BC Data Management Benefits by Increasing Confidence in Datasets Supporting AI and Analytical Tools using Supply Chain Examples (blockchain for software system safety)

Based on Research Project:
Blockchain Technology in Support of Navy Logistics and Global Supply Chains

PI: Tony Kendall (Information Sciences)
Arijit Das (Computer Sciences)
Bruce Nagy (NAWC, Weapons Division)
Avantika Ghosh (Intern, UC Berkley)

Agenda

- What is system safety
- Quick review of Hyperledger Fabric (HLF) blockchain technology
- Review of blockchain project for Navy Supply Chain
- Review of new blockchain use cases for software system safety in support of data and training set integrity and provenance.

What is System Safety?

A risk management strategy based on identification, analysis of hazards, and application of remedial controls using a systems-based approach.

Motivation for Using HLF

- Consensus based providing tracking of assets, provenance and integrity of the data (immutability)--traceable and transparent.
- Datasets and training sets are also assets so BC can be used.
- AI/ML and system safety for data usually falls into the two highest software control categories:
  - Level 1(Autonomous)
  - Level 2 (Semi-Autonomous), MILSTD-882E.
- Threats to training sets include AI poisoning, etc.
- **Bonus**: Data scientists/analysts need to find and quickly access trusted datasets, algorithms, models.

Three Hyperledger Platforms

- IBM/Oracle Blockchain Demo (using HLF with consensus BC)
- Hyperledger Fabric Linux Foundation version on NPS Linux Virtual Machine.

