Lens Protocol 1.0

Jefferson Ding
Student
FranklinDAO, University of Penn.
Philadelphia, USA
tyding@seas.upenn.edu

Rohin Arya
Student
University of Western Ontario
London, Canada
rarya4@uwo.ca

***Abstract*—This whitepaper introduces a decentralized credit and lending bureau designed to bridge traditional Web2.0 credit systems with the evolving Web3.0 landscape. Our solution integrates trusted credit reports from conventional sources with comprehensive analysis of on-chain transactions to offer a transparent, real-time, and inclusive approach to consumer credit evaluation. Leveraging Rootstock's EVM-compatible sidechain on Bitcoin, we employ smart contracts to manage and score credit data, ensuring data integrity and transparency through blockchain technology. Our innovative approach not only enhances the accuracy of credit scores by incorporating Web3.0 behavioral insights but also opens up financial opportunities for underserved populations. By combining the strengths of traditional and decentralized finance, our platform aims to create a more efficient, transparent, and equitable credit ecosystem.**

I. Introduction

In today's financial landscape, credit reporting and lending are crucial components for economic growth and consumer empowerment. However, traditional credit systems lack transparency and often fail to consider the evolving dynamics of Web3.0. Our project aims to build a decentralized credit and lending bureau that bridges the gap between Web2.0 and Web3.0 credit systems, creating an innovative, instant, and transparent solution for consumer credit evaluation.

The Lens Protocol sets out to revolutionize credit reporting and lending by integrating trusted Web2.0 credit data on chain with comprehensive Web3.0 transaction analysis, ensuring transparency, accuracy, and inclusiveness in credit scoring.

II. Features

Trusted Credit Reports: Accepts and verifies credit reports from traditional, trusted parties. Integrates existing Web2.0 credit data to establish a baseline credit score.

Web3.0 Transaction Aggregation: Collects and analyzes on-chain transactions from various blockchain networks. Utilizes smart contracts to automate data aggregation and credit scoring.

Transparent Consumer Credit: Implements a decentralized ledger to record and maintain transparent credit histories. Ensures data integrity and immutability through blockchain technology.

Instant Credit Evaluation: Provides real-time credit score updates based on the latest transaction data. Enables instant credit decisions for lenders and consumers.

Consumer Behavior Analysis: Analyzes consumer behavior through Web3.0 interactions, such as DeFi activities, NFT transactions, and other blockchain-based engagements. Enhances credit scoring models with behavioral insights from decentralized finance ecosystems.

III. Technical Architecture

The technical architecture of our platform is robust and scalable. We utilize Rootstock's EVM-compatible sidechain on Bitcoin to ensure security and scalability. Smart contracts, written in Solidity, manage the credit data and scoring algorithms, automating the entire process and ensuring efficiency.

For the consumer-facing application, we have chosen React Native. This allows us to build a seamless and user-friendly app that can be accessed on both iOS and Android devices, ensuring wide accessibility and a consistent user experience.

Our data aggregation layer integrates with various blockchain networks to gather transaction data. Decentralized oracles are used to fetch off-chain credit reports and on-chain data, ensuring comprehensive and accurate data collection. The credit scoring algorithms combine traditional credit scoring models with machine learning techniques to analyze Web3.0 data, continuously improving scoring accuracy by incorporating new data points and trends.

IV. The Lenscrypt 2.0 Protocol

The illustrated protocol demonstrates a secure data access system using a combination of symmetric and asymmetric encryption methods to ensure confidentiality and integrity of user scores and reports.

Components

- **Vendor Module:**
  - Utilizes a Universal Vendor Key (UVK) to encrypt and decrypt vendor-specific data.
  - Generates an Encrypted Vendor Score Access Token (EV-SAT) using symmetric encryption (AES).

