دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

بررسی کارایی و امنیت بلاک‌چین در قراردادهای هوشمند

گزارش سمینار کارشناسی ارشد مهندسی کامپیوتر
گرایش نرم‌افزار

نگارش

شروین حاجی‌اسمعیلی

استاد راهنما

دکتر مقصود عباس‌پور

تابستان ۹۷

دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

گزارش سمینار کارشناسی ارشد مهندسی کامپیوتر - گرایش نرم‌افزار

تحت عنوان:

بررسی کارایی و امنیت بلاک‌چین در قراردادهای هوشمند

در تاریخ پایان‌نامه دانشجو، ، توسط کمیته تخصصی داوران مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنما اول:	نام و نام خانوادگی	امضا
۲- استاد راهنما دوم:	نام و نام خانوادگی	امضا (در صورت نیاز)
۳- استاد مشاور:	نام و نام خانوادگی	امضا (در صورت نیاز)
۴- استاد داور (داخلی):	نام و نام خانوادگی	امضا
۵- استاد داور (خارجی):	نام و نام خانوادگی	امضا
۶- نماینده تحصیلات تکمیلی:	نام و نام خانوادگی	امضا

با سپاس و قدردانی از

پدران و مادرانی که خود را فدای تربیت فرزاندان خود کردند و

اساتید و معلمانی که در تمام دوران زندگی، راهنمای جانسوز ما بودند.

آوردن این صفحه اختیاریست.

کلیه حقوق مادی مترتب بر نتایج مطالعات،
ابتکارات و نوآوری‌های ناشی از تحقیق موضوع
این پایان‌نامه متعلق به دانشگاه شهید بهشتی
می‌باشد.

به نام خدا

نام و نام خانوادگی: شروین حاجی‌اسمعیلی

عنوان پایان‌نامه: بررسی کارایی و امنیت بلاک‌چین در قراردادهای هوشمند

استاد راهنما: دکتر مقصود عباس‌پور

اینجانب شروین حاجی‌اسمعیلی تهیه‌کننده گزارش سمینار کارشناسی ارشد حاضر، خود را ملزم به حفظ امانت‌داری و قدردانی از زحمات سایر محققین و نویسندگان بنابر قانون Copyright می‌دانم. بدین وسیله اعلام می‌نمایم که مسئولیت کلیه مطالب درج شده با اینجانب می‌باشد و در صورت استفاده از اشکال، جداول و مطالب سایر منابع، بلافاصله مرجع آن ذکر شده و سایر مطالب از کار تحقیقاتی اینجانب استخراج گشته است و امانت‌داری را به صورت کامل رعایت نموده‌ام. در صورتی که خلاف این مطلب ثابت شود، مسئولیت کلیه عواقب قانونی با شخص اینجانب می‌باشد.

نام و نام خانوادگی: شروین حاجی‌اسمعیلی

تاریخ و امضا:

تقدیم به

رهجویان علم و فناوری و دوست‌داران علم و دانش

آوردن این صفحه اختیاریست.

فهرست مطالب

چکیده

لورم ایپسوم (به انگلیسی lorem ipsum) متنی بی مفهوم است که تشکیل شده از کلمات معنی دار یا بی معنی کنار هم. کاربر با دیدن متن لورم ایپسوم تصور میکند متنی که در صفحه مشاهده میکند این متن واقعی و مربوط به توضیحات صفحه مورد نظر است واقعی است. حالا سوال اینجاست که این متن « لورم ایپسوم » به چه دردی میخورد و اساسا برای چه منظور و هدفی ساخته شده است؟ پیش از بوجود آمدن لورم ایپسوم ، طراحان وب سایت در پروژه های وب سایت و طراحان کرافیک در پروژه های طراحی کاتولوگ ، بروشور ، پوستر و ... همواره با این مشکل مواجه بودند که صفحات پروژه خود را پیش از آنکه متن اصلی توسط کارفرما ارائه گردد و در صفحه مورد نظر قرار گیرد چگونه پر کنند؟؟ اکثر طراحان با نوشتن یک جمله مانند «این یک متن نمونه است» ویا «توضیحات در این بخش قرار خواهند گرفت» و کپی آن به تعداد زیاد یک یا چند پاراگراف متن میساختند که تمامی متن ها و کلمات ، جملات و پاراگراف ها تکراری بود و از این رو منظره خوبی برای بیننده نداشت و ضمنا به هیچ وجه واقعی به نظر نمیرسید تا بتواند شکل و شمایل تمام شده پروژه را نشان دهد. از این رو متنی ساخته شد که با دو کلمه (به فارسی : لورم ایپسوم) آغاز میشد وبا همین نام در بین طراحان وب و گرافیک شناخته و به سرعت محبوب شد. وب سایت های سازنده لورم ایپسوم میتوانند هر تعداد کلمه و پاراگراف که بخواهید به صوورت تکراری یا غیر تکراری برایتان بسازند و تحویلتان بدهند تا از آنها در پروژه هایتان استفاده کنید. (لورم ایپسوم فارسی) متن های لورم ایپسوم را به زبان فارسی و علاوه بر زبان فارسی به انگلیسی ، عربی ، ترکی استانبولی و ... برایتان میسازد. زبان های دیگر نیز رفته رفته به بانک اطلاعاتی لورم ایسپوم فارسی اضافه خواهند شد.

