

بسم الله الرحمن الرحيم

پروژه کاربردی درس بلاکچین

دکتر مداح علی

امیرحسین رستمی

96101635

پرهام محمدی

96102342

در این پروژه قصد داریم تا وسعت صنعت بلاکچین را نمایان کنیم. برای این منظور 3 کاربرد صنعتی بالقوه یا بالفعل را توضیح خواهیم داد. این 3 کاربرد به صورتی انتخاب شده است تا دو موضوع نشان داده شود. اول اینکه مبحث بلاکچین بر خلاف آنچه معمولاً تصور شود ، صرفاً مختص به امور مالی نمی باشد. دوم آنکه کاربردهای بلاکچین می تواند از کوچک مقیاس ترین حوزه تا بزرگ مقیاس ترین حوزه را در بر بگیرد.

این 3 کاربرد عبارتند از :

1 – Block chain governance

این کاربرد نشان می دهد که وسعت و مقیاس بلاکچین می تواند تا حدی پیش برود که با حکومت ها رقابت کند.

2 – Supply chain

این کاربرد نشان می دهد که بلاکچین صرفاً مسائل مالی را پوشش نمی دهد و می تواند زیرساخت صنایع بسیاری را شکل دهد.

3 – Escrows

این کاربرد نشان می دهد که در کاربرد مالی بلاکچین و رمزارزها ، چگونه بلاکچین از صرف تراکنش های مالی می تواند فراتر برود و در شمایل مختلف در زندگی اقتصادی ما قرار بگیرد.

Block chain governance

به عبارت ساده ، "حاکمیت" ساختاری است که هر یک از اعضای جامعه توافق می کند که از آن پیروی کند. هر آنچه که ما استفاده می کنیم تحت نوعی حاکمیت است. هدف اصلی آن تأمین نیازهای جامعه با منابع موجود تا حد ممکن با کارایی و پایداری طولانی مدت ساختار است. این شامل هر نوع گروهی می شود ، خواه در دنیای واقعی باشد یا دیجیتال. بنابراین ، برای هر نوع مؤسسه ، سازمان یا سرویس ، حکومت به طور فزاینده ای ضروری می شود به ویژه هنگامی که رشد کنند. سبک حکمرانی نیز باید متناسب با نیاز فعلی ادامه یابد ، اما گفتن این کار بسیار آسان تر از انجام است. در ابتدا ، بلاکچین یک سیستم بدون حاکمیت و با کاربرهای محدود و جامعه کوچک بود. اما با افزایش اندازه و پیچیدگی ، مدیریت بهتر خواستار حاکمیت مناسب است. درک اینکه چگونه حکومت decentralized کار می کند یک بحث متفاوت است. از این رو بهتر است ابتدا خود را با قالب های سنتی حکمرانی آشنا کنید.

قالب های حاکمیت

امروزه انواع مختلفی از سبک های حکمرانی وجود دارد ، اما همه آنها از دو نوع اصلی ناشی شده اند.

- حکومت مستقیم :

همانطور که از نامش پیداست ، به معنای ناب آن مستقیم و بدون واسطه است. هر یک از اعضای جامعه مستقیماً به هر تصمیمی رأی می دهد و هر اقدامی لازم است انجام را انجام می دهد ، و هیچ استثنایی وجود ندارد. نقاط قوت : در اینجا هر رأی واقعاً شمارش می شود - از آنجا که هیچ واسطه ای وجود ندارد ، شفافیت کامل را باعث می شود - این باعث می شود تا حداقل تقسیم و بیشترین فرصت همکاری و بحث آزاد برای تصمیم گیری مهیا شود. افراد تمایل دارند کنترل بیشتری بر آنچه بدست می آورند داشته باشند - دولت بسیار بیشتر پاسخگو است - هر مقام سرکش در دولت می تواند به سرعت برکنار شود - رأی دادن در اینجا بیشتر از اینکه یک امتیاز باشد یک مسئولیت است نقاط ضعف : اغلب ثابت می شود که دستیابی به اجماع بسیار دشوار است - آموزش همه درمورد موضوع و روند رأی گیری ، می تواند هزینه بر باشد - برخی از افراد ممکن است تمایلی به شرکت در آن نداشته باشند - برخی از کاربران می توانند بدون در نظر گرفتن سود جمعی ، خودخواهانه رأی دهند. بزرگترین مشکل این است که هرچه گروه بزرگتر شود ، مدیریت آنها تا حدی غیرکارآمدتر می شود.

- حاکمیت نماینده :

در این مدل ، همه اعضای جامعه رأی می دهند تا چند نفر را به عنوان نماینده خود انتخاب کنند که همه تصمیمات حاکم را از طرف آنها می گیرند ، به قوانین جدید رأی می دهند و آنها را اجرا می کنند. جوانب مثبت و منفی این مدل حکومتی به شرح زیر است :

نقاط قوت : این مدل کارآمد است و می توان سریعتر تصمیم گیری کرد – معمولاً تصمیمات نهایی بسیار متعادل است و برای سود جمعی است. مردم باید نمایندگان خود را انتخاب کنند – مقرون به صرفه است زیرا اطلاع رسانی به گروه کوچکی از نمایندگان آسان تر است و همچنین آنها افراد آگاهی نیز هستند – اینگونه مدیریت یک گروه عظیم نسبتاً آسان تر است.

نقاط ضعف : نمایندگان ممکن است پس از انتخاب به نفع شخصی خود کار کنند – آنها ممکن است طبق اعتماد مردم رفتار نکنند – بعضی از بخشهای مردم همیشه از این تصمیم ناراضی خواهند بود زیرا تصمیمات متناسب با اکثریت است – عدم پاسخگویی نمایندگان وجود دارد – احتمال بالایی وجود دارد که اقدامات فریبدهای برای انتخابات توسط نمایندگان انجام شود.

بعداً در این مبحث به این نکات نیاز خواهید شد تا به روشنی فهمیده شود که چگونه حاکمیت با بلاکچین ادغام شده است.

