A Reference Model for Security Risk Management of the Blockchain-based Applications

Mubashar Iqbal[0000−0003−0543−613X]

Institute of Computer Science, University of Tartu, Tartu, Estonia
mubashar.iqbal@ut.ee

Abstract. In order to realise the true potential of blockchain-based applications, the first step is to understand the associated risks and vulnerabilities. Blockchain-based applications are considered to be less vulnerable but there are certain security risks *(e.g., Sybil and Double-spending, etc)* within the blockchain-based applications that are debatable. There exists no comprehensive blockchain-based security reference model to systematically evaluate the security of blockchain-based applications. In this study, we illustrate the PhD thesis research work to build an ontology-based reference model for security risk management of blockchain-based applications. A reference model would establish a common ground and systematic understanding for professionals and researchers regarding the security of the blockchain-based application.

Keywords: Blockchain · Security Risks · Security Risk Management · Blockchain-based Security Reference Model

1 Introduction

A first cryptocurrency *bitcoin* introduced a concept of blockchain technology. Blockchain is a distributed immutable ledger technology [16] and over the past few years, blockchain technology is emerging in various fields and so blockchain-based applications. The security of blockchain-based applications is an important aspect of its acceptability. However, the involvement of the monetary assets raises security concerns, mainly when the attackers stole the monetary assets or damages the system. For example, the reentrancy attack on the Ethereum based decentralised autonomous organization (DAO) smart contracts when an adversary gained control of over $60 million Ethers [2, 12].

In order to realise the true potential of blockchain-based applications, the first step is to understand the associated risks and vulnerabilities. These risks and vulnerabilities could be exploited by an attacker and affect valuable assets and services. Mostly, the security issues arise by the wrong security decisions, incomplete knowledge, or misunderstanding the security needs of the software. In [7], the security risks that appear *(e.g., Sybil and Double-spending, etc)* within

the blockchain-based applications are debatable. However, there exists no comprehensive (or standardised) blockchain-based security reference model to systematically evaluate the security of blockchain-based applications. There exist few studies reporting on security challenges in the blockchain platforms [6, 17], but do not focus on the security of the blockchain-based applications.

The main research objective is formulated as follows: *How to assist the development of a reference model for security risk management of blockchain-based applications?* The blockchain-based security reference model would help to overcome the problems that are discussed above by enabling the systematic evaluation, understanding the main components and their relationships within the blockchain-based applications. A reference model would establish a common ground and systematic understanding for professionals and researchers regarding the security of the blockchain-based applications. It would also communicate security requirements to technical experts more effectively and efficiently.

Hence, the blockchain-based security reference model is required for security risk management of blockchain-based applications to identify security risks and their impacts timely. Ultimately, the reference model would lead to reducing the possible security risks to the blockchain-based applications.

This paper introduces the research work for the PhD thesis. The paper is structured as follows: Section 2 describes the research questions and foreseen outcome. Section 3 presents the research method. Section 4 discusses the preliminary results. Sections 5 presents the work in progress. Section 6 presents the background and related Work. Section 7 discusses the concluding remarks.

2 Research Questions and Foreseen Outcome

The aim of this research is to build a blockchain-based security reference model as a blockchain-based security risk management tool to systematically evaluate the security needs of *blockchain-based applications*. In order to achieve the aim, this research establishes the four main research questions. The research questions represent the step-by-step approach to reach the desired outcome. The research questions are:

[RQ1]: What is the state-of-the-art in the security of the blockchain-based applications?

In the RQ1, our research objectives were two-fold. First, we identify a list of security risks that are mitigated by the blockchain-based application. Second, the security risks that appear within the blockchain-based application after incorporating the blockchain technology.

[RQ2]: What are the means to analyse the security risks within the blockchain-based applications?

In the RQ2, we performed an analysis of security risks that are mitigated and appear within the blockchain-based applications to build conceptual models. Also, what assets to secure from the security risks, the potential vulnerabilities of security risks and countermeasures to mitigate the vulnerabilities.

[RQ3]: How to transform the conceptual models to a reference model for security risks management of the blockchain-based applications?

In the RQ3, we identify the common components *(e.g., concepts alignment)* of blockchain-based applications from the conceptual models *(knowledge from RQ2)* and feasible modelling language to build the reference model.

[RQ4]: How could the reference model be validated?

