Freeman Family

July 4, 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

یک سیستم پولی نظیر-به-نظیر

ذخیره ارزش + واسطه تبادل + واحد مساحبه

1.7 میلیارد از بزرگسالان دنیا به سیستم مالی جهانی دسترسی ندارند، در حالی که 1.3 میلیارد نفر دیگر هم از پوشش کافی برخوردار نیستند. Epic Cash با مرتبط کردن افراد به بازار جهانی، پتانسیل افراد را شکوفا میکند. سریع، تقریباً رایگان، و در دسترس برای همگان.

Version 7.1b

فهرست

I. خلاصه

Epic Cash آخرین نقطه در مسیر رسیدن به پول اینترنتی P2P واقعی است، سنگ بنای یک سیستم مالی خصوصی. ارز Epic تبدیل شدن به مؤثرترین ارز دیجیتال دنیا در حفاظت از حریم خصوصی را نشانه رفته است. به منظور تحقق این هدف، سه اصل کارایی پول را برآورده میکند:

1.ذخیره ارزش: قابلیت ذخیره، بازیابی و مبادله در آینده و با ارزش قابل پیش بینی در هنگام بازیابی.
2.واسطه تبادل: هر چیز پذیرفته شده به عنوان استاندارد ارزش و قابل داد و ستد در ازای کالا و خدمات.
3.واحد محاسبه: واحدی که به وسیله آن ارزش یک چیز محاسبه و مقایسه میشود.

	EPIC	BTC	$ USD
ذخیره ارزش	✓	✓	✗
واسطه تبادل	✓	✗	✓
واحد محاسبه	✓	✗	✓

در سال 2009، Bitcoin به عنوان اولین ارز دیجیتالی بر پایه بلاکچین ظهور کرد، و به همراه آن سه ویژگی تعیین کننده که سایر ارزهای دیجیتال بر اساس آن ارزیابی میشوند:

- **غیر متمرکز** – "بلاکچین ها از منظر سیاسی غیرمتمرکز (هیچ شخصی آنها را کنترل نمیکند) و از منظر معماری غیرمتمرکز هستند (هیچ نقطه شکستی در زیرساخت آنها وجود ندارد)..."[1].
- **تغییر ناپذیری** – تراکنش ها نمیتوانند بازگشت داده شوند ؛
  a. بازنویسی تاریخ باید به شدت‌سخت یا غیرممکن باشد؛
  b. جابجایی دارایی برای هرکس به‌جز دارنده کلید خصوصی مرتبط با دارایی باید غیر ممکن باشد؛
  c. تمام تراکنش ها در بلاکچین ذخیره شده اند.
- **عدم نیاز به اعتماد** – برای عملکرد شبکه، هیچ کس نیاز به اعتماد به یک واحد مرکزی یا طرف مقابل خود ندارد.

بیتکوین ضمن رعایت اصول آزمایش شده در طول زمان، روش های تکنولوژیکی جدیدی را در ساختار سیاست مالی خود به کار برد. موفقیت بیتکوین به شدت با عرضه محدود آن به همراه ویژگی های عدم نیاز به اعتماد، تغییر ناپذیری و غیرمتمرکز بودن بلاکچین مرتبط است. Epic Cash سیاست مالی بیتکوین را در کاهش تورم و عرضه محدود دنبال میکند تا اطمینان حاصل کند که ارز Epic میتواند به عنوان یک ذخیره ارزش مؤثر، عمل کند .

با وجود موفقیت بیکوین، کاستی های خاصی از زمان آغاز به کار آن، یعنی 10 سال پیش، آشکار شده است. پروژه های دیگر سعی در برطرف کردن این کاستی ها داشته اند و ما بهترین ها را بررسی کرده ایم تا از آنها به عنوان نقطه شروع خود استفاده کنیم. ما تصمیم گرفتیم تا از کد پایه Grin و کارهای عالی چندین پروژه دیگر استفاده کنیم تا به ما در رسیدن به دستاورد های دشوار و کشف عیب های پیشینیان Epic Cash به درستی کمک کنند. Epic Cash دارای ویژگی های کلیدی برای ارز ایده آل بودن است:

- **امنیت** – بلاکچین hsaC cipE با محافظت از جزئیات تراکنش ها از شخص ثالث، از ناشناس بودن دارندگان و استفاده کنندگان cipE محافظت میکند، و به گونه ای طراحی شده است که غیرقابل ردیابی و نامرئی در برابر رصد شدن باشد.
- **سرعت** – تراکنش های Epic Cash روان و پیوسته بوده و بسیار سریع تر از تکنولوژی نسل های گذشته بلاکچین اجرا میشود. در حالی که بیتکوین به شش بلوک 10 دقیقه ای برای تکمیل تأیید تراکنش ها نیاز دارد، تراکنش های Epic به محض استخراج یک بلوک 1 دقیقه ای در یک بلوک تأییدی انجام میشود.
- **تعویض پذیری** – ارزش مقدار مشخصی از Epic همیشه باید برابر با مقدار دیگری از Epic باشد، همان طور که یک ین یا یوان همیشه برابر با یک ین یا یوان قابل جایگزین دیگر است.
- **مقیاس پذیری** – Epic Cash یک بلاکچین که از لحاظ فضایی کارآمد است را برقرار میکند، که بر روی آن گره های جدید به راحتی بدون تجهیزات منابع فشرده، قابل دسترسی خواهد بود. بلاکچین Epic Cash قادر به حداقل توان خروجی دو برابر بیتکوین است.

[1] Buterin, Vitalik, *The Meaning of Decentralization*, 6 February, 2017,
https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. حریم خصوصی

استفاده امروز از پول را می توان به عنوان انتقال انبوه مقادیر حساب بین مردم و نهادها تعریف کرد. با پاسخ دادن به سؤالات زیر می توانید چشم انداز پول در هر مقطع زمانی مشخص را ترسیم کنید:

1. چه کسانی آن را نگه میدارند و به چه میزان؟

2. چه کسی با چه کسی و به چه میزان داد و ستد میکند؟

برای ارزهای مرسوم اعتباری و در واقع بیت کوین نیز می توانیم به ایـن سـؤالات پاسخ دهیم. با انجام ایـن کـار، می توان چیزهای زیادی در مورد زندگی مردم آشکار کرد، مانند الگوهای مصرف، دارایی ها و طرفهای معاملات. با ردیابی نقل و انتقالات دارایی، می توان نتایج دقیقی درباره علایق و اهداف یک فرد کسب کـرد. بـدون حفظ حریم خصوصی، داده های تراکنش ها می توانند اطلاعات خطرناکی در دست اشخاص ثالث سودجو باشند.

استفاده از ارز رمزنگاری در دهه گذشته، استمرار "حفاظت از حریم خصوصی" را در پیاده سازی های متفاوت بلاکچین نشان می دهد. مقیاس حریم خصوصی که باید در نظر گرفته شود، از علنی از یکسو تا ناشناس در سوی دیگر است. با از بین رفتن حریم خصوصی، یک سنگ بنای اساسی ارزرمـــز، یعنی عدم نیاز به اعتماد از بین میرود. همانطور که از موفقیت سرویس های تجزیه و تحلیل بلاکچین بیتکوین مشهود است، بیت کوین بیشتر مناسب سمت شفاف طیف حریم خصوصی است. کاربران باید به طور فزاینده قدم هایی را برای اطمینان از عدم معامله در بیت کوین آلوده انجام دهند. راه حل Epic Cash سـوزن را به سمت ناشناس طیف می چرخاند و این ویژگی اساسی را با مهندسی حریم خصوصی فرد و پوشیدگی تراکنش ها در سطح پایه ای سیستم، تضمین میکند.

