Digitalizzazione, smart contract e sistemi di registrazione di transazioni in Internet

Dai sistemi centralizzati alla Blockchain

Nicola Mazzocca

Professore di Sistemi di Elaborazione

Università di Napoli Federico II

Cosa si intende per transazione

- Nella teoria delle basi di dati, il termine **transazione** indica una qualunque sequenza di operazioni lecite che, se eseguita in modo corretto, produce una variazione nello stato di una base di dati.
- Il **contratto** è l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale.
- Nell'ordinamento civile italiano la **transazione** è il **contratto** con il quale le parti, facendosi reciproche concessioni, pongono fine ad una lite già incominciata o prevengono una lite che potrà sorgere tra di loro. Tale nozione è accolta dal codice civile all'art. 1965.
- Nel linguaggio tecnico-economico, operazione commerciale, per lo più con riferimento alla compravendita.

Transazioni nei sistemi distribuiti

Elementi essenziali delle transazioni

- Tracciabilità
- Imputabilità, attraverso l'identità digitale di soggetti e oggetti, realizzata mediante token
- Immutabilità
- Certezza temporale
- **ACID** deriva dall'acronimo inglese **Atomicity**, **Consistency**, **Isolation**, e **Durability** (Atomicità, Coerenza, Isolamento e Durabilità)

Gestione delle transazioni

- Gestione delle registrazioni delle transazioni:
  - Centralizzato o distribuito
  - Responsabilità di uno o più enti (eventualmente con funzioni e poteri diversi)
  - Intermediazione e imparzialità
- Gestione automatica delle attività previste da contratti che richiedono di effettuare più transazioni in relazione al verificarsi di specifici eventi.
- Interoperabilità tra sistemi intergenti mediante scambio di informazioni.

Aspetto normativo

- Norme di diverso rango definiscono le modalità per il trattamento delle informazioni (transazioni) nei sistemi digitali.
  - Tali norme tengono conto dell'ordinamento giuridico (Civil Law e Common Law)
- Le informazioni (transazioni) contenute in Registri Pubblici devono essere conservati e aggiornati in relazione alle norme previste, che ne definiscono in modo rigoroso l'intero ciclo di vita.
- I rapporti tra le parti avvengono attraverso lo scambio di attività che sono regolamentate in termini di principi generali, mentre le specifiche attività e accordi sono lasciate alla libera iniziativa dei singoli.

Metodologie e tecnologie informatiche

- Criptografia e sistemi hardware di calcolo
- Basi di dati e sistemi di memorizzazione veloci
- Reti e protocolli
- Servizi abilitanti:
  - Firma digitale
  - Protocollo informatico
  - Conservazione
  - Blockchain

Sistemi per la gestione di registrazione distribuiti

Sistemi di registrazione di transazioni che non necessitano di intermediazione, totalmente aperti o limitati a gruppi qualificati.

- Blockchain senza permesso
- Blockchain con permesso

Introduzione a Blockchain

Cos’è Blockchain

- «Un registro digitale le cui voci sono raggruppate in blocchi, concatenati in ordine cronologico, e la cui integrità è garantita dall’uso della criptografia.» Wikipedia.org

- È un sistema **distribuito** in cui è possibile memorizzare in maniera **permanente** qualsiasi tipo di elemento, senza la necessità di un’autorità centrale fidata.

  - Ogni nodo della rete attraverso cui è implementata possiede una copia locale del registro.

  - È possibile aggiungere blocchi di elementi al sistema. Una volta aggiunto un blocco non è possibile modificarlo o eliminarlo.

Caratteristiche principali

- Introdotta nel 2008 da un “anonimo” noto come *Satoshi Nakamoto*
- Ogni cambiamento di stato deve essere verificato dai tutti i nodi
- Assicura la trasparenza
- L’integrità è garantita attraverso la verifica dei nodi mediante applicazione di tecniche crittografiche.
- La ridondanza è assicurata replicando il sistema trai diversi nodi
- È necessario valutare le problematiche di identificazione, anonimato e privacy

Origini di Blockchain

- Esistono diverse piattaforme che operano secondo il modello della Blockchain: Bitcoin, Ethereum, Corda, Hyperledger.
- Ha avuto il ruolo di libro mastro (*ledger*) nella note criptovaluta *Bitcoin.*
- ATTENZIONE: Blockchain ≠ Bitcoin
  - Bitcoin, come le altre criptovalute, è un'applicazione basata su Blockchain.
  - Blockchain non richiede una criptovaluta per poter essere applicata.

