海洋協議1.0版
技術白皮書

Ocean1.0 TORN
隱私交易技術解決方案

目录
contents

1、简介
Introduction

海洋協議Ocean1.0實現了零知識隱私解決方案：一種智能合約，該合約接受海啸站中的交易（以後也將以EVM代幣形式），以便以後可以在不參考原始交易的情況下提取該金額。

2、協議說明
Explanation

●該協議具有以下功能:
將數字資產（TORN標準）存入智能合約。這可以在固定金額（以N表示）的單筆交易完成。 N 鈔票被稱為硬幣。
●可以通過兩種方式從智能合約中轉移/提取資金:
-通過中繼器提取N，同時將f醚作為費用發送到中繼器地址t和（N f）到指定接收者。 f和t的值由發送方選擇。 在這種情況下，提款交易由中繼員發起，並支付應該由f支付的汽油費。
●-將N 提取給指定的接收者，交易由接收者發起。 接收者應有足夠波場幣支付交易的汽油費。 這種情況下，費用f被認為等於0。

2. 1安裝

●令B = 0，1。令e為SNARK證明中使用的配對運算，它是在素數q的組上定義的。
●令H1：B * Zp為[Ped]中定義的Pedersen哈希函數。令H2：（Zp，Zp）Zp為MiMC哈希函數[AGR + 16]定義為海綿操作模式下Feistel模式下的MiMC排列。
●設一個高度為20的Merkle樹，其中每個非葉子節點用H2對其2個子節點進行哈希處理。初始化時所有葉子均為0值。後來，零值逐漸被Zp中的其他值替換。設O（l）為樹中索引為l（從葉子l到根的路徑上的姊妹節點的值，用R表示）的葉子的Merkle開口。讓我們稱k B248為零，r B248為隨機性。讓我們表示海啸地址
A的硬幣接收者。
●令S [R，h，A，f，t]為具有公共價值R，h，A，f，t的知識陳述：
S [R，h，A，f，t] = {I KNOW k，r∈B248，l∈B16，O∈Z16這樣h = H1（k）
AND O是位置R處H2（k || r）到R}（1）的開口
其中A和f包含在語句的上下文中。在這裏，h稱為無效散列，是位串的串聯。

●令D =（dp，du）是使用某些受信任的設置過程創建的S的ZK-SNARK [Gro16]驗證密鑰對。設Prove（dp，T，k，r，l，A，f，t）→P為使用dp的證明構造函數，並以Verify（du，P，R，h，A，f，t）為證明驗證者。

●令C為具有以下功能的智能合約：

它將最後的n = 100個根值存儲在歷史記錄數組中。對於最新的Merkle樹，它還存儲從最後添加的葉到根的路徑上的節點值，這些值是計算下一個根所必需的。

●它接受帶有數據C Zp的N TON的付款。將值C添加到Merkle樹中，重新計算從上一個添加的值到最新根的路徑。先前的根將添加到歷史記錄數組。

●根據提交的公共價值（R，h，A，f，t）驗證所謂的證據P。如果驗證成功，則合同釋放（N-f）ETH到地址A，並向中繼器地址t收費f TON。

●通過檢查之前沒有出現過來自證明的無效散列來驗證硬幣是否沒有被提取過，如果是，則將其添加到無效散列列表中。

2. 2存幣

要存入硬幣，用戶進行如下操作：

2.2.1.生成兩個亂數k，r∈B248並計算

C = H1（k || r）

2.2.2發送帶有N TON的海啸交易，以與數據C簽約，後者被解釋為無符號的256位整數。 如果樹未滿，則合同接受交易並將C添加到樹中作為新的非零葉。

2. 3提幣

要提取樹中位置為l的硬幣（k，r），用戶需要進行以下操作：

2.3.1.選擇收信人地址A，費用值f≤N;

2.3.2.從合同中存儲的根中選擇一個根R，然後計算以R結尾的開放度O（l）。

2.3.3.計算無效哈希h = H1（k）。

2.3.4.通過在dp上調用Prove來計算證明P。

2.3.5.通過以下方式之一進行提款：

●發送波場交易到合約C，在交易數據中提供R，h，A，f，t，P。

●向中繼器發送請求，以提供事務數據R，h，A，f，t，P。 然後，應該假設中繼器與提供的數據進行交易以將合同C合同化。

●合同驗證了無效散列的證明和唯一性。 在成功的情況下，它將（N f）發送給A，將f發送給中繼器t，並將h添加到無效散列表中。

3、實現
Implementation

●用於鏈外使用的加密功能在circomlib庫中實現。 開發Merkle樹,存入和提取邏輯的可靠性是作者的觀點。 MiMC的可靠性實現是由iden3實現的。

●SNARK密鑰對和可靠性驗證碼由開發者使用SnarkJS生成。其他協議邏輯（如波場交易組成，SNARK證明構造調用）由開發者編寫.

4、安全聲明
Safetystatement

●海洋協議Ocean1.0擁有以下安全屬性：
・只能提取存入合同的硬幣；
・不能兩次提取硬幣；
●如果知道其參數（k，r），則任何硬幣都可以提取一次，除非具有相同k的硬幣已被存入並撤回。
●如果k或r未知，則無法提取硬幣。如果攻擊者不知道k，他將無法阻止知道（k，r）的人提取硬幣（這包括所有在前進行交易的情況）。
證明具有約束力：不能將同一證明與不同的無效哈希，另一個收件人地址或新的費用金額一起使用。
●海洋協議Ocean1.0使用的密碼原語至少具有126位安全性（BN254曲線除外，離散對數問題具有類似100位安全性的BN254曲線），並且安全性不會因其組成而降低。
●對於每筆提款，自從合同具有波場幣的最後一刻起直到證明中的根部形成為止的每筆存款都可能是潛在的硬幣，儘管根據用戶的行為，某些硬幣更可能被提款。

參考技術文檔：

★[AGR + 16] Martin R. Albrecht，Lorenzo Grassi，Christian Rechberger等。 “ MiMC：有效的加密和具有最小乘法複雜性的密碼散列”。於：ASIACRYPT（1）。 卷 10031.電腦科學講義。2016年，第191-219頁（引用於第1頁）。
★[Gro16]詹斯・格羅斯（Jens Groth）。 “關於基於配對的非互動式參數的大小”。 於：EUROCRYPT 2016。 9666. LNCS。 Springer，2016年，第305-326頁（引自第2頁）。
★[Ped]Iden3PedersenHash。 https://iden3-docs.readthedocs.io/en/latest/iden3_repos/search/publications/zkproof-standards-workshop-2/pedersen-hash / pedersen。 html。

海洋協議

Ocean1.0 TORN
隱私交易技術解決方案