بیت کوین و نحوه استخراج آن

محمد دی دری خمسه مطلق
زهرا سادات موسوی

چکیده:

بیت کوین یک پول دیجیتالی رمزنگاری شده است که امروزه در دنیای فناوری، استفاده از آن مورد توجه قرار گرفته است. سال ۲۰۰۸ دامنه پایگاه Bitcoin.org در اینترنت ثبت شد و تا به امروز نیز مشخص نیست که چه کسی این دامنه را به ثبت رسانده است. بیت کوین اصولا به صورت الکترونیکی وجود دارد، در واقع بیت کوین به منظور پول الکترونیکی بودن طراحی شده است، درحالی که پول سنتی اصولا به صورت فیزیکی است و حساب هایی که در بانک وجود دارد را می توان در صورت تمایل به سرعت به وجه نقد تبدیل کند.از همین رو هدف این مقاله تعریف بیت کوین و شیوه استخراج آن بود. به همین منظور با استفاده از روش مدلسازی، استراتژی و روند استخراج بیت کوین مورد بررسی قرار گرفت که نتایج این بررسی ها نشان داد سیستم بیت کوین فاقد یک سیستم ثابت، قانون مدار و سازگار با انگیزه است. اگرچه کاربران در این سیستم تابع قوانین هستند اما رفتار آنها تنها بواسطه توافق به ثبات می رسد. همچنین بیت کوین نسبت به قوانین دولت اصلاح پذیر است، این بدین معناست که با تغییر قوانین، سیستم بیت کوین نیز دستخوش تغییر می شود.

کلیدواژه: بیت کوین، پولی دیجیتالی، رمزنگاری، استخراج

مقدمه:

دو عامل که بعد مهمی از ساختار اقتصادی و مالی یک کشور را شکل می دهند، سیستم پرداخت و تسویه است. هزینه سیستم پرداخت هر کشوری معادل ۳درصد GDP است (روی و ساهوو[1] ۲۰۱۶). یک سیستم پرداخت کارآمد می تواند جریان نقدینگی را در اقتصاد تضمین کند. امروزه بدلیل رشد و توسعه تکنولوژی، روند استفاده از روش های سنتی پرداخت به سمت پرداخت های دیجیتالی متمایل شده است یعنی از پرداخت نقدی به پرداخت الکترونیکی. این سیستم با

[1] -Roy& Sahoo

استفاده از ابزارهای مالی دیجیتالی اعم از دبیت کارت، کارت های اعتباری یا چک های الکترونیکی شکل می گیرد. پیشرفت و پیچیدگی تکنولوژی، زمینه را برای استفاده از پول های سطح بالا معروف به پول های رمزی یا همان بیت کوین[۲]فراهم کرده است. پول دیجیتالی همانند پول واقعی است که جریان نقدینگی را بدون هیچ مانعی تحریک می کند.پول دیجیتالی مفهومی است که بعد از پیدایش بیت کوین مورد توجه قرار گرفت. در استفاده از پول دیجتالی از رمزنگاری برای تضمین امنیت آن استفاده می شود. یکی از ویژگی های بارز پول دیجیتالی، امنیت آن است. اولین پول دیجیتالی که مورد توجه عموم قرار گرفت، بیت کوین بود که در سال ۲۰۰۹ توسط فردی بنام ساتوشی ناکاماتو معرفی شد. هدف از بوجود آوردن بیت کوین، ایجاد سیستم پرداخت الکترونیکی صرفا برمبنای رمزنگاری بود (ناکاماتو[۳] ۲۰۰۸). افرادی که از بیت کوین استفاده می کنند، آن را در کیف الکترونیکی ذخیره می کنند و از آن در معاملات خود بهره می گیرند. بیت کوین ها همانند هر واحد پولی دارای ارزش بوده و مردم از آن برای خرید کالاها و خدمات استفاده می کنند.

پول دیجیتالی، پولی است که به شکل اطلاعات الکتریکی برای تبادل کالا و خدمات استفاده می شود و به دودسته قابل ردیابی/گمنامی، بلادرنگ/غیربلادرنگ تقسیم می شوند. درصورتی پول دیجیتالی قابل ردیابی است که بانک و بازرگانان بتوانند نشانه های رمزدار پول را برای صاحبش ردیابی کنند و در صورتی گمنام می ماند که بانک با همکاری بازرگان رمز پول را نتواند شناسایی کند. ویژگی بلادرنگ و غیر بلادرنگ بودن لزوم مشارکت و یا عدم مشارکت بانک در پرداخت را مشخص می کند. از دیگر خواص پول دیجیتالی، غیر قابل استفاده مجدد بودن، غیر قابل جعل کردن، غیر قابل ازدیاد و غیر قابل ردیابی است(عشوریان و جانوسپاه، ۱۳۸۷). بیت کوین به صورت فیزیکی وجود ندارد و تنها حساب هایی شامل رمزهای عمومی و خصوصی وجود دارد. اطلاعات حساب ها بهمراه تراکنش های صورت گرفته بین حساب ها در یک دفترکل ثبت می شود که نیازمند حجم وسیعی از توان محاسباتی کامپیوتری برای تأیید و ثبت این اطلاعات در سرتاسر کامپیوترهای عضو شبکه در جهان می باشد(هادسون[۴] ۲۰۱۴).

بیت کوین یک ارز غیرمتمرکز است که با فناوری نظیر به نظیر مدیریت می شود. تمامی فعالیت ها مانند انتشارات بیت کوین، پردازش و اعتبارسنجی معاملات توسط شبکه انجام می شود و هیچ واسطه یا مرجع مرکزی برای سرکشی یا دخالت در فرآیند وجود ندارد، برعکس پول سنتی که توسط بانک مرکزی یک کشور در راستای تعهد این نهاد برای کنترل سیاست های پولی منتشر می شود. بیت کوین اصولا به صورت الکترونیکی وجود دارد، در واقع بیت کوین به منظور پول الکترونیکی بودن طراحی شده است، درحالی که پول سنتی اصولا به صورت فیزیکی است و حساب هایی که در بانک وجود دارد را می توان در صورت تمایل به سرعت به وجه نقد تبدیل کند(دعائی و حسینی، ۱۳۹۳).

[2] -Bitcoin
[3] - Nakamato
[4] - Hodson

سال ۲۰۰۸ دامنه پایگاه Bitcoin.org در اینترنت ثبت شد و تا به امروز نیز مشخص نیست که چه کسی این دامنه را به ثبت رسانده است. اکتبر سال ۲۰۰۸ فردی به نام ساتوشی ناکاموتو در خبرنامه رمزگذاری شده ای به نام metzdowd.com اعلام کرد: «من درحال کار برروی سیستم پولی الکترونیکی جدیدی هستم که کاملا نظیر به نظیر و بدون دخالت شخص ثالث می شود.»

مقاله علمی مذکور سرمنشأ این پول مجازی یعنی بیت کوین بوده و معروف به مقاله سفید با عنوان " بیت کوین: سیستم پولی الکترونیکی نظیر به نظیر" می باشد. در ژانویه ۲۰۰۹ بلوک صفر بیت کوین در دنیای اینترنت استخراج شد که تنها شامل پیغامی مبنی برشروع بکار سیستم بوده و جایزه آن ۵۰ بیت کوین برای ساتوشی بود. چند روز بعد اولین نسخه از نرم افزار بیت کوین به صورت متن بازارائه شد و فردای آن روز بلوک یک بیت کوین استخراج گردید و تراکنش بیت کوین بین کاربران اولیه صورت گرفت. ارزش بیت کوین هیچ پشتوانه ای نداشته و کاملا بستگی به میزان عرضه وتقاضا داشت(هادسون، ۲۰۱۴). از این رو با توجه به مطالب ارائه شده، هدف از این مقاله بررسی بیت کوین و نحوه استخراج آن می باشد.

پیشینه تحقیق:

لو و وانگ[5](۲۰۱۴) موضوع بیت کوین همانند پول را مورد مطالعه قرار دادند. آنها بیت کوین را با سایر نوآوری ها در تسهیل خدمات پرداخت مورد مقایسه قرار داده و مستنداتی را در این زمینه گردآوری کردند و در نهایت به این نتیجه رسیدند که بسیاری از عوامل در رشد و توسعه بیت کوین و سایر سیستم های پرداخت جایگزین نقش دارند و اینکه بیت کوین در صورتی به رسمیت شناخته می شود که بتواند به یک تکنولوژی پرداخت تبدیل شود.

اکاریا، توماس و پانی[6](۲۰۱۸) ثبات بیت کوین و کاربردهای آن را به عنوان یک واحد پولی در کشور هند مورد بررسی قرار دادند. آنها با استفاده از نرم افزارEviews و آزمودن داده های سری زمان به گرداوری داده ها پرداختند و نشان دادند که هند برخلاف سایر کشورها نسبت به نقش بیت کوین به عنوان ابزاری برای سرمایه گذاری سکوت اختیار کرده است. این کشور معتقد است که بیت کوین ویژگی پول های رایج را ندارد و همین مسئله استفاده از آن را سخت و دشوار کرده است.

هیل، کریشنامورتی، کودیاک و شولتز[7](۲۰۱۸) چگونگی تغییر تجارت را با استفاده از قیمت بیت کوین مورد مطالعه قرار دادند و به این نتیجه رسیدند که برخی عوامل در تعیین قیمت بیت کوین نقش بسزایی دارند و اینکه درک صحیحی از مزیت بیت کوین در معاملات برای تعیین قیمت این پول دیجیتالی وجود ندارد.

5 - Lo& Wang
6 - Acharya, Thomas, Pani
7 - Hale, Krishnamurthy, Kudyalk& Shultz

لو[8](۲۰۱۸) حباب بیت کوین، ریسک های مالی و پاسخ های تنظیمی را مورد مطالعه قرار داد و به این نتیجه رسید که تعیین میزان حباب بیت کوین، موعد ترکیدن حباب و پاسخ های دولت به این مسئله بسیار سخت و دشوار است و اینکه باید از خوش بینی زیاد نسبت به آینده تکنولوژی بیت کوین، بلاک چین و سایر پول های رمزی پرهیز شود زیرا زیاده روی در این مسئله منجر به خسارات مالی می شود.

ماتز، هیلر، هنز، زیگولدروف، مولامن، هالفلد و ورل[9](۲۰۱۸) تاثیر محتوای قرارداد بلاک چین در مورد بیت کوین را به روش کمیتی مورد تحلیل قرار دادند. آنها با مطالعه مزیت ها و خطرات استفاده از بلاک چین به تحلیل کمیت و کیفیت محتوای بلاک چین پرداختند و به این نتیجه رسیدند که ذخیره داده های غیرمالی کاربران در بلاک چین با مزیت ها و معایبی همراه است زیرا بدلیل نبود یک قانون جامع و کامل، محتوای غیرقانونی بلاک چین می تواند مشکلاتی را برای کاربران بوجود آورد و بلاک چین را به یک تکنولوژی غیرقانونی تبدیل کند.

کرول، داوی و فلتن[10](۲۰۱۳) استخراج بیت کوین را در حضور مخالفان مورد مطالعه قرار دادند.آنها با استفاده از مدلسازی فرایند استخراج به این نتیجه رسیدند که بیت کوین یک سیستم ثابت، قانون مدار و سازگار با انگیزه نیست. آنها نشان دادند که بیت کوین نسبت به قوانین دولت اصلاح پذیر است. بنابراین ساختار بیت کوین تابع قوانین و قانون گذاران می باشد.

روش تحقیق:

با توجه به هدف مقاله مبنی بر شیوه استخراج بیت کوین، در این مقاله ابتدا به تعریف بیت کوین و بلاک چین- زیرساخت آن پرداخته و سپس عملکرد آن را توصیف نموده و فرایند و استراتژی استخراج را شرح می دهیم و درنهایت با استفاده از یک تکنیک مدلسازی، شیوه استخراج بیت کوین را به کمک یک پروتکل بازی تشریح کرده و به کشف مکانیسم عمل آن می پردازیم.

بیت کوین:

بیت کوین یک پول رمزی یا دیجیتالی است که پشتیبانی از آن به کمک اموال ملموس یا ناملموس انجام نمی شود. بیت کوین یک شبکه نامتمرکز و متکی به سیستم سطح به سطح است که با استفاده از آن، معاملات تایید می شوند. اولین بیت کوین در سال ۲۰۰۹ توسط فردی بنام ساتوشی ناکاماتو راه اندازی شد که وی با استفاده از رمزنگاری، این پول را استخراج کرد (ناکاماتو، ۲۰۰۸).

[8] - Lu
[9] - Matzutt, Hiller, Henze, Ziegeldorf, Müllmann, Hohlfeld& Wehrle
[10] - Kroll, Davey& Felten

بیت کوین یک شی رمزنگاری شده با ارزش ثابت است که با زنجیره ای از امضاهای دیجتالی نشان داده می شود که این امضاهای دیجیتالی در معاملات بکار می رود. هر بیت کوین یک هویت دارد که صاحب آن با انجام معامله و امضای آن، پول دیجیتالی را از یک آدرس به آدرس دیگر جابجا می کند(کرول و همکاران، ۲۰۱۳).

لو و وانگ (۲۰۱۴) بیت کوین را یک شبکه سطح به سطح تعریف کردند که به واگذاری حق تملک بدون نیاز به واسطه کمک می کند. آنها بیت کوین را نوعی پول مجازی دانستند که نوعی نواوری را در بخش اقتصاد و امور مالی بوجود آورده است.

به عقیده لورنگ لو(۲۰۱۸) سیستم بیت کوین یک سیستم سطح به سطح است که معاملات بین کاربران و بدون دخالت واسطه اتفاق می افتد. هرکاربر عضو کوچکی از سیستم بیت کوین است. تبادل بیت کوین در بلاک چین روی می دهد که یک سیستم نامتمرکز و در دسترس عموم می باشد. بیت کوین و بلاک چین نه تنها خط مقدم انقلاب تکنولوژی هستند بلکه ایدئولوژی بازار آزاد آدام اسمیت را منعکس می کنند.

بلاک چین زیرساخت و دفتر اصلی بیت کوین است که پلتفورم امنی را برای داد و ستد و تجارت شرکت ها فراهم کرده است(چو و کوپل[11]۲۰۱۷; برنستن و شار[12]۲۰۱۸) . بلاک چین به محاسبه رویدادهای دیجیتالی اعم از انتقال پول با واحدهای رمزی کمک می کند. بلاک چین ها داده ها را از پیام های کوتاه گرفته تا تصویر ثبت می کنند(ماتز و همکاران، ۲۰۱۸).

عملکرد بیت کوین:

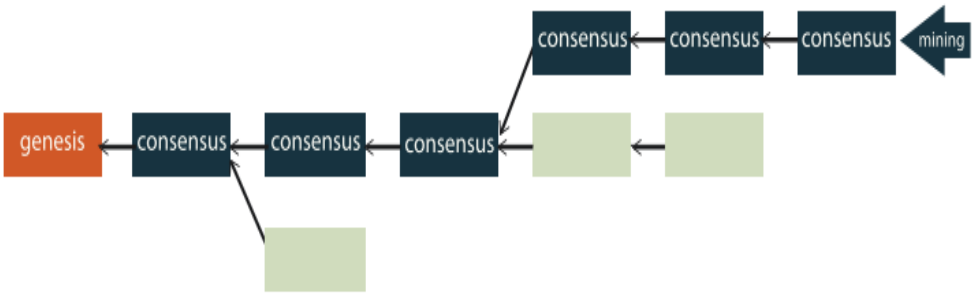
بیت کوین یک واحد پولی رمزی است که توزیع آن بدون دخالت مقامات انجام می شود(دی[13]۱۹۹۸). بیت کوین یک کاغذ سفید کوچک است که همراه با اجرای مرجع منتشر می شود(P2P digital bitcoin). بیت کوین یک شی رمزنگاری شده با ارزش ثابت است که به صورت زنجیره ای از امضاهای دیجیتالی روی معاملاتی نمایش داده می شود که در این معاملات از سکه استفاده می شود. با چک کردن صحت و درستی امضاهای رمزی تاریخ دار می توان از صحت و اعتبار سکه اطمینان یافت. هر بیت کوین دارای یک شناسه و آدرسی متشکل از یک کلید عمومی است. دارنده بیت کوین می تواند با امضای معامله، بیت کوین ها را از یک آدرس به آدرس دیگر انتقال دهد. در این معامله، ورودی و خروجی های زیادی اتفاق می افتد. گاهی یک ارزش اضافی در معامله ظاهر می شود که این ارزش باید برای فرستنده ارسال شود زیرا سکه ها با ارزش ثابت باید به شیوه "یا همه یا هیچ" جابجا شوند. اگر کل ارزش ورودی بیش از ارزش خروجی باشد، به این تفاضل، هزینه معامله گفته می شود که این هزینه باید به فردی پرداخت شود که این معامله را به بلاک چین ضمیمه کرده است.

---

[1] - Chiu and Koeppl
[1] - Berensten and Schar
[1] - Dai

اگرچه این پروتکل به گیرنده بیت کوین اجازه می دهد تا رمز معامله را تایید کند اما از خرج مضاعف بیت کوین ها جلوگیری نمی کند. یعنی در حالیکه گیرنده می تواند تایید کند که فرستنده بیت کوین ها را انتقال داده اما مطمئن نیست که آیا سکه ها برای او ارسال شده است.

به منظور جلوگیری از خرج مضاعف، بازیکنان بیت کوین در یک پروتکل سطح به سطح وارد شده و یک سرویس توزیعی مجهز به ثبت زمان را با فراهم کردن یک پایگاه کاملا سریالی از هر معامله اجرا می کنند. معاملات به ترتیب وارد بلوک هایی می شوند که این بلوک ها حاوی یک عدد سریالی، ساعت شمار، هش رمزی(به کل حدسیات در هر ثانیه گفته می شود) از بلوک قبلی، فراداده، مصنوعات و مجموعه ای از معاملات بیت کوین می باشد. بلوک ها یک زنجیره هش را تشکیل می دهند: هر بلوک جدید حاوی هش رمزی از بلوک های قبلی است که به فرد اجازه تایید یا رد آن را می دهد. بلاک چین حاوی لینک های پسرو است، این بدین معناست که یک مسیر از پشت هر بلوک تا جلوی آن امتداد دارد. اما مسیر مسیر پیشرو از یک بلوک ممکن است منحصربفرد نباشد. بنابراین مکان بیت کوین به شکل درختی است که شاخه های آن همزمان با رشد، منشعب می شوند. شکل ۱بلاک چین را نشان می دهد.



شکل ۱: نمونه ای از بلاک چین

شکل ۱: نمونه ای از یک بلاک چین. اولین بلوک در سمت چپ قرار دارد. فرایند استخراج در بلندترین شاخه از درخت روی می دهد. سایر شاخه ها و شاخه هایی با بلوک های نامعتبر کنارگذاشته می شوند.

هر بازیکن در این بازی می تواند بلوک های جدیدی را استخراج کند که این بلوک ها، معاملات جدید را به محل ثبت بیت کوین اضافه می کنند. یک بلوک جدید در صورتی به محل ثبت بیت کوین اضافه می شود که نوع مصنوعی آن بگونه ای انتخاب شود که هش بلوک جدید کمتر از ارزش موردنظر باشد. این نوعی معمای محاسباتی است که انجام آن بسیار سخت و دشوار است اما نتیجه آن براحتی اثبات می شود. حل این معما نشان می دهد که فرد تلاش زیادی برای حل آن کرده است(بیکر و همکاران[۱۴]؛ ۲۰۱۳؛ دورک و ناور[۱۵]؛ ۱۹۹۲؛ لوری و کلیتون[۱۶]؛ ۲۰۰۴).

[1] - Becker, Breuker, Heide, Holler, Rauer, Ohme [4]
[1] - Dwork and Navor [5]
[1] - Laurie and Clayton [6]

روند اثبات در بیت کوین با استفاده از hashcash است(باک[17]،۲۰۰۲). سختی این معما بدلیل استفاده از یک الگوریتم تطبیقی برمبنای تاریخ بلاک چین است که باید ثبات آن در بلندمدت حفظ شود تا بلوک جدید هر ۱۰ دقیقه استخراج شود.

ویژگی مکانیسم استخراج این است که اگر دو شاخه از درخت وجود داشته باشد و گروهی از افراد، یک شاخه را بوجود آورند پس شاخه ای که متعلق به افرادی با قدرت محاسباتی بیشتر است، با سرعت بیشتری رشد می کند. این بدین معناست که افراد به شاخه ای رای می دهند که گسترش بیشتری داشته است و طبق قانون بیت کوین، بلندترین شاخه، شاخه ای است که اعتبار و صحت بیشتری دارد.

زمانی که یک کاربر قصد انتقال و جابجایی بیت کوین ها را به کاربر دیگر دارد، او مورد معامله را امضا کرده و آن را در شبکه سطح به سطح بیت کوین میان دوستانش توزیع می کند. سپس همین دوستان مجددا آن را توزیع می کنند که اینکار شبکه را از همه معاملات اشباع می کند. همه افرادی که بیت کوین را استخراج می کنند، می کوشند تا یک بلوک جدید را به همراه معاملات بوجود آورند.

بیت کوین های جدید بواسطه فرایند استخراج بوجود می آیند. هر فرد، یک معامله را به بلوک اضافه می کند که این کار عایدی را بوجود می آورد که این عایدی بین همه افراد توزیع می شود. این روش انگیزه کاربران را برای شرکت در این معامله و استخراج بیت کوین افزایش می دهد. تعداد بیت کوین هایی که به این روش ایجاد می شود، براساس یک جدول زمانی از پیش تعیین شده تنظیم می شود که عایدی آن در هر ساعت معادل ۲۱هزار بلوک است. عایدی حاصل از استخراج، ۵۰ بیت کوین به ازای هر بلوک است. فرایند استخراج همیشه عایدی را تضمین نمی کند. اولین کسی که یک راهکار مناسب را پیدا می کند، بلاک چین را گسترش داده و عایدی را نصیب خود می کند. سپس همه افراد در تبعیت از این فرد می کوشند تا یک معمای جدید را حل کنند و بلوک دیگری را به بلاک چین اضافه نمایند.

بیت کوین ها عموما بی نام هستند و نام و نشانی ندارد زیرا آدرس بیت کوین ها ازکلیدهای عمومی گرفته می شود و همه افراد می توانند با ورود به اینترنت به آن دست یابند اما در عمل این افراد قابل شناسایی هستند. معاملاتی که با اسامی مختلف شکل می گیرند، در صورتی که با برخی شرایط مرتبط باشند، قابل شناسایی هستند(ران و شامیر[18]،۲۰۱۳). لازم به ذکر است که بیت کوین هنگامی که توسط خود کاربر استفاده می شود، بی نام و نشان است اما زحمت بکارگیری صحیح آن بسیار سنگین است. بیشتر کاربران، بیت کوین هاشان را به صورت سپرده نگهداری می کنند(Bitcoin Exchange). که این سپرده حاوی حجم زیادی از اطلاعات در مورد دارنده بیت کوین است. اخیرا با گسترش پروتکل بیت کوین، ضمانت های قابل اثبات و قوی نیز فراهم شده است که هنوز این ضمانت ها بدرستی بکار گرفته نشده اند(میرز، گارمان، گرین و رابین[19]،۲۰۱۳).

[1] - Back
[1] - Ron and Shamir
[1] - Miers, Garman, Green and Rubin
[7]
[8]
[9]

استخراج بیت کوین:

بیت کوین مورد توجه بسیاری از کاربرانی قرار گرفته که بدنبال استخراج پول های جدید و پیشرفت در آینده هستند. فرایند ایجاد بیت کوین های جدید، استخراج گفته می شود که کاربران با استفاده از نرم افزارهای خاص به حل این موضوع می پردازند. در گذشته، کاربران به کمک کامپیوترهای شخصی و پردازنده ها و با حل مسائل ریاضی، بیت کوین را استخراج می کردند اما بعدها با استفاده از کارت گرافیک در بازی ها و انیمیشن های ۳بعدی توانستند الگوریتم های بیت کوین را به اجرا در آورند. اخیرا نیز از مدارهای جامع خاص نرم افزار(ASTC) برای استخراج بیت کوین استفاده می شود که این سیستم قدرت زیادی در انجام محاسبات دارد و برق کمتری مصرف می کند(لو، ۲۰۱۸).

بیت کوین دارای شناسه و آدرس است. مالک بیت کوین با انجام معامله و امضای آن، پول دیجیتالی را از یک نشانی به نشانی دیگر انتقال می دهد. ممکن است اشخاص درونی و بیرونی در معامله حضور داشته باشند. اگر ارزش بیت کوین های درونی بیشتر از ارزش بیت کوین های بیرونی باشد، به تفاضل این دو ارزش، هزینه معامله گفته می شود که این هزینه به فردی پرداخت می شود که معامله را در بلاک چین امضا کرده است. اگرچه این پروتکل به گیرنده بیت کوین اجازه می دهد تا معامله را با استفاده از رمزنگاری تایید کند اما از خرج دو برابر بیت کوین ها جلوگیری نمی کند. یعنی درحالیکه گیرنده تایید می کند که فرستنده بیت کوین ها را انتقال داده اما او به هیچ وجه نمی تواند از انتقال و پرداخت سکه ها مطمئن شود.

بیت کوین ها وابسته به ۳ نوع توافق هستند. کاربران باید نسبت به قوانین تعیین ۱- صحت و درستی معاملات، ۲- نوع معاملات و ۳- ارزش واحد پولی با یکدیگر به توافق برسند. بنابراین موفقیت بیت کوین منوط به ۳ نوع توافق است:

۱-توافق نسبت به قوانین: کاربران باید نسبت به تایید و صحت و درستی معاملات به توافق برسند. تنها معاملات معتبر در پایگاه بیت کوین به ثبت می رسند.

۲-توافق نسبت به حالت: کاربران باید نسبت به نوع معاملات به توافق برسند یعنی آنها باید از تاریخ معاملات و حتی مالکان سکه مطلع باشند.

۳-توافق نسبت به ارزشمند بودن بیت کوین: کاربران باید نسبت به ارزش بیت کوین و پذیرش آن در سیستم پرداخت به توافق برسند.

هریک از این موارد وابسته به یکدیگر هستند بدین معنا که به توافق رسیدن برای تعیین تاریخ معامله بدون توجه به قوانین بسیار سخت است و همچنین توافق کردن برای ارزش بیت کوین درصورتی که مالک بیت کوین نتواند به ارزش موردنظر برسد، امکان پذیر نیست.

پذیرش قوانین یک فرایند اجتماعی است. کاربران باید به درک مشترکی از قوانین برسند تا این قوانین به صورت کد وارد نرم افزاری شود که هر کاربر از آن استفاده می کند. در بیت کوین، گروه های کوچک و افراد می توانند قدرت خود را اعمال کنند.

پذیرش نوع معامله یک مسئله تکنولوژیک در سیستم های توزیعی است. هر فرد می تواند بخشی از معامله محسوب شود و بقیه افراد لازم است در گروه های بزرگ و در سطح شبکه همکاری کنند تا بتوانند به درک مناسبی از حالت کلی برسند. پذیرش تکنولوژی الزامی است حتی اگر برخی افراد از قوانین سرپیچی کنند. در سیستم های توزیعی، رفتار انحرافی در صورتی قابل تحمل است که اکثریت افراد صادق و هماهنگ باشند. به هرحال در بیت کوین چنین فرض می شود که افراد طبق انگیزه و تمایلاتشان رفتار می کنند.

پذیرش ارزش بیت کوین بخشی از همان توافق است که برای هر واحد پولی ضروری می باشد. چنین ارزشی اغلب به عنوان مدلی از نقطه کانونی در این بازی قلمداد می شود.

مدلسازی فرایند استخراج:

با یک مدل ساده می توان نشان داد که چگونه کاربران تصمیم به استخراج بیت کوین می گیرند. فرض می کنیم که فردی بنام Minnie می خواهد توانایی خود را برای استخراج بیت کوین محک بزند. او قادر است با سرمایه گذاری روی منابعی مثل تجهیزات و برق، بیت کوین را با هزینه c دلار در هر ثانیه استخراج کند. این سرمایه گذاری به Minnie اجازه می دهد تا درهر ثانیه با استفاده از حدسیات (هش)، معما را حل کند که حل این معما با G حدس انجام می شود و اینکه حل یک معما (استخراج یک واحدپولی) معادل یک پاداش از بیت کوین با ارزش V است. و بالاخره فرض می کنیم که همه افراد همین تصمیم را می گیرند. پس Minnie در هر ثانیه PV/G دلار را کسب می کند و درصورتی سرمایه گذاری می کند که

$$G<\frac{PV}{C}$$

به هرحال Minnie تنها فردی نیست که می تواند بیت کوین را استخراج کند. تعداد حدسیات برای حل معمای G به دفعات استخراج بستگی دارد به طوری که دفعات استخراج واحدهای جدید ثابت می ماند به عنوان مثال R واحد جدید در ثانیه. فرض می کنیم که N فرد قصد استخراج بیت کوین را دارند. پس در هر زمان،

$$R=\sum_{i=1}^{N}\frac{P_i}{G}$$

دراینجا P تعداد حدسیات در هرثانیه، صورت معادله بالا و $\bar{C}=\sum_{i=1}^{N}C_i$. کل هزینه ای است که صرف استخراج می شود. پس G=P/R است بنابراین Minnie تنها در صورتی وارد بازار بیت کوین می شود که معادله زیر برقرار باشد:

$$\frac{\bar{P}}{R}<\frac{\bar{P}V}{\bar{C}}\Longrightarrow\bar{C}<RV$$

از همین رو در اینجا یک موازنه کلی برقرار است که در آن، استخراج دلارها به ازای هر ثانیه مساوی با کل هزینه استخراج است.

$$C=RV$$

این موازنه تا زمانی برقرار است که افراد بتوانند تصمیم فوری در مورد استخراج بگیرند. در عمل، این افراد با هزینه های مربوط به مصرف سرمایه برای تجهیزات مواجه می شوند و این بدین معناست که c یک تابع ثابت و حاشیه است. بنابراین افراد سرمایه زیادی را صرف استخراج می کنند تا بتوانند هزینه های ثابت را جبران کنند که این سرمایه بیشتر از هزینه های ناچیز در هر واحد زمان است.

در دایره بیت کوین، به کل حدسیات در هر ثانیه، هش شبکه گفته می شود. نرخ هش شبکه به ازای هر ثانیه تقریبا ۱۱۹ ترلیون هش است که این، شبکه بیت کوین را به یکی از بزرگترین پروژه های محاسباتی تبدیل کرده است. در مجموع، شبکه اعتبارسنجی معامله بیت کوین قویتر از قدرت محاسبه ۵۰۰ ابرکامپیوتر است که این، هرکسی را در ارتباط با هزینه اعتبارسنجی معامله در بیت کوین به مکث و تعجب وا می دارد. نرخ هش مستقیما قابل اندازه گیری نیست زیرا پایگاه بیت کوین تنها حاوی راهکارهایی برای حل معماست و میزان محاسبات را برای پیدا کردن راهکارها بحساب نمی آورد.

توازن در عملیات استخراج بیت کوین منجر به این نتیجه می شود که از آنجایی که منابع استخراجی باید با واحدهای پولی غیر از بیت کوین خریداری شوند، ارزش استخراج با قیمت معامله بیت کوین نوسان پیدا می کند. بنابراین اگر قیمت بیت کوین افت کند، انگیزه برای استخراج نیز کمتر می شود و این منجر به تشکیل حلقه مرگ می شود که در این حلقه، از بین رفتن اعتماد به بیت کوین موجب افت قیمت آن می شود که افت قیمت نیز انگیزه را برای استخراج کمتر کرده و کمتر شدن نرخ استخراج منجر به افت شدید واحد پولی و در نهایت از بین رفتن اعتماد به واحد پولی می شود.این حلقه، فقدان توافق در بازی ارزش را منعکس می کند. بنابراین عمل استخراج، ارزش زیادی را برای فرد بدنبال ندارد. اگر بیت کوین بگونه ای تغییر کند که یک واحد استخراج با هزینه c منجر به تولید ارزش $f<c$ شود.، پس تلاش افراد با تابع $\frac{c}{f}$ افزایش می یابد که در این صورت همان مقدار منابع به هدر می رود. لازم به ذکر است که تغییر فرایند استخراج می تواند مفید باشد بگونه ای که این فرایند، ارزشی را بوجود آورد که توسط فرد قابل استخراج نباشد.

استراتژی استخراج:

در اینجا فرض می کنیم که فردی تصمیم به استخراج بیت کوین گرفته. بنابراین برای خرید $P^*=f(C^*)$ در هر ثانیه، مبلغ C^* را سرمایه گذاری می کند. اکنون او باید شیوه استخراج را انتخاب کند. طبق قانون بیت کوین، چنین فردی باید تابع قانون باشد اما او بهره خود را صرفنظر از قوانین بیت کوین به حداکثر افزایش می دهد.

هیچ یک از قوانین بیت کوین به خودی خود اجرا نمی شود و این احتمال وجود دارد که کاربران، قانون را نادیده بگیرند. به عنوان مثال طبق قانون، یک معامله دارای امضاهای دیجیتالی معتبری است که به صاحب پول تعلق دارد. هرکسی می تواند از رمزنگاری برای تشخیص هرگونه تخلف از قوانین استفاده کند. اما قانون تنها در صورتی لازم الاجرا خواهد بود که افراد از معاملاتی که فاقد امضاهای دیجیتالی معتبر است، چشم پوشی کنند.

چگونه این فرد با استخراج بیت کوین می تواند به بیشترین عایدی دست یابد؟ او باید در پایگاه بیت کوین، واحدهای جدیدی را بوجود آورد. اگرچه مستندات اغلب از پایگاه بیت کوین به عنوان زنجیره ای از واحدها سخن می گویند اما به طور کلی این پایگاه می تواند در چندین نقطه منشعب شود و منجر به ایجاد ساختاری شود که بیشتر همانند یک درخت پرشاخ و برگ است. اصولا هدف از استخراج، بوجود آوردن یک واحد جدید و گسترش هریک از شاخه ها یا ایجاد یک شاخه جدید در درخت است.

طبق اسناد بیت کوین، افراد بدنبال گسترش بلندترین شاخه هستند. اگر همه افراد از این قانون تبعیت کنند، بلندترین شاخه رشد خواهد کرد و در صورت منشعب شدن، رشد یک شاخه از شاخه دیگر سبقت می گیرد. البته تصور می شود که منشعب شدن برای بیت کوین خطرناک است زیرا این انشعابات مدل های متعدد و رقابتی از معامله را پدید آورده و شبهاتی را نسبت به صاحب پول ایجاد می کند.

در اینجا فرایند استخراج به صورت یک بازی بین کاربران مدلسازی می شود. هر کاربر یک استراتژی s را انتخاب می کند که این استراتژی، تابعی است که ساختار بلاک چین L را برای انتخاب نوع شاخه ای که باید عمل استخراج از آن صورت گیرد، به تصویر می کشد، یعنی $S(L)=b^*$ بدین معناست که s، b^* را با توجه به پایگاه L انتخاب می کند. هر کاربر یک استراتژی را قبل از بازی انتخاب می کند. سود هر کاربر، عایدی حاصل از استخراج واحدی است که به ازای هر دور استخراج بدست می آید. به هرحال این عایدی در صورتی ارزشمند است که واحد تازه استخراج شده با توافق به نقطه نهایی برسد.

درصورتی که دو بلاک چین Lr و Lr+1 تنها با افزودن یک واحد جدید b با واحد والد متفاوت شوند، استراتژی S را یکنواخت می نامیم که در این صورت، $S(Lr+1)=b$ می باشد. اگر با استفاده از این استراتژی، درخت از یک نقطه خاص گسترده شود، پس افزودن یک واحد جدید به همین نقطه باعث می شود که استراتژی به یک واحد جدید حرکت کند. استراتژی بلندترین زنجیره که در اسناد بیت کوین موجود است، یکنواخت می باشد بشرطی که بلندترین زنجیره بواسطه یک واحد گسترده شود و بلندترین زنجیره باقی ماند.

اگر S یک استراتژی یکنواخت باشد، پس بازی استخراج از یک حالت موازنه برخوردار است که همه افراد در آن بازی می کنند. انتخاب استراتژی استخراج S^* در یک بازی بدین معناست که همه افراد موظفند که با یک استراتژی یکنواخت بازی کنند. اگر فرد با استراتژی S بازی کند، پس همه افراد نیز با همین استراتژی یکنواخت بازی می کنند و این یکنواخت بودن بدین معناست که یک شاخه بدون محدودیت رشد می کند. درنتیجه هر واحدی که با موفقیت استخراج می شود، در بلندمدت روی شاخه باقی خواهد ماند. اگر فرد استراتژی را به استراتژی دیگری تغییر دهد، نمی تواند واحدهای جدید را بوجود آورد زیرا نرخ واحدآفرینی مستقل و جدا از شاخه های اوست. تنها تاثیر این تغییر استراتژی این است که امکان بوجود آمدن برخی یا همه واحدها روی شاخه وجود دارد. بنابراین تغییر استراتژی S می تواند بهره را کمتر کند و این ثابت می کند که $(S,S,\ldots,S)$ یک موازنه هش است.

این مدل به بازی بورس یا تضمین اعتماد شبیه است. در شکار بورس، همکاری و هرگونه تخلف از قوانین، متقابل بوده و نتایج آن متوازن است. در بیت کوین شاهد تخلف از قوانین به صورت متقابل هستیم.

بنابراین استراتژی یکنواخت نوعی موازنه است که بواسطه همه افراد استفاده می شود. به این معنا که هیچ استراتژی یکنواختی برتر از دیگری نیست. افراد جدید همان استراتژی را دنبال می کنند که بواسطه اکثریت افراد استفاده می شود. انتخاب استراتژی لازمه هماهنگی است و راهکاری که به نظر جذاب تر است، به عنوان نقطه کانونی درنظر گرفته می شود. دلیل انتخاب استراتژی بلندترین زنجیره این است که این استراتژی در اجرای بیت کوین کاربرد دارد. زمانی که ظرفیت جدیدی برای استخراج در سیستم وارد می شود، این انتخاب ثابت می ماند.

هزینه معاملات:

در پروتکل بیت کوین، یک هزینه معامله برای فرد در نظر گرفته می شود. اگر ارزش این معامله در بیت کوین کمتر از حد معین باشد، به این ارزش، هزینه معامله گفته می شود که مبلغ معامله توسط مدیران برای استخراج یک بلوک حاوی همان معامله جمع آوری می شود. هزینه معامله به فردی تعلق می گیرد که بیت کوین را استخراج کرده است.

انگیزه فرد، استخراج بلوک ها از هر معامله ای است که هزینه غیرصفر دارد. در صورت مساوی بودن تمامی شرایط، فرد بجای ردکردن هزینه، ترجیح می دهد کمترین هزینه را بپذیرد. اگرچه فرد مایل است که هزینه بیشتری از معامله را بدست آورد اما همه افراد می دانند که اگر آنها معامله را نپذیرند و آن را رد کنند، فرد دیگر می تواند آن را به تصرف درآورد و هزینه را نصیب خود کند. اگر افراد در توافق با یکدیگر، کاربرانی که هزینه معاملات را کم کرده اند را بایکوت کنند، چنین قراردادی تصدیق نمی شود و افراد قادرند بواسطه استخراج بیت کوین از این قرارداد صرفنظر کنند. کاربران از همکاری با یکدیگر سود می برند. آنها هزینه معاملات را کم می کنند تا افراد دیگری وارد معامله شوند اما کاربر از هزینه های بیشتر سود می برد که اینکار ارزش را بدون بهره برجای می گذارد.

درحالت توازن انتظار داریم که هزینه معاملات برای کاربران اندک باشد و این افراد این هزینه ها را نصیب خود می کنند. در واقع آنچه مشاهده می کنیم این است که هزینه عایدی حاصل از استخراج، روزانه معادل ۳۶۰۰ بیت کوین است در حالیکه متوسط هزینه معاملات روزانه حدود ۵۰ بیت کوین است. مکانیسم هزینه معاملات شبیه بازی کلاسیک اولتیماتوم است(اوش و رات،[2]۱۹۸۹).که در این بازی،یک قانون برای هزینه معاملات تعریف می شود. کاربری که هزینه معاملات را بسیار کم عرضه می کند، اولتیماتومی برای یک فرد خاص محسوب نمی شود بلکه معرفی یک فرد موفق در زمینه بیت کوین، فرصتی برای جمع آوری هزینه معاملات است. تا زمانی که هر فرد مایل به پذیرش این معاملات باشد، هزینه ها به مناقصه گذاشته می شود.

2 - Ochs and Roth

بنابراین انتظار نداریم که هزینه معاملات نقش بلندمدتی را در سیستم بیت کوین بازی کند. اما معتقدیم که تغییر قوانین هنگامی ضروری است که هزینه معاملات، نقش خود را در سیستم بیت کوین بازی کند.

حاکمیت بیت کوین:

سیستم بیت کوین نیازمند حاکمیتی است که بتواند بر چالش های ساختاری بلندمدت غلبه کند. لازمه حفظ سیستم بیت کوین، انگیزه ی استخراج است. اگر انگیزه ی استخراج کافی نباشد، عمل استخراج فروکش خواهد کرد. درحال حاضر عایدی استخراج باید به حد کفایت باشد اما طبق قوانین بیت کوین، عایدی استخراج تابع زمان افت می کند. هزینه معاملات که طبق قانون داوطلبانه و اختیاری است، نمی تواند متفاوت باشد.

تنها راه برای حفظ سلامت سیستم بیت کوین، تغییر قوانین است که این احتمالا با حفظ عایدی استخراج در سطحی بالاتر از حد تعیین شده و یا اجباری کردن هزینه معاملات امکان پذیر است. گروه های مختلف از هر راهکاری سود می برند. انتخاب گزینه های عایدی حاصل از استخراج و هزینه معاملات منوط به یک تصمیم اقتصادی است: اینکه آیا باید منابع پولی را افزایش داد یا مالیات برای معاملات تعیین کرد. در هر صورت، انگیزه بالا برای استخراج بیت کوین باعث گسترش منابع جهت استخراج می شود.

این انتخاب اختلافات سیاسی را در جامعه بیت کوین بهمراه دارد. برخی اعضا به حفظ ثبات منابع پولی اعتقاد دارند و برخی تصور می کنند که افزایش عایدی استخراج باعث تورم پایه پولی می شود. از سوی دیگر مالیات روی معاملات به کسانی آسیب می زند که متکی به معاملات هستند و فشار کمتر به افرادی وارد می شود که بیت کوین ها را خریدکرده و آن را نگهداری می کنند.

چالش دیگر در حفظ سلامت و ثبات سیستم بیت کوین بدلیل مسائل اندازه گیری یا امنیت است که در این صورت نیاز به حاکمیتی است که بتواند بر این چالش ها غلبه کند. اگرچه این حاکمیت غیررسمی است اما جامعه بیت کوین نیازمند روشی برای رسیدن به تصمیمات و عمل کردن به آنهاست.

ساختار حاکمیت بواسطه مدیریت اجرای بیت کوین شکل می گیرد. اولین طراحان این نرم افزار به این جامعه احترام گذاشته و عقاید آنها را مورد توجه قرار دادند. قدرت رهبری این این پروژه همانند سایر پروژه های منبع باز به دست افرادی است که با استفاده از نرم افزار، مدل را به دیگران انتقال می دهند. این انتقال، انشعاباتی را بوجود می آورد که اگر حمایت کافی از این جمعیت به عمل بیاید، این انشعابات پابرجا خواهد ماند. این بدین معناست که انشعابات متعدد از بیت کوین به شکل پول های کمتر رایج با تنوع کمتر بوجود می آید.به نظر می رسد که بنیاد بیت کوین در زمینه فعالیت های تبلیغاتی نقش بسزایی دارد بنابراین می توان نتیجه گرفت که طراحان تاثیر بسزایی بر ترویج بیت کوین در بلندمدت دارند.

