آموزش Polkadot برای مبتدیان

راهنمای غیر فنی برای غیر متمرکزسازی،

بلاک چین و Polkadot

Gbaci

آموزش Polkadot برای مبتدیان: راهنمای غیر فنی برای غیر متمرکزسازی، بلاک چین و Polkadot

انتشار توسط gbaci

لاگوس، نیجریه

ویرایش توسط AnaelleLTD

چاپ اول

تقدیر و تشکر

نوشتن این کتاب به لطف بلاکچین Polkadot امکان پذیر شد، مکانیزمی که به جامعه Polkadot اجازه می دهد تا پروژه ها و ایده هایی را که به پذیرش بیشتر فناوری های Polkadot کمک می کند، تامین مالی شوند.

همچنین از اعضای شورای Polkadot که وظیفه اجرا و نظارت و هدایت شبکه به سمت ثبات و رشد طولانی مدت را دارند، سپاسگزاریم. بی شک فداکاری آنها کمک بزرگی به پیشرفت و شکوفایی دو سال گذشته بلاکچین داشته است.

جا دارد تا از Emre Surmeli به خاطر راهنمایی های بسیار مفیدش در مدت زمان بررسی فنی محتوای این کتاب قدردانی کنم. همچنین Bill Laboon رئیس آموزش بنیاد وب3 نیز در ارائه این کتاب نیز نقش بسزایی داشته اند.
من به خاطر مهارت‌های ویرایش تخصصی و ریزبینانه در مورد فناوری‌های بلاک چین ، که خواندن این کتاب را بسیار آسان‌تر کرده است، به Anaelle LTD مدیون هستم.

در پایان، می‌خواهم از اعضای جامعه Polkadot که با پاسخ به توییت‌ها، نظرسنجی‌ها و فراخوان‌ها برای بررسی پیش‌نویس در نگارش این کتاب مشارکت داشته اند تشکر کنم. یک جامعه همواره به اندازه فداکاری اعضایش قوی به نظر می رسد و من از عضویت در سیستمی که مملو از افراد متعهد و مشتاق به کمک هست، بسیار خرسندم.

صفحه بندی

پیشگفتار

تا قرن پانزدهم، بازرگانی اروپا تحت سلطه ونیزی ها و جنوویس ها بود که تجارت مدیترانه نیز تحت کنترل آنها بود. این تاجران کالاهایی را از بازرگانان بندر اسکندریه در مصر می خریدند که عمدتا از هند به سراسر جهان می رفت و سپس به بازرگانان عرب فروخته و از این طریق به دریای سرخ در مصر منتقل و در قاهره فروخته می‌شدند. اینجا بود که سلطان مصر قبل از رسیدن این کالاها به بازرگانان اسکندریه، از فروشندگان مالیات سنگینی دریافت می‌کرد. از آن طرف، ونیزی‌ها و جنوویسها کالاهای گفته شده را در سرتاسر اروپا با قیمت‌های بسیار گران توزیع کردند. با این حال، همانطور که در همه سیستم های ناکارآمد، در این سیستم هم برخی به ضرر دیگران سود نیز می بردند، برخی نیز وجود داشتند که این وضعیت موجود را با تمام وجود به چالش می کشیدند.

در پایان قرن پانزدهم، پرتغالی‌ها یک مسیر مستقیم به هند را کشف کردند که به آنها اجازه می‌داد واسطه ها را کنار گذاشته و بتوانند محصولات خود را با کسری از آنچه اروپایی‌ها باید بپردازند، حمل کنند. این امر منجر به تغییرات اساسی در نحوه عملکرد دنیای قدیم شد و در عرض چند سال، نقش ونزی ها و جنوایی ها را از لیست بازیگران مرتبط با تجارت شرق حذف کرد.

فناوری بلاک چین را "کشف پرتغالی ها از مسیر مستقیم به هند" در نظر بگیرید. ایده اصلی این است که برای برهم زدن «دنیای قدیم»، زیرساخت‌های خاصی باید وجود می داشت. در مثال بالا، در سالهای اول کشف این روش و تا زمانی که بخش های پورت مانند ایمن شدند، ارتباطات برقرار شد و مواردی تامینی ایجاد نشد، البته که کار زیادی هم نمی شد در این زمینه صورت داد. اجرای این زیرساخت ضربه نهایی ای بود که ونیزی ها را نابود کرد و راه کاملاً جدیدی را برای تجارت و زیر ساخت های مربوط به آن ایجاد کرد.

امروزه زیرساخت هایی که برای راه اندازی بلاک چین و عناصر مختلف وجود دارد. صنایع مختلف شروع به همگرایی کرده اند و امور مالی مربوط به رمز ارزها بسیار مورد توجه قرار گرفته است. هنگامی که همه این بخش ها به صورت در هم تنیده ایجاد شوند ما می توانیم در مورد نوع نوآوری که به وجود می آید حدس هایی هم بزنیم. آینده ممکن است هیجان انگیز باشد و مشخص شده که پروژه‌های بلاک چین باید با پروژه‌های دیگر و همچنین با دیگر افراد خارج از دنیای رمزنگاری ارتباط برقرار کنند و تعامل داشته باشند.

همانطور که نشان داده میشود، دنیا دیگر تحت سلطه یک بلاک چین نیست. ما وارد دوران چند بخشی شدیم و این همان جایی است که Polkadot نقش اصلی را ایفا خواهد کرد، و در طول این کتاب متوجه این مسئله خواهید شد.

در امور مالی سنتی، یک نگرش مبتکرانه علیه بیت کوین و همه پیامدهای آن وجود دارد که باعث شده بسیاری (از جمله من) نتوانند مزایای فناوری بلاک چین را در مراحل اولیه آن ببینند. خوشبختانه این نگرش در حال تغییر است. امور مالی سنتی با وجود تأثیر منفی مداوم بر سیستم مالی و اقتصادی جهانی، چالش‌های زیادی دارد که هنوز نتوانسته بر آنها غلبه کند. به عنوان مثال، بانکداری در بخش مالی سنتی، سیستمی از بخش ها را اجرا می کند که با سایر فعالان بازار همسو نیست. بانکداران هم جزو این دسته هستند و بسیار کوته فکرانه عمل می کنند. به طوری که روی پاداش پایان سال متمرکز هستند و پاسخگوی اعمال خود نیستند. این تنظیمات منجر به شیوه‌های بانکی غیرقابل قبولی شده است. همانطور که جهان در طول بحران مالی بزرگ شاهد آن بود، زمانی که حس طمع باعث شد تا محصولات سرمایه‌گذاری به‌عنوان بخش های ایمن قیمت‌گذاری شوند، اما در واقع این امر باعث آن شد که همه چیز بسیار پرخطر جلوه داده شود. توصیه‌های سرمایه‌گذاری به هیچ عنوان بر اساس منافع سرمایه‌گذاران نیست، بلکه بر اساس میزان کارمزد ایجاد شده و داده‌های ذخیره‌شده در نهادهای متمرکز ارائه می‌شوند.

زمانی که مطالعه فناوری بلاک چین را شروع کردم، متوجه شدم که شبکه‌های غیرمتمرکز و «بدون مجوز» مشکلات اعتماد و امنیت را به گونه‌ای حل می‌کنند که دیگر مجبور نیستیم تنها به شرکت‌ها تکیه کنیم. من یاد گرفتم که بخش های گنجانده شده در پروتکل های بلاک چین تضمین می کند که منافع اقتصادی همسو هستند و شرکت کنندگان در این فرآیند می توانند پاسخگو باشند. کسانی که می‌خواهند از یک شبکه استفاده کنند تا پیشنهاد هایی در مورد مدیریت شبکه ارائه کنند و یا از طریق کمک به امنیت شبکه کسب درآمد کنند، باید دارای نشانه‌هایی از پروژه‌های مذکور باشند. تمامی موارد مطرح شده منجر به ایجاد یک سری رفتارهای شایسته می گردد که در صورتی نقض آن افراد سرمایه های خودشان را از دست می دهند.

مدتی طول کشید تا بیت کوین و ویژگی های منحصر به فرد آن را به عنوان عضوی جدید در دنیای پولی درک کنم و بدانم چگونه ظهور آن کاری که ما با پول انجام می دهیم را تکمیل می کند. ابتدا در دنیای کاری خودم با بلاک چین بیت کوین آشنا شدم، پروتکلی که وظیفه آن ثبت تراکنش های بیت کوین است. سپس در مورد اتریوم چیزهایی یاد گرفتم. یک بلاک چین "قابل برنامه ریزی" که پروتکل آن امکان ساخت برنامه های کاربردی و قراردادهای هوشمند را می دهد و زنجیره ای از تراکنش ها را ایجاد می کند. اتریوم را به عنوان یک تلفن هوشمند در نظر بگیرید که در آن می توانید برنامه ها را دانلود و اجرا کنید، در حالی که بلاک چین بیت کوین یک تلفن ثابت است که منحصراً برای برقراری و دریافت تماس استفاده می شود.

اتریوم جعبه پاندورایی را گشود که می‌تواند با فناوری بلاک چین کارهایی را انجام دهد. با افزایش ترافیک در بلاک چین اتریوم، معایب آن نیز ظاهر گردید. که از شناخته شده ترین آنها می توان به هزینه های گس (کارمزد ساخت) بالا در معاملات اشاره کرد. با این حال، برخی از این ایرادات مشهود نیستند. بلاک چین اتریوم ساختارش این گونه است که هر دقیقه بروزرسانی ندارد، بنابراین، زمانی که به ارتقاء نیاز باشد، اجرای آن بسیار دشوار و طولانی است. یکی دیگر از اشکالات این است که بلاک چین اتریوم برای برقراری ارتباط با زنجیره های دیگر ساخته نشده است، زیرا در طراحی اولیه آن بحث قابلیت همکاری در نظر گرفته نشده بود. همین مشکلات بود که پای Polkadot را به این دنیا باز کرد.

Polkadot بلاک چین های مستقلی به نام "Parachian" را قادر می سازد تا به آن متصل شوند و اساساً اتصال و امنیت را برای آنها مدیریت می کند. Polkadot می تواند طراحی خود را در طول زمان تغییر دهد و امکان همکاری بین زنجیره های مختلف را فراهم می کند. Polkadot کل فضای بلاک چین را بسیار توسعه پذیرتر می‌کند و اثرات شبکه را افزایش می‌دهد. اساساً مانند راه‌آهنی است که شهرها را به هم متصل می‌کند و امکان شکوفایی فعالیت‌های اقتصادی را فراهم می‌کند.

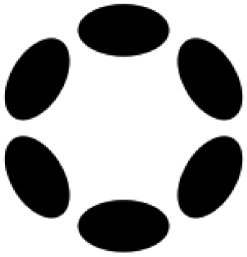
با توجه به سرعت نوآوری در فضای بلاک چین، و به دلیل این واقعیت که من خودم یک دانشمند کامپیوتر یا توسعه دهنده نیستم، تشخیص اینکه کدام پروژه های بلاک چین تفاوت ایجاد می کنند، امری دشوار است. در نمونه پرتغالی که قبلاً دیدیم، اگر در لیسبون بودید و در مورد این کشف باخبر می شدید، می توانستید روی یک کشتی سرمایه گذاری کنید و از طریق آن با واردات ادویه تجارت کنید. این امر بسیار پر ریسک بود، زیرا در آن روزها کشتی های زیادی بودند که به راحتی و با امنیت به مبدا باز نمی گشتند. سرمایه گذاری بهتری مانند یک کارخانه کشتی سازی را تصور کنید که در آن نه تنها از طریق فروش کشتی هایی که می سازید، بلکه از طریق حق امتیاز بالقوه حاصل از حمل و نقل موفقیت آمیزی که هیئت های تجاری دارند نیز سود می برید.

من در مورد Polkadot دقیقاً همین تصور را دارم. Polkadot برای برنده شدن در حراج و اجاره یک اسلات، به بلاک چین های مستقل نیاز دارد تا بتوانند به زیرساخت Polkadot متصل شده و به Parachian تبدیل شوند. این بدان معناست که پروژه‌ها می‌توانند روی موارد کاربردی خود تمرکز کنند و به Polkadot اجازه دهند تا امنیت و اتصال را حفظ کند. حامیان این Parachian ها می‌توانند DOT ها که رمز ارز بومی Polkadot است را وارد پروژه‌ها کنند و در صورت برنده شدن یک اسلات Parachian، در پروژه‌هایی که به عنوان ارز دیجیتال دارند پاداش دریافت کنند. این سیستم تضمین می‌کند که پروژه‌ها کیفیت و ارتباط با کاربران نهایی و حمایت جامعه خود را حفظ کنند تا پس از پایان اجاره نامه هایشان، به استقرار در Polkadot در بیایند. این مجموعه فوق‌العاده تضمین می‌کند که اکوسیستم Polkadot همیشه بهترین پروژه‌ها را دریافت می‌کند و در نوآوری پیشتاز باقی می‌ماند. به همین دلیل است که فکر می کنم Polkadot نقش اساسی در فضای بلاک چین ایفا خواهد کرد.

پیش از این هرگز در جهان، میلیون ها انسان فوق العاده باهوش به طور همزمان روی پروتکل های اپن سورس کار نکرده بودند، که این موضوع باعث انفجار Cambrian در استفاده از بلاک چین شده است. ما در این مسیر تازه کاریم و این لحظه فوق العاده ای می باشد. شاید پس از خواندن کتاب **gbaci**، با من موافق باشید که سرمایه گذاری در بیت کوین سرمایه گذاری در قیمت است، سرمایه گذاری در بلاک چین سرمایه گذاری در نوآوری است، و سرمایه گذاری در Polkadot سرمایه گذاری در سیستم راه آهن است که بسیاری از این نوآوری ها را به جلو خواهد برد.

ژان فیلیپ تیسوت

موسس و مدیر پورتفولیوی آروکا کاپیتال



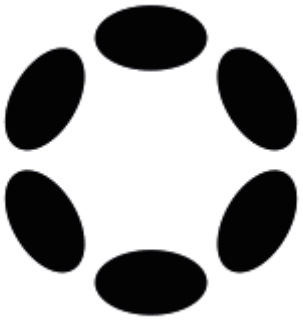
مقدمه ای مختصر

از زمان راه اندازی در 26 می 2020، Polkadot نظر طیف گسترده ای از افرادی را که دارای ارزش های یکسانی در مورد آینده سازمان انسانی هستند به خود جلب کرده است. Polkadot یک بلاک چین است که هدف اصلی آن اتصال بلاک چین های دیگر است. با توجه به اینکه تعداد کمی از مردم می دانند بلاک چین چیست، طبیعی است که تصور کنند این ایده که Polkadot بلاک چینی است که سایر بلاک چین ها را به هم متصل می کند، شبیه به یک سری موارد بدون کاربرد است. بنابراین، تلاش برای درک اینکه Polkadot چیست و چگونه کار می کند، در حال حاضر یک تلاش فکری دشوار است و یا حداقل قبلا اینگونه بوده است.

این کتاب تنها با هدف ساده سازی پیچیدگی بسیار زیاد Polkadot نوشته شده است تا خواننده معمولی بتواند این اکوسیستم را بدون هیچ دانش فنی قبلی در مورد بلاک چین یا شبکه های کامپیوتری درک کند. برای دستیابی به این امر، از بحث های تخصصی زیادی چشم پوشی شده است. بنابراین، اگرچه این کتاب برای یک خواننده معمولی ایده آل است، اما ممکن است برای یک فرد با اطلاعات فنی اینطور نباشد. با این اوصاف، هنوز چیزهای زیادی برای یادگیری در مورد Polkadot وجود دارد که در این مقوله قرار نمی‌گیرد. که از جمله می توانیم مدیریت و حکمرانی، وام‌های گروهی ، و حراج‌های Parachian را نیز نام ببریم.

امید نویسنده این است که خواننده به همان اندازه مجذوب شود که اولین بار کتاب Polkadot را خوانده است، سندی که چشم انداز جسورانه ای را برای فناوری بلاک چین و وب غیرمتمرکز (معروف به وب 3.0) ترسیم می کند و در مورد حل مشکل مقیاس پذیری (برای حداکثر پذیرش)، امنیت مشترک (برای حداکثر تنوع)، و قابلیت همکاری (برای حداکثر نوآوری و قابلیت استفاده) را نیز راه حل هایی دارد. ایده اولیه Polkadot به وضوح نشان داد که هدف آن امکان پذیر سازی انبوه از طریق مالکیت دیجیتال و آزادی برای افراد، از طریق ساخت انواع مختلف بلاک چین است که هر کدام به صنعت متفاوتی اختصاص داده شده است که نیاز به تغییرات اساسی دارد.

اما من سعی می کنم مفاهیم را جلوتر ببرم. همچنین توضیحی در مورد چیستی Polkadot و چگونگی کاری که در آینده انجام خواهد داد را نیز به شما خواهم داد. اول، ما با چرایی آن شروع می کنیم. من دریافته‌ام که ساده‌ترین راه برای درک یک فناوری جدید، درک فلسفه‌ای است که باعث ایجاد آن شده است. بنابراین، ما با فلسفه غیر متمرکز سازی شروع می کنیم.



فلسفه غیر متمرکز سازی

هدف من در این فصل توضیح علت ضرورت غیرمتمرکز سازی است. چرا ابتدا از این طریق باید کارتان را انجام دهید؟ زیرا به نظر می رسد در میان افرادی که به دنیای غیرمتمرکز فراخوانده شده اند، سوء تفاهم وجود دارد. بسیاری برای کسب سود می آیند و معتقدند که تمام این صنعت به این موضوع مربوط می شود.

البته، سازندگان زیادی در این فضا هستند که فقط روی افزایش سهام خود در زندگی متمرکز هستند و این اصلا موضوع بدی نیست. منظورم این است که هرکسی آزاد است هر کاری می خواهد انجام دهد. اما فراموش نکنیم که بیت کوین، با ارزش بالای 600 میلیارد دلار، واکنشی در برابر ظلم و ستم برخی اقتصاد دانان به نظر می رسید. Vitalik Buterin ، مبتکر اتریوم، به دلیل برخی موارد مجبور به ایجاد این رمز ارز شد. در یک حکایت معروف، او به یاد می آورد که وقتی بازی معروف World of Warcraft تمام دارایی های درون بازی او را به طور یک جانبه تصاحب کرد، او را به گریه انداخت.

هر دو مورد در رابطه با آزادی فرد بوده است. آیا پول نیز در کار بود؟ آیا سود مالی هدف نهایی بود؟ یا نه. هدف همیشه این بود که بشریت را به مکانی بهتر هدایت کنیم که آزادی فردی بیشتری نیز درون خودش دارد. اگر غیر متمرکز سازی این هدف نهایی را از دست بدهد، آنگاه از کنترل خارج خواهد شد، چیزی که بیشتر شبیه به رفتار یک مار آبی بوده است.

درس هایی از اجداد ما: ضرورت متمرکز سازی

اصطلاح متمرکز سازی و غیرمتمرکز سازی به روش های مختلف مدیریت قدرت، مالکیت و اختیار اشاره دارد. قدرت، مالکیت و اختیار مستقیماً با امنیت در ارتباط هستند زیرا:

1. کسی که مالک است مسئول امنیت چیزی است که دارد.

2. مالك بر آنچه که مالکیت دارد، قدرت و اختیار دارد.

در یک سیستم متمرکز، هر سه ویژگی (قدرت، مالکیت و اختیار) به یک مرکز - پادشاه، شورا، دولت، مدیر عامل، مدیریت و غیره سرازیر می‌شوند و از آن بخش به سایر موارد صادر می شوند. به این ترتیب، دولت یک عامل مرکزی است که امور ملی را سازماندهی می‌کند، در حالی که یک شرکت عامل مرکزی سازماندهی امور تجاری است. این شیوه متمرکز سازماندهی برای قرن‌ها به خوبی به ما خدمت کرده است، زیرا مؤثرترین روشی بود که برای گرد هم آمدن و برای ساختن تمدن‌ها داشتیم، اما همیشه اینطور نبود. متمرکز سازی در این بخش ، همانطور که ما آن را می شناسیم، با اختراع کشاورزی آغاز شد.

قبل از کشاورزی، اجداد شکارچی ما که گردآورنده ما نیز بودند، نه در یک مکان مستقر بودند و نه مالک چیزهای زیادی بودند. بنابراین آنها به طور طبیعی نیازی به نگرانی در مورد امنیت به روشی که ما در حال حاضر هستیم، نداشتند. نحوه حکومت آنها غیرمتمرکز تر بود، به طوری که قبیله ها به طور جمعی تصمیم می گرفتند که چه کاری انجام دهند و کجا بروند. اما با یافتن مزایای کشاورزی، اجداد شکارچی ما سبک زندگی عشایری خود را برای یک زندگی کم تحرک برگزیدند.

از آن به بعد، مردم زمین های کشاورزی، خانه ها و روستاهایی با مرزهای مشخص ترسیم کردند. با تامین مواد غذایی پایدارتر، انفجار جمعیت نیز رخ داد که مشکلات جدیدی را آشکار کرد.

برای هر چیزی، اجداد ما تصمیمات زیادی داشتند. باید پرسید آنها چگونه زمین را تقسیم می کردند؟ چه کسی اختلافات را حل می کرد؟ چه کسی در زمان جنگ رهبری میکرد؟ برای دفاع از خود و برای فتح چه کاری انجام می دادند؟ تصور کنید گروهی از سربازان از طرف پادشاه رقیب، برای فتح یک پادشاهی 5000 نفری می آمدند. اگر پادشاهی مورد تهاجم بر یک مدل سازماندهی غیر متمرکز تکیه می کرد، باید قبل از رسیدن به نتیجه، در مورد آن بحث و گفتگو میکردند. تا آن زمان، پادشاهی شان قطعاً توسط مهاجمان تسخیر شده بود.

بنابراین، یک حالت جدید سازماندهی لازم بود تا با رفاه و سبک زندگی جدید ما مطابقت داشته باشد. سپس رواج تمرکز به عنوان اصل سازماندهی واقعی ما آغاز شد.

متمرکز سازی تا حد زیادی به لطف تخصص امکان پذیر شد، که در آن همه اعضای قبیله دیگر نیازی به کشاورز شدن نداشتند. به لطف یک منبع غذایی پایدار، افراد می توانستند با توجه به استعدادهای خود و وظایف موجود، در زمینه های دیگر متخصص شوند. اجداد ما دریافتند که اگر برخی از افراد وظیفه رهبری داشته باشند می توان به صورت کارآمد در این زمینه عمل کرد. حالا متوجه میشوید در این موقعیت چه اتفاقی می‌افتاد. جامعه تصمیم گرفت قدرت، مالکیت و اختیار خود را به خاطر کارایی بیشتر به بخش مرکزی (شاه، شورا و غیره) واگذار کند. این تکامل توسط Thomas Hobbes در لویاتان (1651) توصیف شد. به گفته هابز، یک سازمان توانا زمانی به حیات خود می‌رسد که اعضای آن از حق خود برای زندگی بر اساس قوانین طبیعت چشم پوشی کنند (معروف به «هر کدام برای خودش») و تمام اختیارات خود را به حاکمیت (عامل مرکزی) واگذار کنند، که این امر ماحصل این فرآیند می باشد. پس باید پذیرفت که از این پس قوانین وضع شده توسط حاکم را باید رعایت کرد. این شیوه سازماندهی برای قرن ها

به خوبی به ما خدمت کرده است: این مورد به تقویت تمدن ها کمک کرده و آنها را به وضعیت فعلی خود ارتقا داده است.

افسردگی، سانسور و اعتراضات: سمت تاریک متمرکزسازی

فروپاشی بازار مسکن ایالات متحده در سال 2007، که هیچ بخشی آن را پیش بینی نمی کرد، ناشی از توهمات گسترده ایمنی در سرمایه گذاری های انتزاعی بود که به ندرت کسی آن را درک میکرد. این سیستم در حال حاضر هم مانند همان زمان پیچیده است و بحران مشابهی ممکن است دوباره اتفاق بیفتد. شاید همین فردا

— Hans Rosling, Factfulness

همانطور که همه ما میدانیم، هر چیزی یک جنبه تاریک دارد. در مورد متمرکزسازی، ما در معرض تاریک‌ترین جنبه‌های آن بوده‌ایم، هر بار با این فرض که اوضاع هرگز بدتر نمی‌شود. اما واقعیت به ما ثابت کرده است که اشتباه می کنیم.

در سال 2008، اقتصاد جهانی با اقدامات چند بانکدار در آمریکا به بحران بزرگ مالی کشیده شد. در مورد این موضوع می توانید یک لحظه فکر کنید. تمام دنیا به خاطر چند انسان که در نهایت به خاطر طمع و بی کفایتی خود دستمزدهای هنگفتی دریافت کردند، درد و رنجی را تجربه کردند.

مشکل واقعی بحران این بود که بانکداران در بازی هیچ نقش خاصی نداشتند. آن‌ها با پول دیگران بازی می‌کردند و وقتی پول را از دست دادند، عواقب خاصی برایشان نداشت، اما بقیه دنیا مجبور بودند پول بدهند. این یک شکست طراحی شده انگیزشی در دنیای مالی سنتی بود، به همین دلیل است که جنبش جدیدWEB3 یک تحول خوشایند بود. اگر پروتکل های مالی غیرمتمرکز به هر دلیلی ضرر می کردند، هیچ دولتی وجود نداشت که آنها را نجات دهد.

من شخصاً جنبه تاریک تمرکز را در جریان اعتراضات EndSARS در نیجریه تجربه کرده ام. دولت نیجریه با سوء استفاده از قدرت خود، بانک ها را مجبور به مسدود کردن حساب های افرادی کرد که به تظاهرات مسالمت آمیز کمک و تسهیل می کردند (من می توانم شهادت بدهم که این اعتراضات مسالمت آمیز بود زیرا من همه آن را دنبال کردم). بیت کوین و اتریوم یک هفته بیشتر در این جنبش دوام آوردند، درست قبل از اینکه دولت تظاهرات را به نا امیدکننده ترین شکلی که می توان تصور کرد سرکوب کند. آنها ارتش را به Lekki Tollgate در لاگوس فرستادند، جایی که سربازان به سمت معترضان تیراندازی کردند و شهروندانی را که فقط خواهان زندگی بهتر بودند، مجروح کرده و کشتند. تا امروز، با فکر کردن به این موضوع اشک در چشمانم جاری می شود. اینکه یک دولت می تواند ارتش را بر سر شهروندان بی گناه روانه کند، بالاترین سوء استفاده از قدرت متمرکز است. بخش تلخ تر ماجرا این بود که اعتراضات با وحشیگری پلیس سرکوب میشد. که این امر توسط واحد پلیس سرکوبگر به نام SARS در مقابل جوانان نیجریه ای اعمال می شد. در اینجا گزارش CNN از این فاجعه را میخوانید.
من همچنین می‌توانم فیس‌بوک، گوگل و سایر محصولات و سرویس‌های وب را که از آنها استفاده می‌کنیم به عنوان نمونه‌هایی از تمرکز اشتباه در نظر بگیرم. وب فعلی به گونه ای ساختار یافته است که در طول زمان سطح بیشتری از تمرکز را ایجاد می کند. گوگل به دلیل داده هایی که می تواند به آنها دسترسی داشته باشد، اما در واقع مالک آنها نیست، برای تبلیغ کنندگان بسیار ارزشمند است.

همین امر در مورد اینستاگرام و سایر برنامه های رسانه اجتماعی که ما استفاده می کنیم نیز صدق می کند. بدون داده های کاربر، ارزش آنها بسیار کمتر از آنچه در حال حاضر هستند خواهد بود. این شرکت‌ها در گرفتن داده‌های ما برای رشد امپراتوری‌های میلیارد دلاری بدون پرداخت یک سکه به ما که مالکان واقعی هستیم، تخصص دارند. حتی بدتر از آن، آنها می توانند ما را هر زمان که بخواهند سانسور کنند (و این کار را انجام می دهند). این واقعیتی است که ما در آن زندگی می‌کنیم و رشد کرده‌ایم و باید آن را بپذیریم. زیرا تا قبل از ظهور بیت‌کوین هیچ جایگزین واقعی نداشتیم. اما حالا به بیت کوین خواهیم رسید.

برای درک بیشتر جنبه تاریک تمرکز، ما نیاز به کشف سه گانگی - مالکیت، قدرت و اقتدار داریم. واژه مالکیت، به مالکیت یک کالا اشاره دارد. در مورد کشور، زمین متعلق به دولت است، مگر در مواردی که شهروندان این زمین ها را در تملک داشته باشند. اما حتی در این موارد، دولت ها همچنان این حق را برای خود محفوظ می دارند که

زمین های مذکور را مصادره کنند. قدرت به توانایی انجام عمل اشاره دارد. در یک کشور، قدرت در سراسر جامعه توزیع می شود و سهم بیشتری متعلق به دولت است (تقسیم به سلسله مراتب). بنابراین، رئیس جمهور قدرت بیشتری نسبت به معاون رئیس جمهور دارد، زیرا او توانایی انجام کارهای بیشتر از معاون رئیس جمهور را دارد. شهروندان هم قدرت دارند زیرا می توانند رای دهند و اعتراض کنند.

اقتدار به توانایی کنترل اشاره دارد. طبیعتاً کسی که مالکیت و قدرت دارد به طور پیش فرض اختیار نیز دارد. در فضای فعلی رسانه های اجتماعی، شما مالک هیچ چیزی نیستید، حتی حساب کاربری خودتان هم شامل این موضوع می شود. به همین دلیل است که ممکن است مسدود یا معلق شوید. شما همچنین قدرت زیادی بر هیچ چیز دیگری ندارید، جز اینکه اگر از شرایط راضی نیستید میتوانید پلتفرم را ترک کنید، و در نهایت، شما هیچ اختیاری ندارید که به شرکت بگویید چه کاری انجام دهد، مگر در موردی که تعداد زیادی از اعضای جامعه با شما موافق باشند (زیرا شرکت ها دوست دارند به خواست اکثریت اعضا عمل کنند). این وضعیت فعلی حتی در مورد حساب بانکی شما هم صادق است. بانک ها می توانند حساب های شما را به هر دلیلی مسدود کنند، به خصوص اگر دولت از آنها بخواهد.

این بدان معنا نیست که داشتن این اختیارات برای دولت یا بانک ها بد است. زیرا حقیقت این است که گاهی اوقات از این قدرت به خوبی بهره میبرند. اما اغلب از قدرت سوء استفاده می شود. این فقط ماهیت قدرت است - اگر قدرت خیلی بزرگ باشد، فساد ایجاد خواهد کرد. این یکی از مشکلات اصلی تمرکز است که این امر، انباشت قدرت زیادی را در دست چند نفر ایجاب می کند. طبیعتاً این موضوع در برخی افراد عقده‌های برتری ایجاد می‌کند و آنها را به افرادی ظالم تبدیل می‌کند (واژه «ظالم» فقط مختص سران دولت‌های سرکش نیست).

