دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

ارائه‌ی یک روش رای‌گیری امن مبتنی بر بلاک‌چین

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر
گرایش نرم‌افزار

نگارش

شروین حاجی‌اسمعیلی

استاد راهنما

دکتر مقصود عباس‌پور

تابستان ۹۷

دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر - گرایش نرم‌افزار

تحت عنوان:

ارائه‌ی یک روش رای‌گیری امن مبتنی بر بلاک‌چین

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: ارائه‌ی یک روش رای‌گیری امن مبتنی بر بلاک‌چین

استاد راهنما: دکتر مقصود عباس‌پور

اینجانب شروین حاجی‌اسمعیلی تهیه‌کننده پایان‌نامه 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

فهرست تصاویر

فهرست جداول

چکیده

از سال ۲۰۰۹ تاکنون، با فراگیری بیت‌کوین شاهد افزایش کاربردهای بلاک‌چین و سیستم‌های توزیع‌شده و بدون نیاز به اعتماد بوده‌ایم. بعد از انتشار بستر اتریوم تا به امروز قراردادهای هوشمند توزیع‌شده 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 بلاک‌چین بررسی کنیم.

در این تحقیق ابتدا به معرفی ارزهای 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: بلاک‌جین، اتریوم، امنیت، قرارداد هوشمند، رای‌گیری

فصل ۱

مقدمه

امروزه از روش‌های متعددی برای رای‌گیری استفاده می‌شود. رای‌گیری سنتی به کمک صندوق‌های رای و برگه رای‌های کاغذی انجام می‌شود. با توجه به سختی استفاده از این روش در انتخابات‌های بزرگ، فعالیت‌های زیادی در راستای رای‌گیری الکترونیک انجام شده است. اولین سیستم رای‌گیری الکترونیک در سال ۱۹۶۰ طراحی شده است و اولین استفاده بزرگ از آن‌ها در چند ایالت آمریکا در سال ۱۹۶۴ برای انتخابات ریاست جمهوری بود.

امنیت در رای‌گیری همواره یک مسئله‌ی پیچیده بوده است که در سیستم‌های سنتی به کمک بررسی‌های انسانی و اعتماد به برگزارکننده تامین می‌شده ولی به کمک رمزنگاری در رای‌گیری الکترونیک می‌توانیم نیاز به شخص معتمد در رای‌گیری را کمرنگ کنیم. هدف نهایی ما در این تحقیق ارائه‌ی یک روش رای‌گیری امن بدون نیاز به اعتماد به شخص ثالث است.

۱.۱ نیازمندی‌های رای‌گیری ایده‌آل

یک فرایند رای‌گیری ایده‌آل باید بتواند شروط زیر را بدون نیاز به اعتماد به شخص ثالث ارضا کند:

- هر فرد واجد شرایط دقیقا یک بار بتواند رای دهد.
- هیچ کسی نتواند به جای فرد دیگری رای دهد.
- هیچ فردی مجبور به رای دادن نشود.
- هیچ فردی مجبور به رای دادن به کاندیدای خاصی نشود.
- از شمارش هر رای اطمینان حاصل شود.
- نتیجه‌ی آرا ناشناس باقی بماند.
- بسته به نیاز بتوان نتایج لحظه‌ای انتخابات را (بدون آسیب به شرط‌های قبلی) دید.

۲.۱ سیستم‌های رای‌گیری سنتی

در رای‌گیری سنتی فرد برای رای‌دادن به یکی از حوزه‌های رای‌گیری مراجعه کرده و با ارائه‌ی مدارک شناسایی خود یک برگه‌ی رای دریافت می‌کند. برگه رای دارای دو بخش است: قسمتی که برای ردیابی با اطلاعات شخصی فرد پر می‌شود و یک قسمت بی‌نام که فرد کاندیدای مورد نظر خود را در آن ثبت کرده و در یک صندوق می‌اندازد. با بررسی مدارک شناسایی، شرط دوم فرایند رای‌گیری ایده‌آل تایید شده و با ثبت شدن اطلاعات فرد به عنوان یک رای‌دهنده از رای دادن دوباره‌ی او جلوگیری می‌شود. امنیت شخصی افراد در حوزه توسط برگزارکننده‌ی انتخابات و پلیس تامین می‌شود و در صورتی که فردی به تحت فشار مجبور به مراجعه به حوزه‌ی رای‌گیری شده باشد می‌تواند با گزینه‌ی «رای سفید» از رای دادن خودداری کند.