Blockchain senza permesso

Blockchain senza permesso

- Una Blockchain senza permesso *(permissionless)* è una particolare Blockchain accessibile da chiunque.
  - Qualsiasi nodo può entrare e lasciare la rete in qualunque momento.
- Esempio: Bitcoin

Bitcoin

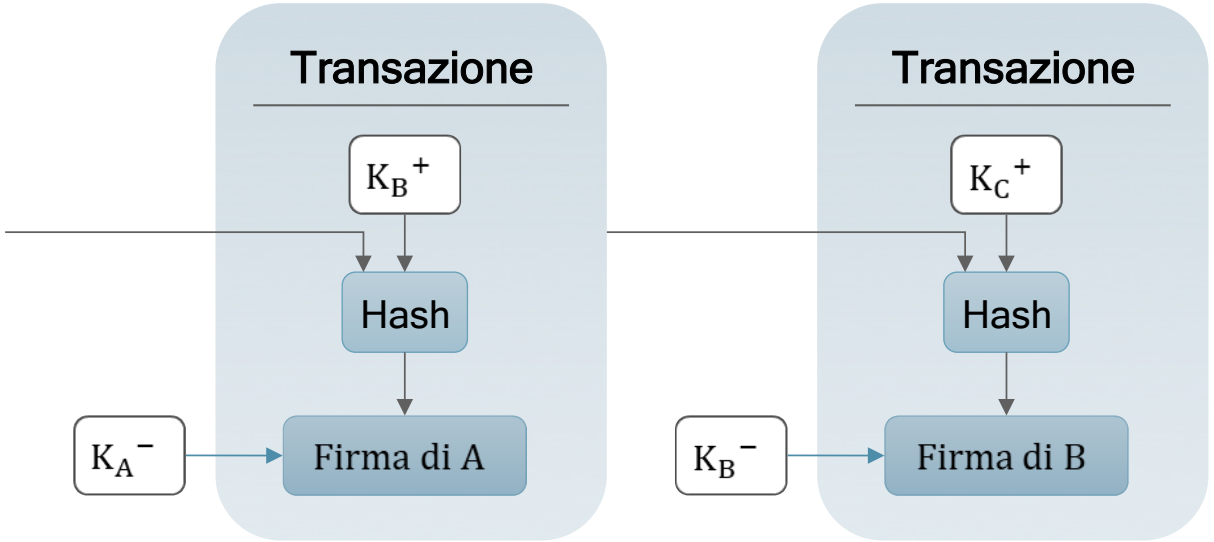
- È una valuta digitale decentralizzata in cui lo scambio di moneta avviene attraverso una rete *peer-to-peer* (p2p), senza il coinvolgimento di istituzioni finanziare.
- Le transazioni sono verificate attraverso criptografia da particolari nodi della rete, detti **miners**.
  - Il processo di validazione prende il nome di **bitcoin mining**.
- Le transazioni validate vengono registrare all'interno di una Blockchain pubblica, condivisa tra tutti i nodi.
  - L'utilizzo di una Blockchain risolve il problema del *double spending.*

Bitcoin Wallet

- Ogni utente della rete possiede un portafoglio digitale *(bitcoin wallet),* a cui sono associati due elementi:
  - Una **chiave pubblica** K_A^+, detta *indirizzo bitcoin,* costituita da un codice alfanumerico di 34 caratteri e utilizzata per inviare e ricevere pagamenti.
  - Una **chiave privata** K_A^-, necessaria per provare l'identità di ogni utente coinvolto in una transazione, secondo un meccanismo noto come *firma crittografica.*
- In questo modo si realizzano meccanismi di identificazione anonima.