پوشیدگی هویت

پوشیدگی تراکنش

پوشیدگی هویت

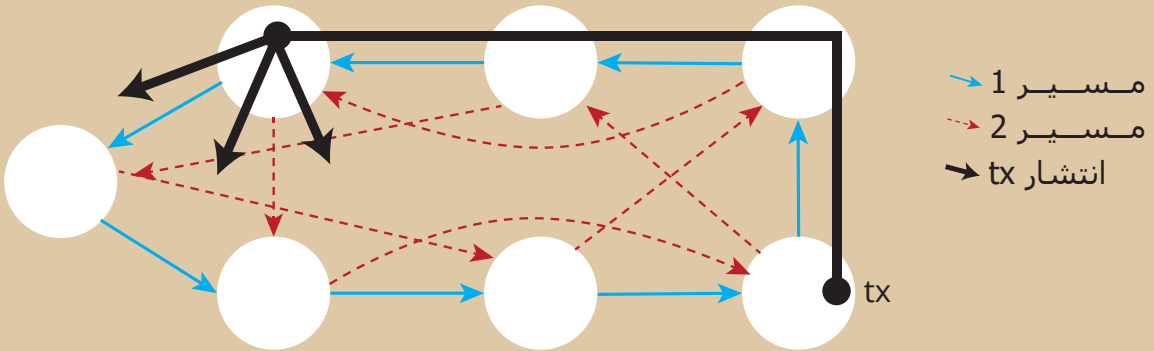
بیشتر ارزرمزها مانند بیت کوین در کیف پولهایی ذخیره می شوند که آدرس آنها به کلید عمومی برگرفته از کلیدهای خصوصی کیف پول، ارجاع میدهند. می توان این آدرس ها را به عنوان مکان یاب گاوصندوق خصوصی شخص، در دنیای دیجیتال تصور کرد. بلاکچین Epic Cash آدرس ها را به طور کامل حذف میکند و در عوض، از یک امضای چندکاربره استفاده می کند که کلیه کلیدهای عمومی و خصوصی بر پایه یکبارمصرف بودن تولید می شوند.

افزون بر حذف آدرس های کیف پول، بلاکچین hsaC cipE با اطمینان از اینکه آدرس های PI قابل ردیابی نیستند، پوشیدگی هویت را تضمین می کند. این کار را از طریق پروتکل noiednaD++ انجام می دهد. پروتکل noiednaD++ با بهبود روی پروتکل قبلی خود یعنی پروتکل اصلی noiednaD، نتیجه کار مداوم 7 محقق در تلاش برای دفاع از حملات تغییر نام روی بلاکچین است. از طریق Dandelion++، تراکنش ها از مسیرهای درهم تنیده تصادفی، یا "کابل ها"، عبور می کنند، و سپس ناگهان به یک شبکه بزرگ از گره ها مانند تخم های یک گل قاصدک هنگام دمیدن به آن، نفوذ میکنند (شکل 1). این امر ردیابی معاملات به سرمنشاء آنها، و به همین دلیل آدرسهای IP مولد آنها را تقریباً غیرممکن میسازد.

از آنجا که آدرس های کیف پول بیت کوین یک مکان یاب گاوصندوق دنیای دیجیتالی هستند، می توان از طریق آن به آدرس پروتکل اینترنت (IP) یک مالک رسید، که مالک را به یک کامپیوتر در یک مکان مشخص در هر لحظه از زمان متصل میکند. به بیان ساده: وقتی یک تراکنش بیت کوین انجام می شود ،تراکنش از یک مرکز ارتباطی به نام "گره" انتشار میابد و سپس به گره های دیگر موسوم به "نظیر" گسترش میابد. این اطلاعات سپس به سرعت به نظیرهای آن گره ها به طور متوالی در کل شبکه توزیع می شود. این فرآیند به درستی "پروتکل شایعات" نامگذاری شده است. به سادگی، هر بیت کوین یک موقعیت آنلاین مشخص و یک مکان فیزیکی دارد که آن بیتکوین، یا به عبارت دیگر صاحب بیتکوین میتواند در آنجا پیدا شود. همانطور که روزنامه نگار گریس کافین اشاره کرده است، بیت کوین "مخفی تر از جستجوی گوگل از طریق اینترنت خانگی نیست."[2]

شکل 1: ناشناس کردن تراکنش ها با پروتکل Dandelion++

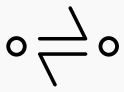
Dandelion++ پیام ها را در یکی از دو مسیر درهم تنیده روی یک گراف 4-منتظم ارسال می کند، سپس با استفاده از پخش آن را انتشار می دهد. در شکل،تراکنش از طریق مسیر آبی توپر، منتشر می شود.[3] این روند، ردیابی تراکنش ها به منبع آنها را بسیار دشوار می کند، در نتیجه حریم خصوصی را حفظ می کند.



[2] F2Caffyn, Grace, *Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,* 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', *Proc. ACM Meas. Anal. Comput. Sys.*, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

پوشیدگی تراکنش



بلاکچین Epic Cash با پنهان کردن مقادیر و رابطه فرستنده و گیرنده یک تراکنش، پوشیدگی تراکنش را تضمین می کند. این کار با استفاده از ایده های آشنا از تراکنش های محرمانه[4] (*Confidential Transactions (CT*) و *CoinJoin*[5]، روش هایی که پیشتر توسط Gregory Maxwell (توسعه دهنده هسته بیت کوین ، بنیان گذار و CTO از (Blockmaster) تهیه شده است، حاصل می شود.

CT، که ابتدا توسط Adam Back ساخته شد و بعدا توسطMaxwell بهبود داده شد، با شکستن تراکنش به بخش های کوچکتر از طریق homomorphic encryption، یک روش انجام محاسبات روی اطلاعات رمزگذاری شده بدون رمزگشایی در ابتدا، برای حفظ حریم خصوصی، کار می کند. پس از تقسیم، ناظران نمی توانند مبلغ واقعی تراکنش ها را به دلیل فاکتورهای کورکننده ببینند، سیستمی که اعداد تصادفی را به ترکیب تکه های تراکنش اضافه می کند تا مقادیر آن تکه ها را پنهان کند. درنهایت، فقط طرفهای درگیر در تراکنش، مقدار تراکنش را می دانند، در حالی که تراکنش توسط شبکه از طریق تأیید اینکه مجموع مقادیر خروجی برابر است با مجموع مقادیر ورودی، و مجموع فاکتورهای کورکننده خروجی برابر است با مجموع فاکتورهای کورکننده ورودی، تأیید شده است.

برای پیچیده تر کردن کار برای دیدگان کنجکاو، تمام تراکنش های Epic Cash با CT پوشانده شده و سپس با هم مخلوط می شوند تا ارتباطات بین طرفهای تراکنش پنهان شود. این کار از طریق ایده دوم Maxwell، یعنی **Coinjoin** انجام میشود.

برای توضیح ساده تر CoinJoin، تصور کنید که A و B و C به ترتیب Epic را به، X Y و Z ارسال می کنند.اگر از طریق CoinJoin ارسال شده باشند، تمام آنچه که مشخص است این است که A و B و C در حال ارسال هستند و X و Y و Z دریافت می کنند، در حالی که مبلغ تراکنش غیرقابل رؤیت است. سیستم CoinJoin از طریق One-Way Aggregate Signatures (OWAS) که همه تراکنش های درون یک بلاک را در یک تراکنش واحد انجام می دهد، برای Epic Cash ضروری است.