In the RQ4, we validate the reference model to answer *"Will the use of a reference model improve the security of the blockchain-based application?"*

The outcome of this research is *an ontology-based reference model for security risk management of the blockchain-based applications*. This reference model would evaluate the security needs of blockchain-based applications and help to explore the protected assets, security risks, and potential countermeasures. The reference model would not be dependent on the specific blockchain type or blockchain platform. It would be generic enough to perform a security risk management of different blockchain platforms-based applications.

3 Research Method

This research work follows four distinct research method approaches (Fig. 1), where each research approach represent the one research question respectively.

State-of-the-Art Technique: We follow the state-of-the-art technique to answer *RQ1*. In this stage, we conducted a systematic literature review (SLR) [7] to identify and understand the security risks related to the blockchain-based applications. The SLR approach led us to explore the security field of blockchain-based applications from two different perspectives. Firstly, we explain what security risks of the centralised applications are mitigated by introducing the blockchain-based applications. Secondly, we report the security risks of the blockchain-based applications which appear after introducing the blockchain technology.

Analytic Methodology: In the second stage, we analyse [8, 10, 9] the results of the SLR and built conceptual models of Ethereum and Hyperledger Fabric platforms-based applications. The analysis follows the security risk management (SRM) domain model [3, 13]. The analysis helps to identify the assets to secure, vulnerabilities, and how the vulnerabilities affect different assets within

the blockchain-based applications. The analysis results show the countermeasures to mitigate the identified vulnerabilities.

Proposal of Solution: The proposal of solution brings the concept of building the blockchain-based security reference model by using the ontology, and knowledge reasoning (from stage 1 & 2). The conceptual models that are built in a stage 2 transform into a blockchain-based security reference model by identifying the common components and their relationships.

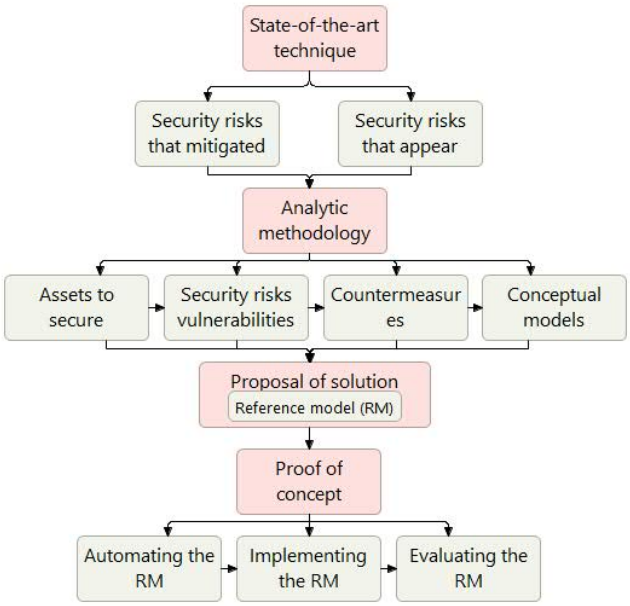

Fig. 1. The execution of research method and the main contributions.

Proof of Concept: In the final stage, the validation of the reference model will be performed. The validation stage includes three different phases: In the first phase, we automate the reference model to analyse the security of a blockchain-based application by a predefined set of rules in a controlled environment. In the second phase, we develop a blockchain-based application by implementing the newly built reference model analysis. In the third phase, we evaluate the effectiveness of the reference model. The effectiveness will be measured by using the requirements engineering techniques(e.g., meetings, questionnaires, and interviews). The experts will be approached who develop the blockchain-based application using the reference model.

4 Preliminary Results

The first year of the PhD focuses on the state-of-the-art of security risks on the blockchain-based applications. Firstly, we perform the SLR [7] by follow-

ing the SLR settings [11] and identify 68 research papers that were further analysed. The main contributions of this study are: 1) a list of security risks in the blockchain-based applications which are mitigated by incorporating the blockchain technology *(see Table 1)*, 2) a list of security risks in the blockchain-based applications which are appeared within blockchain-based applications by incorporating the blockchain technology *(see Table 1)*, 3) aggregate a list of possible countermeasures, and 4) an overview of the prominent research domains *(see Table 1)* which are nourishing by the blockchain. The results of this study could be seen as a preliminary checklist of security risks when implementing blockchain-based applications.

Table 1. Security risks of Ethereum- & Hyperledger Fabric-based applications & technology domains. The study identify other security risks [7] but this table only showing those risks that appear more than once in total within the mentioned applications & technology domains.