با وجود یک صندوق برای چندین رای و نبودن هیچ نشانه‌ی شناسایی در آرا، هیچ راهی برای فهمیدن رای یک فرد خاص - حتی اگر برگه‌های رای به دست رقیب بیفتد - وجود ندارد.

احزار هویت و شمارش رای‌ها به عهده‌ی برگزارکننده‌ی انتخابات است و تنها از طریق یک شخص ثالث برای بازشماری آرا می‌توان از اجرای درست آن‌ها اطمینان حاصل کرد.

با توجه به هزینه‌ی زیاد شمارش در انتخابات‌های بزرگ راهی برای اعلام لحظه‌ای نتایج با هزینه‌ی معقول وجود ندارد.

همانطور که می‌بینیم در روش‌های فعلی انتخابات بسیاری از شرایط مورد نیاز یک انتخابات خوب با هزینه‌ی نسبتا زیاد فراهم می‌شود. از دیگر مشکلات انتخابات به این روش می‌توان به نیازمندی به یک برگزارکننده‌ی مورد اعتماد اشاره کرد. باید به برگزارکننده اعتماد شود تا:

۱. امنیت حوزه‌ی انتخابات را تامین کند.

۲. افراد را به درستی احراز هویت کند.

۳. همه‌ی رای‌ها را بشمرد.

۴. تغییری در رای‌ها ندهد.

۳.۱ مشکلات و چالش‌های رای‌گیری الکترونیک

دو مسئله‌ی اساسی در یک سیستم رای‌گیری امنیت و حریم خصوصی است. مخالفین رای‌گیری الکترونیک از کم هزینه بودن تقلب و تغییر رای‌های ثبت شده در انتخابات الکترونیکی می‌گویند و رد کاغذی در یک انتخابات را یک فاکتور مهم برای امنیت آن می‌دانند. هزینه تغییر میلیون‌ها رای در یک سیستم کامپیوتری بسیار پایین‌تر از تولید چند میلیون رای کاغذی تقلبی برای تغییر نتیجه‌ی یک انتخابات است.

بزرگترین مسئله در به‌کارگیری رای‌گیری الکترونیک مسئله‌ی اعتماد به یک سیستم کامپیوتری است. از نظر بسیاری از رای‌دهندگان رای دادن با کامپیوتر شخصی می‌تواند ریسک تغییر رای تا رسیدن آن به سرورهای رای‌گیری ایجاد کند. از طرف دیگر عدم امکان بررسی و تایید انسانی عملیات کامپیوتر، حس امنیت کمتری القا می‌کند.

مسئله‌ی دیگر پرهزینه بودن ساخت زیرساخت‌های رای‌گیری الکترونیک و خطر پیدایش مشکلات امنیتی در هر سیستم کامپیوتری - چه از نظر نرم‌افزار و چه سخت‌افزار - است. این مشکل باعث شده تعدادی از کشورها از جمله هلند، ایرلند و آلمان فرایند ایجاد زیرساخت لازم را شروع کرده و در ادامه این فرایند را ملقی کنند. دلیل اصلی اعلام شده برای این مسائل قابل اتکا نبودن سیستم‌های رای‌گیری الکترونیکی اعلام شده است.

برای مثال 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 و به دلیل نداشتن بودجه‌ی کافی برای تعمیرات و بروزرسانی، در معرض خطر کرش [2] کردن هستند که می‌تواند باعث کندی فرایند و حتی گاها از دست رفتن رای‌های مردم شود. علاوه بر این، قدیمی بودن دستگاه‌ها می‌تواند ریسک‌های امنیتی ایجاد کند.

یک مشکل دیگر در پیاده‌سازی‌های بسیاری از رای‌گیری الکترونیک، نیاز به اینترنت و توانایی استفاده از کامپیوتر است. این مسئله می‌تواند دسترسی بسیاری از افرادی واجد شرایط را - به دلیل نقص جسمی و یا عدم توانایی کار با کامپیوتر - محدود کند. در سیستم‌های فعلی که مبتنی بر حوزه‌های رای‌گیری هستند می‌توانند با

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

[2] crash

کمک انسانی در خود حوزه تا حدی این مشکلات را رفع کنند.

