CS 4457A/9657A: Computer Networks II

Securing UAVs systems by consortium based blockchain

Presented by:

Hardeep Singh Raike
Ria Ria
Aasminpreet Singh Kainth
Sai Lakshmi Pravallika

UAV

A UAV (Unmanned Aerial Vehicle) or UAS (Unmanned Aerial System) is any aircraft that can navigate without a human pilot on board.

Different Types of UAV:

- Multi Rotor Drones (Application-Aerial Photography)
- Fixed Wing Drone. (Needs training to run this)
- Single Rotor Drone.(More Fly time)
- Hybrid VTOL(Application- Amazon Prime Delivery)

Modern UAV looks like

Different Application of UAV

1) Logistic Process.
   a) Transport drones
   b) Smart Inventory drones
   c) Delivery drones(e.g. Prime Air, DHL-Pakecopter)
   d) Warehouse management drones
2) The Military
3) NASA
4) Crowd Surveillance
5) Disaster Management

Why UAVs are important ?

Savings in distribution cost.

Faster deliveries.

Possibility of **reaching areas that are difficult to access.**

They reduce urban traffic and **CO2 emissions**.

Helps to **control inventories** and movements within the warehouse itself.

No shifts are needed: drones can operate 24 hours 365 days a year

Problem Statement

UAV are being used to most of the applications in distributed manner for e.g. to in inventory management tasks, Disaster relief. But, such distributed operations make them susceptible to cyber attacks.

Prime objective is to obtain the secure UAV ecosystem over in distributed setting along with minimum latency.

Public Block Chain Concept

Type of distributed ledger.

Comprises of unchangeable, digitally recorded data in packages called blocks.

These digitally recorded blocks of data is stored in linear chain.

Each block in chain contains the information which is cryptographically hashed.

The block of hashed data drawn upon the previous-block in the chain.

Thus, it ensures all data in overall “blockchain” has not been tampered with and remains unchanged.

Block Chain help in achieving Proactive distributive data management

Because of distributed ledger, each party involved in task is connected with the others.

Improve efficiency .

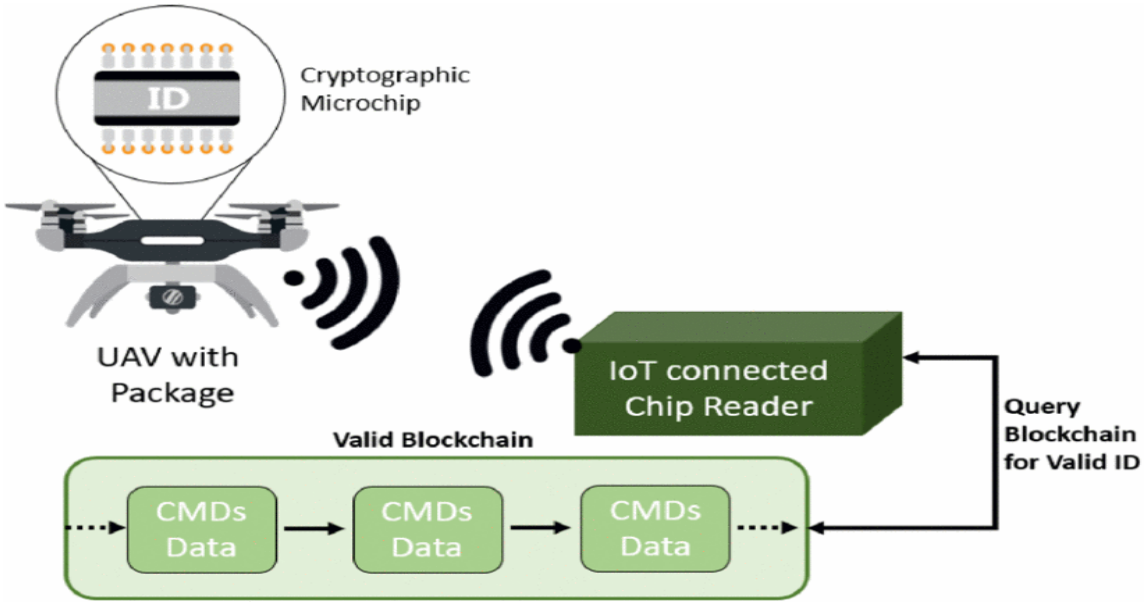
It helps to maintain real time data. Records, are stored and available to everyone within the network.

Predict market demand more accurately in case of inventory management as data can’t be tampered and database is continuously evolving.

Block chain itself is a database, thus we don’t need any other database.

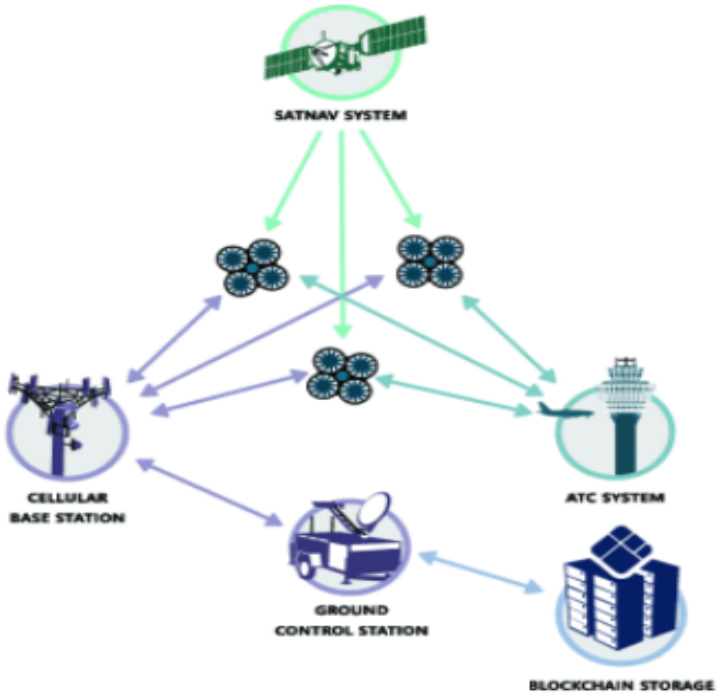
Relevant work

A company named chronicled has developed a prototype solution to use Cryptographic microchips as identifiers for UAV's and use IoT connected chip reader device to check for UAV's unique signature in blockchain network to authenticate UAV for Package delivery.



Relevant work

UAVNet to based on blockchain structures.