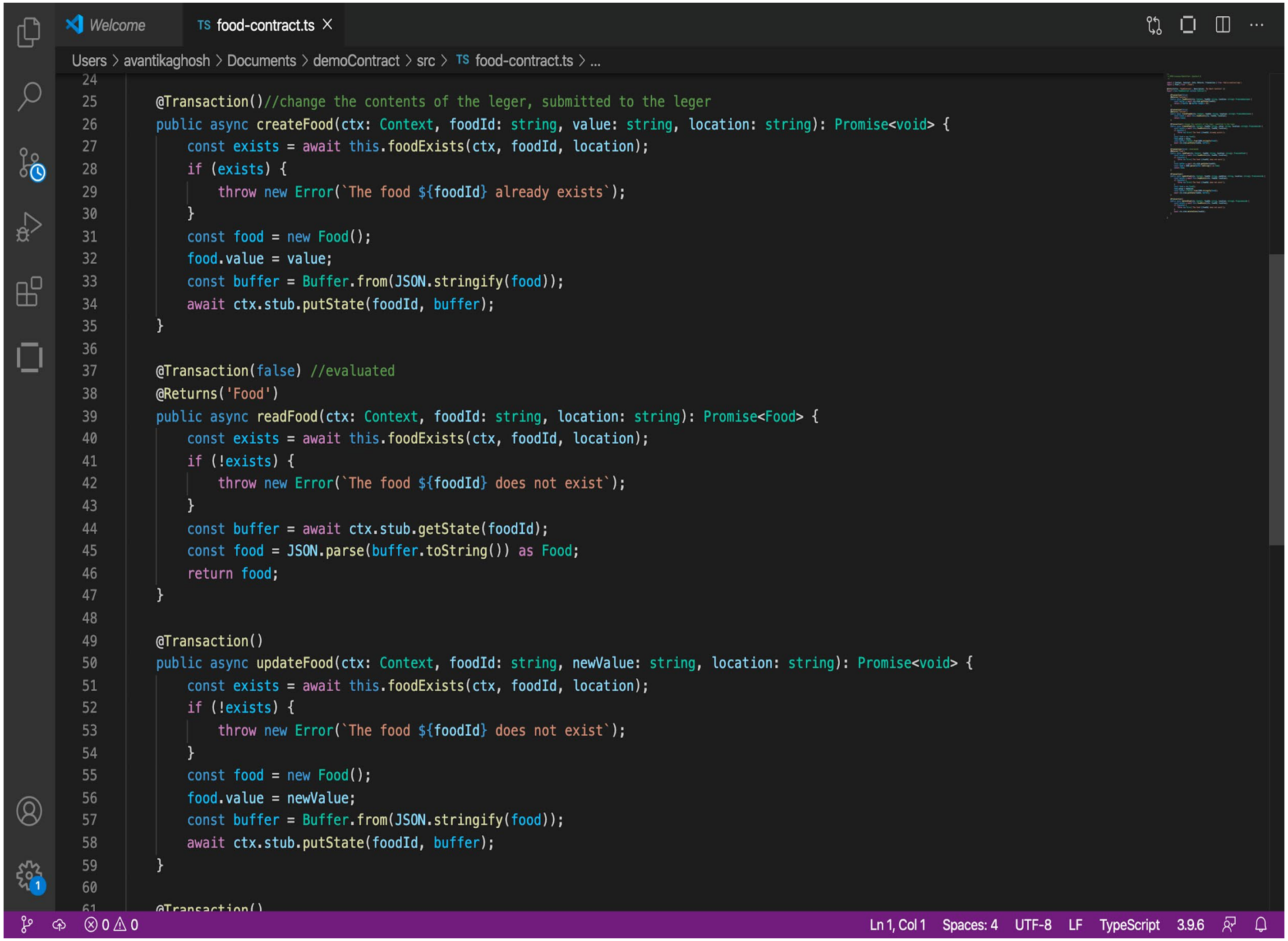
Supply Chain Research Questions

Our focus is finding a Blockchain use case for Navy Logistics and Global Supply Chain such as the CLO (Combat Logistics Office) as well