

ZELDHASH پروتکل

ZELD شکار نادرترین تراکنش‌های بیت‌کوین و کسب

نوشته Ouziel Slama

انکیزههای ۱

- برای هیجان‌شکار، هر تراکنش فرصتی برای کشف جیزی نادر می‌شود — کنجدی دیجیتال که در دید آشکار روی بلاکچین پنهان شده است.
- این الگوهای صفرهای ابتدایی نه تنها نادر هستند — بلکه می‌توانند فشردماسازی را نیز بهبود بخشدند 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!

استخراج ۲ ZELD

آن با حداقل ۶ صفر شروع شود. پاداش بر اساس مقایسه txid باشد 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:

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

تعداد صفرهایی 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. نیستند ZELD واجد شرایط پاداش Coinbase توجه: تراکنش‌های

۳ توزیع ZELD

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

- وجود داشته باشد، کل پاداش را دریافت می‌کند `OP_RETURN`-غیر UTXO اکریک.
- ها به جز آخری، به نسبت ارزش هر UTXO وجود داشته باشد، پاداش به همه UTXO اکردو یا بیشتر `OP_RETURN`-غیر 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 ۸۶ از پاداش دریافت می‌کند، دومی و سومی ZELD.

4 انتقال ZELD

های جدید در تراکنش توزیع می‌شوند. دو روش UTXO ها به ZELD پیوست شده خرج می‌شوند ZELD هایی با وقتی هنکام 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 بیتلکلوزی خروجی، به استثنای آخرین خروجی اگر چندین خروجی وجود داشته باشد.

4.2 روش ۲: توزیع سفارشی از طریق OP_RETURN

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

4.2.1 فرمت OP_RETURN:

- شروع می‌شود ”ZELD“ باعده شامل داده‌هایی باشد که با پیشوند ۴ بایتی OP_RETURN اسکریپت
- کدگذاری شوند CBOR پس از پیشوند، داده‌ها باعده در فرمت
- را نشان دهد (Vec) باعده یک بردار از اعداد صحیح ۶۴ بایتی بدون علامت CBOR داده
- خروجی مربوطه ارسال شود UTXO 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 خروج 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 برمی‌کردد
- تازه استخراج شده همیشه به صورت نسبی توزیع می‌شوند و سپس با توزیع سفارشی ترکیب می‌شوند ZELD پادashهای

4.2.3: مثال

برای توزیع در ۳ خروجی داریم و می‌خواهیم ۶۰۰ به اولی، ۳۰۰ به دومی و ۱۰۰ به سومی بفرستیم اگر ZELD

بنگاه:

- معتبری یافته 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 خروج برای دریافت آنها وجود ندارد

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