حریم خصوصی: خلاصه

بلاکچین Epic Cash از حریم خصوصی افراد و تراکنش های آنها محافظت می کند:

- ***پروتکل Dandelion++*** **– مسیرهای دیجیتال یک تراکنش را از آدرس IPفرستنده تراکنش جدا می کند؛**
- **حذف آدرس های کیف پول - هیچ شناسه موقعیت مکانی برای گاوصندوق های دیجیتالی درون بلاکچین وجود ندارد. تراکنش ها مستقیماً و به صورت شخص به شخص بر پایه کیف پول به کیف پول ایجاد میشوند.**
- ***CoinJoin*** **– تراکنش ها را در بسته هایی ترکیب میکند تا رابطه بین طرفین تراکنش را بپوشاند؛**
- **تراکنش های محرمانه - تراکنش ها را به چند قطعه تقسیم کرده و فاکتورهای کورکننده را در مجموعه این قطعات اضافه میکند، تامقادیر قطعات و سایر پارامترهای تراکنش مشخص نشود.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. تعویض پذیری

Charlie Lee , خالق Litecoin اظهار داشت که تعویض پذیری تنها ویژگی پول معمول است که در بیتکوین و لایتکوین وجود ندارد، و اذعان داشت که امنیت و تعویض پذیری زمینه تلاش های بعدی در این سکه ها هستند[6] . Andreas Antonopoulos, یکی از برجسته ترین متخصصان زمینه بلاکچین معتقد است "... سکه های آلوده تخریب کننده هستند. اگر تعویض پذیری و حریم خصوصی را از بین ببرید، ارز را از بین برده اید."[7]

تعویض پذیری خاصیت مجموعه ای از کالاها یا دارایی هاست که تضمین میکند واحدهای جداگانه آن مجموعه از ارزش مساوی بردخوردار بوده و قابل تعویض باشند. این همان چیزی است که اولین ارزها را از سیستم داد و ستد کالای پیش از خود متمایز میکند. بدون اعتمادبه تعویض پذیری پول، آن پول به‌سرعت کارایی خود را از دست میدهد. همانطور که در زیر نشان داده شده است، تعویض پذیری اکثر ارزرمزها قطعی نیست، در حالی که معماری معماری حریم خصوصی Epic Cash غیرقابل نفوذ بودن در برابر تهدیدات مشابه را تضمین میکند.

بیشتر ارزرمزهای مشابه بیت کوین را، به دلیل ماهیت بلاکچین های شفاف که بر روی آنها ساخته شده اند، می توان با اطمینان از هر کیف پولی که در آن نگهداری شده اند، ردیابی کرد. اشخاص ثالث مستقل و دولتها، بلاکچین بیت کوین را با ابزارهای پیچیده ای برای شناسایی سریع سکه های مورد استفاده در فعالیت های قبلی نظارت می کنند. این به طور طبیعی این نگرانی ها را به وجود می آورد که ممکن است روزی سکه های آلوده از معاملات منع شوند و دارندگان قانونمدار بعدی آنها ، دچار زیان شوند

در 19 مارس 2019، دفتر کنترل دارایی های خارجی آمریکا (OFAC) اعلام کرد در نظر دارد آدرس ارزهای دیجیتال را در لیست افراد با ملیت های خاص وارد کند (SDNs)، که اشخاصی هستند که افراد یا مشاغل آمریکایی از معامله با آنها منع شده اند. حتی نگران کننده تر این که OFAC وارد کردن آدرس هایی که اکنون آن سکه های آلوده را دارند به لیست SDN رد نکرده است، که صاحبان بیگناه سکه های آلوده را به دلیل ارتباط با سکه های آلوده ای که دارند وارد لیست سیاه مجرمانه میکند. این امر موجب شده است که Andrew Hinkes، استاد حقوقی دانشگاه نیویورک، از کنایه بوسه خداحافظی بر تعویض پذیری" و این که مردم باید انتظار برتری سکه های تازه استخراج شده یا سکه هایی که تمیز بودن آنها تایید شده است..."[8] را داشته باشند.

با در نظر گرفتن این تحولات، تصور رنج بردن از یک آشفتگی در بازار دور از ذهن نیست. با این حال، Epic یکی از معدود ارزهای رمزنگاری شده است که به دلیل ویژگی های محرمانگی قوی که قبلاً در این مقاله اشاره شد، از این مشکل جلوگیری می کند. با از بین بردن پیوند بین هویت و مالکیت و رابطه بین طرفهای تراکنش، Epic هرگز نمی تواند به یک شخص یا یک فعالیت نسبت داده شود. به این ترتیب ، ارزش Epic از کاربران خود مستقل باقی میماند و درجه بالایی از حریم خصوصی و امنیت را ممکن میکند که توسط بازیگران مخرب در عرصه های جنایی، مالی یا سیاسی به راحتی قابل تخریب و دستکاری نیست.

> **"... سکه های آلوده مخرب هستند. اگر تعویض پذیری و حریم خصوصی را از بین ببرید، ارز را از بین میبرید."**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. مقیاس پذیری

Epic Cash یک پیاده سازی MimbleWimble است که پیشرفت هایی را در زمینه مقیاس پذیری در نتیجه طراحی کارآمد فضا که داده تراکنش تکراری را حذف میکند موجب میشود. عملکرد Cut-Through که مسئولیت این امر را بر عهده دارد تمضین می دهد که این بلاکچین برخلاف اکثر ارزهای رمزپایه ، از جمله بیتکوین ، به مرور زمان ا ز لحاظ فضایی کارآمدتر میشود و گره های جدید را می توان با حداقل سرمایه گذاری در حافظه و قدرت محاسبه کامپیوتری ایجاد کرد. با کارآمد نگه داشتن فضا، یک شبکه گسترده پراکنده را ایجاد می کند و عدم تمرکز را تقویت می کند. علاوه بر این، در حالی که هر گره بیت کوین باید کل زنجیره را ذخیره کند، گره هایEpic Cash قادر به کمک به امنیت شبکه بر اساس یک زیر مجموعه کوچک از بلوک ها هستند.

اکثر ارزرمزها نیاز به ذخیره نامحدود کلیه داده های تراکنش در بلاکچین های خود دارند. در حال حاضر هر روز 0.1353 گیگابایت حافظه به زنجیره بیت کوین افـزوده میشود، در حالی که زنجیره اتریوم با سرعتی بیشتر یعنی 0.2719 گیگابایت در روز افزایش می یابد. اگر زنجیره بیت کوین با سرعت فعلی خود رشد کند، تا زمانی که آخرین بلوک پاداش آن در سال 2140 استخراج شود، سرانجام به اندازه تقریبی 6ترابایت خواهد رسید. اتریوم تا آن تاریخ از 10 ترابایت بیشتر خواهد شد[9]. در اکثر بلاکچین ها بدون MimbleWimble، تراکنش ها باید توسط گره ها در سرتاسر جهان تأیید شوند. با افزایش داده ها، بار هر گره نیز افزایش می یابد. حتی با تنها 200گیگابایت (انـدازه تقریبی زنجیره فعلی بیتکوین) ، همگام سازی داده ها به یک شبکه پایدار و دیسک با سرعت بالای خواندن و نوشتن نیاز دارد.

