

کوین ایران 

بررسی انواع الگوریتم های اجماع دنیای رمز ارز ها

فهرست مطالب

۳	 بررسی انواع الگوریتم های اجماع دنیای رمز ارز ها
۴	 گواه اثبات کار
۵	 گواه اثبات سهام
۸	 گواه اثبات ظرفیت
۱۰	 گواه اثبات فضا
۱۰	 گواه اثبات زمان سپری شده
۱۱	 گواه اثبات سوزاندن
۱۲	 گواه اثبات فعالیت
۱۲	 گواه اثبات قدرت
۱۳	 گواه اثبات سهام اعطایی
۱۳	 تحمل پذیری خطای بیزانس
۱۴	 تحمل پذیری خطای بیزانس کاربردی
۱۴	 توافق بیزانس یکپارچه
۱۵	 گواه اثبات اهمیت
۱۵	 گراف جهت دار غیر مدور
۱۷	 منابع



بررسی انواع الگوریتم های اجماع دنیای رمز ارز ها

الگوریتم اجماع، فرآیندی در علوم کامپیوتر است که برای دستیابی به توافق بر روی یک مقدار داده ای واحد در میان سیستم های توزیع شده مورد استفاده قرار می گیرد. الگوریتم های اجماع برای رسیدن به قابلیت اطمینان در یک شبکه شامل گره های غیر قابل اعتماد طراحی شده اند. حل این مسئله که معمولاً با عنوان مشکل اجماع شناخته می شود در رایانه های توزیع شده و سیستم های چند عاملی بسیار حائز اهمیت است. برای تطبیق پذیری با این واقعیت، الگوریتم های اجماع لزوماً فرض می کنند که برخی از فرآیندها و سیستم ها در دسترس نیستند و برخی از ارتباطات از بین خواهند رفت. بنابراین، الگوریتم های اجماع باید به صورت تحمل پذیر خطا طراحی شوند. کاربردهای الگوریتم های اجماع شامل موارد زیر است [۱]:

- تصمیم گیری در مورد ارسال یک تراکنش توزیع شده به یک پایگاه داده
- تعیین گره هایی به عنوان سر گروه برای انجام برخی از وظایف توزیع شده
- همگام سازی نسخه های ماشین حالت و تضمین سازگاری در میان آنها

مکانیسم های اجماع روشی برای تضمین یک توافق دو طرفه بر روی نکات داده ای و وضعیت تمام داده ها به شمار می روند. این مکانیسم ها در شبکه بلاک چین تضمین می کنند که هر کدام از بازیگران شبکه، یک کپی از دفتر کل یکسان را در اختیار دارند. مکانیسم های اجماع مختلف، امنیت و چارچوب اقتصادی پروتکل رمزنگاری را تحت تأثیر قرار می دهند. این مکانیسم ها به شکل های متفاوت برای بلاک چین های مختلف ارائه می شوند. مکانیسم های اجماع در آغاز راه قرار دارند و پیش بینی مکانیسم غالب در آینده دشوار است. ایجاد مکانیسم های اجماع بر اساس طراحی مکانیسم انجام می شود که یک فرآیند دو مرحله ای است [۲]:

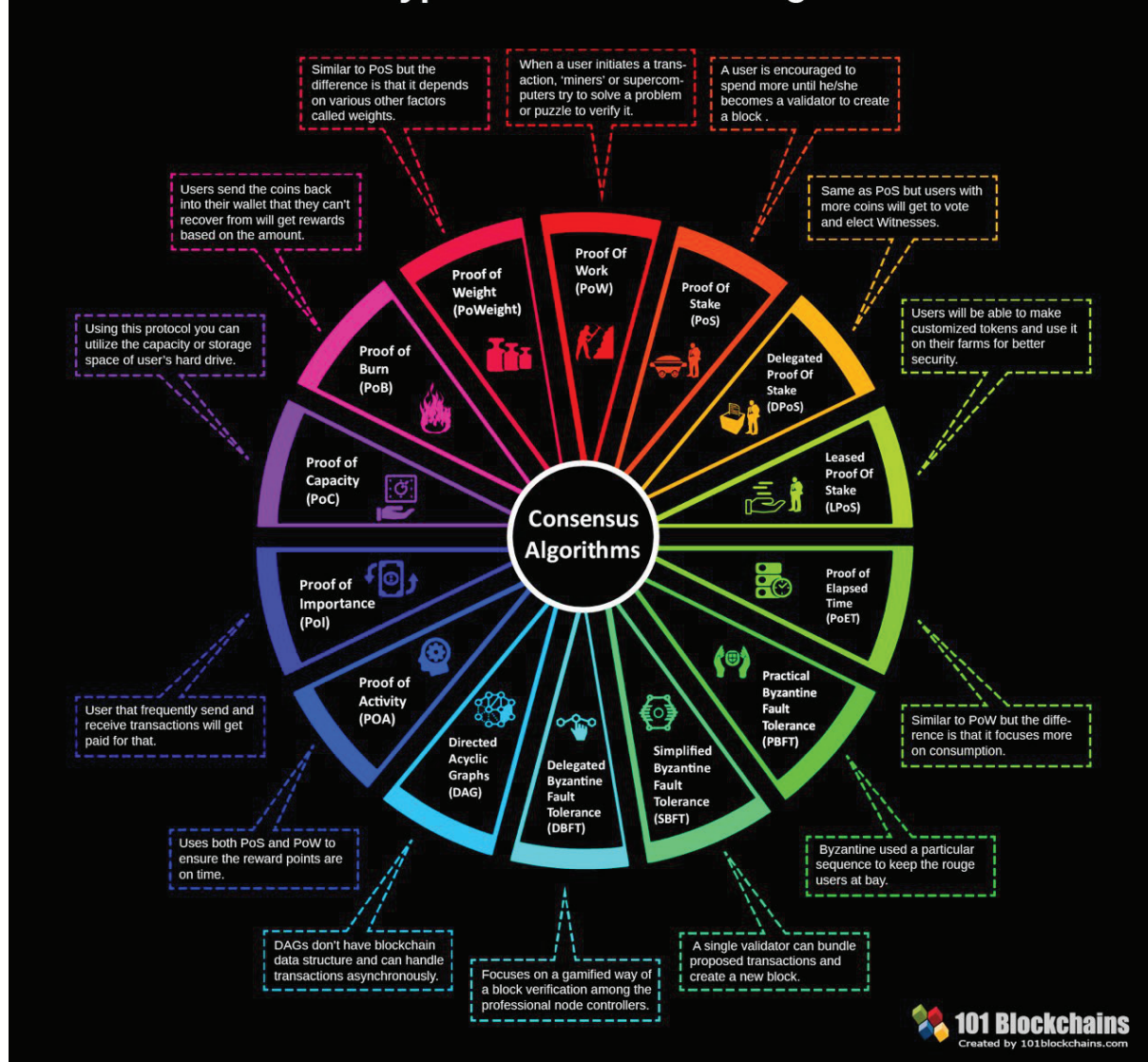
(۱) در نظر گرفتن نتیجه مورد نظر

(۲) عملکرد وارونه برای ایجاد یک بازی و تشویق بازیگران برای انجام آن بازی و تولید خروجی مورد نظر

