Architetture Dati

UniShare

Davide Cozzi
@dlcgold

Indice

Capitolo 1

Introduzione

Questi appunti sono presi a lezione. Per quanto sia stata fatta una revisione è altamente probabile (praticamente certo) che possano contenere errori, sia di stampa che di vero e proprio contenuto. Per eventuali proposte di correzione effettuare una pull request. Link: `https://github.com/dlcgold/Appunti`.

Capitolo 2

Sistemi centralizzati

Definizione 1. *Un **DBMS (DataBase Management System)** è un sistema, ovvero un software, in grado di gestire collezioni di dati che siano:*

- *grandi, ovvero di dimensioni maggiori della memoria centrale dei sistemi di calcolo usati (se ho a che fare con una quantità di dati non così grande e con un uso personale posso affidarmi ad una hashmap piuttosto che ad un db)*
- *persistenti, ovvero con un periodo di vita indipendente dalle singole esecuzioni dei programmi che le utilizzano e per molto tempo*
- *condivise, ovvero usate da diversi applicativi e diversi utenti (fattore che porta anche allo studio del carico di lavoro, workload). L'accesso può essere sia in scrittura che in lettura (ovviamente anche entrambi) a seconda del caso. SI pongono quindi problemi di concorrenza e sicurezza*
- *affidabili, sia resistente dal punto di vista hardware (un guasto non deve farmi perdere i dati) che dal punto di vista della sicurezza informatica. Le transazioni devono essere quindi **atomiche** (o tutto o niente) e **definitive** (che non verranno più dimenticate). Il software può cambiare mentre i dati no*

A livello di architettura per un *sistema centralizzati* si hanno:

- uno o più *storage* per memorizzare i dati, a loro volta su uno o più file del *file system*
- il *DBMS*, il componente software che funge da componente logico

- diverse applicazioni che elaborano i dati provenienti dal db (*lettura*) ed eventualmente scrivono dati sullo stesso (*scrittura*)
- il **DBA (*DataBase Administrator*)** che tramite riga di comando o GUI si occupa di manutenzione, sicurezza, ottimizzazione etc... del DBMS

L'*architettura dati* di un DBMS è definita dall'ente *ANSI/SPARC* e è a tre livelli:

1. diversi **schemi esterni**, porzioni di db messi a disposizione per le varie applicazioni
2. uno **schema logico (o concettuale)**, che fa riferimento al *modello relazionale* dei dati ed è indipendente dalla tecnologia usata. Avendo un unico schema logico si ha un'unica semantica (perlomeno a livello astratto). Si ha unica base di dati, quindi un unico insieme di record interrogati e aggiornati da tutti gli utenti. Non si ha nessuna forma di eterogeneità concettuale
3. uno **schema fisico**, che fa riferimento alla tecnologia usata per implementare le tabelle per salvare i dati. Si ha un'unica rappresentazione fisica dei dati e quindi nessuna distribuzione e nessuna eterogeneità fisica

Un unico schema fisico è collegato ad un unico schema logico.
Inoltre si hanno:

- un **unico linguaggio di interrogazione** e quindi un'unica modalità di accesso ai dati
- un unico sistema di gestione per accesso, aggiornamento e gestione per la transazioni e le interrogazioni
- un'unica modalità di ripristino in caso d'emergenza
- un unico amministratore dei dati
- **nessuna autonomia gestionale**

Per il discorso della persistenza dei dati si ha necessità di una memoria secondaria dove il DBMS salva le strutture dati, studiando un modo efficiente di trasferimento dei dati nel *buffer* in memoria centrale. Il *buffer* è un'area di memoria (o meglio un componente software) nella memoria centrale che

cerca, tramite una logica di "vicinanza", di mettere i dati della memoria secondaria in quella centrale. Si usa il **principio di località**.
A causa degli accessi condivisi al db si hanno problemi di **concorrenza**, avendo accesso multi-utente alla stessa dei dati condivisa, accesso che necessità anche di meccanismi di **autorizzazione**. In merito alla concorrenza si ha che le transazioni sono corrette se **seriali** (ordinate temporalmente) ma questo non è sempre applicabile e quindi si deve stabilire un *controllo della concorrenza*.
Per accedere ai dati di un db si hanno le **query (*interrogazioni*)** che fanno parte del modello logico a cui si interfaccia l'utente. Essendo i dati nelle memorie secondarie bisogna cercare un modo di rendere gli accessi performanti, in primis tramite opportune strutture fisiche in quanto e strutture logiche non sarebbero efficienti in memoria secondaria. Bisogna fare in modo che gli accessi alla memoria secondaria siano il più limitati possibili e quindi bisogna ottimizzare l'esecuzione delle query. Ovviamente una scansione lineare delle tabelle sarebbe troppo dispendiosa con tabelle grosse, ricordando che i file sono ad accesso sequenziale. Inoltre un ipotetico *join* tra tabelle renderebbe ancora più complesso l'accesso, soprattutto se *full-join*.
Per poter garantire tutto ciò che è stato detto l'architettura del DBMS deve essere organizzata in termini di *funzionalità cooperanti*:

- un **query compiler** che prende una query in SQL e la traduce con un compilatore
- un **gestore di interrogazioni e aggiornamenti** che trasforma le query in SQL in algebra relazionale facendo operazioni di ottimizzazione
- un **gestore dei metodi di accesso** per permettere il passaggio tra file e tabelle passando dal **gestore del buffer** e il **gestore della memoria secondaria** dove i dati non sono in forma tabellare ma di file e pagine
- un **DDL compiler**, dove DDL sta per Data Description Language, che si occupa dei comandi del DBA
- un **gestore della concorrenza**, che garantisce il controllo della concorrenza
- un **gestore dell'affidabilità**, che garantisce che un dato non vada perso
- un **gestore delle transazioni**

Gli ultimi quattro entrano in uso specialmente in fase di scrittura.
Tutto deve essere veloce!
In un sistema distribuito la parte di query compiler, gestore delle interrogazioni, gestore delle transazioni e gestore della concorrenza resta invariato mentre il resto cambia drasticamente (in quanto i dati sono distribuiti) dovendo gestire diversamente l'accesso ai dati e la sua sicurezza. Bisogna gestire anche come i vari nodi devono interagire coi dati.

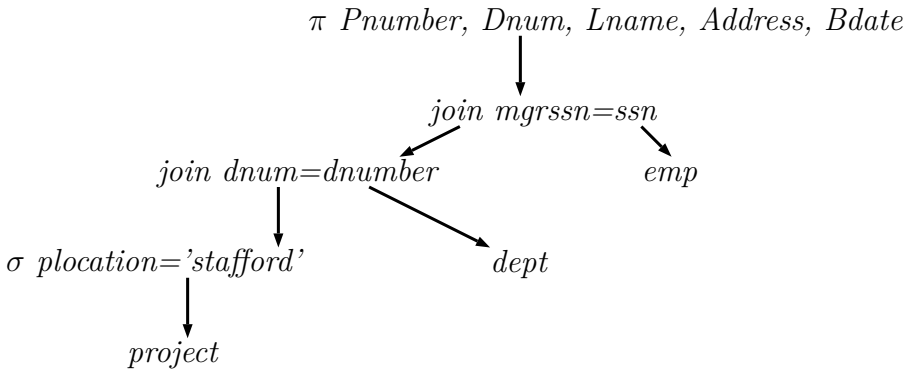
2.1 Ottimizzazione delle query

Ottimizzare le query è tutt'altro che banale.
Il primo step è il **parsing**, che stabilisce se la query è sensata dal punto di vista sintattico e se i vari nomi di tabelle e attributi sono coerenti con lo schema. Per questo ultimo aspetta ci si appoggia al **Data Catalog**, un particolare db che contiene informazioni sui vari database, in primis sui vari nomi delle tabelle e per ciascuna sui nomi di ogni attributo. SI ha quindi una soluzione per gestire i *metadati*. Il parser effettua un'analisi lessicale, per la sintattica e la semantica, usando il dizionario e l a traduzione in algebra relazionale, producendo un **query tree**. Si calcola anche un **query plan logico**, utilizzando regole sintattiche di buon senso, per capire cosa fare prima (per esempio se fare prima una *select* o un *join*) per ottenere il risultato corretto nel minor tempo possibile (prima di fare una *join* magari seleziono prima una sottotabella con i dati potenzialmente utili, togliendo quelli sicuramente inutili... magari quel *join* può anche essere evitato). La query viene quindi rappresentata come un albero dove e foglie corrispondono alle strutture dati logiche, ovvero le tabelle. I nodi interni sono invece le varie **operazioni algebriche (*select, join, proiezione, prodotto cartesiano* e *operazioni insiemistiche*)**.

Esempio 1. *Vediamo una query:*

```
SELECT Pnumber, Dnum, Lname, Address, Bdate
FROM Project P, Dept D, Emp E
Where P.dnum=D.dnumber and E.ssn = D.mgrssn
and P.location = 'Stafford'
```

che produce:



ma l'ottimizzatore va oltre (magari invertendo i where etc...) con un query plan più efficiente che permette di cambiare automaticamente le query in altre più efficienti.

Si ha un db chiamato **Statistics** che contiene statistiche sulla storia delle query nonché altre informazioni sui dati. L'uso di tale db permette di ottimizzare le query.
Solo dopo questo processo si ha la trasformazione delle tabelle logiche in strutture fisiche e metodi di accesso alla memoria e la trasformazione delle operazioni algebriche nelle loro implementazioni sulle strutture fisiche. Per la trasformazione si usano proprietà algebriche e una stima dei costi delle operazioni fondamentali per diversi metodi di accesso (in poche parole le regole della ricerca operativa). L'ottimizzazione ha complessità **esponenziale** e quindi si introducono approssimazioni basate su euristiche, usando un'**alberatura di costi** usando la tecnica del **Branch&Bound**.

2.2 Transazioni

Una **transazione** è l'insieme di istruzioni di accesso in lettura e scrittura ai dati, istruzioni eventualmente inserite in un linguaggio di programmazione. Una transazione gode di proprietà che garantiscono la corretta esecuzione anche in ambito di concorrenza e sicurezza, tanto che sono paradigmatiche

del modello relazionale. Le transazioni iniziano con un **begin-transaction** (a volte finiscono con *end-transaction*, opzionale) e all'interno deve essere eseguito tra:

- **commit work**, per terminare correttamente la lettura e/o scrittura
- **rollback work**, per abortire la transazione

Un **sistema transazionale OLTP (*OnLine Transaction Processing*)** è in grado di definire ed eseguire transazioni per conto di un certo numero di applicazioni concorrenti anche alto.

Esempio 2. *Vediamo un esempio di transazione (esempio di addebito su un conto corrente e accredito su un altro):*

```
start transaction;
update ContoCorrente
  set Saldo = Saldo + 10 where
  NumConto = 12202;
update ContoCorrente
  set Saldo = Saldo - 10 where
  NumConto = 42177;
commit work;
```

oppure, con anche la verifica che ci siano ancora soldi dopo il prelievo (con eventuale aborto):

```
start transaction;
update ContoCorrente
  set Saldo = Saldo + 10 where
  NumConto = 12202;
update ContoCorrente
  set Saldo = Saldo - 10 where
  NumConto = 42177;
select Saldo into A
  from ContoCorrente
  where NumConto = 42177;
if (A >= 0) then commit work
else rollback work;
```

Il controllo può essere fatto a posteriori grazie al rollback che permette di "dimenticare" tutte le operazioni precedenti

Le istruzioni commit work e rollback work possono comparire più volte all'interno del programma ma esattamente una delle due deve essere eseguita. Si ha un **approccio binario**.
Bisogna approfondire quindi le **unità di elaborazione** che hanno le proprietà cosiddette *ACID*:

- **Atomicità**, ovvero una transazione è un'unità atomica di elaborazione. Non si può lasciare il db in uno "stato intermedio". Un problema prima del commit cancella tutto le operazioni svolte (*UNDO*) e un problema dopo il commit non deve avere conseguenze, se necessario vanno ripetute le operazioni (*REDO*)
- **Consistenza**, ovvero la transazione rispetta i vincoli di integrità (se lo stato iniziale è corretto lo è anche quello finale). Quindi se ci sono violazioni non devono restare alla fine (nel caso *rollback*)
- **Isolamento**, ovvero la transazione non risente delle altre transazioni concorrenti. Una transazione non espone i suoi stati intermedi evitando l'*effetto domino* (si evita che il rollback di una transazione vada in cascata con le altre). L'esecuzione concorrente di una collezione di transazioni deve produrre un risultato che si potrebbe ottenere con una esecuzione sequenziale
- **Durabilità** (ovvero persistenza), ovvero gli effetti di una transazione andata in commit non vanno persi anche in presenza di guasti (a tal fine si sfrutta il **recovery manager**, che garantisce l'affidabilità, del DBMS)

2.3 Gestore della concorrenza

Il **gestore della concorrenza** permette di eseguire in parallelo più operazioni.
Definiamo **schedule** come una sequenza di esecuzione di un insieme di transazioni. Uno schedule è **seriale** se se una transazione termina prima che la successiva iniziale, altrimenti è **non seriale**. Qualora non sia seriale si potrebbero avere problemi.
Si sfrutta quindi la **proprietà di isolamento** facendo in modo che ogni transazione esegua come se non ci fosse concorrenza: *un insieme di transazioni eseguite concorrentemente produce lo stesso risultato che produrrebbe una (qualsiasi) delle possibili esecuzioni sequenziali delle stesse transazioni allora si ha la proprietà di isolamento.*

Si ha quindi che uno schedule è serializzabile se l'esito della sua esecuzione è lo stesso che si avrebbe con una qualsiasi sequenza seriale delle transazioni contenute.
Si hanno quindi diversi algoritmi per il controllo della concorrenza secondo varie tipologie:

- controllo basato su *conflict equivalence*
- controllo di concorrenza basato su *locks (protocollo 2PL o two phase locking, shared locks e gestione dei deadlock*). Il protocollo 2PL è usato nei DBMS dove per costruzione si hanno schedule serializzabili usando i lock per bloccare l'accesso alla risorse da parte di una transazione fino a che una risorsa non sia rilasciata. Si hanno quindi i concetti di *lock* e *unlock* che garantiscono l'uso esclusivo di una risorsa e l'autorizzazione esclusiva dell'uso di una risorsa viene dato dal gestore delle transazioni. Si hanno delle **tabelle di lock**. Si ha che, in ogni transazione, tutte le richieste di *lock* precedono tutti gli *unlock* (che comunque devono essere fatti dopo l'operazione di *commit*)
- controllo di concorrenza basato su *timestamps*

Capitolo 3

Sistemi distribuiti relazionali

Abbiamo visto nei sistemi centralizzati come ci fosse una sola base dati. In un sistema distribuito abbiamo diversi **basi dati locali**, diverse applicazioni su ogni nodo di elaborazione (dove ogni nodo condivide varie informazioni) con gli utenti che accedono alle varie applicazioni. Questo tipo di architettura prende il nome di **architettura shared nothing**, in quanto i DBMS di ogni singola macchina sono autonome (anche di vendor diversi) ma che lavorano insieme.
Un sistema distribuito permette non solo di avere dati "distribuiti" tra vari nodi ma anche di "duplicarne" alcuni per diversi scopi, coi nodi collegati in rete (addirittura si hanno soluzioni interamente distribuite nel cloud).
Confrontando un db distribuito con un multi-database (ovvero vari database completi da "unificare") notiamo come entrambi abbiano un'alta distribuzione, il primo una bassa eterogeneità (a differenza del secondo, dove nei vari db potrei avere forte differenza di tipologia dei dati contenuti). Si ha anche bassa autonomia nel caso si db distribuiti a differenza del multi-database (dove ogni db è singolarmente autonomo).
Bisogna capire cosa distribuire. Si hanno diverse condizioni (che possono essere presenti simultaneamente):

