IEEE Open Journal of
Intelligent Transportation
Systems

Received 23 June 2021; revised 27 July 2021; accepted 16 August 2021. Date of publication 23 August 2021; date of current version 6 September 2021.

*Digital Object Identifier 10.1109/OJITS.2021.3106863*

# Cyber-Security Risk Assessment Framework for Blockchains in Smart Mobility

**RANWA AL MALLAH[1] (Member, IEEE), DAVID LÓPEZ[2], AND BILAL FAROOQ[1] (Member, IEEE)**

[1]Laboratory of Innovations in Transportation, Ryerson University, Toronto, ON M5G1G3, Canada

[2]Instituto de Ingeniería, Universidad Nacional Atónoma de México, Mexico City, Mexico City 04510, Mexico

CORRESPONDING AUTHOR: B. FAROOQ (e-mail: bilal.farooq@ryerson.ca)

This work was supported by the Canada Research Program in Disruptive Transportation Technology and Services.

This article has supplementary downloadable material available at https://doi.org/10.1109/OJITS.2021.3106863, provided by the authors.

**ABSTRACT** Use of distributed ledger technologies like blockchain is becoming more common in transportation/mobility ecosystems. However, cyber-security failures may occur at places where the blockchain system connects with the real world. In this paper, we propose a novel risk assessment framework for blockchain applications in smart mobility. We aim at systematically quantifying the risk by presenting ordinal values because although vulnerabilities exist in a system, it's the probability that they can be exploited and the impact of this exploitation that determine if in fact, the vulnerability corresponds to a significant risk. As a case study, we carry out an analysis in terms of quantifying the risk associated to a multi-layered Blockchain framework for Smart Mobility Data-markets (BSMD). We first construct an actor-based analysis to determine the impact of the attacks. Then, a scenario-based analysis determines the probability of occurrence of each threat. Finally, a combined analysis is developed to determine which attack outcomes have the highest risk. In the case study of the public permissioned BSMD, the outcomes of the risk analysis highlight the highest risk factors according to their impact on the victims in terms of monetary, privacy, integrity and trust. The analysis uncovers specific blockchain technology security vulnerabilities in the transportation ecosystem by exposing new attack vectors.

**INDEX TERMS** Attack, blockchain, cyber security, mobility, risk, vulnerabilities.

## I. INTRODUCTION

BLOCKCHAIN technology is a secure platform that maintains past records of digital events by creating an irrefutable record in a public ledger [1]–[4]. From the birth of the first blockchain system, the technology has experienced many stages of development: blockchain 1.0, blockchain 2.0, and blockchain 3.0. Blockchain 1.0 deploys cryptocurrencies, such as currency transfers, currency settlements, and digital payments. Blockchain 2.0 includes *smart contracts* and handles more than cash transactions. The third category is related to applications beyond currencies, finance, and markets. It includes domains, such as government, science, literacy, art, and culture.

In the transportation field, a multi-layered Blockchain framework for Smart Mobility Data-market (BSMD) was recently proposed by [5]. BSMD is a public-closed blockchain designed to solve the issues related to the sharing of large-scale mobility data. A public-closed blockchain represents the level of permission where anyone can do the transactions and have access to the ledger but only a restricted set of participants can be involved in the consensus mechanism. Data from the individuals, governments, universities and companies are distributed on the network and stored in a decentralized manner, the data transactions are recorded and must have the authorization of the owners.

Recently, many fraud, breaches and threats have occurred in transportation systems and in many blockchain-based applications. In an attempt to access sensitive data about the customers, in 2016, information of 57 million Uber customers and drivers were leaked [6]. Criminals manipulated *smart contracts* in the *Ethereum* blockchain with a Decentralized Autonomous Organization (DAO) hack, to steal around 60 million dollars [7]. Moreover, a coded

The review of this article was arranged by Associate Editor Hyunbum Kim.

intrusion or system vulnerability could allow even more negative consequences to the security of the system [1]. For example, if successful, an attacker would gain access not only to the information stored at the point of attack, but also to all information recorded in the ledger. Thus, blockchain security needs to be assessed in terms of risk exposure. We provide an analysis that is unique and much needed in the context of ever rising cyber-security and privacy needs in smart mobility. The proposed methodology can be applied to other blockchain-based systems in transportation and is not limited to the use case under study.

The aim of a risk assessment has always been, on the one hand, to identify the threat that represents the highest risk and, on the other hand, to determine the residual risk in order to choose most effective countermeasures. Li *et al.* [8] conducted a cyber-security risk analysis on the popular distributed ledger systems. In our study, we aim at systematically quantifying the risk by presenting the ordinal values. We are of the view that although vulnerabilities exist in a system, it is the probability that they can be exploited and the impact of this exploitation that determine if in fact, the vulnerability corresponds to a significant risk. The risk is thus a function of probability as well as the impact and can be systematically quantified. In fact, we developed a cyber-security risk assessment framework consisting of three main steps, namely: 1) actor-based risk analysis to extract the impact, 2) scenario-based risk analysis to extract the probability, and 3) combined risk assessment to quantify the risk.

We identified risks in the transportation domain associated to the threats that aim at the disruption of the blockchain network. We determine which vulnerabilities to address and in what priority. We also provide guidance on which attack vectors and related vulnerabilities should be addressed in priority by highlighting attack vectors that represent the most cumulative risk. The risk assessment will shed light on the appropriate countermeasures that can be deployed as a security-by-design to avoid cyberattacks. The key contributions of this paper are:

- Risk assessment methodology, enabling the systematic quantification of the risk associated not only to the blockchain technology, but also to its ecosystem.
- Application of the risk assessment methodology to a realistic blockchain for smart mobility data-markets and analysis of the attacks in terms of their impact on the economy, privacy, integrity and trust.
- Identification of the riskiest attack vectors on the blockchain network for transportation data sharing extending the knowledge of the threats affecting the blockchain network in order to provide guidance on which threats should be addressed in priority.

This paper is organized as follows. Related work is provided in Section II. In Section III, we present the methodology followed by the risk analysis of a blockchain in transportation domain, i.e., BSMD in Section IV. We provide an impact analysis in Section V and a discussion in Section VI. Finally, conclusions and future work are outlined in Section VII.

## II. RELATED WORK

With the decentralized consensus mechanism of blockchain, *smart contracts* allow mutually distrusted users to complete data exchange or transaction without the need of any third-party trusted authority [9]–[11]. *Hyperledger* is a widely used blockchain supporting *smart contracts* [12]. However, *smart contracts* with security vulnerabilities may lead to financial losses. Atzei *et al.* [13] analyzed the security vulnerabilities of *Ethereum smart contracts*.

On the other hand since blockchains are overlay-networks on top of other networks, they are expected to inherit security and privacy issues from the underlying networks. The main blockchain-oriented services provided by the network layer are peer management and discovery, such as Domain Name resolution System (DNS) and network routing protocols. Thus, threats may come from Man-In-The-Middle (MITM) attacks, network partitioning, de-anonymization, and availability attacks. In this context, countermeasures contain protection of availability, naming, routing, anonymity, and data [14]. Insiders may pose a serious threat to security because a compromised node may already have administrative privileges or obtain them by exploiting a system, network, or security vulnerabilities [15].

Only a few studies have presented a blockchain cyber-security risk analysis [8], [13], [14]. None of the studies estimate the risk of a vulnerability based on the probability that it will be exploited successfully and the impact that it will have on the network. We propose a risk assessment that, like Jagannathan and Sorini [16] consists of three main steps namely: 1) threat identification, 2) risk estimation, and 3) risk characterization. The difference between their work and ours lies in that we applied the methodology to the multi-layered blockchain for smart mobility data-market and not to medical devices.

López and Farooq [5] proposed the Blockchain for Smart Mobility Data-markets (BSMD) where the nodes of the blockchain network own their data and can share it with other nodes. Nodes in BSMD are divided into *passive nodes* and *active nodes*. *Passive nodes* may read or host copies of the ledger. This type of node is suitable for individuals or small businesses who want to participate and take advantage of the network, but do not have the resources for running nodes for extended periods of time. *Active nodes* can write blocks and store updated versions of the ledger for other nodes to connect. This type of node is suitable for governments, universities or companies who have the resources for these tasks. In the blockchain there are *smart contracts* available that the nodes need to sign before any transaction of information is conducted.

Particularly, the BSMD is composed of six layers. The Identification layer contains mobility information and other

data that the nodes own. The Privacy layer is the differential privacy model for accessing location based services. In the Contract layer are the set of *smart contracts* and the brokers who facilitate data transactions between nodes. The Communication layer contains the Decentralized Identifiers of the nodes who serve as endpoints to establish peer-to-peer connections. The Consensus layer contains the consensus algorithms in which the *active nodes* agree to write transactions in the ledger. Finally, in the Incentive layer are the rewards the *active nodes* receive for participating in consensus and the reward nodes receive for sharing (selling) their information. In order to demonstrate the BSMD as a distributed mobility information management system, it was implemented on *Hyperledger* Iroha, which is a public-closed blockchain. *Hyperledger* is a framework for permission networks. All participants have known identities, and every user participating in a transaction must register on the network in order to obtain an enrollment ID.

## III. METHODOLOGY

We present a cyber-security risk assessment framework for blockchains in smart mobility. Our methodology quantifies the risk and identifies the attack vectors that represent the most cumulative risk—thus enabling the determination of vulnerabilities that can be addressed prior to implementation. Our work will provide guidance as to what should be addressed in priority so that security solutions can be implemented at the early stages of development as a security-by-design philosophy.

We start by defining the terms that will be used in the risk assessment.

- *Actor:* Individual or organization who performs malicious activities.
- *Attack goal:* Malicious effect of the actor.
- *Scenario:* Events produced by the actor to attain its attack goal.
- *Impact:* Quantity representing the attack goal's effect.
- *Threat:* The combination of the actor and the scenario used to attain his attack goal.
- *Vulnerability:* Flaw in the system that can be exploited by actors.
- *Attack vector:* Subset of vulnerabilities for which there is a demonstrated attack method by which the vulnerability is exploited by the actor to reach its goal.
- *Probability (P):* Unnormalized likelihood that a particular threat materialize during a given period of time.
- *Risk (R):* Quantification of a threat = Impact x Probability.

The evaluation methodology is divided into three steps, as shown in Fig. 1 and described below.

*Step 1-Actor-based risk analysis:* In the first step of the methodology, we will determine the impact of the attacks on the BSMD. We start by identifying the different actors and their attack goals. We then use Table 1 to quantify the impact of the attacks. In this paper, we propose a four-scale for ranking the relative gravity of an element. This scale is adapted from those given in ISO 27005 and ISO 31000 standards to apply to our context [17]. As values vary from 1 to 4, this approach avoids quantifying in terms of monetary value. The proposed scale is reused throughout the other parts of the risk assessment to avoid the pitfalls of working with the values that represent different dimensions. This will enable us to consider in the same manner as for the individual elements the combined risk value obtained by automatically summing up the numerical rankings.

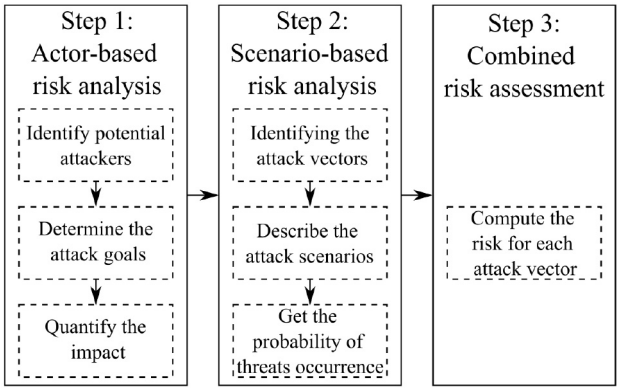



**FIGURE 1.** Steps of the methodology of the risk assessment.

*Step 2-Scenario-based risk analysis:* In the risk analysis based on the attack scenario, we estimate the probability of occurrence of threats (scenario and actor). Thus, we start by identifying the attack vectors, i.e., exploitable vulnerabilities. Next, we describe the attack scenarios leading to the achievement of the attack goals determined in step 1. We then calculate the probability of occurrence of threats using (1).

$$P = c + o + m, \tag{1}$$

where:

$c$ actor's capacity to attack
$o$ actor's opportunity to attack
$m$ actor's motivation to attack.

*Step 3-Combined risk assessment:* In the combined risk assessment, we calculate the risk as per (2) associated with each attack scenario based on the most likely actor. We use the impact results from step 1 and the maximum probability per attack scenario results from step 2. Finally, we calculate the overall risk associated with each attack vector.

$$R = I \times P_{MAX} \tag{2}$$

where:

$I$ attack goal impact
$P_{MAX}$ maximum probability per attack scenario.