بنابراین، ضرورت کنار گذاشتن تمرکز دلایلی دارد:

1. تاریخ تا حدی ثابت کرده است که قدرت بیش از حد باعث فساد می شود.
2. متمرکز کردن، باعث ایجاد نقاط شکست میشود و غلبه بر کنترل یک سیستم را آسان می کند. یک تصویر کامل از این داستان، ماجرای Atahuallpa است.

Atahuallpa پادشاه مطلق بزرگ‌ترین و پیشرفته‌ترین ایالت در دنیای جدید بود، در حالی که Pizarro نماینده امپراتور روم مقدس چارلز پنجم بود. (همچنین به عنوان شاه چارلز اول اسپانیا شناخته می‌شود)، او پادشاه قدرتمندترین ایالت اروپا بود. پیزارو، که گروهی متشکل از 168 سرباز اسپانیایی را رهبری می‌کرد، در مناطق گمنامی حضور داشت، از ساکنان محلی بی‌اطلاع بود، با نزدیک‌ترین اسپانیایی‌ها (1000 مایل به سمت شمال در پاناما) ارتباط خوبی داشت و بسیار دورتر از آنچه دسترسی به موقع جهت اعزام نیروهای کمکی داشته باشد. آتاهوالپا در بخش مرکزی امپراتوری خود در میان میلیون‌ها رعیت بود که بلافاصله توسط ارتش 80000 سرباز خود محاصره شد. او اخیراً در جنگ با سایر سرخپوستان پیروز شده بود. با این وجود، پیزارو، آتاهوالپا را در عرض چند دقیقه پس از اینکه دو رهبر برای اولین بار با یکدیگر ملاقات کردند، دستگیر کرد. پیزارو هشت ماه زندانی خود را نگه داشت و در ازای وعده آزادی او، بزرگترین باج تاریخ را گرفت. پیزارو پس از دریافت باج که طلا بود و حجم آن برای پر کردن اتاقی به طول 22 فوت و عرض 17 فوت تا ارتفاع بیش از 8 فوت کافی بود باز هم از از قول خود سرپیچی کرد و آتاهوالپا را اعدام کرد.
دستگیری آتاهوالپا برای فتح امپراتوری Inca ها توسط اروپایی ها تعیین کننده بود.

اگرچه سلاح‌های برتر اسپانیایی‌ها در هر صورت پیروزی نهایی اسپانیا را تضمین می‌کرد، همچنان تسخیر فتح را سریع‌تر و بی‌نهایت آسان‌تر کرد. آتاهوالپا توسط اینکاها به عنوان خدای خورشید مورد احترام بود و بر رعایای خود که حتی دستوراتی را که از اسارت صادر می کرد اطاعت می کردند، قدرت مطلق داشت. ماه‌ها تا زمان مرگ به پیزارو فرصت داده شد تا احزاب کاوشگر را بدون مزاحمت به سایر بخش‌های امپراتوری اینکا بفرستد و از پاناما نیروهای کمکی بفرستد. زمانی که نبرد بین اسپانیایی ها و اینکاها سرانجام پس از اعدام آتاهوالپا آغاز شد، نیروهای اسپانیایی قدرتمندتر بودند و تجهیزات زیادی داشتند.

— Jared Diamond; Guns, Germs, and Steel

3. متمرکز سازی افراد را تشویق می کند تا قدرت و مسئولیت خود را کنار بگذارند و به ناچار منجر به تصمیم گیری ای می شود که بسیاری از افراد جامعه را به حاشیه می برد.
4. . تمرکز، عدم تقارن در مالکیت، قدرت و اقتدار ایجاد می کند و سرنوشت بسیاری را در دست عده معدودی قرار می دهد.

تنها راه حل در این زمینه چیست؟

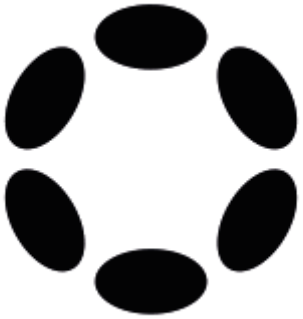
یک راه حل برای رفع مشکلات تمرکز، شیوه غیر متمرکز سازی است. شاید تنها راه حل نباشد، اما بهترین گزینه ای است که در حال حاضر داریم. غیر متمرکز سازی، در بخش درونی خود، به توزیع مجدد قدرت و اختیار از تعداد معدودی در مرکز جامعه به کل اطلاق می شود. در چنین سیستمی، یک فرد یا گروه بر سیستم حکومت نمی کند: خطرات، مسئولیت ها و پاداش ها بین همه تقسیم می شود. بنابراین، بزرگترین جذابیت غیر متمرکز سازی تعادلی است که باید در نظر بگیریم. بهتر است بدانیم که ما به دلیل اقدام جمعی خود به جای اقدامات عده ای معدود به ته دره میافتیم. بهتر است بدانیم که هیچ کس را نمی توان به دلیل صحبت در برابر بی عدالتی، ظلم، فساد، تعصب و ... ساکت کرد.

فلسفه غیر متمرکزسازی، فروپاشی ساختارهای متمرکز قدرت است. نتیجه طبیعی چنین فلسفه ای آزادی بیشتر است. اما ماهیت و نوع آزادی بستگی به این دارد که در مورد کدام سیستم غیرمتمرکز صحبت می کنیم. بیت کوین با هدف آزادی مالی ایجاد شد تا به مردم این امکان را بدهد که خود را از یک ماشین اقتصادی که عمیقاً از آن ناراضی بودند رها کنند. اتریوم می‌خواست به توسعه‌دهندگان این آزادی را ارائه دهد که اپلیکیشن‌هایی بسازند که می‌توانند دنیا را تغییر دهند و به افزایش مالی غیرمتمرکز (که از نظر بسیاری از افراد این مورد منجر به آزادی می شود نه آنچه که بانکداران انجام می‌دهند) و NFT (که به سازندگان مسیری برای آزادی هنر بر خلاف چیزی که صنعت هنر در دهه ها دیده است) ارائه کند. اینها فقط دو مورد استفاده پرچمداران اول هستند. انتظار می رود که ظرف ده سال آینده، محصولات غیرمتمرکز بیشتری وارد بازار شوند و جایگزین هایی برای سیستم های فعلی ارائه دهند.

به طور خلاصه مزایای غیر متمرکز سازی عبارتند از:

1. امنیت بیشتر، زیرا نمی توان سیستم را از بخش مرکزی مورد سرقت قرارداد. به عنوان مثال، اگر گوگل هک شود، هکر به تمام اطلاعاتی که گوگل دارد دسترسی پیدا می کند. اگر ذهن رئیس جمهور توسط عوامل تاریک (یا بیگانگان) ربوده شده باشد، ملت به حماقت تازه کشف شده او پی نمی برند، زیرا نظام، سران زیادی دارد.
2. انصاف بیشتر، زیرا افراد بیشتری در تصمیم گیری دخیل هستند. جامعه فقط در رابطه با مسائل کلیدی ای عمل می‌کند که اکثریت چنین اقدامی را تایید کنند، و این بیشتر با اصل ایده‌آل برابری همه، مطابقت دارد. اگر تنها تعداد کمی از افراد برای جامعه تصمیم بگیرند، دیری نمی‌گذرد که این عده کم تصمیماتی می‌گیرند که به نفع خودشان باشد و از جامعه سوء استفاده میکنند.
3. توزیع بهتر مالکیت، چند نفر نباید مالک همه چیز باشند، زیرا این با طراحی زندگی در تضاد است. شیر مالک جنگل نیست، حتی اگر بتواند تقریباً همه حیوانات جنگل را بکشد. اگر مالکیت به اشتراک گذاشته نشود، رشد و پیشرفت تنها به نفع عده کمی است و این وضعیت غم انگیزی است که نابرابری بیشتر را تقویت می کند.

در فصل بعد، چگونگی دستیابی به غیر متمرکز سازی را بررسی خواهیم کرد.



نحوه غیر متمرکز سازی

ما در هر ساعت هزاران سلول عصبی را از دست می دهیم، اما این مورد به دلیل ماهیت بسیار پراکنده تمام فرآیندهای ذهنی ما، عملاً هیچ تاثیری در عملکرد ما ندارد. هیچ یک از سلول های مغزی ما آنقدر مهم نیستند، هیچ نورونی در بخش مدیریت اجرایی بدن ما وجود ندارد.

— Ray Kurzweil; The Age of Spiritual Machines

با درک ضرورت، هدف و مزایای غیر متمرکز سازی، اکنون چگونگی دستیابی به اصل غیر متمرکز سازی را در عمل بررسی خواهیم کرد.

در گذشته، نسبتاً غیرممکن بود که بسیاری از انسان‌ها به‌صورت غیرمتمرکز برای رسیدن به هدفی بزرگ‌تر با یکدیگر همکاری کنند. همانطور که قبلاً توضیح داده شد، هر تلاشی در سازمان برای رسیدن به یک هدف بزرگ توسط متمرکز سازی تسهیل می شد. اما چرا اینطور است؟

خوب، بزرگ‌ترین مشکلی که ما با آن مواجه می‌شویم این است که وقتی تلاش می‌کنیم افراد زیادی با هم کار کنند باید اعتماد را در بین شان بگسترانیم. به همین دلیل است که تمرکز مدل سازمانی غالب در قرون گذشته وجود داشته است. متمرکز سازی با دادن یک قدرت مرکزی به همه اعضا، مسئله اعتماد را دور زد. بانک‌ها اینگونه کار می کنند: هدف اصلی آنها کمک به ما برای پیگیری این است که چه کسی چه چیزی دارد و چه کسی می‌تواند چه چیزی ارسال کند. تا حدودی دلیل وجود دولت ها نیز به همین است: برای کمک به ما در تعیین اینکه چه کسی می تواند و باید چه کاری انجام دهد ما باید تمامی مسائل را در نظر بگیریم. ما به بانک‌ها اعتماد می‌کنیم که پول ما را ایمن نگه دارند، به دولت‌ها برای حفظ امنیت و تسهیل رفاه و شرکت‌های رسانه‌های اجتماعی برای ارائه خدمات اعتماد داریم. بنابراین، وقتی صحبت از غیرمتمرکز سازی به میان می‌آید، این سوال پیش می‌آید: چگونه می‌توانید تا حد امکان به افراد بیشتری اعتماد کنید؟

پاسخ کوتاه در این مورد این است که شما نمی توانید چنین کاری را انجام دهید. اعتماد عبارت است از ردیابی اطلاعات به روشی امن به طوری که هیچ کس نتواند اعتبار آن را زیر سوال ببرد. راه حل متمرکز سازی واگذاری اعتماد به یک نهاد، از طریق قدرت، اختیار یا مالکیت بوده است. اما این موضوع ریسک هایی دارد:

1. متمرکزسازی عدم تقارن اطلاعاتی را ایجاد می‌کند که برخی از کنترل‌کننده‌های متمرکز با هزینه‌های بسیاری از سهامداران به نفع خود استفاده می‌کنند. به عنوان مثال، زمانی که یک تاجر قبل از دیگران از تصمیم دولت مطلع می شود، به این دلیل است که با چند سناتور دوست است و می تواند از موقعیت خود استفاده کند. بانکداران و کسب و کارها همیشه با هم تبانی می کنند، به همان شیوه ای که دولت ها و بانک ها با هم همکاری می کنند. به طور خلاصه، افرادی که در مناصب قدرت هستند، انگیزه می‌یابند که برنامه‌ریزی کنند و منافع خود را بر منافع جمعی مقدم می‌دارند.

2. جمع‌آوری و راستی‌آزمایی متمرکز اطلاعات، یک نقطه شکست را نشان می‌دهد. این مورد می تواند به روش های مختلف ظاهر شود. از یک طرف، سرورهای متمرکز (رایانه هایی که اطلاعات در آنها ذخیره می شود، سوابق بانکی، سوابق دولتی، داده های کاربر و غیره) می توانند هک شوند. از آنجایی که هکر تنها باید روی یک بخش حمله تمرکز کند، انگیزه ای برای نفوذ و سرقت داده ها نیز وجود دارد. از سوی دیگر، اگر برای این منبع اطلاعاتی اتفاقی بیفتد، برای همیشه از بین خواهد رفت.

پس چگونه بر مشکلات اعتماد خود غلبه کنیم و به غیر متمرکز سازی برسیم؟

روند کار

اول، ما باید تشخیص دهیم که مشکل واقعی در همسویی نادرست ریسک و انگیزه ها بین شرکت کنندگان است. سیستم‌های کنونی ما، از جمله دموکراسی، به افراد بدون راهکار در بازی اجازه می‌دهد تصمیماتی بگیرند که به نفع خود و آسیب به دیگران باشد. بنابراین، زمانی که بحران بانکی در سال 2008 رخ داد، به این دلیل نبود که نخبگان بانکی عمدتاً ظالم بودند. بلکه سیستم اجازه داد که سنگدلی و طمع آنها بر اقتصاد جهانی تاثیر بگذارد. با این حال، اگر اشتباهات آنها عواقب منفی برای دارایی خودشان به همراه داشت، شاید آنها قبل از ورود به بازار گندیده مسکن، اقدامات لازم را انجام می دادند. راهکار این بازی به معنای مسئولیت پذیری نسبت به اعمال خود و عواقب آن است: اگر شما به اشتباه رفتار کنید و پول خود را از دست بدهید، باید هزینه این ضرر را بپردازید. علاوه بر این، شما نباید فرصت بازی با وجوه دیگران را از طریق تصمیم‌گیری بد داشته باشید و در عین حال از کمک‌های مالی دولتی بهره ببرید. این موضوع تبعات غیرمنصفانه ای بر روی چندین حساب کاربری دیگر اعمال میکند.

بنابراین، چگونه می‌توانیم به راهکاری در بازی با مقیاس درست، دست پیدا کنیم؟ بلاک چین و تمام فناوری های مجاور آن چه نقشی ایفا خواهند کرد؟

بلاک چین چیست؟

بلاک چین یک پایگاه داده (مجموعه ای سازمان یافته از داده ها) است. اما با پایگاه‌های داده‌ای که با برنامه‌های web2 (فیس‌بوک، اینستاگرام و گوگل به آنها عادت کرده‌ایم) متفاوت است، که بیشتر آنها پایگاه‌های اطلاعاتی مجاز و متمرکز هستند که توسط یک مرجع کنترل می‌شوند.داده های موجود در بلاک چین دارای ویژگی های منحصر به فردی است که آن را از پایگاه های داده سنتی متمایز می کند که به صورت زیر بیان میشوند:

1. این داده توسط یک شبکه عمومی، غیرمتمرکز و همتا به همتا از رایانه ها میزبانی می شود.
2. با رمزنگاری و یک پروتکل اجماع، ایمنی بوجود می آید که به گونه ای طراحی شده که کنترل آن را دشوار، اما هماهنگ ماندن رایانه ها را آسان می سازد.
3. این داده دارای روندی تغییر ناپذیر است، به این معنی که نمی‌توانید رکوردهای داده موجود را بدون تایید اکثریت از گره‌های شبکه به‌روزرسانی یا حذف کنید. بنابراین، اگرچه امکان حذف و دستکاری داده ها در یک بلاک چین وجود دارد، اما تنها زمانی امکان پذیر است که اکثریت با این کار موافقت کنند.

با این ویژگی های منحصر به فرد، پایگاه داده بلاک چین برای برنامه هایی که برای معتبر بودن به اجماع اجتماعی نیاز دارند، مانند حاکمیت و ارزها، بسیار مفید واقع می شود.

راه دیگر برای در نظر گرفتن بلاک چین شبکه ای از گره ها (رایانه ها، سرورها و غیره) است که بدون ثبت و تایید داده ها توسط مرجع مرکزی کار می کنند. این داده‌ها می‌توانند هر چیزی مثل تراکنش‌ها، مانده حساب‌ها و وضعیت‌های شبکه ذخیره شده باشد که هر عضو شبکه آزادانه به آن دسترسی دارد خواهد بود.

برای ساخت این پایگاه داده غیر متمرکز به نام بلاک چین، ذینفعان مستعار مختلف باید با هم همکاری کنند. اما چگونه افرادی را که یکدیگر را نمی شناسند میتوانند بدون نظارت یک مقام مرکزی به یکدیگر اعتماد داشته باشند؟ خوب،

شما اعتماد را از این معادله خارج کنید. شاید به روشی دیگر، اعتماد را به گونه‌ای خودکار در نظر میگیرد که شرکت‌کنندگان شبکه نیازی به اعتماد به یکدیگر ندارند، بلکه به پروتکل مورد نظر اعتماد خواهند کرد.

پروتکل چیست؟

یک پروتکل صرفاً مجموعه ای از دستورالعمل ها است که یک نرم افزار کامپیوتری از طریق آنها کار می کند. HTTP یا TCP/UDP و IP را می توانید از این نوع در نظر بگیرید. *مثل ده فرمان یا کدهای حمورابی.*

یک پروتکل قوانین تعامل را برای همه شرکت کنندگان در یک شبکه تعیین می کند به طوری که افراد جدید می توانند آزادانه عضویت یا ترک شبکه را انتخاب کنند. مهمتر از همه، پروتکل را نمی توان توسط هیچ شرکت کننده یا گروهی از شرکت کنندگان تغییر داد. هر گونه به روز رسانی تنها زمانی می تواند انجام شود که اکثریت شرکت کنندگان شبکه با این تغییر موافقت کنند. توجه داشته باشید که این موضوع به طور مشخص با کشور یا شرکتی که تنظیم کننده زیر و بم این تغییرات می باشد متفاوت است.

بنابراین، بلاک چین ها به هر شرکت کننده در شبکه آزادی انتخاب جهت ترک شبکه و همچنین مسئولیت مدیریت شبکه را می دهند. مالکیت جمعی و رهبری تعیین کننده نام شبکه است. با این حال، همه بلاک چین ها از این رویکرد پیروی نمی کنند.

می توان به یک پروتکل اعتماد کرد زیرا قوانین آن از ابتدا مشخص است. به عنوان مثال در مورد بیت کوین، پروتکل بیان می کند که یک بلاک (در این مورد بیشتر در یک بیت) تنها زمانی تولید می شود که یک معمای رمزنگاری شده توسط اکثر گره ها (رایانه ها) در شبکه باشد و به تایید برسد. به عبارت ساده تر، هیچ تراکنش جدیدی به دفتر کل اضافه نخواهد شد، مگر اینکه اکثر گره ها تایید کنند که این تراکنش معتبر هستند. در هنگام ایجاد این بلاک جدید، BTC جدید به عنوان یک پاداش برای افراد در نظر گرفته میشود. به طور خلاصه، این همان پروتکل بیت کوین است.

بنابراین کارکرد بلاکچین ها چیست؟

به طور مداوم از بلاک چین به عنوان دفتر کل جهانی یاد می شود و این موضوع درستی می باشد. اما گفتن اینکه بلاک چین یک دفتر کل می باشد، گاهی اوقات می‌تواند یک مفهوم تخیلی گمراه‌کننده باشد، زیرا هیچ ساختاری به طور کلی وجود دارد که هر شخص غیر متخصص بتواند آن را بررسی کند. اصطلاح دفتر کل فقط برای تشبیه شباهت بین یک فرآیند کامپیوتری و یک فرآیند انسانی استفاده می شود. بنابراین، بلاک چین یک دفتر کل است زیرا اطلاعات را ذخیره می کند، نه به این دلیل که یک دفتر کل واقعی برای حسابداری است. با این حال، حفظ این مقایسه ها نیز عالی به نظر می رسد، زیرا به خوبی توصیف می کند که یک بلاک چین چه کارهایی انجام می دهد. از این به بعد، بر ارائه توضیح بهتر در مورد چگونگی ساخت این دفتر تمرکز خواهم کرد.

برای درک بلاک چین، باید کلمه بلاک چین را به اجزای احتمالی آن تقسیم کنیم.

Blockchain = بلاک های روی یک زنجیره

یا

Blockchain = بلاک + زنجیره

اما تعریف بلاک چیست؟

بلاک مجموعه ای از اطلاعات تایید شده است که با هم بسته بندی شده و آماده اضافه شدن به دفتر کل می باشند. یک بلاک به ندرت از یک تراکنش تنها ساخته می‌شود، اما شامل بسیاری از تراکنش‌های همراه با هم است. برای ایجاد یک بلاک، تراکنش‌های معتبری که در شبکه انجام شده‌اند (مانند ارسال نشانه‌ها، تغییر نام در یک سایت رسانه اجتماعی غیرمتمرکز، تعویض نشانه‌ها یا ارسال نظر) با استفاده از رمزنگاری جمع‌آوری و قفل می‌شوند. رمزنگاری رشته‌ای است (درست مانند زیست‌شناسی، شیمی، فیزیک و غیره) که بر ایجاد امنیت قوی با استفاده از پازل‌های

دشوار بر اساس ریاضیات قابل اثبات تمرکز دارد. هدف از مهر و موم کردن بلاک ها با استفاده از رمزنگاری، جلوگیری از ایجاد مشکل در آینده می باشد.

شما می توانید یک بلاک را به عنوان یک سطل تصور کنید. هر بلاک به عنوان یک سطل خالی شروع می شود، سپس کاربران نهایی از شبکه استفاده می کنند و سطل را با تراکنش های خود پر می کنند. وقتی سطل پر شد، مهر و موم شده و برای مراجع بعدی نگه داشته خواهد شد. اکنون، مهم است که بدانیم مهر و موم کردن بلاک تنها زمانی امکان پذیر است که بسیاری از افراد (گره ها) تاکید کنند که تراکنش های موجود در آن بلاک معتبر هستند. همانطور که در زمان تایید که هیچ کس سعی نکرده است توکن هایی را ارسال کند یا ادعای مالکیت آنها را داشته باشد یا اقدامات متقلبانه دیگری انجام دهد، پس از مهر و موم شدن، بلاک نمی تواند برای تغییر هر تراکنش باز شود، اما می توان از آن به عنوان مرجع برای تایید سوابق داده استفاده کرد.

پس چه زمان چین و یا زنجیره وارد عمل می شود؟

خب، به احتمال زیاد چندین بلاک وجود دارد. درست است؟ از آنجایی که هر بلاک فقط می تواند شامل تعداد محدودی تراکنش باشد. بنابراین، زنجیره‌ای کردن بلاک‌ها برای رمزگشایی و ردیابی توالی تراکنش‌ها ضروری می‌شود. حال باید پرسید که کدام بلاک در بخش اول خواهد بود. فرآیند زنجیره‌سازی با خود بلاک تفاوت چندانی ندارد. من فقط به طور ساده توضیحاتم را تقسیم کردم تا بتوانید درک بهتری از روند داشته باشید. در واقعیت، هر بلاک جدید زنجیره را توسعه می‌دهد و در مورد بلاک چین، اثبات کار آن را ایمن‌تر می‌کند.

اما در یک سطح عمیق تر می توانیم اینگونه بررسی کنیم که، چگونه یک بلاک چین به این سطح از امنیت غیرمتمرکز دست می یابد؟ بلاک چین های مختلف عملکرد های متفاوتی نسبت به این موضوع دارند. اما با وجود تفاوت‌های آنها، دو موضوع اصلی در تجزیه و تحلیل بلاک چین وجود دارد.

برای اینکه یک بلاک چین بتواند وظیفه اش را انجام دهد، به کامپیوترهای زیادی نیاز دارد که دائماً با یکدیگر در ارتباط باشد. به این می گویند شبکه سازی، یا به اصطلاح انسانی تر می توانیم بگوییم که این یک جور شایعه سازی می باشد. به این ترتیب داده ها در سراسر شبکه منتقل می شوند. به طور خلاصه، داده ها از یک رایانه به رایانه دیگر کپی می شوند تا زمانی که همه رایانه های موجود در شبکه این داده ها را داشته باشند. بدون شبکه، هیچ بلاک چین آنطور که ما می شناسیم وجود نخواهد داشت.

دومین مؤلفه اصلی یک بلاک چین مکانیسم اجماع آن است. به این معنی که چگونه شرکت‌کنندگان مختلف شبکه (گره‌ها، رایانه‌ها، سرورها) به این نتیجه می‌رسند که کدام داده معتبر و کدام نادرست است. مکانیزم اجماع دارای دو جنبه اصلی است:

- اجماع - فرآیند کپی و تأیید داده ها (بلوک ها) از یک گره به گره دیگر را شامل می شود.
- بخش نهایی - فرایند اضافه کردن بلوک جدید به زنجیره را شامل می شود. تفاوت بین این دو بسیار واضح تر در زیر توضیح داده خواهد شد.

به طور طبیعی، هر بلاک چین مکانیزم اجماع منحصر به فرد خود را دارد، مگر اینکه یک بلاک چین جدید با استفاده از کد (پروتکل) یک بلاک چین دیگر ایجاد شود. با این حال، تمام سیستم های اجماع مختلف را می توان به سه دسته اصلی طبقه بندی کرد.

اثبات کار (PoW)

الگوریتم اثبات کار الگوریتمی است که برای جلوگیری از هرزنامه ایمیل ایجاد شده است و اساساً بارگذاری مخرب سرورهای ایمیل را برای رایانه ها دشوار می کند. برای دستیابی به این هدف، سرور ایمیل به IP ارسال کننده یک معمای کوچک برای حل کردن می دهد که نیاز به تلاش محاسباتی دلخواه دارد. پس از اتمام، رایانه راه حلی را ارائه می کند، که اثبات کار خودش می باشد و بدنه ایمیل را هم شامل می شود. این فرآیند توسط مشتری بیت کوین پذیرفته شده و به عنوان مکانیزم اجماع مورد استفاده قرار گرفت.

با اثبات کار، کامپیوترها تنها زمانی به توافق می رسند که عملکرد در این خصوص، حل یک معمای رمزنگاری شده باشد. هرکسی که راه حلی برای معمای رمزنگاری ارائه دهد، ابتدا تولید کننده بلاک می شود و برای آن پاداش می گیرد. این روش اجماع اخیراً به دلیل عملیات انرژی بر آن مورد انتقاد قرار گرفته است. در چنین شبکه‌ای، امنیت یک سیستم تا حدودی به سختی معمای رمزنگاری مرتبط است، بنابراین نیاز به صرف انرژی بیشتری نیز دارد.

اثبات سهام (PoS)

این روش اجماع برای غلبه بر کاستی های اثبات عملکرد از نظر مصرف انرژی ابداع شد. این روش، محاسبات رایانه ای و پازل های رمزنگاری را برای منافع اقتصادی مبادله می کند، به طوری که امنیت یک سیستم به تعداد توکن هایی که در شبکه وجود دارد وابسته است. از اینجاست که کل ایده ی استکینگ (در ادامه در مورد این موضوع بیشتر توضیح داده خواهد شد) از آن سرچشمه گرفت. منطق آن به سادگی نشان می دهد که اگر یک سیستم توسط قدرت اقتصادی بزرگی پشتیبانی شود، ربودن سیستم مذکور تقریبا غیر ممکن خواهد بود، زیرا هر کسی که به دنبال انجام این کار باشد، هزینه های بیشتری را متحمل خواهد شد. به عنوان مثال، یک بلاک چین PoS که تنها 2 میلیون دلار موجودی دارد، بسیار راحت تر از یک شبکه با سهام یک میلیارد دلاری مورد سرقت قرار میگیرد.

اجماع مرکب

بیشتر بلاک چین‌های مدرن از یک اجماع مرکب استفاده می‌کنند که اثبات کار را با اثبات سهام ترکیب می‌کند و بهترین‌ها را از هر دو محیط، برای ایجاد یک شبکه امن‌تر و کارآمدتر استفاده می‌کند. با سیستم های اجماع مرکب، تفاوت جزئی بین اجماع و بخش نهایی تا حدودی آشکار می شود.

قبل از اینکه یک بلاک به زنجیره اضافه شود، باید توسط بسیاری از ماینرها (یا اعتبار دهنده) تأیید شود. این فرآیند تأیید مداوم، که شامل کپی کردن داده ها از یک گره به گره دیگر است، اجماع نامیده می شود. هنگامی که تاییدات کافی انجام شد، همانطور که توسط قوانین پروتکل مشخص شده است، بلاک مورد نظر « به شدت پشتیبانی شده» نهایی می‌شود، یعنی به بلاک چین اضافه می‌شود. با جدا کردن این دو فرآیند، توسعه دهندگان می توانند بلاک چین را از نظر سرعت، امنیت و مقیاس پذیری بهتر، بهینه کنند.

شرکت کنندگان بلاک چین چه کسانی هستند؟

گره های کامل: این افراد مسئول امنیت شبکه هستند. شما می توانید آنها را به عنوان پرسنل امنیتی در نظر بگیرید. بسته به بلاک چین، می‌توان آن‌ها را به نام‌های مختلفی نامید: که شامل استخراج‌کننده (بیت‌کوین و اتریوم)، اعتبارسنج (Polkadot، Cosmos) و غیره می شود. صرف نظر از نام آنها، هدف آنها یکسان است که شامل ایمن سازی شبکه است. آنها این کار را با ثبت و تایید تراکنش ها به صورت غیر متمرکز انجام می دهند.

سازندگان (برنامه های غیرمتمرکز و بلاک چین): سازندگان شبیه به بنیانگذاران در دنیای کنونی وب 2.0 هستند. آنها بیشتر برنامه نویسانی هستند که برنامه های غیرمتمرکز یا بلاک چین های جدیدتری را برای کار ایجاد می کنند.

گره های سبک (کاربران نهایی، کیف پول ها و مشتریان): بسیاری از افراد در این دسته برای استفاده از بلاکچین ها هرگز نیازی به دانستن نحوه کارکرد بلاک چین نخواهند داشت. در واقع، هدف نوآوری فعلی بلاک چین این است که کاربر نهایی را وادار کند تا بدون اینکه متوجه شود با بلاک چین تعامل کند. اینها افرادی هستند که از dApps و سرویس های ایجاد شده توسط سازندگان استفاده می کنند.

اگر مفهوم بلاک چین هنوز یک نگرش به نظر می رسد، پس نگران نباشید. ما اکنون تاریخچه بلاک چین ها را بررسی می کنیم و امیدواریم که زمینه بیشتری بدست آورید و در نتیجه می توانید درک بهتری نیز از کل فرآیند داشته باشید.

تکامل بلاک چین

ظهور اولین بیت کوین

در سیستم قدیم، اگر نیاز به ارسال پول برای دوستی داشتید، باید به بانک مراجعه می‌کردید و از ماموران می‌خواستید که از طرف شما پول برایش ارسال کنند. اگر در مناطق روستایی جهان زندگی می کردید، موانع شما نه تنها مالی بلکه فیزیکی نیز بود.