- le applicazioni, fra loro cooperanti, risiedono su più nodi elaborativi **(elaborazione distribuita**)
- l'archivio informativo è distribuito su più nodi (**base di dati distribuita**)

La distribuzione si dice essere **ortogonale e trasparente** agli altri.
Capire cosa distribuire è una parte consistente dello studio di come costruire un'architettura distribuita (magari frutto di situazioni particolari come la "fusione" di due sistemi a causa di un'acquisizione aziendale etc... dove

diverse logiche applicative e diverse strutture dati possono creare situazioni molto pericolose).
Possiamo classificare i db distribuiti. Si ha innanzitutto che un **DBMS Distribuito Eterogeneo Autonomo** è in generale una federazione di DBMS che collaborano nel fornire servizi di accesso ai dati con livelli di *trasparenza* definiti (infatti le diversità tra db nei nodi vengono "nascosti" a vari *livelli di trasparenza* per distribuzione, eterogeneità e autonomia). Come abbiamo visto esiste l'esigenza di integrare a posteriori vari db preesistenti (anche a causa di integrazione di nuovi applicativi o nuove cooperazioni di processi) e questa situazione è spinta dallo sviluppo della rete.
Possiamo quindi dividere i livello di federazione su tre categorie tra loro ortogonali (ovvero indipendenti):

- autonomia
- distribuzione
- eterogeneità

Autonomia

L'**autonomia** fa riferimento al grado di indipendenza tra i nodi e si hanno diverse forme:

- **autonomia di progetto**, il livello "massimo" dove ogni nodo ha un proprio modello dei dati e di gestione delle transazioni
- **autonomia di condivisione**, dove ogni nodo sceglie la porzione di dati da condividere ma condividendo con gli altri nodi lo schema comune
- **autonomia di esecuzione**, dove ogni nodo sceglie in che modo eseguire le transazioni

Si hanno quindi:

- **DBMS Strettamente integrati** con nessuna autonomia, con dati logicamente centralizzati, un unico data manager per le transazioni applicative e vari data manager locali che non operano in modo autonomo ma eseguono le direttive centrali
- **DBMS semi-autonomi**, dove ogni data manager è autonomo ma partecipa a transazioni globali, dove una parte dei dati è condivisa e dove sono richieste modifiche architetturali per poter fare parte della federazione

- **DBMS Peer to Peer** completamente autonomi, dove ogni DBMS lavora in completa autonomia ed è inconsapevole dell'esistenza degli altri

Distribuzione

Per la **distribuzione** dei dati si hanno 3 livelli classici:

- **distribuzione client/server**, in cui la gestione dei dati è concentrata nei server, mentre i client forniscono l'ambiente applicativo e la presentazione
- **distribuzione Peer to Peer**, in cui non c'è distinzione tra client e server, e tutti i nodi del sistema hanno identiche funzionalità DBMS
- **nessuna distribuzione**

Le prime due possono anche non essere distinte.

Eterogeneità

L'**eterogeneità** può invece riguardare vari aspetti:

- **modello dei dati** (relazionale, XML, object oriented (OO), json)
- **linguaggio di query** (diversi dialetti SQL, query by example, linguaggi di interrogazione OO o XML)
- **gestione delle transazione** (protocolli diversi per il gestore della concorrenza o per il recovery)
- **schema concettuale e logico** (concetti rappresentati in uno schema come attributo e in altri come entità)

Quindi si hanno vari tipi di DBMS:

- **DBMS distribuito omogeneo (DDBMS)** quando si ha alta distribuzione ma non si hanno autonomia ed eterogeneità (gestiti solitamente dallo stesso vendor)
- **DBMS eterogeneo logicamente integrato (data warehouse)** quando si ha alta eterogeneità ma non si hanno distribuzione e autonomia

- **DBMS distribuiti eterogenei** quando si ha alta eterogeneità e distribuzione ma non autonomia
- **DBMS federati distribuiti** quando si ha alta distribuzione, semi autonomia e non eterogeneità
- **DBMS distribuiti federati eterogenei** quando si ha alta distribuzione ed eterogeneità e semi autonomia
- **multi db MS**, totalmente autonomi ed eventualmente omogenei o eterogenei

Si hanno molti altri sistemi in base alle 3 categorie.

3.1 DDBMS

Parliamo di **DBMS distribuito omogeneo (*DDBMS*)**.
Studiamo uno schema in cui si passa da un sistema centralizzato ad un sistema distribuito.
Si hanno due architetture di riferimento:

- l'**architettura dati**
- l'**architettura funzionale**, ovvero l'insieme di tecnologie a supporto dell'architettura dati

Non avendo eterogeneità mantengo lo stesso schema di un DBMS centralizzato ma distribuisco dati bisogna prendere lo schema centralizzato e aggiungere componenti tra lo schema logico e lo schema fisico. Infatti non si avrà più un solo schema logico e un unisco schema fisico ma tanti schemi logici e fisici locali (ad ogni logico corrisponde un fisico). I vari schemi logici inoltre si interfacciano con uno **schema logico globale**, i vari schemi logici locali non sono quindi altro che delle *viste* dello schema logico globale. Questa organizzazione tra schemi logici locali e schema logico globale è la cosiddetta **organizzazione LAV (*Local As View*)**. In ogni caso il progettista interroga lo schema logico globale e saranno varie tecnologie ad interrogare gli schemi logici locali (si fa una sorta di routing delle query).
Per ciascuna funzione (come query processing, transaction manager etc...) si possono avere vari tipi di gestione:

- centralizzata/gerarchica o distribuita

- con assegnazione statica o dinamica dei ruoli

Lo schema globale viene progettato prima degli schemi locali.
Ovviamente cambia il **processo di progettazione** nel caso dei DDBMS. Normalmente si ha un approccio *top-down* per la progettazione, con:

1. analisi dei requisiti
2. progettazione concettuale
3. progettazione logica
4. progettazione fisica

ma questo tipo di progettazione va cambiato e quindi si introduce una nuova fase e si cambiano le ultime due:

1. analisi dei requisiti
2. progettazione concettuale
3. **progettazione della distribuzione**, per capire dove mettere i dati
4. progettazione logica **locale**, che traduce dallo schema concettuale globale allo schema logico locale solo alcuni concetti
5. progettazione fisica **locale**

Si introduce il concetto di **portabilità**, ovvero la capacità di eseguire le stesse applicazioni DB su ambienti runtime diversi (anche con SQL diversi e differenti dallo standard). La portabilità è a *compile-time*
Si ha anche il concetto di **interoperabilità** (tra vendors diversi), ovvero la capacità di eseguire applicazioni che coinvolgono contemporaneamente sistemi diversi ed eterogenei (con zero autonomia). A tal fine sono stati introdotti dei *middleware*, tra cui **ODBC** che si occupa dell'accesso a dati di diversi vendor. ODBC, a livello architetturale, si pone sopra il DBMS e da un'immagine indipendente da ciò che c'è sotto (funziona come una sorta di *driver*), trasformando tutto in una sorta di SQL standard. Si hanno anche dei protocolli, come **X-Open Distributed Transaction Processing (*DTP*)** (che è una descrizione architetturale abilitante il protocollo di esecuzione di transazioni distribuite), che consentono di eseguire delle transazioni secondo una logica diversa. Questo protocollo stabilisce una serie di API che vengono implementate da ogni singolo DBMS per offrire una connettività standard (approccio molto usato per transazioni con vendor diversi). Il protocollo funziona sia se si ha che fare con omogeneità che con eterogeneità.
Si hanno altri approcci:

- **basi dati parallele**, con incremento delle prestazione mediante parallelismo sia di storage devices che di processore (scalabilità orizzontale). Un esempio sono le **basi dati GRID**
- **basi dati replicate** dove si ha la replicazione della stessa informazione su diversi server per motivi di performance. Importanti per i temi della consistenza e della sicurezza
- **Data warehouses**, ovvero DBMS centralizzati, risultato dell'integrazione di fonti eterogenee, dedicati nel dettaglio alla gestione di dati per il supporto alle decisioni. Prevede la *cristallizzazione* dei dati, acquisiti da varie sorgenti, creando un nuovo schema con la memorizzazione dei dati in formato nuovo (solitamente relazionale). Non usa un approccio LAV

3.1.1 Caratteristiche dei DDBMS

Si hanno vari tipi di architetture DDBMS:

- **shared-everything**, ad esempio *SMP server*, dove il db management system e il disco sono in un unico nodo
- **shared-disk**, ad esempio *Oracle RAC*, dove diversi db management systems agiscono su una stessa **SAN (*Storage Area Network*)**, ovvero un'architettura dati di puro storage (con tanti dischi in raid). I vari db accedono ai dati secondo una certa regolazione. Viene distribuito il carico sui db ma si hanno problemi di concorrenza e hanno grandi problemi di scalabilità e costo economico
- **shared-nothing**, sempre più usati, dove ogni db management system ha il suo disco. È molto scalabile e, a patto di gestire la complessità, posso aggiungere nodi in modo illimitato (**scalabilità orizzontale**). Si presta molto all'ambiente cloud. Sono *architetture federate*.

Vediamo quindi le proprietà generali di un DDBMS (facendo esplicito riferimento alle architetture *shared-nothing* per la loro scalabilità):

- **località**, secondo il *principio di località*, che garantisce un aumento di performances (nonché di sicurezza) tenendo i dati si trovano "vicino" alle applicazioni che li utilizzano più frequentemente

- **modularità**, permettendo di scalare orizzontalmente e permettendo modifiche a dati ed applicazioni a basso costo
- **resistenza ai guasti**
- **prestazioni ed efficienza**

Concentrandoci sulla **località** si ha che la partizione dei dati corrisponde spesso ad una partizione naturale delle applicazioni e degli utenti. I dati risiedono più vicino a dove vengono più usati ma possono comunque essere raggiunti anche da lontano (*globalmente*). Si cerca inoltre sempre di più di spostare i dati verso le applicazioni (paradigma ribaltato nel caso di *big data*).
In merito alla **modularità** si nota come la distribuzione dinamica dei dati si adatta meglio alle esigenze delle applicazioni (magari spostando solo sottotabelle verso alcuni nodi etc. . ., sia in modo trasparente rispetto all'utente che altrimenti).
Parlando di **resistenza ai guasti** si ha una maggior fragilità a causa delle unità che aumentano di numero ma si ha **ridondanza** e quindi maggiore resistenza ai guasti di dati e applicazioni ridondate (*fail soft*).
Discorso più interessante è da farsi sulle **prestazioni**. Ogni nodo in un sistema shared-nothing gestisce db di dimensioni ridotte. Inoltre ogni nodo può essere ottimizzato ad hoc ed è più semplice gestire e ottimizzare applicazioni locali. Si ha inoltre distribuzione del carico totale e parallelismo tra transazioni locali che fanno parte di una stessa transazione distribuita (anche se questo aspetta obbliga soluzioni di coordinamento e appesantisce il carico sulla rete, che rischia di diventare un "collo di bottiglia").
I DDBMS hanno ovviamente **funzionalità** specifiche.
Ogni server ha buona capacità di gestire transazioni indipendentemente, anche se le interazione distribuita tra server rappresentata un carico supplementare. Per le interrogazioni si ha che le query arrivano dalle applicazioni e i risultati dai server mentre per le transazioni le richieste transazionali arrivano dalle applicazioni ma sono richiesti **dati di controllo** per il coordinamento.
' La gestione della rete deve essere ottimizzata e serve uno studio sulla distribuzione locale dei dati.
Ricapitolando si hanno le seguenti funzionalità specifiche:

- **trasmissione** di query, transizioni, frammenti di db e dati di controllo tra i nodi
- **frammentazione, replicazione e trasparenza** (secondo vari livelli), fattori legati alla natura distribuita dei dati

- un **query processor** e un **query plan** per la previsione di una strategia globale accanto a strategie per le query locali. Si gestisce il passaggio tra schema logico globale e quelli locali. Chi esegue la query lo fa senza pensare alla frammentazione dei dati
- **controllo di concorrenza** tramite algoritmi distribuiti, fondamentale per gli accessi *in scrittura*
- **strategie di recovery** e **gestione dei guasti**, sia in merito alla rete che all'hardware stesso

3.1.2 Frammentazione e replicazione

Si definisce **frammentazione** come la possibilità di allocare porzioni (*chunk*) diverse del db su nodi diversi.
Si definisce **replicazione** come la possibilità di allocare stesse porzioni del db su nodi diversi.
Si definisce **trasparenza** come la possibilità per l'applicazione di accedere ai dati senza sapere dove sono allocati (serve qualcosa che instradi le query).

frammentazione

Esistono due tipi di frammentazione:

1. **frammentazione orizzontale**, che prevede di prendere una tabella e frammentare in base alle righe (le prime n da una parte, le seconde m dall'altra etc...). Si mantiene quindi inalterato lo schema in quanto ottengo solamente delle tabelle più piccole in quanto pezzi. Per spezzare uso una *select* (per la **selezione**) che selezioni ogni volta un certo "blocco" di tabella
2. **frammentazione verticale**, che consente di ridurre la dimensionalità della tabelle spezzandola in base alle colonne. In ogni nuova tabella però la prima colonna deve essere uguale alla prima della tabella originale (ovvero dove si ha la chiave primaria), questo per garantire che si possa ricomporre la tabella (e lo schema) originale (con operazioni di *join*, o meglio un *natural join*) e garantire la trasparenza. Anche in questo caso uso una *select* (per la **proiezione**) che selezioni ogni volta un certo numero di colonne da mettere nella nuova tabella

Bisogna quindi garantire:

- **completezza**, ovvero ogni record della relazione R di partenza deve poter essere ritrovato in almeno uno dei frammenti
- **ricostruibilità**, ovvero la relazione R di partenza deve poter essere ricostruita senza perdita di informazione a partire dai frammenti
- **disgiunzione**, ovvero ogni record della relazione R deve essere rappresentato in uno solo dei frammenti
- **replicazione**, l'opposto della disgiunzione

Quindi possiamo definire meglio le proprietà dei due tipi di frammentazione per la relazione R, frammentata in diversi R_i:

1. **orizzontale**:
   - $schema(R_i) = schema(R)$, $\forall i$
   - ogni R_i contiene un sottoinsieme dei record di R
   - è definita da una proiezione su una condizione ci: $\sigma_{ci}(R)$
   - garantisce la completezza, infatti $R_1 \cup R_2 \cup \dots R_n = R$
   - l'unione garantisce la ricostruibilità
2. **verticale**:
   - $schema(R) = L = (A_1, \dots, A_m)$ e $schema(R_i) = L_i = (A_{i1}, \dots, A_{ik})$
   - garantisce la completezza, infatti $L_1 \cup L_2 \cup \dots L_n = L$, dove i vari L_i sono i frammenti verticali ed L è la tabella originale
   - si garantisce la ricostruibilità in quanto $L_i \cap L_j \supseteq chiave\ primaria(R)$, $\forall i \neq j$ (ovvero ogni frammento deve contenere la chiave primaria)

Replicazione

Approfondiamo ora la **replicazione**. Si hanno diversi aspetti positivi per l'accesso *in lettura*, come il miglioramento delle prestazioni in quanto consente la coesistenza di applicazioni con requisiti operazionali diversi sugli stessi dati e aumenta la *località dei dati* usati da ogni applicazioni. Nel momento in cui si ha l'accesso *in scrittura* si hanno però diversi aspetti negativi. Si hanno diverse complicazioni architetturali, tra cui la gestione della transazioni e

l'updates di copie multiple, che devono essere tutte aggiornate. Inoltre bisogna studiare dal punto di vista progettuale cosa replicare, quanto replicare (ovvero capire quante copie mantenere), dove allocare le copie e le politiche per gestirle.
In merito all'allocazione studiamo anche gli **schemi di allocazione**. Ogni frammento può essere allocato su un nodo diverso. Lo schema globale quindi è solo *virtuale* (in quanto non materializzato in un solo nodo) e lo **schema di allocazione** definisce il *mapping* tra un frammento e un nodo. Si ha quindi una tabella, un **catalogo**, che ci da informazioni sul partizionamento, associando ogni frammento al nodo in cui è allocato.

