HF1 Safe crossings for autonomous cars

Unguarded level crossings will pose a special challenge for autonomous vehicles; from the safety point of view, relying only on the on-board sensor packages and intelligence to decide whether it is safe to cross (no train is approaching) will be problematic. At the same time, the railway infrastructure – commonly partitioned into blocks https://en.wikipedia.org/wiki/Railway\_signalling#Block\_signalling – “knows” where the trains are; e.g., safety systems ensure that no train can enter a block already (or still) occupied by a train.

The task is to design and implement a train crossing smart contract with the following features:

1. The railroad infrastructure must periodically signal the crossing to be in a “FREE TO CROSS” state. This state has a preset validity time; if the last update is older than that, the crossing must be assumed to be in a “LOCKED” state. This can happen either on a train approaching or a failure of the infrastructure.
2. Autonomous vehicles wanting to cross must request permission to do so.
3. Permission may be granted only if the intersection is not in a “LOCKED” state.
4. Additionally, an intersection comprises of one or more lanes. A single lane can accommodate a fix number of crossing cars, predetermined by the railroad infrastructure managing authority.
5. Autonomous vehicles must explicitly release their permission after leaving the crossing. Failure to do so will later involve legal action; for this purpose, their identity must be recorded on the ledger, but in a privacy-preserving way (as much as possible).
6. As an additional safety measure, using a means of communication independent from the one used by the above mentioned infrastructure, approaching trains also explicitly request the crossing to get into the “LOCKED” state (and release this signal only when they passed it).
7. However, if the intersection is still occupied, it transitions into a special state (also signaling this to the train) where the train will have priority to request crossing, i.e., no more cars are granted crossing permission, until the train crosses.
8. If the train can't gain permission in a predetermined time since the original try, it is assumed that there is an obstacle in the crossing, and the train can break or halt.

Note: this exercise does reflect some of the concepts used in safety critical engineering, but falls far from a full, real-life safety strategy. (I.e., don’t build a real system from this specification. If you happen to be a rail fan, <https://arxiv.org/abs/1901.06236> and <https://www.deutschebahn.com/en/Digitalization/technology/New-Technology/blockchain-3520362> are good reads.)

***Homework owner: Attila Klenik (attila.klenik@edu.bme.hu)***