حال حکومت بلاکچینی را تعریف می کنیم :

بیشتر شرکت ها و ارگان های حاکمیت ماهیت decentralized دارند ، بنابراین یک تیم رهبری معمولاً آنها را اداره می کند. با این حال Block chain یک شبکه decentralized است که دارای بسیاری از اجزا و ویژگی های منعطف است. این یک سیستم همیشه در حال تحول است که همیشه باید سعی کند خود را با نیاز کاربر تطبیق دهد و کنترل کند. بنابراین مکانیزم چگونگی سازگاری بلاکچین و برقراری ارتباط با زمان و نیازهای متغیر ، مدیریت بلاکچین نامیده می شود. در ادامه بیشتر توضیح خواهیم داد.

سازگاری و قابلیت ارتقا به دو ویژگی اساسی در مورد حاکمیت بلاکچین تبدیل می شوند. به گفته بسیاری از کارشناسان ، توانایی یک شبکه بلاکچین برای تکامل و ارتقا در میان توسعه مداوم ، یک تمایز اصلی برای حفظ جریان و رقابت است.

حال به این موضوع خواهیم پرداخت که در حکومت بلاکچینی چه اجزا و نقش هایی وجود دارد. حاکمیت بلاکچین معمولاً شامل چهار جامعه مرکزی است ، اینکه هر گروه به چه اندازه درگیر است بستگی به معماری بلاکچین مورد نظر دارد. این جوامع به شرح زیر است :

Core Developers: آنها مسئول حفظ کد اصلی زیربنای بلاکچین هستند. اگرچه آنها می توانند برای اصلاح کد مرکزی کد اضافه یا حذف کنند ، اما نمی توانند آن را در کل شبکه اعمال کنند.

Node Operators: اعمال کردن ویژگی‌های جدید که در گروه قبل ذکر شد ، وظیفه این گروه است. از آنجا که آنها یک نسخه کامل از دفتر بلاکچین دارند و آن را روی رایانه های خود اجرا می کنند ، می توانند تصمیم بگیرند که آیا این ویژگی را در گره های خود پیاده سازی می کنند یا خیر. توسعه دهندگان کد برای توافق در مورد ویژگی های ارائه شده به اپراتورهای گره وابسته هستند.

Token Holders: اینها کاربر و اشخاصی هستند که token بلاکچین را در اختیار دارند. بسته به بلاکچین های مختلف ، آنها درجات مختلفی از حق رأی دارند که با آن می توانند در مورد اینکه چه ویژگی برای پیاده سازی استفاده شود ، تعیین قیمت ها و غیره تصمیم بگیرند. به طور کلی ، سرمایه گذاران قسمت عمده ای از جامعه اصلی دارندگان رمز را تشکیل می دهند.

Block chain تیم : این می تواند یک شرکت یا یک سازمان غیرانتفاعی باشد که نقش های مختلفی را بر عهده دارد. نقش اصلی هدایت صندوق و توسعه پروژه است. آنها همچنین نمایانگر جوامع گسترده تری از سرمایه گذاران و حامیان برای مذاکره با توسعه دهندگان کد و اپراتورهای گره هستند و همچنین اغلب نقش بازاریابی را بر عهده می گیرند. به عنوان مثال Ripple نمونه ای از پروژه است که توسط یک شرکت مدیریت می شود.

روشهای مختلفی برای دسته بندی روشهای حاکمیت وجود دارد. در مورد بلاکچین ، شناسایی مشخصه های اصلی برای ارزیابی و توسعه یک ساختار حاکم بر بلاکچین بسیار مهم است. در مقایسه با حاکمیت فعلی سازمان های معمولی ، می توان به چهار دسته فکر کرد که بسیار مرتبط با حاکمیت بلاکچین هستند :

1. اجماع
2. مشوق ها و انگیزه ها
3. اطلاعات
4. ساختار حکومت

در بخش بعدی به هر یک از این موارد خواهیم پرداخت و نشان خواهیم داد که چگونه آنها پارامترهای مهمی برای اداره بهینه بلاکچین هستند.

بلاکچین حکومتی را می توان در دو دسته کلی طبقه بندی کرد :

- On-chain Governance
- Off-chain Governance

حاکمیت Off-chain

حاکمیت Off-chain معمولاً باعث ایجاد تعادل بین جامعه بلاکچین می شود ، به عنوان مثال توسعه دهندگان اصلی آن ، استخراج کنندگان ، کاربران و سازمان های تجاری. بیت کوین و اتریوم هر دو از این مدل حاکمیت پیروی می کنند. این نوع مدل حکمرانی به ساختار سنتی حکمرانی شباهت دارد ، اما برخی از شباهت ها و همچنین برخی تفاوت هایی با مدل های سنتی حکمرانی وجود دارد. مدل Off-chain نسبتاً متمرکز است ، به این معنی که تعداد کمی از افراد تصمیم می گیرند. بسیاری از کاربران جریان اصلی به دلیل کمبود دانش فنی یا قدرت مالی ، حرفی برای گفتن ندارند یا تأثیر کافی در تصمیم گیری ندارند. این شبیه دولت مستقیمی است که قبلاً در مورد آن بحث کردیم ، و به همین دلیل بسیاری معتقدند که حاکمیت مستقیم تهدیدی برای پایداری بلاکچین است. با این حال ، این شباهت ها در این واقعیت نهفته است که گرچه متمرکز است ، Off-Chain انعطاف پذیری بسیار بیشتری نسبت به ساختارهای سنتی در عملکرد ایجاد می کند. به عنوان مثال Hard fork را در نظر بگیرید. کاربر می تواند انتخاب کند که کدام بلاکچین را دنبال کند. قیمت تقسیم پروتکل اصلی زنجیره ای در مقایسه با سناریوهای حاکمیت سنتی در صنایع یا دولت بسیار کمتر است. بیایید بررسی کنیم که چهار مؤلفه تأثیرگذار بر استراتژی حاکمیت Off-chain چگونه است.