این به معنای چند موضوع مهم است که به ترتیب عبارتند از: شما کنترل کامل پول خود را نداشتید، و بانک آزاد بود که پول شما را قرض دهد و سود آن را بدون هیچ پاداشی برای شما، کسب کند. علاوه بر این، آنها می توانستند این پول را از طریق گمانه زنی های بی پروا از دست بدهند و هرگز پاسخگوی این کار نباشند. شاید فکر کنید این مورد درست نباشد ولی این موضوع برای مدت طولانی وجود داشت تا اینکه بیت کوین بازی را به روش های غیرمنتظره ای تغییر داد. با بیت کوین، برای اولین بار، مردم می توانند مبالغ خود را به صورت دیجیتالی برای هر کسی در هر کجای دنیا که قرار دارد ارسال کنند، بدون اینکه واسطه ای از آنها درخواست اسناد یا هزینه های بالا کند.

با بیت کوین، تنها چیزی که باید پرداخت می کردید، کمی هزینه تراکنش به پروتکل بود تا انتقال خود را انجام دهید. اگر انتقال ناموفق بود، بازپرداخت دریافت می کنید و دیگر نیازی به واسطه نیست. این شبکه می تواند رشد کند و جایگزین سیستم بانکداری سنتی شود.

سه راه برای فکر کردن به بیت کوین وجود دارد:

1. یک سیستم/پروتکل برای انتقال ارزش دیجیتال.
2. طلای دیجیتال.
3. بخش سرمایه گذاری.

از آنجایی که بیت‌کوین به یکی از دارایی ها با بالاترین عملکرد در سالهای اخیر تبدیل شده است، بیشتر مردم ترجیح می‌دهند آن را به‌عنوان یک سرمایه‌گذاری به جای «پول نقد دیجیتال»، همانطور که در ابتدا در نظر گرفته شده بود ببینند.

حال اتریوم نیز به میدان آمد

در تلاشی برای گسترش قابلیت‌های شبکه در طول سال‌ها، جامعه بیت‌کوین سعی کرد «سکه‌های رنگی» ایجاد کند که توکن‌هایی روی آن ، اطراف یا به‌عنوان یک کپی از بیت‌کوین برای نمایش دارایی‌ها و ایده‌های مختلف باشند. با این حال، پلتفرم‌ها آنطور که در نظر گرفته شده بود کار نمی‌کردند و نمی‌توانستند محدودیت‌های کد بیت‌کوین را پشت سر بگذارند.

Vitalik Buterin چند سال بیت کوین را مورد مطالعه قرار داد و به این نتیجه رسید که، "اگر این فناوری را عمومی تر کنیم چه خواهد شد؟" ویتالیک با تحریک این ایده، وایت پیپر اتریوم را در سال 2014 نوشت و چارچوبی را برای یک بلاک چین همه منظوره ایجاد کرد که توسعه دهندگان می توانستند توکن های سفارشی را بر اساس آن بسازند و طراحی کنند. برای پرداخت هزینه محاسباتی که برای اجرای کدشان لازم است، توسعه‌دهندگان باید از یک توکن بومی به نام اتر (ETH) استفاده کنند.
اساسا، اتریوم به عنوان یک ابر رایانه جهانی که بر روی یک بلاک چین به عنوان پایگاه داده آن اجرا می شود، مفهوم سازی شد. اتریوم با در نظر گرفتن ساختار اولیه یک بلاک چین، پلتفرمی ساخت که امکان انعطاف پذیری بیشتری را در موارد استفاده آن فراهم می کرد. اتریوم را به عنوان یک پلت فرم اینترنتی باز در نظر بگیرید که امکان ایجاد هر نوع وب سایت/برنامه ای را فراهم می کند، در حالی که بیت کوین یک پلتفرم اینترنت باز است که به طور کامل با یک وب سایت/برنامه واحد پر شده است.

بنابراین، از طریق ظهور اتریوم یک جزء جدید از اکوسیستم بلاک چین نیز پدید آمد: برنامه های غیرمتمرکز (dApps) نیز شامل این بخش ها بودند.

قبل از اینکه به زنجیره های متقابل برویم، مهم است که قراردادهای هوشمند را مورد بررسی قرار دهیم.

بررسی اطلاعاتی در خصوص قرارداد های هوشمند

اگرچه قراردادهای هوشمند از طریق اتریوم محبوب شدند، اما اینها در سال 1994 توسط Nick Szabo ابداع شده بودند. درست همانطور که بلاک چین ها ابزارهای مورد نیاز برای همکاری، بدون نیاز به اعتماد به یکدیگر را در اختیار شرکت‌کنندگان مختلف شبکه قرار می‌دهند، قراردادهای هوشمند نیز مکانیزمی را برای تسهیل اعتماد در بین افراد در بخش های اقتصادی فراهم می‌کنند. حال این بخش چه تفاوتی با بلاک چین دارد؟ بلاک چین مجموعه ای از قوانین می باشد که در مورد نحوه عملکرد یک شبکه مواردی را در اختیار ما قرار می دهد، در حالی که یک قرارداد هوشمند مجموعه ای از قوانین در مورد نحوه انجام تراکنش ها می باشد.

برای درک بهتر قراردادهای هوشمند، بیایید به سیاست های بیمه نگاهی بیندازیم. در تنظیم قرارداد بیمه معمولی، مدعی باید برای بیمه‌گر اثبات کند که ادعایش معتبر است و می‌تواند شواهدی ارائه کند. فرض کنید شما بیمه ماشین گرفتید و بیمه ماشین شما بدون اینکه شما مقصر باشید به پایان رسیده است. شرکت بیمه می تواند بیمه را طبق توافق پرداخت کند یا به بهانه بررسی موضوع تاخیراتی را ایجاد کند. گاهی اوقات، این بررسی ها ماه ها طول می کشد و در طی آن باید به وسایل حمل و نقل عمومی متوسل شوید. این بدان معنا نیست که تحقیقاتی لازم نیست در این بخش انجام شوند، اما برای پیشبرد هدف قراردادهای هوشمند، فرض می کنیم که شرکت بیمه نیت بدی داشته باشد. با یک قرارداد هوشمند، این مورد هیچ وقت بوجود نخواهد آمد.
قرارداد هوشمند یک برنامه می باشد که به صورت خودکار اجرا می شود که هر زمان که مجموعه ای از پارامترهای از پیش تعریف شده برآورده شود اجرا خواهد شد. بنابراین، در مثال بیمه نشان می دهیم که چگونه کارها می توانند تحت یک توافق نامه مبتنی بر قرارداد هوشمند پیش بروند. ابتدا، زمانی که خودروی شما به صورت کلی بررسی می شود، یک سنسور در خودرو این اطلاعات را به قرارداد هوشمند ارسال می کند. هنگامی که قرارداد هوشمند داده ها را تأیید کرد، شاید با نگاشت داده ها به گزارش های خبری از منطقه، به طور خودکار خسارت بیمه شما را بدون منتظر ماندن برای مجوزهای بیشتر از شرکت بیمه پرداخت نماید.

بیایید این فرآیند را برای بخش مالی اعمال کنیم. این امکان وجود دارد که به تنهایی یک پلتفرم وام دهی و استقراض غیرمتمرکز را از طریق قدرت قراردادهای هوشمند اجرا کنید. زیرا شرکت کنندگان می توانند بدون اعتماد به سایر شرکت کنندگان دیگر به قرارداد شما اعتماد کنند. بنابراین، یک ارائه‌دهنده نقدینگی یعنی کسی که پولی را برای استقراض دیگران فراهم می‌کند، انگیزه میگیرد که توکن‌های خود را برای قرض دادن به سایر کاربران سپرده‌گذاری کند، زیرا تضمین می‌شود که هر زمان که تصمیم به برداشت نقدینگی (توکن‌ها) گرفته شود، قرارداد هوشمند آن را همراه با تمام پاداش هایی که شامل شده و به فرد ارائه دهنده نقدینگی تعلق می گیرد، ارائه دهد. به همین ترتیب، وام گیرنده می تواند اعتماد کند که قرارداد هوشمند شرایط معامله (نرخ بهره و/یا جریمه) را تغییر نمی دهد و پس از بازپرداخت وام، وثیقه او به صورت خودکار به خودش بازگردانده می شود.

اکنون یک هشدار بزرگ وجود دارد. یک قرارداد هوشمند فقط به اندازه کدی که آن را ایجاد می کند ایمن است. بسیاری از هک‌هایی که منجر به از دست دادن سرمایه می‌شوند در فضای وب 3.0 به دلیل قراردادهای هوشمند معیوب انجام شده‌اند. بنابراین، قبل از معامله با یک قرارداد هوشمند، توصیه می‌شود اگر از نظر فنی آگاهی کامل دارید، کد را بررسی کنید یا به طور کلی بررسی کنید که کد قرارداد هوشمند حسابرسی شده باشد.

نکته دیگری که باید در نظر داشت این است که یک قرارداد هوشمند را می توان در صنایع مختلف و برای اهداف مختلف مورد استفاده قرار داد. تا زمانی که هدف نهایی تسهیل اعتماد بین طرفین مختلف اقتصادی از طریق اجرای بی وقفه قرارداد باشد این امر انجام خواهد شد. به عنوان مثال، یک قرارداد هوشمند بین یک تامین کننده و یک خرده فروش تنها زمانی وجه را به تامین‌کننده پرداخت می‌کند که تایید کند کالا به انبار/فروشگاه خرده‌فروش عرضه شده است.

در بلندمدت، توسعه قراردادهای هوشمند به طور فزاینده ای بر کد های دقیق (توسعه دهندگان)، اقتصاد پویا (اقتصاد دانان) و عملکردهای تابع قانون (وکلا) متکی خواهد بود. از این رو، برای توسعه قراردادهای هوشمند و هوشمندتر کردن آنها، باید رویکردی چند رشته ای در پیش بگیریم.

با بررسی این موضوع می توانیم نگاه خود را به زنجیره های متقابل معطوف کنیم.

ظهور زنجیره های متقاطع

به دنبال موفقیت چشمگیر اتریوم، جایی که موفقیت به معنای پذیرش توسط افراد بیشتر معنا پیدا می کند، بلاک چین های چند لایه-1 ایجاد شدند. اما پروتکل لایه-1 بودن به چه معنا می باشد؟ تا به حال، درک این موضوع زیاد مهم نبود، اما همانطور که به بررسی دقیق Polkadot نزدیک می شویم، مهم است که بفهمیم لایه‌ها چه چیزی را نشان می‌دهند.

بلاک چین لایه-1 شبیه کشوری با مرزهای مهر و موم شده است. در داخل این کشور، اطلاعات می تواند بین همه شرکت کنندگان بدون نیاز به اعتماد جریان یابد. شاید بپرسید چرا؟ زیرا قبلاً با قانون اساسی همه چیز در این کشور انجام می گرفته است. با معرفی قراردادهای هوشمند اتریوم، یک لایه-1 (کشور) می تواند چندین زیر پروتکل (حالت) داشته باشد که هر یک به طور یکپارچه با یکدیگر ارتباط برقرار می کنند. اما به دلیل مرزهای مهر و موم شده اش، این لایه-1 نمی تواند ارتباط مستقیمی با دنیای خارج داشته باشد.

یک تصور اشتباه رایج در میان برخی از پذیرندگان اولیه بلاک چین این است که یک بلاک چین تک لایه-1 تمام چیزی است که برای صنعت بلاک چین، برای انجام برخی فعالیت ها مورد نیاز است. این دیدگاه از صنعت اغلب توسط کسانی که رویکرد حداکثری به پذیرش بلاک چین دارند، تداوم می یابد. بنابراین، یافتن افرادی که معتقدند هر چیزی غیر از بیت کوین یک کلاهبرداری است و واقعاً غیرمتمرکز نیست، غیرمعمول می باشد. برخی دیگر اتریوم را خوب می دانند و ادعا می کنند که اتریوم به مراتب بهتر از بیت کوین است و سایر بلاک چین ها نیز مازاد خواهند بود. اکثر افراد در این زمینه اطلاعات نادرست دارند یا صرفاً به دنبال کسب درآمد از هر توکنی هستند که در اختیارشان می باشد.

حقیقت این است که صنعت بلاک چین برای آینده‌ای چند زنجیره‌ای آماده است و هر بلاک چین جدید بخش جدیدی را به ارمغان می‌آورد که می‌تواند توسط بلاک‌چین‌های موجود مورد استفاده قرار گیرد. بنابراین، اگر یک بلاک چین بر غیر متمرکز کردن امور مالی و دیگری برعدم تمرکز هویت ، متمرکز باشند، در حین کار با یکدیگر نسبت به یک بلاک چین همه منظوره موثرتر عمل خواهند کرد. توضیح این جزئیات مفهومی مستلزم درک توضیحات فنی است. بنابراین فعلا از آن صرف نظر می کنیم. نکته این است که چیزی به عنوان حکومت یک بلاک چین بر بقیه وجود ندارد، مثلا در این مورد به معنای وجود یک شرکت آنلاین است که بر اینترنت حاکمیت دارد.

اگر واقعیت جهان چند زنجیره‌ای است و لایه‌های-۱ کشورهای عایق شده را داراست، چگونه این کشورهای دارای مرزهای بسته باید به هم اتصال یابند؟ راه حل هایی برای این مشکل وجود دارد.

اولین مورد که توسط Cosmos بررسی میشود این است که به هر لایه-1، ساختار شبکه یکسانی بدهیم، به طوری که تبادل اطلاعات بین زنجیره‌ها از طریق یک پل تخصصی آسان‌تر شود. در این مورد، پل در لغت به معنای دروازه ورود به کشور دیگر است. این رویکرد قطعا مشکل اتصال زنجیره‌ها را حل می‌کند، اما حتی در مقایسه با اتریوم، جز بهینه‌ترین راه‌اندازی ها نمی باشد.

در اتریوم، قراردادهای هوشمند می توانند به دو روش متمایز با یکدیگر تعامل داشته باشند:

1. ارسال و دریافت توکن - قراردادهای هوشمند می توانند توکن ها را بدون هیچ گونه تأیید رسمی مبادله کنند.
2. صدور دستور العملی که نشان می دهد یک قرارداد هوشمند می تواند از یک قرارداد هوشمند دیگر بخواهد تا یک معامله را انجام دهد. این جادوی واقعی ترکیبی است که به موجب آن قراردادهای هوشمند مختلف انجام می‌شوند.

این بخش می تواند در یک تراکنش یا برنامه استفاده شود و بدون دخالت انسان ارتباطاتی را ایجاد کند.

در پروتکل ارتباطی بین زنجیره‌ای Cosmos، تنها اطلاعاتی که می‌توان انتقال داده توکن‌ها هستند. بنابراین، بلاک چین ها نمی توانند به یکدیگر دستور دهند تا اقدامات خاصی را انجام دهند. به این ترتیب، می توانید این سطح از ارتباط را تا حدودی ابتدایی (ترکیب پذیری در سطح پایین) در نظر بگیرید. برای رسیدن به سطح بالاتری از ترکیب پذیری، مشابه آنچه قراردادهای هوشمند از آن بهره می برند، لایه پایین تری لازم است که در این بخش Polkadot بهترین تاثیر را دارد.

Polkadot یک پروتکل لایه-0 است که به دنبال اتصال چندین بلاک چین لایه-1 بدون شکستن قابلیت ترکیب پذیری در سطح بالا است. در این راه‌اندازی، بلاک‌چین‌ها می‌توانند برای ارسال توکن‌ها و تغییر وضعیت یکدیگر با هم ارتباط برقرار کنند.

Polkadot به توابع منحصر به فرد انتقال حالت لایه-1 احترام گذاشته و نیازی به رعایت تابع تغییر حالت زنجیره رله ندارد. این فقط به اثبات اعتبار تغییر حالتی احتمالی یک لایه-1 نیازدارد. به عبارت دیگر، Polkadot لایه-0 (سیاره) قوانین هر لایه-1 (کشوری) که به آن متصل می شود را در نظر می گیرد. تنها چیزی که نیاز دارد اثبات معتبر بودن این قوانین یا تغییرات آن است. این ساختاری است که به Parachian ها این آزادی را می‌دهد تا مکانیسم‌های اجماع و نهایی خود را توسعه دهند.

حال «تغییر حالت» واقعاً در این بخش به چه معناست؟ بیایید به یک مثال نگاه کنیم. یک بلاک چین لایه-1 متمرکز بر غیر متمرکز کردن امور مالی، می تواند با درخواست اطلاعات کاربر ذخیره شده در زنجیره هویت، وضعیت لایه-1 دیگری را که بر متمرکزسازی هویت متمرکز شده، تغییر دهد. این وضعیت تغییر می کند، زیرا زنجیره هویت برای انجام این درخواست نیاز به انجام یک تراکنش جدید دارد. اگر چه هیچ نشانه ای مبادله نمی شود، اما ارزش بیشتری ارائه شده است، زیرا اطلاعات ارائه شده توسط زنجیره هویت به طور بالقوه می تواند توسط زنجیره مالی برای پرداخت به کاربر استفاده شود. این تنها یک مثال از بسیاری از مواردی است که هسته اصلی، دارای اختلال ایجاد شده توسط فناوری‌های بلاک چین است.

اما قبل از اینکه به ماهیت مخرب بلاک چین بپردازم، اجازه دهید به یک لایه دیگر در دنیای چند زنجیره ای خود بپردازیم: لایه-2. بلاک چین های لایه-2 برای مقیاس بندی بلاک چین های لایه-1 ایجاد شده اند، یعنی افزایش سرعت یا افزایش ظرفیت بلاک چین های مذکور را شامل می شوند. به عنوان مثال، اتریوم حداقل دارای سه پروتکل لایه-2 است که به مقیاس آن کمک می کنند و شامل آربیتروم و پالیگان و آپتیمیسم است. مکانیزمی که از طریق آن، این امکان فراهم می شود، به درک اولیه شما از بلاک چین مربوط نیست. آنچه مهم است این است که بدانید لایه-2 روی لایه-1 کار کرد خاصی دارد.

یک اشتباه کوچک در مورد توکن ها

چرا توکن ها برای بلاک چین ضروری هستند و چند نوع از آنها وجود دارد؟

برای شروع، همه پروژه های بلاک چین به توکن نیاز ندارند. بیشتر بلاک چین‌های خصوصی متعلق به کسب‌وکارها و شرکت‌ها توکن ندارند و به خوبی کار می‌کنند. گفتنی است، توکن‌ها برای بلاک چین‌های عمومی ضروری هستند، زیرا از آنها برای شروع تراکنش‌ها و پرداخت هزینه‌های تراکنش در زنجیره استفاده می‌شود. در غیر این صورت، زنجیره با تراکنش های هرزنامه متوقف می شود. به این دلایل، برای استفاده از بلاک چین بیت کوین به بیت کوین، برای استفاده از اتریوم به اتریوم و برای استفاده از شبکه Polkadot به DOT، پرداخت هایی انجام می دهید. برای شبکه‌های اثبات سهام، توکن‌ها نیز برای اهداف امنیتی مورد نیاز هستند که در فصل 3 در این مورد بیشتر توضیح داده شده است.

توجه به این نکته مهم است که همه توکن ها توکن های کاربردی نیستند (یعنی توکن هایی که برای تراکنش های مرتبط با شبکه استفاده می شوند). برخی از توکن‌ها، توکن‌های حاکمیتی هستند که فقط به کاربر این امکان را می‌دهند تا در مورد تصمیماتی که بر آینده پروژه تأثیر می‌گذارد رأی دهد. اکثر dApp های میزبانی شده روی لایه- 1 توکن های حاکمیتی صادر می کنند که هیچ کاربردی ندارند، با این حال برخی از نشانه های حاکمیتی را می توان برای به دست آوردن سود سهام استفاده کرد، اگرچه مکانیسم های دقیق از پروژه ای به پروژه دیگر متفاوت است.

تمام توکن‌های ذکر شده در بالا، توکن‌های قابل تعویض هستند. گروهی از اقلام زمانی قابل تعویض هستند که هر مورد در این گروه با دیگری یکسان باشد، به طوری که هیچ عضوی دارای انحصار نباشد. این بدان معنی است که آنها همیشه می توانند بدون هیچ گونه اصطحکاک با یکدیگر مبادله شوند. اما همه توکن ها در فناوری بلاک چین قابل تعویض نیستند. فقط برخی غیر قابل تعویض هستند.

اگر تعویض پذیری کیفیت را بالا ببرد پس روندی مشابه را در پی دارد، پس غیرقابل تغییر بودن توانایی، داشتن هویت و منحصر به فرد بودن را نشان می دهد. این تمام چیزی است که در مورد آن وجود دارد. بنابراین، یک توکن غیرقابل تعویض (NFT) تا زمانی که یک آیتم/شیء واحد هنگام اضافه شدن به بلاک چین، ضرب (ایجاد) شده باشد، یک توکن منحصر به فرد است. بنابراین وقتی امروز درباره مجموعه‌های NFT می‌شنوید، معمولاً به این معنی است که آنها گروهی از توکن‌ها و قطعه‌های منحصربه‌فرد هستند.

حال که این مسائل حل شد بیایید ماهیت مخرب بلاک چین را بررسی کنیم

بلاک چین و وب 3.0: ماهیت از هم گسیخته وب 2.0

مانند بسیاری از فناوری‌هایی که قبل از آن‌ها عرضه شده‌اند، بلاک‌چین‌ها می‌خواهند وضعیت موجود را به چالش بکشند. برخلاف فناوری‌های قبلی که به‌صورت مخفیانه اختلال ایجاد می‌کردند، بلاک‌چین‌ها عمداً و آشکارا به صورت انقلابی عمل می کنند و به دنبال تغییر درک ما از اعتماد و خودکارسازی آن هستند. حال می توانید از خود بپرسید که کدام صنعت انسان محور نیاز به اعتماد ندارد؟ هر جا دلالی هست، بحث اعتماد است. بنابراین، بسیاری از زمینه ها برای ایجاد اختلال از طریق استفاده از بلاک چین آماده هستند. در زیر برخی از صنایع که در حال حاضر توسط بلاک چین در حال تغییر شکل هستند، آورده شده است:

- بخش مالی
- حاکمیت
- دارایی
- هویت
- داده
- زنجیره تامین

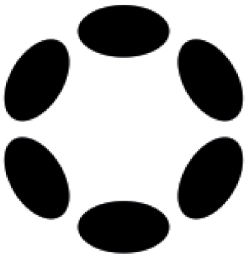
هسته اصلی این اختلال، تفاوت در بحث اخلاقی بین دنیای دیجیتال موجود و دنیای دیجیتال جدید، و بین وب 2.0 و وب 3.0 است. ابتدا Web 1.0 وجود داشت، مرحله ای از اینترنت که در طی آن کاربران نهایی فقط می توانستند داده ها را بخوانند. ایمیل‌ها، خبرنامه‌ها، وب‌سایت‌های ثابت و غیره نیز بر این امر غالب بودند.

سپس وب 2.0 به بازار آمد، مرحله ای که در طی آن کاربران نهایی می توانستند داده ها را بخوانند و بنویسند. وب 2.0 با بزرگ کردن شبکه های اجتماعی، به ما اجازه داد تا بیشتر به هم متصل شویم و چیزهای خوبی را در جهان به وجود آورد. با این حال، بسیاری از استثمار های ناخواسته اجازه یافتند که بیداد کنند تا اینکه به هیولایی تبدیل شدند که نابرابری و سوء استفاده بیشتری از کاربران نهایی بوجود آوردند. با انتقال داده ها، سانسور کاربر، و بهره برداری از داده های کاربر نیز همه چیز مشخص شده بود.

وب 3.0 از کاستی های وب 2.0 متولد شد و مرحله ای را به ارمغان آورده است که کاربران نهایی می توانند داده ها را بخوانند، بنویسند و داشته باشند. با مالکیت دیجیتال، یک پارادایم کاملاً جدید به وجود می آید که چند دهه طول می کشد تا خود را به طور کامل تعریف کند. در حالت ایده آل، تجربه کاربری Web 2.0 و Web 3.0 برای کاربر نهایی بسیار مشابه باقی خواهد ماند، در حالی که سازندگان و بنیانگذاران پروژه باید برای رسیدن به روندهای جدید فعالیت هایی را انجام دهند. برای کاربر نهایی، چالش واقعی درک ایده‌آل‌هایی است که زیربنای یک بخش اصلی است، و همچنین مزایا و معایب نگهداری از دارایی‌های دیجیتال را دارد که بعد در موردش بحث می کنیم.

آنچه مهم است که به آن توجه شود، مقیاس اختلالی است که ممکن است وجود داشته باشد . از نظر تئوری، هر شرکت وب 2.0 که فکرش را بکنید می تواند از دیدگاه وب 3.0 سازماندهی مجدد شود. به یاد داشته باشید که تفاوت اصلی بین وب 2.0 و وب 3.0 مالکیت و آزادی واقعی است. از خود بپرسید که آیا صنعتی وجود دارد که نتوان آن را تغییر شکل داد تا انصاف و شمول بیشتری را ترویج کند؟ تقریباً غیر ممکن است که بتوانید چیزی را پیدا کنید که همانطوری که هست بهینه شده باشد، و به همین دلیل است که سرعت اختلال بلاک چین همین طور ادامه می یابد. در حال حاضر، این حرکت رو به جلو از نظر دامنه محدود است زیرا هر بلاک چین شبیه یک جزیره عمل می کند.

خوشبختانه، Polkadot راهی برای حداکثر اختلال ارائه می دهد و بقیه این کتاب به توضیح چیستی آن و چگونگی برنامه ریزی برای رسیدن به هدف نهایی اختصاص دارد.



فصل 1

در بخش دات

درک Polkadot در نگاه اول می تواند دشوار باشد. برخی از آنها به دلیل مفهوم ناآشنای بلاک چین، بدون قراردادهای هوشمند که زنجیره‌های یک بلاک دیگر را به هم متصل کند، فوراً به تعویق می‌افتند. معدود مواردی که پیچیدگی اولیه را پشت سر می‌گذارند، باید با لایه‌های دیگر پیچیدگی مقابله کنند: مدیریت زنجیره‌ای، ارتقاء و دیگر موارد مثل Parachian، وام‌های جمعی، مزایده‌ها، پیام‌های زنجیره‌ای متقابل و سایر مواردی که در این امر وجود دارد. برخی مصمم هستند که از این نقطه عبور کنند، با کمک ویدیوهای GavinWood که طراحی اکوسیستم را در یوتیوب توضیح می دهد، کاغذ سفید (وایت پیپر)، ویکی Polkadot و سایر منابع مفید این اتفاق میافتد. چیزی که همه ما در پایان این سفر پیچیده می یابیم، این است که Polkadot بسیار بیشتر از یک بلاک چین ساده است.

هر شبکه بلاک چین ذاتاً به دنبال امنیت است، اما این اصلاً کار آسانی نیست. از آنجایی که امنیت هم به امنیت شبکه و هم به امنیت اقتصادی اشاره دارد، انتظار می رود که:

- بلاک چین به شدت غیرمتمرکز باشد و بردارهای حمله کم ارزش یا بدون ارزش زیاد داشته باشد (مانند رایانه های مرکزی که اطلاعات حساس را ذخیره می کنند). این به معنای واداشتن بسیاری از ماینرها برای تایید تراکنش ها در شبکه است. اگر تعداد آنها خیلی کم باشد، ممکن است تبانی کرده و به شبکه آسیب برساند.
- بلاک چین دارای ارزش کافی در بازار به اندازه ای است که حمله به شبکه را از نظر اقتصادی دشوار می کند. به عنوان مثال، اگر یک بلاک چین دارای ارزش بازار (قیمت هر توکن ضربدر تعداد کل توکن‌های در گردش) 15 میلیون دلار باشد، هر کسی که توانایی پرداخت 15 میلیون دلار را داشته باشد می‌تواند کنترل شبکه را در دست بگیرد. همچنین، اگر یک نفر دارای تعداد زیادی توکن باشد، می‌تواند با فروش همه توکن‌های خود به یکباره قیمت آن را کاهش دهد و سپس در صورت ارزان بودن آنها را دوباره بخرد. این باعث دستکاری سرمایه بازار شبکه می شود. در یک شبکه PoS که در آن ارزش کل توکن های موجود در شبکه برابر با هزینه حمله به آن شبکه است، چنین دستکاری ممکن است دشوار باشد. این به این دلیل است که اگرچه ممکن است 15 میلیون دلار داشته باشید، اما به احتمال زیاد یافتن افراد کافی برای فروش توکن های 15 میلیون دلاری شما بسیار دشوار خواهد بود.

به طور خلاصه، راه اندازی یک بلاک چین جدید آسان نیست. چگونه می‌توانیم انواع بلاک چین را اجرا کنیم و همچنان از همان سطح امنیت در سراسر جهان برخوردار باشیم؟ این اولین مشکلی است که Polkadot قصد حل آن را دارد. با ایجاد یک محیط چند زنجیره ای ناهمسان که سایر بلاک چین ها می توانند به آن متصل شوند و در نتیجه از امنیت موجود در آن بهره مند شوند. به عبارت دیگر، Polkadot منظومه ای را ایجاد می کند که در آن تمام سیارات (بلاک چین ها) از انرژی (امنیت) خورشید (زنجیره رله Polkadot) بهره می برند.

مشکل دوم مربوط به قابلیت همکاری است. همانطور که در فصل 0.5 توضیح دادم، DeFi (مالی غیرمتمرکز) به طور تصاعدی رشد کرد (50 میلیارد دلار ارزش کل در کمتر از 15 ماه قفل شد) زیرا اتریوم تعاملات یکپارچه بین قراردادهای هوشمند را فعال کرد که منجر به موارد استفاده از چرخه بازار گاوی شد. حال به این موضوع فکر کنید که هر قرارداد هوشمند خانه ای است که برای تمام خدمه خانه های دیگر در کشور (بلاک چین) قابل دسترسی است. بنابراین، اگر نانوایی نیاز به کره داشته باشد، خدمتکار او می تواند بدون اجازه به خانه آشپز وارد شود و کره را بردارد. در دنیای واقعی، این را می‌توان دزدی نامید. اما از آنجایی که خانه خود یک وسیله هوشمند و متصل است، می داند که کره توسط خدمتکار نانوا به امانت گرفته می شود و در نهایت بازگردانده می شود. این یک تصویر بسیار ساده از آنچه اتفاق می‌افتد است، که فرآیندهای اساسی را توضیح می‌دهد.