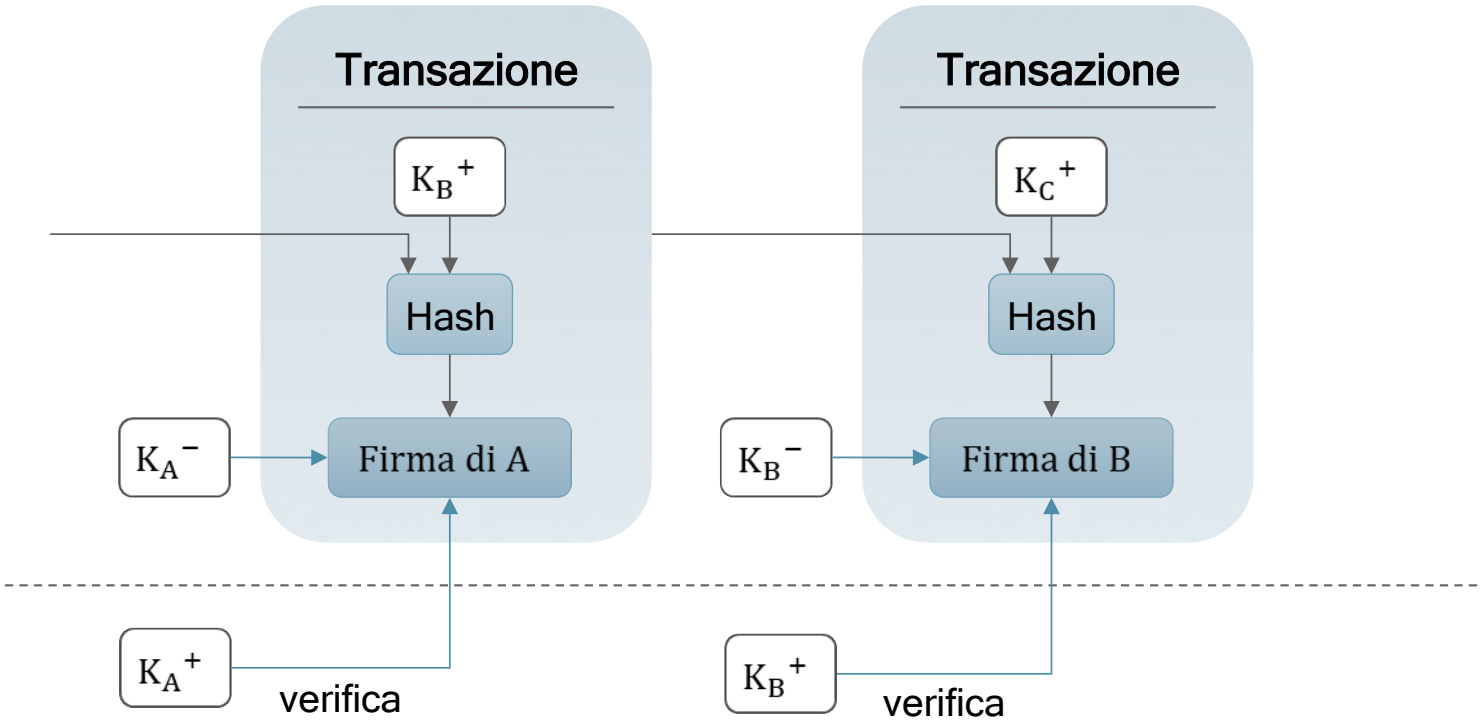
Transazioni (1/3)

- Un utente firma digitalmente, attraverso la propria chiave privata K_A^-, l'hash della transazione precedente e della chiave pubblica K_B^+ del destinatario.



Transazioni (2/3)

- Il destinatario può verificare la validità della firma attraverso la chiave pubblica del mittente K_A^+.



