KIR Proposal: Klaytn Bug Bounty Program

Date: *2021.06.22*

Summary

Security is the most important property of Klaytn and security issues can lead to direct financial losses as well as service failures. To maintain Klaytn security continuously, Klaytn needs a long-term security program such as a bug bounty program. The bug bounty program is a kind of proactive deal offering for White Hat hackers. The participants of the program report bugs or security flaws and are compensated for their reporting.
The goal of this project is to run a bug bounty program for the security of the Klaytn client. The Golang source code in the Klaytn GitHub repository is the main scope of the program, and Ground X will operate a test node for program participants. If a bug is reported and found positive, Ground X will mitigate the reported issue and send rewards to the reporter via the bug bounty platform. All positively reported vulnerabilities, mitigations, and reward history will be posted every two months in the form of a progress report. The project budget will be used for two purposes: 1) Registration and operation fee on a bug bounty platform 2) Reward for bug reporters. When the project is finished, the remaining budget will be refunded to the KIR fund or will be used to maintain the program longer if we get enough consent from the council.

Team (Individuals, Corporation) Introduction

Corporation
Ground X Corp. is the blockchain subsidiary of Korea's largest mobile platform, Kakao, with over 50 million monthly users. By developing a scalable blockchain platform with tangible and practical blockchain services, it aspires to achieve mass adoption of blockchain-empowered services as to substantiate the value and utility of blockchain technology. Ground X Corp. has been developing Klaytn, a global public blockchain providing user-friendly UX/UI and enterprise-friendly Developer Experience (DX) environment for developers to create blockchain services. Ground X Corp. also prioritizes its efforts on the development of other services and businesses including leveraging blockchain to drive social impact.

Individuals
For the campaign, Ground X Corp will arrange 5 people who will proceed with the project.

Name	Main Role	Details
Kyungup Kim	General Management	Manages the overall project
Donghwan Kwon	Communication	Communicates with a bounty platform

	Review & Development	Reviews bug reports and fixes bugs
Jeongkyun Oh	Review & Development	Reviews bug reports and fixes bugs
Yoomee Ko	Review & Development	Reviews bug reports and fixes bugs
Hyochan Kim	Review & Development	Reviews bug reports and fixes bugs

Motivation

Security is the most important property of Klaytn. All behaviors, including value transfer, execution of contracts, and transaction history retrieval, are performed with confidence in Klaytn node security. Security issues in Klaytn can lead to direct financial losses as well as service failures such as the financial system. However, software security is not achieved by a few security audits. It is impossible to find all vulnerabilities with a few security audits, and as hacking techniques advance, new vulnerabilities may be revealed. Besides, Klaytn's source code is constantly changing to develop new features. Therefore, Klaytn should have a long-term program for its security.

One of the popular ways to enhance the security of software is providing a bug bounty program. It is a kind of proactive deal offering for White Hat hackers. The program allows White Hat hackers or developers to discover bugs or security flaws. When participants of the program find a bug in the target software, they can submit a proof of concept along with their report. If their finding turns out to be positive, the organization of the program gives compensation. Bug bounty programs have been implemented by a large number of organizations, including Google, Facebook, Ethereum, and Hyperledger.

The bug bounty program has benefits compared to other security audit methods. First of all, anyone can participate to enhance the security of software. The program will provide an incentive for developers to spend their time understanding Klaytn and finding novel issues without time limit or methodology restriction as long as they don't violate the rules of the program. Further, it helps to deter malicious activities by legitimately rewarding them.

Project Description

The goal of this project is to run a bug bounty program for the security of Klaytn with the following details. For professional operation and fairness, we plan to register the bounty program to a bug bounty platform.

Bug Bounty Program Details

Scope

Followings are included in the scope.

- Golang source code in Klaytn Github repository (released version)
    - https://github.com/klaytn/klaytn/tree/master
- Essential smart contract code of Cypress network (Mainnet)
    - https://github.com/klaytn/klaytn/tree/master/contracts
- An endpoint node of the Baobab network
    - An endpoint will be publicly open only for this bug bounty program
- Caver SDK
    - caver-js, caver-java

Out of Scope

Followings are NOT included in the scope.

- Test code in Klaytn Github repository
- Smart contracts not included in the Klaytn Github repository
- All Klaytn nodes except for the Baobab endpoint node Ground X prepared for this bounty program
- web3 SDK

Categories of Vulnerabilities

The severity of reported vulnerabilities will be classified as follows. Although some vulnerabilities are classified in the same category, the severity can be classified differently depending on the impact, possibility, or requirements.

Category	**Severity (up to)**	**Notes**
Consensus Failure	Critical	- Consensus safety failure - Consensus liveness failure - Non-validator nodes affect to consensus process
Remote Code Execution	Critical	- Execute system functions of Klaytn nodes remotely
Unauthorized Value Transfer	Critical	- Transferring other account’s KLAY
Account Key Flaws	Critical - Medium	- Updating other account’s account keys - Using a role-based key in inappropriate ways for the role
Smart Contract	High	- Vulnerabilities in the reward related

Vulnerabilities		smart contracts
Sensitive Data Exposure	High - Medium	- Unauthorized attackers acquire or abuse a node key
P2P Protocol Bug	Medium	- DoS through Klaytn P2P protocol
Abusing Node APIs	Medium	- Using unauthorized node APIs - DoS through Klaytn node public APIs
Information Leak	Low	- Node key exposure in the node log - Acquiring CN's IP address

Rewards

The maximum reward according to the severity of reported bugs is as follows. The final reward amount can be changed by review. Bug reproducibility, test cases, and report quality can be reflected also.

