

# بررسی ساختار بلاک چین و نحوه تاثیر گذاری

علی عسگری

[ali8asgari@gmail.com](mailto:ali8asgari@gmail.com)

چکیده- با بررسی اجمالی فناوری بلاک چین در میابیم که این فناوری در سال های دور بیشترین کاربرد را خواهد داشت و البته برای استفاده از این فناوری در زیرساخت ها ، دولت ها میتوانند آن را گسترش دهند ، البته لازم به ذکر است که فرضیه ی دیگری مطرح است که در آن ، این فناوری بر علیه قدرت دولت ها و سیستم های مالی و اطلاعاتی ایشان است.

**واژه های کلیدی:** بلاک چین - سیستم - بانکداری - مهندسی نرم افزار - ساختار بلاک چین - بیت کوین - اتریوم - رپبل

## 1- مقدمه

بانک صادر شده بود و پیش بینی میشد که 80 درصد ایشان از سال 2017 فعالیت خود را آغاز کنند.

استفان کونارد بیان نموده است که :

فناوری بلاکچین ویژگی های خاصی دارد که میتواند در صنعت مالی کشورها مورد استفاده قرار بگیرد اما تا به امروز این فناوری در مقیاس های بزرگ در یک جامعه مدرن مورد استفاده قرار نگرفته است. این محقق به مرور منابع و تحقیق های گذشتگان در رابطه با استفاده فناوری بلاکچین در صنعت مالی پرداخته است. یکی از ویژگی های فناوری بلاکچین مقیاس پذیری آن می باشد که این قابلیت را ایجاد می کند که از مقیاس روستا تا کشور و حتی قاره ها مورد استفاده قرار گیرد. همچنین با بیان اینکه وظیفه اصلی بلاک چین ذخیره و انتقال اطلاعات است اما می تواند در مسائل مالی مورد استفاده قرار گیرد ، یکی از نکات محوری مربوط به تفکر استفاده از این فناوری که در واقع ستون این آرمان است را بیان میکند .

[2][3]

اخیرا موسسه های بین المللی که شامل ملل متحد و صندوق بین المللی پول بعلاوه ملت های پیشرفته از قبیل: امریکا، انگلستان، ژاپن توجه زیادی به فناوری بلاکچین و نقش آن در فناوری مالی داشته اند. بنابراین کشورهای مثل روسیه، چین، هند، آفریقای جنوبی و دیگر کشورهای در حال توسعه تحقیقات خودشان را در زمینه فناوری بلاک چین آغاز کرده اند که البته در ادامه به نقد برخی مسائل خواهیم پرداخت.

لازم به ذکر است که برخلاف ایالات متحده رییس بانک خلق چین از حامیان حرکت نظام بانکداری در کشورش به سمت بلاک چین است و چینی ها حداقل در بازی رسانه ای حمایت از تکنولوژی بلاک چین حتی در اوج شیوع ویروس ووهان در کشورشان نیز کوتاه نیامدند.

## 2-1- سیستم های مالی

تا پیش از سال 2018 حدود 40 بانک از امریکا و تنها 2 بانک از چین را یک کنسرسیوم بنام R3 در خود جای داده بود و باید بیان شود که این کنسرسیوم بر پایه نوعی بلام چین غیر متمرکز بنا نهاده شده است.

در سه بخش با سه تیتر مختلف به بررسی بلاک چین خواهیم پرداخت ، سیستم بانکداری فعلی را بررسی میکنیم و سعی میکنیم بیان کنیم که آیا فناوری بلاک چین در این سیستم پذیرا و تاثیر گذار خواهد بود یا خیر.

هم چنین بررسی خواهیم کرد که فلسفه پیدایش بلاک چین چه بوده است و بیت کوین که نماد یک محصول موفق ، با تکیه بر این فناوری بوده است بررسی میشود.

به امنیت موجود در سیستم خواهیم پرداخت و البته بحث مصرف انرژی برای پایداری سیستم را بررسی خواهیم کرد.

## 2- سیستم های بانکداری و بلاک چین

به بررسی فناوری بلاک چین در سیستم های بانکداری میپردازیم

نویسندگان با بیان اینکه در جهان امروز صنایع بزرگ و کوچک به سمت این تکنولوژی در حال حرکت هستند متن خود را آغاز و سعی بر نشان دادن اهمیت تکنولوژی بلاک چین داشته اند .

سیستم بانکداری سیستم بسیار سنگینی می باشد که با وجود استفاده از بانکداری الکترونیکی برای سمت کاربر ، نسبتا فرایندهای تراکنش و زیرساخت فنی و مدیریتی خود را همچنان سنتی و کلاسیک نگه داشته است

نویسندگان با بیان تاثیر فناوری بلاک چین در زمینه های سرعت بخشیدن به تراکنش ها، بالا بردن امنیت، مقابله با اختلاس های بانکی و ذخیره سازی اطلاعات مشتری ها و کاهش در زمان و هزینه های مربوط به عملیات های بانکی ، در ابتدای نگارش خود ذهنیت آرمانی و ایده آل خود را در این مورد نشان میدهند و بواقع نکات بیان شده همان هدف هایی است که برای تحقیقشان سیستم بانکداری حداقل به یک فناوری برتر نیازمند است.

در ادامه با بیان برخی آمار و ارقام رشد گرایش به استفاده آزمایش از زنجیره بلوک توسط بانکهای سراسر جهان ، بار دیگر اهمیت موضوع مورد بحث نشان داده شده است. پیش از سال 2017 مجوز پرداختن به این فناوری برای حدود 2500

از لحاظ توزیع زیرساخت بحث انتقال و ذخیره داده در ابعاد بالا و وسیع به دو نوع متمرکز و غیرمتمرکز تا کنون قابل پیاده سازی بوده است.

مسئله قابل ملاحظه دیگر بحث پیدایش صرافی ها و سیستم های مبادله آنلاین و امن دارایی از قبیل پول و غیره می باشد که اشاره کوتاهی به ایشان شده است و با استفاده از بستر بلاک چین این صنایع نیز رشد نمایی جالبی را تجربه کرده اند.

پیش از پرداختن به باید ها و نباید های هر فناوری در سیستم بانکداری به نقد برخی از مطالب بیان شده تا اینجا میپردازیم.

از آنجا که تغییر کامل تکنولوژی آنها در بحث زیرساخت فناوری به کل برای صنایع هزینه بر و بسیار دشوار می باشد در نتیجه به نظر نمیرسد که صنایع خرد علاقه و توان کافی برای ایجاد این تغییر اساسی را از خود نشان دهند.

نویسندگان رفتن پی تکنولوژی بلاک چین را به صنایع کوچک و بزرگ بسط داده است در حالی که هیچ گونه دیتا یا آمار در این مورد را ذکر نکرده است.

علاوه بر این نکاتی که در مورد مزایای استفاده از بلاک چین برای بانکها بیان شده کاملاً آرمانی میباشد و بهتر بود تحت عنوان مزایای محتمل از آنها یاد شود که دستیابی به همه آنها باهم نیز امری محال شمرده میشود.

ضعف دیگر نویسنده عدم بیان و تشریح تقریباً هیچ کلام فنی و مهندسی در طول نگارش است که با توجه به عضویت ایشان در جایگاه رده بالای سیستم آموزشی این انتظار می رفت که چگونگی برخی مطالب را از لحاظ معنایی و فنی تشریح نمایند.

من سعی میکنم در مورد مزایای استفاده از بلاک چین خیلی کوتاه ضعف فنی نویسندگان را جبران نمایم. لازم به بیان است که امروز بلاک چین های بسیاری توسط اشخاص و شرکت ها توسعه داده شده اند به این معنا که هنگامی که در مورد بلاک چین صحبت میکنیم در مورد یک یا دو روش محدود ذخیره اطلاعات در دیتابیس غیر رابطه ای صحبت نمی کنیم. در حال مقایسه چند سیستم مدیریت دیتابیس ساده نیز نیستیم. راجع به بلاک چین های پیشرفته و پیچیده ای صحبت میکنیم که تفاوت ها بنیادین فنی و پایه ای و حتی فلسفی با یکدیگر دارند.

## 2-2- بحث ارز ها

در مورد ارز های دیجیتال در آینده صحبت خواهیم کرد اما باید گفته شود که برای مثال ارزی بنام اتریوم که بر پایه بلاک چین خودش توسعه داده شده است

امروز به چند ارز متفاوت تبدیل شده است نظیر اتریوم و اتریوم کلاسیک ؛ حال این سوال پیش می آید که تفاوت این دو در چیست ؟

تیم فنی اتریوم پس از توسعه و انتشار اتریوم از لحاظ فلسفی دچار اختلاف می شوند و تصمیم به جدایی می گیرند و در واقع اتریوم کلاسیک اتریوم است که بر پایه بلاک چین اولیه ای که تیم فنی توسعه داده بود ادامه میدهد و اتریوم کنونی ساختار

کاری و فنی خود را تغییر میدهند. حال علت را چنین بیان کرده اند که پس از یک سری حملات سنگین به زیر ساخت این ارز در ابتدای راه خود که باعث میشود عمده ارز های موجود با نام اتریوم از دسترس خارج شوند، دو دیدگاه در تیم بوجود میاید. مهندسانی که امروز در تیم اتریوم کلاسیک فعالیت می کنند اعتقاد دارند که ایشان باید تصور کنند همانند یک بانک که مورد سرقت قرار گرفته اند می باشد و نباید تغییری در خود ایجاد کنند و بواقع با روش های سابق ادامه دهند، اما توسعه دهندگانی که امروز اتریوم را به اوج رسانده اند و اخیراً با رشد 100 درصدی ارزش ارز خود مواجه شدند بنا به گفته هایشان به نظام بانکداری و سیستم ایشان بدبین بوده و ترجیح دادند روش ها و متد های خود را تغییر دهند.

## 3-2- وسعت فناوری بلاک چین

پس باید گفته شود که دنیای بلاکچین بسیار وسیع است. بیت کوین بی شک موفق ترین محصول فناوری بلاک چین است اما با بررسی زیرساخت این پلتفرم باید گفت که هزینه تراکنش بالایی دارد و چنین پلتفرم رویایی ای که به بهترین شکل پیاده سازی شده نیز با آرمان های گفته شده توسط نویسندگان همخوانی ندارد. این پرسش ها پیش می آید که بلاک چین که با موضوعیت عدم انحصار و پراکندگی منابع بوجود آمده است، حال آیا شما میخواهید از تعداد محدودی بلاک چین و ایجاد کنسرسیوم های چند گانه در دنیا آن را به یک ابزار برای انحصار دوباره قدرت بدل کنید؟

آیا این کار امکان پذیر است ؟ ارتباط بین بلاک چین ها را چگونه مدیریت می کنید ؟ و سوال های بی شمار دیگری از این قبیل وجود دارد.

نکته بعدی که شاید بر همگان پوشیده نباشد پیشروی ایالات متحده آمریکا در عرصه فناوری بلاک چین حداقل در فاز تحقیق با وجود سخنان تند و تیز بسیاری در این کشور از جمله دونالد ترامپ یا سرمایه گذار بزرگ وارن بافت و غیره میباشد. نویسنده اشاره مختصری به سیستم های اکسچنج و صرافی های آنلاین داشت. به این لیست سیستم های مبادله آنی را اضافه کنید.

باید بپذیریم که موفق ترین محصول بلاکچین، ارز های دیجیتال می باشد، شاید برای سیستم های بانکداری چندان جذاب نباشد ولی واقعیت این است که گرم ترین بازار فناوری بلاکچین بازار فرزند دلبدش ارز های دیجیتال است و پلتفرم های بسیاری برای مبادله و ذخیره این ارز ها راه افتاده اند که از نامدارترین آن می توان به باینس اشاره کرد.

فلسفه ای که ارز های دیجیتال از آن پیروی میکنند چندان مورد قبول سیستم های بانکداری نیست و بالعکس، در ادامه سعی میشود به این موضوع نیز پرداخته گردد.

## 4-2- لازمه استفاده از فناوری بلاک چین در ساختار صنعت بانکداری

بانک ملی استرالیا نیز برای انتقال 10 دلار به کانادا از ریپل استفاده کرد و این تراکنش در مدت 10 ثانیه انجام شد.

### 8-2- آیا حذف واسطه های بین بانکی ممکن است؟

جواب داده شده به این سوال این است که الزامی که برای تحقق این امر وجود دارد غیر متمرکز سازیست، به عنوان مثال بیت کوین به وسیله غیر متمرکز سازی توانسته است تقریباً بدون واسطه گسترش یافته و پایدار بماند، که حصول این امر در بحث بانکداری بشدت مشکل بیان شده است.

در ادامه و در بیان نکته آخر به نظر نمیرسد که قانون مند سازی بستر بلاک چین فعلاً در کشور ایران در دسترس باشد، علاوه بر ابهامات حقوقی بلاکچین در ایران باید ابهامات فقهی را نیز برطرف کند.

از آن سو چینی ها بشدت به این امر علاقه نشان داده اند و امریکایی ها نیز با وجود اینکه در بحث قانون مند سازی پیش نرفته اند، اما نشان داده اند که گسترش بلاک چین چندان به تمجید مسئولین نیازی ندارد.

برای نقد مطالب بیان شده باید گفت که بسیاری از مشکلات داخلی بانک های ایران ناشی از استراتژی های مدیریتی اشتباه، ضعف اقتصادی کشور، کاهش اعتبار ارز ملی و قوانین ضعیف حوزه بانکداری ما بوده اند و نسبت دادن بلاک چین به راه حل اینگونه مشکلات تا حدی ضعف در سنجش و فرار رو به جلوست.

هر چند که در بحث مشکلات خارجی ما محتمل است که بلاک چین بتواند گره گشا باشد، چرا که اکنون بانکهای ما برای انتقال وجه بین المللی مجبورند با هماهنگی بانک دوم در کشور دوم، در یک بانک سوم در کشور سوم حساب باز کنند و بانک سوم بتواند حساب بانک اول و دوم را پذیرفته و تراکنششان را انجام دهد، این فرآیند بسیار سخت میباشد.

در بحث حذف شرکت های واسطه نیز باید توجه شود که تنها بحث فنی مطرح نخواهد بود، این شرکت ها بسیار ثروتمند، با نفوذ و قدرتمند می باشد و حذف ایشان یک جنگ اقتصادی میطلبد.

در مورد ریپل اما باید گفت ارز دیجیتال محبوب دولت هاست، با بودجه دولتی در آمریکا توسعه یافته و تنها ارز دیجیتالیست که ایالت متحده از آن حمایت میکند. احتمالاً این ارز و پلتفرمش بستر مناسبی برای سیستم بانکداری ایجاد میکنند، چرا که اگر یک پلتفرم وابسته به دولتها چنین کاری را انجام ندهد، پیش بینی پلتفرم مناسب برای بانکها جهت توسعه دشوار خواهد بود.

در پایان باید گفت متأسفانه بعثت ضعف هایی که در مقاله و بیان نویسندگان احساس میشد مجبور به اضافه کردن نکات و نظرات شخصی خود شدم که سعی میگردم در ادامه بررسی دیگر مقالات چنین مسئله ای کمتر نمایان شود. [1]

بانک های ایرانی امروز با مشکل کاهش اعتبار بین مردم، افزایش ریسک و کاهش سود دهی و سخت تر شدن واگذاری تسهیلات و... مواجه اند و با توجه به گرایش اکثر آنها به بانکداری الکترونیک و سیستم هوشمند، از خیز بلند بسمت تکنولوژی سطح بالای بلاک چین به عنوان راه حلی برای رفع برخی مشکلات بانکی یاد شده. لازم به بیان این نکته نیز هست که علاوه بر مشکلات داخلی یاد شده میتوان از مشکل ارتباط با بانکهای خارجی نیز به عنوان یک مشکل کلیدی یاد کرد.

### 5-2- سیاست های داخلی صنعت بانکداری ایران و رشد

#### فناوری دیجیتال

بانک سپه نخستین بار در سال 90 میلادی اولین دستگاه ای تی ام را در کشور راه اندازی، 2002 سیستم شتاب و تلفن بانک و در سال 2008 موبایل بانک وارد سیستم بانکداری شد.

### 6-2- سیاست های خارجی صنعت بانکداری ایران و تحریمها

در سال 2001 حدود 57 بانک خصوصی و دولتی ایرانی در کشور های خارجی فعالیت خود را آغاز کردند اما متأسفانه در پی تحریمها روز به روز از این تعداد کاسته و با تحریم دولت آمریکا در سال 2012 مبنی بر عدم اجازه بانکهای ایرانی از شبکه سوئیفت که زیرساخت تراکنش های بین المللی را فراهم می ساخت عملاً نظام بانکداری ایران را وارد فاز جدیدی از مشکلات کرد، در این میان برخی منابع ادعا کرده اند روسیه و ایران برای استفاده نکردن از دلار، سیستم پرداخت مبتنی بر بلاکچین و جایگزین سوئیفت را کلید زده اند، هر چند که این مسئله جای تأمل و بحث فراوان دارد.

### 7-2- سناریو ها و کاربرد های مختلف

ایجاد یک مکانیسم اعتباری برای رفع عدم اعتماد بین طرفین معاملات و کاهش هزینه های مربوط به مسایل فنی از اهداف استفاده از بلاکچین در سیستم بانکی بیان شده است و نیز بیان شده است که مسائلی از قبیل بازدهی کم، وقفه در تراکنش، اختلاس و تقلب، ریسک های عملیاتی می باشد که این مسایل اصلی میتواند با استفاده از فناوری بلاک چین حل شود.

در بحث پرداخت های داخل بانکی نیز شرکت های خصوصی ای ایجاد شده است که به عنوان واسطه عمل می کنند که شامل فرایندهای پیچیده ای که شامل حسابداری، اصلاح تراکنش ها، اصلاح تراز، شروع پرداخت و غیره می باشد و از آن به عنوان فرآیندی پر هزینه و زمان بر یاد میشود که حداقل 3 روز ذکر شده، همین مسئله باعث پایین آمدن راندمان بانک در شفاف سازی تراکنش ها میشود و از فناوری بلاک چین به عنوان راه حلی برای حذف این شرکت های واسطه یاد شده است.

در حال حاضر تعدادی از بانکها از نمونه آزمایشی فناوری بلاکچین استفاده میکنند، برای مثال پلتفرم ریپل یکی از این پلتفرم هاست که عملیات هایی که در سیستم سنتی 2 روز زمان طلب می کردند را تنها در چند ثانیه انجام میدهند.

### 3- سیستم نظارت بر مجموعه پرداخت بر اساس تکنولوژی بلاک چین با استفاده از کیف پول دیجیتال بیت کوین

در ابتدای مباحثی که در این نوشته بیان خواهد شد به سنتی بودن سیستم بانکداری ای که امروز شاهد آن هستیم اشاره می شود، حال باید اینگونه نتیجه گیری کرد که سیستم بانکداری الکترونیک و آنلاین امروز ؛ در مقایسه با تکنولوژی بلاک چین کاملاً سنتی بنظر میرسد. مسائلی مثل ساعت اداری و سختی انتقال پول بین المللی در سیستم بانکداری امروز مطرح می باشد در حالی که بلاک چین از این مسائل مبرا است. به عنوان مثال، در صورت ارسال مبلغ پول از بانک مرکزی ایالات متحده به یک بانک در چین نه تنها باید تا رسیدن به ساعت های اداری این دو بانک ملی مختلف صبر کرد، بلکه پرداخت کننده همچنین حتی پس از انتقال به چین و ارائه مدارک اظهارنامه برای تأیید منبع این پول باید 3 روز کاری منتظر بماند. سوم این که، مشتری در نهایت باید تا 750 دلار NT هزینه کند.

گفتنیست که تکنولوژی بلاک چین در حال تبدیل شدن به بهترین راه حل برای حل مسئله تفاوت زمان انتقال بین المللی پول است. بر اساس ساختار همتا به همتا و ناشناس بودن در فناوری بلاکچین، مشتریان برای اعلام منابع مالی نیازی به رفتن به بانک و نیازی به پرداخت هزینه برای انتقال بین المللی ندارند.

به گمانم به ناگاه آب سردی بر تفکر ورود بلاک چین به سیستم بانکداری ریخته شد، با وجود مزایایی که بر اثر کاربرد بلاک چین در سیستم بانکداری بوجود خواهد آمد اما اگر به پاراگرافی که در بالا بیان شد توجه کنید یک سوال اساسی بوجود خواهد آمد ؛ در ادامه سعی خواهیم کرد که سوال مربوطه را واضح تر بیان کنیم.

#### 1-3- در مقایسه با موسسات مالی

بیت کوین یک سیستم نقدی الکترونیکی P2P است. طراحی منحصر بفرد می تواند مزایای بیشتری مانند کاهش خطر حملات سایبری را به همراه داشته باشد، زیرا ذخیره سازی زنجیره ای از طریق تکنولوژی شبکه P2P در سرتاسر کامپیوتر های در حال اجرا و متصل به تمام گره های اینترنتی توزیع شده است. امروزه حجم زنجیره بیت کوین به بیش از 100 گیگابایت رسیده است. تمام داده ها در تراکنش بیت کوین از 2009 به طور دائمی در زیر بلوک های زنجیره ای ذخیره می شوند. بر اساس آمار رایانه های سیستم بیت کوین در جهان بیش از 6000 گره شبکه هستند. این بدان معنی است که اطلاعات بلاکچین بیش از شش هزار بار کپی شده است. چنین مقدار زیادی از گره های شبکه برای تهیه نسخه پشتیبان بلاکچین می تواند ثبات شبکه بیت کوین را تضمین کند. عدم عملکرد صحیح یک کامپیوتر میزبان بر عملکرد نرمال بیت کوین تاثیر نمی گذارد. علاوه بر این، به دلیل سیستم غیر

متمرکزی که در شبکه بیت کوین اعمال می شود، مردم در هر زمان نیاز به عملیات، مدیریت و نگهداری دستی ندارند. بنابراین، سیستم بیت کوین می تواند به طور مداوم بدون اختلال در ثبات نسبتاً خوب موجود، پیوسته در حال کار باشد، این سیستم در واقع بسیار متفاوت از سازمان های مالی متمرکز سنتی است. سیستم معاملات مالی سنتی متشکل از بسیاری از سازمان های مالی مرسوم است. کاربران باید به استفاده از جریان پرداخت بسته برای استفاده از خدمات مالی این سازمان ها اعتماد کنند. با این حال، سیستم تراکنش های مالی متمرکز پاره ای از مشکلات را متحمل است که باید برطرف شود. به عنوان مثال، از زمانی که همه اطلاعات تراکنش به طور مرکزی مدیریت می شود، مشتریان مجاز به دسترسی آزاد به اطلاعات مربوط به اطلاعات تراکنش خود نیستند. این تراکنش ها به صورت عمومی بررسی نشده و مشتریان مجبور به اعتماد به شرکت های مالی خود در زمینه ایمنی صندوق ها، از جمله جریان مالی هستند. اگر این موسسات مالی مرکزی سنتی تکنولوژی بلاک چین را در سیستم جریان مالی خود اعمال کنند. تکنولوژی بلاک چین به کار برده خواهد شد تا نشان دهد که سوابق تراکنش ها برای همه مشتریان به طور شفاف در دسترس است. بنابراین، هیچ مسئله ای در مورد جریان نقدی ناشناخته نخواهد ماند. این سیستم نه تنها جریان مالی را شفاف نگه می دارد، بلکه تضمین می کند که سوابق معاملات تراکنش ها با تغییر و حذف رو به رو نخواهد بود.

#### 2-3- پرسش های اساسی

پس حال شاید بتوان آن پرسشی که قصد داشتیم برایتان بوجود آوریم را واضح تر بیان کنیم ، در دنیایی که بلاک چین ها و ارزهای دیجیتال توسعه یافته اند و فروشندگان و شرکت ها به ایشان رو آورده اند ، پس اصلاً چه نیازی به سیستم بانکداری وجود دارد؟

بعنوان یک شهروند عادی نظارت همه جانبه دولت ها بر زندگی شخصیتان را میپسندید و همچنان اعتماد به سیستم های بانکداری و وام های ایشان ستون اصلی زندگی تجاریتان را تشکیل میدهند ؟

یا اینکه با درک مفهوم و فلسفه بلاک چین امیدوار شدید که میشود به عصر جدیدی از توزیع اطلاعات در دنیا رسید؟

حال باید بیشتر رفتار خصمانه دولت هایی مثل امریکا حداقل در ظاهر با این سیستم را درک کنید ، چرا که در مقابل کشوری بنام روسیه و شخصی بنام پوتین از حامیان اصلی این تکنولوژی میباشند ، دلیل این امر نیست باید برایتان واضح شده باشد، توسعه بلاکچین میتواند دلار آمریکا را از معاملات بین المللی حذف کند ، در این صورت کشور هایی که به پشتوانه دلار آمریکایی که مبادله میکنند ، از بانک مرکزی آمریکا خواستار بازگشت سرمایه ذخیره شده خود هستند که این به معنای سقوط کامل دلار خارجی امریکاست.

### 3-3- نقش دولتها

دولت آمریکا با عملکرد هوشمندانه در مقابل ارزی مثل بیت کوین سعی بر توسعه پلتفرم و ارزی بنام ریپل شد که ما نیز پیش از این راجع به ریپل مطالبی بیان کرده ایم. باید گفت که توسعه بلاک چین در زیرساخت و استفاده از آن در بستر سیستمهای خدمات رسانی، قدرت و هزینه قابل توجهی می طلبد، پس شاید این دولت ها باشند که بتوانند این تکنولوژی را توسعه دهند و از آن به نفع خود استفاده کنند، در غیر این صورت بسیار متضرر خواهند شد. حال بیا بیا بررسی کنیم در صورت مداخله دولت و گسترش این تکنولوژی وضعیت کسب و کارها و شرکت ها به چه شکل تغییر میکند.

در این صورت فروشنده می تواند صحت الگوریتم را با استفاده از فناوری بلاکچین جهت اعتماد به تراکنش بپذیرد و به طور دقیق تر تمام جزئیات تراکنش را درک میکند و یا حتی وضعیت کسب و کار شرکت را که به راحتی ارائه شده است، می سنجد. سپس، منابع انسانی را می توان به طور موثری برای تولید گزارش های مالی و آماری کاهش داد. سرانجام، دولت می تواند به راحتی تمام اطلاعات کسب و کار را بررسی کند. همچنین می تواند برای جمع آوری مالیات، یک روش عملیاتی استاندارد، قابل اعتماد و کاملاً اتوماتیک داشته باشد. این سیستم نه تنها می تواند هزینه کلی را کاهش دهد، بلکه اشتباهات در روش مالیات دولتی را نیز کاهش می دهد.

### 3-4- پرداختن به چگونگی

مجموعه ای از سیستم نظارت بر مجموعه پرداخت بر اساس سیستم بلاکچین پیشنهاد شده است که BPCSS نامیده می شود. گفتنیست که این سیستم برای تراکنش های بین مشتریان و فروشگاه های تجاری به کار می رود که از کیف پول دیجیتال بیت کوین استفاده می کنند.

در ادامه به بررسی و مقایسه روش های انتقال پول الکترونیکی خواهیم پرداخت، این مسئله بسیار مهم است و ویژگی هایی نظیر سرعت تراکنش و امنیت اطلاعات تراکنش از اهمیت بالایی در این مقایسه برخوردارند.

ابتدا تکنولوژی محبوب تراکنش های مالی مربوط به ویزا را بدون استفاده از ارز فیزیکی معرفی می کنیم.

### 3-5- تکنولوژی ویزا

بدهی ویزا یک دبیت کارت (کارت بدهی) می باشد، که می تواند پول را از دستگاه خودپرداز برداشته و همچنین پول را به طور مستقیم به فروشگاه ارسال می کند. کارت بدهی را می توان به طور مستقیم از حساب سپرده کاربر شارژ کرد. اگر موجودی حساب کاربر ناکافی باشد، روند تراکنش تکمیل نخواهد شد. این امر نرخ بهره متناوب یا حواله ی بیش از حد را ایجاد نمیکند، به طوری که صاحبان کارت ها می توانند به راحتی بودجه و هزینه های خود را کنترل کنند. بدهی ویزا از کارت خوان تراشه برای خواندن داده ها در کارت اعتباری استفاده می کند. اطلاعات شامل آرم ویزا و شماره کارت 16

### 3-6- داده های تراکنش بلاکچین ثبات

در ساختار بلاکچین، تمام اطلاعات پس از تاییدیه در بلاکچین ثبت شده و نمی توانند حذف شوند. بر اساس خصوصیات بلاکچین، هنگام اتصال بلوک جدید به بلوک اصلی مقدار هش بلوک قدیمی در بلوک جدید ذخیره می شود. تا زمانی که یک مقدار در بلوک حتی کمی اصلاح شود، ارزش هش کاملاً متفاوت خواهد شد، به این معنی که، اثر بهمن رخ خواهد داد. به دلیل این که ساختار که تمام اطلاعات هرگز تغییر نخواهد کرد، اگر نتیجه تایید تغییر کند، بلوک توسط سیستم پذیرفته نخواهد شد. بنابراین، تمام اسناد تراکنش هایی که در بلاکچین ذخیره شده اند، نمی توانند اصلاح و حذف شوند.

### 3-7- معماری شبکه همتا به همتا

سیستم تجاری بلاکچین بر اساس معماری شبکه P2P است و مالک ویژگی های غیر متمرکز می باشد. به دلیل پروتکل غیر متمرکز P2P، تمام گره ها نه تنها نقش مشتریان را بازی می کنند، بلکه نقش سرورها را نیز بازی می کنند. در این شبکه غیر متمرکز در جهان، در مقایسه با سرور متمرکز سنتی که معمولاً در سرویس وب با مقیاس یک رقمی سرور میزبان ارائه می شود، سیستم بیت کوین می تواند به بیش از 6000 گره گسترش یابد. بنابراین، شبکه بیت کوین می تواند برای جلوگیری از حملات عدم پذیرش سرویس بهتر رفتار می کند. در سال های اخیر، به دلیل شیوع و ناشناس بودن بیتکوین، این

کریپتو اینترنتی می باشد، در حالی که بیت کوین معروف ترین است. بیت کوین بلاک چین یکی از موثر ترین سیستم های جریان انتقالی در بسیاری از کشورها در سراسر جهان است. ارز کریپتو اینترنتی از تکنولوژی بلاک چین برای تکمیل انتقال وجوه صندوق بین کاربران استفاده می کند.

#### **b. بلاک چین 2.0 - قرارداد هوشمند**

در واقع بلاکچین 2.0 قرارداد هوشمندانه است. تکنولوژی امروزه ی بلاکچین بر روی کاربرد اقتصاد و امور مالی بازار تمرکز دارد. علاوه بر سادگی انتقال بودجه، محصولات مالی ایجاد شده در زندگی نیز می تواند اشیائی برای اعمال بلاکچین آنها شامل سهام، اوراق قرضه آتی، وام، حقوق مالکیت، دارایی ها و قراردادهای باشد. مرحله ابتدایی بلاکچین 1.0 به طور گسترده ای در ذخیره سازی معاملات مورد استفاده قرار می گیرد. علاوه بر استفاده از سوابق معامله، بلاک چین را می توان به عنوان یک پایگاه داده فهرست موجودی برای ضبط، ردیابی و انتقال همه دارایی ها در نظر گرفت. علاوه بر این، می تواند به عنوان ثبت اطلاعات هر گونه تشکیل دارایی، ثبت نام، موجودی و اطلاعات معامله باشد.

#### **c. بلاک چین 3.0 - برنامه های غیر متمرکز:**

بلاک چین 3.0 . نه تنها از قید برنامه های اقتصاد بازاری و مالی رها شده است، بلکه تأکید بیشتر آن روی حوزه های دولت، سلامت، فرهنگ، ادبیات هنر و زمینه های دیگر است. برای مثال، در دولت ارمنستان، طی سال های اخیر کارت هویت ملی، در ساختار بلاکچین ساخته شده است، تا قراردادهای تجاری یا حتی گواهی ازدواج از طریق آن امضا شود. [4]

#### **4- پایداری بیت کوین و زنجیره های بلوک**

ساتوشی ناکاموتو فردی ناشناس در سال 2008 برای اولین بار از ایجاد واحدی دیجیتالی بنام بیت کوین خبر داد، وی با پیشی گرفتن از تلاش های ناکام اشخاص و شرکت هایی که پروژه های شکست خورده ای نظیر بی کوین و بیت گولد را ایجاد کرده بود توانست مشکلاتی نظیر متمرکز بودن و بحث دابل اسپندینگ را برطرف کند.

تراکنش ها در سیستم بیت کوین در یک دفتر معامله عمومی (زنجیره بلوک) ذخیره می شود، که به این ذخیره سازی نامتمرکز، و به صورت شبکه شخص به شخص می باشد. بیت کوین، انتشار ارز نامتمرکز و مجوز معاملات را فراهم می کند. امنیت زنجیره بلوک بستگی به یک الگوریتم فشرده محاسباتی برای استخراج بیت کوین دارد که از صرف چندباره بیت کوین ها و دستکاری معاملات تایید شده، جلوگیری می نماید. این الگوریتم "تاییدیه-فعالیت" مقضاضی انرژی می باشد. مقدار انرژی که در واقع صرف می شود، جای شک دارد. بحث ما این است که این انرژی که در حال حاضر مصرف می شود، طیفی بین 100 الی 500 مگاوات را دارد. ما توسعه هایی که در سخت افزار استخراج بیت کوین صورت گرفته است را مورد بحث قرار می دهیم.

روش به عنوان راه اصلی برای پرداخت به بدافزار (ویروس) رانسوم ویر تبدیل شده است. با این حال، بلاکچین بر اساس شبکه P2P است. حتی یک داده گره تک توسط رمزنگاری مهاجم رانسوم ویر قفل می شود. چنین اجباری برای شبکه غیر متمرکز بیت کوین تهدید بزرگی نیست، گره های اطلاعات بسیاری در شبکه بیت کوین وجود دارد و آسیب یک گره تنها تأثیر چندانی نخواهند داشت.

#### **- 3-8 ناشناس بودن**

در جامعه فعلی، حفاظت از اطلاعات شخصی به مهم ترین موضوع برای شرکت ها تبدیل شده است. همه حساب های ایجاد شده در سیستم بلاکچین مستقیم رابطه مستقیم با موجودات در دنیای واقعی ایجاد نمی کند، پس ناشناس است. به نظر می رسد همه حساب هایی که در سیستم بلاکچین هستند بصورت فردی، ناشناس و جداگانه ایجاد شده اند و می تواند به طور مؤثر از حریم خصوصی مصرف کنندگان حفاظت کنند. با این حال، تراکنش ویزا متفاوت است و کاربران بسیاری از اطلاعات شخصی را برای میزبان مرکزی در شرکت ویزا آشکار خواهند کرد. این ممکن است خطر نشت اطلاعات شخصی را افزایش دهد که در فناوری بلاکچین، این مشکل را می توان به طریق مقرون به صرفه ای برطرف کرد.

#### **- 3-9 مشکل بلاک چین بیت کوین، ظرفیت ناکافی بلوک**

بیت کوین در اصل برای پیاده سازی الگوریتم اثبات کار طراحی شده است به طوری که ایجاد یک بلوک بیت کوین می تواند به طور متوسط تقریباً در هر ده دقیقه کامل شود. اندازه بلوک به طور پیش فرض به صورت 1MB تنظیم شده است. فرض بر این است که بلوک با توجه به اندازه متوسط 300 بایت در یک تراکنش بیت کوین فعلی به طور کامل از تراکنش ها پر شده است، و سپس هر بلوک می تواند حداکثر سه هزار تراکنش را انجام دهد، می توانیم بگوییم، 5 تا 6 تراکنش در هر ثانیه می تواند در سیستم بیت کوین تکمیل شود. شرکت پرداخت متمرکز الکترونیکی مانند ویزا به متوسط 2000 و حداکثر 4000 تراکنش در هر ثانیه رسیده است. با این حال، سیستم بیت کوین تنها می تواند 5 تا 6 تراکنش را در هر ثانیه انجام دهد و البته فضای بسیاری برای بهبود دارد.

#### **- 3-10 برنامه های بلاک چین**

با این حال، بر اساس تکنولوژی بلاک چین، برنامه های کاربردی غیر از ارز دیجیتالی می تواند ایجاد شود. قرارداد الکترونیکی که اتریوم نامیده می شود، از تکنولوژی امضای حلقه برای ارائه کامل معاملات ناشناس در سیستم پول الکترونیکی به نام مونرو و وبلاگ غیر متمرکز به نام استیم استفاده می کنند، حال باید گفت که با توجه به مطالب بیان شده کاربرد بلاک چین دقیقاً به سه دسته تقسیم میشود.

#### **a. بلاکچین 1.0 - ارز دیجیتال**

بلاکچین 1.0 عمدتاً در پول، مانند سیستم های انتقال مالی، مبادله و سیستم های پرداخت تثبیت شده اند. شایع ترین آنها ارز

**1-4- فلسفه پیدایش سیستم بلاکچین**

علاوه بر نکات فنی بهتر است با فلسفه پیدایش بیت کوین و تاریخچه بشر در استفاده از پول نیز آشنا شویم در ابتدا، ارزها مستقیماً از فلزات با ارزش مانند طلا و نقره، ضرب می شدند. بعدها، اسکناس های کاغذی معرفی شدند و ارزش ظاهری ارز از ارزش اسمی آن جدا بود، اما ارزها همچنان توسط سپرده ها طلا پشتیبانی می شدند. امروزه، صدور ارزها به صورت شناور و آزادانه صادر می شود و تنها به دلیل اعتقاد و اعتبار دولت ها، حمایت می شوند. بیت کوین یک سیستم غیر متمرکز است که تلاش دارد بر ضعف های صدور و ارزش های مبتنی بر طلا غلبه کند. البته با ذکر این نکته که ارزش های رایج که به آنها فیات گفته می شود دیگر به پشتوانه طلا عمل نمی کنند و همانطور که بیان شد بر اساس اعتبار دولت ها صادر میشوند. راجع به بیت کوین و مقایسه اجمالی آن با روند موسسات مالی و بانک ها باید گفت که توسط مقامات مرکزی، مانند دولت ها و یا بانک های مرکزی، اداره نمی شود و واسطه ای برای انتشار ارز یا حل و فصل و اعتباردهی معاملات بوده و می تواند کمترین هزینه تراکنش را در پرداخت ها فراهم کند. اساس بیت کوین، برخی از استانداردهای دولت مرکزی، حفاظت و ارتقا بیت کوین را فراهم کرده است، اما به عنوان یک بانک مرکزی عمل نکرده و ارزی را منتشر نمی کند همین مسئله برای بسیاری کافیت تا به این ارز دیجیتال گرایش پیدا کنند.

اکوسیستم یا فضای بیت کوین، شبکه ای از کاربران است که با استفاده از درگاه بیت کوین از طریق اینترنت، با هم در تعامل می باشند. درگاه بیت کوین، به صورت یک برنامه کاربردی نرم افزار منبع باز در دسترس است و به کاربران امکان می دهد بیت کوین ها را ذخیره و برای خرید و فروش کالاها منتقل کنند یا بیت کوین ها را در مقابل سایر ارزها تبادل نمایند. انتشار بیت کوین ها در حالی درون شبکه انجام می شود که تراکنش ها در فرایندی به نام استخراج بیت کوین، انجام می گردند.

**2-4- مرور کلی سیستم بیت کوین**

سیستم بیت کوین، یک شبکه توزیع یافته فرد به فرد است. هیچ سرور مرکزی یا نقطه کنترلی در آن وجود ندارد، و تمام گره ها در شبکه به طور برابر همسان هستند. هر تراکنش برای انتقال مقداری بیت کوین در میان کاربران به شبکه بیت کوین که در یک مبادله تراکنشی توزیع شده، زنجیره بلوک، ذخیره شده است. زنجیره بلوک، حاوی کل تاریخچه تراکنش های بیت کوین می باشد. هر گره در شبکه یک (به صورت کامل یا بخشی) نسخه از زنجیره بلوک را نگه می دارد. تراکنش های جدید به سرعت در میان سایر گره ها در شبکه پخش می شود. یک تراکنش در حقیقت یک انتقال از منبع سرمایه (به نام ورودی) به مقصد (به نام خروجی) می باشد. ورودی های تراکنش و خروجی ها به حساب ها یا ترازها مرتبط نمی باشند:

یک ورودی مرجعی برای یک خروجی خرج نشده تراکنش از فرستنده در تراکنش قبلی است. قبل از پیش فرستادن یک تراکنش به همسایه آن، هر گره ابتدا تراکنش را اعتبارسنجی می کند، که شامل بررسی ترکیب و ساختار و اینکه آیا انتقال معتبر از مقداری از خروجی های خرج نشده تراکنش هنوز وجود دارد یا نه، می باشد. هر گره به صورت مستقل، تراکنش های دریافتی را بررسی می کند، و استخری از تراکنش های معتبر می سازد. تراکنش های معتبر به زنجیره بلوک در فرایند به نام استخراج بیت کوین، افزوده می شوند. هر گره، تعدادی از تراکنش های معتبر را در یک بلوک جمع آوری کرده و سعی در محاسبه یک مخلوط رمزنگاری از بلوک که محدودیت های مشخصی را برآورده می سازد، دارد.

یک مخلوط رمزنگاری، نوعی از مجموعه های متقابل برای بلوک است که یک طرفه و مقاوم در برابر برخورد می باشد. یافتن رمزی که محدودیت ها نشان داده شده سیستم بیت کوین را تامین کند، یک وظیفه محاسبه ای فشرده است که تنها از طریق نیروی بسیار زیادی قابل اجرا شدن است. این امر مسابقه ای را در میان گره ها در شبکه جهت یافتن هرچه سریع تر رمزی معتبر، ایجاد می کند. اولین گره ای که چنین رمزی را یافت، بلوک را می برد، که بدین معنی است که این بلوک به زنجیره بلوک اضافه شده و در شبکه منتشر می شود. هرچند، محاسبه رمز معتبر سخت می باشد، بررسی اینکه آیا یک رمز معتبر است ساده بوده و بنابراین هر گره که بلوک را دریافت کند می تواند به سرعت شناسایی کند آیا بلوک جدید معتبر است یا خیر. زمانی که یک گره یک بلوک معتبر جدیدی را دریافت می کند، فرایند استخراج را برای بلوک فعلی متوقف کرده و استخراج را برای بلوک جدید آغاز می کند. گره ای که پیروز بلوک است، یک بلوک پاداش می گیرد، که مقدار ثابتی از بیت کوین ها است. بنابراین، صدور بیت کوین ها (ضرب سکه) در طول فرایند استخراج بیت کوین انجام می شود. گره ای که بلوک را برده است، نیز هزینه های تراکنشی را برای هر تراکنش قرار گرفته شده در بلوک دریافت می کند. به طور متوسط هر 10 دقیقه، یک گره می تواند بلوک جدید را تصاحب کند.

یک مورد می تواند این باشد که چند گره به طور همزمان یک بلوک معتبر ایجاد کنند که موجب شود، نسخه های متعددی از زنجیره بلوک "چند شاخه شدن" forks به طور موقت رخ دهد. چند شاخه ها، به محض آنکه یکی از آنها بلوک های بیشتری را دربرگیرد، تعیین می شوند. محاسبات برای یافتن و بررسی یک ترکیب رمزنگاری بلوک در طول استخراج بیت کوین به شبکه بیت کوین امکان می دهد تا در مورد تراکنش ها، به اجماع برسند. این امر به راحتی موضوع صرف چندبرابر را حل نموده و بنابراین مقداری از بیت کوین ها نمی توانند دوبار مصرف شوند. فرایند استخراج بیت کوین صدور ارز را غیرمتمرکز کرده و تراکنش ها به وضوح به طور عادی از طریق بانک های مرکزی و پاک سازی انجام می شوند. در اقتصاد، بیت کوین ها در برخی از زمینه ها مانند

پول در نظر گرفته می شوند، زیرا آن یک واحد حسابداری، ابزار پرداختی و نگهداری ارزش را ارائه می دهد. حتی این بحث مطرح می شود که بیت کوین به دلیل تلاش محاسباتی برای استخراج بیت کوین دارای ارزش ذاتی است.

هر بلوک تنها حاوی محدودیت ها نمی باشد، بلکه رمز بلوک قبلی پذیرفته شده در زنجیره بلوک را نیز دربردارد. بنابراین، بلوک ها در زنجیره بلوک به یکدیگر متصل شده اند؛ آنها زنجیره ای از بلوک ها را ساخته که به همین اساس آن را "زنجیره بلوک" می نامند. این امر، امنیت را به گونه ای فراهم می کند که یک گره با هدف تخریب نمی تواند به راحتی جایگزین شده یا تراکنشی که پیش از این پذیرفته شده است را تعدیل کرده یا تراکنش جدیدی را به بلوک از پیش پذیرفته شده اضافه کند، زیرا این امر نیازمند بازنویسی محاسبات برای یافتن رمزی معتبر برای بلوک تعدیل شده، می باشد. و از آنجایی که بلوک های جدید به طور مستمر به زنجیره بلوک اضافه می شود، هر بلوک به بلوک قبلی متصل می شود، همچنین رمزهای بلوک های تازه اضافه شده، مجدد محاسبه می شود.

پاداش اولیه بلوک، 50 BTC تنظیم شده است. پاداش در هر 210000 بلوک نصف می شود، که تقریباً برابر با 4 سال می باشد. این امر تا سال 2140 زمانی که استخراج پاداش به زیر  $10^{-8}$  BTC کاهش یابد، که کمترین واحد بیت کوین بوده که به عنوان ساتوشی شناخته می شود. پس از آن، هزینه تراکنش انگیزه لازم برای ادامه دادن استخراج بلوک های جدید را فراهم می کند. درگاه بیت کوین شامل یک الگوریتم برای تنظیم می باشد که به طور متوسط هر 10 دقیقه، از طریق تعدیل نمودن مشکل بودن یافتن رمز جدید، یک بلوک جدید استخراج می شود. این امر نیازمند ادامه دار بودن با بهبودها در عملکرد استخراج سخت افزار است که استخراج های بیت کوین را برای محاسبه بیشتر و بیشتر رمزها در هر ثانیه را فراهم می کند.

### 4-3- زنجیره های بلوک

زنجیره بلوک بر مبنای ارزشهایی مانند بیت کوین است، اما می تواند در بسیاری دیگر از کاربردهای مالی و تجاری نیز به کار رود. یک مثال برجسته قراردادهای هوشمند، برای مثال همانطور که در اتریوم پیشنهاد شده است، می باشد. یک قرارداد می تواند یک انتقال را زمانی که رویدادهای مشخصی رخ داده است اجرا کند، مانند پرداخت سپرده امنیتی، در حالی که اجرای صحیح توسط درگاه توافقی اجباری می باشد.

زنجیره های بلوک می توانند به صورت زنجیره های بلوک عمومی، زنجیره های بلوک اختصاصی یا زنجیره های بلوک کنسرسیوم طبقه بندی شوند. بیت کوین یک مثال از زنجیره بلوک عمومی است، در حالی که تمام سوابق برای عموم قابل مشاهده بوده و هر فردی می تواند نقشی در فرایند توافقی داشته باشد. یک زنجیره بلوک اختصاصی کاملاً توسط یک سازمان تحت کنترل است و یک گروه بسته از مشارکت کنندگان شناخته شده، که شبکه های متمرکز را به جای شبکه های غیرمتمرکز به کار می برند. یک زنجیره بلوک کنسرسیوم به

صورت بخشی غیرمتمرکز است، در حالی که تراکنش ها از طریق مجموعه گره های انتخابی اعتباردهی می شوند. زنجیره های بلوک اختصاصی و کنسرسیوم ممکن است به سایر کاربران امکان خواندن سوابق را در زنجیره بلوک بدهند. زنجیره های بلوک عمومی متکی بر درگاههای توافقی مانند اثبات کار است که اطمینان حاصل می کند تراکنش ها تا زمانی که هیچ استخراج کننده ای بیش از 50% توان رمز شبکه را کنترل نکند، نمی توانند دستکاری شوند. تراکنش ها در زنجیره بلوک اختصاصی و کنسرسیوم تا جایی که مشارکت کنندگان اصلی به توافق رسیده باشند قابل ویرایش هستند، بنابراین یک درگاه توافقی قوی مانند اثبات کار مورد نیاز نمی باشد. این امر امنیت را کاهش می دهد اما بهره وری و زمان انتظار را بهبود می دهد و بنابراین مصرف انرژی به ندرت یک موضوع نگران کننده می شود.

### 4-4- سخت افزار برای استخراج بیت کوین و نگرانی های موجود

استخراج بیت کوین، از آنجایی جذاب است که انگیزه های مالی قوی را پیشنهاد می کند. برای هر بلوک استخراج شده، استخراج کننده، بلوک پاداش را همچنین هزینه تراکنش از تراکنش های بلوک را دریافت می کند. همانطور که بیت کوین محبوبیت به دست می آورد، مسابقه ای بین استخراج کننده ها برقرار می شود، تنها استخراج کننده هایی باقی خواهند ماند که رقابتی ترین سخت افزار استخراج را به کار برده و کمترین هزینه الکتریسیته را صرف می کنند.

سخت افزار استخراج بیت کوین، در 4 نسل دیده شده است، آخرین و مناسب ترین سخت افزار در سال 2013 ارائه شده است که برای اجرای محاسبات رمزنگاری تا جایی که امکان دارد به صورت کارآمد، بهینه سازی شده اند.

بسیاری از استخراج کننده های بزرگ در نزدیکی منابع ارزان الکتریکی، مانند سدهای هیدروالکتریکی (چین، جمهوری گرجستان) و نیروگاههای گرمایشی زمین (ایسلند) قرار دارند، چرا که منبع ارزان الکتریکی یعنی پیشی گرفتن از رقبا.

مسابقه های بیت کوین، هزینه های سرمایه را افزایش میدهد که موانعی را برای تازه واردین جهت ورود و مواردی را برای استخراج کننده ها ایجاد می کند که نمی توانند از آن بیرون بیایند. این امر منجر به یک بازار انحصاری oligopolistic می شود. براساس داده از سایت bitcoinchain.com، پنج استخراج کننده بزرگ، که بیشتر مبتنی بر چین می باشند، بیش از 85% از بلوک ها در سال 2016 استخراج کرد. این امر خطرانی، مانند مداخلات دولت و تضعیف اصول بیت کوین به عنوان ارز دیجیتال نامتمرکز، ایجاد می کند.

### 4-5- هزینه های انرژی استخراج بیت کوین

در این مقاله نویسنده پایداری استخراج بیت کوین را با پایداری استخراج طلا و سیستم بانکداری مقایسه می کند. انرژی مصرف شده در هر سال برای استخراج طلا و چرخه بازیافت مقدار PJ 500 برای چاپ اسکناس و ضرب سکه در PJ 40، و برای سیستم بانکداری با در نظر گرفتن ATM ها و شعبه های



در زیر ساخت ها و در صنعت ، به کمک دولت ها و در سال های دور بطور رسمی آغاز خواهد شد.

### مراجع

- [1] مصطفوی، ناصر؛ فرشید ابراهیمی اوردکلو و ابراهیم عباسی، ۱۳۹۸، کاربرد فناوری بلاک چین در صنعت بانکداری، دومین کنفرانس بین المللی راهکارهای نوین پژوهشی در مدیریت، حسابداری و اقتصاد، تهران، شرکت همایش آروین البرز
- [2] Stefan Konrad Johansen "A Comprehensive Literature Review on the Blockchain Technology as an Technological Enabler for Innovation" Mannheim University, Department of Information Systems. 2017.
- [3] - Mu Qi-Guo. First Report on Survey of Blockchain Technology: Potential to Disrupt All Industries [J]. Report by Chuancai Securities Co., Ltd, 2016-01-12.
- [4] Vranken, Harald. / **Sustainability of bitcoin and blockchains**. In: Current Opinion in Environmental Sustainability. 2017 ; Vol. 28. pp. 1-9
- [5] Po-Wei Chen , Bo-Sian Jiang , Chia-Hui Wang "Blockchain-based Payment Collection Supervision System using Pervasive Bitcoin Digital Wallet" School of Software and Microelectronics, Peking University , Department of Computer Science and Information Engineering, Ming Chuan University, 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)

بانک (که خدمات بیشتری نسبت به تراکنش صرف دارند) در PJ 2340 تخمین زده است. در مقایسه با این اعداد، انرژی مصرف شده برای استخراج بیت کوین در طیف 3-16 PJ نسبتاً کم است. با این حال، سهم بیت کوین در سیستم مالی فعلی نیز نسبتاً کم می باشد و زمانی که مقیاس بیت کوین بالا می رود، تلاش برای استخراج بیت کوین صورت می گیرد.[5]

### 5- نتیجه گیری

نگارش این بخش اندکی سخت تر به نظر میرسد ، چرا که زوایای مختلفی برای نگرستن به موضوعات مطرح شده نمایان شده اند ، پس نتیجه گیری تنها برداشت شخصی اینجانب میباشد.

سیستم بانکداری میتواند به کمک زنجیره های بلوک خود را تقویت کند ، اما به صراحت می توان دید که بخشی از فعالیت های بنا شده بر پیکر بلاک چین ، نظام سرمایه داری را نشانه رفته که یکی از اصلی ترین پشتوانه های نظام سرمایه داری ای که امروز شناخته شده است ، سیستم بانکداری است.

گسترش هر چه بیشتر ارز های دیجیتالی ، در راس آن ها بیت کوین و یا اتریوم ، به معنای کاهش قدرت سیستم های مالی و بانکداری ، اوضاع برای دولت ها زمانی وخیم تر خواهد شد که متوجه شوند اصلی ترین و موفق ترین محصول بر پایه بلاک چین ، ارز های دیجیتالی میباشد.

حامیان ارز های دیجیتالی معتقدند که این ارز ها ، تمرکز اطلاعات و اعتبار را به مردم باز خواهد گرداند.

در مورد مصرف انرژی این سیستم هم ، همانطور که بیان شد ، در مقایسه با سیستم های مالی ، حداقل تا امروز به مراتب انرژی کمتری مصرف میکند. در ساختار بلاکچین، تمام اطلاعات پس از تاییدیه در بلاکچین ثبت شده و نمی توانند حذف شوند. بر اساس خصوصیات بلاکچین، هنگام اتصال بلوک جدید به بلوک اصلی مقدار هش بلوک قدیمی در بلوک جدید ذخیره می شود. تا زمانی که یک مقدار در بلوک حتی کمی اصلاح شود، ارزش هش کاملاً متفاوت خواهد شد، به این معنی که، اثر بهمن رخ خواهد داد. به دلیل این که ساختار که تمام اطلاعات هرگز تغییر نخواهد کرد، اگر نتیجه تایید تغییر کند، بلوک توسط سیستم پذیرفته نخواهد شد. بنابراین، تمام اسناد تراکنش هایی که در بلاک چین ذخیره شده اند ، نمیتوانند اصلاح و حذف گردند.

گفتنیست که قرار داد های هوشمند بر پایه اتریوم مستعد توجه ویژه می باشد و پیش بینی میشود در آینده نزدیک شاهد رشد اعتبار این تکنولوژی و افزایش فرصت های استفاده باشیم.

اما در مورد استفاده از بلاک چین در زیرساخت ها و با استارتاپ ها باید گفت که این امر بطور فراگیر به ای زودی ها محقق نخواهد شد، این مهم نیازمند حمایت و مداخله دولت هاست.

البته در سال های آینده کم و بیش استفاده از این فناوری را در فلان بخش از فلان دولت خواهیم شنید ، یا فلان استارتاپ خدماتی با تکیه بر بلاک چین آغاز به کار کرد اما بلاک چین