ZELDHASH 協議

尋找比特幣最稀有的交易並賺取 **ZELD**。

作者：Ouziel Slama

1 動機

- 為了追尋的刺激。每筆交易都成為發現稀有事物的機會——隱藏在區塊鏈上的數位寶藏。
- 這些前導零模式不僅稀有——它們還可能增強壓縮效果，有可能簡化區塊鏈儲存和處理效率。
- 任何人都可以透過尋找稀有交易來賺取 ZELD——不像比特幣區塊挖礦那樣每個區塊只有一個贏家。尋找對所有人開放。
- 如果成功，ZELD 代幣最終可以報銷交易費用——獎勵那些發現最稀有交易的尋找者！

2 ZELD 挖礦

要挖掘 ZELD，您必須廣播一筆 txid 以至少 6 個零開頭的比特幣交易。獎勵根據您的交易與區塊中最佳交易的比較來計算：

- 在給定區塊中，以最多零開頭的交易可獲得 4096 ZELD
- 比最佳交易少一個零的交易可獲得 4096/16 或 256 ZELD
- 比最佳交易少兩個零的交易可獲得 4096 / 16 / 16 或 16 ZELD
- 以此類推。

因此使用的公式如下：

```
reward = 4096 / 16 ^ (max_zero_count - zero_count)
```

其中 `max_zero_count` 等於最佳交易開頭的零的數量，`zero_count` 是我們計算獎勵的交易開頭的零的數量。

注意： Coinbase 交易不符合 ZELD 獎勵資格。

3 ZELD 分配

以 6 個或更多零開頭的交易所賺取的 ZELD 將分配給 UTXO。分配方式如下：

- 如果只有一個非 OP_RETURN UTXO，它將獲得全部獎勵。
- 如果有兩個或更多非 OP_RETURN UTXO，獎勵將按每個 UTXO 的價值比例分配給除最後一個以外的所有 UTXO
- 由於計算僅使用整數，除法的可能餘數將分配給第一個非 OP_RETURN UTXO。

例如，如果一筆獲得 256 ZELD 的交易包含 4 個輸出，分別為 500、500、500 和 2000 聰，第一個輸出獲得 86 ZELD 獎勵，第二個和第三個各獲得 85 ZELD。

4 轉移 ZELD

當帶有 ZELD 的 UTXO 被花費時，ZELD 將分配給交易中的新 UTXO。轉移 ZELD 時有兩種分配方法：

4.1 方法 1：自動按比例分配

預設情況下，分配方式與獎勵完全相同——根據輸出 UTXO 的比特幣價值按比例分配，如果有多個輸出則排除最後一個輸出。

4.2 方法 2：透過 OP_RETURN 自訂分配

您可以透過在交易中包含帶有自訂分配資料的 OP_RETURN 輸出來精確指定 ZELD 應該如何分配。這允許對 ZELD 轉移進行精確控制。

4.2.1 OP_RETURN 格式：

- OP_RETURN 腳本必須包含以 4 位元組前綴 “ZELD” 開頭的資料
- 在前綴之後，資料必須以 CBOR 格式編碼
- CBOR 資料應表示無符號 64 位元整數向量（Vec）
- 每個整數指定要傳送到相應輸出 UTXO 的 ZELD 數量

4.2.2 分配規則：

- 分配陣列中的值的數量會自動調整以匹配非 OP_RETURN 輸出的數量
- 如果陣列太長，多餘的值將被刪除
- 如果陣列太短，將追加零
- 分配值的總和不能超過正在花費的 ZELD 總量
- 如果總和小於總量，差額將新增到第一個輸出
- 如果總和超過總量，交易將回退到按比例分配
- 新挖掘的 ZELD 獎勵始終按比例分配，然後與自訂分配合併

4.2.3 範例：

如果您有 1000 ZELD 要分配給 3 個輸出，並希望向第一個傳送 600，向第二個傳送 300，向第三個傳送 100，您的 OP_RETURN 將包含 “ZELD” 後跟 [600, 300, 100] 的 CBOR 編碼。

注意：
- 如果未找到有效的 OP_RETURN 分配，交易將自動使用按比例分配方法。
- 如果交易僅包含一個 OP_RETURN 輸出，附加到交易輸入的任何 ZELD 以及任何新獲得的獎勵將被永久銷毀，因為沒有可花費的輸出來接收它們。
- 當存在多個 OP_RETURN 輸出時，只有交易中最後出現且攜帶有效 ZELD+CBOR 有效載荷的那個將被考慮用於分配。