netservice
Information Technology

flosslab
Innovation at Work

La Blockchain

Cos'è e perché se ne parla

Marco Di Francesco

Business Unit Manager - Area Blockchain

Responsabile Scientifico presso Flosslab dei progetti di ricerca basati su tecnologie blockchain

Responsabile del progetto Almacert per la certificazione delle lauree su blockchain

Consulente presso il Laboratorio sulle Criptovalute del Dipartimento del Tesoro

Blockchain

Dalla criptovaluta a un nuovo paradigma organizzativo

- Cosa è una blockchain?
- Quali sono le sue origini?
- Come funziona e a quali esigenze risponde?
- Quali sono le sue criticità e come si sta evolvendo?
- Quali sono i principali casi d’uso?

Cos’è la Blockchain

Buzzword tecnologiche degli ultimi anni

Tra le tante, la Blockchain è una “buzzword” anomala:

Dobbiamo pensare alla blockchain come a qualcosa più simile a Internet

Una tecnologia che permette di scambiare “Asset” in maniera diretta, senza intermediari, in mutua fiducia tra le parti

Cos’è la Blockchain

Nuovo paradigma tecnologico

Un asset non viene più mantenuto da un’unica autorità centrale ma la conoscenza e il mantenimento sono **distribuite** globalmente

Una transazione permette di **registrare** una passaggio di asset, viene inviata da un nodo e viene ricevuta in pochi secondi da tutti gli altri nodi

Le transazioni vengono periodicamente memorizzate in un blocco e qui **cristallizzate**: una volta approvato il blocco diventano immutabili

I blocchi vengono approvati (minati) grazie al “**consenso**” della rete blockchain

Il consenso rappresenta la fiducia tra i sistemi distribuiti

- Problemi che sono stati studiati dagli anni ‘70 e ‘80
- Se alcuni nodi del mio sistema distribuito sono corrotti (Generali Bizantini traditori) io sono in grado, entro determinate ipotesi, di mantenere l'affidabilità e stabilità generale dell’intero sistema
- Si parla di problematiche di “consenso” tra nodi

L’obiettivo è arrivare ad un accordo sullo stato complessivo di un sistema, attraverso messaggi tra i diversi nodi che partecipano ad una rete

Esempio pratico

Cosa intendiamo con Blockchain

Un foglio di carta può memorizzare al massimo 25 transazioni

Quando il foglio è completo viene accettato da un gruppo di consenso ed aggiunto in coda ai “fogli” precedentemente inseriti

Un foglio inserito non può essere più modificato da nessuno perchè l’alterazione sarebbe immediatamente scoperta dagli altri

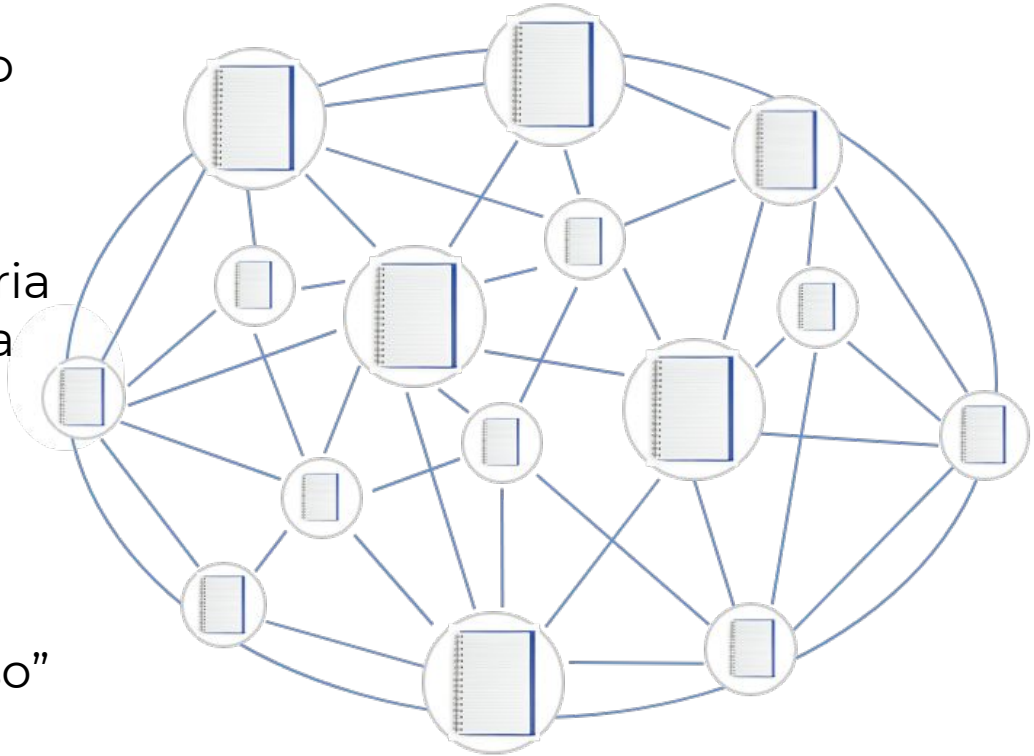
Esempio pratico

Cosa intendiamo con Blockchain

Tutti quanti hanno la copia dello stesso identico registro

Tutti quanti aggiornano la propria copia quando una nuova pagina “Blocco” viene condivisa

La condivisione di una nuova pagina avviene tramite le procedure definite dal “consenso”



Cos’è la Blockchain

L’aspetto filosofico dietro alla visione

Proviamo ad immaginare un mondo senza intermediari…

Abbiamo sempre avuto necessità di Autorità Centrali per fidarci gli uni con gli altri:

- Intermediari Finanziari (Bancari e Non Bancari)
- Intermediari Marittimi
- Intermediari Immobiliari
- Notai per la stipula di un contratto