کارها و افراد با هم نقش بهتری دارند و شبکه های بلاک چین نیز از این قاعده مستثنی نیستند. اگر هر بلاک چین را به عنوان یک ارائه دهنده خدمات اینترنتی در نظر بگیرید، درک اینکه چرا یک بلاک چین ممکن است بخواهد با هویت دیگری با محتوا، و دیگران با امور بانکی، بازی، حریم خصوصی و غیره سروکار داشته باشد، آسان‌تر می‌شود. امکانات بی‌پایان می‌شوند، مانند وب 1.0. با توجه به پتانسیل بلاک چین ها، استفاده نکردن از فرصت برای ایجاد تعاملات غنی تر بین بلاک چین های تخصصی مختلف، غیرمسئولانه است و در اینجاست Polkadot که وارد عمل می شود. مشابه نحوه اتصال TCP/IP به گره های مختلف برای ایجاد اینترنت، Polkadot نیز اتصال شبکه های بلاک چین را شامل می شود، در واقع تبدیل شدن به شبکه ای از شبکه های بلاک چین.

پس Polkadot چیست؟

Polkadot در هسته خود، یک بلاک چین لایه-0 اثبات سهام است، که سایر بلاک چین ها را به هم متصل می کند. هدف Polkadot بهینه سازی **مقیاس پذیری**، **قابلیت همکاری** و **امنیت مشترک** برای تمام شبکه های متصل به خود است.

ما هر ویژگی را به نوبه خود در نظر خواهیم گرفت، تا توضیح دهیم که مشکلات اصلی چیست و چگونه Polkadot آنها را با طراحی حل می کند.

امنیت مشترک به چه معناست

Polkadot برای پرداختن به موضوع چندین زنجیره ایزوله و با سطوح امنیت جدا، چارچوبی را ارائه می دهد که در آن زنجیره های مختلف می توانند عملیات امنیتی را به اشتراک بگذارند. این زنجیره‌ها به جای تکیه بر هر بلاک چین لایه-1 برای ارائه مجموعه اعتبار دهنده های خود، برای ایمن کردن شبکه و توکنی با ارزش بازار کافی و بزرگ، می‌توانند امنیت Polkadot، پروتکل لایه-0 را تقویت کنند. در عمل، اگر Polkadot دارای ارزش بازار ۱۰ میلیارد دلاری باشد، هر بلاک چین لایه-۱ جدیدی که در Polkadot مستقر می‌شود، با همین ۱۰ میلیارد دلار از نظر اقتصادی تامین می‌شود. علاوه بر امنیت اقتصادی، این زنجیره همچنین امنیت شبکه را از مجموعه بزرگ اعتباردهنده های Polkadot به دست خواهد آورد. این اولین مورد در فناوری بلاک چین است که در نوع خود شاهکاری بوده که قبلاً دیده نشده است.

قابلیت همکاری

این نکته برجسته پروتکل لایه-0 Polkadot است. ما قبلاً دیده بودیم که dApp ها وقتی آزادانه با یکدیگر ارتباط برقرار می کنند چه کاری میتوانند انجام دهند، اکنون در مورد اینکه وقتی بلاک چین های مختلف به طور موثر یکدیگر را در عملیات روزانه خود ادغام کنند چه اتفاقی می افتد، صحبت می کنیم. شاید تصور کردن در این مقطع

زمانی سخت باشد، اما مطمئناً زمانی که به فصل 5 و Parachains برسیم، آسان تر خواهد شد. در حال حاضر، فقط به یاد داشته باشید که بخش بزرگی از طراحی Polkadot در مورد اطمینان از قابلیت همکاری بین بلاک چین های لایه-1 ناهمگون است.

مقیاس پذیری

اگر بلاک چین ها در سطح جهانی مقیاس نشوند، هرگز نمی توانند انصاف و شمول بیشتری را به ارمغان بیاورند. راه حل Polkadot برای این موضوع استفاده از "sharding" است که به شبکه اجازه می دهد تا تراکنش های مختلف را به صورت موازی اجرا کند. به عنوان مثال، اتریوم، همانطور که در سال 2021 وجود داشت، یک شبکه تک-شارد است که در آن تراکنش‌ها یکی پس از دیگری پردازش می‌شوند و هر گره باید داده‌های کل بلاک چین را ذخیره کند. در یک شبکه تک شارد، همه تراکنش ها، اگرچه ماهیت بسیار متفاوتی دارند، اما در یک شارد انجام خواهند شد. در حالی که در یک شبکه چند شارد، تراکنش‌ها به صورت موازی و در داخل خرده‌های مربوطه خود اجرا می‌شوند. در این مورد، هر خرده (شارد) مربوط به یک بلاک چین متفاوت است، به طوری که تراکنش های DeFi بر روی خرده DeFi انجام می شود، در حالی که تراکنش های NFT بر روی خرده NFT انجام می شود. باز هم، این یک توصیف بیش از حد ساده از آنچه اتفاق می‌افتد است، اما باید به شما در درک فرآیندهای مقیاس‌پذیری کمک کند.

در Polkadot، هر زنجیره لایه-1 می‌تواند شبکه خود را برای موارد استفاده مختلف سفارشی کند، بنابراین مشکل مقیاس‌پذیری را در یک زمینه باز با محاسبات موازی کارآمد (که در آن شبکه در حال پردازش انواع مختلف تراکنش‌ها بر روی گره‌های مختلف است) حل می‌کند. به این ترتیب، یک زنجیره لایه-1 متمرکز بر عدم تمرکز هویت، به طراحی سیستم مشابهی که بر متمرکز سازی مالی متمرکز است، نیاز نخواهد داشت. بنابر این، شبکه با استفاده از موارد زیر مقیاس پذیرتر می شود:

1. اطمینان از اینکه هر شبکه (Parachian) برای موارد استفاده خود بهینه شده است.
2. اجرای تراکنش های مختلف به صورت موازی انجام می شود.

برای مثال، فرض کنید 1000 گره دارید که اعتبار تراکنش ها را در شبکه شما تأیید می کند. در یک مدل تک شارد، همه 1000 گره تراکنش های یکسانی را پردازش می کنند. در مدل 4 شارد، گره ها به چهار گروه 250 تایی تقسیم می شوند. سپس هر گروه از گره ها انواع مختلفی از تراکنش ها را پردازش می کنند. گروه A تراکنش ها را از زنجیره هویت پردازش می کند، در حالی که گروه B تراکنش ها را از زنجیره مالی، گروه C از زنجیره حاکمیت و گروه D زنجیره داده را پردازش می کند. به این ترتیب، ما هنوز 1000 رایانه داریم، اما به دلیل نحوه چیدمان آنها، کارهای بسیار بیشتری انجام می دهیم.

قابلیت ارتقا فورکلس (Forkless)

دروغ گفتم. قابلیت همکاری زنجیره ای، نقطه برجسته طراحی Polkadot است. اما تنها مورد نیز نیست.

مشکل بین اتریوم و اتریوم کلاسیک را به خاطر دارید؟ یا شکاف بین بیت کوین و بیت کوین کش؟ آنها به این دلیل اتفاق افتادند که زنجیره اصلی و متعارف باید پروتکل های اصلی خود را از طریق هارد فورک ارتقا دهد. فورک، همانطور که از نامش پیداست، مسیر متفاوتی را به ذینفعان در یک مقطع زمانی خاص ارائه می دهد. فورک ها ممکن است یک ویژگی مطلوب در یک شبکه به نظر برسند، اما برای لحظه ای کشوری را در نظر بگیرید که هر بار که شهروندانش در مورد نتیجه رای گیری بحث بزرگی دارند، تجزیه می شود. این کشور با خروج بیشتر مردم، کوچکتر می شود و هر بار بخشی از سرمایه انسانی اصلی خود را از دست می دهد. البته، با توجه به اینکه بلاک چین ها مشابه کشورهای ملی دیجیتال هستند، فورک ها برای رشد بلندمدت ایده آل نیستند. برای رونق طولانی مدت شبکه، ضروری است که جامعه راهی برای حل اختلافات و ارتقاء پروتکل ها بدون اینکه خود را در معرض خطر قرار دهد، بیابد. بنابراین، Polkadot امکان به روزرسانی های فرکلس را فراهم می‌کند، و نحوه انجام این کار را در فصل 4 توضیح خواهیم داد.

در حال حاضر کافی است مروری بر برخی از ویژگی های کلیدی، که Polkadot را خاص می کند داشته باشیم، زیرا در فصل بعدی به بررسی طراحی فنی Polkadot خواهیم پرداخت. قبل از آن، اجازه دهید کمی در مورد علت هرج و مرج اکوسیستم Polkadot صحبت کنیم.

یادداشتی کوتاه در مورد Kusama - عامل هرج و مرج

اگرچه این کتاب به طور انحصاری از Polkadot بدون اشاره به کوساما صحبت می کند، مهم است که بدانیم این دو بلاک چین، هم از نظر فناوری و هم از نظر مفهومی، عمیقاً به هم مرتبط هستند. Kusama اغلب به عنوان یک شبکه آزمایشی زنده برای Polkadot در نظر گرفته می شود، اما اینطور نیست. کوساما یک زنجیره رله مستقل و تمام عیار با برنامه‌های حراج، نامزدهای Parachian، حاکمیت و جوامع خاص خود است. کوساما پیشتاز پیشرفت ها در اکوسیستم Polkadot است: به این ترتیب که هر قابلیتی که در Polkadot مستقر شده است، در درجه اول در کوساما مستقر می‌شود. کوساما نسخه بیرحمی از Polkadot است که اساساً برای محافظت از Polkadot در مقابل تجربه اختلالات غیرمنتظره و رفتارهای واقعی بوجود آمده است.

بنابراین، تفاوت‌های اصلی بین Polkadot و Kusama به سرعت پیاده‌سازی و توکِنومیک باز می گردد، زیرا سیستم حاکمیت کوساما چهار برابر سریع تر از Polkadot اجرا می‌شود، و همچنین منبع پیدایش KSM صد برابر کوچک تر از DOT است. به همین دلیل، شعار کوساما - که جامعه به سرعت آن را پذیرفته است - "منتظر هرج و مرج باشید" است، زیرا نمی توان گفت در دنیای خشن و تجربی کوساما چه اتفاقی خواهد افتاد.

در حالی که این کتاب به صراحت به نام کوساما اشاره نمی کند، باید درک کرد که هر ذکر Polkadot به طور پیش فرض شامل کوساما نیز می شود. تصمیم به تمرکز محتوای این کتاب بر روی Polkadot عمدتاً برای جلوگیری از تحمیل اطلاعات بیش از حد به خواننده بوده اما اگر بخواهید در یک کلمه به هر دو اکوسیستم Polkadot و کوساما اشاره کنید، دانستن اصطلاح DotSama کفایت می کند.

فصل 2

شبکه

Polkadot اغلب به دلیل پیچیده بودن مورد انتقاد قرار می گیرد و این اکثراً درست است. گفته می شود، این پیچیدگی بر اساس یک معماری فنی ساده ساخته شده است که تنها از دو بخش اصلی تشکیل شده است که زنجیره رله و Parachian را شامل می شود. زنجیره رله، هاب مرکزی است که همه Parachian ها به آن متصل می شوند. این فصل کوتاه تنها بر روی زنجیره رله تمرکز خواهد کرد. Parachian در فصل 5 به طور کامل پوشش داده خواهد شد.

تصویر: زنجیره رله Polkadot

زنجیر رله

برای مجسم سازی هدف پیدایش زنجیره رله، یک لوله دایره ای را تصور کنید که بسیاری از لوله های دیگر به آن متصل می شوند. این لوله های اتصال می توانند به هر شکلی باشند و هر عملکردی را ارائه دهند، به شرطی که از قوانین مشابه لوله اصلی استفاده کنند.

وظیفه اصلی زنجیره رله، تامین امنیت و قابلیت همکاری مشترک برای تمام Parachian های آن است. اما برای انجام این کار، خود زنجیره رله ابتدا باید تا حد امکان ایمن باشد. منظورم این است که اگر امنیت شما به خطر بیفتد،

چگونه می توانید به نیروهای امنیتی خود وام دهید؟ برای درک اینکه چگونه زنجیره رله یکپارچگی خود را در طول زمان حفظ می کند، باید دو جنبه کلیدی شبکه های بلاک چین را در نظر بگیریم.

یک بلاک چین عمومی، یک محیط جستجو شده است. زیرا هیچ کس جریان اطلاعات (اعم از تایید یا بازیابی) را که روی آن رد و بدل می شود کنترل نمی کند. این بدان معنی است که اکثر گره های شبکه باید قبل از ایجاد و اتصال به زنجیره بلوک ها، در مورد اعتبار یک بلوک جدید توافق کنند. اما چگونه گره ها در مورد اینکه کدام تراکنش ها (داده ها) معتبر هستند به توافق می رسند و این از طریق فرایندی به نام اجماع اتفاق می‌افتد؟

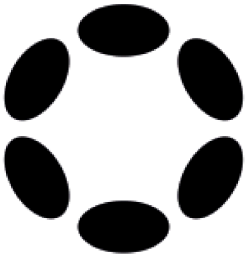
جزئیات کامل مکانیسم اجماع زنجیره رله برای این کتاب بیش از اندازه فنی است. بنابراین آنچه در اینجا ارائه می‌شود توضیحی بسیار ساده می باشد. پیاده سازی امروزی زنجیره رله Polkadot از مکانیزم اجماع ترکیبی استفاده می‌کند، به این معنی که اثبات سهام را با اثبات کار ترکیب می‌کند تا بهترین نتیجه را از هر دو محیط به دست آورد.

به عنوان یک قاعده کلی، دو فرآیند برای اجماع بلاک چین وجود دارد، یعنی تولید بلوک و بخش نهایی. تولید بلوک به فرآیند ایجاد بلوک های جدید اشاره دارد، در حالی که نهایی شدن به فرآیند تأیید بلوک ها بر روی زنجیره اشاره دارد. زنجیره رله Polkadot، مانند تمام شبکه های بلاک چین غیر متمرکز، تلاش می کند تا چند مشکل را از طریق اجماع خود حل کند که به صورت زیر می باشد:

- استحکام در برابر تبانی های مخرب، به گونه ای که تنها چند عملگر خوب برای حفظ یکپارچگی زنجیره لازم است. این بدان معنی است که اگر تنها چند گره صادق وجود داشته باشد، کمتر از 50٪ یکپارچگی زنجیره با وجود دستکاری گره های فاسد همچنان حفظ می شود.
- سرعت انتقالات و تأیید تراکنش برای مقیاس پذیری.
- انعطاف پذیری شبکه به گونه ای که به طور مکرر یا اصلاً کاهش پیدا نکند.
- درجه بالاتر عدم تمرکز، به طوری که هیچ گروهی از شرکت کنندگان شبکه، کنترل کاملی بر شبکه نداشته باشد.

برای اطمینان از اجرای موفقیت آمیز این راه حل ها در سراسر فرآیند، زنجیره رله از یک BABE و یک GRANDPA استفاده می کند. توضیح دقیق هر دو پروتکل برای مقاله ما در خصوص Polkadot ضروری نیست، پس به ضمیمه فنی منتقل شده است.

در مرحله بعد، درمیابیم که چگونه زنجیره رله امنیت خود را از تایید کننده ها، نامزدها و بخش های جمع کننده ها به دست می آورد.



فصل 3

ایمن سازی شبکه

با درک طراحی فنی که امنیت فناوری را تسهیل می کند، اکنون می توانیم به این امنیت دست بیابیم.

باید پرسید Polkadot چگونه امنیت اقتصادی خود را تضمین می کند؟ برای پاسخ به این سوال ما به نقش های مختلف موجود در شبکه می پردازیم.

فلسفه استکینگ

شبکه های غیر متمرکز با استفاده از مفهوم تئوری بازی‌ها برای طراحی سیستمی که در آن نقش ها، مسئولیت ها و انگیزه هایی برای همسو کردن اقدامات همه شرکت کنندگان در شبکه وجود دارد، به همکاری بین بسیاری از افراد دست می‌یابند. این یکی از دلایل اصلی ضروری بودن توکن‌ها برای بسیاری از سیستم‌های غیرمتمرکز است. پاداش‌های اقتصادی مکانیسم تشویقی نهایی است که برای بیت کوین، BTC و برای اتریوم، ETH است. بنابراین، قدرت امنیت یک بلاک چین تنها با کیفیت کد آن تعیین نمی شود بلکه همچنین با کیفیت طراحی مشوق و نشانه آن که در اصل، نظریه بازی است، تعریف می شود. به عنوان مثال، همه ماینرهای بیت کوین بلوک هایی را برای پاداش در بیت کوین ایجاد و تأیید می کنند. در یک سیستم اثبات کار مانند بیت کوین، نقش های شبکه کم و محدود به ماینرها است. این موضوع به این دلیل است که شبکه فقط به گره ها، بیت کوین ها و کاربران نیاز دارد.

در سیستم اثبات سهام، علاوه بر گره ها، شبکه به کاربرانی نیاز دارد که برای ایمن سازی شبکه، مقداری از سهام را کنار بگذارند. به یاد داشته باشید که بلاک چین های اثبات سهام، هم به امنیت تکنولوژیکی و هم بر امنیت اقتصادی تکیه می کنند، به طوری که اثرات زیست محیطی توسط اقتصاد جبران می شود. امنیت یک بلاک چین اثبات کار تنها به اندازه تعداد گره هایی است که آن را ایمن می کنند، در حالی که امنیت یک بلاک چین اثبات استک به تعداد گره ها و ارزش سهام آن بستگی دارد، که سهام ارزش اقتصادی آن است. بنابر این، فرآیند ایمن سازی شبکه در یک بلاک چین PoS، staking نامیده می شود. دو مزیت کلیدی PoS نسبت به PoW وجود دارد:

- PoS مصرف انرژی بسیار کمتری نسبت به PoW دارد. این یک نکته بسیار مهم است زیرا فناوری های ما تاثیر بیشتری بر تغییرات آب و هوایی دارند. به عنوان مثال، داده های ثبت شده نشان می دهد که هفت سال از گرم ترین سال ها در دوره 1880-2020 همگی پس از سال 2014 رخ داده اند.
- PoS مشارکت بیشتری را برای جامعه در امنیت شبکه ارائه می دهد و در نتیجه به متمرکز سازی بیشتر دست می یابد. این موضوع به این دلیل است که PoW مسئولیت امنیت شبکه را به سمت افراد باهوش فنی با ابزار و مهارت‌های اجرای یک گره منتقل می‌کند. با گذشت زمان، این امر ناگزیر منجر به افزایش سطح تمرکز می شود.

سه نوع شرکت کننده وجود دارد که روی ایمن سازی شبکه Polkadot کار می کنند: اعتبار دهنده، بخش نامزدها و بخش جمع کننده ها.

اعتبار دهنده

اعتبار دهندگان در Polkadot مانند ماینرهای بیت کوین هستند. آن‌ها گره‌هایی را اجرا می‌کنند که تراکنش‌ها را پردازش و تأیید می‌کنند، بلوک‌ها را ایجاد می‌کنند و تاریخچه بلاک چین را ذخیره می‌کنند. بدون آنها شبکه ای وجود نخواهد داشت. نکات کلیدی که باید به آنها توجه کرد عبارتند از:

- آنها زیرساخت فیزیکی را فراهم می کنند که شبکه بر روی آن اجرا می شود.
- آنها باید اطمینان حاصل کنند که در مواقع لزوم همیشه آنلاین هستند (به ویژه زمانی که وظیفه دارند یک بلاک جدید ایجاد می کنند).

این فرآیند به همان اندازه که تجهیزات کامپیوتری مربوطه را بدست آورده و کد Polkadot را اجرا کنید، ساده است. هنگامی که یک گره مستقر می شود، اکثر عملیات های معمول می توانند خودکار شوند، در حالی که اعتبار دهنده ها می توانند بر عیب یابی و حفظ اتصال تمرکز کنند. برای تلاش‌های اقتصادی و فیزیکی، اعتباردهنده‌ها در توکن‌های DOT پاداش می‌گیرند. تعداد کل اعتباردهنده‌ها در شبکه پارامتری است که می‌توان آن را بر اساس تقاضای شبکه

تنظیم کرد، از چند مورد شروع و اکنون به ۲۹۷ (از ژانویه ۲۰۲۲) می‌رسد. هدف رسیدن به 1000 تایید کننده است.

ممکن است کسی به این عدد نگاه کند و بپرسد که آیا برای حمایت از متمرکزسازی کافی است یا خیر، به خصوص وقتی در نظر بگیریم که بیت کوین بیش از 20000 ماینر دارد و اتریوم 1.0 بیش از 10000 ماینر دارد. برای درک اینکه چرا 1000 اعتبار دهنده کافی است، باید به خاطر داشته باشیم که اجماع Polkadot چگونه کار می کند. Polkadot با انتخاب تصادفی اعتبار دهنده ها از طریق ماژول تولید بلوک BABE و مجزا نگه داشتن اطلاعات مربوط به اعتبار دهنده بلوک، امکان تبانی بین اعتبار دهنده ها را محدود می کند. این رویه همچنین با این پیش‌فرض تضمین می‌شود که همه اعتباردهنده‌ها باید به‌طور هم‌زمان برای اعتبار دهنده تک تک بلوک‌ها رقابت کنند.

وقتی گفته می شود که Polkadot 1000 تایید کننده را هدف قرار می دهد، به این معنی نیست که فقط 1000 نفر واجد شرایط برای تایید صلاحیت هستند. بلکه، به این معنی است که تولید و تأیید بلوک توسط 1000 اعتبار دهنده به طور همزمان انجام می شود، در حالی که هر اعتبار دهنده دیگری، به عنوان کاندید اعتبار دهنده عمل می کند. در پایان، تعداد کم اعتبار دهنده ها نه تنها برای کاهش ردپای کربنی، بلکه برای دستیابی به مقیاس‌پذیری مفید است. اگر 13000 اعتبار دهنده و 3/2 اعتبار دهنده ها در مجموعه فعال باشند (کسانی که در حال حاضر در اجماع شبکه شرکت می کنند) باید موافقت کنند، در این صورت هر تراکنش باید قبل از پردازش برای حدود 7500 اعتبار دهنده منتظر بماند، که به ناچار سرعت شبکه را کند می کند.

هدف متمرکزسازی این نیست که تا حد امکان اعتباردهنده‌های بیشتری داشته باشیم، بلکه تا حد امکان مشارکت‌کنندگان شبکه‌ای بیشتر باشد. همه چیز در مورد مالکیت، قدرت و اختیار است. به همین دلیل است که اثبات سهام استک، سیستم بسیار مطلوب تری است، زیرا بسیاری از افراد ابزار راه اندازی این گره ها را ندارند. اگر امنیت شبکه فقط توسط اعتبار دهنده یا استخراج کننده ها تامین شود، بخش بزرگی از جامعه کنار گذاشته می شود. با اثبات سهام استک، هر فرد نوعی که هیچ چیز در مورد رایانه یا کدنویسی نمی داند، می تواند نقش اصلی را در امنیت شبکه ایفا کند و همچنین جوایزی کسب کند. در مقابل، بلاک‌چین‌های اثبات کار به تمرکز مالکیت، قدرت و حاکمیت در اطراف متخصصان فنی و اپراتورهای تجهیزات ماینینگ منجر می‌شوند. هدف اصلی برای یک سیستم اثبات سهام استکینگ، اطمینان از این است که مکانیسم های استکینگ موجود، متمرکزسازی را بیشتر تقویت کند. برای درک اینکه چگونه Polkadot به این هدف دست می یابد، نقش نامزدها را بررسی خواهیم کرد.

نامزدها

اگر در حال خواندن این کتاب هستید، احتمال اینکه نامزد شوید یا به دنبال آن باشید، بسیار زیاد است. نقش یک نامزد در تامین امنیت شبکه بسیار کمتر از یک اعتبار دهنده فنی است. این به این دلیل است که از نامزدها خواسته می‌شود که توکن‌های خود را برای حمایت از اعتبار دهنده‌هایی که کار سنگین اجرای گره‌ها را انجام می‌دهند، قفل کنند. از آنجایی که اوراق قرضه مورد نیاز برای تبدیل شدن به یک اعتباردهنده مقدار زیادی است (در حال حاضر 1.4 میلیون DOT)، اعتبار دهنده‌ها برای واجد شرایط بودن برای نقش خود، باید از پشتیبانی مداوم تعداد زیادی از توکن‌های نامزد ها اطمینان حاصل کنند. هنگامی که پاداش ها به اعتباردهنده پرداخت می شود، بخشی از آن پاداش ها به این نامزدها می رسد. مبلغ دقیق در نهایت بر اساس تعداد کل توکن‌های موجود و درصد کمیسیون تعیین‌شده توسط اعتبار دهنده مشخص میشود.

برخلاف بسیاری از سیستم‌های PoS که نامگذاران را مجبور می‌کنند همه توکن‌های خود را با یک اعتبار دهنده منفرد پیوند دهند، Polkadot از مکانیزم پیشرفته‌ای استفاده می‌کند که به هر نامدهنده اجازه می‌دهد تا حداکثر ۱۶ اعتبار دهنده را انتخاب کند. از این میان، تنها تعداد کمی از تایید کنندگان موفق می شوند در طول انتخاباتی که در هر دوره برگزار می شود (که تقریباً یک روز در Polkadot است) در مجموعه فعال پذیرفته شوند. با انتخاب 16 اعتباردهنده، نامزدها به خود شانس بیشتری برای کسب حداکثر پاداش می دهند. این به این دلیل است که زنجیره رله ای که توکن های خود را بر روی آن قرار می دهید دارای پروتکلی است که فرآیند استکینگ را برای همه نامزدها و اعتبار دهنده ها بهینه می کند، تا حداکثر امنیت را تضمین کند. جزئیات این اقدام بیش از حد فنی است، بنابراین من فقط یک خلاصه اولیه از عملکردهای اصلی آن را ارائه خواهم کرد:

حداکثر مشارکت نامزد - الگوریتم (پروتکل) با انتخاب حداقل یکی از تایید کننده های نامزد برای هر دوره، مشارکت نامزد در اجماع را به حداکثر می رساند. یک دوره، مدت زمان در زنجیره‌های بلوکی است – کمی شبیه روزهایی که ما انسان‌ها داریم – که به تعداد بلوک‌های تولید شده مشخص می‌شود: ۶ ساعت در کوسامان و ۲۴ ساعت در Polkadot. هنگامی که یک نامزد 16 اعتبار دهنده را انتخاب می کند، این مکانیسم تضمین می کند که حداقل یکی از آن شانزده مورد در مجموعه فعال باشد.

خطر تمرکز را به حداقل برسانید - این از طریق تئوری بازی به دست می آید. طبیعی است که انسان‌ها به دنبال چیزی هستند که مطمئن‌تر است و اغلب محبوب‌ترین گزینه‌های موجود است. به عنوان مثال، اگر بسیاری از نامزدها یک اعتبار دهنده را انتخاب کنند، سایر نامزدها تمایل دارند همان اعتبار دهنده را انتخاب کنند. به این ترتیب است که تمرکز رخ می دهد، زیرا اعتبار دهنده در نهایت قدرت بیشتری از آنچه در ابتدا به دنبال آن بود، در شبکه به دست می آورد. برای کاهش این خطر، پروتکل شرط بندی پاداش های مساوی را به همه اعتبار دهندگان، صرف نظر از وزن سهام آنها یا تعداد نامزدهایی که از آنها حمایت میکنند، پرداخت می کند. اما اعتبار دهندگانی که نامزدهای زیادی دارند، در مجموع به ازای هر شرط بندی DOT پاداش کمتری پرداخت خواهند کرد. در پایان، تنها نامزدهایی که بیشترین DOT ها را با این اعتباردهنده های محبوب به اشتراک می گذارند، بیشترین سهم را از جوایز دریافت می کنند، در حالی که نامزدهایی که تعداد زیادی DOT شرط بندی نکرده اند، بسیار کمتر (یا هیچی، بسته به میزان اشتراک) دریافت خواهند کرد. تعداد نامزدهایی که در چنین شرایطی پاداش دریافت می کنند، متغیر است و در طول زمان متفاوت خواهد بود. این به عنوان مکانیزمی در نظر گرفته شده است تا هر نامزدی را مجبور کند که دائماً نامزدهای خود را بررسی کند و اطمینان حاصل کند که حداکثر پاداش را برای مشارکت در شبکه خود دریافت می کند.

نحوه نامزد شدن چگونه است؟

اولین گام برای نامزدی، گرفتن توکن های DOT است که برای آن به یک حساب کاربری و یک کیف پول نیاز دارید. می توانید از کیف پول هایی مانندPolkadot-JS، Fearless، Talisman، Nova Polkawallet و از کیف پول های اکوسیستمی دیگر نیز استفاده کنید. یکی از چیزهایی که باید به خاطر بسپارید این است که، پس از اینکه وجوه خود را برای استکینگ عرضه کردید، تحت یک دوره اجباری 28 روزه قرار خواهید گرفت. به این معنی که از لحظه ای که انتخاب می کنید توکن های خود را لغو و برداشت کنید، 28 روز طول می کشد تا توکن های خود را پس بگیرید.

برای جلوگیری از این وقفه، می توانید با شخص ثالثی شریک شوید که به شما آزادی بیشتری می دهد، مانند برخی صرافی های متمرکز. به شما این امکان را می دهد که فوراً سهام خود را برداشت کنید. راه حل بهتر این است که از پلتفرم های غیرمتمرکز استفاده کنید که به شما یک توکن مشتق در زمانی که DOT خود را به اشتراک می گذارید، می دهد. به عنوان مثال، می توانید DOT خود را با استفاده از Acala (در ادامه در مورد آنها بیشتر توضیح میدهیم) و LDOT که مخفف "DOT مایع" است را دریافت کنید. تفاوت بین DOT و توکن مشتق شده LDOT در این است که LDOT در حالی که برای استفاده در پروتکل‌های DeFi در سراسر اکوسیستم در دسترس باقی می‌ماند، جوایزی دریافت می‌کند. به این ترتیب که وقتی می‌خواهید LDOTهای خود را به DOT تبدیل کنید، تعداد DOTهای بیشتری نسبت به قبل خواهید داشت. LDOT تنها نشانه ای نیست که این عملکرد را انجام می دهد. Parachian های دیگری نیز وجود دارند که همان سرویس استیکینگ مایع را ارائه می دهند، اما با نام های متفاوتی برای توکن هایشان (بایفراست vDOT و xDOT مالی موازی).

کار واقعی نامزدها، به انتخاب 16 تایید کننده شما خلاصه می شود. اگر از طریق یک پلتفرم شخص ثالث استک می کنید، پس نیازی به انجام این فرآیند ندارید. با این حال، اگر به تنهایی استک می کنید، باید یاد بگیرید که چگونه اعتباردهنده های مناسب را انتخاب کنید.