as other possible use cases. Specifically:

Three Use Cases

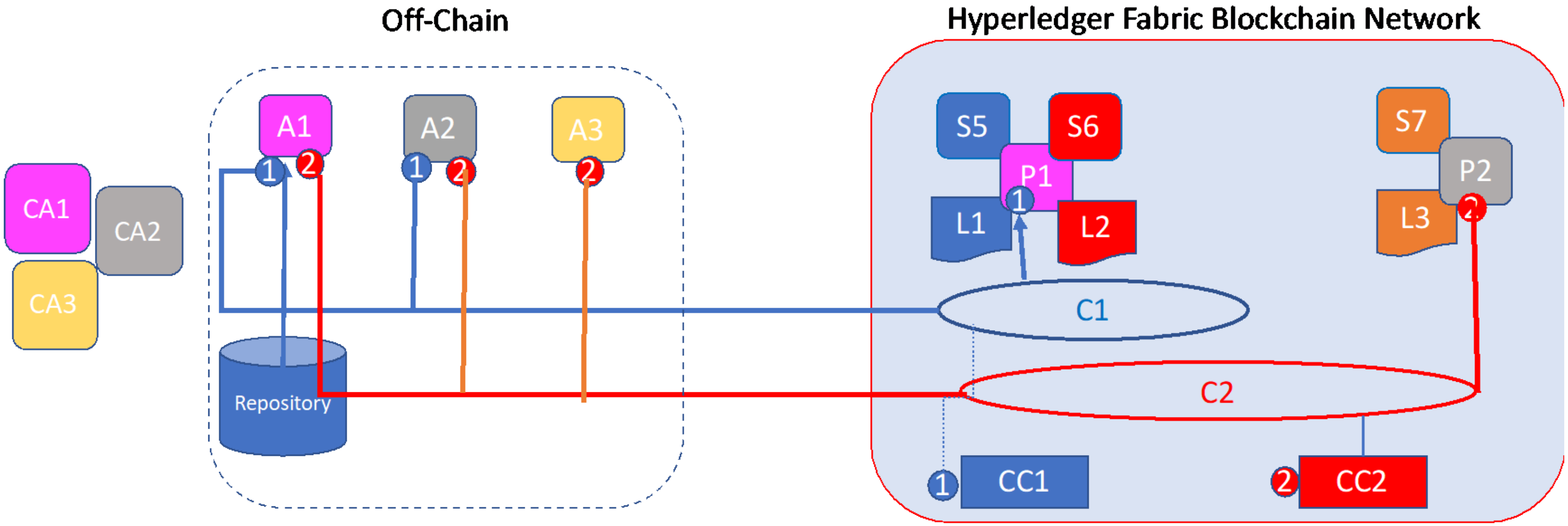
1. Financial and inventory transaction audit trails
2. Serial number tracking
3. Maintenance log integrity.