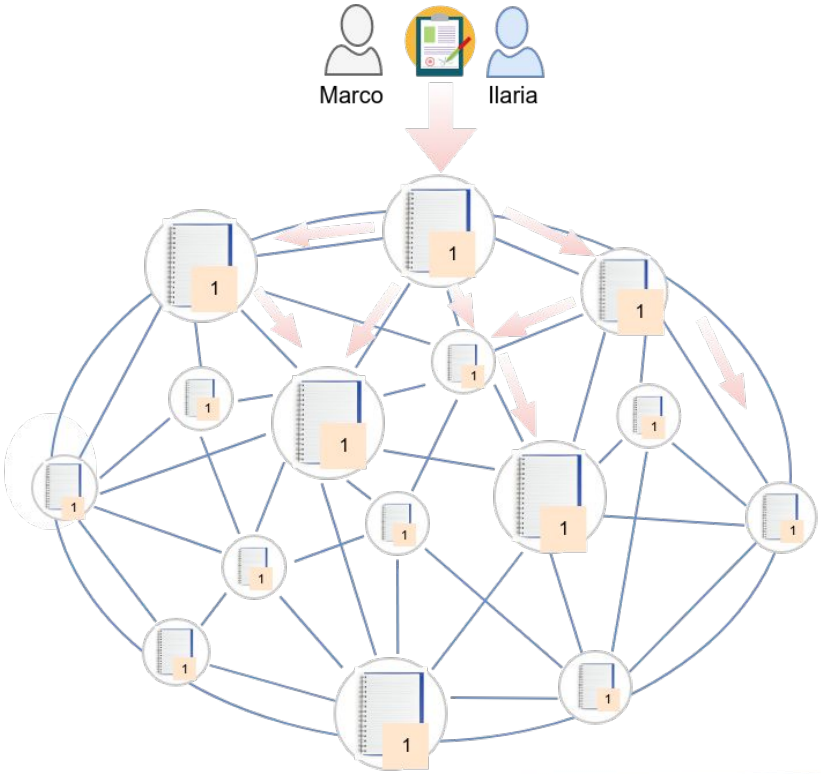
Esempio pratico

Cosa intendiamo con Blockchain

Marco e Ilaria raggiungono un accordo per uno scambio di un “bene”

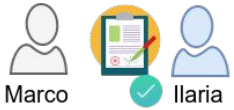
Firmano entrambi l’accordo e lo comunicano a tutti gli altri partecipanti della blockchain

L’accordo di diffonde nella rete e progressivamente tutti quanti vengono a conoscenza dell’accordo in cui Marco cede ad Ilaria uno specifico bene



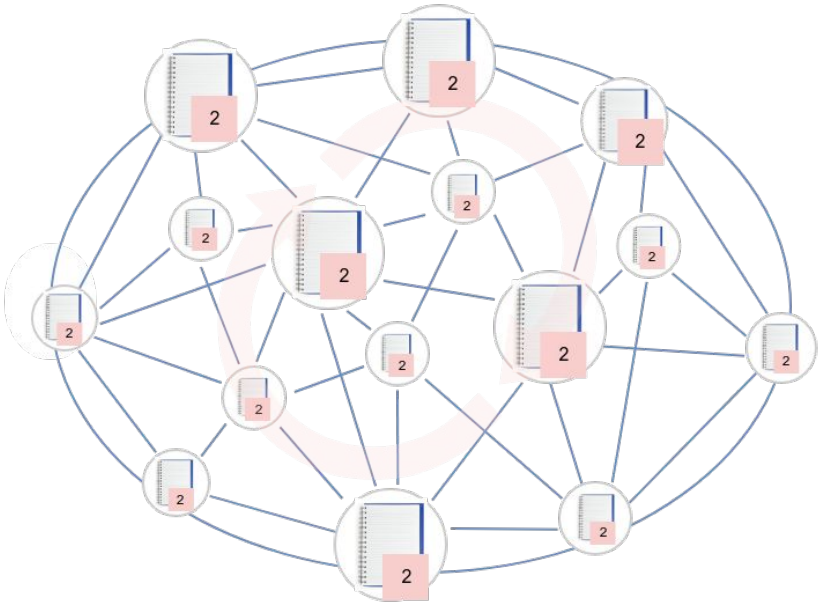
Esempio pratico

Cosa intendiamo con Blockchain



La rete blockchain attraverso il consenso approva una nuova pagina condivisa che viene aggiunta alle precedenti

Nella nuova pagina è registrato anche l'accordo tra Marco e Ilaria che a quel punto è scritto indelebilmente nella blockchain

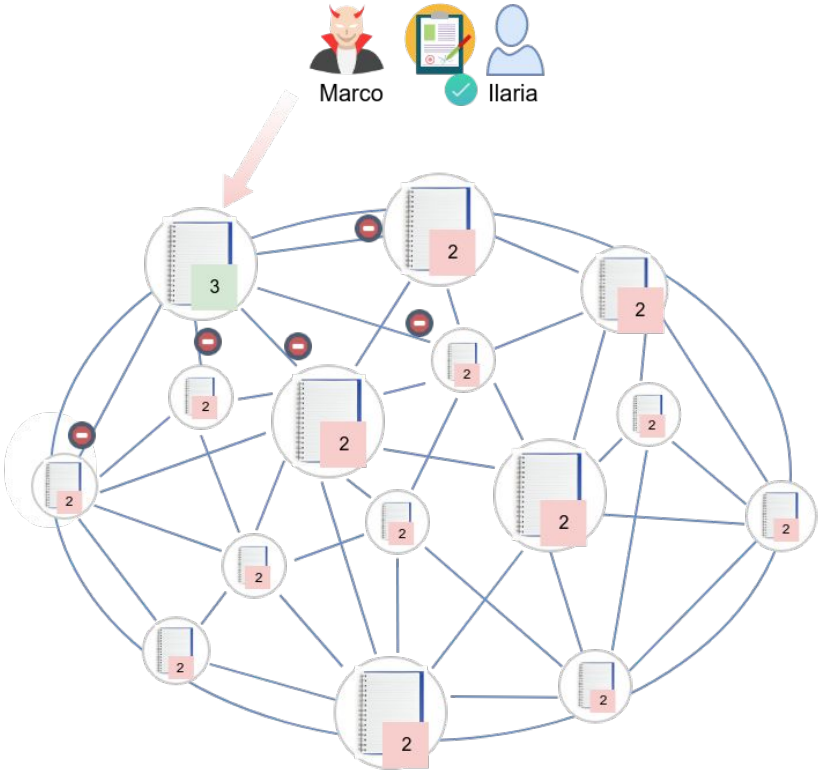


Esempio pratico

Cosa intendiamo con Blockchain

Se uno o più nodi “traditori”, modificando le proprie pagine, provassero a dichiarare che l’accordo non è mai avvenuto, dovrebbero vincere la resistenza della rete: **“Attacco del 51%.”**

Se Marco provasse a rivendere lo stesso bene già venduto ad una terza persona, la rete si accorgerebbe subito del tentativo di **“double spending”**



