SIT724- Task 3.1

Paper 1:

N. Atzei, M. Bartoletti, and T. Cimoli, “A Survey of Attacks on Ethereum Smart Contracts (SoK),” in *Principles of Security and Trust*, M. Maffei and M. Ryan, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2017, pp. 164–186. doi: 10.1007/978-3-662-54455-6_8.

- Evaluation:

This research paper is noteworthy as it delves into the susceptibilities present in smart contracts that are implemented on blockchain platforms, with a particular emphasis on Ethereum. The authors conduct an analysis of diverse categories of vulnerabilities that may be present in smart contracts and deliberate on their potential ramifications.

The focus of the assessment presented in this paper is to discern and classify distinct susceptibilities detected in smart contracts. The authors have utilized a methodical methodology to scrutinize a considerable quantity of intelligent contracts, evaluating their programming and detecting plausible security vulnerabilities. The vulnerabilities are categorized into various groups, including but not limited to access control, arithmetic, exception handling, and time manipulation.

The manuscript systematically presents the outcomes of the assessment, offering valuable perspectives on the frequency and gravity of distinct susceptibilities. The frequency of occurrence for each type of vulnerability is analyzed by the authors, who also employ statistical methods to measure their impact. Additionally, they conduct a comparative analysis of vulnerabilities present in various smart contracts, with the aim of identifying prevalent patterns and trends.

In addition, the assessment encompasses empirical instances of weaknesses in smart contracts that have been identified and leveraged in previous occurrences. The implications of said vulnerabilities and their associated risks are discussed by the authors.

In general, the assessment presented in this paper enhances the comprehension of smart contract vulnerabilities through a methodical examination of their incidence and ramifications. The text offers significant perspectives to professionals in the blockchain security domain, including developers, auditors, and researchers. It emphasizes the criticality of secure coding practices and the necessity of comprehensive smart contract audits prior to deployment.

- RQ’s

1. Research Question 1: What are the prevalent categories of vulnerabilities that are typically identified in smart contracts that have been deployed on the Ethereum blockchain?
2. Research Question 2 pertains to the prevalence of various types of vulnerabilities observed in the analyzed smart contracts.
3. Research Question 3 pertains to the determination of the severity level of diverse smart contract vulnerabilities and their potential impact on the security of blockchain systems.
4. Research Question 4 pertains to the identification of patterns or trends in the incidence of vulnerabilities across various smart contracts.
5. Research Question 5 pertains to the correlation between the vulnerabilities detected during the assessment and their manifestation in practical scenarios of smart contract breaches.

- Result Presentation and Conclusion structure:

The findings of the investigation on vulnerabilities in smart contracts are presented in the results section of the paper. The initial step involves presenting a comprehensive summary of the dataset under scrutiny, encompassing the quantity and categories of intelligent contracts scrutinized. Subsequently, the segment proceeds to showcase the ascertained susceptibilities, classifying them according to their characteristics and ramifications. Every vulnerability is meticulously explicated, emphasizing its attributes, probable ramifications, and frequent incidence. The utilization of statistical analysis and metrics can aid in the quantification of various vulnerabilities' prevalence and severity. Visual aids such as charts, tables, and graphs can be utilized to effectively present data and enhance comprehension.

The concluding segment of the manuscript provides a concise overview of the primary outcomes and ramifications of the investigation. The initial step involves the reiteration of the research objectives and research questions that are tackled within the paper. Subsequently, the authors delve into a discussion of the primary findings derived from the outcomes, underscoring the importance of the detected weaknesses and their plausible ramifications on the security of blockchain systems and smart contracts. The conclusion section of the analysis report serves to underscore any discernible patterns, trends, or noteworthy observations that have been identified during the course of the analysis. Moreover, the paper may address the constraints of the research and potential avenues for future investigation. The conclusion serves as a concluding remark that underscores the significance of mitigating smart contract vulnerabilities and potentially offers guidance to developers, auditors, and policymakers in bolstering the security of smart contracts and encouraging the implementation of optimal procedures.

Paper 2:

> Ł. Mazurek, “EthVer: Formal Verification of Randomized Ethereum Smart Contracts,” in *Financial Cryptography and Data Security. FC 2021 International Workshops*, M. Bernhard, A. Bracciali, L. Gudgeon, T. Haines, A. Klages-Mundt, S. Matsuo, D. Perez, M. Sala, and S. Werner, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2021, pp. 364–380. doi: 10.1007/978-3-662-63958-0_30.

- Evaluation:

The subject matter at hand pertains to an assessment of automated verification techniques utilized in the context of smart contracts. The authors present a comprehensive survey of various methodologies, including static analysis, model checking, and theorem proving, and evaluate their respective strengths and weaknesses. Additionally, they assess the current level of advancement in the respective domain, emphasizing unresolved research obstacles and potential avenues for further investigation.

