MEMO

Confusion Capital Grant Program

From: LexDAO & friends @MetaCamp Costa Rica
To: Confusion Capital
Date: June 06, 2024

re: SSL+ front-end standardization and safe harbor for SSL+ platforms

Problems

There is a need to regulate websites that use the client-server dynamic to offer the front-end interface for decentralized finance. Unlike the back-end of decentralized finance, the front-end is not audited. Because the decentralized finance back-end is trustless but the front-end interface still requires the client to trust the server, the security can be bypassed by a malicious front-end.

There are myriad examples of when incompetent or bad actor servers have abused this trust, as identity theft or to commit cryptofraud. Indeed, this front-end trust layer affects traditional finance websites as well. These types of attacks require very little skill to execute, and are very hard for non-technical users to detect.

The Confusion Capital community has already prioritized consumer protection for front-end interfaces.

Abstract

DNS is a highly centralized solution and if regulators aim to control it, as is currently being entertained, we will quickly see distributed solutions proliferate to shift liability from the projects onto the platforms. For instance, limo[1] or iNFTs[2] are existing workarounds.

To anticipate this proliferation, we propose establishing a working group that can build safe harbor initiatives, so that platforms such as limo and OpenSea can self-regulate (absolve from liability). As DMCA successes show with YouTube and OpenSea, it is important that we continue to ensures safe environments for consumers to interact with platforms.

1 https://eth.limo/
2 https://ape.mirror.xyz/FjUVEcUrDmQISEmcVarGEDHt6mLK9VOjLbxXgFy4edE

By having platforms involved, we have an opportunity to extend consumer protection beyond what SSL offers, especially for users of DeFi applications, due to their rapid development, often unknown sources of deployment, and so on.

We propose the establishment of an "**SSL+**" standard that extends the security of SSL, by adding hashed verification of code. Platforms can leverage the SSL+ standard to ensure serving of regulated front-ends. Through the SSL+ standard, regulators can provide clear and safe guidance for platforms to adhere, using a strategy of self-regulation. Consumers then have the confidence to enjoy the decentralized web in peeeeeeace.

Implementation Strategy

Phase 1 (This Phase): Develop ERC standard + Establish Safe Harbor Methodology & Language
Phase 2: Establish Regulated Platform of Verified Front-ends
Phase 3: SSL+ standard mark legitimatized and active

Phase 1 Detail

* finalize research and discussion among peers in the domain of decentralized security to validate the standardization model
* publish an article for the Journal of Legal Engineering that clearly explains what SSL+ is, how it can drastically improve front-end security (public good)
* develop an Ethereum Request for Comment "ERC" for a minimum-opinion necessary iNFT standard, as an ‘addendum’ to the minimum-opinion necessary ERC-721 NFT standard (public good)
* develop recommendations for an SSL+ safe-harbor system appropriate for NFT platforms (public good)
    * ensure NFT platforms do not incur client-server decentralized finance front-end regulation liability
    * ensure consumer protection for client-RPC decentralized finance front-ends

Ask

Book a call to discuss this memo at https://calend.ly/lexgrants .

Use of Funds

* fund core contribution
    * research and writing
    * project management
    * development
    * retrospective upon completion of phase 1
* fund emergent development needs