZAZIONE

La **Notarizzazione** di documenti digitali, avviene mediante il calcolo dell'impronta **hash** del documento ed il salvataggio del **timestamp** al momento della generazione dell'impronta.

Essendo la blockchain, per sua definizione, una **Distributed Ledger Technology** (più comunemente **DLT**), diventa una valida soluzione per realizzare la notarizzazione in quanto implementa un'alternativa forte alla "**timestamp authority**" che garantisce la marca temporale.

Elementi chiave

- Poter scegliere un'implementazione di blockchain (Bitcoin, Ethereum, Ripple, Hyperledger ecc.) per notarizzare i documenti rende possibile eliminare il "vendor lock in" verso la **certification authority**.
- Blockchain rappresenta uno standard aperto e "semplice" che permette di ottenere un risultato con maggiore facilità.
- La notarizzazione consente una **verifica pubblica** della **data**, **autenticità** e **integrità** del contenuto del documento senza esporre pubblicamente il contenuto dello stesso.

SINEKARTA

WWW.SINEKARTA.COM

Integrando la decennale esperienza in ambito documentale (mediante la suite **Alfresco**) con le competenze sulla tecnologia blockchain, JENIA ha realizzato una soluzione di Notarizzazione, denominata **Sinekarta**, in grado di integrarsi mediante **web service** con qualsiasi applicazione web.

La soluzione gestisce:

- Insieme di documenti di diversi formati (immagini, pdf, musiche, email, etc)
- Calcola l'impronta di ciascun documento.
- Crea un nuovo documento contenitore di impronte.
- Scrive sulla Blockchain le informazioni necessarie alla Notarizzazione.
- Crea il certificato di avvenuta notarizzazione.
- Espone un servizio pubblico per la verifica della notarizzazione.

Certificato Notarizzazione Documenti del 06/08/2019



Questo certificato fornisce la conferma dell'avvenuta Notarizzazione all'interno della rete blockchain di Bitcoin del file XML, generato da Sinekarta®, che rappresenta i file caricati in Alfresco con l'aspetto di tipo **TimeStampable** nella data 2019-08-06. Sulla base del contenuto del file XML (più precisamente, il codice hash ad esso associato), è stata eseguita una transazione Bitcoin di tipo **OP_RETURN** che ha permesso di salvare definitivamente l'informazione all'interno di un blocco del sistema decentralizzato blockchain.

Scansionando il QR Code associato ad ogni transazione è possibile verificare l'autenticità delle operazioni riportate all'interno della rete Blockchain di Bitcoin.

Timestamp: martedì 6 agosto 2019 12.01.10 CEST

Hash del documento: 359953924559d99b70d7532ef5e576c47fb35c316e9648c62bb12c5805f8f1

Transazione # 1

Bitcoin Transaction id
[071c5d61b391167e493461b773f267734a9a8394867832c5672b16d6e8b1](https://blockchain.info/tx/071c5d61b391167e493461b773f267734a9a8394867832c5672b16d6e8b1)
OP_RETURN DATA
da30380079c410b311b6645203e2a2c4e4570215aae138a1f90d2334f5d47ead



Bitcoin block # [200004](#)
Merkle Root 34c1878c1740c62da1bb0cd895f6c9ca9ae13cc93c936c5b89df178d463ce57

Transazione # 2

Bitcoin Transaction id
[700ec32ad110f131c2684cd6997713798c709867bcb495432b0926c5302](https://blockchain.info/tx/700ec32ad110f131c2684cd6997713798c709867bcb495432b0926c5302)
OP_RETURN DATA
93724201a196cc96b88Dec09954a082b2ear60F913139f6e0de10db4e625c



Bitcoin block # [200004](#)
Merkle Root 34c1878c1740c62da1bb0cd895f6c9ca9ae13cc93c936c5b89df178d463ce57

Transazione # 3

Bitcoin Transaction id
[27269090b613654275ca731ebc1773c60997a14181d43008686449372097c](https://blockchain.info/tx/27269090b613654275ca731ebc1773c60997a14181d43008686449372097c)
OP_RETURN DATA
7e2686f85c1b1133207fb6d450daca57e9d77f85862aa081a52431a744b0



Bitcoin block # [200004](#)
Merkle Root 34c1878c1740c62da1bb0cd895f6c9ca9ae13cc93c936c5b89df178d463ce57

Notarizzazione realizzata da Sinekarta © 2019 - <http://www.sinekarta.com> - Questo certificato è un **Open TimeStamp** di github.com/jenia/opensign
Questo certificato è valido solo se convalidato con uno dei tool online hash4loperatore.it/it/en/

CASO D'USO SMART CONTRACT

Lo Smart Contract è un programma la cui esecuzione e i cui risultati sono garantiti integri dalle proprietà della blockchain, nel nostro caso quella pubblica di **Ethereum**.

lo Smart Contract deve essere in grado di garantire che:

- il codice con cui è stato scritto non possa essere modificato;
- le fonti di dati che determinano le condizioni di applicazione siano **certificate e affidabili**;
- le modalità di lettura e controllo di queste fonti siano a loro volta certificate.

Emerge che lo Smart Contract deve essere preciso sia nella sua stesura sia nella gestione delle regole che ne determinano

l'applicazione e delle regole che devono governarne le eventuali anomalie.

La rete Ethereum, proprio per questo scopo, mette a disposizione, per realizzare **Smart Contract**, la piattaforma di sviluppo e deploy denominata **Remix** che rende disponibili strumenti per scrivere codice **Solidity** e poterne verificare la corretta esecuzione.

Dati questi elementi fondamentali, JENIA negli ultimi anni ha effettuato importanti investimenti nell'apprendimento di tale tecnologia con il principale obiettivo di riuscire ad **integrare**, nelle diverse applicazioni, la blockchain.

LICENZE SOFTWARE

La criticità intrinseca nella gestione delle licenze software è poterne verificare la validità ed eventualmente estenderne la durata.

JENIA ha **realizzato** una soluzione, basata su Smart Contract per rete Ethereum, con l'obiettivo di rendere disponibili delle librerie in grado di dialogare con la blockchain allo scopo di rendere semplice e immediato il controllo o la modifica di una licenza software.

L'approccio tecnologico adottato permette di ottenere

- Un sistema decentralizzato.
- Fail safe.
- Aperto,
- Sicuro.