لایه اجماع یا توافق جمعی یکی از مهمترین لایه ها در هر سیستم مبتنی بر بلاک چین است. این لایه برای حفظ قابلیت اعتماد شبکه با فرض وجود اعضای غیر قابل اعتماد ایجاد شده است. یک فرد یا یک رایانه [به عنوان نماینده فرد] می خواهند خدماتی مانند ارسال ایمیل، ثبت تراکنش های مالی، ذخیره سازی اطلاعات یا هر خدمات دیگری را ارائه دهند. اگر انجام این خدمات هزینه ای نداشته باشد یا هزینه آن به اندازه کافی ناچیز باشد، استفاده از این خدمات برای امور نامربوط و بی ارزش و یا به قصد خرابکاری توجیه پذیر خواهد بود که به آن مشکل Nothing at Stake یا سنگ مفت گفته می شود.

برای جلوگیری از استفاده نامربوط باید هزینه ای برای خدمات ایجاد کرد و خدمات دهنده باید به روشی این هزینه را اثبات کند. در سامانه هایی غیر متمرکز استفاده از تنبیه های قانونی و نهاد های متمرکز بازرسی و اعمال قانون امکان پذیر نیست و سامانه باید روشی جایگزین برای ثبات هزینه خدمات ارائه نماید.

Different Types of Consensus Algorithms



شکل ۱- انواع مکانیسم‌های اجماع [۳]

گواه اثبات کار

پروتکل گواه اثبات کار^۱ (POW) با هدف بازدارندگی در برابر حملات سایبری مانند منع سرویس توزیع شده (DDoS) طراحی شده است. مفهوم گواه اثبات کار پیش از معرفی بیت کوین توسط ساتوشی ناکاموتو نیز وجود داشته ولی مهم ترین کاربرد آن در ایجاد اجماع توزیع شده و بدون نیاز به اعتماد در بیت کوین بوده است. چنین اجماعی امکان ارسال و/ یا دریافت پول بدون نیاز به اعتماد به سرویس های شخص ثالث را فراهم می کند [۴].

گواه اثبات کار یک الزام برای تعریف یک محاسبه کامپیوتری پیچیده و گران قیمت است که به آن استخراج نیز گفته می شود. عملیات استخراج باید برای ایجاد یک گروه جدید از تراکنش های غیر قابل اعتماد در قالب بلاک بر روی دفتر کل توزیع شده به نام بلاک چین انجام شود. این عملیات با هدف تأیید مشروعیت یک معامله (جلوگیری از خرج

کردن دوباره) و ایجاد رمز ارز های جدید با اعطای پاداش برای انجام کار قبلی انجام می شود.

در انجام یک تراکنش، مراحل زیر طی می شود [۴]:

- تراکنش های انجام شده در یک بلاک جمع می شوند
- مشروعیت تراکنش های انجام شده توسط استخراج کنندگان تأیید می شود
- مسأله ریاضی نامتقارن که با عنوان مشکل گواه اثبات کار شناخته می شود توسط استخراج کنندگان حل می شود
- جایزه به اولین نفری تعلق می گیرد که مسأله مربوط به بلاک را حل کرده است
- تراکنش های تأیید شده در بلاک چین عمومی ذخیره می گردند

مکانیسم اجماع گواه اثبات کار مبنای رمز ارز های محبوب و رایجی مانند بیت کوین محسوب می شود. این مکانیسم یک سیستم استخراج مبتنی بر قدرت محاسباتی کامپیوتر است و کاربران مشارکت کننده باید مسائل ریاضیاتی دشواری را برای تعیین اعتبار تراکنش ها حل کنند. شبکه های بزرگ رمزنگاری مانند بیت کوین، الگوریتم گواه اثبات کار را بنیان کار خود قرار داده اند، زیرا این الگوریتم به نامتمرکز بودن قدرت و کنترل روی توزیع و پیاده سازی تغییرات عمده اقتصادی و فنی در شبکه کمک می کند [۵].



گواه اثبات سهام

گواه اثبات سهام^۲ (POS) الگوریتمی برای رسیدن به توافق جمعی در یک سیستم پولی مبتنی بر بلاکچین است که روشی متفاوت از گواه اثبات کار در پیش می گیرد. در این سیستم، انتخاب بر خلاف POW، سازنده بلاک بعد کاملاً تصادفی نیست و سیستم با اضافه شدن پارامترهایی از حالت کاملاً تصادفی خارج می شود. پارامترهای معرفی

شده با الگوریتم جدید، باعث ایجاد رابطه مستقیم بین "شانس یک فرد برای موفقیت در پیدا کردن جواب معمای ریاضیاتی برای ایجاد بلاک" و میزان "پولی که فرد در سیستم دارد" می شود [۶].

در گواه اثبات کار هر چه توان محاسباتی بیشتری داشته باشید، شانس موفقیت بیشتری برای ایجاد بلاک دارید، یعنی استخراج کننده ای موفق تر است که کامپیوتر های قوی تری داشته باشد. در سیستم گواه اثبات سهام هر چه پول بیشتری در سیستم داشته باشید شانس بیشتری برای ایجاد بلاک دارید. لازم به ذکر است که در سیستم گواه اثبات سهام استخراج کنندگان دیگر وجود ندارند و گره هایی که مشغول اعتبار سنجی و تولید بلاک های جدید هستند را سازنده بلاک می نامند.

باید به این امر توجه داشته باشیم که معمولاً در سیستم های POS (گواه اثبات سهام) با ایجاد بلاک جدید پول جدیدی ایجاد نمی شود و معمولاً همه پول ها از ابتدا ایجاد شده و میزان آنها ثابت است. در نتیجه سازندگان بلاک (معادل ماینرها در POW) بر هزینه ای که بابت تراکنش ها پرداخت می شود، به عنوان منبع درآمد تکیه خواهند کرد.