## IV. RISK ANALYSIS OF BSMD

We present in this section the details of the application of our methodology to the BSMD, a blockchain ecosystem in

**TABLE 1.** Impact levels for mobility data-market adapted from ICS-CERT [18].

| Level | Description | Impact types | | | |
|---|---|---|---|---|---|
| | | Monetary | Privacy | Integrity | Trust |
| 1 | Minor | Minimal monetary loss | Minimal impact on the privacy of any of the nodes in BSMD (Individuals, Companies, Universities and Government) | Minimal impact on the integrity of the mobility data, transactions and integrity of the users | Minor impact on the trust of the BSMD network |
| 2 | Significant | Significant monetary loss | Significant on the privacy of the nodes in BSMD | Significant impact on the integrity of the mobility data, transactions and integrity of the users | Significant impact on the trust of the BSMD network |
| 3 | Severe | Severe monetary loss | Severe on the privacy | Severe impact on the integrity of the mobility data, transactions and integrity of the users | Severe impact on the trust of the BSMD network |
| 4 | Catastrophic | Catastrophic monetary | Catastrophic on the privacy of the nodes in BSMD | Catastrophic impact on the integrity of the mobility data, transactions and integrity of the users | Catastrophic impact on the trust of the BSMD |

transportation. The BSMD is programmed on Python and is build upon the Hyperledger: Iroha ledger software. The BSMD is set up with at least four nodes; two active nodes are needed for maintaining the ledger and participate in consensus mechanisms, while two passive nodes are needed for transacting information. Depending on the size of the BSMD network, the active nodes might need more processing and storage power than an average home computer. In contrast, the active nodes can run on microcomputers like a RaspberryPi.

**TABLE 2.** 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 on the nodes of the network | 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 in the blockchain network to make errors | 2 | - | 3 | 3 |

### A. STEP 1 - ACTOR-BASED RISK ANALYSIS

In a previous work [19] applied the first step of the methodology to the BSMD. For readability, we summarize herein their findings of the actor-based risk analysis. Five actors are identified: $A_1$-Cybercriminals, $A_2$-Industrial spies, $A_3$-Foreign Intelligence Agencies, $A_4$-Terrorist groups, $A_5$-Insider threat. $A_5$ may be an active node of the blockchain network or an infrastructure node that becomes malicious and exploits the blockchain system.

Five attack goals are also identified in the context of smart mobility: $G_1$-Gain knowledge about the data-market, $G_2$-Access sensitive data on the nodes of the network, $G_3$-Manipulate and modify blockchain information, $G_4$-Sabotage activities, $G_5$-Induce participants in the blockchain network to make errors.

The attack goals will have different types of consequences: Monetary (M), Privacy (P), Integrity (I) and Trust (T). The impact levels associated to the consequences are described in Table 1. The results of the actor-based risk analysis are summarized in Table 2.

For a detailed description of the actors, the attack goals and the explanation of the impact analysis by attack goal, we refer the reader to the original paper [19].

### B. STEP 2 - SCENARIO-BASED RISK ANALYSIS

In the second step of the methodology, we identify the exploitable vulnerabilities and describe the attack scenarios leading to the achievement of the attack goals determined in the first step in order estimate the probability of occurrence of threats.

#### 1) VULNERABILITIES

We first expose all the practical vulnerabilities ($V_i$) affecting the BSMD ecosystem. We gathered this information from several sources, including: [1], [8], [14]. We record 22 vulnerabilities and present them in Table 3. We separate the vulnerabilities in six groups based on the layer of the BSMD they affect, as shown in Fig. 2. Some vulnerabilities are applicable to more than one layer (i.e., $V_4$, $V_{13}$). Since the current implementation of BSMD is on the *Hyperledger* platform, we focused mainly on the vulnerabilities of permissioned blockchains. For a detailed explanation of each vulnerability, please read the supplementary material (AFL11-2020) submitted with this manuscript.

#### 2) ATTACK SCENARIOS

Once we identified the actors and their goals, we are interested in the strategy that they will use to achieve a certain attack. Precisely, they will exploit vulnerabilities of the BSMD system to achieve their goals via an attack scenario. An attack scenario is the sequence of events that must occur for the attack to take place. We identified 22 attack scenarios ($S_i$) and organized them according to the corresponding layer of the BSMD as per Fig. 2. It is important to mention that although the vulnerabilities mentioned in this paper exist, no attacks have been reported yet in an environment other than the controlled environment of research laboratories. Thus,

**TABLE 3.** Description of the vulnerabilities ($V_i$) affecting the BSMD ecosystem.

| Vulnerability | Label | Description |
|---|---|---|
| Improper key protection mechanism | $V_1$ | Users store private keys in a file. If it is lost/stolen/corrupted by a malware, the key cannot be recovered. |
| Unauthenticated data feeds | $V_2$ | Nodes may inject wrong data, resulting in corrupted mobility applications. |
| Unsecure cryptographic signature algorithm | $V_3$ | Mathematical complexity does not necessarily guarantee the security of a cryptographic algorithm. Implementation can lower the security level. |
| Privacy threats to user identity | $V_4$ | Pseudonymous identities can be traced to real identities. Obfuscation of user identities is required to provide unlinkability to users. |
| Weak privacy protection measures | $V_5$ | Techniques for hiding the real location of the user from the location based service provider are not robust, may be exploited and lead to privacy leakage. |
| Lack of monitoring of smart contract application | $V_6$ | Poor access management on *smart contracts* like call stack and type casts might deviate *smart contracts*' intended behaviour to malicious transactions. |
| Program design of smart contract | $V_7$ | Yamashita et al. [17] surveyed the vulnerabilities associated with chaincodes developed using Go language and observed that there are 14 potential risks. |
| Program writing of smart contract | $V_8$ | Huang et al. [18] identified two vulnerabilities named *unhandeled errors* and *unchecked input arguments*. |
| Design flaws of the blockchain platform | $V_9$ | Shaw [19] exposed that chaincode can perform port scans, exploit hosts discovered and accept commands from a remote command-and-control server. |
| DNS rebinding | $V_{10}$ | Client-side scripts are only allowed to access content on the same host that served the script. DNS rebinding circumvents this protection by abusing the DNS. |
| Absence of BGP security extensions | $V_{11}$ | Border Gateway Protocol (BGP) security extensions are not widely deployed which may expose network operators to Internet prefixes hijacking [20]. |
| Lack of node monitoring and prevention techniques | $V_{12}$ | While VPNs are in general secure, lack of prevention techniques that minimize trust and maximize trustworthiness pose a serious security threat. |
| Poor architecture design | $V_{13}$ | Private ledger network may get split into parallel fork chains creating ambiguity among child blocks and being susceptible to several attacks in parallel fork chains. |
| Tolerated power of adversary | $V_{14}$ | In BFT-based consensus algorithm, the amount of control an attacker would need is 33.3% to manipulate and modify the blockchain information. |
| Lack of peer privacy | $V_{15}$ | The identity of an endorser is known to all members within a channel. This opens a gateway for attacks on endorsers. |
| Consensus flaws: constant committee members | $V_{16}$ | The current BFTs rely on a special replica called as primary. If this primary is a malicious node then it can delay the requests of the transactions. |
| Asynchronous delivery of messages | $V_{17}$ | Network links can be unreliable, speeds change rapidly, and network delays may be adversarially induced. This vulnerability motivates asynchronous BFT protocols. |
| Unpredictable state | $V_{18}$ | Luu et al. [21] discovered the unpredictable state vulnerability where the state of the contract is changed before invoking. |
| Timestamping | $V_{19}$ | The timestamp of a block can be changed by a malicious miner. Timestamp-dependent contracts are vulnerable. |
| Lack of intrusion prevention/detection mechanisms | $V_{20}$ | Malicious activities should be detected before consensus can be reached. |
| Non-deterministic transactions | $V_{21}$ | It is important that chaincode transactions are deterministic, otherwise state of peers might diverge. |
| Absence of incentive | $V_{22}$ | Operations can be executed in quantity in one transaction. |

we proceeded to the best of our knowledge to put forward a list of possible scenarios. As new vulnerabilities may be uncovered in the future, more scenarios may be added to the list. Furthermore, as illustrated in Table 4, an attack goal can be achieved by means of different scenarios. That is why, various scenarios appear in multiple attack goals. We carry out a scenario-based risk analysis by attack goal since the impact of an attack depends on the attack goal and the actor's motivation changes from one attack goal to the other. The detailed explanation of the scenarios is provided in Appendix A. However, in the following, we present an in depth description of attack scenarios $S_2$, $S_{11}$, $S_{18}$ and $S_{20}$ and specifically provide the detailed steps of their execution by using diagrams. We depict the details of these specific scenarios because the attacks conducted by the actors exploit vulnerabilities at all distinct layers of the BSMD ecosystem.

**TABLE 4.** Possible scenarios per attack goal.

| Attack goal | Label | Scenarios |
|---|---|---|
| Gain knowledge about the data-market | $G_1$ | $S_1$, $S_3$, $S_4$, $S_7$, $S_8$, $S_{10}$, $S_{12}$, $S_{20}$ |
| Access sensitive data on the nodes of the network | $G_2$ | $S_1$, $S_3$, $S_4$, $S_7$, $S_8$, $S_{10}$, $S_{12}$, $S_{20}$ |
| Manipulate and modify blockchain information | $G_3$ | $S_1$, $S_{10}$, $S_{11}$, $S_{14}$, $S_{15}$, $S_{16}$, $S_{17}$, $S_{18}$, $S_{19}$, $S_{21}$ |
| Sabotage activities | $G_4$ | $S_1$, $S_2$, $S_5$, $S_6$, $S_7$, $S_8$, $S_9$, $S_{10}$. $S_{11}$, $S_{12}$, $S_{13}$, $S_{14}$, $S_{15}$. $S_{16}$, $S_{17}$ $S_{18}$, $S_{19}$, $S_{21}$, $S_{22}$ |
| Induce participants in the blockchain network to make errors | $G_5$ | $S_1$, $S_2$, $S_5$, $S_6$, $S_7$, $S_8$, $S_9$, $S_{10}$. $S_{11}$, $S_{12}$, $S_{13}$, $S_{14}$, $S_{15}$. $S_{16}$, $S_{17}$ $S_{18}$, $S_{19}$, $S_{21}$, $S_{22}$ |

*False data injection ($S_2$):* If proper identity management is not set for the private blockchain, attackers may exploit the unauthenticated data feed vulnerability ($V_2$) so that ledgers will be susceptible to false data injection. A strong permissioned network is required because attackers may also exploit poor network design and misbehaving nodes may produce wrong data to inject into the system. We present

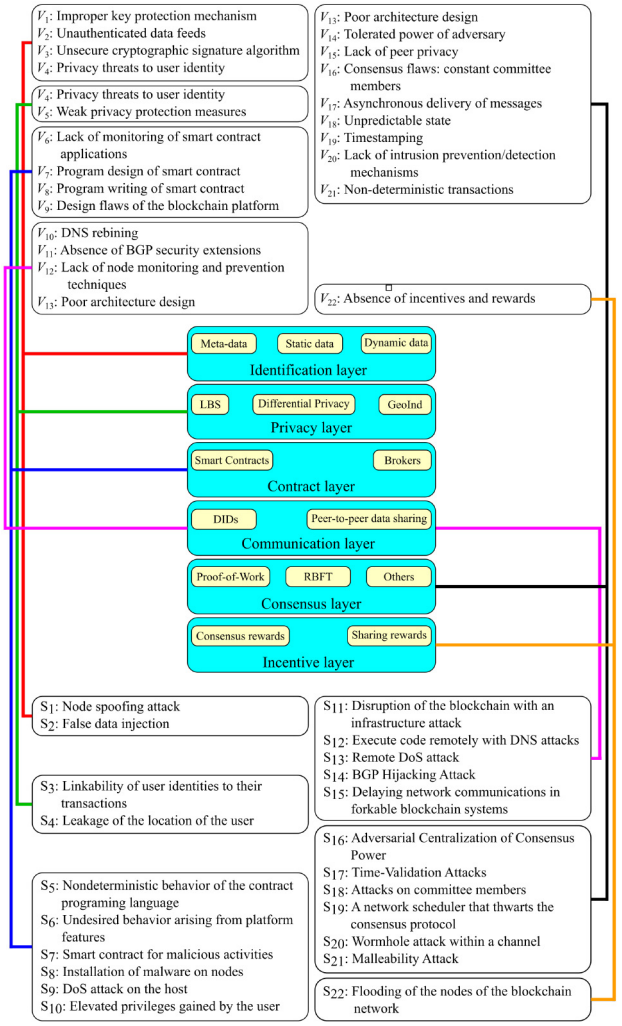



**FIGURE 2.** Vulnerabilities ($V_i$) and Attack scenarios ($S_i$) affecting the BSMD ecosystem depending on the affected layer of the BSMD.

the diagram of the detailed steps of this attack scenario in Fig. 3.

