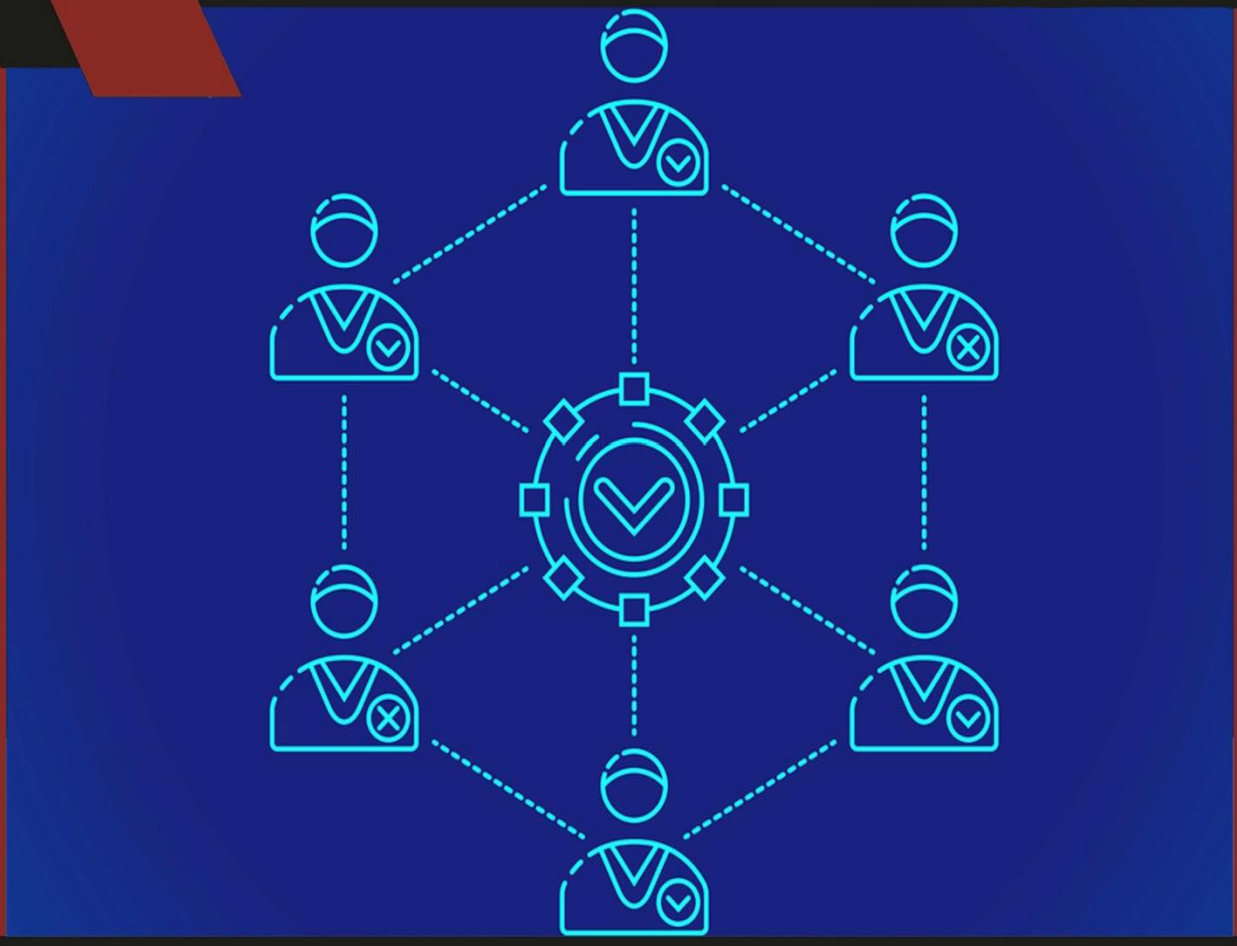
بررسی انواع الگوریتم های اجماع Consensus در ارزهای دیجیتال



نویسنده: امید فدوی

بررسی انواع پروتکل هایا الگوریتم های اجماع در بلاک چین و ارزهای دیجیتال و تفاوت آنها

در این مقاله می خواهیم انواع الگوریتم های اجماع را به شما معرفی کنیم. این الگوریتم های اجماع که به نام الگوریتم های ارز دیجیتال نیز شناحته می شوند در واقع راه کاری هستند که هر کدام از ارز های دیجیتال و شبکه های بلاک چین برای خود استفاده می کنند. در این مقاله لیست الگوریتم ارزهای دیجیتال را به شما معرفی می کنیم و مزایا و معایب هر کدام از آن ها را برایتان بیان می کنیم.

فهرست مطالب

غیر متمرکز بودن

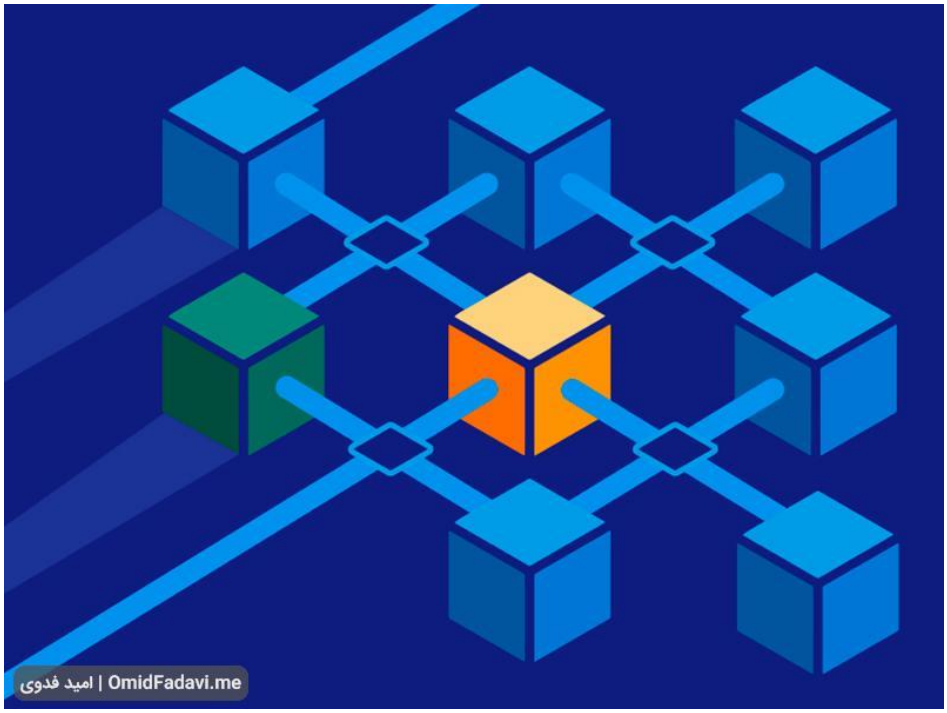
یکی از ویژگی های بلاک چین و در پی آن ارز های دیجیتال که همیشه هم در مقالات به آن اشاره کرده ایم، غیر متمرکز بودن آن ها است. اگر بخواهیم به زبان ساده غیر متمرکز بودن را تعریف کنیم باید بگوییم در این حالت اطلاعات و مواردی که در سیستم وجود دارند در یک سرور مرکزی ذخیره و یا پردازش نمی شوند. در این حالت تمامی اطلاعات به صورت پخش شده در چندین دستگاه نگهداری می شود. به سرور هایی که این اطلاعات را نگهداری می کنند به اصطلاح نود یا گره گفته می شود.

امنیت

بزرگ ترین دلیلی که باعث شده است از این نوع دفتر کل های توزیع شده استفاده شود، امنیت بسیار بالا و همچنین اطمینان از عدم نابودی و از بین رفتن داده ها است. در این نوع بلاک چین ها حتی اگر اطلاعات یک کامپیوتر به کلی از بین برود هیچ جای نگرانی وجود ندارد زیرا این اطلاعات در هزاران و یا میلیون ها دستگاه دیگر وجود دارد.

حال اگر این اطلاعات نیاز به تغییر و به روز رسانی داشته باشند این اتفاق باید در تمام گره ها رخ دهد. برای این کار مفهومی به نام الگوریتم اجماع مورد استفاده قرار می گیرد.

الگوریتم اجماع به زبان ساده به معنی روش هایی برای به توافق رسیدن اعضای درون شبکه است.



کاربرد های الگوریتم اجماع

به طور کلی می توان سه مورد زیر را برای کاربرد های این الگوریتم ها ذکر کرد:

- تصمیم گیری برای این که آیا یک تراکنش صلاحیت تایید شدن و در ادامه ذخیره شدن بر روی دفتر کل را دارد و یا خیر
- انتخاب گره ها (نود ها) برای مدیریت امور انجام شده بر روی دفتر کل
- تضمین یکدست سازی اطلاعات بر روی سیستم های سرویس دهنده به شبکه

الگوریتم های اجماع

سیستم توافق توزیع شده و یا همان به اصطلاح «اجماع»، به این معنا است که در زمان ارسال و یا دریافت پول و ارز از هر شخص، دیگر نیاز نباشد تا به سرویس های شخص ثالث مانند بانک ها و یا موسسات مالی اعتماد کنید.

در روش های پرداخت به صورت سنتی، شما باید به یک سرویس شخص ثالث که هر دو طرف معامله با آن موافق باشید اعتماد کنید تا بتوانید تراکنشتان را انجام دهید. برای مثال شما برای ارسال و یا دریافت پول باید به سرویس هایی مانند بانک ها، پی پال، مستر کارت و یا ویزا کارت اعتماد کنید. این سرویس ها تمام تاریخچه تراکنش های شما و همچنین موجودی شما را ذخیره و نگه داری می کنند.

اما در مورد ارز های دیجیتال مانند بیت کوین همچین موردی وجود ندارد. در ارز های دیجیتالی هر شخص یک کپی از دفتر کل توزیع شده را دریافت می کند و به صورت مستقیم این امکان را دارد تا بتواند اطلاعات مورد تایید خود را در این دفتر وارد کنند. در ادامه مقاله مهم ترین الگوریتم های اجماع را برایتان معرفی می کنیم.

اگر می خواهید خودتان دست به کار شده و ارز دیجیتال مورد نظرتان را استخراج نمایید حتما از ***آموزش استخراج ارز دیجیتال*** دیدن فرمایید. در این آموزش تمام نکات و آموزش ها به زبان ساده و عملی به شما نمایش داده شده و اگر کاربر مبتدی هستید نیز می توانید از این آموزش به خوبی استفاده نمایید.

انواع الگوریتم های اجماع: الگوریتم گواه اثبات کار (Proof of Work)

پروتکل گواه اثبات کار، پروتکلی است که ساتوشی ناکاموتو برای بیت کوین پیاده کرده است. ناکاموتو این الگوریتم را برای انتخاب گره ها در بیت کوین انتخاب کرده است و آن بیشتر برای محافظت در برابر خطا های بیزانس استفاده می شود. از جمله مشکلاتی که با این الگوریتم حل می شود مشکل دو بار خرج کردن پول ها است.

یک گره در شبکه وظیفه دارد تا یک مسئله رمزنگاری شده را حل کند. در این حالت، احتمال یافتن پاسخ درست به میزان تلاش و قدرت محاسبه بستگی دارد. یافتن پاسخ مسئله ها بسیار دشوار است و فقط با حدس زدن می توان به جواب درست دست پیدا کرد.

بنابراین باید این طور به شما بگوییم:

- هر گره در شبکه می تواند برای پیدا کردن جواب مسئله تلاش کند
- تعداد زیادی از گره ها در شبکه بیت کوین برای پیدا کردن جواب در مدت زمان معینی تلاش می کنند. (در شبکه بیت کوین این مدت زمان ۱۰ دقیقه است)
- راه حل را تنها می توان به صورت تصادفی پیدا کرد.

گره مخرب

گره ای که بخواهد به صورت مخرب در شبکه فعالیت کند، فرصت بسیار کمی برای وارد کردن بلاک مخرب در شبکه دارد. این احتمال زمانی زیاد می شود که فرد یا گروه حمله کننده بتواند حداقل ۵۱ درصد از کل نیروی موجود در شبکه را در اختیار داشته باشد. به همین دلیل می توان گفت روش گواه اثبات کار یک سیستم غیر قابل نفوذ را ارائه داده است. این سیستم تنها در حالتی قابل نفوذ می شود که بتوان حداقل ۵۱ درصد نیروی شبکه را تامین کرد.

گاهی اوقات ممکن است که بیشتر از یک گره و به صورت هم زمان به جواب مسئله دست پیدا کنند. هنگامی که این اتفاق رخ دهد، هر یک از گره های یابنده جواب، یک بلاک را پیشنهاد می دهد و آن را برای شبکه ارسال می کند.

در این حالت، این بلاک ها توسط بلاک های کناری برداشت می شود و به صورت موقت یک بلاک چین شکل گرفته و بلاک های جدید به آن زنجیره اضافه می شوند. در نهایت پروتکل گواه اثبات کار، شاخه ای که طول بیشتری دارد و طولانی تر است را به عنوان زنجیره رسمی شناسایی می کند و سایر بلاک ها را از بین می برد.

نقاط قوت الگوریتم PoW

در شبکه بیت کوین هر گره ای که برای ایجاد بلاک جدید موفق عمل کند و انتخاب شود، بابت فعالیت در شبکه و ثبت تراکنش ها پاداش دریافت می کند. این پاداش به صورت بیت کوین به آن گره داده می شود.

از آن جا که انجام محاسبات و پیدا کردن جواب درست مسئله کاری بسیار سخت و البته پر هزینه می باشد، ماینر های فعال در شبکه معمولا بر روی یک شاخه از بلاک چین تمرکز می کنند. آن ها شاخه ای را انتخاب می کنند که به نظر می رسد به عنوان شاخه اصلی شناخته می شود.