(1) Blockchain as a external storage

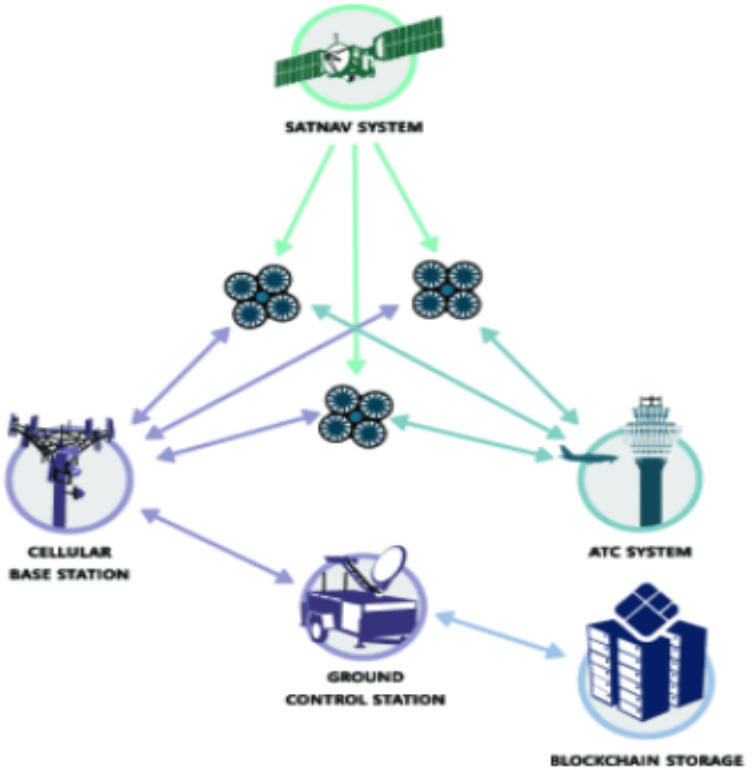
Relevant work

Storing the ledger on small UAV.

However, Heavy computations required by blockchain for PoG consensus algorithm is also a challenge for UAVs to undertake as they are resource constrained devices.

The entities in the participating in the blockchain network are not trusted by any central authority.

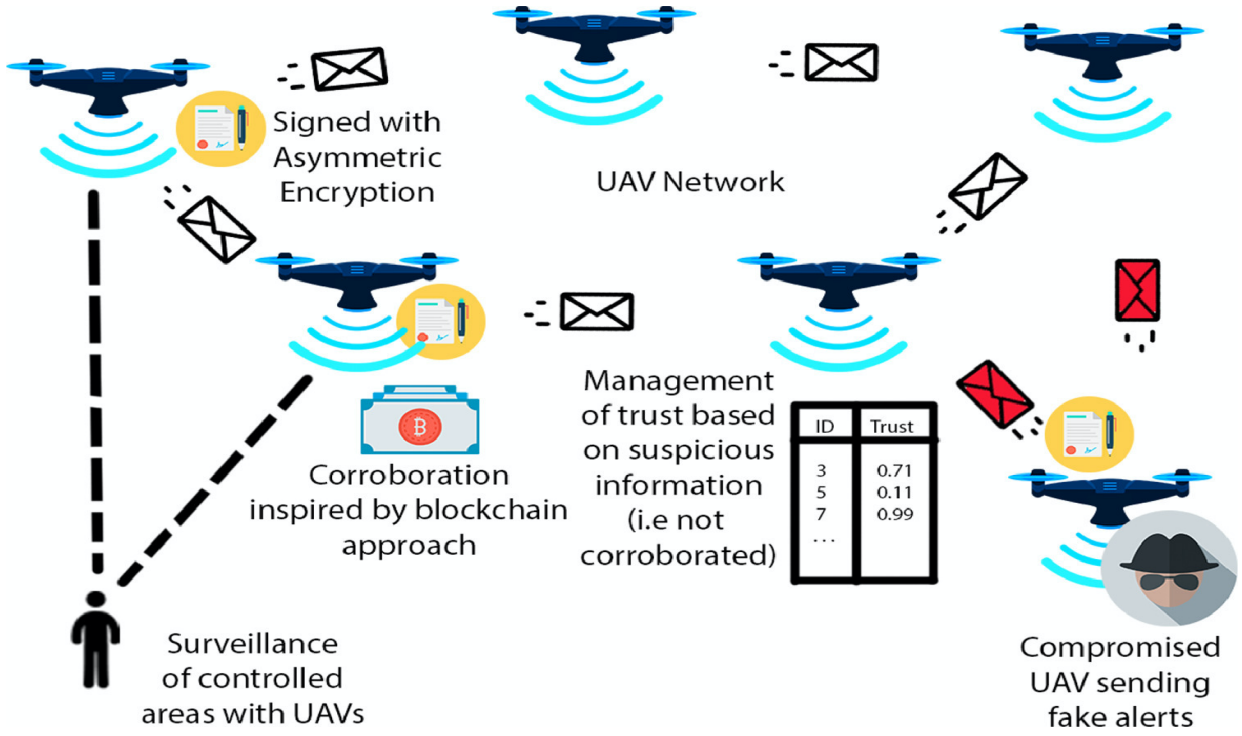
As Blockchain is public here not confidential.



(1) Blockchain as a external storage

Relevant work

Another research have used principles of blockchain to maintain security in UAV networks for surveillance and detect compromised UAVs based on trust policies.



What we have strived to improve ?

As UAV's are used in many application to collect data so the data store must fulfill following security requirements -

Trusted origin of data – it must determined that the data originated from a valid Actor not from any intruder or malicious UAV.

Confidentiality – The data store must be encrypted using strong encryption algorithm and only the entities provided access must be able to decrypt the data.

Immutability of data – The data storage used to store the data collected by UAV's must be practically immutable. However maintaining data integrity in distributed database scenario's with muti-party compute is difficult task.

What we need to improve ?

Reliability – The distributed nature of blockchain based data storage removes the possibility of Single point failure.

Known identities – In multi party secure network for UAV's the identity of each member involved should be known and controlled whereas in public blockchain the members are untrusted and anonymous.

Accountability – If any anomaly is detected, the malicious entity should be identified for further investigation with immediate revocation of access permission by the central authority.

Efficiency and throughput – As UAV's are used in mission critical application so it should be computationally intensive to ensure the data integrity as in public blockchains. As public blockchains use proof of work as consensus algorithm.

How we address the problem?

