رویکرد سیستمی بر بلاک چین در بیت کوین

سینا پرهازه ، محمد امین میرزاگل تبار ، علی تازیکی ، زینب اکبری

تابستان ۱۴۰۰

چکیده

در این مقاله به تحلیل سیستمی ساختار بلاکچین در بیت کوین در هفت فصل پرداخته شده است. در فصل اول به مقدمه ای برای آماده شدن ذهن خواننده ، در فصل دوم به ارائه ی تعاریف و اصطلاحات لازم برای درک و فهم این مقاله ، در فصل سوم به تحلیل سیستمی بلاکچین برای شناخت اجزای آن ، در فصل چهارم به سطح بندی و دسته بندی سیستم برای شناخت دقیق تر اجزا و روابط و درک سلسه مراتب و سطوح سیستم ، در فصل پنجم به شناخت ساختار و پیچیدگی های این سیستم ، در فصل ششم به بررسی تغییر و تحول ، مرحله بندی و چرخه عمر این سیستم ، در نهایت در فصل هفتم به ارائه نتایج با استفاده از یکپارچه سازی و ترکیب پرداخته می شود.

۱ مقدمه

۱.۱ معرفی و صورت مسئله

اولین باری که نام بیتکوین را شنیدیم به سادگی از کنار از رد شدیم تا چند سال بعد همه نگاه ها و دوباره نگاه پر از حسرت ما به بیتکوین جلب شد چیزی که در ابتدا شبیه به سکه های مجازی در بازی های آنلاین بود و امکان تصور کاربردی برای آن وجود نداشت یادگیری درباره ی بلاکچین بیتکوین دور ریختن تمام باور های قدیمی درمورد پول یا طلا یا هرچیزی که به عنوان ذخیره ی ارزش استفاده میشود بود سیستمی که فساد و رشوه در آن معنی ندارد همچنین ما با بلاکچین توانستیم به دنیایی غیر متمرکز و بدون فساد فکر کنیم تمام هدف ما در این پروژه پاسخ به پرسش هایی مانند بیت کوین چیست؟،ساختار بیتکوین چگونه کار میکند؟،بیتکوین چه آینده ای خواهد داشت ؟ است

۲.۱ پیشینه و اهمیت موضوع

برای پی بردن به اهمیت موضوع بیتکوین باید به تاریخچه پول نگاه کنیم در ابتدا انسان ها از مبادله کالا به کالا استفاده میکردند به عنوان مثال ۱ کیلوگرم گوشت را با ۱۰ کیلوگرم نمک طرفین باهم مبادله میکردند این شیوه مبادله اشکالاتی به همراه داشت به عنوان مثال من اگر گوشت داشتم و نمک میخواستم نمیتوانستم فردی را پیدا کنم که نمک داشته باشد و یا گوشت بخواهد یا در این حالت شاد من چیزی نمیخواستم و میخواستم مقداری گوشت را پسانداز کنم در این حالت نمیتوانستم پس انداز کنم در اینجا بود که پای پول به میان آمد پول از نظر اقتصاد دانان کلاسیک سه ویژگی اصلی دارد ۱-واسط تبادل باشد،۲-واحد حساب باشد(یعنی بتوان بهای یک چیز را با آن تعیین کرد)،۳-ذخیره ارزش باشد یعنی چیزی که بتوان آن را ذخیره کرد که تا در آینده همچنان دارای ارزش است ابتدا سنگ به عنوان پول توسط مردمان اهالی یپ استفاده شد بعد ها به دلیل کمیابی طلا و نقره به عنوان پول استفاده شدند ولی باز خود طلا و نقره هم مشکلاتی داشتند بزرگترین مشکل آن ها مشکل حمل و نقل بود حمل مقدار زیادی طلا در سفر ها هم سخت و سنگین بود و هم خطرناک (دزدی توسط راهزنان در مسیر سفر) برای حل این مشکل مردم به سمت ضرب سکه و گرفتن فاکتور هایی از طلا حرکت کردند(فرد مقداری طلا را به انباری میسپرد و در ازای آن فاکتوری دریافت میکرد که نشان میداد این فرد صاحب این میزان از طلا است) این فاکتور که نشان دهنده مقدار خاصی از طلا و یا نقره بود همان پول کاغذی است همان دلاریست که مردم تا سال ۱۹۷۰ از آن استفاده میکردند

در واقع تا سال ۱۹۷۰ هرر دلار نشان دهنده ی میزان خاصی از طلا و یا نقره بود و شما با مراجعه به فدرال رزرو میتوانستید طلا و یا نقره متناسب با پولی را که داشتید دریافت کنید اما در دهه ی ۷۰ میلادی اتفاقی تاریخی در پول افتاد در ۱۵ اکتبر ۱۹۷۱ ریچارد نیکسون رئیس جمهور وقت آمریکا امکان دریافت طلا در ازای دلار را لغو کرد و به صورت غیر رسمی پایان عصر استاندارد طلا را اعلام کرد تلاش های دوباره برای بازگشت به استاندارد طلا بی نتیجه ماند و تا پایان دهه هفتاد میلادی تقریبا تمام کشور ها از استاندارد طلا خارج شدند پول بدون پشتوانه اثراتی مخربی مانند تورم (آنچه در ونزوئلا میبینیم) و رکود اقتصادی (همانند آنچه در ۲۰۰۸ در تمام دنیا رخ داد)، از انجا که انسان همواره به دنبال تمرکز زدایی قدرت بوده (به همین علت دموکراسی بوجود آمد) این ایده در ذهن فرد یا گروهی به نام ساتوشی ناکاموتو شکل گرفت که چرا به پولی درست نکند که به معنای واقعی محدود باشد نه مانند طلا که به هر حال محدود نیست و قدرت تصمیم گیری پولی جهان که در اختیار دول و بانک مرکزی هاست را از آن ها بگیرد جالب است بدانید در اولین بلاک بیتکوین ساتوشی ناکاموتو این پیام که از روزنامه تایمزبود را نوشت که نشریه تایمز/ ژانویه ۲۰۰۹/ رئیس خزانه در آستانه دومین کمک مالی به بانک ها ،این پیام به یکی از اخبار منتشر شده در روزنامه تایمز اشاره داشت مبنی بر اینکه رئیس خزانه وقت بریتانیا برای نجات بانک ها از بحران به دنبال کمک مالی به آن هاست ساتوشی با قرار دادن این پیام قصد داشت ضعف سیستم بانکداری و هدف بوجود آمدن بیتکوین را نشان بدهد جالب است بدانید از پایان عصر استاندارد طلا یعنی ۱۹۷۱ تا به امروز ارزش ۱۰۰ دلار امروز به اندازه ۱۴ دلار آن زمان است به عبارت دیگر دلار ۸۶ درصد از ارزش خود را از دست داده .

۳.۱ ساختار پژوهش

همانگونه که در بخش معرفی و صورت مسئله گفته شد ما به دنبال پاسخ به پرسش هایی مانند بیتکوین چیست ؟ ، ساختار بلاکچین بیتکوین به چه شکل کار میکند ؟، بیتکوین به کدام سمت حرکت میکند ؟، ما اجزا و اصطلاحات مربوط به بلاکچین بیتکوین را معرفی میکنیم و سپس دسته بنده و سطح بنده میکنیم و با تحلیل رفتاری و ساختاری خود بلاکچین بیتکوین و تحلیل رفتار جامعه در برابر همچین پدیده ای به سوالات مطرح شده پاسخ میدهیم

۲ تعریف شناسی

۱.۲ بلاکچین

به هرگونه سیستم غیرمتمرکز برای ثبت و ضبط هرگونه داده بلاکچین میگوند این داده ها هرنوع داده این میتواند باشد از اطلاعات تراکنش ها تا ویژگی های محصول و هرچیز دیگری بگذارید ساده تر بیان کنیم فرض کنید با چند نفر که همدیگر را نمی نشناسید همسفر شدید و یک نفر باید مادرخرج شود ولی هیچکس نیست که همه به آن اعتماد داشته باشند،کسی که حساب کتاب را درست بنویسد و چیزی را از یاد نبرد و دفترچه حساب را گم نکند و یا حتی تقلبی نکند یکی از بهترین راهکار ها این است که به جای این که یک نفر هر حسابی که انجام میشود را بنویسد همه ی افراد اینکار را بکنند در اینصورت زمان حساب کتاب نهابب اگر اختلافی هم بین حساب ها پیش بیاید میتوانیم مبنا را نظر اکثریت قرار دهیم بلاکچین تقریبا همین است.

۲.۲ نود

: در جواب این سوال ابتدا باید بدانیم شبکه زمان ارسال تراکنش چگونه کار میکند هنگام ارسال بیتکوین به شبکه شما اعلام میکنید که مقداری از حساب شما کسر شود و به حساب گیرنده واریز شود نود ها یا همان کامپیوتر های موجود در شبکه بیتکوین پیام شمارا دریافت کرده و آن را در دفاتر خود اعمال میکنند سپس پیام ها به دیگر نود ها پاس میدهند و به این ترتیب همه ی تراکنش را بررسی کرده و دفتر کل خود را بروز میکنند .

۳.۲ امضای دیجیتال و کلید های عمومی و خصوصی

وقتی یک چک را برای نقد کردن به بانک میبرید اولین چیزی که کارمند بانک برای انجام درخواست شما بررسی میکند چیست بدیهیست که امضای فرد دارنده ی دسته ی چک است در شبکه ی بیتکوین هم هر پیام تراکنش باید امضای معتبر داشته باشد تا قبول شود امضایی از جنس دیجیتال چیزی که نتوان آن را جعل کرد دردرون هر کیف پول بیتکوین دو رشته ی متنی وجود دارد که مجزا هستند اما باهم ارتباط مکمل دارند (کلید عمومی و کلید خصوصی)

هرکس برای ارسال بیتکوین باید پیام تراکنش را با کلید خصوصی کیف پولش امضا و به شبکه ارسال کند به این شکل بدون این که نیازه به استفاده از نام و مشخصات هویتی در شبکه بیتکوین باشد مشخص میشود که بیتکوین ها دقیقا از طرف کیف پول دارنده بیتکوین ارسال شده اند داشتن کلید خصوصی به منزله داشتن دارایی هاست و برای همین گفته میشود که هرگز نباید کلید خصوصی کیف پول خود را در اختیار فرد دیگری قرار بدهید

۴.۲ استخر استخراج

به دلیل بالا رفتن سختی شبکه بیتکوین و سخت بودن انجام عمل ماینینگ به صورت فردی ماینر ها به صورت گروهی در محل های مجازی که استخر استخراج نام دارند جمع میشوند تا برای استخراج از قدرت پردازش جمعی استفاده کنند به عبارت دیگر ماینر های سراسر دنیا دستگاه های استخراج خود را به استخر های معتبر متصل میکنند و استخر استخراج به نمایندگی از همه و مجموع قدرت پردازشی که دارد برای ماینینگ و به دست اوردن پاداش بلوک تلاش میکنند .

