



دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

بررسی کارایی و امنیت بلاک چین در قراردادهای هوشمند

گزارش سمینار کارشناسی ارشد مهندسی کامپیوتر
گرایش نرم افزار

نگارش

شروین حاجی اسمعیلی

استاد راهنما

دکتر مقصود عباس پور

تابستان ۹۷



دانشگاه شهید بهشتی
دانشکده مهندسی و علوم کامپیوتر

گزارش سمینار کارشناسی ارشد مهندسی کامپیوتر - گرایش نرم افزار
تحت عنوان:

بررسی کارایی و امنیت بلاک چین در قراردادهای هوشمند

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

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

با سپاس و قدردانی از

پدران و مادرانی که خود را فدای تربیت فرزندان 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 حاجی اسمعیلی

عنوان پایان نامه: بررسی کارایی و امنیت بلاک چین در قراردادهای هوشمند

استاد راهنما: دکتر مقصود عباس پور

اینجانب شروین حاجی اسمعیلی تهیه کننده گزارش سمینار کارشناسی ارشد حاضر، خود را ملزم به حفظ امانت داری و قدردانی از زحمات سایر محققین و نویسندگان بنابر قانون Copyright می دانم. بدین وسیله اعلام می نمایم که مسئولیت کلیه مطالب درج شده با اینجانب می باشد 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 امانت داری را به صورت کامل رعایت نموده ام. در صورتی که خلاف این مطلب ثابت شود، مسئولیت کلیه عواقب قانونی با شخص اینجانب می باشد.

نام و نام خانوادگی: شروین حاجی اسمعیلی

تاریخ و امضا:

تقدیم به

رهجویان علم و فناوری و دوستداران علم و دانش

آوردن این صفحه اختیاریست.

فهرست مطالب

۱	مقدمه	۱
۵	تعریف مفاهیم	۲
۹	مروری بر پژوهش‌های مرتبط	۳
۱۰	۱.۳ امنیت بلاک چین و ماین کردن	۱۰
۱۱	۲.۳ امنیت قراردادهای اتریوم	۱۱
۱۲	۳.۳ حریم خصوصی	۱۲
۱۳	۴ طرح مسئله	۱۳
۱۶	مراجع	۱۶

چکیده

از سال ۲۰۰۹ تاکنون، با فراگیری بیت کوین شاهد افزایش کاربردهای بلاک چین و سیستم‌های توزیع شده و بدون نیاز به اعتماد بوده‌ایم. بعد از انتشار بستر اتریوم تا به امروز قراردادهای هوشمند توزیع شده در این بستر رشد قابل توجهی داشته‌اند. به همین دلیل بررسی امنیتی قراردادهای این بستر اهمیت ویژه‌ای دارد. همچنین با ساخت این بستر فرصت مناسبی است تا سرویس‌های بیشمار مبتنی بر اعتماد فعلی خود و راه‌های جایگزین آن‌ها را در بستر بلاک چین بررسی کنیم.

در این تحقیق ابتدا به معرفی ارزشهای دیجیتال و نحوه‌ی کارکرد آن‌ها می‌پردازیم، سپس تحقیقات امنیتی خود بسترها و کاربردهای آن‌ها را بررسی کرده و در نهایت به کاربرد آن‌ها برای رای‌گیری دیجیتال و چالش‌های این کار اشاره خواهیم کرد.