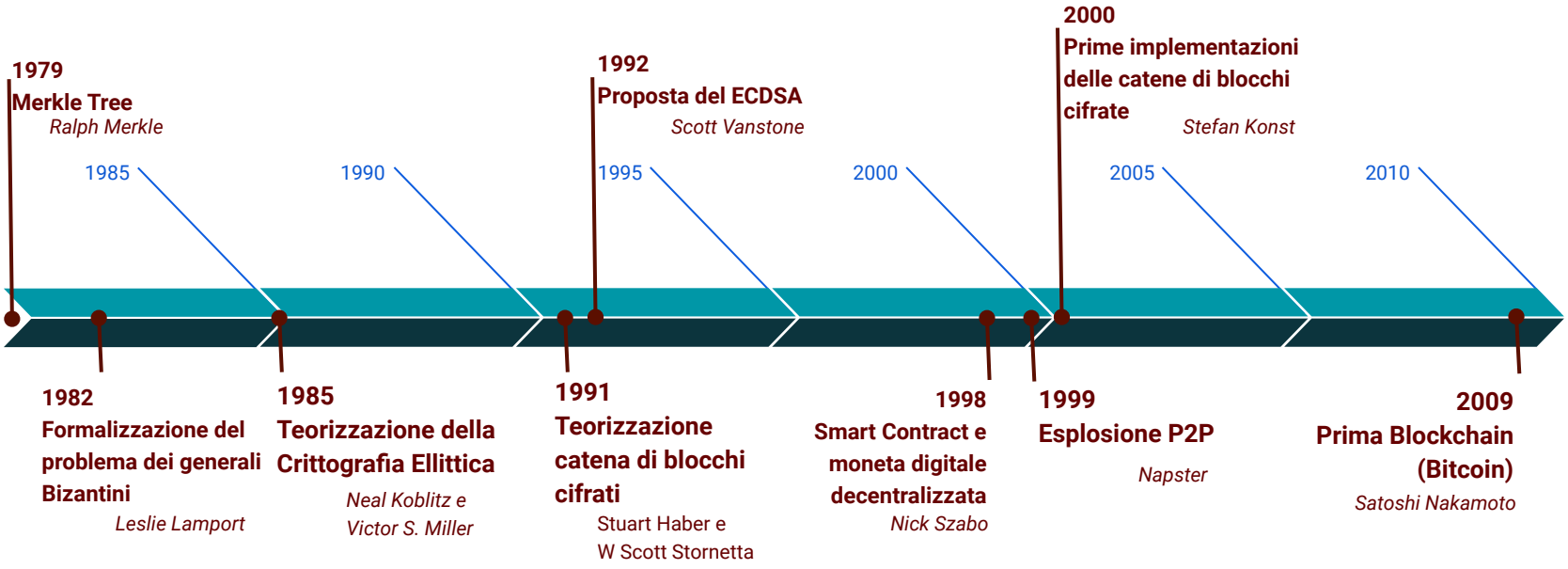
La Blockchain

Trend di sviluppo

Le origini della Blockchain

Evoluzione delle tecnologie abilitanti

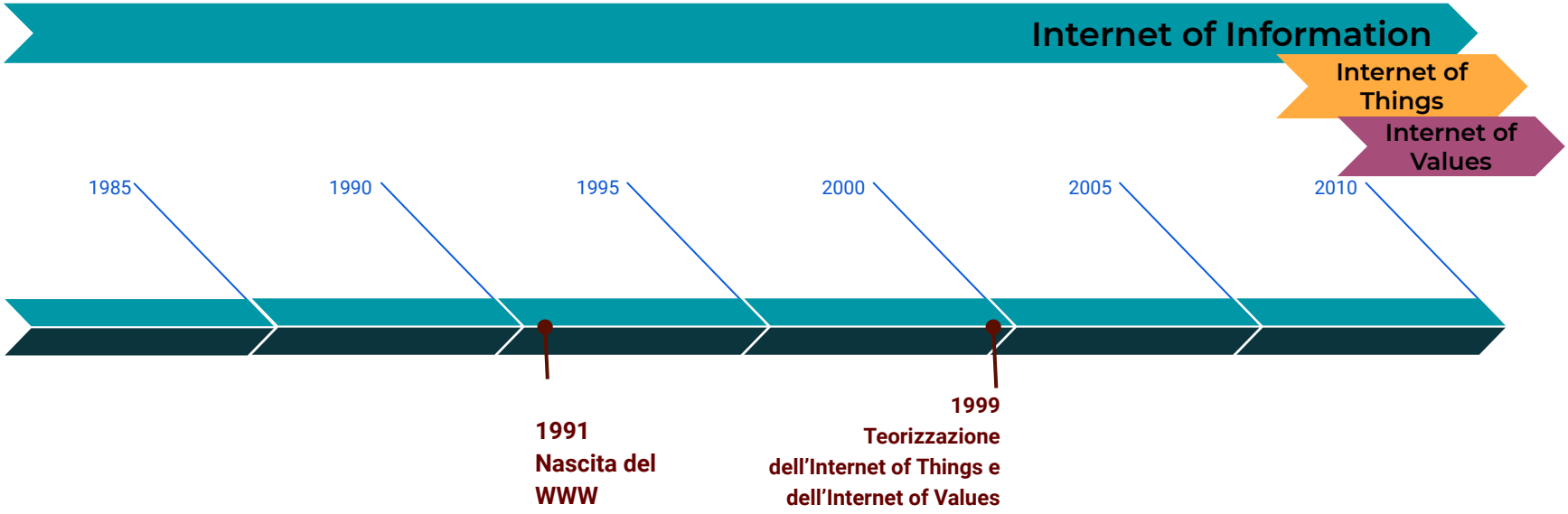
Le tecnologie di base sono state consolidate decenni prima rispetto alla nascita della prima blockchain



Le origini della Blockchain

L'evoluzione della stessa Internet

La blockchain ha cambiato l'utilizzo stesso di Internet:



La prima Blockchain

BITCOIN

Tutto funziona grazie ad una forma di consenso nota come *“Proof of Work”*

Accessibile e Pubblica: basata su Internet, chiunque può parteciparvi, non occorre nessun invito

Decentralizzata: funziona anche in presenza di tentativi di frode: non richiede di dare fiducia ai partecipanti

Anonima (o pseudo-anonima)

Sicura: garanzia del possesso e impossibilità di duplicarla

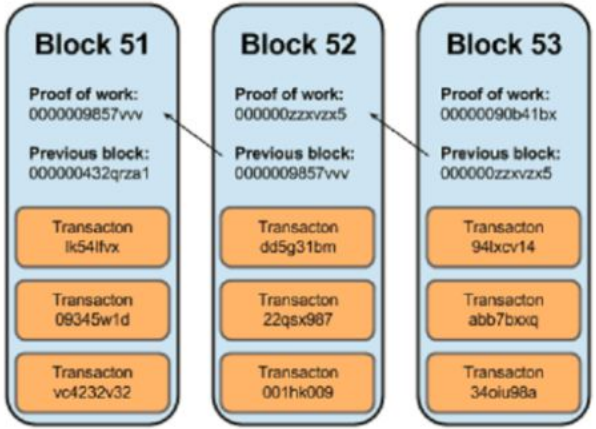
Equa: distribuita gradualmente e senza preferenze

Open Source: non potrebbe essere altrimenti

La Blockchain Bitcoin

Caratteristiche

- Le transazioni *validate* sono aggregate in blocchi (insiemi di transazioni, da poche a circa 2500)
- Nei BTC, si valida un nuovo blocco ogni circa 10 minuti
- Ogni blocco include anche l'*hash* del blocco precedente, e quindi i blocchi sono in una catena
- Una volta inserito un blocco nella BC, le transazioni contenute non sono più revocabili in alcun modo!



