Actor-based Risk Analysis for Blockchains in Smart Mobility

Ranwa Al Mallah, Bilal Farooq

Laboratory of Innovations in Transportation,
Ryerson University, Toronto, Canada,
CryBlock @ MobiCom 2020

September 25, 2020

Table of Contents

Table of Contents

Motivation

- Nowadays, transportation data are shared across multiple entities and stored in central servers.
- Multi-layered Blockchain framework for Smart Mobility Data-market (BSMD) was recently proposed to solve the privacy, security and management [1].
- Security issues related to blockchain are critical in terms of cybersecurity.

Related work

Studies	Methodology	Drawbacks
Li et al., [2]	- Examination of security risks/survey of attacks to popular blockchains. - Analyze related vulnerabilities exploited.	-Do not consider the risk as a function of probability and impact. - Real scope of the risk is not described.
Atzei et al., [3]	-Analyze security vulnerabilities of smart contracts. -Show a series of attacks.	-Don't account for various nature of threats. - Isolate analysis from a security programming.
Homoliak et al., [4]	-Hierarchy of four layers. -Identified four threat agents and report vulnerabilities at each layer.	-Don't quantify risk. -Generic architecture not evaluated on realistic blockchain.

Multi-layered Blockchain model for Smart Mobility Data-market (BSMD)