واژگان کلیدی: بلاک چین، اتریوم، امنیت، قرارداد هوشمند، رای‌گیری

فصل ۱

مقدمه

با معرفی بیت کوین^۱ به عنوان یک ارز دیجیتال بدون پشتوانه و ارزش ذاتی در سال ۲۰۰۸ [۱] و فراگیر شدن استفاده از این بستر برای تراکنش‌های مالی، در مورد دلیل موفقیت آن مطالعات بسیاری صورت گرفت. اما با گذشت زمان توجه‌ها بیشتر به تکنولوژی مورد استفاده‌ی این ارز دیجیتال و به طور خاص بلاک‌چین^۲ جلب شد. از استفاده‌های بلاک‌چین 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 لیست تغییرناپذیر به کمک اثبات کار، راه‌حلی توزیع‌شده برای مسئله‌ی ژنرال‌های بیزنتین^۳ ایجاد کرد که خود باعث تولید ارزهای جدید بر بسترهای مستقل شده و کاربردهای جدید شد. اتریوم [۲]، یکی از بلندپروازانه‌ترین ایده‌هایی است که تا کنون دیده شده است. تراکنش‌های بیت‌کوین توانایی ثبت اسکرپت‌هایی را که قواعدی برای تراکنش ثبت کنند، دارند اما برخی از ویژگی‌های معمول زبان‌های برنامه‌نویسی turing-complete مانند حلقه را پشتیبانی نمی‌کنند. هدف از ساخت اتریوم ساخت یک زبان برنامه‌نویسی 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 قابل دسترس باشد، حتی به قیمت کم شدن بهره‌وری کل سیستم.
- **کامل بودن:** اتریوم باید یک زبان turing-complete داشته باشد و پیاده‌سازی هر مدلی ریاضی در آن ممکن باشد.
- **بخش‌پذیری**^۴: قسمت‌های اتریوم باید مجزا بوده و توانایی تعویض الگوریتم‌های و ساختار داده‌های سیستم مانند درخت پاتریشا را، بدون آگاهی دیگر قسمت‌های سیستم از این تغییر، داشته باشند.
- **جابجایی:** جزئیات پروتکل اتریوم باید قابل تغییر باشند.
- **برابری:** سیستم نباید فعالانه جلوی دسته‌ای از کاربردها رو بگیرد یا آن‌ها رو محدود کند.

^۱ Bitcoin

^۲ Blockchain

^۳ Byzantine generals

^۴ Modularity

با یه وجود آمدن اتریوم به عنوان یک بستر کامل، بی اعتماد و توزیع شده برای قراردادهای هوشمند، کاربردهای ذکر شده را می توان به سادگی و با نوشتن چند خط کد پیاده سازی کرد. این سادگی در پیاده سازی باعث جذب بسیاری از توسعه دهندگان می شود و آن ها می توانند کاربردهای جدیدی پیاده سازی کنند و به عنوان یک کارپرداز خودکار در این بستر فعالیت کنند. تغییرناپذیری قراردادهایی که در بستر بلاک چین نوشته می شوند باعث اعتماد مشتریان به آن قرارداد می شود اما 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 اندازه ی ۵۰ میلیون دلار اتر از یک سازمان کرودفاندینگ در اثر یک باگ امنیتی از یک قرارداد آن ها دزدیده شد^۱. با توجه به تغییر ناپذیر بودن بلاک چین هیچ راهی جز تغییر پروتکل برای بازگرداندن پول وجود نداشت. 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، دسته ی اول کسانی که از بازگردانده شدن پول به سازمان حمایت می کردند و بلاک چین جدید رو به عنوان بلاک چین اصلی اتریوم پذیرفتند و دسته ی دوم با این استدلال که قانون اتریوم کد قراردادهاست و مبلغ قرارداد درست به هکرها تعلق می گیرد، بلاک چین جدید را قبول نکرده و به روش قبلی ادامه دادند. از نمونه های دیگر این مسئله می توان به قفل شدن ۳۰۰ میلیون دلار^۳ اتر متعلق به شرکت parity در نوایر ۲۰۱۷ اشاره کرد.

لازم به ذکر است که هیچ کدام از مشکلات امنیتی نام برده شده مشکل خود بستر اتریوم نبوده و مشکل اصلی استفاده ی اشتباه از زبان برنامه نویسی آن و قابلیت های آن ها بوده است. با وجود این توجه به مسائل امنیتی در این بستر جدید و نا آشنا با توجه به طرز تفکر متفاوت از برنامه نویسی عادی بسیار اهمیت دارد.

در ادامه ی این تحقیق به بررسی دقیق تر بعضی از این مشکلات امنیتی خواهیم پرداخت.

مسئله ی مهم در زمینه ی قراردادهای هوشمند اتریوم، کاربردهای ممکن و یا مناسب این بستر است که از جمله موارد برجسته می توان به کاربردهای زیر اشاره کرد:

- ارزهای جدید

- سیستم های هویت

^۱ <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/>

^۲ Hard fork

^۳ <https://hackernoon.com/how-ethereum-lost-300-million-dollars-bfedf7ba0c19>

- فایل سیستم‌های توزیع شده

- سازمان‌های خودکار توزیع شده

در ادامه‌ی این تحقیق ابتدا در فصل دوم به تعریف مفاهیم به کار برده شده می پردازیم، سپس در فصل سوم

کارهای پیشین را بررسی کرده و در فصل چهارم مسئله‌ی پیشنهادی را مطرح خواهیم کرد.