Trasparenza

Con la **trasparenza** si ha la separazione della semantica di alto livello dalle modalità di frammentazione e allocazione. Si separa quindi la *logica applicativa* dalla *logica dei dati* ma per farlo serve uno strato software che gestisca la traduzione dallo schema unico ai sottoschemi, comportando un aumento di complessità del sistema e una perdita di prestazioni (problemi che si riducono con un *mapping* integrato del DDBMS).
Le applicazioni (transazioni, interrogazioni) non devono essere modificate a seguito di cambiamenti nella definizione e organizzazione dei dati e si hanno due tipi di trasparenza, che si applicano agli schemi ANSI-SPARC nel modello distribuito (schema logico globale e schemi logici/fisici locali):

1. **trasparenza logica (o indipendenza logica)**, ovvero in dipendenza dell'applicazione da modifiche dello schema logico. Un'applicazione che usa un frammento non viene modificata se vengono modificati altri frammenti

2. **trasparenza fisica (o indipendenza fisica)**, ovvero in dipendenza dell'applicazione da modifiche dello schema fisico

Frammentazione e allocazione sono tra lo schema logico globale e ogni schema logico locale.
Si hanno quindi tre livelli di trasparenza:

- **trasparenza di frammentazione**, che permette di ignorare l'esistenza dei frammenti ed è lo scenario migliore per la programmazione applicativa con un'applicazione scritta in SQL standard. Il sistema si occupa di convertire query globali in locali e relazioni in sotto-relazioni. La scomposizione delle query per ogni sotto-relazione è detta **query rewriting**

- **trasparenza di replicazione/allocazione**, dove l'applicazione è consapevole dei frammenti ma non dei nodi in cui si trovano. In questo caso la query è già spezzata in quanto si sa di avere a che fare con un sistema frammentato
- **trasparenza di linguaggio**, dove l'applicazione specifica sia i frammenti che i nodi, nodi che possono offrire interfacce che non sono SQL standard. Tuttavia l'applicazione sarà scritta in SQL standard a prescindere dai linguaggi locali dei nodi. Le query vengono quindi tradotte ottimizzatone di query. *Questo è il livello di trasparenza più basso*

3.2 Query distribuite

Analizzeremo prevalentemente DDBMS distribuiti *shared-nothing* e, in seguito, *architetture di replica* (con un *replication server* atto a gestire al replica). Le query sono ovviamente le operazioni più importanti. Possono essere di sola *lettura* (tramite operazioni come la *select*) o anche di *scrittura*. Le due tipologie di operazioni vengono gestite in modo molto differente (la lettura sincrona non è un problema, se non hardware risolvibile con una distribuzione del carico, a differenza della scrittura sincrona). Le operazioni devono essere eseguite **velocemente**.

3.2.1 Accesso in lettura

Studiamo prima le **query in scrittura**.
Esistono, in un sistema relazionale, una serie di attività che convertono la query in SQL in algebra relazionale e solo dopo si ha la distribuzione. L'utente, ignaro dello schema distribuito, interroga lo schema logico globale e il DDBMS decompone la query secondo una localizzazione specifica in base ai singoli frammenti (ovvero deve distribuire la query in modo sensato). Si ha anche un'ottimizzazione globale della query prima della distribuzione in modo che anche la distribuzione stessa sia ottimizzabile correttamente, infatti il gestore delle interrogazioni manda ai singoli nodi i giusti frammenti di query che verranno ottimizzati localmente. Ho quindi nel complesso 4 fasi che compongono il **query processor**:

1. **query decomposition**
2. **data localization**
3. **global query optimization**

4. **local optimization**

Query decomposition

La *query decomposition* opera sullo schema logico globale non tenendo conto della distribuzione. In questo caso si hanno tecniche di ottimizzazione algebrica (usando quindi l'algebra relazionale indipendentemente dalla distribuzione) analoghe a quelle usati in sistemi centralizzati e si ha come output un **query tree** non ottimizzato rispetto ai **costi di comunicazione**. Il costo di comunicazione riguarda il costo di uso della **rete** e dipende da vari fattori. Il costo di comunicazione è il vero "collo di bottiglia" in sistemi distribuiti.

Data localization

La *data localization* considera la frammentazione delle tabelle e la distribuzione, capendo ad esempio dove effettuare le *select* etc.... Si procede quindi all'ottimizzazione delle operazioni rispetto alla frammentazione, tramite **tecniche di riduzione**. Viene quindi prodotta una query efficiente per la frammentazione ma non ottimizzata. Supponiamo per esempio di avere una tabella su 3 nodi (distribuita tramite frammentazione orizzontalmente) e che di base la query faccia la richiesta a tutti e tre (facendo l'unione dei risultati). Usando la tecnica di riduzione, qualora, per esempio, effettivamente sia necessaria solo in un nodo, si avrà che la query sarà distribuita unicamente nel nodo corretto.

Global query optimization

La *global query optimization* si basa sulle statistiche sui frammenti per effettuare l'ottimizzazione. Viene arricchito il **query tree**, creato con gli operatori dell'algebra relazionale, tramite gli **operatori di comunicazione** (ovvero *send* e *receive*), che vengono effettuati tra nodi. Alcune query, dopo aver tenuto conto dei tempi di comunicazione, potranno essere eseguite in parallelo (grazie all'indipendenza data dallo *shared-nothing*). In questo caso le decisione più rilevanti riguardano le operazioni di *join* (che è uno degli operatori più complicati) e,in particolare (come vedremo più avanti), l'ordine tra i *join* n-ari e la scelta tra *join* e *semijoin* (un operatore particolare per i sistemi distribuiti). L'operatore di *join* infatti "ingrandisce" i dati "fondendo" tabelle, che magari sono frammentate in più tabelle su vari nodi. L'uso di *send* e *receive* permette la comunicazione dei dati tra i nodi, anche se questo rischia di diventare troppo esoso in termini di prestazioni. Si hanno quindi degli **algoritmi di calcolo del costo adattivi** e si deve studiare la rete e i suoi

ritardi, che dipendono dalla *topologia* della rete stessa e dal carico applicativo. Si ha quindi una fase di **ottimizzazione a runtime**, dove si riadatta il **query plan**. Per riadattarlo si fa in primis monitoring sull'esecuzione della query, si procede adattando il modello di costo (eventualmente con software automatici) e, eventualmente, riadattando la query se si calcola uno scarto di costo troppo elevato. È il DBA che stabilisce delle soglie temporali entro le quali ottenere una risposta. Per questo conta la trasparenza, in quanto non è l'applicazione che deve interessarsi di questo aspetto. Si introduce un nuovo *layer* di complessità.
In alcuni casi è impossibile ad avere un DDBMS che si occupi di questo tipo di ottimizzazioni.
La distribuzione non è predicibile a priori. Vediamo un semplice esempio:

Esempio 3. *Si supponga di avere il seguente schema:*

- *Employee (eno, ename, title), di cardinalità 400*
- *AssiGN(eno, projectno, resp, dur), di cardinalità 1000 e dove* resp *rappresentata il tipo di responsabilità*

Si ha la seguente query: trovare i nomi dei dipendenti che sono anche manager di progetti:

```
SELECT ename
FROM Employee E JOIN AssiGN A on E.eno=A.eno
WHERE resp=''manager''
```

Che, in algebra relazionale già abbastanza ottimizzata ipotizzando che ci siano pochi manager, sarebbe:

$$\pi_{ename}(EMP >\!<_{eno} (\sigma_{resp=''manager''}(ASG)))$$

Supponiamo di avere poi 5 nodi uguali, il quinto per il risultato e i primi 4 frammentati orizzontalmente secondo questo schema di divisione per nodo:

1. $ASG1 = \sigma_{eno} \leq' E3'(ASG)$
2. $ASG2 = \sigma_{eno} >' E3'(ASG)$
3. $EMP1 = \sigma_{eno} \leq' E3'(EMP)$
4. $EMP2 = \sigma_{eno} >' E3'(EMP)$

Vediamo quindi una prima esecuzione:

- *chiedo al nodo 1 i manager e sposto i risultati di* $\sigma_{resp=''manager''}(ASG1)$ *sul nodo 3 (dove sono descritti in modo più completo) come* $(ASG'1)$*. Il risultato di* $EMP1 >_{eno} (ASG1)$*, calcolato sul nodo 4, lo porto sul nodo 5* $EMP'1$

- *chiedo al nodo 2 i manager e sposto i risultati di* $\sigma_{resp=''manager''}(ASG'2)$ *sul nodo 4 (dove sono descritti in modo più completo) come* $(ASG'2)$*. Il risultato di* $EMP2 >_{eno} (ASG'2)$*, calcolato sul nodo 4, lo porto sul nodo 5 come* $EMP'2$

- *sul nodo 5 il risultato sarà* $EMP'1 \cup EMP'2$

Vediamo una seconda soluzione:

- *contemporaneamente chiedo al nodo 1 e la nodo 3 di mandare al nodo 5 tutti i manager. Sempre contemporaneamente a queste due operazioni chiedo al nodo 2 e al nodo 4 di mandare al nodo 5 tutte le informazioni. I tempi saranno basati sul più lento dei quattro nodi, che determinerà il tempo massimo dell'operazione (che sono circa calcolabili a priori tramite la tabella delle statistiche)*

- *nel nodo 5 calcolo il risultato:*

$$(EMP1 \cup EMP2) >_{eno} \sigma_{resp=''manager''}(ASG1 \cup ASG2)$$

I tempi di trasporto detteranno quale soluzione tra le due è la più performante ma, viste le cardinalità esigue di dati, probabilmente vince la seconda (dove si ha un solo spostamento globale). Questa seconda strategia costringe a pensare a particolari strutture di accesso secondarie dette ***indici****, che permettono interrogazioni efficaci ma che* ***non possono essere "portati"*** *in sistemi distribuiti. Quindi nel nodo 5 non ho gli* ***indici*** *e quindi devo fare l'intero* ***prodotto cartesiano*** *per il join (che però in questo caso ha un tempo trascurabile, grazie alla bassa cardinalità dei dati, rispetto ai costi di trasferimento, generalmente non trascurabili rispetto ai costi delle operazioni interne ad un nodo).*

Riprendendo l'esempio definiamo:

- **costo di messaggio** come il costo fisso di spedizione o ricezione di un messaggio (detto *setup*)

- **costo di trasmissione** come il costo, fisso rispetto alla topologia, di trasmissione dati

- **costo di comunicazione** come la somma tra il costo di messaggio, moltiplicato per il numero di messaggi, più il costo di trasmissione, moltiplicato per il numero di *bytes* trasmessi
- **costo totale** come la somma dei costi delle operazioni (*I/O* e *CPU*) più i costi di comunicazione (*comunicazione*)
- **response time** come la somma dei costi qualora si tenga conto del *parallelismo delle trasmissioni*, quindi come la somma tra il costo di messaggio, moltiplicato per il numero di messaggi comunicati in modo sequenziale, più il costo di trasmissione, moltiplicato per il numero di *bytes* trasmessi in modo sequenziale. In questo conto volendo posso usare dei **pesi** basati sulla cardinalità delle unità da trasferire e tenere conto del massimo tempo di risposta che si ottiene

Si ha quindi che:

- nelle **grandi reti geografiche** i costi di *comunicazione* sono molto maggiori del costo di *I/O*, circa di 10 volte
- nelle **reti locali** i costi di *comunicazione* e *I/O* sono paragonabili, grazie alle reti *gigabit* in locale

Tendenzialmente il costo di comunicazione è ancora il **fattore critico** ma sempre meno.
Bisogna scegliere cosa **minimizzare**:

- il *response time*, aumentando il parallelismo che però può portare ad un aumento del *costo totale*, con un maggior numero di trasmissione e un maggior processing locale. Nell'esempio 3 potrebbe sembrare la seconda soluzione, che effettivamente parallelizza di più ma non minimizza i costi di risposta
- il *costo totale*, senza tener conto del parallelismo utilizzando meglio le risorse e aumentando il *throughput* ma peggiorando così il *response time*. Nell'esempio 3 è la prima soluzione

Join e Semijoin

Il **join** presenta il problema di portare alla perdita dell'**indice**. Bisogna quindi studiare come effettuare l'operazione tra due tabelle su due nodi diversi. Una prima operazione è data dell'operazione di *semijoin*.

Definizione 2. *Definiamo, in algebra relazionale, l'operazione semijoin, tra due tabelle R e S, sull'attributo A, come:*

$$R \ semijoin_A \ S \equiv \pi_{R^*}(R \ join_A \ A)$$

dove R^* è l'insieme degli attributi di R.
In altre parole scelgo esplicitamente di tenere solo gli attributi di R dopo il semijoin.
Quindi con $R \ semijoin_A \ S$ ho la proiezione sugli attributi di R operazione di join e quindi ho che il semijoin non è ***commutativo****.*
Dalla seconda tabella porto solo la serie di attributi che mi servono esplicitamente ($\pi_A(S)$) riducendo il carico di lavoro.
Alla fine il nostro R' con i risultati del semijoin sarà trasportato nel nodo di S

Prese due tabelle allocate su nodi differenti, il *join* tra di esse può quindi essere calcolato tramite operazioni di *semijoin*, valgono infatti le seguenti equivalenze (che portano a diverse strategie a seconda della stima dei costi):

- $R \ join_\theta \ S \iff (R \ semijoin_\theta \ S) \ join_\theta \ S$
- $R \ join_\theta \ S \iff R \ join_\theta \ (S \ semijoin_\theta \ R)$
- $R \ join_\theta \ S \iff (R \ semijoin_\theta \ S) \ join_\theta \ (A \ semijoin_\theta \ R)$

In tutti i casi si riduce lo spostamento dei dati.
L'uso del *semijoin* è conveniente sse il costo del suo calcolo e del trasferimento del risultato è inferiore al costo del trasferimento dell'intera relazione e del costo dell'intero *join* (e questo dipende dal numero di attributi coinvolti).
Avere più di un join complica la situazione, anche solo per la scelta dell'ordine in cui eseguirli.

