Sistemi Cooperativi e Reti Sociali

Lezione 5

Daniele Margiotta, Gabriele Prestifilippo, Luca Squadrone

20 maggio 2019

Indice

Capitolo 1

Distributed Ledger, Blockchain, HyperLedger Project

1.1 Distributed Ledger Technology

Le tecnologie Distributed Ledger (DLT) sono sistemi basati su un registro distribuito, ossia sistemi in cui tutti i membri o nodi di una rete possiedono la medesima copia di un database che può essere letto e modificato in modo indipendente dai singoli nodi.

Attraverso un meccanismo di consenso, il libro mastro è garantito per essere coerente. In questo database vengono registrate le transazioni (come lo scambio di beni o informazioni) tra i partecipanti alla rete. I dati non sono memorizzati su un solo computer ma su più macchine collegate tra loro attraverso una rete peer-to-peer. Ciascun nodo è autorizzato ad aggiornare e gestire il libro contabile distribuito in modo indipendente, ma sotto il controllo consensuale degli altri nodi. Gli aggiornamenti non sono più gestiti, come accadeva tradizionalmente, sotto il controllo rigoroso di un'autorità centrale, ma sono invece creati e caricati da ciascun nodo in modo appunto indipendente. In questo modo ogni partecipante è in grado di processare e controllare ogni transazione ma, nello stesso tempo ogni singola transazione, essendo gestita in autonomia, deve essere verificata, votata e approvata dalla maggioranza dei partecipanti alla rete. Qui nasce il concetto alla base dei Distributed Ledgers, ovvero il Consenso. I registri dei vari nodi vengono infatti aggiornati solamente al raggiungimento di un consenso sulle operazioni che vengono svolte. L'aggiornamento viene trasmesso a ciascun partecipante affinché tutti i registri siano coerenti. Grazie alle tecniche criptografiche e di hashing che caratterizzano la tecnologia blockchain, ogni operazione rimane memorizzata in modo indelebile ed immutabile su ogni singolo nodo.

1.1.1 Il consenso

Il consenso è il processo che permette di mantenere sincronizzate le transazioni attraverso la rete.

Questo processo è necessario per garantire che i registri vengano aggiornati mantenendo ordinate le informazioni, solo quando le transazioni sono approvate dagli altri partecipanti. Esistono diversi algoritmi di gestione del consenso, ciascuno con i propri vantaggi e svantaggi, che li rendono utilizzabili solamente in certi casi. Gli algoritmi di consenso più utilizzati sono:

- Proof of Work: usato in Bitcoin ed Ethereum, richiede ai validatori (miners) di risolvere complessi problemi crittografici.
  - Pro: funziona nelle reti di tipo pubblico, quindi non fidate;
  - Contro: estremamente oneroso dal punto di vista energetico ed è lento nella conferma delle transazioni.
- Proof of Stake: Richiede ai validatori di depositare della valuta come garanzia.
  - Pro: funziona nelle reti non fidate;
  - Contro: richiede necessariamente che il sistema sia basato su una criptovaluta ed esiste il problema "nothing at stake" dove, in caso di fallimento del consenso, ad un nodo non costa nulla votare per più ramificazioni della stessa blockchain, il che impedisce al consenso di risolversi.
- Solo: usato in Hyperledger Fabric v1.0, le transazioni vengono validate da un solo nodo, senza di fatto richiedere il consenso ad altri.
  - Pro: Molto veloce, adatto in fase di sviluppo;
  - Contro: non c'è consenso, usabile solo per test.
- Kafka: usato in Hyperledger Fabric v1.0, sono presenti dei servizi di ordinamento che distribuiscono ai vari nodi i blocchi ordinati.
  - Pro: efficiente e tollerante ai guasti;
  - Contro: non c'è una verifica contro attività malevoli.
- PBFT (Practical Byzantine Fault Tolerance): viene aggiunto un nuovo blocco se più dei 2/3 di tutti i nodi di convalida sono concordi.
  - Pro: abbastanza efficiente e fornisce un minimo controllo contro i nodi malevoli;
  - Contro: i validatori sono conosciuti e connessi tra di loro.

1.2 La differenza tra DLT, blockchain e criptovalute

DLT o **Distributed Ledger Technology** è un database distribuito su diversi nodi o dispositivi informatici, i quali singolarmente partecipano alla rete replicando e salvando una copia del ledger o libro mastro.

Non c'è alcuna autorità centrale al comando, nessun arbitro, e ogni nodo che procede alla registrazione e al salvataggio, lavora in modo indipendente.

Il principio su cui si basa il DLT è il consenso tramite il voto. Ad ogni aggiornamento, ogni nodo esegue un voto per garantire che la maggioranza sia d'accordo con la conclusione raggiunta e cioè si verifica il consenso.

Blockchain è in sostanza una forma speciale di DLT. Solo blockchain, infatti, è quel DLT che impiega una catena di blocchi per fornire il consenso al registro distribuito.

Anche blockchain, essendo gestita da reti peer-to-peer, può esistere senza alcuna autorità centrale e utilizza un consenso algoritmico per procedere con l'aggiornamento del database.

Ma ciò che rende la blockchain unica rispetto agli altri DLT è il raggruppamento e l'organizzazione in blocchi. Sono, infatti, i blocchi che vengono collegati tra loro e protetti mediante crittografia.