Il consenso PoW (Proof of Work)

Il ruolo dei minatori nella verifica delle transazioni

- Alla base dell'algoritmo di consenso PoW c'è l'assenza di fiducia tra i nodi della rete: configurazione "Trustless"
- Invece di eleggere un nodo come proponente e di coordinare i nodi restanti, il consenso è deciso in base al **nodo più veloce nel risolvere un problema** di computazione.
  Il nodo che arriva per primo alla soluzione del problema di calcolo è quello che determina lo stato successivo del sistema
- Questo tipo di consenso funziona dando per scontato che i nodi consumino (spendano) **capacità di calcolo per diventare i produttori** del blocco successivo, e premiando economicamente il nodo eletto generando nuova valuta
- **chiunque** può fare il *miner*

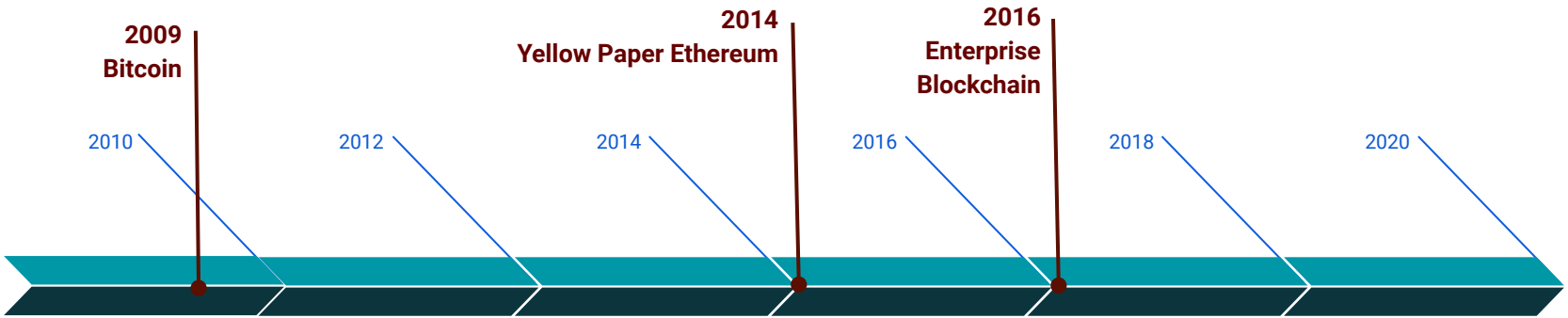
Una moderna mining farm

La rete dei miner Bitcoin è ad oggi più potente di un'ipotetica rete dei 500 supercomputer più potenti al mondo

La soluzione
«home-based»
è molto romantica
ma antieconomica

L'evoluzione delle Blockchain

Dove stiamo andando



Generazione 1.0

Pubbliche
Consenso Proof of Work

Generazione 2.0

Pubbliche e Permissioned
Smart Contract

Generazione 3.0

Interoperabilità tra BC
Scalabilità

COSMOS

EOS

Lightning network

RAIDEN

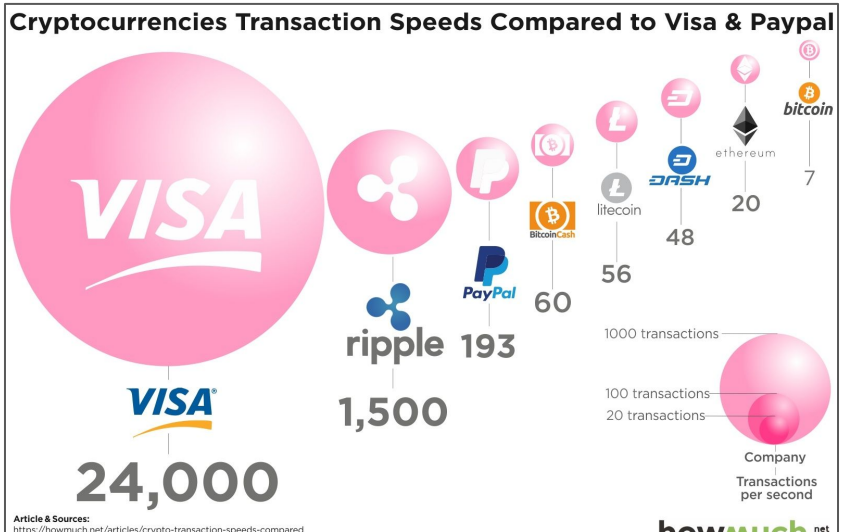
Blockchain 2.0

L’introduzione degli Smart Contract

- L’esecuzione di un programma software è deterministica e immutabile (a parità di input e di stato): il codice può essere considerato un contratto
- La blockchain ha capacità computazionali grazie all’introduzione nel 2015 degli **Smart Contract** nella blockchain Ethereum, colmando la lacuna di Bitcoin
- Uno Smart Contract è un programma che gira sui nodi della blockchain, ereditandone trasparenza e sicurezza; i contraenti si obbligano ad accettare il risultato delle sue elaborazioni
- Una volta che le clausole contrattuali sono inserite nel codice di uno Smart Contract, e questo è accettato dai contraenti, gli effetti non sono più legati alla loro volontà o all'azione di intermediari

Scrivere su blockchain pubblica comporta alcune problematiche:

- **lentezza** nell'approvazione delle transazioni
- **costi** di scrittura estremamente volatili
- complessità rispetto alle normative **GDPR**
- **visibilità** del dato
- gestione della **criptovaluta**
- **scalabilità** a lungo termine



Risposta ai molti problemi

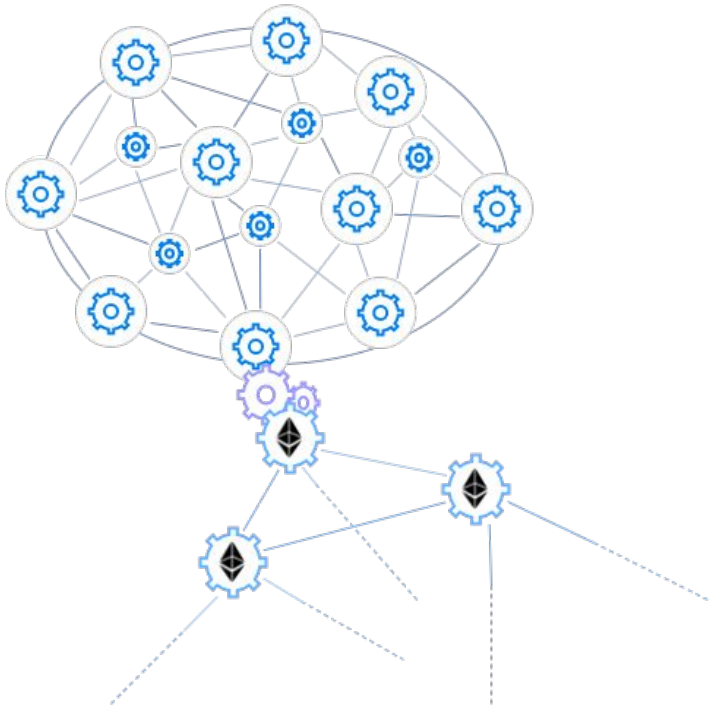
Decentralizzazione e SideChain

Poter gestire i propri asset e i propri processi in un contesto “amico”, certificando periodicamente la mia blockchain su una blockchain pubblica riconosciuta