اجماع : در خارج از زنجیره ، رهبران جامعه معمولاً تصمیم می گیرند. در مورد بیت کوین ، بازیکنان بزرگ استخراج مانند Bitmain ، توسعه دهندگان اصلی و نهادهای تجاری با یکدیگر تعامل دارند و به توافق کلی می رسند. مشوق : اگرچه انگیزه خوبی وجود دارد ، اما نوع انگیزه برای نهادها یا جوامع مختلف پروژه های خارج از زنجیره متفاوت است. در حالی که استخراج کنندگان کارمزد دریافت می کنند ، توسعه دهندگان خواهان ادغام کنترل شده در تغییر شبکه و موفقیت روزافزون آن هستند و از طرف دیگر ، مشاغل به دنبال هر چیزی هستند که برای آنها بهتر باشد. این انگیزه متفاوت دارای پتانسیل قابل توجهی برای ایجاد مشکلات و در نتیجه ایجاد یک Hard fork است. Hard fork معروف بدنام بیت کوین کش به دلیل مشکلات انگیزه ای بود.

اطلاعات : اطلاعات در مورد بیت کوین و سایر بلاک چین ها یک پیشنهاد منحصر به فرد است. شفافیت ذاتی و ماهیت غیرمتمرکز بیت کوین بینش هایی را در مورد مکانیک پلتفرم های موجود در دولت ها یا شرکت های بزرگ ارائه می دهد. این شفافیت عمیقاً مفید است ، اما همچنین می تواند انگیزه های قطبی توسط طرف های مختلف را برانگیزد به محض آنکه شبکه در موقعیت های ریشه دار شده تأثیر بگذارد. اطلاعات در بلاکچین ها کامل نیستند ، اما بسیار بهتر از مدل های سنتی حکمرانی هستند و قادر به حل کردن پراکندگی اطلاعات در اینترنت هستند. ساختار حاکم Off-Chain گرچه به اندازه شرکت های معمولی فناوری و سایر سازمان های رسانه ای متمرکز نیست ، با این حال سطح بالایی از تمرکز را در خود جای داده است. آنچه آن را از ساختار سلسله مراتبی ساختار حاکمیت سنتی متمایز می کند ، توانایی توسعه دهندگان در مشارکت در تصمیم گیری است. یک مثال عالی برای این کار مکانیسم پیشنهاد Bitcoin BIP است. اکنون ، می توان از طریق استراتژی متمرکز ، حاکمیت Off-chain را به سه دسته تقسیم کرد :

1. Benevolent Dictator for Life
2. Core Development Team
3. Open Governance

:Benevolent Dictator for Life

این یک نوع مدل Off-chain است که سازنده اصلی یا لیدر تیم توسعه دهنده یا در یک کلام یک شخص واحد ، قدرت و اختیار نهایی را در مورد تصمیمات مربوط به بلاکچین دارد. این مدل به درستی "دیکتاتور خیرخواه برای زندگی" نامگذاری شده است. این ساده ترین استراتژی حاکمیت موجود است. مدیر عامل فیس بوک ، مارک زاکربگ ، قدرت تأیید یا رد هر تصمیمی را دارد ، بنابراین نقشه راه آینده فیس بوک را کنترل می کند.

:Core Development Team

در اینجا تمام تصمیمات مربوط به عملکرد و ویژگی ها توسط تیمی از فعال ترین هسته های سازنده گرفته می شود و بنابراین نقشه راه بلاکچین را شکل می دهند. همه کاربران می توانند ویژگی هایی را درخواست کنند یا آنها را ارائه دهند ، اما اینکه آیا بالاخره آن را پیاده سازی می کنند یا آن را در نسخه رسمی در دسترس قرار می دهند ، در دست توسعه دهندگان اصلی است. بیشتر پروژه های برنامه نویسی منبع باز از این نوع حاکمیت استفاده می کنند. این روش حاکمیتی معمولاً در پروژه های برنامه نویسی منبع باز استفاده می شود.

:Open Governance

حکمرانی آزاد مانند حکومت نمایندگی یا دموکراسی است. در اینجا ، انجمن کاربران بلاکچین تیمی را انتخاب می کند تا تمام تصمیمات حاکمیتی برای بلاکچین را اتخاذ کند. این تیم معمولاً شامل توسعه دهندگان اصلی ، سرمایه گذاران برجسته و صاحبان بلاکچین است. به عنوان مثال ، Corda ، از یک روش حاکمیت باز استفاده می کند. Hyperledger یکی از انواع بلاک چین های حاکمیت باز است. مقام نهایی تصمیمات فنی در Hyperledger ، از میان فعالان آن انتخاب می شود. سیستم حاکمیت Off-chain ادغام بسیاری از تصمیمات فردی است که در طول زمان اتخاذ شده اند و بنابراین سیستم حکمرانی به آرامی به سمت تکامل می رود. همچنین این قطعات متنوع تصمیمات ، تجزیه و تحلیل از منظر کلان را بسیار دشوار می کند.

حاکمیت On-chain

این برخلاف سایر روشهای Off-Chain، آخرین دستاورد در ساختارهای حاکم بر بلاکچین است که به طور انحصاری برای بلاکچین ایجاد شده است. ماهیت بسیار دموکراتیک تر، روش حاکمیت On-Chain مفاهیم جذاب، امیدوار کننده و در عین حال قطبی را در این مدل ارائه می دهد. دموکراسی مستقیم در حاکمیت On-Chain به لطف مکانیزم رأی گیری داخلی بلاکچین تحقق می یابد که می تواند مطابق طراحی خاص شبکه بهینه شود. توجه داشته باشید که در اینجا، مشارکت اپراتورهای گره در حاکمیت کاملاً غیرضروری است، زیرا آنها فقط باید روند موجود روی On-chain را دنبال کنند. این تصمیمات پیش فرض را قدرتمند می کند و موجب جلوگیری از Hard fork می شود. در ساده ترین شکل، تصور کنید که جامعه به دو گروه کاملاً متفاوت تقسیم شده باشد که دو درخواست زیر را دارند:

درخواست گروه اول افزایش اندازه بلوک برای به حداکثر رساندن بازده در لایه پایه می باشد.

درخواست گروه دوم، درست کردن یک لایه دوم مانند شبکه lightning است.

