

ZELDHASH פרוטוקול

צחו את העסקאות הנדרות ביותר של ביטקוין והרוויזו ZELD.

מאת Ouziel Slama

מניעים 1

- בשבייל הריגוש של הצד. כל עסקה הופכת להזמנה לגלות שהוא נדייר – אוצר דיגיטלי מוסתר לעין על הבלוקצ'ין.
- הדפוסים האלה של אפסים מוביילים אינם רק נדרירים – הם גם יכולים לשפר דחיסה, מה שעלול ליעיל את אחסון הבלוקצ'ין ויעילות העבודה.
- על ידי ציד עסקאות נדרירות – אין מנצח היחיד לככל בלוק כמו בכריית בלוקים של ביטקוין. ZELD כל אחד יכול להרוויזו הצד פתוח לכלום.
- יכולים בסופו של דבר להחזיר عملות עסקה – לתגמל ציידים שמגלים את הממצאים הנדרירים ZELD אם יצליחו, טוקני ביותר!

2 כריית ZELD

שליה מתחילה לפחות 6 אפסים. הפרס מוחושב על סמך איך העסקה txid-עליכם לשדר עסקה ביטקוין שה ZELD כדי לכרכות: שככם משתמשת בעסקה הטובה ביותר בבלוק

- ZELD בבלוק נתון, עסקאות שמתחלילות עם הכיוון הרבה אפסים מרוויזות 4096
- ZELD עסקאות עם אפס אחד פחות מהעסקאות הטובות ביותר מרוויזות 4096/16 או 256
- ZELD עסקאות עם שני אפסים פחות מרוויזות 4096 / 16 / 16 או 16
- וכו'.

לכן הנוסחה המשמשת היא כדלקמן:

$$\text{reward} = 4096 / 16 ^ (\max_zero_count - zero_count)$$

הוא מספר האפסים שמתחלילים את העסקה הטובה ביותר ועוד max_zero_count שווה למספר האפסים שמתחלילים את העסקה הטובה ביותר ועוד max_zero_count כאשר max_zero_count הוא מספר האפסים שמתחלילים את העסקה הטובה ביותר ועוד max_zero_count.

אינן זכויות לפרסוי Coinbase הערכה: עסקאות ZELD.

3 חלוקת ZELD

חלוקת מתבצעת כדלקמן UTXOs-שהורוויזו עם עסקה שמתחלילה ב-6 אפסים או יותר מחולקים ל:

- הוא מקבל את כל הפרס, OP_RETURN, יחיד שאינו UTXO אם יש.
- כמעט לאחרון, ביחס לערך של הUTXOs, הפרס מחולק לכל ה-OP_RETURN שאינם OP_RETURN אם יש שניים או יותר UTXO בכל.
- הראשון שאינו UTXO-מכיוון שהחישובים נעשים רק עם מספרים שלמים, השARING האפשרית של החלוקה מחולקת ל OP_RETURN.

מכילה 4 פלטיהם עם 500, 500, 500 ו-2000 סאטoshi בהתאם, הפלט הראשון LODוגמה, אם עסקה שמרוויזה ZELD מפהרס, השני והשלישי ZELD 85 מקבל 86.

4 העברת ZELD

החדשים בעסקה. יש שתי שיטות לחלוקת UTXOs-ZELDs-מחולקים לUTXOs-ZELDs-מצורפים מוצאים, ה עם UTXOs כאשר ZELDs בעות העברתם:

4.1 שיטה 1: חלוקה יחסית אוטומטית

הפלט, UTXOs כביררת מודול, החלוקת נעשית בדיק באותו אופן כמו הפרטים – יחסית על בסיס ערכי הביטוקין של למעט הפלט האחרון אם יש מספר פלטים.

4.2 שיטה 2: חלוקה מותאמת אישית דרך OP_RETURN

בעסקה שלכם עם נחוני OP_RETURN צריכים להיות מחולקים על ידי הכללת פלט ZELDs שהם יכולים לציין איך חלוקה מותאמת אישית. זה מאפשר שליטה מדויקת על העברות ZELD.

4.2.1 OP_RETURN פורתט:

- “ZELD” חייב להכיל נתונים שמתיחסים עם הקידומת של 4 בתים OP_RETURN סקורייפט
- CBOR אחרי הקידומת, הנתונים חייבים להיות מקודדים בפורמט
- צריכים ליצג וקטור של מספרים שלמים לא חתומים של 64 בית CBOR נחוני
- הפלט המתאים UTXO-ZELDs-לשלה כל מספר שלם מצין כמה

4.2.2 כללי חלוקה:

- OP RETURN מספר הערכיהם במערך החלוקת מותאם אוטומטית כדי להתאים למספר הפלטים שאינם
- אם המערך ארוך מדי, ערכיהם נוספים מוסרים
- אם המערך קצר מדי, אפסים מתווספים
- המוצאים-ZELDs-הסכום הכלול של ערכי החלוקת לא יכול לעלות על סך ה
- אם הסכום קטן מהסך הכלול, ההפרש מתווסף לפט הראשון
- אם הסכום עולה על הסך הכלול, העסקה חוזרת לחלוקה יחסית
- שנכרו לאחרונה מחולקים תמיד יחסית ואו משולבים עם החלוקת המותאמת אישית ZELD פרטי.

4.2.3 דוגמה:

1000-OP_RETURN-פלט ל-3 פלטים ואתם רוצים לשלה 600 לראשון, 300 לשני, ו-100 לשישי, ה ZELD אם יש לכם יכול CBOR [100,300,600] ואחריו קידוד “ZELD” שלם יוכל.

הערות:

- חוקית, העסקה משתמשת אוטומטית בשיטת החלוקת היחסית OP_RETURN אם לא נמצא חלוקה
- מצורף לקלטי העסקה וכל פרט שהורווח לאחרונה נשרפים ZELD אחד, כל OP_RETURN אם עסקה מכילה רק פלט.
- לצמצמות כי אין פלטים שניין להוציא כדי לקבל אותם.
- חוקי נלקח בחשבון ZELD+CBOR רק זה שמופיע אחרון בעסקה ונושא מטען, OP_RETURN כאשר קיימים מספר פלטי חלוקה.