بیت کوین چیست؟

همه چیز از سال ۲۰۰۸ و انتشار مقاله‌ای که نوعی پول الکترونیک به نام بیت کوین در آن معرفی شده بود آغاز شد. هویت ناشناسی به نام **ساتوشی ناکاموتو** آغازگر انقلابی بود که سال‌ها بعد به تیتر اول رسانه‌ها تبدیل شد و اقتصاددانان را به بحث‌های نظری گسترده درباره آن وادار کرد.

بیت کوین بر خلاف پول‌های امروزی که عرضه و توزیع آن‌ها در اختیار دولت‌هاست، در کنترل هیچ فرد، گروه و یا سازمان خاصی نیست. افرادی که وارد شبکه این ارز دیجیتال می‌شوند، باید قوانین مربوط به شبکه را بپذیرند. این قوانین به صورت کدهای برنامه‌نویسی است که در اینترنت توسط همه قابل مشاهده است.

«Bitcoin»نخستین ارز دیجیتالی است. هیچ‌کس نمی‌داند که چه کسی آن را ساخته است. البته این موضوع تازه‌ای نیست. چون بیشتر ارزهای دیجیتالی در سکوت تولید می‌شوند.

گفته می‌شود که سازنده بیت کوین، فردی به نام «ساتوشی ناکوموتو» (Satoshi Nakomoto) است. دقیقا مشخص نیست که ساتوشی ناکوموتو واقعا یک فرد است یا گروهی از افراد تحت این نام، اقدام به تولید Bitcoin کرده‌اند.

بیت کوین یک دارایی دیجیتال است که بر بستر شبکه بلاک چین پیاده‌سازی شده است. **بلاک چین** یک سیستم به اشتراک گذاری اطلاعات است که همه افراد حاضر در آن شبکه به این اطلاعات که در دفتر کل نگه‌داری می‌شوند دسترسی دارند.

در سیستم بانکداری فقط بانک از نقل و انتقال دارایی و تمام جزئیات آن باخبر می‌شود، اما در بلاک چین این اطلاعات در دفتر کل مرکزی که همه به آن دسترسی دارند ثبت می‌شود.

در هر اشتراک‌گذاری کد فرستنده، کد گیرنده و مبلغ ارسالی مشخص می‌شود، در دفتر ثبت می‌گردد و تا ابد امکان رجوع به آن وجود دارد. حجم فعلی دفتر Bitcoin به بیش از ۳۲۰ گیگابایت رسیده است.

هر کیف پول یک سیستم امنیتی قوی دارد که از دو کد تشکیل شده است، یک کلید **خصوصی و یک کلید عمومی**. هر تراکنشی که در شبکه رمزارزها انجام می‌شود با کلید خصوصی شما که بر اساس یک سیستم رمزنگاری خیلی قوی تولید شده است، امضا می‌گردد.

توجه داشته باشید فقط شما به کلید خصوصی دسترسی دارید ولی هنگامی که تراکنش در دفتر مرکزی ثبت شود، افراد می‌توانند آن تراکنش را بر اساس کلید عمومی مشاهده کنند.

کلید خصوصی و کلید عمومی

در هر کیف پول دیجیتالی یک کلید خصوصی و یک کلید عمومی وجود دارد.کلید خصوصی را نمایانگر یک رمز ارز می دانند .یعنی هر کلید خصوصی نشان دهنده یک ارز دیجیتال است.کلید خصوصی باعث حفظ امنیت ارزهای دیجیتال می شود به این صورت که دسترسی افراد دیگر به سرمایه شما را از بین می برد.کلید عمومی در واقع همان آدرس ولت دیجیتالی شما است.اما باید بدانید کلید عمومی از روی کلید خصوصی ساخته می شود.با استفاده از کلید خصوصی است که شما می توانید موجودی ولت خود را برداشت کنید یا انتقال دهید .بنابراین بخاطر داشته باشید که حفظ و نگهداری کلید خصوصی از اهمیت ویژه ای برخوردار است.

یک کلید خصوصی یک شکل پیچیده از رمزنگاری است، در واقع یک سری اعداد و حروف است که باعث می شود هکرها نتوانند آن را هک کنند .کلید خصوصی عضوی جدایی نا پذیر از بیت کوین و Altcoinاست و در مقابل سرقت و دسترسی غیرمجاز به صندوق ها کاربرها را کمک می کند.

این کلید همواره با یک کلید عمومی همراه است تا الگوریتم های رمزگذاری و رمزنگاری متن را تنظیم کند. به عنوان بخشی از رمزنگاری کلید عمومی در حین رمزگذاری کلید نامتقارن ایجاد شده و برای رمزگشایی و تبدیل پیام به یک قالب قابل خواندن استفاده می شود.

این رمزارز روی شبکه بلاکچین که با استفاده از پروتکل‌هایی خاص، امنیت آن تضمین می‌شود کار می‌کند. نودها (چه نودهای معمولی و چه ماینرها) با پیروی از یک سری دستورات خاص به تایید یا رد تراکنش می‌پردازند. همچنین نودهای استخراج‌کننده یا ماینر، نقش اساسی در امنیت شبکه دارند.

بر خلاف ارزهای فیات(کاغذی) رایج در کشورها، ارز دیجیتال، تحت نظارت هیچ سازمان یا دولتی نیست. می‌توان این ویژگی را به طور همزمان، نقطه قوت و ضعف آن به شمار آورد. چون به دلیل نبود نظارت بر این سیستم، گزینه‌ای مناسب برای کلاه‌برداری به شمار می‌رود؛ کما اینکه تا به امروز بارها این اتفاق افتاده است.

نود بیت کوین چیست؟

شبکه بلاک چین، یک تکنولوژی غیرمتمرکز است که هیچ دولت، سازمان یا شخصی بر آن نظارت ندارد. علی‌رغم تمام مزایای این سیستم بدون یک نهاد نظارتی سنجش اعتبار عملیاتی که در شبکه انجام می‌شود ممکن است مختل شوند.

نودها (Nodeدر شبکه بلاک چین بیت کوین نقش همان نهاد نظارتی را بر عهده دارند؛ اما از آنجایی که تکنولوژی بلاک چین، غیرمتمرکز است تمام سیستم‌های متصل در شبکه این کار را انجام می‌دهند و نظارت فقط تحت اختیار یک شخص یا سازمان نیست.

نودها – هر کامپیوتری که به طور مستقیم به شبکه متصل شود و دفتر کل را دریافت کند – در شبکه بلاکچین وظیفه کسب اطمینان از تمرکززدایی و همچنین تبدیل بلاکچین به یک بستر امن برای تراکنش‌ها در شبکه را به عهده دارند.

برای اینکه نودها بتوانند در نظارت و تایید تراکنش‌ها نقشی داشته باشند باید برنامه مربوطه را روی سیستم خود نصب کنند و به سایر نودها یا سیستم‌های متصل در شبکه وصل شوند تا شبکه بتواند از قدرت سیستم آنها برای اعتبارسنجی و تایید تراکنش‌ها کمک بگیرند.

مثال

اگر شخص x بخواهد در شبکه، تراکنشی انجام دهد – مثلا یک واحد از این رمزارز را به شخص y بفرستد – باید درخواست خود را به شبکه اعلام کند. نودها تراکنش را دریافت کرده، آن را ثبت می‌کنند و سپس به نودهای اطراف خود می‌فرستند.

اما نودها به جز ارسال تراکنش به نودهای اطراف باید صحت تراکنش دریافتی را بسنجند؛ مثلا اگر شخص x بخواهد ۲ واحد اتریوم به شخص y ارسال کند ولی دارایی او فقط یک واحد اتریوم باشد، نودها این تراکنش را به عنوان یک تراکنش معیوب شناسایی می‌کنند و این تراکنش انجام نخواهد شد.

برای این کار نودها باید به سابقه تراکنش‌ها مراجعه کنند. فردی که درخواست تراکنش ارسال یک واحد اتریوم را دارد با پیوند تراکنش‌های قبلی خود به شبکه ثابت می‌کند که موجودی او حداقل یک واحد اتریوم است.

بررسی میزان دارایی مورد نیاز یک بار توسط کیف‌پول شخص ارسال‌کننده تراکنش و یک بار توسط نودها انجام می‌شود

بلاک چین چیست؟

نگهداری توزیع شده اطلاعات تراکنش‌ها در بیت کوین، به وسیله فناوری بلاک چین ممکن شده است. بلاک چین به زبان ساده، یک دفترچه یادداشت دیجیتال است که اطلاعات آن به صورت غیرقابل تغییر بین همه نودها توزیع شده است. بلاک چین مفهومی گسترده‌تر از بیت کوین است که می‌تواند کاربردهای دیگری هم داشته باشد. اگر بخواهیم خیلی ساده این تفاوت را نشان بدهیم، بلاک چین را می‌توانیم به اینترنت و بیت کوین را به موتور جستجوی معروفی مانند گوگل تشبیه کنیم.

به دلیل وجود بلاک چین، نودها تاریخچه‌های تراکنش را پیش خود نگه می‌دارند. زمانی که یکی از آن‌ها بخواهد مقداری بیت کوین به دیگری بفرستد، با ارسال درخواست خود در قالب تراکنش، نودها دفترچه‌های دیجیتالی‌شان را ورق می‌زنند و موجودی فرستنده را به دست می‌آورند تا از امکان‌پذیر بودن انجام این تراکنش اطمینان حاصل کنند. دفترچه دیجیتالی نودها از برگه‌هایی تشکیل شده که در بلاک چین آن‌ها را با نام بلاک می‌شناسیم و درون آن‌ها اطلاعات و داده‌ها قرار می‌گیرند. در صورتی که تراکنش با قوانین شبکه مغایرتی نداشته باشد، تراکنش معتبر شناخته می‌شود و همانند خط تولیدی یک کارخانه منتظر وارد شدن به مرحله بعدی، یعنی فرایند تایید تراکنش می‌شود.

استخراج

هدف ماینرها دسترسی به بیت کوین‌های استخراج نشده و البته ایجاد امنیت در شبکه است. ماینرها با تولید بلاک‌هایی از تراکنش‌های معتبر و اتصال آن به بلاکچین، پاداش دریافت می‌کنند. برای اینکه از ایجاد بلاک‌های متعدد و دستکاری شبکه جلوگیری شود، فقط نودهایی که ماینر هستند حق ساخت بلاک را دارند.

سیستم Bitcoin به این صورت طراحی شده است که برای هر بلاک با کمک تابع درهم‌ساز هش‌نگار یک مسئله ریاضی ایجاد می‌کند. هر کدام از ماینرها که بتوانند زودتر به جواب این مسئله برسند مفتخر به اضافه کردن بلاک به انتهای زنجیره می‌شوند.

یک نود در شبکه، کامپیوتر قدرتمندی است که نرم‌افزار بیت کوین را اجرا کرده، در روند انتقال اطلاعات مشارکت می‌کند و به این ترتیب به حفظ شبکه بیت کوین کمک می‌کند.

نودها می‌توانند ماینر یا همان استخراج‌کننده باشند یا فقط به وسیله اشتراک گذاری سیستم خود در حفظ امنیت شبکه و تایید تراکنش‌ها نقش داشته باشند.

در ابتدای پیدایش این رمزارز، همه‌ی نودها به عنوان ماینر عمل می‌کردند. با گذشت زمان و سخت‌تر شدن کار، نودهای ماینر با استفاده از کارت‌های گرافیک سعی داشتند در رقابت پیروز شوند، اما رفته‌رفته کارت‌های گرافیک نیز از پس عملیات استخراج بر نیامدند.

نودهای ماینر مجبور شدند برای استخراج از دستگاه‌های سخت‌افزاری خاصی که فقط برای استخراج تولید شده بودند استفاده کنند.

مروزه رقابت بر سر استخراج بسیار سخت شده است. حتی افرادی که دستگاه‌های سخت‌افزاری قوی هم داشتند اکنون شانس چندانی برای رقابت ندارند. از این رو شاهد پیدایش استخرهای استخراج هستیم. در واقع، ماینرها با اشتراک‌گذاری قدرت هش خود می‌پذیرند که با دریافت سود کمتر، شانس‌شان را برای دریافت سود، افزایش دهند.

برای فعالیت به عنوان ماینر باید به قدرت هش‌ریت دستگاه ماینر توجه کرد. این بدان معنی است که دستگاه ماینر شما قدرت حدس زدن چند جواب را در یک ثانیه دارد؟

مورد بعدی که باید به آن توجه کرد این است که توان مصرفی دستگاه ماینر شما چند وات است؟

قیمت برق در کشوری که زندگی می‌کنید هم جز مواردی است که در هنگام تصمیم‌گیری برای فعالیت در این حوزه باید به آن‌ها توجه داشته باشید.

البته اگر می‌خواهید در استخر استخراج فعالیت کنید باید به کارمزدی که استخر از شما مطالبه می‌کند نیز توجه داشته باشید.

هر ۱۰ دقیقه یک بلاک جدید ایجاد می‌شود. اگر قدرت هش یک دستگاه ماینر آن‌قدر بالا باشد که بتواند مثلا در ۶ دقیقه جواب مسئله را پیدا کند، در شبکه بی‌نظمی ایجاد می‌شود. به همین دلیل سختی شبکه در شبکه بیت کوین تعبیه شد.

شبکه با سنجش قدرت پردازش ماینرهای حاضر در آن تقریبا هر ۲ هفته یک بار سختی را به‌روزرسانی می‌کند.

بیت کوین چه مزیت‌هایی دارد؟

شفاف است

دیجیتالی بودن

امنیت بالایی دارد

غیرمتمرکز است

سرعت بالا و کارمزد کم

تضمین انجام تراکنش

شفاف است

تمام تراکنش‌های این رمزارز در دفترکلی که همه به اطلاعات آن دسترسی دارند ثبت می‌شود. هر کیف پول یک کلید خصوصی و یک کلید عمومی دارد. کلید عمومی در تراکنش‌های ثبت شده قابل مشاهده است. با مراجعه به دفترکل مرکزی می‌توان میزان دارایی را مشاهده کرد.

امنیت بالایی دارد

این رمزارز روی شبکه بلاکچین که با استفاده از پروتکل‌هایی خاص، امنیت آن تضمین می‌شود کار می‌کند. نودها (چه نودهای معمولی و چه ماینرها) با پیروی از یک سری دستورات خاص به تایید یا رد تراکنش می‌پردازند. همچنین نودهای استخراج‌کننده یا ماینر، نقش اساسی در امنیت شبکه دارند.

غیرمتمرکز است

بر خلاف ارزهای فیات رایج در کشورها، ارز دیجیتال، تحت نظارت هیچ سازمان یا دولتی نیست. می‌توان این ویژگی را به طور همزمان، نقطه قوت و ضعف آن به شمار آورد. چون به دلیل نبود نظارت بر این سیستم، گزینه‌ای مناسب برای کلاه‌برداری به شمار می‌رود؛ کما اینکه تا به امروز بارها این اتفاق افتاده است.

سرعت بالا و کارمزد کم

نقل و انتقال دارایی توسط این رمزارز در مدت زمان کوتاهی انجام می‌شود. این در حالی است که اگر تجار بخواهند به صورت بین‌المللی نقل و انتقالات مالی داشته باشند باید چند روز منتظر بمانند.

گذشته از این، کارمزد انتقال ارزهای دیجیتال، بسیار کمتر از انتقال ارزهای فیات است. البته با افزایش سختی شبکه، کارمزد ارزهای رمزنگاری شده هم روندی صعودی به خود گرفته است.

تضمین انجام تراکنش

تراکنش‌های صورت گرفته در شبکه بیت کوین به هیچ عنوان لغو نمی‌شوند. به همین دلیل اگر شما رمزارز خود را اشتباها به شخصی که نمی‌شناسید بفرستید دیگر امکان برگشت ارزهای دیجیتالی شما وجود ندارد. ولی اگر فرد را بشناسید تنها با ارسال مجدد فرد، ارزهای شما بازگردانده می‌شوند.

دیجیتالی بودن

Bitcoin یک ارز کاملا مجازی است که معادل فیزیکی ندارد. به همین دلیل برای ذخیره آن به فضای خاصی نیاز ندارید.

چه عواملی بر قیمت بیت کوین تاثیر می‌گذارند؟

عرضه و تقاضا

فورک

هاوینگ

قوانین رگولاتوری

رویدادهای سیاسی

رسانه اجتماعی

عرضه و تقاضا

در هر ارز، کالا و خدمات، اگر تقاضا زیاد باشد قیمت آن نیز افزایش پیدا می‌کند. از سال ۲۰۱۷ که افراد بیشتری با بلاکچین و کاربرد آن آشنا شدند، افراد بیشتری خواهان این ارز دیجیتال شدند. همین موضوع باعث شد که قیمت آن به دلیل تقاضای بیشتر بالا رود.

فورک

«فورک» نیز از عواملی است که بر تمام رمزارزهای پیاده شده بر بستر بلاک چین تاثیر می‌گذارد.

در بسیاری از مواقع به دارندگان کیف‌پولی خاص پس از انجام فورک گفته می‌شود که اگر مقداری خاص از « «Bitcoinرا داشته باشید، مقداری از بیتکوین‌کش نیز به شما تعلق می‌گیرد.

همین موضوع باعث می‌شود که افراد، دارایی ارز دیجیتال خود را افزایش دهند یا حتی اگر هیچ موجودی ندارند اقدام به خرید کنند. البته موارد استثنا نیز وجود دارد.

هاوینگ

هاوینگ یا نصف شدن پاداش استخراج هر چهار سال که باعث ایجاد تورم منفی می‌شود بر قیمت این رمزارز موثر است. در ابتدا پاداش استخراج ۵۰ واحد بود، سپس ۲۵ و بعد به ۵/۱۲ رسید و در اردیبهشت سال ۹۹ به ۲۵/۶ واحد رسید. این مورد باز هم به داستان عرضه و تقاضا اشاره دارد. بیت کوین روز به روز شناخته شده‌تر می‌شود، افراد بیشتری آن می‌پذیرند و خواهان آن هستند. از طرف دیگر با گذشت زمان، عرضه آن کم و کمتر می‌شود و همین موضوع باعث بالاتر رفتن قیمتش می‌شود.