یکی از مشکلات اساسی سیستم های بر پایه گواه اثبات کار نیاز زیاد به منابع پردازشی برای ایجاد بلاک به شکل امن در سیستم است؛ مثلاً تخمین زده می شود که شبکه بیت کوین در حال حاضر ۸۶/۱۱ ترا وات (در حد کل کشور بوسنی) انرژی مصرف می کند.

برای اینکه یک نفر بتواند وارد گردونه افراد سازنده بلاک شود باید توانایی محاسباتی داشته باشد که تاثیر چندانی در شانس موفقیت ندارد و فقط برای انجام پردازش های ساده سیستم، مثل جمع کردن و اعتبار سنجی تراکنش ها استفاده می شود. همینطور برای اینکه اعداد مربوط به فرمول را محاسبه کند نیاز به داشتن پول یا سهام (عددی محاسبه شده از پول در گردش یا در حالت ایستای فرد یا هر فرمول وابسته دیگر) در سیستم است. در ادامه ما الگوریتم استفاده شده در Nxt را توضیح می دهیم که البته قبل از آن باید با چند مفهوم اولیه آشنا شویم.



مقدار هدف پایه ای^۳ برابر عددی است که با فرمولی خاص از بلاک قبلی به دست می‌آید. دلیل وجود این عدد تنظیم زمان ایجاد بلاک در حدودی خاص و تعیین شده از طرف پروتکل است؛ مثلاً در Nxt حدود ۶۰ ثانیه.

مقدار هدف^۴ (که هدف فردی است) یک عدد وابسته به حساب کاربر است. برای محاسبه این عدد دو پارامتر مشترک برای همه شرکت کنندگان و یک پارامتر مختص هر فرد استفاده می‌شود که به شرح ذیل است:

مقدار هدف جدید (T) با استفاده از رابطه $T = T_b \times S \times B_e$ محاسبه می‌شود که با حاصلضرب عدد هدف پایه (Tb)، تعداد ثانیه های گذشته از بلاک قبلی (S) و موجودی حساب موثر فرد (Be) برابر است.

الگوریتم ساختن بلاک در سیستم مبتنی بر گواه اثبات سهام بدین صورت است:

- امضای ساخت بلاک قبلی را در کنار کلید عمومی خود می‌گذارید و حاصل را هش می‌کنید.
- عدد هدف را برای حساب خود در زمان فعلی محاسبه کنید.
- ۸ بایت اول هش بدست آمده را با مقدار عدد هدف مقایسه کنید، اگر کوچکتر نبود به مرحله ۲ برمی‌گردید.
- ۲۵۵ تا از تراکنش‌های تایید نشده را جمع کنید و یک بلاک جدید بسازید و با همه اطلاعات دیگر برای همه کسانی که می‌شناسید بفرستید.
- پایان

مهمترین بخش این سیستم و سیستم‌های مشابه ایجاد رابطه بین موجودی حساب کاربر، و شانس او برای امکان ایجاد بلاک بعد است. وجود فاکتور زمان در فرمول برای تضمین ایجاد بلاک است و طولانی شدن زمان، اجازه ایجاد بلاک را نمی‌دهد.

روش گواه اثبات سهام با پیاده سازی های متفاوت در کریپتوکارنسی های مختلفی مانند PeercoinT, Nxt و Blackcoin استفاده شده است.

گواه اثبات سهام مشکلات مهمی را بر طرف می‌کند با این وجود معایبی نیز به همراه دارد.

- با انتقال تضمین امنیت شبکه از انرژی مصرف شده به پول و ارزشی که در شبکه وجود دارد حمله ۵۱ درصدی یا حملات مشابه از لحاظ فنی سخت تر شده و جلوگیری از آن ها آسان تر خواهد گردید. در صورت وجود چنین حمله هایی و در بدترین حالت، شبکه توسط هارد فورک به حالت قبلی بر می‌گردد.
- کاهش مصرف انرژی شبکه و نیاز شبکه به دستگاه ها و سیستم های بزرگ، آسیب کمتری به محیط زیست وارد می‌کند و باعث هدر رفتن منابع نمی‌شود.
- از لحاظ تئوری بازی (Game theory) کسی که قصد حمله به شبکه دارد چون نیازمند داشتن مقدار زیاد پول در شبکه است انگیزه پایین و هزینه بسیار بالا برای ایجاد آسیب به شبکه دارد. در مقابل مثلاً در سیستم های گواه اثبات کار یک نیروی مهاجم که توانایی محاسباتی بیشتری از نیمی از شبکه را دارد با هزینه فقط انرژی (دستگاه‌ها همچنان قابل استفاده هستند) و به صورت مستمر می‌تواند به یک شبکه حمله کند تا سرانجام شبکه را به طور کامل از کار بیاندازد.
- ابتدایی ترین مشکلی که برای این سیستم ها مطرح می‌شود مساله در خطر نبودن منبع است