Security risks that are mitigated by introducing the blockchain-based applications.									
	Applications					Technology			
	Healthcare	Resource monit.	Financial	Smart vehicles	Voting	Security layer	IoT	other	Total
Data tampering attack	6	5	1	4	3	2	5	6	32
DoS/DDoS attack	0	5	1	3	1	7	3	5	25
MitM attack	1	4	1	1	1	2	2	2	14
Identity theft/Hijacking	1	2	0	0	0	0	1	1	5
Spoofing attack	0	0	0	0	1	0	1	2	4
Other risks/threats	2	0	1	0	1	5	5	3	17
Security risks that appear within the blockchain-based applications.									
Sybil attack	1	1	1	1	2	1	1	5	13
Double spending attack	0	4	2	0	0	2	0	2	10
51% attack	0	4	0	0	1	1	0	2	8
Deanonymization attack	0	2	1	1	1	1	1	0	7
Replay attack	0	2	1	0	0	4	0	0	7
Quantum comp. threat	1	0	0	0	0	2	0	2	5
Selfish mining attack	0	1	1	0	0	2	0	0	4
SC reentrancy attack	0	0	0	0	0	3	0	0	3
Other risks/threats	0	11	5	0	0	2	1	1	20
Total	12	41	15	10	11	34	20	31	174

Next, the results of SLR are analysed by the SRM domain model in two different phases. Firstly, the analysis represents the discussion on a comparison of blockchain-based applications *(e.g., Ethereum- and Hyperledger Fabric-based applications)* [8] to identify how blockchain-based applications mitigate data tampering risks. Secondly, we conducted a similar study to analyse Sybil and Double-spending risks [9] that appeared within blockchain-based applications after introducing the blockchain technology. The main contributions of both studies are as follows: 1) assets to be secured from the security risks 2) conceptual model of security risks for Ethereum-based applications 3) conceptual model of countermeasures for Ethereum-based applications 4) conceptual model

of security risks for Hyperledger Fabric-based applications 5) conceptual model of countermeasures for Hyperledger Fabric-based applications 6) the comparison of countermeasures. The models were constructed by an ArchiMate[1] modelling language. The ArchiMate offers a uniform structure to model different components of software applications [1]. The architectures modelling support us in the analysis of blockchain-based applications. The visual representation leads to a clear understanding and categorisation of the assets in different layers.

In order to validate the effectiveness of conceptual models and results so far *(the above mentioned preliminary results)*, we analysed the case of *"capital markets post-trade matching and confirmation"* [10]. The study has been performed by using the blockchain-based Corda platform. The reason to use Corda was to investigate the different emerging blockchain platforms to understand what are the similarities, differences, and approach as compared to Ethereum and Hyperledger Fabric to build blockchain-based applications.

5 Work in Progress

Currently, we are working on transforming the conceptual models to build an ontology-based reference model for security risk management of the blockchain-based applications. The work is in an initial phase where we are organising the components of the model and the processes. Figure 2 presents the abstract representation of the reference model. The reference model would include three main components: 1) define the settings 2) analysis based on the defined settings and risks assessment 3) guidelines of security risks and countermeasures. The analysis and risk assessment component include a *repository of security risks and countermeasures.*

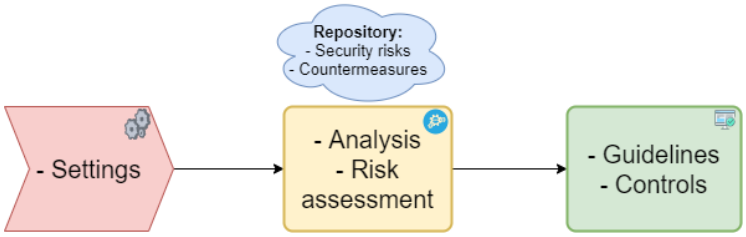

Fig. 2. The abstract representation of a reference model for security risk management of blockchain-based applications. The reference model includes three main components.

6 Background and Related Work

There already exist software security risk management frameworks *(e.g., NIST cybersecurity framework [4, 14], ISO 27001 International information security*

[1] https://www.archimatetool.com/

standard [5], etc.) to assess and improve their ability to prevent, detect, and respond to cyberattacks. The study [4] discusses to customise the NIST framework when developing the cybersecurity programs for the permissioned blockchain networks. The report states, *"the NIST framework as it is not a one-size-fits-all approach to managing cybersecurity risk because organizations will continue to have unique risks, different threats, different vulnerabilities, different risk tolerances, and how they implement the practices in the framework will vary"*. In addition to this, there are different blockchain platforms and their settings that also play an important role in the security of the blockchain-based applications.

