Blockchain a supporto della filiera produttiva: Stato dell'Arte e Potenzialità

Introduzione agli Smart contract

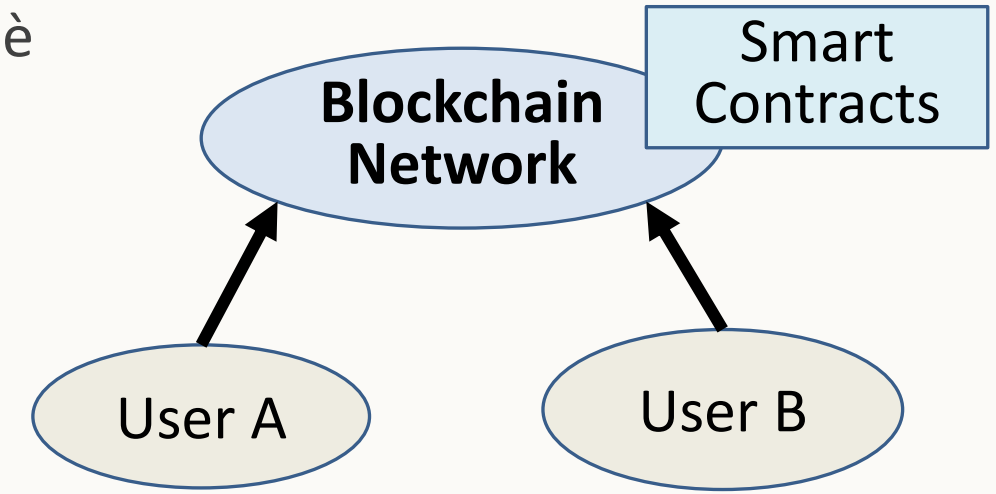
LUCA FERRETTI

UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

WEBINAR BI-REX, 19 NOVEMBRE 2020

Smart contract: definizioni brevi (da Internet)

- Software in esecuzione su un **sistema distribuito**, che **non assume parti fidate** per l'esecuzione delle sue funzionalità
- Software per **controllare** l'evoluzione dello stato di un **sistema transazionale**
- Contratto che si **autogestisce**, contiene al suo interno tutti i **termini di un accordo** fra parti ed è in grado di applicarli automaticamente tramite l'impiego di codice
- Permette l'esecuzione di transazioni e l'applicazione di accordi in **modo fidato senza la necessità di autorità centrali fidate**



Dalle Crypto-valute agli Smart Contract

Estendere i sistemi blockchain specializzati per crypto-valute a **sistemi transazionali programmabili general-purpose**

- Mantenere il paradigma fondato su di un **registro comune distribuito**
- Non limitare le operazioni a sole **transazioni per scambiare valore**
- Fornire un **sistema «personalizzabile»**, che permette ad ognuno di definire le operazioni ammissibili
  - Possibilità di definire le **interfacce** che descrivono il sistema
  - Possibilità di definire la **regole di validità e di consistenza** del sistema

Aspetto di uno Smart Contract (Ethereum Simple storage)

Lo smart contract può essere considerato **un servizio «serverless»**, solitamente implementabile tramite linguaggi di programmazione ad oggetti

- Gli utilizzatori possono interagire con le funzionalità tramite i metodi

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Aspetto di uno Smart Contract (Hyperledger car exchange example)

Seller Organization

ORG1

```
application:

seller = ORG1;
buyer = ORG2;
transfer(CAR1, seller, buyer);
```

```
car contract:

 query(car):
  get(car);
  return car;

 transfer(car, buyer, seller):
  get(car);
  car.owner = buyer;
  put(car);
  return car;

 update(car, properties):
  get(car);
  car.colour = properties.colour;
  put(car);
  return car;
```

Buyer Organization

ORG2

```
application:

seller = ORG2;
buyer = ORG1;
transfer(CAR2, seller, buyer);
```

Smart contract: requisiti, paradigmi e architetture

Una blockchain può essere di qualche utilità se consideriamo

- Problematiche di **fiducia**
  - fra i soggetti che partecipano al sistema
  - da parte di soggetti terzi che non partecipano al sistema
- Requisiti di **alta affidabilità e resilienza** di un sistema

D'altra parte, non sempre desideriamo avere tutti questi contributi, e non tutte le blockchain danno tutti questi contributi