همه دارندگان token رأی خود را در این باره می دهند و هرکدام که بیشترین آرا را کسب کند به طور خودکار در زنجیره قرار می گیرد. با دادن قدرت تصمیم گیری و کنترل بیشتر به اعضای جامعه، تمرکز روی نیازهای جامعه قرار خواهد گرفت. حال بررسی می کنیم که چهار مؤلفه تأثیرگذار بر استراتژی حاکمیت On-chain چگونه است:

اجماع: پروتکل بلاکچین در مدل حاکمیت On-Chain، امکان دستیابی به اتفاق نظر را از طریق مکانیزم رأی گیری مستقیم فراهم می کند. این روش اجماعی بیشتر به دموکراسی مستقیم (همانطور که قبلاً بحث شد) با چند بهینه سازی کوچک متناسب با نیاز هر بلاکچین شباهت دارد. نتایج رأی به صورت الگوریتمی اداره می شود و به صورت خودکار مستقیماً در پروتکل تعبیه می شود. این یک شکل کاملاً جدید از اجماع برای حاکمیت است، بنابراین مورد واقعی در عمل برای ارزیابی موفقیت یا عدم موفقیت آن وجود ندارد.

مشوق ها: مشوق های موجود در مدل حاکمیت On-Chain بسیار متفاوت از مدل Off-Chain است. قدرت تصمیم گیری از توسعه دهندگان و استخراج کنندگان به کاربران عمومی در حاکمیت On-Chain منتقل می شود. در حالی که دموکراسی محقق شده است، اکنون چقدر این روش برای هدایت توسعه زنجیره بلوک در مسیر درست موثر خواهد بود. درست مانند یکی از موارد منفی که در دموکراسی مستقیم ذکر شده است، مورد سوال است. با انگیزه های متفاوت، تضاد منافع بین کاربران ایجاد می شود. بدون دانش فنی مناسب، که مطمئناً بسیاری از کاربران از آن برخوردار نخواهند بود، ممکن است کاربران برای مصلحت جامعه تصمیم نگیرند.

اطلاعات: شفافیت در مورد اطلاعات در سیستم On-Chain بسیار بهتر از آن است که در حاکمیت Off-chain ارائه می شود از آنجایی که کاربران نیز در این امر دخیل هستند. پیشنهادهای مختلف برای توسعه و همچنین رأی دادن اکنون علنی است. هر تصمیم مهم، اما یک تصمیم ضروری مانند تصمیم برای کاهش پاداش بلوک پیشنهاد می شود و از طریق رأی گیری از طرف ذینفعان یا یک مکانیزم ترکیبی روی زنجیره از On/Off و با شفافیت کامل اجرا می شود.

به غیر از پیشنهاد BIP Bitcoin با شفافیت بهبود یافته ، هیچ بلاک چین دیگری وجود ندارد که بتواند سطح شفافیت مشابهی را در ساختار حاکمیت Off-chain خود ارائه دهد.

ساختار حاکم : این ویژگی شگفت انگیز مدل On-Chain است. وظیفه حاکمیت بر روی خود بلاکچین انجام می شود. همانطور که گفته شد ، از آنجا که اجماع از طریق سازوکار رای گیری غیرمتمرکز حاصل می شود ، به بلاکچین امکان می دهد تا بسیار سازگارتر و انعطاف پذیرتر از نمونه On-chain خود باشد. در اینجا ، پروتکل های نحوه فعالیت بلاکچین در قراردادهای هوشمند زنجیره ای ذخیره می شود که دارای قابلیت ها و رویه های داخلی برای اصلاحات است. قوانین مربوط به عملکرد بلاکچین در خود بلاکچین ذخیره می شود - حاکمیت decentral مناسب برای یک شبکه decentral.

ما دیده ایم که با بزرگتر شدن یک گروه یا جامعه ، مردم سالاری یا دموکراسی به دلیل احساسات یا خودخواه بودن افراد ، شروع به شکست می کنند. این یک خطر عمده برای سازوکار حاکم بر On-Chain است زیرا بسیاری از کاربران در اینجا ناشناس یا در بهترین حالت شبه ناشناس هستند.

در حاکمیت On-chain مسئله مقیاس پذیری همچنان یک نگرانی عمده است. هرچه جامعه بزرگتر باشد ، اداره موثر آن پیچیده تر و دشوارتر می شود. جامعه بلاکچین با توجه به ارزش حاکمیت On-chain تقسیم و شاخه شاخه می شود. از نظر تئوری ، هرگونه تغییر می تواند در خود بلاکچین کدنویسی شود و از طریق نهادهای مجاز رأی داده شود و سپس به صورت خودکار در کد اجرا شود. اما ، در واقع ، این رویکرد چالش های جدی ایجاد می کند :

- همه اعضا باید در راستای منافع کل گروه عمل کنند ، که در یک جامعه بزرگ و متفاوت تضمین نمی شود.
- بلاکچین ها غیرقابل تغییر هستند ، بنابراین به محض اینکه آرا برای هرگونه تغییر پیشنهادی قرار گرفت ، نمی توان آن را پس گرفت.
- یک گرایش طبیعی برای بازآفرینی مدل های حاکمیت بر روی پویایی های On-chain ، احتمال اصطکاک و فرسایش زیادی را ایجاد می کند.
- دستیابی به پایداری طولانی مدت با یک مدل حکمرانی تجربی به زمان و تلاش بسیار بیشتری نیاز دارد.