3 Base Target Value

4 Target Value

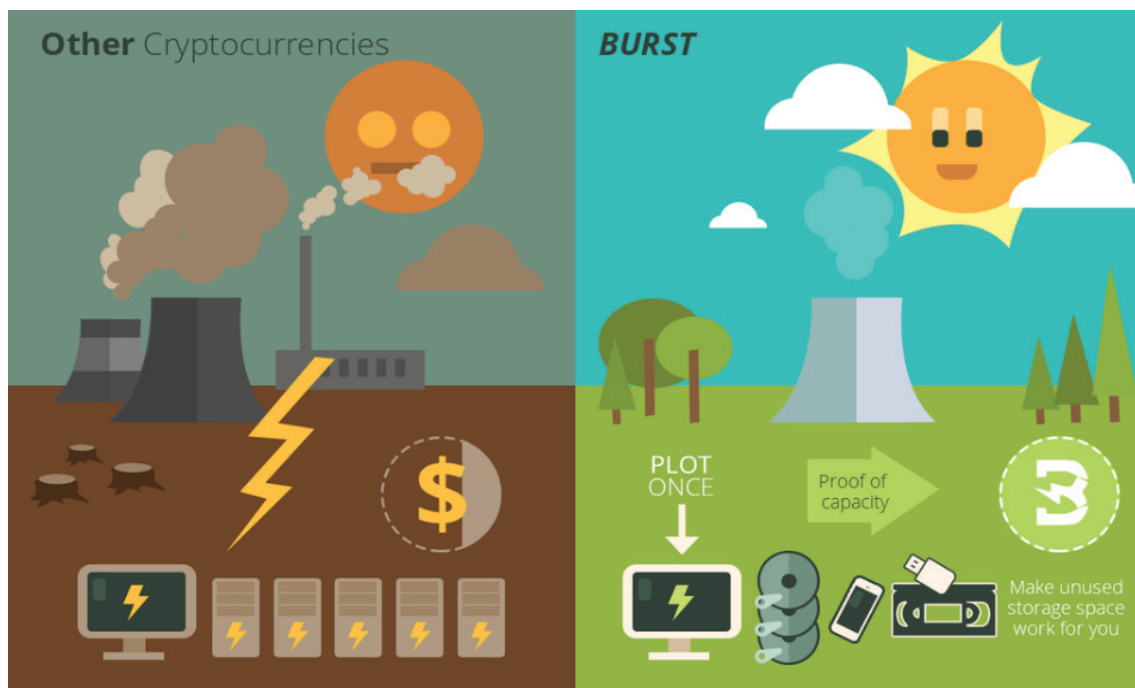
(nothing at stake) که در سیستم های اولیه وجود داشته است. مهاجم می تواند در زمان ایجاد انشعاب (Fork) با هر دو شاخه همراهی کند. هر کدام از الگوریتم ها روش خاصی برای مواجهه با این مشکل دارند. مثلاً در روش پیشنهادی در اتریوم احتمالاً کسی که قصد آسیب زدن به سیستم را داشته باشد مبالغی را که به عنوان تضمین برای ورود به فرایند ساختن بلاک در جایی ذخیره کرده را از دست خواهد داد.

- خطر مرکزیت: کسانی که بیشترین میزان پول را در سیستم دارند قاعداً می توانند آن را کنترل کنند. در صورت داشتن میزان کافی سهام می توان سانسور در سیستم و جلوگیری از بعضی تراکنش ها را اعمال نمود.

گواه اثبات ظرفیت

گواه اثبات ظرفیت^۵ مانند گواه اثبات کار جزو روش های اثبات ارزش داشتن انجام گرفتن خدمات و پایبندی به قوانین از طرف ارائه دهنده خدمات است. در این روش ارائه دهنده خدمات یا استخراج کننده به جای صرف توان پردازشی [انرژی و هزینه آن به طور غیر مستقیم] سعی می کند با اثبات داشتن فضا و ظرفیت ذخیره و بازیابی اطلاعات (هزینه خرید و نگهداری دستگاه های نگهداری اطلاعات به طور غیر مستقیم) هزینه خود را تثبیت کند. کاهش استفاده از انرژی و در واقع سبز بودن این روش یکی از مهمترین دلایل معرفی آن است. این روش هزینه انجام شده برای گواهی هزینه را از به کارگیری انرژی بدون بازگشت به خرید تجهیزات دارای قابلیت استفاده و بازیابی مجدد انتقال می دهد [۷].

برسٹ کوین (Burstcoin) اولین رمز ارزی بود که از این روش استفاده کرده و نیز ماشین تورینگ کامل قبل از اتریوم و کانترپارتهی را عرضه کرد. بلاک پیدایش برسٹ کوین در سال ۲۰۱۴ ایجاد شد و برنامه نویس اصلی و اولیه با نام مستعار برسٹ کوین نیز مانند ناکاموتو بعد از مدتی ناپدید شد.



شکل ۲ - گواه اثبات ظرفیت [۸]

استخراج کننده ها در این الگوریتم، سگمنت ها یا بخش هایی از داده را ایجاد می کنند که به آن پلات گفته می شود و در دیسک سخت ذخیره می گردند. در این الگوریتم، داده ها به گونه ای در دیسک سخت ذخیره می شوند که در هر بخشی از دیسک سخت یک پلات قرار دارد و در هر بخشی از پلات یک هش که به نوعی با آدرس عمومی^۶ فرد در ارتباط است. هر کدام از این بخش ها باید به نوعی با سایر بخش ها در ارتباط باشد که نتوان یکی از این بخش ها را بدون وجود سایر بخش ها ایجاد کرد (اطمینان از ذخیره ی بخش ها بر روی دیسک سخت) و بتوان از ذخیره شدن همه بخش ها با درخواست کردن تنها قسمت کمی از آنها مطمئن شد.

الگوریتم ساده شده گواه اثبات ظرفیت دارای مراحل زیر است:

- پلات های داده را با استفاده از الگوریتم پلات ایجاد، و روی دیسک سخت ذخیره کن. پلاتینگ به معنای شناسایی تمامی راه حل های ممکن برای الگوریتم هشینگ قبل از آغاز استخراج می باشد.
 - امضای بلاک قبل و شماره بلاک فعلی را به هم بچسبان و نتیجه را هش کن.
 - نتیجه هش شده را تقسیم بر ۴۰۹۶ کرده و عدد به دست آمده را «عدد انتخاب» نام گذاری کن.
 - با استفاده از عدد انتخاب از پلات ذخیره شده در موقعیت یک، یک عدد پیدا کن.
 - عدد به دست آمده را به امضای قبلی بچسبان و نتیجه را هش کن.
 - حاصل تقسیم این عدد بر هدف پایه (Base Target) یک عدد به ثانیه خواهد بود که «مهلت» را نشان خواهد داد.
 - اگر بیشتر از یک پلات داری، به مرحله ۴ برو و همه مهلت های ممکن را ایجاد کن.
 - اگر از زمان ایجاد بلاک قبلی به اندازه مهلت زمان گذشته بود شما اجازه دارید یک بلاک جدید بسازید و آن را انتشار دهید.
- مکانیسم اجماع گواه اثبات ظرفیت تلاش می کند تا کوتاه ترین راه حل برای الگوریتم هشینگ را برای ایجاد بلاک بعدی انتخاب کند.

مهم ترین مزایا و معایب این الگوریتم شامل موارد زیر است:

- مصرف کم انرژی و آسایب کمتر به محیط زیست
- استفاده از امکانات قابل استفاده در سایر مصارف
- عدم امکان طراحی مدارهای ویژه (ASIC) که باعث هدررفت سرمایه می شود
- غیر متمرکز بودن
- امکان استخراج برای همگان و حتی در دستگاه های ضعیف و کوچک مانند گوشی های هوشمند
- ارزان بودن امکان استخراج در این سیستم باعث ایجاد مشکلات «سنگ مفت» می شود که هماهنگی در لایه هماهنگی را دچار چالش کرده و نیازمندی برای ایجاد مکانیزم های تنبیهی را ایجاد می کند.
- مشکل زمان-حافظه^۷ مشکلی است که در برست کوین وجود دارد و به مهاجم این امکان را می دهد که با ذخیره مقادیر کمتر و استفاده از توان محاسباتی به جای آن (در موارد خاص) به گونه ای سیستم را دور بزند و بتواند با توجه به میزان پلات های ذخیره شده شانس بیشتری از شانس واقعی به دست آورد.

