Intro to Blockchain

Independent Project Proposal | Samarth Tambad

Project Focus

All or most of the projects will fall into one of the following three categories, Teams will probably build their projects in the context of HL Fabric, but projects in the context of Ethereum are also permitted.

Application: Development of an interesting application involving inter-organisation collaboration, in a domain chosen by the team. Example domains could include finance, supply chain, eCommerce, healthcare, education, Internet-of-Things, auctions, etc. The application should address both on-chain components and off-chain components.

Proposal

Each team should prepare a short document (2 to 3) pages) that describes the project they will create. The proposal should indicate the following.

1. The challenge or goal to be demonstrated by the software (e.g., create a system illustrating the utility of Blockchain to support a given application area, or create a framework and tool that enables model-driven specification, implementation and maintenance of access management for Blockchain applications)
2. A list of resources (books, articles, code bases, etc.), if any, that the team will draw inspiration or examples from. This should also include discussion of what will make the project different from things already available in the literature or on the web.
3. A high-level diagram and description of the architecture of the proposed solution.
4. A high-level week-by-week schedule of the planned design, implementation, testing (and perhaps other) activities.
5. Proposal for how the system can be demo-ed to a business-aware senior software engineer. (Having a UI for the demo is optional)
6. A short list of questions that can be used to evaluate the success of the project.
7. A high-level description of the primary foci of each of the team members.

Progress Reports

A primary component of the project evaluation will be progress reports presented by the teams to the Instructor. These 15-minute meetings will be face-to-face or via skype (or similar). In the progress report the team will describe current status of the project, possibly give a demo of some aspects, and may be asked questions about the project and/or underlying principles. Each team is expected to provide three progress reports during the period between March 17 and May 19.

Evaluation

The projects will be evaluated based on the difficulty of the software being created, how well the software matches the proposed goals, the novelty of the solution approach, the quality of the code, the effectiveness of the demos, and the team's understanding of underlying principles.

Repository: https://github.com/samarthtambad/blockchain-for-law-enforcement

Ideas Explored

1. Use of blockchain by the police department to maintain criminal records on an immutable ledger so that it cannot be erased.
2. Government maintained single central identity (pros: eliminates identity theft, census, etc)
3. Track how the government and its units spend the budget, using blockchain (pros: transparency, no corruption)
4. Judicial proceedings and evidence on blockchain (to prevent tampering and modification) for fair trials
5. Automated deduction of tax at source of payment using smart contract
6. Using blockchain and smart contracts to maintain student records between different departments within the University (pros: minimal administrative work)
7. Keep track of patient's hospital visits and use smart contracts for automated processing of health insurance
8. Capturing votes onto an immutable distributed ledger
9. Track the food along the supply chain in order to prevent adultration
10. Maintain real estate asset ownership information on distributed ledger

Goal

Create a system illustrating the utility of Blockchain to maintain criminal case records on an immutable ledger by the police departments. The evidence collected against a criminal (except any physical form of the evidence) that has been added onto the ledger can be admissible by the Court of Law during criminal proceedings.

Benefits

1. A central database that could be modified by a hacker or a person with access/power but not a distributed ledger.
2. Everyone involved is accountable as chain of events is available. Any lapse of duty such as improper documentation, loss of evidence, etc can be determined and corrected.
3. Courts can be granted permission to invoke queries relating to fetching the evidence for a particular case.

References

1. https://www.dhs.gov/sites/default/files/publications/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf
2. https://gcn.com/articles/2019/04/17/blockchain-public-safety.aspx
3. https://www.ncjrs.gov/pdffiles1/nij/178280.pdf
4. https://www.coindesk.com/chinas-police-ministry-touts-blockchain-for-secure-evidence-storage
5. https://arxiv.org/pdf/1807.10359.pdf
6. https://consensys.net/blockchain-use-cases/government-and-the-public-sector/