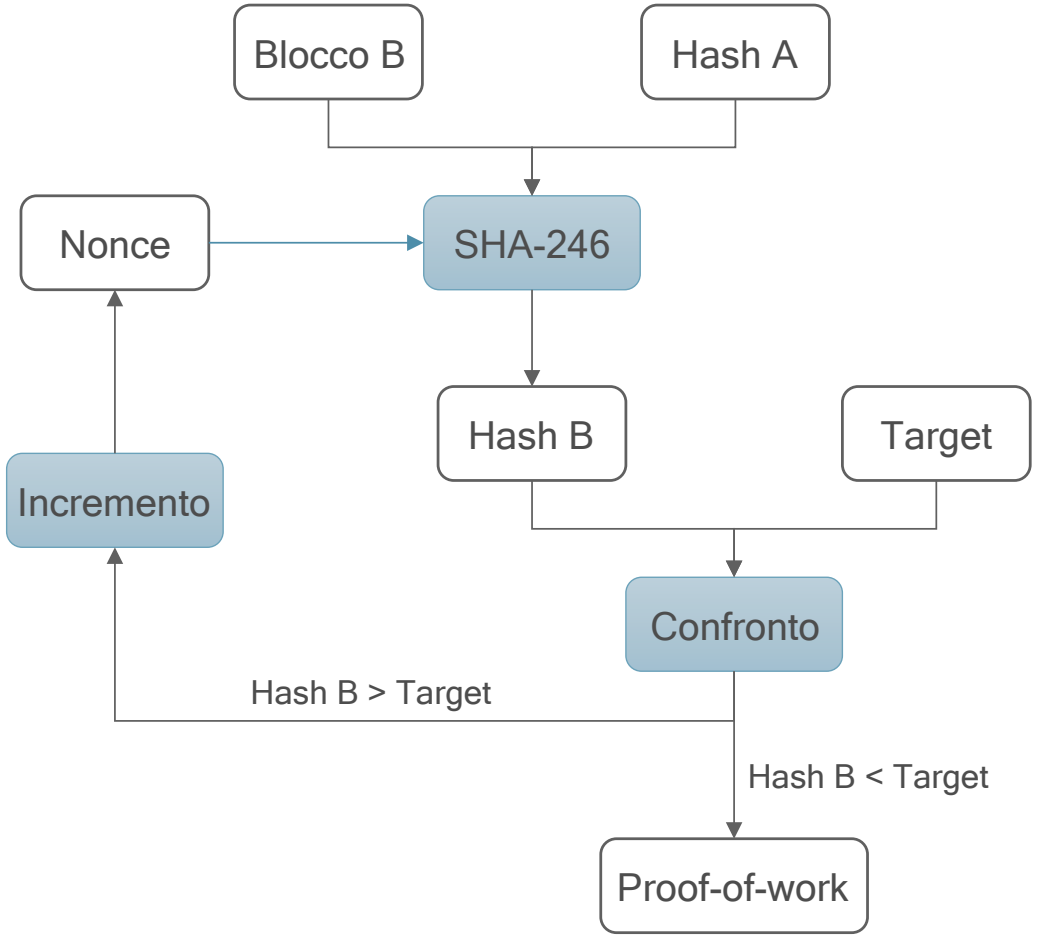
Transazioni (3/3)

- È possibile inserire all'interno delle transazioni una quantità limitata di logica applicativa, mediante opportuni **script.**
- In questo modo è possibile introdurre semplici condizioni di abilitazione delle transazioni.
  - Esempio: invio di bitcoin da un utente all'altro, abilitando il ricevente a spenderli esclusivamente in un determinato modo.

Bitcoin Mining (1/3)

- Le transazione ricevute dai miners sono riunite in blocchi.
- Ad ogni blocco viene applicato un algoritmo di hash, noto come **SHA-256**, tenendo conto del valore hash del blocco precedente.
  - Il processo si ripete incrementando un certo numero, detto *nonce,* fino a quando il valore hash risultante non diventa inferiore ad un determinato valore, detto *target value.*
  - Il valore del target value viene modificato dalla rete stessa, in modo da aumentare o ridurre la difficoltà del problema. In questo modo è possibile rendere tempo di mining costante e pari a circa 10 minuti.

Bitcoin Mining (2/3)



Bitcoin Mining (3/3)

- Il processo di mining richiede un elevato dispendio di potenza di calcolo e risorse energetiche.
  - Possibile soluzione: Hardware dedicato (AISIC)
  - Evoluzione: *Approximate computing*
- Sono previsti alcuni **incentivi** per indurre i miners a contribuire allo sviluppo della rete.
  - Per convenzione, la prima transazione di un blocco aggiunge moneta al creatore stesso del blocco.
  - È richiesto al mittente di una transazione il pagamento di una commissione, detta *transaction fee.*

Blocco

Blocco

Hash: 00f261e4bc80d8eb9b0db...

Previous: 00143f3bade113fb08...

Time: 2019-09-05 14:57:31

Transasioni:

08192caf5e39a692157277c...
429fc65e43ddd9e1b25fc46b...
F1b3885c4be1ae95a2c2aea...
95655198e5ff9cc0f157ff1b0..
5d178cc1ca62dfc05419c9a7...

Fasi della catena

Transazione	Creazione del blocco	Verifica del blocco	Ricerca del consenso	Inserimento del blocco nella catena
• Viene eseguita una transazione da un utente della rete.	• I miners raccolgono diverse transazioni in un unico blocco.	• I miners ricercano il valore hash del blocco applicando l'algoritmo di criptografia.	• Una volta determinato il valore hash viene trasmesso a tutti i nodi della rete che ne verificano la validità.	• Il nuovo blocco viene aggiunto in modo permanente alla catena.