Local optimization

La *local optimization* si occupa dell'ottimizzazione degli schemi locali. Ogni nodo riceve una *fragment query* e la ottimizza, con tecniche analoghe ai sistemi centralizzati, in modo completamente indipendente. Si hanno comunque operazioni di ottimizzazione locale a priori sul fatto che il *global query optimization* punti a ridurre i costi di comunicazione (nel caso di un DDBMS in rete geografica) o ad aumentare il parallelismo (in caso di DDBMS in rete locale).
In ogni caso nella progettazione di sistemi di gestione dati distribuiti bisogna tener conto di:

- tipologie di query distribuite
- stime o statistiche sullo storico query distribuite già eseguite (fatto periodicamente dal DDBMS)
- topologia della rete
- carico aspettato e workload previsto

3.2.2 Accesso in scrittura e controllo di concorrenza

In questo caso la situazione si complica. Un conto è avere delle **remote requests (read-only)**, che possono essere un numero arbitrario di query SQL in sola lettura, un altro è avere delle **remote transactions (read-write)**, ovvero un numero arbitrario di operazioni SQL che prevedono anche *insert* e *update*. Ragionando in un'ottica in cui si ha un numero arbitrario di server si parla di **distribuited requests**, dove ogni singola operazione SQL si può riferire, grazie ad un *ottimizzatore distribuito*, a qualunque insieme di server, e di **distribuited transactions**, dove ogni operazione è diretta ad un unico server e dove le transazioni possono modificare più di un db, tutto ciò grazie ad un *protocollo transazionale di coordinamento distribuito*, detto **two-phase commit** (in questo caso si ha spesso a che fare con sistemi *eterogenei* e *federati*). Deve valore la **proprietà di atomicità** di *ACID*. Sempre riguardo *ACID* si ha che la **proprietà di consistenza** non dipende dalla distribuzione, in quanto le proprietà sono indipendenti dall'allocazione, e si ha che la **proprietà di durabilità** viene garantita localmente. Vanno invece rivisti architetturalmente la **proprietà di atomicità**, tramite componenti come il *reliability control* e il *recovery manager* (in caso di guasti), e la **proprietà di isolamento**, tramite il *concurrency control* (senza il quale si può incorrere in *update fantasma*, dove un *update* viene cancellato da uno seguente).
Rivedendo i **principi del controllo di concorrenza**.

Definizione 3. *Data una transazione t_i si ha che essa viene scomposta in sotto-transazioni t_{ij} a seconda del nodo j-simo su cui viene eseguita. A sua volta una transizione t_{ij} viene nominata r_{ij} per le operazioni di lettura e w_{ij} per le operazioni di scrittura. L'uso di una risorsa x viene indicata, per esempio, con $r_{ij}(x)$ o $w_{ij}(x)$.*

Ogni sotto-transazione viene schedulata in modo indipendente di server di ciascun nodo e quindi la **schedule globale** (dove *schedules* indica le sequenze delle transazioni da eseguire) dipende dalle **schedules locali** di ogni nodo.
Purtroppo **la serializzabilità locale di ogni schedule non garantisce**

la sua serializzabilità globale. Si viene a creare un **grafo globale dei conflitti** in quanto i conflitti non sono a livello locale ma a livello globale (infatti si hanno risorse occupate tra i vari nodi, si arriva, in certi casi, ad una **situazione di deadlock**).
Si ha quindi che lo *schedule globale* è serializzabile sse **gli ordini di serializzazione sono gli stessi per tutti i nodi coinvolti** (nel caso in cui il db non sia replicato).
Qualora si abbia un db replicato si aggiunge un altro problema qualora le scritture riguardino due repliche diverse. In tal caso si può violare la **mutua consistenza** (che dice che al termine della transazione tutte le copie devono avere lo stesso valore) dei due db locali, anche con due schedule localmente seriali. Si introduce quindi un **protocollo di controllo delle repliche**. Il **protocollo di controllo delle repliche** viene chiamato **ROWA (*Read Once Write All*)**. In base a questo protocollo, dato un item logico X (con $x_1 \dots x_n$ items fisici), si ha che le transazioni vedono solamente X ed è il protocollo che si occupa di mappare *read(X)* su una copia qualunque e *write(X)* su tutte le copie. Questo meccanismo torna utile nell'uso standard delle repliche, permettendo al client di leggere dal nodo più vicino ma imponendo, eventualmente, la scrittura su tutte le copie e bloccando le operazioni fino a quando l'ultima scrittura non è avvenuta. Si hanno purtroppo problemi di perdita di prestazioni a causa di questa scrittura "di massa". Per lo stesso problema si hanno anche condizioni di rilascio tramite *protocolli asincroni*.

3.2.3 2 phase locking

Anche l'**algoritmo 2PL (*2 Phase Locking*)** viene esteso al caso di schemi distribuiti. Si hanno due possibili strategie:

1. **primary site**, *centralized*, in quanto basata sui siti
2. **primary copy**, in quanto basata sulle copie

2PL prevede che prima di rilasciare un *lock* debba averli richiesti tutti, e nello *stricted 2PL* solo dopo che sia anche stato effettuato il *commit*.
Nel caso di *centralized 2PL* si ha un **lock manager (LM)** per ogni nodo, è un'architettura "master-slave". Il "master" è appunto il *lock manager* che gestisce i *lock* per l'intero db distribuito. Gli "slave" sono invece i *data processor*, che seguono quanto fa il *lock manager coordinatore* (che se non è disponibile per problemi tecnici del nodo comporta seri problemi in quanto la scelta di un nuovo *lock manager* tra quelli di ogni nodo è parecchio complicata).
Si ha inoltre che il **transaction manager (TM)** del nodo in cui inizia la

transazione sarà ritenuto il *TM coordinatore* dei transaction manager. La transazione anche in questo caso sarà eseguita dai *data processor* nei vari nodi. Il TM coordinatore formula all'LM coordinatore le richieste di *lock*, che vengono concesse tramite l'*algoritmo 2PL*. Una volta concesse il TM coordinatore le comunica ai vari *data processor*, assegnando ad essi i vari lock e l'accesso ai dati. AL termine delle operazioni i *data processor* comunicheranno il termine al TM coordinatore che a sua volta lo comunicherà all'LM coordinatore, che rilascerà i lock. Si ha però un effetto "collo di bottiglia" sul nodo del LM che deve gestire moltissime richieste e fino a che non risponde sistema va in *wait*. Una soluzione a questo problema è individuata nella tecnica della **copia primaria**. Prima dell'assegnazione del *lock*, viene individuata per ogni risorsa una *copia primaria*. Inoltre si ha che i diversi nodi hanno diversi *lock manager* attivi, ognuno che gestisce una partizione dei lock complessivi, relativi alle risorse primarie residenti nel nodo. Inoltre, per ogni risorsa nella transazione, il TM comunica le richieste di lock al LM responsabile della copia primaria, che assegna i *lock*. Si evita quindi il "collo di bottiglia" ma è necessario determinare a priori il LM per ogni risorsa. Inoltre si necessità di una **directory globale** dove tutti i nodi "vedono tutto".

3.2.4 Gestione dei deadlock

Indipendentemente da quanto appena discusso si può creare un'**attesa circolare** tra transazioni di due o più nodi. Bisogna quindi applicare un algoritmo distribuito. Per costruire l'algoritmo dobbiamo ragionare che siamo in una "rete tra pari" *Peer-to-Peer* (e non "master-slave") e quindi bisogna definire un protocollo su cui costruire l'algoritmo *asincrono e distribuito*. L'algoritmo potrebbe partire su uno qualsiasi dei nodi.
Si ipotizza innanzitutto che tutte le sotto-transazioni siano attivate in modo sincrono, tramite *Remote Procedure Call (RPC)* bloccante, ovvero una transazione chiede di fare un'operazione su un certo nodo facendo una RPC ad un altro nodo, mettendosi in attesa fino a che non finisce. Si possono generare due tipi di attesa:

1. **attesa da RPC**, una sotto-transazione su un nodo attende un'altra sotto-transazione, della stessa transazione, su un altro nodo

2. **attesa da rilascio di risorsa**, una sotto-transazione su un nodo attende un'altra sotto-transazione, della stessa transazione, sullo stesso nodo a causa del rilascio di una risorsa (che normalmente è la tipica situazione che porta ad un deadlock in un sistema centralizzato)

La composizione dei due tipi di attesa può generare un **deadlock globale**. E' possibile caratterizzare le condizioni di attesa su ciascun nodo tramite condizioni di precedenza e serve quindi specificare qualche notazione, per rappresentare il fatto che ogni nodo deve capire quali sono le transazioni sono in attesa per una chiamata esterna o per l'accesso ad una risorsa interna:

- EXT_i per una chiamata all'esecuzione di una transazione sul nodo i
- $x < y$ per indicare che x sta aspettando il rilascio di una risorsa da parte di y (che può essere anche EXT)
- indichiamo quindi la **sequenza di attesa generale** al nodo k come:
$$EXT < T_{ik} < T_{jk} < EXT$$

Esempio 4. *Sul DBMS1 si ha:*

$$EXT2 < T_{21} < T_{11} < EXT2$$

e sul DBMS2:

$$EXT1 < T_{12} < T_{22} < EXT1$$

ovvero sul nodo 2 c'è la transazione 1 che sta aspettando che finisca. La transazione 1 sul nodo 1 sta aspettando che la transazione 2 sul nodo 1 finisca, che a sua volta sta aspettando che la transazione sul nodo 2 finisca. Però sul DBMS2 scopriamo che la transazione 1 sul nodo 1 è in attesa della transazione 2 sul nodo 2 finisca. Quest'ultima sta aspettando che finisca la transazione 1 sul nodo 2 che a sua volta attende la transazione sul nodo 1. Si ha quindi un ***deadlock distribuito****, rappresentato nell'immagine 3.1.*

Per risolvere il problema del **deadlock distribuito** ogni nodo, ad un certo punto con un suo ordine temporale, prende la sua sequenza di attesa e la aggiunge ad alle condizioni di attesa locale degli altri nodi legati da EXT. Dopodiché analizza la situazione, rilevando potenziali **deadlock locali**, e comunica le sequenze di attesa alle altre istanze dell'algoritmo, ovvero agli altri nodi. Qualora si abbia un *deadlock locale* si crea un grafo dedicato allo stesso dove sarà possibile notare un ciclo, che rappresenta il deadlock. Ovviamente è possibile evitare che due nodi scoprano lo stesso deadlock, rendendo così quindi più efficiente l'algoritmo che invia le sequenze di attesa solo in alcuni modi:

1. **in avanti**, verso il nodo dove è attiva la sotto-transizione attesa (nodo nel quale vede che non ci siano deadlock (???)). Nei sistemi

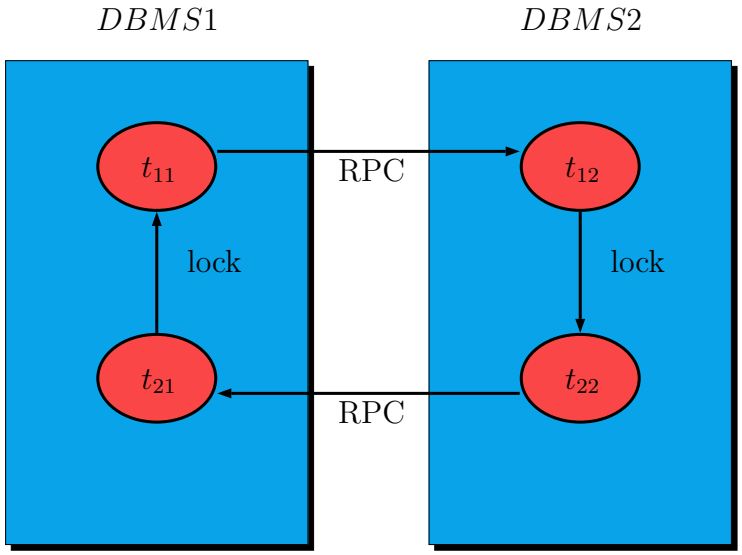


Figura 3.1: Grafico dell'esempio di deadlock distribuito

Peer-to-Peer questi sono meccanismi *coreografati*, decisi a priori. *Esempio alla slide 68 del quarto PDF della costruzione di un grafo delle transazioni con presenza di ciclo*

2. solamente quando l'identificatore del secondo nodo attende il rilascio della risorsa identificatore del primo nodo

3.2.5 Recovery management

Approfondiamo quindi come garantire la **proprietà di atomicità**.
Abbiamo visto come uno dei guasti possibili in un sistema distribuito sia quello legato alla perdita di messaggi sulla rete, nonché al partizionamento delle stessa (comportando magari l'isolamento dei nodi). Ricapitolando abbiamo diversi tipi di guasti:

- **guasti nei nodi**, sia *soft* che hard
- **perdita di messaggi**, che lascia l'esecuzione di un protocollo in uno stato di *indecisione*, in quanto ogni messaggio del protocollo è seguito da un *ack* e la perdita o del messaggio o dell'*ack* stesso genera incertezza (non potendo decidere se il messaggio sia arrivato o meno)
- **partizionamento della rete**, dove una transazione distribuita può essere attiva contemporaneamente su più sotto-reti temporaneamente isolate. In questa situazione i singoli nodi non riescono

a capire bene chi sia isolato e la cosa può portare i nodi a fare scelte contraddittorie

Si è quindi studiato il **protocollo two phase commit (*2PC*)** che cerca di funzionare in presenza di guasti di rete. Questo tipo di protocollo consente ad una transizione di giungere ad un eventuale *commit* o *abort* su ciascuno dei nodi che partecipano alla transazione. In questo protocollo la decisione di *commit* o *abort* tra due o più **resource managers (RM)** (i server) viene certificata da un **transaction manager (TM)** (il coordinatore). Lo scambio dei messaggi (e il salvataggio di un log per ciascuno) tra TM e RMs è ciò su cui si basa il protocollo 2PC. Si ha quindi sempre un'architettura "master-slave" (in modo metaforico si può rappresentare come il prete che unisce in matrimonio i due sposi). Si ha quindi il TM che interroga i RMs riguardo allo stato della loro esecuzione.