نقاط ضعف الگوریتم PoW

چندین نقطه ضعف شناخته شده برای این الگوریتم وجود دارد که از مهم ترین آن ها می توان به هزینه ها و مصرف انرژی بسیار بالای آن اشاره کرد. علاوه بر آن، موارد زیر را هم به لیست نقطه ضعف های این الگوریتم اضافه کنید:

استخراج متمرکز

همان طور که می دانید در بخش پردازنده های کامپیوتری یا همان CPUها، اختلافات زیادی در بین مدل های مختلف و قدرت های آنان وجود دارد. از این رو به طور معمول افرادی که از سیستم های با قدرت پایین استفاده می کنند، نسبت به افراد با سیستم های قدرتمند شانس بسیار کمتری برای حل مسئله و دریافت پاداش دارند.

در نتیجه، الگوریتم گواه اثبات کار نمی تواند الزامات الگوریتم اجماع را براورده سازد. بر اساس این الزامات، گره های تصادفی باید در میان گسترده ترین جمعیت ممکن از شرکت کنندگان و ماینر ها انتخاب شوند. وجود این ضعف باعث می شود تا خطر متمرکز شدن استخراج بالا رود. یکی از این خطر ها استخر های بزرگ پول هستند.

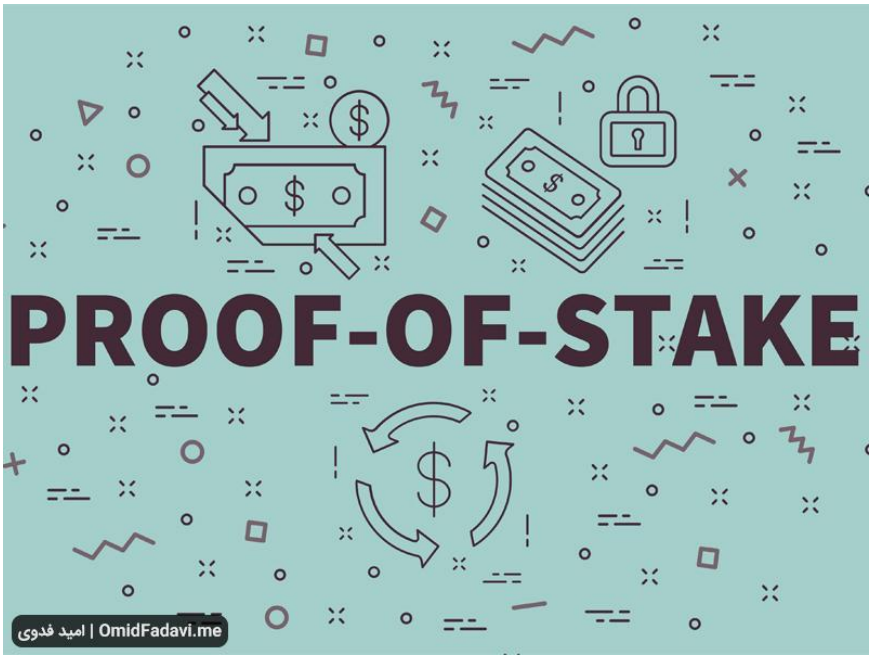
تاخیر زمانی زیاد

در شبکه بیت کوین، بلاک های جدید هر ۱۰ دقیقه ایجاد می شوند. در نتیجه ی این زمان، انتظار برای تایید شدن یک بلاک تولید شده ممکن است تا ساعت ها زمان ببرد. دلیل این اتفاق هم این است که یک تراکنش حتما باید توسط گره هایی که در زنجیره اصلی وجود دارند تایید شود. علت این کارهم این است که مطمئن شویم بلاک تولید شده به شاخه اصلی در بلاک چین اصلی وصل شده است.

نرخ پایین تراکنش

حداکثر بلاک های تایید شده توسط الگوریتم گواه اثبات کار در شبکه ارز دیجیتال بیت کوین، مقدار هفت تراکنش در هر ثانیه است. این مقدار با توجه به تعداد بالای تراکنش ها در شبکه بسیار ناچیز است.

انواع الگوریتم های اجماع: الگوریتم گواه اثبات سهام (Proof of Stake)



الگوریتم گواه اثبات سهام و یا به طور خلاصه PoSیکی دیگر از الگوریتم های اجماع بسیار معروف و پر کاربرد در دنیای بلاک چین است. در این الگوریتم، بلاک های جدید به جای آن که استخراج شوند، ساخته می شوند. در این الگوریتم، گره ی انتخاب شده برای ایجاد شدن بلاک بعدی، از طریق یک فرایند به صورت تصادفی انتخاب می شود. این انتخاب شدن البته به دارایی ذخیره شده در کیف پول مربوط به آن گره هم بستگی دارد. در این الگوریتم هیچ کدام از گره های نمی توانند نوبت خود را پیش بینی کنند.

در این الگوریتم تعداد مشخصی از سکه ها در استخر سهام نگهداری می شود تا شانس ایجاد بلاک جدید را خریداری کنند.

مقایسه با الگوریتم اثبات گواه کار

در الگوریتم اثبات گواه کار، به ماینر ها برای حل کردن مسئله ریاضی و در ادامه آن تایید شدن تراکنش ها و ایجاد شدن بلاک های جدید پاداش داده می شد. در الگوریتم اثبات گواه سهام اما این خالق بلاک جدید است که نسبت به میزان سرمایه اش یک راه قطعی را انتخاب می کند. در نتیجه در این روش هیچ پاداشی در کار نیست. در این الگوریتم ماینر فقط کارمزد تراکنش ها را دریافت می کند.

البته باید این نکته را هم به شما بگوییم که در الگوریتم اثبات گواه سهام به جای استفاده از کلمه ماینر، از کلمه Forgerاستفاده می شود.

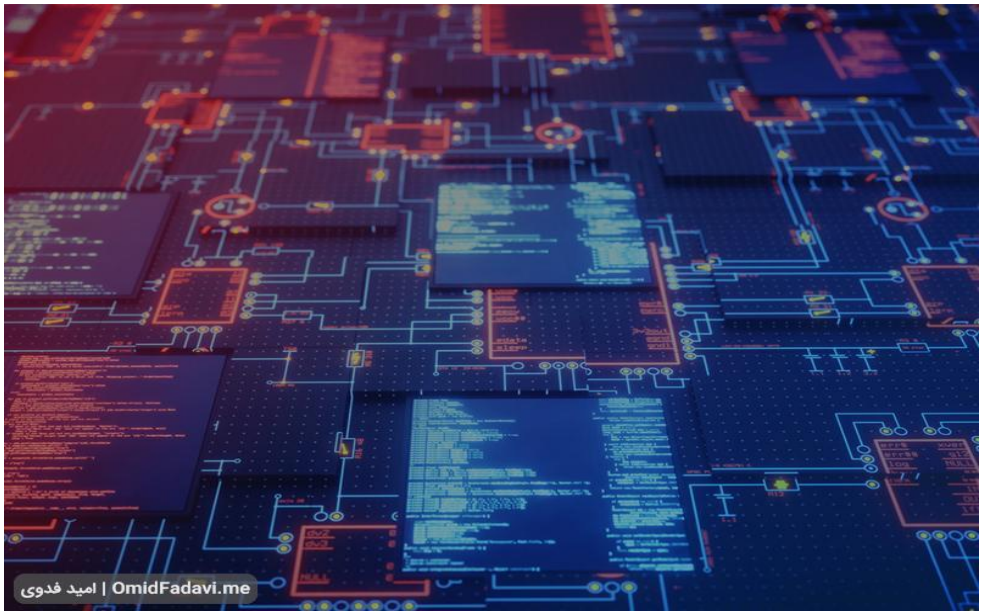
نقاط قوت الگوریتم (PoS)

این الگوریتم در مقایسه با الگوریتم گواه اثبات کار از مزایای بیشتری برخوردار است. الگوریتم گواه اثبات سهام انرژی و قدرت محاسباتی بسیار زیادی مصرف نمی کند. این الگوریتم با جلوگیری از ایجاد استخر های استخراج متمرکز، خطر حملات مخرب را به طور چشمگیری کاهش می دهد. همچنین در این روش با توجه به این که سازنده هر بلاک، مالکیت بخشی از آن سکه ها را نیز بر عهده دارد، کسی که وظیفه محافظت از سکه ها را دارد، خود مالک بخشی از آن ها نیز هست.

نقاط ضعف الگوریتم (PoS)

یکی از نقاط ضعفی که الگوریتم گواه اثبات سهام با آن رو به رو است در خطر نبودن سهام داران می باشد. یک ماینر در شبکه می تواند در زمان هایی که یک انشعاب ایجاد می شود، با هر دو شاخه همراهی کند. این کار باعث جلوگیری از اجماع بین گره ها می شود و خطر دو بار خرج کردن را به همراه دارد.

انواع الگوریتم های اجماع: الگوریتم گواه اثبات فعالیت (Proof of Activity)



این الگوریتم در اصل یک ترکیب از دو الگوریتم قبلی یعنی گواه اثبات کار و گواه اثبات سهام می باشد. در این روش در ابتدا ماینر های نوع PoWمقدار هش مربوط به بلاک را حل می کنند. سپس با حل کردن آن، بلاک های جدید و پیشنهادی را به شبکه ارسال می کنند. پس از این که این عملیات انجام شد و پیشنهاد به شبکه ارسال شد، شبکه از هش ارسال شده استفاده می کند و عدد شبه تصادفی مانند Nرا ایجاد می کند. این عدد شبه تصادفی به کلید عمومی دارندگان آن سکه متصل است.

سپس سهام داران و افراد موجود در PoS بلاک را امضا و تایید می کنند. درخواست در ابتدا برای اولین ماینر PoSارسال می شود. در صورتی که از او پاسخی دریافت نشود، شبکه به طور خودکار درخواست را برای گره بعدی می فرستد. این چرخه آن قدر ادامه پیدا می کند تا در نهایت بلاک تایید شود.

نقاط قوت الگوریتم (PoA)

با استفاده از این روش، ماینر های PoS بعد از این که مسئله حل شد درگیر بلاک می شوند. همان طور که گفتیم حل کردن مسئله در این الگوریتم وظیفه ماینر های PoW می باشد. با استفاده از این روش، حتی اگر ماینر های PoS بیشتر از ۵۰ سکه ها را نیز در اختیار داشته باشند باز هم نمی توانند در شبکه اخلال ایجاد کنند و کنترل آن را در دست بگیرند.

علاوه بر موارد بالا، اگر مقدار عدد تصادفی Nبیشتر از یک باشد، نظر سایر ماینر ها نیز اهمیت دارد.

نقاط ضعف الگوریتم (PoA)

این الگوریتم نیاز به تبادل اطلاعات به صورت دائمی دارد. برای این که ترافیک شبکه کاهش یابد، الگو یا همان بلاک پیشنهادی شامل لیست تراکنش ها نمی باشد. این لیست توسط آخرین ماینر که بلاک را امضا می کند به شبکه اضافه می شود.

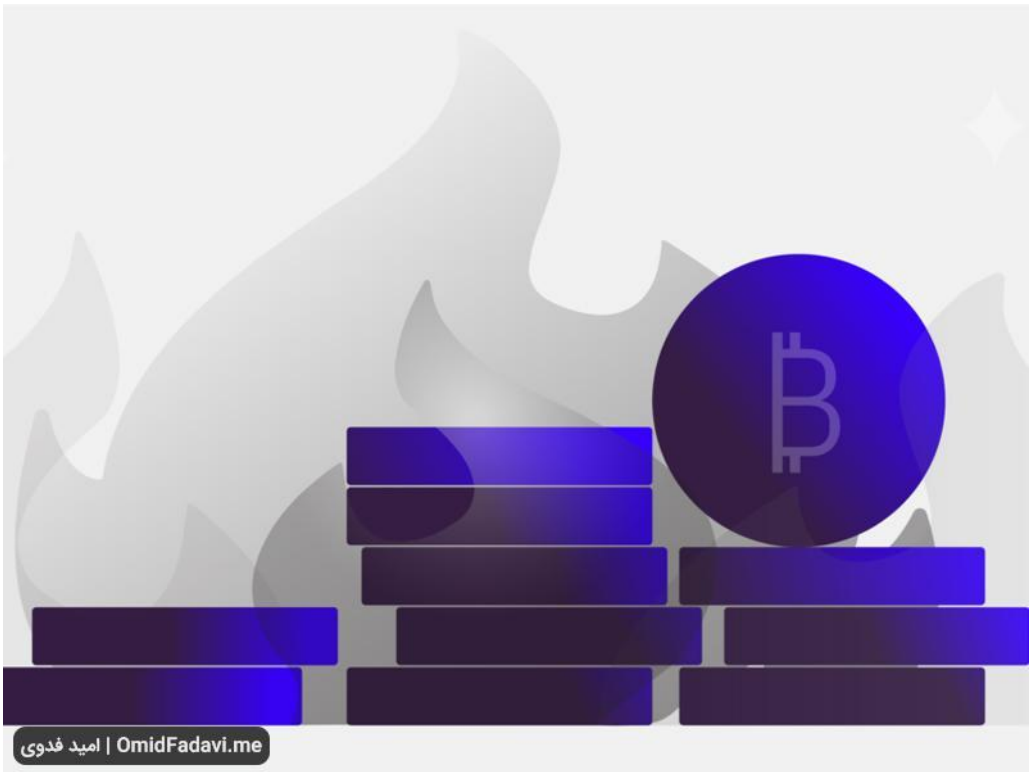
برای مثال: اگر عدد تصادفی Nبرابر با ۳ باشد و فقط ده درصد از ماینر ها در شبکه آنلاین باشند، آن گاه ماینر های PoW باید پیش از آن که یک بلاک امضا شود، ۱۰۰۰ بلاک پیشنهادی را تولید کنند.

