ASSIGNMENT #6

CSBC1020 – Blockchain Applications for Industry

FALL ‘21

Submitted by :
Gazi Mohammed Ashab Hossain
Student ID: 219019231

Submitted to :
Victor Li

Submitted on :
23.11.2021

1.No systems are 100% secured. Which part of Everledger's diamond tracing system is most vulnerable to frauds? Please explain why?

- Everledger was created to minimize fraud in the diamond industry. The system is deployed on IBM's Hyperledger Fabric for greater transparency to the open market places and global supply chain- by ensuring that all industry participants have maintained the authenticity of the asset. Specifically, the Everledger platform was created to only have one version of the truth for all involved parties regarding the asset.

  Even though Hyperledger was chosen to solidify the security aspects of the network, not every system is 100% secure, as they say. Everledger had updated their network from Ethereum, Eris, and BigchainDB to Hyperledger in 2016. In doing so, they have a more secure privatized system that has very few or no loose ends. The vulnerability of fraud that could arise are mentioned below:

  Firstly, Denial of Service (DoS) attacks are a possibility as the identity of an endorser/participant is known to all members on the chain. This could be done to maliciously block transactions or to degrade network efficiency. Secondly, a wormhole attack (i.e. leaking of ledger information to the outside world by a compromised member) is also possible if there are dishonest or shady members on the chain. It is important to mention that although Everledger has placed necessary precautions for these sorts of attacks by implementing High Security Business Networks on IBM Bluemix and LinuxONE, attacks like these in a larger scale (with multiple cooperating bad actors) might still be possible.

  If a scenario occurs where a policy needs to be endorsed by 2/3 organizations, some of these organizations could tamper with a transaction with read/write sets that the running chaincode wouldn't generate, and then commit it to the blockchain. Assuming the remaining endorsers are cooperating with the fraudulent organization(s), the system can be plagued with frauds.

  I would suggest economically incentivizing the endorsers with tokens/scarce currency of the network; that would enable a system like Everledger to plug these theoretical holes.

2.Between Walmart's food tracing system and Everledger's diamond tracking system, which one is more susceptible to frauds?

- ***Walmart Food Tracking:*** Walmart has partnered with IBM to implement Hyperledger Fabric in order to deploy a decentralized food supply ecosystem. It was done to enforce better traceability and thus the overall quality of the products. Till date, Walmart can trace the origin of 25 products from 5 different suppliers using this system. It has recently announced that all their fresh leafy greens suppliers must adapt to the system to apply traceability – kicking off their future plans to include more products and categories in the system.

  Everledger's Diamond Tracking: Everledger uses blockchain to trace and secure assets in the diamond industry. The system is deployed on IBM's Hyperledger Fabric for greater transparency to the open market places and global supply chain- by ensuring that all industry participants have maintained the authenticity of the asset.

  Susceptibility to frauds:

  Walmart and Everledger both have applied the Hyperledger system for better traceability of their products. However, Walmart has numerous products that might need to be traced and secured i.e. leafy greens, dairy products, fresh vegetables, fruits and any other perishable goods. These goods aren't particularly high priced but requires traceability nonetheless. On the other hand, Everledger products are primarily limited to diamonds, art, precious gems, and other minerals (so far). These goods are generally extremely high priced and thus require traceability to verify their origins.

  If we're talking about susceptibility to fraud, I would lean toward the Walmart Food Tracking system. Because in their system configuration, there would have to be a significantly large number of participants and nodes on the blockchain such as manufacturers, packaging, vendors, logistics etc. for ***each*** product. The more participant nodes there are on the chain, the higher the chances of fraudulent activity. However, unless there is a large scale attack on the system, these fraudulent activities wouldn't be too expensive to overcome and consequently patch up.

  Everledger on the other hand, would have a much small number of participants on the network compared to Walmart Food Tracking. Everledger's participants up till now, appears to be for an asset and not a product; meaning there is a lot more

exclusivity when choosing participant nodes. Lesser participant nodes on the chain means low chances of mishaps and frauds. That being said, if the nodes are somehow compromised by fraud or an attack, the repercussions would be extravagant. It is also important to mention that Everledger has deployed IBM Bluemix and LinuxONE to implement High Security Business Model Architecture to enforce security on the system, which makes it less susceptible to frauds. Walmart Food Tracking hasn't yet implemented these systems, and it would massively reinforce their security measures if/when they do.

3.Canada is the world's largest producer of icewines. A large percentage of icewines sold in Asia may be fake. If you were to design a blockchain-based icewine tracking system, what metadata about bottled wine should be recorded onto the blockchain?