2PC in assenza di guasti

Si hanno diverse fasi:

1. durante la prima fase il TM interroga (con un *prepare* o *ready_to_commit*) tutti i nodi per capire come ciascun nodo intenda terminare la transazione, autonomamente o irrevocabilmente *commit* o *abort* (magari per violazione della concorrenza locale o per violazione di qualche vincolo di consistenza etc...). I nodi risponderanno quindi o con *ready_to_commit* o con *not_ready_to_commit*

2. nella seconda fase il TM prende la decisione globale. Si ha che se anche solo un nodo richiede un *abort* allora si avrà *abort* per tutti i nodi, altrimenti *commit*, chiudendo la transazione. Il TM si occupa anche di comunicare ai RMs la decisione finale per poter procedere con le azioni locali

Le fasi sono schematizzate in figura 3.2.
Come abbiamo detto precedentemente si ha la raccolta di *log* nei quali compaiono due tipi di record:

1. **record di transazione**, con le informazioni sulle operazioni effettuate

2. **record di sistema**, con l'evento di *checkpoint* e di *dump* (ovvero la copia esatta del db in un certo stato)

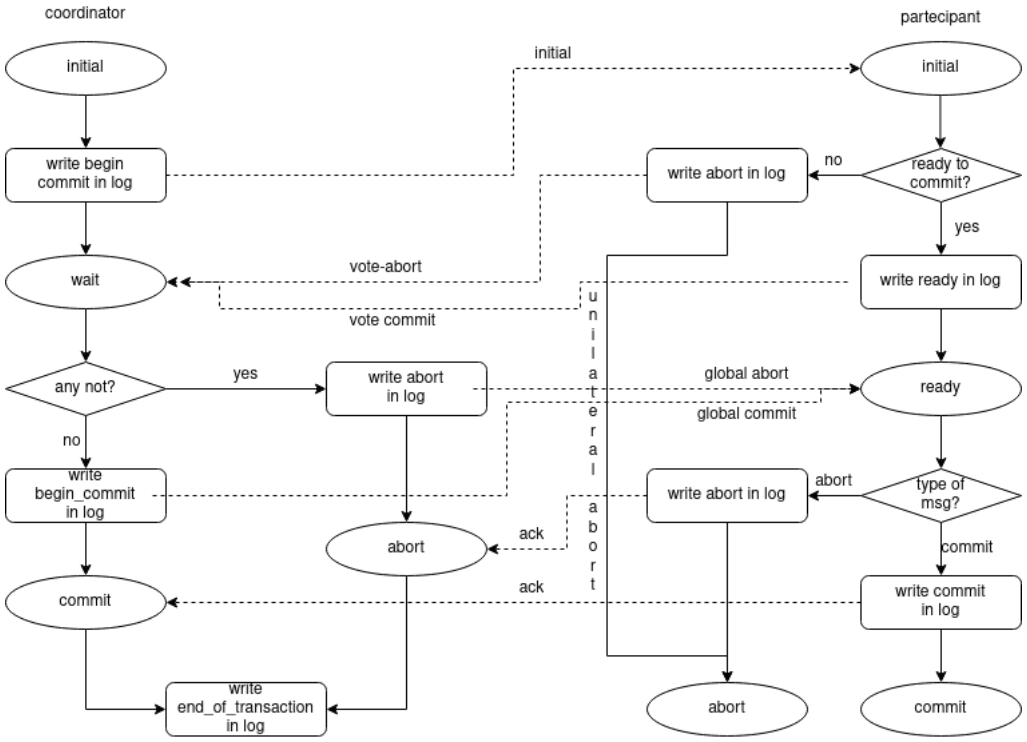


Figura 3.2: Diagramma del protocollo 2PC, dove negli ovali abbiamo le *decisioni* e nei rettangoli le *azioni sui log*. Entrambi i tipi di frecce indicano un *messaggio*. La prima fase è fino alle decisioni globali incluse.

Le scritture sui log avvengono prima della decisione delle operazioni, che a loro volta si suddividono in *prepare* e *global decision*. Ai log del TM vengono aggiunti ulteriori dettagli:

- **prepare record** (in figura 3.2 *begin_commit*) che contiene l'identità (nodi e transazioni) di tutti i RMs
- **global commit** o **global abort** che descrive la decisione globale. La decisione del TM diventa esecutiva quando scrive nel proprio log **global commit** o **global abort**
- **complete record** (in figura 3.2 *begin_of_transaction*), che viene scritto alla fine del protocollo

Al log dei RMs vengono aggiunti ulteriori dettagli:

- **ready record**, per segnalare la disponibilità irrevocabile a partecipare alla fase di commit. Si hanno diverse politiche sul **pro-**

tocollo 2PL (*recoverable, 2PL, ACR, strict 2PL*). Inoltre questo log contiene l'indicazione del TM e i records (come nel caso centralizzato), ovvero *begin, insert, delete, update, commit*

- **not ready record** (in figura 3.2 *abort*) per segnalare l'indisponibilità del RM al commit

In entrambe le fasi del 2PC possono avvenire guasti e in entrambe tutte le componenti devono poter decidere in base al loro stato. Viene quindi introdotto l'uso di **timers**, stabilendo un **timeout** entro il quale il TM aspetta una risposta (in entrambe le fasi, anche se nella prima è più importante). Se il timeout viene superato si lancia un *abort*. Vediamo distinte le due fasi

1. il TM scrive *prepare* nel suo log e invia *prepare* ai RMs, fissando un timeout massimo per le riposte. Gli RMs *recoverable*, ovvero pronti al *commit*, scrivono *ready* nel loro log e inviano *ready* al TM. Gli RMs non *recoverable*, ovvero non pronti al *commit* a causa di un deadlock, scrivono *not-ready* nel loro log e terminano il protocollo, con un *log unilaterale*. Il TM, come detto scrive nel suo log **global commit** o il **global abort**, il secondo nel caso in cui ci sia anche solo un *not-ready* o che scatti il timeout (assumendo che i nodi che non hanno risposto siano in *failure*).

2. il TM trasmette la decisione globale e fissa un secondo *timeout*. Gli RMs *ready* agiscono di conseguenza scrivendo *commit* o *abort* nei loro log e inviando un *ack* al TM. Solo dopo effettuano in locale *commit* o *abort*. Il TM raccoglie gli *ack* e, in assenza di qualche risposta, fissa un nuovo *timeout* ripetendo la trasmissione per gli RMs problematici. Questo fino a che non avrà ricevuto da tutti un *ack* e in quel momento scrive *complete* nel suo log

Abbiamo quindi appena visto un **paradigma centralizzato** "master-salve" dove i vari RMs non comunicano tra loro. Il TM è quindi il collo di bottiglia". Si hanno altri paradigmi:

- **lineare**, dove gli RMs hanno un ordine prestabilito e comunicano sempre secondo un ordine prestabilito. Il TM è solo il primo di tale ordine. Questo paradigma è utile per reti senza possibilità di *broadcast*

- **distribuito**. In questo caso nella prima fase il TM comunica coi vari RMs, che però rispondono a tutti. I vari RMs decidono in base alle informazioni ricevute dagli altri RMs (comunicano

tra loro in *broadcast*) e quindi non è più necessaria la seconda fase di *2PC*. Si genera una gran quantità di messaggi tra i vari RMs, avendo una situazione "tra pari" *Peer-to-Peer*, creando un problema di prestazioni, dovendo garantire la comunicazione tra tutti i nodi (anche tramite *ack*)

2PC in caso di guasto

In uno stato di guasto, nel caso **centralizzato**, un RM nello stato *ready* perde la sua autonomia e attende la decisione del TM. Nel caso di guasto del TM i vari RMs sono lasciati in *stato di incertezza* e le risorse allocate alla transazione restano bloccate.

Definizione 4. *Definiamo* ***finestra di incertezza*** *come la finestra temporale fra la scrittura di ready nel log dei RMs e la scrittura di* commit *o* abort*. Questo intervallo è ridotto al minimo da* ***2PC****.*

Durante la finestra di incertezza tutte le risorse acquisite tramite meccanismi di *lock* restano bloccate e, in caso di guasto durante la *finestra di incertezza*, TM e RMs usano i **protocolli di recovery**.
Si possono avere diversi guasti:

- **guasti di componenti**, ovvero guasti al TM o ai RMs.
- **perdita di messaggi o partizionamento della rete**

Guasti di componenti In questo caso devono essere usati protocolli con due compiti:

1. assicurare la terminazione delle procedure. Sono i **protocolli di terminazione**
2. assicurare il ripristino. Sono i **protocolli di recovery**

In entrambi i casi questi protocolli funzionano sia che il guasto interessi un solo componente che più di uno.
Partiamo dal caso in cui cada un RM. Può cadere prima di iniziare il protocollo, non rispondendo al *prepare* e portando all'*abort*. Può cadere dopo il *ready_to_commit* e se quando si riprende vede nei log lo stato *ready* si mette in *wait* non sapendo bene come fare (nel caso di *abort* semplicemente chiuderà il protocollo). Il TM provvederà a inviare a tale RM *commit* o *abort*. Non si hanno quindi problemi al protocollo, o si va diretti all'*abort* o si aspetta. Il TM capisce che un RM è caduto grazie al *timeout*.

Più complesso è il caso in cui cada il TM. Se cade prima di ricevere le risposte al *prepare*, quando si sarà ripreso, guarderà lo stato delle risposte al *prepare* ricevute, altrimenti si avrà un *abort unilaterale*.
Vengono introdotti gli **algoritmi bizantini** nel caso in cui il TM cada e il RMs debbano decidere insieme cosa fare. Per decidere serve visibilità.
Quindi, ricapitolando per le cadute del TM:

- cade quanto l'ultimo record del log è *prepare*, magari bloccando alcuni RMs. In tal caso si hanno 2 opzioni di recovery:
    1. decidere *global abort*, e procedere con la seconda fase di 2PC
    2. ripetere la prima fase, sperando di giungere a un *global commit*, richiedendo nuovamente lo stato dei RM
- cade quanto l'ultimo record del log è *global-commit* o *global-abort* il TM deve ripete la seconda fase in quanto alcuni RMs potrebbero essere bloccati o comunque ignari della decisione presa prima della caduta
- l'ultimo record nel log è una *complete*, in tal caso non si hanno problemi

Ricapitoliamo anche le cadute dell'RM:

- l'ultimo record nei log è di *azione*, *abort* o *commit*, come nel caso centralizzato e in tal caso di procede con un **warm restart**:
    - nel caso di *abort* o *azione* si procede con l'*undo* dell'operazione
    - nel caso di *commit* di effettua nuovamente la transazione
- l'ultimo record nei log è *ready* e in tal caso l'RM si blocca non conoscendo la decisione del TM e si inseriscono, durante *warm restart*, nel *ready set* le transazioni dubbie. Si hanno quindi due alternative:
    1. **remote recovery**, ovvero l'RM chiede al TM cosa è accaduto
    2. il TM riesegue la seconda fase del protocollo

Perdita di messaggi e partizionamento della rete In questo caso il TM non riesce a distinguere tra perdita di messaggi *prepare* o *ready* nella prima fase e procede, scattando i *timeout*, con un **global abort**.
Durante la seconda fase la non distinzione tra perdita di *ack* o di decisioni dei gli RM porta alla ripetizione della seconda fase dopo il *timeout*.
Se durante lo svolgimento del protocollo 2pc si partiziona la rete avendo due sottoreti una con TM e RM1 che e la seconda sottorete con RM2, RM3. In questo caso il TM continua a mandare il messaggio della global decision a RM2 RM3 dopo lo scadere del timeout. Si concluderà comunque, con alte probabilità, con un *abort* da parte del TM.

Ottimizzazioni di 2PC

2PC può essere ottimizzato per:

- ridurre il numero di messaggi tra TM e RMs
- ridurre le scritture nei log

Si hanno due tipi di ottimizzazione:

1. **ottimizzazione read-only**, quando un RM sa che se la propria transazione è *read-only* allora non influenza l'esito finale della transazione. Al *prepare* risponde *read-only* e termina il protocollo. Il TM ignora i partecipanti *read-only* dalla seconda fase e, qualora si sapesse a priori, possono anche essere direttamente esclusi dal protocollo
2. **ottimizzazione presumed abort** che si basa sulla regola "scordarsi gli *abort* e ricordasi i *commit*". In questo caso il TM abbandona la transazione dopo la decisione di abort senza scrivere *global abort* nel log e senza aspettare risposta dai vari RMs. Se il TM riceve richiesta di un *remote recovery* il TM decide per il *global abort*. Non sarà più necessario quindi scriver e*global abort* o *prepare* nei log ma solo *global commit, ready* e *commit*

Protocollo X/Open

Il protocollo 2PC è stato adottato nel protocollo **X/Open DTP (*Distributed Transaction Processing*)**, che è un consorzio di vendors che vogliono rendere portabile lo standard dell'ambiente UNIX. In questo protocollo si ha il *TX interface* per la comunicazione tra il TM e l'applicazione e si ha l'*XA interface* per la comunicazione tra TM e RMs. Ogni vendor ha la sua implementazione del modello.

3.3 Repliche

Parliamo ora delle tecnologie per la **replicazione di dati**.
Tra le principali soluzioni architetturale troviamo **IBM replication technologies** e **Microsoft SQL Server replication technologies** (*i dettagli delle implementazioni non saranno oggetto d'esame*).

Definizione 5. *La **replica** è il processo di cerare e mantenere istanze dello stesso db allineate tra loro, consentendo la condivisione di dati ma anche comportando cambiamenti architetturali. Si ha che le eventuali modifiche devono essere viste da tutti i nodi.*

Definizione 6. *Definiamo **sincronizzazione** è il processo che m i consente di allineare le copie, prima o poi.*

In base all'ultima definizione si capisce che spesso le copie non sono aggiornate istantaneamente. Si ha quindi la **replica sincrona** o la **replica asincrona** (non avendo allineamento *realtime*). IBM preferisce un approccio *based and mode based* mentre Microsoft uno basato su *snapshot, transactional* e *merge*.
Vediamo le differenze tra le due repliche:

- le **repliche sincrone** cercano di far si che tutte le repliche vengano aggiornate contemporaneamente (ad esempio si ha il protocollo ROWA). Scrivo in modo sincrono su tutti nodi e solo quando tutte le repliche confermano la scrittura avanzo con le transazioni (che fallisce se ho nodi non disponibili). Nelle repliche sincrone si necessitano molti scambi di messaggi. Di fatto si obbliga due o più *storage* ad aggiornarsi e a fare *rollback* in caso di fallimento. Si hanno quindi alte disponibilità, un auto *fail-over* (bloccando la transazioni in caso di guasti sui nodi) e un *data loss* minimo. Le repliche sincrone vengono soprattutto usate nei *disaster recovery*, ovvero in situazioni *mission critical* (ad esempio sistemi bancari dove i db di backup, almeno 3, devono stare a centinaia di kilometri di distanza, in zone sismiche tra loro diverse). Gli svantaggi delle repliche sincrone sono la necessità di una rete valida, si hanno problemi di scalabilità, di costi e minor flessibilità

- nelle **repliche asincrone** prima si aggiorna il db *target* e poi le repliche (normalmente dopo pochi secondi ma anche dopo giorni). Si hanno evidenti vantaggi di costo, scalabilità e flessibilità (perché in caso di problema lavoro in primis sul db principale) ma a

rischio di *data loss* (nell'intervallo di tempo tra la scrittura del db principale e delle repliche). Normalmente si usano soluzioni asincrone per accessi online e la loro efficienza, per bilanciamento del calcolo etc...