پروژه Meissa

این پروژه یکی از برنامه هایی است که قصد دارد از این الگوریتم در برنامه خود استفاده کند. آن ها می خواهند با استفاده از این الگوریتم از تمام گره ها یا همان کامپیوتر هایی که در سراسر شبکه فعال هستند استفاده کنند و با استفاده از قدرت آن ها به شکل کاملا ایمن، یک ابر کامپیوتر جهانی توزیع شده ایجاد کنند. این ابر کامپیوتر برای هدف های مختلفی مانند پروژه های غیر متمرکز، سیستم های انتقال پول و به اشتراک گذاشتن منابع مورد استفاده قرار می گیرد.

این الگوریتم علاوه بر نام فوق، با عنوان Delegated Proof of Activity یا به طور خلاصه DPoA نیز شناخته می شود. این الگوریتم هم از همان اصول PoA استفاده می کند و تفاوتی در آن ها وجود ندارد.

انواع الگوریتم های اجماع: الگوریتم گواه اثبات سوزاندن Proof of Burn



در این الگوریتم، انتخاب گره هایی که قرار است نقش ماینر ها را در شبکه بازی کنند، با توجه به سکه هایی است که این گره ها سوزانده اند. سوزاندن در ارز های دیجیتال به این معنا است که بخشی از سکه ها از چرخه معاملات خارج شوند. برای مثال می توان سکه ها را با ارسال آن ها به آدرس های غیر قابل برداشت سوزاند. سپس گره های انتخاب شده می توانند فعالیت کرده و تراکنش ها را تایید کنند و پس از آن کارمزد آن ها را دریافت کنند. البته در این روش باید از زمان سوزانده شدن کوین ها مدت مشخصی گذشته باشد تا بتوان مطمئن شد دیگر امکان استفاده از آن ها وجود ندارد.

سوزاندن سکه ها

از نظر گره ها، سوزاندن سکه ها گران تر از نگه داشتن آن ها به شمار می رود. بنابر این، این امکان وجود دارد که یک گره، شبکه را با امضا کردن بلاک ها در زنجیره های موازی فریب دهد.

شاید برای شما هم این سوال پیش آمده است که چه مقدار کوین باید برای این کار سوزانده شود؟ ماینر ها به طور معمول ارز های دیجیتال و رمزنگاری شده خود را با نرخ متوسطی که با میزان کارمزد های هر تراکنش ارتباط دارد می سوزانند. به طور کلی اگر بخواهیم این الگوریتم را با الگوریتم گواه اثبات کار مقایسه کنیم، هزینه استخراج در این الگوریتم پایین تر است. دلیل آن هم تفاوت در سخت افزار های مورد نیاز است که در روش گواه اثبات کار، هزینه سخت افزار بسیار زیاد است.

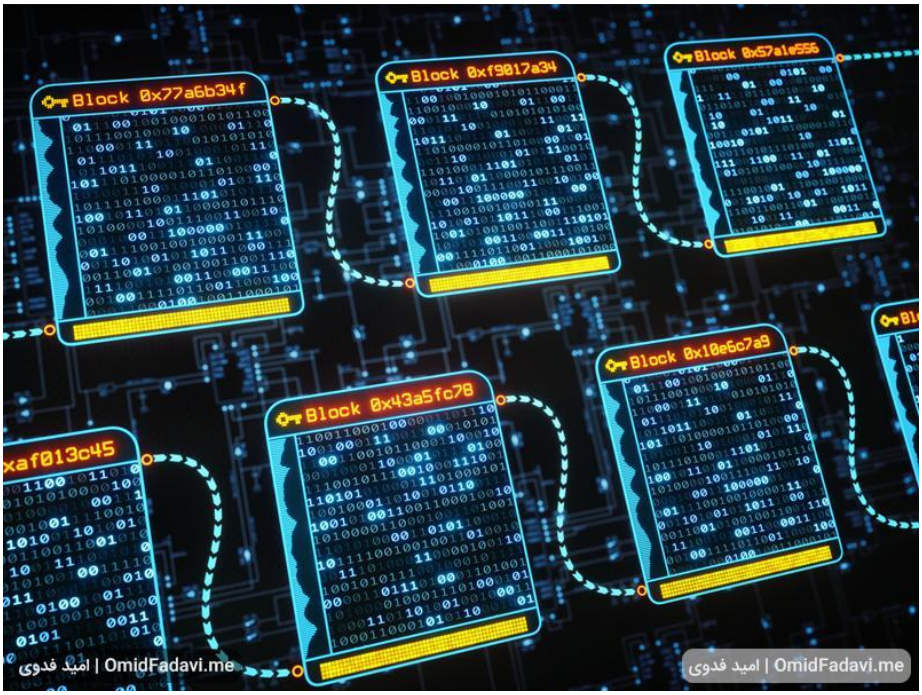
نقاط قوت الگوریتم (PoB)

شما به هیچ سخت افزاری نیاز ندارید. برای استفاده از این الگوریتم تنها باید سکه بسوزانید.

نقاط ضعف الگوریتم (PoB)

این الگوریتم را تنها زمانی می توان استفاده کرد که پیش از آن با استفاده از روش ها و الگوریتم های دیگر سکه را استخراج کرده باشید.

انواع الگوریتم های اجماع: الگوریتم گواه اثبات فضا Proof of Capacity



م اصلی این الگوریتم اثبات فضا می باشد اما به آن الگوریتم اثبات ظرفیت نیز گفته می شود. این الگوریتم برای حل یک چالش که از سوی ارائه دهنده ی سرویس مطرح شده است، یک مقدار غیر اسمی از پول و یا حافظه را اختصاص می دهد. الگوریتم با این کار نشان می دهد که یک فرد سهم مشروعی در یک سرویس را دارد.

این الگوریتم برای اولین بار توسط زیمبووسکی و در سال ۲۰۱۵ معرفی شد.

شباهت به الگوریتم اثبات کار

الگوریتم اثبات فضا از نظر کلی شبیه به الگوریتم اثبات کار می باشد. تفاوت این دو الگوریتم در این است که به جای استفاده از رایانش از فضای ابری استفاده می شود.

این الگوریتم به کارکرد حافظه سخت و همچنین اثبات برگشت پذیر بستگی دارد در عین حالی که بسیار با آن ها تفاوت دارد.

در این الگوریتم، گره ی انتخاب شده برای ایجاد بلاک بعدی از طریق یک فرایند که به صورت شبه تصادفی برگزار می شود انتخاب می شود. در این الگوریتم باید مقداری از حافظه دستگاه و یا همان فضای هارد دیسک را در شبکه به اشتراک بگذارید. در نتیجه می توان این طور عنوان کرد که این روش کمی مانند گواه اثبات کار است. تفاوت آن در این است که به جای توابعی که مخصوص پردازشگر های کامپیوتر است، از توابع مخصوص به خود استفاده می کند.

هر مگابایت حافظه که در شبکه به اشتراک گذاشته شود، در اصل یک بلیط اضافه برای استخراج است. این الگوریتم به شاخه های مختلفی تقسیم می شود اما در نهایت همه ی آن ها شبیه به یکدیگر هستند و فقط کمی جزئیات آن ها با یکدیگر متفاوت است.

نقاط قوت الگوریتم (PoC)

- این الگوریتم مشابه الگوریتم اثبات گواه کار است. در این الگوریتم به جای رایانش از فضا استفاده می شود. در نتیجه این الگوریتم با محیط زیست سازگاری بیشتری دارد
- می توان از این الگوریتم برای تعیین بدافزار در شبکه استفاده کرد
- می توان از آن برای تمهیدات ضد اسپم و یا پیشگیری از حملات رد سرویس استفاده کرد

الگوریم PoC نسبت به الگوریتم گواه اثبات کار عادلانه تر می باشد و همچنین خطر ماینینگ به صورت متمرکز را کاهش می دهد. در این الگوریتم ماینر ها برای ذخیره داده های مفید عمومی در شبکه انگیزه پیدا می کنند.

نقاط ضعف الگوریتم (PoC)

- مشوق سازی در آن سخت است

در این روش مشکل nothing-at-stake وجود دارد. این مشکل در الگوریتم هایی مانند PoCو یا PoW وجود دارد. در این الگوریتم ها گره ها توانایی استخراج را دارند اما لزوما در ارزی که ماین می کنند سرمایه ای ندارند. این موضوع باعث می شود که ماینر ها هیچ گونه تعهدی نسبت به شبکه نداشته باشند.

برای مثال همان طور که گفتیم در روش PoS، ماینر ها حتما در ارزی که استخراج می کنند سهم و نقش دارند. در نتیجه دغدغه و تعهد بیشتری برای سلامت شبکه دارند.

دلیل آن هم این است که در صورتی که به شبکه آسیبی برسد، خود ماینر ها نیز ضرر خواهند کرد.

در الگوریتم PoC یک گره این شانس را دارد تا در یک زنجیره جایگزین نیز شانس خود را امتحان کند. نتیجه ی این کار این است که بسیاری از گره ها این امکان را دارند که به صورت همزمان و بدون صرف منابع بسیار زیاد در زنجیر های مختلف بلاک ماین کنند.

انواع الگوریتم های اجماع: الگوریتم Proof of Elapsed Time

در این الگوریتم گره ها به صورت قرعه کشی انتخاب می شوند. این الگوریتم از محیط اجرای TEE استفاده می کند تا مطمئن باشد فرایند انتخاب به صورت درست برگزار می شود. TEE توسط سخت افزار های خاص و ویژه کمپانی اینتل ارائه می شوند. در این الگوریتم هر تایید کننده بلاک در کوتاه ترین زمان و بر اساس یک تابع مطمئن و قابل اعتماد برای تولید بلاک جدید انتخاب می شود. در این انتخابات، ماینر ها به صورت تصادفی و از سراسر شبکه انتخاب می شوند.

این الگوریتم اغلب بر روی شبکه های خصوصی و شبکه های دارای مجوز استفاده می شود. در این گونه بلاک چین ها افراد برای آن که مجوز دسترسی به شبکه را پیدا کنند باید هویتشان را تایید کنند. این شبکه برای انتخاب گره یک سیستم قرعه کشی منصفانه دارد و تمام اعضای شرکت کننده در آن شانس یکسانی برای انتخاب شدن دارند.

فرایند کار در این شبکه به این صورت است که هر گره باید منتظر یک دوره زمانی بماند. پس از این که این دوره زمانی فرا رسید، اولین فردی که کار را به طور کامل انجام دهد برنده ی بلاک می شود.

این مفهوم برای اولین بار در سال ۲۰۱۶ و توسط کمپانی اینتل طراحی و معرفی شد.

نقاط قوت الگوریتم (PoET)

- هزینه پایین برای مشارکت. با این کار مردم می توانند به راحتی در آن ثبت نام کنند و شبکه غیر متمرکز می شود
- تایید مشروعیت برای انتخاب رهبر برای همه کاربران ساده است
- هزینه ای که برای کنترل فرایند گزینش رهبر پرداخت می شود بخشی از ارزش به دست آمده آن است

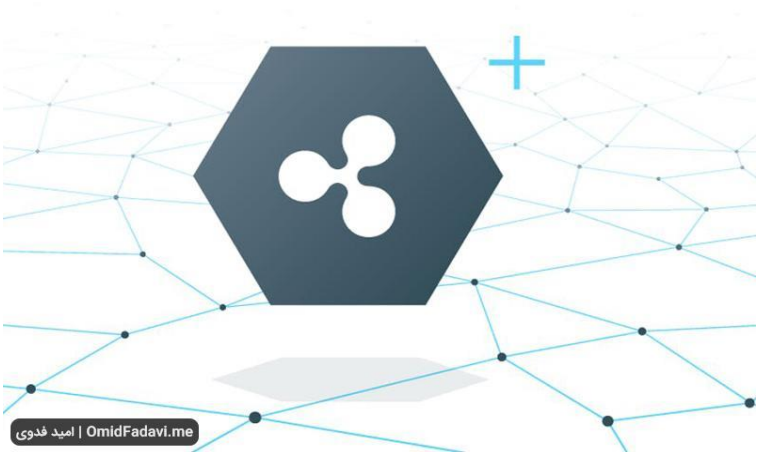
در این الگوریتم نقدینگی کوتاه مدت اهمیت بالایی ندارد. همچنین این الگوریتم مصرف برق و انرژی خیلی زیادی نیز احتیاج ندارد و استخراج با آن ارزان تر انجام می شود. به همین دلایل نیز احتمال افزایش جمعیت ماینر ها وجود دارد و همین مسئله این الگوریتم اجماع را مستحکم تر می نماید.

نقاط ضعف الگوریتم (PoET)

- این پروتکل ارزان است اما برای استفاده از آن می توان از سخت افزار های تخصصی و گران قیمت استفاده کرد. در نتیجه امکان استفاده به صورت انبوه را ندارد
- برای بلاک چین های عمومی مناسب نیست

برای استفاده از این الگوریتم نیاز به سخت افزار های ساخت شرکت اینتل هست.

انواع الگوریتم های اجماع: پروتکل اجماع ریپل



ریپل یک پروتکل و پلتفرم پرداخت است که بر روی بستر بلاک چین پیاده سازی شده است. هدف ایجاد ریپل، استفاده های مالی و ارزی و ایجاد درگاه های پرداخت عنوان شده است. در پروتکل ریپل، هر گره (برای مثال گره X) یک لیست منحصر به فرد دارد. اطلاعات درون این لیست شامل گره های دیگر قابل اعتماد در شبکه توسط گره X است.

در این پروتکل حداقل ۴۰ درصد از گره های موجود در لیست منحصر به فرد گره Xباید در لیست دیگر گره ها نیز باشد. برای این که در این اجماع یک تراکنش تایید شود، باید هر گره مجموعه ای از تراکنش ها را منتشر کند و پس از آن رای گیری از سایر گره های موجود در لیست شروع می شود. پس از انجام رای گیری گره های باید لیست منحصر به فرد خود را در ارتباط با این گره به روز رسانی کنند.