فصل ۲

تعريف مفاهيم

در این بخش به تعریف مفاهیم به کار برده شده در این تحقیق می پردازیم:

- **بلاک چین:** بلاک چین ساختار داده ای است متشکل از بلوک های متوالی که هر یک هشی از بلوک قبلی اش را شامل می شود. در نتیجه برای ساختاری درست، باید با تغییر یک بلوک، تمام بلوک های بعد از آن را نیز تغییر داد.

- **اثبات کار^۱:** روش اثبات کار بر اساس hashcash [۳] -یک روش برای جلوگیری از حملات DDoS طراحی شده است- ساخته شده است. روش کار hashcash بدین صورت است:

برای این که یک ایمیل توسط سرور ارسال شود، همراه متن ایمیل کلاینت باید رشته ای ارسال کند تا اگر هش SHA-1 از آن گرفته شود ۲۰ بیت اول آن صفر شوند. به دلیلی تصادفی بودن هش رشته، باید با امتحان کردن رشته های مختلف به یک رشته ی مناسب رسید. زمان حل این مسئله برای کامپیوترهای 1 GHZ حدود یک ثانیه و برای بررسی درست بودن آن هش تنها ۲ میکروثانیه است.

زمان یک ثانیه ای برای کاربر عادی که قصد ارسال یک ایمیل را دارد، قابل قبول است اما برای مهاجمی که قصد spam کردن توسط این سرویس را داشته باشد، یک ثانیه در ازای هر ایمیل هزینه ی زیادی خواهد بود.

در بستر بیت کوین از این روش برای توافق بر بلوک های بعدی بلاک چین به صورت زیر استفاده می شود:

هر بلوک جدید شامل تعدادی تراکنش، برای ثبت در بلاک چین است تا توسط ماینرها به یک بلوک تبدیل شود. اما برای پذیرفته شدن این بلوک توسط دیگر ماینرها، باید در این بلاک یک nounce قرار گیرد به صورتی که هش بلاک از عددی که توسط پروتکل بیت کوین انتخاب می شود کمتر باشد. این شرط در طول زمان به صورت خودکار به روزرسانی می شود به طوری که در هر لحظه به صورت میانگین اضافه کردن یک بلوک ۱۰ دقیقه از کل شبکه زمان ببرد. از آنجایی که تنها راه یافتن همچین رشته ای بروت فورس^۲ است، توان محاسباتی بالاتر احتمال یافتن بلوک بعدی را افزایش خواهد داد.

¹ Proof of work

² Brute force

• **مسئله‌ی ژنرال‌های بیزنتین:** مسئله‌ی ژنرال‌های بیزنتین یا تحمل خطای بیزنتین مدلی از تحمل خطا در سیستم‌های توزیع شده است که در آن تعدادی ژنرال ارتش با هم به صورت پیام‌های یک به یک صحبت می‌کنند و در ساده‌ترین حالت در مورد حمله یا عقب‌نشینی در یک نبرد تصمیم می‌گیرند. اما تعدادی از آن‌ها خائن بوده و برای توافق غلط جمع تلاش می‌کنند (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 $1 + 3k$ ژنرال، با رای‌گیری می‌توان تا k خائن را تحمل کرد. راه حل خلاقانه‌ی بیت‌کوین برای حل این مسئله استفاده از بلاک‌چین برای ذخیره‌ی اطلاعات و اثبات کار برای اضافه کردن بلوک به بلاک‌چین است.

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

احتمال موفقیت حمله‌ی A مساوی $2^{\left(\frac{A's \text{ computational power}}{\text{Bitcoin network's computational power}}\right)}$ است. اگر توان محاسباتی A از دیگر قسمت‌های شبکه کمتر باشد، این کسر عددی کوچک‌تر از ۰.۵ است. اگر این کار به موقع با موفقیت انجام نشود، سه بلوک عقب می‌افتد و توان فرمول بالا تبدیل به سه می‌شود و احتمال موفقیتش کمتر از پیش می‌شود.

این مسئله مسئله‌ی قمارباز^۱ نام دارد که نشان داده می‌شود در آن در طول زمان احتمال موفقیت مهاجم به صورت نمایی کاهش پیدا می‌کند.