Severity	**Rewards[1] (up to)**	**Details**
Critical	$50,000	- High impact to the entire network - Financial loss of random accounts
High	$20,000	- High impact to the entire network but possibility is not that high - High impact to the core cell network - Financial loss of a specific account
Medium	$10,000	- High impact to a specific node - High impact to the core cell network but very storing privileges required (e.g., CN/PN, ISP or node administrator can attack)
Low	$2,000	- High impact to a specific node but very storing privileges required (e.g., CN/PN, ISP or node administrator can attack) - Vulnerabilities that doesn't lead to attack directly
None	$500	- Reports that helped Klaytn development - correcting implementation flaws - improving code efficiency - Improving documentation and comments

[1] The same amount with Ethereum 2.0 bounty reward is set except for *None* grade

Rules

These are the rules to operate the program safely and fairly. All participants in the bounty program should keep the following rules.

- All employees of Ground X and Klaytn contributors receiving pay directly or indirectly from Ground X or Klaytn Pte. Ltd. can not receive a reward.
- If you disclose vulnerabilities without the consent of Ground X, you cannot claim a reward.
- Do not attack any Klaytn blockchain application or Klaytn related services.

Project Milestones and Schedule

Expected project completion time: 12 months

Date	**Task**	**Criteria**
start date + 2 months	- Launch Klaytn bounty program on a bug bounty platform	Milestone 1
start date + 4 months	- Review reported bugs and fix them - Submit a progress report #1	Milestone 2
start date + 6 months	- Consider another bounty program for Caver - Review reported bugs and fix them - Submit a progress report #2	Milestone 3
start date + 8 months	- Review reported bugs and fix them - Submit a progress report #3	Milestone 4
start date + 10 months	- Review reported bugs and fix them - Submit a progress report #4	Milestone 5
start date + 12 months	- Review reported bugs and fix them - Submit a final report	Milestone 6

Key Deliverables

The most important thing in this project is to run the bounty program fairly and transparently. For fairness and transparency, we will write progress reports and a final report publicizing the history of bounties. And, we will also provide a test environment to encourage more engagement in the bounty program.

1. Progress/Final Reports

    - *Summary of reported issues*: Statistics of all reports and a summary of all valid bug reports will be included.
    - *Status of vulnerabilities and fixes*: Status of bugs and source code update history to fix the bugs will be included.
    - *Reward details*: All reward distribution history will be written. The attestation of a bug bounty platform will be included also and we encourage the platform to make the reward history public on their platform.

2. Running a test node for the bounty program
    - A public Klaytn node of the Baobab network will be operated during the bounty program. Any white hackers can easily test using the public node.

Budget

We expect $450,000 for the total budget to operate the bug bounty program successfully for one year. However, the exact cost will be different from our expectations because the cost depends on the participant of hackers. Even though we have planned our budget claim every two months, **we will not claim the additional reward reserve for hackers if the reserve was not spent enough for the previous milestone. When the program is finished, the remaining budget will be refunded to the KIR fund or will be used to maintain the program longer if we get enough consent from the council.** We believe that the bug bounty program should go on.

Purpose

1. *Registration and operation fee on a bug bounty platform*
   We will add the Klaytn bug bounty program on a bug bounty platform run by a cybersecurity company such as HackerOne[2] or Theori[3]. The company will connect the Klaytn bounty program with penetration testers and cybersecurity researchers. It also provides additional management plans for receiving bug reports, pre-reviewing the validity of reports, and distributing rewards. The registration fee including additional plans for one year needs to be paid at the beginning of the bounty program.

2. *Reward reserve for bug reporters*
   Instead of Ground X, the bounty platform rewards hackers who report positive vulnerabilities. To reward quickly and fairly, we will reserve enough rewards for the platform in advance.

[2] One of the largest bug bounty platforms. https://www.hackerone.com/
[3] Cypersecurity R&D company which did source code auditing and penetration testing for Klyatn. https://theori.io/

Expected Klay Funding Plan

Expected Date	Purpose	Budget
start date	Registration and operation fee on a bug bounty platform	$100,000[4]
	Reward reserve for hackers #1	$100,000[5]
start date + 2 months	Reward reserve for hackers #2	$50,000
start date + 4 months	Reward reserve for hackers #3	$50,000
start date + 6 months	Reward reserve for hackers #4	$50,000
start date + 8 months	Reward reserve for hackers #5	$50,000
start date + 10 months	Reward reserve for hackers #6	$50,000
Total		**$450,000**

Attachments

This field is left blank.

Feedback

This field is left blank.

[4] The price is the maximum price for the bounty program registration and operation. The exact price can be changed depending on the bounty platform and plans. The rest of the money will be used for the reward reserve for hackers.

[5] The price was calculated assuming the following number of vulnerability reports: 1 Critical ($5,000) + 1 High ($2,000) + 2 Medium ($1,000 * 2) + 5 Low ($200 * 5)