*Disruption of the blockchain with an infrastructure attack ($S_{11}$):* Without node monitoring and prevention techniques ($V_{12}$) that minimize trust and maximize trustworthiness, insiders may pose a serious threat to security. A compromised node may already have administrative privileges or obtain them by exploiting a system, network, or security vulnerabilities. This infrastructure attack models the threat from an active node, Internet service provider, company or nation-state that has contiguous IP addresses. The attacker monopolizes incoming and outgoing connections and creates a logical partition on the BSMD network. As a result, the BSMD network might suffer from disruption. A victim node's view of BSMD will be filtered due to this attack. We present the diagram of the detailed steps of this attack scenario in Fig. 4.

*Attacks on committee members ($S_{18}$):* Attackers may exploit consensus flaws such as the constant committee members vulnerability ($V_{16}$) and the lack of peer privacy ($V_{15}$) to perform attacks on the consensus committee members. Firstly, if the identity of an endorser is known to all members within a channel, this opens a gateway for DoS attack on endorsers in order to either block transaction pertaining to a client, or to degrade network efficiency. DoS attack has a significant effect on the network efficiency. The throughput is reduced followed by the increase in latency.

As the identity of endorsers is known to everyone in the BSMD network, an insider malicious peer can launch a DoS attack on endorsers to achieve two objectives. The first motive of an adversary is to block node transactions for updating into the ledger. The attacker will constantly eavesdrop the BSMD network traffic; whenever the target client proposes a transaction to chosen endorsers during the transaction proposal phase, endorser sends a response back to the client after endorsing the transaction. The attacker can modify or dump a certain number of responses by the endorsers so as to defeat the policy requirement of the chaincode for the transaction which means failing of transaction proposal phase. The client will have to again repeat the transaction proposal. Similar attacks in every attempt of the client will prevent him from proposing a transaction.

The second motive of the attacker is to degrade the overall BSMD network efficiency, throughput or latency. Targeting specific endorsers in the network will lead to failure of endorsement of transactions, which will directly affect the rate of block generation in the ledger. We present the diagram of the detailed steps of this attack scenario in Fig. 5.

*Wormhole attack within a channel ($S_{20}$):* Due to the fact that the sender and receiver identities are not hidden on the channel of a permissioned blockchain as per vulnerability ($V_{15}$), the permissioned blockchain technology is prone to wormhole attack. Within a channel, compromising a member leads to leakage of ledger information of all members, to everyone outside the channel. Within a private network, a malicious node creates a virtual private network with the outside network and leaks the information of its own private network. This attack can be launched without any knowledge of honest nodes of the private network. To address this weakness in the consensus design, techniques to anonymize sender and receiver identity inside a channel should be implemented. We present the diagram of the detailed steps of this attack scenario in Fig. 6.

### 3) PROBABILITIES OF OCCURRENCE

A threat represents a pair of actor-scenario. The probability of occurrence ($P$) represents the chance that a given threat materializes. It is the likelihood that an actor achieves an attack scenario with success, thus, the goal of the attack. We calculate the probability by threat, i.e., for each actor of each scenario. According to 1, the un-normalized probability $P$ is the sum of the three actors attributes: capacity (c), opportunity (o) and motivation (m). The $c$, $o$, $m$ values vary from 1 to 4, with 4 corresponding to a higher likelihood.

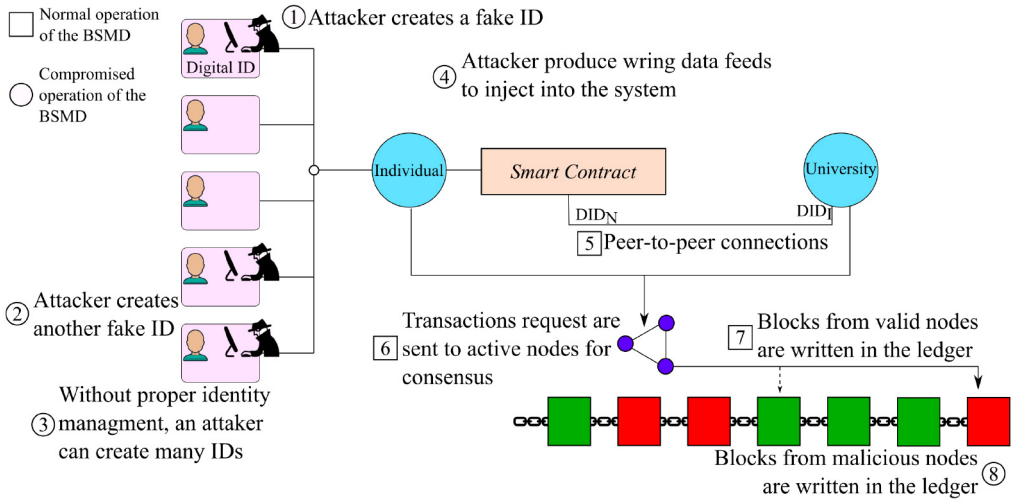



**FIGURE 3.** Detailed steps of attack scenario $S_2$: False data injection.

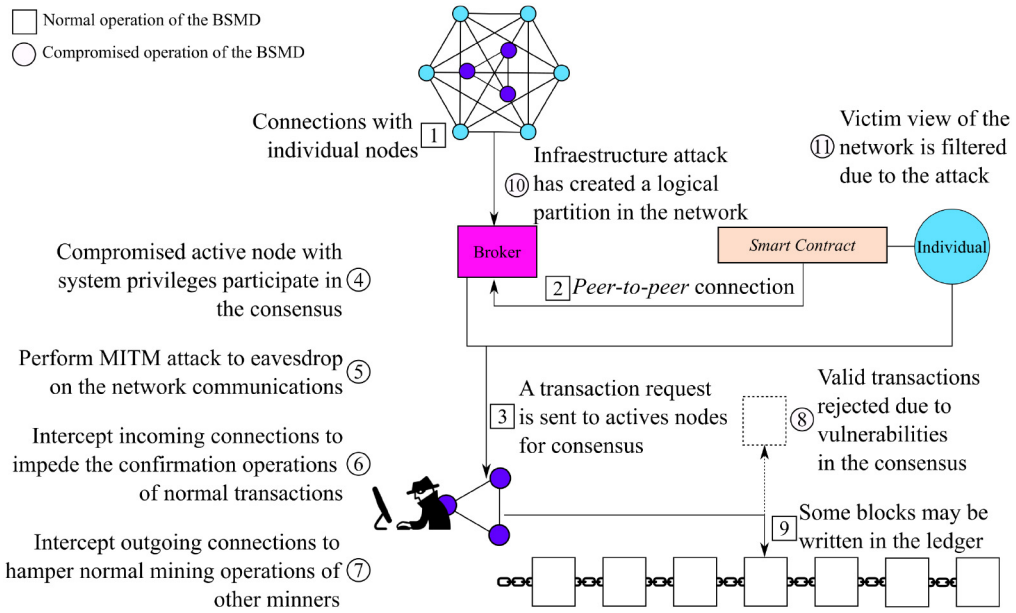



**FIGURE 4.** Detailed steps of attack scenario $S_{11}$: Disruption of the blockchain with an infrastructure attack.

*Capacity:* It represents the knowledge required to perform the attack, the software tools or the equipment needed and the technical complexity of the attack in the terms of the vulnerabilities required to conduct the attack. For every scenario of every attack goal, we examine every actor's capacity.

$A_1$ are experts in the development of malicious code, if there is much less information available about the architecture. Actor type $A_4$ represents the experts in the field of Web attack. On the other hand, $A_2$ and $A_3$ normally are specialists in the extraction of information from people or systems, are experts with solid technical knowledge of computer programming and have more human resources. They often have specialized human resources. When solid knowledge of computer programming and architecture is required, actor $A_3$ recruits experts with exceptional technical skills and have more human resources than Actor $A_4$. On the other hand, $A_3$, $A_4$, $A_5$ capacity will be higher because they have more human resources and specialized personnel, than actor $A_1$.

*Opportunity:* The attacker's opportunity is evaluated regarding constraints in terms of time, space and the ability for the attacker to be access the network. In terms of the space constraint, $A_2$ and $A_3$ have the same opportunities. Actors $A_2$ and $A_3$ will have higher opportunity than of Actors $A_1$ and $A_4$. Actors $A_4$ are specifically trained to infiltrate private sites without being noticed. In terms of time constraint, actors $A_2$ and $A_3$ have better possibilities to know when certain events will take place. Scenarios that take place during circumstances during which there are constraints in terms of time and space, actor $A_3$'s and $A_5$'s opportunity is higher than that of Actors $A_1$ and $A_4$, because we consider

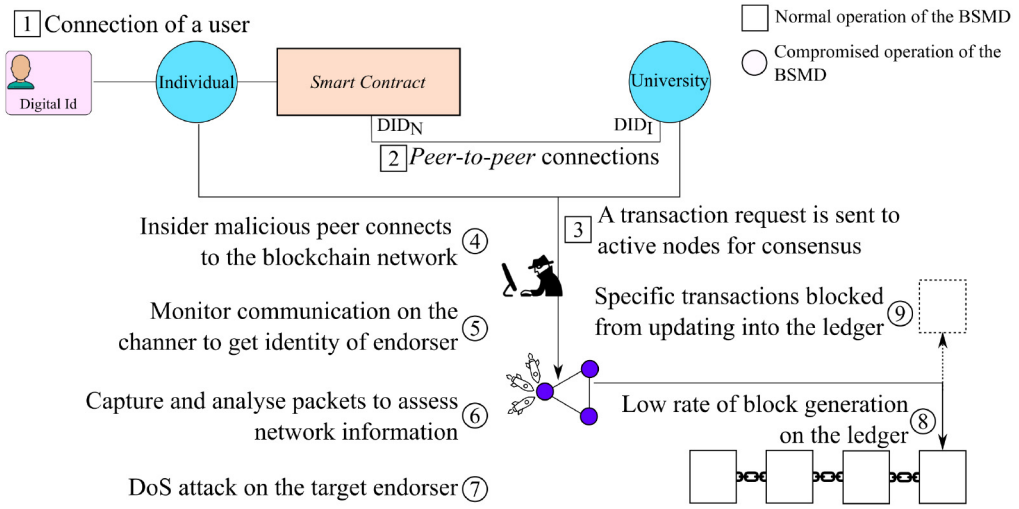



**FIGURE 5.** Detailed steps of attack scenario $S_{18}$: Attacks on committee members.

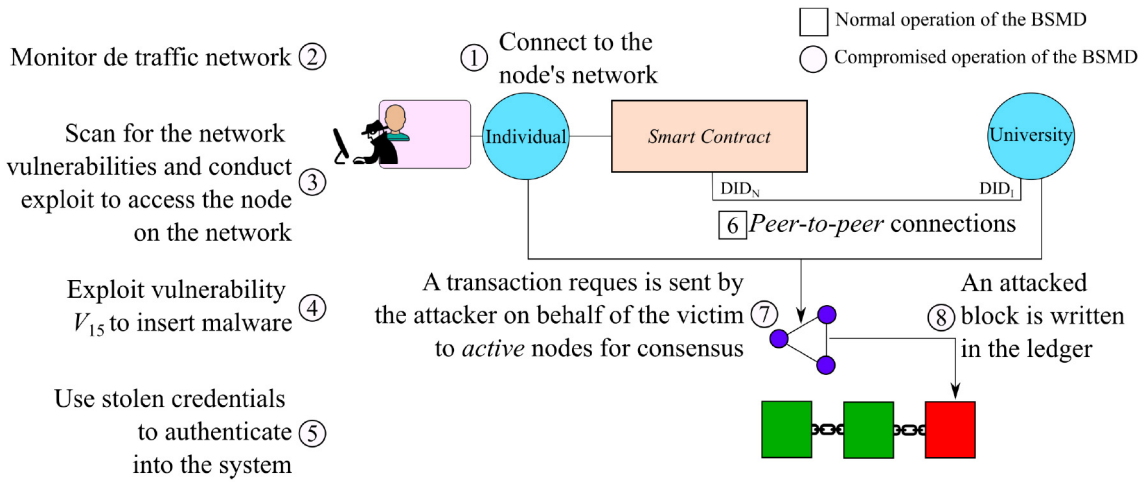



**FIGURE 6.** Detailed steps of attack scenario $S_{20}$: Wormhole attack within a channel.

that an insider can have the same skills as a secret agent to infiltrate a network. For Web attacks where there is no restriction of time and space, the actors' opportunity will be higher.