Garanzie di una architettura basata su Smart Contract

ESECUZIONE VERIFICATA

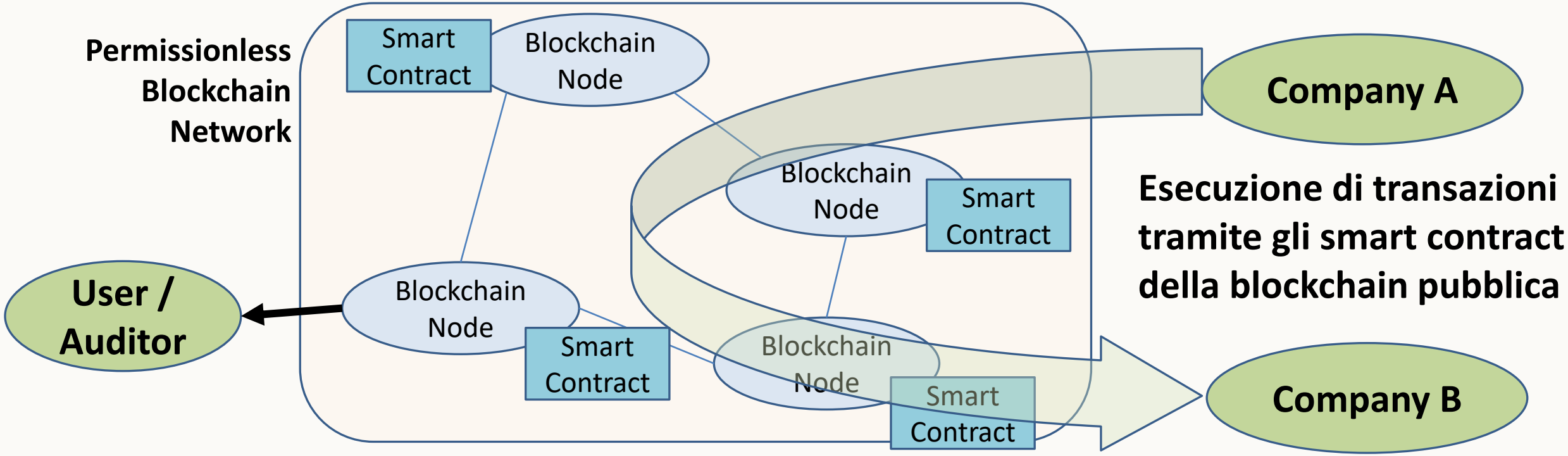
- Lo smart contract impedisce l'esecuzione di una transazione considerata non valida
- Da preferire nel caso sia all'origine di scelte critiche
- Potenzialmente più complesso e più costoso, e non sempre possibile, soprattutto nel caso di requisiti di confidenzialità

OSSERVABILITÀ DELLE OPERAZIONI

- Lo smart contract non verifica completamente la correttezza della logica applicativa, ma registra input e output in maniera che possano essere verificati a posteriori
- Da preferire per ottenere maggiore flessibilità, ad esempio in scenari complessi in cui lo smart contract non può avere tutti i mezzi per verificare a priori la correttezza dell'esecuzione

