Hello,

Thank you for your interest in ChainSecurity. Here is more information on us, our services, and our process for code assessments.

Our background:

We are www.ChainSecurity.com, an ETH Zurich spin-off founded by academic researchers in 2017. We joined PwC Switzerland in 2020 and spun off in April 2021. This was the rebirth of ChainSecurity. Leading blockchain security engineers and seasoned executives from PwC make up a world-class team who brings quality, reliability, and experience.

Our team has an extensive track record in code assessments across various networks. Most work was done with Ethereum-based projects and we are one of the top contributors to the security of the Ethereum network. (https://bounty.ethereum.org #3 Chainsecurity, #16 Dominic Brütsch)

If you want to know how our reports look, feel free to check out one of our reports on https://chainsecurity.com/security-audit/maker-protocol-liquidations-2-0/

Our services:

We perform technical audits of:

- New blockchains and DLTs, as well as updates (for example, our team was the one that identified the vulnerability in Ethereum's Constantinople update https://medium.com/chainsecurity/constantinople-enables-new-reentrancy-attack-ace4088297d9
- Smart contracts, dApps, DAOs, and all blockchain-related applications and systems

We audit distributed systems for:

- Security
- Correctness (Does the system perform the desired functions?
- Design (Is the system as efficient as it can be?)

We offer architecture recommendations to corporations and governments looking to develop distributed systems and:

- Avoid costly design mistakes,
- Foster security,
- Improve scalability.

Our code assessments work flow:

1. First, you will get a rough idea of the audit cost and the potential slot you might get. For this, could you please inform Emilie of the (approximate) numbers of line of code you want to have audited?

2. If this initial estimate sounds good to you, we will provide a precise estimate of time and cost. For this, we will need to look at your code. It doesn't need to be completely final at this point, as you will have a chance to submit an updated version before the audit. Just let us know how close you think you are to the final version. All documentation is welcome.
There are two methods to share your code with us, either:

- Share with our GitHub or GitLab account (preferred method)
  - audits@ChainSecurity.com (@ChainSecurityAudits)
- Send a zip via email.

2a. We keep all data confidential, with or without NDA, as you would expect from a professional service firm. However, if you wish to have an NDA in place before sending your code, please send us the information below and we will send you our standard NDA.

- The full name and address of your company,
- The full name and function of the company representative who will sign the NDA.

3. Based on the provided code, we will send you a proposal with a price and timeline estimate. If the terms of the proposal look fine for you, we will start your onboarding process, which includes risk assessment and KYC. We would need the legal information of your company and responsible executives and will provide you with a questionnaire to streamline the process.

4. While the onboarding process is ongoing, we will formalize the terms of the proposal in an Engagement Letter, which will include a detailed timeline.

5. On your "code freeze" date, you will share with us the final version of your code, along with the required documentation and specifications. We will start the audit.

6. At the end of the first phase of the audit, you will receive an intermediate report with our findings.

7. You will have time to fix issues and reply to the findings.

8. We will review the fixes and send the final report.

I'd be happy to jump on a call to continue the conversation. Feel free to reach out to emilie.raffo@chainsecurity.com, or on Telegram **@EmilieRaffo**