واژگان کلیدی: بلاک‌جین، اتریوم، امنیت، رای‌گیری

فصل ۱

مقدمه

با معرفی بیت‌کوین [1] به عنوان یک ارز دیجیتال بدون پشتوانه و ارزش ذاتی در سال ۲۰۰۸ [۱] و فراگیر شدن استفاده‌ی از این بستر برای تراکنش‌های مالی مطالعات بسیاری در مورد دلیل موفقیت آن شد. اما با گذشت زمان توجه‌ها بیشتر به تکنولوژی مورد استفاده‌ی این ارز دیجیتال و به طور خاص بلاک‌چین [2] جلب شد. از استفاده‌های دربلاک‌چین بیت کوین برای تولید ابزارهای مالی جدید می‌توان به سکه‌های رنگی به عنوان ارزهای جدید و Namecoin برای بستر خرید و فروش دامنه و نام اشاره کرد.

استفاده از بلاک‌چین به عنوان یک لیست تغییرناپذیر به کمک اثبات کار یک راه‌حل توزیع‌شده برای مسئله‌ی ژنرال‌های بیزنتین [3] را ایجاد کرد که خود باعث تولید ارزهای جدید به روی بسترهای مستقل شده و برای کاربردهای جدید شد. یکی از بلندپروازانه‌ترین ایده‌هایی که تا به امروز دیده شده اتریوم [۲] است. تراکنش‌های بیت‌کوین توانایی ثبت اسکرپت‌هایی که قواعدی برای تراکنش ثبت کنند را دارند ولی تعدادی از خصوصیت‌های معمول زبان‌های برنامه‌نویسی turing-complete مانند حلقه را پشتیبانی نمی‌کنند. هدف از ساخت اتریوم ساخت یک زبان برنامه نویسی turing-complete برای این بستر است.

فلسفه‌ی ساخت پروتکل اتریوم رو می‌توان در این ۵ پایه خلاصه کرد:

- **سادگی:** پروتکل باید برای برنامه‌نویسان ساده و دردسترس باشد حتی به قیمت از کم شدن بهره‌وری کل سیستم.
- **کامل بودن:** اتریوم باید یک زبان turing-complete داشته باشد و هر مدل ریاضی را بتوان با آن پیاده کرد.
- **بخش‌پذیری** [4]: قسمت‌های اتریوم باید از هم جدا باشند و توانایی عوض کردن الگوریتم‌های و ساختارداده‌های سیستم مانند درخت پاتریشا وجود داشته باشد، بدون این که قسمت‌های دیگر سیستم از این تغییر باخبر شوند
- **چابکی:** جزییات پروتکل اتریوم باید قابل تغییر باشند.
- **برابری:** سیستم نباید فعلانه جلوی یک دسته از کاربردها رو بگیرد یا آن‌ها رو محدود کند.

