Ethereum Custody@PostFinance

Secure Digital Asset Custody Service PoC

Students

Samuel Maissen

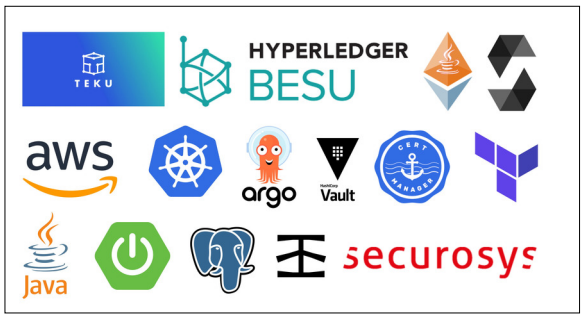
Mirio Eggmann

Introduction: In April 2023, PostFinance entered a partnership with Sygnum, a leading digital asset bank. This collaboration aims to offer regulated digital asset banking services to PostFinance customers through Sygnum's B2B platform. This initiative marks PostFinance's entry into the digital asset market, allowing customers to buy, store, and sell major cryptocurrencies like Bitcoin and Ethereum. Looking ahead, PostFinance aims to evaluate whether and in what ways it would be beneficial to internalize parts of such a solution in the future.

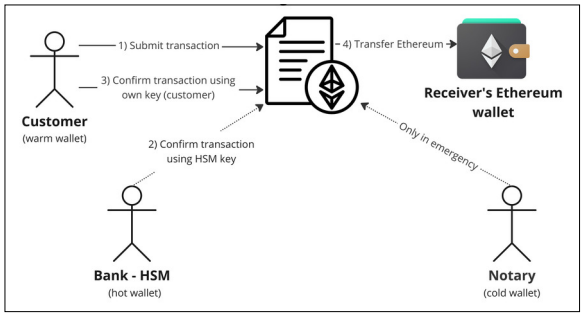
Definition of Task: In collaboration with PostFinance, this project explored the challenges of a self-managed custody solution for PostFinance's digital assets offering, focusing on Ethereum as a case study. The goal was to evaluate and build a secure custody setup in the form of a PoC, focusing on securely storing private keys, establishing a full node in the cloud, and building an application that provides a comprehensible API to create wallets, enable the buying and selling of Ethereum, and allow the execution of transactions.

Result: The PoC conducted as part of this project includes an application named Custodian, written in Java and using Spring Boot, which offers a RESTful HTTP API. This API enables the creation of secure single- and multisig wallets, processing buy and sell orders, and executing Ethereum mainnet and Sepolia testnet transactions with these wallets. The private key material is securely stored in an HSM from the Swiss-based company Securosys, specifically chosen for this project. Communication with the Ethereum network occurs through a self-operated full node setup, utilizing Besu as the execution client and Teku as the consensus client. To deploy our software components, a Kubernetes cluster was set up on an AWS EC2 instance using Terraform and MicroK8s. The build and deployment processes are managed through a combination of GitHub Actions for continuous integration with automated testing and ArgoCD for continuous deployment. Furthermore, the project includes an analysis of secure custody using multisig smart contracts, HSM technology, and a combination of hot, warm, and cold storage.

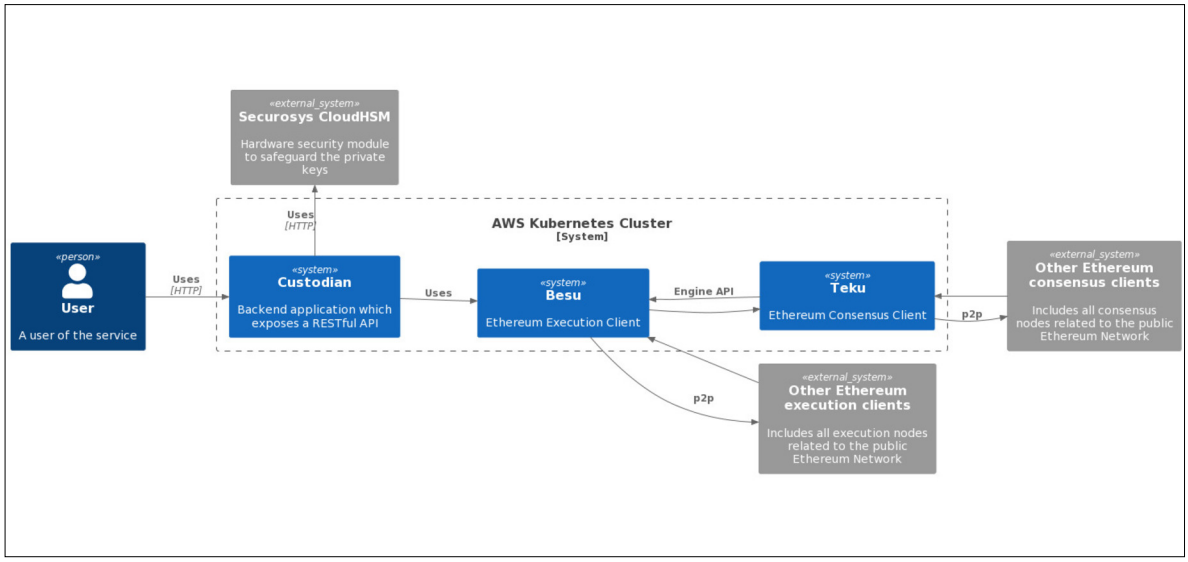
Techstack
Own presentment



Multisig Smart Contract
Own presentment



System Overview
Own presentment



Advisor
Dr. Thomas Bocek

Subject Area
Internet Technologies and Applications

Project Partner
PostFinance AG, Bern