*Motivation:* The motivation represents the likelihood that the attackers will put the resources in place and conduct the attack scenario given what they will gain from the successful accomplishment of the attack goal. We evaluate the motivation according to whether the goal of the attack is the purpose of the attacker. Both Actors $A_3$ and $A_4$ benefit from gaining access to sensitive personal information. For $A_3$, this attack objective is in line with their profession. Thus the motivation of Actor $A_3$ will be higher than that of Actor $A_4$ because for $A_3$ this attack objective is an end in itself while for $A_4$ it is a means to an end, i.e., sow national disorder.

However, $A_2$'s motivation is the highest when it comes to gaining knowledge of the data-market, since the goal of this attack is the purpose of their profession. Actors $A_3$ and $A_4$ follow them with the same level of motivation. The motivation of $A_1$ is the lowest because obtaining system information is not an end but a means to accomplish their activities. Finally, $A_1$ and $A_5$ may conduct attacks in order to make money while $A_3$ and $A_4$ are motivated by the opportunity to cause harm. $A_1$ would make money through ransom. $A_5$'s motivation to some scenarios will make him earn a large amount of money. Actors $A_3$ and $A_4$'s motivation is the same, although high, it is lower than that of $A_5$.

Fig. 7 illustrates the relationship between attack goals, $G_i$, scenarios, $S_j$ and actors, $A_k$ such that $i \in \{1, 2 \ldots, 5\}, j \in \{1, 2 \ldots, 22\}$ and $k \in \{1, 2, 3, 4, 5\}$. The relationship between $G_i$ and $S_j$ is defined by Table 4 and all actors $A_k$ can intervene in any scenario $S_j$. This relationship defines how the probability of occurrence of threats, $P$, is computed. Hence, $P$ is a function of attack goals $G_i$, scenarios, $S_j$ and actors, $A_k$. According to (1), $P$ is computed as the sum of the actors attributes for an attack goal at a specific scenario, therefore, each actor attribute (capacity, opportunity or motivation) is,

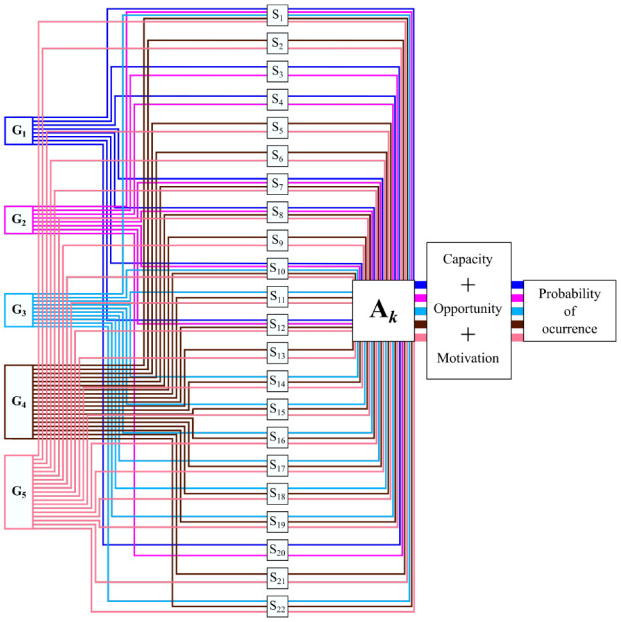



**FIGURE 7.** Probability of occurrence of identified threat.

also, a function of $G_i$, $S_j$ and $A_k$. Hence the probability of occurrence of identified threat, $P$, is defined in (3).

$$P(G_i, S_j, A_k) = c(G_i, S_j, A_k) + o(G_i, S_j, A_k) + m(G_i, S_j, A_k) \tag{3}$$

such that:

$$\begin{aligned} f &: S_j \mapsto G_i \ : f \text{ is given by Table 4} \\ c(G_i, S_j, A_k) &\in \{1, 2, 3, 4\} \\ o(G_i, S_j, A_k) &\in \{1, 2, 3, 4\} \\ m(G_i, S_j, A_k) &\in \{1, 2, 3, 4\} \\ i &\in \{1, 2, 3, 4, 5\} \\ j &\in \{1, 2 \ldots, 22\} \\ k &\in \{1, 2, 3, 4, 5\} \end{aligned}$$

The rates assigned to $c(G_i, S_j, A_k)$, $o(G_i, S_j, A_k)$ and $c(G_i, S_j, A_k)$ for each possible combination of $G_i$, $S_j$ and $A_k$ are shown in Appendix B. It also shows the results of $P(G_i, S_j, A_k)$. An open source code for computing $P(G_i, S_j, A_k)$ for a given $G_i$, $S_j$ and $A_k$ can be found at: https://github.com/LiTrans/BSMD/tree/master/security/risk_assessment_framework.

### C. STEP 3 - COMBINED RISK ASSESSMENT

According to step 3 of our methodology, we calculate the risk as per( 2) ($R = I \times P_{MAX}$) associated with each attack scenario based on the most likely actor. $P_{MAX}$ is computed as the maximum probability of occurrence of all actors for each attack goal at each valid scenario, and its shown in (4).

$$P_{MAX}(G_i, S_j) = \max_{1 \le k \le 5} \{P(G_i, S_j, A_k)\} \tag{4}$$

**TABLE 5.** Risk characterization.

| Risk levels | Values | Risk treatment |
|---|---|---|
| Unacceptable | $R \geq 36$ | Refuse |
| Undesirable | $24 \leq R < 36$ | Manage |
| Acceptable | $12 < R < 24$ | Accept |
| Negligible | $0 \leq R \leq 12$ | Accept |

such that:

$$\begin{aligned} f &: S_j \mapsto G_i \ : f \text{ is given by Table 4} \\ i &\in \{1, 2, 3, 4, 5\} \\ j &\in \{1, 2 \ldots, 22\} \end{aligned}$$

The impacts, $I$, are obtained from Table 1 and each impact type (monetary, privacy, trust or integrity) is associated to an attack goal, i.e., each impact type is a function of $G_i$. Hence the risk of an impact for an attack goal at a valid scenario is computed as in (5):

$$R_T(G_i, S_j) = I_T(G_i) \times P_{MAX}(G_i, S_j) \tag{5}$$

such that:

$$\begin{aligned} f &: S_j \mapsto G_i \ : f \text{ is given by Table 4} \\ T &\in \{monetary, privacy, integrity, trust\} \\ i &\in \{1, 2, 3, 4, 5\} \\ j &\in \{1, 2 \ldots, 22\} \end{aligned}$$

The risk, $R_T(G_i, S_j)$, thus corresponds to the unnormalized probability, $P_{MAX}(G_i, S_j)$, ranging from 3 to 12, times the impact, $I_T(G_i)$ ranging from 1 to 4. In such a setup, $R_T(G_i, S_j)$ values vary between 3 and 48. This gives insight of the risk that each threat (scenario and actor pair) represents separately for each impact type. Thus, the analysis responds to the needs of the individuals of the blockchain network as well as those of the other nodes such as the companies, universities and government. Each group will be able to assess its riskiest threat.

Depending on the risk value, different risk management techniques can be chosen as per Table 5. The techniques to manage the risk are refuse, manage or accept. The acceptability of a risk is subjective and may depend on factors such as resources, budget and number of users affected. In this paper, we consider that the risk should be refused when it's considered unacceptable because of its catastrophic consequences. The risk should be accepted when it is either negligible or acceptable because the benefits that the system brings outweigh its potential risks.

In Fig. 8, we present the results of the combined risk assessment for all attack goals at the corresponding scenarios. Each graph on Fig. 8 corresponds to an attack goal, $G_i$, and its associated scenarios, $S_j$. The bars indicate $R_T(G_i, S_j)$, i.e., the associated risk for a given attack goal, scenario and impact type. The monetary impact type is represented with the magenta bars, the privacy impact type is the blue bar, the integrity impact type is the brown bar and the trust impact type is the cyan bar. The green, yellow, orange and red

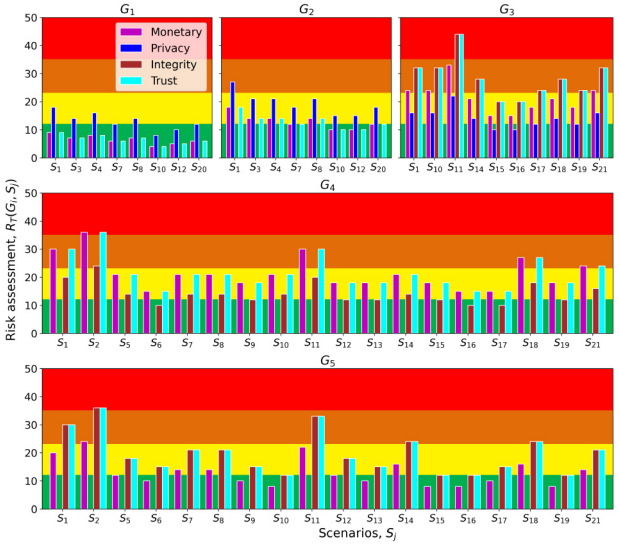



**FIGURE 8.** Combined risk assessment for each Attack Goal at each Impact.

colored areas mark the limits for the negligible, acceptable, undesirable and unacceptable risk levels, respectively.

The detailed results of $R_T(G_i, S_j)$ for all $T \in \{monetary, privacy, integrity, trust\}$, $i \in \{1, 2 \ldots, 5\}$ and $j \in \{1, 2 \ldots, 22\}$ such that $S_j \in G_i$ are presented in Appendix C. A repository reproducing the results shown in the Appendix and Fig. 8 can be found at: https://github.com/LiTrans/BSMD/tree/master/security/risk_assessment_framework.

From Fig. 8 we note that in terms of monetary, privacy, integrity and trust, $G_1$ does not represent a potential risk that needs to be managed. However, $G_3$ contains several threats that represent a risk that is either unacceptable or undesirable. In terms of privacy, only one threat represents a potential risk that needs to be managed. In the following section is presented a thorough impact and risk analysis.

## V. IMPACT ANALYSIS

In this section, from the combined risk assessment, we look at the monetary, privacy, integrity and trust impact. We focus on the threats representing either an unacceptable or an undesirable risk for the nodes of the blockchain network.

### A. MONETARY IMPACT

Attack goals $G_3$, $G_4$ and $G_5$ represent a risk in terms of economic losses. The victims of the attacks may be individuals participating in the blockchain network, universities, transport agencies, government nodes or companies. $G_3$ contains four undesirable threats (Scenarios $S_1$ with actors $A_1$ and $A_5$, $S_{10}$ with actor $A_5$, $S_{11}$ with actor $A_5$, and $S_{21}$ with actor $A_5$). These threats should be managed with priority. To solve the threats associated with Scenario $S_1$, it is essential to ensure proper key protection techniques.

By analyzing the other threats, we realism that the actor's attack method is always the same. The insider adversary is a member of the network. Precisely, the insider exploits the lack of peer privacy to conduct the attacks. To mitigate the threats associated to Scenarios $S_{11}$ and $S_{21}$, privacy preservation techniques against the internal attacker should be implemented as proposed in [25]. More reliable Virtual Private Network (VPN) solutions should be adopted, even if they require more investment and monitoring. Also, preventive models against inside adversary specific to *Hyperledger* is needed. The threat posed by Scenario $S_{10}$ can be managed by fixing design flaws of the blockchain platform. If resources are not properly configured, chaincode (*Hyperledger*'s definition of smart contract) that usually runs in a secured Docker container can be compromised and manipulated by the attacker to exploit any vulnerable hosts that it discovers and accept commands from, and exfiltrate results to, a remote command-and-Řcontrol server.

$G_4$ contains one unacceptable threat ($S_2$ with actors $A_1$, $A_3$ and $A_4$) and five undesirable threats (Scenarios $S_1$ with actors $A_1$, $S_{11}$ with actor $A_5$, $S_{18}$ with actor $A_5$, $S_{21}$ with actor $A_5$, and, $S_{22}$ with all actors). The unacceptable threat should be managed with high priority by setting proper identity management. The threats posed by $S_{18}$ can be managed by the implementation of anonymizing endorsers techniques to avoid the pre-knowledge of endorsers in the chaincode. The committee should always change its members and the committees should constantly change how they proceed so that attacks on committee members are not possible. Finally, the threat related to scenario $S_{22}$ is particular since it is feasible by all actors or cyber threat sources against the blockchain ecosystem. If no incentive or rewards are put in place, operations can be executed in quantity on the blockchain in one transaction causing nodes to be exhausted and thus corrupting the blockchain system. Precisely, there should be a price to pay to ask for a service, either it be with a system collecting real money or tokens per transaction to be made. Otherwise, some malicious participants may exploit this opportunity by sending many fake transactions to drain an active node from its resources, since in the current version of the BSMD there is no price to pay to ask for a service.