[1] Bitcoin

[2] Blockchain

[3] Byzantine generals

[4] Modularity

با بوجود آمدن اتریوم به عنوان یک بستر کامل، بی‌اعتماد و توزیع‌شده برای قراردادهای هوشمند کاربردهای اشاره شده در بالا را می‌توانن به سادگی با نوشتن چند خط کد پیاده کرد. این سادگی در پیاده‌سازی باعث جذب بسیاری از توسعه‌دهندگان می‌شود که می‌توانند کاربردهای جدیدی پیاده کنند که به عنوان یک کارپرداز خودکار در این بستر فعالیت کنند. تغییرناپذیری قراردادهایی که در بستر بلاک‌چین نوشته می‌شوند باعث اعتماد مشتریان آن‌ها به آن قرارداد می‌شود ولی این تغییرناپذیری به معنی این است که اگر قرارداد «اشتباهی» در این بستر نوشته شود راهی برای تصحیح آن نیست. برای مثال در سال ۲۰۱۶ به اندازه‌ی ۵۰ میلیون دلار اتر از یک سازمان کرودفاندینگ در اثر یک باگ امنیتی از بک قرارداد آن‌ها دزدیده شد [۱] . با توجه به تغییر ناپذیر بودن بلاک‌چین هیچ راهی جز تغییر پروتکل برای بازگرداندن پول وجود نداشت و در نهایت با یک انشعاب سخت [۲] از این بستر پول به آن مجموعه بازگردانده شد. این تصمیم برای تغییر سیستم باعث شد کاربران اتریوم به دو دسته تقسیم شوند، دسته‌ی اول کسانی که از بازگردانده شدن پول به سازمان حمایت می‌کردند و بلاک‌چین جدید رو به عنوان بلاک‌چین اصلی اتریوم قبول کردند و دسته‌ی دوم که با این استدلال که قانون اتریوم کد قراردادهاست و چون قرارداد به درستی اجرا شده باید آن مبلغ به هکرها تعلق بگیرد، بلاک‌چین جدید را قبول نکرده و بلاک‌چین قبلی را ادامه دادند. از نمونه‌های دیگر این مسئله می‌توان به قفل شدن ۳۰۰ میلیون دلار [۳] اتر متعلق به شرکت parity در نوابر ۲۰۱۷ اشاره کرد.

لازم به ذکر است که هیچ کدام از مشکلات امنیتی نام برده شده مشکل خود بستر اتریوم نبوده و مسئله استفاده‌ی اشتباه از زبان برنامه‌نویسی آن و قابلیت‌های آن‌ها بوده است. با این وجود توجه به مسائل امنیتی در این بستر ناآشنا و جدید با توجه به طرز فکر متفاوت از برنامه‌نویسی عادی بسیار مهم است.

در ادامه‌ی این تحقیق به بررسی دقیق‌تر بعضی از این مشکلات امنیتی خواهیم پرداخت.

یک سوال مهم در زمینه‌ی قراردادهای هوشمند اتریوم کاربردهای ممکن و یا مناسب این بستر است. از کاربرداهای معروف این بستر به کاربردهای زیر می‌توان اشاره کرد:

- ارزهای جدید

[1] "https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/"

[2] Hard fork

[3] "https://hackernoon.com/how-ethereum-lost-300-million-dollars-bfedf7ba0c19"

- سیستم‌های هویت
- فایل‌سیستم‌های توزیع‌شده
- سازمان‌های خودکار توزیع‌شده

در ادامه‌ی این تحقیق ابتدا به تعریف مفاهیم پرکاربرد آن می‌پردازیم و در فصل سوم به بررسی کارهای پیشین پرداخته و در نهایت در فصل چهارم به تعریف مسئله‌ی پیشنهادی این تحقیق خواهیم پرداخت.

فصل ۲

تعریف مفاهیم

در این بخش تعریف مفاهیم مورد استفاده در این تحقیق می‌پردازیم.

- **بلاک‌چین:** بلاک‌چین یک ساختارداده متشکل از بلوک‌های پشت‌سرهم که هر بلوک شامل هشی از خودش بلوک قبلی هم هست. در نتیجه به تغییر یک بلوک باید تمام بلوک‌های بعد از آن را تغییر داد تا ساختار درست باشد.

- **اثبات کار** [1]: روش اثبات کار بر اساس hashcash [۳] که یک روش برای جلوگیری از حملات DDoS طراحی شده بود ساخته شده است. روش کار hashcash به شکل زیر است:

برای این که یک ایمیل توسط سرور ارسال شود همراه متن ایمیل کلاینت باید که رشته‌ای ارسال کند که اگر هش SHA-1 آن از آن گرفته شود ۲۰ بیت اول آن صفر خواهند بود. به دلیلی تصادفی بودن هش رشته باید با امتحان کردن رشته‌های مختلف به یک رشته‌ی مناسب برسد. زمان حل این مسئله برای کامپوترهای 1 GHZ آن زمان حدود یک ثانیه بود و زمان بررسی درست بودن آن هش تنها ۲ میکروثانیه است.