Sample smart contract for tracking food shipments (Language: Typescript)


Welcome
TS food-contract.ts ×
Users › avantikaghosh › Documents › demoContract › src › TS food-contract.ts › ...
⊗ 0 ⚠ 0
Ln 1, Col 1
Spaces: 4
UTF-8
LF
TypeScript
3.9.6

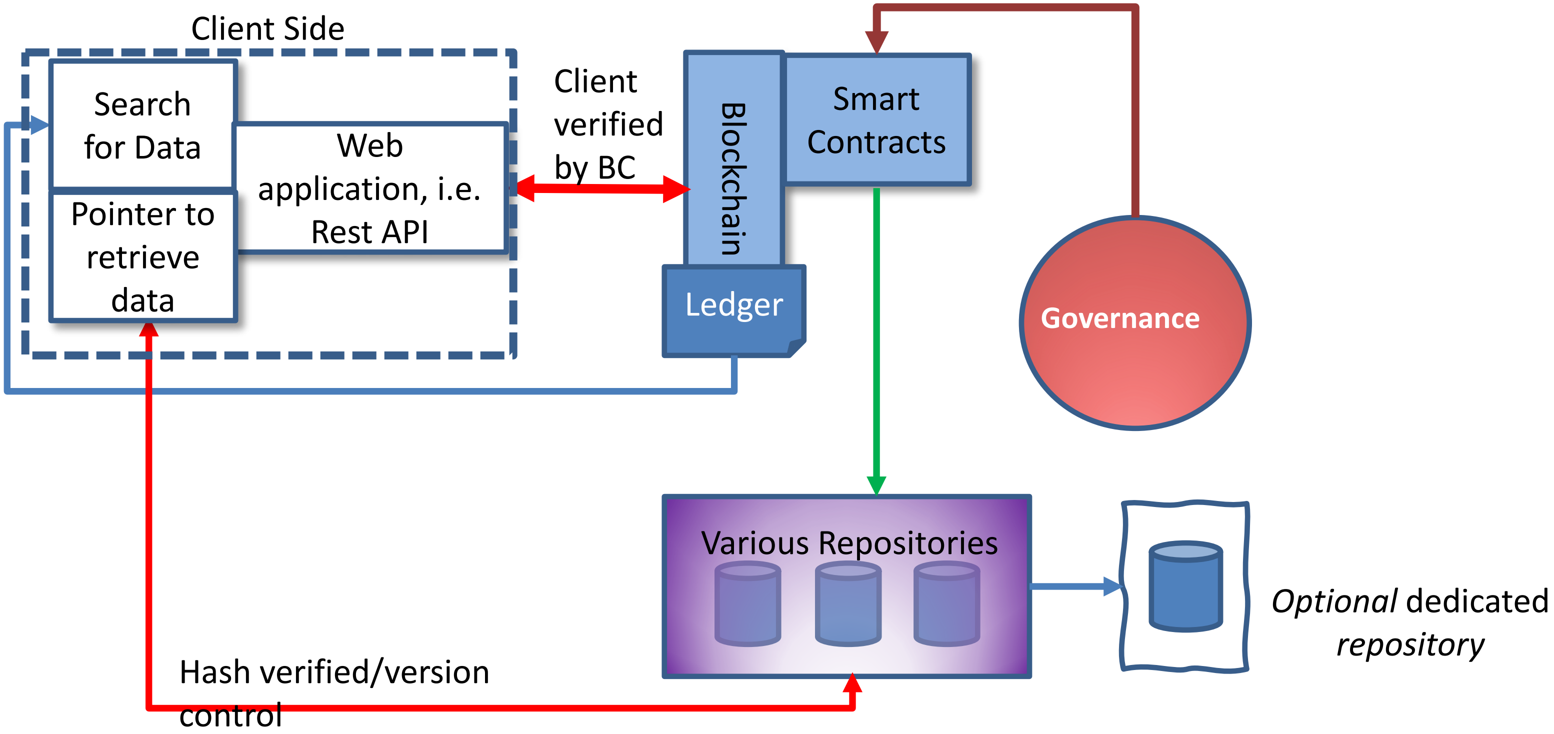
```typescript

    @Transaction()//change the contents of the leger, submitted to the leger
    public async createFood(ctx: Context, foodId: string, value: string, location: string): Promise<void> {
        const exists = await this.foodExists(ctx, foodId, location);
        if (exists) {
            throw new Error(`The food ${foodId} already exists`);
        }
        const food = new Food();
        food.value = value;
        const buffer = Buffer.from(JSON.stringify(food));
        await ctx.stub.putState(foodId, buffer);
    }

    @Transaction(false) //evaluated
    @Returns('Food')
    public async readFood(ctx: Context, foodId: string, location: string): Promise<Food> {
        const exists = await this.foodExists(ctx, foodId, location);
        if (!exists) {
            throw new Error(`The food ${foodId} does not exist`);
        }
        const buffer = await ctx.stub.getState(foodId);
        const food = JSON.parse(buffer.toString()) as Food;
        return food;
    }

    @Transaction()
    public async updateFood(ctx: Context, foodId: string, newValue: string, location: string): Promise<void> {
        const exists = await this.foodExists(ctx, foodId, location);
        if (!exists) {
            throw new Error(`The food ${foodId} does not exist`);
        }
        const food = new Food();
        food.value = newValue;
        const buffer = Buffer.from(JSON.stringify(food));
        await ctx.stub.putState(foodId, buffer);
    }

    @Transaction()
```