هنگامی که یک مجموعه تراکنش موفق شود حداقل ۸۰ درصد رای از سایر گره ها دریافت کند، آن لیست کاندید به یک بلاک معتبر در شبکه بلاک چین ریپل تقسیم می شود.

انواع الگوریتم های اجماع: پروتکل اجماع استلار

استلار هم مانند ریپل یک پروتکل پرداخت است. این پروتکل بر بستر بلاک چین توسعه یافته است و برای مسائل مالی و ارزی طراحی شده است. این پروتکل برای کار خود از دو مفهوم استفاده می کند. مفهوم اول quorumنام دارد. این مفهوم مجموعه ای از گره های کافی برای رسیدن به یک توافق است.

مفهوم بعدیquorum slice است. این عنوان یک زیر مجموعه برایquorum است و کار آن قانع کردن گره برای رسیدن به توافق است.

در این اجماع برای دست یابی به یک توافق سراسری، quorumها باید تقسیم بشوند.
برای این کار در مرحله اول هر گره رای گیری اولیه در خصوص تراکنش ها را انجام می دهد. سپس هر گره تراکنش های مورد تایید خود را انجام می دهد و به تراکنش های دیگر رای نمی دهد. البته در این میان اگر quorum sliceیک تراکنش را بپذیرد، گره هم آن را قبول می کند.

در مرحله آخر رای گیری کلی انجام می شود و نشانه توافق در سطح شبکه است.

انواع الگوریتم های اجماع: الگوریتم اثبات تاخیر کار (Delayed Proof of Work)

مزایا

- مصرف انرژی به صورت بهینه
- امنیت بالا
- امکان اضافه کردن ارزش به سایر بلاک چین ها توسط تامین به صورت غیر مستقیم بیت کوین (و یا سایر سکه ها) بدون نیاز به هرگونه پرداخت هزینه بابت تراکنش

معایب

- فقط بلاک چین هایی که از اثبات کار و یا اثبات سهام استفاده می کنند می توانند در این اجماع نیز شرکت کنند.

- میزان هش گره های مختلف در وضعیت Notaries باید حتما درج شود. در صورتی که این کار انجام نشود تفاوت میان نرخ هش ها می تواند باعث انفجار شود!

توضیح

این الگوریتم یک روش ترکیبی است. در این روش شما می توانید از یک بلاک چین در حالی استفاده کنید که امنیت آن از قدرت هش یک بلاک چین دیگر تامین شده است. انجام این کار هم به این صورت است که گروهی از نود ها اسناد و داده های مورد نیاز را از بلاک چین اول به بلاک چین دوم ارسال می کنند.

این بلاک چین می تواند برای انجام کار خود از هر دو روش اثبات سهام و اثبات کار استفاده کند و می تواند خودش را به هر نوع بلاک چینی که تمایل دارد متصل کند. در حال حاضر شبکه بیت کوین و نرخ هشی که دارد توانسته است بالاترین سطح امنیت را نسبت به سایر بلاک چین هایی که توسط اثبات تاخیر کار فعالیت می کنند به ارمغان آورد.

اولین سیستم بلاک چین که از این فناوری استفاده کرده است کومودو نام دارد. کومودو به بلاک چین بیت کوین متصل شده است.

انواع گره

این الگوریتم از دو نوع گره پشتیبانی می کند. گره معمولی و گره اسناد.

در این الگوریتم تعداد ۶۴ توسط افرادی که از شبکه نفع می برند، به منظور اضافه کردن بلاک های تایید شده از بلاک چین اثبات تاخیر کار انتخاب می شود.

حال شبکه کومودو برای آن که در بین گره های اسنادی جنگ و درگیری پیش نیاید و میزان کارآمدی شبکه کاهش پیدا نکند، یک روش ماینینگ به صورت دوره ای ایجاد کرده است. این روش بر روی دو گره فعالیت می کند.

در حالت No Notary می توان مانند حالت سنتی و قدیمی اثبات کار فعالیت کرد و در آن گره ها اجازه استخراج بلاک را دارند. در حالتی که Notaryفعال باشد نمایندگان درون شبکه می توانند با نرخ سختی شبکه بسیار پایین تری ماینینگ خود را انجام دهند.

انواع الگوریتم های اجماع: الگوریتم اثبات سهام محول شده (EoS)

مزایا

- مصرف انرژی بهینه شده
- سرعت بالا. این پروتکل زمانی برابر ۰.۵ ثانیه برای هر بلاک دارد.

معایب

- کمی تا قسمتی متمرکز
- شرکت کنندگانی که در این پروتکل سهام زیادی دارند می توانند به خودشان رای دهند تا به یک گره و تایید کننده تبدیل شوند. این مورد اخیرا در این پروتکل زیاد دیده شده است.

توضیح

در این نوع الگوریتم، سهام داران و افرادی که در شبکه فعالیت می کنند می توانند در سیستم رهبرانی را انتخاب کنند و از سمت آن ها رای دهند. همین کار باعث می شود این الگوریتم از الگوریتم اثبات سهام سرعت بیشتری داشته باشد.

در این الگوریتم شاهدان و کسانی که به عنوان تایید کننده در شبکه فعالیت می کنند به ازای تولید هر بلاک کارمزد دریافت می کنند. میزان این کارمزد را سهام داران تعیین می کنند. اگر شاهدان در این شبکه در بازه زمانی که مشخص شده بلاکی تولید نکنند، نوبتشان رد شده و این کار به شاهد بعدی محول می شود. این کار آن قدر ادامه پیدا می کند تا سرانجام یکی از شاهدان کار را انجام دهد.

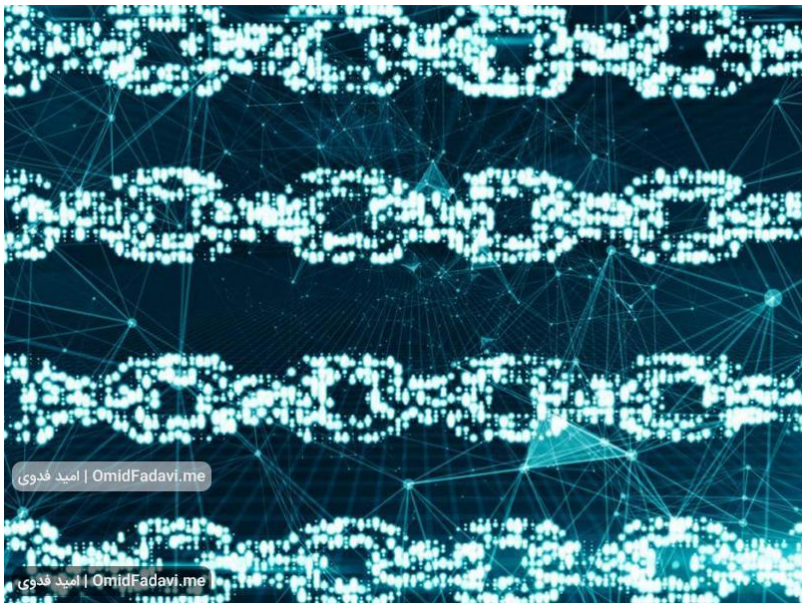
در این الگوریتم به طور معمول، تمامی نود ها در یک زمان با یکدیگر رقابت می کنند تا بلاک های جدید را شکل دهند.

این کار از شکل گیری بلاک های پی در پی از سوی نود ها جلو گیری می کند و همچنین مشکل دو بار خرج کردن را نیز بر طرف می کند.

در این نوع الگوریتم شرکت کنندگان می توانند به جای رقابت کردن با یکدیگر، برای تولید بلاک های جدید با یکدیگر همکاری کنند.

این الگوریتم می تواند با استفاده از متمرکز کردن ساخت بلاک ها به صورت حدودی، انجام سفارشات را بسیار سریع تر از سایر الگوریتم ها انجام دهد. این الگوریتم برای تولید بلاک به زمان بسیار کم ۰.۵ ثانیه نیاز دارد.

انواع الگوریتم های اجماع: الگوریتم اثبات مسئولیت (Proof of Authority)



مزایا

- مصرف انرژی بهینه شده
- سرعت بالا

معایب

- کمی متمرکز است. این الگوریتم قابلیت استفاده در بلاک چین های عمومی را دارا می باشد اما در بخش بلاک چین های خصوصی نیازمند مجوز دسترسی است.

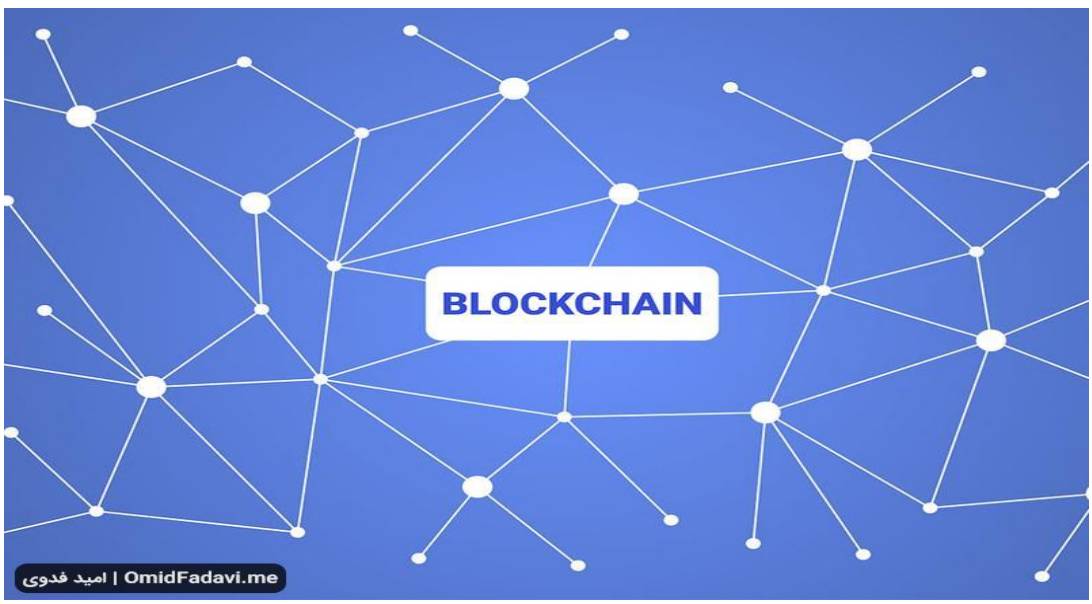
توضیح

در این نوع الگوریتم، تراکنش ها و همچنین بلاک ها از سوی حساب های تایید شده و به نام تایید کنندگان مطمئن و معتبر شناخته می شوند. تایید کنندگان در این الگوریتم از نرم افزار هایی استفاده می کنند تا بتوانند تراکنش ها را با موفقیت در بلاک قرار دهند. خوبی این فرایند این است که این کار به طور خودکار انجام می شود و دیگر نیاز نیست تا فرد به طور مستقیم و دائم بر روی کامپیوتر خود نظارت داشته باشد. البته شما باید همیشه از کامپیوتر خود مراقبت کنید تا دست افراد خرابکار به آن نرسد.

برای این که در این الگوریتم تایید کننده شوید باید این سه شرط را داشته باشید: هویت شما باید به طور رسمی در شبکه تایید شده باشد. صلاحیت انجام کار به سختی به دست می آید تا حق تایید بلاک های تایید شده و ارزش گذاری درست شود. باید برای برقراری ارتباط و انجام مسئولیت ها یکپارچگی کامل وجود داشته باشد.

با استفاده از این الگوریتم افراد این حق را دارند تا در شبکه تبدیل به یک تایید کننده شوند. در نتیجه یک مشوق برای حفظ موقعیتی که قبلا به دست آورده اند وجود دارد. تایید کنندگان موجود در شبکه با اضافه کردن شهرت به هویت خودشان تشویق می شوند تا فرآیند انجام تراکنش ها را نگه دارند. دلیل این ماجرا هم این است که هیچ تایید کننده ای دوست ندارد تا شهرتی و اعتباری را که به سختی درون شبکه به دست آورده است را از بین ببرد.

انواع الگوریتم های اجماع: الگوریتم اثبات وزن (Proof of Weight)



مزایا

- مصرف انرژی به صورت بهینه شده
- قابلیت شخصی سازی
- مقیاس پذیر

معایب

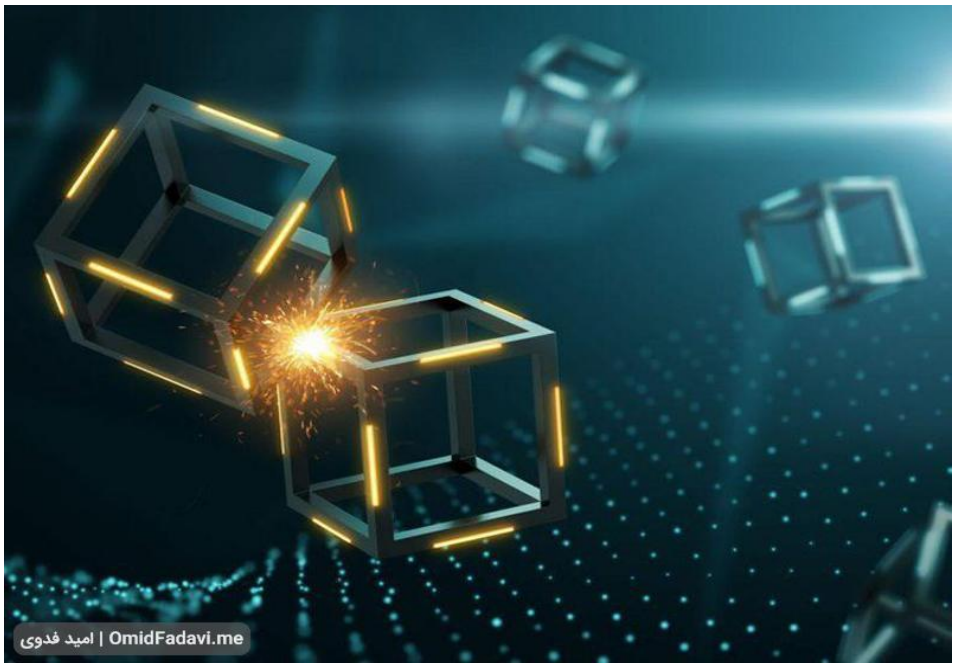
- ارائه کردن مشوق در آن سخت است

توضیح

این الگوریتم توسط مدل اجماع آلگورند طراحی و ساخته شده است. در سیستم هایی که از روش PoS استفاده می شود، درصد سکه های تحت تملک تایید کننده نشان دهنده احتمال پیدا کردن بلاک است. اما در الگوریتم اثبات وزن از مقادیر وزنی به صورت نسبی استفاده می شود.

