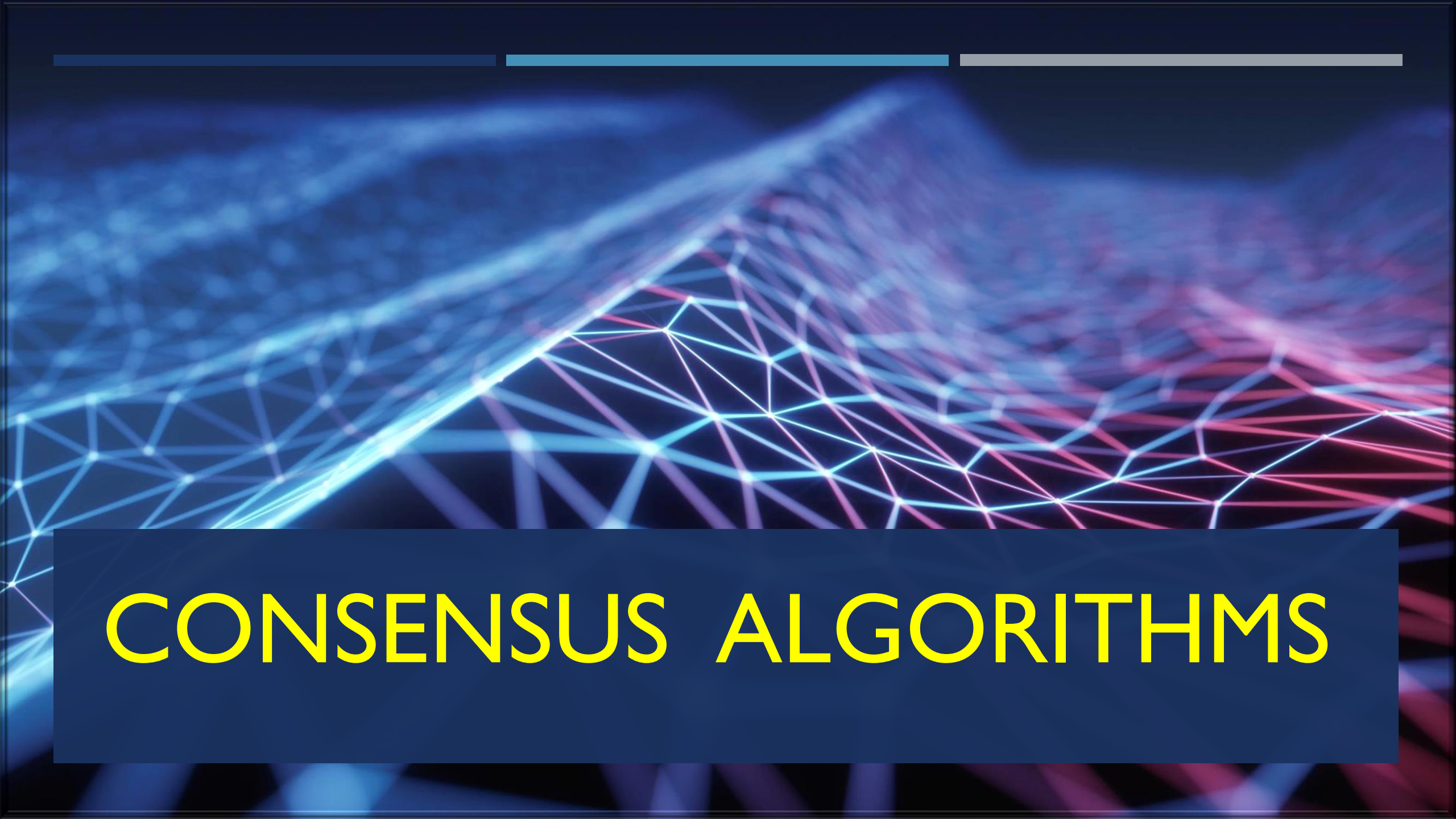
