

ZELDHASH پروتکل

ZELD شکار نادرترین تراکنش‌های بیت‌کوین و کسب

Ouziel Slama نوشته

انکیزه‌ها 1

- برای می‌جان شکار. هر تراکنش فرصتی برای کشف چیزی نادر می‌شود — کنجی دیجیتالی که در دید آشکار روی بلاکچین پنهان شده است.
- این الگوهای صفرهای ابتدایی نه تنها نادر هستند — بلکه می‌توانند فشرده‌سازی را نیز بهبود بخشند و به طور بالقوه ذخیره‌سازی بلاکچین و کارایی پردازش را بهینه کنند.
- کسب کند — نه مانند استخراج بلوک بیت‌کوین با یک برنده در هر ZELD هر کسی می‌تواند با شکار تراکنش‌های نادر بلوک. شکار برای همه باز است.
- می‌توانند در نهایت هزینه‌های تراکنش را بازپرداخت کنند — به شکارچی‌انی که ZELD در صورت موفقیت، توکن‌های نادرترین یافته‌ها را کشف می‌کنند پاداش دهند!

ZELD استخراج 2

آن با حداقل ۶ صفر شروع شود. پاداش بر اساس مقایسه txid باید یک تراکنش بیت‌کوین پخش کنید که ZELD برای استخراج تراکنش شما با بهترین تراکنش در بلوک محاسبه می‌شود:

- کسب می‌کنند ZELD در یک بلوک مشخص، تراکنش‌هایی که با بیشترین صفر شروع می‌شوند ۴۰۹۶
- کسب می‌کنند ZELD تراکنش‌هایی با یک صفر کمتر از بهترین تراکنش‌ها ۴۰۹۶/۱۶ یا ۲۵۶
- کسب می‌کنند ZELD تراکنش‌هایی با دو صفر کمتر ۴۰۹۶ / ۱۶ / ۱۶ یا ۱۶
- و غیره.

بنابراین فرمول استفاده شده به شرح زیر است:

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

تعداد صفرهایی zero_count برابر با تعداد صفرهایی است که بهترین تراکنش را شروع می‌کنند و max_zero_count که در آن است که تراکنشی را که پاداش آن را محاسبه می‌کنیم شروع می‌کنند.

نمی‌ستند ZELD واجد شرایط پاداش Coinbase توجه: تراکنش‌های

ZELD توزیع 3

ها توزیع می‌شوند. توزیع به شرح زیر UTXO های کسب شده با تراکنشی که با ۶ صفر یا بیشتر شروع می‌شود به ZELD انجام می‌شود:

- وجود داشته باشد، کل پاداش را دریافت می‌کند OP_RETURN-غیر UTXO اگر یک
- ها به جز آخری، به نسبت ارزش هر UTXO وجود داشته باشد، پاداش به همه OP_RETURN-غیر UTXO اگر دو یا بیشتر UTXO توزیع می‌شود

- OP_RETURN-غیر UTXO از آنجا که محاسبات فقط با اعداد صحیح انجام می‌شود، باقی‌مانده احتمالی تقسیم به اولین توزیع می‌شود.

کسب می‌کند شامل ۴ خروجی با ۵۰۰، ۵۰۰ و ۲۰۰۰ ساتوشی باشد، خروجی ZELD به عنوان مثال، اگر تراکنشی که ۲۵۶ ZELD از پاداش دریافت می‌کند، دومی و سومی ۸۵ ZELD اول ۸۶

4 ZELD انتقال

های جدید در تراکنش توزیع می‌شوند. دو روش UTXO ها به ZELD، پیوست شده خرج می‌شوند ZELD هایی با UTXO وقتی هنگام انتقال آنها وجود دارد ZELD برای توزیع

4.1 روش ۱: توزیع نسبی خودکار

های UTXO به طور پیش‌فرض، توزیع دقیقاً به همان روش پاداش‌ها انجام می‌شود — به نسبت بر اساس ارزش بی‌تفاوتی خروجی، به استثنای آخرین خروجی اگر چندی خروجی وجود داشته باشد

4.2 OP_RETURN روش ۲: توزیع سفارشی از طریق

در تراکنش OP_RETURN ها چگونه باید توزیع شوند با اضافه کردن یک خروجی ZELD می‌توانید دقیقاً مشخص کنید که را فراهم می‌کند ZELD خود با داده‌های توزیع سفارشی. این امکان کنترل دقیق بر انتقالات

4.2.1 فرمت OP_RETURN:

- شروع می‌شود “ZELD” باید شامل داده‌هایی باشد که با پی‌شوند ۴ بیتی OP_RETURN اس‌کرپت
- کدگذاری شوند CBOR پس از پی‌شوند، داده‌ها باید در فرمت
- را نشان دهد (Vec) باید یک بردار از اعداد صحیح ۶۴ بیتی بدون علامت CBOR داده
- خروجی مربوطه ارسال شود UTXO به ZELD هر عدد صحیح مشخص می‌کند که چند

4.2.2 قوانین توزیع:

- مطابقت داشته باشد OP_RETURN-تعداد مقادیر در آرایه توزیع به طور خودکار تنظیم می‌شود تا با تعداد خروجی‌های غیر
- اگر آرایه خیلی بلند باشد، مقادیر اضافی حذف می‌شوند
- اگر آرایه خیلی کوتاه باشد، صفرها اضافه می‌شوند
- های در حال خرج شدن بیشتر باشد ZELD مجموع کل مقادیر توزیع نمی‌تواند از کل
- اگر مجموع کمتر از کل باشد، تفاوت به اولین خروجی اضافه می‌شود
- اگر مجموع از کل بیشتر شود، تراکنش به توزیع نسبی برمی‌گردد
- تازه استخراج شده هم‌یشه به صورت نسبی توزیع می‌شوند و سپس با توزیع سفارشی ترکیب می‌شوند ZELD پاداش‌های

4.2.3 مثال:

برای توزیع در ۳ خروجی دارید و می‌خواهید ۶۰۰ به اولی، ۳۰۰ به دومی و ۱۰۰ به سومی بفرستید ZELD اگر ۱۰۰۰ از [100, 300, 600] خواهد بود CBOR و سپس کدگذاری “ZELD” شما شامل OP_RETURN

نکات:

- معتبری یافت نشود، تراکنش به طور خودکار از روش توزیع نسبی استفاده می‌کند OP_RETURN اگر هیچ توزیع
- پیوست شده به ورودی‌های تراکنش و هر پاداش تازه ZELD باشد، هر OP_RETURN اگر تراکنش فقط شامل یک خروجی
- کسب شده برای هم‌یشه سوزانده می‌شود زیرا هیچ خروجی قابل خرج برای دریافت آنها وجود ندارد

- معتبر payload وجود دارد، فقط آن‌گاه آخرین بار در تراکنش ظاهر می‌شود و OP_RETURN هنگامی که چندین خروجی را حمل می‌کنند برای توزیع در نظر گرفته می‌شود ZELD+CBOR.