الگوریتم های اثبات شهرت و اثبات فضا از این الگوریتم گرفته شده اند.

انواع الگوریتم های اجماع: الگوریتم اثبات شهرت (Proof of Reputation)



مزایا

- برای شبکه های خصوصی و دارای مجوز خوب و کارآمد است

معایب

- فقط در بلاک چین های خصوصی و دارای مجوز قابل استفاده است

توضیح

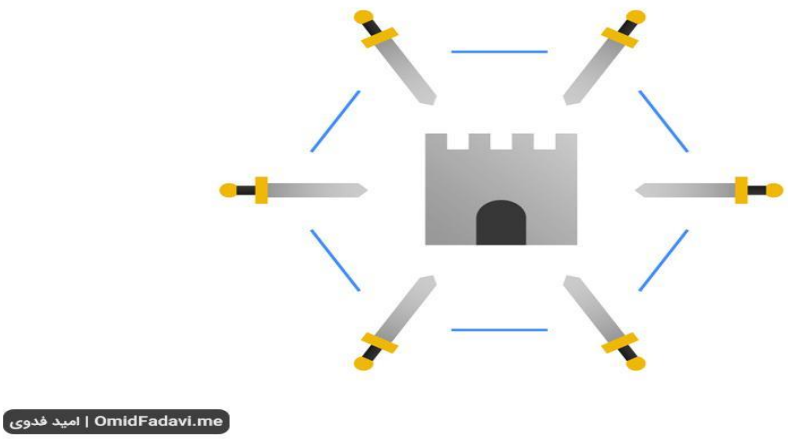
این الگوریتم مانند الگوریتم اثبات اختیار است. الگوریتم اثبات شهرت برای این که بتواند امنیت شبکه ی خود را تامین کند به شهرت افراد شرکت کننده در آن وابسته است. یک شرکت کننده و یا کسی که وظیفه امضا کردن بلاک را بر عهده دارد، باید آن قدر شهرت داشته باشد و شناخته شده باشد که در صورتی که قصد داشته باشد تقلب کند و یا در سیستم خرابکاری کند با عواقب مالی و تجاری بسیار قابل توجه رو به رو شور.

البته این توضیح و مفهوم کاملا نسبی است. زیرا در هر حال وقتی یک کسب و کار سعی کند در شبکه خرابکاری کند ضررخواهد کرد. اما این ضرر در شرکت ها و کسب و کار های بزرگ بسیار بیشتر و چشمگیر تر است. به همین دلیل است که شرکت های بزرگ شانس انتخاب بیشتری نسبت به شرکت های کوچک دارند.

هنگامی که شهرت یک تایید کننده در شبکه تایید شود، می تواند فعالیت خود را شروع کند.

این الگوریتم در حال حاضر توسط گوچین در حال استفاده می باشد.

انواع الگوریتم های اجماع: الگوریتم تحمل خطای بیزانس (Byzantine Fault Tolerance)



مزایا

- سرعت بالا
- مقیاس پذیر است

معایب

- به صورت معمول برای شبکه های خصوصی و نیازمند به مجوز استفاده می شود

توضیح

یک مشکل قدیمی و سنتی در رایانش های توزیع شده وجود دارد. این مشکل با ژنرال های بیزانس تعریف می شود.

باید این مشکل را در قالب یک مثال برایتان تعریف کنیم. فکر کنید چندین ژنرال بیزانس وجود دارد و هر کدام قسمت های مربوط به خودشان را توسط یک ارتش بیزانس محاصره کرده اند. حال این ژنرال ها باید به طور دسته جمعی تصمیم بگیرند که آیا حمله کنند و یا نکنند. در این میان اگر برخی از ژنرال ها بدون هماهنگی با دیگران و به تنهایی حمله کنند، آن محاصره از بین می رود.

در این موارد ژنرال ها معمولا از یک دیگر فاصله دارند و برای این که بتوانند با یکدیگر ارتباط برقرار کنند باید برای هم پیام بفرستند.

چندین پروتکل رمزارز برای اجماع در سیستم های خود از این شبکه استفاده می کنند. در ادامه دو نوع از این پروتکل ها را برایتان معرفی می کنیم.

تحمل عملی خطای بیزانس (PBFT)

یکی از اولین راه حل ها برای حل مشکل توسط تحمل عملی خطای بیزانس مطرح شده است. این نسخه در حال حاضر توسط هایپرلجر فابریک در حال استفاده می باشد. این الگوریتم با چند ژنرال از پیش تعیین شده به خوبی و با هماهنگی کامل فعالیت می کند.

از مزیت های تحمل عملی خطای بیزانس می توان به میزان خروجی بسیار بالای آن اشاره کرد. البته این الگوریتم عیب های خودش را هم دارد که از جمله آن ها می توان به متمرکز شدن شبکه اشاره کرد. این شبکه همچنین به مجوز دسترسی نیز نیاز دارد.

توافق یکپارچه بیزانس (FBA)

این مورد هم دسته ی دیگری از پروتکل ها هستند که برای رفع خطای بیزانس از روش توافق یکپارچه بیزانس استفاده می کنند. در حال حاضر ارز های دیجیتال ریپل و استلار در شبکه خود از این نوع راه حل استفاده می کنند.

ایده کلی این راه حل به این صورت است که در آن هر ژنرال مسئول زنجیره و بخش خودش است و با بررسی و دسته بندی پیام ها می تواند به حقیقت دست پیدا کند.

در ارز دیجیتال ریپل این ژنرال های درون شبکه از قبل و توسط بنیاد ریپل انتخاب می شوند. در ارز استلار اما، هر کسی می تواند به عنوان تایید کننده فعالیت کند. در این ارز این خود شما هستید که تصمیم می گیرید به چه کسی اطمینان و اعتماد کنید.

از مزیت های این راه کار می توان به خروجی بسیار بالا، هزینه پایین برای انجام تراکنش و مقیاس پذیری قابل قبول شبکه اشاره کرد.

انواع الگوریتم های اجماع: الگوریتم تحمل نیابتی خطای بیزانس (dBFT)

مزایا

سرعت بالا
مقیاس پذیر است

معایب

همه شرکت کنندگان برای تبدیل شدن به زنجیره ریشه تلاش می کنند. امکان به وجود آمدن چندین زنجیره ریشه وجود دارد

توضیح

این الگوریتم یک مکانیزم اجماع خطای بیزانس است که در آن امکان مشارکت به صورت گسترده به صورت رای گیری واسطه ای فراهم شده است. این الگوریتم توسط نئو مورد استفاده قرار گرفته است. کسانی که از توکن های نئو استفاده می کنند می توانند با انجام رای گیری، کتابداری که می خواهند حمایت کنند را انتخاب نمایند. این گروه منتخب توسط الگوریتم BFTبه اجماع می رسد و می تواند بلاک های جدید را تهیه نماید. در شبکه نئو رای گیری به جای آن که ثابت باشد در دنیای واقعی ادامه پیدا خواهد کرد.

این الگوریتم از قطعیت خوب و قابل قبولی برخوردار است. در این الگوریتم به محض آن که تاییدیه ها نهایی شوند، دیگر بلاک نمی تواند تقسیم شود و به دو شاخه تقسیم شود. به همین دلیل تراکنش دیگر قابل برگشت نخواهد بود.

در الگوریتم نئو تولید هر بلاک جدید تقریبا بین ۱۵ تا ۲۰ ثانیه طول می کشد.

تحمل خطا

این الگوریتم تحمل خطایی برابر F = [(n-1) / 3]را برای شبکه به همراه دارد. در این فرمول nبرابر با تعداد گره های شبکه است. این فرمول و میزان تحمل خطا شامل امنیت شبکه و دسترسی ها هم می شود و همچنین در برابر شکست های عمومی و شکست های بیزانس نیز از خود مقاومت نشان می دهد.

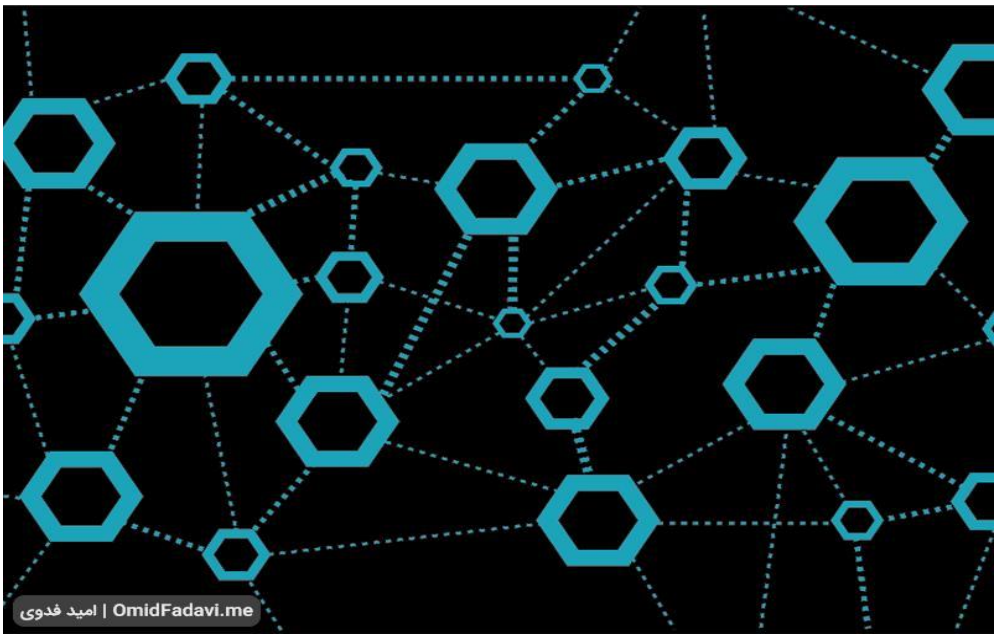
این الگوریتم همان طور که گفتیم از از میزان قطعیت خوب و کافی برخوردار است و پس از تایید تراکنش ها دیگر امکان بازگشت آن ها و یا دو شاخه شدن زنجیره وجود ندارد.

در این الگوریتم خروجی تراکنش ها تا میزان ۱۰ هزار تراکنش بر ثانیه محاسبه می شود که این مقدار در میان بلاک چین هایی که عمومی هستند رقم بسیار خوبی به شمار می رود. این مقدار همچنین امکان پشتیبانی از اپلیکیشن های تجاری را به طور گسترده فراهم می کند.

این الگوریتم همچنین تکنولوژی هویت دیجیتالی را می تواند ترکیب کند. یعنی یک گره یا کتاب دار در شبکه می تواند یک نام واقعی از افراد و یا موسسات باشد.

اگر درباره فناوری بلاکچین سوال و ابهامی دارید می توانید از ***پکیج بلاکچین*** چیست استفاده نمایید. این پکیج به مدت محدود رایگان شده است و پیشنهاد می کنیم این فرصت طلایی را از دست ندهید.

انواع الگوریتم های اجماع: الگوریتم اجماع RAFT



مزایا

- مدلی ساده تر از الگوریتم اجماع Paxosاما با امنیت بالا
- قابلیت پیاده سازی در اکثر زبان های برنامه نویسی

معایب

به طور معمول برای شبکه های خصوصی و نیازمند به مجوز استفاده می شود

توضیح

این الگوریتم به عنوان یک جایگزین برای الگوریتم Paxos طراحی شده است. البته این الگوریتم در نهایت نسبت به آن چه که قرار بود باشد بسیار امن تر شده است و همچنین ویژگی های بیشتری نیز دارد. این الگوریتم یک راه کلی تر را برای توزیع یک ماشین حالت در دسته ای از سیستم های رایانشی ارائه می کند. این الگوریتم در فرآیند انجام خود این اطمینان را حاصل می کند که هر گره در دسته بر مجموعه ی یکسان و برابری از انتقال های وضعیت توافق دارند.

این الگوریتم به کمک انتخاب یک رهبر به اجماع کلی می رسد. یک سرور در این الگوریتم دو حالت دارد، یا رهبر است و یا دنبال کننده. سرور ها در این الگوریتم می توانند کاندید رهبر شدن بشوند. رهبر در این الگوریتم وظیفه دارد تا فهرست را برای دنبال کنندگانش تکرار کند. او همچنین به طور منظم پیام هایی را می فرستد که وجود خود را یادآور شود. این پیام ها در این شبکه مانند ضربان قلب است!

هر دنبال کننده ای که در این شبکه فعالیت دارد یک زمان مشخص دارد که در آن زمان مشخص باید منتظر ارسال پیام ضربان قلب از رهبر خود باشد. هنگامی که این پیام توسط دنبال کننده دریافت شود، زمان بندی دوباره تنظیم می شود. اگر در این مدت هیچ ضربانی دریافت نشود، دنبال کننده به دنبال انتخاب یک رهبر دیگر می رود.