برای یک کاربر عادی که قصد ارسال یک ایمیل را دارد زمان یک ثانیه‌ای قابل‌قبول است اما اگر یک مهاجم قصد spam کردن توسط این سرویس را داشته باشد زمان یک ثانیه برای هر ایمیل هزینه‌ی بسیار بالایی خواهد بود.

در بستر بیت‌کوین از این روش برای توافق بر بلوک‌های بعدی بلاک‌چین به صورت زیر استفاده می‌شود: هر بلوک جدید حاوی تعدادی تراکنش برای ثبت در بلاک‌چین توسط ماینترها به یک بلوک تبدیل می‌شود. ولی برای این که این بلوک توسط بقیه پذیرفته شود باید در این بلاک یک nounce قراردهند به صورتی که هش بلاک از یک عددی که توسط پروتکل بیت‌کوین انتخاب می‌شود کمتر باشد. این شرط در طول زمان به صورت خودکار به روزرسانی می‌شود به طوری که در هر لحظه به صورت میانگین اضافه کردن بلاک ۱۰ دقیقه از کل شبکه زمان ببرد. از آنجایی که تنها راه پیدا کردن همچین رشته‌ای بروت‌فورس [2] است، توان محاسباتی بالاتر باعث شانس بیشتر برای پیدا کردن بلوک بعدی خواهد شد.

- **مسئله‌ی جنرال‌های بیزنتین**

[1] Proof of work

[2] Bruteforce

مسئله‌ی جنرال‌های بیزنتین یا تحمل خطای بیزنتین مدلی از تحمل خطا در سیستم‌های توزیع شده است. در این مسئله تعدادی جنرال یک ارتش با هم به صورت پیام‌های یک به یک صحبت می‌کنند و در ساده‌ترین حالت در مورد حمله کردن یا عقب‌نشینی در یک نبرد تصمیم می‌گیرند. ولی تعدادی از این جنرال‌ها خائن بوده و تلاش می‌کنند که جمع به توافق غلطی برسد (توافق درست توافقی است که اگر هیچ خائنی وجود نداشت به آن می‌رسیدند) و یا با جواب ندادن مانع تصمیم‌گیری آن‌ها شوند. در ساده‌ترین حالت و بدون استفاده از امضاهای دیجیتال ثابت می‌شود که برای $3k + 1$ جنرال، با رای‌گیری می‌توان تا k خائن را تحمل کرد. راه‌حل خلاقانه‌ی بیت‌کوین برای حل این مسئله استفاده از بلاک‌چین برای ذخیره‌ی اطلاعات و استفاده از اثبات کار برای اضافه کردن بلوک به بلاک‌چین است.

برای نشان دادن نحوه‌ی حل این مسئله یک مثال را بررسی می‌کنیم. فرض می‌کنیم شخص A یک بیت‌کوین را به B منتقل کرده و این تراکنش در بلاک‌چین ثبت شده و در ازای آن کالایی دریافت کرده، حال قصد دارد که این تراکنش رو از بلاک‌چین بیت‌کوین حذف کند تا بتواند آن را ۲ بار خرج کند. از آنجایی که نودهای شبکه‌ی بیت‌ککوین اگر ۲ زنجیره از بلوک‌ها دریافت کنند زنجیره‌ی بلندتر را قبول خواهند کرد باید ۲ بلوک سالم بسازد قبل از این که کل شبکه یک بلوک به شبکه اضافه کنند.

احتمال موفقت حمله‌ی A مساوی $(\frac{A's\ computational\ power}{Bitcoin\ network's\ computational\ power})^2$ است. اگر توان محاسباتی A از بقیه‌ی شبکه کمتر باشد این کسر یک عدد کوچک‌تر از ۵.۰ است. اگر در این کار به موقع موفق نشود سه بلاک عقب می‌افتد و توان فرمول بالا تبدیل به سه می‌شود و احتمال موفقیتش کمتر از پیش نیز می‌شود. این مسئله مسئله‌ی قماربار [1] نام دارد که نشان داده می‌شود در آن در طول زمان احتمال موفقت مهاجم به صورت نمایی کاهش پیدا می‌کند.