Hyperledger Blockchain for System Safety (Use Case Examples)



Note: Does not include all blockchain elements.

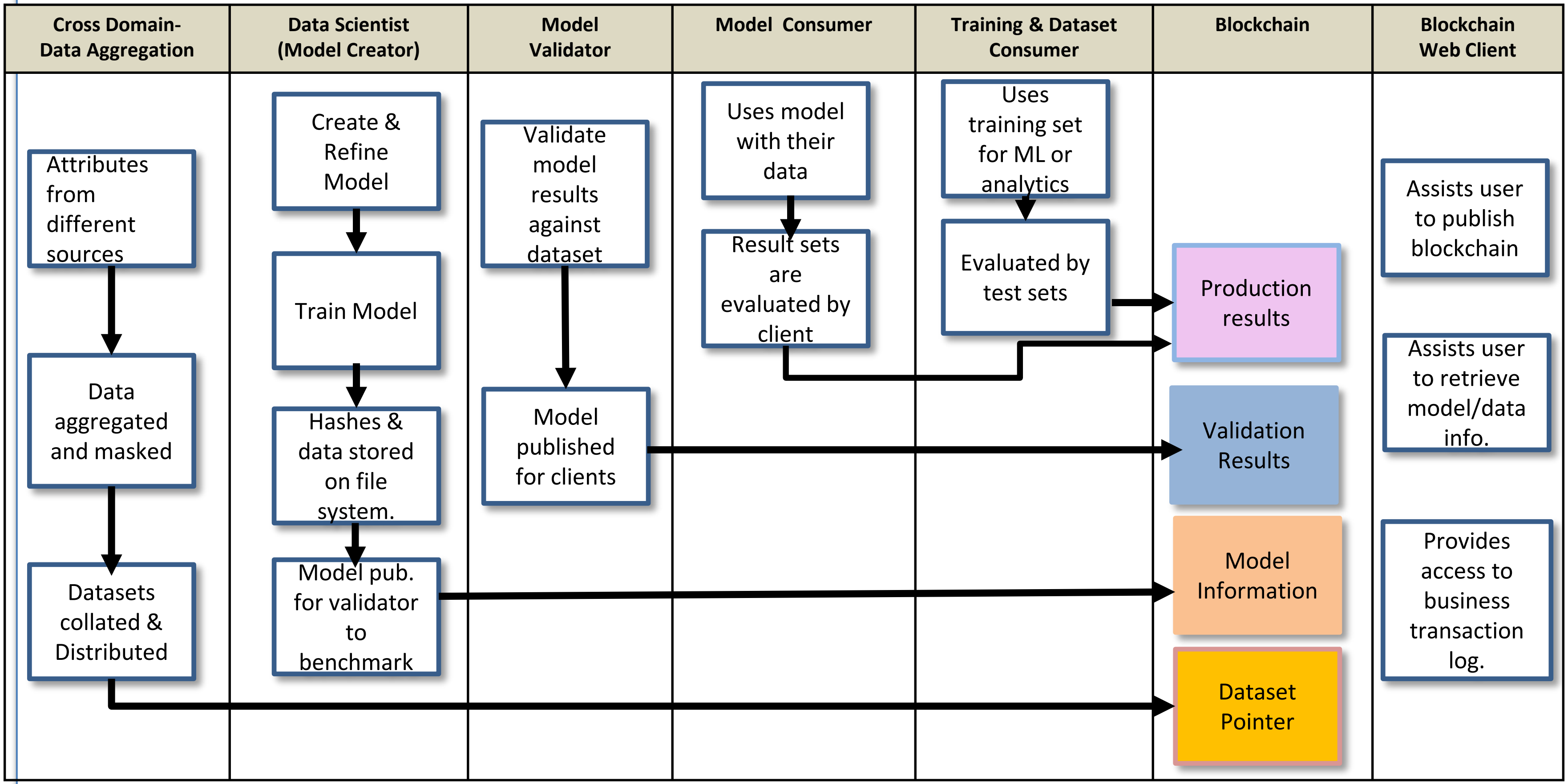
Data Scientist Use Case Example



Federated Learning (FL)

- Collaborative ML technique whereby the devices collectively train and update a shared ML model while preserving their datasets.
  - Some devices on the edge may prove untrustworthy
  - Reputation-aware FL
    - Trust through BC consensus
    - Trust algorithms implemented through BC smart contracts.
    - Integration of certain non-DoD IoT devices on the edge through HLF.

Various Scenarios using HLF



Cross Domain-Data Aggregation

Attributes from different sources

Data aggregated and masked

Datasets collated & Distributed

Data Scientist (Model Creator)

Create & Refine Model

Train Model

Hashes & data stored on file system.

Model pub. for validator to benchmark

Model Validator

Validate model results against dataset

Model published for clients

Model Consumer

Uses model with their data

Result sets are evaluated by client

Training & Dataset Consumer

Uses training set for ML or analytics

Evaluated by test sets

Blockchain

Production results

Validation Results

Model Information

Dataset Pointer

Blockchain Web Client

Assists user to publish blockchain

Assists user to retrieve model/data info.

Provides access to business transaction log.

Adapted from Oracle

Special Thanks to:

System Safety Topic Sponsor:
Naval Ordnance Safety and Security Activity (NOSSA)

System Safety Topic PI: Dr. Bonnie Johnson
Naval Postgraduate School

Logistics Topic Sponsor: CAPT Lugo
OPNAV N414
Supply Chain Operations - Emerging and Logistics IT

Tom Plunkett
Consulting Solutions Director
Oracle Consulting

Keyauri Kendrick
IBM Federal
Technical Solutions Specialist

Our Interns:
Avantika Ghosh (UC Berkley)
Aroshi Ghosh (Santa Clara HS)

Virtual Labs (via VPN)

- Oracle Database for GCSS-MC
- Aviation Maintenance DB
- NPS virtual Linux Red Hat to host Hyperledger Fabric Blockchain
- Support from ITACS