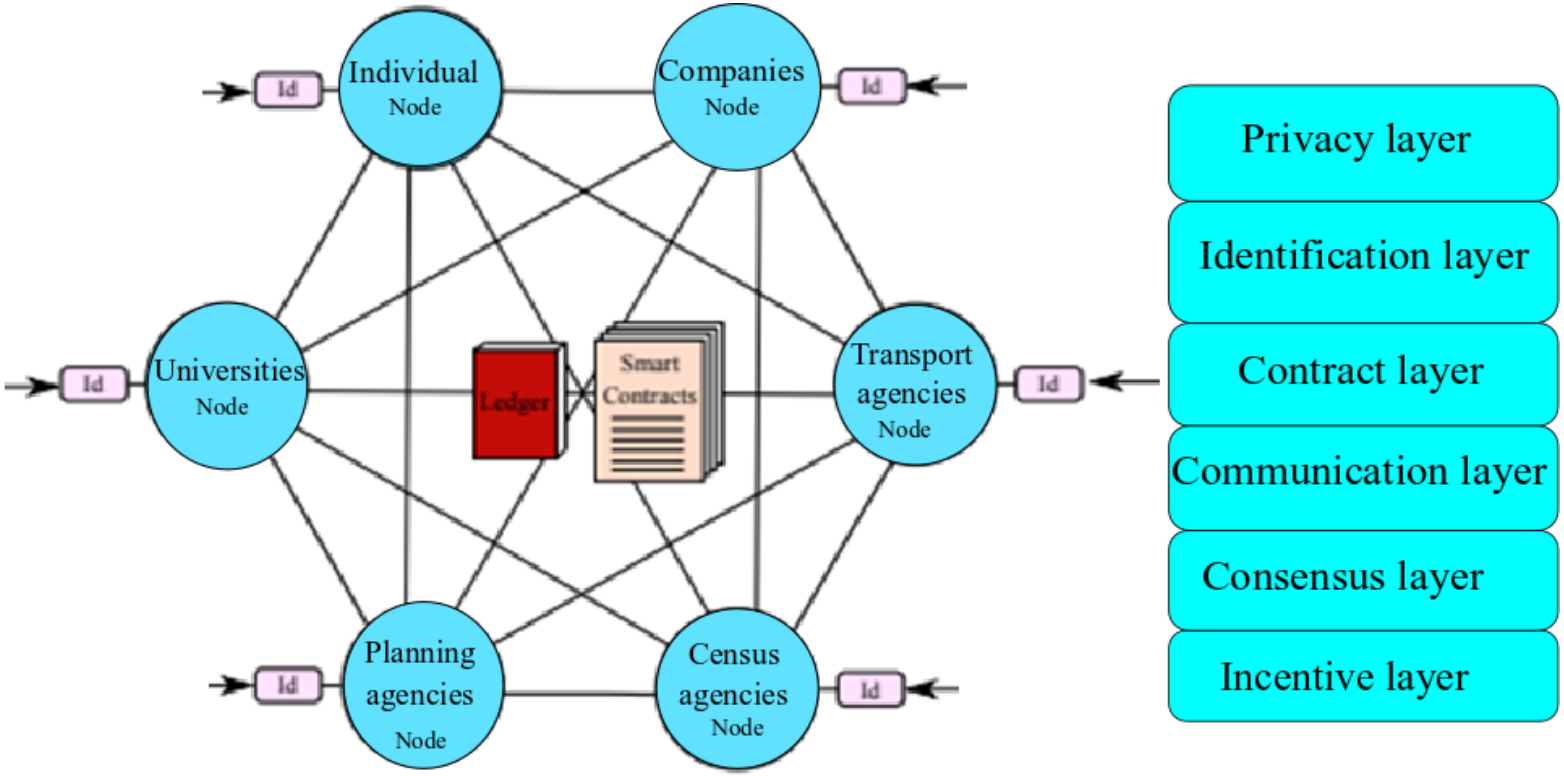

Table of Contents

Methodology

- **Definitions:**
  - Actor: Entity violates integrity/privacy/confidentiality to obtain a benefit.
  - Attack goal: Final effect desired by actor with impact on victim.
  - Scenario: Set of actions carried by actor to achieve his attack goal.
  - Impact: Quantification of the attack goal's effect on the victim.
  - Vulnerability: A flaw that offers the opportunity to damage a system.
- **Actor-based risk analysis:**
  - STEP 1: Identify potential actors.
  - STEP 2: Determine the attack goals.
  - STEP 3: Quantify the impact on the victim of such attack goals.

Table of Contents

Actor-based risk analysis : Step 1

- Identify potential actors:
  - **A1. Cybercriminals**
  - **A2. Industrial spies**
  - **A3. Foreign Intelligence Agencies**
  - **A4. Terrorist groups**
  - **A5. Insider threat**

Actor-based risk analysis : Step 2

- Determine the attack goals:
  - **G1. Gain knowledge about the data-market**
  - **G2. Access sensitive data on the nodes of the network**
  - **G3. Manipulate and modify blockchain information**
  - **G4. Sabotage activities**
  - **G5. Induce participants in the blockchain network to make errors**

Actor-based risk analysis : Step 3

- Impact types: Monetary, Privacy, Integrity, Trust.

Impact levels	Risk treatment
1. Minor	Accept
2. Significant	Accept
3. Severe	Manage
4 . Catastrophic	Refuse

Actor-based risk analysis : Step 3

- Impact on the victims by attack goal - Monetary (M), Privacy (P), Integrity (I) and Trust (T). Impact scale ranges from 1 to 4, with 4 being the most severe.

Goal	**M**	**P**	**I**	**T**
G_1 - Gain knowledge about the data-market	1	2	-	1
G_2 - Access sensitive data	2	3	-	2
G_3 - Manipulate and modify blockchain information	3	2	4	4
G_4 - Sabotage activities	3	-	2	3
G_5 - Induce participants to make errors	2	-	3	3

Table of Contents

Outcomes

- In terms of monetary, privacy, integrity and trust, G3 represents a risk that is either unacceptable or undesirable.
- G1 results in an acceptable or negligible risk because the benefits that the system brings are greater than the potential risk.
- In terms of monetary impact, G2, G3, G4 and G5 represent a risk in terms of economic losses.
- In terms of privacy impact, G2 is the riskiest attack goal.
- In terms of integrity and trust, G3 and G5 have a catastrophic impact on the trust of the blockchain system.

Table of Contents

Conclusion and future work

- Actor-based risk analysis of a realistic blockchain for smart mobility data-markets showed impacts at four scales.
- Extend the analysis to a scenario-based risk assessment.
- Perform a combined risk assessment.
- Detection mechanisms specific for the data-market ecosystem should be designed.

References

[1] D. Lopez, B. Farooq, A multi-layered blockchain framework for smart mobility data-markets, in: Transportation Research Part C: Emerging Technologies, 2020, pp. 588-615.
[2] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems (2017).
[3] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International conference on principles of security and trust, Springer, 2017, pp. 164–186.
[4] I. Homoliak, S. Venugopalan, Q. Hum, P. Szalachowski, A security reference architecture for blockchains, in: 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019, pp. 390–397.

THANK YOU

ranwa.almallah@ryerson.ca