قوانین رگولاتوری

اینکه دولت‌ها در قبال بیت کوین چه سیاستی را اتخاذ کنند می‌تواند تاثیر به‌سزایی بر قیمت آن داشته باشد. مواردی همچون «گرفتن مجوز برای ورود ماینر» و به طور کلی مقبولیت رمزارزها از طرف دولت بر قیمت آنها تاثیر می‌گذارد.

رویدادهای سیاسی

هیچ‌وقت فراموش نکنید که پول ترسو است و به دنبال یک جای امن می‌گردد. مثلا امروز در بورس است، فردا در طلا و بعد هم در بازار کریپتوکارنسی. عبارتی به نام «اسمارت مانی» یا «پول هوشمند» در اقتصاد وجود دارد که می‌گوید «پول هوشمند در اوج بازار گاوی از آن خارج شده و به بازاری می‌رود که هنوز رشد خود را آغاز نکرده است

دارندگان پول هوشمند با تحلیل‌های درستی که از اتفاقات سیاسی دارند خیلی زودتر از افراد عادی می‌توانند تاثیر اتفاقات سیاسی همچون روابط کشورها با هم را تحلیل کرده و به این ترتیب روی ارزش رمزارزها تاثیرگذار باشند.

رسانه اجتماعی

رسانه‌های اجتماعی همچون «ردیت»، «توئیتر» و ... نیز بر قیمت رمزارزها تاثیرگذار هستند. زمانی که تعداد توئیت‌ها در رابطه با بیت کوین بالا می‌رود احتمالا باید منتظر تاثیر آن توئیت‌ها بر قیمت باشیم. بسته به اینکه توئیت‌ها منفی یا مثبت باشند می‌توانند قیمت را افزایش یا کاهش دهند.

همچنین با بررسی «گوگل ترندز» می‌توان دریافت که کاربران گوگل به چه میزان رمزارزها را جستجو کرده‌اند. وقتی میزان جستجو زیاد شود یعنی می‌توان احتمال داد که منابع مالی زیادی وارد این بازار می‌شوند.

معایب کار با بیت کوین

دخالت احتمالی دولت ها

بدون پشتوانه مالی

هیچ راهی برای برگرداندن بیت کوین از دست رفته شما وجود ندارد

محدودیت در تعداد تراکنش های هم زمان

دخالت احتمالی دولت ها

یکی از مزیت‌های بیت کوین عدم دخالت هیچ دولتی در فرآیند تراکنش‌ها و ارزش‌گذاری‌های آن است؛ اما برخی مواقع دولت‌ها می‌توانند به یک مانع تبدیل شوند. برای مثال در چند وقت اخیر دولت آمریکا به شدت از طریق صرافی‌های بیت کوین به دنبال افراد نقل‌وانتقال دهنده پول در این شبکه بوده است. از طرفی برخی دولت‌ها هم خریدوفروش بیت کوین را ممنوع اعلام نموده‌اند. البته هنوز دولت ایران عکس‌العملی برای ممنوعیت این شبکه مالی در کشور نداشته است.

بدون پشتوانه مالی

نداشتن پشتوانه مالی و عدم حاکمیت پولی در سیستم کاری بیت کوین، هم می‌تواند یک مزیت بزرگ باشد و هم تبدیل به یک اشکال بارز در آن شود. ارزش فعلی این ارز دیجیتال روی میزان عرضه و تقاضا و اعتماد مردم به ارزش ذاتی آن برای سرمایه‌گذاری پایه‌گذاری شده است. اگر تنها یک نفر در دنیا ادعای هک کردن این شبکه را داشته باشد، در عرض چند دقیقه بیت کوین تمام ارزش خود را از دست خواهد داد.

هیچ راهی برای برگرداندن بیت کوین از دست رفته شما وجود ندارد

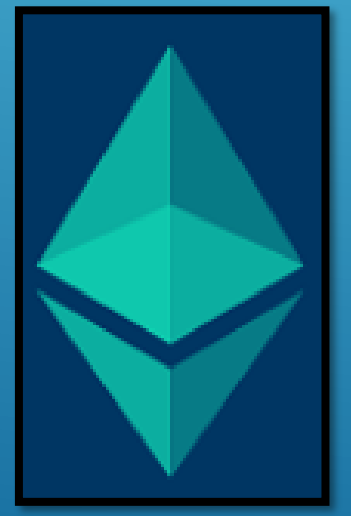
این هم یکی از معایبی است که بسیاری از افراد و متخصصین برای نحوه کار بیت کوین برشمرده‌اند. در حساب‌های بانکی اگر شما رمز کارت خود را فراموش کرده و یا حتی آن را گم کنید، تنها با یک مراجعه ساده به بانک همه چیز به حالت عادی برمی‌گردد. اگر شما کیف پول دیجیتالی یا الکترونیکی خود را به هر دلیلی گم کنید، رمز شناسایی بیت کوین خود را فراموش نمایید و یا اشتباهاً بیت کوین خود را به یک آدرس اشتباهی بفرستید، هیچ راهی برای برگشت بیت کوین ازدست‌رفته وجود نخواهد داشت. زیرا اصلاً مرکزی برای رسیدگی به این وضعیت‌ها وجود ندارد. البته وجود چنین مرکزی با اصل و اساس نحوه کار بیت کوین نیز در تناقض است.

محدودیت در تعداد تراکنش های هم زمان

اگر تعداد افرادی که در آن واحد برای نقل‌وانتقال بیت کوین اقدام می‌نمایند، به شدت افزایش یابد، این روند می‌توانند در شبکه همتای بیت کوین سرعت فرآیندهای مالی را به شدت کاهش دهد. نحوه انتقال بیت کوین به این صورت است که هر نقل‌وانتقالی باید توسط یک شبکه بزرگ جهانی تائید گردد. روند دریافت این تأییدیه در این شرایط می‌تواند ساعت‌ها به طول انجامد.

اتریوم چیست؟

ETHEREUM



مقدمه

در ساده‌ترین تعریف، اتریوم یک زیرساخت آزاد مبتنی بر فناوری بلاک چین است که می‌توان روی آن برنامه‌های کامپیوتری غیرمتمرکز را اجرا کرد. غیرمتمرکز بودن اتریوم یعنی این سیستم به‌تنهایی متعلق به هیچ‌کس نیست و آن را یک یا چند شخص خاص کنترل نمی‌کنند. همه می‌توانند مالک این شبکه باشند و همه می‌توانند در کنترل آن نقش داشته باشند. به‌لطف ساختار توزیع‌شده و غیرمتمرکز اتریوم، پس از پیاده‌سازی یک برنامه روی شبکه اتریوم، این برنامه دیگر قابل‌توقف و دستکاری نیست، حتی اگر خود خالق آن بخواهد.

مقاله معرفی یا همان وایت پیپر این پروژه در سال ۲۰۱۳ منتشر شد و در سال ۲۰۱۵ رسماً شبکه اتریوم شروع به کار کرد. ایده‌ی اصلی این پروژه، یک جوان روسی – کانادایی به‌نام **ویتالیک بوترین** (Vitalik Buterin)است که از حامیان بیت کوین بود و با الهام از بیت کوین ایده «غیرمتمرکز کردنِ همه چیز» را ارائه داد.

بلاک چین اتریوم برای اجرای کدهای برنامه نویسی برنامه‌های غیرمتمرکز طراحی شده است. مانند بیت کوین، اتریوم نیز یک بلاک چین توزیع شده عمومی است. اگر چه تفاوت‌های فنی زیادی بین این دو وجود دارد اما مهمترین تفاوت این دو اهداف و قابلیت‌هایشان است. بیت کوین یک برنامه کاربردی خاص از فناوری بلاک چین است. در واقع بیت کوین با هدف ایجاد یک سیستم پرداخت جهانی، همتا به همتا و غیرمتمرکز ایجاد شده است. برای درک بیشتر این موضوع، بلاک چین بیت کوین را سیستم عاملی در نظر بگیرید که فقط یک نرم افزار به نام بیت کوین روی آن اجرا می‌شود. در نقطه مقابل، بلاک چین اتریوم را سیستم عاملی در نظر بگیرید که هزاران نرم افزار و سرویس مختلف می‌توانند روی آن فعالیت کنند. با این حساب، درک مفهوم «توکن» برایتان آسان‌تر خواهد شد. در واقع یک توکن، ارز برنامه‌ای غیرمتمرکز است که خودش بلاک چین خصوصی ندارد و از بلاک چین‌های دیگر مثل اتریوم استفاده می‌کند.

در بلاک چین اتریوم، ماینرها برای یک ارز دیجیتال رمزنگاری شده به نام «اتر» که شبکه را تامین می‌کند، کار می‌کنند. اتر یک ارز دیجیتال تجاری و قابل حمل است که برای پرداخت هزینه‌های تراکنش نرم افراز مورد نظر،

قرارداد هوشمند چیست؟

قرارداد هوشمند یا (smart contract) یک پروتکل است که از آن برای تنظیم قراردادها استفاده می‌شود. در واقع قرارداد هوشمند، یک پروتکل ویژه است که برای مشارکت، تأیید یا اجرای مفاد یک قرارداد خاص، فعال می‌شود. قراردادهای هوشمند، معامله‌ها و فرایندها را به صورت کاملا تضمینی و بدون حضور اشخاص ثالث انجام می‌دهند. فعالیت و ثبت‌های قرارداد هوشمند، قابل پیگیری و غیر قابل برگشت هستند. این قراردادها به طور خودکار، شامل تمام اطلاعات مربوط به شرایط قرارداد و اجرای تمام اقدامات هدف گذاری شده می‌شوند.

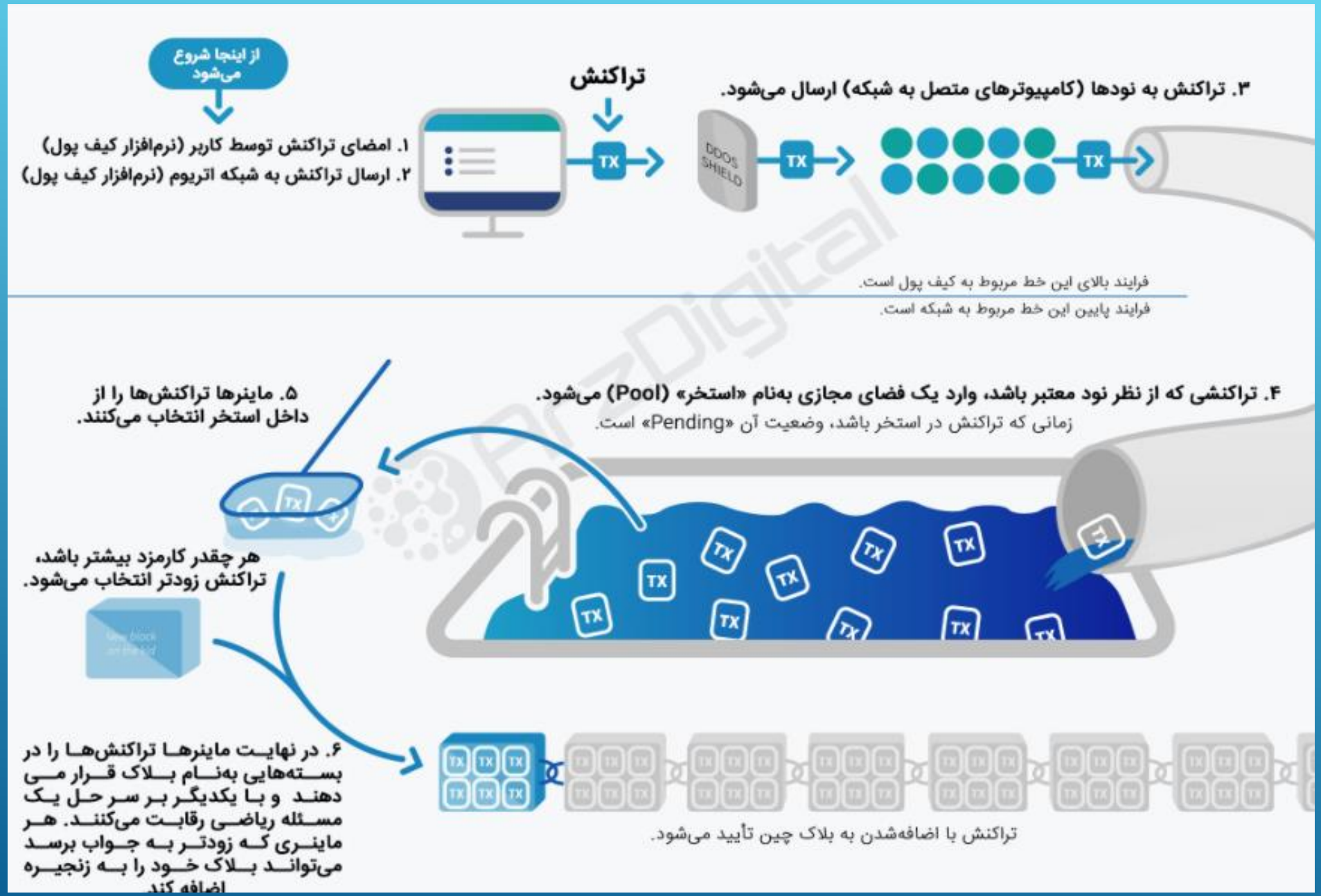
آنچه که باعث تفاوت قرارداد معمولی و قرارداد هوشمند می‌شود این است که در قراردادهای هوشمند کدهای کامپیوتری مشکل نیاز به اعتماد را برطرف می‌کنند. همان طور که گفتیم زمانی‌که یک قرارداد هوشمند بر روی یک بلاک چینِ آزاد مثل اتریوم اجرا شود، دیگر قابل‌توقف نیست و هیچ‌کس نمی‌تواند جلوی اجرای آن را بگیرد. با قراردادهای هوشمند می‌توان برنامه‌ها و پروژه‌هایی را ساخت که بدون هیچ‌گونه واسطه و از کارافتادگی به کار خود ادامه دهند، به‌طوری که حتی خودِ برنامه‌نویس قرارداد هوشمند هم نمی‌تواند کد قرارداد هوشمند ثبت‌شده در بلاک چین را تغییر دهد.

هوشمند

عادی

در حوزه معاملات مالی، ثبت سوابق، مالکیت دارایی، وثیقه، بیمه، تحقیقات علمی، پزشکی، انتخابات، توسعه محصول، زنجیره تأمین و در تمام زمینه‌هایی که بخواهیم نیاز به اعتماد را به حداقل برسانیم می‌توان از قراردادهای هوشمند اتریوم استفاده کرد. امروزه توسعه‌دهندگان می‌توانند با کمک قراردادهای هوشمند، بدون نیاز به ایجاد یک بلاک چین جدید، با استفاده از بلاک چین اتریوم پروژه‌های خود را بسازند و حتی برای آن ارز دیجیتال (توکن) ایجاد کنند. زبان برنامه‌نویسی قراردادهای هوشمند اتریوم **سالیدیتی** است

م چگونه کار میکند؟



ستخراج

ماینینگ با نام علمی اثبات کار (Proof Of Work)، یکی از روش‌های رایج برای اجماع و حفظ امنیت شبکه‌های بلاک چینی است. طبق این الگوریتم، فرایند ایجاد بلاک رقابتی است و هر کس بخواهد در کار ایجاد بلاک‌های حاوی تراکنش سهیم باشد باید با قدرت پردازش سخت‌افزارهای کامپیوتری یک معادله ریاضی پیچیده را حل کند. هر کس زودتر به جواب برسد، برنده این رقابت خواهد بود و پس از ایجاد بلاک پاداش دریافت می‌کند. این پاداش در شبکه اتریوم، ارز دیجیتال اتر است. ماینرها همچنین کارمزد تراکنش‌ها را دریافت می‌کنند.

بنابراین، ماینرها (یا همان نودهای ماینینگ) مقدار زیادی قدرت پردازش به شبکه اختصاص می‌دهند که با قدرت چند ابر کامپیوتر برابری می‌کند. در این صورت اگر کسی بخواهد به شبکه حمله کند و یا تغییری در بلاک چین دهد، مجبور است قدرت پردازشی بیشتر از نیمی از ماینرها را داشته باشد

هرچه تعداد ماینرها افزایش می‌یابد، امنیت شبکه هم بیشتر می‌شود و به این ترتیب، اعتماد به آن افزایش خواهد یافت.

در شبکه اتریوم تعیین شده است که هر ۱۴ ثانیه بلاک‌های جدید ساخته شود. حالا ممکن است به‌عنوان مثال یک ماینر قدرتمند وارد شبکه شود و بتواند جواب معادله بلاک‌ها را در ۵ ثانیه بیابد. در این حالت، شبکه معادله ریاضی را سخت‌تر می‌کند که به آن افزایش «سختی استخراج» می‌گوییم. در حالتی که هم که تعداد ماینرها کم شود، شبکه سختی استخراج را کاهش می‌دهد تا جواب معادله به‌طور میانگین در همان ۱۴ ثانیه پیدا شود.

گس (GAS) چیست؟

برای انجام هر تراکنش در شبکه اتریوم باید کارمزد پرداخت شود. گس (سوخت) همان کارمزد شبکه اتریوم است که به‌صورت اتر از کاربر دریافت می‌شود.

در مورد گس با دو مفهوم سروکار داریم:

گس لیمیت Gas limit

گس پرایس Gas price

برای انجام تراکنش، کاربر باید گس لیمیت مشخص کند. گس لیمیت مقدار سوختی است که کاربر حاضر است برای انجام یک عمل در شبکه پرداخت کند و وقتی به تنهایی صحبت از گس می‌شود، منظور همان گس لیمیت است.

اگر گس لیمیت کمتر از حد مشخصی تعیین شود، عملیات در شبکه انجام نخواهد شد. برای انجام یک تراکنش معمولی در اتریوم گس لیمیت باید حداقل ۲۱,۰۰۰ باشد، اما اجرای عملیات‌های اضافه نیازمند گس لیمیت متفاوت است. در صورتی که گس لیمیتی که کاربر مشخص کرده است، کافی نباشد، عملیات انجام نخواهد شد، اما در صورتی که گس لیمیت اضافی وارد شود، باقیمانده به کاربر بازمی‌گردد.