$G_5$ contains two undesirable threats (Scenarios $S_2$ with actors $A_1$, $A_3$ and $A_4$ and $S_{22}$ with all actors) that need to be managed in a similar way as described above. From an economic point of view, vulnerability $V_2$ must be eliminated because its exploitation constitutes an unacceptable risk for the users and all the nodes of the BSMD network. $V_2$ is eliminated by the implementation of robust authentication solutions specifically designed for the data-market ecosystem. Defense mechanisms should be deployed particularly with regards to unauthenticated data feeds because of their potential to produce falsified mobility data. On another hand, since $V_{22}$ can be exploited by any attacker, the vulnerability can be eliminated by the designers of the blockchain system by a proper implementation of the blockchain framework to account for incentives and rewards as a means to control the transactions flowing on the network. Finally, vulnerabilities $V_1$, $V_9$, $V_{12}$, $V_{15}$, $V_{16}$ can be eliminated with privacy preservation schemes and robust VPN techniques.

### B. PRIVACY IMPACT

The results presented in Fig. 8 reveal that $G_2$ is the riskiest attack goal in terms of privacy. This is because of the undesirable risk that Scenario $S_1$ conducted by $A_1$ represents, i.e., cybercriminals that use compromised computer systems to commit identity theft. To solve the threat associated with Scenario $S_1$, it is essential to implement proper key protection techniques. If the keys are not maintained securely, the compromise could lead to fraudulent transactions.

### C. INTEGRITY IMPACT

From Fig. 8, we realise that $G_3$ contains one unacceptable threat to the integrity of the individuals or the blockchain network ($S_{11}$ with actor $A_5$) exploiting vulnerability $V_{12}$. This threat should be managed with high priority. As mentioned above, privacy preservation techniques, monitoring and preventive models against the internal attacker should be implemented. Such techniques will also help in addressing the threats related to attack scenarios $S_1$, $S_{10}$, $S_{14}$, $S_{17}$, $S_{18}$, $S_{19}$ and $S_{21}$. In fact, these threats constitute an undesirable risk to the integrity of the system and need to be mitigated. By analyzing them, we notice that the actor is almost always an insider, a corrupted active node of the blockchain network, or an infrastructure node that maliciously exploits the blockchain system for economic reward. Once $V_{12}$ is adequately managed, the vulnerabilities exploited by the attack scenarios should be eliminated. This is feasible by widely deploying BGP security extensions, fixing consensus flaws and to avoid attacks related to scenario $S_{17}$, a node can build a reputation list of trusted peers or employ a timestamping authority.

Again, the threat from scenario $S_2$, that was unacceptable in terms of monetary loss, is only undesirable in terms of integrity. Attack goal $G_4$ thus contains this one undesirable threat that can be addressed by implementing identity management techniques.

Finally, when it comes to inducing participants in the blockchain network to make errors, we notice from Fig. 8, that this attack goal represents a major risk in terms of integrity. $G_5$ contains two unacceptable threats ($S_2$ with actors $A_1$, $A_3$ and $A_4$, and $S_{22}$ with all actors) and four undesirable risks (Scenarios $S_1$ with actors $A_1$ and $A_5$, $S_{11}$ with actor $A_5$, $S_{14}$ with actor $A_5$ and $S_{18}$ with actor $A_5$).

### D. TRUST IMPACT

In $G_3$, an attacker that manipulates and modifies the blockchain information will have catastrophic impact on the trust of the BSMD network. It is because the entities will have no belief in the reliability of the transactions in the blockchain. $G_3$ contains one unacceptable threat ($S_{11}$ with actor $A_5$) by exploiting vulnerability $V_{12}$ and seven undesirable threats related to attack scenarios ($S_1$, $S_{10}$, $S_{14}$, $S_{17}$, $S_{18}$, $S_{19}$ and $S_{21}$).

$G_4$ contains one unacceptable threat ($S_2$ with actors $A_1$, $A_3$ and $A_4$) and five undesirable threats (Scenarios $S_1$ with actors $A_1$, $S_{11}$ with actor $A_5$, $S_{18}$ with actor $A_5$, $S_{21}$ with actor $A_5$, and, $S_{22}$ with all actors). These threats are the same as the ones that had a monetary impact on the system and can be managed in the same manner.

Finally, when it comes to inducing participants in the blockchain network to make errors, we notice from Fig. 8, that this attack goal represents a major risk in terms of trust in the blockchain ecosystem. $G_5$ contains two unacceptable threats ($S_2$ with actors $A_1$, $A_3$ and $A_4$, and $S_{22}$ with all actors) and four undesirable risks (Scenarios $S_1$ with actors $A_1$ and $A_5$, $S_{11}$ with actor $A_5$, $S_{14}$ with actor $A_5$ and $S_{18}$ with actor $A_5$). We notice that these threats are the same as the one that affected the integrity of the system. Thus they can be managed by the same techniques already proposed in this section.

## VI. DISCUSSION

The risk assessment reveals that the higher risks factors correspond to attackers that exploit the vulnerabilities in the blockchain system with the aim to conduct sabotage activities ($G_4$). Particularly, we identified that the threat from false data injection, i.e., scenario $S_2$ with actors $A_1$, $A_3$ and $A_4$ represents an unacceptable risk because of its monetary and trust impact. Malicious activities have the potential to generate severe monetary loss by exploiting the victims in exchange of money. Moreover, sabotage activities may induce an entity to not receive rewards for its service and disruption of the network will have severe consequences on the trust of BSMD.

On the other hand, if attackers are able to inject the ecosystem with falsified transportation information ($G_5$), by conducting the same attack scenario $S_2$, potentially they will have a severe impact on the integrity of the users and mobility data. Also, if some nodes of the blockchain use the transport-related data acquired from the blockchain for traffic applications, this will necessary degrade the performance of the application and have a severe consequence on the trust of BSMD. Accordingly, it is essential that this threat is managed with high priority by setting proper identity management techniques. Vulnerability $V_2$ exploited by the attackers of this scenario must be eliminated by the implementation of robust authentication solutions specifically designed for the data-market ecosystem. Defense mechanisms should be deployed specifically with regards to unauthenticated data feeds because of their potential to produce falsified mobility data.

Another outcome of the risk analysis is that two other threats related to the disruption of the blockchain with an infrastructure attack (attack scenario $S_{11}$ with actor $A_5$) and flooding of the nodes of the blockchain network ($S_{22}$ with all actors) represent an unacceptable risk that needs to be mitigated with high priority. The attacks will have catastrophic impact on the integrity and trust of the BSMD ecosystem because there will be no belief in the transactions in the ledger.

Particularly, since any attacker can exploit the absence of incentive and rewards ($V_{22}$) to conduct scenario $S_{22}$, this vulnerability should be eliminated by a proper implementation of the blockchain framework to account for incentives and rewards as a means to control the transactions flowing on the network. To mitigate the threat associated to scenario $S_{11}$, privacy preservation techniques, monitoring and preventive models against the internal attacker should be implemented specifically for permissioned blockchains.

Finally, the risk analysis revealed that gaining knowledge about the data-market ($G_1$) and accessing sensitive data on the nodes of the network ($G_2$) are attack goals that represent negligible and acceptable risk levels. In fact, attackers can compromise other technologies easier in order to have access to confidential data. Consequently, information disclosure in this context is not considered as severe.

## VII. CONCLUSION

We proposed a risk assessment framework for cyberattacks on smart mobility/transportation systems using blockchain technology. As a case study, we used the multi-layered Blockchain framework for Smart Mobility Data-markets (BSMD), a public permissioned blockchain. We consider the risk as a function of probability and impact. We proposed to quantify the risk associated to the blockchain technology, thus, our risk assessment consists of three main steps namely: 1) actor-based risk analysis to extract the impact 2) scenario-based risk analysis to extract the probability, and 3) combined risk assessment to quantify the risk.

The outcomes of the risk analysis show that the higher risks correspond to attackers that are able to inject the ecosystem with falsified transportation information and exploit the vulnerabilities in the blockchain system to conduct sabotage activities. The disruption of the blockchain with an infrastructure attack, and the flooding of the nodes of the blockchain network due to the absence of incentive and rewards in the implementation also represent an unacceptable risk.

In future work, we will study solutions designed for the data-market ecosystem in particular regarding unauthenticated data feeds, because of their potential to produce falsified mobility data. Specifically the threats that aim at the disruption of the applications supported by the blockchain and coming from the connection between the digital and the physical world because it is important to create awareness in the early stages of their development.

## APPENDIX A
## DETAILED DESCRIPTION OF THE ATTACK SCENARIOS

### $S_1$: NODE SPOOFING ATTACK

Node spoofing is when an attacker steals DID credentials exploiting vulnerability $V_1$ and communicates with another node on behalf of the user. If cryptographic keys are not stored or maintained properly, it could cause the compromise and disclosure of private keys leading to fraudulent transactions or loss of assets. This will lead to the compromising of the integrity and privacy of the operations. Wallet theft uses classic mechanisms such as phishing, which include system hacking, the installation of buggy software, and the incorrect use of wallets. The attacker may exploit the vulnerabilities in the different DID protection schemes to conduct the following attacks: Opening communication channels with multiple nodes, sharing transport data, intercepting information from other nodes, forging of transactions, hampering normal mining operations of other miners and correlating DIDs in the ledger to track single nodes.

### $S_3$: LINKABILITY OF USER IDENTITIES TO THEIR TRANSACTIONS

In BSMD, given that a node will have one unique DID per transaction, it is difficult for an attacker to correlate DIDs in the ledger to track single nodes. In fact, if users were only identified by one DID, an attacker wishing to de-anonymize users may exploit vulnerability $V_3$ and $V_4$ to construct the one-to-many mapping between users and DIDs and associate information external to the system with the users. This attack is prevented in BSMD by storing the mapping of a user to his or her DID on that user's node only and by allowing each user to generate as many DIDs as required.

However, many work points to the difficulty in maintaining anonymity where network data on user behaviour is available and illustrates how seemingly minor information leakages can be aggregated to pose significant risks [26]. Using an appropriate network representation, it is possible to associate many DIDs with each other, and with external identifying information. With appropriate tools, the activity of known nodes can be observed in detail. Even more, large centralized nodes such as government, universities and companies are capable of identifying and tracking considerable portions of user activity.

In fact, user identities may be linked with their transactions by various deanonymization techniques, such as network flow and temporal analysis, address clustering, transaction fingerprinting, TCP/IP operation of the underlying peer-to-peer network and context discovery (partial node directory associating nodes and their DIDs with off-network information). Attackers may use global network properties, such as degree distribution, to identify outliers. They can use local network properties to examine the context in which a node operates by observing the nodes with which he or she interacts with either directly or indirectly. The dynamic nature of the network also enables attackers to perform flow and temporal analyses by examining the significant flows between groups of nodes over time.

### $S_4$: LEAKAGE OF THE LOCATION OF THE USER

BSMD implements techniques which consist of hiding the real location of the user using either $K$-anonymity or a Differential privacy called Geo-indistinguishability (GeoInd). Unfortunately, these privacy protection measures are not very robust and may lead to privacy leakage of its sender.

Attackers may use the weak privacy protection vulnerability $V_5$ to extract the real location of the user and thus compromise the confidentiality of the data.

#### $S_5$: NON-DETERMINISTIC BEHAVIOR OF THE CONTRACT PROGRAMMING LANGUAGE

Source code of contracts is often not public in contrast to their bytecode. For this reason, bytecode decompilers, analyzers, and automated exploit generators can be utilized by attackers to conduct code analysis and exploit the vulnerabilities $V_7$ and $V_{21}$ in the program design and writing of *smart contracts*. The threat agents may stand for developers who intentionally introduce semantic bugs in *smart contracts*, bugs that represent backdoors. Most security vulnerabilities in Fabric chaincodes arise from the non-deterministic behavior of Go, which may lead to consensus failure [21].

#### $S_6$: UNDESIRED BEHAVIOR ARISING FROM PLATFORM FEATURES

Attackers can exploit vulnerabilities $V_9$ and $V_{18}$ pertaining to design flaws in the blockchain platform, particularly some range query methods so that phantom reads (malicious data) in the code are not detected. Also, by exploiting the read your write vulnerability, attackers may force the system to get into an unexpected behavior.