- **انشعاب** [2]: منظور از انشعاب در ارزهای دیجیتال تبدیل یک بلاک‌چین به دو بلاک‌چین است، گاها برای ساخت ارزهای جدید از بلاک‌چین موجود یک ارز دیگر مثل بیت‌کوین استفاده می‌شود، این کار باعث می‌شود که شروع بلاک‌چین آسان‌تر و امن‌تر شود. در روال عادی کار بیت‌کوین نیز ممکن است انشعابی رخ دهد اما هر ماینری که متوجه انشعابی شود به صورت خودکار بلندترین زنجیره را به عنوان زنجیره‌ی

[1] Gambler's Ruin

[2] fork

درست انتخاب می‌کند. در صورتی که یک انشعاب برای تولید بلاک‌چین جدید انجام گیرد و بلوک‌هایی قبلی که در آن وجود داشتند همچنان درست حساب شوند این انشعاب را انشعاب نرم و اگر بلوک‌های قبلی مورد قبول سیستم جدید نباشند انشعاب را انشعاب سخت می‌نامیم.

- **ماین‌کردن:** به عملیات پیدا ساختن بلوک‌های جدید روی بلاک‌چین به هدف پیدا کردن بلاک‌های درست و دریافت جایزه‌ی آن‌ها ماین‌کردن می‌گوییم.

- **ماینینگ پول:** از آن جایی که ماین کردن برای یک نفر با توجه به احتمال پایین این که بتوانند بلاک معتبر را زودتر از بقیه‌ی شبکه پیدا کنند بسیار پایین است، ماینینگ‌پول‌ها شکل گرفته‌اند. با تقسیم کردن کار بین چندین ماشین شانس پیدا کردن بلوک معتبر بیشتر می‌شود و جایزه‌ی ماین کردن به نسبت توان محاسباتی بین شرکت‌کنندگان تقسیم می‌شود. برای بدست آوردن توان محاسباتی که هر ماشین برای این کار مصرف کرده از تعداد بلوک‌هایی که هش آن‌ها به اندازه‌ی کافی برای درست بودن کوچک نیست ولی به جواب درست نزدیکند استفاده می‌شود.

- **قرارداد هوشمند** لفظ قراردادهای هوشمند اولین بار در سال ۱۹۹۳ توسط N.Szabo [۴] به عنوان یک پروتکل تراکنش کامپیوتری که شروط یک قرارداد را اجرا می‌کند. در اولین مثال معروف قراردادهای هوشمند یک وندینگ ماشین [1] را مثال زد که در ازای سکه‌ی به طور اتوماتیک کالای مورد نظر را به مشتری می‌دهد، همینطور از آنجایی که بدون پول دادن هرگز کالایی نمی‌دهد و امنیت سکه‌ها را از طریق صندوق خود تا حد معقولی تامین می‌کند قرارداد مناسبی بین مشتری و تولیدکننده‌ی کالا محسوب می‌شود. هدف نهایی قراردادهای هوشمند کاهش نیاز به اعتماد کردن و افراد میانی در یک قرارداد است و با بوجود آمدن بسترهای ارز دیجیتال و راه‌حل‌های جدید مسئله‌ی جنرال‌های بیزنتین بستر مناسبی برای ساخت قراردادهای هوشمند و توزیع‌شده بدون نیاز به اعتماد به شخص ثالث بوجود آمده است. با وجودی که به کمک زبان اسکریپتینگ بیت‌کوین می‌توان مدل‌های مختلفی از قراردادهای هوشمند را تولید کرد، با اتریوم به به کمک زبان برنامه‌نویسی turing-complete آن در تئوری می‌توان هر قرارداد هوشمند ممکن را تولید کرد.

[1] vending machine

فصل ۳

مروری بر پژوهش‌های مرتبط

در این بخش به مروری بر کارهای انحام شده تاکنون می‌پردازیم. این مقالات را به سه دسته‌ی زیر تقسیم می‌کنیم.

۱.۳ امنیت بلاک‌چین و ماین‌کردن

در روش امنیتی بیت‌کوین که از طریق حل کردن یک مسئله‌ی سخت محاسباتی ثابت بلاک‌های جدید به بلاک‌چین اضافه می‌شوند چند مسئله‌ی امنیتی رخ می‌دهد، اول این که به دلیل این که عملیات ماین‌کردن احتیاجی به کل بلاک‌چین ندارد و افراد می‌توانند کار را تقسیم کنند احتمال بوجود امدن یک ماینینگ پول که بیش از پنجاه درصد توان محاسباتی را داشته باشد بالا می‌رود. بعضی پزوهش‌ها در این زمینه برای تولید مسائل مناسب برای اثبات کار که در عین‌حال قابل تقسیم و موازی انجام شدن هم باشند انجام شده است.

