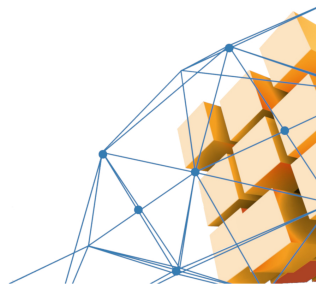
Politecnico di Torino
1859
Dipartimento di Scienze Matematiche "G. L. Lagrange"
DISMA
ECCELLENZA 2018•2022

Corda: una piattaforma blockchain progettata per i servizi finanziari

Autori:
Beji Mahdi s304665
Bonelli Martina s299777
Kiefer Riccardo s301286
Papapietro Sara s305726

Corso di Laurea in Ingegneria Matematica



Introduzione

Corda è una piattaforma blockchain con ledger distributo utilizzata per la gestione di transazioni finanziarie, sviluppata con la nascita nel 2015 del Consorzio R3.
I principi legati al business:

1. *inclusione*
2. *identità assicurata*
3. *privacy*
4. *logica condivisa*
5. *base giuridica*
6. *immutabilità*

Struttura

Le **transazioni** sono composte da **state object** e **command** e validate con controlli specificati nello **smart contract** che consiste in un'unica funzione, il *verify()*.
Corrispondono al ciclo di vita di uno *state object*, *consumato* e *ricreato* ad ogni funzione eseguita.
I partecipanti possiedono una copia solo delle transazioni alle quali prendono parte.
Ogni nodo possiede un ledger univoco che tiene traccia di queste transazioni: il **vault**.

CordApp

I nodi Corda devono eseguire CordApp, un'applicazione decentralizzata che si basa su tre elementi essenziali:

- lo **state**, che rappresenta un'azione condivisa tra i nodi della rete;
- il **contract**, che ha due scopi:
  - essere il riferimento alla documentazione legale generale che le due parti hanno concordato;
  - verificare che la proposta di transazione sia valida;
- il **flow**, che è la comunicazione tra i nodi della rete, in cui un nodo costruisce una transazione (*initiator*) e la invia alla controparte (*responder*).

Algoritmo di consenso

Corda non utilizza l'algoritmo della Proof of Work, non esiste un algoritmo preimpostato e può implementare diversi modelli di approvazione e validazione. I punti fondamentali sono:

- **Validità** della transazione nelle mani degli smart contract: ogni contratto ha dei vincoli che devono essere rispettati quando avviene una transazione.
- **Unicità** della transazione: gli stati consumati da una transazione non sono già stati consumati da un'altra.

Nodi Notarili

- **Obiettivo:** gestire la questione del *double spend*.
- **Soluzione:** è necessaria la presenza di un'entità della quale tutti i nodi si fidano per scegliere tra due transazioni ugualmente valide ma in conflitto.

Nodi Notarili

- Sono nodi a cui si chiede di *"contrassegnare questo stato come speso, se non lo è già stato"*.
- Qualsiasi transazione che desideri spendere uno stato, deve fare una richiesta al notaio prima che possa essere finalizzata.
- Nonostante il nodo notarile agisca come una parte centralizzata, i vantaggi di privacy e scalabilità di una rete distribuita vengono mantenuti, perché solo una piccola quantità di dati deve essere trasmessa al notaio ed è coinvolto solo per un breve periodo della durata complessiva della transazione.

Confronto con altre piattaforme

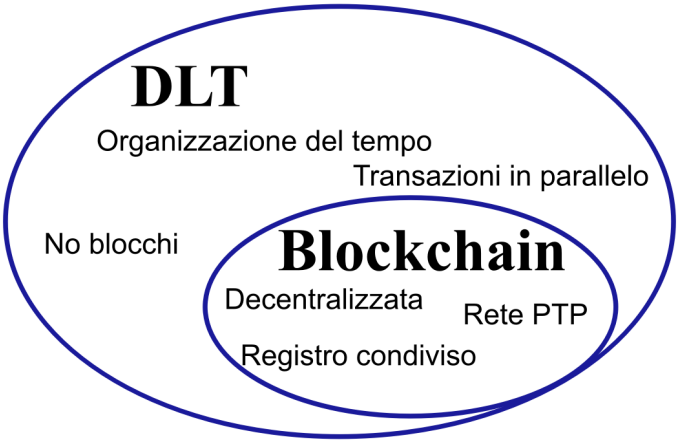
Confrontiamo Corda con il funzionamento di Bitcoin e di Ethereum.
Similitudine:

1. **BTC:**
   - Multi input e output.
2. **ETH:**
   - Codice complesso eseguito su Macchiana Virtuale.
   - Permettono la creazione di Dapp.

Per capire qualche differenza, abbiamo spiegato se Corda è considerata come una blockchain o una DLT.

Confronto con altre piattaforme

DLT (Distributed Ledger Technology)



Confronto con altre piattaforme

Differenze con BTC

Corda	BTC
No mining, No PoW	Mining tramite PoW
Dati di tipo arbitrario: es. attachments	Formato della transazione rigido
Timestamp	Inserzione di blocco
Identificazione	possibile anonimato

Confronto con altre piattaforme

Differenze con ETH

Corda

- No mining, No PoW
- Progettata per applicazioni aziendali
- Timestamp
- Identificazione e privacy

ETH

- Mining tramite PoS
- Ha un obiettivo piu ampio di creazione di Dapp
- Inserzione di blocco
- Anonimato e transazioni pubbliche

Conclusioni

Vantaggi

Corda utilizza un sistema **permissioned** in cui la validazione delle transazioni è ristretta ad un numero limitato e certificato di utenti. I vantaggi sono in termini di:

1. **Privacy**, alto livello di sicurezza garantito da:
   - Visibilità parziale dei dati.
   - Transaction tear-off.
   - Randomizzazione della chiave.
   - Cifratura.
2. **Scalabilità**, possibilità di parallelizzare processi.
3. **Controllo di accesso**, read-only access.

Conclusioni

Applicazioni

Interessanti campi di applicazione possono essere:

1. **Finanza**: quanto visto sin'ora.
2. **Assistenza sanitaria**: cartelle cliniche elettroniche (EHR).
3. **Digital Asset**: archiviazione, gestione ed elaborazione risorse digitali.
4. **Energia**: monitoraggio certificati energetici.
5. **Supply chain**: monitoraggio in tempo reale delle risorse nella catena di approvvigionamento.

Conclusioni

Svantaggi

- **Costo** singolo nodo: Corda mantiene ancora i costi e le caratteristiche della rete originaria, ideata per gestire sistemi bancari.
- **Kotlin**: il linguaggio con cui Corda è stato scritto. Nononostante spesso sia possibile utilizzare la sua controparte Java tramite JVM molte repository risultano scritte in Kotlin. Bisogna tener conto del tempo di apprendimento di tale linguaggio.

Grazie per l'attenzione

Politecnico di Torino