- Limito i costi
- Non condivido dati sensibili
- Posso scrivere maggiori informazioni
- Ho una velocità di scrittura anche due ordini di grandezza più elevata
- Maggiore scalabilità
- Mantengo l’alta immutabilità della soluzione

Risposta ai molti problemi

Decentralizzazione e SideChain



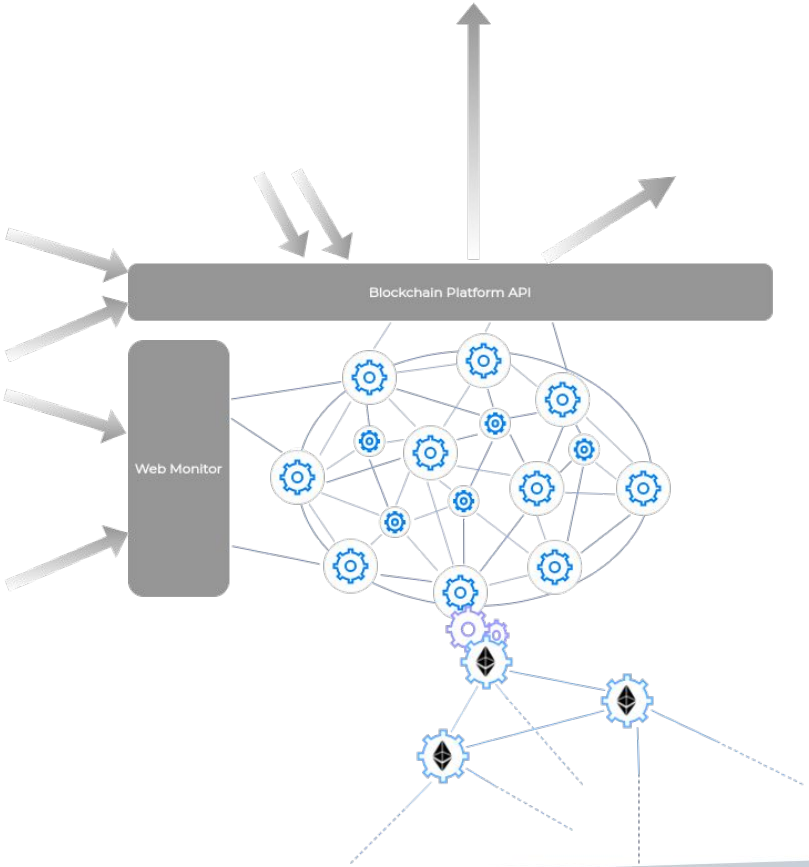
Certificare su una blockchain pubblica è essenziale per non insinuare il dubbio di “autoreferenzialità” ma dare prova della effettiva immutabilità della sidechain in un contesto pubblico

La certificazione periodica va a registrare informazioni non sensibili sulla blockchain pubblica: ad esempio l’impronta digitale dell’ultimo blocco generato

Si può rafforzare con una certificazione “a doppio binario” della blockchain pubblica nella sidechain

Blockchain “divide”

Accesso alla Blockchain As a Service



Semplificare l’accesso alla tecnologia blockchain attraverso servizi di alto livello:

- certificazione e notarizzazione
- registrazione avanzamento di un processo
- registrazione di voto

Visualizzare la blockchain attraverso dei “Web Explorer” senza alcuna competenza tecnologica

Pubblica o privata?

È possibile avere una «propria» blockchain

	PUBBLICA (Nessuna entità centrale)	**PRIVATA (Entità di controllo)**
Partecipanti	Senza Permessi • Anonimi • Possono essere maligni	Con Permessi • Identificati • Affidabili
Consenso	Proof of something • Ampio consumo energetico • Nessuna finalità predefinita • Attacco 51%	Voto o algoritmo di consenso «multi-nodo» • Leggero e veloce • Basso consumo energetico • Logiche di consenso personalizzabili
Frequenza transazioni	Bassa (10 min)	Alta (100 msec)
Vantaggi	Nessun intermediario Autogovernata	Riduzione dei costi di transazione (meno ridondanza e più trasparenza)
Costi	Criptovaluta per scrittura ed esecuzione smart contract	Risorse per il dispiegamento e la manutenzione della rete di nodi

Sintesi

Torniamo alla blockchain

- La blockchain è un **registro pubblico** di tutte le transazioni, reso immutabile usando la crittografia
- Non è soggetta a un'autorità centrale
- È replicata su tutti i nodi di una rete P2P, ed è un “database” cui si può solo aggiungere informazione, ma non cancellarla
- Riceve in continuazione nuove transazioni, validate tramite crittografia asimmetrica
- Gli utenti sono identificati da un «address», la cui chiave privata è posseduta solo dall’utente ed è sicura

Caratteristiche

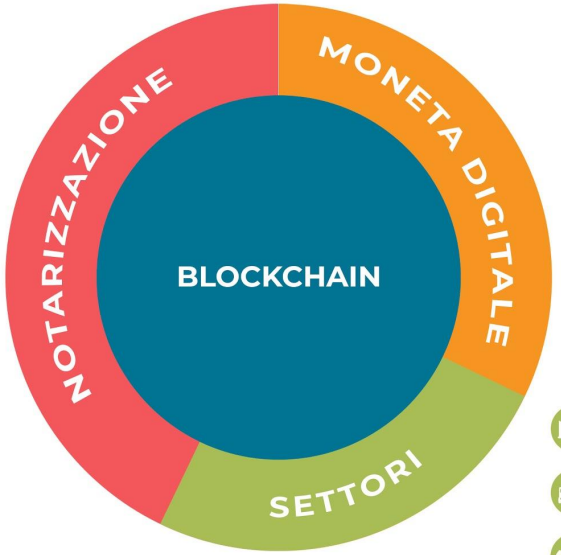
La «piattaforma blockchain»

Decentralizzazione	Le informazioni sono memorizzate su più nodi, dando resilienza e sicurezza
Tracciabilità	Tutte le transazioni sono tracciabili per ogni parte, e se ne può conoscere con certezza la provenienza
Disintermediazione	Le transazioni sono gestite senza intermediari e senza un'autorità centrale di gestione
Trasparenza	I contenuti sono accessibili e verificabili da tutti
Immutabilità	I dati accettati non sono più modificabili in alcun modo
Programmabilità	Si possono programmare azioni complesse (Smart Contract), anch'esse totalmente verificabili
Low-cost	Open source, poca manutenzione e costi di gestione bassi