In caso di perdita di dati bisogna analizzare i singoli contratti per capire legalmente come rispondere di dati che non verranno recuperati probabilmente.
Ci sono vari contesti in cui pensare alla replica dei dati:

- condivisione di dati da utenti tra loro scollegati. Un esempio è una copia su un portatile con una replica usata da un commerciale. Si possono avere conflitti nel momento in cui più utenti con db replicati lavorano offline. Si ha il *merge conflict*
- *data consolidation*, ovvero quando un'azienda vuole tenere più copie dei dati in vari punti e alla fine bisogna riportare i dati a livello centrale a cadenza periodica. Può servire per fare data warehousing o anche solo semplicemente per monitorare le vendite delle varie filiali o per aggiornare il catalogo
- *data distribution* che è il caso degli *e-commerce*. È un caso tipicamente *mission-critical* e bisogna aumentare l'accesso ai dati e si ha una costante sincronizzazione realtime bidirezionale per evitare problemi. Un altro caso è la distribuzione tra diversi uffici, dove le repliche locali hanno magari dati non presenti nel db globale
- prestazioni, accesso efficiente, *load balancing* e accesso offline. Se non si hanno necessità di update immediati (tipo un sito vetrina) allora la replica garantisce la disponibilità e l'accessibilità a basso costo. Con il load balancing scarico gli utenti su diverse macchine replicate, in primis per le molte realtà di sola lettura o comunque con pochissime scritture (un esempio può anche essere un social network dove anche eventuali ritardi di qualche secondo non sono problematici). Per la disponibilità bisogna fare un forte testing dell'intera architettura, se cade un server bisogna puntare ad una replica e bisogna essere sicuri e spesso i costi sono troppo alti (*RIVEDERE QUESTA PARTE*)
- separazione tra *data entry* e *reporting*, se si usa lo stesso server per entrambi i compiti (che in pratica sono scrittura costante e lettura costante) può essere utile separare in due server. Si evitano così i rallentamenti dati dai *lock*. Bisogna studiare i tempi di sincronizzazione

- coesistenza di applicazioni, questo è un caso particolare. Qualora sia necessario cambiare applicazione devo, eventualmente, cambiare anche i sistemi. Bisogna quindi travasare i dati vecchi e durante il trasferimento bisogna comunque mantenere funzionanti le applicazioni. Quindi bisogna far coesistere i due database durante il trasferimento (facendo il travaso di notte bloccando le transazioni). I costi sono incredibili e si può avere anche coesistenza delle applicazioni e non solo dei dati, con migrazioni parziali (magari per area geografica) etc... questo comporta che magari due filiali devono collaborare con due applicazioni e due db diversi

Ci sono anche casi in cui non si dovrebbe replicare:

- quando ci sono frequenti update su più copie, portando le copie a possibili conflitti che devono essere scoperti e gestiti "manualmente"
- quando la consistenza è *critical* magari in contesti di trasferimento di fondi etc.... In questo caso solitamente si impone un protocollo ROWA (con transazioni *ACID compliant*), riducendo le prestazioni per avere l'autorizzazione dei *commit* da parte delle repliche

Ma spesso bisogna comunque replicare "scegliendo il male minore" (ad esempio nelle banche) e bisogna quindi analizzare il singolo caso, anche in base al budget. Inoltre non bastano le tecnologie serve un'ottima organizzazione.
Concludendo si ha che i benefici della replica sono:

- disponibilità
- affidabilità
- prestazioni
- riduzione di carico
- lavoro offline
- supporto a molti utenti

Distinguiamo anche delle classi di tipologie di replica:

- **data distribution**, di tipo *1:many*, con un *source* che distribuisce, in modo sincrono o asincrono, le varie copie passive ai *target*

- **Peer-to-Peer**, dove i vari nodi sono interconnessi e si aggiornano tra di loro. Si usa un approccio ROWA
- **data consolidation**, di tipo *many:1*, dove ho più *source* che aggiornano un *target* a livello centrale
- **bi-directional** (per il *conflict detention resolution*), dove una copia primaria e uno secondaria possono leggere e scrivere a vicenda tra loro (è quindi una versione semplificata del *Peer-to-Peer* con due Peer)
- **multi-Tier staging**, in cui si hanno meccanismi intermedi tra *source* e *target* con "aree di deposito" dette aree di *staging*

Per realizzare una replica posso fare in diversi modi:

- faccio letteralmente il backup del disco con una persona che stacca il disco dal server e lo copia, riattaccando infine copia e disco originale
- posso prima fare il backup attaccando un altro disco e poi mettere nella nuova macchina il disco copia
- posso fare una *replica incrementale*, ovvero faccio un *full backup* e sposto solo il file di *log* delle transazioni nel nuovo server, rieseguendo quanto fatto (essendo contenuto nel *log*). Quindi prima faccio un *full backup* e poi un *backup* del *log*, questo per ogni replica. Un'alternativa è l'**event publish**. Un **event publish** è una replica senza *apply* e leggo i file di log. Analizzando gli eventi tramite particolari meccanismi riscrivo quindi sull'architettura target. Da un *publisher* si passa ad un *distributor* e infine ai *subscriber*

Sulle slide *repliche* si ha un approfondimento delle architetture IBM e Microsoft opzionali per il corso.

Un **db parallelo** è studiato per le prestazioni. Si ha accesso parallelo ai dati, parallelismo *intra-query* (stessa query su frammenti diversi), parallelismo *inter-query* (tante query diverse) e sono fatti da elementi hardware posti vicini tra loro.
Parliamo di **persistenza dei dati**. Bisogna garantire la durabilità dei dati,

bisogna quindi usare un db. Si hanno anche problemi per creare oggetti persistenti a partire da un linguaggio OOP, si ha il cosiddetto l'**object-relational paradigm mismatch**. Si separa quindi l'aspetto OOP e l'aspetto relazionale per risolvere il problema per poi "mappare" l'uno nell'altro, tramite i **data mapper**. Si hanno operazioni **CRUD**:

- Create
- Read
- Update
- Delete

Si ha quindi il cosiddetto **Object–relational mapping**, ovvero questa tecnica di mapping. Si hanno vari framework che lo implementano.
Storicamente si è provato a fare db ad oggetti ma con scarsi risultati.

3.4 Prima esercitazione

Esercizio 1. *Si consideri un db con le seguenti relazioni (e quindi tabelle):*

- *PRODUCTION (SerialNumber, PartType, Model, Quantity, Machine)*
- *PICKUP (SerialNumber, Lot,* ***Client, SalesPerson****, Amount)*
- *CLIENT (Name, City, Address)*
- *SALESPERSON (Name, City, Address)*

(con sottolineate le chiavi primarie e in grassetto le chiavi di integrità referenziale)

e ci poniamo l'obiettivo di partizionare il db secondo determinate specifiche.
Si assume che si abbiano le seguenti specifiche organizzative:

- *si hanno 4 centri di produzione (Dublino, San Jose, Zurigo* e *Taiwan, ciascuno responsabile, rispettivamente, di cpu, keyboard, screen* e *cable) e 3 centri di vendita (San Jose, Zurigo* e *Taiwan)*

- *le vendite sono distribuite secondo le località geografiche, i clienti a Zurigo sono serviti solo dai venditori di Zurigo etc.... SI ha però che i venditori di Zurigo servono anche Dublino*
- *ogni area geografica ha il proprio db (avremo quindi 4 db)*

Vogliamo studiare una ***frammentazione orizzontale*** *delle 4 tabelle.*
Ricordiamo quindi che abbiamo 4 centri di produzione (ciascuno responsabile di un prodotto e con un db ciascuno) e 3 punti di vendita.
Partiamo con la frammentazione della relazione PRODUCTION*, ottenendo 4 tabelle, una per componente prodotto, ottenendo (con σ abbiamo l'operazione di selezione nell'algebra relazionale):*

- $PRODUCTION_1 = \sigma_{partType=cpu}(PRODUCTION)$
- $PRODUCTION_2 = \sigma_{partType=keyboard}(PRODUCTION)$
- $PRODUCTION_3 = \sigma_{partType=screen}(PRODUCTION)$
- $PRODUCTION_4 = \sigma_{partType=cable}(PRODUCTION)$

Passiamo alla relazione PICKUP*. Anche in questo caso si frammenta per il prodotto facendo il join con la tabella* PRODUCTION*(ricordando che π è l'operazione di proiezione/join nell'algebra relazionale). Per comodità indichiamo tutti gli attributi di* PICKUP *con pick, avendo quindi:*

$$pick = SerialNumber, Lot, Client, SalesPerson, Amount$$

indico anche con SN SerialNumber

- $PICKUP_1 = \pi_{pick}(\sigma_{partType=cpu}(PICKUP\ SN = SN(PRODUCTION)))$
- $PICKUP_2 = \pi_{pick}(\sigma_{partType=keyboard}(PICKUP\ SN = SN(PRODUCTION)))$
- $PICKUP_3 = \pi_{pick}(\sigma_{partType=screen}(PICKUP\ SN = SN(PRODUCTION)))$
- $PICKUP_4 = \pi_{pick}(\sigma_{partType=cable}(PICKUP\ SN = SN(PRODUCTION)))$

Prendo quindi una proiezione di tutti gli elementi di PICKUP separando nei vari PICKUP in base al prodotto.
Passo a alle tabelle SALESPERSON*. Abbiamo 3 punti di vendita, quindi, circa come per* PRODUCTION*, frammento in base alle città di vendita:*

- $SALESPERSON_1 = \sigma_{City="SanJose"}(SALESPERSON)$
- $SALESPERSON_2 = \sigma_{City="Zurigo"}(SALESPERSON)$
- $SALESPERSON_3 = \sigma_{City="Taiwan"}(SALESPERSON)$

Manca solamente CLIENT. *Anche in questo caso divido in base alle città, ricordando che Zurigo e Dublino sono clienti entrambi di Zurigo:*

- $CLIENT_1 = \sigma_{City="SanJose"}(CLIENT)$
- $CLIENT_2 = \sigma_{City="Zurigo" \text{ or } City="Dublino"}(CLIENT)$
- $CLIENT_3 = \sigma_{City="Taiwan"}(CLIENT)$

Abbiamo finito la frammentazione e quindi dobbiamo solo distribuire tali tabelle:

- *le quattro tabelle con indice 1 andranno a San Jose, in* `company.sanjose.com`
- *le quattro tabelle con indice 2 andranno a Zurigo, in* `company.zurigo.com`
- *le quattro tabelle con indice 3 andranno a Taiwan, in* `company.taiwan.com`
- *le due tabelle con indice 4 andranno a Dublino (che quindi avrà solo parte di* PRODUCTION *e parte di* PICKUP *in quanto a Dublino non si ha un punto vendita), in* `company.dublino.com`

Esercizio 2. *Vediamo un esercizio in merito alla trasparenza, che ricordiamo essere a tre livelli:*

1. *di frammentazione*
2. *di replicazione/allocazione*
3. *di linguaggio*

Si chiede di fare delle interrogazioni, tenendo conto dei livelli di trasparenza, sul db costruito nell'esercizio precedente.
La prima query ci chiede di determinare la quantità dei prodotti che hanno valore "77y6878" (abbiamo quindi a che fare con la trasparenza di frammentazione, infatti interroghiamo come se avessimo a che fare con un solo db):

```
Procedure Query1(:Quan):
 Select Quantity in :Quan
 From PRODUCTION
 Where SerialNumber="77y6878"
End Procedure
```

(con **:Quan** *indichiamo il nome della tabella).*
Vediamo ora come fare nel caso di trasparenza di allocazione, quindi si sa di avere a che fare con un db distribuito. La query quindi si "sposterà" alla ricerca del giusto frammento:

```
Procedure Query2(:Quan):
 Select Quantity in :Quan
 From PRODUCTION_1
 Where SerialNumber="77y6878"

 if :empty then
 Select Quantity in :Quan
 From PRODUCTION_2
 Where SerialNumber="77y6878"

 if :empty then
 Select Quantity in :Quan
 From PRODUCTION_3
 Where SerialNumber="77y6878"

 if :empty then
 Select Quantity in :Quan
 From PRODUCTION_4
 Where SerialNumber="77y6878"
End Procedure
```

Vediamo ora come funziona per la trasparenza di linguaggio. In tal caso dobbiamo considerare sia le frammentazioni che i vari indirizzi di allocazione, ovvero i `company.città.com`*:*

```
Procedure Query3(:Quan):
 Select Quantity in :Quan
 From PRODUCTION_1@company.sanjose.com
 Where SerialNumber="77y6878"

 if :empty then
 Select Quantity in :Quan
 From PRODUCTION_2@company.zurigo.com
 Where SerialNumber="77y6878"

 if :empty then
 Select Quantity in :Quan
```

```
 From PRODUCTION_3@company.taiwan.com
 Where SerialNumber="77y6878"

 if :empty then
 Select Quantity in :Quan
 From PRODUCTION_4@company.dublino.com
 Where SerialNumber="77y6878"
End Procedure
```

Nelle slide usa `union` *al posto di* `if :empty then`.

Esercizio 3. *Sempre sul db del primo esercizio effettuiamo la seguente query: determinare le macchine che utilizzano come componente "keyboard" e sono vendute al cliente "Brown".*
Per praticità vediamo solo la trasparenza di frammentazione e quella di allocazione.
Partiamo con la trasparenza di frammentazione:

```
Procedure Query1(:Machine)
 Select Machine in :Machine
 From PRODUCTION join PICKUP on
 PRODUCTION.SerialNumber=PICKUP.SerialNumber
 Where PartType = "keyboard" AND Client="Brown"
End Procedure
```

Vediamo il caso di trasparenza di allocazione (e sappiamo che "keyboard" è solo in $PRODUCTION_2$ quindi interroghiamo un solo frammento e senza chiedere la specifica del partType):

```
Procedure Query2(:Machine)
 Select Machine in :Machine
 From PRODUCTION_2 join PICKUP on
 PRODUCTION_2.SerialNumber=PICKUP_2.SerialNumber
 Where Client="Brown"
End Procedure
```

Se avessimo voluto fare anche la trasparenza di linguaggio non sarebbe cambiato nulla dato che $PRODUCTION_2$ è solo a Zurigo.

Esercizio 4. *Sempre sul db del primo esercizio effettuiamo il cambiamento di indirizzo del cliente "Brown" che si sposta da "27 Church St.", Dublino, a "43 Park Hoi St.", Taiwan. Abbiamo quindi un cambio di allocazione nel db.*
Partiamo con la trasparenza di frammentazione:

```
Procedure Update1
 Update Client
 Set Address  = "43 Park Hoi St.", City="Taiwan"
 Where Name="Brown"
End Procedure
```

La cosa si complica nel caso di trasparenza di allocazione, tenendo conto delle due città e dei loro db:

```
Procedure Update2
 Delete CLIENT_2
 Where Name="Brown"

 Insert into CLIENT_3 (Name, Address, City)
 values ("Brown", "43 Park Hoi St.", "Taiwan")
End Procedure
```

Se avessimo voluto fare anche la trasparenza di linguaggio non sarebbe cambiato nulla poiché le frammentazioni sono in locazioni diverse

Esercizio 5. *Sempre sul db del primo esercizio effettuiamo la seguente query: calcolare la somma di tutti gli ordini ricevuti a SanJose, Zurigo e Taiwan. Partiamo con la trasparenza di frammentazione:*

```
Procedure Query1
 Select City, sum(Amount)
 From PICKUP join SALESPERSON on
 SalesPerson = Name
 Groub by city
End Procedure
```

Passiamo alla trasparenza di allocazione. Mi serviranno tutti i frammenti di `SALESPERSON`*. Inoltre devo considerare i vari* `PICKUP`*, tutti e quattro per il discorso delle vendite su Dublino:*

```
Procedure Query2
 Create view PICKUP as
 PICKUP_1 union PICKUP_2 union PICKUP_3 union PICKUP_4

 Select City, sum(Amount)
 From SALESPERSON_1 join PICKUP on
 SalesPerson=Name
 union
```

```
 From SALESPERSON_2 join PICKUP on
 SalesPerson=Name
 union
 From SALESPERSON_3 join PICKUP on
 SalesPerson=Name
End Procedure
```

Esercizio 6. *Sempre sul db del primo esercizio cerchiamo di massimizzare il parallelismo delle inter-query.*
Prendiamo la seguente query: estrarre la somma delle quantità di produzione che sono raggruppate secondo i tipi e i modelli delle componenti.

```
Procedure Query1
 Select sum(Quantity), Model, PartType
 from PRODUCTION
 Group by (Model, PartType)
End Procedure
```

Vogliamo però massimizzare il parallelismo, divido quindi tra le varie frammentazioni:

```
Procedure Query1
 Select sum(Quantity), Model, PartType
 from PRODUCTION_1
 Group by (Model, PartType)

 Select sum(Quantity), Model, PartType
 from PRODUCTION_2
 Group by (Model, PartType)

 Select sum(Quantity), Model, PartType
 from PRODUCTION_3
 Group by (Model, PartType)

 Select sum(Quantity), Model, PartType
 from PRODUCTION_4
 Group by (Model, PartType)
End Procedure
```

massimizziamo il parallelismo inter-query se si consideriamo che ogni partizione ha un DBMS diverso. Volendo potrei dividere la query ancora a seconda del modello, evitando il `group by` *(cosa utile nel caso in cui si abbia a che fare con un sistema fortemente multicore)*

Esercizio 7. *Vediamo un esempio di db replicato che può produrre inconsistenza.*
Prendiamo l'esempio del db prodotto nel primo esercizio. Supponiamo che ogni frammento di PRODUCTION *sia allocato a tutti i DBMS. Però ogni DBMS utilizza un frammento e trasmette i cambiamenti del frammento agli altri DBMS, permettendo di avere copie del db. In caso di fallimento di un DBMS il db sarebbe comunque accessibile dagli altri sistemi e non so avrebbe problemi con le query, avendo che il fallimento è trasparente sia ai client che al db stesso. Purtroppo quando si ha un fallimento si può generare un partizionamento di rete e questo può comportare delle inconsistenze. Se, per esempio, due transazioni tolgono 800 ad una certa quantità la seconda in ordine temporale fallirà ma se avvengono in due DBMS non connessi non falliranno, producendo inconsistenza.*

Esercizio 8. *Data una replicazione simmetrica dire quando produce inconsistenza. Un esempio è un db senza il concurrency control e quindi due transazioni come quelle dell'esercizio precedente possono causare inconsistenza anche senza fallimento della rete.*

Capitolo 4

Blockchains

Questa lezione è stata tenuta dal prof. Leporati.
Nonostante qualche ambiguità ed errore di scrittura, nel capitolo si userà il termine "nodo" quando si parla di rete P2P e il termine "blocco" quando ci si riferisce ai blocchi interni alla blockchain.

