ZELDHASH 协议

寻找比特币最稀有的交易并赚取 **ZELD**。

作者：Ouziel Slama

1 动机

- 为了追寻的刺激。每笔交易都成为发现稀有事物的机会——隐藏在区块链上的数字宝藏。
- 这些前导零模式不仅稀有——它们还可能增强压缩效果，有可能简化区块链存储和处理效率。
- 任何人都可以通过寻找稀有交易来赚取 ZELD——不像比特币区块挖矿那样每个区块只有一个赢家。寻找对所有人开放。
- 如果成功，ZELD 代币最终可以报销交易费用——奖励那些发现最稀有交易的寻找者！

2 ZELD 挖矿

要挖掘 ZELD，您必须广播一笔 txid 以至少 6 个零开头的比特币交易。奖励根据您的交易与区块中最佳交易的比较来计算：

- 在给定区块中，以最多零开头的交易可获得 4096 ZELD
- 比最佳交易少一个零的交易可获得 4096/16 或 256 ZELD
- 比最佳交易少两个零的交易可获得 4096 / 16 / 16 或 16 ZELD
- 以此类推。

因此使用的公式如下：

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

其中 `max_zero_count` 等于最佳交易开头的零的数量，`zero_count` 是我们计算奖励的交易开头的零的数量。

注意： Coinbase 交易不符合 ZELD 奖励资格。

3 ZELD 分配

以 6 个或更多零开头的交易所赚取的 ZELD 将分配给 UTXO。分配方式如下：

- 如果只有一个非 OP_RETURN UTXO，它将获得全部奖励。
- 如果有两个或更多非 OP_RETURN UTXO，奖励将按每个 UTXO 的价值比例分配给除最后一个以外的所有 UTXO
- 由于计算仅使用整数，除法的可能余数将分配给第一个非 OP_RETURN UTXO。

例如，如果一笔获得 256 ZELD 的交易包含 4 个输出，分别为 500、500、500 和 2000 聪，第一个输出获得 86 ZELD 奖励，第二个和第三个各获得 85 ZELD。

4 转移 ZELD

当带有 ZELD 的 UTXO 被花费时，ZELD 将分配给交易中的新 UTXO。转移 ZELD 时有两种分配方法：

4.1 方法 1：自动按比例分配

默认情况下，分配方式与奖励完全相同——根据输出 UTXO 的比特币价值按比例分配，如果有多个输出则排除最后一个输出。

4.2 方法 2：通过 OP_RETURN 自定义分配

您可以通过在交易中包含带有自定义分配数据的 OP_RETURN 输出来精确指定 ZELD 应该如何分配。这允许对 ZELD 转移进行精确控制。

4.2.1 OP_RETURN 格式：

- OP_RETURN 脚本必须包含以 4 字节前缀 “ZELD” 开头的数据
- 在前缀之后，数据必须以 CBOR 格式编码
- CBOR 数据应表示无符号 64 位整数向量（Vec）
- 每个整数指定要发送到相应输出 UTXO 的 ZELD 数量

4.2.2 分配规则：

- 分配数组中的值的数量会自动调整以匹配非 OP_RETURN 输出的数量
- 如果数组太长，多余的值将被删除
- 如果数组太短，将追加零
- 分配值的总和不能超过正在花费的 ZELD 总量
- 如果总和小于总量，差额将添加到第一个输出
- 如果总和超过总量，交易将回退到按比例分配
- 新挖掘的 ZELD 奖励始终按比例分配，然后与自定义分配合并

4.2.3 示例：

如果您有 1000 ZELD 要分配给 3 个输出，并希望向第一个发送 600，向第二个发送 300，向第三个发送 100，您的 OP_RETURN 将包含 “ZELD” 后跟 [600, 300, 100] 的 CBOR 编码。

注意：
- 如果未找到有效的 OP_RETURN 分配，交易将自动使用按比例分配方法。
- 如果交易仅包含一个 OP_RETURN 输出，附加到交易输入的任何 ZELD 以及任何新获得的奖励将被永久销毁，因为没有可花费的输出来接收它们。
- 当存在多个 OP_RETURN 输出时，只有交易中最后出现且携带有效 ZELD+CBOR 有效载荷的那个将被考虑用于分配。