- Canada imports majority of its Icewine to Asia. But the imported Icewine sold in China may be fake for an estimated 80 percent of the time. This deprecates the value of Icewine and the legitimacy it has as an exclusive product becomes nonexistent.

  To tackle this fraudulent behavior, items like Icewine can be supplied through a secure blockchain system. As it promises traceability and transparency, faking this an item would be an expensive endeavor. If we follow Everledger's policy, the bottled Icewine can be tagged with various IoT devices to keep track of them with their digital thumbprint, as shown below:

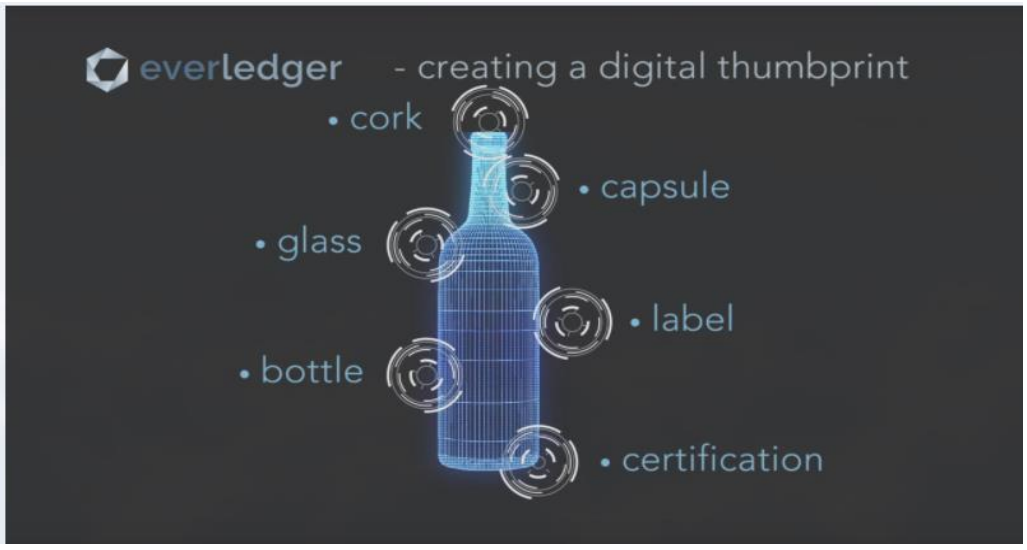

Image credit

We could also use a QR-code that would break upon opening the bottle to verify the authenticity of the bottle. It can be either a private chain or a permissioned public chain. The metadata on each block could include:

- a bottle uuid/hashId (attached at manufacturing)
- a restaurant/store id –attached when distributing the goods (If private blockchain is adapted)
- manufacturer Id
- date of manufacturing
- product grade (any scale could be used)
- IoT device Id (if used)
- And finally, a boolean state (sealed/unsealed) of the bottle. A real time update will occur when breaking the seal.

In the case of bottled Icewine, using an IoT device may increase security but with the expenses in mind, a robust QR code which would only break upon opening a bottle might be sufficient. In the event of the QR codes being faked, IoT devices should be adopted.

The buyers and sellers of the product should also be able to scan the code/device to verify the origin of the bottle; subsequently decreasing counterfeit product consumption.

References:

[1] CSBC 1020 Course Module

[2] "A close look at everledger-how blockchain secures luxury goods," Altoros, 23-Sep-2019. [Online]. Available: https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/. [Accessed: 23-Nov-2021].

[3] "Edge 2016 | The power of the individual | full version," YouTube, 25-Sep-2016. [Online]. Available: https://www.youtube.com/watch?v=GAdjL-nultI. [Accessed: 23-Nov-2021].

[4] N. Andola, M. Raghav, S. Gogoi, and S. Venkatesan, "Vulnerabilities on hyperledger fabric," Pervasive and Mobile Computing, 11-Jul-2019. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S157411921830720X. [Accessed: 23-Nov-2021].

[5] "Fabric@lists.hyperledger.org: I have five questions about the security of fabric.," Groups.io. [Online]. Available: https://lists.hyperledger.org/g/fabric/topic/69113154. [Accessed: 23-Nov-2021].

[6] "Walmart case study," Hyperledger Foundation, 25-Mar-2019. [Online]. Available: https://www.hyperledger.org/learn/publications/walmart-case-study. [Accessed: 23-Nov-2021].

[7] B. O'Donnell, "China's fake ice wine epidemic," Wine Spectator, 03-Feb-2011. [Online]. Available: https://www.winespectator.com/articles/china-s-fake-ice-wine-epidemic-44430. [Accessed: 23-Nov-2021].