Smart Contract per abilitare la trasparenza presso terzi

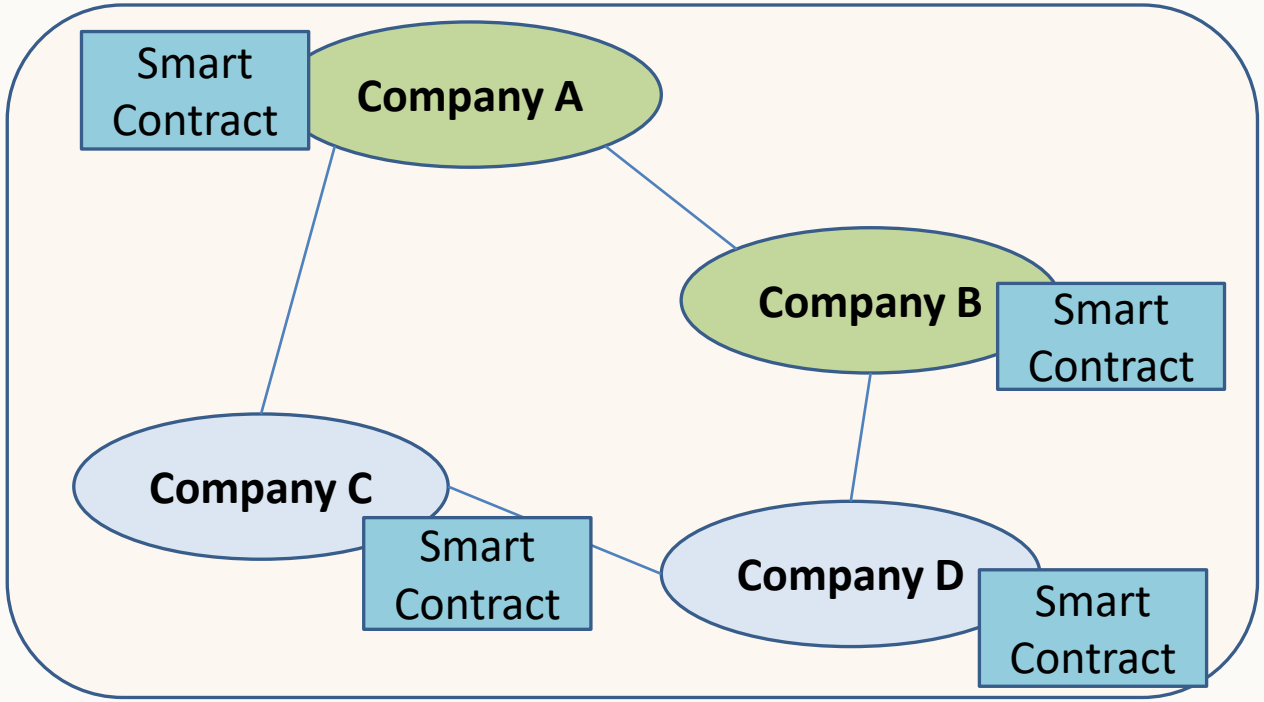
Delle aziende possono effettuare delle operazioni tramite smart contract scritti sulla blockchain pubblica e **utenti terzi** possono **osservare e controllare** questi scambi



Smart Contract per implementare la fiducia in contesti di federazione

Delle aziende in accordo possono costruire una federazione che ha degli **obiettivi di alto livello comuni**. La federazione fa automaticamente da garante in ogni transazione

Permissioned Federated Blockchain Network

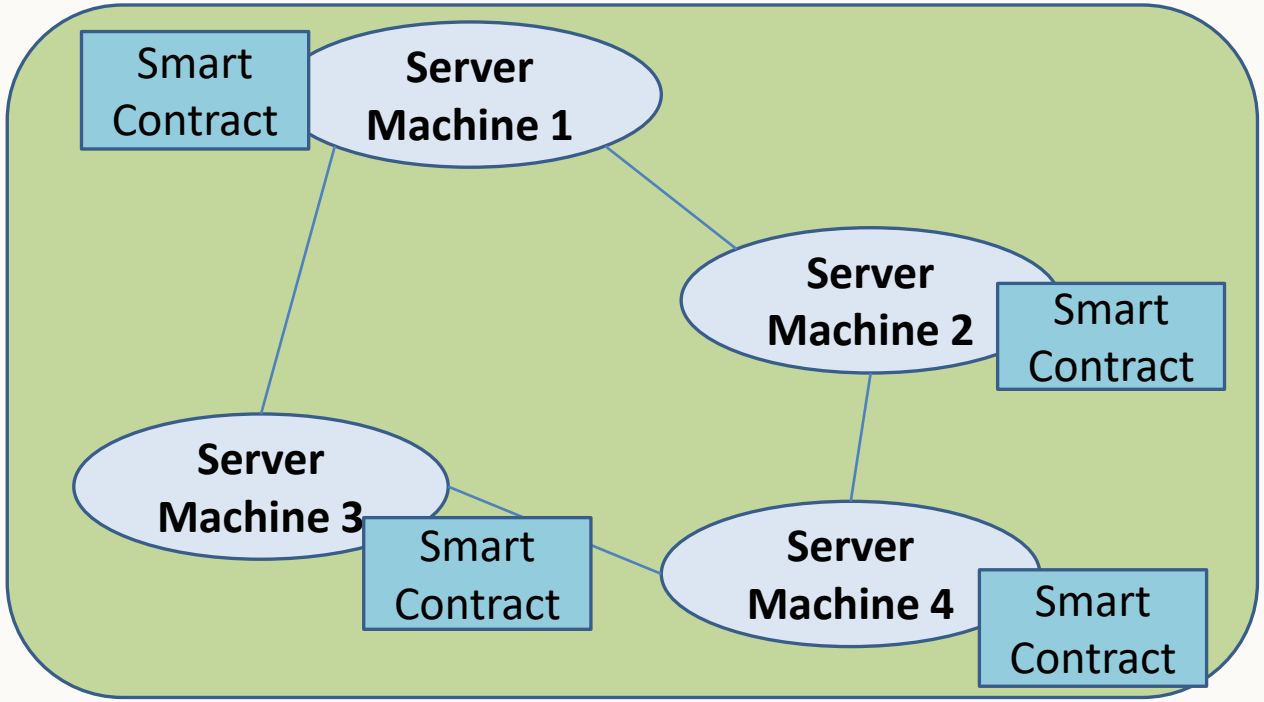


Ogni transazione che viene svolta da ognuno viene registrata e validata anche da tutti gli altri

