

ZELDHASH פרוטוקול

ZELD צודו את העסקאות הנדירות ביותר של ביטקוין והרוויחו

מאת Ouziel Slama

מניעים 1

- בשביל הריגוש של הצייד. כל עסקה הופכת להזדמנות לגלות משהו נדיר – אוצר דיגיטלי מוסתר לעין על הבלוקצ'יין.
- הדפוסים האלה של אפסים מובילים אינם רק נדירים – הם גם יכולים לשפר דחיסה, מה שעלול לייצל את אחסון הבלוקצ'יין ויעילות העיבוד.
- על ידי ציד עסקאות נדירות – אין מנצח יחיד לכל בלוק כמו בכריית בלוקים של ביטקוין. ZELD כל אחד יכול להרוויח. הצייד פתוח לכולם.
- יוכלו בסופו של דבר להחזיר עמלות עסקה – לתגמל ציידים שמגלים את הממצאים הנדירים ZELD אם יצליח, טוקני ביותר!

ZELD כריית 2

שלה מתחיל בלפחות 6 אפסים. הפרס מחושב על סמך איך העסקה txid-עליכם לשדר עסקת ביטקוין שה ZELD כדי לזכות שלכם משתווה לעסקה הטובה ביותר בבלוק:

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

לכן הנוסחה המשמשת היא כדלקמן:

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

הוא מספר האפסים zero_count-שווה למספר האפסים שמתחילים את העסקה הטובה ביותר ו max_zero_count כאשר שמתחילים את העסקה שעבורה אנו מחשבים את הפרס.

ZELD אינן זכאיות לפרסי Coinbase הערה: עסקאות

ZELD חלוקת 3

החלוקה מתבצעת כדלקמן. UTXOs-שהורווחו עם עסקה שמתחילה ב-6 אפסים או יותר מחולקים ל ZELDs:

- הוא מקבל את כל הפרס, OP_RETURN יחיד שאינו UTXO אם יש.
- למעט האחרון, ביחס לערך של UTXOs-הפרס מחולק לכל ה, OP_RETURN שאינם UTXOs אם יש שניים או יותר כל UTXO
- הראשון שאינו UTXO-מכיוון שהחשובים נעשים רק עם מספרים שלמים, השארית האפשרית של החילוק מחולקת ל OP_RETURN.

מכילה 4 פלטים עם 500, 500, 500 ו-2000 סאטושי בהתאמה, הפלט הראשון ZELD לדוגמה, אם עסקה שמרוויחה 256 ZELD מהפרס, השני והשלישי ZELD 85 מקבל 86

4 ZELD העברת

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

4.1 שיטה 1: חלוקה יחסית אוטומטית

הפלט, UTXOs כברירת מחדל, החלוקה נעשית בדיוק באותו אופן כמו הפרסים – יחסית על בסיס ערכי הביטקוין של. למעט הפלט האחרון אם יש מספר פלטים

4.2 OP_RETURN שיטה 2: חלוקה מותאמת אישית דרך

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

4.2.1 OP_RETURN פורמט:

- “ZELD” חייב להכיל נתונים שמתחילים עם הקידומת של 4 בתים OP_RETURN סקריפט
- CBOR אחרי הקידומת, הנתונים חייבים להיות מקודדים בפורמט
- (Vec) צריכים לייצג וקטור של מספרים שלמים לא חתומים של 64 ביט CBOR נתוני
- הפלט המתאים UTXO-לשלוח ל ZELDs כל מספר שלם מציין כמה

4.2.2 כללי חלוקה:

- OP_RETURN מספר הערכים במערך החלוקה מותאם אוטומטית כדי להתאים למספר הפלטים שאינם
- אם המערך ארוך מדי, ערכים נוספים מוסרים
- אם המערך קצר מדי, אפסים מתווספים
- המוצאים ZELDs-הסכום הכולל של ערכי החלוקה לא יכול לעלות על סך ה
- אם הסכום קטן מהסך הכולל, ההפרש מתווסף לפלט הראשון
- אם הסכום עולה על הסך הכולל, העסקה חוזרת לחלוקה יחסית
- שנכרו לאחרונה מחולקים תמיד יחסית ואז משולבים עם החלוקה המותאמת אישית ZELD פרסי

4.2.3 דוגמה:

OP_RETURN-לחלק ל-3 פלטים ואתם רוצים לשלוח 600 לראשון, 300 לשני, ו-100 לשלישי, ה ZELD אם יש לכם 1000 של [100, 300, 600] CBOR ואחריו קידוד “ZELD” שלכם יכול

הערות:

- חוקית, העסקה משתמשת אוטומטית בשיטת החלוקה היחסית OP_RETURN אם לא נמצאת חלוקת
- מצורף לקלטי העסקה וכל פרס שהורוח לאחרונה נשרפים ZELD אחד, כל OP_RETURN אם עסקה מכילה רק פלט לצמיתות כי אין פלטים שניתן להוציא כדי לקבל אותם
- חוקי נלקח בחשבון ZELD+CBOR רק זה שמופיע אחרון בעסקה ונושא מטען, OP_RETURN כאשר קיימים מספר פלטי לחלוקה