Blockchain con permesso

Blockchain con permesso

- Una Blockchain con permesso *(permissioned)* è una particolare Blockchain il cui l'accesso in scrittura e/o in lettura è controllato.
  - In questo modo determinate operazioni sono consentite esclusivamente a nodi qualificati.
  - Possono essere utilizzate diverse strategie per validare i blocchi
  - I nodi della rete possono avere diverse funzioni finalizzate alla gestione della Blockchain
- In modo molto schematico è possibile distinguere:
  - Blockchain che utilizzano come infrastruttura di base una piattaforma simile a quella della Blockchain di Bitcoin.
  - Blockchain che prevedono la presenza di una sorta di *entità* in grado di attribuire a ciascun nodo della rete il diritto di eseguire o meno determinate operazioni.

Smart Contract

Smart Contract

- Rappresenta un accordo fra due parti trascritto in software in modo da automatizzare le azioni da intraprendere in funzione degli eventi previsti dal contratto.

  “un protocollo di transizione svolto da un computer che esegue i termini di un contratto” (Szabo-1994)

- Quando si parla di smart contract vanno considerati tre aspetti:

  - Quello operazionale che riguarda la tecnologia software da utilizzare e da eseguire, non necessariamente su un *ledger* distribuito, per rispettare le obbligazioni previste dal contratto;

  - Quello legale che si concentra su come definire l'accordo fra le parti e come implementarlo in software;

  - La manutenibilità rispetto alle condizioni negoziate per garantire l’aderenza del software con l’accordo legale definito;

Funzionamento Smart Contract

- Quando si verifica un evento il contratto viene invocato ed aggiorna il suo stato in base alle azioni previste dall'accordo, ad esempio cambiare il proprietario di un bene in corrispondenza di un evento di pagamento.

```
invocaContratto(evento e){
    stato_attuale = leggiStato();
    s = cambiaStatoContratto(stato_attuale,e);
    salvaStato(s);
}
```

Modello con Smart Contract

- In questo modello è presente un database contenente oggetti *statefull*.
- Il salvataggio delle transazioni provoca l'invocazione di smart contracts, i quali si occupano di aggiornare lo stato degli oggetti in funzione del servizio offerto.

Modello con Smart Contract e Blockchain

- Nei casi precedenti il gestore dei servizi deve certificare la validità delle operazioni che avvengono nel sistema.

- Il registro delle transazioni viene sostituito con una blockchain che permette di:

  - Eliminare la terza parte che si occupa di validare le operazioni;

  - Avere soggetti indipendenti, ognuno ha la sua copia del registro;

  - Autenticare in modo non centralizzato in quanto le operazioni avvengono nel registro locale;

  - Gestire la riservatezza in quanto gli utenti espongono solo le informazioni necessarie alla validazione;

Hyperledger Fabric

- È un distributed ledger che supporta la definizione di smart contracts.
- Ciascuno dei nodi che fanno parte della rete contengono una copia del ledger e sono chiamati *peer*.
- Il consenso fra i peers sulle transazioni da aggiungere è ottenuto grazie a dei nodi *orderer* che si occupano di fornire il servizio di ordering.