مسئله‌ی دیگر بوجود آمدن سخت‌افزارهای مخصوص این مسئله است که باعث می‌شود عملیات ماین کردن از یک عملیات توزیع‌شده که تمام افراد در آن شرکت می‌کنند یه عملیاتی نیازمند سرمایه‌ی اولیه‌ی بالا شود. امنیت بیت‌کوین در گرو این موضوع است که به نفع تمام افرادی که ماین می‌کنند است که در پروتکل رو رعایت کنند اما در این تحقیق [۵] نشان داده شده که این گزاره همواره درست نیست و در بعضی شرایط با برای ماینینگ‌پول‌ها به صرفه است که از توان مصرفی خود در یک ماینینگ‌پول رقیب استفاده کنند و اگر هش درست را برای رقیب پیدا کردند آن را اعلام نکنند [۶] .

یک تحقیق دیگر [۷] نشان داد در شرایطی برای ماینینگ‌پول‌ها به صرفه است که اگر هش درست را پیدا کردند به بقیه اعلام نکنند تا برای بلوک بعدی به دلیل زودتر شروع کردن شانس بالاتری داشته باشند.

با توجه به این شرایط و همچنین هزینه‌ی محاسباتی بالایی که ماین‌کردن در شرایط فعلی بیت‌کوین و بسیاری از ارزهای دیجیتال دیگر دارد تحقیقات بسیاری برای پیدا کردن روش‌های دیگر به جای استفاده از اثبات کار برای اضافه کردن بلوک به بلاک‌چین شده که در ادامه به تعدادی از آن‌ها اشاره می‌کنیم:

- **اثبات سهم** [1] : به این صورت است که هر ماین‌کننده‌ای که سهم بیشتری از سکه‌های بستر را داشته باشد،

[1] proof of stake

شانس بیشتری برای ساختن بلوک بعدی دارد. ایده‌ی کلی این روش این است که در صورت پیش آمدن مشکلی برای بستر این افراد بیشترین ضرر را خواهند کرد.

- **اثبات سن سکه**[1]: یک روش ارائه شده توسط Peercoin است که در آن برای ماین کردن به مقدار سکه‌ی قدیمی (عمر سکه مدت زمانی که در یک حساب ساکن مانده باشد تعریف می‌شود) هر ماین‌کننده توجه می‌شود.
- **اثبات سپرده**[2]: در این روش برای ساخت بلوک جدید باید مقداری سکه توسط ماین‌کننده در یک حساب برای مدت زمانی قفل شوند.
- **اثبات سوزاندن**[3]: در این روش برای ساخت بلوک باید مقداری سکه را به حسابی غیرقابل دسترس (مثلا حسابی با کلید عمومی تماما صفر) منتقل کرد.
- **اثبات فعالیت**[4]: در این روش تعدادی کاربر در هر مرحله به صورت تصادفی برای اضافه‌کردن بلوک انتخاب می‌شوند و باید در مدت زمانی محدود با یک پیغام امضا شده به آن پاسخ دهند.
- **Stellar Consensus Protocol** [۸]: در این روش با بوجود آمدن طبیعی کاربرهای قابل اعتماد و ساخت لایه‌هایی از اعتماد که بی‌شباهت به لایه‌های ISP نیستند برای انتخاب بلوک بعدی تصمیم می‌گیرند. در این روش هر کاربر خود انتخاب می‌کند که چه افرادی در مورد درستی تراکنش او تصمیم بگیرند.

۲.۳ امنیت قراردادهای اتریوم

واضح است که با بوجود آمدن ارزهای دیجیتال مانند بیت‌کوین و تراکنش‌های نیمه‌ناشناس در آن‌ها بستری مناسبی برای تراکنش‌های غیرقانونی و مجرمانه بوجود آمد، به کمک بستر اسکرپیتینگ بیت‌کوین و در ادامه بستر کامل قراردادهای هوشمند مسئله‌ی قراردادهای مجرمانه به طور جدی‌تری مسئله خواهد شد. در تحقیق‌های [۹]

[1] proof of coin-age
[2] proof of deposit
[3] proof of burn
[4] proof of activity

[۱۰] به بررسی دقیق‌تر این کاربردها پرداخته شده است. برای مثال قراردادهایی برای لو دادن اسناد محرمانه و یا حتی دزدین کلیدهای رمزنگاری از جمله کاربردهای ممکن این قراردادها هستند.