گس پرایس هم مقدار هزینه‌ای است که شما باید برای هر گس لیمیت پرداخت کنید. هزینه گس با اتر پرداخت می‌شود، اما چون این رقم بسیار پایین است با آن را با واحد « «Weiنمایش می‌دهند. هر ۱ Wei برابر است با ۰٫۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۱ اتر. شبکه اتریوم هر کس را آزاد می‌گذارد تا هر چقدر دوست دارد هزینه گس یا همان گس پرایس را تعیین کند، اما اگر گس پرایس شما بیش از اندازه پایین باشد، ماینرها تراکنش شما را تأیید نمی‌کنند و ترجیح می‌دهند تراکنش‌هایی را تأیید کنند که کارمزد بالاتری دارند. بنابراین، مقدار گس پرایس برای انجام عملیات، نسبت به شلوغی یا خلوتی شبکه می‌تواند متفاوت باشد.

ETH Fee = Gas limit × Gas Price

توکن ERC-20

استاندارد ERC-20 لیستی از قوانینی است که برای یک توکن باید در نظر گرفته شود تا بتواند روی اکوسیستم اتریوم ساخته شود.

پروژه‌های مختلفی که روی شبکه اتریوم فعالیت می‌کنند، با استفاده از امکان ERC-20می‌توانند توکن‌های خود را با نام و نماد دلخواه ایجاد کنند. هر کس امروز می‌تواند با پرداخت چند دلار کارمزد، توکن خاص خودش را بسازد، اما این توکن ارزشی ندارد چون موردمصرف و کاربردی برای آن تعیین نشده است. فقط وقتی این توکن‌ها ارزشمند می‌شوند که کاربرد داشته باشند و کسی حاضر باشد برای دریافت خدماتی، آن توکن را بخرد.

همچنین تیم توسعه پروژه‌های بلاک چینی می‌توانند قبل از راه‌اندازی بلاک چین مستقل خود، برای جذب سرمایه روی بلاک چین اتریوم توکن بسازند و در عرضه اولیه (ICO) پیش‌فروش کنند. سپس زمانی که شبکه اصلی و بلاک چین خود را ساختند، توکن‌های اتریومی را به بلاک چین خود انتقال دهند. به‌عنوان یکی از نمونه‌های بارز می‌توان به پروژه ترون اشاره کرد. این پروژه هم‌اکنون رقیب اتریوم است، اما قبل از راه‌اندازی شبکه اصلی خود، توکن‌های TRXرا روی بلاک چین اتریوم عرضه کرد و پس از مستقل‌شدن آنها را به شبکه ترون منتقل کرد.

پیدایش اتریوم کلاسیک

در اواسط ۲۰۱۵ اتریوم رسماً عرضه شد و تا اوایل ۲۰۱۶ برنامه‌های توسعه طبق نقشه راه به‌خوبی اجرا می‌شدند. اما ناگهان در ۱۷ ژوییه ۲۰۱۶، هکری موفق شد با استفاده از یک اشکال در کد یکی از برنامه‌های اجراشده روی اتریوم، با نام «DAO»، حدود ۳٫۶ میلیون واحد اتر را به سرقت ببرد که در آن ارزششان زمان معادل بیش از ۵۰ میلیون دلار بود و ۱۴٪ کل اترهای درگردش را شامل می‌شد.

به این نکته توجه داشته باشید که خود اتریوم هک نشده بود، بلکه تنها برنامه‌ای روی این شبکه موردحمله قرار گرفته بود. با این حال، به‌دلیل نوپابودن اتریوم و بالابودن مبلغ به‌سرقت‌رفته، تیم اتریوم در نهایت تصمیم گرفت با یک هارد فورک، مبالغ را بازگردانند. هارد فورک به‌معنای به‌روزرسانی گسترده (به‌نوعی تغییر قوانین) در بلاک چین است.

به‌عقیده گروه مخالف با هارد فورک، «کد قانون است» و نباید برای برگشت تراکنش‌ها، در بلاک چین تغییری ایجاد کرد. آنها معتقد بودند این کار ذات تمرکززدایی را زیر سؤال می‌برد. به‌همین دلیل در نتیجه هارد فورک، عده زیادی تصمیم گرفتند همچنان روی نسخه قبلی فعالیت کنند و به‌همین دلیل، اتریوم قبلی، اتریوم کلاسیک نام گرفت و هر کدام راه خود را رفتند.

اکنون اتریوم کلاسیک یک پروژه تقریباً رهاشده است و با فاصله زیادی از اتریوم، با کاهش قیمت شدید در رده‌های پایین بازار ارزهای دیجیتال قرار دارد. همچنین به‌دلیل فعالیت نکردن استخراج‌کنندگان به اندازه کافی بر روی این شبکه، تاکنون به آن چند حمله با خسارت‌های چندمیلیون دلاری انجام شده است. با این حال، عده زیادی همچنان معتقدند اتریوم کلاسیک، اتریوم واقعی است و امیدوار هستند دوباره به اوج برسد.

هارد فورک Hard Fork سافت فورک Soft Fork چیست ؟

در ارزهای رمزنگاری شده، فورک (fork)به تغییرات در زیر ساخت و قوانین کدهای یک رمز ارز گفته می‌شود که این اتفاق می‌تواند به صورت کلی (هارد فورک) و یا جزئی (سافت فورک) رخ دهد. در نوع هارد فورک، در عمل یک بلاک چین جدید ایجاد شده و بلاک‌های جدید با نودهای شبکه پیشین همخوانی ندارند ولی در نوع سافت فورک، این سازگاری وجود دارد

« فورک » اصطلاحی در برنامه‌نویسی است که به معنای بهینه سازی یک کد متن باز می‌باشد. کدهای فورک شده معمولا شبیه کدهای معمولی هستند اما اصلاحات مهمی در آن‌ها صورت گرفته و به صورت « شاخه‌های چنگال » به موازات یکدیگر عمل می‌کنند. گاهی برای آزمایش کردن یک فرآیند از فورک استفاده می‌شود اما فورک ها در زمینه رمز ارز ها اغلب برای اعمال تغییرات بنیادی استفاده می‌شوند و یا اینکه برای ایجاد دارایی جدیدی با مشخصات مشابه (اما نه یکسان) نسبت به دارایی اصلی به کار گرفته می‌شوند.

همه فورک ها تعمدی و ارادی نیستند. با وجود کد پایه متن باز که در پهنه‌ای گسترده توزیع شده است، در برخی موارد هنگامی‌که همه گره‌ها اطلاعات یکسانی را تکثیر نمی‌کنند، فورکی به صورت تصادفی به وجود می‌آید. استخراج‌کنندگان معمولا این فورک ها را شناسایی و رفع می‌کنند. با این وجود بیشتر فورک های موجود در رمز ارزها ناشی از اختلاف نظر بر سر ویژگی های ذاتی ایجاد شده‌اند.

به طور کلی در برنامه‌نویسی دو نوع فورک: سخت (هارد فورک) و نرم (سافت‌فورک) وجود دارد. هارد فورک تغییری در یک پروتکل است که باعث نامعتبر شدن نسخه‌های پیشین می‌شود. اگر نسخه‌های قبلی همچنان به اجرا درآیند، در نهایت پروتکل کاملا متفاوتی پیدا خواهند کرد و دیتای آن‌ها نسبت به نسخه جدید متفاوت خواهد شد. این مساله باعث سردرگمی‌شدید می‌شود و ممکن است به خطا بیانجامد. در بیت کوین، گاهی برای تعریف پارامترهایی همچون اندازه بلوک، دشواری مسائل رمزنگاری‌شده‌ای که نیاز به حل دارند، محدودیت اطلاعات اضافی قابل افزودن و غیره، لازم است از هارد فورک استفاده شود. بروزرسانی و ایجاد تغییر در هر یک از این قوانین باعث می‌شود بلوک‌ها از سوی یک پروتکل جدید پذیرفته شوند اما از سوی نسخه‌های قبلی رد شوند؛ در نتیجه مشکلات بزرگی ایجاد می‌شود که حتی ممکن است وجوه از دست بروند.

هارد فورک به این صورت بوده و معمولا با آشفتگی همراه است. هارد فورک ها ریسک زیادی هم دارند زیرا ممکن است بیت کوین های پرداخت شده در یک بلوک جدید امکان خرج شدن در یک بلوک قدیمی‌تر را داشته باشند

سافت فورک این قابلیت را دارد که همچنان با نسخه‌های قدیمی‌تر کار کند. برای نمونه اگر با اعمال قوانین سختگیرانه‌تر، یک پروتکل تغییر پیدا کند و تغییری کلی اعمال شود یا تابع جدیدی افزوده شود که به هیچ وجه روی ساختار تاثیر نمی‌گذارد، آنگاه بلوک‌های نسخه‌ی جدید توسط گره‌های نسخه‌ی قدیمی پذیرفته می‌شوند. عکس این روند امکان پذیر نیست و نسخه‌ی جدید که سختگیرانه‌تر است، بلوک‌های نسخه‌ی قدیمی را قبول نخواهد کرد. در بیت کوین، در حالت ایده آل استخراج‌کنندگان نسخه قدیمی متوجه می‌شوند که بلوک‌های آن‌ها رد شده است و در نتیجه خود را ارتقاء می‌دهند. هرچه استخراج‌کنندگان بیشتری به نسخه جدید ارتقاء پیدا کنند، زنجیره‌ی دارای بیشترین بلوک‌های جدید بلندتر می‌شود و در نتیجه کار بلوک‌های نسخه قدیمی مدام سخت‌تر شده و ماینرها به فکر ارتقاء می‌افتند و به این ترتیب سیستم خود را اصلاح می‌کند.
سافت فورک ها برخلاف هارد فورک ها فاقد ریسک خرج دوباره هستند، زیرا تریدرها و کاربرانی که با گره‌های قدیمی‌کار می‌کنند هر دو نوع بلوک نسخه قدیمی و جدید را می‌بینند.

آیاس یا EOS

مقدمه

ایاس جزء یکی از پروژه های موفق در دنیای رمز ارزها می باشد که با یک هدف مشابه به اتریوم، مانند اجرای قرارداد های هوشمند و برنامه های غیر متمرکز (DApps) ایجاد شده است

EOSپلتفرمی است که برای ساخت برنامه های غیر متمرکز طراحی شده است . این پلتفرم غیر متمرکز امکان استفاده از قرار داداهای هوشمند و DAppها را فراهم می کند ، که این امر این ارز دیجیتال را به یکی از رقبای اتریوم تبدیل کرده است . این سیستم عامل بلاک چین در تاریخ 31 ژانویه 2018 منتشر شد و در مدت بیش از چند سال ، سیزدهمین رتبه را در سایت CoinMarketCapکسب کرده است .

EOSادعا می کند قوی ترین زیر ساخت برای برنامه های غیر متمرکز است . اساسا ، EOSیک فناوری بلاکچین است که دقیقا شبیه به اتریوم است . آنها قصد دارند بلاکچین اختتصاصی خود را با لیست طولانی از ویژگی های چشمگیر ایجاد کنند

در واقع EOSبرنامه های بزرگی دارد . این نرم افزاری است که به عنوان یک سیستم عامل غیر متمرکز عمل خواهد کرد . سپس توسعه دهندگان می توانند برنامه ها را بر روی نرم افزار EOSبسازند . قابل توجه ترین ویژگی این ارز دیجیتال مقیاس پذیری افقی آن است ، این بدان معناست که که بلاکچین EOS قادر به اجرای موازی قراردادهای هوشمند و پردازش همزمان معاملات است .

تاریخچه

EOSجزئی از الگوریتم اثبات سهام و یا PoSاست که توسط شخص بنییان گذار Dan Larimerایجاد شده است. این سیستم کمتر متمرکز است و یا به اصطلاح از انرژی کمتری به مراتب استفاده می کند و فوق العاده سریع است . علاوه بر این ، هیچ کارمزدی در بلاکچین EOSوجود نخواهد داشت . این امر همچنین آنها را از رقابت جدا می کند و می تواند به آنها کمک کند تا از سیستم عامل خود استفاده گسترده تری کنند .

پروژه ارز دیجیتال ایاس توسط شرکتی به نام Black.Oneتاسیس شد. این شرکت توسط براندن بلومر، که در ابتدا یک پروژه معمولی با هدف جذب فناوری بلاکچین بود ،شروع به کار کرد.توسعه دهندگان این پروژه افرادی به نام های لیمر استوی (موسس استیم(و دانیل لارمیر (بنیان گذار بیت شیرز) هستند.

بلومر یک کار آفرین است که یکی از کارهای آن فروش سرمایه های مجازی برای بازی های ویدئویی است . لارمیر یک برنامه نویس نرم افزاری است که فعالیت های خود را در زمینه ارز دیجیتال شروع کرده است .

عرضه اولیه در سال 2017 توسط شرکت خصوصی Block.Oneشروع و تا سال 2018 ادامه داشت. وایت پیپر این ارز نیز در سال 2017 منتشر شد. طبق مقاله ای که در 1 ژوئن 2018 در مورد فروش اولیه سکه های ایاس در سایت خبرگذاری کوین تلگراف به انتشار رسیده، پروژه ایاس رکورد جذب سرمایه 4 میلیارد دلاری در مدت زمان یک سال را زده است.توکن های ایاس ابتدا بر روی شبکه اتریوم قرار داشته اند و این توکن ها در کیف پول اتریوم نیز ذخیره می شدند و در سال 2018 این توکن ها بر روی شبکه اصلی خودشان انتقال داده شدند.

1

متاسفانه ، برخی از متمایزترین ویژگی های EOS، ویژگی هایی است که منتقدان خاص کمترین علاقه را به آن دارند . برخی از آنها معتقدند که دخالت گسترده Block.Oneدر این پروژه به معنای متمرکز بودن آن است و برخی معتقدند که این مخالف آنچه بلاکچین ها و رمز ارزها برای دستیابی به آن بوده اند ، است .

به طور کلی از جمله ویژگی های این رمز ارز می توان به موارد زیر اشاره کرد :

1.مقیاس پذیری

2.انعطاف پذیری

3.پردازش چندگانه

این موارد از جمله اصلی ترین و عمده ترین ویژگی های این رمز ارز به شمار می روند .

کوین EOSروی بلاکچین EOSکار می کند و از الگوریتم اثبات سهام استفاده می کند . هرکسی می تواند از آن برای ایجاد قراردادهای هوشمند با عملکرد بالا استفاده کند . به عبارت دیگر ، EOSبه گونه ای طراحی شده است که برای کسب و کارها و کاربران ، کاربردی تر است و برنامه های مبتنی بر بلاکچین را به گونه ای کاربر پسندتر از اتریوم ایجاد می کند .

یکی از ایده های اصلی EOSایجاد برنامه های بلاکچین است که مانند برنامه های تحت وب کار می کنند . توجه داشته باشید که تا کنون برنامه های بلاکچین موفق به عملکرد یکسانی نشده اند و به اعتقاد آنها این امر باعث اتخاذ تصمیم عمومی می شود .

به علاوه ، EOSدارای یک حاکمیت غیرمتمرکز قانونی است . این یکی از اصلی ترین ویژگی هایی است که موسسان معتقدند برای ایجاد یک سیستم عادلانه بسیار حیاتی است . آنها ادعا می کنند که EOSبه غیر از مکانهایی که کوین EOSایجاد می شود ، غیرمتمرکز تر از بیت کوین و اتریوم است .ظاهرا بیت کوین توسط چهار استخر استخراج و اتریوم توسط دو استخر استخراج کنترل می شود . این بدان معنا می باشد که تقریبا تمام نیرو توسط این گروه ها کنترل می شوند . از طرف دیگر ، EOSدارای 21 ذینفع است که بلاک ساز هستند نه ماینر .

این امر تقسیم قدرت را به طور قابل توجهی انجام می دهد و باید منجر به ساختاری غیر متمرکز در حاکمیت شود. این نیز مهم است زیرا اگر این استخرهای استخراج از بین بروند ، می تواند تاثیر منفی بر روی ارزهای دیجیتال داشته باشد و اعتبار معامله را متوقف کند .

خصوصیات بلاکچین EOS

3

مقیاس پذیری : مقیاس پذیری بزرگترین مشکل در فضاهای مبتنی بر بلاکچین می باشد.
ویزا و پی پال به ترتیب ، 1600 و 200 تراکنش را در ثانیه انجام می دهند. در مقابل آنها بیت کوین با 8 تراکنش و اتریوم 20 تراکنش در ثانیه را تایید تراکنش می کنند.
ایاس مدعی آن است که با استفاده از DPOSیا همان مکانیسم توافق اثبات سهام، به سادگی می تواند میلیون ها تراکنش را در ثانیه تآیید کند.

نعطاف پذیری: بر اثر حمله DAO،سیستم اتریوم با مشکل مواجه شد و توسعه دهندگان ناچار به فورک شدند.به دلیل استفاده ایاس از DPOS، در صورت خرابی برنامه، سیستم اصلی به مشکل نخواهد خورد.

حاکمیت : حاکمیت با شکل گیری قابلیت و انتخاب قانون توسط خود جامعه در EOSانتخاب می شود. قوانینی که برای شبکه توسط اعضا تعیین می شود، همه توسعه دهندگان برای استفاده از پروتکل باید از آن استفاده کنند.

پردازش برابر و مساوی: دستورالعمل های برنامه در بین چند پردازنده، در پردازش مساوی تقسیم می شود. با به اجرا در آمدن این کار، زمان اجرای آن برنامه نیز کاهش چشمگیری می یابد. ارز دیجیتال ایاس با استفاده از ارتباط ناهمزمان، مقیاس پذیری و قابلیت همکاری، پردازش موازی (Smart Contracts)یا همان قراردادهای هوشمند را فراهم می کند.

مقیاس پذیری افقی: از آنجا که در مقیاس پذیری عمودی، با اضافه کردن قدرت پردازش بیشتر مقیاس پذیری انجام می شود، اما مقیاس پذیری افقی با تشکیل ظرفیت برای افزودن کامپیوتر و همچنین قدرت پردازش بیشتر ،شکل می گیرد.

قابلیت همکاری: به توانایی یک سیستم کامپیوتری برای تبادل و استفاده از اطلاعات می باشد.

سیستم عامل غیرمتمرکز: سیستم عامل غیر متمرکز از مهمترین ویژگی های رمز ارز EOSمی باشد. برای ارزهای دیجیتال سیستم عامل ویندوز و مک را تصور کنید. هم اکنون اتریوم یک ابر کامپیوتر غیرمتمرکز است ،همچنین EOS ادعا می کند که یک سیستم عامل غیرمتمرکز می باشد.