Definizione 7. *Una **blockchain**, in poche parole, è un registro pubblico, condiviso e decentralizzato che memorizza la proprietà di beni digitali.*

È quindi un registro in cui vengono memorizzate informazioni relative alla proprietà di qualcosa che può essere rappresentato tramite sequenze di bit (quindi qualcosa di digitale come i *bitcoin* o altre criptovalute).
Vengono memorizzate anche le **transazioni**, ovvero i cambi di proprietà.
Essendo pubblico tutti possono vedere cosa è stato registrato e in particolare "chi possiede cosa" e la storia di una certa proprietà.
Questo registro è condiviso in quanto gestito da più persone ed è decentralizzato in quanto non esiste un nucleo che abbia di poteri da amministratore rispetto agli altri, tutti sono allo stesso livello.
Questo registro è organizzato in blocchi. Si ha un primo blocco detto **genesis block** che da il via a tutto. Si hanno poi altri blocchi, in nero, collegati a questo e che formano una catena. Un blocco si lega al successivo tramite particolari funzioni crittografiche, dette **funzioni di hash crittografico**. Nel dettaglio il collegamento tra un blocco e il successivo è dato dal fatto che il valore di hash del blocco è contenuta all'interno del blocco successivo, facendo in modo che si estremamente difficile alterare il contenuto di un blocco, ovvero diverse transazioni, che sono organizzate secondo una precisa struttura dati che consente di verificare la validità in modo veloce ed efficiente. Per ogni blocco si calcola quindi l'hash e lo si salva nel blocco successivo. Per modificare una transazione quindi dovrei calcolare l'hash e dovrei fare il check con il blocco successivo. Quindi tutti possono verificare la validità

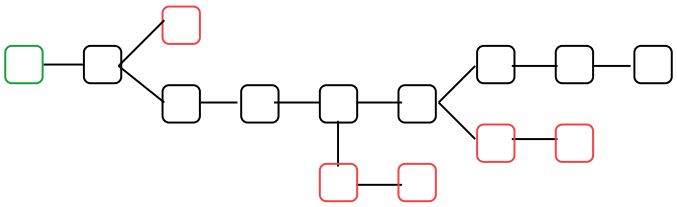


Figura 4.1: Esempio di schema di blockchain. In verde a sinistra troviamo il **genesis block**. In nero i blocchi che formano la catena. In rosso abbiamo i nodi *orfani*. Per comodità è stata rappresentata in orizzontale con la parte "alta" a destra

della blockchain. Modificare i dati in modo tale da ottenere lo stesso hash però è davvero difficile.

Si hanno vari nodi per l'uso della blockchain. I vari nodi sono nodi di una **rete Peer-to-Peer (*P2P*)** (come quelle per la condivisione di file come *torrent*, dove quindi ogni computer fa sia da *client* che da *server*). I vari nodi osservavano le proposte di transazione che vengono fatte dagli utenti (anche utenti che solo usano la blockchain), verificano che siano valide (ad esempio verificando che non avvenga il *double-spending*, ovvero, per esempio, una doppia concessione dello stesso bene), eseguono un **protocollo di consenso** (in quanto potrebbero esserci nodi "disonesti", con per esempio utenti che vorrebbero appropriarsi di beni altrui come bitcoin, si procede quindi a maggioranza secondo il *proof-of-work*) e infine procedono validando la transazione aggiungendo il blocco alla fine della blockchain ("in cima"). Una copia della blockchain viene memorizzata in ogni nodo della rete P2P alla fine della transazione, quindi quando i nodi sono d'accordo sull'aggiunta del blocco allora ciascuno lo aggiunge alla propria copia della blockchain (altrimenti qualsiasi proposta futura verrebbe bocciata).

In molte blockchain se si stabilisce che due blocchi possono essere attaccati ad un certo blocco e si inizia a lavorare su entrambi formando quindi due nuove catene. Alla fine "vince" la catena più lunga, fermando la continuazione dell'altro ramo. I blocchi del ramo "perdente" vengono resi *orfani* lasciando quindi una sola catena attiva. Le transazioni nei nodi *orfani* vengono dimenticate e bisognerà reinserirle. Questa cosa è molto inefficiente.

Ci sono reti, come quella *bitcoin*, in cui una transazione è valida sse vengono aggiunti 6 blocchi al di sopra di quello che contiene la transazione.

Le transazioni sono **pseudo-anonime** (comodo ambito bitcoin dove, come per i contanti, non si sa per quali mani sono passati quei soldi e per cosa sono stati usati prima). Ci sono vari meccanismi per rendere anonime le cose, alcuni migliori (come quelli di *monero* o *zcash*) e alcuni peggiori (come quelli

di *bitcoin* ed *ethereum*).
Si ha un ramo della *computer foreniscs* che si occupa di capire chi ha fatto certe transazioni, esplicitamente di criptovalute, sulla blockchain. Quindi si prova a raggiungere l'anonimato ma non sempre si riesce (basta un utente che paghi in *bitcoin* su un sito rivelando la propria identità).

4.1 Bitcoin

Bitcoin è una criptovaluta proposta da Satoshi Nakamoto (probabilmente un nome falso in quanto in molti stati creare valuta, anche digitale, è reato) nel 2008. Non è nato all'improvviso ma molte idee all'interno di *bitcoin* erano già presenti i diversi paper di crittografia precedenti (ad esempio la *proof-of-work* era già presente all'interno della gestione dello spam delle mail, dove veniva imposto un certo sforzo computazionale per mandare una mail in modo che l'invio non fosse completamente "gratuito", comportando che si possano mandare al massimo circa 2000 mail al giorno, al più di attrezzarsi con dei super computer). Ci sono stati tanti precedenti di tentativi di creazione di un sostituto digitale del denaro, con diverse difficoltà a causa di anonimato e *double-spending*. Inoltre rappresentare una moneta con una sequenza di bit consente la copia illimitata di tale sequenza, creando copie perfettamente identiche. Una soluzione per evitare il *double-spending* è quella di usare una *trust third party (TTP)*, ovvero tipicamente una banca che segna le transazioni monetarie, diventando però un "collo di bottiglia", venendo interpellata in tutte le transazioni. Inoltre la banca è conscia delle transazioni di denaro, che perdono così l'anonimato. L'idea di Satoshi Nakamoto e stata quella di unire vari protocolli crittografici usando al posto della banca un registro condiviso, una blockchain appunto, in cui vengono salvate le transazioni e dove vengono anche controllate, permettendo di evitare il *double-spending*. Si usa la blockchain quindi per creare un *trust*, sostituendo la funzione delle banche. Nel **genesis block** di *bitcoin* c'è infatti un messaggio (nel posto del blocco dedicato alla "causale") che fa riferimento al potere eccessivo delle banche.
Le proprietà memorizzate nella blockchain *Bitcoin* sono chiamate direttamente, come abbiamo già scritto, **bitcoins (*BTC*)** o frazioni di essi. Le transazioni sono parecchio complicate, con una struttura dati complessa, con diverse transazioni in ingresso (infatti una transazione può contenere transazioni), campi per generare nuovi bitcoin,0diversi *script di transazione* in output (scritti in un linguaggio "particolare").
Non verrà trattata nel dettaglio la conformazione delle transazioni.
Se un utente A vuole mandare un *bitcoin* ad un utente B, usando il pro-

prio client, che spesso viene chiamato **wallet**, specifica la quantità che vuole mandare e l'indirizzo di B. Ogni utente ha associato quindi un indirizzo, in qualità di lunga sequenza di numeri. Per ottenere l'indirizzo viene usata una **chiave pubblica**, usando quindi la *crittografia a chiave pubblica* in cui si usano algoritmi di cifratura e de-cifratura. Ciascuno crea con questi algoritmi una copia *chiave pubblica/chiave privata*, rende pubblica la *chiave pubblica* e comunica di usare quella chiave pubblica per risalire all'indirizzo a cui farsi spedire i *bitcoin*, infatti data la chiave pubblica all'utente che deve inviare i bitcoin la userà per cifrare il messaggio in modo che, tramite la chiave privata, solo il legittimo destinatario possa decifrare il messaggio.
Dalla chiave pubblica quindi ottiene l'indirizzo al quale A deve mandare i soldi per farli ricevere a B. Quindi l'indirizzo è una sorta di identità per B che però può generarsi tutte le coppie di chiavi che vuole, combinando poi i vari bitcoin ricevuti ai vari indirizzi che ha generato tramite la complessa struttura della transazione. Questa possibilità di generare infinite chiavi però è solo uno *pseudo-anonimato*.
Bisogna però anche dimostrare che A è proprietario dei *bitcoins* che vuole inviare a B. Per farlo A "firma" digitalmente la transazione tramite la sua *chiave segreta*. I nodi della rete P2P, che sono detti **miners**, verificano che la firma di A sia valida, verificano che non ci sia il *double-spending* e infine validano la transazione mettendola in un nuovo blocco della blockchain. Se B, che ha ricevuto i *bitcoins*, vuole a sua volta mandarli a C avvia una transazione esattamente come descritto sopra, firmando con a chiave privata che era accoppiata alla chiave pubblica con la quale A gli aveva mandato i *bitcoins*, permettendo che la firma sia verificata e validata. Quindi sulla blockchain il possedimento di un *bitcoin* è rappresentato dal fatto che si può inviare una transazione per cui quel *bitcoin* può essere dato a qualcun altro (ovviamente si è usato *bitcoin* ma si poteva parlare anche di più *bitcoins* o, vedremo in seguito, frazioni, che molto piccole, di esso). Non è segnato da nessuna parte quanti *bitcoins* possiede un certo utente ma solo le catene di transazioni che sono state fatte da ciascun *bitcoin*, vedendo quindi chi è l'ultimo proprietario. È quindi essenziale memorizzare le chiavi in quanto possedere equivale a conoscere una chiave segreta.
La blockchain registra ogni singola transazione (e sono circa un migliaio ogni 10 minuti, con un blocco che riesce a contenere circa un migliaio di transazioni e i blocchi vengono aggiunti uno ogni 10 minuti circa) e attualmente, in data 19 Ottobre 2020, si è arrivati a 290GB di blockchain.

4.1.1 Miners

Abbiamo parlato prima dei membri della rete P2P della blockchain *Bitcoin*, detti appunto **miners**.
I *miners* lavorano su un *pool* di transazioni proposte dai vari *wallet*. I miners scelgono circa un migliaio di queste transazioni alla volta e cercano di formare il nuovo blocco, validando le transazioni. Effettuano quindi i calcoli computazionali del *proof-of-work* per cui dimostrano di aver fatto un certo sforzo per avere il **diritto** di essere quelli che aggiungono il prossimo blocco alla catena. Avendo un'aggiunta ogni 10 minuti si ha una fortissima concorrenza tra i *miners*. Inoltre il carico di lavoro richiesto diventa sempre più difficile in quanto, grazie alla **legge di Moore**, diventa sempre più facile risolvere il "puzzle" crittografico, per il *proof-of-work,* che serve a risolvere il nuovo blocco e quindi il "puzzle" viene reso sempre più difficile (ovvero se un blocco arriva in meno di 10 minuti il blocco successivo sarà più difficile da produrre, in modo che nuovamente servano almeno 10 minuti, anche se equivalentemente verrà reso più facile se ci vogliono troppi minuti in più di 10, avendo così **autoregolazione**). Bisogna quindi parlare di questo "problema" crittografico da risolvere e per farlo bisogna un attimo specificare meglio le *funzioni di hash*.

Definizione 8. *Le **funzioni di hash** sono funzioni crittografiche che prendono in input una sequenza di bit, in teoria arbitrariamente lunga, anche se ogni funzione ha un limite teorico (ma praticamente irraggiungibile), e produce una sequenza che vorrebbe essere univoca (ma che non lo è) di poche centinaia di bit. Per esempio SHA1 produce in output una sequenza di 160 bit, MD5 di 128 bit, SHA256 di 256 bit (una di quelle usate in Bitcoin), RIPEMD di 160 bit (anch'essa usata in Bitcoin) etc...*
Le funzioni di hash devono essere sufficientemente facili da calcolare a partire da un certo input

L'idea è quindi è che prendo un file e, usando ad esempio SHA256, mi esce una sequenza di 256 bit, univoca per quel file. Purtroppo il dominio della funzione (ovvero i bit del file) è molto più grande del codominio (ovvero tutte le possibili sequenze di 256 bit) e quindi non si può avere davvero una **funzione iniettiva** e quindi si avranno sempre due sequenze in input che producono lo stesso output e quando questo avviene si ha una **collisione**. Le collisioni sono inevitabili ma le funzioni di hash sono fatte in modo tale che sia estremamente difficile trovare due input diversi che producano lo stesso output, motivo per cui si può anche pensare che le hash siano univoche. Si ha anche che è estremamente difficile cercare esplicitamente un input che abbai lo stesso hash di un altro, rendendo quindi molto difficile sostituire un

input dato con un altro ottenendo comunque lo stesso output, imbrogliando. Quest'ultimo problema è più difficile di quello della *collisione* (dove ho, nella pratica, un grado di liberà in più avendo due input).
Si hanno altre due proprietà:

1. dato un hash è estremamente difficile trovare un input, per questo si dice che la funzione di hash è *one-way* (essendo molto facile da calcolare ma difficilissimo da invertire)

2. anche se cambio un solo bit dell'input ottengo un output completamente diverso a quello ottenuto prima del cambiamento, rendendo impossibile capire la regola di calcolo o anche solo fare indagini statistiche. Infatti hash significa anche "polpettone", cosa che rappresenta bene l'azione di spezzettamento, calcolo e rimescolamento (con anche valori semi casuali) dell'input fatte dalle funzioni per calcolare l'output

