HYPERLEDGER

EB 20/21	Enterprise Blockchain Technologies	Number:	4
Module I - Introduction		Issue Date:	-
Background: Introduction to Hyperledger Fabric		Due Date:	-

Instructors Guide

This document provides a proposal for a solution for Lab4 [1].

1 B4S QUC - Fabric Version

Consider the Fabric version of Blockchain4Students - a blockchain dedicated to improving continuous improvement in education.

Let us think about possible implementation. B4S QUC should implement a Transparent Curricular Unit Quality System. Students give their feedback on courses/professors of their university through a student group. Schools and universities are rewarded reputation tokens based on the quality of their students' feedback. This allows making professors directly accountable for their students, yielding incentives for the universities to support their improvement.

1.1 Threats to Privacy

Exercise 1: Can a centralized system implement the use case?

A: No. A centralized system like Tecnico's may alter the evaluations' results or collude with participants due to a wide range of reasons. The intermediary between the feedback (students, professors), and the public (student candidate, high school student, other higher education institutions) is the university. This poses threats, as the institution is biased towards showing a good image. Via a blockchain, students and professors directly report feedback to the network via their representing parties, allowing for better transparency, accountability, and decentralization.

Exercise 2: Which privacy concerns arise regarding this network?

Given students feedback, there is the danger of students being identified by the professor or university. The feedback should be given anonymously and confidentially.

Exercise 3: How can one assure privacy and confidentiality for students and professors, without sacrificing traceability?

A student ID is registered on the students' group, which is associated with each feedback. In case of dispute, the law can enforce the students' group to identify the student. Otherwise, in normal conditions, the id is not disclosed, and privacy is assured.

Exercise 4: What would a suitable endorsement policy be, for the studied ecosystem?

A: at least an independent organization approving transactions; n out of 2n signatures from universities; k out of 2k signatures from student groups; i out of 2i signatures from professors departments

1.2 Data Integrity Threats

Exercise 5: Elaborate on the following threats:

Threat 1 *feedback entry tampering from an external element: An attacker violates the integrity of the feedback entries by editing them.*

Threat 1 (T1) is an external adversary gaining access to the feedback entries. Attackers can edit the feedback entries at their will, i.e., deleting them or decreasing the score. This attack has a higher severity of information systems that do not replicate data. The attacker can permanently delete information.

Threat 2 *feedback entry tampering from an internal adversary: An attacker from one of the stakeholders violates the integrity of the feedback entries by editing them directly.*

Threat 2 (T2) is similar to T1, with a higher degree of severity. If adversaries are insiders, they have direct access to the protected resource. An internal adversary might know peculiar ways to obfuscate such activities.

Threat 3 *feedback entry tampering by the system administrator: The administrator of the system, with the highest permissions, violates the integrity of the feedback entries by editing them. There is the possibility of obfuscating activity traces by deleting evidence on other systems.*

Threat 3 (T3) is similar to T2, with higher severity. Administrators have access to all resources and can, theoretically, delete all traces.

Threat 4 *A participant edits feedback entries that are protected by the blockchain.*

T4 is not severe if using a permissioned, private blockchain, like Hyperledger Fabric (Fabric), because transactions have to be endorsed before committed. Even if any participant on the network tries to modify feedback entries maliciously on its ledger, they cannot change other peers' ledger state, as honest endorsers would not endorse such transactions.

Threat 5 *The majority of participants conspire and modify the feedback entries.*

T5 evolves from T4, where the minority of nodes try to tamper with feedback entries. Members from the network can collude to alter feedback entries' integrity to trick an external auditor. If all participants on a network want to change its state, it is theoretically possible. The participants can follow the protocol and rewrite the world state, submitting new transactions from the point they want to change the state. Another way to mitigate this threat is to periodically send the last hash block of the permissioned blockchain, as a transaction, to a public blockchain at the expense of paying fees.

Exercise 6: How to alleviate the mentioned threats?

A: Threats 1-3 are alleviated by using a blockchain. Threat 4 is alleviated by Fabric's endorsement policies. Threat 5 is solved by adding a notary organization that is independent of any university.

References

[1] R. Belchior, A. Vasconcelos, and M. Correia, "Towards Secure, Decentralized, and Automatic Audits with Blockchain," in *European Conference on Information Systems*, 2020.