La Blockchain

Applicazioni e Casi d’uso

Applicazioni della blockchain



- CERTIFICAZIONE DI PROPRIETÀ
- PROPRIETÀ INTELLETTUALE
- PROOF OF EXISTENCE
- CONTRATTI DIGITALI
- CERTIFICAZIONE DATI E DOCUMENTI
- VOTING
- IDENTITÀ DIGITALE
- FIRMA DIGITALE

- PAGAMENTI GLOBALI
- PRESTITI P2P
- CAMBIO VALUTA
- CROWDFUNDING
- MICROPRESTITI
- TRASFERIMENTI

- INDUSTRIA
- LOGISTICA
- FINANZIARIO E ASSICURATIVO
- AGRIFOOD
- HEALTHCARE
- UTILITIES
- COMMERCIO
- GOVERNANCE

Almacert

Certificazione dei diploma supplement

Voti e titoli accademici sono fondamentali per partecipare a concorsi e dimostrare il reale possesso dei titoli.

La soluzione **Almacert** sfrutta le potenzialità della blockchain nel processo di certificazione documentale (**B-Cert**), e garantisce:

- La titolarità dei documenti presentati
- La non alterazione o falsificazione dei documenti
- La data di reale acquisizione dei titoli
- La fruizione di documenti certificati digitalmente
- La disponibilità dei documenti certificati in ambito internazionale

Almacert

Certificazione dei diploma supplement

Obiettivi

- Attestare l'**autenticità del titolo di studio** sia per accreditare lo studente che ha ottenuto il titolo, sia per supportare l'istituto che è in grado di verificare e fornire prova di autenticità del titolo.
- Eliminare il problema di frodi e falsificazione dei titoli di studio, molto diffuso in Italia.

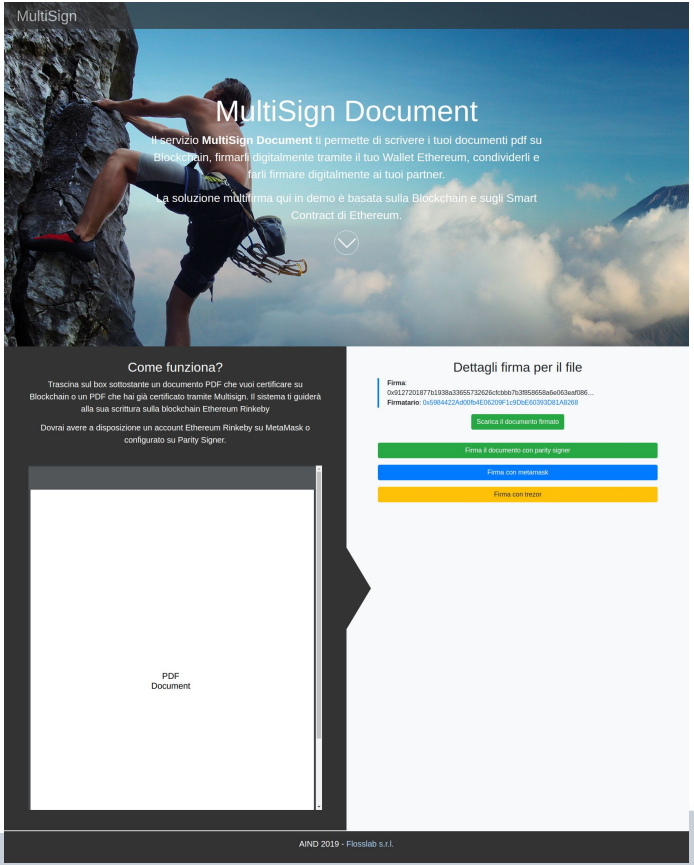
ALMACERT

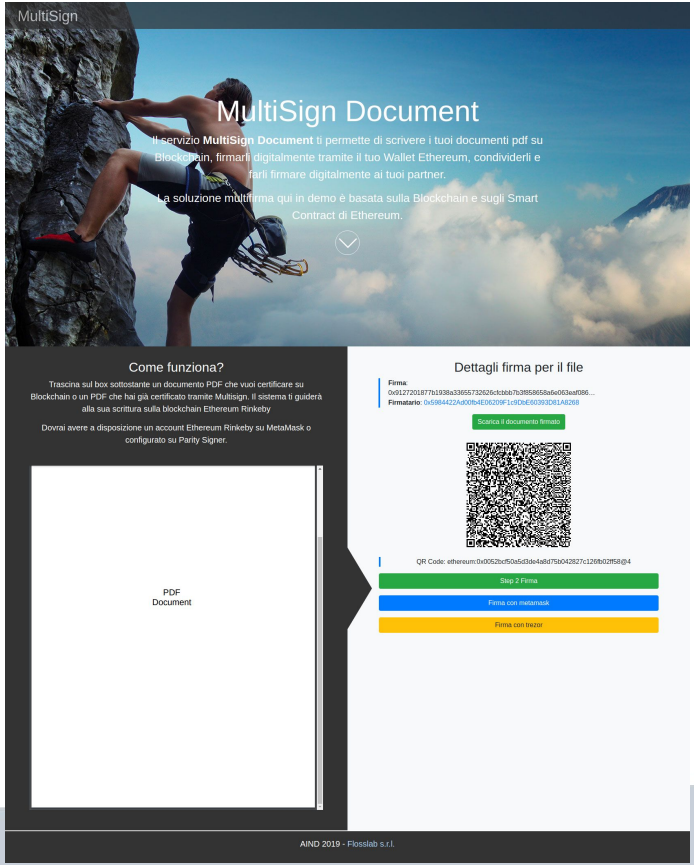
Principali Funzionalità

- Il **servizio di certificazione** permette di creare l'impronta digitale univoca, associarla al titolo di studio e di generare una transazione sulla BC in cui esiste la corrispondenza impronta digitale del diploma - matricola dello studente.
- Il **servizio di verifica** permette di verificare che il titolo di studio sia stato effettivamente creato dall'Address dell'istituto e che esista la corrispondenza impronta digitale del diploma-matricola dello studente.

B-Sign

Firma digitale multipla

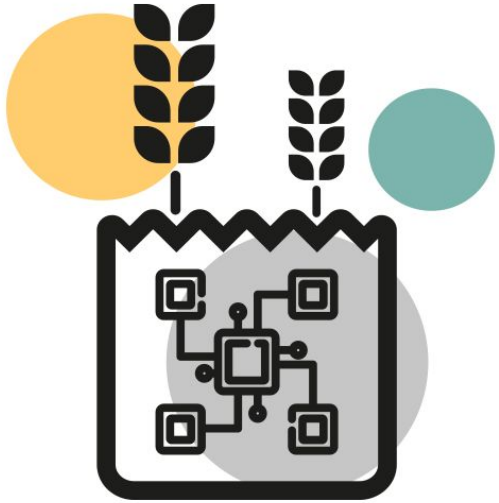




B-Supply

Certificare l’intera filiera agro-alimentare

Nel settore agroalimentare, la blockchain dà al consumatore finale la possibilità di risalire in modo semplice, automatico e garantito la filiera del prodotto acquistato.