#### $S_7$: SMART CONTRACT FOR MALICIOUS ACTIVITIES

Attackers may exploit the lack of monitoring of smart contract applications (vulnerabilities $V_6$ and $V_{20}$) to leverage *smart contracts* for a variety of malicious activities. On one hand, a Criminal Smart Contract (CSC) can facilitate the leakage of confidential information, theft of cryptographic keys, and various sabotage activities. Such a CSC might pay a reward for (confidential) delivery of a target private key. In most of the existing blockchain platforms, pseudonymous transactions provide a nest for criminal *smart contracts* [27].

Also, lack of monitoring of *smart contracts* may allow denial-of-service (DoS) attacks. Attackers could simply introduce *smart contracts* that take a very long time to execute, thus severely reducing the performance of the blockchain [28]. To address DoS attacks from untrusted chaincode, an node in the BSMD can simply abort an execution according to a local policy if it suspects a DoS attack. Due to the permissioned nature of Fabric, detecting clients that try to mount a DoS attack by flooding the network with invalid transactions should not be challenging. This is due to the fact that the ledger of Fabric contains all transactions, including those that are deemed invalid. One approach would be to black-list such clients according to a policy that could be put in place.

#### $S_8$: INSTALLATION OF MALWARE ON NODES

Attackers may exploit the security design flaw (vulnerability $V_9$) pertaining to insufficient chaincode sandboxing to install malicious chaincode. Remote Access Trojan (RAT) malware create a foothold in a corporate network that allows other systems to be scanned and attacked.

The installation of malicious chaincode would be a non-trivial exercise for most threat actors, given the level of access required. However, plausible scenarios exist. For example, an attacker may infiltrate the organization responsible for developing and maintaining the chaincode for an existing ledger, and then publish an update containing the malicious data. Note that the chaincode does not necessarily contain any overtly malicious functionality at the time it is installed on the network. It merely needs to be able to download and execute code from a command-and-control server at some future point in time.

#### $S_9$: DOS ATTACK ON THE HOST

Design miscalculations, or malware can easily result in a DoS attack if host resources are not properly configured (vulnerability $V_9$), because all containers share kernel resources. If one container can monopolize access to certain resources (memory, or user IDs , CPU, memory, disk I/O), it can starve out other containers on the host, resulting in DoS, whereby legitimate users are unable to access part or all of the system.

#### $S_{10}$: ELEVATED PRIVILEGES GAINED BY THE USER

If the host system is not configured correctly through the Docker container, an attacker can gain various privileges or can bypass isolation checks by exploiting vulnerability $V_9$, thus accessing sensitive information from the host. Normally, it should not be possible for an attacker to gain access to other containers or the host. However, since users are not namespaced, any process that breaks out of a container will have the same privileges on the host as it did in the container. In addition, by default, the Docker daemon runs as a root. This can cause potential elevation attacks (elevated privileges gained by user), such as those of the root user, usually through a bug in the application code that needs to run with additional privileges.

#### $S_{12}$: EXECUTE CODE REMOTELY WITH DNS ATTACKS

Node.js and Go can be exploited to execute code remotely using the DNS rebinding vulnerability $V_{10}$. The attack is possible from a malicious website that accesses the Web browser on a computer that has network access to the computer running the Node.js or Go process [29]. The malicious website can use a DNS rebinding vulnerability to trick the Web browser and bypass same-origin-policy checks, allowing HTTP connections to the localhost or to a host on the local network. If a process with an active debug port is running on the localhost or on a host on the local network, the malicious website can connect to it as a debugger and get full access to the code execution.

This attack can be used to breach a private network by causing the victim's Web browser to access computers at private IP addresses and return the results to the attacker. It can also be employed to use the victim machine for spamming, distributed DoS attacks, or other malicious activities.

### $S_{13}$: REMOTE DOS ATTACK

An attacker may exploit specific security flaws in Node.js as per vulnerability $V_7$ to conduct a remote DoS attack. Node.js crashing or throwing an exception could be remotely exploited using some of the existing WebSocket clients [30]. For validating nodes of the BSMD system, this attack leads to disruption of some blockchain dependent services. One mitigation is to peer only with white-listed nodes. Methods to prevent volumetric Distributed DoS (DDoS) include on-premise filtering with an extra network device, cloud filtering via redirection of traffic through a cloud when DDoS is detected or through a cloud DDoS mitigation service.

### $S_{14}$: BGP HIJACKING ATTACK

To intercept the network traffic of blockchain, attackers either leverage or manipulate BGP routing through vulnerability $V_{11}$. BGP hijacking typically requires the control of network operators, which could potentially be exploited to delay network messages. Routing attacks, including both node level and network-level attacks, may split the network, or delay the speed of block propagation. Also, Internet service providers may intercept connections to conduct network hijacking attacks.

### $S_{15}$: DELAYING NETWORK COMMUNICATIONS IN FORKABLE BLOCKCHAIN SYSTEMS

A fork can split the consensus group and potentially make the PBFT consensus stall, which can further be aggravated. To manipulate forks, the key strategy is to isolate a group of nodes, i.e., to partition the network for a given duration by delaying network communications between subgroups of nodes. An attacker can exploit vulnerability $V_{13}$, at the network level, the BGP hijacking, and at the application-level protocol to surround the targeted nodes with ones under the attacker's control. As a result, it would cause the network to fail to establish a common acceptance truth or a unique authoritative chronology blockchain.

Also, in a weakly synchronous network where block propagation and message exchange among committee members can suffer from uncertain delays, tentative blocks can result in a fork. To resolve the forks of tentative blocks, a recovery protocol should run to accept a tentative block if there is any. Specially, the recovery protocol needs to be invoked by a synchronized committee. Forks should be resolved timely and orphan consensus forks should be blocked. To "orphan" a block means to deny it into the main chain.

### $S_{16}$: ADVERSARIAL CENTRALIZATION OF CONSENSUS POWER

A design assumption about the decentralized distribution of consensus power can be violated. In fact, an attacker can exploit vulnerability $V_{14}$ to manipulate and modify the blockchain information. Nodes may be malicious and wish to alter the outcome of the consensus protocol by deviating from it. They may vote wrong, equivocate (tell different nodes different votes), relay wrong votes to the nodes they are connected to and lie about who they are connected to. In Byzantine attacks, a quorum of 1/3 adversarial consensus nodes might cause the protocol being disrupted or even halted. An attacker can conduct the following attacks.

- Forging of transactions by reversing transactions.
- Excluding and modifying the ordering of transactions.
- Hampering normal mining operations of other miners.
- Impeding the confirmation operation of normal transactions.

In terms of security, there are certainly advantages of private blockchains where the miners or validators cannot be anonymous. *Hyperledger* uses its own chaincode to secure transactions and achieve consensus. BSMD is a public closed blockchain, the number and the nodes that participate in consensus are known. An organization pre-selects the participants and thus, they are highly trusted. Therefore, the chances of someone acting maliciously on a network are less because malicious nodes can be identified and fines can be applied to those guilty of such practices.

### $S_{17}$: TIME-VALIDATION ATTACKS

An attacker can exploit the timestamping consensus flaw $V_{19}$ by connecting a significant number of nodes and propagating inaccurate timestamps. This action can slow down or speed up the victim node's network time. When such

**TABLE 6.** Probability of occurrence of identified threats for $G_1$ - Gain knowledge about the data-market.

| $S_j$ | $A_k$ | c | o | m | P |
|---|---|---|---|---|---|
| $S_1$ | $A_1$ | 3 | 3 | 2 | 8 |
| | $A_2$ | 2 | 3 | 4 | 9 |
| | $A_3$ | 2 | 3 | 3 | 8 |
| | $A_4$ | 1 | 2 | 3 | 6 |
| $S_3$ | $A_1$ | 1 | 2 | 1 | 4 |
| | $A_2$ | 2 | 2 | 3 | 7 |
| | $A_3$ | 2 | 2 | 2 | 6 |
| | $A_4$ | 2 | 1 | 2 | 5 |
| $S_4$ | $A_1$ | 1 | 1 | 2 | 4 |
| | $A_2$ | 2 | 2 | 4 | 8 |
| | $A_3$ | 2 | 2 | 3 | 7 |
| | $A_4$ | 2 | 2 | 3 | 7 |
| $S_7$ | $A_1$ | 2 | 2 | 1 | 5 |
| | $A_2$ | 2 | 2 | 2 | 6 |
| | $A_3$ | 1 | 2 | 1 | 4 |
| | $A_4$ | 2 | 2 | 1 | 5 |
| $S_8$ | $A_1$ | 3 | 2 | 2 | 7 |
| | $A_2$ | 2 | 2 | 2 | 6 |
| | $A_3$ | 2 | 1 | 1 | 4 |
| | $A_4$ | 2 | 1 | 1 | 4 |
| $S_{10}$ | $A_1$ | 2 | 1 | 1 | 4 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 1 | 1 | 3 |
| $S_{12}$ | $A_1$ | 2 | 1 | 1 | 4 |
| | $A_2$ | 2 | 1 | 2 | 5 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 1 | 1 | 3 |
| $S_{20}$ | $A_1$ | 2 | 2 | 1 | 5 |
| | $A_2$ | 2 | 2 | 2 | 6 |
| | $A_3$ | 2 | 2 | 1 | 5 |
| | $A_4$ | 1 | 2 | 1 | 4 |

**TABLE 7.** Probability of occurrence of identified threats for $G_2$ - Access sensitive data on the nodes of the network.

| $S_j$ | $A_k$ | c | o | m | P |
|---|---|---|---|---|---|
| $S_1$ | $A_1$ | 3 | 3 | 3 | 9 |
| | $A_2$ | 2 | 3 | 3 | 8 |
| | $A_3$ | 2 | 3 | 3 | 8 |
| | $A_4$ | 1 | 2 | 4 | 7 |
| $S_3$ | $A_1$ | 1 | 1 | 2 | 4 |
| | $A_2$ | 2 | 2 | 2 | 6 |
| | $A_3$ | 2 | 2 | 3 | 7 |
| | $A_4$ | 2 | 1 | 4 | 7 |
| $S_4$ | $A_1$ | 1 | 2 | 1 | 4 |
| | $A_2$ | 3 | 2 | 2 | 7 |
| | $A_3$ | 3 | 2 | 2 | 7 |
| | $A_4$ | 2 | 1 | 3 | 6 |
| $S_7$ | $A_1$ | 2 | 3 | 1 | 6 |
| | $A_2$ | 2 | 2 | 1 | 5 |
| | $A_3$ | 2 | 2 | 2 | 6 |
| | $A_4$ | 2 | 1 | 2 | 5 |
| $S_8$ | $A_1$ | 3 | 2 | 2 | 7 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 2 | 2 | 2 | 6 |
| | $A_4$ | 2 | 2 | 2 | 6 |
| $S_{10}$ | $A_1$ | 2 | 2 | 1 | 5 |
| | $A_2$ | 2 | 1 | 1 | 4 |
| | $A_3$ | 2 | 1 | 2 | 5 |
| | $A_4$ | 1 | 1 | 2 | 4 |
| $S_{12}$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 1 | 1 | 2 | 4 |
| $S_{20}$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 2 | 2 | 5 |
| | $A_3$ | 1 | 2 | 3 | 6 |
| | $A_4$ | 1 | 1 | 3 | 5 |

a desynchronized node creates a block, this block can be discarded by a network due to freshness constraints.

### $S_{19}$: A NETWORK SCHEDULER THAT THWARTS THE CONSENSUS PROTOCOL

Many BFT protocols assume synchronous delivery of messages. However, this assumption and vulnerability $V_{17}$ can be violated by an unpredictable network scheduler, as demonstrated on PBFT protocol in [31]. At any given time, the designated leader is responsible for proposing the next batch of transactions. If progress is not made, either because the leader is faulty or because the network has stalled, then the nodes attempt to elect a new leader. The PBFT protocol critically relies on a weakly synchronous network for liveness.

First, the scheduler assumes that a single node has crashed. Then, the network delays messages whenever a correct node is the leader, preventing progress and causing the next node in round-robin order to become the new leader. When the crashed node is the next up to become the leader, the scheduler immediately heals the network partition and delivers messages very rapidly among the honest nodes; however, since the leader has crashed, no progress is made here either. This attack violates the weak synchrony assumption because it must delay messages for longer and longer each cycle, since PBFT widens its timeout interval after each failed leader election. On the other hand, it provides larger and larger periods of synchrony as well. However, since these periods of synchrony occur at inconvenient times, PBFT is unable to make use of them.