انتخاب اعتبار دهنده مناسب

انتخاب اعتبار دهنده مناسب به دلیل واقعیت احتمال ریزش، فرآیندی حیاتی است. اگر اعتباردهنده‌ای را انتخاب کنید که عملکرد بدخواهانه ای دارد، در این صورت در خطر از دست دادن توکن‌های به‌دست‌آمده خود هستید، که این یک

تراژدی خواهد بود. یکی دیگر از دلایلی که می‌خواهید اعتباردهنده های مناسب را انتخاب کنید، به حداکثر رساندن پاداش‌های شرطبندی است. برخی اعتباردهنده ها به شما امکان می دهند بیشتر از دیگران درآمد کسب کنید و این وظیفه شماست که پاداش های خود را به حداکثر برسانید. هنگام انتخاب اعتبار دهنده مناسب، چند نکته وجود دارد که باید در نظر بگیرید.

پوسته تایید کننده در بازی - برای هر کسی سخت است که وقتی چیزی برای از دست دادن دارد، بدخواهانه یا بی دقت عمل کند. این موضوع همچنین به عنوان داشتن پوسته در بازی شناخته می شود. اگر اعتباردهنده هیچ توکنی در انبار خود نداشته باشد، به این معنی است که اگر از سیستم حذف شود چیزی برای از دست دادن ندارد. اما نامزدهای او عواقب اعمالش را متحمل خواهند شد. با این حال، اگر او پاداش دریافت کند، می تواند این پاداش های بزرگ را برای خود حفظ کند. بنابراین، توصیه نمی‌شود که سهام خود را روی یک اعتبار دهنده بدون ذینفع یا خود استک قرار دهید، مگر اینکه اطمینان داشته باشید که بدخواهانه یا بی‌دقت عمل نمی‌کند.

هویت اعتبار دهنده - زمانی که همه افراد در شبکه هویت او را می شناسند، برای هر کسی سخت است که بدخواهانه عمل کند. البته، این شما را از اشتباه اعتبار دهنده هم نجات نمی دهد، اما یک قانون سرانگشتی قابل اعتماد برای استفاده است. افرادی که هویت خود را در زنجیره نشان می دهند قابل اعتمادتر از کسانی هستند که این کار را نمی کنند، زیرا شهرت آنها در خط است. در مورد شخصی با هویت زنجیره ای، می توانید با آنها تماس بگیرید تا در صورت نگرانی در مورد تراکنش ها، با او در تماس باشید تا بفهمید چه اتفاقی می افتد. اگرچه برخی اعتبار دهنده ها تصمیم میگیرند از حساب کاربری خود خارج شده و با حساب اعتباری جدید و هویت جدید، که احتمالاً مشابه همان نسخه اصلی است، فقط با چند تغییر در جزئیات، مجددا عضو شوند.

کمیسیون اعتبار دهنده - برای سود بیشتر، عاقلانه تر است که اعتبار دهنده هایی را با کمترین کمیسیون انتخاب کنید. اعتبار دهنده با 50 درصد کمیسیون، 50 درصد از تمام جوایز شرط بندی را دریافت می کند و تنها 50 درصد آن را بین نامزدها تقسیم می کند. اما یکی با 10 درصد کمیسیون فقط 10 درصد از تمام پاداش ها را می گیرد که مطمئناً دومی بسیار سودآورتر است.

سابقه حذف تایید کنندگان - تصمیم گیری در مورد یک شخص یا نهاد بر اساس عملکرد گذشته طبیعی است. در مورد اعتبار دهنده ها، شما نمی خواهید اعتبار دهنده هایی را معرفی کنید که در گذشته دارای حذف های متعدد بوده اند. با این حال، گاهی اوقات اعتباردهنده‌ها می‌توانند رویدادهایی را کاهش دهند که کاملاً تقصیر آنها نیست. این شبکه گاهی اوقات ممکن است با مشکلاتی مواجه شود که باعث می شود اعتبار دهنده های صادق و کوشا جریمه شوند.

برای اطلاعات بیشتر در مورد ایمن‌ترین راه برای معرفی اعتبار دهنده، این راهنما را بررسی کنید.

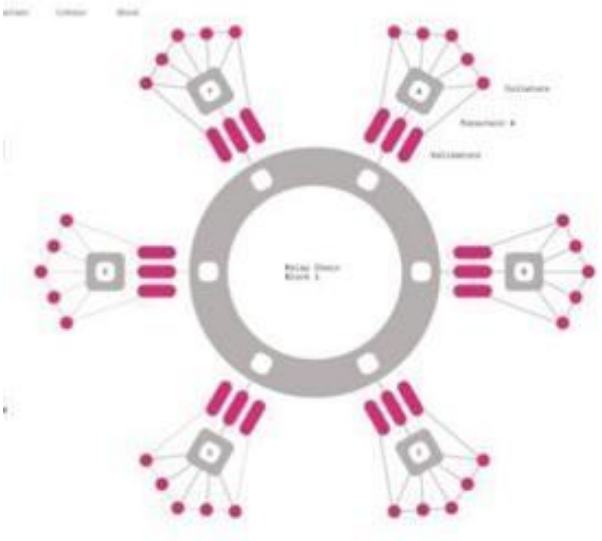
جمع‌آوری‌کننده‌ها

در حالی که اعتباردهنده‌ها بلوک‌هایی را برای زنجیره رله ایجاد و تأیید می‌کنند، جمع‌کننده‌ها بلوک‌هایی را برای Parachianها ایجاد و تأیید می‌کنند. به خاطر داشته باشید که مکانیسم های مشابه (BABE و GRANDPA) در Parachian ها در حال عملکرد هستند. شما می توانید جمع آوری کننده ها را به عنوان اعتبار دهنده Parachian در نظر بگیرید، زیرا آنها باید یک گره کامل از Parachian و همچنین زنجیره رله را اجرا کنند. وقتی جمع‌آوری کننده ها در یک Parachian بر روی بلوک‌های Parachian جدید توافق می‌کنند، این بلوک‌ها را به اعتبار دهنده‌های زنجیره رله ارسال می‌کنند تا در زنجیره رله گنجانده شوند. به این ترتیب، بلوک های تراکنش تایید، ارسال و توسط جمع کننده ها و بیشتر توسط اعتبار دهنده، تایید و به همراه اعتبار دهنده زنجیره رله که به طور تصادفی به Parachian ها اختصاص داده شده است، به زنجیره رله اضافه می شوند.

به عنوان مثال، در دوره اول، که x تعداد بلوک طول می کشد، اعتبار دهنده V1، V2 و V3 به Parachian A اختصاص داده می شود. این بدان معناست که جمع کننده های Parachian A تراکنش های خود را به V1، V2 و V3 ارسال می کنند و بقیه را ترک می کنند. اعتبار دهنده های دیگر آزاد هستند تا تراکنش های سایر Parachian ها را تایید کنند. هنگامی که این اعتبار دهنده ها تأیید را به پایان رساندند، تراکنش های تایید شده خود را برای تایید بیشتر قبل از اضافه شدن تراکنش ها به زنجیره رله، به بقیه اعتبار دهنده های زنجیره رله پیشنهاد می کنند. به یاد داشته باشید که بیشتر این موارد تقریباً خودکار است. اعتبار دهندگان از قبل نمی دانند روی کدام Parachian کار

خواهند کرد. در پایان دوره، اعتبار دهنده های V1، V2 و V3 از Parachian A دور می شوند، به طوری که مجموعه جدیدی از اعتبار دهنده تراکنش ها، Parachian A را برای مدت زمان دوره دوم تایید می کنند.

این فرآیند با به حداقل رساندن و مهار خطر تبانی بین جمع‌آوری کننده ها و اعتبار دهنده‌ها، امنیت شبکه را تقویت می‌کند. به عنوان مثال، اگر در طول یک دوره حمله ای صورت می گرفت، در آغاز دوره بعدی، این حمله توسط تایید کنندگان صادق مقابله می شد.



زنجیره رله

زنجیره اتصال Polkadot که فراهم کننده امنیت اقتصادی و پروتکلهای همکاری میباشد.

پاراچین

زنجیره های شخص ثالث که برای قابلیت همکاری، مقیاس پذیری و امنیت تلفیقی به Polkadot متصل می شوند.

ز

1. اداره ملی اقیانوسی و جوی. (2021، ژانویه). سال 2020 دومین سال گرم ترین سال زمین بود، درست پس از 2016.
.https://www.noaa.gov/news/2020-was-earth-s-2nd-hottest-year-just-behind-2016
تاریخ بازدید: 31-08-2021.

فصل 4

اداره شبکه

وقتی پول نقد باعث کنار گذاشتن سیستم کلاسیک شد

در سال 2016، 60 میلیون دلار ETH در چیزی که اکنون "هک DAO" نامیده می شود به سرقت رفت. این خلاصه ای از چگونگی وقوع آن است.

در آوریل 2016، تعداد زیادی از مردم توکن‌های اتریوم خود را در یک قرارداد هوشمند جمع کردند تا اولین سازمان غیرمتمرکز خودمختار (DAO)، اکوسیستم کریپتو را تأمین مالی کنند. 150 میلیون دلار در این تامین مالی جمعی، جمع آوری شد. با این حال، کمتر از سه ماه بعد، قرارداد هوشمند هک شد و یک کاربر متجاوز، شروع به تخلیه سرمایه کرد. جامعه وحشت زده شده بود. به زودی، گروهی از هکرهای کلاه سفید ظاهر شدند که با همکاری یکدیگر سعی در متوقف کردن مجرم داشتند. جزئیات نحوه وقوع هک برای این کتاب بسیار فنی است، اما واضح بود که هکر کلاه سیاه از نقصی در کد قرارداد هوشمند استفاده کرده است. از آنجایی که مهاجم فقط می‌توانست توکن‌ها را خیلی آهسته خارج کند، جمعی از هکرهای کلاه سفید در نهایت راهی برای متوقف کردن سوء استفاده پیدا کردند. اما امدادگران اشتباهی مرتکب شدند که در نهایت به دزد اجازه داد تا پول ها را آزاد کند: تنها راه حل باقی مانده بازگشت زنجیره و لغو این رویداد بود.

با توجه به اینکه دزدی درست جلوی چشم جامعه اتریوم اتفاق افتاده بود، ممکن است فکر می‌کنید که تصمیم‌گیری در مورد اقدام درست نتیجه‌گیری آسانی است. اما اینطور نبود. ابتدا، جامعه باید راهی برای نظرسنجی از کاربران شبکه اتریوم در مورد آنچه که فکر می‌کردند در آینده اتفاق می‌افتد، میجست. این امر به این دلیل است که در آن زمان، عموماً پذیرفته شده بود که داده‌های بلاک چین غیرقابل تغییر است و توسط رمزنگاری مهر و موم شده است و هر آنچه در زنجیره اتفاق افتاده است هرگز قابل بازگشت نیست. اما، در این مورد، از آنجایی که 60 میلیون دلار به سرقت رفته بود، ایده آل ها باید با واقعیت مقابله می کردند. و واقعیت این بود که امکان تغییر اطلاعات ذخیره شده در بلاک چین اتریوم وجود داشت.

در نتیجه این کشف، دو کارگروه پدید آمد. از یک طرف، اکثریت می خواستند با برگرداندن زنجیره به بلوک قبل از حمله، تاریخ سرقت را پاک کنند. از سوی دیگر، متخصصان متمرکزسازی مخالف دستکاری در تغییرناپذیری بلاک چین اتریوم بودند. در پایان، رای گیری انجام شد و 80 درصد از جامعه به حذف هک از تاریخچه بلاک چین اتریوم رای دادند. برای انجام این کار، باید فورکی برای به روز رسانی بلاک چین و بازنویسی کد اصلی ایجاد میشد. اما برای اینکه فورک پیش برود، همه گره‌های شبکه باید به‌روزرسانی را میپذیرفتند، تا شبکه بتواند وارد وضعیت جدیدی شود و در مسیر جدیدی حرکت کند. بنابراین، هنگامی که به روز رسانی انجام شد، تمام آثار هک پاک شد و اکثر اعضای جامعه خوشحال بودند که اخلاق پیروز شده است و برای مهاجم هیچ چیزی باقی نمی ماند. یا برعکس؟

به زودی مشخص شد که اگرچه شبکه اتریوم به زنجیره جدیدی راه یافته بود و در حال نوشتن تاریخ جدیدی بود، گره هایی وجود داشتند که مسیر ارتقای جدید را دنبال نکردند. اساساً، آنها انتخاب کرده بودند که در زنجیره متعارف قدیمی اتریوم باقی بمانند، با سوابق سرقت هنوز وجود داشت. به زودی، مرحله جدیدی از وحشت بوجود آمد: آیا اپراتورهای گره عمدا این کار را انجام می دادند؟ ممکن است این هم نوعی هک باشد؟ تلاش هایی برای ارتباط با ماینرها انجام شد و در نهایت مشخص شد که این اقدام عمدی بوده است، اما دلایل آن هنوز ناشناخته مانده است. زنجیره قدیمی که از فورک خودداری می کرد؛ به عنوان اتریوم کلاسیک شناخته شد. شما می‌توانید در مورد این داستان در کتاب Out of the Ether، کتابی از Matthew Leising که در آگوست 2020 منتشر شد، اطلاعات بیشتری کسب کنید. برای برجسته کردن اهمیت طراحی حاکمیت زنجیره‌ای Polkadot و ارتقاء بدون فورک، لازم بود در این قسمت از تاریخ کاوش کنیم.
حالا ممکن است تعجب کنید: مشکل بزرگ فورک کردن اتریوم به اتریوم کلاسیک چیست؟ از منظر غیر متمرکزسازی، منطقی است که به هر شرکت کننده شبکه آزادی انتخاب اینکه آیا فورک مناسب است یا نه داده شود، بنابراین یکپارچگی زنجیره حفظ می شود. اما خطرات بزرگ دیگری نیز برای جامعه به همراه دارد: زمانی که چند

ماینر توافق خود را با شبکه اتریوم قطع کردند و تصمیم گرفتند در زنجیره قدیمی باقی بمانند، امنیت اتریوم در سه سطح به خطر افتاد:

1. شبکه با تعداد کمتری ماینرها برای استخراج معاملات به جا ماند.
2. ارزش ETH تحت تأثیر قرار گرفت. زیرا قیمت آن به سمت سقوط آزاد رفت
3. اعتماد جامعه با هک و فورک غیرمنتظره، متزلزل شد.

متاسفانه، این تنها فورک بحث برانگیز در تاریخ شبکه های بلاک چین نیست. در مورد بیت کوین نیز این اتفاق افتاد. زمانی چنین شد که جامعه بیت کوین در مورد سرعت بلاک چین بیت کوین وارد بحث و جدال شد و راه های مختلفی را برای مقیاس بندی شبکه و افزایش تعداد تراکنش هایی که می توانند در یک بلوک قرار گیرند پیشنهاد کردند. یک گروه می خواستند اندازه بلوک را 8 برابر افزایش دهد تا 8 برابر تراکنش های بیشتر در ثانیه پردازش شود. اما این همچنین زمان اعتبار دهنده بلوک را بیش از 10 دقیقه افزایش می داد. زیرا شبکه منتظر می ماند تا بلوک های بزرگتر پر شوند. سایرین فکر می کردند که دستکاری در پروتکل بیت کوین نوعی بدعت است.

هیچ رأی و مشورتی وجود نداشت؛ بخشی از شبکه بیت‌کوین به شبکه جدیدی به نام بیت‌کوین کش منشعب شد که باعث شد کدهای موجود را به‌روزرسانی کنند تا اندازه بلوک خود را افزایش دهند. در طول سال‌ها، بیت‌کوین در بسیاری از شبکه‌های دیگر فورک شده است، با این حال، قدرت استخراجی که این فورک‌ها را ایمن می‌کند، بیشتر و بیشتر در دستان چند استخر بزرگ ماینینگ متمرکز می‌شود.

بنابراین، این شبکه های فورک شده می توانند به راحتی مورد حمله قرار گیرند زیرا ارزش مشابه بیت کوین را ندارند و نمی توانند به اندازه کافی مشارکت کنندگان شبکه را جذب کنند. این به این دلیل است که قدرت هر شبکه غیرمتمرکز در قدرت تعداد و سطوح مشارکت در جامعه آن نهفته است.

وقتی امروز به بیت‌کوین و اتریوم نگاه می‌کنیم، به نظر می‌رسد که این فورک‌ها هیچ تاثیری بر شبکه‌ها نداشته‌اند، اما این یک مشکل است. با نگاه ساده انگارانه به وضعیت موجود، این واقعیت که هر دو شبکه با وجود این اپیزودهای بحث برانگیز تا اینجا پیش رفته اند، دلیلی بر بهینه بودن طراحی آنها نیست. بلکه به مشکلی اشاره می‌کند که در تمام شبکه‌های بلاک چین وجود دارد: اگر کد برای دیدن و کپی کردن همه در دسترس باشد، فورک کردن آن آسان است و اگر یک شبکه را به اندازه کافی منشعب کنید، می توانید برای همیشه به امنیت آن آسیب وارد کنید. زیرا دور کردن ماینرها یا اعضای جامعه، منجر به از دست رفتن ارزش شبکه و قدرت اجماع می شود.

بنابراین چگونه می توانید از تضعیف یک شبکه و جامعه آن جلوگیری کنید؟ پاسخ Polkadot این است که باید یک فرآیند حاکمیت زنجیره ای را ارائه دهد که هر شرکت کننده بتواند به آن اعتماد کند. همراه با ارتقاء بدون فورک، یک بلاک چین دریافت خواهید داشت که به راحتی و بدون اعمال تغییرات مختل شده، قابل ارتقا است. برای درک چگونگی آن، اجازه دهید به مکانیسم حکومتی Polkadot بپردازیم. این بخش از قالب پرسش و پاسخ پیروی می کند.

حکومت بر Polkadot

1. حکمرانی برای چیست؟

هدف اصلی حاکمیت در هر سیستمی، اصلاح پارامترهای سیستم است. در مورد کشورها، اینها لوایح جدید و تجدید نظر در قانون اساسی خواهند بود. در مورد Polkadot، هدف داده های زنجیره ای خواهند بود. برخی از نمونه ها عبارتند از:

- به روز رسانی موجودی کاربر (به عنوان مثال در مورد سرقت یا گم شدن کلید)
- به روز رسانی زمان اجرا
- اتصال یا جدا کردن پاراچین ها و پاراتریدها

2. ساختار حاکمیت چیست؟

ساختار حاکمیت زنجیره ای Polkadot دارای 3 بازو است: شورا، کمیته فنی و جامعه (که «اتاق همه پرسی» یا تعداد دارندگان DOT در دسترس برای رأی دادن نیز نامیده می شود). بیایید هر یک از آنها را با جزئیات بررسی کنیم.

شورا - این بخش یک گروه 24-6 عضوی است که نماینده همه دارندگان DOT هستند. هدف اصلی آنها بررسی پیشنهادهایی است که هدف آنها ارائه مسیرهای جدید به شبکه Polkadot است.

آن ها چه می توانند بکنند؟

- انتخاب اعضای کمیته فنی
- رای دادن به پیشنهادات شورا - همه پیشنهادات (رفراندم، خزانه داری، جایزه، نکات) قبل از انتقال به مرحله بعدی باید صریحاً توسط شورا تصویب یا رد شوند.تنها استثناء پیشنهادات تحت رهبری جامعه است.
- در صورتی که پیشنهادی برای اکوسیستم مضر تشخیص داده شود، همه پرسی را وتو کنند. گفته می شود، وتوی آنها می تواند از طریق یک رای عمومی دیگر لغو شود.
- همه پرسی سریع در مواقع اضطراری فنی.

چه کسی می تواند به شورا بپیوندد؟

هر دارنده DOT.

چگونه انتخاب می شوند؟

یک دارنده DOT که مایل به پیوستن به شورا است، فقط باید خودش را نامزد کند و آرای کافی برای ورود به مجموعه انتخابی را جمع کند. دارندگان DOT می توانند اعضای شورا را برای اداره شبکه از طرف خود با ارائه دادن توکن های خود انتخاب کنند، به همان روشی که اعتبار دهنده خود را انتخاب می کنند. به این ترتیب، هر دارنده DOT که مایل به عضویت در شورا است باید برای همکاری با نامزدها هم تمایل داشته باشد. زیرا اعضای شورا بر اساس حمایت و ترجیحی که رای دهندگان به آنها داده اند انتخاب می شوند.

هر دو هفته یکبار انتخاباتی برای تغییر ترکیب شورا برگزار می شود تا از خویشاوند گرایی جلوگیری شود. این برای تشویق مشارکت جامعه در حکومت طراحی شده است. زیرا از دارندگان منفعل دعوت می کند تا قدرت DOTS خود را به سایر اعضایی که مایل به اداره شبکه هستند تفویض کنند. اما این فقط یک سناریوی ایده آل است. در واقع، همان اعضای شورا اغلب برای ماه ها در صندلی خود باقی می‌مانند، زیرا کاندیداهای شورا به تعداد کافی وجود ندارند و رای دهندگان به ندرت فهرست نامزدهای مورد نظر خود را تغییر می‌دهند.

مکانیسم رأی گیری چیست؟

انتخاب اعضای شورا با استفاده از همان مکانیزم اجرا شده در استکینگ انجام می شود. با این حال، از آنجایی که این انتخاب به وزن توکن بستگی دارد، این شانس وجود دارد که به مرور زمان، شبکه به کاربرانی که تعداد زیادی DOT به نام «اوراکل» دارند، علاقه مند شود. در حال حاضر هیچ راه حل کاملی برای این مشکل وجود ندارد، اما روش Phragmén که در Polkadot استفاده می شود راه حل جالبی ارائه می دهد. این امر به این دلیل است که الگوریتم آن وزن نشانه پشت هر نامزد را در نظر می گیرد، اما تنها بر اساس آن اطلاعات تصمیم نمی گیرد. بلکه، این روش نتایج را برای سناریوهای ایده‌آل زیر بهینه می‌کند:

1. کل مبلغ مورد نظر را به حداکثر برسد تا حداکثر امنیت اقتصادی تضمین شود.
2. به حداکثر رساندن سهام پشت اعتبار سنج با حداقل سهام، به طوری که همه نامزدها برای به دست آوردن حامیانی که به آنها امکان دسترسی به مجموعه فعال را می دهد، به رقابت ادامه دهند.
3. واریانس سهام در مجموعه را به حداقل برسانید تا تفاوت زیادی بین اعتبار دهنده های دارای بالاترین و پایین ترین استک ها وجود نداشته باشد.

در مجموع، روش فراگمن در ایجاد درجه خاصی از انصاف، با در نظر گرفتن جزئیات، کار شایسته ای انجام می دهد. برای درک عملکرد درونی آن، وقت بگذارید و این مقاله ویکی را بخوانید.

کمیته فنی : TC یا کمیته فنی از توسعه دهندگانی تشکیل شده است که در پایگاه کد Polkadot مشارکت داشته اند. آنها وظیفه دارند از عملکرد روان شبکه، اطمینان حاصل کنند.

آن ها چه می توانند بکنند؟

- ارائه پیشنهادات به شورا

- پیشنهادات سریع معمولا در موارد اضطراری فنی
- وتوی همه پرسی را از طریق توصیه به شورا – در صورت ایجاد خطر امنیتی برای زنجیره رله Polkadot از طریق رفراندوم

چه کسانی می توانند به کمیته فنی بپیوندند؟

تیم ها با اکثریت رای شورا به سادگی به کمیته فنی اضافه یا از آن حذف می شوند.

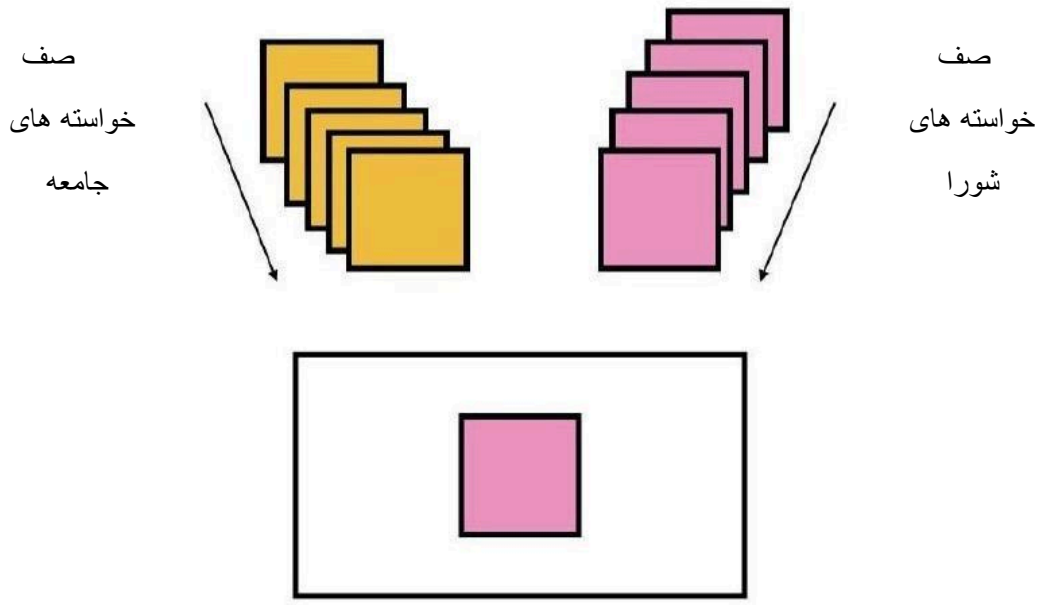
جامعه - متشکل از دارندگان DOT است که می توانند و مایل به شرکت در فعالیت های زیر هستند:

1. معرفی اعضای شورا
2. ارائه پیشنهادات
3. رای دادن به همه پرسی

3.تصمیمات چگونه گرفته می شود؟

هر تصمیمی که در مورد هدایت Polkadot گرفته می شود با یک پیشنهاد شروع می شود. یک پیشنهاد می تواند توسط هر یک از سه بازوی حاکمیتی ارائه شود. اگرچه همه پیشنهادات کمیته فنی به شورا ارائه می شود و سپس در مورد آن رای می دهد. اگر پیشنهاد موفقیت آمیز باشد، به یک همه پرسی عمومی تبدیل می شود. به این ترتیب، دو صف پیشنهاد اصلی وجود دارد: یکی برای پیشنهادات تحت رهبری جامعه و دیگری برای پیشنهادات تحت رهبری شورا.
در هر "چرخه رای گیری" (28 روز در Polkadot)، پیشنهادی که با بیشترین تعداد توکن پشتیبانی می شود به یک همه پرسی عمومی تبدیل می شود. در هر رفراندوم فقط یک پیشنهاد وجود دارد، مگر در شرایط اضطراری که کمیته فنی نیاز به پیگیری سریع یک یا چند پیشنهاد تکمیلی دارد.

اگر پیشنهادی از صف جامعه در آخرین چرخه رای‌گیری به رای گذاشته شود، پیشنهاد برتر از صف شورا در چرخه رای‌گیری جدید نمایش داده می‌شود. این رویکرد نوبتی کمک می کند تا اطمینان حاصل شود که جامعه، شورا و کمیته فنی می توانند فعالانه در تصمیم گیری به موقع شرکت کنند.



روند رفراندوم: صف دوتایی

4.چرخه حیات پروپوزال چیست؟

هر پیشنهادی که از طریق حاکمیت زنجیره‌ای ارسال می‌شود، می‌تواند تحت هر یک از وضعیت‌های زیر قرار گیرد:

ثانویه - وقتی عضوی از جامعه پیشنهادی را ارائه می‌کند، باید برخی از DOT ها را ببندد. اگر پیشنهاد برای سایر اعضای جامعه ارزشمند است، آن‌ها می‌توانند با قفل کردن تعداد بیشتری از DOT در پیوند اصلی، آن را ثانویه کنند. هرچه DOT های بیشتری در حمایت از یک پروپوزال قفل شوند، این پیشنهاد سریعتر به بالای صف می رسد و در این مرحله وضعیت تغییر می کند. روند مشابهی برای پیشنهادات شورا در حال اجرا است.

در انتظار - وقتی پیشنهادی به بالای صف رسید، به زودی به یک همه پرسی عمومی رسمی تبدیل می شود. توجه به این نکته ضروری است که پس از تعیین زمان بندی پیشنهاد، DOT های قفل شده به پیشنهاد دهندگان/حامیان بازگردانده می شوند.

لغو شده ها - اگر پیشنهادی برای زنجیره رله Polkadot خطرناک در نظر گرفته شود، می تواند توسط کمیته فنی لغو شود. اگر چنین پیشنهادی قبل از مشخص شدن ماهیت تهدید، به وضعیت رفراندوم برسد، اکثریت دو سوم شورا می تواند همه پرسی را لغو کند. اگر لغو رفراندوم بحث برانگیز باشد، تصمیم گیری به جامعه منتقل می شود. هنگامی که یک پیشنهاد یا رفراندوم لغو می شود، تمام توکن های سپرده شده به عنوان بخشی از اوراق قرضه آن سوزانده می شوند.

لیست سیاه - پیشنهادی که خطر قابل توجهی برای سیستم ایجاد می کند، به عنوان مثال، یک خطای کد گذاری می تواند توسط پروتکل در لیست سیاه قرار گیرد. یک پیشنهاد در لیست سیاه را نمی توان دوباره به صف اضافه کرد مگر اینکه اصلاح شده باشد.

5.آرا چگونه محاسبه می شود؟

برای محاسبه نتایج رفراندوم، دو مکانیسم اصلی وجود دارد که ارزش بررسی دارد.

ضریب محکومیت - این یک حوزه کلیدی از حاکمیت است که بیشترین نظریه های بازی را ایجاد می کند. این به این دلیل است که سیستمی که به شدت به اثبات استک ها متکی است، باید فرآیندهای مؤثری را برای یکسان کردن زمین بازی برای دارندگان توکن داشته باشد. در Polkadot، این عمل توسط ضریب محکومیت پشتیبانی می شود.

به عنوان مثال، فرض کنید که در همه پرسی فقط دو رأی دهنده وجود دارد: رأی دهنده G و رأی دهنده B.

رأی دهنده G با 20 DOT.

رأی دهنده B با 90 DOT.

به طور طبیعی، ما انتظار داریم که نظر رأی دهنده B برنده شود. وقتی ضریب محکومیت را معرفی می‌کنید، اینطور نیست. زیرا هم تعداد توکن‌های قفل شده و هم مدت زمان قفل در نتیجه نهایی لحاظ می‌شوند.

بیایید نگاهی عمیق‌تر به اعتقاد رای‌دهنده G و رأی‌دهنده B داشته باشیم.

رأی‌های G با 20 DOT برای 6 چرخه رأی‌گیری قفل باشد.

رأی‌های B با 90 DOT برای 1 چرخه رأی‌گیری قفل باشد.

براساس مشخصات بلاک چین Polkadot، یک چرخه رای گیری 4 هفته است و هر چرخه ضریب محکومیت را با نسبت 1 افزایش می دهد. بنابراین، در مثال بالا، نتیجه اینطور به نظر میرسد.