انواع الگوریتم های اجماع: الگوریتم گراف جهت دار غیر مدور (Directed Acyclic Graphs)

مزایا

- مقیاس پذیری بالا به دلیل نوع ساختار غیر خطی
- سرعت بالا
- مصرف انرژی به صورت بهینه شده
- در این الگوریتم قطعیت به سرعت به دست می آید

معایب

تنها راه پیاده سازی قرارداد های هوشمند استفاده از اوراکل ها است

توضیح

گراف های جهت دارد غیر مدور یک حالت عمومی تر از بلاک چین ها هستند. این نوع از الگوریتم ها به دلیل مقیاس پذیری و ظرفیت بالایی که دارند بسیار مشهور هستند.

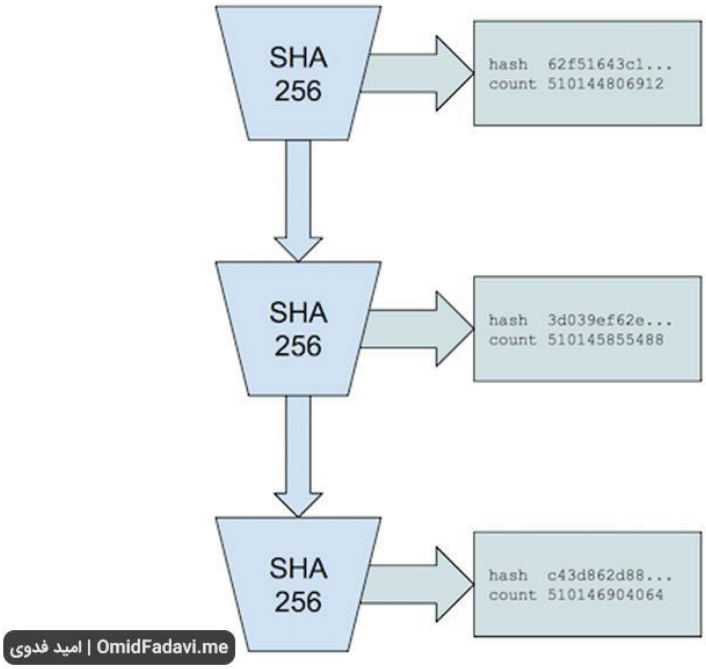
به طور کلی در ساختار شبکه های بلاک چین یک سیستم خطی وجود دارد. در این سیستم خطی بلاک ها به صورت یک به یک به زنجیره اضافه می شوند. این کار باعث می شود سرعت بلاک چین پایین آید و کند شود. دلیل آن هم این است که بلاک ها نمی توانند با هم و به صورت هم زمان به زنجیره اضافه شوند.

در این نوع الگوریتم اما بلاک ها به صورت موازی اضافه می شوند و هر بلاک می تواند تراکنش های پیش از خود را تایید کند. این باعث می شود این الگوریتم مقیاس پذیری بیشتری داشته باشد.

در این الگوریتم می توانید تنوع های زیر را داشته باشید:

- ترتیب بندی تراکنش ها به چه صورت انجام شود؟
- قطعیت چگونه به دست آید؟
- الگوریتم انتخاب بلاک قبلی جهت تایید و یا الگوریتم انتخاب Tip

انواع الگوریتم های اجماع: الگوریتم اثبات تاریخ



ایده ی اصلی در الگوریتم اثبات تاریخ به این صورت است که شما به جای آن که به برچسب های زمانی هر تراکنش اعتماد کنید، می توانید این را ثابت کنید که تراکنش زمانی قبل، و یا بعد از یک رویداد رخ داده است.

برای مثال هنگامی که شما از صفحه ی اول یک روزنامه (مانند نیویورک تایمز) عکس می گیرید، درواقع دارید این را ثابت می کنید که عکس گرفته شده توسط شما بعد از انتشار روزنامه بوده است. با این کار شما راهی برای تاثیر گذاشتن بر روی آن چه که آن روزنامه چاپ کرده است ایجاد کرده اید. شما با استفاده از الگوریتم اثبات تاریخ می توانید یک سابقه ی تاریخی درست کرده و با استفاده از آن ثابت کنید که یک رویداد در چه لحظه ی مشخصی روی داده است.

برچسب های زمانی اثبات تاریخ

الگوریتم اثبات تاریخ یک تابع تاخیر به قابلیت تایید است که میزان تکرار بسیار بالایی را دارا می باشد. یک تابع تاخیر قابل تایید برای آن که ارزشیابی شود نیازمند تعدادی مراحل متوالی و مشخص است. خروجی این تابع یک مقدار منحصر به فرد است که می توان آن را به صورت بهینه و عمومی تایید کرد.

پیاده سازی این الگوریتم به صورتی است که از یک مقدار هش مقاوم ترتیبی استفاده می کند. این مقدار به طور مداوم بر خودش اجرا می شود و خروجی قبلی را به عنوان ورودی بعدی در نظر می گیرد. شمارش ها و ثبت خروجی کنونی هم به صورت دوره ای انجام می پذیرد.

برای مثال در الگوریتم هش بیت کوین، یعنی SHA256، موازی ساختن این فرایند بدون حمله و با استفاده از هسته های ۲ به توان ۱۲ ممکن نمی باشد.

پس از انجام این مراحل است که می توانیم مطمئن باشیم که در بین هر شمارشگر در هنگام تولید، زمانی واقعی مصرف شده است و درواقع سفارش ثبت شده در هر شمارشگر با سفارش ثبت شده در دنیای واقعی مطابقت دارد.

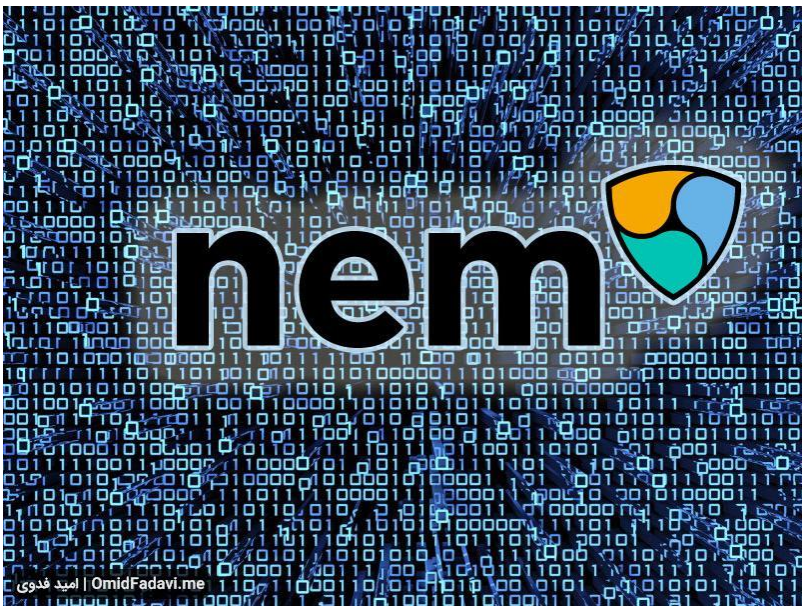
انواع الگوریتم های اجماع: الگوریتم اثبات شتاب سهام

این الگوریتم در حال حاضر توسط ردکوین در حال استفاده می باشد.

الگوریتم اثبات شتاب سهام که با عنوان خلاصه شده ی PoSV نیز شناخته می شود، به عنوان یک جایگزین برای دو الگوریتم اثبات کار و اثبات سهام معرفی شده است. این الگوریتم به این جهت طراحی شده است تا به شبکه ی همتا به همتا امنیت بیشتری بدهد و همچنین تراکنش های ردکوین را نیز تایید کند. رمزارز ردکوین به منظور تسهیل در تعاملات اجتماعی در عصر دیجیتال طراحی و توسعه داده شده است.

این الگوریتم برای دو هدف کلی طراحی شده است. یکی برای تشویق تملک و سهام و دیگری برای فعالیت و شتاب. هر دوی این موارد با اهداف ردکوین به عنوان یک ارز همخوانی و هماهنگی دارند. از جمله اهداف این ارز ذخیره ارزش و ابزار تبادل می باشد.

انواع الگوریتم های اجماع: الگوریتم اثبات اهمیت



این الگوریتم در حال حاضر توسط NEMاستفاده می شود.

از مزیت های این الگوریتم می توان به این مورد اشاره کرد که این الگوریتم در ارزشیابی سهام، از روش اثبات سهام عملکرد بهتری را ارائه می دهد.

الگوریتم اثبات اهمیت که توسط NEMمورد استفاده قرار گرفته است، علاوه بر این که به تعداد سکه ها وابسته است، همچنین به این احتمال که اقدام سیستم والد باید پاداش بگیرد نیز وابستگی دارد. در این الگوریتم شانس ایجاد یک بلاک به عوامل متفاوتی بستگی دارد. از جمله ی این عوامل می توان به میزان اعتبار، مقدار موجودی و همچنین تعداد تراکنش های انجام شده اشاره کرد. در این الگوریتم مجموعه ی این عوامل را به عنوان گردش اهمیت نام گذاری کرده اند. این الگوریتم به کاربران یک تصویر امیدبخش از یک عضو مفید در سیستم را ارائه می دهد.

حداقل موجودی

کاربران برای این که بتوانند در این الگوریتم واجد شرایط گردش اهمیت باشند باید حداقل در حساب خود مقدار ۱۰ هزار XEMداشته باشند. شاید الان به این فکر می کنید که به دست آوردن این مقدار سکه خیلی سخت و پر هزینه است. اما باید بگوییم در حال حاضر بیشتر از ۹ میلیارد سکه ی XEMدر گردش است، پس به دست آوردن ده هزار سکه چندان کار پر هزینه ای نمی باشد. البته باید بدانید که این احتمال وجود دارد که محدودیت ده هزار سکه در آینده تغییر یابد و مقدارش کمتر و یا بیشتر شود، اما فعلا حداقل موجودی مورد نیاز ۱۰ هزار XEMمی باشد.

گردش اهمیت در این الگوریتم صرفا با احتمال و اندازه ی سهام انجام نمی گیرد و برای آن یک الگوریتم خاص تعریف شده است.

همچنین باید این نکته را هم بدانید که الگوریتم استفاده شده در شبکه ی NEMدر برابر دستکاری های اختیاری نیز مقاوم شده است. در این اجماع همچنین حملات سیبل و حلقه نیز با استفاده از یک سری مکانیزم های ساختاری کاهش یافته اند.

باید این نکته را در نظر داشته باشید که الگوریتم اثبات اهمیت با الگوریتم اثبات سهام تفاوت دارد. البته در میان این دو الگوریتم شباهت هایی وجود دارد.

انواع الگوریتم های اجماع: الگوریتم اثبات هویت

الگوریتم اثبات هویت یا Proof of Identityدر اصل یک مدرک رمزنگاری می باشد که به ما این را می گوید که هر کاربری که کلید خصوصی را بداند، مانند یک کاربر با هویت معتبر شناخته می شود و از رمزنگاری، به یک تراکنش خاص متصل شده است. هر فردی از هر گروهی می تواند یک PoFبسازد و آن را به هر شخصی مانند یک گره پردازشگر بفرستد.

انواع الگوریتم های اجماع: الگوریتم اثبات زمان

این الگوریتم توسط Chronologicدر حال استفاده می باشد.

این الگوریتم توسط کرونولوچیک معرفی شده و توسط خود آن ها نیز در حال استفاده می باشد. آنان در حال برنامه ریزی هستند تا بتوانند یک بلاک چین جدا طراحی کنند. توسعه دهنده اصلی این الگوریتم در صحبتی این گونه گفته است:

«در این جا بزرگ ترین مشکلی که ما با آن رو به رو هستیم این است که بزرگ ترین عددی که این امکان را دارد تا در یک متغیر سالیدیتی ذخیره شود باید از ترتیب بزرگی ۱۰۷۶ باشد. این کار زمان تولید توکن ها را برای ما سخت کرده است.»

انواع الگوریتم های اجماع: الگوریتم اثبات وجود

این الگوریتم در حال حاضر توسط DragonChain و HeroNode و Poex.io استفاده می شود.

الگوریتم اثبات وجود و یا Proof of Existenceیک سرویس آنلاین می باشد که وجود فایل های کامپیوتری در زمان مشخص را با استفاده از تراکنش های دارای برچسب زمانی در شبکه ی بلاک چین بیت کوین تایید می کند.

این الگوریتم اثبات برای اولین بار در سال ۲۰۱۳ و به عنوان یک پروژه متن باز کار خود را آغاز کرد. توسعه دهندگان اصلی این الگوریتم اثبات، مانوئل آراوز و استبان اوردانو هستند.

این الگوریتم را می توان در موارد زیر استفاده کرد:

- توافق امضای دیجیتال بدون آن که محتوای واقعی افشا شود
- مشخص کردن تملک داده بدون آن که محتوای واقعی افشا شود
- امکان زدن برچسب زمانی به اسناد
- ثابت کردن تملک
- بررسی کردن یکپارچگی داده

انواع الگوریتم های اجماع: الگوریتم Ouroboros

این الگوریتم در حال حاضر توسط کاردانو مورد استفاده قرار گرفته است.

اگر بخواهیم درباره ی این الگوریتم توضیح بدهیم باید بگوییم Ouroboros نوعی از اثبات سهام به همراه ضمانت های امنیتی می باشد. همان طور که گفتیم این الگوریم در حال حاضر توسط کاردانو استفاده می شود.

برای این که بتوانید توکن های شبکه ی کاردانو را به دست آورید نیاز به هیچ فشار زیاد و صرف انرژی زیادی ندارید. برای به دست آوردن این توکن ها باید از Ouroboros استفاده کنید. این سیستم به تازگی مورد بررسی قرار گرفته است و ایرادات و باگ های موجود در آن تا حد بسیار زیادی بر طرف شده است. Ouroboros معادل یک دستگاه استخراج در الگوریتم PoW می باشد و همان امکانات استخراج را به شما می دهدو امکاناتی مانند تولید بلاک های جدید و همچنین تایید کردن تراکنش ها. همچنین در این سیستم الگوریتمی به نام «ساتوشی را دنبال کن» و یا به انگلیسی Follow Satoshi که با استفاده از آن می توانید به صورت تصادفی ماینینگ کنید.