در نتیجه، استخراج به طور فزاینده ای در میان استخرهای بزرگ که از منابع محاسباتی پرهزینه استفاده می کنند متمرکز میشود. **اگر قرار بود کل تاریخچه بلاکچین بیتکوین روی بلاکچین Epic Cash ذخیره شود، تقریباً روی 90% فضای کمتر جای می گیرد.** کوچکتر سریعتر است زیـرا هر تراکنش برای انتقال و ایمن شدن به زمان کمتری نیا ز دارد. MimbleWimble این معضل ذخیره سازی را با یک روش خلاقانه هرس بلوک، که به آن "Cut-Through"گفته می شود، حل می کند. برای درک اینکه چگونه Cut-Throughکار می کند، بهتر است ابتدا به چگونگی تشکیل تراکنش ها و بلاک ها در یک بلاکچین MimbleWimble نگاهی بیندازیم.

ورودی:

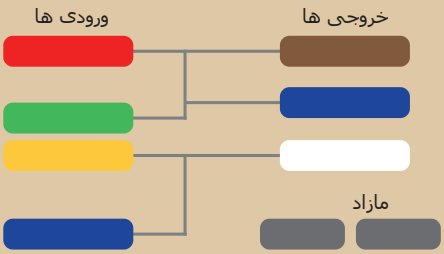
ارجاع به خروجی های قدیمی؛

خروجی:

خروجی **تراکنش های محرمانه** و **تأییدکننده های دامنده**؛

مازاد:

اختلاف بین خروجی ها و ورودی ها, به اضافه **امضاها** (برای تأیید اعتبار و اثبات عدم تورم)



شکل 2 :
بخش های تراکنش MimbleWimble

[9] Li, Crypto, *Blockchain's Big Data Problem,* 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

تمام بلاک های Epic Cash شامل:

یک لیست از مقادیر اضافه و امضاها.

درخت های مرکل از خروجی های تراکنش و تأیید کننده های دامنه؛

درخت های مرکل از ورودی های تراکنش؛

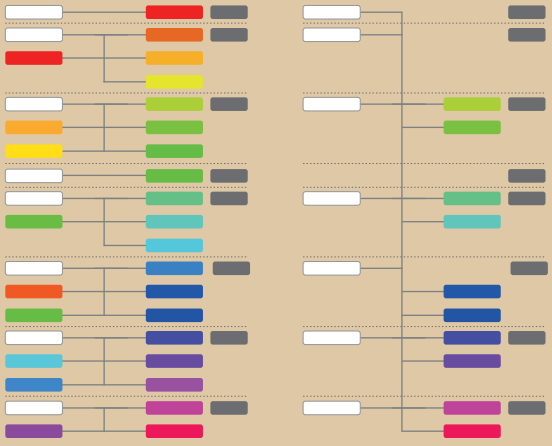
در شکل های 2 و 3 ، اقتباس گرفته از ارائه های Andrew Polestra[10] ، می توانیم Epic تازه استخراج شده را با خانه های ورودی سفید رنگ ببینیم. سلولهای با رنگ مشابه نشانگر خروجی هایی با ورودی های خرج شده مشابه هستند. با استفاده از فرآیندCut-Through ، ورودی ها و خروجی های خرج شده مرتبط با آن برای آزاد کردن فضای بلاک، حذف میوشند، که باعث کاهش میزان داده های لازم برای ذخیره سازی در بلاکچین می شود. در حالی که تراکنش ها از دفتر کل حذف شده اند ، باقی هسته های اضافی (تنها 100 بایت) برای همیشه ثبت میکند که تراکنش انجام شده است.

همچنانکه بلوکها به وجود می آیند، MimbleWimble فرایند CutThrough را در سراسر بلوکها اعمال می کند، به طوری که در دراز مدت تمام چیزی که باقی می مانند سرآیندهای بلوک (تقریباً 250 بایت)، تراکنش های خرج نشده و هسته های تراکنش (تقریباً 100 بایت) هستند. Grin، دومین پیاده سازی MimbleWimble که قرار است راه اندازی شود، نشان داد که یک زنجیره MimbleWimble با تعداد مشابهی از تراکنش ها نسبت به زنجیره بیتکوین نزدیک به 10 ٪ اندازه زنجیره بیتکوین خواهد بود.[11] علاوه بر این، اندازه یک گره "با اندازه چند گیگابایت برای زنجیره ای در مقیاس بیتکوین، و به طور بالقوه قابلیت بهینه سازی تا چند مگابایت" را خواهد داشت.[12]

این در تقابلی واضح با بیتکوین است، که در آن باید کل بلاکچین توسط هر گره ذخیره شود. با گذشت زمان، با افزایش راندمان فضایی بلاکچین Epic Cash نسبت به بلاکچین بیتکوین ، به همین ترتیب راندمان هزینه مشارکت گره ها در شبکه Epi Cash نیز افزایش خواهد یافت. موانع کمتر برای مشارکت به اطمینان از تاب آوری اساسی در لایه گره طراحی شبکه کمک می کند.

Epic Cash از طریق اجرای MimbleWimble و هرس زنجیره با فرآیند Cut-Through، مقیاس پذیری را به روشی که غالباً توسط جامعه ارزرمزها نادیده گرفته شده، ارائه می دهد. این چیزی است که ماهیت بیت کوین و پروژه های مشابه را نمایش میدهد: عدم تمرکز. صرف نظر از اینکه یک سکه در هر ثانیه چند تراکنش را می تواند پردازش کند، اگر نتواند توسط یک شبکه گسترده و متنوع تحقق یابد، چه فایده ای خواهد داشت؟ اگر الزامات حافظه به گونه ای باشد که اعتبارسنجی در نهایت به سمت گروه های استخراجی قدرتمند کشیده شود، آنگاه همه تلاش های جامعه ارزرمزها برای ایجاد یک اکوسیستم غیر متمرکز از بین میرود. برای تأمین توان اضافی، اجرای یک لایه سبک لایتنینگ 2 به عنوان یک هدف کوتاه مدت در نقشه راه توسعه Epic Cash برنامه ریزی شده است.

تراکنش های اضافی غربال میشوند



شکل 3 :
تراکنش های MimbleWimble
قبل و بعد از Cut-Through.

[10] SF Bitcoin Developers, *MimbleWimble with Andrew Poelstra,* 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, *Grin Blockchain Size,* December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, *Introduction to Mimblewimble and Grin,* 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

۷. سیاست پولی

سیاست پولی Epic Cash و بیتکوین بسیار مشابه است. موجودی در گردش Epic Cash ابتدا با سرعت افزایش میابد و سپس با موجودی در گردش بیتکوین در سال 2028 همگام میشود. از آن پس با شتاب رو به کاهشی افزایش میابد تا به حداکثر موجودی 21 میلیون Epic در سال 2140 برسد. Epic Cash دارای ویژگی هایی برای تبدیل شدن به یک ذخیره امن در طولانی مدت است زیرا موجودی در گردش در هر نقطه در طول چرخه انتشار آن مشخص است و در یک موجودی حداکثری مشخص به اوج خود می رسد. سیاست پولی Epic Cash با چهار ویژگی زیر مشخص می شود:

- موجودی در گردش Epic و نرخ انتشار آن بامقادیر بیتکوین درEpic Singularity در حدود 24 می 2028 همزمان می شوند. پس از Singularity، نرخ انتشار با شتاب کاهش میابد، در حالی که موجودی در گردش با شتاب کاهنده ای افزایش میابد؛
- انتشار سریع طی نه سال اول عمر خود، که طی آن 20,343,750 Epic (یعنی 96.875% از کل موجودی) استخراج می شود. میزان دقیق انتشار در بخش برنامه انتشار این مقاله مشخص شده است ؛
- Epic دارای ساختار تقسیم تا 8 عدد اعشار است ، به گونه ای که: 1 Epic برابر با 100،000،000 فریمن است (دقیقاً همانطور که 1 بیت کوین برابر با 100،000،000 ساتوشی است)؛
- عرضه 21 میلیون Epic در سال 2140 به آخرین حد خود خواهد رسید، تقریباً همزمان با رسیدن بیتکوین به موجودی حداکثر 21 میلیون واحدی خود؛

سیاست پولی Epic Cash به دلایل زیر به پیروی از بیتکوین مدل شده است:

- در ده سال گذشته از زمان آغاز به کار بیتکوین، مردم با مدل بیتکوین و سابقه اثبات شده آن آشنا هستند. Epic با همگام سازی تقریبی با موجودی در گردش بیت کوین و با تقلید از میزان حداکثر موجودی و ساختار تقسیم پذیر بیتکوین، مسیر کمترین مقاومت در قبال پذیرش عموم را پیش می گیرد.
- موافق بودن با اصول اقتصادی بیتکوین، یعنی کمیابی و قابل پیش بینی بودن موجودی در گردش که زمینه ویژگی های ذخیره ارزش قدرتمند آن است.

VI. برنامه انتشار

Epic Cash در کل دارای 33 دوره استخراج است که هریک از آنها با کاهش در پاداش بلوک نسبت به دوره قبل خود مشخص شده است. Epic Genesis تاریخی که بلوک شماره #1 Epic استخراج شود، در تاریخ 1 آگوست 2019 روی میدهد. بلوکها یک بلوک در دقیقه استخراج میشوند. پنج دوره اول نزدیک به 97٪ از حداکثر میزان موجودی Epic را تولید می کند، که 20 سال از تولید بیت کوین را تقریباً در 9 سال پوشش میدهد. این را می توان فرصتی برای "بازگرداندن ساعت" برای کسانی دانست که از رشد تماشایی بیتکوین غافل مانده اند.

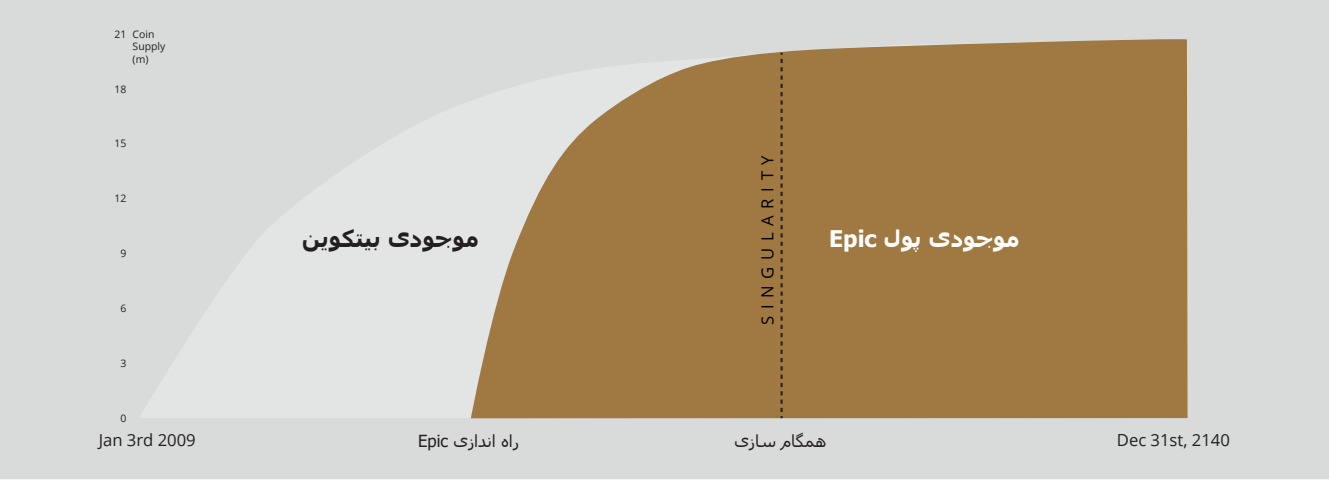
برنامه انتشار در جدول 1، تاریخ شروع و پایان هفت دوره اول استخراج، پاداش بلوک مربوط به آنها، و پس از آن موجودی در گردش برای هر دوره را تشریح می کند. برای اختصار، دوره های 8تا 33در جدول درج نشده اند. برای آن دوره ها کافی است بدانید که هر دوره دقیقاً مانند بیت کوین نصف پاداش دوره قبلی خود را خواهد داشت. میزان Epic منتشر شده در هر یک از این دوره ها، مجموع پاداش های بلوک در دوره 4 ساله (تقریبا 1460 روز) خواهد بود.

در Epic Singularity در سال 2028، موجودی در گردش Epic از موجودی در گردش بیتکوین عبور میکند، که در این مرحله Epic Cash الگوی پاداش بلوک بیتکوین halving آن را به کار میگیرد، که در آن هر چهار سال پاداش بلوک نصف میشود. تنها استثناء این است که بلوک های Epic همچنان یکی در هر دقیقه، در مقابل نرخ بیت کوین یک بلوک در هر ده دقیقه، استخراج میشوند. با این کار، موجودی در گردش Epic تقریباً با موجودی در گردش بیت کوین برای باقی زمان وجودشان، برابر میمانند.

جدول 1: برنامه انتشار هفت دوره اول استخراج. داده ها تقریب نزدیک هستند.

دوره	1	2	3	4	5	SINGULARITY	6	7
پاداش بلوک	16	8	4	2	1		0.15625	0.078125
روز شروع	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
روز پایان	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
طول (به روز)	334	470	601	800	1019		1460	1460
موجودی شروع	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
موجودی پایان	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% از بیشترین موجودی	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

شکل 4: برنامه انتشار Epic و بیتکوین



VII. استخراج

بلاکچین Epic Cash با پذیرا بودن از طیف گسترده ای از سخت افزارهای محاسباتی، عدم تمرکز را دنبال می کند. استخراج Epic از ابتدا برای CPU ها GPUs و ASICs ها با استفاده از سه الگوریتم مربوط به الگوریتم هشینگ: ProgPow ، RandomX و CuckATOo31 + موجود است. الگوریتم ها می توانند بدون نیاز به هیچ گونه کاستی در زمینه یکپارچگی شبکه، به سادگی تعویض شوند.

1 RandomX و CPU ها

RandomX یک الگوریتم Proof-of-Work (اثبات کار) بهینه سازی شده برای CPU های همه منظوره است. برای رسیدن به اهداف زیر از اجرای برنامه تصادفی با تکنیک های memory-hard استفاده میکند:

- جلوگیری از توسعه ASIC های تک تراشه ای؛
- به حداقل رساندن برتری راندمان سخت افزارهای تخصصی بر CPUهای همه منظوره.