چند تفاوت عمده بین Ethereum و EOS

اتریوم و ایاس دو مورد از برجسته ترین پروژه های بلاکچین هستند . در حالی که اتریوم می خواهد محاسبات جهانی را غیر متمرکز کند ، هدف EOSاجرای سریع برنامه های غیر متمرکز و یا همان DAppهاست . برای دستیابی به این اهداف ، هر پروتکل از الگوریتم های متفاوتی استفاده می کند .

اتریوم توجه زیادی به تمرکز زدایی بر روی هسته خود دارد ، در حالی که ارز دیجیتال ایاس با حذف ویژگی های غیر متمرکز به سرعت آن بهبود می بخشد . بسته به هدف ، هر کدام از این پروژه ها موافقان و مخالفان خود را دارند .با مقایسه این دو سیستم عامل ، EOSممکن است جایگزین Ethereumبه عنوان سیستم عامل قرارداد هوشمند شود . ارز دیجیتال EOSبسیاری از مسائل Ethereumمانند کارمزدهای معامله و مقیاس پذیری را بهبود بخشیده است اما به دلیل متمرکز بودن مدل ، بحث برانگیز است .

اگر اتریوم بتواند الگوریتم اثبات سهام را اجرا کند ، EOSممکن است قادر به ادامه این روند نباشد . با این حال اگر غول بلاکچین اتریوم نتواند هزینه های معامله را کاهش دهد ، EOSمی تواند از اتریوم به عنوان یک سیستم عامل غیر متمرکز پیشی بگیرد

نام ارز دیجیتال	اتریوم (ETH)	ایاس (EOS)
مکانیزم شبکه	گواهی اثبات کار (PoW)	گواهی اثبات سهام محول شده (DPoS)
ارزش بازار	۴۴ میلیارد دلار	۶.۹ میلیارد دلار
عرضه کل	۱۰۰ میلیون ETH	۸۹۶ میلیون EOS
تاریخ ساخت	جولای سال ۲۰۱۵ میلادی	ژوئن سال ۲۰۱۷ میلادی
تیم توسعه دهنده	Ethereum Foundation	Block.one
کارمزد تراکنش ها	کمتر از ۱ دلار	رایگان
هزینه های سالیانه شبکه	۱۱ درصد که صرف هزینه های برق می‌شود	۵ درصد که صرف توسعه شبکه می‌شود
زمان لازم برای تایید یک تراکنش	۵ تا ۴۰ ثانیه	۱.۵ ثانیه
پهنای باند شبکه	۱۰ تراکنش در ثانیه (TPS)	بیش از ۳۰۰ هزار تراکنش در ثانیه (TPS)

عوامل تاثیر گذار بر روی قیمت ارز دیجیتال EOS

1.عرضه و تقاضا

رابطه بین عرضه و تقاضا مهمترین موضوعی است که باید در هنگام پیش بینی قیمت به ان توجه کرد . برای مثال وقتی تعداد افرادی که قصد خرید EOSرا دارند از تعداد فروشندگان بیشتر باشد ، این بدان معناست که تقاضا بیشتر از میزان عرضه است . این باعث افزایش قیمت ایاس می شود . وقتی تعداد افرادی که می خواهند این ارز را بفروشند بیشتر از افرادی است که می خواهند این ارز را بخرند ، برعکس است و قیمت ارز EOSافت می کند .

2.نقض امنیت

در دنیای ارزهای دیجیتال ، وقتی دارایی ها مطبوعات بدی در رسانه ها یا شبکه های اجتماعی دریافت می کنند ، می تواند به سرعت اعتماد سرمایه گذار را از بین ببرد و باعث شود بسیاری از افراد فروش دارایی های خود را شروع کنند . همانطور که در بالا توضیح دادیم ، این امر باعث می شود که عرضه بیشتر از تقاضا باشد و باعث افت قیمت شود .

3.محبوبیت DAppها

تقاضا برای برنامه های غیر متمرکز و یا همان DAppها در طول سال افزایش یافته است ، زیرا کاربران قصد دارند فرایند های مختلف مالی خود را به دور از حوزه مشاغل بزرگ انجام دهند . از آنجا که سیستم عامل EOS.IOاز توسعه DAppها پشتیبانی می کند ، در موقعیت ایده آل برای استفاده از تقاضا قرار دارد . با ادامه رشد تقاضا ، قیمت EOS نیز می تواند افزایش یابد .

کیف پول های ارز دیجیتال EOS

1.Ledger Nano X

2.Edge Wallet

3.Free Wallet

4.Lumi Wallet

5.Scatter EOS Wallet

6.ImToken Wallet

7.SimplEOS Wallet

8.Infinito EOS Wallet

با توجه به اینکه این ارز دیجیتال استخراج نمی شود و این رمز ارز یک توکن ERC-20است ، شما می توانید اتریوم را استخراج کرده و سپس اتریوم خود را از طریق سیستم تبادل Binanceبه EOSتبدیل کنید . در واقع شما می توانید هر کوین را استخراج کنید و آن را به اتریوم یا بیت کوین و سپس به EOSتبدیل کنید .شما می توانید با دنبال کردن مراحل زیر مقداری EOSرا در کیف پول مورد نظر خود ذخیره کنید .

1.نرم افزاراستخراج را بارگیری نمایید و آن را برای استخر استخراج مورد نظر خود تنظیم کنید .

2.اتریوم را استخراج کنید .

3. (ETH) را به صرافی بایننس و یا دیگر صرافی ها که امکان معاوضه ی ارزهای دیجیتال را دارند ، ارسال کنید .

4.ارز دیجیتال اتریوم خود را به EOSتبدیل کنید .

5.پس از اینکه موفق به استخراج شدید ارز خود را در کیف پولی که این رمز ارز را پشتیبانی می کند ، ذخیره نمایید .

آینده ارز دیجیتال EOSچگونه است ؟

بین سالهای 2021 تا 2025 سایت DigitalCoinPriceپیش بینی کرده است که قیمت EOSبا افزایش قیمت قابل توجهی برخوردار خواهد بود . قیمت متوسط آن در طول سال 2022 ، 7.88 دلار خواهد بود که بسیار خوش بینانه است . با جلوتر رفتن در سال 2023 تا 2025 ، قبل از ادامه صعود به 11.89 دلار ، می توانید شاهد سقوط قیمت در سال 2024 باشیم . این رقم در حدود 5 برابر قیمت فعلی خود ، نرخ امیدوار کننده ای برای رشد هر سرمایه گذار دارای EOSدر کارنامه خود خواهد بود .

در طی 5 سال ، Coinlikerمعتقد است EOSمی تواند قیمت های سرسام آور 175.98 دلار را به دست آورد . در نظر گرفتن ATHقبلی EOSفقط 17.89 دلار است . طبق گفته Nomics، این نرخ رشد فوق العاده استقبال خواهد شد . ممکن است بیش از حد خوش بینانه به نظر برسد ، اما Coinlikerدر وب سایت خود ادعا کرده است که پیش بینی آن چنان خوش بینانه نیست که بسیاری از سرمایه گذاران تصور می کنند . این پلتفرم تکامل فناوری EOSو افزایش استفاده از این ارز دیجیتال را به عنوان دو عامل اصلی برای رشد این ارز در 5 سال آینده دانسته اند .

مزایا و معایب ایاس

مزایا

سرعت پردازش بالا

رایگان بودن تراکنش ها

پشتیبانی از قراردادهای هوشمند و برنامه های غیرمتمرکز ((dApps

استفاده از الگوریتم گواهی اثبات سهم محول شده ((DPoS

کار با آن برای توسعه دهندگان بسیار راحت است و به راحتی توسعه دهندگان می‌توانند برنامه‌های غیرمتمرکز را کنار یکدیگر قرار دهند.

براساس میزان توکنی که دارید، مالکیت شبکه ایاس را هم در اختیار دارید و به معادل همان مقدار دسترسی به پهنای باند شبکه خواهید داشت.

معایب

نگرانی ها در مورد تمرکز شبکه ایاس (EOS؛) مکانیزم حاکمیت ایاس چنان طراحی شده است که در هر زمان معین تنها 21 تولیدکننده بلوك داشته باشد و عملکرد کلی شبکه به رأی سهامداران بستگی دارد.

رقبای متعدد ایاس (EOS؛) هنوز مشخص نیست که نتیجه رقابت اتریوم و ایاس چه خواهد بود. علاوه بر اتریوم، EOSباید با بلاک چین های دیگر از جمله Tron، Neo، Rchain رقابت کند و برای اینکه میدان را به رقبا نبازد، همواره باید در حال توسعه و بهبود پلتفرم خود باشد.

پروژه ایاس به این علت که بدون ارائه یک نمونه اولیه از شبکه اصلی EOSمبلغ یک میلیارد دلار از طریق عرضه اولیه سکه (ICOاخود جمع آوری کرد، با انتقادات شدیدی مواجه شد.

بیت کوین کش

یا BCH

یکی از رمز ارز های پایه بیت کوین کش،است. که با تغییراتی روی کد بیت کوین واندازه هر بلوک در سال ۲۰۱۷ ایجاد شد.نماد بیت کوین کش Bchاست. وپدیده هاردفورک (جداشدن) منجر به انشعاب یا جدا شدن بیت کوین کش از بیت کوین شد.

بیت کوین کش کاملا غیر متمرکز است. وهیچ بانک یا واسطه ای برای جا به جایی ندارد.

بیت کوین کش با افزایش سایز بلاک که در بیت کوین محدود به 1 مگابایت است، امکان پردازش تراکنش‌های بیشتری را فراهم می‌کند. یک بیت کوین کش با افزایش اندازه بلوک ها ، امکان پردازش معاملات بیشتر و بهبود مقیاس پذیری را فراهم می کند .به عبارت دیگر می توان گفت این ارز دیجیتال ، یک سیستم نقدینگی الکترونیکی نظیر به نظیر است که هدف از برپایی آن تبدیل شدن به پول جهانی سالم با پرداخت سریع ، امنیت و ظرفیت معاملات بالا است .

در سال 2010 ، میانگین اندازه بلوک در بلاک چین بیت کوین کمتر از 100 کیلو بایت بود و متوسط هزینه برای یک معامله فقط دو سنت بود . این موضوع باعث شد بلاک چین آن در برابر حملات بسیار آسیب پذیر باشد .

اندازه متوسط یک بلوک تا ژانویه 2015 به 600 kافزایش یافته بود . پس از آن تعداد تراکنش های استفاده شده از بیت کوین افزایش یافت و این باعث ایجاد معاملات تایید نشده شد و میانگین زمان انجام تراکنش رو به بالا رفت .

توسعه دهندگان برای حل مشکلات دو راه حل ارائه دادند : یکی از این راه حل ها افزایش متوسط اندازه بلوک یا حذف بخش های خاصی از معامله برای برقرار کردن داده های بیشتر در زنجیره بلوک است . تیم Bitcoin Coreکه مسئول توسعه و نگهداری الگوریتمی است که بیت کوین را تامین می کند ، پیشنهاد افزایش بلوک را رد کرد . به همین دلیل یک کوین جدید با اندازه بلوک انعطاف پذیر ایجاد کرد

بیت کوین کش برای اولین باردر صرافی ارزهای دیجیتال با قیمت 900 دلارارائه شد .صرافی های بزرگ همانند Coinbaseو ItBitبیت کوین کش را تحریم کردند و از بیت کوین کش حمایت نکردند.

Bitmain، بزرگترین پلتفرم استخراج ارزهای دیجیتال ، از بیت کوین کش پشتیبانی کرد. این پلتفرم با اطمینان از تامین سکه برای معامله در صرافی های ارز دیجیتال هنگام راه اندازی بیت کوین کش صحبت به میان آورد . و در این میان ، قیمت بیت کوین کش در دسامبر 2017 به 4091 دلار افزایش یافت .

پس از گذشت زمان بیت کوین کش از بیت کوین جدا شد و بعد از گذشت یک سال تحت اثر فورک قرار گرفت . در نوابر 2018 ، Bitcoincashبه Bitcoin Cash SVو Bitcoin Cash ABCتقسیم شد . این اختلاف نظر بر روی به روز رسانی های این پلتفرم بود که این به روز رسانی شامل استفاده از قراردادهای هوشمند در بلاک چین بیت کوین بود و متوسط اندازه بلوک را افزایش داد .

پس از هاردفورک معلوم شد که پشتیبانی بیشتری از بیت‌کوین ای‌بی‌سی نسبت به بیت‌کوین اس‌وی شده است. و به‌همین دلیل Bitcoin ABC همان بیتکوین‌کش اصلی است. و Bitcoin SV رمزارز جدیدی شناخته شد.

به دور از اختلاف نظرهای ایدئولوژیک و اندازه بلاک، شباهت‌هایی نیز بین بیت کوین و بیت کوین کش وجود دارد. هر دوی این ارزها از مکانیسم اجماع اثبات کار یا همان استخراج (ماینینگ)بهره میبرند.و برای تایید تراکنش‌ها و تولید سکه‌های جدید استفاده می‌کنند.عرضه کل هر دوی آن‌ها محدود به 21 میلیون واحد است. علاوه بر این، هر دوی این ارزها از تابع هش SHA256 برای هش کردن اطلاعات بلاک استفاده می‌کنند.

بر خلاف بیت کوین کش ، Bitcoinتقسیم بندی می کند تا بتواند خواسته های یک سیستم پرداخت جهانی را بر آورده کند . در زمان تقسیم ، اندازه بلوک بیت کوین کش از یک مگا بایت به 8 مگا بایت افزایش یافت . این افزایش اندازه به این معنی می باشد که بیت کوین کش می تواند معاملات بیشتری را در ثانیه انجام دهد ، در حالی که هزینه ها را بسیار پایین نگه دارد و اینکه مشکلات تاخیر پرداخت و هزینه های بالا برخی از کاربران را در شبکه Bitcoinحل می کند . و اندازه بیت کوین کش در نوامبر سال 2020 ، 32 مگا بایت است .به طور خلاصه می توان گفت ارز دیجیتال بیت کوین کش از نظر سرعت انجام معاملات با رمز ارز بیت کوین متفاوت است .

معایب بیت کوین کش

بیت کوین کش بسیار متمرکز است و تعداد استخرهای آن در حال حاضر محدود است. این موضوع می‌تواند بسیار تاثیرگذار باشد چراکه آینده‌ی این ارز به شدت وابسته به این چند استخر است.

به دلیل افزایش نگرانی‌ها در خصوص تمرکز این ارز دیجیتالص و نام تجاری‌اش، این کوین هنوز نتوانسته تمایزی بین خود و ارز دیجیتال بیت کوین ایجاد کند و این موجب کاهش اعتماد سرمایه‌گذاران به این کریپتوکارنسی شده است.

سرمایه‌گذاران هنوز این ارز دیجیتال را به عنوان یک دارایی بلندمدت در نظر نمی‌گیرند و از آن بیشتر به عنوان یک ابزار کوتاه‌مدت استفاده می‌کنند. به همین دلیل، فعلا این کریپتوکارنسی آینده‌ای مبهم و نامشخص دارد.

این ارز دیجیتال نرخ پذیرش و مخاطبان کمتری نسبت به بیت کوین دارد و این باعث شده در هنگام معاملات، بیت کوین کش از جفت‌های معاملاتی کمتری برخوردار باشد.

کیف پول های ارز دیجیتال بیت کوین کش

Electron Cash،

CoUnit

Bitcoin.Com

Mobi

Bitpay

Stash

StrongCoin

Coinomi

Jaxx

Exodus

Ledger Nano

Trezor

KeepKey

در اولین روز آغاز فعالیت شبکه‌اش، یعنی 1 آگوست سال 2017، 310 دلار بود.و 5 ماه بعد، یعنی در 20 دسامبر همان سال به بالاترین قیمت تاریخ خود یعنی 4,355 دلار دست یافت.

این رشد سریع و قابل توجه سبب شد تا سرمایه‌گذارانی که بر روی این سرمایه‌گذاری کرده بودند، در کمتر از 6 ماه سودی 1000 درصدی نصیبشان شود.بر خلاف میل طرفداران بیت کوین در سال 2017 ، بیت کوین کش یکی از بهترین عملکردها را داشته است .

الگوریتم مورداستفاده در استخراج بیت کوین کش Sha 256است و استخراج آن توسط دستگاه های ایسیک انچام می گیرد.شرکت بیت مین که یکی از بزرگترین تولید کنندگان دستگاه های ای سیک در دنیا است دستگاه های استخراج بیت کوین کش با نام انت ماینر را تولید می کند.برای خرید دستگاه باید به مواردی همچون میزان مصرف برق، قدرت پردازش و... توجه کنید.دستگاه های ماینر بیت کوین کش را می توان از سایت تولید کننده اصلی و سایر فروشگاه های معتبر بین المللی تخیه کرد اما کاربران ایرانی به دلیل وجود تحریم ها امکان خرید مستقیم را نخواهند داشت

POLKADOT

بستری برای ساخت برنامه‌های کامپیوتری غیرمتمرکز بدون خطر توقف یا دستکاری، تراکنش‌های فوق سریع و ارزان، رقیب اتریوم، شبکه‌ای با هزاران بلاک چین و ارز دیجیتالی که در رتبه‌های بالای بازار قرار گرفته است و سرمایه‌گذاران زیادی منتظر جهش نجومی آن هستند؛ همه این عناوین مربوط به پولکادات هستند.

پولکادات نسل جدید پروتکل‌های بلاک چین است. این پروژه سعی دارد شبکه‌ای واحد از بلاک چین‌های هدفمند و یکپارچه ایجاد کرده و از این طریق بر مشکلات مقیاس‌پذیری (کندی و پرهزینه بودن تراکنش‌ها) و تعامل‌پذیری در فضای ارزهای دیجیتال غلبه کند

ارز دیجیتال شبکه پولکادات، **DOT** نام دارد که کاربرد اصلی آن پرداخت هزینه‌های شبکه و همچنین تصمیم‌گیری برای آینده شبکه است. در حقیقت، هر فرد با داشتن دات می‌تواند یک حق رأی را برای آینده این شبکه به دست بیاورد. مانند بیت کوین، اتر و سایر ارزهای دیجیتال، سرمایه‌گذاری روی ارز دات، در حقیقت سرمایه‌گذاری روی آینده شبکه است و قیمت این ارز دیجیتال هم با عرضه و تقاضا و امیدواری‌ها نسبت به آینده شبکه پولکادات بالا و پایین خواهد شد.