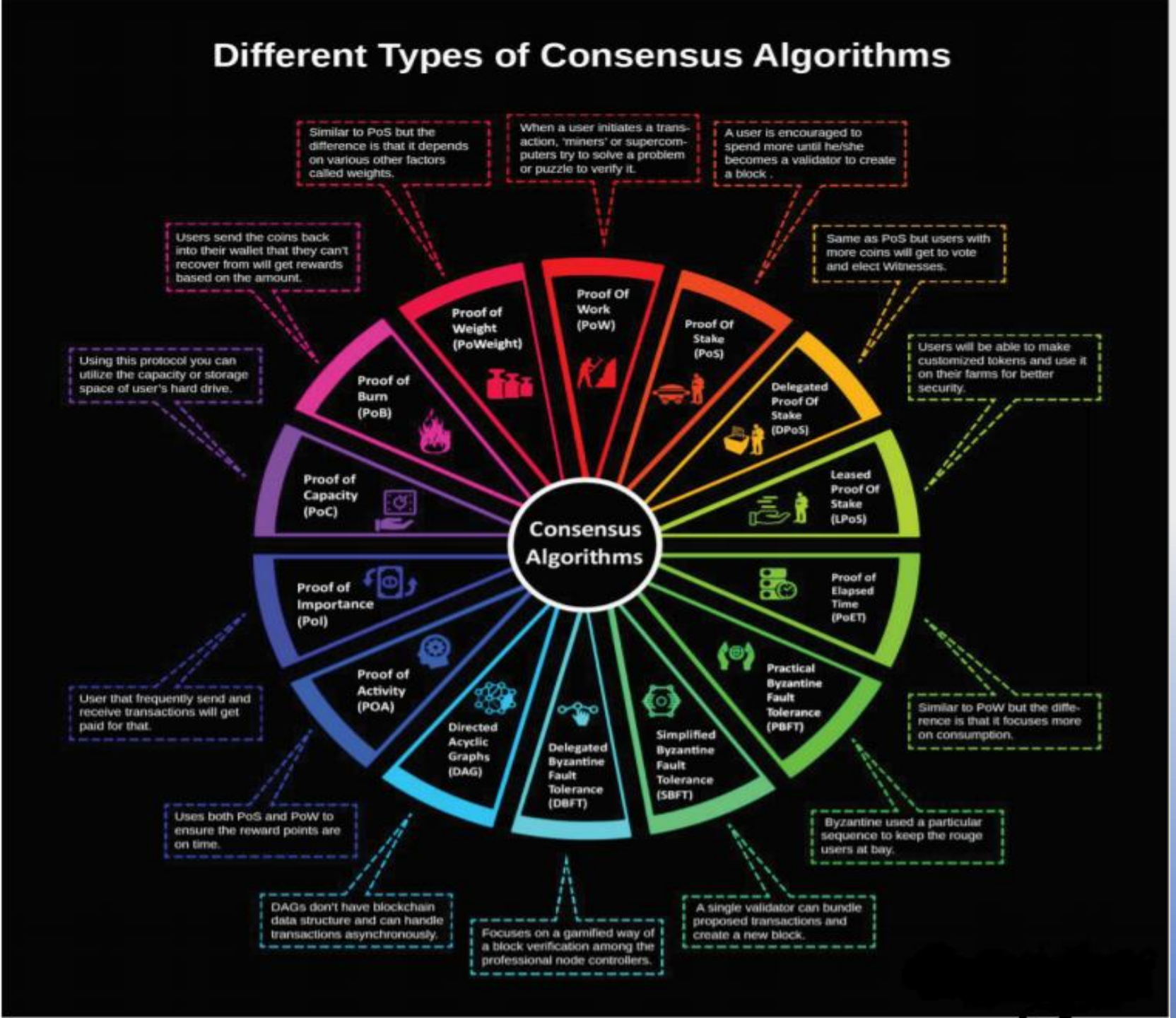