• **انشعاب^۲:** منظور از انشعاب در ارزهای دیجیتال تبدیل یک بلاک‌چین به دو بلاک‌چین است. گاهی برای ساخت ارزهای جدید از بلاک‌چین موجود ارزهای دیگر مثل بیت‌کوین استفاده می‌شود. این کار باعث شروع آسان‌تر و سریع‌تر بلاک‌چین می‌شود. در روال عادی کار بیت‌کوین نیز ممکن است انشعابی رخ

^۱ Gambler's Ruin

^۲ fork

دهد اما هر ماینری که متوجه انشعابی شود به صورت خودکار بلندترین زنجیره را به عنوان زنجیره‌ی درست انتخاب می‌کند. هنگامی که یک انشعاب برای تولید بلاک‌چین جدید انجام گیرد و بلوک‌هایی قبلی آن همچنان درست حساب شوند این انشعاب را انشعاب نرم و مورد قبول سیستم جدید نباشند انشعاب را انشعاب سخت می‌نامیم.

- **ماین کردن:** به عملیات ساختن بلوک‌های جدید بر بلاک‌چین با هدف پیدا کردن بلاک‌های درست و دریافت جایزه‌ی آن‌ها، ماین کردن می‌گوییم.

- **ماینینگ پول:** از آن جای که ماین کردن برای یک نفر با توجه به کم بودن احتمال یافتن بلوک معتبر را زودتر از بقیه‌ی شبکه به صرفه نیست، ماینینگ پول‌ها شکل گرفته‌اند. با تقسیم کردن کار بین چندین ماشین شانس پیدا کردن بلوک معتبر بیشتر شده و جایزه‌ی ماین کردن به نسبت توان محاسباتی بین شرکت‌کنندگان تقسیم می‌شود. برای بدست آوردن توان محاسباتی مصرف شده‌ی هر ماشین 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، مطرح شد. در اولین مثال معروف قراردادهای هوشمند یک وندینگ ماشین^۱ را مثال زد که در ازای سکه‌ی به طور اتوماتیک کالای مورد نظر را به مشتری می‌دهد، همچنین از آنجای که بدون سکه هرگز کالایی نمی‌دهد و صندوق، امنیت سکه‌ها را تا حدودی تأمین 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 بسترهای ارز دیجیتال و راه‌حل‌های جدید مسئله‌ی ژنرال‌های بی‌زنتین بستر مناسبی برای ساخت قراردادهای هوشمند و توزیع شده بدون نیاز به اعتماد به شخص ثالث بوجود آمده است. با وجود این که به کمک زبان اسکریپتینگ بیت‌کوین می‌توان مدل‌های مختلفی از قراردادهای هوشمند را تولید کرد، با اتریوم به کمک زبان برنامه‌نویسی turing-complete آن در تئوری می‌توان هر قرارداد هوشمند ممکن را تولید کرد.

^۱ vending machine

فصل ۳

مروری بر پژوهش‌های مرتبط

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

۱.۳ امنیت بلاک‌چین و ماین کردن

در روش امنیتی بیت‌کوین که از طریق حل یک مسئله‌ی سخت محاسباتی ثابت بلاک‌های جدید به بلاک‌چین اضافه می‌شوند چند مسئله‌ی امنیتی رخ می‌دهد؛ نخست به دلیل این که عملیات ماین کردن نیازی به تمام بلاک‌چین ندارد و افراد می‌توانند کار را تقسیم کنند احتمال بوجود آمدن یک ماینینگ پول که بیش از پنجاه درصد توان محاسباتی را داشته باشد بالا می‌رود. بعضی پژوهش‌ها در این زمینه برای تولید مسائل مناسب برای اثبات کار، که در عین حال قابل تقسیم و موازی انجام شدن هم باشند، انجام شده است.

مورد دیگر، بوجود آمدن سخت‌افزارهای مخصوص این مسئله است که باعث می‌شود عملیات ماین کردن از یک عملیات توزیع شده که تمام افراد در آن شرکت می‌کنند به عملیاتی که به سرمایه‌ی اولیه زیاد نیاز دارد، تبدیل شود. امنیت بیت‌کوین در گرو این موضوع است که به نفع تمامی ماینرهاست که پروتکل را رعایت کنند اما در این تحقیق [۵] نشان داده شده که این گزاره همواره درست نیست و در بعضی شرایط به نفع ماینینگ پول‌هاست که از توان مصرفی خود در یک ماینینگ پول رقیب استفاده کنند و اگر هش درست را برای رقیب پیدا کردند آن را اعلام نکنند [۶].