**TABLE 8.** Probability of occurrence of identified threats for $G_3$ - Manipulate and modify blockchain information.

| $S_j$ | $A_k$ | c | o | m | P |
|---|---|---|---|---|---|
| $S_1$ | $A_1$ | 2 | 3 | 3 | 8 |
| | $A_2$ | 1 | 2 | 3 | 6 |
| | $A_3$ | 1 | 2 | 3 | 6 |
| | $A_4$ | 2 | 2 | 4 | 8 |
| $S_{10}$ | $A_1$ | 3 | 1 | 1 | 5 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 3 | 3 | 2 | 8 |
| $S_{11}$ | $A_1$ | 1 | 1 | 2 | 4 |
| | $A_2$ | 1 | 2 | 3 | 6 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 4 | 3 | 4 | 11 |
| $S_{14}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 3 | 2 | 2 | 7 |
| $S_{15}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 1 | 2 | 5 |
| $S_{16}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 1 | 3 | 5 |
| $S_{17}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 2 | 2 | 6 |
| $S_{18}$ | $A_1$ | 3 | 1 | 2 | 6 |
| | $A_2$ | 2 | 2 | 2 | 6 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 3 | 2 | 2 | 7 |
| $S_{19}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 2 | 2 | 6 |
| $S_{21}$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 4 | 2 | 2 | 8 |

### $S_{21}$: MALLEABILITY ATTACK

In *Hyperledger* network, the ledger of a channel inside the *Hyperledger* limits the accessibility to only members that are part of the channel. The client can choose an endorser of its choice during the transaction proposal phase, due to which the identity of the endorser is disclosed to everyone in the network, including an insider adversary. If an attacker is a member of the channel on *Hyperledger*, as in conventional data sharing schemes, the attacker can eavesdrop all the network traffic inside a channel of *Hyperledger* fabric by exploiting vulnerability $V_{15}$. The attacker also has access to every transaction present in the ledger. When a sender broadcasts his transaction to other peers, the adversary can modify the content of a transaction, i.e., the signature or even modify the receiver identity and then recalculate the transaction hash and further broadcast the transaction. The sender waits for the endorsement of his transaction, which

**TABLE 9.** Probability of identified threats for $G_4$ - Sabotage activities.

| $S_j$ | $A_k$ | c | o | m | P |
|---|---|---|---|---|---|
| $S_1$ | $A_1$ | 3 | 3 | 4 | 10 |
| | $A_2$ | 2 | 2 | 4 | 8 |
| | $A_3$ | 2 | 2 | 4 | 8 |
| | $A_4$ | 2 | 2 | 2 | 6 |
| $S_2$ | $A_1$ | 4 | 4 | 4 | 12 |
| | $A_2$ | 4 | 4 | 4 | 12 |
| | $A_3$ | 4 | 4 | 4 | 12 |
| | $A_4$ | 4 | 4 | 2 | 10 |
| $S_5$ | $A_1$ | 3 | 1 | 3 | 7 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 1 | 2 | 4 | 7 |
| $S_6$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 1 | 2 | 2 | 5 |
| $S_7$ | $A_1$ | 4 | 1 | 2 | 7 |
| | $A_2$ | 2 | 1 | 1 | 4 |
| | $A_3$ | 2 | 1 | 1 | 4 |
| | $A_4$ | 1 | 1 | 2 | 4 |
| $S_8$ | $A_1$ | 4 | 1 | 2 | 7 |
| | $A_2$ | 3 | 1 | 2 | 6 |
| | $A_3$ | 3 | 1 | 2 | 6 |
| | $A_4$ | 1 | 2 | 2 | 5 |
| $S_9$ | $A_1$ | 2 | 1 | 3 | 6 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 1 | 2 | 2 | 5 |
| $S_{10}$ | $A_1$ | 2 | 1 | 3 | 6 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 2 | 2 | 3 | 7 |
| $S_{11}$ | $A_1$ | 1 | 1 | 3 | 5 |
| | $A_2$ | 1 | 2 | 3 | 7 |
| | $A_3$ | 1 | 1 | 4 | 6 |
| | $A_4$ | 4 | 3 | 3 | 10 |
| $S_{12}$ | $A_1$ | 3 | 1 | 2 | 6 |
| | $A_2$ | 2 | 1 | 2 | 5 |
| | $A_3$ | 2 | 1 | 2 | 5 |
| | $A_4$ | 1 | 2 | 1 | 4 |
| $S_{13}$ | $A_1$ | 2 | 2 | 2 | 6 |
| | $A_2$ | 2 | 1 | 2 | 5 |
| | $A_3$ | 2 | 1 | 2 | 5 |
| | $A_4$ | 1 | 2 | 2 | 5 |
| $S_{14}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 2 | 1 | 4 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 2 | 3 | 7 |
| $S_{15}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 2 | 2 | 6 |
| $S_{16}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 1 | 1 | 3 | 5 |
| $S_{17}$ | $A_1$ | 1 | 1 | 2 | 4 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 1 | 2 | 5 |
| $S_{18}$ | $A_1$ | 3 | 1 | 2 | 6 |
| | $A_2$ | 2 | 2 | 2 | 6 |
| | $A_3$ | 2 | 1 | 2 | 5 |
| | $A_4$ | 4 | 3 | 2 | 9 |
| $S_{19}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 2 | 2 | 6 |
| $S_{21}$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 4 | 2 | 2 | 8 |
| $S_{22}$ | $A_1$ | 4 | 4 | 3 | 11 |
| | $A_2$ | 4 | 4 | 3 | 11 |
| | $A_3$ | 4 | 4 | 3 | 11 |
| | $A_4$ | 4 | 4 | 3 | 11 |

**TABLE 10.** Probabilities for $G_5$ - Induce participants in the blockchain network to make errors.

| $S_j$ | $A_k$ | c | o | m | P |
|---|---|---|---|---|---|
| $S_1$ | $A_1$ | 4 | 3 | 3 | 10 |
| | $A_2$ | 4 | 2 | 3 | 9 |
| | $A_3$ | 4 | 2 | 3 | 9 |
| | $A_4$ | 2 | 2 | 3 | 7 |
| $S_2$ | $A_1$ | 4 | 4 | 4 | 12 |
| | $A_2$ | 4 | 4 | 4 | 12 |
| | $A_3$ | 4 | 4 | 4 | 12 |
| | $A_4$ | 4 | 4 | 3 | 11 |
| $S_5$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 2 | 3 | 6 |
| $S_6$ | $A_1$ | 2 | 1 | 1 | 4 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 2 | 2 | 5 |
| $S_7$ | $A_1$ | 3 | 1 | 3 | 7 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 2 | 1 | 4 |
| $S_8$ | $A_1$ | 3 | 1 | 3 | 7 |
| | $A_2$ | 2 | 2 | 2 | 6 |
| | $A_3$ | 2 | 1 | 2 | 5 |
| | $A_4$ | 1 | 2 | 2 | 5 |
| $S_9$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 1 | 2 | 4 |
| $S_{10}$ | $A_1$ | 1 | 1 | 2 | 4 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 1 | 1 | 4 |
| $S_{11}$ | $A_1$ | 1 | 1 | 2 | 4 |
| | $A_2$ | 1 | 2 | 2 | 5 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 4 | 3 | 4 | 11 |
| $S_{12}$ | $A_1$ | 2 | 1 | 3 | 6 |
| | $A_2$ | 1 | 1 | 3 | 5 |
| | $A_3$ | 1 | 1 | 3 | 5 |
| | $A_4$ | 1 | 1 | 1 | 3 |
| $S_{13}$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 1 | 1 | 1 | 3 |
| $S_{14}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 2 | 2 | 4 | 8 |
| $S_{15}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 1 | 2 | 4 |
| $S_{16}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 1 | 1 | 2 | 4 |
| $S_{17}$ | $A_1$ | 1 | 1 | 2 | 4 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 2 | 1 | 2 | 5 |
| $S_{18}$ | $A_1$ | 2 | 1 | 1 | 4 |
| | $A_2$ | 1 | 1 | 2 | 4 |
| | $A_3$ | 1 | 1 | 2 | 4 |
| | $A_4$ | 3 | 2 | 3 | 8 |
| $S_{19}$ | $A_1$ | 1 | 1 | 1 | 3 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 1 | 1 | 2 | 4 |
| $S_{21}$ | $A_1$ | 2 | 1 | 2 | 5 |
| | $A_2$ | 1 | 1 | 1 | 3 |
| | $A_3$ | 1 | 1 | 1 | 3 |
| | $A_4$ | 3 | 2 | 2 | 7 |
| $S_{22}$ | $A_1$ | 4 | 4 | 4 | 12 |
| | $A_2$ | 4 | 4 | 4 | 12 |
| | $A_3$ | 4 | 4 | 4 | 12 |
| | $A_4$ | 4 | 4 | 4 | 12 |

never happens as the transaction hash was modified by the adversary. In this situation, the sender being confused, resend the transaction to the receiver [32].

### *$S_{22}$: FLOODING OF THE NODES OF THE BLOCKCHAIN NETWORK*

If no incentive is put in place an attacker can exploit vulnerability $V_{22}$ and initiate operations in quantity in one

transaction. This will cause the user to consume a lot of computing resources, and block synchronization for the *active nodes* will be significantly slower compared with the normal situation. An attacker can also initiate a DoS attack on the blockchain. They create a million empty accounts which need to be stored in the state tree. This attack causes a waste of hard disk resources. At the same time, the node information synchronization and transaction processing speed are significantly decreased.

## APPENDIX B
## DETAILED COMPUTATION OF PROBABILITIES OF OCCURRENCE

The un-normalized probability of occurrence is the sum of the three actors attributes: capacity ($c$), opportunity ($o$) and motivation ($m$). The $c$, $o$, $m$ values vary from 1 to 4, with 4 corresponding to a higher likelihood. The un-normalized probability of occurrence $P(G_i, S_j, A_k)$ as follows:

$$P(G_i, S_j, A_k) = c(G_i, S_j, A_k) + o(G_i, S_j, A_k) + m(G_i, S_j, A_k)$$

such that:

$$\begin{aligned} f : S_j \mapsto G_i \; &: f \text{ is given by Table 4} \\ c(G_i, S_j, A_k) &\in \{1, 2, 3, 4\} \\ o(G_i, S_j, A_k) &\in \{1, 2, 3, 4\} \\ m(G_i, S_j, A_k) &\in \{1, 2, 3, 4\} \\ i &\in \{1, 2 \ldots, 5\} \\ j &\in \{1, 2 \ldots, 22\} \\ k &\in \{1, 2, 3, 4, 5\} \end{aligned}$$

The Tables 6, 7, 8, 9, 10 show the rates assigned to $c(G_i, S_j, A_k)$, $o(G_i, S_j, A_k)$, $c(G_i, S_j, A_k)$ for a given attack goal, $G_i$, scenario, $S_j$, and actor $A_k$.

## APPENDIX C
## DETAILED COMPUTATION OF THE RISK ASSESSMENT

The risk of an impact of an attack goal at a valid scenario is computed as follows:

$$R_T(G_i, S_j) = I_T(G_i) \times P_{MAX}(G_i, S_j)$$

such that:

$$\begin{aligned} f : S_j \mapsto G_i \; &: f \text{ is given by Table 4} \\ T &\in \{monetary, privacy, integrity, trust\} \\ i &\in \{1, 2 \ldots, 5\} \\ j &\in \{1, 2 \ldots, 22\} \end{aligned}$$

In Tables 11 and 12, we present the results of the combined risk assessment for a given attack goal, scenario and impact type.