I blocchi vengono continuamente aggiunti alla catena, consentendo solo di aggiungere dati al database distribuito. infatti, i dati, una volta registrati, non sono più modificabili o eliminabili. Inoltre, nella catena, i blocchi sono chiusi da un tipo di firma crittografica chiamata hash, che sarà uguale all' hash del blocco successivo.

Esistono consorzi come R3, Hyperledger ed Enterprise Ethereum Alliance che progettano e sviluppano a pieno le potenzialità di DLT e blockchain.

Blockchain e DLT sono entrambi registri distribuiti decentralizzati che procedono applicando il consenso tra i nodi in modo trasparente e non hackerabile.

Ma blockchain è quel DLT speciale che utilizza la catena di blocchi per organizzare e registrare i dati, i quali possono essere solo aggiunti.

Infine la **criptovaluta** è una moneta digitale che funziona come mezzo di scambio ed utilizza la crittografia per proteggere e verificare la transazioni. La criptovaluta più famosa è il Bitcoin che appunto utilizza il sistema blockchain.

Tuttavia è doveroso precisare che non tutte le criptovalute sono basate su blockchain (ad esempio IOTA è basata su Tangle).

1.3 Smart Contract

Uno Smart Contract è la traduzione (o trasposizione) in codice di un contratto in modo da verificare in automatico l'avverarsi di determinate condizioni e di eseguire automaticamente azioni nel momento in cui le condizioni concordate tra le parti sono raggiunte e verificate.

Se un contratto standard è rafforzato dalla legge, uno smart contract è rafforzato dall'immutabilità e l'oggettività dei codici crittografici. Uno Smart Contract è essenzialmente un programma che esegue inevitabilmente le condizioni prestabilite dagli sviluppatori, o meglio, un contratto tradizionale i cui effetti sono garantiti da un algoritmo.

Lo Smart Contract ha bisogno di un supporto legale per la sua stesura, ma non ne ha bisogno per la sua verifica e per la sua attivazione. Ai contraenti spetta il compito di definire condizioni, clausole, modalità e regole di controllo e azione, ma una volta che il loro contratto è diventato codice (dunque uno Smart Contract) e viene accettato, gli effetti non dipendono più dalla loro volontà. Questo punto è estremamente rilevante perché rappresenta la "certezza di giudizio oggettivo", escludendo qualsiasi forma di interpretazione. All'interno di una blockchain, gli Smart Contracts vengono integrati per supportare l'aggior-

namento coerente delle informazioni e per realizzare le funzionalità tipiche del libro contabile, come transazioni, interrogazioni ed elaborazione dati.

1.3.1 Come funziona?

Attraverso lo Smart Contract è possibile garantire che al verificarsi di alcune condizioni poste in precedenza inevitabilmente si spieghino gli effetti concordati previamente dalle parti. Il fondamento logico che viene eseguito è facilmente trascrivibile con la frase "if-this-then-that" (se questo accade allora succede). Una volta che due o più parti identificano un interesse comune, scrivono insieme uno smart contract ponendo le condizioni e gli effetti desiderati e lo inseriscono nella Blockchain. A questo punto la stessa Blockchain diventa il garante del contratto. Quando nella rete si ottiene il consenso, il contratto esegue le sue condizioni, e di conseguenza la Blockchain verrà aggiornata dalla modifica di stato del sistema.

1.3.2 I vantaggi

I settori d'utilizzo per gli smart contract sono molteplici: dagli e-Commerce come e-Bay, alle Assicurazioni per gli autoveicoli, ai diversi servizi online. I principali vantaggi sono:

- Indipendenza - la transizione non necessita di intermediari come avvocati o notai;
- Risparmio - proprio perchè annullano la necessità di intermediari, gli smart contract permettono di risparmiare denaro;
- Sicurezza - i documenti criptati, immuni a qualsiasi tipo di attacco e duplicati molte volte;
- Precisione - gli smart contract fanno risparmiare tempo, denaro ed evitano gli errori.

1.4 HyperLedger Project

Hyperledger è un progetto open source fondato nel 2015 dalla Linux Foundation per supportare lo sviluppo collaborativo di Distributed Ledgers basati su tecnologia blockchain. L'obiettivo del progetto è far progredire la collaborazione intersettoriale sviluppando blockchain e registri distribuiti, con particolare attenzione al miglioramento delle prestazioni e dell'affidabilità di questi sistemi in modo che siano in grado di supportare transazioni commerciali dalle principali società tecnologiche, finanziarie e della distribuzione a livello globale. Il progetto integra standard e protocolli open ed indipendenti, attraverso un framework composto da moduli specifici a seconda degli usi. Tra questi moduli vi sono blockchains con funzionalità di consenso e storage, servizi per la gestione delle identità, il controllo degli accessi e Smart Contracts. Attualmente nel progetto sono coinvolti più di 180 membri, tra cui diversi sviluppatori indipendenti di software blockchain (Blockchain, ConsenSys, Digital Asset, R3, Onchain), società tecnologiche (Cisco, Fujitsu, Hitachi, IBM, Intel, NEC, NTT DATA, Red Hat, VMware), aziende di servizi finanziari, software aziendali (SAP) ed altri.