Business and Logistics

☐ Feedback on paper topic and references
☐ Problem set 1 due today
Acknowledgements

☐ Some material taken from author’s teaching slides based on Distributed Systems: Concepts and Design book

☐ Some figures taken from Distributed Systems: Concepts and Design book
Lecture Objectives

☐ Present the problem of distributed transactions
☐ Discuss the two phase commit protocol
☐ Discuss distributed concurrency control
  ☐ Based on local concurrency control at each server
  ☐ Distributed deadlock detection is complex
☐ Discuss distributed deadlock detection
  ☐ A centralized solution is not scalable
  ☐ Phantom deadlocks are a problem
  ☐ Use edge chasing
☐ Discuss recovery to ensure atomicity and durability
  ☐ Transaction log and checkpoints
Distributed Transactions

- Have been considering single server
- In general, data items belonging to a service may be distributed among several servers
- Client transactions involve multiple servers
  - Directly by requests made by a client
  - Indirectly via requests made by servers
- Distributed transaction
  - Any transaction whose activities involve multiple servers is a distributed transaction
- Client transactions that involve multiple servers indirectly may be modelled as nested transactions
Distributed Transactions (continued)

- Refers to a flat or nested transaction that accesses objects managed by multiple servers
- Transaction commitment is still a problem
- When a distributed transaction comes to an end
  - Either all of the servers commit the transaction
  - Or all of them abort the transaction
- One of the servers is *coordinator*
  - Ensure the same outcome at all of the servers
- The “two-phase commit protocol” is the most commonly used protocol for achieving this
Structuring of Distributed Transactions

- Simple distributed (flat) transaction
  - Client makes requests to more than one server
  - Each server carries out the client’s requests without invoking operations on other servers
  - Transaction accesses servers’ data items sequentially
  - When locking is used, a transaction can only be waiting for one data item at a time

- Nested transaction
  - Server invokes operations on other servers
  - Hierarchy of nested transactions (sub-transactions)
  - Sub-transactions at same level can run concurrently
  - Hierarchical or flattened commit protocols
Distributed Transaction Types

(a) Flat transaction

(b) Nested transactions

Issues?
Case Study: Nested Banking Transaction

\[ T = \text{openTransaction} \]
\[ \text{openSubTransaction} \]
\[ a.\text{withdraw}(10); \]
\[ \text{openSubTransaction} \]
\[ b.\text{withdraw}(20); \]
\[ \text{openSubTransaction} \]
\[ c.\text{deposit}(10); \]
\[ \text{openSubTransaction} \]
\[ d.\text{deposit}(20); \]
\[ \text{closeTransaction} \]

What subtractions can run in parallel?
Requirements for Distributed Transactions

☐ Atomicity

- Either all of the servers involved commit
- Or all of them abort
- Coordinator ensures the same outcome
- Depends on protocol chosen
- “Two-phase commit protocol” is common

☐ Concurrency control

- Local control to ensure transactions are serializable
- Must be serialized globally as well
- Extension of concurrency control methods for single server transactions
Coordinator of a Distributed Transaction

- Distributed servers need to coordinate their actions when the transaction commits
- Client sends *OpenTransaction* request to server
- Server returns *transaction ID (TID)*
  - Must be unique within a distributed system
  - Server ID + unique ID within server
- First server in the transaction become *coordinator*
  - Responsible for adding servers
  - Responsible for committing or aborting
  - Servers managing a transaction object are *participants*
    - cooperates with coordinator in commit protocol
  - Records list of participants and coordinator ID
Same as in single server case except for join()

\begin{itemize}
\item \texttt{openTransaction()} -> \texttt{trans};
  starts a new transaction and delivers a unique TID \texttt{trans}
  to be used in the other operations in the transaction
\item \texttt{closeTransaction()} \rightarrow (commit, abort);
  ends a transaction: a \textit{commit} return value indicates that
  the transaction has committed; an \textit{abort} return value
  indicates that it has aborted
\item \texttt{join()} \rightarrow (commit, abort);
  informs a coordinator that a new participant has joined
  the transaction \texttt{trans}
\item \texttt{abortTransaction()};
  aborts the transaction
\end{itemize}
**AddServer** Transactional Service Function