Securing UAV ECO-SYSTEM

a) Confidential Consortium Framework(CCF) by Microsoft Azure helps to minimize transmission latency and enhance security.

b) Main features of CCF:

1. Block Chain
2. Consensus Algorithm, i.e., RAFT
3. Trusted Execution environment, i.e., TEE

Why we have chosen a Consortium Framework?

It is assumed to be more faster as compared to blockchain.

As it removes the consensus overhead and keep the execution simple.

Trusted network of enclaves running on physical nodes which is backed by TEE.

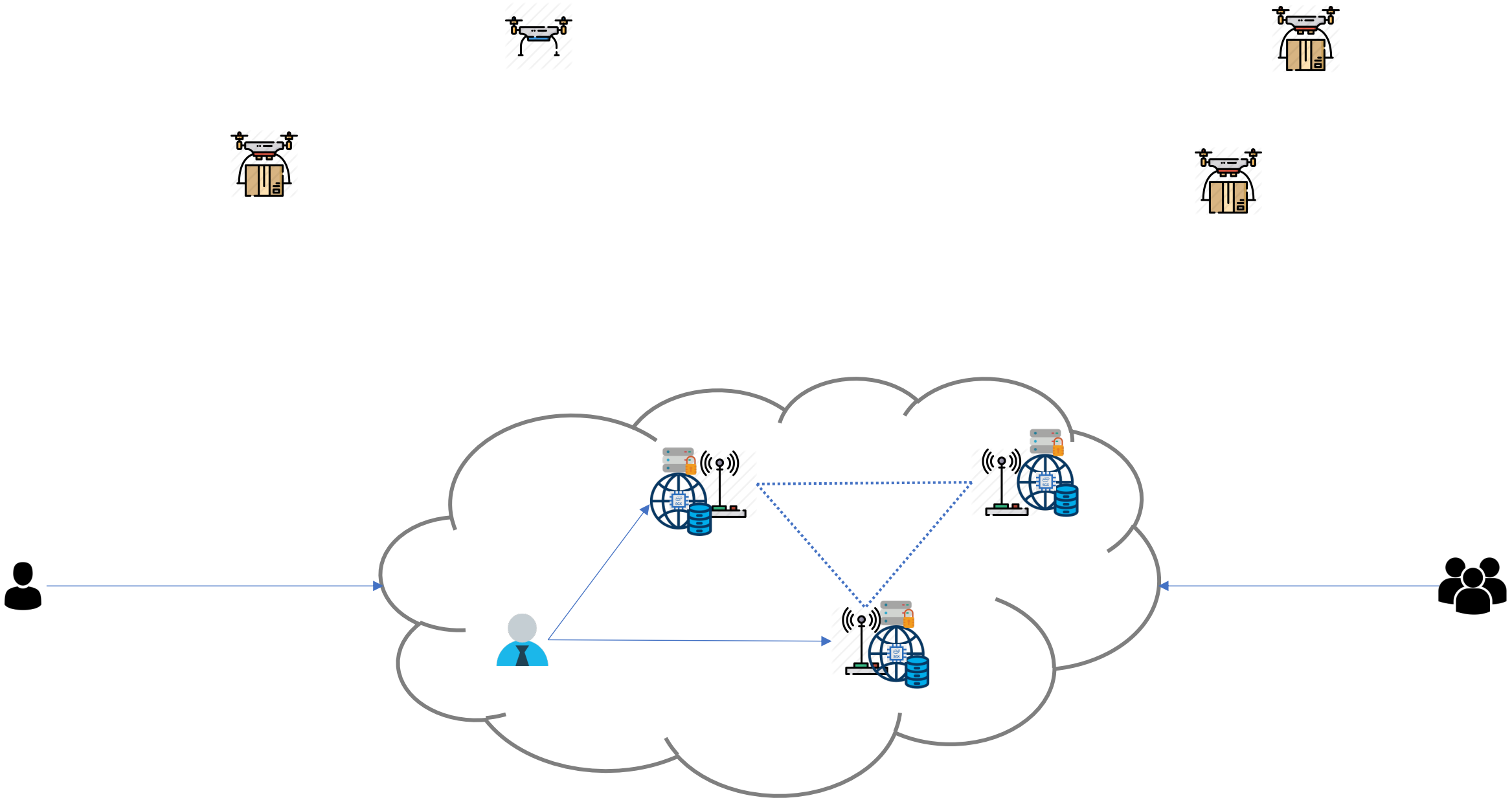
TEE guarantees code and data loaded inside to be protected with respected to be protected with respect to confidentiality and integrity.

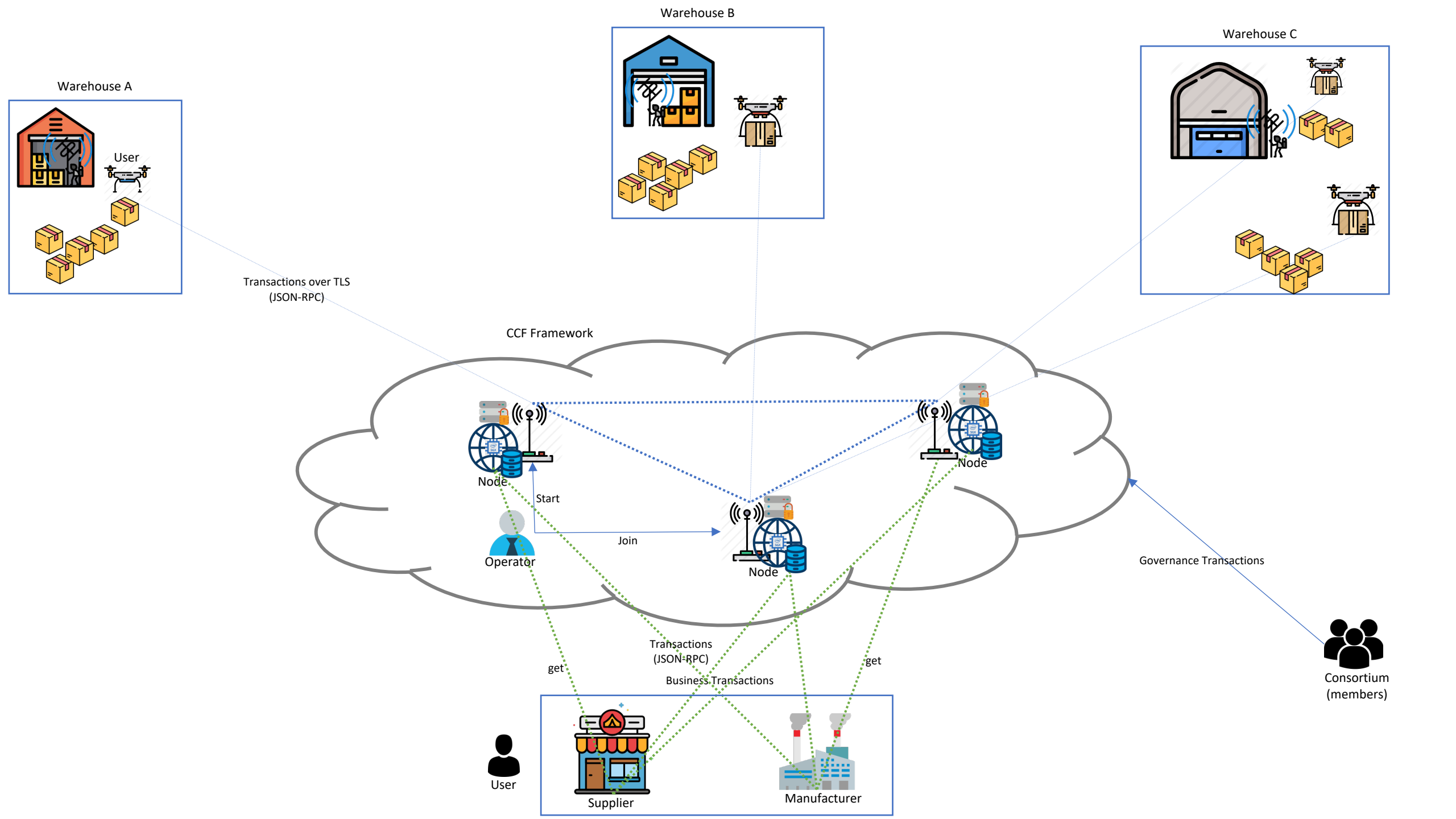
CCF(Confidential Consortium Framework)