Similarly, the OWASP is planning to build the blockchain security framework [15]. The project is aiming to create a comprehensive framework that would cover blockchain security from the ideation stage to the production stage. According to the OWASP project, *"it would help to define security requirements, selecting programming language, consensus protocols, functional security review, security testing requirements, audit and logging requirements, forensic readiness"*. The OWASP project is relevant to this PhD thesis research but currently, it is in a very initial phase as compared to our progress on this topic.

Our aim is to build a blockchain-specific security reference model for evaluating the security of blockchain-based applications. One relevant research [6] that presents the stacked hierarchy of various threats and threat-risk assessment using ISO/IEC 15408. In [17], the authors discussed the security and privacy of blockchain by following the survey approach. The research discussed the blockchain security and privacy properties by presenting the architecture of blockchain systems. Similar to a previous study [6], this study also explains the security of blockchain systems. The study illustrates the consensus algorithms, hash chained storage, mixing protocols, anonymous signatures, non-interactive zero-knowledge proof to gain an in-depth understanding of the security and privacy of blockchain systems. Both research studies focus on a security reference architecture for *blockchain systems (frameworks)* that is different from our research focus. For example, we are focusing on the *security of the blockchain-based applications*, not the blockchain systems.

7 Concluding Remarks

In this paper, we discussed the PhD thesis research work to build *an ontology-based reference model for security risk management of the blockchain-based applications*. We have completed the first two research questions *(RQ1 & RQ2)* and currently, working on a *RQ3* that relates to building the reference model. A reference model would systematically evaluate the security of blockchain-based applications. The reference model would establish a common ground and systematic understanding for professionals and researchers regarding the security of the blockchain-based applications. The reference model will be validated by the proof of concept *(Section 3)* that includes automating the reference model and implementing it to build a real-time blockchain-based application. In order to

evaluate the effectiveness of the reference model, the experts will be approached to participate in the validation process.

Acknowledgement

This PhD thesis is supervised by Prof. Raimundas Matulevičius at the Institute of Computer Science, University of Tartu, Estonia.

References

1. Aldea, A., Franken, H., Iacob, M.E., Quartel, D.: Strategy on a Page : An ArchiMate - based tool for visualizing and designing strategy (2018)
2. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on Ethereum smart contracts (SoK) (2017)
3. Dubois, É., Mayer, N., Heymans, P., Matulevičius, R.: Intentional perspectives on information systems engineering (2010)
4. English, E., Kim, A.D., Nonaka, M.: Advancing Blockchain Cybersecurity : Technical and Policy Considerations for the Financial Services Industry. In: Cybersecurity policy and resilience (2018)
5. Governance, I.: ISO 27001 Risk Assessments https://bit.ly/3aaAbW1
6. Homoliak, I., Venugopalan, S., Hum, Q., Szalachowski, P.: A security reference architecture for blockchains. In: 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019 (2019)
7. Iqbal, M., Matulevičius, R.: Blockchain-Based Application Security Risks: A Systematic Literature Review. In: CAiSE 2019 Workshop
8. Iqbal, M., Matulevičius, R.: Comparison of Blockchain-Based Solutions to Mitigate Data Tampering Security Risk. In: BPM 2019 Blockchain Forum
9. Iqbal, M., Matulevičius, R.: Exploring Sybil and Double-spending Risks in the Blockchain-based Applications
10. Iqbal, M., Matulevičius, R.: Managing Security Risks in Post-Trade Matching and Confirmation using CorDapp. In: 14th International Baltic Conference on Databases and Information Systems (2020)
11. Kitchenham, B., Charters, S.: Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3. In: Engineering **45**(4ve) (2007)
12. Liu, C., Liu, H., Cao, Z., Chen, Z., Chen, B., Roscoe, B.: ReGuard: Finding reentrancy bugs in smart contracts. In: International Conference on Software Engineering (2018)
13. Matulevičius, R.: Fundamentals of Secure System Modelling. Springer International Publishing, 1 edn. (2017)
14. NIST: Cybersecurity Framework: Helping organizations to better understand and improve their management of cybersecurity risk, https://bit.ly/2XHm9Zh
15. Pahl, M.: OWASP Blockchain Security Framework, https://bit.ly/2VwZGM2
16. Sato, T., Himura, Y.: Smart-Contract Based System Operations for Permissioned Blockchain. In: 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 (2018)
17. Zhang, R., Xue, R., Liu, L.: Security and privacy on blockchain. ACM Computing Surveys **52**(3) (2019)