بیایید اکنون برخی از پروژه های بلاکچین را که از حاکمیت On-Chain استفاده می کنند ، بررسی کنیم :
گرچه هنوز در ابتدای راه است ، اما هر روز پروژه های زنجیره ای بیشتری به وجود می آیند. بیایید برخی از این پروژه ها را بررسی کنیم :

:Tezos

یکی از پروژه های اصلی مدل حاکمیت On-Chain است و به نظر می رسد آنها مسئله خودگردانی را حل کرده اند. از Tezos به عنوان زنجیره بلوکی خود اصلاح کننده یاد می شود زیرا می تواند بدون نیاز به Hard fork ، مطابق با نیازهای فعلی تکامل یابد (به معنی عدم تقسیم زنجیره). Smart contract مبتنی بر proof of stake ، به کاربران امکان می

دهد برای هرگونه تغییر در سیستم ، از جمله بازنویسی های زنجیره ای ، رای دهند. از آنجا که رأی گیری در سکوی Tezos ترکیبی از حاکمیت زنجیره ای و رویدادهای خود اصلاح است ، فرایند رأی گیری می تواند با توجه به نیازهای جامعه اصلاح شود. استفاده از نسخه ای از مدل proof of stake (اثبات liquid) بدان معنی است که رای گیری در اینجا بر اساس سهم کاربران انجام می شود. سیستم رأی گیری مبتنی بر stake ، به این معنی است که هرچه کاربر از منابع مالی بیشتری برخوردار باشد ، تصمیم وی از ارزش بیشتری برخوردار است. اما از آنجا که کاربران متوسط قدرت مالی کافی ندارند ، Tezos تمایل دارد به سمت centralization حرکت کند. این مسئله مشابه دموکراسی مستقیم "قوانین اکثریت" را نشان می دهد. اما یک ویژگی به نام دموکراسی های تفویضی وجود دارد که در آن کاربران می توانند رای خود را به دیگران تفویض کنند ، و باعث می شود Tezos بیشتر به دموکراسی representative برسد.

:Decred

تصدیق مدل حاکمیت زنجیره ای مورد استفاده در Decred نسبتاً پیچیده است زیرا هدف آن انتقال قدرت به سهامداران و miner ها است. بلاکچین براساس حاکمیت رأی دادن دارندگان token است. Decred شامل سازوکار اجماع ترکیبی مبتنی بر proof of work و proof of stake برای دستیابی به آن است. پروژه ماهیت خود را دقیقاً مانند Dash تأمین می کند زیرا بخشی از هر پاداش بلوک به صندوق یارانه پروژه می رسد تا از توسعه بیشتر آن پشتیبانی کند. چیزی که در اینجا منحصر به فرد است این است که سهامداران از نحوه تخصیص این صندوق استقلال کامل دارند. جامعه می تواند پیشنهادهای مختلف بهبودی را ارائه دهد و سپس از طریق روند رأی گیری ticket ، در مورد بودجه پیشرفت های خاص رأی گیری کند. در اینجا تمام افرادی که در Decred سرمایه گذاری کرده اند می توانند در تصمیم گیری شرکت کنند. با این حال ، روند رأی گیری مستقیماً در On-chain اتفاق نمی افتد و بنابراین مورد شفافیت نگرانی ایجاد می کند.

: DFINITY

DFINITY با عنوان "رایانه اینترنتی" یک رایانه ابری غیرمتمرکز است. این یک مکانیسم حاکم الگوریتمی به نام (BLS) "Blockchain Nervous System" برای محافظت همزمان از کاربران در برابر حملات و همچنین بهینه سازی پویا حاکمیت و امنیت درون زنجیره ای به کار می برد. این ویژگی DFINITY را قادر می سازد تا در صورت هک شدن ، قابلیت بازنویسی زنجیره ای را فراهم کند. این یک مکانیزم اجماع proof of syake بسیار بهینه شده است. سازوکار رأی دهی ، رأی گیری حد نصاب نامیده می شود نوعی سازوکار رأی گیری مستقیم است که به عنوان "قانون اوباش" شناخته می شود. این پروژه هنوز به درستی راه اندازی نشده است. بنابراین ، اگرچه پتانسیل بالقوه است ، اما باید آزمایش شود.

: EOS

EOS نمونه دیگری از حاکمیت On-Chain است. از سازوکار توافق proof of stake (DPoS) استفاده می کند. هر کاربر یا شرکت کننده ای در اینجا باید برای باز کردن یک حساب در سیستم ، token های EOS را خریداری کند که به آنها حق رأی نیز می دهد. EOS به miner ها قدرت رأی نمی دهد.

نتیجه گیری پایانی : از بحث فوق مشهود است که هیچ حلقه ای وجود ندارد که بتواند بر همه آنها حکومت کند. همچنین ، هیچ روش مشخصی وجود ندارد که بتواند هر بلاکچینی را مدیریت کند. موارد مختلف استفاده نیاز به فرآیندهای مختلف حکومت دارند. آزمون و خطا ، خلاق بودن با روش های موجود ، نوآوری مداوم و بحث های سازنده و مفید ، بهترین مسیر ماست تا به راهی مناسب برای بلاکچین حکومتی نزدیک تر شویم. همانطور که در حال حاضر به نظر می رسد ، یک سیستم حاکمیتی ترکیبی از Off-Chain و On-Chain بیشتر احتمال دارد تا موفق باشد است ، اگرچه هیچ چیز قطعی نیست. مهم نیست که توسعه دهندگان کدام روش ها را برای تصمیم استفاده می کنند ، یک چیز همیشه درست خواهد ماند - تمام اجزای جامعه بلاکچین آنهایی را ترجیح می دهند که به بهترین شکل ، نیازهای آنها را تأمین کند.

Supply chain

بلاکچین فناوری ایجاد شده برای پشتیبانی از معاملات بیت کوین است. به گفته تشویق کنندگان آن، فناوری بلاکچین این پتانسیل را دارد که اثربخشی و سودآوری اکثر مشاغل را به ویژه در بخش مالی، افزایش دهد.

درک مفهوم بلاک چین

بلاکچین یک فناوری مبتنی بر اینترنت است که به دلیل توانایی در اعتبار سنجی عمومی، ثبت و توزیع معاملات در دفترهای رمزگذاری شده‌ی تغییر ناپذیر، بسیار ارزشمند است. این فناوری برای پشتیبانی از معاملات بیت کوین اختراع شده است، ارزش رمزنگاری شده دیجیتال که به طور مستقل از یک بانک مرکزی کار می‌کند. در حقیقت، فناوری بلاکچین بستر ایجاد و توزیع دفتر یا ثبت هر معامله بیت کوین را به هزاران، اگر نه میلیون ها رایانه متصل به شبکه ها در همه نقاط جهان، فراهم می‌کند.