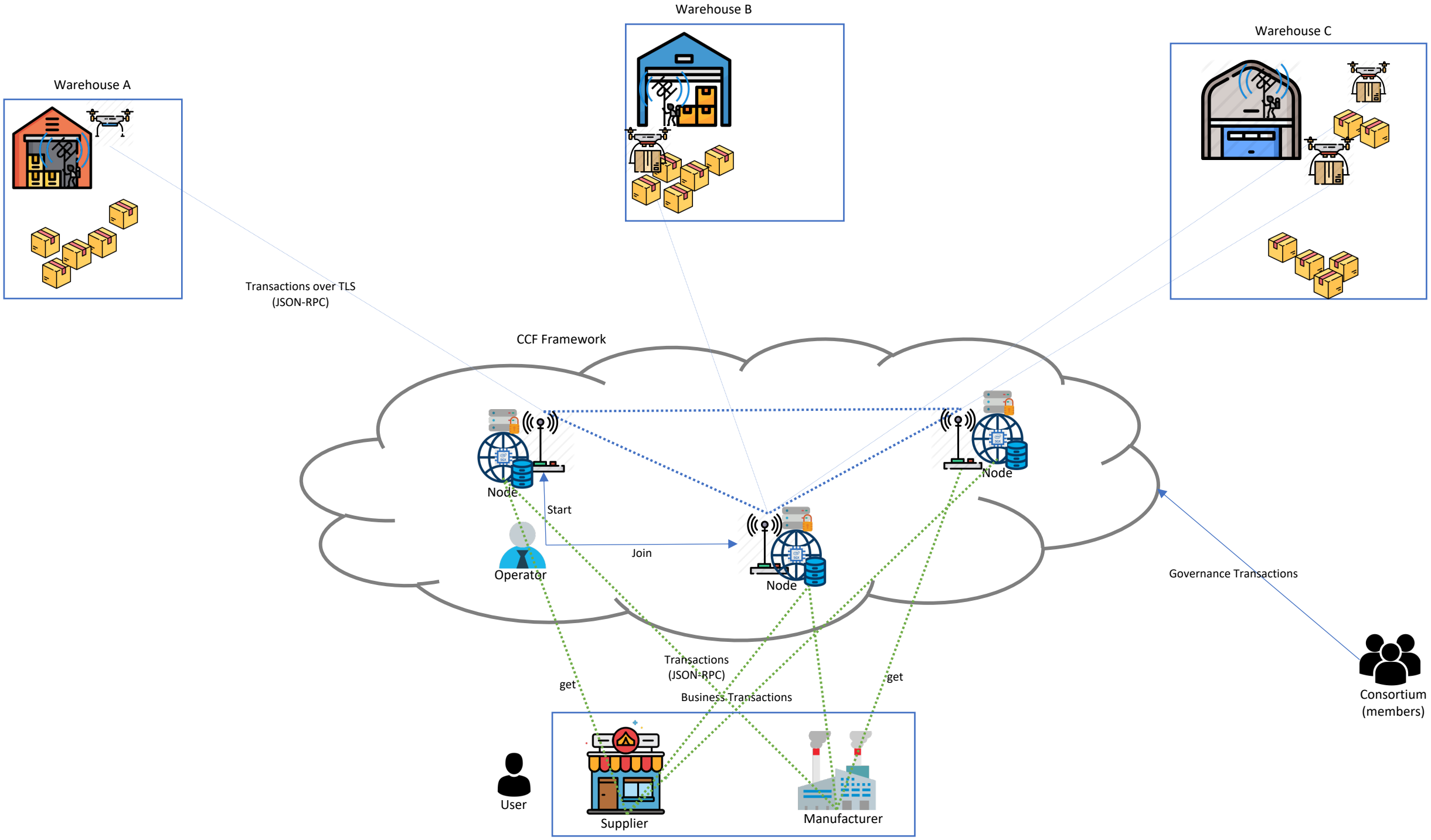
An open source confidential block chain network.