طبق گفته تیم توسعه‌دهنده پولکادات، این پروژه قصد دارد با گردآوری بهترین ویژگی‌ها از بلاک چین‌های چندمنظوره، راه را برای ظهور برنامه‌های غیرمتمرکز با کاربردهای واقعی هموار کرده و دسترسی به خدمات غیرمتمرکز را برای همه کاربران تسهیل کند.

هدف بلاک چین‌های نسل یک در ذخیره و انتقال امن ارزش، به‌صورت غیرمتمرکز و همتابه‌همتا خلاصه می‌شود. پس از آن بلاک چین‌های نسل دوم با هدف رفع مشکلات دنیای واقعی (همچون امور مالی غیرمتمرکز، اینترنت اشیا، رهگیری کالاها، مدیریت اسناد و مدارک، مدیریت سامانه‌های حمل ونقل، مدیریت هویت‌های دیجیتال، ثبت مالکیت مادی و معنوی، ذخیره‌سازی غیرمتمرکز و پردازش ابری غیرمتمرکز) پا به عرصه گذاشتند. با این حال محدودیت‌های موجود در طراحی این سیستم‌ها مانع از مقبولیت گسترده آنها در میان کاربران شده است. هدف پولکادات رفع محدودیت‌ها و چالش‌های فعلی بلاک چین است.

هدف نهایی پولکادات تبدیل‌شدن به اینترنتِ بلاک چین‌ها است؛ بلاک چین‌هایی که می‌خواهند به‌طور یکپارچه با یکدیگر ارتباط داشته باشند.

پولکادات امکان ارسال هر نوع داده‌ای را میان هر نوع بلاک چینی فراهم ساخته است، با این امید که استفاده‌های گوناگون از بلاک چین را در دنیای واقعی ممکن سازد.

سرعت پایین تراکنش‌ها، افزایش غیرمنطقی کارمزدها در بازه‌های زمانی خاص، هاردفورک‌های (به‌روزرسانی‌های اساسی) پی‌درپی، مدیریت وابسته به اشخاص و در نهایت، نبود قابلیت تبدیل مستقیم ارزهای دیجیتال به یکدیگر (به‌دلیل انزوای بلاک چین‌ها نسبت به هم) از جمله مهم‌ترین نقاط ضعف بلاک چین‌های کنونی محسوب می‌شوند.

این در حالی است که طراحی منحصربه‌فرد پولکادات، مزایای قابل‌توجهی را نسبت به شبکه‌های سنتی موجود به ارمغان آورده و این شبکه را نسبت به سایر پلتفرم‌های بلاک چینی متمایز می‌کند:

مقیاس‌پذیری
قابلیت ارتقای شبکه بدون انجام هاردفورک
مدیریت شفاف و غیرمتمرکز
تعامل‌پذیری و ارتباط میان‌زنجیره‌ای

مقیاس‌پذیری Scalablity

مقیاس‌پذیری به توانایی بزرگ‌شدن و افزایش ظرفیت یک سیستم در هنگام افزایش پردازش‌ها گفته می‌شود.

شبکه پولکادات از روشی به نام «شاردینگ ناهمگون» **Heterogeneous Sharding** استفاده می‌کند. به این معنی که چندین بلاک چین مستقل به نام «پاراچین» **Parachain** را از طریق یک شبکه واحد به یکدیگر متصل کرده و به آنها این امکان را می‌دهد که تراکنش‌ها را به‌صورت موازی پردازش کنند و در بستری امن با یکدیگر تبادل داده داشته باشند.

به‌لطف مدل شاردینگ ناهمگون پولکادات، هر زنجیره در شبکه برای کاربرد خاص خود بهینه‌سازی می‌شود. این مدل در مقایسه با مدل «یک پروتکل برای همه کاربردها» که اتریوم و سایر پلتفرم‌های قرارداد هوشمند از آن استفاده می‌کنند، به‌مراتب مقیاس‌پذیری بیشتری دارد. زنجیره‌های بیشتر و تخصصی‌تر، به‌معنای فرصت بیشتر برای نوآوری است.

بر اساس آخرین سنجش‌های صورت‌گرفته روی شبکه پولکادات، سرعت ثبت تراکنش‌ها بدون استفاده از پاراچین‌ها ۱٬۰۰۰ تراکنش بر ثانیه و با استفاده از حداکثر توان عملیاتی پاراچین‌ها می‌تواند به حدود ۱,۰۰۰,۰۰۰ تراکنش بر ثانیه هم برسد.

قابلیت ارتقای شبکه بدون انجام هاردفورک

بلاک چین‌ها نیز مانند همه نرم‌افزارها، به‌منظور کارکرد صحیح نیازمند به‌روزرسانی هستند. با این حال، به‌روزرسانی بلاک چین بسیار سخت‌تر و پیچیده‌تر از به‌روزرسانی اپلیکیشن‌ها، بازی‌ها و مرورگرهاست. بلاک چین‌های معمولی برای انجام به‌روزرسانی نیازمند انشعاب (فورک‌کردن) شبکه هستند، به این معنی که زنجیره‌ای جدید با قوانینی جدید تشکیل داده و کاربران را به استفاده از این زنجیره ترغیب می‌کنند. این درحالی است که برنامه‌ریزی و اجرای یک فورک ماه‌ها زمان می‌برد و از همه مهم‌تر این‌که انجام هاردفورک‌های پی‌درپی در شبکه باعث چند دستگی جامعه کاربران و توسعه‌دهندگان شبکه خواهد شد.

شبکه پولکادات با تحول این فرایند، این امکان را فراهم کرده است که بلاک چین‌ها بدون نیاز به فورک کردن زنجیره، خود را به‌روزرسانی کنند. این به‌روزرسانی‌های بدون فورک، از طریق سیستم حاکمیتیِ درون زنجیره‌ای (روی بلاک چین) و شفافِ پولکادات انجام می‌شوند. پولکادات با بهره‌گیری از این قابلیت، به پروژه‌های گوناگون این امکان را می‌دهد تا به‌سرعت با تغییرات فناوری سازگار شده و همیشه به‌روز و چابک باقی بمانند. این قابلیت همچنین خطرات ناشی از هاردفورک‌های چالش‌برانگیز شبکه را (که مانعی جدی برای ورود بسیاری از سازمان‌ها به این حوزه است) به‌طرز چشمگیری کاهش می‌دهد.

مدیریت شفاف و غیرمتمرکز

تمامی صاحبان ارز دیجیتال دات **DOT** می‌توانند پیشنهادات مدنظر خود را برای تغییر پروتکل ارائه داده و به پیشنهادات موجود رأی دهند. آنها همچنین می‌توانند در انتخاب اعضای شورای حاکمیت که نماینده تمامی ذی‌نفعان شبکه هستند، مشارکت کنند. در ادامه این مقاله درباره سازوکارهای حاکمیتی پولکادات توضیحات بیشتری ارائه خواهیم داد.

تعامل‌پذیری و ارتباط میان زنجیره‌ای

قابلیت تعامل‌پذیری و پیام‌رسانی میان‌زنجیره‌ای پولکادات، امکان برقراری ارتباط، مبادله ارزش و به اشتراک گذاشتن عملکردها را برای بلاک چین‌های فعال در شبکه ممکن ساخته و از نوآوری‌های بیشتر در این ساختار استقبال می‌کند.

به‌لطف قابلیت پل‌های بلاک چینی پولکادات، پاراچین‌های پولکادات همچنین می‌توانند با پروتکل‌های محبوب اقتصاد غیرمتمرکز **(DeFi)** و دارایی‌های دیجیتال موجود بر روی شبکه‌های خارجی مانند بیت کوین و اتریوم هم تعامل داشته باشند.

ارز دیجیتال پولکادات یا به‌طور دقیق‌تر ارز دیجیتال DOT ، به سه منظور مشخص در شبکه مورداستفاده قرار می‌گیرد:

حاکمیت شبکه (Governance) : صاحبان توکن **DOT** کنترل کاملی بر شبکه دارند. تمامی امتیازاتی که در پلتفرم‌های دیگر در انحصار ماینرهاست، در پلتفرم پولکادات به مشارکت‌کنندگان در ریلِی‌چین (دارندگان توکن **DOT**) اعطا شده است. این امتیازات شامل مدیریت رویدادهای خاص همچون به‌روزرسانی و رفع مشکلات پروتکل هستند.

سهام‌گذاری (Staking) : شبکه پولکادات بر اساس نظریه بازی، صاحبان توکن **DOT** را به رفتار صحیح و سازنده در شبکه ترغیب می‌کند. افراد درستکار از طریق این مکانیسم پاداش دریافت می‌کنند در حالی که افراد خرابکار توکن‌های سهام‌گذاری شده خود را در شبکه از دست خواهند داد. این روش ایمنی شبکه را تضمین می‌کند.

انجام اثبات سهام پولکادات به‌صورت مستقیم بسیار پیچیده و دشوار است. با این حال، کاربران عادی برای اثبات سهام فقط کافی است از کیف پول‌ها یا صرافی‌هایی (مانند بایننس) که از اثبات سهام پولکادات پشتیبانی می‌کنند استفاده کنند و دارایی خود را برای کسب سود به شبکه اختصاص دهند. پاداش اثبات سهام پولکادات چیزی بین ۵ تا ۲۰ درصد در سال است.

وثیقه‌گذاری (Bonding) : پاراچین‌های جدید (بلاک چین‌های جدید در پولکادات) با وثیقه‌گذاری توکن‌های **DOT** به شبکه اضافه می‌شوند. پاراچین‌های منقضی‌شده یا غیرقابل‌استفاده از طریق حذف توکن‌های وثیقه، حذف خواهند شد. این فرایند نوعی اثبات سهام محسوب می‌شود.

هدف از ایجاد شبکه پولکادات رفع مشکلات مقیاس‌پذیری، تعامل‌پذیری و مدیریت بلاک چین‌ها است. به همین خاطر، شبکه پولکادات به‌گونه‌ای طراحی شده است که از یک سو امکان فعالیت موازی بلاک چین‌های گوناگون را فراهم کند و از سوی دیگر با استفاده از مدل امنیت اشتراکی، تمامی آنها را در یک شبکه واحد گرد هم آورد. همچنین برخلاف بلاک چین‌های سنتی که به‌صورت مجزا از یکدیگر کار می‌کنند، تمامی زنجیره‌های شبکه پولکادات با یکدیگر در ارتباط بوده و قادر به ارسال و دریافت هر نوع پیامی به یکدیگر هستند.

زنجیره‌های موجود در شبکه پولکادات

ریلِی‌چین (Relay Chain): زنجیره ریلِی‌چین، قلب شبکه پولکادات و عنصر هماهنگ‌کننده تمامی اجزای شبکه است. هریک از بلاک چین‌های مستقل شبکه پولکادات، با اتصال به ریلِی‌چین و اشتراک‌گذاری بلاک‌های خود در این زنجیره، از مدل امنیت اشتراکی پلتفرم پولکادات بهره‌مند می‌شوند. نودهای اعتبارسنج شبکه پولکادات با سهام‌گذاری توکن‌های دات بر روی ریلِی‌چین، مسئولیت اعتبارسنجی و تأیید بلاک‌های ارسالی از تمام بلاک چین‌های شبکه را بر عهده می‌گیرند. همچنین همه تصمیم‌گیری‌های حاکمیتی شبکه، با مشارکت صاحبان توکن‌های دات در همه‌پرسی‌های برگزارشده در ریلِی‌چین انجام می‌گیرد.

پاراچین‌ها (Parachains): پاراچین‌ها بلاک چین‌های مستقلی هستند که هریک دارای کاربردها، ویژگی‌ها و قوانین خاص خود بوده و با استفاده از زیرساخت خاص شبکه پولکادات که «سابستریت» **(Substrate)** نام دارد ساخته می‌شوند. واژه پاراچین برگرفته از عبارت **((Parallelized chains))** به‌معنای زنجیره‌های موازی است. بنابراین تراکنش‌های شبکه، به‌صورت موازی روی پاراچین‌ها اجرا شده و در بازه‌های زمانی مشخصی روی ریلی‌چین ثبت می‌شوند. هریک از این بازه‌های زمانی مشخص یک اسلات **(Slot)** نامیده می‌شود و هر پاراچین اسلات مخصوص به خود را روی ریلی‌چین در اختیار دارد. تراکنش‌های انجام‌شده در هر پاراچین، توسط نودهای رابط **(Collators)** پردازش شده و در بلاک‌ها ثبت می‌شوند. علاوه بر این، هر پاراچین می‌تواند با ارسال و دریافت تراکنش از دیگر پاراچین‌ها، با آنها در ارتباط باشد.

پاراتریدها (Parathreads): پاراتریدها (یا زنجیره‌های موازی)، ساختارهای داده جایگزینی برای پاراچین‌ها هستند. این زنجیره‌ها از منظر فنی شباهت بسیاری به پاراچین‌ها دارند، اما نحوه اتصال آنها به شبکه و مدل اقتصادی‌شان اندکی با پاراچین‌ها تفاوت دارد. صاحبان کسب‌وکارها یا برنامه‌های غیرمتمرکز گوناگون، می‌توانند به‌جای اجاره یک اسلات اختصاصی پاراچین و اتصال همیشگی به ریلِی‌چین، با مبلغی بسیار کمتر یک پاراترید را در اختیار گرفته و تنها در مواقع موردنیاز به ریلِی چین متصل شوند. مدل اقتصادی پاراتریدها اصطلاحاً «پرداخت بر اساس استفاده» نامیده می‌شود. به این معنی که پاراتریدهای گوناگون در صورت نیاز به ثبت بلاک روی ریلِی‌چین، با شرکت در یک مزایده عمومی اسلات بعدی شبکه را در اختیار گرفته و بلاک خود را به ریلِی‌چین ارسال می‌کنند.

پل‌ها (Bridges): پل‌های شبکه پولکادات، نوع خاصی از پاراچین‌ها هستند که به‌منظور برقراری ارتباط میان بلاک چین‌های متفاوت، با قوانین اقتصادی و زیرساخت‌های فنی متفاوت مورداستفاده قرار می‌گیرند. این پل‌ها با ساختار غیرمتمرکز و بدون نیاز به اعتماد خود، امکان ارسال و دریافت تراکنش از سایر بلاک چین‌های سنتی نظیر بیت کوین و اتریوم را فراهم می‌کنند. با بهره‌گیری از فناوری پل‌های بلاک چین، مشکل ایزوله‌بودن بلاک چین‌ها برطرف شده و تعامل‌پذیری میان شبکه‌های بلاک چینی گوناگون محقق می‌شود.

مشارکت‌کنندگان در شبکه پولکادات

نودهای اعتبارسنج **(Validators)** : اعتبارسنج‌ها مسئول حفظ امنیت ریلِی‌چین هستند. هریک از دارندگان توکن‌های دات، می‌توانند با سهام‌گذاری توکن‌های خود، تبدیل به یک نود اعتبارسنج شده و وظیفه ساخت بلاک‌های ریلِی‌چین را برعهده بگیرند. نودهای اعتبارسنج بلاک‌های پیشنهادی از سوی پاراچین‌ها را دریافت کرده و با اعتبارسنجی این بلاک‌ها، آنها را در ریلِی‌چین ثبت می‌کنند. این نودها در صورت عملکرد صحیح، پاداش ساخت بلاک (شامل کارمزد تراکنش‌ها) را دریافت خواهند کرد.

نودهای رابط (**Collators**) : نودهای رابط هر پاراچین تراکنش‌های کاربران پاراچین را جمع‌آوری و اجرا می‌کنند، سپس این تراکنش‌ها را در یک بلاک کاندید گردآوری کرده و آن را همراه با اثبات انتقال حالت، به نودهای اعتبارسنج مربوط به پاراچین خود ارائه می‌دهند. اختیارات نودهای رابط هر پاراچین، درست مشابه اختیاراتی است که در بلاک چین‌های مبتنی بر اثبات کار به ماینرها داده می‌شود.

نودهای گزیننده(**Naminators**) :ممکن است افرادی مایل به مشارکت در امنیت ریلی‌چین و کسب درآمد از شبکه پولکادات باشند، اما توانایی یا حوصله راه‌اندازی یک فول‌نود تمام‌وقت (سیستمی که همیشه روشن باشد) را نداشته باشند. این افراد می‌توانند یک نود گزیننده راه‌اندازی کنند تا با گزینش اعتبارسنج‌های قابل‌اعتماد، در امنیت شبکه سهیم شده و درآمد کسب کنند. هر گزیننده به نسبت مبلغی که در شبکه سهام‌گذاری کرده، حق رأی خواهد داشت. در صورتی که هریک از این اعتبارسنج‌ها رفتار خرابکارانه‌ای از خود نشان دهند، نود اعتبارسنج جریمه شده و نودهای گزینندهای که او را انتخاب کرده‌اند نیز توکن‌های سهام‌گذاری خود را از دست خواهند داد.

نودهای ناظر (**Fishermen**): فیشرمن‌ها یا ناظران نیز مانند نودهای رابط، فول‌نود پاراچین مخصوص به خود هستند اما نقشی متفاوت در شبکه پولکادات ایفا می‌کنند. ناظران به‌جای تولید بلاک‌های پاراچین و انتقال حالت‌ها (وظیفه‌ای که نودهای رابط هر پاراچین انجام می‌دهند)، بر این روند نظارت کرده و اطمینان حاصل می‌کنند که هیچ انتقال حالت نامعتبری در پاراچین انجام نشود. آنها در صورت مشاهده رفتار خرابکارانه در پاراچین، این رفتار را گزارش می‌دهند و در صورتی که صحت گزارش آنها اثبات شود، پاداش قابل‌توجهی از شبکه دریافت می‌کنند. همچنین در صورتی که گزارش آنها اشتباه باشد، با ریسک از دست‌دادن توکن‌های سهام‌گذاری‌شده خود مواجه خواهند بود.