مشکلات مطرح شده موانع بزرگی برای فراگیری سیستم‌های رای‌گیری کاملا الکترونیکی برای انتخابات‌های مهم و بزرگ هستند که یک سیستم رای‌گیری مناسب باید آن‌ها را تا جای ممکن رفع کند.

۴.۱ انگیزه و هدف

هدف این تحقیق، طراجی یک سیستم رای‌گیری الکترونیک است که شرایط رای‌گیری ایده‌آل را تا جای ممکن بدون نیاز به اعتماد به شخص ثالث ایفا کند. با فراگیری تکنولوژی زنجیره‌ی قالبی برای ایجاد سیستم‌های توزیع شده بدون نیاز به اعتماد (برای مثال بیت‌کوین به عنوان یک ارز دیجیتال بدون نیاز به اعتماد)، پلتفرم‌هایی برای رای‌گیری الکترونیک ایجاد شدند که امنیت شمارش آرا را با عمومی ساختن فرایند رای‌گیری تامین می‌کردند.
با وجودی که راه‌حل ارائه شده‌ی این سیستم‌ها مسئله‌ی اطمینان از شمارش رای‌ها را حل می‌کرد، مسئله‌ی حریم شخصی در این روش‌ها حل نشده است و انتخابات‌های برگزار شده با این سیستم‌ها امنتیت کمتری در قبال ناشناس ماندن رای‌ها ارائه می‌کنند.

برای مثال حالتی را فرض کنید که یک رای‌دهنده تهدید می‌شود که باید به یک کاندیدای خاص رای بدهد، در سیستم‌های سنتی رای‌گیری به دلیل بی‌نام بودن برگه‌های رای بعد از اتمام فرایند رای‌گیری راهی برای اطمینان حاصل کردن از نتیجه‌ی رای فرد نیست. از طرفی به دلیل امنیت حوزه‌های رای‌گیری راهی برای اطمینان از نتیجه‌ی رای یک نفر در حین فرایند رای‌گیری هم نیست. پس راهی برای محبور کردن یک نفر که به یک کاندیدای خاص رای بدهد وجود ندارد. اما در سیستم‌های مبتنی بر زنجیره‌ی قالبی هر رای داده شده به امضای الکترونیکی فرد امضا شده است و این موضوع می‌تواند با عمومی شدن زنجیره‌ی قالبی بعد از رای‌گیری باعث لو رفتن نتیجه‌ی رای آن فرد شود.

این مشکلات مانع بزرگی برای استفاده‌ی فراگیر این سیستم‌ها خواهد بود. هدف ما در این تحقیق ارائه امنیت و هزینه‌ی کم ناشی از استفاده از این روش‌های رای‌گیری، بدون ایجاد ریسک‌های جدید در حریم خصوصی رای‌دهندگان است.

نتیجه‌ی این تحقیق یک سیستم رای‌گیری الکترونیک است که قیاس با سیستم‌های سنتی انتخابات هزینه‌ها

را کاهش خواهد داد. در عین حال کمترین تغییر برای رای‌دهندگان خواهد داشت که باعث افزایش دسترس‌پذیری این سیستم خواهد شد. همچنین تمامی آرا رای‌دهندگان در قبال یک مهاجم خارجی و حتی خود برگزار کننده‌ی انتخابات ناشناس خواهند ماند.

از طرفی این سیستم یک رد الکترونیک غیرقابل انکار از تمام ارا، در قبال یک زنجیره‌ی قالبی، ارائه خواهد کرد که توانایی اثبات درستی شمارش را برای شخص ثالث بدون ایجاد خطری برای ناشناسی رای‌ها خواهد داد.

تمامی این قابلیت‌ها بدون نیاز اعتماد به برگزارکننده‌ی انتخابات خواهد بود و هرگونه تخطی از پروتکل ارائه شده توسط حوزه‌های رای‌گیری قابل ردیابی از طریق اطلاعات ثبت شده در زنجیره‌ی قالبی خواهد بود.