Key Components of CCF:

1. TEE(Trusted Execution Environment): Secure area of main processor. Example: Intel-SGX
2. Decentralized Database System: A database that is installed on systems that are geographically located at different locations. Example: Orbit DB
3. Cryptography: Highly secured Hashing algorithms. Example: SHA2-256




Warehouse A
User
Warehouse B
Warehouse C
Transactions over TLS
(JSON-RPC)
CCF Framework
Node
Start
Join
Operator
Node
Node
Governance Transactions
Consortium
(members)
Transactions
(JSON-RPC)
Business Transactions
get
get
User
Supplier
Manufacturer

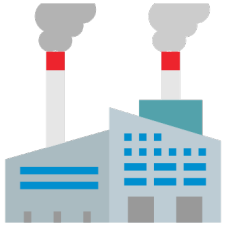

Warehouse A
Warehouse B
Warehouse C
Transactions over TLS
(JSON-RPC)
CCF Framework
Node
Node
Node
Start
Join
Operator
Governance Transactions
Consortium
(members)
Transactions
(JSON-RPC)
Business Transactions
get
get
User
Supplier
Manufacturer

Clients

Operator

User

Supplier

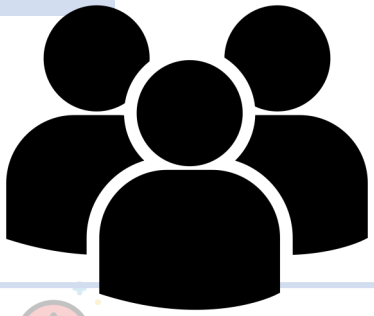


Manufacturer

Consortium
(members)

Clients

Consortium (members)