اجماع اثبات سهام در شبکه پولکادات

امنیت شبکه پولکادات از طریق الگوریتم اجماع ترکیبی «گرندپا/بیب» (**GRANDPA/BABE**) تأمین می‌شود. این الگوریتم نوعی اجماع مبتنی بر اثبات سهام است که متناسب با پولکادات طراحی شده است. الگوریتم **GRANDPA/BABE** روشی ترکیبی است که از مزایای روش‌های اثبات کار و اثبات سهام بهره‌مند بوده و از معایب آنها پرهیز می‌کند. به‌طور خلاصه روش اثبات کار، حداکثر امنیت را برای شبکه تأمین می‌کند اما مقیاس‌پذیر نیست؛ از سوی دیگر روش اثبات سهام، مقیاس‌پذیری شبکه را افزایش می‌دهد، اما تا حدودی از امنیت شبکه می‌کاهد. الگوریتم **GRANDPA/BABE** چیزی بین این دو روش است.

پولکادات از مکانیسم (**Nominated Proof-of-Stake**) یا «اثبات سهام نامزدشده» برای تعیین اعتبارسنج‌ها استفاده می‌کند. در این مکانیسم، نودهای اعتبارسنج (**validators**) و نودهای گزیننده (**nominators**) نقش اصلی را در امنیت شبکه ایفا می‌کنند. به این صورت که نودهای گزیننده با سهام‌گذاری دارایی‌های خود در شبکه، می‌توانند به نودهای اعتبارسنج مورداعتماد خود رأی داده و آنها را انتخاب کنند.

این مکانیسم از جهاتی شبیه به روش اثبات سهام نمایندگی شده (**DPoS**) است. با این تفاوت که در روش **NPoS**، نودهای گزیننده در برابر انتخاب خود مسئولیت بیشتری دارند. به این معنی که در صورت خرابکاری نودهای اعتبارسنج، مبلغ سهام‌گذاری شده توسط گزینندگان، به‌عنوان جریمه از دست خواهد رفت؛ در حالی که در روش **DPoS** سهام‌گذاران مسئولیتی در برابر رفتار نمایندگان منتخب خود ندارند.

CARDANO

بنیان‌گذار کاردانو، چارز هاسکینسون (CHARLES HOSKINSON) است که خودش یکی از اعضای تیم اتریوم بوده است. سال ۲۰۱۵ پروژه کاردانو کلید خورد و به مدت دو سال به‌منظور یافتن راه حل‌هایی برای مشکلات اتریوم و بیت کوین، مورد تحقیق و بررسی قرار گرفت. کاردانو توانست با ایجاد فرایندهای جدید در تأیید تراکنش‌ها و ایجاد بلاک، مسائل مقیاس‌پذیری در بیت کوین و قراردادهای هوشمند در اتریوم را حل کند.

چارز هاسکینسون، بیت کوین را از نسل اول بلاک چین و اتریوم را از نسل دوم بلاک چین در نظر می‌گیرد. طبق عقیده او، ما به یک نسل سومی از بلاک چین‌ها نیاز داریم که کاردانو این نیاز را برطرف می‌کند.

کاردانو یک پلتفرم مبتنی بر بلاک چین است که مانند اتریوم امکان ایجاد و اجرای قراردادهای هوشمند را فراهم می‌کند؛ با این تفاوت که کاردانو خود را پیشگام در **«نسل سوم بلاک چین»** می‌نامد و امنیت آن با استفاده از معماری چند لایه تأمین شده است

از این شبکه می‌توان برای انتقال پول دیجیتالی و همچنین ثبت قراردادهای هوشمند و ساخت برنامه‌های غیرمتمرکز استفاده کرد

در حال حاضر سه بنیاد و شرکت زیر روی توسعه کاردانو کار می‌کنند:

THE CARDANO FOUNDATION

IOHK

EMURGO

بجز شرکت‌های بالا، ده‌ها تیم دیگر به شکل جداگانه در حال کار بروی کد منبع‌باز کاردانو و ساخت برنامه‌های غیرمتمرکز روی آن هستند.

پس از دو سال تحقیق و آزمایش، در ۲۸ سپتامبر ۲۰۱۷ (۶ مهر ۹۶) شبکه اصلی کاردانو راه‌اندازی و کمی بعد ارز دیجیتال کاردانو **ADA** به فهرست بیترکس، بزرگ‌ترین صرافی ارز دیجیتال آن زمان، اضافه شد.

برخلاف بسیاری از ارزهای دیجیتال دیگر مانند بیت کوین که از روش ماینینگ

یا همان اثبات کار برای حفظ امنیت شبکه و تأیید تراکنش‌ها استفاده می‌کنند،

کاردانو از الگوریتم **اثبات سهام** بهره می‌برد.

الگوریتم اثبات سهام کاردانو اوروبروس (Ouroboros)نام دارد.

اثبات انجام کار Work Proof of چیست؟

اثبات کار یک فرایند است که طی آن افرادی به نام ماینر یا استخراج کننده کامپیوترهای خود را برای حل مسائل ریاضی در اختیار شبکه قرار می دهند و نسبت به فعالیت خود کوین جدید استخراج شده به آن ها تعلق می گیرد. به منظور جلوگیری از ماین شدن همه کوین ها در مدت کوتاه، پروتکل ارزها معمولا به نوعی طراحی می شوند که به صورت خودکار سختی محاسبات بیشتر و بیشتر شود.

وقتی قصد ارسال یک تراکنش را دارید، در پشت صحنه، اتفاقات زیر رخ می‌دهد :

تراکنش ها در چیزهایی به نام بلاک دسته بندی می شوند.

ماینرها تراکنش های درون بلاک را بررسی و در صورت صحیح بودن، تایید می‌کنند.

برای انجام این کار، کامپیوترهای ماینر باید یک سری معادلات ریاضی را حل کنند.

به اولین ماینر که معادله بلاک را حل کند،پاداش داده می شود. این پاداش به مرور زمان برای حفظ شبکه تغییر می کند. مثلا تا سال ۲۰۱۴ ،این پاداش ۲۵ بیت کوین بود.

این "معادلات ریاضی" یک ویژگی کلیدی دارد: نامتقارن بودن. در حقیقت، کار استخراج یا همان معادلات ریاضی آرام آرام سخت تر و سخت تر می شود.

تمام ماینرها برای حل زوتر معادلات یک بلاک، همواره با یکدیگر در حال رقابت هستند. وقتی یک ماینر در نهایت راه حل مناسب را پیدا می کند، بلافاصله آن را به تمام شبکه اعلام می‌کند و توسط پروتکل به او پاداش داده خواهد شد.

اثبات سهام چیست؟

مفهوم اثبات سهام بیان می‌کند که یک شخص می‌تواند معاملات بلوکی را با توجه به اینکه چند سکه در دست دارد، استخراج یا اعتبارسنجی کند.

این بدان معناست که هرچه بیت‌کوین یا آلت‌کوین بیشتری متعلق به یک ماینر باشد، قدرت استخراج وی نیز بیشتر است.

ویژگی‌های کلیدی:

- اثبات سهام به عنوان جایگزینی برای الگوریتم اثبات کارایجاد شد، که الگوریتم اجماع اصلی در فناوری بلاکچین است، و برای تأیید معاملات و افزودن بلوک‌های جدید به زنجیره استفاده می‌شود.

-الگوریتم اثبات کار به مقدار زیادی انرژی احتیاج دارد و استخراج¬ کنندگان برای فروش نهایی اسکناس نیاز به فروش سکه‌های خود دارند؛ اما اثبات سهام قدرت استخراج را براساس درصد سکه‌های نگهداری شده توسط یک ماینر تعیین می کند.

- اثبات سهام از نظر پتانسیل حمله ماینرها به شبکه ریسک کمتری دارد.

مزایای اصلی روش اثبات کار:

دفاع در برابر حملات ضد داس و تأثیر کم سهم در استخراج است. الگوریتم اثبات کار محدودیت‌هایی را برای اقدامات در شبکه اعمال می‌کند. حمله کارآمد به قدرت محاسباتی بالا و زمان زیادی برای انجام محاسبات نیاز دارد.

برای استخراج مهم نیست که چقدر پول در کیف پول خود دارید؛ آنچه مهم است داشتن قدرت محاسباتی زیاد برای حل معماها و تشکیل بلوک‌های جدید است. بنابراین دارندگان مبالغ هنگفت، تصمیم گیری برای کل شبکه را بر عهده ندارند.

با استفاده از اثبات سهام، اگر کسی بخواهد به شبکه حمله کند و کنترل آن را به دست بگیرد، مجبور است بیش از ۵۱ درصد از تمام واحدهای ارز دیجیتال مورد نظر (مثل کاردانو) را بخرد و به شبکه اختصاص دهد. خرید ۵۱ درصد از کل واحدهای یک ارز دیجیتال بسیار مشکل است و با استناد به اصل عرضه و تقاضا در بازار تقریباً امکان‌پذیر نیست.

اورو

بروس

در این الگورتیم، زمان واقعی به دوره‌های زمانی (epochs) تقسیم می‌شود. هر دوره زمانی هم خود به دوره‌های زمانی کوتاه‌تری به نام «اسلات» (slot)تقسیم می‌شود. این دوره‌های زمانی مانند کارکنان شیفتی در یک کارخانه عمل می‌کنند؛ یعنی زمانی که یک دوره زمانی به پایان می‌رسد، کار دوره زمانی دیگر شروع می‌شود.

در پروژه کاردانو، محدوده زمانی که اسلات‌ها دربرمی‌گیرند متفاوت است و می‌تواند در الگوریتم آن تغییر داده شود.

هر اسلات یک رهبر دارد که به آن رهبر اسلات (SL)می‌گویند. این رهبر ها را دارندگان واحدهای کاردانو (ADA)با رای خود در شبکه انتخاب می‌کنند.

این رهبران اسلات مسئول ایجاد و تایید تراکنش‌های بلوک‌هایی هستند که به بلاک چین کاردانو اضافه می‌شوند. هر رهبر فقط می‌تواند یک بلوک تولید کند. این مکانیزم سبب می‌شود که نتوان در یک دوره زمانی خاص، بیشتر از تعداد خاصی بلاک تولید کرد.

اگر رهبری در یک اسلات که مسئول ایجاد بلوک و تأیید تراکنش‌های آن است، نتواند کار خود را انجام دهند (مثلاً آنلاین نباشد)، آن‌گاه حق تولید بلاک را از دست می‌دهد و پاداشی نمی‌گیرد.

تراکنش‌هایی که توسط رهبران اسلات ایجاد شده، توسط تأییدکنندگان ورودی (Input Endorsers)مورد تأیید قرار می‌گیرد. این تایید کنندگان ورودی، دومین مجموعه از دارندگان سکه هستند که مسئول اجرای پروتکل‌اند. در یک دوره زمانی مشخص ممکن است از یک تا چندین تایید کننده وجود داشته باشد. حق رأیی که هر کدام از این تاییدکنندگان برای تایید تراکنش‌ها دارند، بر اساس تعداد سکه‌هایی است که نگهداری می‌کنند.

برای اطمینان از اینکه نتایج حاصل از تایید تراکنش‌ها بی طرفانه بوده است، این سیستم رأی‌گیری بر اساس دو ورودی طراحی شده است.

سیستم اولیه یک **سیستم محاسباتی با چندین شرکت‌کننده** است. مجموعه‌ای از دارندگان سکه، محاسباتی را در شبکه انجام داده و نتایج آن را با یکدیگر به اشتراک می‌گذارند.

سیستم دوم بر اساس **توزیع ثروت یا سهام** است. نودهایی که تعداد سکه‌های بیشتری دارند، شانس بیشتری دارند تا به عنوان رهبر یک اسلات انتخاب شوند.

تمرکز اصلی پروژه کاردانو بر روی حل مشکل **مقیاس‌پذیری** است. برای این منظور پروژه کاردانو از یک **تکنولوژی به نام رینا (RINA)** استفاده می‌کند. رینا یک نوع جدید از ساختارسازی برای شبکه‌ها است و هدف آن ساخت شبکه‌ای است که حریم خصوصی، شفافیت، مقیاس‌پذیری را ارائه می‌دهد. به عبارت دیگر، رینا این امکان را برای کاردانو فراهم می‌کند که با افزایش حجم تراکنش‌ها تا هزاران تراکنش در ثانیه، سرعت انجام آنها و هزینه لازم برای انجام تراکنش‌ها تغییر نکند.

کاردانو برای این کار از یک ساختار دو لایه‌ای استفاده می‌کند:

لایه اجماع یا CSL

لایه محاسباتی یا CCL

لایه اجماع CSL

لایه CSL اولین لایه پلتفرم کاردانو به شمار می‌رود

و هدف آن استفاده از یک الگوریتم اجماع مبتنی

بر اثبات سهام (PoS) برای ایجاد بلوک‌های

لایه محاسباتی CCL

این لایه دومین لایه پلتفرم کاردانو است و شامل اطلاعاتی در مورد نحوه انجام تراکنش‌ها می باشد.

با وجود اینکه لایه مربوط به پردازش تراکنش‌ها CCL از لایه مربوط به اجماع و تایید تراکنش‌ها CSL جداست، کاربران کاردانو می‌توانند با استفاده از لایه محاسباتی CCL، در زمان بررسی تراکنش‌ها، قوانین مختلفی را ایجاد کنند که بر روی لایه اجماع CSL اعمال شود.

برای مثال، با استفاده از لایه محاسباتی CCL می‌توان دفتر کلی ایجاد کرد که تراکنش‌های مشکوک و ناشناس در لایه اجماع CSL ثبت نشود.

IOHK شرکت علمی و مهندسی است که فناوری‌های موجود در شبکه کاردانو را ایجاد می‌کند. آن‌ها همچنین این پروتکل‌ها را ازطریق یک رویکرد دوجانبه طراحی و نگه‌داری می‌کنند.

شرکت ژاپنی EMURGO این تیم روی مشاغل تجاری و چگونگی پیشرفت استفاده از فناوری بلاک‌چین در صنایع متمرکز است.

سال ۲۰۱۷ شرکت IOHK به دانشگاه ادینبورگ کمک کرد تا آزمایشگاه فناوری بلاک‌چین را راه‌اندازی کند. سال ۲۰۱۹، وزیر آموزش‌وپرورش گرجستان، میخائیل باتیاشویلی و چارلز هاسکینسون با دانشگاه آزاد تفلیس تفاهم‌نامه‌ای برای استفاده از کاردانو برای ساخت سیستم تأیید اعتبار امضا کردند. سال ۲۰۱۸، کاردانو با دولت اتیوپی همکاری کرد تا کاردانو بتواند فناوری خود را در صنایع مختلف در سراسر کشور به‌کار گیرد. افزون‌براین، IOHK شرکت توسعه‌دهنده کاردانو، معادل ۵۰۰ هزار دلار رمزارز ADAرا به دانشگاه وایومینگ اهدا کرد تا از توسعه فناوری بلاک‌چین پشتیبانی کند. تولیدکننده کفش نیوبالانس برای ردیابی اصالت جدیدترین کفش بسکتبال خود از بلاک‌چین دفتر توزیع‌شده استفاده خواهد کرد. این پلتفرم در بلاک‌چین کاردانو ساخته خواهد شد.

تیم کاردانو برای ایجاد چشم‌اندازی از آینده، نقشه راهی برای خود تنظیم کرده است و می‌کوشد تا به برخی از اصول و فلسفه پایبند باشد. کانون توجه این تیم بر پذیرش مجموعه‌ای از اصول طراحی، بهترین روش‌های مهندسی و راه‌های اکتشاف معطوف شده است.

موارد زیر برخی از این اصول و مبانی را تشکیل می‌دهد و مستقیما از وب‌سایت کاردانو گرفته شده است:

تفکیک حسابداری و محاسبه به لایه‌های مختلف

پیاده‌سازی اجزای اصلی در کد عملکردی بسیار مدولار

استفاده از گروه‌های کوچکی از دانشگاهیان و توسعه‌دهندگان که با تحقیقات بررسی‌شده برای توسعه پلتفرم همتا به همتا رقابت می‌کنند.

استفاده زیاد از تیم‌های بین‌رشته‌ای؛ ازجمله استفاده زودهنگام از متخصصان امنیتی

تکرار سریع بین مقالات سفید و پیاده‌سازی و تحقیقات جدید برای اصلاح موارد کشف‌شده هنگام بازبینی موردنیاز خواهد بود.

ایجاد توانایی در به‌روزرسانی سیستم‌های پس از استقرار و بدون اختلال و ازبین‌بردن شبکه

توسعه مکانیسم بودجه غیرمتمرکز برای کارهای آینده

دیدی طولانی‌مدت درباره بهبود طراحی رمزارزها برای استفاده در گوشی‌های هوشمند و ایجاد تجربه کاربری منطقی و ایمن

نزدیک‌کردن سهامداران به پلتفرم و نگه‌داری ایمن رمزارز آن‌ها

تصدیق نیاز به حساب چندین دارایی در دفتر

چکیده تراکنش‌ها شامل فراداده اختیاری به‌منظور مطابقت بهتر با نیازهای سیستم‌های قدیمی

یادگیری و الهام از تقریبا هزار آلت‌کوین با پذیرفتن ویژگی‌هایی که منطقی است.

اتخاذ فرایندی مطابق با استانداردها و با الهام از گروه ویژه‌ای از مهندسان اینترنتی با استفاده از پایه‌ای اختصاصی برای قفل‌کردن طرح پروتکل نهایی

ایجاد فضایی سالم برای تنظیم مقررات برای تعامل و تجارت بدون به‌خطرانداختن برخی از اصول اصلی به ارث رسیده از بیت‌کوین

برنامه‌نویسی کاردانو در هسکل Haskell انجام و قراردادهای هوشمند آن در پلوتوس Plutus کدگذاری می‌شود. برای درک اینکه چرا چنین رویکردی منحصربه‌فرد است، باید برخی اصول درباره زبان‌های برنامه‌نویسی را بهتر درک کنیم. وقتی از زبان برنامه‌نویسی صحبت می‌شود، آن‌ها در برنامه‌نویسی ضروری و کاربردی دسته‌بندی می‌شوند.