همچنین atezi [۱۱] به بررسی مشکلات امنیتی معمول قراردادهای در بستر اتریوم و تله‌ی معمول این زبان برنامه‌نویسی و روش‌های تصحیح آن‌ها پرداخت. از اشتباهاتی که وی در تحقیق خود به آن‌ها پرداخته می‌توان به نحوه‌ی نوشتن قراردادی که در سال ۲۰۱۶ باعث انشعاب بلاک‌چین اتریوم شد اشاره کرد.

۳.۳ حریم خصوصی

از کارهای دیگر بر روی امنیت تراکنش‌ها می‌توان به تلاش‌هایی برای تبدیل کردن این بسترها از بسترهای تراکنش نیمه‌ناشناس به تراکنش‌های ناشناس اشاره کرد. کارهایی مانند zerocash و بستر HAWK [۱۲] و یا E. Heilman در مقاله‌ی [۱۳] به بررسی روش‌های تولید تراکنش‌های کاملا ناشناس بر روی بسترهای موجود یا خارج از آن‌ها پرداخته‌اند.

فصل ۴

طرح مسئله

با بوجود آمدن سازمان‌های خودکار توزیع‌شده در بستر اتریوم تلاش‌های بسیاری برای ساخت سازمان‌هایی برای کاربردهایی که در ساختار فعلی جامعه احتیاج به اعتماد به یک سازمان مرکزی دارند در بستر بلاک‌چین شده است .

یکی از این کاربردها سیستم‌های رای‌گیری هستند. در شرایط فعلی برای راه انداختن یک سیستم رای‌گیری سیستم‌های خودکاری وجود دارند که استفاده از آن‌ها نیازمند اعتماد به نگه‌دارندگان آن سیستم‌ها (که در بسیاری از کاربردها دولت‌ها این نقش را به عهده دارند) و همچنین امنیت این سیستم‌هاست.

یک تحقیق معروف از دانشگاه NYU در سال ۲۰۱۵ [1] توضیح داد که ماشین‌های رای‌گیری الکترونیکی که در ۴۳ ایالت آمریکا استفاده می‌شوند در سال ۲۰۱۶ به دهمین سال استفاده شدن می‌رسند. ساختار و نرم‌افزار قدیمی این دستگاه‌ها باعث می‌شود که احتمال هک شدن آن به شدت بالا برود.

در سال ۲۰۱۶ اوکراین و ایالات متحده‌ی آمریکا قراردادی برای ساخت یک سیستم رای‌گیری بر روی بستر اتریوم امضا کردند [2]. این پتانسیل تکنولوژی بلاک‌چین در زمینه‌ی رای‌گیری باعث تولید چند نمونه [۱۴] از سیستم‌های رای‌گیری بر بستر بلاک‌چین نیز شده که از آن‌ها می‌توان به VoteBook [۱۵] توسط شرکت Kaspersky که یک شرکت پیشرو دز زمینه‌ی امنیت است اشاره کرد.

فلسفه‌ی ساخت این سیستم به صورتی است که تلاش می‌کند برای کاربرانی که از سیستم‌هایی رای‌گیری فعلی استفاده می‌کنند کمترین تغییر در رفتار نیاز باشد.

از مثال‌های دیگر سیستم‌های رای‌گیری مبتنی بر بلاک‌چین می‌توان به استارت‌آپ Follow My Vote اشاره کرد. نجوه‌ی کار این سیستم با سیستم VoteBook تفاوت اساسی دارد و برای رای‌دادن احتیاج دارد که نرم‌افزاری برای رای‌دادن به روی کامپیتور و یا تلفن‌همراه کاربران نصب شود.

و در نهایت یکی از موفق‌ترین سیستم‌های رای‌گیری مبتنی بر بلاک‌چین موجود در حال حاضر VoteWatcher ساخته شده توسط یک شاخه از شرکت blockchain Technologies Corporation است که یک شرکت بزرگ برای ارائه‌ی سرویس‌های مبتنی بر بلاک‌چین است. طبق وب‌سایت این محصول تاکنون بیش از صدهزار رای در بیشتر از ۲۰ رای‌گیری مختلف توسط این سیستم شمارش شده‌است.

[1] https://www.brennancenter.org/publication/americas-voting-machines-risk

[2] http://www.coinfox.info/news/4794-ukraine-to-introduce-etherium-based-e-voting

مدل اسفاده‌ی VoteWatcher به سیستم VoteBook بسیار شبیه است و تفاوت رفتاری زیادی با مدل‌های رای‌گیری الکترونیکی فعلی برای کاربران ندارد.