تحقیق دیگر [۷] نشان داد در شرایطی برای به نفع ماینینگ پول‌هاست که اگر هش درست را پیدا کردند به دیگران اعلام نکنند تا برای بلوک بعدی به دلیل زودتر شروع کردن شانس بیشتری داشته باشند.

با توجه به این شرایط و همچنین هزینه‌ی محاسباتی بالایی که ماین کردن 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^۱: به این صورت است که هر ماین‌کننده‌ای که سهم بیشتری در سکه‌های بستر داشته باشد،

^۱ proof of stake

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

- **اثبات سن سکه^۱:** 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^۲:** در این روش برای ساخت بلوک جدید باید مقداری سکه توسط ماین‌کننده در یک حساب برای مدت زمانی قفل شوند.

- **اثبات سوزاندن^۳:** در این روش برای ساخت بلوک باید مقداری سکه را به حسابی غیرقابل دسترس (مثلاً حسابی با کلید عمومی تماماً صفر) منتقل کرد.

- **اثبات فعالیت^۴:** در این روش تعدادی کاربر در هر مرحله به صورت تصادفی برای اضافه کردن 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 وجود آمدن طبیعی کاربرهای قابل اعتماد و ساخت لایه‌هایی از اعتماد که بی‌شباهت به لایه‌های ISP نیست، برای انتخاب بلوک بعدی تصمیم می‌گیرند. همچنین هر کاربر خود انتخاب می‌کند که چه افرادی در مورد درستی تراکنش او تصمیم بگیرند.

۲.۳ امنیت قراردادهای اتریوم

بدیهی است که با وجود آمدن ارزهای دیجیتال مانند بیت‌کوین و تراکنش‌های نیمه‌ناشناس در آن‌ها بستری مناسبی برای تراکنش‌های غیرقانونی و مجرمانه وجود 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]

^۱ proof of coin-age

^۲ proof of deposit

^۳ proof of burn

^۴ 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 [۱۲] و بستر HAWK [۱۳] و یا E. Heilman در مقاله‌ی [۱۴] به بررسی روش‌های تولید تراکنش‌های کاملاً 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 ۲۰۱۵^۱ 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 متحده آمریکا قراردادی برای ساخت یک سیستم رای‌گیری بر روی بستر اتریوم امضا کردند.^۲ این پتانسیل تکنولوژی بلاک‌چین در زمینه‌ی رای‌گیری باعث تولید چند نمونه [۱۵] از سیستم‌های رای‌گیری بر بستر بلاک‌چین نیز شده که از آن‌ها می‌توان به VoteBook [۱۶] توسط شرکت Kaspersky که یک شرکت پیشرو در 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. نحوه‌ی کار این سیستم با سیستم VoteBook تفاوت اساسی دارد و برای رای‌دادن احتیاج دارد که نرم‌افزاری برای رای‌دادن به روی کامپیوتر و یا تلفن همراه 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 صد هزار رای در بیشتر از ۲۰ رای‌گیری مختلف توسط این سیستم شمارش شده است.

^۱ <https://www.brennancenter.org/publication/americas-voting-machines-risk>

^۲ <http://www.coinfox.info/news/4794-ukraine-to-introduce-ethereum-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 پشتیبانی 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 جمع کردن 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 cryptocurrencies," *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] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zero-cash : Decentralized anonymous payments from bitcoin," *2014 IEEE Symposium on Security and Privacy*, pp.459-474, 2014.
- [13] "Hawk : The blockchain model of cryptography and privacy-preserving smart contracts," *IEEE Symposium on Security and Privacy*, pp.839-858, 2016.
- [14] E. Heilman, foteini Baldimtsi, and S. Goldberg, "Blindly signed contracts : Anonymous on-blockchain and o -blockchain bitcoin transactions," *Financial Cryptography and Data Security*, 2016.
- [15] R. Osgood, "The future of democracy : Blockchain voting," *COMP116: Information Security*, 2016.
- [16] 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:

Since Bitcoin's wide adaption in 2009 there has been a abundance of trustless applications based of Bitcoin's use of blockchain technology and after the release of Ethereum's smart contract platform we are seeing more and more usages of smart contracts. With this increase in usage of these platforms we on must be mindful of the security implications of these platforms.

In This research we first review the basics of digital currencies and their underlying technologies and then review the security considerations of their platforms and the applications based on them and finally move to voting as a usecase of these platforms and consider the challenges we face while implementing such a system.

Keywords: Blockchain, Ethereum, Security, Smart Contracts, 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. Maghsoud Abbaspour

2018