ZELDHASH プロトコル

ビットコインの最も希少なトランザクションを狩り、**ZELD** を獲得しよう。

著者：Ouziel Slama

1 動機

- 狩りのスリルのために。すべてのトランザクションが希少なものを発見する機会となります – ブロックチェーン上で目に見える場所に隠されたデジタルの宝物です。
- これらの先頭ゼロのパターンは単に希少なだけでなく – 圧縮を強化し、ブロックチェーンのストレージと処理効率を合理化する可能性があります。
- 誰でも希少なトランザクションを狩ることで ZELD を獲得できます – ビットコインブロックマイニングのようにブロックごとに単一の勝者ではありません。狩りはすべての人に開かれています。
- 成功すれば、ZELD トークンは最終的にトランザクション手数料を払い戻すことができます – 最も希少な発見をしたハンターに報酬を与えます!

2 ZELD マイニング

ZELD をマイニングするには、txid が少なくとも 6 つのゼロで始まるビットコイントランザクションをブロードキャストする必要があります。報酬は、あなたのトランザクションがブロック内の最良のトランザクションとどのように比較されるかに基づいて計算されます:

- 特定のブロックでは、最も多くのゼロで始まるトランザクションが 4096 ZELD を獲得します
- 最良のトランザクションより 1 つゼロが少ないトランザクションは 4096/16 または 256 ZELD を獲得します
- 2 つゼロが少ないトランザクションは 4096 / 16 / 16 または 16 ZELD を獲得します
- など。

したがって、使用される式は次のとおりです:

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

ここで `max_zero_count` は最良のトランザクションを開始するゼロの数に等しく、`zero_count` は報酬を計算するトランザクションを開始するゼロの数です。

注: コインベーストランザクションは ZELD 報酬の対象外です。

3 ZELD 配分

6 つ以上のゼロで始まるトランザクションで獲得した ZELD は UTXO に配分されます。配分は次のように行われます:

- 単一の非 OP_RETURN UTXO がある場合、報酬全体を受け取ります。

- 2 つ以上の非 OP_RETURN UTXO がある場合、報酬は最後のものを除くすべての UTXO に各 UTXO の値に比例して配分されます
- 計算は整数のみで行われるため、除算の余りは最初の非 OP_RETURN UTXO に配分されます。

例えば、256 ZELD を獲得したトランザクションにそれぞれ 500、500、500、2000 サトシの 4 つの出力が含まれている場合、最初の出力は報酬の 86 ZELD を受け取り、2 番目と 3 番目は 85 ZELD を受け取ります。

4 ZELD の移動

添付された ZELD を持つ UTXO が使用されると、ZELD はトランザクション内の新しい UTXO に配分されます。ZELD を移動する際に配分する 2 つの方法があります:

4.1 方法 1: 自動比例配分

デフォルトでは、配分は報酬とまったく同じ方法で行われます – 出力 UTXO のビットコイン値に基づいて比例的に、複数の出力がある場合は最後の出力を除きます。

4.2 方法 2: OP_RETURN によるカスタム配分

カスタム配分データを含む OP_RETURN 出力をトランザクションに含めることで、ZELD がどのように配分されるべきかを正確に指定できます。これにより、ZELD 転送を正確に制御できます。

4.2.1 OP_RETURN フォーマット:

- OP_RETURN スクリプトには 4 バイトプレフィックス「ZELD」で始まるデータが含まれている必要があります
- プレフィックスの後、データは CBOR 形式でエンコードされている必要があります
- CBOR データは符号なし 64 ビット整数のベクトル（Vec）を表す必要があります
- 各整数は対応する出力 UTXO に送信する ZELD の数を指定します

4.2.2 配分ルール:

- 配分配列の値の数は非 OP_RETURN 出力の数に一致するように自動的に調整されます
- 配列が長すぎる場合、余分な値は削除されます
- 配列が短すぎる場合、ゼロが追加されます
- 配分値の合計は使用されている ZELD の合計を超えることはできません
- 合計が総計より少ない場合、差額は最初の出力に追加されます
- 合計が総計を超える場合、トランザクションは比例配分に戻ります
- 新しくマイニングされた ZELD 報酬は常に比例的に配分され、その後カスタム配分と組み合わされます

4.2.3 例:

3 つの出力に 1000 ZELD を配分し、最初に 600、2 番目に 300、3 番目に 100 を送りたい場合、OP_RETURN には「ZELD」の後に[600, 300, 100]の CBOR エンコーディングが含まれます。

注:

- 有効な OP_RETURN 配分が見つからない場合、トランザクションは自動的に比例配分方法を使用します。
- トランザクションに OP_RETURN 出力が 1 つだけ含まれている場合、トランザクションの入力に添付された ZELD および新しく獲得した報酬は、受け取るための使用可能な出力がないため、永久に焼却されます。
- 複数の OP_RETURN 出力がある場合、トランザクションで最後に表示され、有効な ZELD+CBOR ペイロードを持つものだけが配分に考慮されます。