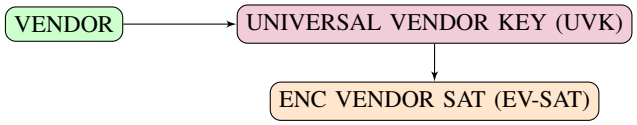

Fig. 1. Vendor and User Keys

- **Lenscrypt Metadata On Chain:**

– Manages metadata using both symmetric (AES) and asymmetric (RSA) encryption.
– The metadata includes encrypted tokens (EV-SAT and EU-SAT) to control access.

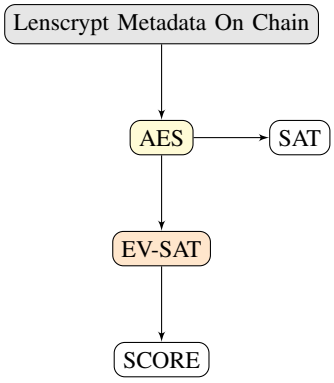

Fig. 2. Lenscrypt Metadata On Chain

- **User Data Module (UDM):**
  – Stores user scores and reports.
  – Scores are encrypted using a Score Access Token (SAT) and AES.
  – Reports are encrypted with the User Public Key (UPK) and AES.

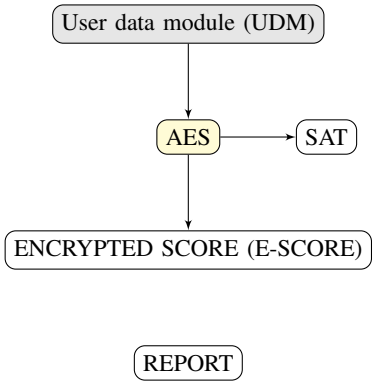

Fig. 3. User Data Module (UDM)

- **User Module:**
  – Uses public/private key pairs (UPK/USK) for encryption and decryption of user-specific data.
  – Generates an Encrypted User Score Access Token (EU-SAT) for secure score access.

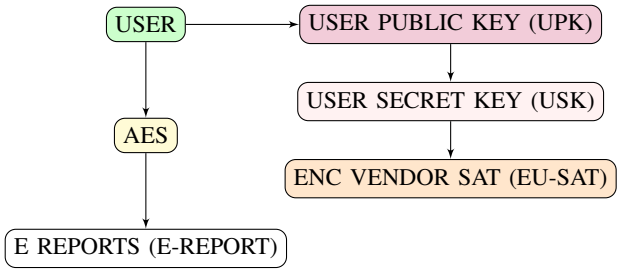

Fig. 4. User Elements

Access Control

- **Vendors Accessing Scores:**
  – Vendors decrypt the EV-SAT using UVK.
  – Access the encrypted score (E-SCORE) using SAT and AES.
- **Users Accessing Scores:**
  – Users decrypt the EU-SAT using USK.
  – Access the encrypted score (E-SCORE) using SAT and AES.
- **Users Accessing Reports:**
  – Users decrypt the encrypted report (E-REPORT) using UPK and AES.

Security Mechanisms

- **Symmetric Encryption (AES):** Ensures data confidentiality with a shared key for encrypting and decrypting user scores and reports.
- **Asymmetric Encryption (RSA):** Utilized for securely exchanging tokens and keys between vendors and users.
- **Access Tokens (SAT, EV-SAT, EU-SAT):** Provide granular control over who can access specific data, enhancing security.

This protocol ensures that both vendors and users can securely access and manage sensitive data while maintaining high levels of security through robust encryption techniques.

V. Benefits and Conclusion

The benefits of our decentralized credit and lending bureau are multifaceted. Transparency is a major advantage, as it ensures that all credit data and scoring processes are visible and verifiable on the blockchain. This significantly reduces the risk of fraud and data manipulation, fostering greater trust among all stakeholders.

Inclusiveness is another key benefit. Our platform enables underserved and unbanked populations to build credit through Web3.0 activities. By considering both traditional and blockchain-based financial behaviors, we provide a comprehensive credit evaluation that democratizes access to credit.

Efficiency is also greatly enhanced. By streamlining credit evaluation processes, we reduce time and costs for lenders and consumers. This facilitates faster credit decisions and improved access to financial services, benefiting all parties involved.