โปรโตคอล **ZELDHASH**

ล่าธุรกรรม **Bitcoin** ที่หายากที่สุดและรับ **ZELD**

โดย Ouziel Slama

1 แรงจูงใจ

- เพื่อความตื่นเต้นของการล่า ทุกธุรกรรมกลายเป็นโอกาสในการค้นพบสิ่งที่หายาก — สมบัติดิจิทัลที่ซ่อนอยู่ในที่เปิดเผยบนบล็อกเชน
- รูปแบบเลขศูนย์นำหน้าเหล่านี้ไม่ได้หายากเพียงอย่างเดียว — มันยังสามารถเพิ่มประสิทธิภาพการบีบอัด อาจทำให้การจัดเก็บบล็อกเชนและประสิทธิภาพการประมวลผลดีขึ้น
- ใครก็ตามสามารถรับ ZELD โดยการล่าธุรกรรมที่หายาก — ไม่มีผู้ชนะเพียงคนเดียวต่อบล็อกเหมือนในการขุดบล็อก Bitcoin การล่าเปิดสำหรับทุกคน
- หากประสบความสำเร็จ โทเค็น ZELD อาจชดเชยค่าธรรมเนียมธุรกรรมในที่สุด — รางวัลสำหรับนักล่าที่ค้นพบสิ่งที่หายากที่สุด!

2 การขุด **ZELD**

ในการขุด ZELD คุณต้องออกอากาศธุรกรรม Bitcoin ที่ txid เริ่มต้นด้วยเลขศูนย์อย่างน้อย 6 ตัว รางวัลคำนวณตามว่าธุรกรรมของคุณเปรียบเทียบกับธุรกรรมที่ดีที่สุดในบล็อกอย่างไร:

- ในบล็อกที่กำหนด ธุรกรรมที่เริ่มต้นด้วยเลขศูนย์มากที่สุดจะได้รับ 4096 ZELD
- ธุรกรรมที่มีเลขศูนย์น้อยกว่าธุรกรรมที่ดีที่สุดหนึ่งตัวจะได้รับ 4096/16 หรือ 256 ZELD
- ธุรกรรมที่มีเลขศูนย์น้อยกว่าสองตัวจะได้รับ 4096 / 16 / 16 หรือ 16 ZELD
- เป็นต้น

ดังนั้นสูตรที่ใช้มีดังนี้:

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

โดยที่ `max_zero_count` เท่ากับจำนวนเลขศูนย์ที่เริ่มต้นธุรกรรมที่ดีที่สุด และ `zero_count` คือจำนวนเลขศูนย์ที่เริ่มต้นธุรกรรมที่เราคำนวณรางวัล

หมายเหตุ: ธุรกรรม Coinbase ไม่มีสิทธิ์รับรางวัล ZELD

3 การแจกจ่าย **ZELD**

ZELD ที่ได้รับจากธุรกรรมที่เริ่มต้นด้วยเลขศูนย์ 6 ตัวขึ้นไปจะถูกแจกจ่ายไปยัง UTXO การแจกจ่ายดำเนินการดังนี้:

- หากมี UTXO ที่ไม่ใช่ OP_RETURN เพียงตัวเดียว มันจะได้รับรางวัลทั้งหมด
- หากมี UTXO ที่ไม่ใช่ OP_RETURN สองตัวขึ้นไป รางวัลจะถูกแจกจ่ายไปยัง UTXO ทั้งหมด ยกเว้นตัวสุดท้าย ตามสัดส่วนของมูลค่าของแต่ละ UTXO

- เนื่องจากการคำนวณทำด้วยจำนวนเต็มเท่านั้น เศษที่เป็นไปได้จากการหารจะถูกแจกจ่ายไปยัง UTXO ที่ไม่ใช่ OP_RETURN ตัวแรก

ตัวอย่างเช่น หากธุรกรรมที่ได้รับ 256 ZELD มี 4 เอาต์พุตที่มี 500, 500, 500 และ 2000 Satoshi ตามลำดับ เอาต์พุตแรกจะได้รับ 86 ZELD จากรางวัล ตัวที่สองและสามได้รับ 85 ZELD