Operator

User

Supplier

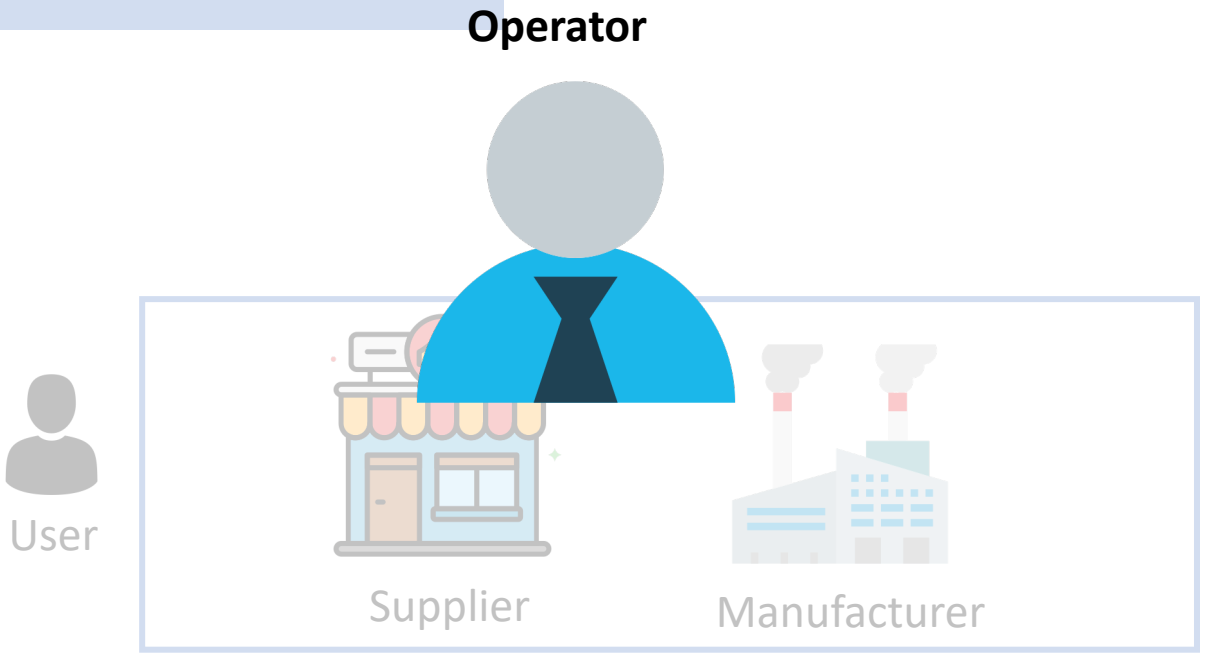
Manufacturer

constitute the consortium

follow the constitution

unique proposal id

Clients



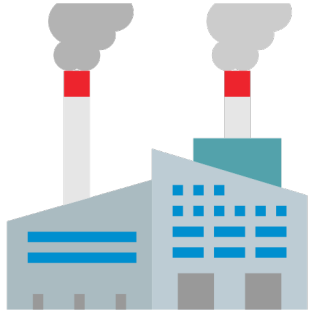
in charge of operating a CCF network

identities are not registered

Entities

User

Supplier



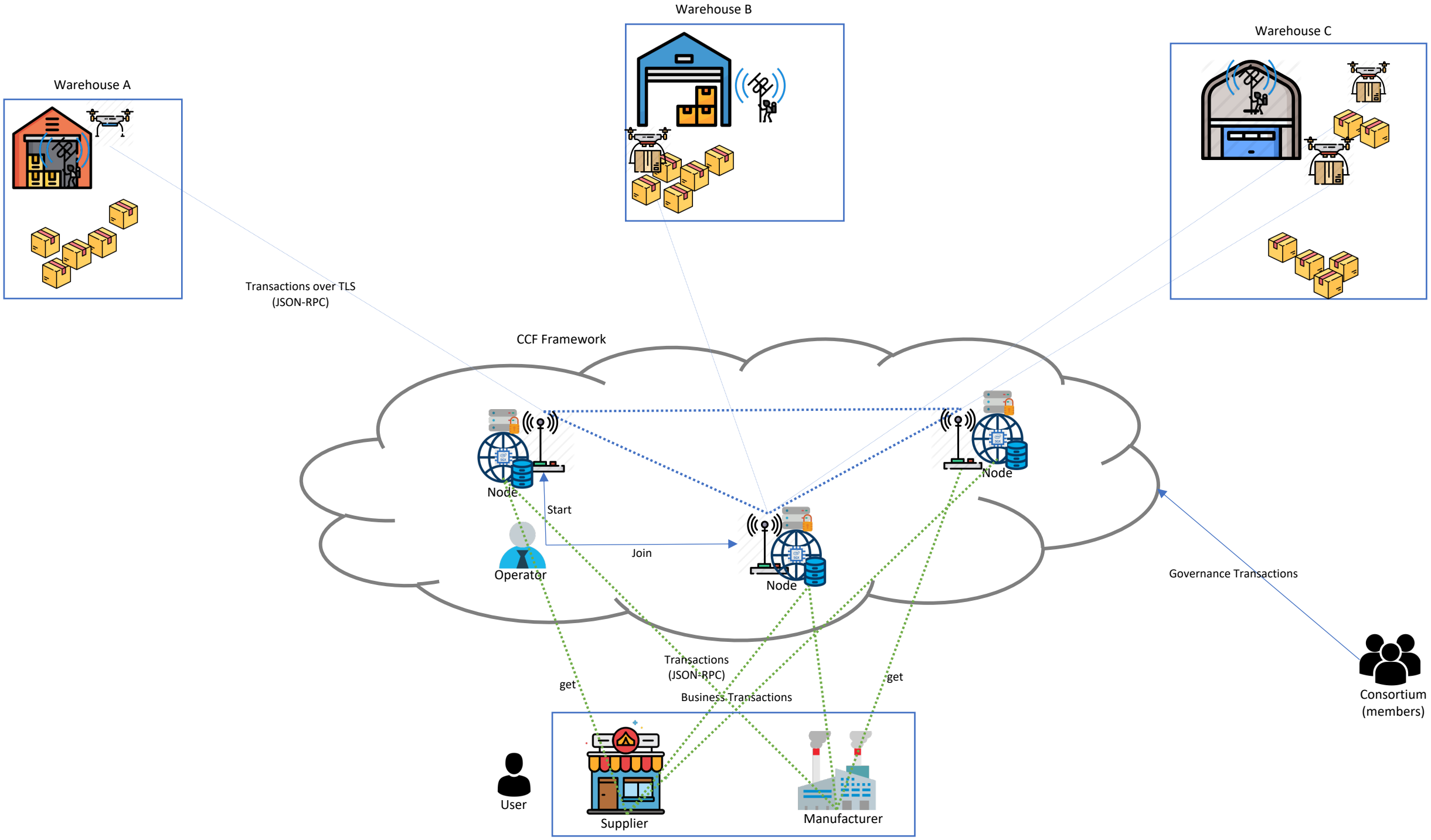
Manufacturer

Operator

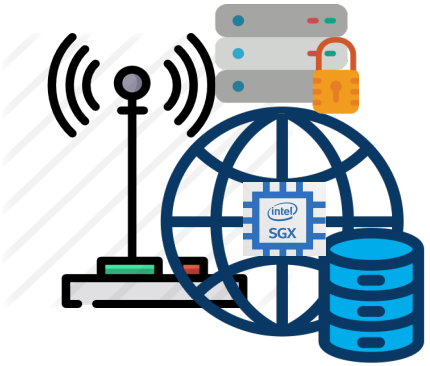
Consortium
(members)

directly interact with the transaction engine/application

public identity should be voted

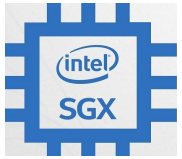

Warehouse A
Warehouse B
Warehouse C
Transactions over TLS
(JSON-RPC)
CCF Framework
Node
Start
Join
Operator
Node
Node
Governance Transactions
Consortium
(members)
Transactions
(JSON-RPC)
Business Transactions
get
get
User
Supplier
Manufacturer