CONSENSUS ALGORITHMS



همانطور که در اسلایدهای قبلی توضیح داده شد الگوریتم‌های اجماع به این معناست که یک گروه بر سر یک روش با هم به توافق می‌رسند. الگوریتم اجماع، به زبان ساده یعنی روش‌هایی برای به توافق رسیدن اعضای یک شبکه بر اساس ساز و کار این الگوریتم تمام نودهای شبکه به تایید [redacted] و ایجاد بلاک‌های جدید می پردازند.

کاربردهای الگوریتم های اجماع

- 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 شمارمی 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 تأثیرقرار می دهند. این مکانیسم ها به شکل های متفاوت برای بلاک چین های مختلف ارائه می شوند

گواه اثبات کار

گواه اثبات سهام

گواه اثبات ظرفیت

گواه اثبات فضا

گواه اثبات زمان سپری شده

گواه اثبات سوزاندن

گواه اثبات فعالیت

گواه اثبات قدرت

گواه اثبات سهام اعطایی

تحمل پذیری خطای بیزانس

تحمل پذیری خطای بیزانس کاربردی

توافق بیزانس یکپارچه

گواه اثبات اهمیت

گراف جهت دار غیر مدور

روش اثبات کار یا proof of work (POW) :

این روش اجماع که در سلایدهای قبلی به طور مفصل توضیح داده شده یکی از معروف ترین روش های اجماع است که اولین بار در بلاک چین بیت کوین از آن استفاده شد و در حال حاضر سایر ارزهای دیجیتال هم بر اساس همین روش کار می کنند.علاوه بر بیت کوین ارزهای دیجیتال دیگری مانند لایت کوین، بیت کوین کش، مونرو، زی کش و دش از

روش اثبات کار یا proof of work (POW) :

در بیت کوین گواه اثبات کار به همراه هشینگ در سیستم ماینینگ به کار رفت و روشی به وجود آورد که از نفوذ هکرها جلوگیری می‌کرد.
در این روش، داده‌هایی که باید در بلاک‌ها نوشته شود، با کمک الگوریتمی وابسته به هش ، هش می شوند.
در میان افراد حاضر در شبکه، کسی که هش درست را پیدا کرده باشد، باید برای گرفتن تایید، آن را به همه شبکه ارسال کند.
افراد دیگر در شبکه به تایید یا رد هش ارسال شده می‌پردازند و در صورتی که بیش از ۵۰ درصد (۵۰+۱) آن را تایید کنند، بلاک به عنوان یک بلاک معتبر بسته می‌شود.
در این روش گره‌ای که موفق به حل مسئله شود پاداش دریافت می‌کند

مزایا POW:

- دریافت بیت کوین به عنوان پاداش علاوه بر دریافت کارمزد تایید تراکنش ها

معایب POW :

- مصرف بالای برق و انرژی

- حملات ۵۱درصدی

در صورتی که شخص، شرکت یا سازمانی توانایی تصاحب ۵۱ درصد از قدرت محاسباتی شبکه را داشته باشد، عملا الگوریتم اجماع برای تامین امنیت کارساز نخواهد بود و آن شخص یا موسسه می‌تواند با اضافه کردن یک بلاک نامعتبر به شبکه، امنیت شبکه را به خطر بیندازد

الگوریتم اجماع اثبات سهام proof of stake :

این روش برای رفع معایب روش اثبات کار ایجاد شد . هدف هر دو الگوریتم برای دستیابی به اتفاق نظر در بلاک چین یکسان است ولی روند رسیدن به هدف در اونها کاملاً متفاوته.برای توضیح این روش ابتدا باید با مفهوم staking آشنا شوید.

Staking:

استیک کردن به معنای نگهداری دارایی‌ها در یک کیف پول رمز ارز است، تا امنیت و عملکرد شبکه بلاک چین را تامین کند. به بیانی دیگر، استیکینگ قفل کردن رمز ارزها به منظور دریافت پاداش است. در بیشتر موارد، شما می‌توانید کوین‌ها و توکن‌های خود را به صورت مستقیم در کیف پول کریپتوی خود استیک کنید. از طرفی، بسیاری از صرافی‌ها خدمات استیکینگ را به کاربران خود ارائه می‌دهند.
در واقع شما رمز ارزهای خود را نگهداری می‌کنید تا بتوانید تراکنش‌ها را تایید کنید و از شبکه پشتیبانی کنید. در ازای نگهداری کریپتو و قدرت بخشیدن به شبکه، شما پاداش دریافت می‌کنید

. شما با استیک کردن می‌توانید درآمد انفعالی برای خود ایجاد کنید. علاوه بر پاداش Staking ، زمانی که قیمت توکن یا کوین شما افزایش یافت، از آنجا هم سود اضافی دریافت می‌کنید. البته باید بدانید که تمام رمز ارزها از استیکینگ پشتیبانی نمی‌کنند.