4 การย้าย **ZELD**

เมื่อ UTXO ที่มี ZELD แนบถูกใช้ ZELD จะถูกแจกจ่ายไปยัง UTXO ใหม่ในธุรกรรม มีสองวิธีในการแจกจ่าย ZELD เมื่อย้าย:

4.1 วิธีที่ 1: การแจกจ่ายตามสัดส่วนอัตโนมัติ

โดยค่าเริ่มต้น การแจกจ่ายทำในลักษณะเดียวกับรางวัล — ตามสัดส่วนตามมูลค่า Bitcoin ของ UTXO เอาต์พุต ไม่รวมเอาต์พุตสุดท้ายหากมีเอาต์พุตหลายตัว

4.2 วิธีที่ 2: การแจกจ่ายแบบกำหนดเองผ่าน **OP_RETURN**

คุณสามารถระบุได้อย่างชัดเจนว่า ZELD ควรถูกแจกจ่ายอย่างไรโดยรวมเอาต์พุต OP_RETURN ในธุรกรรมของคุณพร้อมกับข้อมูลการแจกจ่ายแบบกำหนดเอง นี่ช่วยให้ควบคุมการโอน ZELD ได้อย่างแม่นยำ

4.2.1 รูปแบบ **OP_RETURN:**

- สคริปต์ OP_RETURN ต้องมีข้อมูลที่เริ่มต้นด้วยคำนำหน้า 4 ไบต์ “ZELD”
- หลังจากคำนำหน้า ข้อมูลต้องถูกเข้ารหัสในรูปแบบ CBOR
- ข้อมูล CBOR ควรแทนเวกเตอร์ของจำนวนเต็มไม่มีเครื่องหมาย 64 บิต (Vec)
- แต่ละจำนวนเต็มระบุจำนวน ZELD ที่จะส่งไปยัง UTXO เอาต์พุตที่สอดคล้องกัน

4.2.2 กฎการแจกจ่าย:

- จำนวนค่าในอาร์เรย์การแจกจ่ายจะถูกปรับโดยอัตโนมัติเพื่อให้ตรงกับจำนวนเอาต์พุตที่ไม่ใช่ OP_RETURN
- หากอาร์เรย์ยาวเกินไป ค่าพิเศษจะถูกลบ
- หากอาร์เรย์สั้นเกินไป ศูนย์จะถูกเพิ่ม
- ผลรวมของค่าการแจกจ่ายไม่สามารถเกินจำนวน ZELD ทั้งหมดที่กำลังใช้
- หากผลรวมน้อยกว่าจำนวนทั้งหมด ส่วนต่างจะถูกเพิ่มไปยังเอาต์พุตแรก
- หากผลรวมเกินจำนวนทั้งหมด ธุรกรรมจะกลับไปใช้การแจกจ่ายตามสัดส่วน
- รางวัล ZELD ที่ขุดใหม่จะถูกแจกจ่ายตามสัดส่วนเสมอ แล้วจึงรวมกับการแจกจ่ายแบบกำหนดเอง

4.2.3 ตัวอย่าง:

หากคุณมี 1000 ZELD ที่จะแจกจ่ายใน 3 เอาต์พุต และต้องการส่ง 600 ไปยังตัวแรก 300 ไปยังตัวที่สอง และ 100 ไปยังตัวที่สาม OP_RETURN ของคุณจะมี “ZELD” ตามด้วยการเข้ารหัส CBOR ของ [600, 300, 100]

หมายเหตุ:
- หากไม่พบการแจกจ่าย OP_RETURN ที่ถูกต้อง ธุรกรรมจะใช้วิธีการแจกจ่ายตามสัดส่วนโดยอัตโนมัติ
- หากธุรกรรมมีเอาต์พุต OP_RETURN เพียงตัวเดียว ZELD ใดๆ ที่แนบกับอินพุตของธุรกรรม และรางวัลใหม่ที่ได้รับจะถูกเผาอย่างถาวรเพราะไม่มีเอาต์พุตที่สามารถใช้ได้เพื่อรับพวกมัน

- เมื่อมีเอาต์พุต OP_RETURN หลายตัว เฉพาะตัวที่ปรากฏท้ายสุดในธุรกรรมและมี payload ZELD+CBOR ที่ถูกต้องเท่านั้นที่จะถูกพิจารณาสำหรับการแจกจ่าย