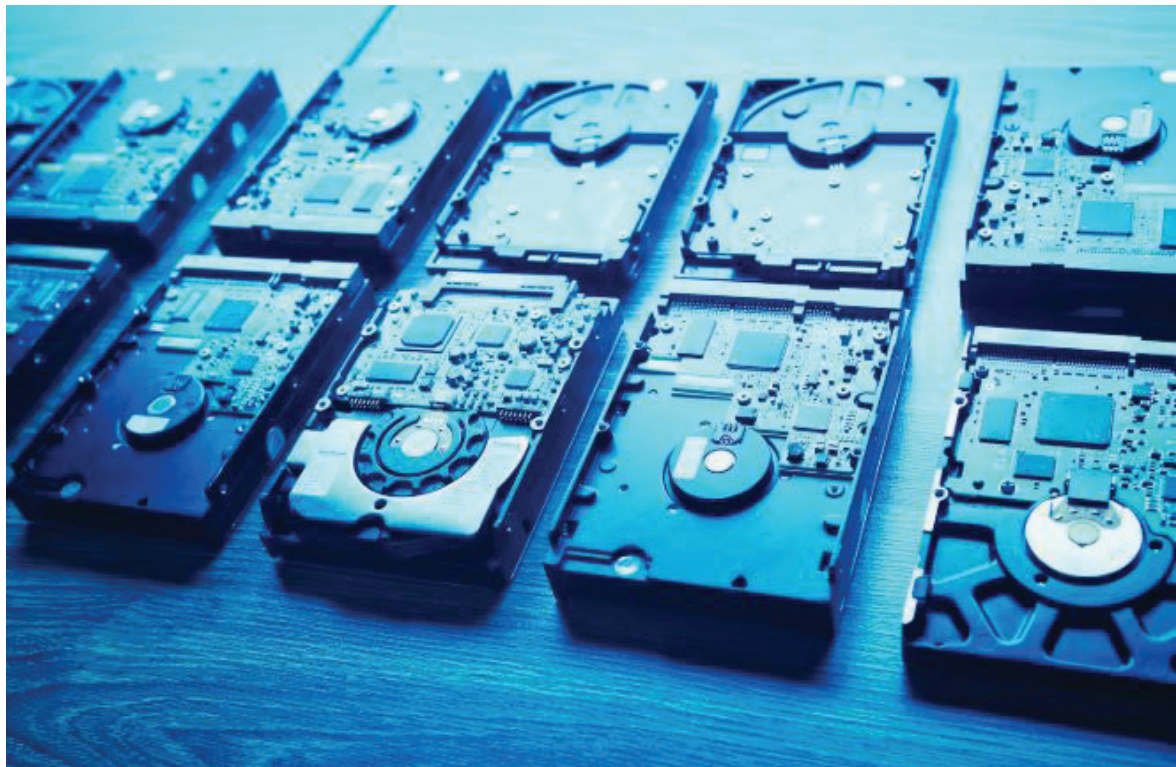
6 Public Key

7 Time-memory Tradeoffs

گواه اثبات فضا

گواه اثبات فضا^۸ روشی جدید برای استخراج رمز ارز ها است که توسط آقای Bram Cohen، بنیان گذار وب سایت معروف BitTorrent و تعدادی از همکاران او شامل Joel Alwen، Danylo Khilko، Leonid Reyzin و حمزه ابوصالح ارائه شده است. روش گواه اثبات فضا به جای استفاده از توان پردازشی که برای افزودن تراکنش های جدید بیت کوین به بلاک چین آن استفاده می شود تمرکز خود را بر روی استفاده بیشتر از حافظه سیستم قرار می دهد و همین امر باعث مصرف بسیار کمتر انرژی و به تبع آن هزینه و آسیب کمتر به منابع محیط زیست می شود. از آنجا که استفاده از این روش مصرف برق بسیار کمتری داشته و نیازمند توان پردازشی بسیار کمتری از سخت افزارها و منابع سیستمی می باشد، انتظار می رود که این روش زمینه ساز ورود بسیاری از افراد با سیستم های کامپیوتری خانگی به صنعت استخراج رمز ارز ها باشد [۹].

در روش جدید، فضای آزاد حافظه سیستم استخراج کنندگان در اختیار شبکه قرار می گیرد تا در صورت ممکن، به نسبت فضای خالی سیستم آن ها به ظرفیت کل فضای شبکه، یک بلاک جدید استخراج شود. انتظار می رود این روش جدید استخراج زمینه ساز ظهور رمز ارز های جدیدی باشد، هر چند به طور قطع نمی توان این موضوع را پیش بینی نمود.



گواه اثبات زمان سپری شده

مکانیسم اجماع گواه اثبات زمان سپری شده^۹ (PoET) بر اساس مقدار زمان باقی مانده از یک مدت زمان مشخص مانند زمان امتحان عمل می کند. این مکانیسم برای شروع از بلاک چین مجوزدار استفاده می کند، به این معنی که

8 Proof of Space

9 Proof of Elapsed Time (PoET)

تمامی گره های سیستم قابل شناسایی بوده و در شبکه پذیرفته شده اند. نکته قابل توجه در گواه اثبات زمان سپری شده در این است که زمان سنج متفاوتی برای هر کدام از گره ها وجود دارد. در این روش، هر کدام از مشارکت کنندگان شبکه یک زمان انتظار تصادفی دریافت می کنند و هر گرهی که زمان انتظار او به پایان برسد می تواند بلاک بعدی بلاک چین را ایجاد نماید [۲].

مکانیسم اجماع PoET در سال ۲۰۱۶ توسط اینتل معرفی گردید و می تواند در Hyperledger Sawtooth مورد استفاده قرار گیرد. Sawtooth پلتفرمی برای ایجاد، پیاده سازی و اجرای دفاتر کل توزیع شده می باشد. گواه اثبات زمان سپری شده بر خلاف گواه اثبات سهام، زمان استراحتی برای گره ها در نظر می گیرد که به افزایش کارایی آن در مصرف انرژی منجر شده است.

گواه اثبات سوزاندن

مکانیسم اجماع گواه اثبات سوزاندن^{۱۰} (POB) از روش ارسال کوین ها به یک آدرس غیر قابل استفاده^{۱۱} [بدون بازگشت] برای ایجاد شانس تولید بلاک بعدی استفاده می کند. آدرس های غیر قابل استفاده در نقطه پایانی تمامی تراکنش های گواه اثبات سوزاندن قرار دارند. آنها سلول های ذخیره سازی برای کوین هایی هستند که از طریق اجماع گواه اثبات سوزاندن قربانی می شوند. از آنجا که آدرس ها به طور تصادفی تولید می شوند هیچ کسی نمی تواند کلید خصوصی آن ها را تشخیص دهد و کوین ها نابود می شوند [۲].

در این روش، استخراج کنندگان با توجه به کوین هایی [سرمایه های کوتاه مدت] که می سوزانند مجوز های لازم برای ادامه حیات و استخراج بلاک بعدی در بلاک چین را دریافت می کنند. افرادی که سکه های بیشتری سوزانده باشند از شانس بیشتری برای انتخاب شدن برخوردارند. با این وجود، شانس اعطایی با گذر زمان کاهش می یابد و برای دریافت شانس دوباره تولید بلاک باید کوین های جدیدی سوزانده شود.



10 Proof of Burn (POB)

11 Eater

این مکانیسم در کوتاه مدت هزینه هایی را به کاربر تحمیل می کند ولی امکان دستیابی به دستاورد های بزرگتر در آینده می تواند کاربران را به مشارکت در پروژه ترغیب کند و در نتیجه این شبکه را حفظ نماید. با این وجود، سوزاندن کوین ها هیچ تضمینی برای انتخاب کاربر به منظور استخراج بلاک بعدی ارائه نمی دهد. همانند گواه اثبات سهام، این فرآیند به نفع نهنگ هایی است که می توانند سرمایه بیشتری جذب کنند.

Slimcoin از الگوریتم اجماع گواه اثبات سوزاندن در شبکه خود استفاده کرده است و Counterparty نیز از این روش در ایجاد توکن از طریق سوزاندن رمز ارز های دیگر بهره می گیرد. کاربران Counterparty بیت کوین های خود را به آدرس های غیر قابل بازگشت ارسال می کنند و در عوض توکن های XCP دریافت می کنند.

گواه اثبات فعالیت

همه مکانیسم های اجماع تلاش می کنند تا چیزی را ثابت کنند. برای مثال، استخراج کنندگان در گواه اثبات کار تلاش می کنند تا کار سخت افزار های استخراج خود برای حل معمای ریاضی را نشان دهند. گره های استخراج کننده در گواه اثبات فعالیت^{۱۲} نیز تلاش می کنند تا دخالت مستقیم در روند استخراج و امضای بلاک بعدی در بلاک چین را نشان دهند. گواه اثبات فعالیت تلاشی برای اختراع دوباره چرخ ندارد و تغییر زیادی در الگوریتم های گواه اثبات کار و گواه اثبات سهام ایجاد نکرده است. این مکانیسم ترکیبی از این دو روش اجماع می باشد. فرآیند استخراج با گواه اثبات کار شروع می شود و پس از یافتن بلاک بعدی به رویکرد گواه اثبات سهام تغییر می کند [۲].

بلاک هایی که در این روش تولید می شوند فقط شامل سرآیند^{۱۳} (هدر) و آدرس جایزه استخراج کننده می باشند در حالی که در روش POW اطلاعات بیشتری مانند ریشه تراکنش و Nonce در بلاک ها ذخیره می شوند. برای ارزیابی بلاک ها از یک گروه تصادفی از گره های اعتبار سنجی برای امضای بلاک استفاده می شود. شانس انتخاب یک گره با افزایش اندازه کیف پول گره افزایش می یابد. هزینه های استخراج نیز بین استخراج کنندگان حاضر در یافتن بلاک و گره های امضا کننده آن تقسیم می شود. Decred (DCR) پروژه ای بود که در سال ۲۰۱۶ با استفاده از این مکانیسم راه اندازی گردید.

گواه اثبات قدرت

بلاک چین از جمله فناوری های پیشتاز به شمار می رود با این وجود، محدودیت هایی نیز دارد. همانند بسیاری از سیستم ها، بلاک چین نیز بدهستان های^{۱۴} مخصوص به خود را دارد. ویتالیک بوتورین^{۱۵} از این موضوع به عنوان Scalability Trilema یاد می کند که سه خصیصه مطلوب بلاک چین یعنی مقیاس پذیری، غیر متمرکز بودن و امنیت را نمایش می دهند. ولی سه ضلع این مثلث به سختی کنار هم قرار می گیرند و معمولاً دو مورد از آن ها را به طور همزمان می توان پوشش داد. با توجه به رشد روز افزون برنامه کاربردی توزیع شده (dApps) در بستر اتریوم و دیگر پلتفرم های بلاک چین، مقیاس پذیری در کوتاه مدت از اهمیت بالاتری برخوردار است [۲].

بر خلاف اجماع گواه اثبات سهام که سهم گره ها بر اساس ارزش پولی آنها است، سهم هر گره در اجماع گواه

12 Proof of Activity

13 Header

14 Tradeoffs

15 Vitalik Buterin

اثبات قدرت^{۱۶} بر اساس هویت واقعی گره ها در سیستم تعیین می شود. این یک چرخه در گواه اثبات سهام است که مخاطرات مربوط به چگونگی ارزیابی یک سهم توسط اعضای شبکه را مشخص می کند. در حالی که گواه اثبات سهام، سرمایه های مالی را در مرکز توجه قرار می دهد ولی مکانیسم اجماع گواه اثبات قدرت، انگیزه ها را از طریق در معرض خطر قرار دادن سرمایه اجتماعی [شهرت گره ها] هماهنگ می کند.

گره هایی به عنوان ارزیاب در شبکه وجود دارند که از شهرت خود به عنوان سهم در شبکه استفاده می کنند و در مقابل تنها گره هایی هستند که می توانند اعتبار یک بلاک را تأیید کنند. با توجه به نقش مهم این گره ها، باید از وجود یک فرآیند استاندارد و قوی برای شناسایی اعتبارسنج ها اطمینان حاصل شود. یک پروسه قابل اطمینان برای ایجاد مجوز تمامی اعتبار سنج ها مورد نیاز است. همچنین تعداد اعتبارسنج ها باید محدود باشد تا انگیزه کافی برای حفظ این سمت وجود داشته باشد.

مکانیسم اجماع گواه اثبات قدرت با شناسایی اعتبارسنج ها ذاتاً به یک روش متمرکز تبدیل می شود. بنابراین روشی مناسب برای بلاک چین های خصوصی و کنسرسیومی مانند گروهی از بانک ها یا شرکت های بیمه به شمار می رود. پروژه های Kovan, Rinkeby, Giveth, TomoChain, Go Chain و Colony از جمله مواردی می باشند که از گواه اثبات قدرت استفاده کرده اند.

گواه اثبات سهام اعطایی

مکانیسم های اجماع امروزی، کاربران را در یک چرخه دموکراتیک قرار می دهند. همان طور که می توان حدس زد گواه اثبات سهام اعطایی^{۱۷} (DPoS) تغییر یافته گواه اثبات سهام است که برای اعتبارسنجی بلاک ها به یک گروه از نمایندگان از طرف تمام گره های شبکه متکی است. معمولاً ۲۱ تا ۱۰۰ نماینده با استفاده از اجماع DPoS در شبکه انتخاب می شوند. این روش سازمان دهی و کنترل را آسان تر کرده و امکان انتشار شرایط بلاک در شرایط مشخص را افزایش می دهد. اگر نماینده انتخاب شده در ارائه گزارش های مورد نیاز تأخیر کرده یا اشتباه کند گره های شبکه می توانند برای جایگزینی او رأی گیری کنند [۲].

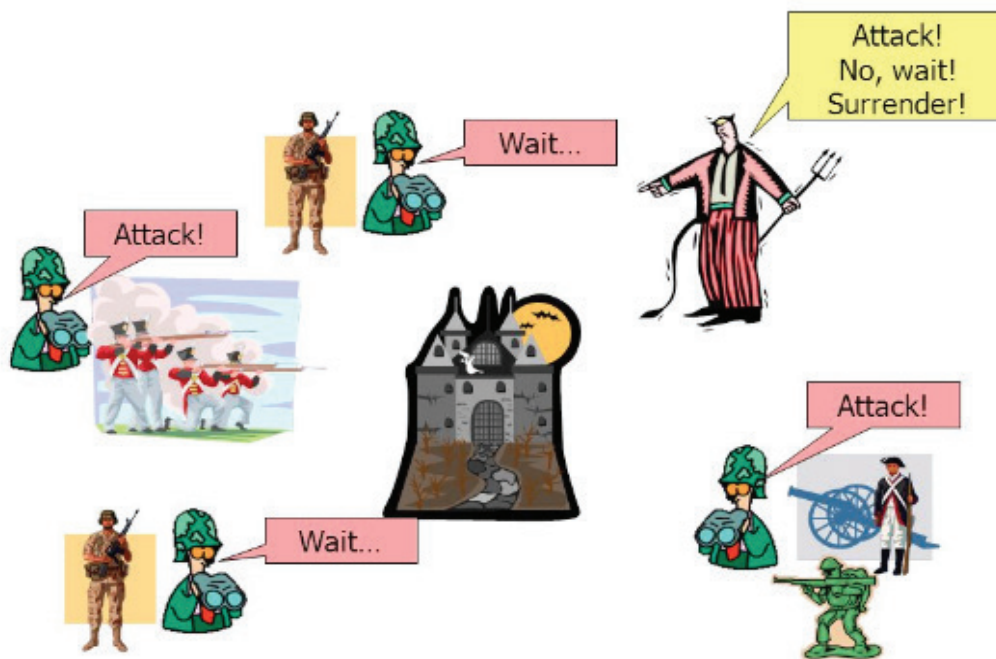
از مهم ترین ویژگی های این مکانیسم می توان به مقیاس پذیری، مصرف بهینه انرژی و هزینه پایین تراکنش ها اشاره کرد. ولی با وجود تمامی این مزایا، این مکانیسم نیمه متمرکز محسوب می شود. این مکانیسم در BitShares، EOS و Steemit مورد استفاده قرار گرفته است.

تحمل پذیری خطای بیزانس

مجموعه ای از ژنرال های بیزانس، یک شهر را با نیروهای خود محاصره کرده اند تا در آینده به آن حمله کنند. با این حال، برای این که این محاصره نتیجه بخش باشد باید بر روی زمان حمله به اجماع برسند. اگر هماهنگی ژنرال ها با موفقیت انجام نشود حمله شکست خواهد خورد [۲].

16 Proof of Authority (PoA)

17 Delegated Proof of Stake (DPoS)



شکل ۳- تحمل پذیری خطای بیزانس [۱۰]

مشکل ژنرال های بیزانس^{۱۸} یک مشکل کلاسیک است که به یک نوع محبوب تر از اجماع با عنوان تحمل پذیری خطای بیزانس^{۱۹} (BFT) برای سیستم های رمزنگاری اشاره می کند. BFT برای تأیید قابل اعتماد بودن اطلاعاتی که دریافت کرده است به گروهی از ژنرالها یا اعتبار سنجان وابسته است. ژنرال ها برای نهایی سازی استراتژی خود نمی توانند به طور همزمان با یکدیگر ارتباط داشته باشند. آنها برای برقراری ارتباط از پیام رسان ها استفاده می کنند. با توجه به خطرات موجود در مسیر، قابلیت اعتماد پیام های دریافتی بسیار پایین است.

این مکانیسم در کنار هزینه های پایین تراکنش، بازده بسیار بالایی داشته و از مقیاس پذیری بالایی برخوردار است. با این وجود، فقط در شبکه های متمرکز و مجوزدار مورد استفاده قرار می گیرد. نسخه های متفاوتی از این مکانیسم اجماع توسعه داده شده است که در ادامه به دو مورد از آن اشاره می شود.

تحمل پذیری خطای بیزانس کاربردی

تحمل پذیری خطای بیزانس کاربردی^{۲۰} (PBFT) در Hyperledger Fabric مورد استفاده قرار گرفته است. PBFT از ۲۰ ارزیاب از پیش انتخاب شده به منظور تعیین اجماع برای شبکه استفاده می کند.

توافق بیزانس یکپارچه

توافق بیزانس یکپارچه^{۲۱} (FBA) در شبکه های استلار و ریپل مورد استفاده قرار گرفته است. FBA از هر کدام از گره ها (ژنرال ها) می خواهد که اعتماد مورد نیاز را برای هر یک از زنجیره های مربوطه ایجاد کنند.

18 Byzantine Generals Problem (BGP)

19 Byzantine Fault Tolerance (BFT)

20 Practical Byzantine Fault Tolerance (PBFT)

21 Federated Byzantine Agreement (FBA)

گواه اثبات اهمیت

الگوریتم های اجماع مختلف را می توان در یک شبکه غیر متمرکز به منظور انگیزه دادن به کاربران برای پیروی از مجموعه ای از قوانین به کار برد. هر کدام از الگوریتم ها مزایا و معایب خاص خود را دارند که بسته به فعالیت تشویقی مورد نظر شبکه برای کاربران، درجات مختلفی از موفقیت را به همراه دارند. گواه اثبات اهمیت^{۲۲} (POI) فاکتور های دیگری را شناسایی می کند که می توانند در شناسایی ارزشمندترین گره ها برای شبکه مورد استفاده قرار گیرند. برای مثال، اگر درصد بالایی از سهم ها در مکانیسم اجماع گواه اثبات سهام در دست افراد خاصی متمرکز شود نمی توان انگیزه کافی برای مشارکت دیگر اعضای شبکه ایجاد کرد [۲].

فاکتور های کلیدی مکانیسم اجماع گواه اثبات اهمیت شامل موارد زیر می باشد.

- انتقال های خالص^{۲۳} یا کل هزینه در ۳۰ روز گذشته
- اختصاص مقداری از ارز برای ایجاد بلاک
- وزن بیشتر گره های خوشه بندی شده و یکپارچه سازی شده

این مکانیسم توسط New Economy Movement (XEM) معرفی شده است و برای ایجاد یک گره اصلی یا سهم باید حداقل ۱۰۰۰ XEM داشته باشید. مکانیسم اجماع گواه اثبات اهمیت برخلاف گواه اثبات سهام تلاش می کند که شانس های ذخیره سازی سهم ها را کاهش دهد. روش های سنتی فقط به موقعیت ها توجه می کردند و هیچ ارزشی در شبکه انتقال پیدا نمی کرد. انتقال های خالص درجه بندی بهتری از اداره کنندگان ایستگاه های جابجایی ارائه می دهند. همچنین در این روش، هزینه های حاشیه ای برای ایجاد یک بلاک صفر است و این بدین معنی است که اگر انشعابی ایجاد شود کاربران می توانند اعتبار بلاک ها را با استفاده از POS تأیید نمایند.



گراف جهت دار غیر مدور

اکثر مکانیسم های اجماع رویکرد یکسانی دارند و تنها در انواع مختلفی از فناوری دفتر کل توزیع شده مورد استفاده قرار گرفته اند. گراف جهت دار غیر مدور^{۲۴} (DAG) یکی از شکل های محبوب اجماع برای ساختار های پایگاه

22 Proof of Importance (POI)

23 Net Transfers

24 Direct Acyclic Graphs (DAG)

داده غیر بلاک چینی است که نقاط قوت و ضعف خود را در مدیریت داده ها دارد [۲].

IOTA از نوعی الگوریتم اجماع استفاده می کند که با نام Tangle شناخته می شود و نوعی گراف جهت دار غیر مدور است. در این روش، هر گره برای ارسال تراکنش باید دو تراکنش انجام شده را تأیید نماید. افزایش تعداد تراکنش های Tangle موجب تقویت سیستم بررسی و تعادل هر چه بیشتر شبکه می شود. تراکنش ها از طریق مشارکت کاربران برای تأمین امنیت شبکه به واسطه تأیید تراکنش های گذشته تأیید می شوند و هیچ هزینه ای به شبکه تحمیل نمی کنند. علاوه بر این، شبکه IOTA ناهمگام است و نیازی نیست تمامی تراکنش ها در زمان یکسانی رخ دهند. معاملات پولی یک زیر مجموعه کوچک از تعاملات بین دستگاه های متصل شده را نشان می دهند. Tangle مقیاس پذیر بوده و هزینه پیاده سازی پایینی دارد و نسبت به بلاک چین می تواند ساختار پایگاه داده سودمند تری برای مبادلات اینترنت اشیا ارائه دهد [۲].



- [1] M. Rouse, "consensus algorithm," whatis.com, . Available: <https://whatis.techtarget.com/definition/consensus-algorithm>. [2018].
- [2] Daily Bit, "9 Types of Consensus Mechanisms That You Didn't Know About," Medium, 2018. Available: <https://medium.com/the-daily-bit/9-types-of-consensus-mechanisms-that-you-didnt-know-about-49ec365179da>. [2018].
- [3] Available: <http://101blockchains.com>.
- [4] Blockgeeks, "Proof of Work vs Proof of Stake: Basic Mining Guide," Blockgeeks. Available: <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>. [2018].
- [5] ا. محقق, "گواه اثبات کار در مقابل گواه اثبات سهام," کوین ایران, ۱۳۹۵. [درون خطی]. Available: <https://coiniran.com/>. ۱۳۹۷.
- [6] م. بنی اسد, "گواه اثبات سهام (proof of stake) چیست؟," کوین ایران, ۱۳۹۶. . Available: <https://coiniran.com/>. ۱۳۹۷.
- [7] م. بنی اسد, "گواه اثبات ظرفیت چیست؟," کوین ایران, ۱۳۹۶. [درون خطی]. Available: <https://coiniran.com/>. ۱۳۹۷.
- [8] Available: <https://www.bitex.in/mining-with-your-hard-disk-proof-of-capacity/>.
- [9] آ. جنگمیری, "معرفی یک روش استخراج سازگار با محیط زیست توسط سازنده BitTorrent به نام "گواه اثبات فضا", " کوین ایران, ۱۳۹۶. [۱۳۹۷]. Available: <https://coiniran.com/>.
- [10] Available: <http://slideplayer.com/slide/5163640/>.

کوین ایران بزرگ‌ترین پایگاه خبری فارسی زبان در حوزه فناوری بلاک‌چین، ارزهای رمزنگاری شده و پلتفرم‌های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیوند و آرش محبوب، با هدف اطلاع‌رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه‌مند به رمز ارزها راه‌اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید. هدف کوین ایران از معرفی فناوری بلاکچین، ایجاد محیطی پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به جوامع فارسی زبان است.

www.coiniran.com



کوین ایران در شبکه‌های اجتماعی

نویسنده: تورج اکبری

طراحی و گرافیک: تورج اکبری