مقیاس پذیری

فرآیند Ouroboros امکان استخراج توکن های کاردانو را برای کاربران فراهم می کند. همان طور که گفتیم برای استخراج این توکن نیاز به صرف انرژی زیادی نمی باشد، به همین دلیل الگوریتم بلاک چین کاردانو به شدت مقیاس پذیر شده است.

شخص پشت پرده ی این الگوریتم و ارائه دهنده ی آن پروفسور آگلوس کیاپاس می باشد. این پروفسور مسئول بخش تحقیقات IOHKمی باشد. این الگوریتم در بخش اول به صورت ریاضی ارائه و اثبات شد. سپس برای این که در آینده از پدید آمدن مشکلات ساختاری جلوگیری شود تحت بررسی های همتا قرار گرفت.

در این الگوریتم برای استخراج کنندگان و یا همان ماینر ها، عنوان Slotدر نظر گرفته شده است. سرپرست Slotشدن در این الگوریتم معادل استخراج کنندگان در الگوریتم هایی مانند اثبات کار می باشد.

ماکلین در این الگوریتم این امکان را دارند تا بلاک های جدید را بسازند و تراکنش های جدید را تایید کنند. هر گره در شبکه در صورتی که ارزش مثبتی داشته باشد به عنوان یک سهامدار شناخته می شود و می تواند به عنوان یک سرپرست در شبکه انتخاب شود.

در الگوریتم اثبات سهام به شما گفتیم که انتخاب سهام دار و در واقع شخصی که بلاک بعدی را خواهد ساخت به صورت تصادفی انجام می شود. البته این انتخاب تصادفی با سهمی که آن شخص در شبکه دارد هم متناسب است. ارزش نسبی سهم هر شخص نیز به این صورت انتخاب می شود که مقدار توکن های آن ها تقسیم بر تعداد کل توکن های موجود در سیستم می شود.

سرپرست

هنگامی که یک گره موفق شود تا اولین بلاک خود را با موفقیت بسازد، رسما به عنوان یک سرپرست Slotدر شبکه معرفی می شود. مسئولیتی که سرپرست ها در این جایگاه دارند شامل بررسی تراکنش هایی می شود که پیش تر توسط سایر گره ها تایید شده است. همچنین ساختن بلاک های جدید برای هر قسمت از تراکنش ها، اختصاص دادن کلید های شخصی برای بلاک ها و اعمال کردن آن در زنجیره اصلی نیز از دیگر وظایف سرپرست ها می باشد.

سرپرستان باید در بازه های زمانی مشخص بلاک های جدید خود را ایجاد کنند. این بلاک های جدید در شبکه ی کاردانو Slotنام دارد و مدت زمان مورد نیاز برای تولید هر بلاک ۲۰ ثانیه می باشد. اگر این زمان را برای تولید بلاک جدید از دست بدهید باید تا زمان انتخاب مجدد صبر کنید.

ساتوشی را دنبال کن

همان طور که گفتیم با استفاده از یک الگوریتم دیگر به نام ساتوشی را دنبال کن می توانید به صورت تصادفی استخراج را انجام دهید. این الگوریتم به این صورت کار می کند که به صورت اتوماتیک برای شما یک سکه را انتخاب می کند و در صورتی که شما از مالکان این سکه باشید به عنوان سرپرست Slotانتخاب می شوید.

در این سیستم هرچه تعداد سکه های بیشتری را در اختیار داشته باشید، شانس انتخاب سکه ها را افزایش خواهید داد.

اگر شما به عنوان سرپرست انتخاب شوید تنها کاری که نیاز است تا انجام دهید این است که کیف پول خود را برای گره باز نگه دارید و بر روی سکه هایتان فعالیت انجام دهید.

در واقع این سیستم این امکان را به شما می دهد تا با کمک یک سیستم ماینینگ مقرون به صرفه فعالیت خود را ادامه دهید. این ماجرا تا زمانی که شما در این پلتفرم سکه های کافی را داشته باشید ادامه می یابد.

انواع الگوریتم های اجماع: الگوریتم اثبات قابلیت بازیابی

این الگوریتم توسط مایکروسافت در حال استفاده می باشد.

الگوریتم اثبات قابلیت بازیابی یا Proof of Retrivability که به طور خلاصه به آن PoR نیز می گویند، یک اثبات فشرده با استفاده از یک سیستم فایل یا همان اثبات کننده به یک کلاینت و یا دریافت کننده است. در این الگوریتم فایل هدف (برای مثال فایل F) دست نخورده باقی می ماند. به این معنی که کلاینت این امکان را دارد تا آن را به طور کامل بازیابی کند.

فرآیند انجام کار در این الگوریتم به گونه ای است که این اثبات ها پیچیدگی ارتباطی کمتری نسبت به مخابره ی خود فایل هدف دارند. در نتیجه این الگوریتم و بلاک هایش، به نوعی یک بلاک جذاب برای سیستم های ذخیره سازی از راه دور به شمار می رود که تضمین بالایی هم به همراه دارد. این الگوریتم می تواند به عنوان یک الگوریتم اجماع برای سیستم هایی که رایانش ابری دارند بسیار مفید باشد.

انواع الگوریتم های اجماع: الگوریتم اثبات باورپذیری

استفاده از این الگوریتم مزایای زیر را برای کاربران به همراه خواهد داشت:

- با استفاده از مفهومی به نام Serviکه در ادامه بیشتر با آن آشنا می شوید، نسبت به الگوریتم سنتی اثبات سهام غیر متمرکز تر عمل می کند.
- در مقایسه با الگوریتم سنتی اثبات سهام از قطعیت با سرعت بالاتری برخوردار است.

این الگوریتم در حال حاضر توسط IOSTمورد استفاده قرار گرفته است.

توضیح الگوریتم

یک چالش همیشگی در مقابل الگوریتم سنتی اثبات سهام قرار دارد و آن هم گرایش آن الگوریتم به طرف تمرکز گرایی می باشد. IOSTکه در حال حاضر از این سیستم استفاده می کند، برای این که این ریسک را کاهش دهد، سرویس Servi را نیز به عنوان یک ابزار سنجش کمک کاربران، به جامعه ی خود یعنی IOST اضافه کرده است. این سرویس همچنین راهی را برای تشویق کاربران برای کمک به ادامه ی توسعه ی شبکه بلاک چین IOSرا ارائه کرده است.استفاده از این مکانیزم در شبکه، ویژگی های زیر را به همراه خواهد داشت:

غیر قابل تبادل

سیستم Servi به عنوان یک ابزار تبادل طراحی و ساخته نشده است، به همین منظور امکان تبادل و یا معامله ی آن وجود ندارد.

خودنابود شونده

سیستم پس از این که یک بلاک تایید شد به صورت اتوماتیک موجودی Serviرا که نزد کاربر تایید کننده قرار دارد از بین برده و پاک سازی می کند. با استفاده از این روش گره هایی که دارای امتیار بالای باورپذیری هستند این امکان را دارند تا در نوبت تایید بلاک قرار گیرند تا فرآیند منصفانه ی تولید بلاک جدید را تضمین کنند.

خود انتشاری

سیستم Serviبه صورت اتوماتیک پس از ارائه ی کمک های مشخصی مانند ارائه ی سرویس های جمعی و یا ارائه خدمات جمعی که توسط نهاد های دیگر و یا کمک های برخی افراد جمع شده است، حساب های مربوطه را به حساب کاربران واریز می کند.

سیستم های سنتی

سیستم های بلاک چین قدیمی تر یا همان سیستم های سنتی، با توجه به اندازه قطعاتشان در زمینه ی امنیت و خروجی داده شده، مراحلی را داشتند که این مراحل می توانست نفع و یا ضرر هایی را به همراه داشته باشد. سیستم هایی که تعداد قطعه هایشان بالا تر است، در کل عملکرد بهتری را از خود نشان می دهند، اما در مقابل، در مواجهه با حملات هکر ها انعطاف پذیری کمتری را از خود نشان می دهند. این ماجرا به صورت بالعکس نیز وجود دارد. این مشکل، یکی از مواردی است که Casperنیز با آن درگیر است.

سیستم IOSTبرای این که بتواند این مشکلات را برطرف کند و همچنین بتواند امنیت شبکه را نیز حفظ کند و میزان خروجی را افزایش دهد، برای شبکه بلاک چین IOSیک پروتکل اجمال اثبات باورپذیری نوآورانه را به کار گرفته است. در این مکانیزم، اثبات باورپذیری تضمین می کند که احتمال رفتار سوء را دارند، اما خروجی تراکنش ها به همراه قطعه ها به صورت چشمگیری افزایش پیدا می کند.

رویکرد درون قطعه ای

الگوریتم اجماع اثبات باورپذیری از یک رویکرد درون قطعه ای اول باورپذیر در سیستم خود استفاده می کند. در این الگوریتم تمام گره ها یا همان تایید کنندگان به دو دسته تقسیم می شوند. دسته ای تحت عنوان گروه باورپذیر و دسته ای دیگر به نام گروه معمولی. تاییدکنندگانی که در گروه باورپذیر قرار دارند تراکنش ها را در مرحله ی اول به سرعت پردازش می کنند. در مرحله بعد، تایید کنندگان اول تراکنش ها را در بخش بعدی نمونه برداری می کنند تا آن تراکنش ها تایید شود و کار کاملا قطعی شود. با این کار تاییدیه آن ها تضمین شود.

در این الگوریتم شانس انتخاب شدن به عنوان یک گره در گروه باورپذیر به عوامل مختلفی بستگی دارد. برخی از این عوامل عبارت اند از موجودی توکن، میزان کمک کردن به جامعه، نوشتن بررسی ها و مواردی از این قبیل. تایید کننده ای که بتواند امتیاز باورپذیری بالاتری را برای خود به دست آورد شانس بیشتری هم برای انتخاب شدن خواهد داشت. تاییدکنندگانی که در دسته باورپذیر قرار دارند برای تعیین کردن مجموعه تراکنش های انجام شده و مشخص کردن ترتیب آنان از یک رویه ی مشخص استفاده می کنند. این رویه باعث می شود تراکنش ها به ترتیب پردازش شود.

تایید کنندگان دسته ی باورپذیر خود گروه های کوچک تری را تشکیل می دهند. این گروه ها به این صورت است که در هر گروه یک تایید کننده وجود دارد. تراکنش ها به صورت تصادفی در میان این تاییدکنندگان تقسم خواهد شد. در نتیجه بلاک های کوچک تر با تاخیر کمتر تولید خواهد شد.

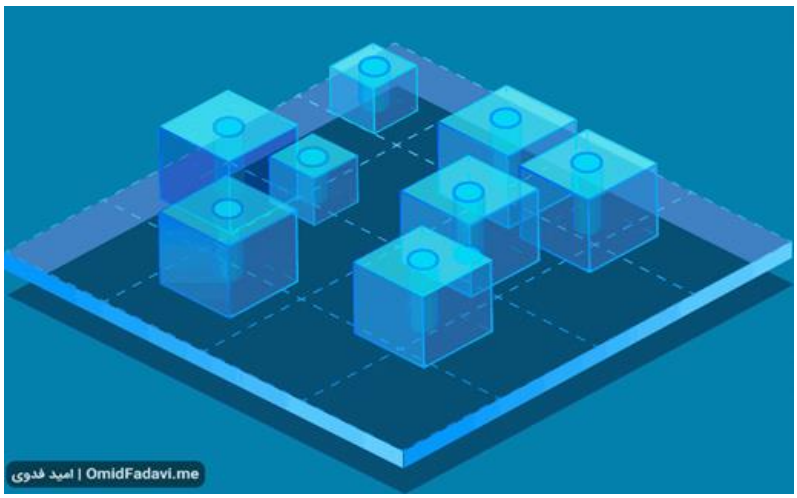
مسائل امنیتی

با تمام این صحبت ها اما هنوز هم امکان بروز مسائل امنیتی وجود دارد. دلیل آن هم این است که در این الگوریتم تنها یک گره کار تایید شدن را انجام می دهد. به همین دلیل این امکان وجود دارد که تعدادی تراکنش فاسد نیز توسط این تایید کنندگان تایید شده و انجام شود. برای این که این مشکل در شبکه برطرف شود، یک نمونه امتحانی در شبکه تعیین می شود که در آن تاییدکنندگان معمولی تراکنش ها را بررسی کرده و تناقضات احتمالی را شناسایی می کنند.

اگر در این میان تاییدکننده ای به عنوان خرابکار در شبکه شناسایی شود، تمام توکن ها و همچنین شهرت خود را در سیستم از دست خواهد داد. با این کار زیان افراد فریب خورده نیز جبران خواهد شد.

استفاده از رویکرد اول باورپذیر باعث می شود تا سرعت پردازش تراکنش ها به شکل کاملا چشمگیری افزایش پیدا کند. دلیل این کار هم این است که تنها یک تایید کننده ی باورپذیر فرآیند تایید را انجام می دهد و احتمال سوء رفتار از آن وجود ندارد.