- **AddServer**(trans, server ID of coordinator)
  - Informs server involved in transaction *trans*
- **AddServer** must be used by the client before any operations are requested in a server not yet joined
  - Supplies transaction ID
  - Supplies transaction coordinator server ID
- **Receipt of AddServer**
  - Initializes local transaction
  - Sends **NewServer** request to coordinator
  - **NewServer**(trans, server ID of worker)
Distributed Banking Transaction

$T = \text{openTransaction}$
$a.\text{withdraw}(4);$  
$c.\text{deposit}(4);$  
$b.\text{withdraw}(3);$  
$d.\text{deposit}(3);$  
$\text{closeTransaction}$

Note: the coordinator is in one of the servers, e.g. BranchX
Coordination and Transaction Completion

- Coordinator and workers knowing each other enables them to collect information needed at commit time.

- Distribution of servers in a transaction can be made transparent to user-level programs:
  - Record ID of server that opens transaction
  - Issue `AddServer` when new server joins with TID

- `CloseTransaction` or `AbortTransaction`:
  - Called when transaction ends
Atomic Commit Protocols (One-Phase)

- Transaction ends when client requests that the transaction should be committed or aborted
- Requires atomicity
- **One-phase atomic commit** protocol
  - Coordinator communicates the commit or abort request to all the servers in the transaction
  - Continue repeating request until all acknowledge
- One-phase atomic commit is inadequate
  - Client requests a commit
  - Does not allow server to unilaterally abort
  - Servers must be able to abort in some situations (Why?)
One-Phase (continued)

- Why would a server be unable to commit?
- Usually associated with concurrency control
  - Use of locking may lead to deadlocks
    - transaction aborts used to break deadlocks
  - Aborts are also used in optimistic concurrency control
- Also the server can crash and be replaced
- How does the client know that a server has aborted a transaction?
- One-phase atomic commit does not allow for server to notify coordinator
- Can timeouts be used somehow?
Commit Protocols

- Commit protocols are designed to work in:
  - Asynchronous system
    - Messages may take a very long time
  - Servers may crash
  - Messages may be lost
  - Assume corrupt and duplicated messages are removed
  - No byzantine faults
    - Servers either crash or they obey their requests
Two-Phase Commit Protocol

- Designed to allow any server to abort its part of the transaction
- Due to atomicity, if one part of a transaction is aborted, the whole transaction must be aborted

First phase (*Voting phase*)
- Each server votes for transaction to be committed or aborted
- Once a server votes commit, it cannot abort it (i.e., change its mind)
- Server must ensure it can commit before voting
  - saves all objects in permanent storage
- Transaction is said to be in a *prepared state*
Second phase \textit{(Completion phase)}

- Every server carries out a joint decision
- If any one server votes to abort, then the decision must be to abort (think of majority function as boolean AND)
- If all servers vote to commit, then the decision is to commit the transaction

The problem is to ensure that all the servers vote and that they all reach the same decision

- Simple with no errors
- Protocol must work correctly in face of failures, lost messages, temporary loss of communication
More on Two-Phase Commit Protocol

- During a transaction, participants communicate with coordinator only to join the transaction
- A client’s request to commit/abort directed to coordinator
- Client abort or server transaction abort
  - Coordinator informs participants immediately
- Two-phase commit protocol comes into play when client asks coordinator to commit
- Voting and completion phases
  - Server-to-server operations
- 2PC is an example of a consensus protocol
In the first phase the coordinator asks all the participants if they are prepared to commit.

In the second phase the coordinator tells them to commit or abort.

A participant agreeing to commit must be able to...
Operations for Two-Phase Commit Protocol

\texttt{canCommit?(trans)} \rightarrow \texttt{Yes / No}
Call from coordinator to participant to ask whether it can commit a transaction. Participant replies with its vote.

\texttt{doCommit(trans)}
Call from coordinator to participant to tell participant to commit its part of a transaction.

\texttt{doAbort(trans)}
Call from coordinator to participant to tell participant to abort its part of a transaction.

\texttt{haveCommitted(trans, participant)}
Call from participant to coordinator to confirm that it has committed the transaction.