یک نکته‌ی مهم در مورد همه‌ی این نمونه‌ها این است که در آن‌ها استفاده‌ای از بلاک‌چین‌های عمومی نمی‌شود و با استفاده از بلاک‌چین‌های اختصاصی کار می‌کنند. در حالت کلی این یک نکته‌ی منفی ولی بسته به کاربرد می‌تواند استفاده از یک بلاک‌چین عمومی به شفافیت سیستم کمک کند.

یک مسئله‌ی دیگر که با وجود امنیت بالای این سیستم‌ها هنوز حل نشده و جای کار دارد سیستم‌های رای‌گیری برای شرایطی که امنیت رای‌دهندگان را نمی‌شود به خوبی تامین کرد است. با وجودی که اکثر سیستم‌های فعلی از قابلیت انتخاب این که رای این رای‌دهنده شمارش نشود پشنیبانی می‌کنند، سیستم پیگیری رای که برای امنیت و اطمینان بیشتر به سیستم اضافه شده می‌تواند حریم خصوصی کاربران را زیر سوال ببرد.

R. Sarres de Almeida در یک بلاگ پست به این مسئله در برزیل و مشکلاتی که این سیستم به وضعیت خرید و فروش و یا تهدید برای رای دادن به یک کاندیدای خاص بوجود می‌آورد پرداخت. در شرایطی که فردی که رشوه داده می‌تواند Ballot ID کسی که رای داده را از او گرفته و نتیجه‌ی رای او را چک کند، خطر خرید و فروش و بخصوص استفاده از خشونت برای جمع‌کردن رای دوچندان می‌شود.

با توجه به این خلا موجود در پیاده‌سازی‌های موجود در این زمینه، هدف این پژوهش طراحی یک سیستم رای‌گیری دیجیتال مبتنی بر بلاک‌چین است که در آن بتوان شمارش هر رای را بررسی کرد ولی امکان وصل کردن به رای داده شده به هیچ وجه ممکن نباشد.

مراجع

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] "Ethereum foundation, ethereum whitepaper, a next-generation smart contract and decentralized application platform,"" *https:|| github.com| ethereum| wiki| wiki| White-Paper*", 2014.

[3] A. beck, "Hashcash: a denial of service counter-measure," 2008.

[4] N. Szabo, "Smart contracts," *http:|| www.fon.hum.uva.nl| rob| Courses| InformationInSpeech| CDROM| L* 1993.

[5] J.Bonneau, A.Miller, J. A.Narayyanan, and E.W.Felten, "Sok: Research prespectives and challenges for bitcoin and cryprocurrencies," *IEEE Symposium on Security and Privacy*, 2015.

[6] N. T. Courtois, "On the longest chain rule and programmed selfdestruction of cryptocurrencies," *arXiv preprint arXiv:1405.0534*.

[7] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Financial Cryptography*, 2014.

[8] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," 2015.

[9] A. Juels, A. Kosba, and E. shi, "The ring of gyges: Investigating the future of criminal smart contracts," *Proceedings of ACM CCS*, pp.283-295, 2013.

[10] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp.254-269.

[11] N. Atzei, M. Bartoletti, and T. Cimon, "A survey of attacks on ethereum smart contracts," *Proceedings of the 6th International Conference on Principles of Security and Trust*, vol.10204, pp.164-186, 2017.

[12] "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," *IEEE Symposium on Security and Privacy*, pp.839-858, 2016.

[13] E. Heilman, foteini Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and o -blockchain bitcoin transactions," *Financial Cryptography and Data Security*, 2016.

[14] R. Osgood, "The future of democracy: Blockchain voting," *COMP116: Information Security*, 2016.

[15] K. kirby, A. Masi, and F. Maymi, "Votebook: A proposal for a blockchain-based electronic voting system," *https:| | www.economist.com| sites| default| files| nyu.pdf*, 2016.

Abstract:

This is Abstract in English.

Keywords: Blockchain, ethereum, security, voting

Shahid Beheshti University

Faculty of Computer Science & Engineering

Usage and Security of Blockchain in Smart Contracts

By

Shervin Hajiesmaili

A THESIS SUBMITTED
FOR THE DEGREE OF
MASTER OF SCIENCE

Supervisor :

Dr. Maghsood Abbaspour

2018