Security/Privacy/Scalability issues in Title of Your Development Project

Full Name of Student
Student's Matriculation Number
Name of Student's School
Nanyang Technological University
Singapore
Email address of Student

Full Name of Student
Student's Matriculation Number
Name of Student's School
Nanyang Technological University
Singapore
Email address of Student

Full Name of Student
Student's Matriculation Number
Name of Student's School
Nanyang Technological University
Singapore
Email address of Student

***Abstract*—This is a template for the term paper of CE/CZ4153 Blockchain Technology course offered at the School of Computer Science and Engineering, Nanyang Technological University, Singapore. The paper should follow a similar style and format to incorporate all the necessary points of introduction, motivation, literature survey, observations, analysis, and solution to the issue. The paper should be 4 to 6 pages in length, including references. In case extra material is needed for analysis or arguments, the authors may include that as appendices, after the references.**

***Index Terms*—blockchain, Ethereum, smart contracts, tokens, may be some more with respect to your specific issue and project.**

I. Introduction

In this section, you should write a few paragraphs on blockchain (brief, can adapt from lectures, in your own words), the issues of security, privacy and scalability in blockchain (brief, can adapt from lectures, in your own words), what your development project topic was, and what you finally developed.

You should also mention exactly which issue out of the three Security, Privacy, Scalability you are going to present, and what would be the overall contribution of this paper. Argument as why this issue is the most important is not required here.

II. Motivation and Literature Survey

A. Motivation

In this subsection, you should clearly argue which one of the three issues – Security, Privacy, Scalability – concerns you the most in case of the Decentralized Application you developed. You may refer to the lectures, invited talks, related works, or any other instance of similar development projects to argue this.

B. Literature Survey

In this subsection, you should carefully curate similar works in the area of your interest, with proper citation (see references). This may include similar development projects or decentralized applications that have faced the same issues, lectures, articles, books or papers that talk about the issue in your case, or any other academic material related to your specific case.

Term Paper submitted for CE/CZ4153 Blockchain Technology, NTU.

III. Observations and Analysis

In this section, start by listing your main observations on the issue you chose in case of your development project. In each case, discuss the major considerations, analyze their impact (and ramifications) on your decentralized application, and compare it with similar cases in the literature, if you found any such case.

A. Issue X in case of Component I

Identify the specific issue X that will affect component Y of your decentralized application (e.g., re-entry bug in case of the auction contract). State why you think this issue may occur, what would be the impact on your application, and whether you know of any similar case in the literature where this happened.

B. Issue Y in case of Component I

There may be more than one issue per component. Think carefully to spot all such issues in your development project and write one subsection on each one of them. In case they are connected, do mention that too in this portion of your paper.

C. Issue Z in case of Component II

There may be more than one component with an issue. Think carefully to spot all such issues in your development project and write one subsection on each one of them. In case they are connected, do mention that too in this portion of your paper.

IV. Proposed Solutions

In this section, propose potential solutions to address the issues that you found in your analysis earlier. These solutions may be inspired from the lectures, invited talks, related works, or any other instance of similar development projects.

A. Solution to Issue X

Identify potential solutions to this issue. Clearly mention how you would apply the solution to your development project, and if you have already applied the solution. Applying the solution is of course not mandatory for the development project.

B. Solution to Issue Y

Identify potential solutions to this issue. Clearly mention how you would apply the solution to your development project, and if you have already applied the solution. Applying the solution is of course not mandatory for the development project. In case the solution to issue X already solves Y, mention that.

C. Solution to Issue Z

Identify potential solutions to this issue. Clearly mention how you would apply the solution to your development project, and if you have already applied the solution. Applying the solution is of course not mandatory for the development project. In case there exists no known solution to issue Z, propose a potential solution on your own, and argue why it may work.

V. Conclusion

In this section, you should mention exactly which issue out of the three – Security, Privacy, Scalability – you presented, and what is the overall contribution of this paper. The contribution may be in terms of your observations, analysis or proposed solutions presented for the issues and the components.

You may follow the IEEE paper format for the Tables, Lists, Figures, References, etc. Keep the format uniform in the paper.

References

[1] A. Narayanan, J. Bonneau, E. W. Felten, A. Miller, and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies – A Comprehensive Introduction," Princeton University Press 2016.

[2] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," IEEE Symp. on Security and Privacy 2015: 104-121.

[3] I. Eyal and E. Gun Sirer, "Majority is not enough: Bitcoin mining is vulnerable," Financial Cryptography, 2014, pp. 436?454.