استخراج Epic با CPU ها نیازمند تخصیص پیوسته 2 گیگابات حافظه فیزیکی RAM و 16 کیلوبایت از حافظه نهان L1 و 256 کیلوبات از حافظه نهان 2L و 2 مگابایت از حافظه نهان L3 برای هر نخ استخراج است[13]. دستگاه های با ویندوز 10 نیازمند 8 گیابایت یا بیشتر رم هستند. غیر قابل تصور که در آینده ای نه چندان دور تلفن های همراه گره های استخراج مناسبی شوند. استفاده ابتدایی از CPU یک فرصت عالی برای بسیاری با قدرت پردازشی متوسط است تا با کمک به امن کردن شبکه Epic Cash پاداش بلوک کسب کنند.

2 ProgPow و GPU ها

Proof-of-Work قابل برنامه نویسی (ProgPow) الگوریتمی است که به پهنای باند حافظه و قدرت محاسباتی هسته در توالی های ریاضی تصادفی بستگی دارد، که از بسیاری از ویژگی های محاسباتی GPU استفاده می کند و از این طریق به طور موثر از کل هزینه انرژی سخت افزار استفاده میکند. از آنجا که ProgPow به طور خاص برای بهره وری کامل ازGPU ها طراحی شده است، دستیابی به راندمان های قابل توجهی بالاتر، از طریق سخت افزارهای تخصصی، هم دشوار و هم گران است. به همین ترتیب، الگوریتم ProgPow انگیزه برای استخرهای بزرگ ASICرا برای پیشی گرفتن از GPU ها کاهش می دهد، همانطور که اغلب در بسیاری از الگوریتم های PoW دیگر ، مانند SHA-256 'بیت کوین' مشاهده می شود. با توسعه فن آوری های شرکت های بزرگ،NVidia وAMD ، پردازنده های گرافیکی قادر به پردازش موازی نتایج استخراج تا چندین برابر بیشتر از CPU ها با معیار سنجش برای یک دستگاه هستند. با توجه به موجودیت گسترده و قدرت پردازشی بالا، GPU ها پشتوانه بسیاری از فعالیت های استخراج را در دوره های اولیه، همانطور که در جدول 2 نشان داده شده است، فراهم می کنند.

3 CuckATOo+31 و ASIC ها

CuckATOo31+ یک الگوریم ASIC دوست است که تغییر یافته الگوریتم Coocko Cycle است که توسط مهندس کامپیوتر آلمانی،John Tromp ، توسعه داده شده است. یک مشابه CuckARoo29که در برابر ASIC مقاوم است، + CuckATOo31بوده که به صورت تصادفی گراف های دوبخشی تولید میکند و به استخراج کننده ها کار یافتن حلقه هایی با طول "N" که از نقطه های آن گرف عبور میکنند را میدهد.

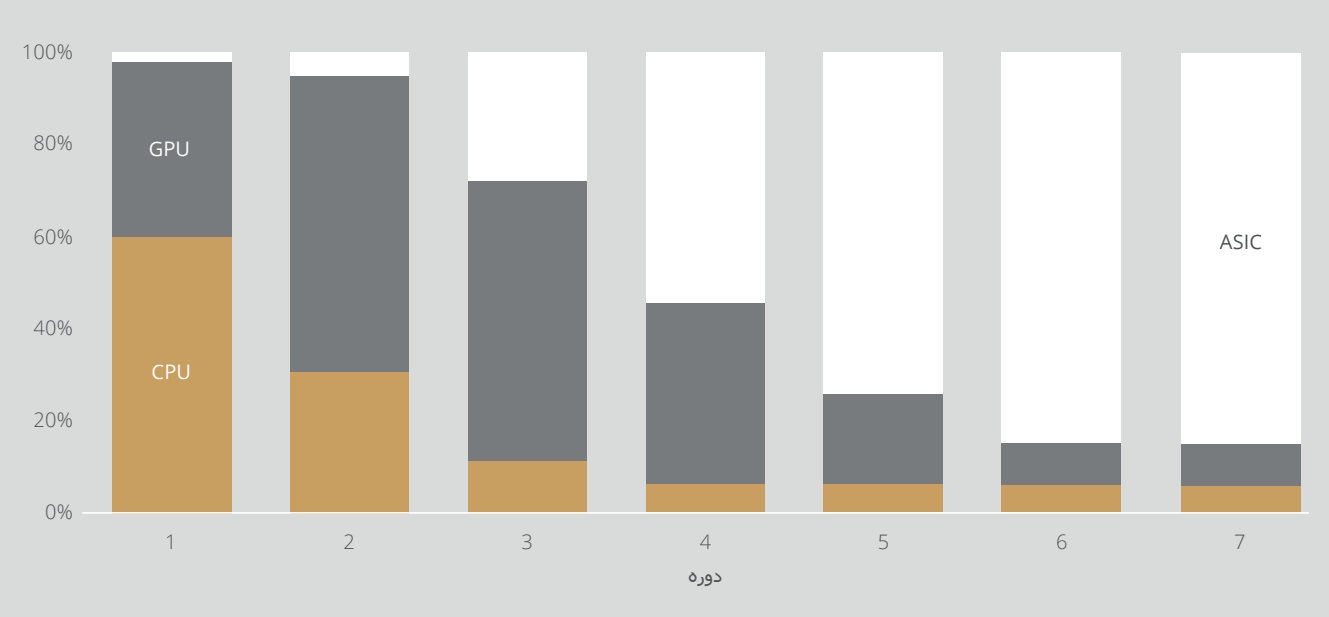
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

این وظیفه ای است محدود به حافظه، به این معنی که زمان حل مسئله به جای وابستگی مطلق به سرعت پردازنده یا GPU، به پهنای باند حافظه محدود می شود. در نتیجه، الگوریتم های Cuckoo Cycle گرمای کمتری تولید می کنند و نسبت به الگوریتم های مرسوم WoP انرژی کمتری مصرف می کنند. الگوریتم ASIC دوست + CuckATOO31 با استفاده از صدها مگابایت SRAM می تواند باعث بهبود کارایی در GPU ها شود در حالی که هنوز با محدودیت حافظه I/O در تنگنا قرار میگیرد[14]. در نهایت، ASIC ها از میان سه گزینه استخراج، بزرگترین پتانسیل اقتصادی در مقیاس بزرگ را ارائه می دهند. با این حال، به خاطر همه گیر شدن، هرچند که به آنها در ابتدا بخش کوچکی از پاداش های استخراج نسبت به CPU ها و GPU ها اختصاص داده می شود، در نهایت ASIC ها، بر فرض وجود اکوسیستم رقابتی تولید کنندگان دستگاه برای +CuckATOO31، اکثریت پاداش بلوک های استخراج شده را به خود اختصاص میدهند.

جدول 2: تخصیص پاداش استخراج. مشمول بازبینی. تخصیص ها جهت دستیابی به حداکثر عدم تمرکز و مطابق با منافع بلند مدت شبکه هدایت می شود.

دوره	1	2	3	4	5	6	7
روزها	334	470	601	800	1019	1460	1460
CPUها	60%	30%	10%	5%	5%	5%	5%
GPUها	38%	65%	62%	40%	20%	10%	10%
ASICها	2%	5%	28%	55%	75%	85%	85%

شکل 5: تخصیص پاداش استخراج هر دوره بر اساس جدول 2. مشمول بازبینی.



[14] Le Sceller, Quentin, *An Introduction to Grin Proof-of-Work,* 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 کمک های حاصل از استخراج

با شروع کار (2019) Epic Genesisو نتیجه گیری در (2028) Epic Singularity، در طی فرآیند استخراج، بخشی از Epic وجود دارد که به شکل سهم مشارکتی استخراج به بنیاد Epic Blockchain تخصیص میابد .