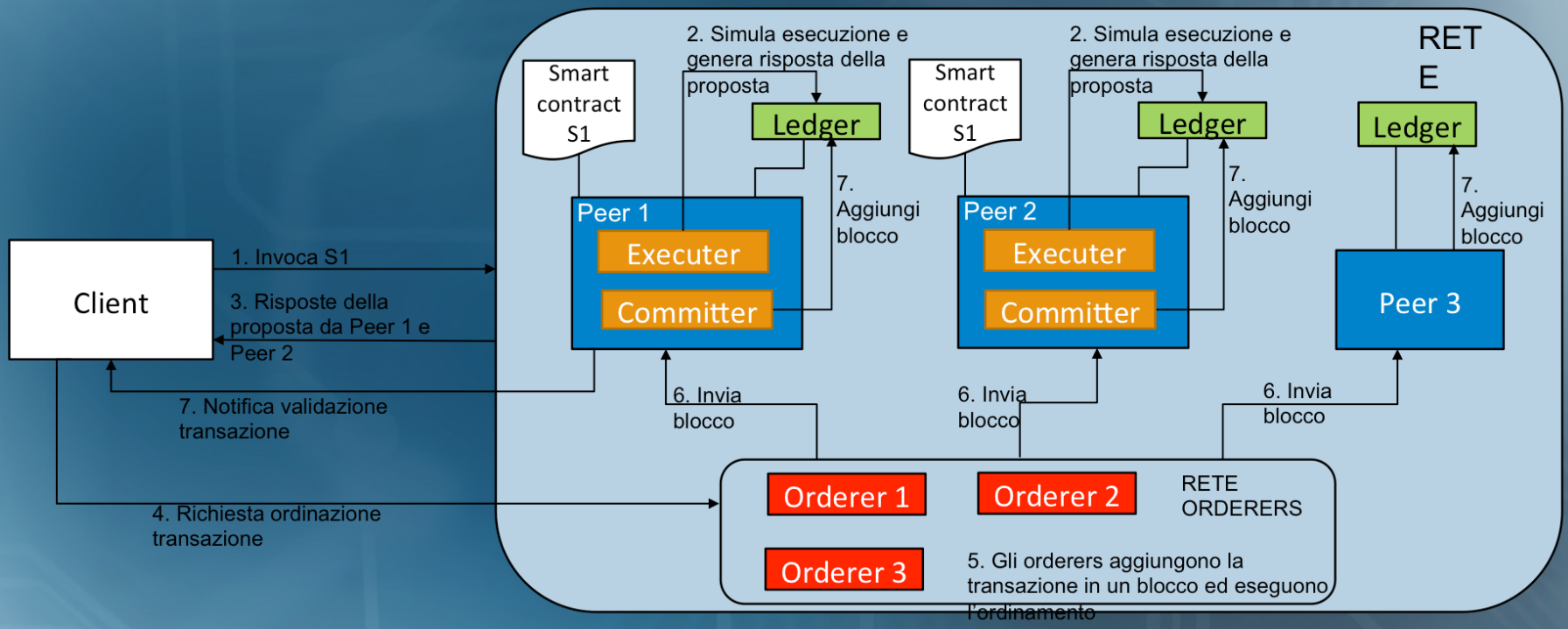
Smart Contract in Hyperledger Fabric

- Un ledger è composto da due elementi:
  - Un *World State* ovvero un database che contiene i valori correnti di un insieme di oggetti, che formano lo stato del ledger. Questi oggetti sono espressi sotto forma di coppia chiave-valore;
  - Una *Blockchain* le cui transazioni tengono traccia di tutti i cambiamenti avvenuti nel world state.
- Gli smart contracts risiedono nei peers e forniscono i metodi per gestire il ciclo di vita degli oggetti contenuti nel world state.

Smart Contract in Hyperledger Fabric

- Un contratto, che viene invocato contattando il peer in cui risiede, effettua una simulazione di esecuzione senza aggiornare il ledger e restituisce una risposta riguardo la proposta.
- Per rendere effettivi i cambiamenti la transazione deve essere inviata agli orderers che la inseriscono in un blocco da inviare ai peers per l'aggiornamento del ledger.

Smart Contract in Hyperledger Fabric



Conclusioni

La realizzazione del sistema ottimale nasce dallo studio di architetture diverse da realizzare tenendo conto dei vincoli di contesto.

Abbiamo molti strumenti da utilizzare e configurare in modo opportuno.

Un nuovo spazio di ricerca e operativo molto interessante si apre per le sue implicazioni tecniche, giuridiche e economiche

Alcuni Riferimenti

1. Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System.* (2008). https://whycryptocurrencies.com/files/bitcoin.pdf
2. Josh Stark: *Making Sense of Blockchain Smart Contracts.* (2016) https://www.coindesk.com/making-sense-smart-contracts
3. Christopher D. Clack, Vikram A. Bakshi, Lee Braine: *Smart Contract Templates: foundations, design landscape and research directions.* (2016) https://arxiv.org/pdf/1608.00771v3.pdf
4. *Hyperledger Fabric Documentation*. https://hyperledger-fabric.readthedocs.io/en/release-1.4/
5. Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn: *Corda: An Introduction.* (2016) https://docs.corda.net/releases/release-M7.0/_static/corda-introductory-whitepaper.pdf
6. www.ethereum.org
7. www.corda.net
8. www.hyperledger.org