Node



Node

Private Network

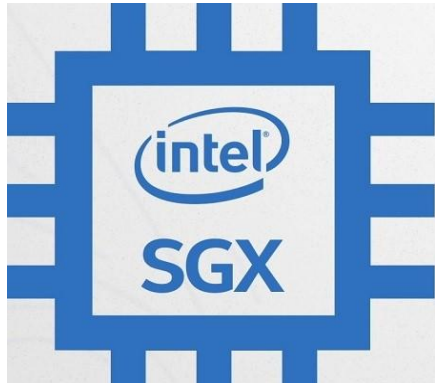


Open Enclave Engine

Distributed Ledger

Node

Private Network



Open Enclave Engine

Distributed Ledger

template generation tool

defines private region of memory

Intel Software Guard Extensions

Node

Private Network

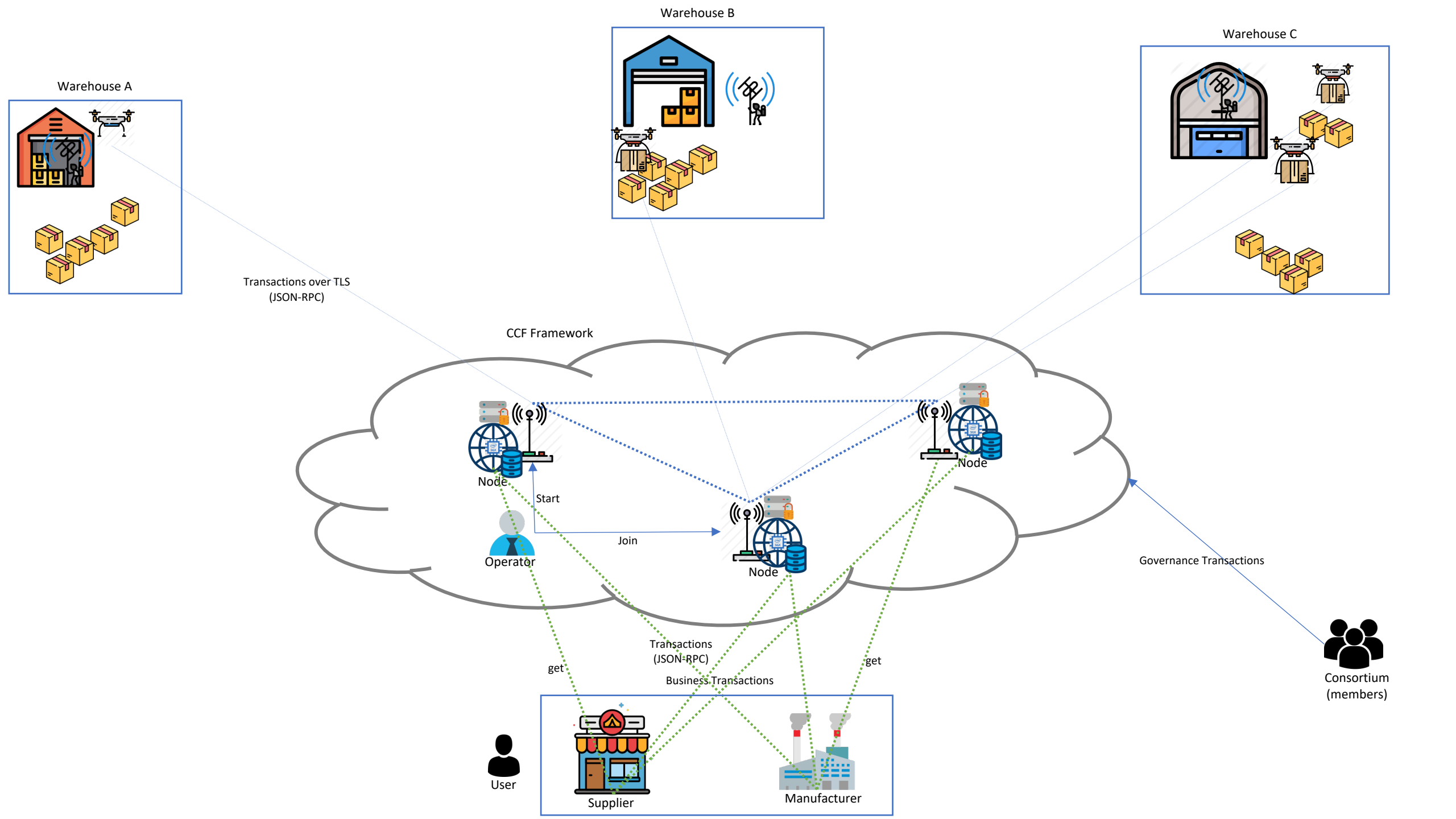
Distributed Ledger

Node

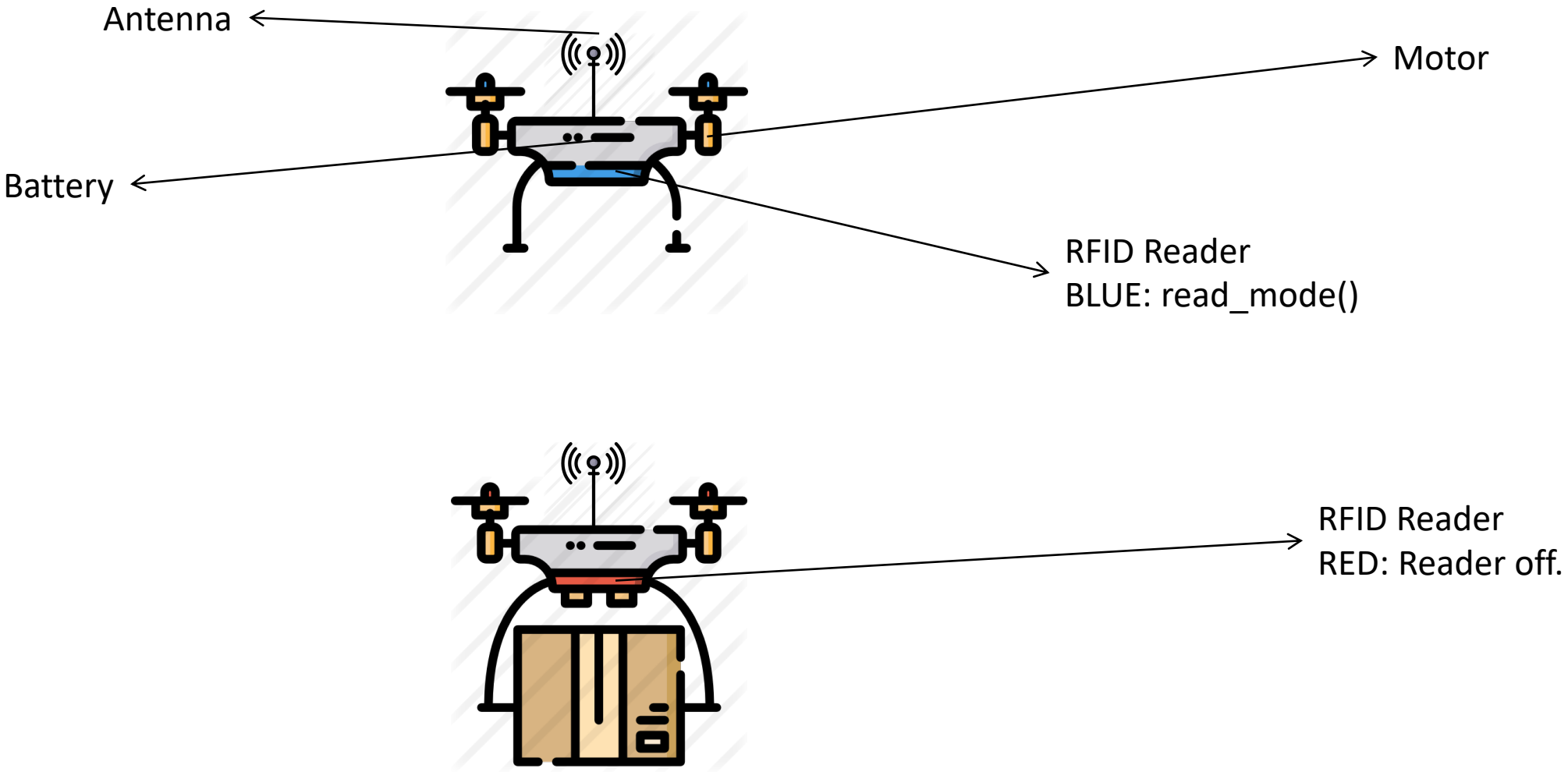
Private Network

Distributed Ledger

intra node communications


Warehouse A
Warehouse B
Warehouse C
Transactions over TLS
(JSON-RPC)
CCF Framework
Node
Node
Node
Start
Join
Operator
Governance Transactions
Consortium
(members)
Transactions
(JSON-RPC)
Business Transactions
get
get
User
Supplier
Manufacturer

Multi-Rotor Drone



Advantages of blockchain implemented on CCF Framework

Throughput and latency approaching database speeds

Richer, more flexible confidentiality models

Network and service policy management through non-centralized governance

Improved efficiency versus traditional blockchain networks

RAFT-Consensus Algorithm

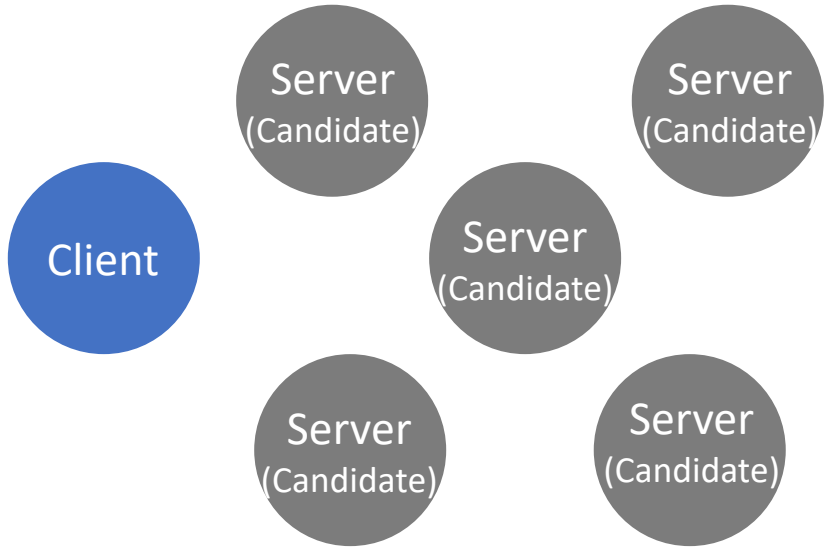
Raft states that each node in a replicated state machine can stay in any of the following three states:

Leader: Only the server elected as leader can interact with the client.