زبان‌های برنامه‌نویسی ضروری:

در رویکردی ضروری، رمزگذار باید تمام مراحلی را قرار دهد که کامپیوتر برای رسیدن به یک هدف انجام می‌دهد. تمام زبان‌های برنامه‌نویسی سنتی مانند C ++ و Java و حتی Solidid زبان‌های برنامه‌نویسی ضروری هستند. به این نوع رویکرد، برنامه‌نویسی الگوریتمی نیز گفته می‌شود.

هسکل و پلوتوس هر دو زبان‌های کاربردی هستند. برخی از مزایای رویکرد کاربردی به‌شرح زیر است:

به ایجاد کد بسیار مطمئن کمک می‌کند؛ زیرا اثبات نحوه رفتار کد آسان‌تر است.

خوانایی و قابلیت نگه‌داری را افزایش می‌دهد؛ زیرا هر عملکرد برای انجام کاری خاص طراحی شده است و توابع نیز مستقل از دولت هستند.

شکستن کد آسان‌تر است و اجرای هرگونه تغییر در کد ساده‌تر خواهد بود. این امر توسعه تکراری را آسان‌تر می‌کند.

عملکردهای فردی را می‌توان به‌راحتی جدا کرد که آزمایش و اشکال‌زدایی آن‌ها را آسان‌تر می‌کند.

با وجود برتری‌های ذکرشده، زبان‌های برنامه‌نویسی مذکور مشکلاتی نیز دارند. برای مثال، یافتن توسعه‌دهنده هسکل بسیار دشوارتر از یافتن توسعه‌دهندگان C ++ و Java است

با نگاهی گذرا به فلسفه کاردانو، بیایید جزئیات سه عنصر و چالش اصلی را بررسی کنیم که این تیم برای حل آن‌ها تلاش می‌کند.

مقیاس‌پذیری

قابلیت همکاری

پایداری

مقالات زیادی درباره فقدان توان عملیاتی در بیت‌کوین و اتریوم نوشته شده است. بیت‌کوین ۷ تراکنش در ثانیه و اتریوم ۱۵ تا ۲۰ تراکنش را مدیریت می‌کند و این اصلا برای سیستم مالی مقبول نیست. کاردانو امیدوار است با سازوکار اجماع خود یعنی اوروبروس Ouroboros این مشکل را حل کند. این الگوریتم اثبات سهام با اطمینانی است.
همان‌طورکه بیان شد، اوروبروس الگوریتم اثبات سهام است

پروتکل اثبات سهام کاردانو قرار است تمرکززدایی بی‌سابقه‌ای را ایجاد کند؛ اما سازوکارهایی که آن را هدایت و بنیان آن را تشکیل می‌دهند، هنوز برای بسیاری ناشناخته باقی مانده است. آگلوس کیائیاس، استاد بزرگ و دانشمند ارشد کاردانو، به عمق مشکلات سیستم‌های غیرمتمرکز پی برد و دیدگاه مفصلی درباره چگونگی مدیریت اوروبروس برای حل این مشکلات ارائه داد. معمولا طراحی سیستم غیرمتمرکز قوی بسیار پیچیده است؛ زیرا آن‌ها به توسعه مدل‌هایی نیاز دارند که به‌طور نظام‌مند تمام تهدیدهای مختلفی را دربر بگیرد که سیستم ممکن است با آن روبه‌رو شود و ثابت کند پایداری و زنده‌بودن سیستم و شبکه در تمامی زمان‌ها حفظ می‌شود.

سیستم غیرمتمرکز مطمئن ضمانت‌های رسمی را دربرابر انواع مختلف شکست و مدل‌های حمله با بزرگ‌ترین و مهم‌ترین کلاس شکست یعنی مدل‌های بیزانس ترکیب می‌کند. مدل‌های بیزانس تضمین می‌کنند که پایداری و فعالیت سیستم حفظ خواهد شد؛ حتی اگر بخش بزرگی از شرکت‌کنندگان در شبکه به‌طور خودسرانه از قوانین شبکه خارج شوند. نکته دوم مدل‌های عقلانیت است که فرض می‌کند تمامی شرکت‌کنندگان در شبکه حداکثرکننده‌های ابزار منطقی هستند؛ به‌همین‌دلیل، خصوصیات سیستم باید ازطریق منافع شخصی آن‌ها ناشی شود.

به‌گفته کیائیاس، آنچه اوروبروس را به‌عنوان پروتکل منحصربه‌فرد می‌کند، این واقعیت است که این پروتکل عناصر مختلف طراحی را ترکیب می‌کند. به‌عبارت‌دیگر، اوروبروس از سهام به‌عنوان منبع اصلی برای شناسایی اهرمی استفاده می‌کند که شرکت‌کنندگان در سیستم دارند.

جدا از مقاومت دربرابر حملات بومی پروتکل‌های اثبات کار، مانند حمله ۵۱ درصدی و حتی فراتر از آن، ذخیره‌سازی باعث می‌شود این پروتکل سازگار با محیطزیست باشد؛ زیرا برای اجرای آن به حداقل منابع فیزیکی نیاز دارد.

به‌طورکلی، اوروبروس پروتکل اثبات سهام مبتنی‌بر زنجیره است که برای تأیید بلوک‌ها به رهبران انتخاب‌شده تصادفی متکی است و مانند اکثر بلاک‌چین‌ها گره‌ای که بلوک بعدی را اضافه می‌کند، پاداش تلاش‌هایشان را دریافت می‌کند.

در شروع هر دوره، سیستم رهبران را از گروه سهام‌داران انتخاب می‌کند (کسانی که ارز را به شبکه اختصاص داده‌اند). اوروبروس به توزیع نشانه‌ها در اکوسیستم نگاه می‌کند و از یک منبع اعداد تصادفی، زمان را به دوره‌هایی تقسیم می‌کند.

سپس هر دوره به اسلات تقسیم می‌شود و هر دوره برای مدت‌زمان بسیار کوتاهی در حدود ۲۰ ثانیه ادامه دارد. درنهایت، هر اسلات رهبر اسلات مخصوص خود را دارد که به‌طور تصادفی انتخاب می‌شود.

رهبر اسلات مانند ماینرها در پروتکل POW اثبات کار عمل می‌کند. درواقع، آن‌ها کسانی هستند که بلوک‌هایی انتخاب می‌کنند که به زنجیره بلوک اضافه می‌شوند. بااین‌حال، آن‌ها می‌توانند تنها یک بلوک را اضافه کنند. اگر رهبر اسلات به نحوی بخت خود را از دست دهد و بلوک را انتخاب نکند، فرصت خود را از دست خواهد داد و باید منتظر بمانند تا دوباره رهبر اسلات شوند. سرانجام، یک یا چند اسلات می‌توانند بدون بلوک‌های تولیدشده خالی بماند؛ اما باید اکثر بلوک‌ها (حداقل ۵۰ درصد یک بلوک) باید در طول یک دوره تولید شوند.

بااین‌اوصاف، قطعا باید متوجه اهمیت و نقش رهبرهای اسلات در اکوسیستم شده باشید؛ بنابراین برای تأیید صلاحیت آن‌ها، شخص باید ۲ درصد از سهام کاردانو را دراختیار داشته باشد. این ذی‌نفعان انتخاب‌کننده نامیده می‌شوند و کسانی هستند که در دوره فعلی، رهبران اسلات را برای دوره بعدی انتخاب می‌کنند. سهام‌داران هرچه بیشتر در سیستم مشارکت کنند، بخت بیشتری برای انتخاب به‌عنوان رهبر اسلات دارند.

اکنون، ازآنجاکه رهبران اسلات قدرت زیادی دارند، باید توجه ویژه‌ای به‌خرج داد و شرایطی ایجاد کرد که تاحدممکن انتخابات بی‌طرفانه باشد. همچنین، باید مقداری تصادف در آن دخیل باشد؛ به‌همین‌دلیل، برای دستیابی به مقدار تصادفی محاسبه چندحزبی (MPC) انجام می‌شود.

در رویکرد مبتنی‌بر محاسبه چندحزبی، هر انتخاب‌کننده اقدامی تصادفی به نام پرتاب سکه را انجام می‌دهد و پس‌ازآن، نتایج خود را با سایر انتخاب‌کنندگان به‌اشتراک می‌گذارد. اگرچه هر انتخاب‌کننده نتایج را تصادفی تولید می‌کنند، درنهایت، اجماع رأی‌ها روی همان مقدار نهایی به‌توافق می‌رسد.

انتخابات به سه مرحله زیر تقسیم می‌شود:

مرحله تعهد
مرحله آشکار
مرحله بازیابی

مرحله تعهد

در مرحله اول، انتخاب‌کننده مقدار تصادفی مخفی تولید می‌کند و سپس تعهد را تشکیل می‌دهد. تعهد پیامی شامل سهام رمزگذاری‌شده (برای مرحله بازیابی این نکته را در ذهن به‌خاطر بسپارید) و اثبات رازداری است. پس‌ازآن، انتخاب‌کننده تعهد را با کلید خصوصی خود امضا و شماره دوره را مشخص می‌کند و کلید عمومی‌اش را ضمیمه قرار می‌دهد. به‌واسطه انجام این کار و ازآنجاکه کلید عمومی به آن متصل است، همه می‌توانند بررسی کنند چه کسی این تعهد را ایجاد کرده است.

افزون‌براین، می‌توان بررسی کرد تعهد به کدام دوره مربوط می‌شود. پس از انجام این کار، انتخاب‌کننده تعهداتش را به سایر انتخاب‌کنندگان می‌فرستد. درنهایت، هر انتخاب‌کننده تعهدات انتخاب‌کننده دیگر را جمع می‌کند. به‌عبارت‌دیگر، تعهدات وارد بلوک می‌شوند و به بخشی از زنجیره بلوک را تشکیل می‌دهند.

مرحله آشکار

مرحله دوم مرحله آشکار است. به تعهداتی مانند جعبه قفل‌شده فکر کنید که در آن راز و ارزش خاصی وجود دارد که می‌تواند قفل جعبه را باز کند. این مقدار خاص، روزنه یا دهانه نامیده می‌شود. این همان چیزی است که در این مرحله وجود دارد و انتخاب‌کنندگان دهانه خود را می‌فرستند. این دهانه‌ها نیز در بلوک قرار می‌گیرند و سپس بخشی از زنجیره بلوک می‌شوند.

مرحله بازیابی

سرانجام، مرحله بازیابی را داریم. در این زمان، انتخاب‌کننده هم تعهدات و هم دهانه‌هایی دراختیار دارد. بااین‌حال، برخی از انتخاب‌کنندگان ممکن است بدخواهانه عمل و تعهدات خود را بدون گذرواژه منتشر کنند و جعبه قفل‌شده را بدون کلمه عبور دراختیار سایرین قرار دهند. به‌منظور دورزدن و غلبه بر این موضوع، انتخاب‌کنندگان صادق می‌توانند تمام سهام رمزگذاری‌شده را ارسال (همان‌طورکه در مرحله تعهد ذکر شد) و به‌راحتی اسرار را بازیابی کنند. بدین‌ترتیب، حتی اگر برخی از انتخاب‌کنندگان به روشی مخرب عمل کنند، سیستم همچنان کار خواهد کرد؛ ازاین‌رو، اوروبروس با پشت‌سرگذاشتن این موانع، تحمل گسل بیزانسی خود را به‌دست می‌آورد.

سرانجام، انتخاب‌کننده تأیید می‌کند تعهدها و گشایش‌ها باهم مطابقت دارند. وقتی این اتفاق می‌افتد، اسرار تعهدات استخراج می‌شود و یک نطفه (بذر) را تشکیل می‌دهد. نطفه یک رشته بایت است که به‌طور تصادفی ایجاد می‌شود. اکنون تمامی انتخاب‌کنندگان این نطفه را دارند. شاید با پیچیدگی این فرایند کمی گمراه شده باشید؛ بنابراین، بیایید برای لحظه‌ای مکث کنیم و بررسی کنیم درحال‌حاضر کجا قرار داریم. ما رهبران اسلات را برای دوره بعدی انتخاب می‌کنیم. برای اطمینان از اینکه انتخابات تاحدممکن مغرضانه باشد، به‌نوعی تصادف نیاز داریم. حال نطفه این تصادفی‌بودن را برای ما فراهم می‌کند و اکنون زمان انتخاب رهبران اسلات فرارسیده است. برای این کار از الگوریتم **Follow the Satoshi** به‌اختصار (FTS) استفاده می‌شود.

الگوریتم FTS

FTS در اصل سکه‌ای تصادفی را از سهام انتخاب می‌کند. هرکسی صاحب این سکه شود، به رهبر اسلات تبدیل می‌شود. این امر بسیار سرراست است؛ به‌همین‌دلیل، هرچه شخص در سیستم بیشتر فعال باشد، بخت بیشتری برای برنده‌شدن در این قرعه‌کشی دارد. رهبران اسلات این قدرت را دارند که نه‌تنها بلوک‌های اصلی بلاک‌چین، بلکه بلوک‌های دیگری نیز در داخل اکوسیستم کاردانو انتخاب کنند

معمولا پهنای باند ساده‌ای به معاملات داده اختصاص داده می‌شود؛ بنابراین با افزایش تعداد تراکنش‌ها، نیاز به منابع شبکه نیز افزایش می‌یابد. این مفهوم کاملا ساده است و اگر سیستم بخواهد میلیون‌ها کاربر را مقیاس‌بندی کند، شبکه برای ادامه حیات خود به ۱۰۰ ترابایت یا اگزابایت منبع نیاز دارد. به‌همین‌ترتیب، حفظ توپولوژی شبکه همگن غیرممکن خواهد بود؛ اما معنی آن چیست.

در توپولوژی شبکه همگن، هر گره در شبکه هر پیامی را ارسال می‌کند. برای مثال، اسکایپ نمونه‌ای بارز از چنین شبکه‌ای است که بیشترین مقدار آن از طبقه‌ای از کاربران گرفته شده و همه علاقه‌مند به برقراری تماس تلفنی هستند. بااین‌حال، در شبکه غیرمتمرکز این می‌تواند برای کوچک‌سازی غیرعملی شود. تمامی گره‌ها ممکن است منابع لازم برای انتقال اطلاعات به روشی مؤثر را نداشته باشند. برای حل این مسئله، کاردانو به‌دنبال نوع جدیدی از فناوری به نام رینا معماری بازگشتی بین‌شبکه‌ای است که جان-دی توسعه داده است. این نوع جدیدی از شبکه‌های ساختاری است که از سیاست‌ها و اصول مهندسی هوشمندانه استفاده می‌کند.

هدف RINA ایجاد شبکه‌ای ناهمگن است که نویدبخش آن حریم خصوصی و شفافیت و مقیاس‌پذیری خواهد بود. این کار را به روشی انجام می‌دهد که می‌توانید حدس بزنید شبکه در ظرفیت رسمی چگونه سازمان‌دهی می‌شود. همچنین، امید است با پروتکل‌های TCP / IP یکپارچه عمل کند. RINA ذاتا از پویایی و شبکه رایانه‌ای چندخانه‌ای و کیفیت خدمات بدون نیاز به مکانیزم‌های اضافه پشتیبانی و محیطی امن و قابل‌برنامه‌ریزی و انگیزه‌ای برای بازار رقابتی‌تر فراهم و تصویب یکپارچه را امکان‌پذیر می‌کند.

قابلیت همکاری

قابلیت همکاری می‌رسیم. بیایید اکوسیستم فعلی را بررسی کنیم. در دنیای رمزارزها کوین‌های مختلفی، ازجمله بیت‌کوین، اتریوم، لایت‌کوین و... وجود دارند. به‌همین‌ترتیب، در نظام مالی سنتی سیستم‌هایی همچون بانک‌های کنونی را داریم که از SWIFTو ACHو... استفاده می‌کنند.

مشکل در این واقعیت است که برقراری ارتباط با این اشخاص منفرد بسیار دشوار است. برای بیت‌کوین سخت است که بداند در شبکه اتریوم چه می‌گذرد و برعکس. وقتی بانک‌ها سعی می‌کنند با رمزارزها ارتباط برقرار کنند، این مسئله دوچندان می‌شود؛ به‌همین‌دلیل، مبادلات رمزنگاری‌شده که درگاهی بین رمزارزها و بانک‌ها را فراهم می‌کنند، بسیار قدرتمند و بااهمیت می‌شوند. بااین‌حال، مشکلی وجود دارد: صرافی‌ها نهاد غیرمتمرکز نیستند و به‌شدت آسیب‌پذیر هستند. آن‌ها می‌توانند هک یا برای مدت طولانی به‌منظور ارتقای سیستم از دسترس خارج شوند. این اساسا اتفاقی است که چندی پیش برای صرافی بایننس رخ داد.

به‌علاوه، چالش دیگری وجود دارد که این ارتباط نادرست بین نظام سنتی و دنیای رمزارزها می‌تواند به نتیجه‌ای فاجعه‌بار در عرضه اولیه سکه‌ها تبدیل شود. در ICOها، نهادی می‌تواند میلیون‌ها دلار در ازای نماد رمزارز خود سرمایه دریافت کند. بااین‌حال، پس‌انداز این پول در حساب‌های بانکی بسیار دشوار است. بدیهی است بانک‌ها می‌خواهند بدانند که این همه پول از کجا تأمین شده و چه کسی آن پول را تهیه کرده است که فهمیدن آن می‌تواند تقریبا غیرممکن باشد.

به‌طورکلی، لازمه ایجاد همکاری راه‌حلی انعطاف‌پذیر و بدون ریسک است. رمزارز نسل‌سومی باید اکوسیستمی را فراهم کند که هر بلاک‌چین فردی بتواند با بلاک‌چین دیگری و با سیستم‌های مالی قدیمی خارجی ارتباط برقرار کند؛ بنابراین، بیایید بررسی کنیم کاردانو چگونه قصد دارد قابلیت همکاری را در دنیای رمزنگاری و نظام مالی سنتی افزایش دهد.