انواع الگوریتم های اجماع: الگوریتم تنگل (آیوتا)

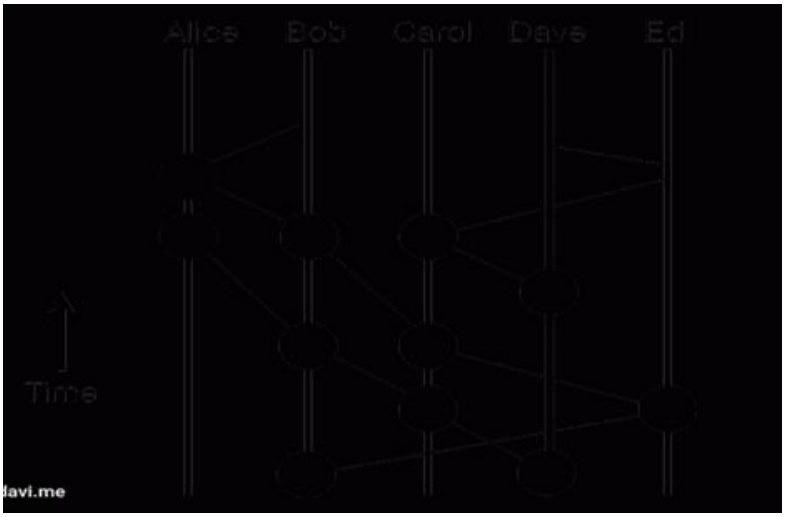


الگوریتم تنگل یک الگوریتم اجماع از نوع DAGمی باشد. این الگوریتم در حال حاضر توسط آیوتا استفاده می شود. کاربر برای آن که بتواند در الگوریتم تنگل یک تراکنش ارسال کند، ابتدا باید دو تراکنش پیش از آن را که دریافت کرده است ثبت و تایید نماید. هرچه تعداد تراکنش هایی که به تنگل اضافه می شوند بیشتر باشد، اجماع دو به یک و پیش پرداخت، باعث می شود تا تایید شدن تراکنش ها هرچه بیشتر مستحکم شود.

از آن جا که در این الگوریتم اجماع توسط تراکنش ها به دست می آید، اگر کسی بتوان میزان یک سوم از تراکنش ها را تولید نماید این امکان را دارد تا سایر افراد شبکه را قانع کند که تراکنش های نامعتبرشان درواقع معتبر است. اما تا زمانی که حجم تراکنش های کافی برای ایجاد یک سوم حجم به وجود نیاید، آیوتا تمام تراکنش های شبکه را در یک گره متمرکز به نام Coordinatorدو بار بررسی می کند.

آیوتا در توضیح Coordinatorاین گونه بیان می کند که این گره مثل یک چرخ کمکی برای شبکه عمل می کند و به محض آن که الگوریتم تنگل به اندازه کافی بزرگ و قدرتمند شود آن را حذف می کنند.

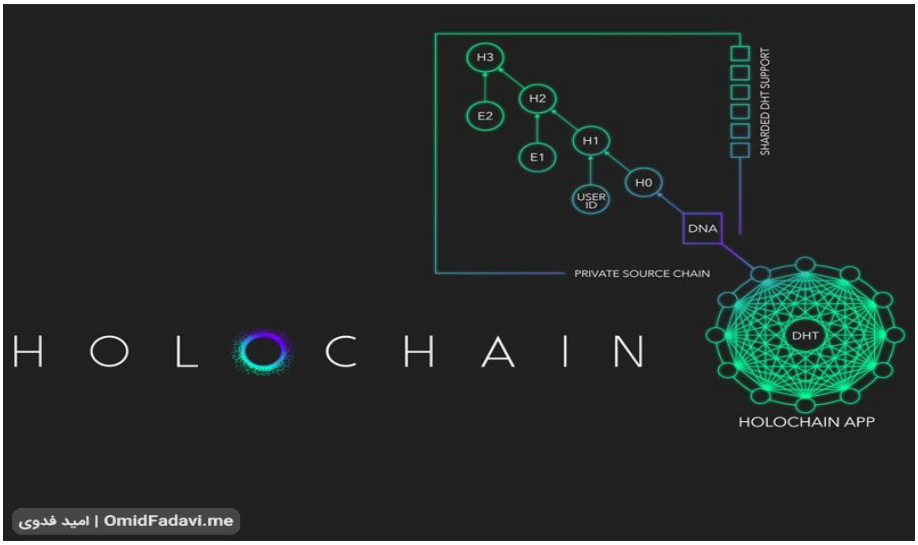
انواع الگوریتم های اجماع: الگوریتم هش گراف



الگوریتم هش گراف یکی از انواع پروتکل های اجماع است. این الگوریتم توسط لیمون بیرد طراحی و توسعه داده شده است. در این الگوریتم فرآیند انجام کار به این صورت است که گره ها تراکنش های مورد تایید و شناخته شده خود را به صورت تصادفی با سایر گره ها به اشتراک می گذارند. در نتیجه ی این چرخش ها، تمام تراکنش ها در بین تمام گره ها می چرخد.

الگوریتم هش گراف برای شبکه های خصوصی گزینه ی بسیار خوبی به شمار می رود. این الگوریتم را در شبکه های عمومی مانند اتریوم و یا دیسپچ مشاهده نخواهید کرد.

انواع الگوریتم های اجماع: الگوریتم هولوچین



این الگوریتم شباهت بسیار زیادی به مدل قبلی یعنی هش گراف دارد، اما هش گراف نیست. این الگوریتم یک ساختار داده ای را ارائه می کند که با استفاده از آن می توان اپلیکیشن های غیر متمرکز را توسعه داد. در این الگوریتم شما زنجیره ی خودتان را دارید و با استفاده از آن می توانید داده های مورد نظر خودتان از جمله تراکنش ها را به زنجیره اضافه کنید.

زنجیره هایی که در این شبکه فعالیت می کنند این توانایی را دارند تا ادغام شده، تقسیم شوند و همچنین به شکل های پیچیده تبدیل شوند.

الگوریتم هولوچین داده ها را به طور غیر متمرکز ذخیره می کند. در هولوچین هر داده ای یک هش دارد که آن هش، اثر ریاضی مربوط به داده است.

اگر در این شبکه شخصی داده ها را دستکاری کند، بین داده ها و هش آن ها عدم تطابق پیش آمده و توسط شبکه شناسایی می شود. سپس این داده به عنوان یک داده غیر معتبر دسته بندی شده و رد خواهد شد. در این الگوریتم امضا های دیجیتالی ضامن مالکیت داده هستند. الگوریتم هولوچین در اصل بیت تورنت است و امضا های دیجیتال به آن اضافه شده است.

انواع الگوریتم های اجماع: الگوریتم بلاک-لاتیس (نانو)

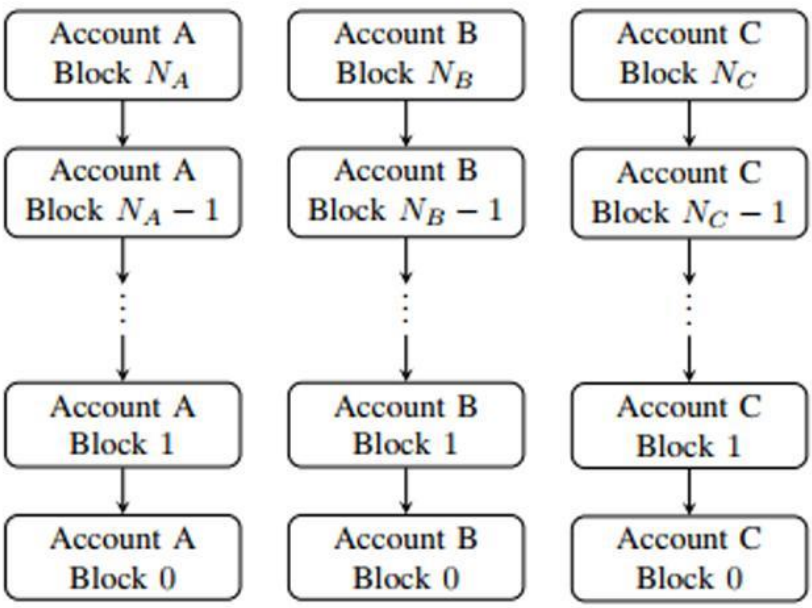


Fig. 2. Each account has its own blockchain containing the account's balance history. Block 0 must be an open transaction (Section IV-B)

نام قبلی این بلاک چین ریل بلاکس بوده است. این الگوریتم با یک پیچ در بلاک چین فعالیت می کند. نام این پیچ بلاک لاتیس می باشد. در این الگوریتم و در بلاک لاتیس، ساختاری وجود دارد به این صورت که همه ی کاربران زنجیره خود را در اختیار دارند. این زنجیره تنها توانایی نوشتن را به کاربران خود می دهد و همه ی کاربران در آن می توانند اطلاعات خود را وارد کنند. تمام کاربران در این الگوریتم یک کپی از زنجیره را دریافت و نگهداری می کنند.

در این الگوریتم هر تراکنش به دو بلاک ارسال در زنجیره ی فرستنده و یک بلاک دریافت در زنجیره دریافت کننده تقسیم می شود. اگر از دور به این الگوریتم نگاه کنید، نحوه کار و فعالیت آن بسیار ساده است و هیچ قسمت پیچیده ای در آن وجود ندارد.

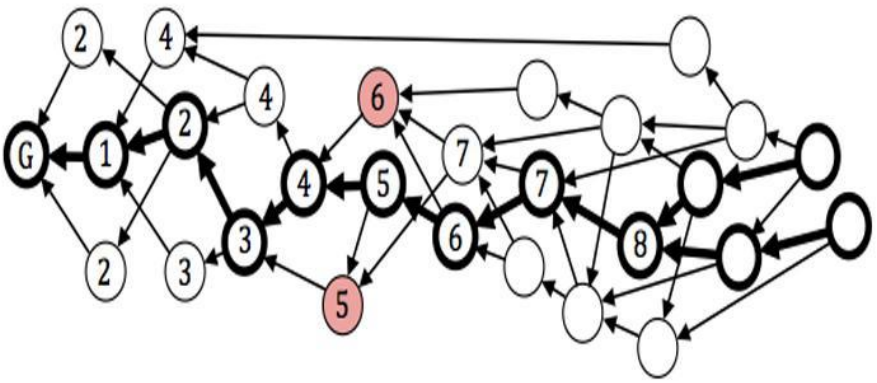
این الگوریتم یک مزیت بزرگ دارد و آن هم به ساختار منحصر به فرد آن مربوط می شود. این ساختار منحصر به فرد باعث این شده است که این الگوریتم در مقابل حملاتی مانند حمله پنی مقاوم شود. این حمله این گونه است که در آن، فرد مهاجم تعداد زنجیره هایی را که در آن گره مسئول آن است را با ارسال مقادیر پایینی از ارایه ی گسترده ای از کیف پول های خالی اشباع و متورم می کند.

انواع الگوریتم های اجماع: الگوریتم اسپکتر

در رابطه با این الگوریتم باید سریالی کردن رویداد های اثبات کار را برای شما توضیح دهیم. در این الگوریتم تایید تراکنش ها از طریق انتخابات بازگشتی انجام می شود. این روش بازگشتی به نام اسپکتر شناخته می شود. اسپکتر در اصل یک راه کار برای مقیاس پذیری در شبکه ی بیت کوین است که از ترکیب اثبات کار و DAGبرای رسیدن به یک اجماع استفاده می کند. در الگوریتم اسپکتر، بلاک ها فقط به یک منبع اشاره نمی کنند و برای استخراج به چندین بلاک اشاره می کنند. با استفاده از این روش، شبکه این امکان را دارد که در هر ثانیه بتواند چندین بلاک را مدیریت کند.

ماین کردن یک بلاک با استفاده از اشاره کردن به چندین منبع باعث ایجاد حمایت از اعتبار آن بلاک می شود. اسپکتر برای فعالیت خود از بلاک هایی با بیشترین برد استفاده می کند. البته این بلاک چین هنوز در دنیای واقعی و با شرایط واقعی امتحان نشده است و امکان دارد در آن مشکلاتی وجود داشته باشد و راه حمله ای برای خرابکار ها در آن باز باشد. اما در هر حال این الگوریتم یک راه کار برای ترمیم شبکه بیت کوین به شمار می رود.

انواع الگوریتم های اجماع: الگوریتم بایت بال



این الگوریتم برای فعالیت خود از DAGاستفاده می کند. در این الگوریتم یک ترکیب ناقص در میان تراکنش ها ایجاد می شود و سپس زنجیره اصلی به DAGاضافه می شود.

در این الگوریتم زنجیره اصلی اجازه تعریف ترتیب کلی در میان تراکنش ها را می دهد. زنجیره ای که در این الگوریتم به صورت مستقیم و یا غیر مستقیم به زنجیره اصلی گنجانده شده، در ترتیب کلی نیز وجود دارد. برای مثال در این الگوریتم اگر مشکل دو بار خرج کردن پیش آید، نسخه ی تراکنشی که پیشتر در ترتیب کلی آمده است به عنوان ترکیب معتبر شناخته شده و سایر تراکنش های انجام شده نا نعتبر می شود.

در بایت بال زنجیره اصلی به صورت قطعی و مطمئن بر اساس موقعیت تراکنش ها در نمودار تعریف شده و مشخص می شود. در صورتی که نیاز دارید در مورد این الگوریتم اطلاعات بیشتری کسب کنید می توانید به وایت پیپر آن مراجعه کنید. اما در حالت کلی باید بدانید که به عنوان یک قانون کلی، این الگوریتم به آن سمت حرکت می کند که تراکنش های درون آن توسط افراد شناخته شده نوشته شده باشد. دلیل این کار هم این است که بتوان آن افراد را به عنوان شاهد در نظر گرفت. لیست شاهد ها توسط کاربران تعریف و مشخص می شود.

فرآیند انجام کار

در این الگوریتم زنجیره اصلی به این صورت مسیر را درون DAGدنبال می کند:

- لیست شاهد ها در تراکنش های مجاور در زنجیره باید یکسان باشد و یا تنها می تواند با یک تغییر متفاوت باشد.
- زنجیره در اکثر تراکنش های نوشته شده توسط شاهدین می چرخد و آن ها را با زنجیره های جایگزین مقایسه می کند.

جمع بندی

در این مقاله سعی کردیم شما را الگوریتم های بلاکچین کارآمد آشنا کنیم. با استفاده از این الگوریتم ها می توانید اکثر ارز های دیجیتال موجود را بدون مشکل استخراج نمایید. در صورتی که هرگونه سوال و ابهامی دارید می توانید از بخش نظرات با ما به اشتراک بگذارید.