G = 20 x 6 = 120 DOTS

B = 90 x 1 = 90 DOTS

همانطور که می بینید، نظر رای دهنده G پیامدهای بیشتری خواهد داشت. زیرا او ضریب محکومیت بیشتری داشت. برای آشنایی بیشتر با این مکانیسم جالب، می توانید این مقاله ویکی را مطالعه کنید.

ما هنوز نمی دانیم که ضریب محکومیت تا چه حد قدرت رای گیری را بین اعضای جامعه، با تعداد کمی DOT و آنهایی که دارای پورتفولیوهای بسیار بزرگتر هستند، مجدداً متعادل می کند. بنابراین این راه حل ممکن است نیاز به تنظیمات بیشتری در آینده داشته باشد.

آخرین نکته ای که باید به آن توجه داشت این است که توکن هایی که برای رای دادن در همه پرسی یا نامزد کردن اعضای شورا استفاده می شوند، به طور موقت قفل هستند و نمی توان آنها را به حساب دیگری منتقل کرد، که هر گونه تلاش برای کار کردن، سیستم را پرهزینه می کند. با این حال، این DOT ها هنوز هم می توانند برای به دست آوردن پاداش های تولید بلاک استک شوند.

تعدیل حد نصاب - این یکی دیگر از حوزه های مهم حاکمیت زنجیره ای است که از تئوری عملکردها در طراحی خود استفاده گسترده ای می کند. بسته به اینکه کدام نهاد حاکمیتی این پیشنهاد را آغاز کرده است، سه راه مختلف برای تعیین نتیجه همه پرسی عمومی وجود دارد.

اکثریت ساده

اگر پیشنهادی با تصویب اکثریت شورا ارائه شود، برای تصویب یا شکست نیاز به اکثریت ساده «آری» یا «نه» دارد. صرف نظر از حضور رای دهندگان، اکثریت نتیجه نهایی رای گیری را تعیین خواهند کرد.

سوگیری مثبت مشارکت

برای همه پرسی که از طرح های تحت رهبری جامعه سرچشمه می گیرد، اوضاع کمی متفاوت است. در این مورد، مکانیسم رأی گیری دارای تعصبی درونی در برابر تغییرات پیشنهادی است که تنها در صورتی می توان آن را جبران کرد که حمایت مثبت قاطع جامعه وجود داشته باشد. اگر تعداد کمی از رای دهندگان حاضر شوند، میزان "آری" مورد نیاز برای ادامه ارتقاء به میزان قابل توجهی افزایش می یابد. به عنوان مثال، در جایی که 19٪ از اعضای جامعه رای خود را به صندوق می اندازند، ممکن است کمتر از 20٪ "نه" برای از بین رفتن 80٪ از "آری" ها لازم باشد.

این مجموعه برای محافظت از اکوسیستم در برابر کاربران مهاجمی طراحی شده است که پیشنهادهای بحث برانگیز را به این امید ارائه می دهند که مشارکت کم همه پرسی به نفع نتایج مورد نظر آنها منجر شود.

سوگیری منفی مشارکت

این مکانیسم هنگام شمارش آرای یک همه پرسی از یک پیشنهاد شورا به دست آمده است، استفاده می کند. در این سناریو، مکانیسم در مقابل رد پیشنهاد قرار می گیرد، به طوری که با تعداد کم رأی دهندگان، درصد «آری» مورد نیاز برای تصویب پیشنهاد پایین خواهد بود. به عنوان مثال، با مشارکت 30 درصدی، تنها 30 درصد «آری» برای سرنگونی 70 درصد «نه» مورد نیاز است. هدف اصلی در اینجا افزایش سرعت به روز رسانی فنی در شبکه است. اگر شورا و جامعه فنی به اتفاق آرا در مورد شایستگی یک پیشنهاد به توافق برسند، می توان فرض کرد که تغییرات پیشنهادی به اکوسیستم ارزش مضاعفی می دهد.

6.پس از رفراندوم چه اتفاقی می افتد؟

اگر یک رفراندوم شکست بخورد، هیچ چیز در زنجیره اتفاق نمی افتد. در صورت تصویب همه پرسی، تغییرات زنجیره ای به طور خودکار توسط سیستم پس از یک دوره انتظار 28 روزه اجرا می شود. این یکی از مزایای حاکمیت زنجیره ای است که در Polkadot کدگذاری شده است، که همچنین نشان می دهد که چرا داشتن گزینه لغو یا لیست سیاه پیشنهادات، مهم است.

با در نظر گرفتن تمام این پارامترهای اصلی، نیاز به اضافه کردن یک بخش دیگر را احساس می کنم.

انتقادات از مکانیسم حکمرانی Polkadot

زنجیره ی Polkadot انتقادهای زیادی را برانگیخته است. اغلب اوقات، این نظرات منفی ناشی از ناآگاهی است تا نظرات قوی در مورد موضوعات خاص. این بخش به رایج ترین انتقادات و یک رد پیشنهاد می پردازد.

1.این شکل دیگری از متمرکز سازی است/ سیستم متمرکز خواهد شد

برخی از مردم بر این باورند که یک فرآیند حاکمیتی قابل مشاهده و فعال فقط شکل دیگری از متمرکز سازی است که منتظر وقوع است. راستش من هم این ترس را دارم. گفته می‌شود، فرآیند حاکمیت واقعاً باعث تمرکز نمی‌شود، این کاربران هستند که این کار را انجام می‌دهند. در حال حاضر، بسیاری از مردم بر این باورند که اتریوم در هنگام تصمیم گیری کاملاً غیر متمرکز است، که این اعتقاد کاملاً درست نیست. اما بنیاد اتریوم با بودجه خود چه می کند؟ چگونه هزینه ها توسط جامعه کنترل یا ردیابی می شود؟ این به این معنی نیست که در پشت پرده چیز مبهمی در حال وقوع است. اینطور نیست. نکته اصلی من این است که هیچ کس در جامعه اتریوم از جزئیات کامل نحوه خرج کردن وجوه و اینکه چه کسی به این پیشنهادات هزینه پاسخ مثبت می دهد، چیزی نمی داند. این به معنای انتقاد از فرآیند اتریوم نیست، بلکه برای جلب توجه به این واقعیت است که اطلاعات برخی از عملکردهای آن نسبتاً مبهم است. بنابراین، چگونه ممکن است کسی واقعاً با داشتن یک روش شفاف تر برای انجام همان کار مشکل داشته باشد؟ من فقط به برخی از جنبه هایی اشاره می کنم که ممکن است نادیده گرفته شود یا آنها را بدیهی تلقی کنیم.

وقتی صحبت از پیشرفت‌های مرتبط با شبکه می‌شود، به طور گسترده پذیرفته شده است که ایده‌های Vitalik Buterin نقشه راه اکوسیستم اتریوم را هدایت می‌کنند. سایر شرکت‌کنندگان اغلب از ایده‌های او در پروژه‌های جدید حمایت می‌کنند، در حالی که اقلیتی از منتقدان قبل از اینکه تغییرات در نهایت توسط ماینرها اجرا شود، به نقص‌ها اشاره می‌کنند. این روند در عمل خوب است، اما می تواند بسیار کند باشد و شفافیت ندارد. همانطور که همان ابتدا در مورد Polkadot گفته می شد، اکنون می توانیم همه تغییرات را تأیید کنیم زیرا همه چیز در زنجیره است.
اگر خزانه ای وجود دارد، جامعه باید بداند چگونه خرج می شود و اگر وجود نداشته باشد، آیا جامعه از داشتن آن سود نمی برد؟ در حال حاضر، هیچ خزانه داری رسمی اتریوم یا بیت کوین وجود ندارد که بتواند همانطور که یک خزانه داری زنجیره ای برای پشتیبانی از تحولات اکوسیستم در دسترس است، منابع مالی را به صورت باز و قابل تایید برای اعضای جامعه تامین کند. فراتر از تامین مالی، بدیهی است که فرآیندهای تصمیم گیری در حال حاضر در دستان یک بنیاد متمرکز است. من شخصاً هیچ تقصیری در این موضوع نمی‌بینم، زیرا تصور اینکه افرادی که سیستمی را ساخته‌اند برای نابودی آن برنامه‌ریزی کنند، دشوار است. به همین دلیل است که ما به طور ضمنی به بنیانگذاران پروژه اعتماد داریم. اما من همچنان طرفدار فرآیندهای زنجیره ای به عنوان راهی برای اتخاذ تصمیمات غیرمتمرکز پایدار مرتبط با شبکه هستم.

در پایان، اگر جامعه ای بهتر می خواهیم، جامعه ای که بازتاب جامعه کنونی باشد اما با قوانین عادلانه تر، به بلاک چین نیاز داریم. این به این دلیل است که بلاک چین ابزاری است که می‌توانیم از آن برای اصلاح یا بهبود سیستم‌های حاکمیتی خود استفاده کنیم. اشتباهات زیادی اتفاق خواهند افتاد و درس های زیادی آموخته خواهند شد، اما در مجموع، آزمایش کردن به مراتب بهتر از انجام ندادن هیچ کاری است.

2.به کاربران مخرب (یا تازه کارها) فرصت آسیب رساندن به شبکه را می دهد

این یک نگرانی قانونی است و خوشبختانه در طراحی حکومت Polkadot به آن توجه شده است. هر کاربر بدی که بخواهد شبکه را از طریق حاکمیت نابود کند، باید مایل به خرج کردن پول (DOT) زیادی باشد. این بدان معناست که هرکسی که می‌خواهد رأی‌ها را به سمت یک نتیجه منفی سوق دهد باید:

1. تعداد زیادی از دارندگان DOT را متقاعد کند که با DOT خود تصمیم بدی بگیرند، یا
2. تصمیم بد خود را تامین مالی کند

هر یک از این سناریوها از نظر بودجه و منابع بسیار پرهزینه خواهد بود. اما اگر یک مبتدی به اشتباه پیشنهاد خطرناکی را ارائه کند، همیشه در سیستم حاکمیت ایست های بازرسی وجود دارد که امکان اصلاح یا لغو را فراهم می کند.

3.برای یک فرد معمولی، این موضوع خیلی پیچیده است

می توانم در این مورد با مردم کاملاً همدلی کنم. حکمرانی سنتی در حال حاضر به قدری پیچیده است که زمینه های آکادمیک خاصی وجود دارد تا در مورد آن به ما آموزش دهند. بنابراین انتظار می رود یک فرآیند حکمرانی که هدف آن غیرمتمرکز سازی کامل است، درس های زیادی از جمله علوم سیاسی، تاریخ، و تئوری بازی ها را در طراحی خود بگنجاند و در نتیجه آن را پیچیده کند. گفته میشود که شما نمیتوانید قانون اساسی کشور خود را با خواندن تنها یک سری از پست های وبلاگ ها به خوبی درک کنید. همانطور که این امر به تلاش زیادی نیاز دارد، درک فرآیند فوق نیز به همان اندازه تلاش نیازمند است.

در مورد Polkadot، تنها چیزی که باید بدانید این است که نقش‌ها و فرآیندهای خاصی وجود دارد که اطلاعات مربوط به آنها بسیار کمتر از یک سند 300 صفحه‌ای است. مانند هر فناوری دیگری، درک چیزی به سادگی به این معناست که بتوان از آن استفاده کرد و بیشترین بهره را برد. درست همانطور که یک انسان معمولی می تواند در مورد یک شورای شهر معمولی بیاموزد، درک اینکه یک شورای زنجیره ای چه کاری می تواند انجام دهد چندان هم سوال سختی نخواهد بود. مسلماً، با کمی درک بیشتر می‌توان برای ساده‌سازی توضیحات فرآیندهای حاکمیتی و رابطهای موجود در حال حاضر اقداماتی انجام داد.

4.متمرکزسازی به معنای عدم حاکمیت است- اتریوم و بیت کوین به خوبی کار می کنند

این انتقاد چندان معتبر نیست زیرا قرار است به همان روشی که اتریوم کلاسیک و بیت کوین کش از زنجیره های اصلی خود جدا شدند، فناوری ها در جهات مختلف تکامل یابند. در حال حاضر، حاکمیت زنجیره ای راهی برای حل تعارض بدون افراط و تفریط و با ارائه ابزارهای قابل تأیید برای رسیدن به هدف ارائه می دهد. به استثنای بیت کوین، اکثر پروژه های غیرمتمرکز دارای بنیاد مولد هستند. اما در این زمینه، اگر گروهی از افراد که در مدیریت موفقیت بلند مدت شبکه، به آنها اعتماد داریم وجود نداشته باشند، بنیاد مولد چه خواهد بود؟ ما واقعاً نمی‌توانیم شاهد چگونگی تصمیم‌گیری‌ها و اقداماتی که در به‌کارگیری این تصمیم‌ها انجام می‌شود، باشیم. ما یک پست وبلاگ اینجا و آنجا با توضیحات مبهم دریافت می کنیم، اما تعداد آرا را نمی بینیم. حال، این بدان معنا نیست که رأی برای اعتبار یک تصمیم ضروری است، بلکه فقط نشان می دهد که ما به تصمیم هایمان ، بدون هیچ داده واقعی برای تأیید مشروعیت آنها ، اعتماد زیادی داریم. در حالی که، در سیستم های بلاک چین غیرمتمرکز، اعتماد تنها به اندازه داده های قابل تاییدی است که روی زنجیره ثبت می شود.

4.اتکای بیش از حد به DOT وجود دارد و شبکه همیشه در اختیار دارندگان بزرگ است

این یکی دیگر از نگرانی های مشروعی است که در گذشته مجبور بودم به شدت درباره آن فکر کنم. اول، چند جنبه وجود دارد که باید آنها را در نظر بگیریم:

1. هر کسی که DOT های بیشتری برای از دست دادن دارد، اگر تصمیمات حاکمیتی بر اکوسیستم تأثیر منفی بگذارد، چیزهای بیشتری از دست خواهد داد. بنابراین، این موضوع نگهدارنده انگیزه برای حمایت از تغییراتی است که برای اکوسیستم بهترین هستند.
2. Polkadot محدودیت های حکمرانی مبتنی بر توکن را تشخیص داده است و راه حلی را برای دور زدن این مسائل پیشنهاد می کند. این سازوکار را معرفی کرده است که به صاحبان کوچک اجازه می دهد تا به آرای خود اهمیت بیشتری دهند.
3. اگر شبکه در جهتی که شما مطلوب می دانید در حال تکامل نیست، شما همیشه آزاد هستید که از اکوسیستم خارج شوید.

اتکای بیش از حد به DOT برای ایمن سازی آینده ی شبکه مورد نیاز است. **اثبات استک**، اثبات سهام است. اگر با استفاده از مکانیسم‌های اثبات استک، امنیت شبکه را بهبود می بخشیم، چرا باید نگران تطبیق آن با حاکمیت باشیم؟ سوال واقعی این است: آیا راه بهتری برای دستیابی به اجماع در مورد تصمیمات حاکمیتی با حفظ عملیات در زنجیره

وجود دارد؟ همچنین ممکن است اگر جامعه بعداً این مرحله را ضروری بداند، اتکای ما به توکن‌ها در نهایت تغییر کند و این زیبایی فرآیندهای حکومتی Polkadot است.

6.مشکلی پیش خواهد آمد، به هر طریقی

ما تمایل داریم نسبت به چیزهای جدید یا ناشناخته تعصب منفی داشته باشیم. من خودم تقریباً در هر موقعیتی می‌توانم بدترین پیامدها را تصور کنم، بنابراین طبیعی است که احتمال وقوع اتفاقی غیرقابل پیش‌بینی در جریان حکومت بر Polkadot را در نظر بگیرم. با این حال، وجود ***یک فرآیند حاکمیتی*** هنوز به من دلایلی برای مثبت ماندن می دهد، زیرا هر اتفاقی که بیفتد، دارندگان DOT می توانند به طور جمعی در مورد مسیر اقدام ترجیحی برای شبکه تصمیم بگیرند و اگر یک ارتقای پیشنهادی جامعه را به دو قسمت تقسیم کند و به بن بست برسیم، آنگاه یک آزمایش واقعی برای انعطاف پذیری شبکه خواهیم داشت.

در مجموع، حکومت زنجیره ای Polkadot یکی از قوی ترین ها در این فضا است. زیرا علوم سیاسی، روانشناسی انسانی و تئوری اقتصادی را در طراحی و اجرای خود گنجانده است. یکی از نکات مهم این است که همه چیزهایی که تا کنون نوشته‌ام ممکن است تغییر کند، زیرا همه چیز در اکوسیستم Polkadot بسیار سریع پیش می‌رود و تقریباً هر پارامتر سیستم را می‌توان توسط شرکت‌کنندگان تنظیم کرد. این چیز خوبی است، زیرا اگر فرضیات اشتباه در مرحله طراحی انجام شده باشد، می توان آنها را در نسخه بعدی سیستم اصلاح کرد. فقط زمان می‌تواند نشان دهد که چه اشتباهاتی انجام داده‌ایم، بنابراین منطقی است که به خود فرصت مشاهده و تأمل را در این بین بدهیم.

نوع جدیدی از خزانه داری

یکی از مزیت های فرآیند حاکمیت زنجیره ای این است که جامعه می تواند از خزانه پروتکل حداکثر استفاده را ببرد. در Polkadot، خزانه داری زنجیره ای توسط شورا مدیریت می شود و تنها هدف آن تقویت، حفظ و رشد اکوسیستم است. از طریق اجزای مختلف به این هدف دست می یابد:

بونتی

محدودیت های عملی در برابر توانایی های اعضای شورا در مورد پیشنهادهای خزانه داری وجود دارد. بسیار بعید است که اعضای شورا همیشه از تخصص لازم برای ارزیابی مناسب از فعالیت های شرح داده شده در همه پیشنهادها برخوردار باشند، بنابراین باید راهی وجود داشته باشد که شورا نظارت بر پیشنهادات را به کارشناسان محول کند.

بونتی پاداشی است برای مجموعه مشخصی از کارها - یا مجموعه مشخصی از اهداف - که باید برای آن مبلغی از پیش تعریف شده به خزانه پرداخت شود. این می تواند توسط هر دارنده DOT، که یک پیشنهاد دهنده نامیده می شود، آغاز شود. هنگامی که پیشنهاد دهنده جایزه ای را پیشنهاد کرد، اجرای پروژه و تأیید آن بر عهده یک متصدی جایزه است. متصدی جایزه می تواند یک شخص یا گروهی از افراد با نمایندگی ای که در بخش محدودی از خزانه تعریف شده تا برای یک هدف خاص استفاده شود، باشد. این می تواند برای رفع یک باگ یا آسیب پذیری، توسعه یک استراتژی، یا نظارت بر مجموعه ای از وظایفی باشد که برای اکوسیستم Polkadot مفید است.

متصدیان پس از تصویب پیشنهاد جایزه، توسط شورا انتخاب می شوند. قبل از تأیید، متصدیان باید برای پذیرش نقش جدید خود وجهی را واریز کنند تا در صورت اقدام بدخواهانه، از بازگشت وجوه به منظور مجازات آنها جلوگیری شود. با این حال، اگر آنها در انجام وظیفه خود برای تکمیل جایزه موفق باشند، سپرده خود و همچنین پاداش جایزه را دریافت خواهند کرد.

((درج تصویر)) از پروسه بونتی

هزینه های پیشنهادی

در حالی که پاداش ها وظایف خاصی را به منظور تکمیل شدن تعریف می کنند، هزینه های پیشنهادی باز تر است. یک پیشنهاد می تواند در جهت ایجاد زیرساخت، آموزش جامعه، ساختن یک پروژه جدید، ایجاد ابزار یا بازاریابی اکوسیستم باشد. تا به امروز، بیش از 100 پیشنهاد مستقل توسط خزانه داری Polkadot تامین مالی شده است، از جمله ایجاد این کتاب. تفاوت اولیه بین یک پیشنهاد هزینه و یک جایزه در این است که پیشنهاد مورد نظر توسط پیشنهاد دهنده آن اجرا می شود.

انعام

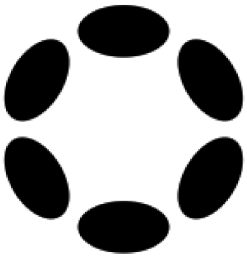
این بخش مثل راهی است که اعضای جامعه به سایر اعضای جامعه به خاطر تلاش هایشان در جهت حفظ و رشد اکوسیستم پاداش می دهند. هر دارنده DOT می تواند برای هر عضوی که کار شایسته ای برای انتقال انجام داده است، انعام درخواست کند. به عنوان مثال، من یک بار توسط یکی از اعضای جامعه برای مقاله ای که در مورد حکومت Polkadot نوشتم، نامزد دریافت انعام شدم.

تامین مالی خزانه

وجوه خزانه داری از منابع مختلفی تامین می شود:

1. **تخفیف ها:** زمانی که اعتبار دهنده به هر دلیلی تخفیف زیادی اعمال کند، مبلغ کاهش یافته به خزانه داری ارسال می شود و به نهادی که اعتبار دهنده را گزارش کرده است پاداشی تعلق میگیرد، که اغلب اعتبار دهنده دیگری است. این پاداش از مقدار تخفیف گرفته می شود و بسته به ماهیت کاهش و تعداد گزارشگران متفاوت خواهد بود.
2. **کارمزد تراکنش:** بخشی از کارمزد تراکنش های هر بلوک به خزانه داری می رود و مابقی به نویسنده بلوک می رسد.
3. **ناکارآمدی سهام:** تورم در سال اول 10 درصد طراحی شده است و نرخ ایده آل سهام 50 درصد کل عرضه تعیین شده است. این به این معنی است که نیمی از تمام توکن‌های موجود باید در حالت ایده‌آل قفل شوند تا تورم به‌عنوان پاداش به طور کامل به اعتبار دهنده‌ها برسد. اگر نرخ سهام به زیر 50٪ کاهش یابد، اعتبار دهنده مبلغ کمتری دریافت می کند و مابقی به خزانه داری می رود.
4. **پاراتریدها:** پاراتریدها در حراج هر بلوک، برای گنجاندن بلوک شرکت می کنند. بخشی از مبلغ پیشنهادی آنها به اعتبار دهنده که بلوک را می پذیرد می رود و مابقی به خزانه داری می رود.

برای جزئیات بیشتر در مورد خزانه داری، می توانید این مقاله ویکی Polkadot را بخوانید.



فصل 5

گسترش شبکه

پس از مشاهده ساختار شبکه، اکنون می‌خواهیم به چگونگی گسترش شبکه از طریق پاراچین ها و ارزش پیشنهادی نهایی Polkadot، نگاهی بیاندازیم. بدون پاراچین ها، زنجیره رله فقط یک شبکه اسکلت است که محدود به عملکردهای ردیابی و حاکمیت است. در مقابل، پاراچین ها را می‌توان هر طور که تیم ساختمانی می‌خواهد طراحی کرد: با یا بدون کارمزد تراکنش، بلوک‌های بزرگتر یا کوچکتر. به طور خلاصه، هر پاراچین کشوری بعنوان برای خودش در نظر گرفته میشود و شما می توانید زنجیره رله را به عنوان شبکه ای در نظر بگیرید که جاده ها و مسیرهای دریایی را که هر یک از این کشورهای مختلف را به هم متصل می کند، ترسیم می کند. هر پاراچین همچنین یک بلاک چین لایه-1 قابل تنظیم است و می تواند در دسته های زیر قرار گیرد:

- شبکه عمومی لایه-1
- شبکه خصوصی لایه-1
- راه حل های مقیاس بندی لایه-2
- پل

این موضع به این دلیل امکان پذیر است که زنجیره رله هیچ پیش فرضی در مورد اجزایی که به آن متصل می شود ندارد. تا زمانی که با استفاده از زبان های برنامه نویسی که توسط Substrate پشتیبانی میشوند ساخته شده باشند، آنها را همانطور که هستند می پذیرد. Substrate چارچوبی برای ساخت بلاک چین های مدرن است که توسط Parity Technologies، شرکتی که توسط W3F مأمور ساخت Polkadot شده بود، ایجاد شده است. بنابراین هر بلاک چین یا شبکه ای که با Substrate ساخته شده است با زنجیره رله Polkadot سازگار است.

اما واقعاً پاراچین چیست؟ یکی بودن یعنی چی؟ پاراچین ها مانند فرزندان یک زنجیره رله هستند زیرا با قدرت اقتصادی زنجیره رله والد خود ایمن شده اند و همچنین می توانند از منابع محاسباتی اعتبار دهنده های زنجیره رله برای عملیات زنجیره ای متقابل استفاده کنند. مزایای پاراچین نسبت به بلاک چین های استاندارد لایه-1 دو جنبه دارد:

- امنیت مشترک
- قابلیت همکاری

مفهوم امنیت مشترک باید تا کنون درک شده باشد، بنابراین اکنون می‌توانیم بر قابلیت همکاری متمرکز شویم، که به عنوان جام مقدس فناوری بلاک چین در نظر گرفته می‌شود.

قابلیت همکاری پاراچین

من معتقدم که قابلیت همکاری، همان ویژگی قاتل بودن در Polkadot است. اگر با بلاک چین آشنایی ندارید، ممکن است این برای شما چندان منطقی نباشد، اما من سعی خواهم کرد توضیح دهم که چرا قابلیت همکاری پاراچین، کلید نوآوری نامحدود در فضای بلاک چین است.

امور مالی غیرمتمرکز و مالکیت دیجیتال غیرمتمرکز (از طریق NFT ها) به لطف قابلیت همکاری و ارتباطات غیرقابل اعتماد بین سیستم‌ها/شبکه‌های خودکار مختلف، به نیروگاه‌هایی تبدیل شدند که امروزه میبینید. معمولاً هنگامی که توکن‌ها از یک پلتفرم به پلتفرم دیگری منتقل می‌شوند و بالعکس، از طریق یک پل، پلتفرم‌های بلاک چین قابلیت تعامل دارند.

به عنوان مثال، اگر بخواهم بیت کوین را به اتریوم بفرستم، تنها کاری که باید انجام دهیم این است که به برنامه بریج رفته و انتقال را انجام دهم. اکنون این یک عملیات بسیار ساده است که می تواند با چند کلیک کامل شود. چیزی که من نمی بینم این است که توکن هایی که از بیت کوین به اتریوم منتقل کردم از نظر فنی هنوز در شبکه بیت کوین هستند. دلیل آن هم این است که روش انتقال پل به این صورت است که توکن‌های BTC من را با ارسال آنها به یک آدرس خاص در شبکه بیت‌کوین مسدود می‌کند، مجموعه جدیدی از توکن‌های مشتق به نام «BTC Wrapped» را در شبکه اتریوم برش می‌دهد و توکن‌های BTC پیچیده شده را به حساب اتریوم خودمان ارسال می کند.

همانطور که گفتم، این یک فرآیند ساده است، اما قابلیت همکاری آنطور که در Polkadot پیاده سازی شده است، نخواهد بود.

دو جنبه برای تعامل وجود دارد:

1. ارسال نشانه ها و پیام ها
2. فراخوانی توابع

امروزه، جنبه اول بسیار پیش پا افتاده است، اما دومی نسبتاً ناشناخته است. برای اینکه بلاک چین

A تابعی از بلاک چین B را فراخوانی کند، باید عملیات بین بلاک چین A و بلاک چین را خودکار کنیم. تا نیاز به واسطه های انسانی را از بین ببریم. در چنین تنظیماتی، بلاک چین A یک قرارداد هوشمند روی بلاک چین B فراخوانی می کند، که به نوبه خود به بلاک چین A پاسخ می دهد و هر اطلاعاتی را به آن می دهد یا هر محاسباتی را که درخواست می شود اجرا می کند.

بیایید از مثال عملی دیگری برای درک این مفهوم استفاده کنیم.

یک کاربر درخواست می کند که از NFT ارزشمند ذخیره شده در زنجیره B به عنوان وثیقه در زنجیره A، یک زنجیره متمرکز بر DeFi، برای گرفتن وام استفاده کند. اما قبل از اینکه زنجیره A بتواند این درخواست وام را بپذیرد، باید چند مورد را تایید کند:

1. آیا کاربر همانی است که می گوید؟
2. آیا کاربر دارای NFT است؟
3. ارزش واقعی NFT چقدر است؟

جدای از این سؤالات، زنجیره A همچنین نیاز به موارد زیر دارد:

1. یک NFT برای نشان دادن موقعیت وام
2. ارسال توکن ها به زنجیره B

برای جمع آوری تمام این داده ها، زنجیره A باید با زنجیره های دیگر تعامل کند.

- برای دانستن هویت واقعی کاربر، زنجیره A با هویت زنجیره C تعامل می‌کند، که تأیید می‌کند کاربر واقعاً همان کسی است که می‌گوید و واجد شرایط دریافت وام است.
- برای تأیید اینکه این کاربر وام معوقی ندارد، CChain A با دو زنجیره DeFi دیگر که شرکای آن هستند، بررسی های متقابل انجام می دهد.
- برای بررسی اینکه کاربر واقعاً مالک این NFT است، زنجیره A به سمت راستی‌آزمایی اطلاعات با زنجیره B می‌رود.

- برای ارزیابی ارزش این NFT و تأیید اینکه آیا نسبت‌های وثیقه مناسب هستند، زنجیره A یک قرارداد هوشمند را در زنجیره D، یک زنجیره پیش‌بینی، آغاز می‌کند. این زنجیره پیش‌بینی مجموعه ای از پیش بینی کننده ها و ارزیابان خود را برای تحلیل ارزش واقعی NFT تشویق می‌کند.
- با تأیید اینکه همه چیز خوب است، زنجیره A اقدام به جمع‌آوری NFT می‌کند و آن را در صندوق NFT خود در زنجیره B قفل می‌کند، در حالی که توکن‌های درخواستی را به کاربر می‌دهد و شروع به جمع‌آوری بازپرداخت‌های نرخ بهره می‌کند.

توجه داشته باشید که من مراحل بیشتری از آنچه برای چنین تراکنشی لازم است را برای اهداف توصیفی اضافه کرده ام.

بنابراین، می بینیم که دو نوع قابلیت همکاری وجود دارد - قوی و ضعیف. با قابلیت همکاری ضعیف، کاربر باید تمام این عملیات را به صورت مجزا انجام دهد و چندین تراکنش را در زنجیره های مختلف امضا کند. با قابلیت همکاری قوی، یک زنجیره می‌تواند از ویژگی‌های زنجیره‌ای متقاطع مانند هویت، پیش‌بینی و خزانه‌های زنجیره‌های دیگر برای ایمن کردن عملیات خود و ارائه تجربه کاربری بهتر استفاده کند.