ادامه توضیحات مربوط به روش اجماع اثبات سهام (POS) :

روشی ست که اجماع را به صورت غیرمتمرکز انجام می‌دهد، اما با هزینه بسیار پایین‌تر.
در این روش تایید کنندگان کنندگان که به آنها Forger هم میگن می‌توانند کریپتوی خود را قفل کنند (استیک کنند) و پروتکل به صورت تصادفی انتخاب می‌کند که کدام یک از مشارکت کنندگان بلاک بعدی را تایید کند. معمولا انتخاب شدن یک مشارکت کننده (Forger)، بستگی به مقدار رمز ارزی دارد که استیک کرده است؛ هر چه مقدار بیشتری رمز ارز استیک کنید، شانس شما بیشتر است
بنابراین تشخیص این که چه کسی بلاک بعدی را بسازد، دیگر میزان توانایی او برای حل کردن مسائل پیچیده با قدرت هش بالا نیست؛ بلکه بستگی به مقدار کوین یا توکن استیک کرده شخص دارد. بنابراین هیچ گره ای نمیتواند نوبت خود را پیش بینی کند و شمار زیادی از کوین ها در استخر سهام نگهداری می شوند تا شانس ایجاد بلوک را خریداری کنند.

در این الگوریتم خبری از دریافت پاداش نیست و تاییدکنندگان ، فقط از طریق کارمزد تراکنش‌ها کسب درآمد می‌کنند.

نمونه هایی از ارزهای دیجیتالی که براساس روش اثبات سهام کار می کنند:

پولکادات(EOS)، و انتولوژی(ONT)

مزایا:

- وابستگی کمتر شبکه به برق
- مقیاس پذیری بالاتر

مقیاس‌پذیری اصطلاحی است که به توانایی بزرگ‌شدن و افزایش ظرفیت یک سیستم درهنگام افزایش پردازش‌ها اطلاق می‌شود
غیرمتمرکزو امن بودن بودن (زیرا مانع ایجاد استخرهای متمرکز ماینینگ می شود و احتمال حملات مخرب را کاهش میدهد)

معایب:

- عدم دریافت پاداش ارز دیجیتال جهت ایجاد بلاک
- خطر double spending (خرج کردن پول دو مرتبه)

چون ارزدیجیتال ، پول فیزیکی نیست پس می‌توان آن را کپی کرد و دوباره از آن استفاده کرد که به آن خطر دو بار خرج کردن و یا double spending می گویند.

تفاوت روش اثبات کار و اثبات سهام:

گواه اثبات سهام خصوصی شده یا وکالتی (dPoS):

بلاک چین‌های مبتنی بر dPoS دارای سیستم رای‌گیری هستن که طی اون، سهامداران شبکه کار خودشون رو به شخص ثالث برون سپاری می‌کنن؛ به عبارت دیگه، میتونن برای انتخاب نمایندگان رای بدن و این نمایندگان از طرف سهامداران به ایمن سازی شبکه خواهند پرداخت. به این نمایندگان، شاهد یا Delegatorنیز گفته میشه و اونها مسئول دستیابی به اجماع طی تولید و تایید بلاک‌های جدید هستند. در این الگوریتم نمایندگان انتخاب شده برخلاف الگوریتم‌های اثبات کار و اثبات سهام با هم دیگر رقابتی برای تایید بلوک‌ها ندارند و درعوض در این راستا به یکدیگر کمک می‌کنند

- مقیاس پذیری بالاتر
- سرعت بالاتر
- مصرف کمتر
- **جامع‌تر از رقبا:**

استفاده از این الگوریتم در مقایسه با الگوریتم اثبات کار توان محاسباتی کمتری را می‌طلبد، از طرف دیگر در مقایسه با الگوریتم اثبات سهام به کاربرانی که سهام کمتری دارند قدرت نظارت بیشتری می‌دهد. با توجه به آنچه گفته شد می‌توان الگوریتم اثبات سهام وکالتی را جامع‌تر از الگوریتم اثبات کار و الگوریتم اثبات سهام معرفی کرد.

انرژی

معایب:

- **شرط حضور افراد**

برای انجام رای‌گیری نیاز به حضور افرادی در شبکه است تا بتوان نظارتی دقیق بر شبکه داشت، و این موضوع باعث می‌شود شبکه تا حدودی متمرکز شود.

آسیب‌پذیر در رابطه با متمرکزسازی

از آنجایی که تعداد شاهدان که از در شبکه‌های مبتنی بر الگوریتم اثبات سهام وکالتی بسیار کمتر از افراد حاضر در شبکه‌های مبتنی بر الگوریتم‌های اثبات کار و اثبات سهام است، می‌توان گفت این شبکه‌ها همیشه در معرض مشکل متمرکزسازی هستند

روش تحمل خطای بیزانس به صورت عملی(PBFT):

خطای بیزانس چیست؟

همانطور که میدانید نودهای شبکه که به غیرمتمرکز ماندن اکوسیستم کمک می‌کنند، برای فعالیت درون شبکه پاداش‌های متناسبی دریافت می‌کنند. اما اگر تعدادی نود خرابکار در شبکه وجود داشته باشند که در انجام تراکنش‌ها اختلال ایجاد کنند چه اتفاق می‌افتد؟ در اینجاست که شبکه با خطای بیزانس مواجه می‌شود. به طور خلاصه، خطای بیزانس وقتی به وجود می‌آید که تعدادی از افراد یا عناصر موثر در یک اکوسیستم، به دلایل مختلف با انجام یک عملیات موافقت نمی‌کنند و تصمیم به ایجاد اختلال در آن عملیات می‌گیرند.