دیدگاه کاردانو ایجاد اینترنت بلاک‌چین است. اکوسیستمی را تصور کنید که بیت‌کوین می‌تواند به اتریوم و ریپل بدون نیاز به انجام مبادلات و متمرکز و درنهایت، به‌طور یکپارچه به لایت‌کوین سرازیر شود. به‌همین‌دلیل، نقل‌وانتقال بین‌زنجیره‌ای چیزی است که کاردانو می‌خواهد بدون هیچ واسطه‌ای آن‌ها را اجرا کند. کاردانو می‌کوشد با بهره‌گیری از اجرای زنجیره‌های جانبی این مهم را عملیاتی کند. سایدچین Sidechain به‌عنوان یک مفهوم مدتی است که در محافل رمزنگاری (زنجیره جانبی) شده است. این ایده بسیار سرراست است؛ زیرا با بهره‌گیری از آن زنجیره‌ای موازی خواهید داشت که همراه‌با زنجیره اصلی کار می‌کند و از قرار معلوم، زنجیره جانبی ازطریق یک گیره دوطرفه به زنجیر اصلی متصل خواهد شد.

کاردانو از زنجیره‌های جانبی مبتنی‌بر تحقیقات کیائیاس میلر و زیندروس (KMZ) شامل اثبات غیرتعاملیِ اثبات کار پشتیبانی خواهد کرد. به‌گفته هاسکینسون، ایده زنجیرهای جانبی از دو عنصر دریافتِ نسخه فشرده بلاک‌چین و ایجاد قابلیت همکاری بین زنجیره‌ها سرچشمه می‌گیرد.

کاردانو برای چه کارهایی استفاده می‌شود؟
وقتی نوبت به افزایش قابلیت همکاری با نظام مالی سنتی می‌رسد، کاردانو می‌خواهد روی سه مانعی تمرکز کند که باعث می‌شود دنیای رمزنگاری با آن‌ها ناسازگار باشد. این سه مانع را فراداده و اسناد و انطباق تشکیل می‌دهند.

فراداده

این امر در فضای ارزهای دیجیتال به‌خوبی برنامه‌ریزی نشده؛ اما در بانکداری سنتی بسیار ضروری است. درحقیقت، این یکی از دلایل اصلی است که بیشتر نهادها برای ارسال ICO تلاش می‌کنند. آن‌ها به‌سادگی فراداده موردنیاز برای ارائه بانک‌ها را ندارند. در نظام مالی کنونی، فراداده از اهمیت بسیار بالایی برخوردار است؛ زیرا می‌تواند در اهدافی مانند کشف و شناسایی منابع و ایجاد سازمان داده‌های الکترونیکی مؤثر باشد.

علاوه‌براین، فراداده‌ها این امکان را فراهم می‌کنند که چگونه داده‌ها در میان سیستم‌های مختلف رَدوبَدل می‌شوند؛ ازاین‌رو، قابلیت همکاری بین طرفین را بهبود می‌بخشد و در حفاظت از منابع بسیار مفید است و به شناسایی خصوصیات و رفتار داده‌ها کمک می‌کند تا درصورت نیاز تکثیر شوند. بااین‌حال، مشکل فراداده این است که بسیار شخصی است و ازآنجاکه داده‌ها دائمی و شفاف در زنجیره بلوک ذخیره می‌شوند، با وضعیتی مواجه هستیم که می‌توان اطلاعات بسیار خصوصی را برای همیشه به بلاک‌چین پیوند دهد. یکی از مباحث اصلی که کاردانو درباره آن تحقیق می‌کند، این است که چگونه فراداده‌ها را به‌طور انتخابی به زنجیره متصل شوند.

اسناد

اسناد همانند آبرداده‌ها، ازطریق انتساب، نام افراد درگیر در معاملات مشخص می‌شود؛ اما آیا اساسا معامله خاص به تمامی افراد نسبت داده می‌شود؟ اگر بلاک‌چین انتساب را به‌طور دائمی به خود برطرف کند، حریم خصوصی افراد درگیر را بسیار خدشه‌دار می‌کند؛ ازاین‌رو، کاردانو در نظر دارد کاربران خود را قادر سازد که اسناد را در هر زمان که لازم باشد، پخش کنند.

انطباق

مانع سوم انطباق است. انطباق شامل عواملی مانند KYC (مشتری خود را بشناسید)، AML (مبارزه با پول‌شویی)، ATF (تأمین مالی ضد تروریسم) و... است. همچنین، از انطباق برای بررسی مشروعیت معامله استفاده می‌شود.، از انطباق برای اطمینان از انجام‌ندادن معامله برای اهداف شرورانه (مثلا پول‌شویی) استفاده می‌شود. درحالی‌که دنیای رمزنگاری در این زمینه واقعا مفید واقع نشده، در دنیای بانکداری بسیار حیاتی است که باید تاریخچه و مشروعیت هر معامله شناخته شود. آنچه کاردانو در حال تحقیق درباره آن است، چگونگی استفاده از فراداده و اسناد همراه‌با انطباق برای کمک به کاربران در هر زمانی است که آن‌ها به تعامل با بانک‌ها نیاز دارند.

پایداری

سرانجام، به ستون سوم یعنی پایداری می‌رسیم. به‌گفته هاسکینسون، این سخت‌ترین مرحله برای غلبه بر مشکلات محسوب می‌شود و بدان‌معنی است که کاردانو چگونه قصد دارد هزینه‌های توسعه و رشد آینده خود را تضمین کند. معمولا برای توسعه پلتفرم و ایجاد برخی پیشرفت‌ها در سیستم، به اعطای کمک‌های مالی و ICOها نیاز خواهد بود. بااین‌حال، هر دو روش با مسئله‌ای واحد دست‌وپنجه نرم می‌کنند. با حمایت‌کردن مشکل تمرکز احتمالی ایجاد خواهد شد. اگر شرکت بزرگی مقدار زیادی کمک بلاعوض به شرکت مبتنی‌بر بلاک‌چین بدهد، ممکن است مسیر تحولات موجود در سیستم را هدایت کنند و تحت‌تأثیر خود قرار دهد. با ICOها این مانند تکان ناگهانی پول، بدون داشتن مدل‌های پایدار است و رمزی کاملا غیرضروری به اکوسیستم می‌افزاید. با این اوصاف، کاری متفاوت و پایدارتر باید انجام شود. کاردانو قصد دارد از رمزارز دَش DASH الهام بگیرد و سیستم خزانه‌داری ایجاد کند.

ICP

INTERNET COMPUTER

پروژه کامپیوتر اینترنتی (Internet Computer) توسط کمپانی دفینیتی (DFINITY)در سال 2016 با هدف ایجاد تحولی عظیم در مفهوم قراردادهای هوشمند و اینترنت به روی کار آمده است و با سرمایه اولیه 195 میلیون دلار آغاز به کار کره است که حدود 4 میلیون دلار از این سرمایه را با عرضه عمومی توکن خود در سال 2017 کسب نموده است. ایده این پروژه در واقع به اشتراک گذاری قدرت پردازشگر سیستم‌های مختلف با کمک اینترنت در قالب محیط بلاکچین برای اجرای کدهای دستوری در فضای ابری می‌باشد.

در تاریخ 10 می فاز جنسیس مرکوری این پروژه که فاز انتهایی آن است راه اندازی شد، که رسما شروع فعالیت این بلاکچین خواهد بود.

کامپیوتر اینترنتی در واقع با تغییر ماهیت و کاربرد اینترنت آن را به بستری برای اجرای نرم افزارها و یا در واقع یک پردازشگر جهانی تبدیل می‌کند. برنامه نویسان می‌توانند با استفاده از کامپیوتر اینترنتی کدهای خود را مستقیما بر روی اینترنت اجرا کنند و این کدها در واقع در کامپیوترهایی به هم متصل در فضای بلاکچین اجرا خواهند شد.

اجرای مستقیم کدهای نرم افزاری در محیط اینترنت، ایده جالبی است که می‌تواند مزایای بسیاری داشته باشد. از جمله امنیت بالایی که از ماهیت غیر متمرکز بودن بستر اجرای نرم افزارها ناشی می‌شود.

در 18 دسامبر سال 2020 ، DFINITYشبکه آلفای ICP را راه اندازی کرد. در گام آخر به سوی تمرکززدایی، در 10 مه 2021 ، دفینیتی اینترنت کامپیوتر را با دامنه‌ی عمومی راه اندازی کرد. این نقطه عطف مهم به این معنی است که اینترنت اکنون به عنوان یک کامپیوتر جهانی به صورت غیرمتمرکز عمل می کند. این کار با انتشار تمام کدهای منبع اینترنت در دامنه عمومی و همچنین ارائه توکن ICPبه دهها هزار نفر از اعضای جامعه برای اداره شبکه ICPمشخص شده است

دومینیک ویلیامز بنیانگذار DFINITYاست. او یک نظریه پرداز رمزنگاری، مسئول اختراع رله آستانه، اجماع شکاف احتمالی و سایر تکنیک های جدید رمزنگاری، کارآفرین و عضو اولیه انجمن های فنی بیت کوین و اتریوم است. پیش از این، او رئیس و CTOآزمایشگاه های Stringبود. او از پیشگامان اولیه دیفای در Mirror Labsو بنیانگذار و مدیرعامل Fight My Monster، یک بازی MMOبرای کودکان که برای میلیون ها کاربر مقیاس گذاری شده بود. او چندین استارت آپ مانند System7، Airdocsو Smartdrivezرا نیز تأسیس کرد. او فارغ التحصیل از King’s College Londonاست.

به عنوان مثال کامپیوترهای اینترنتی سیستم عامل اختصاصی خود را دارند که به دلیل ماهیت غیر متمرکز بودن، به صورت کامل، غیر قابل تغییراند و بنابراین از دسترس هکرها در امان خواهند بود و در نتیجه نیازی به استفاده از فایروال ها، سیستم های پشتیبانی و آنتی ویروس نخواهد بود.

کامپیوتر اینترنتی توسط پروتکلی غیر متمرکز به نام ICP (Internet Computer Protocol) مهیا می‌شود. قدرت پردازش توسط سیستم‌هایی مجزا در نقاط مختلف تامین می‌شود که در محیط بلاکچین به یکدیگر متصل شده اند و سیستمی یکپارچه را تشکیل می‌دهند که امنیتی در حد بلاکچین های قرارداد هوشمند خواهد داشت.

این ارتباط توسط استاندارد جهانی اینترنت (DNS) برقرار می‌شود و کاربران می توانند با مرورگرهای اینترنت و یا گوشی‌های هوشمند به این شبکه متصل شوند. همچنین این پروژه از زبان برنامه نویسی اختصاصی خود به نام Motokoاستفاده خواهد کرد.

این بلاکچین قادر خواهد بود از قراردادهای هوشمند ابتدایی تا نرم افزارهای پیچیده‌ای در قالب دیفای (DeFi)را پشتیبانی کند و ارز نظر تئوری میزبانی برای تمام نرم افزارها و قراردادهای هوشمند فعلی باشد.

بلاکچین بر اساس سیستم **اثبات سهام** فعالیت خواهد کرد و توکن ICP توسط سهامداران برای تضمین امنیت بلاکچین در شبکه قفل خواهد شد (Staking) تا حق رای در تصمیم گیری‌های شرکت را به آنها، عطا کند.

این توکن همچنین ابزاری برای ارتباط کاربران نرم افزارها و و توسعه دهندگان به منظور پرداخت هزینه‌ها و کارمزدها استفاده خواهد شد.

هرچند تیم توسعه دهندگان دفینیتی تمایل ندارند این توکن به صورت یک واحد پولی در نظر گرفته شود و از توسعه دهندگان نرم افزارها درخواست کردند توکن‌های اختصاصی خود را در شبکه ایجاد کنند و در عوض توکن ICP در سیکل‌هایی به عنوان تثبیت کننده پلتفرم و تامین امنیت واحد های پردازشگر غیر متمرکز، به کار خواهد رفت.

پلتفرم ارائه دهنده ارز دیجیتال ICPاست در ساختار خود از الگوریتم اثبات سهام یا PoSاستفاده می نماید و مبتنی بر این الگوریتم می باشد. ارز دیجیتال ICPهمانند دیگر رمزارزهایی که مبتنی بر الگوریتم PoSهستند، قابلیت استخراج ندارد.

در حال حاضر استخراج رمزارزها با استفاده از دستگاه های با توان پردازش بالا امکان پذیر است و برای رمزارزهایی امکان پذیر است که از الگوریتم اثبات کار یا PoWدر ساختار خود استفاده می نمایند و مبتنی بر این الگوریتم هستند.

پلتفرم ارز دیجیتال ICP ویژگی هایی را به ارمغان می آورد که شامل موارد زیر است:

1.**امنیت**: پلتفرم ارز دیجیتال ICPایعنی اینترنت کامپیوتر با مکانیزم اجماع چهار لایه مبتنی بر اثبات سهام PoSتغذیه می شود. که این شامل یک لایه هویت، یک لایه بلاکچین و یک لایه اسناد رسمی است. در کنار هم، این لایه ها امنیت و مقاومت قابل اثبات را در برابر حمله فراهم می کنند در حالی که عدم تمرکز را حفظ می کنند و اطمینان حاصل می کنند که شبکه می تواند از میلیون ها شرکت کننده پشتیبانی کند.

2.**برخوردار بودن از تیم بنیانگذاری قوی**: پروژه اینترنت کامپیوتر توسط یکی از گسترده ترین تیم ها در فضای رمزنگاری در حال کار است یا به نقل از DFINITY، این پروژه توسط برجسته ترین تیم صنعت مهندسان کامپیوتر ساخته شده است

ICP Token چه کاری انجام می دهد؟

تسهیل حاکمیت شبکه: توکن های ICPرا می توان قفل کرد تا سلولهای عصبی ایجاد شود که با رأی دادن در حاکمیت شبکه مشارکت دارند. و از این طریق می توانند جوایز اقتصادی کسب کنند.

تولید چرخه برای محاسبه: ICP ذخیره ارزش منبع را فراهم می کند که می تواند به چرخه تبدیل شود. محاسبه توان در سوختی که هنگام مصرف سوزانده می شود. ICP را با سرعت متغیری به چرخه تبدیل می کند. بنابراین برای اطمینان از اینکه کاربران شبکه می توانند همیشه چرخه های جدیدی را با هزینه تقریباً ثابت به صورت واقعی ایجاد کنند. و طوری انتخاب می شود که هزینه دستیابی به سوخت قابل پیش بینی باشد.

پاداش دادن به مشارکت کنندگان: شبکه ICP قوانین جدیدی را برای پاداش دادن و تشویق افرادی که نقش مهمی دارند وضع کرده. از جمله: الف) ارائه پاداش رأی دادن به کسانی که در حکومت مشارکت می کنند. ب) ارائه جوایز به کسانی که ماشین های گره میزبان شبکه هستند و ج) سایر فعالیتهای متفرقه.

FEG TOKEN

توکن فگ یک ارز دیجیتال پیشرو در حوزه دیفای به حساب می آید

ایده اصلی پروژه فگ تهیه شبکه معاملات غیرمتمرکز می باشد که در بستر بلاکچین اتریوم ایجاد شده است.

به ارز دیجیتال فگ، توکن تورم نیز گفته می شود که حداکثر گردش آن ۱۰۰ کوادریلیون است. نکته شایان ذکر دیگر این است که در هر معامله، مالیات ۱ درصد به دارندگان تقسیم می شود و ۱ درصد دیگر سوزانده خواهد شد، به همین خاطر این موضوع دارندگان را به هولد کردن این ارز تشویق می کند و عرضه را در بازار این رمزارز کاهش می دهد.

در واقع با کاهش عرضه، ارزش رمز افزایش نیز در طول زمان افزایش خواهد یافت. این رابطه متناسب با عکس یک مدل عرضه و تقاضا را ایجاد می کند، همچنین هیچ محدودیتی در تعداد سوزاندن توکن ها وجود نخواهد داشت. نکته جالبی که در این خصوص باید در نظر داشته باشید این است که پروژه فگ به صورت کامل غیرمتمرکز می باشد و هیچ کس مالک اصلی فگ نیست.

هر معامله میزان سوختگی ۱ درصد را به وجود می آورد که موجب کاهش تامین وقت اضافی FEGمی گردد.
FEGبرنامه ریزی شده است تا با انتشار محصولات نوآورانه که پایداری رمز را تضمین می کند، به فضای ارز دیجیتال پیشرفت به مراتب بیشتری را هدیه می کند.

به این خاطر که توکن ارز دیجیتال فگ در شبکه اتریوم قرار دارد و با استاندارد ERC-20به وجود آمده است، می توانید برای ذخیره سازی توکن های فگ، از هر کیف پول سازگار با ETHاقدام نمایید؛ از این روی ارز دیجیتالی فگ را می توانید در کیف پول های سخت افزاری لجر نانو اس، لجر نانو ایکس، ترزور، کیپ کی ذخیره کنید و همچنین کیف پول های نرم افزاری مانند متامسک، تراست والت، کوین بیس و ... نیز می توانند در راستای نگهداری امن و مدیریت ارز دیجیتالی فگ خدمات خوبی را ارائه دهند.

آینده این ارز دیجیتال به این صورت است که با انتشار محصولات نوآورانه که پایداری رمز را تضمین می کند، به فضای رمزنگاری پیشرفت بیشتری کند. البته باید در نظر داشته باشید که هیچ پشتوانه فناوری از ارز دیجیتال فگ پشتیبانی نمی کند! به عبارتی این ارز میم کوین به حساب می آید و نمی توان برای سرمایه گذاری بلند مدت بر روی این سرمایه گذاری حسابی باز کرد. همانطور که گفتیم توکن فگ دارای تورم است و حداکثر گردش آن ۱۰۰ کوادریلیون است.

در هر معامله، مالیات ۱ درصد به دارندگان توزیع می‌شود و ۱ درصد دیگر سوخته خواهد شد. از آنجایی که هیچ محدودیتی در تعداد سوزاندن توکن ها وجود ندارد، می توانیم این برداشت را داشته باشیم که می توانند تعداد بیشتری را از بین ببرند و به این ترتیب قیمت را افزایش دهند. پیش بینی قیمت ارز دیجیتالی فگ برای سال های آینده به شرح زیر می باشد :

قیمت ارز تا پایان سال ۲۰۲۱ : ۰,۰۰۰۰۰۰۰۴ دلار

قیمت ارز تا پایان سال ۲۰۲۲ : ۰,۰۰۰۰۰۰۰۵ دلار

قیمت ارز تا پایان سال ۲۰۲۶ : ۰,۰۰۰۰۰۰۱ دلار

قیمت ارز تا پایان سال ۲۰۲۸ : ۰,۰۰۰۰۰۰۲۲ دلار