Quindi nel *proof-of-work*, per dimostrare di aver svolto una certa quantità di lavoro viene preso il dato di cui devo calcolare l'hash, gli viene aggiunta una quantità casuale detta **nonce (si pronuncia "nons")** e calcolo l'hash del dato concatenato al *nonce* e vado a vedere se il risultato ha un certo numero prefissato di bit più significativi uguali a 0, riduco quindi il codominio, ovvero il numero di possibili output validi, dicendo che devono cominciare con un certo numero di zeri. Aumentando il numero di zeri riduco la probabilità di ottenere un risultato valido scegliendo un *nonce* a caso (e diminuendo ottengo l'opposto). Variando gli zeri ottengo quanto detto sopra in merito al variare del carico computazionale per restare sui 10 minuti.
Quindi, ricapitolando:

- il miner sceglie un migliaio di transazioni più o meno a caso
- il miner spara a caso un valore del *nonce*
- calcola l'hash di tutto il blocco:
  - se ottiene un valore con un numero di bit più significativi uguali a zero accettabile, prima degli altri, manda il blocco nella rete P2P per far validare il nuovo blocco e, se il controllo viene superato, il blocco viene accettato e messo in cima alla blockchain (quindi ogni nodo della P2P lo attacca in cima alla propria copia)
  - se non ottiene tale valore spara a caso un altro *nonce* e ci riprova

Se mentre si sta lavorando un nuovo blocco viene validato (anche dal nodo che stava lavorando al nuovo blocco) un altro blocco bisogna "buttare" quanto costruito anche se non tutto, butto infatti le transazioni che già compaiono nel nuovo blocco convalidato. Inoltre cambio l'hash del nuovo blocco a cui sto lavorando mettendo quello di quello appena convalidato (per il discorso spiegato all'inizio del capitolo).
L'importanza di essere colui che crea il blocco è data dal fatto che l'unico momento in cui si possono creare *bitcoins* è durante la creazione del nuovo blocco, chi aggiunge il blocco ha dei nuovi *bitcoins* che vengono creati insieme al blocco.
Il mining può essere fatto da macchine sempre più performanti (all'inizio bastava un portatile, poi si è passati ad usare i pc di interi uffici di notte (o qualche furbo anche, illegalmente, dell'università), poi si è passati a cluster "home-made" tramite hardware spesso dedicato solo al mining, mentre ora servono cluster estremamente potenti ma che comunque facciano ritornare le spese). Si hanno anche soluzioni di sub-affitto di hardware o di gente che condivide l'hardware per poi dividere i guadagni. A causa di queste *farm* professionali enormi, spesso collocate in paesi freddi per il risparmio del raffreddamento e dove la corrente costa meno (ovvero in zone disabitate di paesi spesso poveri e poco democratici), rischia di danneggiare l'idea di decentralizzazione della blockchain. **Bitcoin** ad un certo punto era in mano di pochissime persone (cinesi) con farm sparse nei monti asiatici. Si rischiano anche manipolazioni truffaldine del mercato, ad esempio proposte di *trading coi bitcoins* (cose comunque vietate nei mercati regolamentati ma non su quello delle criptovalute, non essendo regolamentato, e quindi se il broker di imbroglia sei fregato).
Un altro problema dell'*accentramento* è il cosiddetto **attacco del 51%**. Dato che ogni miner deve vincere contro tutti gli altri per poter essere quello che ha diritto di mettere il nuovo blocco allora se uno riesce a possedere il 51% dell potenza di calcolo dei miners, controllando il 51% dei nodi della rete P2P, praticamente vince sempre, validando sempre le transazioni, anche se non valide (ovviamente almeno il 51%).
"Tutti contro tutti" è anche molto inefficiente dal punto di vista energetico (la rete P2P che gestisce *bitcoin* consuma più di tutta l'Argentina). Per questo si cercano sempre nuovi algoritmi/alternative per il *proof-of-work*, come ad esempio *proof-of-stake*, dove stake sta per "quantità di soldi", ovvero l'idea in cui solo pochi nodi della P2P fanno il mining. Tali nodi vengono scelti in base alla quantità di soldi che ogni nodo ha deciso di rendere disponibili agli altri (su un conto speciale). Quindi chi mette più soldi ha più possibilità di essere scelto.
Al massimo si ha che si potranno costruire 21 milioni di *bitcoins* e questi sono

sempre più difficili da creare (è quindi paragonabile all'oro da un certo punto di vista).
Torniamo a parlare delle transazioni.
Nel caso in cui A voglia dare a B una certa porzione di *bitcoins* deve creare due transazioni:

- una in cui dal totale produce la frazione complementare a quella che deve dare a B, questa transazione è verso se stessi stessi
- una in cui da a B la frazione voluta

In poche parole se A ha 10 *bitcoins* deve fare una transazione a se stessa di 9 e una di 1 a B.
Questo può essere fatto anche avendo più indirizzi di partenza in cui si hanno i *bitcoins*, grazie al fatto che una transazione ha più input, e verso più destinatari, contemporaneamente, in quanto la transazione ammette anche più output nella sua struttura. **La somma totale degli input non deve essere minore a quella in output** (infatti la transazione non verrà validata). Può comunque essere maggiore in quanto la differenza, detta *fee*, può essere un compenso per il miner per far scegliere quella transazione da validare (che quindi non sceglie proprio a caso il migliaio di transazioni in quanto ordina le transazioni in base alle *fee*). Queste *fee* saranno l'unica fonte di guadagno per i miner quando non si potrà più produrre *bitcoins* per il limite visto precedentemente (in quel momento le *fee* aumenteranno di valore probabilmente).
Due blocchi possono essere aggiunti contemporaneamente perché magari due miner in luoghi distanti propagano insieme l'avviso di aver trovato un nuovo blocco valido. Può succedere quindi che vengano aggiunti entrambi anche se uno è destinato a diventare *orfano*.
Proporre una transazione con *fee* pari a 0 può portare al fatto che nessun miner la prenda in carico, comportando la creazione di *transazioni zombie* (che sono parecchie).
Un altro problema di *bitcoin* è che per essere sicuri che una transazione si andata a buon fine devo aspettare 6 blocchi, quindi un'ora di tempo, e questo limita i casi d'uso della moneta (di certo non va bene per prendere il caffè). Il numero di transazioni supportate è comunque minimo rispetto a quelle che si possono effettuare con la moneta fisica.

4.2 Ethereum

Il futuro delle blockchains non ha potenzialmente limiti. Ci sono molte applicazioni e molte varianti, una di queste è **Ethereum**.

Listing 1 Esempio di contratto in Solidity tratto dalla documentazione di Solidity `https://solidity.readthedocs.io/en/v0.7.4/`

```
pragma solidity >=0.4.16 <0.8.0;

contract SimpleStorage {
  uint storedData;

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

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

Ethereum è un altro tipo di blockchain in cui si pone l'attenzione non tanto sulle transazioni quanto sulle **computazioni**. Si ha un modello diverso di blockchain in quanto vengono memorizzate i cosiddetti *ethereum account*. Ogni utente che si registra quindi viene quindi associato ad un account con una certa quantità di criptovaluta, che in questo caso è chiamata **ether (*ETH*)**. Le transazioni avvengono più o meno come in un conto in banca, togliendo *ether* ad uno e dandoli all'altro mentre la validazione delle transazioni avviene quasi come in *bitcoin* anche se si sta cercando di passare alla *proof-of-stake*. La novità di *ethereum* è la possibilità di scrivere/programmare i cosiddetti **smart contract**, ovvero il corrispettivo dei contratti tra persone, dove, per esempio, un utente, per un tot guadagno al mese, concede l'uso di una sua proprietà ad un altro utente. Si usa un linguaggio di programmazione chiamato **Solidity**, simile ad un linguaggio OOP dove al posto degli oggetti si hanno i **contratti** (ma si hanno comunque struct, function etc...). I contratti scritti con Solidity vengono compilati in un bytecode che viene memorizzato sulla blockchain di ethereum (e quindi una copia viene salvata su tutti i nodi della rete P2P). Si possono fare transazioni che trasferiscono soldi oppure posso fare transazioni in cui si invocano funzioni poste all'interno di un certo contratto, in questo caso un miner raccoglierà la richiesta ed eseguirà sulla sua macchina il codice del contratto. Ogni esecuzione di ogni singola operazione del bytecode (che viene eseguito sulla *ethereum virtual machine*) costa una certa quantità di **gas** e quindi bisogna dare una certa quantità di soldi, rappresentati il costo del **gas**, per far eseguire il con-

tratto e, qualora non siano sufficienti, viene sollevata l'eccezione `outOfGas`, il contratto non va a buon fine e i soldi finora spesi vanno persi.
Gli *smart contract* sono codice di cui chiunque può vedere il bytecode e sono una sorta di codice lato server e posso quindi fare dei client che gestiscono le parti "delicate" dei trasferimenti di soldi facendo chiamate ai contratti, che sono elaborati dai miner. La scrittura dei contratti è rischiosa quindi si hanno quindi delle comunità (come *OpenZeppelin*) che controllano i contratti stessi e forniscono delle linee guida e delle librerie da cui attingere, ma nel momento in cui vengono modificati non sono più testati, ovviamente. Un esempio è stato di una startup che ha lasciato una moltiplicazione non protetta da overflow modificando un contratto, preso da *Openzeppelin*, per permettere pagamenti simultanei (banalmente se si doveva dare 10 ETH a due utenti si faceva 10·2 e si controllava che ci fossero effettivamente 20 ETH nel conto prima di effettuare il doppio pagamento). Essendo il bytecode pubblico se ne sono accorti e qualcuno si è fatto un pagamento a due suoi altri account dando una cifra esorbitante, in modo da scatenare l'overflow, il prodotto per 2 dava 0 a causa dell'overflow e quindi si autorizzava la transazione. Questa cosa non sarebbe stata possibile su *bitcoin* ma la diversa implementazione della blockchain di ethereum rendevano possibile la cosa (e irriconoscibile al miner). Creare quindi *smart contract* è estremamente difficile, dovendo essere estremamente sicuri. Inoltre una volta che il contratto è sulla blockchain ci resta, anche se il creatore può chiedere al contratto stesso di autodistruggersi (nel senso che vengono rese invalide le chiamate alle funzioni di quel contratto).
Ci sono vari strumenti per scrivere contratti, l'ide *Remix* e *MetaMask*, che permette di avere un **wallet** su ethereum e di collegarsi sia alla rete principale che a diverse reti, anche locali sul proprio computer, per testing. Tra le reti di testing principali abbiamo *Rapsten* che cerca di emulare al meglio possibile quella principale (dove gli ETH che trasferisco o pago come **gas** sono finti). In altre reti di test si hanno altri algoritmi di consenso, come per esempio, nel caso della rete *Rinkeby* si ha il **proof-of-autority** (dove chi ha diritto a scrivere una certa informazione lo può fare senza il consenso della rete P2P).
L'iter normale di sviluppo di contratti non prevede in primis l'uso delle reti di test in quanto servirebbe troppo tempo ma si usano strumenti come *Ganache* o *Truffle* che sono strumenti di sviluppo in locale che simulano una rete in locale dove si può testare senza **gas** in modo veloce. Solo dopo si passa alla rete di test e poi alla *main net*, la rete principale.
Esiste anche una libreria chiamata *web3*, scritta in *js*, per permettere alle webapp di connettersi a MetaMask.

4.3 Altre blockchains

Si hanno comunque davvero tante diverse blockchains.
Si ha, ad esempio, *Quorum*, una variante di *Ethereum* in cui si possono usare altri algoritmi di consenso e in cui si possono anche creare dei canali di comunicazione privati tra i nodi della rete P2P.
Si hanno quindi diversi tipi di blockchain e in particolare ci sono le blockchain di tipo **permissioned** e non solo quelle di tipo **permissionless** o **pubbliche**.
per blockchain di tipo *permissioned* si intende che i nodi della rete P2P, che tipicamente sono anche quelli che scrivono informazioni e quindi avviare le transazioni, si conoscono ma eventualmente non si fidano, formando così un **consorzio** in cui i partecipanti sono potenzialmente in conflitto (dove magari il fallimento di uno è il successo dell'altro). Se le dichiarazione pubbliche siano vere o meno viene deciso con un servizio di *audit* esterno che valuta le dichiarazioni pubbliche. Non c'è quindi ne mining ne *proof-of-work*, magari nemmeno una criptovaluta. La blockchain diventa quindi un punto in cui implementare politiche di trust tra i partecipanti, obbligandosi a vicenda a dichiarare in modo pubblico (e se imbrogli esci dal consorzio perdendone i vantaggi), fattore che viene aiutato dal fatto che è estremamente difficile alterare la blockchain (dovendo rompere una catena e rifarla, imbrogliando sugli hash etc...) rendendo le dichiarazioni praticamente eterne.
Si hanno quindi:

- **permissionless blockchain**, come *bitcoin* o *ethereum*, dove chiunque può scaricarsi il software e diventare miner
- **permissioned blockchain pubblica**, dove possono vedere tutti, come *Quorum*, *EOS* (con una virtual machine basata su *webassembly* e *smart contract* scritti in *C++*), *Hyperledger* (sviluppata da IBM e ospitata dalla *Linux Foundation*, essendo completamente *Open Source*, di tipo modulare, molto complessa ma efficiente, nata per il business con algoritmi di consenso basato sul **problema dei generali bizantini** e che scrive sulla blockchain solo se necessario etc...) etc... Con queste blockchain si perde il discorso della decentralizzazione, non permettendo che partecipi chiunque ma si ha una *certificate authority* che stabiliscono se uno ha il diritto di scrivere o leggere sula blockchain (e si hanno spesso più amministratori che si controllano a vicenda atti a stabilire chi può fare cosa)
- **permissioned blockchain privata**, dove possono vedere solo quelli che scrivono

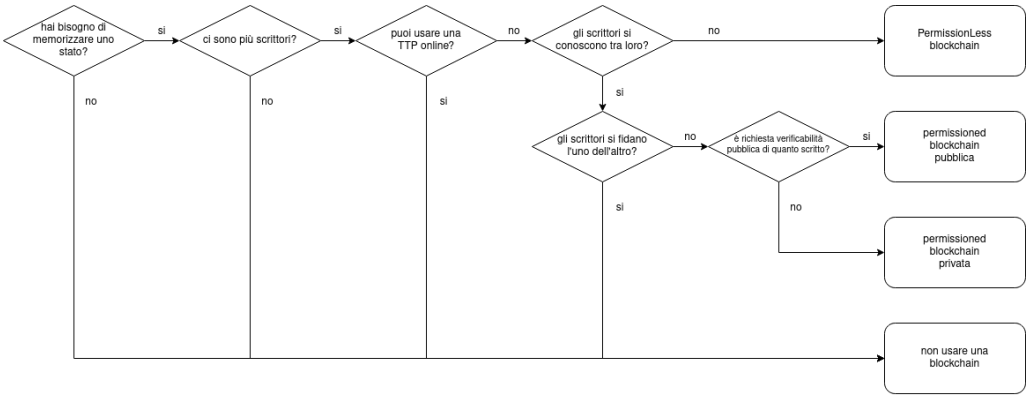


Figura 4.2: Diagramma dei casi di scelta di una blockchain

Grandi aziende, come IBM, Microsoft, SAP etc... che stanno concentrando sullo sviluppo di blockchain ma anche piccole applicazioni, come *CryptoKitties*, basata su Ethereum, che permette di collezionare e crescere "gattini digitali" collezzionabili.
Bisognerebbe inoltre fare un discorso sul rapporto che si ha tra *smart contract* e dispositivi fisici, nonché sull'interpretazione legale degli stessi (e gli avvocati dicono che non sono ne legali ne "smart" per i problemi detti sopra).