Master thesis proposal: Hardening the root of trust of Europe - Fine grain EVM-level monitoring for blockchain threat detection

Student Vlad Constantinescu- 5216648

On 3 June 2021, the European Commission took a bold step toward revolutionizing digital identity by proposing a regulation to update the European digital identity framework. Central to this vision is the introduction of the European digital identity wallet—a cutting-edge solution building upon the foundations laid by the 2024 Regulation on European electronic identification and trust services (eIDAS). This legislative momentum paves the way for a robust, cross-border electronic trust layer across the European Union, where EBSI (the European Blockchain Services Infrastructure) serves as the root-of-trust architecture in each Member State.

EBSI's decentralized structure mitigates single-point-of-failure risks and ensures passport-grade security for critical transactions, empowering EU citizens through verifiable and tamper-resistant digital credentials. However, this trust framework hinges on vigilant, real-time monitoring to safeguard integrity and availability. Security Information and Event Management (SIEM) solutions are essential in detecting, analyzing, and responding to incidents. Yet traditional SIEM tools rarely delve into the low-level Ethereum Virtual Machine (EVM) behaviors—such as detailed gas consumption and smart contract execution traces—needed to uncover subtle vulnerabilities like gas miscalculation (e.g., GHSA-4456-w38r-m53x). This master thesis aims to strengthen the very core of Europe's emerging digital trust fabric by designing and integrating advanced SIEM tooling optimized for EBSI's Hyperledger Besu environment, ensuring that threats are promptly identified and the European trust layer remains secure and resilient.

Hyperledger Besu, a widely-used Ethereum client, also the root technology chosen by EBSI, shows restrictions in its out-of-the-box logging capabilities, providing only coarse-grained events and high-level metrics.

The lack of fine-grained, EVM-level logging limits the ability to detect subtle gas-related vulnerabilities, as current logging mechanisms fail to capture detailed gas flows, sub-call gas allocations, or integer overflow errors in real time. This oversight makes it difficult for SIEM systems to identify attacks that exploit these vulnerabilities.

Additionally, the absence of detailed execution traces delays obstructs analysis, preventing investigators from reconstructing the exact sequence of operations leading to an anomaly. Moreover, in networks with multiple validators, inconsistent or sparse logs obstruct the correlation of events and consensus anomalies, which are crucial for detecting coordinated or network-wide attacks.

These issues present a gap in the current state-of-the-art SIEM tooling for blockchain networks, where there is a need for a methodology that integrates granular EVM-level data into SIEM workflow.

Such methodology would provide continuous, detailed logs of EVM execution, including sub-call level and gas usage per opcode.

Additionally, it would enhance anomaly detection capabilities by correlating fine-grained gas metrics with higher-level network events, improving incident response capabilities and forensic investigations by allowing detailed analysis of malicious transactions or unexpected behavior.

This paper aims to address the identified gap by developing a novel methodology for granular EVM-level gas monitoring and logging in Hyperledger Besu.

By integrating deep EVM instrumentation with traditional SIEM tools (e.g., ELK stack), this research aims to demonstrate that more detailed EMV-level logging and analysis can lead to earlier detection of vulnerabilities, a reduction in false positives, and a stronger security posture for blockchain networks. The approach will be validated through controlled experiments, comparative analysis with existing solutions, and performance benchmarking under various network conditions and attack scenarios.

january 2025