اکنون، با توجه به مزایای قدرتمند پاراچین ها نسبت به سایر بلاک چین های لایه-1، می توانیم درک کنیم که چرا رقابت شدیدی برای اسلات های پاراچین وجود دارد. از آنجایی که زنجیره رله نمی تواند تعداد بی نهایت پاراچین داشته باشد – منابع آن محدود است، طبق نقل قول از وایت پیپر Polkadot، تنها در حدود 100 پاراچین را در حدود یک دهه آینده پشتیبانی خواهد کرد. که این یک چالش جدید را بوجود می آورد: چگونه تعیین کنیم که چه کسی اسلات پاراچین را دریافت می کند؟

مزایده ها و وام های جمعی اسلات پاراچین

در شرایطی که تعداد کمی از اقلام با ارزش برای فروش موجود است اما تقاضای زیادی از سوی خریداران وجود دارد، معقول ترین راه برای توزیع آنها از طریق حراج است، زیرا این روش تضمین می کند کسانی که ارزش بیشتری برای محصول قائل هستند در نهایت صاحب آن خواهند شد. برای Polkadot، یک سیستم غیرمتمرکز با امنیت فنی و اقتصادی و یافتن بهترین راه برای توزیع منابع شبکه گرانبهای آن بسیار مهم است. این زمانی است که حراج های اسلات پاراچین (PSA) وارد عمل می شود. PSAها مکانیزمی قوی هستند که به تخصیص اسلات‌های پاراچین به بالاترین پیشنهاد در میان پروژه‌های مختلف کمک می‌کنند. جزئیات کامل نحوه دستیابی به این امر در زیر خلاصه شده است.

هر حراج اسلات پاراچین، 1 هفته در Polkadot ادامه دارد. در این هفته تیم های پاراچین یشنهادات خود را ارائه می دهند. در پایان مهلت مزایده، یک برنده مشخص می شود. اگر چه، رویه های واقعی کمی پیچیده تر هستند.

هر هفته حراج اسلات پاراچین به 2 مرحله تقسیم می شود: مرحله افتتاحیه و مرحله پایانی. این دو مرحله ضروری هستند. زیرا Polkadot از یک مکانیسم جدید روی زنجیره، با الهام از "حراج شمعی" استفاده می کند. به طور سنتی، اجرای یک حراج شامل تنظیم یک تایمر و اجازه دادن به فرصت دادن به قیمت های پیشنهادی تا اتمام زمان است: این مشابه چیزی است که می توانید در Ebay ببینید. با این حال، از آنجایی که Polkadot برای به حداکثر رساندن امنیت اقتصادی شبکه خود کار می کند، این سبک از حراج یک مشکل بزرگ ایجاد می کند. زیرا پیشنهاد دهندگان را تشویق نمی کند تا بهترین پیشنهادات خود را زودتر ارائه دهند و سیستم را در معرض تک تیراندازان (خبرگان) حراج قرار می دهد.

به عنوان مثال، باب می‌خواهد برای یک نقاشی با 40000 دلار پیشنهاد بدهد، اما تصمیم می‌گیرد که از 15000 دلار شروع کند تا بازار را احساس کند. وقتی پیشنهاد او پیشی گرفت، 500 دلار دیگر اضافه می کند و دوباره پیشنهاد می دهد. پس پیشنهاد او یک بار دیگر سبقت می گیرد، بنابراین او باید به افزایش قیمت ادامه دهد، تا زمانی که تایمر به 3 ثانیه آخر برسد و باب با 28000 دلار برنده شود. متأسفانه، در آخرین ثانیه، آلیس پیشنهاد باب را با پیشنهاد 28500 دلاری خودش قطع می کند و باب در حراج بازنده می شود. اما فاجعه واقعی این است که با توجه به اینکه 28500 دلار بسیار کمتر از بودجه واقعی 40000 دلاری باب است، هنرمند ارزش بیشتری را برای نقاشی از دست می دهد. برای جلوگیری از چنین اقداماتی، "حراج شمعی" در حدود قرن 17-18 ابداع شد. در مرحله

پایانی حراج، برخی رندوم ها و عدم قطعیت‌ها را به بازی گرفت: شرکت‌کنندگان تشویق شدند تا بهترین پیشنهادهای خود را زودتر ارائه دهند، زیرا اگرچه می‌توانستند نقطه شروع حراج را تشخیص دهند، یعنی زمانی که شمع روشن می‌شود، ولی هرگز نمی‌توانستند زمان خاموشی شمع را حدس بزنند که به نشانه پایان حراج بود.

در حال حاضر، اجرای حراج شمع بر روی یک بلاک چین یک امر بی اهمیت نیست، زیرا بلاک چین ها برای پیشنهادات تصادفی ساخته نشده اند. راه‌حل Polkadot، معرفی حراج‌های دو مرحله‌ای و «زمان پایان تصادفی مثل گذشته» است که در مرحله دوم حراج‌ها وارد عمل می‌شود.

در مرحله افتتاحیه که 2 روز به طول می انجامد، پروژه ها پیشنهاداتی را ارائه می دهند که به صورت زنجیره ای ثبت شده و تا پایان مزایده ادامه خواهد داشت. آن‌ها آزادند به اندازه‌ای که فکر می‌کنند برای برنده شدن لازم است، پیشنهاد بدهند، اما همچنین باید مراقب باشند که خزانه‌های خود را از بین نبرند. در مرحله پایانی که 5 روز به طول می‌انجامد، همه پیشنهادات در روز(های) پایانی می‌توانند باطل شوند زیرا زنجیره رله از یک تابع تصادفی قابل تأیید برای انتخاب لحظه پایان حراج معطوف به گذشته استفاده می‌کند. بنابراین، این کاندیدای پاراچین است که در زمان دقیق پایان حراج بیشترین پیشنهاد را دارد و برنده خواهد بود. نتیجه اینکه ممکن است زنجیره رله تصمیم بگیرد که حراج در روز سوم در بلوک شماره 123456 به پایان برسد. این بدان معناست که کاندیدای پاراچین که بالاترین پیشنهاد را پس از بلوک شماره 123456 ارائه کرده است، قطعاً حراج را بازنده خواهد شد. به همین دلیل است که مرحله شروع کردن مهم است. زیرا زنجیره رله همیشه تمام پیشنهادات ارائه شده در مرحله باز بودن را در نظر می گیرد. یک اسلات پاراچین می تواند بسته به تعداد دوره های اسلاتی که تیم برای پروژه خود انتخاب می کند، از 3 ماه تا 2 سال در 1) Polkadot سال در Kusama) باشد. این یک پویایی جالب دیگر را به مزایده ها معرفی می کند. زیرا زنجیره رله اکنون باید هنگام انتخاب برنده شرایط زیر را در نظر بگیرد:

- درآمد اقتصادی را به حداکثر برساند (تیم‌ها را وادار کند تا حد امکان DOT یا KSM پیشنهاد بدهند)
- مدت زمان اسلات را به حداکثر برساند (تیم‌ها را وادار کند تا هرچه بیشتر دوره‌های اسلات پیشنهاد بدهند)

این بدان معناست که آن کاندیدای پاراچینی که بالاترین پیشنهاد کلی را دارد، اما برای کوتاه‌ترین مدت زمان اسلات موجود، از نظر زنجیره رله در مقایسه با کاندیدای پاراچینی که دومین قیمت کلی بالاتر را برای طولانی‌ترین مدت زمان اسلات موجود دارد، مطلوبیت کمتری خواهد داشت. با این حال، توجه داشته باشید که مدت زمان اسلات به دوره‌های اسلاتی نیز بستگی دارد و باید در زمانی که پروژه به آن‌ها نیاز دارد در دسترس باشند. بنابراین این سناریوی ایده آل ممکن است همیشه اجرا نشود.

بدست آوردن اسلات پاراچین می تواند یک امر بسیار پرهزینه باشد. اولین اسلات پاراچین در کوساما 500000 KSM (حدود 90 میلیون دلار) بود که برای غیر متمرکز سازی ایده‌آل نیست، زیرا تعداد کمی از تیم‌ها می‌توانند به‌طور واقع بینانه از عهده پرداخت این مقدار از اجاره دیجیتال برآیند. برای یکسان کردن زمین بازی، Polkadot یک ماژول وام های جمعی ایجاد کرده است که به تیم های پاراچین امکان می دهد DOT ها را از جوامع خود تهیه کنند. این شبیه به دور تامین مالی است، با چند تفاوت قابل توجه:

- توکن‌هایی که جامعه قفل می‌کند به تیم‌های پاراچین داده نمی‌شود. در عوض توسط زنجیره رله نگه داشته می شوند. آن ها را به عنوان سهام بدون پاداش در نظر بگیرید.
- اگر تیم در حراج برنده نشد، توکن ها به مشارکت کنندگان بازپرداخت می شوند.
- اگر تیم برنده حراج باشد، توکن ها برای مدت اجاره روی زنجیره رله چسبانده می شوند. در پایان این دوره اجاره، توکن ها به مشارکت کنندگان وام جمعی بازگردانده می شود.

تیم‌های کاندید پاراچین اغلب برای تشویق اعضای جامعه برای مشارکت در وام‌های جمعی خود در طول حراج‌های اسلات پاراچین ، سهمی از عرضه توکن اصلی خود را به همراه سایر مزایا مانند NFT، توکن‌های مشتق، نرخ‌های پاداش و نقش‌های اجتماعی ویژه به مشارکت‌کنندگان ارائه می‌کنند. برای اعضای انجمن، این به یک سناریوی برد-برد تبدیل می‌شود و تنها ضرری که متحمل می‌شود، پاداش است، زیرا توکن‌های مورد استفاده برای وام‌های جمعی پاراچین و حراج‌ها واجد شرایط شرطبندی پاداش نیستند.

وقتی مکانیسم حراج شمع و ماژول وام های جمعی را کنار هم قرار می‌دهیم، متوجه می‌شویم که Polkadot برای یک جهش بی‌سابقه از نوآوری و گسترش آماده است. من این را به دلایل زیر می گویم:

1. اسلات های پاراچین باید با کمک جامعه به دست بیایند، که تضمین می کند که "بهترین تیم ها" ابتدا به موفقیت خواهند رسید. منظور من از «بهترین تیم‌ها» تیم‌هایی است که می‌توانند هم در زمینه فناوری و هم در تعامل با جامعه عمل کنند. زیرا ممکن است بهترین تیم‌های فناوری تحت الشعاع تیم‌های ضعیف‌تر فناوری قرار بگیرند که درک محکم‌تری از جامعه‌سازی دارند.
2. اسلات پاراچین باید در نهایت تجدید شود، که این امر تضمین می کند تا تیم ها بر ارائه خدمات بهتر به جامعه خود و افزایش خزانه های خود برای غلبه بر اتکا به وام های جمعی تمرکز خواهند کرد. طبیعتاً برخی از پروژه ها نمی توانند جایگاه پاراچین خود را تمدید کنند و این هم خوب است و هم بد. برای پاراچینی بد است که خدمات خود را کاهش می دهد یا متوقف می کند. اما برای اکوسیستم خوب است. زیرا تضمین می کند که هیچ پاراچینی دارای اسلات دائمی نباشد، مگر اینکه ارزش مورد نیاز برای ادامه کار را ایجاد کند.

یکی دیگر از جنبه های هیجان انگیز این طراحی، تنوع پروژه های پاراچین است. به عنوان مثال، اگر 3 زنجیره DeFi در حال رقابت باشند، بعید است که همه آنها موفق باشند. درعوض، تنها 2 نفر ممکن است با ایجاد درآمد کافی و حسن نیت جامعه، جایگاهی به دست آورند. در این حالت، پاراچین سوم به پاراترید تنزل پیدا می کند، در حالی که سایر پروژه های غیر DeFi در شبکه به فعالیت خود ادامه می دهند. توجه داشته باشید که این فقط یک حدس و گمان تئوری است: نکته ای که من به آن توجه می کنم این است که این طراحی تنوع را در بین نامزدهای پاراچین ترویج می کند.

نگاهی کوتاه به پاراتریدها

با توجه به اینکه جایگاه های پاراچین محدود هستند، هر نامزدی با موفقیت به وضعیت پاراچین دست پیدا نمی کند. همچنین، تبدیل شدن به پاراچین ممکن است لزوما برای برخی از پروژه ها مناسب نباشد. از آنجایی که پاراچین ها به زنجیره رله دسترسی بی‌وقفه دارند و می‌توانند هر زمان که بخواهند بلوک‌ها را ارسال کنند، مطلوب هستند. پروژه‌هایی که به چنین منابعی نیاز ندارند بهتر است به یک پاراترید تبدیل شوند. می‌توانید پاراچین ها را به‌عنوان یک سرویس اشتراک در نظر بگیرید، در حالی که پاراتریدها به‌صورت پرداختی هستند.

در زمینه Polkadot، این مدل به دو دلیل ایده‌آل است:

- برای پروژه‌ها ساده است که عملیات پاراچین خود را متوقف کنند. زیرا مجبور نیستند اتصال خود را به زنجیره رله کاملاً از دست بدهند.
- ممکن است پروژه هایی که قادر به دریافت اسلات Parachian نیستند همچنان از امنیت مشترک Polkadot بهره مند شوند.

پاراتریدها چگونه کار می کنند

برخی از اسلات های پاراچین در زنجیره رله برای اجرای پاراترید رزرو می شوند. این اسلات‌های ویژه به نام «ابزار پارترید»، میزبان پروژه‌هایی هستند که می‌خواهند به پاراترید ها تبدیل شوند. برای افزودن یک بلوک به زنجیره رله، این پاراترید ها کاندید بلوک خود شده و هزینه تراکنش را برای جمع آوری کننده واقع در استخر پاراترید می فرستد، که در این استخر به ترتیب به همراه یک پیشنهاد تعیین شده در واحد DOT ارسال می شود.

یک تایید کننده زنجیره رله پیشنهادات را بررسی کرده و تصمیم می گیرد کدام بلوک را در زنجیره رله قرار دهد. انگیزه اولیه برای اعتبار دهنده زنجیره رله، پذیرش نامزدهای بلوکی است که با بالاترین قیمت پیشنهادی ارائه می شوند و بیشترین سود را برای خود ایجاد می کنند. طبق *ویکی Polkadot، "توکن‌های پیشنهادات پاراترید احتمالاً 20-80 تقسیم می‌شوند، به این معنی که 80 درصد به خزانه Polkadot و 20 درصد به نویسنده بلوک می‌رسد. این همان تقسیمی است که در مورد کارمزد تراکنش نیز اعمال می‌شود. مانند بسیاری از پارامترهای دیگر در Polkadot، می توان از طریق یک مکانیسم حاکمیتی تغییر بیابد."*

مروری کوتاه بر کاندیداهای جالب پاراچین (سپتامبر، 2021)

1. Acala DeFi -

Acala اولین کنسرسیوم مالی غیرمتمرکز در نوع خود با چشم انداز ایجاد زیرساخت های مالی باز زنجیره ای برای اکوسیستم Polkadot است. ماموریت آن تبدیل شدن به مرکز DeFi Polkadot است تا استفاده از آن یا ساخت برنامه های مالی را آسان کند، کارایی معاملات را بهبود بخشد و در زمان ارزشمند خود صرفه جویی کند. این بدان معناست که Acala همان ماموریت اتریوم را دارد، تنها تفاوت آن در این است که به طور خاص برای موارد استفاده از DeFi ساخته شده است و استفاده از آن را برای سرویس های DeFi بسیار راحت تر می کند. این پلتفرم مجموعه ای از پروتکل های اصلی را ارائه می دهد که آن ها را به مقصدی شایسته برای هر توسعه دهنده و کاربر DeFi dApp تبدیل می کند.

a) پروتکل Honzon ((aUSD :

این پروتکل پشت aUSD مربوط به Acala است، که یک استیبل کوین غیر متمرکز و چند جانبه است که توسط دارایی های زنجیره ای پشتیبانی می شود. در مقابل، USDT، بزرگترین استیبل کوین از نظر ارزش بازار، یک استیبل کوین متمرکز است که تحت کنترل یک نماینده واحد است. DAI که به طور گسترده پذیرفته شده است، یک استیبل کوین غیر متمرکز، در حال حاضر با این واقعیت محدود شده است که تنها یک نوع وثیقه وجود دارد که می توان برای ضرب آن استفاده کرد، یعنی ETH. این امر توضیح می دهد که چرا DAI در مقایسه با USDT دارای ارزش بازار بسیار پایین تری است. بنابراین، aUSD به دنبال ارائه بهترین های هر دو جهان و اجتناب از محدودیت های استیبل کوین های محبوب است. علاوه بر این، می توان آن را از انواع وثیقه هایی که شامل KSM، BTC، ETH، DOT و هر توکن دیگری که از طریق حاکمیت Acala در لیست سفید قرار گرفته است، استخراج کرد.

b) پروتکل Homa) LDOT)

پروتکل هما یک پروتکل سهامداری غیرمتمرکز است که به کاربران امکان می دهد بدون از دست دادن دسترسی خود به نقدینگی، از مزایای سهام DOT خود بهره مند شوند. بنابراین، کاربران می توانند به جای قرار دادن DOT های خود در زنجیره رله Polkadot از پروتکل هما در Acala dApp استفاده کنند و در ازای آن LDOT دریافت کنند، البته نه لزوماً با نسبت یک به یک. LDOT مخفف DOT مایع است که کاربران می توانند آزادانه از آن به عنوان وثیقه برای گرفتن وام استیبل کوین، نقل و انتقالات یا مبادله استفاده کنند. هنگامی که کاربران می‌خواهند DOTهای سهام شده خود را باز خرید کنند، می‌توانند به سادگی LDOT را به پروتکل بازگردانند و DOT خود را به علاوه پاداش‌های سهام داری، فوراً به کیف پول بازپرداخت کنند، بنابراین از دوره بازگرداندن 28 روزه زنجیره رله جلوگیری می‌کنند.

c) صرافی غیرمتمرکز

این پروتکل مشابه Uniswap، Sushiswap و سایر صرافی‌های غیرمتمرکز است که کاربران را قادر می‌سازد تا توکن‌ها را مبادله کنند، نقدینگی ارائه کنند و پاداش کسب کنند. هدف Acala این است که DeFi را بدون پیچیدگی‌های پروتکل‌های غیرمتمرکز برای همه در دسترس قرار دهد. در حال حاضر، آنها با Current، یک شرکت آمریکایی فین‌تک ، مشارکت دارند که به ایجاد نوع جدیدی از امور مالی به نام "Hybrid Finance" (ترکیبی از مالی غیرمتمرکز و متمرکز) کمک می‌کند. به این معنی که کاربرانی که کیف پول رمزنگاری ندارند می‌توانند از حساب‌های بانکی سنتی خود بازدهی در DeFi استفاده کنند.

2. HydraDX - DeFi

HydraDX، یکی دیگر از بلاک چین های لایه-1 متمرکز بر DeFi، بسیار متفاوت از Acala است. بخش هسته پیشنهاد Omnipool"، HydraDX" است، یک "چاه نقدینگی" که به اندازه کافی عمیق و متنوع است تا بتواند در برابر هر چیزی که بازار به آن وارد می کند مقاومت کند. در حال حاضر، بیشتر معاملات توکن به صورت جفت

انجام می شود، به طوری که اگر بخواهم DOT را با KSM مبادله کنم، باید صرافی ای پیدا کنم که دارای یک جفت DOT/KSM باشد. فقط در این صورت می توانم از DOT به KSM مبادله کنیم. اگر چنین استخری در صرافی وجود نداشته باشد، من مجبور می شوم DOT را به توکنی که با KSM جفت شده است، عوض کنم. مثلاً، من یک جفت DOT/USDT و یک جفت KSM/USDT پیدا کردم، قبل از تعویض USDT با KSM، باید DOT خود را با USDT عوض کنم. این نه سرمایه ای کارآمد است و نه کاربر پسند. حتی زمانی که صرافی‌های غیرمتمرکز مانند Uniswap مبادله بین دو توکن را پیشنهاد می‌کنند که در یک استخر جفت نیستند، این کار را با تعویض خودکار از یک استخر به استخر دیگر انجام می‌دهند که باعث افت زیادی می‌شود.

به لطف قدرت و انعطاف پذیری HydraDX ، Subrate با ایجاد یک استخر واحد (Omnipool) برای هر دارایی، بر این محدودیت غلبه می کند. جزئیات این عمل، چه از نظر مالی و چه از نظر فنی کاملاً تکنیکال است، اما من یک خلاصه اولیه را در اینجا بیان می کنم. برای ایجاد HydraDX، Omnipool از توکن LRNA به عنوان توکن پایه ای استفاده می کند که همه توکن های دیگر با آن معامله میشوند، به طوری که توکن LRNA می تواند به عنوان نهنگ عمل کند. با توجه به اینکه HydraDX یک لایه-1 است، Omnipool آن تنها چیزی نیست که باید ارائه دهد: درواقع، بلوک ساختمانی ای است که بسیاری از برنامه های مالی دیگر بر روی آن قرار می گیرند.

3. KILT - هویت

برای مدت طولانی، داده های ما، به ویژه داده هایی که ما را شناسایی می کنند، برای به دام انداختن، دستکاری و سوء استفاده از ما به کار میرفتند. KILT به دنبال این است که این وضعیت را با غیر متمرکزسازی از فرآیند تصدیق و تأیید اعتبار کاربران به چالش بکشد.

KILT یک پروتکل هویت بلاک چین منبع باز برای صدور گواهینامه های مستقل، ناشناس و قابل تأیید است. KILT مدل های کسب و کار نوآورانه را در مورد هویت و حریم خصوصی امکان پذیر می کند و نیاز به راه حل های هویتی قابل اعتماد در دنیای دیجیتال را برطرف می کند. این به کاربران اجازه می‌دهد تا ویژگی‌های شخصی را بیان کنند، آن‌ها را توسط نهادهای مورد اعتماد تأیید کنند و ادعاهایشان را به عنوان جزئیات مستقل ذخیره کنند.

هسته اصلی KILT این ایده است که کاربران باید مالکیت و حقوق کامل بر اعتبارنامه خود داشته باشند، به طوری که تنها خودشان بتوانند از اطلاعات هویتی در هنگام تعامل با طرف دیگر استفاده کنند. در پروتکل آنها، کسانی هستند که نیاز به گواهینامه صادر شده دارند (مانند متقاضیان کار)، و کسانی که نیاز به تأیید اعتبار دارند (مانند شرکت های استخدام کننده).

هنگامی که بلاک چین KILT به طور کامل تنظیم و اجرا شد، می‌توان به شرکتی که می‌خواهد شما را استخدام کند ثابت کرد که شما همانی هستید که ادعا می‌کنید. این به راحتی امکان پذیر خواهد بود زیرا شرکت فقط باید اطلاعاتی را که در بلاک چین KILT ارائه می دهید بررسی کند. اگر آنها نیاز به تأیید بیشتر داشته باشند، می توانند برای تأیید اعتبار شما، به یک تایید کننده مبلغی پرداخت کنند تا این کار انجام شود.

باز هم، این ایده پایه است. اما به یاد داشته باشید که این یک بلاک چین لایه-1 است و بسیاری از برنامه های ID دیگر را می توان بر روی آن ساخت.

4. IoT - Robonomics

به نظر من، این جالب ترین نامزد پاراچین در DotSama است. من این را می گویم زیرا آنها چیزی را می سازند که هیچ کس دیگری انجام نداده است - ربومونیکس. هسته اصلی ایده آنها، درک این موضوع است که با ظهور اتوماسیون (ربات های خودگردان)، نیاز به چارچوبی برای مدیریت تعاملات ربات به ربات وجود دارد. به عنوان مثال، معمولاً مجموعه‌ای از ربات‌ها و ماشین‌ها برای تولید محصولات در کارخانه‌ها با هم کار می‌کنند، اما همچنان انسان برای تسهیل عملیات بین روبات‌های مذکور مورد نیاز است.

به عنوان مثال، هنگامی که یک کالا یک چرخه را در یک خط تولید طی کرده است، تقریباً همیشه به یک انسان نیاز است تا آن را به خط بعدی منتقل کند تا روند تولید ادامه یابد. در این مورد، تنها به یک انسان نیاز است، زیرا هیچ راهی برای ربات ها وجود ندارد که با خود صحبت کنند و اقدامات خود را به طور مستقل هماهنگ کنند.

با افزودن یک خط ارتباطی خودکار در تعاملات روبات‌ها، دنیای جدیدی از امکانات به روی ما باز می‌شود: اقتصاد ربات. با استفاده از روبونومیکس ، این امکان برای یک ربات کارخانه ای وجود خواهد داشت که یک وسیله نقلیه خودکار را آموزش دهد، به طوری که وقتی محصولات آماده شدند، ربات کارخانه می تواند وسیله نقلیه خودکار را پینگ (فراخوانی) کند تا برای پیکاپ (بارگیری) بیاید. برای جلوگیری از ارسال هرزنامه ربات، ربات حمل و نقل تنها در صورتی به تماس ربات کارخانه واکنش نشان می دهد که ربات کارخانه مقداری توکن به ربات حمل و نقل پرداخت کرده باشد.

برای وضوح بهتر، کلمه "ربات" لزوماً به ماشین های انسان نما اشاره نمی کند. هر ماشین خودکار یک ربات است: یک چاپگر، یک دستگاه قهوه ساز، یک برنامه کامپیوتری تنظیم شده در یک کامیون، یک ربات تجاری. آنها ربات هستند زیرا طوری طراحی شده اند که مجموعه خاصی از اقدامات را به طور خودکار با دریافت ورودی مشخص انجام دهند. روبونومیکس بسیار جالب است زیرا این پروژه می‌خواهد اقتصاد دنیای دیجیتال و دنیای واقعی را از طریق «ربات‌ها» به هم پیوند دهد، درست مانند فیات و کریپتوها که از طریق «اوراکل» به هم مرتبط می‌شوند.

5. Phala - حریم خصوصی

Phala با موضوع اعتماد به کلود محاسباتی مقابله می کند. بلاک چین لایه-1 Phala، یک پلت فرم محاسباتی غیرقابل اعتماد است که پردازش ابری عظیم را بدون به خطر انداختن محرمانه بودن داده ها امکان پذیر می کند. به زبان ساده، Phala در حال ساخت یک کلود غیرمتمرکز و خصوصی از طریق شبکه ای از رایانه های شخصی است که از طریق اجماع بلاک چین گرد هم آمده اند. Phala می‌خواهد سرویس‌های ابری مجاز/web2 مانند Azure، Adobe Cloud، One Drive، Google Drive و AWS را به هم مربوط کند. Phala متعهد به ارائه یک شبکه محاسباتی غیرمتمرکز جهانی است که می تواند آزادانه با قراردادهای هوشمند، پروتکل های ذخیره سازی غیرمتمرکز و خدمات ایندکس گذاری داده ها ترکیب شود.

یکی از محصولات جدید Phala، *Fat Contract* است، ارتقای مورد نظر در مدل قرارداد هوشمند فعلی، که با قدرت و انعطاف پذیری Substrate، چارچوبی که برای ساخت Polkadot و پاراچین های آن استفاده می شود، ممکن ساخته است. به طور سنتی، قراردادهای هوشمند کد خود را روی زنجیره اجرا می‌کنند، به این معنی که شبکه بلاک چین مسئول انجام محاسبات قرارداد هوشمند همراه با اجماع است. اما این قدرت قراردادهای هوشمند را محدود می کند. زیرا آنها به توانایی محاسباتی شبکه (یعنی تولید بلوک، نهایی شدن و غیره) محدود می شوند. با جدا کردن اجزای یک قرارداد هوشمند از اجماع بلاک چین، یک قرارداد هوشمند قدرتمندتر ایجاد می شود.

به زبان ساده، Fat Contracts یک قرارداد هوشمند است که محاسبات را خارج از زنجیره انجام می دهد. این با ویژگی حفظ حریم خصوصی Phala همخوانی دارد که تضمین می کند داده های محاسباتی توسط ماینرها قابل خواندن نیستند. جذابیت اصلی Fat Contracts این است که آنها امکان استفاده بسیار غنی تر و قدرتمندتر از قراردادهای هوشمند را برای طیف وسیع تری از خدمات، به ویژه خدماتی که به قدرت و سرعت پردازش زیادی نیاز دارند، مانند بازی، متاورس، و تجزیه و تحلیل داده ها فراهم میکنند.

6. Crust - Data

کلود ها، افزودنی های بینظیری در زندگی ما بوده اند: دیگر نیازی نیست که همه فایل های دیجیتال خود را در دستگاه های شخصی با فضای دیسک محدود ذخیره کنیم. با این حال، داده‌هایی که در سرورهای ابری متمرکز ذخیره می‌کنید به طور کامل متعلق به شما نیستند و نمی‌توانید مطمئن باشید که داده‌های شما همیشه امن و در دسترس خواهند بود. در مقابل، یک کلود غیرمتمرکز این مزیت را دارد که به یک سرویس ابری یا میزبانی تکیه نمی کند.

Crust یک راه حل ساده و غیرمتمرکز ذخیره سازی ابری را برای کاربران روزمره، حرفه ای ها و توسعه دهندگان ارائه می دهد. با Crust، داده‌های شما در چندین گره در سراسر جهان ذخیره می‌شود و این اطمینان را می‌دهد که می‌توانید این داده‌ها را در هر کجا و در هر زمان بازیابی کنید. علاوه بر این، هر داده ذخیره شده کاملاً متعلق به شما است و فقط شما می توانید به آن دسترسی داشته باشید. این موضوع به این دلیل است که Crust از رمزگذاری پیشرفته داده، قبل از ارسال آن به گره های خود استفاده می کند. در مجموع، Crust به دنبال به چالش کشیدن هر سرویس ذخیره سازی ابری متمرکزی است که در حال حاضر در حال کار است که Box، Dropbox، Google و غیره را نیز شامل می شود.

7. Zeitgeist - Futarchy

Zeitgeist یک بلاک چین لایه-1 است که برخی از اصلی ترین ایده ها را در اکوسیستم Polkadot پیشنهاد می کند. دموکراسی شکل ایده آلی از حکومت است، اما در خصوص مدل های تصمیم گیری اشکالات زیادی دارد. در حال حاضر، تفاوت‌های زیادی در ثروت بین ملت‌ها وجود دارد که نمی‌توان آن را به تفاوت در منابع طبیعی یا توانایی‌های انسانی نسبت داد. در حقیقت، قلب این نابرابری ها در این واقعیت نهفته است که ملت ها، که بسیاری از آنها دموکرات هستند، اغلب سیاست های ناکارآمدی را اتخاذ می کنند. Futarchy خود را به عنوان شکل جدیدی از حکومت معرفی می کند و می خواهد با استفاده از نتایج یک بازار پیش بینی، نحوه تصمیم گیری ها را تغییر دهد.