نتیجه گیری:

نتایج نشان می دهد که بیت کوین یک سیستم ثابت، قانون مدار و سازگار با انگیزه نیست. اگرچه افراد از قوانین آن تبعیت می کنند اما این رفتار فقط بواسطه توافق ثابت است و قوانین در هر زمانی دستخوش تغییر می شود. درنتیجه می توان گفت که بیت کوین نسبت به قوانین دولت، اصلاح پذیر است، به این معنا که درصورت تغییر قوانین، بیت کوین نیز تغییر می کند. فرایند حاکمیت بیت کوین به صورت نیمه رسمی درحال ظهور است. ساختار حاکمیت بیت کوین تابع فشار قانون گذاران یا نسبت قابل توجهی از افراد یا کاربرانی است که تحت فشار قانون هستند و این قانون گذار است که باید بر اجرای بیت کوین و تغییر قوانین فشار بیاورد.

قدرت قانون گذار بواسطه توانایی افراد برای منشعب کردن قوانین بیت کوین محدود می شود. حتی اگر قانون گذار، طراحان را مجبور کند تا تغییراتی را در قوانین بیت کوین و نرم افزارهای آن اعمال کند اما جامعه بیت کوین قادر است قوانین را گسترش دهد و آن را به سایر نقاط نیز بگستراند. بیت کوین در برابر قانون ایمن نیست و همانند سایر پول های سنتی نمی باشد. بیت کوین اولین واحد پولی با منبع باز است. تنها راه برای حفظ سلامت سیستم بیت کوین، تغییر قوانین است که این احتمالا با حفظ عایدی استخراج در سطحی بالاتر از حد تعیین شده و یا اجباری کردن هزینه معاملات امکان پذیر است.

بیت کوین مورد توجه بسیاری از کاربرانی قرار گرفته که بدنبال استخراج پول های جدید و پیشرفت در آینده هستند. فرایند ایجاد بیت کوین های جدید، استخراج گفته می شود که کاربران با استفاده از نرم افزارهای خاص به حل این موضوع می پردازند. در گذشته، کاربران به کمک کامپیوترهای شخصی و پردازنده ها و با حل مسائل ریاضی، بیت کوین را استخراج می کردند اما بعدها با استفاده از کارت گرافیک در بازی ها و انیمیشن های ۳بعدی توانستند الگوریتم های بیت کوین را به اجرا در آورند.

منابع فارسی:

دعائی، میثم. حسینی، میرمیثم. (۱۳۹۳). بیت کوین نخستین پول مجازی. ماهنامه بورس. شماره ۱۱۴۰۱۱۵، ص ۸۴-۸۸.

عشوریان، محسن. جانو سپاه، صفورا. (۱۳۸۷). پیاده سازی نرم افزاری یک سیستم پول دیجیتالی مبتنی بر روش برند، دومین کنفرانس جهانی بانکداری الکترونیکی، تهران، موسسه مطالعات بهره وری و منابع انسانی، https://www.civilica.com/Paper-EBANKING02-EBANKING02_015.html.

منابع انگلیسی:

Acharya. S, Thomas. A, Pani.B.(2018). Volatility of Bitcoin and Its Implication to be a Currency. International Journal of Engineering Technology Science and Research. V.5.P. 2394-3386.

Back, A. (2002). Hashcash-a denial of service counter-measure.

Berentsen, Aleksander, and Fabian Schar. (2018). "A Short Introduction to the World of Cryptocurrencies." Federal Reserve Bank of St. Louis Review 100(1), pp. 1–16. https://research.stlouisfed.org/publications/review/2018/01/10/a-short-introduction-to-the-world-ofcryptocurrencies/.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P., & Böhme, R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In The Economics of Information Security and Privacy (pp. 135-156). Springer, Berlin, Heidelberg.

Bitcoin - P2P Digital Currency. http://bitcoin.org

Chiu, J., & Koeppl, T. V. (2017). The economics of cryptocurrencies–bitcoin and beyond.

Dai, W. (1998). b-money, 1998. URL: http://www. weidai. com/bmoney. txt (visited on 10/12/2017).

Dwork, C., & Naor, M. (1992, August). Pricing via processing or combatting junk mail. In Annual International Cryptology Conference (pp. 139-147). Springer, Berlin, Heidelberg.

Hale, G., Krishnamurthy, A., Kudlyak, M., & Shultz, P. (2018). How Futures Trading Changed Bitcoin Prices. FRBSF Economic Letter, 2018, 12.

Hodson, H. (2014). My Bitcoin road trip: living on virtual money for a day.

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS (Vol. 2013, p. 11).

Laurie, B., & Clayton, R. (2004, May). Proof-of-work proves not to work; version 0.2. In Workshop on Economics and Information, Security.

Lo. S, Wang. J.C.(2014). Bitcoin as money. Current policy perspectives.No.14-4.

Lu, L. (2018). Bitcoin: speculative bubble, financial risk and regulatory response.

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O., & Wehrle, K. (2018). A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). Zerocoin: Anonymous distributed e-cash from bitcoin. In Security and Privacy (SP), 2013 IEEE Symposium on (pp. 397-411). IEEE.

Nakamoto, S. (2008, October 31). Bitcoin.org. Retrieved from Bitcoin.org: https://bitcoin.org/bitcoin.pdf.

Ochs, J., & Roth, A. E. (1989). An experimental study of sequential bargaining. The American Economic Review, 355-384.

Roy, D., & Sahoo, A. (2016). Payment Systems in India: Opportunities and Challenges. The Journal of Internet Banking and Commerce, 21(2).

Ron, D., & Shamir, A. (2013, April). Quantitative analysis of the full bitcoin transaction graph. In International Conference on Financial Cryptography and Data Security (pp. 6-24). Springer, Berlin, Heidelberg.

Abstract:

Bitcoin is a digital cryptography money to be considered by technology experts. The aim of this study was to define bitcoin and the how to mine. Therefore, strategy of bitcoin mining was examined by modelling. The result showed that bitcoin system is not a fixed, rule-driven and incentive-compatible system. Although users follow the rules, their behavior remains stable by agreement. In addition, bitcoin is amenable to the rules of government. It means that the system is altered by changing the rules.

Keyword: Bitcoin**,** Digital money**,** Cryptography**,** Extraction.