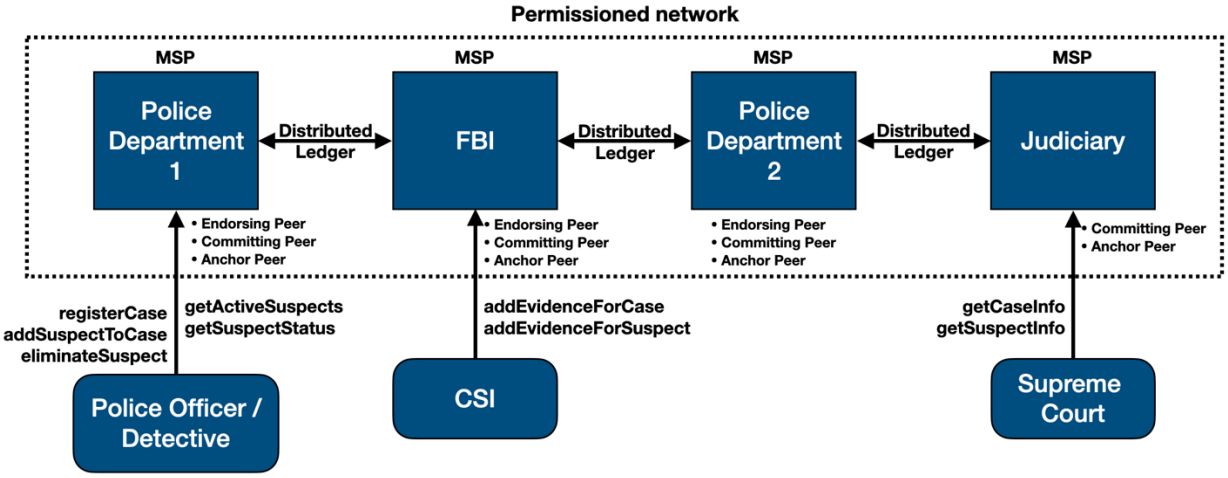
Repository: https://github.com/samarthtambad/blockchain-for-law-enforcement

What makes the project different?

All the literature present online just hints at this as a possible use case. However, there is no available implementation that actually illustrates or verifies the viability of blockchain for it. My project will build a POC that will implement the use case and practically demonstrate the feasibility of using blockchain. Also, I will use Hyperledger Fabric for running the blockchain network. An advantage of using Hyperledger Fabric rather than Ethereum or any other blockchain implementation is that it is a permissioned blockchain that uses consensus for adding blocks rather than proof of work or any such mechanism. This eliminates the need for mining or gas for running smart contracts. The participants of the network themselves maintain the network and the addition of blocks into the blockchain.

High-level Architecture Design

The following diagram illustrates the architecture:



The architecture consists of having FBI and all other police departments as part of the permissioned network each with their MSPs and peers. The network will also include a unit called the judiciary. This unit will participate in the network but will not have an endorsing peer i.e. will not be part of consensus. It will have an MSP and also a committing peer that keeps a copy of the ledger.

A judicial entity or a police officer can query the Blockchain to retrieve records of a criminal or evidence information for a particular case.

List of chaincode transactions:

1. **registerCase** - register a case with a unique case number
2. **addSuspectToCase** - a case could have multiple suspects, add suspect (with a unique id) to a list of suspects for a given case number
3. **addEvidenceForCase** – given a case number, add evidence found with respect to a case but not necessarily against a suspect
4. **addEvidenceForSuspect** - given a case number and suspect id, add evidence found against a particular suspect
5. **eliminateSuspect** - given a case number and suspect id, make suspect not active

Repository: https://github.com/samarthtambad/blockchain-for-law-enforcement

6. **getActiveSuspects -** given a case number, get all currently active suspects for that case
7. **getSuspectStatus -** given a case number and suspect id, retrieve status of the suspect
8. **getCaseInfo** – given a case number, get all relevant information for that case
9. **getSuspectInfo** - given a case number and suspect id, get all information for that suspect

Which State Database to use? LevelDB vs CouchDB

There are two options for state database:

1. LevelDB - Stores records in key-value form. It is a light and minimal database with fast queries. However, it is less efficient for large data. Also, it doesn't support complex queries.
2. CouchDB – Stores records in JSON format. It is efficient and scalable. It also enables complex queries on the Blockchain.

One point against CouchDB is the extra step downloading docker images and setting up. But since records need to be stored in a hierarchical fashion and complex queries may need to be made at some point, using CouchDB from the start makes sense.
https://medium.com/@deeptiman/couchdb-as-a-state-database-in-hyperledger-fabric-adb5d820c82e

Schedule Plan

	TASK	DELIVERABLE
APR1 - APR7	Concretize the architecture, all organisations in the network, list all the invoke and query transactions	Document with all the invoke and query transactions along with descriptions of each
APR8 – APR14	Setup for all organisations, being able to run the network	-
APR15 – APR 21	Implement the chaincode, test	Chaincode transactions working
APR 21 – APR 28	Write code for middleware	-
APR 29 – MAY 5	Write the application flow	Working application
MAY 6 – MAY 12	Test the application flow + buffer	-

Proposal for Demo

In order to demonstrate the use case to a business aware senior-engineer, I will run the entire application flow.

Question for evaluating success

1. Is blockchain feasible for the use case?
2. How suitable is Hyperledger Fabric?
3. What is the potential cost to implement it?
4. Where are the bottlenecks?
5. What are the other issues that arise?
6. Can the issues be solved? How to solve them?

Focus of each team member

Since I am working on the project alone, I will solely be focusing on each of the listed tasks.

Repository: https://github.com/samarthtambad/blockchain-for-law-enforcement