Smart Contract per implementare una rete ad alta resilienza e sicurezza

Una singola azienda (singola autorità) sfrutta il paradigma degli smart contract per implementare un backend altamente resiliente e/o sicuro

Permissioned Single-Authority Blockchain Network



Finché una percentuale di server è correttamente funzionante, la rete funziona

- In questo caso è molto **importante distinguere i tipi di malfunzionamenti a cui il sistema blockchain è in grado di resistere (guasti o compromissioni)**

Architetture per fiducia e trasparenza

- Progettare un sistema basato su Smart Contract richiede architetture complete che prevedano l'opportuna gestione dei dati in tutte le fasi
- Questi sistemi vengono a volte chiamati Distributed Application (DApp)

  - **Gestione dei dati esterni**:
    Chi fornisce i dati agli smart contract?
    Come assicuriamo che quei dati sono veritieri?

  - **Gestione dei dati interni**:
    Possiamo davvero memorizzare tutto su blockchain? Problemi di costi?
    La completa trasparenza è davvero sempre un bene? Problemi di privacy?

Dati e servizi esterni: Oracoli [1]

- Gli oracoli sono sorgenti di dati esterne allo smart contract
  - Possono fornire i dati di input alla logica applicativa
  - Possono essere invocati dagli smart contract stessi per ottenere informazioni

Dati e servizi esterni: Oracoli [2]

- Gli oracoli sono sorgenti di dati esterne allo smart contract
  - Possono fornire i dati di input alla logica applicativa
  - Possono essere invocati dagli smart contract stessi per ottenere informazioni

- **Gli oracoli possono essere anche intermediari di sensori fisici (IoT, RFID, …), nel qual caso l'attendibilità del dato dipende anche dal processo di acquisizione**

Dati e servizi esterni: Oracoli [3]

- Come possiamo fidarci degli oracoli? Rappresentano le «terze parti fidate» di cui volevamo liberarci tramite gli Smart Contract
- **Certificatori** noti nei comuni sistemi di supply chain possono trovare un ruolo nell'ambito delle blockchain
- Alcuni orientamenti di progettazione
  - **Minimizzare e semplificare il loro ruolo**
  - Realizzare smart contract che implementano **meccanismi di autorizzazione** e richiedono l'impiego di protocolli di **non repudiabilità**

Costi di uno Smart Contract Ethereum

In un sistema di sole crypto-valute, tutte le transazioni sono (circa) «uguali», ma soprattutto sono enumerate e prevedibili

- I nodi decidono quali transazioni includere secondo diversi parametri, fra cui il costo offerto nelle transazioni stesse, le cosiddette tasse (**fee**)

In uno smart contract, i nodi chiedono un **pagamento proporzionale allo sforzo di calcolo e alla quantità di dati**

- Si introduce il cosiddetto **gas**, l'unità di misura che indica il costo delle operazioni e dello spazio
- Il costo in termini di gas è fissato nel sistema blockchain, ma **il costo del gas può variare**

Partizionamento dei dati fra Smart Contract e Sistemi di Memorizzazione

- **Memorizzare dati di grandi dimensioni** su smart contract di blockchain permissionless **costa**
- La natura della tecnologia di storage può dipendere dallo specifico scenario di realizzazione
  - Quali garanzie e funzionalità devo realizzare?
  - I dati devono essere pubblicamente disponibili, o solo verificabili?

Gestione della privacy dei dati

- In un sistema blockchain permissionless «tradizionale», **tutte le informazioni sono «nativamente» in chiaro e accessibili a tutti**
- L'unico tipo di garanzia è la pseudonimità degli account
  - Ogni utente è noto per il suo indirizzo pubblico (Wallet), tutte le operazioni e i dati associati a quell'indirizzo sono pubblici
- Le soluzioni attualmente consolidate richiedono di scegliere un **trade-off fra trasparenza, fiducia e privacy**
- Esistono trade-off migliori nell'ambito della **ricerca e delle soluzioni sperimentali**, ma il loro impiego in ambiti industriali è da valutare con (molta) cautela