\texttt{getDecision(trans)} \rightarrow \texttt{Yes / No}
Call from participant to coordinator to ask for the decision on a transaction after it has voted \texttt{Yes} but has still had no reply after some delay. Used to recover from server crash or delayed messages.
Two-Phase Commit Protocol

Phase 1 (Voting phase):

1. The coordinator sends a \textit{canCommit}? request to each of the participants in the transaction.
2. When a participant receives a \textit{canCommit}? request it replies with its vote (\textit{Yes} or \textit{No}) to the coordinator. Before voting \textit{Yes}, it prepares to commit by saving objects in permanent storage. If the vote is \textit{No}, the participant aborts immediately.

Phase 2 (Completion according to outcome of vote):

3. The coordinator collects the votes (including its own).
   (a) If there are no failures and all the votes are \textit{Yes}, the coordinator decides to commit the transaction and sends a \textit{doCommit} request to each of the participants.
   (b) Otherwise the coordinator decides to abort the transaction and sends \textit{doAbort} requests to all participants that voted \textit{Yes}.
4. Participants that voted \textit{Yes} are waiting for a \textit{doCommit} or \textit{doAbort} request from the coordinator. When a participant receives one of these messages it acts accordingly and in the case of commit, makes a \textit{haveCommitted} call as confirmation to the coordinator.
More Two-Phase Commit Protocol (continued)

- Apparently straightforward protocol could fail due to one or more of the servers failing or due to a breakdown in communication.

- To address crashing, each server saves information relating to the two-phase commit protocol in permanent storage (non-volatile, temporary space essentially).

- Timeout actions are included in the protocol:
  - Various stages at which a server cannot progress its part of the protocol until it receives another request or reply from one of the other servers.
  - Timeout for each step at which a process may block.
  - Used to avoid processes blocking forever.
Timeouts Actions

☐ Worker votes *Yes* and waits for coordinator to report on the outcome

☐ Worker is uncertain of the outcome and cannot proceed until get information from coordinator
   ☑ Cannot decide unilaterally and objects cannot be released

☐ Worker times out and makes *GetDecision* request
   ☑ Needs reply to continue protocol
   ☑ Wait for reply (when received continue step 4)

☐ Worker could obtain decision cooperatively
   ☑ Useful when coordinator has failed
   ☑ Still need to get out of uncertain states
Timeouts Actions (continued)

☐ Worker can be delayed when carried out all client requests, but not yet received *CanCommit*? from coordinator
   ☐ Worker can decide to *Abort* unilaterally

☐ Coordinator may be delayed waiting for votes from the workers
   ☐ May decide to abort the transaction
   ☐ Announce *AbortTransaction* to the workers who have already sent their votes
   ☐ Tardy workers voting *Yes* will be ignored (Is this ok?)
Performance of Two-Phase Commit Protocol

☐ All goes well ($N$ servers)
  ☐ ($N-1$) *CanCommit*? messages and replies
  ☐ ($N-1$) *DoCommit* messages
  ☐ Message cost: proportional to $3N$
  ☐ Time cost: three rounds of messages
  ☐ *HaveCommitted* not counted

☐ Worst case
  ☐ Arbitrarily many server and communication failures
  ☐ Can tolerate succession of failures
  ☐ Guarantees to complete eventually (Do you agree?)
Performance (continued)

- Considerable delay to workers in uncertain states
- Occurs when the coordinator has failed and cannot reply to \textit{GetDecision} requests from workers
  - What is happening in this situation?
- Three-phase commit protocols have been designed to alleviate delays
Summary of Two-Phase Commit Protocol

- Distributed transactions involve several servers
- Atomicity requires that the servers participating in a distributed transaction either all commit or all abort
- Atomic commit protocols are designed to achieve this effect, even if servers crash during their execution
- 2PC protocol allows a server to abort unilaterally
  - Includes timeout actions to deal with delays due to servers crashing
  - 2PC protocol can take an unbounded amount of time to complete but is guaranteed to complete eventually
Distributed Concurrency Control

☐ Collection of servers of distributed transactions
   ➢ Jointly responsible for ensuring transaction performed in serial equivalent manner
   ➢ Each manages a set of objects and is responsible for ensuring that they remain consistent when accessed by concurrent transactions

☐ Transaction $T$ occurring before transaction $U$ at one server, it must be in that order at all servers

