

The PEACE Protocol¹

A protocol for transferable encryption rights.

Logical Mechanism LLC²

October 25, 2025

¹This project was funded in Fund 14 of Project Catalyst.

²Contact: support@logicalmechanism.io

Contents

1	Abstract	1
2	Introduction	1
3	Background And Preliminaries	2
4	Cryptographic Primitives Overview	2
4.1	ECIES	2
4.2	AES-GCM	2
4.3	Proxy Re-Encryption	2
5	Protocol Overview	2
5.1	Design Goals And Requirements	2
5.2	On-Chain And Off-Chain Architecture	2
5.3	Key Management And Identity	2
5.4	Protocol Specification	2
6	Security Model	2
6.1	Trust Model	2
7	Threat Analysis	2
7.1	Metadata Leakage	2
8	Limitations And Risks	2
8.1	Performance And On-Chain Cost	2
9	Conclusion	2
	Bibliography	2

1 Abstract

In this report, we introduce the PEACE protocol, an ECIES-based, multi-hop, bidirectional proxy re-encryption scheme for Cardano. PEACE solves the encrypted-NFT problem by providing a decentralized, open-source protocol for transferable encryption rights, enabling creators, collectors, and developers to manage encrypted NFTs without relying on centralized decryption services. This work fills a significant gap in secure, private access to NFTs on Cardano. The PEACE protocol was funded in round 14 of Project Catalyst¹.

2 Introduction

The encrypted NFT problem is one of the most significant issues with current NFT standards on Cardano. Either the data is not encrypted, available to everyone who views the nft, or the data encryption requires some form of centralization, some company doing the encryption on behalf of users. Current solutions [1] claim to offer decentralized encrypted assets (DEA), but lack a publicly available, verifiable cryptographic protocol or an open-source implementation. Most, if not all, of the mechanics behind current DEA solutions remain undisclosed. This report aims to fill that knowledge gap by providing an open-source implementation of a decentralized encryption protocol for encrypted assets on Cardano.

The encryption protocol must allow tradability of both the NFT itself and the right to decrypt the NFT data, implying that the solution must involve smart contracts and a form of encryption that allows data to be re-encrypted for another user without revealing the encrypted content in the process. The bright contract side of the protocol should be reasonably straightforward. It needs a way to price a token to hold the encrypted data and allow other users to receive it. To ensure tradability, the tokens may need to be soulbound. On the other side of the protocol is the encryption required to make this all work. Luckily, this type of encryption has been in cryptography research for quite some time [2] [3] [4]. There are even patented cloud-based solutions already in existence [5]. There is no open-source, fully on-chain, decentralized encryption protocol for encrypting NFT data on Cardano. The PEACE protocol aims to solve this problem.

The solution the PEACE protocol will implement is an ambitious yet well-defined bidirectional multi-hop proxy re-encryption scheme that uses ECIES [6] and AES [7]. Bidirectionality means that Alice may re-encrypt for Bob, and sequentially Bob may re-encrypt back to Alice. Bidirectionality is important for tradability, as there should be no restriction on who can purchase the NFT. Multi-hop means that the flow of encrypted data from Alice to Bob to Carol, and so on, does not end, in the sense that it cannot be re-encrypted for a new user. Multi-hopping is important for tradability, as a single tradable asset does not fit many use cases. An asset should always be tradable if the user wants to trade it. The encryption mechanisms used in the protocol are considered industry standards at the time of this report.

The remainder of this report is as follows. Section 4 discusses the preliminaries and background required for this project. Section 5 will be a brief overview of the required cryptographic primitives. Section 6 will be a detailed description of the protocol. Sections 7, 8, and 9 will dive into the security and threat analysis, and limitations of the protocol, respectively. The goal of this report will be to serve as a go-to reference and description of the PEACE protocol.

¹<https://projectcatalyst.io/funds/14/cardano-use-cases-concepts/decentralized-on-chain-data-encryption>

3 Background And Preliminaries

4 Cryptographic Primitives Overview

4.1 ECIES

4.2 AES-GCM

4.3 Proxy Re-Encryption

5 Protocol Overview

5.1 Design Goals And Requirements

5.2 On-Chain And Off-Chain Architecture

5.3 Key Management And Identity

5.4 Protocol Specification

6 Security Model

6.1 Trust Model

6.1.1 Assumptions

7 Threat Analysis

7.1 Metadata Leakage

8 Limitations And Risks

8.1 Performance And On-Chain Cost

9 Conclusion

Bibliography

- [1] J. Stone, “Stuff.io whitepaper 1.0.” Accessed: Oct. 25, 2025. [Online]. Available: <https://book-io.medium.com/stuff-io-whitepaper-1-0-9529db7cdeaf>
- [2] M. Mambo and E. Okamoto, “Proxy cryptosystems: Delegation of the power to decrypt ciphertexts,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E80–A, no. 1, pp. 54–63, 1997, Available: https://search.ieice.org/bin/summary.php?id=e80-a_1_54
- [3] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in *EUROCRYPT 1998*, Springer, 1998. doi: [10.1007/BFb0054122](https://doi.org/10.1007/BFb0054122).
- [4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in *NDSS 2005*, 2005. Available: <https://www.ndss-symposium.org/ndss2005/improved-proxy-re-encryption-schemes-applications-secure-distributed-storage/>

-
- [5] IronCore Labs, *Recrypt (rust): Transform/proxy re-encryption library*. Accessed: Oct. 25, 2025. [Online]. Available: <https://github.com/IronCoreLabs/recrypt-rs>
 - [6] *IEEE standard specifications for public-key cryptography—amendment 1: Additional techniques*. IEEE, 2004.
 - [7] *Advanced encryption standard (AES)*. NIST, 2001.