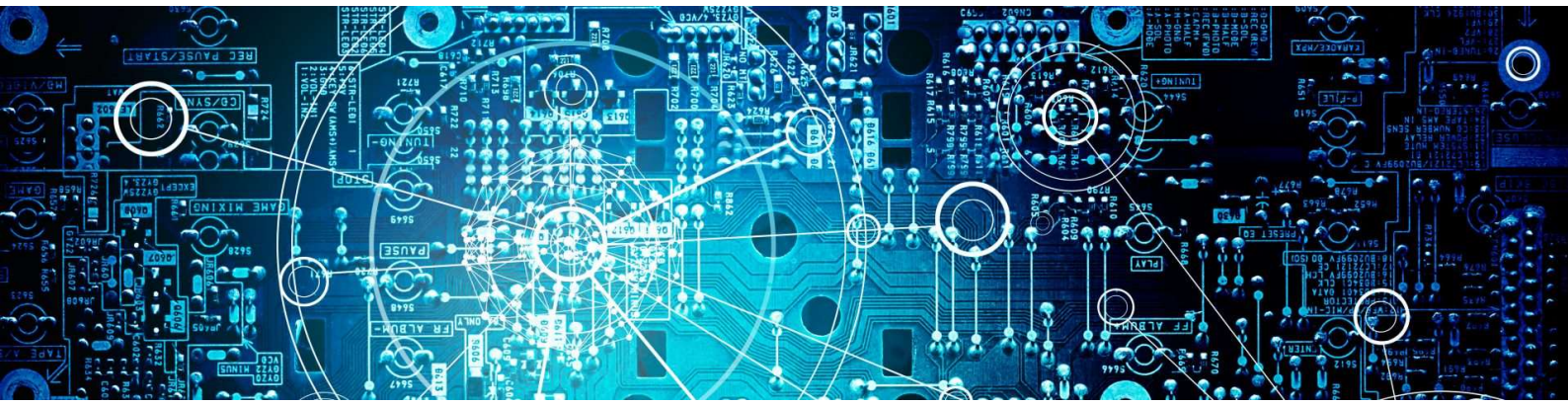
KUDELSKI SECURITY | RESEARCH

Kudelski Security Research

The Latest News from Research at Kudelski Security

HOME CATEGORIES



CODE ASSESSMENT OF THE CONCORDIUM BLOCKCHAIN

June 4, 2021 Nathan Hamiel blockchain Leave a comment

Concordium is a science-based proof-of-stake blockchain created with business applications in mind. It is the first blockchain with identification built into the protocol to meet

SEARCH

Sear

CATEGORIES

Select Ca

ARCHIVES

Select Mc

TWITTER @KUDELSK

regulatory requirements, while delivering a user-friendly platform that can handle smart contracts.

The Concordium Platform is designed to be fast, secure and cost-effective, which is why Concordium and Kudelski Security have been working together to perform threat modeling, code review, and "scenario based" assessment of the underlying code and logic of the Concordium software.

As documented in the White Paper, Concordium implements a Network Layer, Consensus Layer, and Identity Layer. These three layers interact with each other to process transactions and to execute the scalable/secure transactions.

1. From a logical perspective, the system is made up of several different well-defined components and layers.
2. The transactions are sent into a transaction layer and are distributed to all full nodes of the network
3. The consensus layer takes transactions from the transaction pool and "bakes" or proposes a block validating all the transactions within the block
4. The finalization of the blocks is performed by the finalization in the consensus layer
5. The baking layer and the finalization layer makes up the "Konsensus" consensus layer
6. All transactions blocks and votes are sent between the nodes via the peer to peer layer

At the beginning of the engagement, we first wanted to focus on the critical parts of the code which ensured that the foundation was solid, and that consensus and execution remained safe. We focused much of the security review on the following components and their interconnection.

- Haskell & Rust Code that make up the foundational components of the system
- Security effectiveness and correctness of the consensus layer

- Security effectiveness and correctness of the execution layer

During discussions with the core team, we quickly identified some key areas of overall concern

- Are there any scenarios in which the link between consensus and execution fails at unexpected points, or with security concerns?
- Are there any scenarios in which financial loss can incur within the systems including token manipulation or reassignment?

We ruled the following components out of scope for this first engagement

- Analysis of the functional virtual machines (VM), Smart Contracts, and Identity layers
- Haskell code under Acorn
- Deployment of the infrastructure or hardware at scale to validate findings
- Operational execution of the code to perform a pen test of running binaries (memory review, attacks to binaries, theft of secrets)
- Operational assessment of alerting and monitoring when non-ethical behavior is present in the system
- Participation in any running testnet environments.
- Detailed analysis of third-party libraries #included in the system

Following the review, we have come to these conclusions which we have presented to the project team as part of the report output

During the threat modeling exercise, we worked collaboratively with the Concordium team to identify the most important threats to the project. We used this information to guide the code review phase of the project.

During the code review, we found no critical or high-risk scenarios that put the tokens of the system at risk and we made a number of suggestions to improve overall documentation, code quality, and conformance to best practices.

Following the completed review, and during follow-on tests, scenarios were discovered in which unused network messages and test code could cause availability concerns on the network even though these errors would not cause a loss of funds. We completed a follow-on review, looking specifically at the network code and identified a few issues that the Concordium team fixed.

We look forward to continuing the effort with Concordium to bring trust into their ecosystem through diligent review of the critical components of their ecosystem

Related

The Poly Network Hack Explained
August 12, 2021
In "Hacking"

CODE ASSESSMENT OF PROTON CHAIN
March 2, 2021
In "blockchain"

Blockchain: where to start
February 6, 2018
In "Crypto"

AUDIT BLOCKCHAIN CONCORDIUM CRYPTO CRYPTOGRAPHY FEATURED IMAGE SMART CONTRACTS

« Taking the (quantum) leap with go

Intro: Understanding the oxygen protocol »

LEAVE A REPLY

Enter your comment here...