بنیاد EPIC Blockchain به توسعه فنی و ارتقاء آگاهی و کاربرد پروژه Epic Cash در سالهای اولیه آغاز به کار خود، با ایجاد فعالیتهای بازاریابی و توسعه مشارکت ها در صنعت فناوری مالی، میپر دازد.

پس از Singularity ، نقش بنیاد EPIC توسط EPIC Distributed Autonomous Corporation (EDAC) دنبال میشود، که توسط بنیاد، قبل از واگذاری توسعه داده میشود. بنیاد EPIC Blockchain با درصدی از پاداش های استخراج، که از پاداش های بلوک کسر خواهد شود، بر اساس نرخ سالانه زیر، پشتیبانی میشود:

جدول 3: نرخ سالانه کمک های استخراج به بنیاد به صورت درصد از پاداش استخراج

سال	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% از پاداش استخراج	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. نتیجه گیر ی

Epic قصد دارد به عنوان "نقره دیجیتال غیرمتمرکز" شناخته شود، وسیله ای برای داد و ستد مانند جایگاه شناخته شده بیت کوین به عنوان طلای دیجیتال غیر متمرکز. با بازگرداندن خاصیت قابل تعویض بودن از دست رفته بر روی بنیان سخت افزاری بسیار انرژی کارآمدتر و سازگار با محیط زیست، Epic Cash کفه ترازوی قدرت را به سوی کاربران شخصی سنگین میکند، در تضاد کامل با روندهای متمرکز اخیر. ترکیبی از اقتصاد بیتکوین ، تئوری بازی و فرمول اثبات شده proof-of-work با بهترین فن آوری های بلاکچین روز منجر به یک ارز بدون نیاز به اعتماد، غیرقابل دستکاری و غیرمتمرکز (Epic) می شود که مقیاس پذیر، تعویض پذیر بوده و از حریم خصوصی کاربران خود محافظت می کند. بلاکچین Epic Cash باز، عمومی، بدون مرز و مقاوم در برابر سانسور است.از حریم خصوصی و ثروت کاربران خود حفاظت کرده و به افرادی که سخت افزار خود را برای پشتیبانی از شبکه از طریق استخراج به کار میبرند، پاداش می دهد. هرEpic از طریق اثبات کار استخراج می شود. عرضه از صفر شروع می شود و شبکه به صورت عادلانه راه اندازی می شود، با یک شبکه آزمایشی که در حال حاظر در حال اجراست .

حقایق کلیدی Epic Cash:

- **استخراج از 1 آگوست 2019 آغاز میشود .**
- **بلاکچین Epic Cash بر اساس MimbleWimble ساخته شده است**

ویژگی های تعیین کننده پروتکل شامل موارد زیر هستند:

1. **Cut-Through**– حذف اطلاعات اضافی از بلاکچین به منظور ارتقاء بهره وری در فضا، تشویق مشارکت گسترده در اعتبا رسنجی شبکه و عدم تمرکز نظارت شده؛
2. ***CoinJoin*** – بسته بندی تراکنش ها در یک بلوک برای اطمینان از قابلیت تعویض پذیری ارزرمز Epic ؛
3. ***پروتکلDandelion++*** – انتشار تراکنش ها با برقراری ارتباط از طریق کانالهای درهم تنیده، و پخش در شبکه گسترده ای از گره ها، قطع ارتباط تراکنش ها و منشأ آنها ؛
4. **بدون آدرس کیف پول** – استفاده از یک طراحی بزرگ چند امضایی برای تولید کلیدهای خصوصی یکبار استفاده برای طرفین تراکنش، از بین بردن نیاز به آدرسهای کیف پول به طور کامل.

- **سیاست پولی Epic Cash** به منظور همگام سازی موجودی در گردشEpic با موجودی در گردش بیتکوین در تقریباً نه سال و رسیدن به همان حداکثر موجودی 21 میلیون واحد همزمان با بیتکوین، در سال 20140 طراحی شده است. این سیاست کاهش تورم شفافیت،پیش بینی پذیری موجودی و کمبیابی را تضمین میکند و ارزش ذخیره را در طولانی مدت تقویت میکند.

- **استخراج** که از CPUها, GPUها, و ASIC ها از طریق الگوریتم های RandomX, ProgPow, و +CuckATo31 برای سرعت بخشیدن به پذیرش عمومی و کارایی شبکه، استفاده میکند.

IX. مشخصات فنی

نام پروژه: Epic Cash
نام ارز: Epic
زمان بلوک: 60 ثانیه
سایز بلوک: 1 مگابایت
موجودی در شروع: 0
موجودی در پایان: 21,000,000
بلوک آغازین: 1 آگوست 2019
اجماع :(RandomX (CPUs), ProgPow (GPUs) and CuckATOO31+ (ASICs

پیوندها :

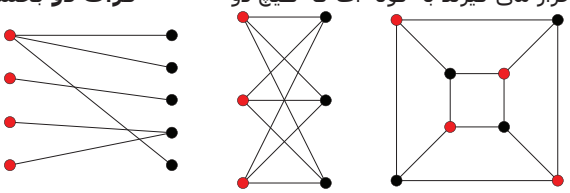
www.epic.tech

t.me/EpicCash – تلگرام

X. واژه نامه

ASIC مدارهای متجمع با کاربرد خاص؛ تراشه هایی که برای هدف واحدی طراحی شده اند

گراف دو بخشی مجموعه ای از رئوس های گراف که در دو مجموعه جداگانه قرار می گیرند به گونه ای که هیچ دو راس گراف در یک مجموعه در مجاورت یکدیگر نباشند.[15]



فاکتور کورکننده یک عنصر تصادفی که برای تسهیل رمزگذاری در یک پیام دیجیتالی گنجانده شده است. یک راز مشترک بین دو طرف که ورودی ها و خروجی های آن تراکنش خاص و همچنین کلیدهای عمومی و خصوصی طرف های تراکنش کننده را رمزگذاری می کند[16]

پاداش بلوک Epic جدید توزیع شده توسط شبکه به عنوان پاداش محاسبات انجام شده برای تأیید تراکنشهای یک بلوک جدید

حافظه نهان یک سخت افزار یا یک مؤلفه نرم افزاری که داده ها را ذخیره می کند تا درخواست های آینده بتوانند سریع تر پاسخ داده شوند.

موجودی در گردش میزان cipE موجود در هر لحظه از زمان

CPU واحد پردازنده مرکزی: مؤلفه کامپیوتری که مسئول تفسیر و اجرای بیشتر دستورات سایر سخت افزارها و نرم افزار رایانه است.

Cut-Through یک فرآیند بلاکچین **MimbleWimble** که به موجب آن ورودی ها و خروجی های خرج شده مرتبط با آن برای آزاد کردن فضای داخل بلوک حذف می شوند و باعث کاهش مقدار داده های مورد نیاز برای ذخیره در بلاکچین می شوند.

تمرکز زدایی میزان پراکندگی عملیات ها و نحوه اداره شبکه

انتشار تولید Epic جدید که توسط استخراج کنندگان به صورت پاداش بلوک به دست آمده است. هر 60 ثانیه با تأیید تراکنش ها در بلاکچین ایجاد می شود .

Epic Singularity نقطه ای که در آن موجودی در گردش Epic با موجودی در گردش بیتکوین (می 2028) همگام میشود.