- **TRASPARENZA**: Tutte le transazioni sono visibili. Più trasparenza significa anche più fiducia da parte del consumatore (si riduce o elimina la possibilità di frodare su provenienza, qualità, trattamenti, quantità prodotte).
- **ROBUSTEZZA E DECENTRALIZZAZIONE**: Poiché i dati sono distribuiti, non ci sono singoli punti di fallimento.
- **IMMUTABILITÀ**: Le transazioni non possono essere manomesse, ma solo corrette con registrazioni successive.

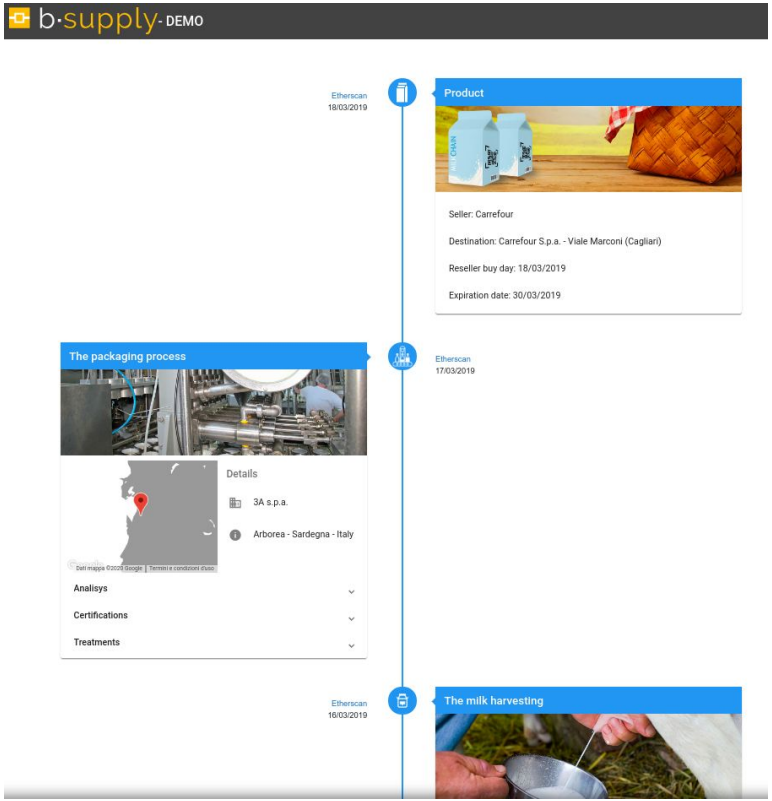
B-Supply

Supply chain nel settore agro-alimentare

- documentazione trasparente e irreversibile di **ogni evento** rilevante per la produzione
- **asseverazione delle produzioni**, da parte di autorità, laboratori e periti certificati dando prova della loro identità e delle loro certificazioni
- integrazioni di registrazioni automatiche eseguite da dispositivi IoT (**Internet of Things**) che sono sempre più diffusi
- **tracciabilità delle quantità prodotte**, in modo che queste non possano essere aumentate introducendo prodotti di origine non certificata
- evidenza di tutti i passi della produzione alle autorità preposte alla **verifica dei disciplinari**
- **conoscenza della storia dei prodotti** per rivenditori e consumatori finali, dal campo sino alla confezione acquistata

B-Supply

Cosa vede l'utente finale



- Tramite un semplicissimo QR-Code messo nel prodotto, il cliente potrà leggere l'intera storia del prodotto che ha comprato
- Il cliente avrà una vista semplice ed immediata ma anche la possibilità di andare attraverso dei link direttamente su un Blockchain Web Explorer o sulla Blockchain stessa

B-Voting

Nasce come progetto di Ricerca

B-Voting è l'innovativo sistema di voto elettronico integrato sviluppato in collaborazione con il Dipartimento di Matematica e Informatica (DMI) dell'Università degli Studi di Cagliari.

I requisiti essenziali che devono essere soddisfatti da un sistema di voto digitale per un uso efficace in voto elettivo:

- ✅ Non consentire la tracciabilità di un voto di un elettore identificandone le credenziali
- ✅ Garantire e dimostrare a un elettore che il suo voto è stato eseguito e correttamente conteggiato
- ✅ Non consentire a un terzo di manomettere un voto.
- ✅ Non abilitare una singola entità al controllo dei voti e quindi rendere impossibile determinare il risultato delle elezioni
- ✅ Consentire solo a individui idonei di votare per un'elezione
- ✅ Scongiurare il voto coatto

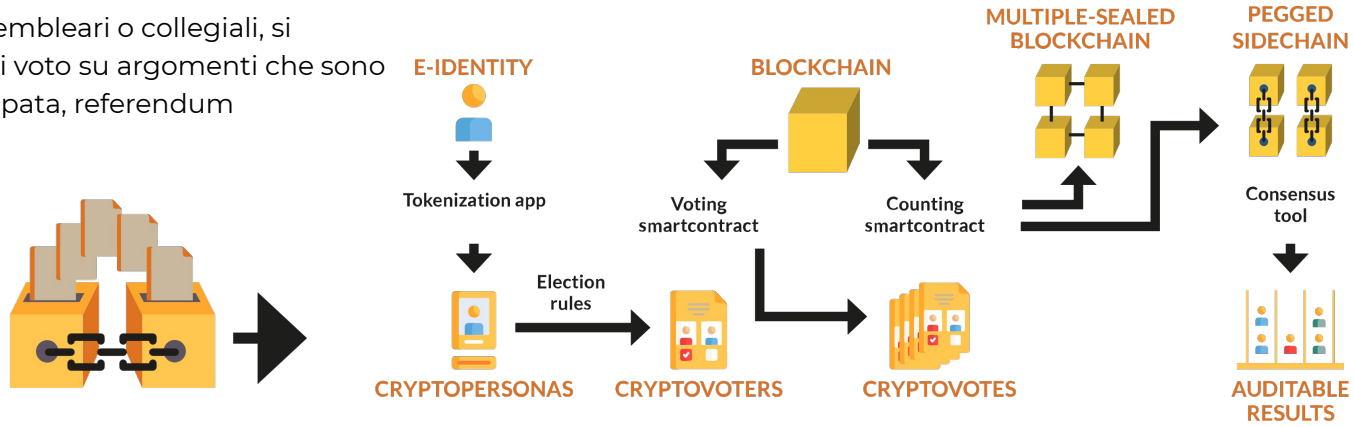
B-Voting

Il voto si distingue nelle seguenti tipologie:

- **Votazioni statutarie**: votazioni previste e regolamentate dallo statuto di associazioni e organizzazioni in genere (rinnovo organi sociali, approvazione del bilancio, etc.)
- **Bilancio partecipativo**: votazioni di progetti e bilanci della pubblica amministrazione che coinvolgono la cittadinanza, sono di tipo consultivo o referendario
- **Votazioni elettive**: esigenze di scelta di uno o più candidati per una determinata carica, votati singolarmente oppure raggruppati in liste
- **Votazioni referendarie**: assembleari o collegiali, si organizzano per necessità di voto su argomenti che sono oggetto di decisione partecipata, referendum

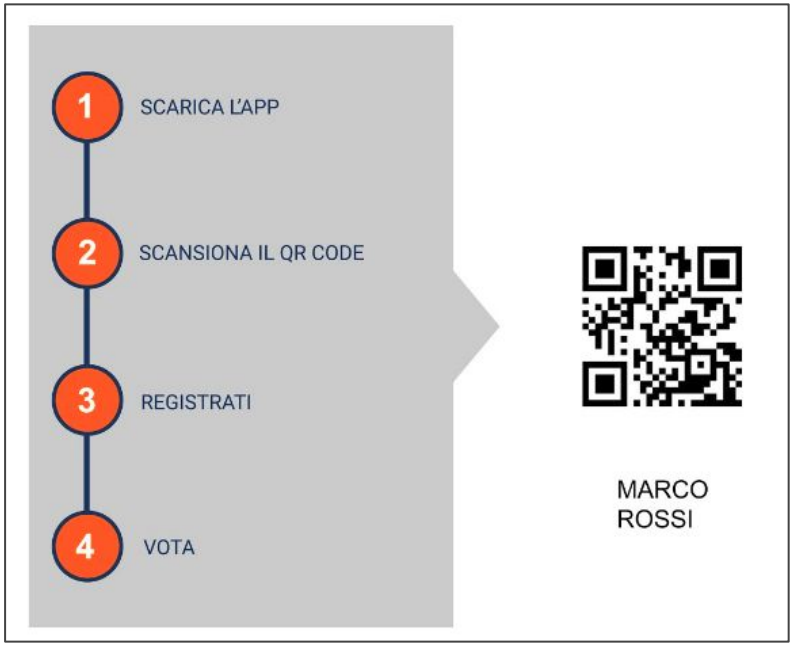
Il sistema gestisce operativamente 3 fasi ben distinte del processo:

- ✔ Attività propedeutiche e formazione delle liste elettorali
- ✔ Gestione della votazione
- ✔ Conteggio dei voti



B-Voting

Caso pratico



Ulteriori casi d'uso

Azienda specializzata in sistemi di telecontrollo

POSSIBILI USE CASE

- Registrare e certificare su Blockchain tracciati sensibili delle flotte aziendali
- Registrare e certificare su Blockchain l'attivazione, la disattivazione, gli allarmi provenienti da sensori ad elevato livello di sicurezza
- Utilizzo degli smart contract per censire e notarizzare l'associazione dispositivo-autoveicolo
- Registrare e certificare su Blockchain eventuali sigilli digitali delle scatole nere

VANTAGGI

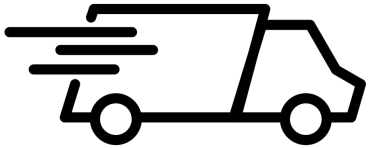
- ➔ produrre una certificazione esterna dell'informazione registrata
- ➔ imporre l'inviolabilità ex-post dei dati registrati
- ➔ trasparenza delle informazioni
- ➔ dare una visibilità in termini di marketing, vista l'attuale assenza di soluzioni simili sul mercato

Ulteriori casi d'uso

Azienda di spedizioni e servizi logistici

POSSIBILI USE CASE

- Certificare su blockchain e smart contract le prove di consegna ai clienti
- Realizzare servizi di tracciatura dei prodotti per le G.D.O. per rendere possibile seguire la storia dei prodotti dall'origine al consumatore, integrando sulla blockchain le modalità di trasporto delle merci e le temperature di mantenimento
- Offrire il tracciamento delle spedizioni critiche per i propri clienti, attraverso scritture immutabili su blockchain pubbliche



VANTAGGI

➔ produrre un tracking esterno dell'informazione registrata
➔ imporre l'inviolabilità ex-post dei dati registrati
➔ trasparenza delle informazioni

La Blockchain

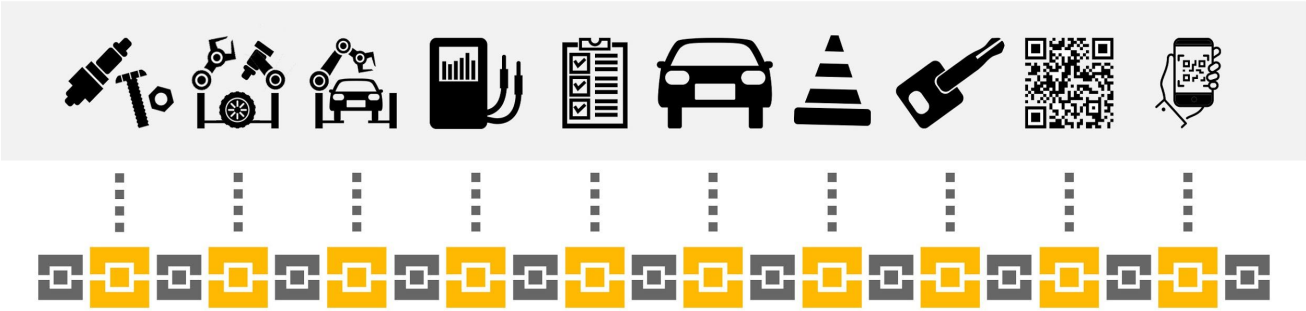
Casi d’uso
per l’industria meccanica

B-Supply

Certificazione processi produzione

Certificare in maniera immutabile il ciclo di approvvigionamento e assemblaggio attraverso la blockchain:

- Registrare su blockchain l'ingresso in magazzino dei lotti da assemblare, tracciando data di ingresso, fornitore, numero pezzi
- Registrare su blockchain tutti gli step del processo di assemblaggio, scrivendo date di avanzamento, pezzi e relativi lotti utilizzati per la produzione
- Tracciare le attività di certificazione di prodotto e di processo tramite sigilli su blockchain
- Registrare le attività di verifica e collaudo
- Produrre un QR-code per ricostruire sulla blockchain l'intera storia dell'assemblato



Spazio alle vostre idee e alle vostre domande

netservice
Information Technology

www.netservice.eu

info@netserv.it

+39 051 624 1989

flosslab
Innovation at Work

www.flosslab.com

info@flosslab.com

+39 070 7512011