**TABLE 11.** Combined risk assessment - *m* : Monetary, *p* : Privacy, *in* : Integrity, *t* : Trust.

| | | | Monetary | | Privacy | | Integrity | | Trust | |
|---|---|---|---|---|---|---|---|---|---|---|
| Goal | $S_j$ | $P_{MAX}$ | $I_m$ | $R_m$ | $I_p$ | $R_p$ | $I_{in}$ | $R_{in}$ | $I_t$ | $R_t$ |
| $G_1$ | $S_1$ | 9 | 1 | 9 | 2 | 18 | - | - | 1 | 9 |
| | $S_3$ | 7 | 1 | 7 | 2 | 14 | - | - | 1 | 7 |
| | $S_4$ | 8 | 1 | 8 | 2 | 16 | - | - | 1 | 8 |
| | $S_7$ | 6 | 1 | 6 | 2 | 12 | - | - | 1 | 6 |
| | $S_8$ | 7 | 1 | 7 | 2 | 14 | - | - | 1 | 7 |
| | $S_{10}$ | 4 | 1 | 4 | 2 | 8 | - | - | 1 | 4 |
| | $S_{12}$ | 5 | 1 | 5 | 2 | 10 | - | - | 1 | 5 |
| | $S_{20}$ | 6 | 1 | 6 | 2 | 12 | - | - | 1 | 6 |
| $G_2$ | $S_1$ | 9 | 2 | 18 | 3 | 27 | - | - | 2 | 18 |
| | $S_3$ | 7 | 2 | 14 | 3 | 21 | - | - | 2 | 14 |
| | $S_4$ | 7 | 2 | 14 | 3 | 21 | - | - | 2 | 14 |
| | $S_7$ | 6 | 2 | 12 | 3 | 18 | - | - | 2 | 12 |
| | $S_8$ | 7 | 2 | 14 | 3 | 21 | - | - | 2 | 14 |
| | $S_{10}$ | 5 | 2 | 10 | 3 | 15 | - | - | 2 | 10 |
| | $S_{12}$ | 5 | 2 | 10 | 3 | 15 | - | - | 2 | 10 |
| | $S_{20}$ | 6 | 2 | 12 | 3 | 18 | - | - | 2 | 12 |
| $G_3$ | $S_1$ | 8 | 3 | 24 | 2 | 16 | 4 | 32 | 4 | 32 |
| | $S_{10}$ | 8 | 3 | 24 | 2 | 16 | 4 | 32 | 4 | 32 |
| | $S_{11}$ | 11 | 3 | 33 | 2 | 22 | 4 | 44 | 4 | 44 |
| | $S_{14}$ | 7 | 3 | 21 | 2 | 14 | 4 | 28 | 4 | 28 |
| | $S_{15}$ | 5 | 3 | 15 | 2 | 10 | 4 | 20 | 4 | 20 |
| | $S_{16}$ | 5 | 3 | 15 | 2 | 10 | 4 | 20 | 4 | 20 |
| | $S_{17}$ | 6 | 3 | 18 | 2 | 12 | 4 | 24 | 4 | 24 |
| | $S_{18}$ | 7 | 3 | 21 | 2 | 14 | 4 | 28 | 4 | 28 |
| | $S_{19}$ | 6 | 3 | 18 | 2 | 12 | 4 | 24 | 4 | 24 |
| | $S_{21}$ | 8 | 3 | 24 | 2 | 16 | 4 | 32 | 4 | 32 |

**TABLE 12.** Combined risk assessment - *m* : Monetary, *p* : Privacy, *in* : Integrity, *t* : Trust.

| | | | Monetary | | Privacy | | Integrity | | Trust | |
|---|---|---|---|---|---|---|---|---|---|---|
| Goal | $S_j$ | $P_{MAX}$ | $I_m$ | $R_m$ | $I_p$ | $R_p$ | $I_{in}$ | $R_{in}$ | $I_t$ | $R_t$ |
| $G_4$ | $S_1$ | 10 | 3 | 30 | - | - | 2 | 20 | 3 | 30 |
| | $S_2$ | 12 | 3 | 36 | - | - | 2 | 24 | 3 | 36 |
| | $S_5$ | 7 | 3 | 21 | - | - | 2 | 14 | 3 | 21 |
| | $S_6$ | 5 | 3 | 15 | - | - | 2 | 10 | 3 | 15 |
| | $S_7$ | 7 | 3 | 21 | - | - | 2 | 14 | 3 | 21 |
| | $S_8$ | 7 | 3 | 21 | - | - | 2 | 14 | 3 | 21 |
| | $S_9$ | 6 | 3 | 18 | - | - | 2 | 12 | 3 | 18 |
| | $S_{10}$ | 7 | 3 | 21 | - | - | 2 | 14 | 3 | 21 |
| | $S_{11}$ | 10 | 3 | 30 | - | - | 2 | 20 | 3 | 30 |
| | $S_{12}$ | 6 | 3 | 18 | - | - | 2 | 12 | 3 | 18 |
| | $S_{13}$ | 6 | 3 | 18 | - | - | 2 | 12 | 3 | 18 |
| | $S_{14}$ | 7 | 3 | 21 | - | - | 2 | 14 | 3 | 21 |
| | $S_{15}$ | 6 | 3 | 18 | - | - | 2 | 12 | 3 | 18 |
| | $S_{16}$ | 5 | 3 | 15 | - | - | 2 | 10 | 3 | 15 |
| | $S_{17}$ | 5 | 3 | 15 | - | - | 2 | 10 | 3 | 15 |
| | $S_{18}$ | 9 | 3 | 27 | - | - | 2 | 18 | 3 | 27 |
| | $S_{19}$ | 6 | 3 | 18 | - | - | 2 | 12 | 3 | 18 |
| | $S_{21}$ | 8 | 3 | 24 | - | - | 2 | 16 | 3 | 24 |
| | $S_{22}$ | 11 | 3 | 33 | - | - | 2 | 22 | 3 | 33 |
| $G_5$ | $S_1$ | 10 | 2 | 20 | - | - | 3 | 30 | 3 | 30 |
| | S2 | 12 | 2 | 24 | - | - | 3 | 36 | 3 | 36 |
| | $S_5$ | 6 | 2 | 12 | - | - | 3 | 18 | 3 | 18 |
| | $S_6$ | 5 | 2 | 10 | - | - | 3 | 15 | 3 | 15 |
| | $S_7$ | 7 | 2 | 14 | - | - | 3 | 21 | 3 | 21 |
| | $S_8$ | 7 | 2 | 14 | - | - | 3 | 21 | 3 | 21 |
| | $S_9$ | 5 | 2 | 10 | - | - | 3 | 15 | 3 | 15 |
| | $S_{10}$ | 4 | 2 | 8 | - | - | 3 | 12 | 3 | 12 |
| | $S_{11}$ | 11 | 2 | 22 | - | - | 3 | 33 | 3 | 33 |
| | $S_{12}$ | 6 | 2 | 12 | - | - | 3 | 18 | 3 | 18 |
| | $S_{13}$ | 5 | 2 | 10 | - | - | 3 | 15 | 3 | 15 |
| | $S_{14}$ | 8 | 2 | 16 | - | - | 3 | 24 | 3 | 24 |
| | $S_{15}$ | 4 | 2 | 8 | - | - | 3 | 12 | 3 | 12 |
| | $S_{16}$ | 4 | 2 | 8 | - | - | 3 | 12 | 3 | 12 |
| | $S_{17}$ | 5 | 2 | 10 | - | - | 3 | 15 | 3 | 15 |
| | $S_{18}$ | 8 | 2 | 16 | - | - | 3 | 24 | 3 | 24 |
| | $S_{19}$ | 4 | 2 | 8 | - | - | 3 | 12 | 3 | 12 |
| | $S_{21}$ | 7 | 2 | 14 | - | - | 3 | 21 | 3 | 21 |
| | $S_{22}$ | 12 | 2 | 24 | - | - | 3 | 36 | 3 | 36 |

## REFERENCES


[1] H. Hasanova, U.-J. Baek, M.-G. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *Int. J. Netw. Manag.*, vol. 29, no. 2, Jan. 2019, Art. no. e2060.

[2] G. Morganti, E. Schiavone, and A. Bondavalli, "Risk assessment of blockchain technology," in *Proc. 8th Latin-Amer. Symp. Dependable Comput. (LADC)*, 2018, pp. 87–96.

[3] J.-G. Dumas, S. Jimenez-Garcès, and F. Şoiman, "Blockchain technology and crypto-assets market analysis: Vulnerabilities and risk assessment," in *Proc. 12th Int. Multi-Conf. Complexity Informat. Cybern.*, 2021, pp. 1–28.

[4] B. S. White, C. G. King, and J. Holladay, "Blockchain security risk assessment and the auditor," *J. Corporate Account. Financ.*, vol. 31, no. 2, pp. 47–53, 2020.

[5] D. López and B. Farooq, "A multi-layered blockchain framework for smart mobility data-markets," *Transp. Res. C, Emerg. Technol.*, vol. 111, pp. 588–615, Feb. 2020.

[6] J. C. Wong, *Uber Concealed Massive Hack That Exposed Data of 57m Users and Drivers*, The Guardian, London, U.K., Nov. 2017. [Online]. Available: https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

[7] M. Mehar, "Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack," *J. Cases Inf. Technol.*, vol. 21, no. 1, pp. 19–32, 2019.

[8] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.

[9] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[10] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[11] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K.-K. R. Choo, "Security challenges and opportunities for smart contracts in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12004–12020, Aug. 2021.

[12] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers DCCL*, 2016, pp. 1–4.

[13] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts SoK," in *Proc. 6th Int. Conf. Principles Security Trust*, vol. 10204, 2017, pp. 164–186.

[14] I. Homoliak, S. Venugopalan, Q. Hum, and P. Szalachowski, "A security reference architecture for blockchains," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 390–397.

[15] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 3–16.

[16] S. Jagannathan and A. Sorini, "A cybersecurity risk analysis methodology for medical devices," in *Proc. IEEE Symp. Product Compliance Eng. (ISPCE)*, May 2015, pp. 1–6.

[17] W. Stallings and L. Brown, *Computer Security: Principles and Practice, Global Edition*. Hoboken, NJ, USA: Pearson Educ., Inc., 2018.

[18] Government Accountability Office (GAO). (2005). *Cyber Threat Source Descriptions*. Accessed: Mar. 20, 2020. [Online]. Available: https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions

[19] R. A. Mallah and B. Farooq, "Actor-based risk analysis for blockchains in smart mobility," in *Proc. 3rd Workshop Cryptocurrencies Blockchains Distrib. Syst.*, 2020, pp. 29–34.

[20] K. Yamashita, Y. Nomura, E. Zhou, B. Pi, and S. Jun, "Potential risks of hyperledger fabric smart contracts," in *Proc. IEEE Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Feb. 2019, pp. 1–10.

[21] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart contract security: A software lifecycle perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019.

[22] G. Shaw. (2017). *Security Assessment Technical Report*. Accessed: Mar. 25, 2020. [Online]. Available: https://wiki.hyperledger.org/download/attachments/2393550/technical_report_linux_foundation_fabric_august_2017_v1.1.pdf

[23] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Security Privacy (SP)*, May 2017, pp. 375–392.

[24] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 254–269.

[25] D. He, N. Kumar, and J.-H. Lee, "Privacy-preserving data aggregation scheme against internal attackers in smart grids," *Wireless Netw.*, vol. 22, no. 2, pp. 491–502, 2016.

[26] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and Privacy in Social Network*. New York, NY, USA: Springer, Jul. 2012, pp. 197–223.

[27] A. Juels, A. Kosba, and E. Shi, "The ring of Gyges: Investigating the future of criminal smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 283–295.

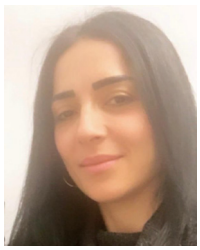
[28] E. Androulaki, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[29] R. Vagg. (2018). *March 2018 Security Releases*. Accessed: Mar. 30, 2020. [Online]. Available: https://nodejs.org/en/blog/vulnerability/march-2018-security-releases/

[30] M. Dawson. (2017). *DoS Security Vulnerability*. Accessed: Feb. 20, 2020. [Online]. Available: https://nodejs.org/en/blog/vulnerability/oct-2017-dos/

[31] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of BFT protocols," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 31–42.

[32] N. Andola, Raghav, M. Gogoi, S. Venkatesan, and S. Verma, "Vulnerabilities on hyperledger fabric," *Pervasive Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101050.

**RANWA AL MALLAH** (Member, IEEE) was born in Beirut, Lebanon. She received the Ph.D. degree in computer science from Polytechnique Montreal, Quebec, Canada.

She is currently a Postodoctoral Fellow of Ryerson University, Toronto, ON, Canada. She worked in the security of cyber–physical systems with the SecSI Research Laboratory, University of Montreal, Quebec. Her current research goal is to develop multidisciplinary, secure and highly intelligent solutions for the planning, and design and operation of cyber–physical systems in the context of smart cities.

**DAVID LÓPEZ** born in Mexico City, Mexico. He received the B.Sc. degree in mathematics, the M.S.Eng. degree in systems engineering-transportation, and the Ph.D. degree in systems engineering-transportation from the Universidad Nacional Autónoma de México (UNAM), Mexico City, Mexico, in 2004, 2011, and 2017, respectively.

He did his post doctoral research with LiTrans, Ryerson University from 2018 to 2019. He is an Associate Researcher with the Instituto de Ingenería, UNAM. He is currently working on personalized shortest paths in multimodal networks and blockhain development for transportation data transactions.

**BILAL FAROOQ** (Member, IEEE) received B.Eng. degree from the University of Engineering and Technology, Pakistan, in 2001, the M.Sc. degree in computer science from the Lahore University of Management Sciences, Pakistan, in 2004, and the Ph.D. degree from the University of Toronto, Canada, in 2011. He is the Canada Research Chair of Disruptive Transportation Technologies and Services and an Associate Professor with Ryerson University, Canada. His current work focuses on the network and behavioral implications of emerging transportation technologies and services. He received the Early Researcher Award in Québec in 2014 and Ontario in 2018, Canada.