نمونه هایی از روش اجماع PBFT:
ارز استلار(XLM)
ارز ریپل(XRP)

راه حل:

راه حل این مسئله، شاخصه‌ای به نام تحمل خطای بیزانس است. این اصطلاح در واقع نشان دهنده ظرفیت یک سیستم دیجیتال برای مقاومت در برابر نوع خاصی از خطاها را نشان می‌دهد. این خطاها معمولا زمانی رخ می‌دهند که مولفه‌های الکترونیکی در هنگام انتقال داده‌ها با خرابی یا اشکال مواجه شوند.

از آنجا بلاک چین‌ها دفتر کل های غیرمتمرکز هستند، توسط هیچ فرد یا نهاد خاصی کنترل نمی‌شوند و اختیار تصمیم‌گیری برای عملیات‌های شبکه در دست نهاد خاصی نیست. به همین خاطر، گفته می‌شود که بلاک چین‌ها دارای امکان مقابله با خطای بیزانس هستند. یعنی حتی اگر عنصر یا عناصر خرابکاری در شبکه وجود داشته باشند، از آنجایی که تمام قدرت شبکه را در دست ندارند، امکان ایجاد اختلال در روند برای آنها وجود ندارد.

در فضای سیستم‌های توزیع شده، تحمل خطای بیزانس (Byzantine Fault Tolerance) یعنی توانایی یک شبکه کامپیوتری توزیع شده برای عملکرد مطلوب و صحیح که در نهایت این عملکرد منجر به اجماع کافی شود. این اجماع در حالی ایجاد می‌شود که مولفه‌ها یا نودهای خرابکار در سیستم در دادن اطلاعات به همتا های دیگر شکست می‌خورند و یا اطلاعات نادرست را به آنها انتقال می‌دهند. هدف از این عملکرد صحیح دفاع در برابر شکست‌های سیستمی مصیبت بار است که این کار با کاهش تاثیرگذاری نودهای خرابکار بر روی عملکرد صحیح شبکه انجام می شود و سبب اجماع درستی می‌شود که توسط نود های صادق در سیستم انجام می‌شود.

مزایا:

- کارمزد پایین تراکنش
- مقیاس پذیری بالا

معایب:

- متمرکز بودن

گواه اثبات ظرفیت

Proof of Capacity

در این روش ارائه دهنده خدمات یا استخراج کننده به جای صرف توان پردازشی 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. برست کوین (Burstcoin) اولین رمز ارزی بود که از این روش استفاده کرده و نیز ماشین تورینگ کامل قبل ازاتریوم و کانترپارتی را عرضه کرد. بالک پیدایش برستکوین در سال ۲۰۱۴ ایجاد شد و برنامه نویس اصلی و اولیه با نام مستعار برست کوین نیز مانند ناکاموتو بعد از مدتی ناپدید شد.

الگوریتم ایجاد پلات

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 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 بخش‌ها ایجاد کرد (اطمینان از ذخیره بخش‌ها 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 ظرفیت

پلات‌های داده را با استفاده از الگوریتم پلات ایجاد کن و روی دیسک سخت ذخیره کن.

امضای بلاک قبل و شماره بلاک فعلی را به هم بچسبان و نتیجه را هش کن

نتیجه هش شده را تقسیم بر ۴۰۹۶ کن و عدد بدست آمده را «عدد انتخاب» بنام

با استفاده از عدد انتخاب از پلات ذخیره شده در یک، یک عدد پیدا کن

عدد بدست امده 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.

مزایا و معایب

مصرف کم انرژی و آسیب کمتر به محیط زیست.

استفاده از امکانات قابل استفاده در سایر مصارف.

عدم امکان طراحی مدارهای ویژه که باعث هدررفت سرمایه میشود ASIC Proof

طراحی شده برای عدم تمرکز.

امکان ماین کردن برای همگان و حتی در دستگاه های ضعیف و کوچک مانند گوشی‌های هوشمند.