مازاد (MimbleWimble) تفاوت میان ورودی ها و خروجی ها و امضاها (برای تأیید هویت و اثبات عدم تورم)

تعویض پذیری خاصیت یک کالا یا دارایی است که اساساً واحدهای مجزای آن قابل تعویض هستند و هر یک از قسمت های آن از قسمت دیگر غیر قابل تشخیص است

پیدایش (رویداد) استخراج اولین Epic و شروع رسمی این بلاکچین

GPU واحد پردازش گرافیکی: واحدی که شامل یک تراشه منطقی قابل برنامه ریزی)پردازنده(است که برای عملکرهای صفحه نمایش تخصیص یافته است. GPU های عمومی می توانند برای استخراج ارزرمز مناسب باشند.

Halving (برای بیتکوین) هر 4 سال اتفاق می افتد. میزان عرضه پس از هر رویداد، 50 درصد کاهش می یابد.

Hash مقدار محاسبه شده با عملکرد هش از یک عدد ورودی پایه .

الگوریتم Hashing (عملکرد) الگوریتم ریاضی که داده های با اندازه دلخواه را به هشی با اندازه ثابت که برای تولید و تأیید امضاهای دیجیتالی، کدهای تأیید صحت پیام (MAC) و سایر روش های تأیید اعتبار استفاده می شود، نگاشت می کند.

Homomorphic Encryption روشی برای انجام محاسبات بر روی اطلاعات رمزگذاری شده ، بدون رمزگشایی در ابتدا.

تغییر ناپذ یری (در برنامه نویسی) وضعیتی که یک شیء پس از ایجاد آن نمی تواند تغییر داده شود.

ورودی (MimbleWimble) مؤلفه یک تراکنش MimbleWimble نماینده سمت فرستنده تراکنش؛ تولید شده از خروجی تراکنش های قبلی.

I/O ورودی/خروجی؛ ارتباط بین یک سیستم پردازش اطلاعات مانند کامپیوتر و دنیای خارج، احتمالاً یک انسان یا سیستم های پردازش اطلاعات دیگر.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

حداکثر موجودی مقدار Epic ای که باید به آن حد رسید تا بعد از آن، موجوی در گردش افزایش نیابد(Epic 21،000،000) .

Memory-Hard استفاده زیاد از رم برای جلوگیری از تلاشها برای اتصالات همزمان در حالت موازی. توابع hard-memory (حافظه سخت) الگوریتم هایی هستند که زمان محاسبه در درجه اول توسط حافظه موجود برای نگهداری داده ها تعیین میشود. همچنین با عنوان توابع memory-bound (مرتبط باحافظه) شناخته می شود.

درخت مرکل ساختار داده ای که در کاربردهای علوم رایانه استفاده می شود. در بلاکچین ها، درختان مرکل امکان تأیید کارامد و امن ساختار داده های بزرگ را امکان پذیر می سازد.

MimbleWimble یک پروتکل ارائه شده توسط یک مشارکت کننده ناشناس ،که با نام Tom Elvis Jedusor در اتاق چت توسعه دهندگان بیتکوین‌شناخته میشود.

چند امضاء یک طرح امضای دیجیتالی که به گروهی از کاربران امکان می دهد یک سند واحد را امضا کنند. معمولاً یک الگوریتم چند امضاء یک امضای مشترک تولید می کند که فشرده تر از مجموعه ای از امضاهای مجزا از همه کاربران است[17].

گره رایانه ای که برای توزیع اطلاعات مربوط به تراکنش ها و بلوک ها، به روش نظیر به نظیر، به یک شبکه بلاکچین متصل می شود و به سایر گره های درون شبکه انشعاب میابد.

One Way Aggregate Signature (OWAS) امضای یک تراکنش متشکل از بسیاری از امضاها که به شکلی رمزگذاری شده اند، که محاسبه امضاهای جداگانه که بخشی از مجموعه هستند بسیار دشوار است.

خروجی (MimbleWimble) مؤلفه یک تراکنش MimbleWimble نماینده سمت گیرنده تراکنش؛ برای ورودی تراکنش های بعدی استفاده میشود.

Pedersen Commitment Scheme یک رمزنگاری بدوی است که به یک تأیید کننده اجازه می دهد تا به یک مقدار انتخاب شده از قبل بدون فاش کردن هیچ اطلاعاتی درباره آن و بدون آنکه بتواند بعداً تعهدش به آن مقدار را تکذیب کند، متعهد شود.

کلید خصوصی یک کلید خصوصی تکه کد کوچکی است که با یک کلید عمومی جفت شده است تا الگوریتم های رمزگذاری و رمزگشایی متن را آغاز کند. به عنوان بخشی از رمزنگاری کلید عمومی در طی رمزگذاری نامتقارن ایجاد شده، و برای رمزگشایی و تبدیل پیام به یک قالب قابل خواندن، استفاده می شود.

Proof of Work (PoW) تکه داده ای که تولید آن دشوار (پرهزینه و وقت گیر) است، اما بررسی آن برای دیگران آسان است و شرایط خاصی را برآورده می کند. Proof of Work (اثبات کار) اغلب در تولید بلوک ارزرمز استفاده می شود.

کلید عمومی یک کلید عمومی در پنهان نگاری به روش رمزنگاری کلید عمومی تولید می شود که از الگوریتم های رمزگذاری کلید نامتقارن استفاده می کند. از کلیدهای عمومی برای تبدیل پیام به یک قالب غیرقابل خواندن استفاده می شود.

RAM (حافظه با دستیابی تصادفی) تراشه های ذخیره داده با دسترسی سریع در یک دستگاه محاسباتی که در آن سیستم عامل (OS)، برنامه های کاربردی و داده های در حال استفاده نگه داشته میشوند تا بتوانند به سرعت توسط پردازنده دستگاه قابل دسترسی باشند.

تأیید کننده دامنه اعتبارسنجی تعهد که تأیید می کند که مقدار ورودی های تراکنش بزرگتر از مقدار خروجی های تراکنش است و اینکه همه مقادیر تراکنش ها مثبت است. تأیید کننده دامنه تضمین میکند که میزان ذخیره پولی دستکاری نشده است.

(دیجیتال) امضاء یک بخش استاندارد از پروتکل بلاکچین، که عمدتاً برای تأمین امنیت تراکنش ها و بلوک های تراکنش ها ، انتقال اطلاعات ، مدیریت قرارداد و موارد دیگری مورد استفاده قرار می گیرد که در آن تشخیص و جلوگیری از هرگونه دستکاری خارجی مهم است. آنها سه مزیت برای ذخیره و انتقال اطلاعات در بلاکچین را ارائه می دهند:

- اگر در اطلاعات ارسالی دستکاری شده باشد فاش‌میکنند ؛
- مشارکت یک طرف خاص در تراکنش راتأیید میکند ؛
- میتواند از لحاظ قانونی الزام آور باشد.

SRAM (حافظه با دستیابی تصادفی ایستا) حافظه (RAM) با دسترسی تصادفی که بیت داده ها را تا زمانی برق داشته باشد، حفظ میکند.

توان خروجی میزان تراکنش ها در ثانیه است که می تواند توسط یک پروتکل خاص ارزرمز انجام شود. کیفیت

عدم نیاز به اعتماد یک شبکه ارزرمز برای پیروی از قوانین یک پروتکل بدون فشار از سوی یک بخش مرکزی.

[17] Bellare, Mihir, Neven, Gregory, 2007, *Identity-based Multi-signatures from RSA*, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH