مدیریت سبز، دوره۱، شماره ۱، اسفند ماه ۱۴۰۰

بررسی مروری اثرگذاری معاملات غیرمتمرکز سبز در تکنولوژی بلاک چین محور

علی غفاری*[۱]، غلامرضا طالقانی[۲]

تاریخ دریافت: تاریخ پذیرش:

چکیده

دنیای امروز، دنیای دیجیتال است. علاوه بر رقابت در ورود به دنیای دیجیتال و استفاده از تکنولوژی های مدرن که از دغدغه های صنایع مختلف می باشد، سرمایه گذاری دیجیتالی و عملیات دیجیتالی از اهم دغدغه های سهامداران یانک و مشتریان حوزه رمزارز در ورود به حوزه رمزارزها می باشد. در این عرصه، می توان از ۸ تکنولوژی به عنوان تکنولوژی های تحول آفرین در تحول دیجیتال که موجبات تغییرات و کسب مزیت رقابتی را فراهم نموده اند نام برد: رسانه های اجتماعی، واقعیت مجازی و افزوده، تحلیل داده و بیگ دیتا، هوش مصنوعی، رایانش ابری، اینترنت اشیاء، رایانش موبایلی و بلاک چین. تکنولوژی بیت کوین به عنوان یک راه حل برای ایجاد و حفظ سوابق دیجیتال قابل اعتماد، با درنظر گیری محدودیت ها، خطرات، معماری امنیت مناسب، کنترل مدیریت زیرساخت، و فرصت ها می باشد ولی فعالیتهای غیر قانونی را نیز باید مدنظر داشت و در جهت آسیب شناسی و کشف تخلفات دیجیتالی در این حوزه برآمد.معماری نرم افزارهای کاربردی جهت تشخیص معاملات غیر قانونی و مشکوک میتواند در این تغییر و رویکرد تحول دیجیتال در حوزه مدیریت سبز، راه گشایی در امنیت عملیات مالی و رضایت سهامداران و مشتریان این حوزه باشد؛ هدف از این مقاله بررسی تکنولوژی سبز مدرن جهت تشخیص هویت کاربران بیت کوین بوده که با استفاده از تکنیک های یادگیری ماشین به یادگیری نحوه رفتار خاصی از شبکه بیت کوین با تکنولوژی سبز به شناسایی معاملات غیرقانونی می پردازد. در این تحقیق، شناسایی هویت یک کاربر، پروتکل و نحوه معاملات آن در بیت کوین و نحوه رفتار از نقطه اتصال تا آخرین بلوک زنجیره ای بر روی شبکه بررسی می گردد.

واژگان کلیدی: بلاک چین، تحول دیجیتال، مدیریت سبز.

۱دانش آموخته کارشناسی ارشد، مدیریت MBA گرایش استراتژی، دانشگاه تهران، تهران، ایران. .(نویسنده مسئول)
alighafary@ut.ac.ir
۲استاد گروه مدیریت دولتی، دانشکده مدیریت دانشگاه تهران، تهران، ایران

مقدمه

در دنیال دیجیتال؛ فناوری بلاک چین کاربردهای زیادی دارد. یکی از کاربردهای آن ایجاد زیرساختهای ارزهای رمز پایه است و فناوری بلاک چین یکی از زیرساختهای اساسی بیت کوین است. به بیان دیگر فناوری بلاک چین در دامنه بسیار وسیعی از برنامه های کاربردی مالی و غیرمالی دیگر نیز به عنوان فناوری زیرساخت به خوبی به کار گرفته شده است و اختراعات متعددی در حوزه های اعتبارسنجی تراکنشهای مراقبتهای بهداشتی، مسائل بانکی، انتخابات و رایانشی به ثبت رسیده است و به همین دلیل دولتها و مراکز قانونگذاری مطالعه پیرامون بهره گیری از آن را در دستورکار خود قرار داده اند (لیندمن[1] و همکاران، ۲۰۱۷). فناوری بلاک چین اولین بار فقط برای تبادل ارزهای دیجیتالی به وجود آمده بود ولی ویژگیهایی مانند متن باز بودن رایگان بودن امکان ثبت اسناد به صورت عمومی و غیرمتمرکز بودن آن باعث شد تا برای ارائه خدمات مختلفی مورد استفاده قرار گیرد.

امروزه پیشرفت سریع فناوری و تغییرات محیطی وسیع، شتاب فزاینده ای به اقتصاد بخشیده و رقابت روز افزون مؤسسات، دستیابی به سود را محدود و احتمال وقوع بحران مالی و نهایتاً ورشکستگی را افزایش داده است (تایلور[2]، ۲۰۱۶). بدین ترتیب تصمیم گیری مالی نسبت به گذشته راهبردی تر شده است. یکی از راه هایی که می توان با استفاده از آن به بهره گیری مناسب از فرصت های سرمایه گذاری و تخصیص بهتر منابع کمک کرد، مدیریت ریسک در معاملات مالی مشکوک است (کوهن[3] و همکاران، ۲۰۱۷).

ادبیات موضوع

تاکنون تحقیقی درباره مطالعه تحلیلی معاملات غیرمتمرکز در تکنولوژی بلاک چین محور مبتنی بر شبکه حوزه رمزارزی به صورت مشخص انجام نشده است. اما تحقیق های زیر تا حدودی با این پژوهش مرتبط می باشند که با بررسی این تحقیقات می توان به نوعی فضای بیشتری را پیش روی این مفهوم شناسی ایجاد کرد

- ✓ ترنر و همکاران (۲۰۱۸) در تحقیقی به معاملات بیت کوین: شناسایی دیجیتال معاملات غیرقانونی (مشکوک) در بلاک چین پرداختند، هدف از این مقاله تعیین این است که آیا معاملات بیت کوین می تواند با تجزیه و تحلیل بلوک های بیت کوین حذف شود. علاوه بر این، تجزیه و تحلیل گراف و استفاده از تکنولوژی رسانه های اجتماعی مدرن مورد بررسی قرار گرفت تا مشخص شود چگونه می توانند هویت کاربران بیت کوین را تشخیص دهند. بررسی تکنیک های یادگیری ماشین و اکتشافات به منظور یادگیری نحوه رفتار خاصی از شبکه بیت کوین با تکنولوژی رسانه های اجتماعی و سایر داده ها برای شناسایی معاملات مشکوک افزایش یافت.

1. Lindman
2. Taylor
3. Cohen

- ✓ (یو[1]، ۲۰۱۷) در پژوهشی به «بررسی بلاک چین براساس تجزیه و تحلیل مالی و کاربردهای آن» پرداخت. در کره و در خارج از کشور، این مقاله به بررسی استفاده از بلاک چین در بخش مالی می پردازد. این مطالعه با هدف بررسی چگونگی استفاده از بلاک چین برای بخش مالی و نحوه پاسخ به شرایط کره ای انجام شده است. یافته های تحقیق حاکی از آن است که موارد داخلی و خارجی، می توان دید که مناطقی که بلوک های بیشتر فعالانه در بخش مالی به کار گرفته می شوند، در حال گسترش پرداخت، انتقال، اوراق بهادار و قراردادهای هوشمند هستند. همچنین، در کره، بسیاری از روش های تأیید هویت براساس تجهیزاتی که توسط مصرف کنندگان در اختیار دارند، به کار می روند.
- ✓ (لی[2] و همکاران، ۲۰۱۷) در پژوهشی به ارائه «چارچوبی جهت تبادل دانش و خدمات متقابل بر اساس محاسبات بلاک چین» پرداخت. هدف از این مقاله پیشنهاد یک چارچوب متقابل شرکتها برای دستیابی به سطح بالایی از تقسیم دانش و خدمات در اکوسیستم های تولید است. یافته های تحقیق حاکی از آن است که اکوسیستم تولید در حال تغییر از سیستم های یکپارچه و متمرکز به سیستم های مشترک و توزیع شده است. چارچوب پیشنهادی شامل توسعه اخیر در محاسبات بلاک چین است که می تواند الزامات ایمن و توزیع شده برای به اشتراک گذاشتن دانش و خدمات در اکوسیستم های تولید را برآورده سازد.
- ✓ در مطالعه ای که (هارلند[3] و همکاران، ۲۰۱۴) در خصوص به‌کارگیری قراردادهای مبتنی بر بلاک چین بر پردازش تراکنش و تصفیه‌حساب بین بیمه‌گران و سرمایه‌گذاران انجام داده اند به نتیجه ای رسیدن که با استفاده از بلاک چین می‌توانند باعث ایجاد افزایش توان تجاری در اوراق قرضه حوادث فاجعه‌آمیز و ایجاد فرصت‌های بیشتر برای کاربرد این فناوری در معاملات بیمه ای شود زیرا اوراق قرضه حوادث فاجعه‌آمیز، ابزارهایی مالی هستند که معمولابین بیمه گذار و سرمایگذاران در خصوص مجموعه‌یی از ریسک‌های خاص مانند ریسک‌های حوادث طبیعی ازجمله توفان و گردباد می باشد.
- ✓ (یو[4] و همکاران، ۲۰۱۶) در تحقیقی که در زمینه داده های بهداشت و در زمینه خدمات بهداشتی انجام شده است به بررسی و تبیین هوش خدمات بهداشتی با شناخت از ریسک های بلاک چین و کنترل آن پرداخته است، در این تحقیق که به شیوه ای تحلیلی انجام شده است، بر لزوم شناخت و کنترل ریسک های بلاک چین تاکید شده است.
- ✓ واچ (۲۰۱۵) در تحقیقی به بررسی ریسک های بلاک چین در زمینه ارز مجازی بیت کوین پرداخته است، در این تحقیق که به شیوه تحلیلی و توصیفی و مروری به انجام رسیده است، ریسک

1 Yoo
2 Li
3 Harland
4 Yue

زیرساختی به عنوان یکی از ریسک های موثری که در زمینه بازار اثرگذار خواهد بود، مطرح شده است.

روش تحقیق

تحقیق حاضر دارای رویکرد مروری داشته است که با مطالعه پیشینه تحقیقات انجام شده و بررسی تحلیلی آنها به انجام رسیده است

یافته ها و نتایج

مفهوم سازی بلاک چین

فناوری بلاک چین به زبان ساده، زنجیرهای از بلوکهای داده است. در درون این بلوکها، دادههای مربوط به تراکنشها نگهداری میشود. در زمان پردازش تراکنشها، این دادهها درون یک بلوک قرار می گیرند و پس از اتمام تراکنش و در صورت تأیید سایر اعضای شبکه، این بلوک به انتهای زنجیره افزوده میشود. در واقع بلوکیچین، پایگاه دادهای است که در آن بخشهای مختلف داده در بلوکهایی ذخیره شدهاند و این بلوکها به ترتیب رخداد به زنجیره افزوده میشوند. مکانیزم اجرایی بلوکیچین به این صورت است که کلیه تراکنشها روی یک دفترکلثبت می شوند و تمامی کاربران پس از اتصال به شبکه، یک کپی از این دفترکل را روی دستگاه خود ذخیره میکنند. به این جهت گفته میشود که بلوکیچین مبتنی بر یک دفترکل توزیع شده میان تمام کاربران است .هر یک از کاربران پس از انجام تراکنش روی دفترکل خود، آن را روی شبکه میفرستند. سایر کاربران این تغییرات را مشاهده و در صورت صحت، تأیید میکنند و به این ترتیب عملیات فوق بر اساس مکانیزم اجماع عمومی سایر اعضای شبکه، نهایی شده و اجرا می شود. به عبارت دیگر، فرایند پردازش تراکنشها به صورت غیرمتمرکز و توسط تمام اعضای بلاکچین انجام می شود و پس از آن که صحت یک تراکنش توسط اعضا تأیید شد، بلوک مربوط به آن به انتهای زنجیره بلوکها افزوده می شود. از این زمان به بعد، یعنی پس از افزوده شدن این بلوک به کل زنجیره، دیگر امکان حذف یا تغییر آن وجود ندارد و تنها میتوان این اطلاعات را با تأیید سایر اعضای شبکه بهروزرسانی کرد. بنابراین از آنجایی که اعمال این تغییرات در دفترکل، به تأیید سایر اعضای شبکه نیاز دارد، هیچ کاربری نمی تواند بدون تأیید سایر اعضا اقدام به تغییر دفترکل کند و به این ترتیب بدون نیاز به هیچ مرجع ناظر متمرکزی، صحت اطلاعات دفترکل تضمین می شود (لی و همکاران[1]، ۲۰۱۷).

مزایای بلاک چین

مزایای استفاده از فناوری بلاک چین بیش از مشکلات هماهنگسازی و چالش های فناوری آن است. یکی از موارد کلیدی نوظهور در استفاده از فناوری بلاک چین «قراردادهای هوشمند» است. قراردادهای هوشمند در اصل برنامه های رایانه ای هستند که می توانند به شکل خودکار شرایط قرارداد را اجرا کنند. وقتی طرفهای

1 Lee et al

معامله با یک وضعیت از قبل تعیین شده در قرارداد هوشمند مواجه می شوند، می توانند به طور خودکار و براساس قرارداد مورد توافق پرداختها را به صاورت شفاف انجام دهند (بیک[1] و همکاران، ۲۰۱۷).

مؤسسات مالی و حوزه رمزارزها دیگر فناوری بلاک چین را به عنوان تهدیدی برای مدلهای کسب وکار سنتی خود به حساب نمی آورند. در واقع بزرگترین حوزه رمزارزهای جهان با تحقیق و مطالعه درخصوص برنامه های کاربردی نوآورانه مبتنی بر بلاک چین به دنبال فرصتهای جدید هستند. بلاک چین می تواند در سه بعد زمینه کاهش هزینه را فراهم سازد:

کارآیی بیشتر فرآیندها: بلاک چین میتواند دقت را در فرآیندهای پیچیده افزایش و نیاز به نظارت و حکمرانی را کاهش دهد. قراردادهای هوشمند به عنوان یکی از بخشهای زنجیرهی بلوکی می تواند با از بین بردن نیاز به تأیید شخص ثالث در قراردادهای متعارف فعلی و همچنین از بین بردن نیاز به قراردادهای کاغذی، در مجموع، هزینه ها و مشکلات قراردادهای این حوزه را کاهش دهد.

انطباق: دادهها و رکوردهای غیرقابل تغییر تراکنشها می توانند در ردگیری محصولات و داراییها بسیار کمک کننده باشد. یک پایگاه دادهی توزیع شده از تراکنشها و اسناد می تواند مشخصات و ویژگیهای محصولات و داراییها را ثبت و ضبط کند و تنها به افراد خاص و مشخص شده ای اجازه دسترسی به اطلاعات را بدهد. مثال یک شرکت می تواند مواد معدنی مورد نیاز خودر را از یک محل مطمئن تهیه کند و خود را از ریسک کانیها و مواد اولیه نامناسب نجات دهد. از این منظر دید داشتن و مشخص بودن ارکان قراردادها و تراکنشها که بر اساس داده های قابل اعتماد شکل گرفتهاند، می تواند به تصمیم گیری هرچه بهتر شرکتها و کسب و کارهای تجاری کمک کند.

دادههای مربوط به انتقال از سنسورهای اینترنت اشیاء: بلاک چین می تواند در ردگیری داده های یکتا از تاریخچه یک تجهیز یا وسیله خاص نیز کمک کننده باشد. داده های ثبت شده در پایگاه دادهی توزیع شده که بر اساس سنسورهای چندگانه فراهم آمده به نوعی می تواند تاریخچه کامل آن تجهیز و ابزار خاص را نشان دهد. ایمنی اطلاعات در تجهیزات و وسایل می تواند بر اساس ویژگیهای خاص بلاک چین حفاظت شود (یعقوبی و همکاران[2]، ۱۳۹۳).

بلاک چین و کاهش هزینه های مالی

بلاک چین می تواند در سه بع زمینه کاهش هزینه را فراهم سازد:

کارآیی بیشتر فرآیندها: زنجیرهی بلوکی می تواند دقت را در فرآیندهای پیچیده افزایش و نیاز به نظارت و حکمرانی را کاهش دهد. قراردادهای هوشمند به عنوان یکی از بخشهای زنجیرهی بلوکی میتواند با از بین بردن نیاز به تأیید شخص ثالث در قراردادهای متعارف فعلی و همچنین از بین بردن نیاز به قراردادهای کاغذی، در مجموع، هزینه ها و مشکالت قراردادهای این حوزه را کاهش دهد.

1. Beck
2 Yaghoubi et al

انطباق: دادهها و رکوردهای غیرقابل تغییر تراکنشها میتوانند در ردگیری محصولات و داراییها بسیار کمک کننده باشد. یک پایگاه داده توزیع شده از تراکنشها و اسناد می تواند مشخصات و ویژگیهای محصولات و داراییها را ثبت و ضبط کند و تنها به افراد خاص و مشخص شده ای اجازه دسترسی به اطلاعات را بدهد. مثال یک شرکت می تواند مواد معدنی مورد نیاز خودر را از یک محل مطمئن تهیه کند و خود را از ریسک کانیها و مواد اولیه نامناسب نجات دهد. از این منظر دید داشتن و مشخص بودن ارکان قراردادها و تراکنشها که بر اساس دادههای قابل اعتماد شکل گرفته اند، میتواند به تصمیم گیری هرچه بهتر شرکتها و کسب و کارهای تجاری کمک کند.

دادهه ای مربوط به انتقال از سنسورهای اینترنت اشیاء: زنجیرهی بلوکی میتواند در ردگیری دادههای یکتا از تاریخچه یک تجهیز یا وسیله خاص نیز کمک کننده باشد. داده های ثبت شده در پایگاه داده توزیع شده که بر اساس سنسورهای چندگانه فراهم آمده به نوعی می تواند تاریخچه کامل آن تجهیز و ابزار خاص را نشان دهد. ایمنی اطلاعات در تجهیزات و وسایل می تواند بر اساس ویژگیهای خاص بلاک چین حفاظت شود (دوری[1] و همکاران،۲۰۱۷).

ریسکهای استفاده از فناوری در معاملات مالی مشکوک

عبارت است از عدم وجود سیستم های خود کار ، شبکه یا منابع اصلی دیگر فناوری اطلاعات که روی فرآیندهای کسب و کار تاثیر منفی می گذارد.

د) تجزیه و تحلیل گران مدرن منابع ریسک را که باعث تغییر و پراکندگی دربازده می شود به دو دسته تقسیم می کنند . این دو نوع ریسک را که به آنها ریسک سیستماتیک و غیرسیستماتیک می گویند به صورت زیر می توان نشان داد:

ریسک سیستماتیک + ریسک غیرسیستماتیک =ریسک کل

۱. ریسک غیرسیستماتیک

به آن قسمت از تغییرپذیری در بازده کلی محصولات مالی که به تغییرپذیری کلی بازار بستگی ندارد، ریسک غیرسیستماتیک می گویند . این نوع ریسک منحصر به محصول خاصی نیست وبه عواملی همچون ریسک تجاری، مالی و ریسک نقدینگی بستگی دارد . این نوع ریسک را میتوان با ایجاد پرتفلیو کاهش داد.

۲. ریسک سیستماتیک

آن قسمت از تغییرپذیری در بازده کلی محصولات مالی را که مستقیما به تغییرات بازار یا اقتصاد بستگی دارد ریسک سیستماتیک گویند . معمولا تمامی اوراق بهادار تا حدودی از ریسک سیستماتیک برخوردارند و دربرگیرنده عواملی همچون ریسک تورم ، بازار و نرخ بهره است .این نوع ریسک غیرقابل کاهش است (کرافت[2]، ۲۰۱۶).

[1] Dorri
[2]. Kraft

ریسکهای استفاده از بلاک چین در معاملات

فناوری بلاک چین محدودیت‌هایی دارد، اما این محدودیت‌ها به برخی از موردهای استفاده نامربوط هستند. برقرار کردن شخصی (محرمانه) بودن و قابلیت اعتماد روی یک بلاک چین عمومی، سخت است، چون هر عضو عمومی (اجتماع) می‌تواند رونوشت (کپی) کاملی از کل سابقه تراکنش‌ها را به دست آورد و بدون محدودیت از آن استفاده کند. حتی اگر طرف‌ها سعی کنند از اسامی مستعار استفاده کنند، مندرجات تراکنش برای عموم قابل مشاهده هستند و استفاده مجدد یا اتصال آدرس‌ها از طریق انتقال وجه رایج دیجیتال می‌تواند فرصت‌هایی برای حملات پیوندی (اتصال) برای بازشناسی شرکت کنندگان فراهم آورد (لوپز-پینتادو[1] و همکاران، ۲۰۱۷).

۱- عدم ذخیره سازی داده های بزرگ (Big Data)

محدویت زنجیره‌های بلوکی این است که آنها برای ذخیره داده‌های بزرگ یعنی حجم‌های زیاد داده‌ها یا داده-های سرعت بالا مناسب نیستند. این یک محدودیت ذاتی (لاینفک) زنجیره‌های بلوکی است. به خاطر تکرار (نسخه‌برداری) عظیم از تعداد زیاد نودهای پردازشی دارنده کپی کاملی از دفتر کل توزیع شده است.

۲- هزینه بالای استفاده از بلاک چین

زنجیره‌های بلوکی به طور عظیمی با نودهای پردازشی تکراری (اضافی) توزیع می‌شوند و یکپارچگی داده‌ها را در مورد تاریخچه (سابقه) کامل تراکنش خود ارائه می‌دهند. این به طور اجتناب‌ناپذیری بر هزینه استفاده از بلاک چین تأثیر می‌گذارد و به این معنیست که بلاک چین مدل هزینه متفاوتی نسبت به زیرساخت مرسوم (ابر یا داخلی (درون زمانی) دارد.

بلاک چین دو مرتبه گران‌تر از ابر است، اما زمان نگهداری ذخیره بلاک چین به شکل دوره‌ای به صورت یک مبلغ تراکنش برای قطعات کوچک تراکنش و داده‌های رویداد پرداخت می‌شود. در حالی که ذخیره در ابر نیازمند مبالغ مداوم ماهانه است. برای انتقال مالی، وجه رایج دیجیتال مبتنی بر بلاک چین می‌تواند مبالغ بسیار پایین‌تری نسبت به انتقالات مرسوم پول داشته باشد. نرخی که می‌توان در آن بلوک‌ها را ایجاد کرد، اغلب با استفاده از مکانیسم دلیل (نشانه کار که به موجب آن یک نود پردازشی فقط می‌تواند با نشان دادن این که کار سختی انجام شده است یک بلوک جدید اضافه کند، محدود می‌شود.

۳- تأخیر در خواندن

زمانی که داده‌ها قبلاً روی بلاک چین نوشته شده‌اند، تأخیر خواندن زمان پاسخ برای دسترسی داده‌های سابقه‌ای (تاریخچه‌ای) از یک مراجعه کننده بلاک چین است. تأخیر خواندن روی بلاک چین می‌تواند خیلی سریع‌تر از فناوری‌های مرسوم باشد، زیرا مراجعین می‌توانند رونوشت (کپی) محلی کاملی از پایگاه داده نگه دارند و به این ترتیب تأخیرهای شبکه وجود ندارند.

---

[1]. López-Pintado

٤- تأخیر در نوشتن

درخواست برای نوشتن داده‌ها در بلاک چین با ارسال یک تراکنش به شبکه انجام می‌شود. تأخیر نوشتن یک احتمال است و منابع بی‌اطمینانی (عدم قطعیت) متعددی وجود دارند. همه زنجیره‌های بلوکی تأخیرهای شبکه کوچکی خواهند داشت. همچنین برای زنجیره‌های بلوکی با هم‌رأیی ناکاموتو، شخص نمی‌تواند خیلی مطمئن باشد که تازه‌ترین بلوک گنجانده شده بعداً باز هم در آن هست. برای افزایش اطمینان‌مان به این که داده‌ها با موفقیت به بلاک چین سپرده شده‌اند، می‌توانیم منتظر یک تعداد از بلوک‌های تأیی بمانیم. منتظر ماندن برای بلوک‌های تأیید بیشتر تأخیر نوشتن را افزایش خواهد داد. ما «زمان شمول (گنجاندن» را زمانی می‌خوانیم که در آن می‌بینیم که یک تراکنش در یک بلوک گنجانده شده و «زمان سپردن» را زمانی می‌خوانیم که در آن تعداد پیش تعریف شده‌ای از بلوک‌های تأیید را دیده‌ایم.

٥- عدم قابلیت اعتماد (رازداری)

قابلیت اعتماد، یعنی این که افشای غیرمجاز (بدون اجازه) اطلاعات، اتفاق نمی‌افتد. برقراری این معمولاً در سیستم‌های مبتنی بر بلاک چین سخت‌تر است، چون پیش فرض اینست که اطلاعات برای هر کسی در شبکه قابل مشاهده است. می‌توان اطلاعات را رمزدار کرد: به صورت نامتقارن با کلید عمومی یک طرف خاص، به گونه‌ای که فقط این طرف بتواند آن را رمزگشایی کند یا به صورت متقارن با یک کلید سرّی به اشتراک گذاشته شده، به گونه‌ای که یک گروه از طرف‌هایی با دسترسی به کلید سرّی بتوانند آن را رمزگشایی کنند. مورد آخر نیازمند یک وسیله تضمین تبادل کلید سرّی خارج از زنجیره است.

اما به محض این که لازم باشد، اطلاعات توسط روش‌های قرارداد هوشمند پردازش شوند، لازم است این اطلاعات رمزگشایی شوند. این به این خاطر است که کد قرارداد هوشمند روی همه نودهای شبکه اجرا می‌شود و به این ترتیب لازم است هر یک از آنها قادر به پردازش داده‌های ورودی باشند. این برای رسیدن به اجماع کلی در مورد نتایج اجرای قراردادهای هوشمند لازم است. جاسازی کلیدها در یک قرارداد هوشمند، کلید را برای همه شرکت‌کنندگان آشکار خواهد ساخت.

٦- عدم قابلیت دسترسی

قابلیت دسترسی، آمادگی برای خدمات صحیح است، در حالی که قابلیت اطمینان، مداوم بودن خدمات صحیح است. به طور خاص‌تر در زمینه سیستم‌های مبتنی بر بلاک چین، قابلیت دسترسی به توانایی احضار کارکردهای سیستم مربوط می‌شود، در حالی که قابلیت اطمینان به دریافت نتایج درست به طور نامتناقض از آن احضار (درخواست)ها اطلاق می‌شود.

عملکرد زنجیره‌های بلوکی عمومی می‌تواند شامل صدها یا هزاران نود (گره) پردازشی مستقل باشد. هر نود نمونه تکرار شده کاملی از تاریخچه (سابقه) تراکنش بلاک چین را نگه می‌دارد و می‌تواند برای کاربران به عنوان یک میانجی (واسطه) تراکنش به شبکه بلاک چین عمل کند. به خاطر این تکرار (نسخه‌برداری، حشو)

عظیم ممکن است از روی سادگی انتظار داشته باشیم که سیستم بلاک چین قابلیت دسترسی بی‌نهایت بالایی داشته باشد. برای زنجیره‌های بلوکی شرایط (مقتضیاتی) وجود دارند که در آن تمایز بین قابلیت اطمینان و قابلیت دسترسی می‌تواند محو (تیره و تار) باشد، چون زمان مشخص شده سراسری (جهانی) وجود ندارد که باید تراکنش تا آن زمان تکمیل شود.

۷-عدم قابلیت تعمیر (نگهداشت‌پذیری)

قابلیت تعمیر (نگهداشت‌پذیری) به پاسخگویی سیستم به تحمل اصلاحات و تعمیرات برمی‌گردد. در سیستم-های مبتنی بر بلاک چین که از قراردادهای هوشمند استفاده می‌کنند، استقرار آن برای قراردادهای هوشمند سخت‌تر از سیستم‌های توزیع شده منظم است. این به این خاطر است که قراردادهای هوشمند، کدی را در بردارند که تعاملات بین طرف‌های بدون اعتماد متقابل را تنظیم می‌کند، اعتماد از این واقعیت مشتق می‌شود که نمی‌توان کد را به آسانی تغییر داد (ژینگ[1] و همکاران، ۲۰۱۶).

اهمیت بلاک چین و ریسک معاملات مشکوک

امروزه معاملات مالی مشکوک در محیط پیچیده و متغیری فعالیت می کنند .در این شرایط معاملات مالی مشکوک برای دستیابی به اهداف خود و کاهش اثر نامطلوب نوسانات، برای مدیریت ریسک هایی که با آن مواجهند، اهمیت زیادی قائل هستند. ماهیت کسب و کار خدمات مالی، پذیرش ریسک است و بدون پذیرش ریسک قادر به سودآوری و رشد نیستند. با توجه به ماهیت کسب و کار خدمات مالی، مدیریت ریسک برای این نوع موسسات از اهمیت ویژه ای برخوردار هستند. در واقع، این موسسات باید ریسک هایی را که می پذیرند، مدیریت کنند.شرکت های ارائه دهنده خدمات مالی مانند حوزه رمزارز ها، با ریسک های بزرگی همچون ریسک بازار (مانند ریسک نرخ ارز، نرخ بهره و قیمت سهام) ریسک نقدینگی، ریسک اعتباری و ریسک عملیاتی (مانند ریسک IT ،نیروی انسانی و قوانین) مواجه هستند (رایمرز و اسچیپرز[2]، ۲۰۱۶).

یکی از روشهایی که در مدیریت ریسک مورد استفاده قرار میگیرد مدیریت بلاک چین است. در دنیای رقابتی کنونی مدیریت بلاک چین یکی از مسائل اساسی پیش روی بنگاههای اقتصادی است که تمامی فعالیتهای سازمان هاو معاملات مالی مشکوک را به منظور تولید محصولات و ارائه خدمات مورد نیاز مشتریان تحت تأثیر قرار میدهد. از این رو توجه به فرصتها و تهدیدهای موجود در عرصه تجارت جهانی و ارزیابی توان سازمان در رویارویی با ریسکهای این عرصه از اهمیت انکارناپذیری برخوردار است . مدیریت ریسک در زنجیرهٔ بلوکی وظیفهٔ شناسایی، تحلیل، ارائه راهکارهای مناسب جهت پاسخگویی، کنترل و پایش ریسکها در چرخه های اقتصادی و تولیدی را بر عهده دارد.در دهه اخیر ، مدیریت بلاک چین از حالت نامحسوس و فرعی خارج شده و به یک عنصر استراتژیک تبدیل گشته است که می تواند تأثیر مثبت و محسوس روی فعالیت

1. Zheng
2. Reimers & Scheepers

های سازمان ها بگذارد. تحولات ناشی از فناوری در شرایط بازار، تغییر شکل شیوه های کسب و کار، توقعات و انتظارات جدید شرکای موجود در بلاک چین و سرانجام تقاضا برای ارزش ایجادشده بیشتر از طرف مصرف کننده نهایی، ازجمله عوامل موجود در تغییر وضعیت مدیریت بلاک چین است (لی[1] و همکاران،۲۰۱۷). شناسایی و مدیریت ریسک های درون معاملات مالی مشکوک و استفاده از رویکردهای هماهنگ کننده ای برای کاهش آسیب پذیری کل بلاک چین به عنوان مدیریت ریسک بلاک چین، تعریف می شود.

شناسایی هویت یک کاربر، پروتکل و نحوه معاملات آن در بیت کوین و نحوه رفتار از نقطه اتصال تا آخرین بلوک زنجیره ای بر روی شبکه

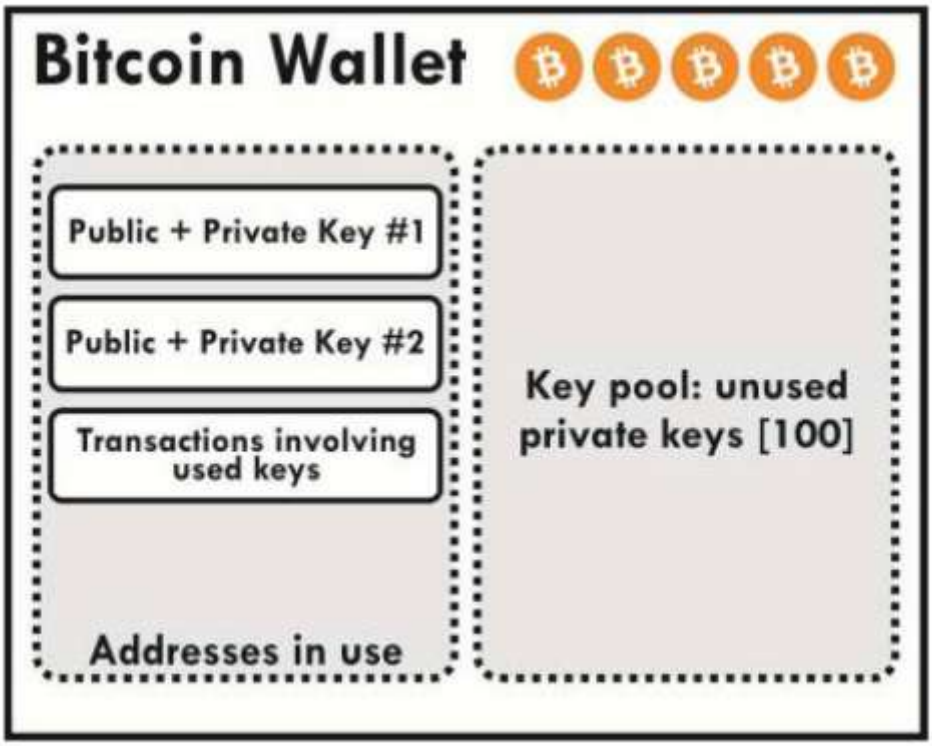
تکنولوژی بلاک چین به عنوان یک راه حل برای ایجاد و حفظ سوابق دیجیتال قابل اعتماد، با درنظر گیری محدودیت ها، خطرات، معماری امنیت مناسب، کنترل مدیریت زیرساخت، و فرصت ها می باشد ولی فعالیتهای غیر قانونی را نیز باید مدنظر داشت و در جهت آسیب شناسی و کشف تخلفات دیجیتالی در این حوزه برآمد.معماری نرم افزارهای کاربردی جهت تشخیص معاملات غیر قانونی و مشکوک میتواند در این تغییر و رویکرد تحول دیجیتال در حوزه مدیریت سبز ، راه گشایی در امنیت عملیات مالی و رضایت سهامداران و مشتریان این حوزه باشد؛ هدف از این مقاله بررسی تکنولوژی رسانه های اجتماعی مدرن جهت تشخیص هویت کاربران بیت کوین بوده که با استفاده از تکنیک های یادگیری ماشین به یادگیری نحوه رفتار خاصی از شبکه بیت کوین با تکنولوژی رسانه های اجتماعی به شناسایی معاملات غیرقانونی می پردازد. در این بخش، شناسایی هویت یک کاربر، پروتکل و نحوه معاملات آن در بیت کوین و نحوه رفتار از نقطه اتصال تا آخرین بلوک زنجیره ای بر روی شبکه بررسی می گردد.

کیف پول بیت کوین

عملکرد کیف پول در حقیقت همان، اطلاعات خصوصی مشتری است. در ساده ترین شکل، ویژگی های موجود در کیف پول شامل بخش خصوصی و عمومی است؛ حساب هایی که در بیت کوین و معاملات مربوط به آن هستند، شامل بخش های عمومی و خصوصی می شوند که اطلاعات کاربران را تحت الشعاع قرار می دهند، کیف پول شروع فرآیند بیت کوین می باشد، این کیف دارای یک بخش استخر کلید نیز می باشد که این بخش بخش خصوصی این کیف بصورت اخص می باشد، که در شکل زیر نمایش داده شده است:

[1] Lei

شکل ۱: کیف پول بیت کوین (برگرفته از : بررا[1]، ۲۰۱۴، ترنر و همکاران، ۲۰۱۷)



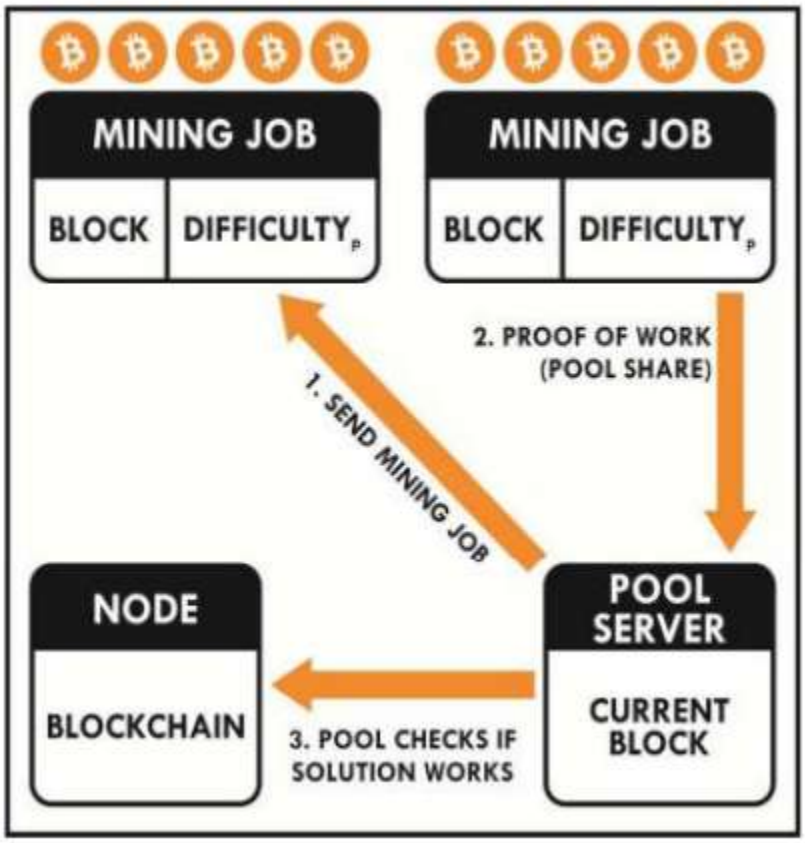
استخراج بیت کوین

استخراج بیت کوین فرایند اضافه کردن تراکنش های اعتباری به بلوک های بیت کوین است که در آن قابلیت صحت سنجی این اضافه شدن بدست آید، استخراج بیت کوین می تواند بسیار سودآور باشد به شرطی که برق ارزان و سخت افزار مناسب این کار را داشته باشید. به خاطر داشته باشید که استخراج بیت کوین رقابتی است. کشور چین به دلیل برق ارزان تر غالب استخراج بیت کوین جهان را در اختیار دارد. (آنتوپولوس[2]، ۲۰۱۰).

این استخراج شامل اتصال از بخش استخراج بیت کوین به بلوک های سرور و از آن آزاد شدن بیت کوین است (ترنر و همکاران[3]، ۲۰۱۷).

1 Barrera
2 Antonopoulos
3 Turner et al

شکل ۲: استخراج بیت کوین (برگرفته از : بررا، ۲۰۱۴ و ترنر و همکاران، ۲۰۱۷)

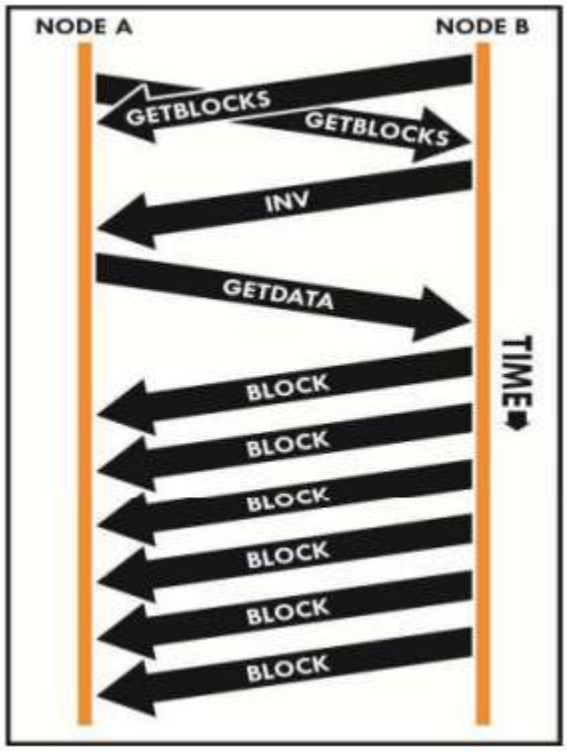


اتصالات و هم افزایی های بیت کوین (گره کامل بلاک چین)

گره کامل بلاک چین حاوی یک نسخه کامل و کاملا هماهنگ شده از دایرکتوری های عمومی، بلاک چین است.

سود عملیاتی به عنوان یک گره بلوک کامل است که می تواند تایید هر معامله را انجام دهد، همچنین مستقل از هر نهاد دیگری در شبکه می باشد (ترنر و همکاران، ۲۰۱۷) که در ادامه نمایش داده شده است:

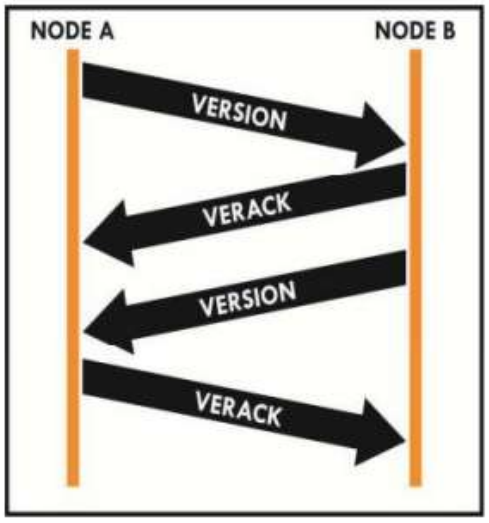
شکل ۳: اتصالات بیت کوین (برگرفته از : بررا، ۲۰۱۴ و ترنر و همکاران، ۲۰۱۷)

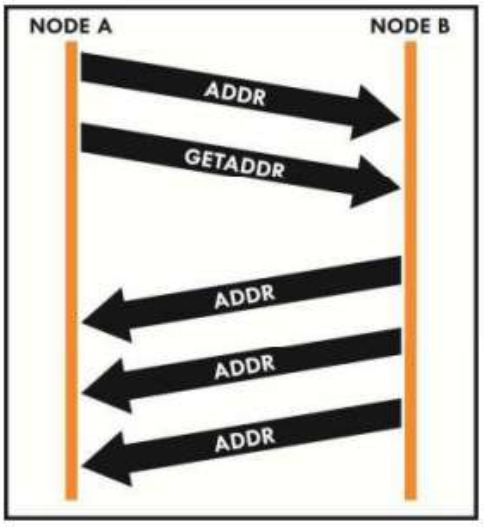


شناسایی شبکه (بیت کوین)

با توجه به ماهیت شبکه peer-to-peer که بیت کوین روی آن اجرا می شود، هر گره بیت کوین شبکه را اجرا می کند؛ مسیریابی برای گره، باید حداقل یکی از همتایان دیگر در شبکه شناسایی شود. برای انجام این، گره های بیت کوین از پروتکل کنترل انتقال (TCP) از طریق پورت ۸۳۳۳ یک پروتکل را اجرا می کنند و شروع به تبادل پیام ها می کند، نحوه این شناسایی در شکل زیر نمایش داده شده است:

شکل ۴: شناسایی و کشف شبکه بیت کوین (برگرفته از : بررا، ۲۰۱۴ ترنر و همکاران، ۲۰۱۷)

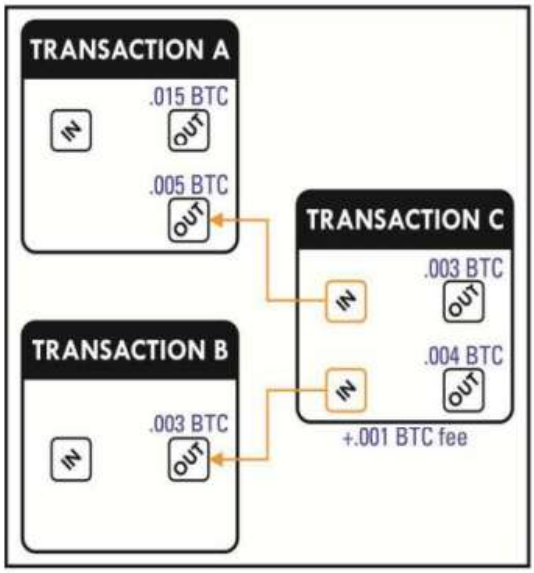


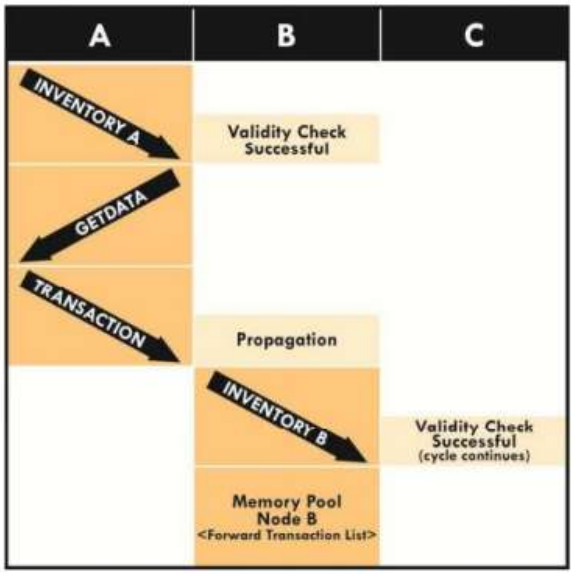


کالبد معاملات بیت کوین

معامله با پیغام دیجیتالی امضا شده حاوی بیت کوین ارسال و دریافت می شود؛ آدرس، همراه با مبلغ معامله، پس از آن، از یک کاربر به شبکه بیت کوین ارسال و پخش می شود، همچنین گره های بیت کوین قادر به ارسال و دریافت، درخواست، مجوز و اعتبار هستند، همچنین این معاملات در حافظه ذخیره می شوند و سپاس اعتبار آنها قابل رصد شدن است (ترنر و همکاران، ۲۰۱۷). شکل زیر این کالبد را نمایش می دهد:

شکل ۵: کالبد معاملات بیت کوین (برگرفته از : بررا، ۲۰۱۴ و ترنر و همکاران، ۲۰۱۷)