ارزان بودن امکان ماین در این سیستم باعث ایجاد مشکلات «سنگ مفت» (Nothing at Stake) می شود که هماهنگی در لایه هماهنگی را دچار چالش می کند و نیازمندی برای ایجاد مکانیزم های تنبیهی را ایجاد می کند.

مشکل زمان-حافظه (time-memory tradeoffs)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 جان آن (در موارد خاص) به گونه‌ای سیستم را دور بزند و بتواند شانسی بیشتر از شانس واقعی اش (بنا به میزان پلات های ذخیره شده) بدست آورد.

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(DAG) یکی از شکل های محبوب اجماع برای ساختار های پایگاه داده غیر بالک چینی است که نقاط قوت و ضعف خود را در مدیریت داده ها دارد

IOTA از نوعی الگوریتم اجماع استفاده می کند که با نام Tangle شناخته می شود و نوعی گراف جهت دار غیرمدور 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 نمیکنند. 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 وهزینه پیاده سازی پایینی دارد و نسبت به بالک چین می تواند ساختار پایگاه داده سودمند تری برای مبادالت اینترنت اشیاء ارائه دهد.

مزایای DAG

در یک DAG، یک گره می تواند به تنهایی تراکنشی را صادر و تأیید کند. برای دستیابی به این هدف ، تراکنش و اعتبار آن باید پیوند داده شود و تأیید حداقل به دو معامله قبلی در DAG اضافه شود.

به دلیل غیرمتمرکز بودن و موازی بودن عملکرد آنها بسیار مقیاس پذیر هستند. زیرا تراکنش ها در DAG مستقل هستند. فرایندهای اعتبارسنجی به همان اندازه مستقل هستند.

تراکنش ها در یک DAG طرحی را ایجاد می کند که به عنوان Double Committed Transactions شناخته می شود. بدان معنا که تحت هر طرحی ، تراکنش فقط با دو تأیید می تواند غیرقابل برگشت باشد . واقعیتی که به لطف کار موازی شبکه ، ممکن است چند ثانیه طول بکشد.

در DAG هیچ ماینری وجود ندارد . بنابراین هیچ هزینه ای یا کمیسیون با ارزش زیاد پرداخت نمی شود. به لطف اعتبار سنجی رمزنگاری شده و عملکرد بالا ، سود کل گره از تراکنش تایید شده با کل حجم تراکنش های شرکت شده در میان سایر سرویس هایی که گره می تواند ارائه دهد ، بازیابی می شود.

معایب گراف DAG

توسعه DAGها پیچیده است . خصوصاً به دلیل الگوریتم اجماع پیچیده و محافظت های لازم برای جلوگیری از سو استفاده از موازی کاری.

DAGها به سیستم های هماهنگی نیاز دارند. این سیستم های هماهنگی به نقطه ای از خرابی تبدیل می شوند که می توانند بر عملکرد شبکه تأثیر منفی بگذارند.

بسیاری از پروژه های DAGاز ابزار رمزنگاری ایمن استفاده نمی کنند . این امر درها را برای حملات باز می کند. این مورد در ارز رمزنگاری شده معروف IOTAارائه شد. مهاجمان از این نقطه ضعف برای دستیابی به وجوه کاربران IOTA و سرقت پول آنها استفاده کردند. در مجموع ، بیش از 10 میلیون دلار به دلیل این حمله خسارت وارد شد.

استفاده از تکنیک های رمزنگاری ضعیف باعث می شود تولید آدرس ها عملاً وجود نداشته باشد ، این یک مسئله جدی حفظ حریم خصوصی است.

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 (DPoS تغییر یافته گواه اثبات سهام است که برای اعتبارسنجی بالک ها به یک گروه ازنمایندگان از طرف تمام گره های شبکه متکی است. معموال 21 تا 100 نماینده با استفاده از اجماع DPoSدر شبکهانتخاب می شوند. این روش سازمان دهی و کنترل را آسان تر کرده و امکان انتشار شرایط بالک 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 میتوانند برای جایگزینی او رأی گیری کنند از مهم ترین ویژگی های این مکانیسم می توان به مقیاس پذیری، مصرف بهینه انرژی و هزینه پایین تراکنش هااشاره کرد. ولی با وجود تمامی این مزایا، این مکانیسم نیمه متمرکز محسوب می شود. این مکانیسم در BitShares، EOSو Steemitمورد استفاده قرار گرفته است.