Emin Mahrt
Aeternity Establishment
Landstr. 123
FL-9495 Triesen

**Security Review Summary: Aeternity Blockchain**

| Version | Changes | Date |
|---|---|---|
| 0.1 | Initial Version | 2018-09-12 |
| 0.2 | Protocol recommendations | 2018-09-18 |
| 0.3 | Source code review, tests on node partially completed | 2018-10-24 |
| 0.4 | Further tests on node completed | 2018-11-13 |
| 0.5 | Review of cryptography code in base app | 2018-11-19 |

# 1 Management Summary

Aeternity is a project with the goal of creating a new blockchain. It aims to provide a number of features which are not available in existing popular blockchains like Bitcoin and Ethereum.

The development of the Aeternity protocol as well as the reference implementations for nodes and wallets have reached a pre-launch stage. Before the launch, Aeternity wants to perform a security review executed by independent security researchers. The scope of this security review includes the protocol design as well as the design and implementation of reference client software.

cnlab security ag (cnlab) is performing this security review. In order to cover the different aspects of the Aeternity blockchain, the review has been divided into several steps:

- Aeternity protocol design
- Node engineering and implementation (Epoch)
- Wallet engineering and implementation

At this point in time, the first step of the security review and most tests on the reference node (Epoch) have been concluded. Tests for the wallets are still ongoing.

## 1.1 Protocol Design

**We arrive at the conclusion that the overall protocol design of the Aeternity protocol provides a solid basis for a blockchain network.**

During our review, **we spotted a problem with the resolution of state channels**. We think that the issue can be addressed in a way that does not endanger the overall protocol.

Furthermore, we formulated a few recommendations in order to improve the network security even further.

Some of these recommendations are guidelines for the implementation of the protocol. They have to be followed during the development of both the reference node and third-party clients.

## 1.2 “Epoch” Node Reference Implementation

Most planned technical tests and a source code review have been concluded. No issues of “high” risk have been found. We found several issues of “medium” and “low” risk which are listed at the end of this report. A final conclusive statement will be provided after the pending tests on the node have been completed.

**We arrive at the conclusion that the reference implementation “Epoch” for an Aeternity node provides a good basis for the network.**

## 1.3 Wallet Implementation

During the security review, cnlab has audited the cryptography-related section of the source code in the base app. The base app is designed as an easy-to-use smartphone app, implemented in “progressive web app” technology. Note that this app is meant for managing small amounts of money for daily use. The project recommends more sophisticated solutions for the management of large assets.

During our review, we found and reported **a problem with the storage of wallet keys**. This issue has been fixed by Aeternity in the meantime.

We arrive at the conclusion that the fixed version of the base app provides adequate security for the purpose of an easy-to-use everyday wallet.

The details of our security assessment are documented in a full report in a separate document. This summary and the corresponding report will be extended and updated after conclusion of further review steps.