☐ Mechanisms
   ➢ Locking
   ➢ Timestamp ordering
   ➢ Optimistic concurrency control
Locks

- In a distributed transaction, the locks on an object are held by the server that manages it
  - The local lock manager decides whether to grant a lock or make the requesting transaction wait
  - It cannot release any locks until it knows that the transaction has been committed or aborted at all the servers involved in the transaction
  - The objects remain locked and are unavailable for other transactions during the atomic commit protocol
    - an aborted transaction releases its locks after phase 1 of the protocol
Distributed Deadlocks

- Single server transactions can experience deadlocks
  - Prevent or detect and then resolve
  - Use of timeouts on locks is clumsy
  - Detection is preferable
    - it uses wait-for graphs
    - transaction is aborted only when involved in deadlock

- Distributed transactions lead to distributed deadlocks
  - Construct global wait-for graph from local ones
  - A cycle in a global wait-for graph that is not in local ones is a distributed deadlock
Distributed Deadlock Detection

- A global wait-for graph can in theory be constructed from local ones
- There can be a cycle in the global wait-for graph that is not in any single local one
  - Distributed deadlock
  - Deadlock iff there is a cycle in the wait-for graph
- Detection of distributed deadlock requires a cycle to be found in global transaction wait-for graph distributed among the servers
  - Utilizes local wait-for graphs
  - Requires communication required between servers
## Interleavings of Transactions U, V, and W

### Servers X, Y, and Z

<table>
<thead>
<tr>
<th></th>
<th>U</th>
<th>V</th>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td>d.deposit(10)</td>
<td>lock D at Z</td>
<td>b.deposit(10) lock B at Y</td>
<td>c.deposit(30) lock C at Z</td>
</tr>
<tr>
<td>a.deposit(20)</td>
<td>lock A at X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b.withdraw(30)</td>
<td>wait at Y</td>
<td>c.withdraw(20) wait at Z</td>
<td>a.withdraw(20) wait at X</td>
</tr>
</tbody>
</table>

- d.deposit(10)
- a.deposit(20)
- b.withdraw(30)
- c.deposit(30)
- a.withdraw(20)
A transaction can only wait for one object at a time

Can leave out the objects, as in (b)
Distributed Deadlock Solutions

- Centralize deadlock detection
  - One server is global deadlock detector
  - Collects local wait-for graphs
  - Builds global wait-for graph and finds cycles
  - Decides how to resolve deadlock
  - Inform servers as to the transactions to be aborted

- Issues
  - Centralized approach has poor reliability
  - Transmitting local wait-for graphs is high
  - Can result in poor performance
Phantom Deadlocks

- Deadlock detected but not really a deadlock (phantom)
- Information about wait-for relationships between transactions eventually collected in one place
- There is a chance that the transaction holding a lock will release it and no deadlock will exist
  - Wait-for state can be old (stale)
- Simple phantom deadlocks will not arise if two-phase locks are used
  - Two-phase locking involves grow then shrink phases
- A phantom deadlock could be detected if a waiting transaction in a deadlock cycle aborts during the deadlock detection procedure
Local and Global Wait-For Graphs

local wait-for graph

local wait-for graph

global deadlock detector
Edge Chasing (Path Pushing)

- Global wait-for graph not constructed
  - Servers involved each know some edges
- Servers attempt to find cycles by forwarding messages called *probes*
  - Follow edges of the graph throughout system
  - Contains transaction wait-for relationships representing a path in the global wait-for graph
- When should a server send out a probe?
- Transaction starts at server and moves to participants
- At any point, a transaction can be either active or waiting at just one of these servers
Potential Distributed Deadlock

![Diagram showing a potential distributed deadlock with nodes C, D, V, Y, W, A, X, and U, with arrows indicating waiting for and held by relationships.]