از آنجا که معاملات و دفترها رمزگذاری شده اند، فناوری بلاکچین امنیت بیشتری نسبت به مدل بانکی ارائه می‌دهد و انتقال فوری آن از طریق اینترنت، روند تسویه حساب های دو تا سه روزه بانک ها و هزینه های همراه برای انتقال پول از یک حساب به حساب دیگر را از بین می‌برد. اصطلاح "بلاکچین" از "بلوک" معاملات معتبر و تغییرناپذیر و چگونگی پیوند آنها به ترتیب زمانی برای تشکیل یک زنجیره مشتق شده است. از این رو اصطلاح "بلاکچین" به کار می‌رود.

در حقیقت بلاکچین ها به دو نوع غالب وجود دارند. دفترهای توزیع شده "بدون مجوز" مانند بیت کوین در دامنه عمومی زندگی می‌کنند، در حالی که دفترهای "مجاز" توسط "بازیگران"، "گره ها" یا "استخراج کنندگان" متمرکز و اداره می‌شوند و در خارج از حوزه عمومی نگهداری می‌شوند. این تمایز در زمینه های زنجیره تأمین پیامدهای مهمی دارد.

ارزش بلاکچین در زنجیره های تأمین

در بیشتر موارد، زنجیره های تأمین امروزی در مقیاس و بدون فناوری بلاکچین کار می‌کنند. حتی در این صورت، این فناوری دنیای فناوری اطلاعات و زنجیره تأمین را به هیجان آورده است. این مقاله همچنین به بسیاری از مقالات الهام بخشیده و بازیکنان و شرکتهای نوپا را برای ایجاد پروژه های آزمایشی امیدوار کننده ترغیب کرده است، از جمله:

- Walmart برای تأیید اعتبار معاملات و صحت و کارایی نگهداری سوابق، برنامه ای را که برای ردیابی گوشت خوک در چین و تولید آن در ایالات متحده است، آزمایش کرد.
- Maersk و IBM در حال کار بر روی معاملات بین مرزی و بین حزبی هستند که از فناوری بلاکچین برای کمک به بهبود کارایی فرآیند استفاده می‌کنند.

- BHP در حال معرفی یک راه حل blockchain است که برای ردیابی نمونه های داخلی و خارجی از طیف وسیعی از ارائه دهندگان ، صفحات گسترده را جایگزین می کند.
- Provenance ، یک شرکت تازه تأسیس در انگلستان ، فقط 800,000 دلار جمع آوری کرد تا از فناوری بلاکچین برای ردیابی مواد غذایی استفاده کند. پیش از این به طور آزمایشی ردیابی ماهی تن را در زنجیره تامین جنوب شرقی آسیا انجام می داد.

این حال ، تا به امروز ، نویسندگان از هیچ برنامه کاربردی گسترده ای در زنجیره تامین مطلع نیستند ، و این یک سوال اساسی را ایجاد می کند: آیا فناوری بلاکچین می تواند به زنجیره های تامین ارزش افزوده دهد؟

همانطور که اکثر محققان می دانند ، بسیاری از زنجیره های تامین امروز داده های خوبی دارند ، که قادر به انتقال آنها در سطوح زنجیره تامین با سرعت نزدیک به زمان واقعی هستند. برای ارزیابی ارزش فناوری blockchain در معرض خطر برای دنیای زنجیره تامین ، ما سه حوزه را بررسی کردیم که می تواند ارزش مند باشد:

1. جایگزینی با فرایندهای آهسته و دستی: اگرچه در حال حاضر زنجیره های تامین می توانند مجموعه های داده بزرگ و پیچیده ای را اداره کنند، اما بسیاری از فرایندهای آنها ، به ویژه آنهایی که در سطوح پایین عرضه می شوند ، کند بوده و کاملاً به کاغذ متکی هستند و مانند این موارد هنوز در صنعت حمل و نقل معمول است.

2. تقویت قابلیت ردیابی. افزایش تقاضای نظارتی و مصرف کننده برای اطلاعات مربوط به منشأ باعث تغییر می شود. علاوه بر این ، بهبود قابلیت ردیابی با کاهش هزینه های بالای مشکلات کیفیت ، از جمله فراخوان ، آسیب به شهرت ، یا از دست دادن درآمد محصولات سیاه یا خاکستری ، ارزش افزوده است. ساده سازی یک پایه تامین پیچیده ، فرصت های ارزش آفرینی بیشتری فراهم می کند .

3. کاهش هزینه های معاملات IT با زنجیره تامین: در این مرحله ، این سود، بیشتر نظری است تا واقعی. بیت کوین برای تأیید اعتبار هر بلاک یا معامله به افراد اعتبار می دهد و به افرادی که بلاک جدیدی را پیشنهاد می دهند ، ملزم به پرداخت هزینه به پیشنهاد خود می پردازد. چنین هزینه ای احتمالاً در زنجیره های تامین گران باشد زیرا مقیاس آنها می تواند سرسام آور باشد. به عنوان مثال ، در یک دوره 90 روزه ، یک تولید کننده اتومبیل معمولاً تقریباً 10 میلیارد تماس برای تامین کنندگان سطح اول خود صادر می کند. همچنین ، همه این معاملات به طور قابل توجهی تقاضا برای ذخیره داده را افزایش می دهد ، یک جز اساسی رویکرد دفتر توزیع شده بلاکچین است. علاوه بر این ، ایجاد و نگهداری نسخه های بی شماری از مجموعه داده ها در محیط زنجیره تامین ، به ویژه در بلاک چین های غیر مجاز غیر عملی خواهد بود.

بزرگترین مانع بلاکچین: چه کسی اجازه می دهد؟

در اتخاذ فناوری بلاکچین برای زنجیره تأمین خود ، یک شرکت ابتدا باید در مورد نوع بلاکچین مورد نیاز خود تصمیم بگیرد. به یاد بیاورید که رویکرد بیت کوین یک بلاک چین بدون مجوز است و دارای افرادی است که شناخته شده یا مورد اعتماد نیستند. یک بلاچین از پروتکل تأیید اجماع برای ایجاد اعتماد در هر بلوک استفاده می کند. هیچ پایگاه داده مرکزی یا حاکمیت مرکزی در این بلاکچین ها وجود ندارد.

