Abstract of Interchain Cosmos SDK Audit

Least Authority performed a security audit of the Cosmos Blockchain SDK, a framework written in Golang for building Proof of Stake state machines. The investigation and analysis were conducted by Gordon Hall and Ramakrishnan Muthukrishnan, along with project management support by Hind Abu-Amr, in collaboration with Tendermint team members Jessy Irwin, Zaki Manian, Christopher Goes, and Jack Zampolin.The audit took place from January 7 - 22, 2019 and the initial audit report was issued on January 23, 2018. A final report was produced on February 22, 2019 following discussions, recommended updates made to the Cosmos SDK by the Tendermint team, and final verification performed by Least Authority.

In order to facilitate high level review of the project and a more nuanced review of particular features, Least Authority and Tendermint approached this audit from a time-boxed perspective - allowing both team’s collaborative efforts, Tendermint’s development progress, and Least Authority’s investigative findings to guide the review. Least authority focused primarily on review of the BaseApp. In addition, the team closely investigated tooling for a chain initialization process, state and transactions documentation, the auth and bank module specification, the F1 Fee Distribution Module, and a review of Tombstone. The goal was to investigate these high priority areas of concern as directed by the Tendermint team and to discover more obvious issues, with the understanding that the time limit prevents a more comprehensive evaluation and elimination of reviewing areas such as the game theory aspects of the consensus algorithms.

Overall, Least Authority found the code base to be very well organized and did not appear to contain unnecessary, excess code. The clean and succinct coding style allows efficient and comprehensive code review, thus facilitating the contributions of others in finding potential vulnerabilities. The code follows ethereum best practices and avoids known bugs such as re-entrancy.

Furthermore, the staking module code is very readable and easy to follow, which is further enhanced by the specification that is explicitly well-defined. The code that implemented this specification is structured such that it is accessible and easy to comprehend. This is particularly important for future contributions and audits side by side to the code.

It was also discovered that tests exist for all major modules (some of them with 100% test coverage) that increase the level of confidence in the correctness of the code. Least Authority strongly suggest continuously striving for a 100% test coverage.

No security issues were identified throughout the duration of the review while one suggestion was made as it relates to random number generation as is documented in the "*Cosmos Blockchain SDK Framework Final Security Audit Report*", to which the Tendermint team has responded by implementing the suggested change.

Least Authority recommend that these exemplary practices are continued as the codebase is expanded in the future and that security audits continue to be a consistent part of the development lifecycle as changes and features are introduced to the codebase in order to optimize the security of the Cosmos SDK implementation.