استدلال اصلی برای Futarchy این است که بازارها تمایل به عملکرد منطقی تر دارند و می توانند به عنوان یک شکل مستقل از حکومت بکار گرفته شوند. Zeitgeist یک بلاک چین لایه-1 ارائه می دهد که به هر کسی امکان می دهد یک بازار پیش بینی برای سنجش نظرات مردم در مورد هر موضوعی ایجاد کند، بنابراین از سیاست گذاری برای شرکت ها، دولت ها، جوامع بلاک چین، DAO ها و سایر سازمان ها حمایت می کند. با بکار گیری Futarchy، تصمیم‌گیری‌ها بر اساس نظرات شناور آزاد اتخاذ نمی‌شود، بلکه بر اساس شرطبندی‌های سنگین مردم مجبور می‌شوند «پول‌هایشان را در جایی امن بگذارند».

بنابراین، انتظار می‌رود که مردم در صورت هزینه بر بودن بیان نظرات خود، دقت و صداقت بیشتری داشته باشند. می توان آینده ای را تصور کرد که نمایندگان مجلس بر اساس نحوه شرط بندی خود تصمیم گیری کنند. بیایید به سوال زیر نگاه کنیم: "آیا کاهش مالیات ها باعث پیشرفت اقتصادی بیشتری می شود؟" در یک دموکراسی، همه اعضا بر اساس نظرات خود یا دیگران رأی می‌دهند. در همین حال، Futarchy از همه اعضا می خواهد که در مورد اینکه آیا کاهش مالیات منجر به پیشرفت اقتصادی می شود یا خیر، موضع مالی اتخاذ کنند. کسانی که قوی ترین عقیده را دارند احتمالاً پول بیشتری را در اختیار خواهند داشت و به طور غیرمستقیم بر نتیجه رأی گیری تأثیر می گذارند.

با چه کسی همراهی می کنید: افرادی که به اندازه کافی به عقیده خود ایمان دارند تا ریسک شرط بندی بزرگ را بپذیرند یا کسانی که آنقدر شجاع نیستند که از نظر خود با بودجه کافی حمایت کنند؟

اما همه این موارد صحیح نیست. برخی نقاط منفی بالقوه برای مدل Futarchy وجود دارد. برخی از افراد ناگزیر از بازی/شرط بندی/ریسک پذیری بخش Futarchy منحرف می شوند تا پول و نفوذ اجتماعی را ایجاد کنند، یعنی پدیده Crypto Twitter که در آن حساب های بزرگ از نفوذ خود برای افزایش قیمت توکن هایی استفاده می کنند که ارزش بازار آنها را ندارند. . همچنین انتظار می‌رود که مردم در نهایت بدون بیان نظر خودشان، تبلیغات و شرطبندی‌های بزرگ را دنبال کنند، که 100 برابر بدتر از دموکراسی است که در آن افراد بی‌تفاوت به دلیل فقدان «انگیزه» به خود زحمت رای دادن نمی‌دهند. بنابراین، Futarchy به اندازه کافی غیرمتمرکز است تا طیف وسیع تری از شرکت کنندگان را جذب کند، اما یک اثر "قمار" نیز وجود دارد که ارتباط شرط بندی ها را تضعیف می کند. فقط در اجرا می‌توانیم ببینیم که چگونه پیش خواهد رفت و به همین دلیل است که من در مورد آینده Zeitgeist هیجان‌زده هستم.

8. Moonbeam - قراردادهای هوشمند

Moonbeam یک پلت فرم قرارداد هوشمند سازگار با اتریوم در شبکه Polkadot است که به توسعه دهندگان این امکان را می دهد تا قراردادهای هوشمند Solidity و frontend های DApp را با حداقل تغییرات در کد اصلی

مستقر کنند. پس از راه اندازی موفقیت آمیز شبکه قناری خود در کوساما (Moonriver)، برخی این پلتفرم را "اتریوم 3.0" نامگذاری کردند.

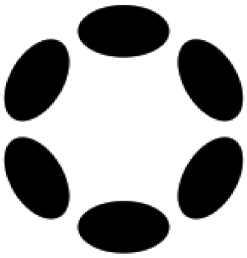
گذشته از قدردانی از ارزش توکن های MOVR که بدون شک این نام را همراهی می کند، این برچسب کاملاً بی مناسبت هم نیست. از طرفی، ادغام نرم Moonbeam با ابزارهای بومی اتریوم، آن را به مقصدی آسان برای همه dApps های اتریوم تبدیل می کند. به این ترتیب، توسعه دهندگان می‌توانند dApp های غنی‌تری بسازند که درگیر محدودیت‌های بلاک چین اتریوم نشوند - هزینه‌های گس غیرمنطقی، ماژولار نبودن، و غیره.

اینها تنها تعدادی از نامزدهای پاراچین متعددی هستند که در Polkadot ساخته شده‌اند. در زیر پیوندهایی به برخی از منابع مفید در پروژه های اکوسیستم وجود دارد:

- https://parachains.info/
- https://dotmarketcap.com/
- https://polkaproject.com/

نکته مهمی که باید به آن توجه کرد این است که اکثر این پروژه ها فقط به عنوان پاراترید ثبت می شوند. تا زمانی که یک پروژه پس از برنده شدن در مزایده اسلات پاراچین به زنجیره رله وصل نشود، کاندیدای پاراچین باقی می ماند. در ابتدای این کتاب، تصور اینکه چرا ما به انواع بلاک چین نیاز داریم، ممکن است برای شما دشوار باشد. امیدوارم این بخش در متقاعد کردن شما به اینکه آینده واقعاً چند زنجیره ای است موفق بوده باشد. در هر صورت، امیدوارم قدردانی بیشتری از تطبیق پذیری بی نهایت پروتکل لایه-0 مانند Polkadot داشته باشید که هدف آن پشتیبانی از نوآوری تصاعدی است که توسعه های لایه-1 آتی می توانند بر اساس آن پیشرفت کنند.

به طور کلی مشکلات بسیاری بصورت حل نشده برای بشریت و سیاره زمین وجود دارد پس هدف هر فناوری باید بهبود زندگی باشد، نه زندگی به معنای محدود کلمه که فقط بشریت را در نظر می گیرد. این نوع تفکری است که ما را به بحران آب و هوایی کنونی سوق داد. زندگی، همانطور که من در اینجا از آن استفاده می کنم، به گیاهان، حیوانات، جو و هر چیزی که بدون آن قادر به ادامه نیستیم، اشاره دارد. آرمان‌های شبکه‌ها و سازمان‌های غیرمتمرکز این است که مردم بتوانند در طول زمان پذیرای مسائل جهانی شوند: به زندگی احترام بگذارند، آزادی، صلح و انصاف را ترویج کنند و در نهایت رفاه انسان را به ارمغان بیاورند. که اگر در دراز مدت نتوانند این کار را انجام دهند، محکوم به تکرار اشتباهات انجام شده در وب 2.0 هستند.



فصل 6

مشارکت در شبکه

در این مرحله از کتاب، شما قبلاً چیزهای زیادی در مورد Polkadot آموخته اید. اما دانش به خاطر دانش بودنش به تنهایی هیچ ارزشی به همراه ندارد: در کاربرد است که دانش ارزش خود را به دست می آورد. این کتاب برای ارائه Polkadot به شیوه ای قابل دسترس نوشته شده است تا افراد بیشتری از شگفتی ها و امکانات این شبکه غیرمتمرکز آگاه شوند. اما این تنها نیمی از داستان است. دلیل مناسب تری که چرا این کتاب نوشته شد، جذب سازندگان و سفیران جدید در اکوسیستم بود، زیرا یک شبکه فقط با اندازه شرکت کنندگانش معتبر است.

اگر از فرصت‌های در حال ظهور در اکوسیستم Polkadot هیجان‌زده هستید یا الهام گرفته‌اید، این فصل کوتاه صمیمانه شما را به شرکت در شبکه دعوت می‌کند.

در اینجا دلایلی وجود دارد که چرا ممکن است بخواهید در Polkadot شرکت کنید:

- واقعاً غیرمتمرکز است.
- به لطف ارتقاهای بدون فورک و روی زنجیره حاکمیتی است.
- جامعه ای پر جنب و جوش و پرشور دارد.
- با مقیاس پذیری خود می تواند سخت ترین ایده ها را در خود جای دهد.
- با ارزش های جهانی مانند آزادی از تبعیض و سانسور همسو است.
- این یک پورتال برای یک *پاراورس* بی حد و حصر از لایه‌های-۱، لایه-۲، قراردادهای هوشمند، dApps، پل‌ها و بسیاری از پروتکل‌های جدید است.

بنابراین، با ساختن یا شرکت در Polkadot، شما در خط مقدم و مرکز نوآوری Web3 قرار می گیرید. اکنون که ایده شرکت کردن به شما عرضه شده است، بیایید نحوه عملکرد آن را در عمل در نظر بگیریم.

نحوه مشارکت در شبکه

در این بخش به بررسی گزینه های پیش روی شما در زمینه مشارکت خواهیم پرداخت.

امنیت

یک شبکه غیرمتمرکز فقط تا زمانی ارزشمند است که ایمن باقی بماند. بنابراین بدیهی ترین راه برای مشارکت در شبکه کمک به امنیت آن است. خوشبختانه، Polkadot یک شبکه اثبات سهام معتبر است که به افراد عادی این شانس را می دهد که به عنوان نگهدارنده، به این شبکه بپیوندند.

چهار نقش متمایز در اینجا وجود دارد:

1. **اعتبار دهنده شوید -** این به تجهیزات و دانش فنی نیاز دارد. با تبدیل شدن به یک اعتبار دهنده، تراکنش ها را تأیید و بلوک ها را تولید می کنید.
2. **جمع کننده شوید -** در حالی که اعتبار دهنده زنجیره رله را ایمن می کند، جمع کننده ها پاراچین ها و پاراتریدها را ایمن می کنند. شما می توانید یک جمع کننده برای پاراچین مورد علاقه خود شوید.
3. **کاندیدا یا نامزد شوید -** اگر نشانه‌های DOT را دارید، می‌توانید به سادگی آن‌ها را با اعتباردهنده‌ها به اشتراک بگذارید تا جوایزی کسب کنید. کیف پول ها و افزونه های مختلفی وجود دارد که می توانید برای این منظور از آنها استفاده کنید (به توصیه های زیر مراجعه کنید).
4. **وام دهنده جمعی شوید -** می توانید DOT های خود را قفل کنید تا به پاراچین کمک کنید شکاف پاراچین را روی زنجیره رله برای مدت زمان مشخصی ایمن کند. که به شما این امکان را می‌دهد تا توکن‌های بومی را از پاراچین دریافت کنید، این انگیزه‌ای برای تنوع سبد سهام است.

تمام عملیات فوق را می توان از طریق افزونه و برنامه های Polkadot-js، رابط های وب رسمی شبکه، تکمیل کرد. با این حال، اکثر کاربران غیر فنی به جایگزین های مبتدی دوستانه بیشتری نیاز دارند.

برخی از کیف پولهای توصیه شده برای Staking و وام های جمعی

1. کیف پول و افزونه Talisman (توصیه شخصی من)
2. کیف پول موبایلی Fearless
3. کیف پول موبایل Nova
4. Polkawallet
5. کیف پول Math

یادداشتی کوتاه در برابر صرافی های متمرکز

اگرچه می توانید DOT های خود را به اشتراک بگذارید و از طریق صرافی های متمرکز مانند بایننس، کراکن و کوین بیس در Polkadot شرکت کنید، اما من عمدا آنها را از لیست توصیه های کیف پول خود حذف کرده ام. این موضوع به این دلیل است که استفاده از صرافی‌های متمرکز برای عملیات‌های زنجیره‌ای برخلاف ایده متمرکزسازی است: وقتی از طریق این صرافی‌ها در وام‌های جمعی سهیم می‌شوید یا در آن مشارکت می‌کنید، عملاً مالکیت توکن‌های خود را در صرافی از دست می‌دهید. این می‌تواند در درازمدت به یک مشکل تبدیل شود زیرا:

1. یک صرافی متمرکز می‌تواند از توکن‌های شما و همچنین سایر کاربران برای مشارکت در حاکمیت و رای دادن به پیشنهادهایی استفاده کند که شما از آنها حمایت نمی‌کنید.
2. یک صرافی متمرکز ممکن است هک شود و اعتباردهنده‌های آن کاهش یابد، که بخش بیشتری از مشارکت‌کنندگان شبکه را در معرض خطر قرار می‌دهد.

سهام داری و وام دادن جمعی از طریق کیف پول‌هایی که توصیه کردم تضمین می‌کند که اقدامات زنجیره‌ای شما همیشه به حسابی مرتبط است که تحت نظارت شما است، برخلاف انتقال حقوق شما برای مشارکت زنجیره‌ای به حسابی که توسط یک تجارت شخص ثالث کنترل می‌شود.

حاکمیت

حکومتداری بعنوان ناشناخته ترین ویژگی شبکه‌های غیرمتمرکز باقی مانده است، به طوری که اکثر همه‌پرسی‌ها موفق به کسب 10 درصد مشارکت در رأی‌دهندگان نشدند. بنابراین، مشارکت شما در فعالیت های حاکمیتی به شبکه روح تازه ای می بخشد. در زیر چند ایده وجود دارد:

1. نامزدی برای شورا
2. رای دادن به نامزدهای شورا و نایب قهرمانان

3. پیشنهاد یا پیشنهادها
4. رای دادن به همه پرسی
5. ارائه نکاتی برای سازندگان اکوسیستم و سفیران
6. به بحث در مورد Discord ،Element ،Polkassembly و Reddit بپیوندید.

می توانید جزئیات بیشتری در مورد این فرآیندها در ویکی Polkadot بیابید.

رشد اکوسیستم

اگر نه ایمن کردن و نه مدیریت شبکه برای شما جذابیت ندارد، می توانید سازنده یا سفیر شوید.

سازنده

یک سازنده فرد یا گروهی از افراد است که روی استقرار پاراچین ، پالت‌های زمان اجرا، قراردادهای هوشمند، dApps و ابزارهای توسعه‌دهنده کار می‌کنند. به عنوان یک سازنده، می‌توانید با درخواست کمک‌های مالی از بنیاد Web3 یا با ارسال پیشنهادهای هزینه به خزانه‌داری زنجیره‌ای، بودجه دریافت کنید. همچنین می‌توانید وارد برنامه Substrate Builders شوید، برنامه‌ای که پروژه‌های فعلی و بالقوه مرتبط با Substrateرا شناسایی، پشتیبانی و راهنمایی می‌کند.

سفیر

این نقش را نباید با موقعیت ارائه شده به عنوان بخشی از برنامه سفیر Polkadot اشتباه گرفت، که می توانید با پر کردن فرم درخواست در اینجا به آن بپیوندید. مسئولیت/وظیفه اصلی یک سفیر کمک به رشد و پذیرش شبکه است. این کار را می‌توان به تمام روش‌هایی که ذهن می‌تواند پیدا کند انجام داد، پس مهمترین چیز هدف نهایی است. به عنوان مثال، نوشتن یک کتاب یا وبلاگ برای این منظور کار شایسته ای است، اما ضبط یک وبینار، آهنگسازی، میزبانی یک جلسه، ایجاد یک توضیح صوتی و تصویری و غیره نیز کارهای موثری است. باز هم، تخیل انسان محدود است. اگر پروژه‌ای دارید که فکر می‌کنید اکوسیستم از آن سود می‌برد، می‌توانید از طریق روشی که در اینجا توضیح داده شده است، از خزانه‌داری زنجیره‌ای درخواست کمک مالی کنید. به عنوان مثال ، این کتاب یک ایده بکر بود که با سرمایه های دریافتی از خزانه زنجیره ای Polkadot امکان پذیر شد.

همگام با اکوسیستم

اولین قدمی که می توانید برای مشارکت در شبکه بردارید این است که نسبت به اخبار اتفاقات اکوسیستم به روز باشید. در زیر پیوندهایی به برخی منابع مهم وجود دارد که به شما کمک می کند تا پیشرفت های اکوسیستم را پیگیری کنید.

1. **DotLeap**
این یک خبرنامه هفتگی است که توسط من و Bruno Škvorc منتشر می شود. این خبرنامه بر انتشار قابل توجه‌ترین به‌روزرسانی‌های اکوسیستم (DotSama (Polkadot + Kusama، پوشش اخبار زنجیره‌های رله، پاراچین ها dApps،، پاراتریدها، جوامع و موارد دیگر تمرکز دارد. این یک نمای کلی واقعاً جامع از اکوسیستم است که هر هفته در Substack و Subsocial منتشر می شود. برای اطلاع از آخرین اخبار اینجا مشترک شوید.

2. **Parachains.info**
این تمیز ترین و جامع ترین وب سایتی است که برای همه چیزها در مورد DotSama دیده ام. این اطلاعات در مورد وام‌های جمعی، مزایده‌ها و پروژه‌های پاراچین - از جمله عرضه و قیمت توکن، سرمایه‌گذاران، پیشرفت نقشه راه، وضعیت کمک مالی بنیاد Web3 و موارد دیگر را ارائه می‌کند. همچنین دارای یک برگه خبری است که اخبار پروژه های رسمی پاراچین را جمع آوری می کند. این یکی دیگر از پروژه های تحت رهبری جامعه است که توسط خزانه داری زنجیره ای تامین مالی شده است.

3. **Dotmarketcap**
این وب سایت شبیه به parachains.info است. به این معنا که اطلاعات مربوط به پروژه های اکوسیستم Polkadot، نامزدهای پاراچین و حراج ها را جمع آوری می کند. فهرستی از پروژه‌های قابل تجارت رتبه‌بندی شده بر اساس ارزش بازار و برخی از بینش‌های ارزشمند را ارائه می‌کند. بزرگترین مزیت آن این

است که تمام اطلاعات مربوط به قیمت توکن و وام‌های جمعی فوراً به‌روزرسانی می‌شود و می‌توانید از وب‌سایت برای پیگیری مجموعه‌ای از پروژه‌های مورد علاقه خود استفاده کنید.

4. **Review NFT**

این خبرنامه هفتگی دیگری است که توسط من (gbaci)و Bruno Škvorc منتشر می شود و تمرکز زیادی بر NFTs و متاورس دارد. این خبرنامه مزیت پوشش اخبار NFT از DotSama و بقیه فضای وب 3 را دارد و برای اشتراک در اینجا در دسترس است.

5. **وبلاگ Polkadot**

این یک وبلاگ رسمی است که توسط بنیاد 3Web اداره و نگهداری می شود. به روز رسانی مکرر نیست و بنابراین توصیه می شود که در وبلاگ مشترک شوید. اگر در DotLeap مشترک شده باشید، هر زمان که جدیدترین مقالات وبلاگ منتشر شوند، به روز رسانی دریافت خواهید کرد.

6. **Polkadot Daily Digest**

گزارش روزانه تقریباً هر روز توسط Bill Laboon، مدیر آموزش و انجمن در بنیاد 3Web نوشته می شود. این خلاصه شامل به روز رسانی های مهم Polkadot و Kusama در مورد زنجیره رله، حاکمیت و بحث های جامعه است. می توانید آن را در r/Polkadot و Subsocial پیدا کنید.

7. **dotTreasury**

این یک وب سایت عالی برای یافتن اطلاعات در مورد خزانه Polkadot است. اطلاعات مربوط به ذخایر خزانه، درآمد، هزینه ها و سایر اطلاعات مربوط به خزانه را ارائه می دهد.

8. **Polkadot A to Z**

این یک مجموعه آموزشی توسط Emre Surmeli ، مربی فنی در بنیاد 3Web است. این مجموعه اطلاعات فنی اصلی در مورد فناوری های Polkadot و Substrate را در یک زمان ارائه می دهد. محتوا در قالب کوتاه قابل هضم ارائه شده است و در حال حاضر در Reddit قرار دارد.

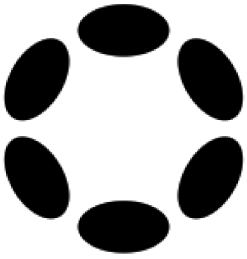
9. **Guide to Polkadot-JS**

دستورالعمل های گام به گام برای دسترسی به عملیات کیف پول برای مبتدیان ارائه می دهد و در این وب سایت موجود است.

10. **?Ser, Have ya 'Heard**

این یک مجموعه آموزشی از ویدیوهای روزانه توسط Jay Chrawnna، یکی از اعضای انجمن است. آخرین اخبار و تحولات در اکوسیستم DotSama را در قالبی بسیار سرگرم کننده برای مخاطبان عمومی تجزیه و تحلیل می کند. در حال حاضر در یوتیوب میزبانی می شود.

همه چیز گفته شد! به پاراورس خوش آمدید.



ضمیمه فنی

A BABE AND GRANDPA

(لطفاً توجه داشته باشید که به دلیل قابلیت ارتقای بدون فورک Polkadot، این مکانیسم توافقی در آینده ممکن است تغییر کند).

قبل از اینکه در مورد BABE و GRANDPA صحبت کنم، باید چیزی در مورد پروتکل های کامپیوتری توضیح دهم.

اول، همیشه به یاد داشته باشید که بلاک چین یک پروتکل است. اما پروتکل چیست؟ پروتکل مجموعه ای از دستورالعمل ها است که یک نرم افزار کامپیوتری با آن کار می کند. می توان به یک پروتکل اعتماد کرد، زیرا قوانین آن از ابتدا مشخص است. شما می توانید پروتکل را به عنوان مجموعه ای از اقدامات خودکار که یک کامپیوتر انجام می دهد در نظر بگیرید.

اکنون، نکته حیاتی که باید در مورد پروتکل ها بدانید این است که یک پروتکل می تواند پروتکل ها و پروتکل های فرعی زیادی را در خود داشته باشد. به این صورت که وقتی می گوییم بلاک چین یک پروتکل است، در واقع منظورمان این است که بلاک چین پروتکلی از پروتکل های فرعی است که هر زیر پروتکل مجهز به قابلیت داشتن زیر پروتکل های دیگر است. هر زیر پروتکل و پروتکل فرعی وظیفه خاصی را بر عهده دارد.

بنابراین در مورد زنجیره رله Polkadot که به خودی خود یک پروتکل است، پروتکل های فرعی و ریز فرعی مختلفی وجود دارد. به همین دلیل است که ما هر دو BABE و GRANDPA را به عنوان پروتکل های فرعی زنجیره رله داریم.

با این توضیحات، اکنون می توانیم با BABE آشنا شویم. برای آدم‌هایی که می‌دانند چگونه کد بخوانند، بسیار جذاب است. اما برای ما متخصصین، او فقط یک BABE است، هرچند هم قدرتمند باشد.

BABE - Blind Assignment for Block Extension (تخصیص Blind به یک بلوک پسوند)

BABEیک پروتکل فرعی در زنجیره رله است که تولید بلوک را هماهنگ می کند. برای انجام این کار به صورت ایمن و غیرمتمرکز، از چند ترفند جالب استفاده می کند:

تخصیصBlind مرسوم به انتخاب تصادفی

اولین ترفندی که در آستین او وجود دارد، فرآیند تخصیص Blind است. دو راه برای تعیین اینکه کدام گره می‌تواند بلوک بعدی را ایجاد کند وجود دارد - به‌طور تصادفی یا قطعی. اگر یک گره از قبل بداند که تعداد x بلوک را ارائه می دهد، این گره زمان کافی برای ایجاد تراکنش های جعلی برای گنجاندن در این بلوک ها را دارد. بنابراین، BABE به طور تصادفی انتخاب می کند. به این ترتیب، گره ها از قبل نمی دانند که کدام بلوک ها را تولید خواهند کرد. این مکانیسم خاص برای توضیح در این کتاب بسیار فنی است، فقط به یاد داشته باشید که BABE گره ها را به صورت تصادفی برای تولید بلوک انتخاب می کند. یکی دیگر از دلایلی که من نمی‌خواهم به جزئیات بیشتر در این کتاب بپردازم این است که شایعه‌ای حاکی از آن است که این مکانیسم در حال خروج از گردونه کاری است. بسیار مایه تاسف است که زمان زیادی را صرف از بین بردن پیچیدگی آن کنیم تا اینکه کمتر از یک سال بعد مجبور به انجام اصلاحات باشیم.

تکالیف چندگانه مرسوم به پشتیبان‌گیری

برای اطمینان از سطح بالاتری از عدم تمرکز، BABE به گره‌های مختلف بلوک یکسانی می‌دهد تا تولید کنند. هدف این است که تولید بلوک رقابتی شود تا در صورت تضاد عملکرد بین گره‌های مختلف در مورد دقت یک بلوک، همه گره‌ها بتوانند بر اساس پارامترهای از پیش تعریف‌شده درباره اینکه کدام بلوک به احتمال زیاد معتبر است رای دهند. به یاد داشته باشید، این یک پروتکل است.

یکی دیگر از مزایای تخصیص چندگانه این است که گاهی اوقات گره ای که برای ایجاد یک بلوک انتخاب شده است ممکن است آفلاین شود یا مشکلات دیگری داشته باشد، که مانع از ایجاد بلوک شود. هنگامی که این اتفاق می افتد، همیشه یک بلوک ثانویه تولید شده که شبکه می تواند بر روی آن به عقب برگردد. بنابراین، برای هر بلوک در انتظار تولید، یک تولید کننده بلوک اولیه وجود دارد که توسط BABE و چندین تولید کننده بلوک ثانویه تعیین شده است.

پروتکل‌های فرعی دیگری در BABE وجود دارد، اما مواردی که من فهرست کرده‌ام قابل توجه‌ترین ها هستند. هر گونه اطلاعات بیشتر ما را به فرو رفتن عمیق در قلمرو فنی سوق می دهد. برای این کار، خواندن مقاله تحقیقاتی زیر در BABE را توصیه می کنم.

GRANDPA - ابزار نهایی

GRANDPA هم مانند BABE پروتکل فرعی دیگری است. اما برخلاف BABE، بر روی نهایی بودن تمرکز دارد و تأیید می کند که بلوک ها معتبر هستند و نمی توان آنها را برگرداند. به طور خلاصه، در جایی که BABE به شبکه کمک می کند تا بلوک ها را به صورت غیرمتمرکز ایجاد کند، GRANDPA به نهایی کردن بلوک ها به صورت غیرمتمرکز کمک می کند. این کار را با اجرای انتخابات در همه گزینه‌های مختلف فورک انجام می‌دهد.

از آنجایی که BABE گره های مختلفی را برای تولید یک بلوک انتخاب می کند، همیشه این سوال وجود دارد که کدام دنباله بلوک درست است. این به این دلیل است که BABE قبل از ورود GRANDPA چند بلوک و فورک مرتبط با آنها را ایجاد می کند. بنابراین وظیفه GRANDPA این است که تصمیم بگیرد کدام فورک زنجیره معتبرتر است.

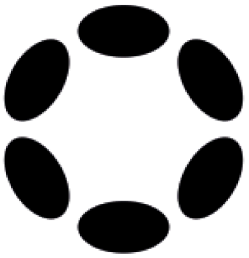
احتمالاً از خود می پرسید: "پس Polkadot هم فورک دارد؟" خوب، اصطلاح مناسب‌تر برای این فورک‌ها در زمینه ما «فشارهای مصنوعی» (فورک‌های کاذب) است، زیرا هنوز نهایی نشده‌اند. هنگامی که یک فورک نهایی شد، تمام گره های دیگر رها می شوند و هر گره در شبکه تصمیم GRANDPA را می پذیرد. اما GRANDPA چگونه تصمیم خود را می گیرد و چگونه می توانیم به او اعتماد کنیم؟ خوب، میدانیم که GRANDPA یک پروتکل است پس فقط کاری را انجام می دهد که به او دستور داده شده است. من این نکته را توضیح می دهم در حالی که تا آنجا که می توانم از جزئیات فنی اجتناب می کنم.

هنگامی که فورک های مختلفی روی زنجیره ایجاد می شود، تصمیم GRANDPA در مورد اینکه کدام فورک به زنجیره نهایی تبدیل می شود توسط:

1. اتصال آن به آخرین بلوک نهایی شده هدایت می شود : هر یک از گزینه های فورک که از آخرین بلوک نهایی توسط GRANDPA برای باقی ماندن به اندازه کافی معتبر در نظر گرفته می شود.
2. تعداد بلوک های اصلی آن : به هر یک از گزینه های فورک با بیشترین تعداد بلوک های اولیه وزن بیشتری داده می شود. بلوک اولیه، بلوکی است که توسط گره ای که BABE به عنوان گره اولیه در نظر گرفته، ایجاد شده است و در آن زمان بلوک مذکور در حال تولید بوده است. به یاد داشته باشید که BABE گره های مختلفی را برای ایجاد یک بلوک انتخاب می کند و تنها یک گره همیشه اولیه است در حالی که بقیه گره ها ثانویه نامیده می شوند.

با داشتن این الزامات، GRANDPA می تواند هر بلوکی را که بیشتر با معیارهای نهایی مطابقت دارد انتخاب کند.

در مجموع، هدف اصلی BABE و GRANDPA ارائه یک راه حل غیرمتمرکز زنجیره رله برای دستیابی به اجماع و قطعیت یعنی امنیت است. غیر متمرکزسازی بیشتر همیشه مورد توجه بوده زیرا تضمین می کند که شبکه بر اساس حقیقت مشترک عمل می کند و نه بر اساس دروغ متمرکز. اگر همه کاربران مخرب تلاش کنند تا داده های زنجیره ای را دستکاری کنند، کار تقریباً غیرممکنی برای انجام دادن خواهند داشت.



درباره نویسنده

Gbaci نویسنده، فیلمساز و موسیقیدانی است که علاقه زیادی به متمرکزسازی و اکوسیستم DotSama دارد.

او بررسی عمیق خود در زمینه فناوری‌های بلاک چین را در دسامبر 2020 آغاز کرد و از آن زمان به عنوان سفیر Polkadot، نویسنده اصلی محتوا در RMRK، و سردبیر مشترک NFT Review و DotLeap که یک خبرنامه هفتگی در مورد همه جزئیات Polkadot و Kusama میباشد فعالیت دارد.

گباجی معتقد است که "RMRK تنها استاندارد NFT خواهد بود که توسط همه استفاده می شود". او به طور حرفه ای با نام *Gillian Baci* به تولید موسیقی می پردازد و موسیقی خود را در قالب مجموعه های چند رسانه ای و قابل تولید در *Singular* منتشر کرده است.

وقتی **گباجی** در حال کار با رمزنگاری یا آهنگسازی نباشد، رمان و فیلمنامه می‌نویسد، فیلم می‌گیرد، کتاب می‌خواند و با ایده‌های بدیع در مورد چگونگی ایجاد تأثیر ماندگار سر و کله می‌کند.

به عنوان یک شهروند جهانی، او معتقد است که همه چیز به هم مرتبط است و همه ما در جوامع خود و در کل جهان یکی هستیم. شما می‌توانید او را در توییتر با آدرس **@gbaciX** دنبال کنید.