حریم خصوصی

برعکس ، در بیشتر زنجیره های تأمین ، طرفین شناخته شده و مورد اعتماد هستند. بعلاوه ، بعید است که دنیای زنجیره تأمین دسترسی آزاد را بپذیرد زیرا کاربران آن نمی خواهند جزئیات اختصاصی مانند تقاضا ، ظرفیت ها ، سفارشات ، قیمت ها ، حاشیه ها را در تمام نقاط زنجیره ارزش برای شرکت کنندگان ناشناخته فاش کنند. این بدان معنی است که اکثر زنجیره های تأمین زنجیره تأمین نیاز به اجازه دارند ، زیرا دسترسی به طور مرکزی کنترل می شود و فقط به اشخاص شناخته شده محدود می شود که ممکن است به بخشهای خاصی از داده محدود شوند.

از نظر تئوری ، این روش اجازه تأیید عمومی یا خصوصی هر بلوک پیشنهادی را می دهد. با این حال این که همه طرفین شناخته شوند ، بعید است. وقتی تعداد عناصر مورد اعتماد اندک باشد ، نیاز به اعتبارسنجی مستقل پروتکل های اجماع مورد استفاده در حوزه عمومی کم خواهد بود.

یک راه حل خوب و کافی بدون بلاکچین

در بسیاری از موارد ، زنجیره های تأمین در حال انتقال میلیاردها معامله و داده ، غالباً در زمان واقعی هستند. این سیستم ها کامل نیستند و بسیاری از زنجیره های تأمین با داده هایی روبرو هستند که قالب آنها متفاوت است ، دسترسی به آنها دشوار است و یا تجسم یا تجزیه و تحلیل آنها در متن داده های بزرگ دشوار است. حتی در این صورت ، امروزه می توان در مقیاس گسترده پایگاه داده های مرکزی مدیریت شده با مدیریت داده ها ، همراه با تجسم زنجیره تأمین و قدرت تحلیلی را به دست آورد.

این راه حل ها بار اضافی برخی از پیچیدگی های فنی که بلاک چین می تواند ایجاد کند را به دوش نمی کشد. بنابراین ، ما معتقدیم که وقتی در همه طرفهای زنجیره تأمین افراد شناخته شده و مورد اعتماد قرار بگیرند ، احتمالاً نیازی به راه حل بلاکچین نیست ، زیرا می توان به این احزاب شناخته شده و مورد اعتماد اعتماد کرد تا نسخه ای واقعی در زمان واقعی ارائه دهند. در چنین شرایطی ، راه حل های متمرکز مانند پورتال ابری یا اتصالات غیر متمرکز نظیر به نظیر کافی است.

تحقیقات ما نشان می دهد که فناوری بلاکچین در نهایت ممکن است راه حل خوبی برای برخی از انواع زنجیره های تأمین باشد ، اما هنوز برای تصویب انبوه آماده نیست. این دیدگاه را بر اساس موارد زیر قرار می دهیم:

- محققان بلاکچین که تا به امروز در این زمینه تحقیق کرده اند، ارزش منحصر به فرد این فناوری را در بخش زنجیره تأمین ثابت نکرده اند.
- فناوری بلاکچین هنوز قادر به گرفتن اطلاعات در میان تعداد زیادی از طرف های غیرقابل اعتماد نیست.
- ارائه شفافیت یا ردیابی کامل می تواند از راه های دیگری حل شود ، نه فقط با بلاکچین.
- هزینه توسعه و اجرای بلاکچین هنوز مشخص نیست و اکنون استانداردهای کمی وجود دارد.
- شکاف بین ظرفیت فعلی بلاکچین و ظرفیت مورد نیاز زنجیره های تأمین بسیار زیاد است.

برای زنجیره های تأمین که در آن شرکت کنندگان شناخته شده یا مورد اعتماد نیستند ، فناوری بلاکچین می تواند اعتماد ، شفافیت و قابلیت ردیابی ایجاد کند. طبق تعریف ، این زنجیره های تأمین پیچیده، احزاب زیادی را درگیر می کنند و در یک محیط تنظیم شده فعالیت می کنند که سطح بالاتری از قابلیت ردیابی را می طلبد.

با این حال ، برای زنجیره تأمین با بازیکنان شناخته شده و مورد اعتماد ، رویکرد پایگاه داده متمرکز به طور کلی بیش از کافی است. این بدان معنا نیست که تمام این زنجیره های تأمین در حال حاضر از یک رویکرد end to end پیروی می کنند و در واقع ، بسیاری از آنها از پایگاه داده هایی استفاده می کنند که فقط دارای قابلیت ردیابی محدود هستند. بنابراین ، بسیاری از این زنجیره های تأمین برای حل چنین مسائلی نیازی به فناوری بلاکچین ندارند ، زیرا می توانند از فناوری های موجود که مناسب تر برای معاملات پر حجم آنها است چه به صورت تنها و چه با همراه استفاده کنند.

برای تخمین هزینه های استفاده از فناوری بلاکچین در دنیای زنجیره تأمین و مقایسه آنها با سایر فناوری ها خیلی زود است. بدون شک ، شرکت های فناوری اطلاعات آمادگی ارائه این اطلاعات را خواهند داشت.

تعدادی از شرکت ها در حال بررسی مزایای استفاده از فناوری بلاکچین در مباحث مشابه هستند ، مانند معرفی قراردادهای هوشمند ، ایجاد سخت گیری بیشتر برای خرید سفارشات یا زنجیره های تقاضا که در آن سیگنال های "تقاضای واقعی" می توانند زنجیره تأمین بالادست را سریع تر گسترش دهند. در حالی که ما از قدرت و وعده فناوری بلاکچین استقبال می کنیم ، به جهان زنجیره تأمین توصیه می کنیم که زمانی را برای سنجش مناسب بودن خود در برابر سایر فناوری های احتمالاً ساده تر و کم هزینه اختصاص دهد.