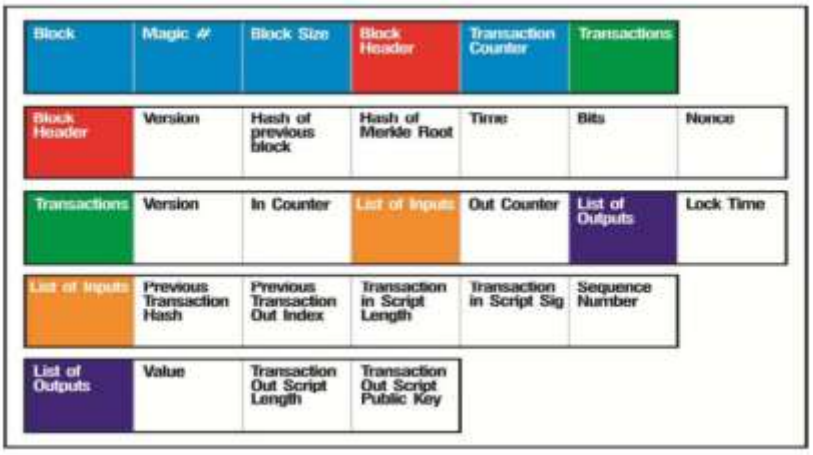




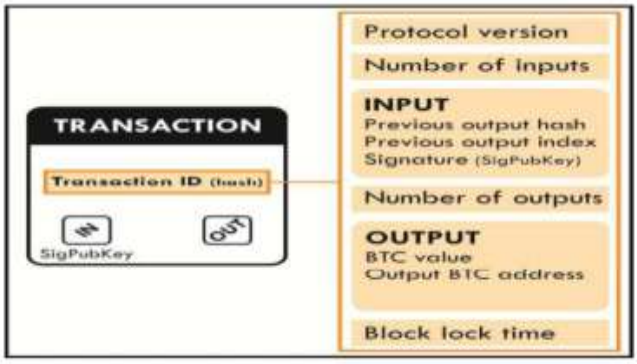
شناسایی هویت کاربر و ساختار معاملات

دو معیار مهم در معامله بیت کوین، 'لیست ورودی ها' و 'لیست خروجی ها' وجود دارد. معاملات می تواند از ورودی های متعدد و خروجی های چندگانه تشکیل شده باشد. خروجی ها از طریق هش معامله و شاخص خروجی مورد استفاده قرار گیرد. مهمتر از همه، شامل امضاء است معامله، scriptSig، که ترکیبی از کلید خصوصی رمزگذاری شده ECDSA است، یک هش از معامله و کلید عمومی آدرس است بوسیله این عناصر هم ساختار معاملات شناسایی و هم ID یا هویت کاربران شناسایی می شود، در خصوص هویت کاربران نسخه پروتکل، ورودی و خروجی ها و زمان لاک شدن بلاک اهمیت خواهد داشت (ترنر و همکاران، ۲۰۱۷) در ادامه هر دوی این موارد نشان داده شده است:

شکل ۶: کالبد معاملات بیت کوین (برگرفته از : ترنر و همکاران، ۲۰۱۷)



شکل ۷: هویت کاربران در بیت کوین (برگرفته از : ترنر و همکاران، ۲۰۱۷)



جمع بندی

بلاک چین دارای ریسک بالاخص در زمینه معاملات مشکوک می باشد، هدف مدیریت ریسک بلاک چین، شناسایی موقعیت های پرمخاطره و تهیه استراتژی هایی برای کاهش احتمال رخداد و اثر واقعه های پرمخاطره در زمینه معاملات مشکوک این حوزه می باشد. چون فناوری‌های اینترنتی، الکترونیکی، روبه گسترش هستند و به همین دلیل یکی از نگرانی های صنعت بازار پول و حوزه رمزارزداری از بابت ریسک‌ها و خطرات مربوط به این ریسک ها در این موسسات می باشند،به همین دلیل استفاده از بلاک چین در ارائه خدمات دولت‌ها و شرکت‌ها و علی الخصوص معاملات مالی مشکوک و نظام پولی و حوزه رمزارزی به مردم از باب جلوگیری از این خسارت‌های سنگین را لازم میدانند، چون در استفاده از بلاک چین هوشمند کردن سیستم‌ها و خدمات مختلف نسبت به جلوگیری از بروز خطرات و خسارت‌ها در دستور کار قرار میگیرند که، کیفیت خدمات و رضایت و رفاه مردم و زندگی بشر را توسعه دهند، پس با این اوصاف از ظهور ویروس‌ها، هکرها، خسارت‌ها، سرقت‌های اینترنتی و... جلوگیری می کند و در نتیجه خدمات‌دهندگان به صورت مستمر باید در جریان به‌روز کردن خدمات و نرم‌افزارهای خود باشند (هارلند[1] و همکاران، ۲۰۰۳).

1. Harland

منابع

Antonopoulos A (2010) Mastering Bitcoin. USA: O'Reilly Media.
Barrera A (2014) A Guide to Bitcoin (Part II): A deep dive into the Bitcoin ecosystem. Available at: http://tech.eu/features/926/bitcoin-ecosystem/ (Accessed 20 September 2015).
Beck, R., & Müller-Bloch, C. (2017). Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization.
Cohen, L., Tyler, R., Contreiras, D., & Buxton, P. (2016). Blockchain's three capital markets innovations explained. *International financial law review*, *35*(26), 9.
Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on* (pp. 618-623). IEEE.
Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, *9*(2), 397-413.
Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, *4*(6), 1832-1843.
Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and risks of Blockchain Technologies–a research agenda.
Rutkin, A. (2016). Blockchain-based microgrid gives power to consumers in New York. *New Scientist*, *2*.
Taylor, P. (2016). Applying blockchain technology to medicine traceability.
Turner, A., & Irwin, A. S. M. (2018). Bitcoin transactions: a digital discovery of illicit activity on the blockchain. *Journal of Financial Crime*, *25*(1), 109-130.
Walch, A. (2015). The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. *NYUJ Legis. & Pub. Pol'y*, *18*, 837.
Yoo, S. (2017). Blockchain based financial case analysis and its implications. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(3), 312-321.
Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*(10), 218.
Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue.
Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.

A review of the impact of green decentralized transactions on China-based blockchain technology

Ali Ghaffari *, Gholamreza Taleghani

Abstract

The world today is the digital world. In addition to competing in the digital world and the use of modern technologies, which are the concerns of various industries, digital investment and digital operations are one of the important concerns of Yank's shareholders and customers of the bank in entering digital banking. In this area, we can mention eight technologies as transformational technologies in digital evolution that have brought about changes and gaining competitive advantage: social media, virtual reality and augmentation, data analysis and data mining, artificial intelligence, Cloud computing, Internet of Things, Mobile Computing and Block chain. Bitcoin technology is a solution to create and maintain reliable digital records, taking into account constraints, risks, appropriate security architecture, infrastructure management control, and opportunities, but illegal activities should also be considered and in the direction Pathology and the discovery of digital violations in this area. The architecture of application software for detecting illegal and suspicious transactions can be in this change and the approach of digital evolution in the field of banking, opening up the security of financial operations and the satisfaction of shareholders and customers in this field; the purpose of this paper is to examine the technology of modern social media for diagnosis. Identity of Bitcoin users, which uses machine learning techniques to learn how specific behavior of the Bitcoin network, is with social media technology to detect illegal transactions. In this research, the identification of a user, the protocol and how it trades in bitcoin, and the behavior of the connection point to the last block chain on the network is examined.

Key Words: Block chain, Digital Transformation, Green Management.