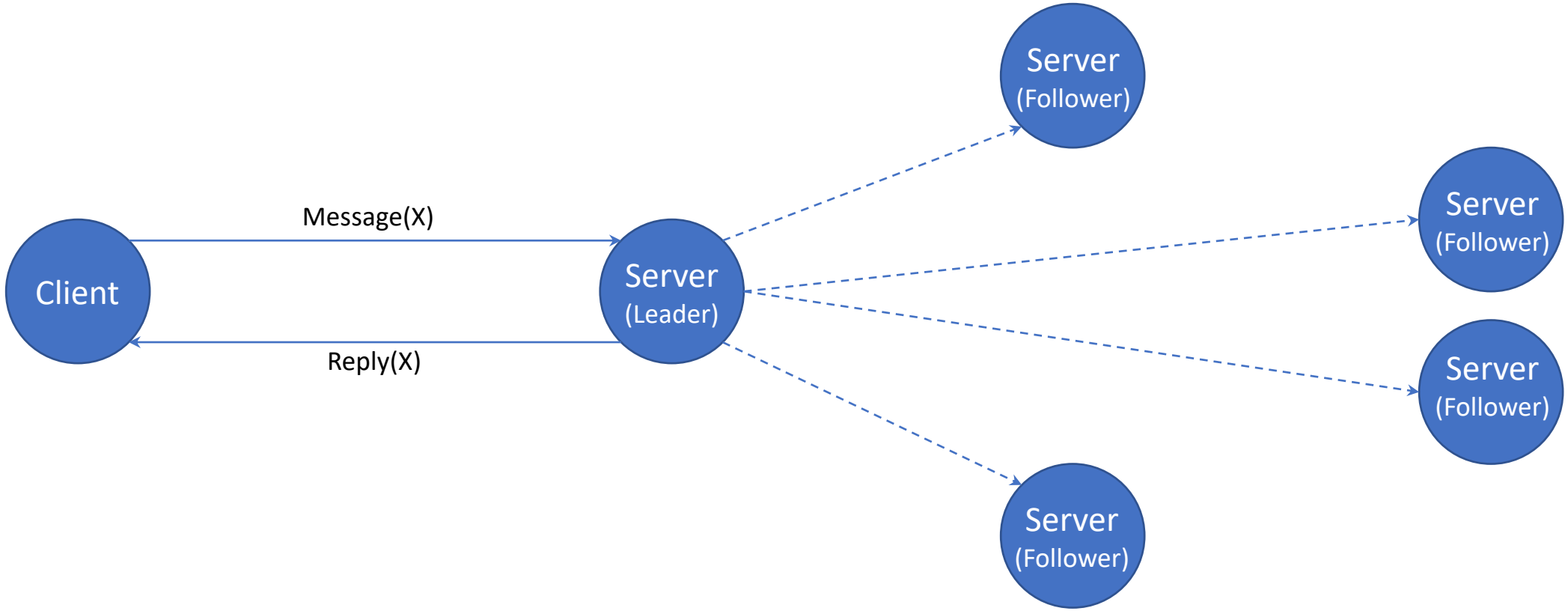
Candidate: At the time of contesting an election to choose the leader server, the servers can ask other servers for votes. Initially, all servers are in the Candidate state.

Follower: Follower servers sync up their copy of data with that of the leader's after every regular time intervals.

Raft Algorithm explained



Raft Algorithm explained



RAFT-Consensus Algorithm

Raft algorithm uses two types of Remote Procedure Calls(RPCs) to carry out the functions :

RequestVotes RPC is sent by the Candidate nodes to gather votes during an election.

AppendEntries is used by the Leader node for replicating the log entries and also as a heartbeat mechanism to check if a server is still up. If heartbeat is responded back to, the server is up else, the server is down.

Election can takes place in three ways:

1. The Candidate node becomes the Leader by receiving the majority of votes from the other nodes and will start sending the heartbeats

2. If the candidate node doesn’t receive majority votes then the term ends up with no leader.

3. If the candidate node requesting vote has lesser term number then, it is rejected and all other nodes retains their candidate state, if the term number is greater, then it is elected as Leader

Leader Election

To maintain these server status, the Raft algorithm divides time into small terms of arbitrary length. Each term is identified by a monotonically increasing number, called **term number**.

If no majority is established, the situation is called a **split vote** and the term ends with no leader.

Raft uses randomized election timeouts to ensure that split votes are rare and that they are resolved quickly. To prevent split votes in the first place, election timeouts are chosen randomly from a fixed interval.

Log Replication

After the leader has been elected, every request is sent to this node. If a follower node receives a request it can just redirect it to the leader or return an error to the client, indicating which node is the leader.

When the leader receives a request, it first appends it to its log, and then send a request to every follower. But the request is not committed yet.

The request will be committed after leader receives the majority confirmation from nodes.

When the followers receive the next heartbeat message they know they can also commit this message.

Challenges

1. Hardware Limitations.

2. Lack of relevant research material.

3. Block-Chain is an emerging technology. Thus, many areas are yet to be explored.

Road Map for upcoming days

Analyse the performance of RAFT in our current framework (Target: 10th December 2019).

Research Paper (Target: 20th December 2019)

Review and Proof Reading (Target: 22nd December 2019)


Warehouse B
Warehouse C
Warehouse A
User
QUESTIONS?
Node
Node
Start
Join
Operator
Node
Governance Transactions
Consortium
(members)
Transactions
(JSON-RPC)
get
get
Business Transactions
User
Supplier
Manufacturer


Warehouse A
Warehouse B
Warehouse C
Transactions over TLS
(JSON-RPC)
CCF Framework
Consortium
(members)
Node
Node
Node
Start
Join
Operator
Governance Transactions
Transactions
(JSON-RPC)
get
get
Business Transactions
User
Supplier
Manufacturer

THANK YOU.