Escrows

در حال حاضر ، ارزش کل بازار Cryptocurrency تقریباً با سرمایه بازار Apple مطابقت دارد. رونق اخیر این صنعت را هیجان انگیزتر کرده است ، اما همانطور که می بینیم ، فضای کافی برای رشد وجود دارد. به هر میزان که ارزهای Crypto بیشتر مورد استفاده قرار می گیرند ، بدون شک مقررات و قوانین نیز به دنبال آن خواهد رفت. با این حال ، اگر قصد دارید از آنها برای پرداخت هزینه کالاها و خدمات استفاده کنید ، می خواهید امنیت خود را حفظ کنید. می توانید درباره شخصی که در حال فروش یا خرید از شما است تحقیق کنید ، اما به خاطر داشته باشید کلاهبرداران معمولاً در فریب مردم مهارت دارند. اینجاست که یک سرویس escrow وارد می شود.

سناریوی ساده زیر را تصور کنید. علی به دنبال فروش یک بیت کوین است. رضا می خواهد خرید کند و پولش را هم دارد. علی انتقال پول را کامل انجام می دهد و رضا پول نقد و بیت کوین هر دو را نگه می دارد. در یک محیط دیجیتالی ، رضا می تواند علی را با چند پروفایل جعلی در شبکه های اجتماعی فریب دهد و بدون هیچ اثری ناپدید شود. کلاهبرداری مانند این یک روی دیگر سکه در دنیای دیجیتال است که این فضا به طور فزاینده ای به هم پیوسته است.

ما در این مثال از بیت کوین استفاده کردیم ، اما کلاهبرداری مشابه با هر محصول یا خدمتی قابل انجام است. در سناریوی ما ، یک سرویس سپرده می تواند این مشکل را قبل از بروز آن حل کند. به طور سنتی ، این توافقی است که شخص ثالث هنگام انجام معامله ، وجوه را بین خریدار و فروشنده نگه می دارد. مزیت اصلی این است که امنیت و آرامش روحی را برای هر دو طرف به ارمغان می آورد. در زمینه ارزهای crypto ، یک سرویس سپرده به همان شیوه کار می کند ، به افراد اجازه می دهد بدون در نظر گرفتن اعتماد به یکدیگر به خرید کالاها ، خدمات یا سایر ارزهای دیجیتال بپردازند.

با بازگشت به همان مثال ، علی می خواهد بیت کوین دیگری را بفروشد و این بار او بهتر می داند. محمد می خواهد خرید کند و او پول پرداخت هم دارد. علی به او می گوید که آخرین بار چه اتفاقی افتاده است و هر دو توافق می کنند که از یکی از خدمات نگهداری رمزارز در خارج از کشور استفاده کنند. علی بیت کوین خود را به شرکت نگهبان می فرستد ، محمد مبلغی را که آنها توافق کردند برای او می فرستد. وقتی علی مبلغ موردنظر را در حساب بانکی خود مشاهده کرد ، به شرکت محافظ اعلام می کند که می تواند بیت کوین را برای محمد ارسال کنند.

چند ماه بعد ، محمد تصمیم می گیرد لپ تاپ خود را بفروشد و خریداری را پیدا می کند که مایل است آنچه را که او شرط کرده است بپردازد ، اما او مطمئن نیست که پرداخت پول را انجام دهد زیرا او محمد را نمی شناسد یا به او اعتماد ندارد. او تجربه علی را به یاد می آورد و پیشنهاد می کند که آنها از همان خدمات escrow استفاده کنند. خریدار مبلغ توافق شده را برای شرکت ارسال می کند و محمد لپ تاپ را برای او ارسال می کند. هنگامی که خریدار آن را دریافت می کند ، او به شرکت اطلاع می دهد که همه کارها منظم است و آنها وجه موردنظر را به محمد می دهند.

با این حال ، گاهی توافق ها به همین سادگی نیستند. بیا بید تصور کنیم علی برای شرکتی کار می کند که به دنبال توسعه دهنده ای برای ساخت و مدیریت فعال وب سایت است. تکمیل این پروژه چند ماه به طول خواهد انجامید و چندین نقطه عطف در طول مسیر وجود دارد که با دستیابی به موفقیت ، پرداختی به سازنده داده می شود. علی یک توسعه دهنده باورنکردنی را پیدا می کند که تمایل دارد به او crypto داده شود. او که از اهمیت دستیابی به این حق آگاه است ، با روسای خود و توسعه دهنده موافقت می کند تا از یک سرویس escrow استفاده کند. پس از نهایی شدن شرایط توافق ، هر دو طرف در صورت وجود اختلافات احتمالی در توافق نامه ، یک قرارداد هوشمند را منعقد می کنند. شرکت سپرده می تواند واسطه آن باشد. قرارداد هوشمند می تواند سه سناریوی اختلاف زیر را منعکس کند:

جیمز و سازنده توافق می کنند: وجه پرداخت می شود یا سازنده علی را بازپرداخت می کند بدون اینکه واسطه درگیر شود توسعه دهنده و واسطه توافق می کنند : نقطه عطف به دست آمده است ، توسعه دهنده وجه را دریافت می کند. واسطه و جیمز توافق دارند: بودجه خود را پس می گیرد.

حال در مورد امنیت آن صحبت کنیم : اگر با یک شرکت معتبر روبرو هستید ، ایمن ترین گزینه شماسست. این سرویس ها بودجه شما را در cold storage نگه می دارند - در انزوای فیزیکی از هر سیستم IT - که این بدان معناست که امکان هک شدن آنها وجود ندارد. این سرویس های escrow بر روی بلاکچین اجرا می شوند ، بنابراین می توانید مطمئن باشید که اطلاعات شما نیز ایمن خواهد بود. به عنوان آخرین تفکر در مورد امنیت ، لازم به ذکر است که بسیاری از ICOها نیز به خدمات سپرده گذاری متوسل می شوند. آنها این کار را برای بهبود اعتبار پروژه انجام می دهند تا شرکت خود را به عنوان قابل اعتماد معرفی می کنند که در نهایت باعث جذب سرمایه بیشتر خواهد شد.