- Added earlier: C, D, Z, V, B
- Just added: A, X, Y, U

Arrows indicate waiting for and held by relationships, creating a circular dependency that can lead to deadlock.
Edge Chasing (Path Pushing) (continued)

- Coordinator records active or waiting for a data item and participants can get this information
  - Lock managers inform coordinators when transactions start waiting or become active
- Coordinator informs workers when transaction is aborted and locks can be released and edges removed in local wait-for graphs
- Edge chasing has three steps:
  - *Initiation*: sending out probes on waiting events
  - *Detection*: receiving probes and detecting cycles
  - *Resolution*: aborting transactions to break deadlock
Edge Chasing (Path Pushing) (continued)

- **Initiation**
  - $T$ waits for $U$ where $U$ is waiting to access a data item at another server (potential deadlock)
  - Send probe containing edge $<T \rightarrow U>$ to server where $U$ is blocked
  - If $U$ sharing a lock, probes sent to holders of lock

- **Detection**
  - Receive $<T \rightarrow U>$: check to see if $U$ also waiting
  - If so and no cycle in probe, transaction it waits for is added to the probe $<T \rightarrow U \rightarrow V>$ and probe is forwarded if necessary

- **Resolution** aborts a transaction to break deadlock
Edge Chasing (Path Pushing) (continued)

- Before a server transmits a probe to another server, it consults the coordinator of the last transaction in the path to find out whether the latter is waiting for another data item elsewhere.
- Most often servers send probes to transaction coordinators which then forward them to the server of the data item the transaction is waiting for.
- Builds global wait-for graph one edge at a time.
- Deadlocks should be found provided waiting transactions do not abort and there are no failures.
  - $2(N-1)$ messages sent for a cycle involving $N$ transactions.
Probes Transmitted to Detect Deadlocks

\[ W \rightarrow U \rightarrow V \rightarrow W \]
Deadlock detected

\[ W \rightarrow U \rightarrow V \]
Initiation

\[ W \rightarrow U \]
\[ W \rightarrow U \rightarrow V \]

\[ W \rightarrow U \rightarrow V \rightarrow W \]

Held by
Waits for
Transaction Priorities

- Every transaction involved in a deadlock cycle can cause deadlock detection to be initiated
- Detection may happen at several different servers
- More than one transaction can be aborted
- Transactions are given priorities such that all transactions are totally ordered
  - Ensures that only one transaction aborted in a cycle
  - Transaction with the lowest priority is aborted
  - Might be used to reduce the number of situations that cause deadlock detected to be initiated
Two Probes Initiated

(a) initial situation

Waits for T

(b) detection initiated at object requested by T

Waits for T

(c) detection initiated at object requested by W

Waits for U

T → U → W → V

T → U → W
Transaction Priorities (continued)

- Detection initiated only when a higher priority transaction starts to wait for a lower priority one
  - Reduce # of probe messages by half

- Priorities used to reduce # of probes forwarded
  - Probes should travel “downhill” from transactions with higher priorities to transactions lower
  - Servers do not forward any probe to a holder with higher priority than the initiator
  - The order in which transactions start waiting can determine whether or not deadlock will be detected
Transaction Priorities (continued)

☐Probe queue
   - Save copies of all the probes received on behalf of each transaction

☐Transaction starts waiting for a data item
   - Forwards the probes in its queue to the server of the data item which propagates probes downhill

☐Algorithm requiring probes stored in probe queues
   - Arrangements to pass on probes to new holds
   - Discard probes for committed/aborted transactions
   - Adds to the complexity of edge-chasing
Probes Travel Downhill

(a) V stores probe when U starts waiting

(b) Probe is forwarded when V starts waiting
Recovery

- Recovery necessary for failure atomicity and durability of transactions
- Recovery manager helps make this happen
  - Saves objects in permanent store for committed transactions
  - Restores server objects after a crash
  - Manage layout of permanent store to improve performance of recoveries
  - Clean up and optimize space usage of permanent store
Recovery and Permanent Store

☐ In distributed transactions, we have a two (or more) phase protocol

☐ Before actual commit occurs, distributed servers agree that they are prepared to commit
   ☑ This must be recorded to permanent store before sending their response to the coordinator

☐ The recovery manager also maintains a list of objects and corresponding values created by active transactions
   ☑ “Tentative versions” of objects
   ☑ Commitment causes tentative versions to replace committed versions
Logging

- Common technique
- Historical record of transactions performed by a server
  - Values, transaction status, intention lists
  - Ordered by order in which transactions occurred (started, committed, aborted)
- Think of the log as a sophisticated version history repository
  - Maintain historical record of changes and operations
  - Allow restoration of the most recent valid snapshot of the system when recovering from crash