- RQ’s:

1. It pertains to identifying the obstacles encountered in the process of formally verifying randomized smart contracts.

   The present inquiry delves into the particular challenges that emerge in the process of formally verifying smart contracts that integrate stochastic elements.

2. It pertains to the approach taken by EthVer in tackling the obstacles encountered in the process of formal verification.

   The present inquiry examines the methodology and techniques utilized by EthVer in order to surmount the challenges that were identified in the first research question.

3. It pertains to the performance implications associated with the utilization of EthVer for the purpose of formal verification.

   The present inquiry scrutinizes the performance attributes of EthVer and evaluates its efficacy in verifying smart contracts that are randomized.

- Result Presentation and Conclusion structure:

The findings of the study are communicated via a comprehensive assessment of EthVer. The assessment encompasses empirical investigations carried out on a collection of practical smart contracts exhibiting stochastic behaviour. The evaluation of EthVer is conducted with regards to its verification duration, resource utilization, and capacity to handle larger workloads.

The concluding section of the manuscript provides a concise overview of the primary discoveries and contributions. The article examines the efficacy of EthVer in tackling the obstacles associated with formal verification of randomized smart contracts. The authors emphasize the advantages of utilizing formal verification techniques to improve the security and dependability of contracts. Additionally, they offer perspectives on potential avenues for further investigation in this domain.

Paper 3:

“Ethereum Smart Contract Development: An Empirical Study of Challenges and Solutions" by T. Rausch et al.”

- Evaluation:

The article titled "Ethereum Smart Contract Development: An Empirical Study of Challenges and Solutions" authored by T. Rausch and colleagues has been assessed through the utilization of an empirical research methodology. The researchers administered a survey and conducted interviews with a cohort of smart contract developers to gather empirical data regarding the obstacles they encounter and the remedies they employ in the process of creating smart contracts on the Ethereum blockchain.

The questionnaire inquired about various subjects such as the process of development, practices of testing, and considerations regarding security. The conducted interviews yielded supplementary perspectives and experiences from the developers. Subsequent to the collection of data, an analysis was conducted to ascertain prevalent themes and patterns pertaining to the obstacles and remedies associated with the development of Ethereum smart contracts.

The manuscript additionally encompasses an analysis of the consequences of the discoveries for forthcoming investigations and advancements. According to the authors, the study has the potential to provide valuable insights for enhancing the development tools, testing frameworks, and security mechanisms of smart contracts on the Ethereum platform. The paper presents a significant contribution to the comprehension of the pragmatic obstacles and remedies involved in the creation of smart contracts on Ethereum. It serves as a beneficial reference for scholars, programmers, and professionals operating within this domain.

- RQ’s

What are the obstacles encountered by developers of smart contracts utilizing the Ethereum platform? The authors have identified a number of challenges that are associated with programming languages, tooling, testing, and deployment. What are the approaches employed by developers to tackle these challenges? The authors have identified a variety of potential solutions, which encompass the utilization of libraries, frameworks, and developer communities, in addition to the implementation of best practices for testing and deployment. What are the potential ramifications of these findings with regards to future research and development? The authors propose that forthcoming investigations should prioritize enhancing tooling and developer education in order to tackle the identified challenges.

- Result Presentation and Conclusion structure:

The authors are expected to employ a methodical approach in presenting their outcomes, arranging their discoveries in a coherent and organized fashion. The utilization of subsections or headings to tackle distinct facets of the research could have facilitated readers in navigating through the diverse challenges and solutions scrutinized. Regarding data presentation, authors may utilize a variety of visual aids, including graphs, charts, and tables, to effectively present quantitative data and offer a succinct and easily comprehensible depiction of their results. Qualitative descriptions or case studies may be employed by individuals to communicate the intricate facets of the difficulties and resolutions encountered, which may include knowledge obtained from interviews, surveys, or examination of actual smart contracts.

It is probable that in the concluding segment, the authors furnish a thorough recapitulation of their research outcomes. The authors may choose to restate the primary obstacles identified in the research, emphasizing their importance and possible consequences for the advancement of Ethereum smart contract technology. Furthermore, the authors may suggest potential remedies or suggestions to tackle these obstacles, utilizing their empirical examination and perspectives. The researchers may engage in a discourse regarding the constraints of their study, recognizing plausible partialities or domains that require additional scrutiny. In addition, the concluding segment may comprise recommendations for forthcoming research avenues, highlighting uncharted facets or burgeoning patterns in the realm of Ethereum smart contract establishment.