۵.۲ هش

هش در بلاکچین چیزی مانند اثرانگشت یا یک امضای منحصر به فرد است که به تنهایی نماینده تمام محتویات بلاک است اگر داده های داخل بلاک کوچکترین تغیری بکنند هش داخل بلاک هم عوض میشود و بلاک کاملا غیر معتبر میشود

۶.۲ هش بلاک قبل

از آنجا که هر هش محتویات و داده های اطلاعات بلاک خود را حمل میکند وجود هش بلاک قبلی داده های بلاک قبلی را به داده های فعلی مربوط میسازد و همین باعث میشود تا اطلاعات گذشته بلاکچین را نتوان تغیر داد پس یکی دیگر از اجزای مهم بلاک علاوه بر داده ها و هش ، هش بلاک قبلی است برای مربوط کردن و وصل کردن این بلاک ها

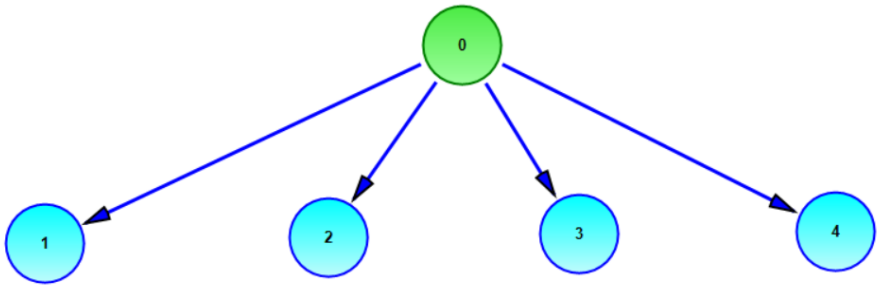
۷.۲ عدد نانس

یک عدد دلخواه است که توسط ماینر مدام عوض می‌شود و با عوض شدن آن هش هدر بلاک هم تغییر می‌کند، تا زمانی که این هش از هدف تعیین شده توسط شبکه مقدار کوچکتری داشته باشد و بلاک به اصطلاح استخراج شود.

۳ تحلیل سیستمی

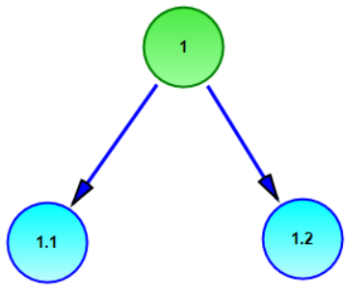
۱.۳ تجزیه سیستم به اجزا و روابط

به طور کلی اجزای تشکیل دهنده ی سیستم بلاک چین را می توان موارد زیر دانست که تعاریفشان در فصل ۲ ارائه شده است: انواع نود ها ، بلاک، زنجیره، پروتکل اجماع، امضای دیجیتال، هش بلاک قبلی، بدنه، اطلاعات تراکنش ها، تایم استمپ، ورژن، ریشه مرکل، کلید خصوصی و کلید عمومی. در ادامه این اجزا رو دسته بندی و بعضی را به عنوان زیرجز دیگر معرفی می کنیم. در این فصل یک تجزیه کلی از سیستم مورد نظر خواهیم داشت و در فصل بعد به موارد جزئی تر خواهیم پرداخت.
از آن جا که بلاک چین در حوزه های فراوانی کاربرد دارد، می توان هر یک از این حوزه ها را به عنوان زیر بخشی از کاربرد بلاک چین در نظر گرفت. این زیر بخش ها شامل ارزهای دیجیتال ، زنجیره تامین ، شبکه سلامت و ... می باشند. رابطه ی بین بلاک چین و این زیر بخش ها در شکل ۱ نمایش داده می شود. ۱ همان ارزهای دیجیتال، ۲ مربوط به زنجیره تامین و ۳ نشانگر شبکه سلامت است و گره ۴ نیز نماینده سایر کاربردهاست.



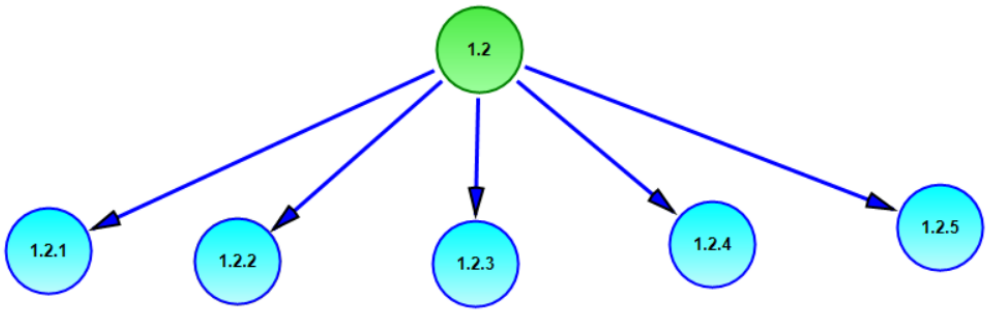
شکل ۱: ارتباط اجزا

همان طور که در فصل های گذشته ذکر شد، هدف ما بررسی رویکرد سیستمی بر بلاک چین در حوزه ارز های دیجیتال و به طور اختصاصی بر روی بیت کوین است. در نتیجه، گره شماره ۱ شکل بالا را ادامه می دهیم و به زیرجزهایش تجزیه می کنیم. در این تجزیه، زیر جز ارزهای دیجیتال به دو زیر جز بیت کوین و آلت کوین ها تجزیه و تقسیم می شود. این تجزیه در شکل۲ قابل مشاهده است؛گره۱.۱ مربوط به بیت کوین و گره ۱.۲ مربوط به آلت کوین هاست.



شکل ۲: ارتباط اجزا

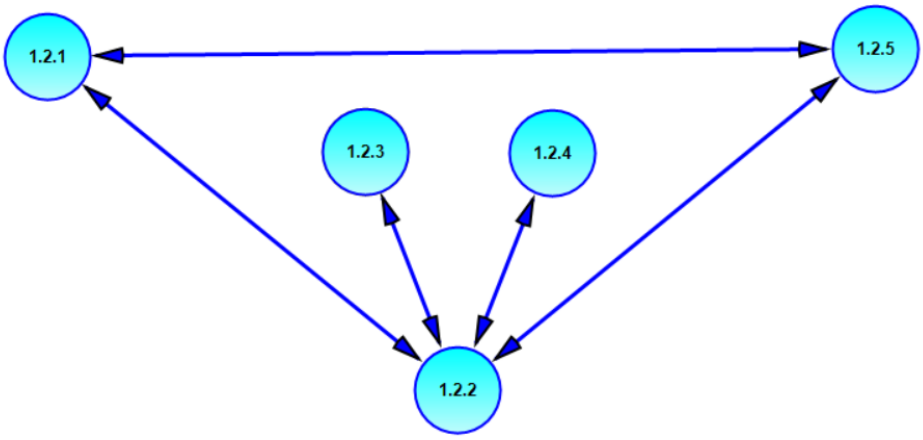
حال زیرجز بیت کوین را با توجه به تعریفاتی که در فصل گذشته داشتیم، می توان به زیرجز های خود تجزیه نمود. این زیر جز ها شامل نود، بلاک، زنجیره، امضای دیجیتال، پروتکل اجتماع می باشند. این تجزیه بندی در شکل ۳ پیاده شده است. گره ۱.۲.۱ نشانگر نودها، ۱.۲.۲ نشانگر بلاک، ۱.۲.۳ نشانگر زنجیره،۱.۲.۴ مربوط به امضای دیجیتال و ۱.۲.۵نیز مربوط به پروتکل اجماع می شود.



شکل ۳: ارتباط اجزا

۲.۳ ارتباط میان اجزا

بین زیر جز های شکل بالا ارتباطاتی وجود دارد. ارتباط میان نود و بلاک و الگوریتم اجماع : می دانیم تراکنش های جدید و تایید شده ی بلاک در فضایی به اسم memory pool یا استخر حافظه هستند و تمام نودها به این استخر دسترسی دارند. تراکنش های جدید موقتا آن جا قرار دارند تا این نودها شروع به چیدن آن ها در یک بلاک جدید می کنند و همزمان کار هش کردن این بلاک هم شروع می شود تا عدد مورد نظر (کوچکتر/مساوی عدد مشخص شده ی فعلی) پیدا شود. یک بلاک دائما در حال آپدیت شدن با تراکنش های جدید و همینطور هش شدن توسط نودهاست، تا وقتی که جواب درست پیدا شود. زمانی که یک ماینر پاسخ یک معما را که در واقع هش یک بلوک است را پیدا می‌کند، آن بلوک را به شبکه ارسال می‌نماید. سایر ماینرها این پاسخ را تایید می‌کنند (الگوریتم اجماع) و بلوک مذکور طی مدت کوتاهی تایید می‌شود. ارتباط میان بلاک و زنجیره : ثبت شدن هش بلاک قبلی در بلاک جدید و ثبت شدن هش بلاک مذکور در بلاک بعدی نشانگر ارتباط میان بلاک مذکور با زنجیره است. ارتباط میان امضای دیجیتال و بلاک : همان طور که می دانیم، از طریق تایع هش امضای دیجیتال مخصوص به بلاک تخصیص داده می شود و امنیت بلاک تضمین می شود. با استفاده از اطلاعات فوق می توانیم ارتباط میان اجزا را به صورت شکل زیر نشان دهیم.

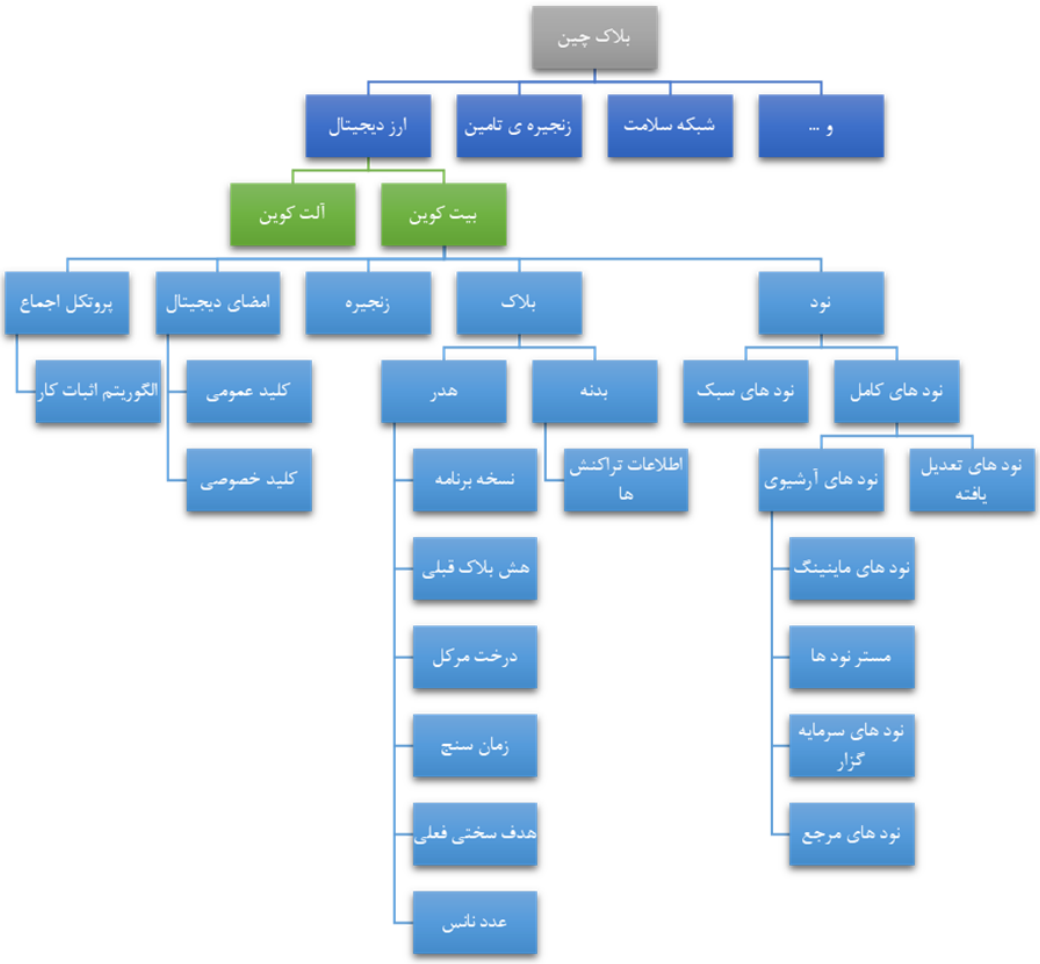


شکل ۴: ارتباط اجزا

۴ دسته بندی و سطح بندی

۱.۴ دسته بندی اجزا و روابط با تکیه بر مشخصه های اصلی

ما در این فصل اجزایی که در فصل ۳ تجزیه شده بود را با توجه به مشخصه ها و روابط دسته بندی میکنیم تا بتوانیم به بررسی این اجزا و روابط این سیستم به صورت دقیق و هدفمند بپردازیم. در شکل زیر دسته بندی اجزا و روابط را مشاهده میکینم:



شکل ۵: دسته بندی اجزا

۲.۴ شناخت دقیق تر هر کدام از اجزا و روابط

۱.۲.۴ نود های سبک

نودهای سبک یا Simplified Payment Verificatio نوع دیگری از نودهای بلاکچینی هستند. این نودها برای دریافت اطلاعات ضروری و برقراری ارتباط با بلاکچین به نودهای بلاکچینی کامل متکی هستند. این نودها یک کپی از زنجیره را ذخیره نمی‌کنند و فقط با جستجوی وضعیت فعلی بلاکچین بلاک آخر را مشخص کرده و تراکنش‌ها را برای پردازش انتقال می‌دهند. از آنجایی که نودهای spv یک نسخه از بلاکچین را ذخیره نمی‌کنند نیاز به منبع زیادی ندارند و در تامین امنیت شبکه نیز نقشی ندارند.

۲.۲.۴ نود های کامل

فول نودها یا نودهای کامل، نودهایی هستند که بصورت مستقیم به شبکه اصلی بلاکچین ارز دیجیتال متصل می‌شوند و با پذیرش کامل مقررات شبکه به عملکرد آن کمک می‌کنند. وظیفه این نودها حفظ اجماع بین نودهای بلاک‌چین،

تایید تراکنش‌ها و کپی‌برداری از بلاک‌چین است. فول نودها با ذخیره کردن یک نسخه کامل از بلاکچین ارز دیجیتال که حاوی تمام بلاک‌ها و تراکنش‌های شبکه آن می‌باشد، امنیت و صحت داده‌ها را با اعتبارسنجی تضمین می‌کنند. در واقع فول نودها ستون فقرات شبکه هستند. هر چه تعداد این فول نودها در شبکه افزایش یابد امنیت شبکه نیز بیشتر می‌شود.

نودهای بلاک‌چینی کامل در تصمیم‌گیری‌های آینده شبکه نقش موثری دارند. هنگامی که برای آینده شبکه یک ارز دیجیتال تصمیم‌گیری می‌شود باید حداقل ۵۱ درصد نودهای کامل موافق این تغییرات باشند تا در شبکه اعمال شوند. در برخی موارد که جامعه یک ارز دیجیتال نمی‌توانند بر روی یک تغییر توافق کنند راه خود را از هم جدا می‌کنند. این امر منجر به هاردفورک می‌شود.

۳.۲.۴ نود های تعدیل یافته

نودهای بلاک‌چینی تعدیل یافته یکی از انواع نودهای کامل می‌باشند. این نودها بلاک‌ها را از ابتدا شروع می‌کنند و تا زمانی که این دانلودها به محدوده خاصی برسند، قدیمی‌ترین باک‌ها را حذف کرده و تنها هدرها (Headers) و موقعیت زنجیره را نگهداری می‌کنند. فرض کنید محدوده ذخیره‌سازی نود ۵۵۰ مگابایت تعیین شود؛ در این حالت این نود ابتدا تمام بلاک‌ها را اعتبار سنجی می‌کند. سپس آخرین بلاک‌هایی که در بلاک‌چین ایجاد شدند را به اندازه حجم ۵۵۰ مگابایت ذخیره می‌کند. نودهای تعدیل یافته به عنوان نود کامل شناخته می‌شوند و می‌تواند در تایید تراکنش‌ها و اجماع شرکت کنند.

۴.۲.۴ نود های آرشیوی

در بیشتر موارد هنگامی که مردم درباره نودهای کامل صحبت می‌کنند منظورشان نودهای آرشیوی است. تصور آنها از نودهای آرشیوی یک سرور می‌باشد که کل بلاکچین را در پایگاه داده‌اش ذخیره کرده است. همانطور که در ابتدای بحث بیان شد، نودهای کامل وظیفه حفظ اجماع و اعتبارسنجی بلاک‌ها را برعهده دارند. نودهای آرشیوی و تعدیل یافته در فضایی که هارد درایو یا کامپیوتر اشغال می‌کند با هم متفاوت هستند.

۵.۲.۴ نود های ماینر

ماینرها نودهایی هستند اثبات می‌کنند کار مورد نیاز برای خلق یک بلاک در بلاک چین به پایان رسیده است. ماینرها یا باید خودشان نود کامل آرشیوی باشند و یا داده‌ها را از نودهای کامل دیگر دریافت کنند. این کار به آنها کمک می‌کند درباره وضعیت کنونی بلاک چین و پارامترهای لازم برای بلاک بعدی را در اختیار داشته باشند. ماینرها با استفاده از سخت افزارهایی مانند سی پی یو و کارت گرافیک معادلات ریاضی پیچیده را حل می‌کنند و از این طریق در فرآیند خلق یک بلاک مشارکت می‌کنند. در این فرایند اولین فردی که معادله را حل کند و اصطلاحا وظیفه را تکمیل نماید، نتایج بدست آمده را به شبکه گزارش می‌دهد و پس از اجماع و تایید نودهای کامل می‌تواند بلاک مورد نظر را به زنجیره اضافه کند و بابت مشارکتشان در این فرآیند پاداش دریافت کنند.

۶.۲.۴ نود های سرمایه گذار

بدست آوردن پول در مکانیزم گواه اثبات سهام مشابه شرکت کردن در قرعه کشی می‌باشد. هدف نهایی این مکانیزم این است که با استفاده از قوانین از پیش تعیین شده و براساس شانس مشخص شود که بلاک بعدی زنجیره را چه کسی ایجاد کند و بابت آن پاداش بگیرد. تعداد، نسبت کوین‌های فرد با کوین‌های موجود در شبکه و مدت زمانی که فرد مالک کوین‌ها بوده است از عواملی می‌باشد که در افزایش شانس فرد برای دریافت پاداش تاثیر می‌گذارد و احتمال انتخاب او را بالا می‌برد. استفاده از این روش نیازی به سخت‌افزارهای گران قیمت ندارد. برای اینکه یک فرد بتواند سرمایه گذار باشد باید به یک نود آرشیوی تبدیل شود. این بدان معناست که کیف پول هسته کوین مورد نظر را دانلود کند و کل بلاکچین را بر روی ابزار خود نگهداری نماید و همیشه کیف پول خود را باز نگه دارد.

۷.۲.۴ نود های مرجع

نودهایی که تا به اینجای بحث بررسی کردیم، نودهایی هستند که می‌توانند به شبکه یک ارز دیجیتال ملحق شوند و وظایفشان را بصورت غیر متمرکز و بدون اجازه گرفتن از کسی انجام دهند. اما استفاده از این رویکرد اشکالاتی

نیز دارد. راه حل رفع این ایرادات بکارگیری سطوحی از تمرکز می‌باشد. در این حالت شبکه‌ها از الگوریتم‌هایی مانند الگوریتم‌های اجماع شامل گواه اثبات سهام خصوصی شده، تحمل خطای بیزانس عملی ، گواه اثبات مرجع استفاده می‌کنند. استفاده از این الگوریتم‌ها شبکه را ملزم می‌کند تعدادی از نودهای بلاکچینی را به عنوان نود مرجع انتخاب کنند. این که چه تعداد نود مرجع در شبکه وجود داشته باشد و یا اینکه چه کسانی به عنوان نود مرجع انتخاب شوند، یا با رای گیری و یا توسط تیم توسعه دهنده مشخص می‌شود. نودهای بلاکچینی مرجع در کنار وظیفه ایجاد و اعتبارسنجی بلاک‌ها باید همزمان اطلاعات را نیز در اختیار کاربران شبکه قرار دهند. چرا که نودهایی که به عنوان نود مرجع انتخاب نشده‌اند برای فعالیت در بلاکچین به این داده‌های گزارش شده احتیاج دارند.

۸.۲.۴ مستر نود ها

مستر نودها در شبکه بلاک‌چین با هدف ذخیره تراکنش‌ها و اعتبار سنجی به آن‌ها ایجاد شده‌اند. این نودها نمی‌توانند یک بلاک را به شبکه بلاک‌چین اضافه کنند. مستر نودهای ماینر یا سرمایه گذار، کسانی هستند که بلاک‌ها را بر روی زنجیره بلاک می‌نویسند. مستر نودها به ایمن شدن شبکه کمک می‌کنند و برای سرویس‌هایی که اراده می‌دهند پاداش دریافت می‌کنند. برای تبدیل شدن به مستر نود فرد باید مقداری وجه را به عنوان وثیقه، نگه‌داری کنند و دائم آنلاین باشد. هم‌چنین بهتر است برای ارائه خدمات میزبانی خود از یک سرور خصوصی مجازی استفاده کند.

۹.۲.۴ هدر بلاک

بلاک هدر به شش جز تقسیم می‌شود:

۱. شماره‌ی نسخه‌ی برنامه (Bitcoin Version Number)

۲. هشِ بلاک قبلی (Previous Block Hash)

۳. ریشه‌ی هشِ درخت درهم سازی یا درخت مرکل (Merkle Tree)

۴. زمان‌سنج از تاریخ ۱ ژانویه‌ی ۱۹۷۰ (Timestamp Unix)

۵. هدف سختی فعلی (Difficulty Target)

۶. عدد تصادفی نانس (Nonce)

هش بلاک قبلی: هش بلاک قبلی ، اصطلاحاً زنجیره بلاکچین است. از آنجا که هش بلاک قبلی در هش بلاک جدید موجود است ، بلاک های بلاکچین همگی بر روی یکدیگر بنا می شوند. بدون این مولفه ، هیچ ارتباط و ترتیب زمانی بین هر بلاک وجود نخواهد داشت.

ریشه هش درخت مرکل: تمام تراکنش های موجود در یک بلاک می توانند در یک هش جمع شوند که این هش ریشه درخت مرکل است.

زمان‌سنج از تاریخ ۱ ژانویه‌ی ۱۹۷۰ : یک مهر زمان در خود بلاک. زمان از ۱۹۷۰.۱.۱ در چند ثانیه داده می شود

هدف سختی: هدف نشان می دهد که هش جدید برای ادعای اعتبار باید چقدر کوچک باشد. به عبارت دیگر ، هر هش یک بیت اندازه دارد. هرچه هدف در بیتها پایین تر باشد ، یافتن یک هش منطبق با آن مشکل تر است. هش با تعداد زیادی صفر در ابتدا کوچکتر از هش بدون صفر است.

عدد تصادفی نانس: متغیری است که با اثبات کار افزایش می یابد. به این ترتیب ، ماینر یک هش معتبر را

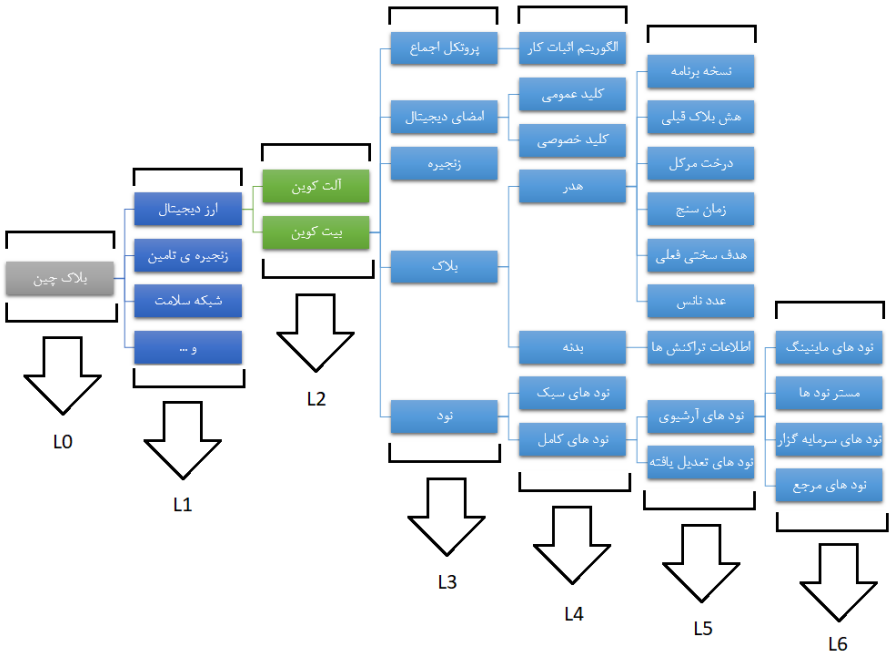
حدس می زند ، هشی که کوچکتر از هدف است. شش مولفه هدر بلاک را تشکیل می دهند. هدر بلاک در بیت کوین نقش اساسی دارد زیرا همه بلاک ها را به یکدیگر متصل می کند.

بدنه ی بلاک: بدنه بلاک همانند فضای بارگیری یک کامیون تصور می شود. این شامل همه معاملات تایید شده با بلاک است. وقتی یک ماینر یک بلاک می سازد ، معاملات را معتبر می داند. یعنی بررسی می کند که فرستنده در واقع پول کافی برای پرداخت کردن دارد. او می تواند به راحتی این اطلاعات را از بلاکچین بخواند. ماینر در بلاک های گذشته نگاه می کند تا ببیند که فرستنده حتی اگر بخواهد ده بیتکوین بفرستد یا حتی ده بیت کوین بدست آورده است یا خیر. معاملات در یک بلاک فقط در یک لیست نیست ، بلکه در اصطلاحاً درخت مرکل وجود دارد.

درخت مرکل: درخت مرکل نام خود را از ریاضیدان رالف مرکل گرفته است. کشف او این بود که اطلاعات زیادی را می توان در یک هش نمایش داد. برای همین، دادهها ابتدا هش می شوند. سپس هش ها مجددا هش آنها صورت می گیرد و ادغام می شوند. سرانجام ، درخت مرکل در یک هش واحد ادغام می شود. این هش آخر را ریشه هش، ریشه درخت نیز می نامند. این اطلاعات مربوط به "برگها" (معاملات فردی) و "شاخه ها" (هش برگها) خود را در یک رشته نسبتاً کوتاه نشان می دهد. ایجاد هش ریشه به شرطی که همه شاخه ها و برگ ها شناخته شده باشد ، سریع و آسان است. عملکرد یک تابع هش را مرور می کنیم: این کار به وضوح و به سرعت در یک جهت کار می کند و تجزیه آن در جهت دیگر غیرممکن است. اگر ریشه هش شناخته شده باشد ، اما معاملات ناشناخته باشند ، حدس تراکنش ها غیرممکن است. بنابراین یک هش ریشه به تنهایی کافی نیست و بقیه بلاک باید ذخیره شود. بنابراین ، استخراج کننده می تواند هش ریشه را در هر زمان با اعتبار سنجی مجدد اطلاعات موجود در بلاک ، اعتبارسنجی کند. تا زمانی که عملکرد هش یکسان باشد ، استخراج کنندگان همیشه هشی کسان را برای ورودی داده دریافت می کنند. این بسیار مفید است زیرا آنها فقط می توانند در یک سطح از هش بودن را بررسی کنند.

۳.۴ سطح بندی اجزاء و روابط و ارایه سسله مراتب سیستم و زیرسیستم های آن بر اساس معیارهای مورد نیاز

حالا که دسته بندی انجام گرفت و اجزا و ارتباطات بین آن ها به طور کامل تشریح شده اند میخواهیم به سطح بندی سیستم و سلسله مراتب آن بپردازیم. در شکل زیر به سطح بندی و سلسله بندی سیستم پرداخته شده است که برای درک بهتر و ساده تر به صورت شکل زیر آورده شده است:



شکل ۶: سطح بندی سیستم

همچنین در نمودار با توجه به شاخه های نمودار، تمام سیستم ها ، زیر سیستم ها و زیر زیر سیستم ها و ... مشخص شده است.

۵ شناخت ساختار و پیچیدگی

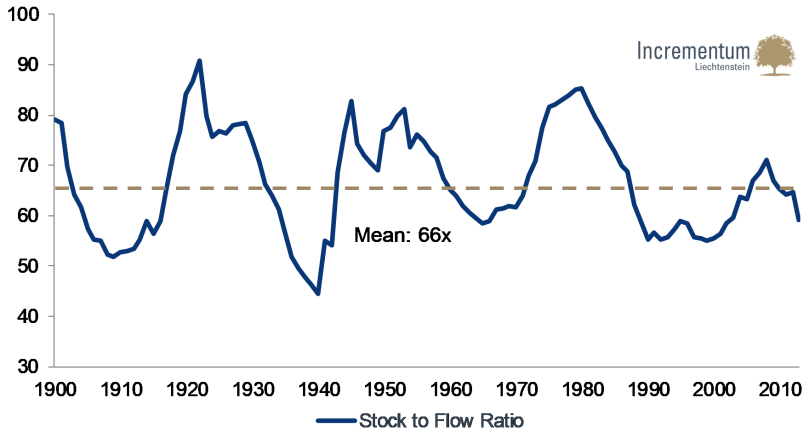
۱.۵ شناخت ساختاری بلاکچین بیت کوین

با شناخت ساختاری بلاکچین بیتکوین ما میتوانیم نسبت به ریسک های این دارایی آگاه تر شویم در ادامه به چند ویژگی و ریسک مهم ساختاری بلاکچین بیت کوین اشاره میکنیم

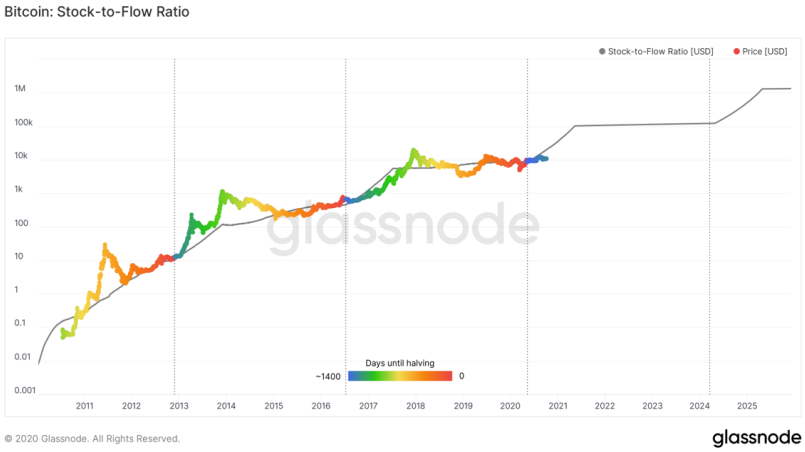
۱.۱.۵ کمیابی

انسان همواره به دنبال دارایی ای بوده که به معنای واقعی نامحدود باشد و تورم نداشته باشد در طی سالیان طلا بدلیل کمیابی و عرضه بسیار کم به عنوان کالای ذخیره ارزش استفاده میشد اما طلا به معنای واقعی کمیاب نیست و طلا هم در طی زمان به دلیل استخراج آن تورم دارد

شاخص انباشت جریان همانطور که از اسم این شاخص هم مشخص است این شاخص معیاری برای کمیابی دارایی ها است و نسبت کل موجودی از دارایی ره به نسبت عرضه ای که آن دارد میسنجد در واقع این شاخص نشان میدهد که چند سال طول میکشد که همان مقدار از دارایی که داریم را دوباره استخراج کنیم



شکل ۷: شاخص انباشت جریان طلا



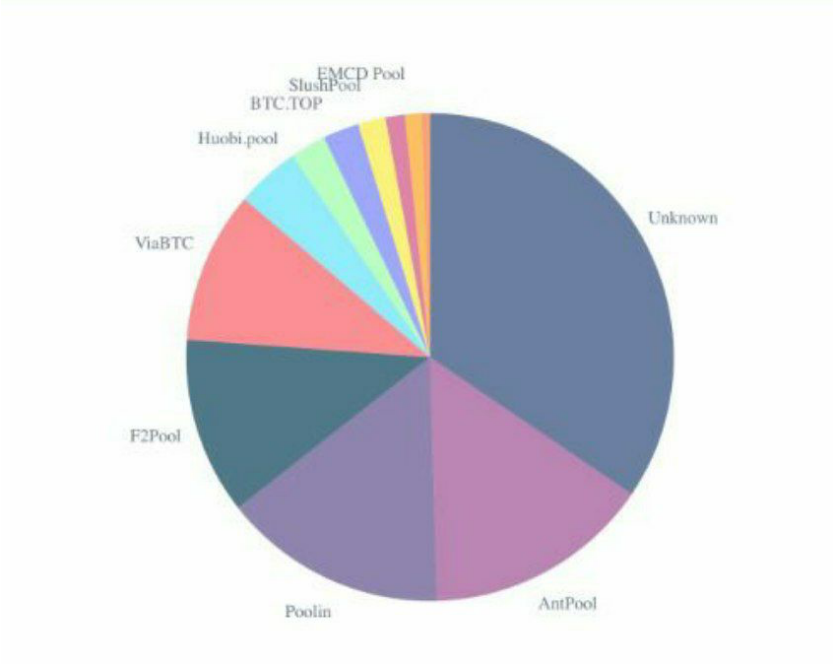
شکل ۸: شاخص انباشت جریان بیتکوین

همانطور که در شکل بالا مشاهدی میکنید شاخص انباشت به جریان طلا بسیار کمتر از بیتکوین است و روند عرضه طلا هم با پیشرفت تکنولوژی در حال افزایش است ولی بیتکوین چون برنامه نویسی شده و یا فرمول ریاضی نوشته شده اثبات شده است که به معنای واقعی کمیاب است

۲.۱.۵ نامتمرکز بودن

از زمانی که بشر متوجه رابطه ی بین قدرت و فساد شد به دنبال نامتمرکز کردن بوده از نامتمرکز کردن قدرت در سیستم سیاسی کشور ها تا نامتمرکز کردن قدرت خلق پول از نظر فنی و ساختاری بیت کوین نه تنها اولین بلکه نامتمرکز ترین ارز در جهان است نامتمرکز است چون هیچ مسئول فنی یا بانک مرکزی ای آن را کنترل نمیکند عرضه ی آن مشخص و ثابت است و شعب این بانک به صورت ماینر در سرتاسر جهان هستند تصویر زیر نشان دهنده

قدرت استخر های استخراج بیت کوین به قدرت هش ریت کل شبکه است در این شکل به خوبی غیر متمرکز بودن را میتوانید ببینید تازه در صورتی که قدرت استخراخ یک استر زیاد شود ماینر ها با قطع کردم ماینر خود با آن استخر و وصل کردن آن به استخر رقیب این تعادل را ایجاد میکنند



شکل ۹:

۳.۱.۵ ریسک حمله ۵۱ درصد

اگر یکی از نود های شبکه بیش از ۵۰ درصد قدرت شبکه را داشته باشد (از انجا که بلاکچین با رای اکثریت ۵۰ درصدی کار میکند) میتواند و در بلاک ها تغیر ایجاد کند و در حساب خود بیت کوین بریزد و یا دوباره بیت کوینی را خرج کند . باید در موضوع را در بررسی ریسک حمله ۵۱ درصدی در نظر بگیریم **آیا با توجه به وضعیت حال حاضر رسیدن به قدرت ۵۱ درصدی شدنیست**؟ نرخ هشریت شبکه بیت کوین ۱۲۳۹۷۶۸۹۵ ترا هش بر ثانیه است برای رسیدن به نصف قدرت شبکه ما به ۷.۱ میلیون دستگاه s19pro(قوی ترین دستگاه بازار) نیاز داریم با درنظر گرفتن میانگین قیمت ۱۰ هزار دلاری برای هر دستگاه ما به ۱۷ میلیارد دلار بودجه نیاز داریم (در نظر داشته باشید که درامد فدرال رزرو ۸۸ میلیارد دلار بوده) پس با توجه به محاسبات بالا تقریبا حمله ۵۱ درصدی توسط سازمانی غیر از دولت ها آن هم دولت های بزرگ غیر ممکن است

فرد هکر با رسیدن به قدرت ۵۱ درصد از کل شبکه با توجه به منافع خود این کار را میکند ؟ با فرض آن که هکری به نصف قدرت شبکه برسد با توجه هزینه فرصت آن آیا تغیری در بلاک و نود ها به نفع خود انجام میدهد ؟ برای پاسخ به این سوال باید درک کنیم چه اتفاقی میفتد وقتی تغیری در بلاک ها رخ میدهد به محض آن که تغیری در بلاک ها رخ بدهد بقیه نود ها متوجه این تغیر خواهند شد و همه متوجه حمله ۵۱ درصدی میشوند و پذیرش عمومی این ارز زیر سوال میرود و پیشبینی میشود که قیمت آن تقریبا به صفر برسد بنابراین ارزش زیادی به هکر نمیرسد در صورتی که کسی که ۵۱ درصد قدرت شبکه را داشته باشد میتواند با استفاده از قدرت پردازشی بالای خود و تایید تراکنش ها نصف بیتکوین های عرضه شده را مال خود کند و از این جهت درامد و سود بسیار بیشتری خواهد داشت پس با درنظر گرفتن هزینه فرصت تغیر دادن بلاک ها منطقی به نظر نمیرسد

۲.۵ شناخت رفتاری بلاکچین بیتکوین به کمک نوسانات قیمت

با توجه به رشد های بسیار بزرگ قیمت بیتکوین(۱۰۰۰ درصدی) هر چهار سال یکبار(اشاره به فرآیند هاوینگ) میتوان فهمید که در عرضه و تقاضای این دارایی اتفاقات اساسی ای میفتد و میتوان این برداشت را کرد که پذیرش بیت کوین به عنوان یک دارایی توسط جامعه روز به روز بیشتر میشود با توجه به تراکنش ها با کارمزد زیاد و کند میتوان این برداشت را کرد که مردم به بیت کوین به دید طلا و مانند دارایی برای ذخیره ارزش نگاه میکنند نه به دید ارز و واسطه برای دریافت کالا و خدمات

شکل ۱۰: نمودار قیمت بیتکوین

همانطور که در شکل فوق مشاهده میکنیم ما بدون این که با ساختار بلاکچین بیتکوین و نحوه عرضه آن آشنا بشویم مشاهده میکنیم که هر چهار سال یکبار جهش های بزرگ قیمتی در بیت کوین داریم و با توجه به صحبت های افرادی مانند ایلان ماسک ، چانگ پنگ ژائو و نظر اکثر صاحب نظران میتوان این ارز را وسیله ای برای ذخیره ارزش و طلای دیجیتال دانست و نه پول دیجیتال

۳.۵ تعیین سهم شناخت ساختاری یا رفتاری در بررسی موضوع پژوهش

برای شناخت بلاکچین بیتکوین باید با نحوه ی عملکرد آن آشنا شد و هم به صورت فنی و ساختاری آن را شناخت و هم به صورت رفتاری که به نظر میرسد قیمت آن مناسب ترین عنصر برای تحلیل رفتاری این دارایی باشد موضوع پروژه ما با هدف معرفی و تحلیل بلاک چین بیت کوین و جواب دادن به پرسش های بلاکچین بیتکوین چیست از کجا آمده است و به کجا میرود است برای تحلیل درست وضعیت این بلاکچین هم باید ساختار و هم باید رفتار آن را مورد تحلیل قرار داد اما از انجا که اطلاعات کافی برای تجزیه تحلیل ساختاری را داریم سعی داریم کفه ی ترازو را به شناخت ساختاری سنگین تر بکنیم

۴.۵ میزان پیچیدیگی بلاکچین بیتکوین

۱.۴.۵ پیچیدگی مفهومی

همانطور که میدانید پیچیدگی مفهومی به شناخت ما از اجزا و روابط سیستم بستگی دارد هرچقدر که ما اجزا سیستم را بهتر بشناسیم پیچیدگی مفهومی سیستم برای ما کمرنگ تر خواهد شد ما در این بخش به پیچیدگی های مفهومی

ای که ممکن است برای اغلب افراد از اجزا و روابط این سیستم پیش بیاید پاسخ میدهیم

مفهوم ماینینگ:

ماینر ها مانند شعب بانک ها تراکنش ها را از حسابی به حساب دیگر انجام میدهند و سیستم بلاکچین برای این که انگیزه قرار دهد که افراد این تراکنش ها را تایید کنند تراکنش ها را در بلاک هایی که هر ده دقیقه ی یک بار عوض میشوند ثبت میکنند و از هر بلاک مقدار مشخصی بیت کوین به عنوان جایزه به ماینر خواهد رسید علاوه بر بیتکوینی که از کامرمزد تراکنش ها بدست می آید به این فرایند تایید تراکنش و جایزه بیت کوینی گرفتن ماینینگ میگویند .

تراکنش چگونه انجام میوشد:

وقتی درخواست تراکنش شما به شبکه ارسال میشود اولین کاری که شبکه میکند چک کردن این است که آیا آن مقدار بیت کوین در حساب شما قرار دارد یا خیر در صورت وجود داشتن آن مقدار بیتکوین از حساب شما خارج شده و وارد مم پول میشود و بعد از تایید بلاک و پیدا کردن هش بلاک توسط ماینر ها آن مقدار بیت کوین از مم پوب به حساب دیگر ارسال میشود

۲.۴.۵ پیچیدگی محاسباتی

ساختار بلاکچین بیت کوین به این دلیل که از عناصر و مولفه های زیادی تشکیل نشده است بیشتر دارای پیچیدگی های مفهومی است تا پیچیدگی محاسباتی ولی از مفهوم پیچیدگی محاسباتی به خوبی در ساختار بلاکچین بیت کوین استفاده شده است .

استفاده از p-problems در بلاک چین بیتکوین

ساعت زمانی بلاکچین بیت کوین بر حسب بلاک هاست به عنوان مثال بعد از هر ۲۱۰،۰۰۰ بلاک عرضه بیت کوین و جایزه ماینر ها نصف میشود و با در نظر گرفتن میانگین ۱۰ دقیقه ای برای هر بلاک این مدت زمان چیزی حدود ۴ سال خواهد بود اما چگونه میشود که هر بلاک در مدت ۱۰ دقیقه هش آن توسط ماینر ها پیدا میشود و ما وارد بلاک بعدی میشویم . برای این که بلاک خا به بلاکچین اضافه شوند هر بلاک باید دارای جواب مسئله ریاضی پیچیده باشد با استفاده از تابع هش تنها راه حل کردن این مسئله ریاضی حدس زدن اعداد است و هر ماینری که زود تر جواب سوال این مسئله ریاضی را پیدا بکند جایزه بلاک را دریافت میکند و آن بلاک را به بلاکچین اضافه میکند و باز ماینر ها به دنبال حل مسئله ی بلاک بعدی میروند این فرایند اظافه شدن بلاک ها باید هر ۱۰ دقیقه یک بار اتفاق بیفتد اما با قوی تر شدن قدرت پردازشی شبکه و ماینر ها امکان دارد که بلاک ها زود تر از ۱۰ دقیقه به بلاکچین اضافه شوند و یا با کمتر شدن قدرت پردازشی شبکه امکان دارد بلاک ها دیر تر از ۱۰ دقیقه به بلاکچین اضافه شوند برای این که این اتفاق نیفتد از مفهوم p-problems استفاده شده است در واقع میزان سختی مسائل ارائه شده توسط سیستم جوری است که ماینر ها بتوانند هر ۱۰ دقیقه جواب را پیدا کنند این میزان سختی مسائل ریاضی ارائه شده هر دو هفته یکبار(هر ۲۰۱۶ بلاک) به صورت خودکار تنظیم میشود. برای نگاه به روند حرکت هش ریت شبکه و سختی شبکه به فصل بعد مراجعه فرمایید .

۶ بررسی تغییر و تحول، مرحله بندی و چرخه عمر موضوع

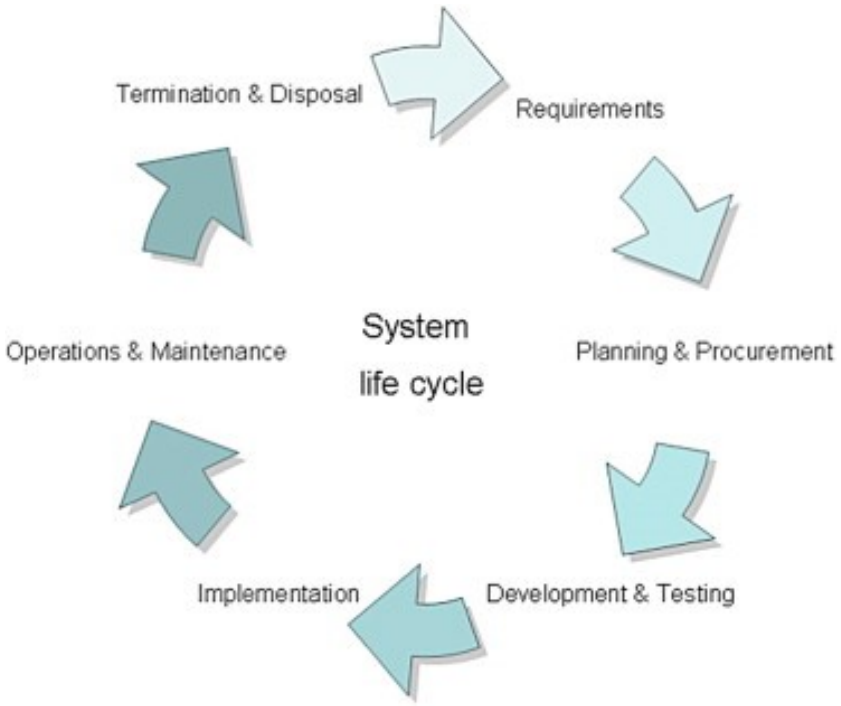
۱.۶ بررسی تغییر سیستم تحول و پویایی سیستم

بیت کوین یک سیستم غیر قابل تغیر و بروزرسانی است یک برنامه ای را تصور کنید که در حال اجرا است شما نمیتوانید برنامه ای که در حال اجرا است با تغیر در کدنویسی آن، آپدیت کنید همانطور که نمیتوانید هواپیمایی که در آسمان در حال پرواز است را اپدیت کنید (در اتریوم با کمک ایجاد فورک اینکار را میکنند) بنابراین سیستم بلاکچین بیتکوین همواره یک سیستم ثابت و ایستاست است اما از انجا که تغیراتی در خود اجزا در طی زمان اتفاق میفتد این سیستم پویایی دارد به عنوان مثال سختی شبکه به صورت خودکار هر دو هفته بروزرسانی میشود نرخ هش ریت شبکه لحظه به لحظه تغیر میکند و عرضه آن هر چهار سال یکبار نصف میشود .

۲.۶ چرخه ی عمر بلاکچین بیتکوین

چرخه عمر بلاکچین بیتکوین رابطه مستقیم با چرخه پذیرش این ارز توسط جامعه دارد چرخه عمر سیستم ها مطابق شکل زیر ابتدا با احساس نیاز به تغیر شروع میشود همانطور که خود بیتکوین هم با احساس نیاز به تغیری در سیستم

پولی دنیا به وجود آمد پس با فرض این که سیستم بلاکچین بیت کوین مورد پذیرش جامعه قرار بگیرد میتوانیم بگوییم تا زمانی که نیاز جدید دیگری در ما انسان ها حس نشود و جایگزینی مناسب تر از بیت کوین نیاید این سیستم زنده است .(پاسخ فرضیات این بخش یعنی مناسب ترین ارز بودن بیت کوین و مورد پذیرش قرار گرفتن این سیستم در قسمت بعد داده میشود)



شکل ۱۱: چرخه ی عمر سیستم

۳.۶ چرخه عمر عرضه بیت کوین

در فرمول ریاضی عرضه بیتکوین از دنباله ی هندسی استفاده شده است فرمول ریاضی عرضه بیتکوین به شکل زیر است :

$$\sum_{i=0}^{32} 210000 * 50/2^i \qquad (۱)$$

عدد iدر این فرمول نشان دهنده ی این موضوع است که چند بار هاوینگ اتفاق افتاده است با این فرمول هر چهارسال یکبار عرضه بیت کوین نصف میشود و اینگونه است که عرضه ی این ارز محدود شده طبق این فرمول بعد از ۳۲ بار هاوینگ یعنی تا سال ۲۱۴۰ تمام بیت کوین ها استخراج میشوند و دیگری بیت کوینی برای استخراج نمیماند در این صورت درآمد ماینر ها فقط به کارمزد تراکنش ها محدود میشود و کم شدن درامد آن امکان دارد امنیت شبکه را به خطر بیندازد اما پیشبینی میشود که شروع شدن تورم منفی بیتکوین از سال ۲۱۴۰ جهش قیمتی زیادی را برای این ارز به دنبال داشته باشد علاوه بر آن با پیشرفت تکنولوژی و بالا رفتن بهره وری دستگاه های استخراج ،استخراج کردن بدون پاداش شبکه هم اقتصادی به نظر میرسد.

۴.۶ چرا بیت کوین مناسب ترین رمز عرض است

همانطور که در بررسی تغیر و تحول این سیستم گفتیم این سیستم غیر قابل تغیر است و پویایی این سیستم محدود به سختی شبکه و هشریت شبکه و عرضه آن است این ویژگی بیت کوین هم بزرگترین نقطه ی ظعف آن است و هم بزرگترین نقطه ی قوت آن از این جهت نقطه ی ضعف است که این سیستم غیر قابل بروزرسانی است و سیستم های پویای جدید میتوانند با قرار دادن برتری هایی در سیستمشان جای این ارز را بگیرند و از این جهت نقطه ی قوت آن است که این ویژگی باعث شده اسمی پشت ایر ارز نباشد و قدرت در این سیستم به معنای واقعی نامتمرکز شده است از آنجا که فلسفه و نیاز اصلی بوجود آمدن این سیستم کمیابی و نامتمرکز بودن است هنوز همچین ارزی به میدان نیامده است به عنوان مثال بزرگترنی رقیب بیت کوین اتریوم است که با شناسایی خالق آن(ویتالیک بوترین) خدشه زیادی به غیر متمرکز کردن آن وارد شده و همچنین حد نهایی برای عرضه این شبکه ندارد

۵.۶ پذیرش سیستم بلاکچین بیت کوین توسط جامعه

ما در این بخش با توجه به داده های روی بلاک ها ((on chain پذیرش این سیستم را توسط مردم مورد مطالعه قرار میدهیم . معیار های نشان دهنده پذیرش این شبکه توسط جامعه عبارتند است :

۱-تعداد آدرس کیف پول های فعال در شبکه

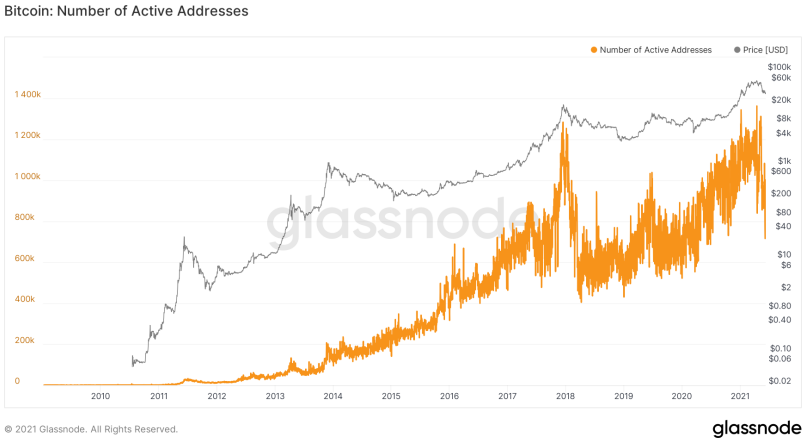
۲-هش ریت (قدرت پردازشی شبکه برای حل مسائل ریاضی)

۳-سختی شبکه (مقدار سختی مسائل ارائه شده که رابطه مستقیم با هشریت شبکه دارد)

۴-تعداد تراکنش های انجام شده توسط در واحد زمانی مشخص

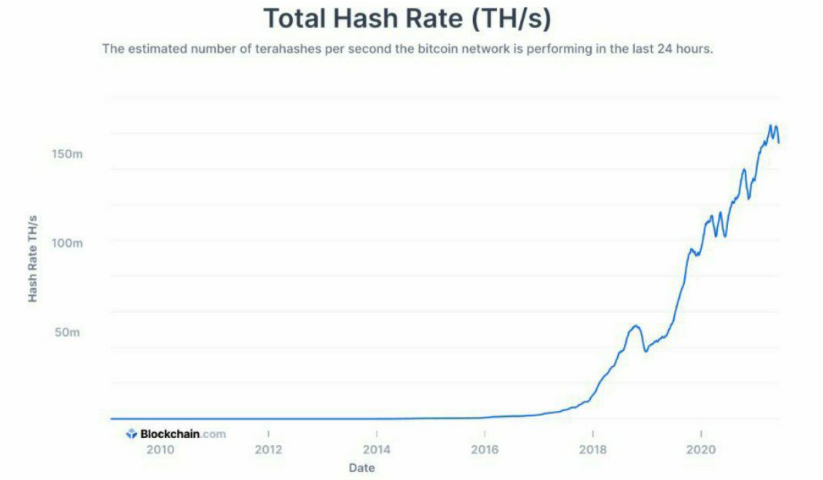
۵-پذیرش سازمانی و دولتی بلاکچین بیتکوین

۱.۵.۶ نمودار تعداد آدرس کیف پول



شکل ۱۲: تعداد آدرس های فعال

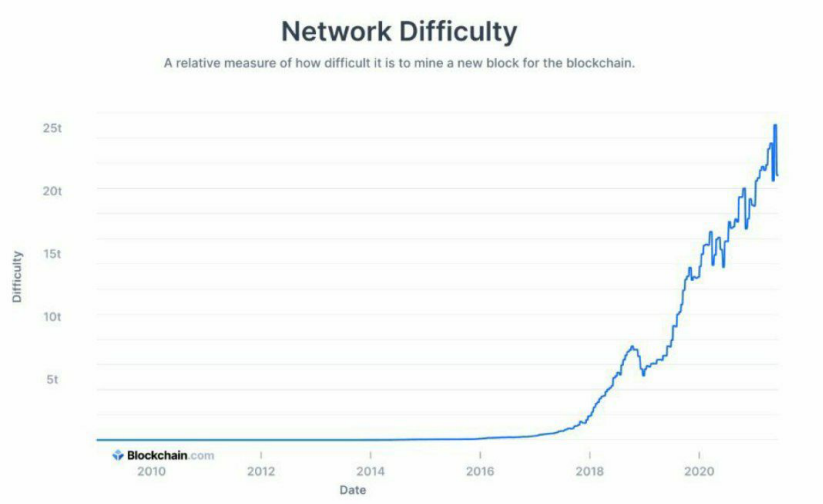
۲.۵.۶ نمودار هش ریت



شکل ۱۳: هش ریت کل

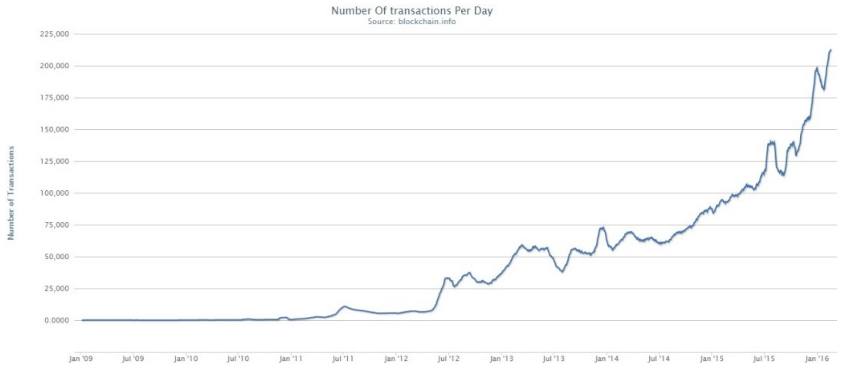
جالب از بدانید در مارچ ۲۰۱۱ هش ریت کل شبکه ۱ ترا هش بوده این یعنی از آن موقع تا می ۲۰۲۱ قدرت پردازشی شبکه ۱۵۰ میلیون برابر شده که این به علت پیشرفت تکنولوژی پردازنده ها و بالارفتن تعداد ماینر هاست با این وجود همواره میانگین زمانی هر بلاک در این دوره های زمانی ۱۰ دقیقه بوده در مورد موضوع در بخش پیچیدگی محاسباتی بیشتر توضیح داده شده است

۳.۵.۶ نمودار سختی شبکه



شکل ۱۴: سختی شبکه

۴.۵.۶ تعداد تراکنش



شکل ۱۵: تعداد تراکنش های انجام شده در روز

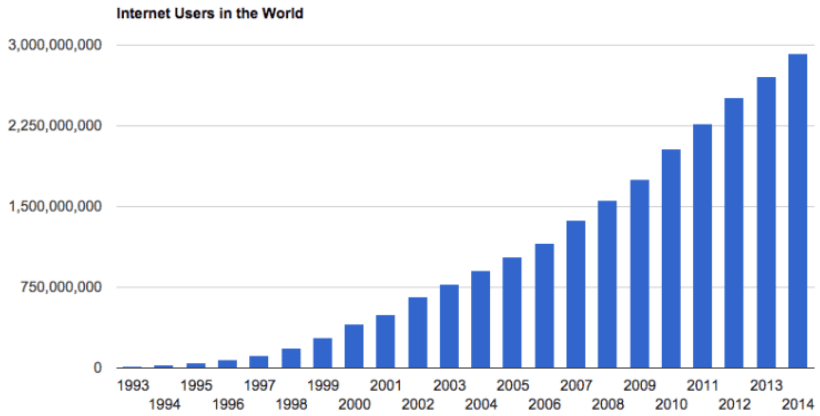
همانطور که مشاهده میکنید میانگین تعداد تراکنش ها در ژانویه ۲۰۱۱ حدود ۴۰۰ عدد بوده در حالی که میانگین حجم تراکنش ها می ۲۰۲۱ حدود ۳۰۰ هزار تراکنش بوده

۵.۵.۶ تحلیلی بر پذیرش سازمانی و دولتی بلاکچین بیتکوین

فیسبوک ، تسلا ، آمازون،اسپیس اکی،علی بابا این ها سازمان هایی هستند که قول استفاده از بیت کوین در شبکه های پرداختی خود را داده اند و دولت ال سالوادور و پاراگوئه هم در پی رسمی کردن این ارز در کشور های خود هستند

۶.۶ تحلیلی بر پذیرش جامعه و مقایسه آن با نمونه های مشابه

با نگاهی به تغیرات تعداد تراکنش ها ، هش ریت شبکه ،تعداد آدرس های فعال، در طی چندین سال گذشته ما شاهد رشد نمایی زیادی در پذیرش این شبکه توسط جامعه هستیم این نمودار ها و این جهش بسیار شبیه رشد استفاده از اینترنت در دهه ۹۰ میلادی و شبیه به رشد استفاده از الکترسیته در گذشته بود گویی بلاکچین سومین انقلاب پس از الکترسیته و اینترنت است



شکل ۱۶: نرخ استفاده کنندگان از اینترنت در جهان

۱.۶.۶ حباب دات کام

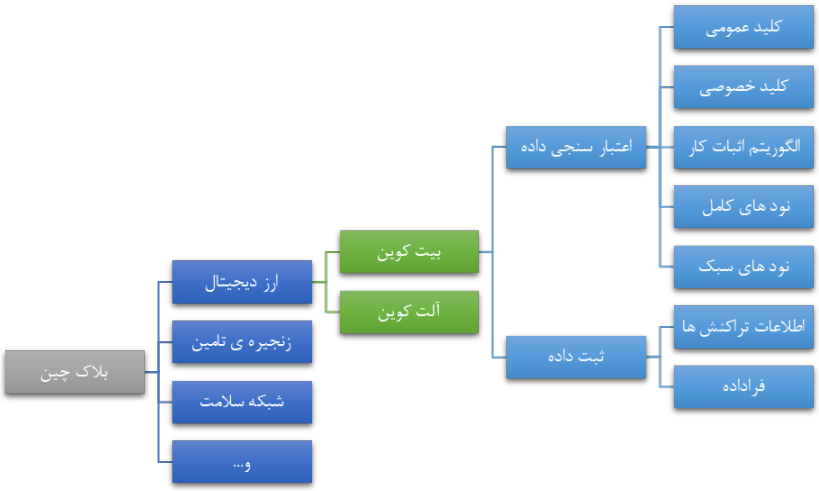
در دهه ۹۰ میلادی همه آینده را از آن اینترنت میدانستند (که البته واقعا هم اینطور بود) شرکت های اینترنتی زیادی از جمله یاهو ،گوگل و آمازون از آن دوران بر میخیزند اما در اواخر دهه ۹۰ میلادی وقتی همه فکر میکردند که آنده از آن اینترنت است به سرمایه گذاری در این بخش پرداختند اما در آن زمان به میزانی که عرضه خدمات اینترنتی بود تقاضا برای این محدوده نبود و هنوز به آن اندازه جامعه اینترنت را نپذیرفته بود اینگونه شد که شرکت های اینترنتی زیادی ورشکست شدند و سهم آن ها ریزش شدیدی را در پی داشت و آن حباب قیمت ها در سهم به حباب دات کام معروف شد وقتی تکنولوژی جدیدی به میدان می آید با حجوم بی رویه و ترس از عقب ماندن جامعه حبابی در آن تکنولوژی شکل میگیرد که میتوانیم منتظر همچین رفتاری در بیت کوین هم باشیم گرچه چندین بار بیت کوین شاهد تخلیه حباب (در سال های ۲۰۱۴و۲۰۱۸) بودیم

۷ ارایه نتایج از طریق یکپارچهسازی و ترکیب

۱.۷ ترکیب اجزاء و روابط حاصل از دستهبندی، سطحبندی و مرحلهبندی با شناخت ایجاد شده در فصلهای قبل

با توجه به دسته بندی ها ، سطح بندی ها ، بررسی دقیق اجزا و روابط بین آنها ، در اینجا میخواهیم اجزایی که قابلیت ترکیب باهم دارند را مشخص کنیم. یعنی اجزایی که تقریبا یک کار خاصی را انجام میدهند و باهمدیگر اشتراکاتی دارند را ترکیب کنیم و به سیستم جامع تری از حالت قبل برسیم و در واقع نگاه کل گرایانه تری به سیستم داشته باشیم. سه زیر سیستم نود ، امضای دیجیتال و پروتکل اجماغ همگی برای ایجاد امنیت و صحت داده ها بر روی بلاکچین و یا اعتبارسنجی داده ها به کار میروند که در نهایت به تولید بلاک جدید می انجامد. با توجه به ارتباط و هدف یکسانی که این سه زیر سیستم باهم دارند آن ها را با هم ترکیب میکنیم و به یک سیستم (خودش یک زیر سیستم برای سطوح بالاست) به نام "اعتبار سنجی داده" تبدیل میکنیم. سپس دو زیرسیستم بلاک و زنجیره که در واقع ساختار ثبت داده ها هستند و اصل و پایه ی سیستم بلاک چین هستند را با هم ترکیب میکنیم و به یک سیستم به نام "ثبت داده" تبدیل میکنیم. زیر بخش های هدر یعنی نسخه ی برنامه ، هش بلاک قبلی ، درخت مرکل ، زمان سنج ، هدف سختی فعلی و عدد نانس را باهم در یک سیستم به نام "فراداده" قرار میدهیم. همانطور که دیدیم نود به دو زیر بخش تقسیم میشود. زیر بخش نود های کامل ، خود به زیر بخش های متعددی تقسیم میشود که با توجه به بررسی اجزا که در فصول قبل انجام شد ، نتیجه میگیریم که نود های ماینینگ ، مستر نود ها ، نود های مرجع ، نود های سرمایه گذار و نود های تعدیل یافته ، تقریبا کاری یکسان انجام میدهند (اعتبار سنجی داده ها) ولی با روش های متفاوت. پس این زیر سیستم ها را هم میتوان با هم ترکیب کرد و به یک سیستم به نام نود های کامل

که در فصل های قبل توضیح داده شده است تبدیل کرد. البته در واقع این نود هایی که نام برده ایم زیر سیستمی از نود های کامل هستند و ما با فرآیند ترکیب انگار زیر سیستم های نود های کامل را از ساختارمان حذف کردیم و زیر سیستم نود های کامل را به یک مولفه تبدیل کردیم ، چون قابل تجزیه بیتشر است ولی با توجه فرآیند ترکیب صورت گرفته ، تجزیه بیشتر صورت نمیگیرد. با توضیحات داده شده ما سه فرآیند ترکیب انجام داده ایم که ساختار سیستم ما بعد از ترکیب به صورت زیر است:



شکل ۱۷: ساختار سیستم پس از ترکیب

۲.۷ ارائه ی نگاه کل گرا نسبت به موضوع تحلیل شده

برای داشتن یک نگاه کل گرایانه به این سیستم ، میخواهیم بیت کوین را در ابر سیستم اقصاد جهانی بررسی کنیم. تأثیر بیت کوین بر اقتصاد جهانی روندی در حال ظهور است که موجب تغییراتی اساسی در اقتصاد کل دنیا شده است. از آنجا که بیت کوین برای تغییر سیستم مالی موجود و حذف واسطه های مالی طراحی شده، از پتانسیل بالایی برای تأثیرگذاری بر اقتصاد جهانی برخوردار است. در بعضی موارد هم می تواند به عنوان یک دارایی امن عمل کند. به نوعی باید گفت، استفاده از ارزهای دیجیتال یک روش جایگزین برای سیستم مالی جهانی است. بخش های بانکی، سرمایه گذاران، دولت ها و شرکت ها به استفاده از این نوع ارزها علاقه نشان داده اند. بیت کوین دارای ویژگی هایی است که می تواند بر دیگر انواع پول ها و ارزهای سنتی از جمله طلا و غیره، چیرگی یابد و به همین علت است که توانایی تأثیر بر اقتصاد جهانی را دارد در ادامه برخی تأثیرات قابل مشاهده بیت کوین بر اقتصاد جهانی را باهم میبینیم:

تغییر در سرمایه گذاری جهانی

بسیاری از سرمایه گذاران در حال حاضر ارزهای دیجیتال، به ویژه بیت کوین را به سبد دارایی ها و سهام خود اضافه می کنند. از سوی دیگر برخی متخصصان نگران سقوط قیمت بیت کوین هستند که ممکن است بحران های مالی جهانی را به همراه داشته باشید. اما در پایان روز، سرمایه گذاران ارزهای دیجیتال را مانعی در برابر متضرر شدن از تورم می بینند.

تراکنش ها را از دلار جدا میسازد

ارزهای دیجیتال هیچ ارتباطی با دلار آمریکا ندارند. در حال حاضر طرفین یک معامله روش هایی دیگر غیر از پرداخت با دلار آمریکا را در اختیار داشته و در واقع می توانند سیاست های ایالات متحده آمریکا را دور بزنند هر چند که ممکن است این امر تهدیدی برای دولت آمریکا به حساب بیاید، زیرا که دلار آمریکا به عنوان یک ارز قدرتمند و جهانی در مبادلات مطرح است، اما در واقع بوسیله بیت کوین انجام معاملات بین المللی بیشتری ممکن خواهد بود.

حذف نیاز به واسطه ها

بیت کوین ذاتا به نحوی طراحی شده که برای معاملات دو نفره به نفر سوم و یا هر نوع واسطه ای نیاز نباشد. بیت کوین برخلاف ارزهای سنتی مانند دلار، برای تبادل نیازی به واسطه هایی همچون بانک ها ندارند. در واقع معاملات به صورت غیر متمرکز تأیید می شوند. همین امر موجب نگرانی مؤسسات بانکی شده، چرا که بیت کوین نیاز به خدمات بانکی را حذف نموده است. بعلاوه با حذف واسطه هایی مانند بانک، سرعت معاملات نیز به شدت افزایش خواهد یافت.

ترغیب بیتشر به معاملات بین المللی

از آنجا که هنوز بسیاری از مردم جهان به لحاظ اقتصادی ضعیف بوده و حتی حساب بانکی هم ندارند، بیت کوین می تواند فرصتی عالی برای تعاملات و معاملات جهانی برای آن ها فراهم سازد. یک کیف پول دیجیتال، تمام آنچه را که برای یک داد و ستد بین المللی نیاز است را برای هر فردی در هر کجای جهان فراهم می کند. در سه ماهه پایانی سال ۲۰۲۰، روزانه به طور متوسط ۲۸۷۴۹۲ معامله به واسطه بیت کوین انجام شده است. معامله با بیت کوین کاملاً سریع، شفاف، محرمانه و امن است. همچنین ، هزینه های تراکنش ممکن است بسیار مقرون به صرفه تر از سیستم های پرداخت معمولی (کارت های اعتباری یا نقدی) باشد.

اعتماد زیاد به پول فیات را کاهش می دهد

بیت کوین به عنوان یک ارز غیرمتمرکز، از هرگونه تأثیر مسائل اقتصادی و سیاسی که اغلب می تواند ارزهای سنتی را تحت تأثیر قرار دهد، عاری است. به همین خاطر است که بیت کوین به عنوان یک ارز دیجیتال طراحی شده است تا بتواند جایگزینی برای پول سنتی و یا همان فیات باشد. امروزه مشتریان به انتقال دیجیتالی به عنوان وسیله ای مفید برای پرداخت هزینه محصولات و خدمات، اعتماد بیشتری از خود نشان می دهند. استفاده از بیت کوین به عنوان روش پرداخت می تواند اعتماد به پول سنتی یا فیات را به شدت کاهش دهد. جالبتر اینکه، افرادی که به صورت تفننی نیز وارد بازار بیت کوین شده اند، اعتقاد دارند پول های مجازی آن ها درست به اندازه پول های سنتی، ایمن هستند.

قوانین بیت کوین

اکنون که بیت کوین در همه جای جهان گسترده شده، مقامات ملی و منطقه ای، در حال تطبیق قوانین مالی خود با بیت کوین هستند. در همین راستا، برخی بانک های مرکزی سعی می کنند این سیستم مالی تازه تأسیس را تحت کنترل خود در آورند. برخی دیگر از کشورها رویکردهایی متفاوت نسبت به ارزهای دیجیتال اتخاذ کرده اند، مثلاً برخی از آن ها (الجزایر، بولیوی، مراکش، نپال، پاکستان و ویتنام)، هر گونه فعالیت در زمینه ارزهای دیجیتال و از جمله بیت کوین را ممنوع کرده اند. در مقابل برخی کشورها خودشان از این ارزها برای پرداخت و داد و ستد استفاده می کنند. مثلاً در ایالات متحده آمریکا، کانادا، استرالیا و اتحادیه اروپا، حتی سازمان های دولتی می توانند در معاملات خود از ارزهای دیجیتال و از جمله بیت کوین استفاده کنند.

موانع ورود به بازار را برداشته و بازار های جدیدی پدید می آورد

بیت کوین یک شبکه معاملات غیرمتمرکز جهانی ایجاد نموده و ضرورت وجود هرگونه نهاد متمرکز برای صدور و تسویه ارز را از بین برده است. در واقع دری را برای نوع جدیدی از بازار و فرصت ها گشوده که هیچ دولت و یا فردی توانایی و اجازه کنترل بازارهای مالی آن را ندارد. بنابراین نه تنها سرمایه گذاران ریسک پذیر، بانک ها و دیگر نهادهای مالی را برای ورود به این بازارها ترغیب می کند، بلکه آن ها می توانند با استفاده از عرضه اولیه سکه (ICO) قوانین و مقررات را دور بزنند. از سویی با استفاده از ICO، استارتاپ ها و مشاغل کوچک در سرتاسر جهان می توانند به منظور توسعه کسب و کارشان، سکه های خود را به فروش برسانند.

دسترسی به سیستم اعتباری را آسان می سازد

بیت کوین دسترسی افسارگسیخته به یک سیستم اعتباری قابل اعتماد را امکان پذیر می سازد چرا که بیت کوین نوعی ارز دیجیتال کنترل نشده و کاملاً مبتنی بر داده است. اگر قیمت برای مدت طولانی ثابت بماند، می تواند از افرادی که در طول زمان از تجار جهانی جدا شده اند، عبور کند. بنابراین، بیت کوین بازارهای جدید و همچنین فرصت های نو را ایجاد نموده که در نهایت می تواند به رشد پایدار و فراگیر در اقتصاد جهانی کمک نماید. جالبتر اینکه بیت

کوین برای معاملات به هیچ هزینه گزافی احتیاج ندارد و همین باعث جذابیت آن برای کاربران و افرادی که قصد استفاده از آن را دارند خواهد شد.

تغییرات در صنعت انتقال بین المللی پول

انتقال پول بین کشورها، رشد اقتصادی را برای آن ها به همراه خواهد داشت. بسیاری از مردم در سراسر جهان در خارج از کشور خود، کار می کنند و به طور منظم برای خانواده ها و عزیزانشان در کشورشان پول می فرستند.

در حال حاضر، کار انتقال پول توسط واسطه هایی مانند بانک ها و دیگر اراده دهندگان خدمات انتقال پول انجام شده و هزینه های بالایی را برای استفاده کنندگان از این خدمات به همراه خواهد داشت. از سویی انتقال پول به این شیوه، زمان بر بوده و گاهی اوقات چند روز طول می کشد تا پول به دست دریافت کننده برسد. اینجاست که بیت کوین نقش خود را به رخ خواهد کشید.

بیت کوین می تواند بدون مکث و به شکلی ایمن به سراسر جهان منتقل شود. این ارز دیجیتال محبوب روند ارسال حواله ها به خارج از کشور را بسیار آسان تر، ارزان تر و ایمن تر می کند. امروزه حداقل ۱۱ ارائه دهنده بیت کوین، از جمله rabbit ، BitPesa و Abra، خدمات حواله خارجی را آغاز کرده اند.

۳.۷ ارئه ی برداشت ها و دریافت های افراد همکار در طرح از نتایج پژوهش

در اینجا به ارائه ی خلاصه برداشت های افراد گروه از نتیجه ی پروژه در چند جمله می پردازیم:

سینا پرهازه

سیستم بلاک چین سیستمی نوآورانه و هوشمندانه برای ثبت داده ها ، بدون امکان تقلب و با امنیت فوقالعاده است. این داده ها میتوانند ، اطلاعات موجود در یک زنجیره ی تامین ، اطلاعات بیماران در یک شبکه ی سلامت ، رای ها در یک سیستم رای گیری ، اطلاعات مالیاتی ، تراکنش های بانکی و ... باشند که به دلیل ویژگی نامتمرکز بودن ، سیستم را از فساد سیستماتیک در امان نگه میدارد.

علی تازیکی

همواره بشر در حال حرکت به سمت تمرکز زدای قدرت بوده و در این برهه از زمان ، با تمرکز زدایی قدرت مدیریت پولی در برابر تورم ناجوانمردانه ای که دولت ها از مردم می گرفتند تصمیم گرفت بایسته و این انقلابی است که از کیپتوگرافی شروع شد و به انقلاب بلاک چین متصل شد که تمرکز زدایی و شفافیت از دو رکن اصلی آن است.

محمد امین میرزا گل تبار

سیستم بلاک چین در حوزه بیت کوین را میتوان مجموعه ای از اجزا و روابط در نظر گرفت که هر کدام از آن ها به نوبه ی خود بخشی از وظایف که باعث برپایی و درست کارکردن سیستم می شود ا انجام می دهند. اگر هرکدام از این اجزا وجود نداشته باشند (حتی کوچکترین جز) هدف اصلی زنجیره بلوکی که ممانعت از تقلب و دزدی به سبک نوین است دچار تهدید جدی می شود.

زینب اکبری

بلاک چین سیستمی است که با استفاده از رمزنگاری و توزیع داده ها امکان دست کاری اطلاعات را تقریبا از بین می برد. تفاوت اصلی سیستم بلاک چین با سیستم های دیگر آن است که اطلاعات ذخیره شده در این سیستم ، میان همه ی اعضای شبکه به اشتراک گذاشته میشود ، که باعث جلوگیری از دستکاری می شود.

همچنین با بررسی نتیجه گیری های اعضای گروه میتوانیم دریابیم که اقای پرهازه و تازیکی بیشتر نگاهی کل گرایانه به سیستم دارند در صورتی که آقای میرزا گل تبار و خانم اکبری بیتشر نگاهی مبتنی بر تجزیه سیستم دارند.

۴.۷ ارائه ی پیشنهاد های مدیریتی با توجه به تحلیل سیستمی موضوع برای مدیران، سازمان ها و شرکت ها

با توجه به موضوع پروژه ی ما که با بررسی ها و تحلیل های انجام شده نتیجه گرفتیم ساختار بلاک چین یک ساختار کاملا مقاوم در مقابل هک ، تغییرات و خرابکاری است و از امنیت بسیار بسیار بالایی برخوردار است. موضوعاتی وجود دارد مثل مصرف برق و حمله ی ۵۱ درصدی (زمانی که یک فرد یا نهاد بتواند بیش از ۵۰ درصد قدرت پردازش شبکه (هش‌ریت) را از آن خود کند. با این کار، امکان دستکاری بلاک چین فراهم می‌شود) که نگرانی هایی را درمورد آینده

ی بیت کوین به وجود آورده است. ما با توجه به بررسی های ما در حوضه ی مصرف برق بیت کوین ، نتیجه گرفتیم که مصرف برق بیت کوین با مصرف برقی که در نظام بانکداری و یا در استخراج طلا استفاده میشود تقریبا برابر است و یا حتی کمتر است. طبق گفته ی گلکسی دیجیتال مصرف برق نظام بانکداری ۷۲.۲۶۳ ترا وات ساعت در سال و مصرف برق استخراج طلا ۶۱.۲۴۰ ترا وات ساعت در سال است در حالی که مصرف برق شبکه بیتکوین ۸۹.۱۱۳ ترا وات ساعت در سال است. همینطور حمله ی ۵۱ درصدی به شبکه بیت کوین در حال حاضر غیر قابل انجام است و فقط نگرانی از جانب کامپیوتر های کوانتمی که در آینده به وجود میآید وجود دارد که این احتمال را ممکن میسازد ، ولی همراه با توسعه ی چنین کامپیوتر هایی سیستم رمز نگاری پیشرفته تری به وجود خواهد آمد و بلاکچین از کامپیوتر های کوانتمی درامان خواهد بود . این ها را گفتیم تا به این مطلب برسیم که گروه ما فکر میکند آینده برای ارز های دیجیتال است ، شاید در حال حاظر دولت ها توان مقابله با این سیستم را داشته باشند ولی درآینده فکر نمیکنیم بتوان در مقابل آن ایستادگی کرد . پس با استدلال های آورده شده ، پیشنهاد هایی که به سازمان ها ، نهاد ها و مخصوصا بانک ها داریم این است که در مقابل ارز های دیجیتال ایستادگی نکنند و آن ها را قبول کنند و سیستم های خود را بر اساس تغیرات جدیدی که این ارزها در دنیا می توانند ایجاد کنند ، به روز کنند تا از رقابت با شرکت های دیگر جا نمانند.

۸ منابع پژوهش

۱- کتاب یک ساتوشی اثر محمد آذرنیوار و نیما ملک پور
۲- www.glassnodes.com
۳- www.blockchain.com
۴- www.arzdigital.com
۵- www.btc.com
۶- www.bitcoin.org
۷- www.economist.com
۸- www.oreilly.com
۹- www.mihanblockchain.com
۱۰- www.nobitex.ir
۱۱-www.walex.ir
۱۲-www.iranrich.com