فصل ۲

تعریف مفاهیم

در این بخش به معرفی بعضی مفاهیم پایه برای این تحقیق می‌پردازیم. در ابتدا با مفاهیم زنجیره‌ی قالبی و انواع و کاربردهای آن آشنا می‌شویم و در ادامه به بررسی اثبات‌های بی‌دانش می‌پردازیم. این دو تکنولوژی ابزارهای تئوری لازم برای ساخت سیستم رای‌گیری امن خواهند بود.

۱.۲ زنجیره‌ی قالبی

زنجیره‌ی قالبی ساختمان‌داده‌ایست که به مانند لینک‌لیست [۱] از بلوک‌های متوالی تشکیل شده ولی در زنجیره‌ی قالبی هر بلوک هش [۲] عنصر قبلی خود را نیز نگه‌می‌دارد. هدف از این کار ساخت یک ساختار داده‌ی صرفا افزایشی [۳] است که در آن بلوک‌های قبلی تغییرناپذیرند. تغییر هر بلوک باعث تغییر بلوک بعدی خواهد شد و این موضوع تشخیص تغییر در بلوک‌های پیشین را بسیار ساده می‌کند.

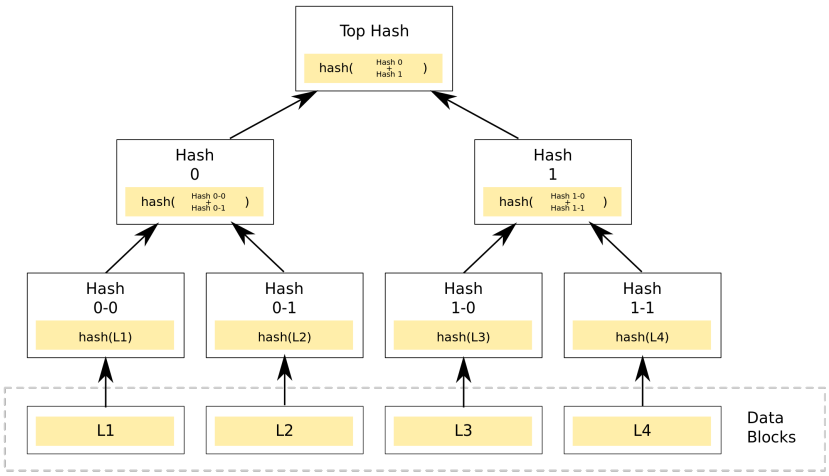
۱.۱.۲ پیاده‌سازی زنجیره‌ی قالبی

برای پیاده‌سازی یک زنجیره‌ی قالبی معمولا از درخت مرکل [۴] استفاده می‌شود. درخت مرکل یا درخت هش، نوعی درخت دودویی [۵] است که در آن هر راس هش فرزندان خود را نگه‌داشته و برگ‌ها هش داده‌ی ذخیره‌شده در خودشان را نگه می‌دارند. این روش نگه‌داری اطلاعات باعث می‌شود که درچه‌ی زمانی بررسی وجود یک بلوک داده در زنجیره‌ی قالبی از N به $\log N$ کاهش یابد. به دلیل این نوع ساختار یک درخت مرکل، هر تغییری در درخت باعث تغییر هش در ریشه‌ی آن خواهد شد و به دلیل رندم بودن خروجی یک هش خوب، هش ریشه‌ی درخت مرکل هیچ ویژگی قابل پیشبینیی ندارد.

۲.۱.۲ انواع زنجیره‌ی قالبی

در این تحقیق زنجیره‌ی قالبی‌ها را از دو نظر دسته‌بندی می‌کنیم. زنجیره‌ی قالبی‌ها می‌توانند عمومی یا خصوصی باشند، در زنجیره‌ی قالبی‌های عمومی اضافه‌کردن بلوک به زنجیره‌ی قالبی دسترسی خاصی نمی‌خواهد

[1] Linked list
[2] Hash
[3] Append only
[4] Merkle tree
[5] Binary tree



شکل ۱.۲: یک درخت مرکل

و هر کسی می‌تواند در آن‌ها بنویسد ولی در زنجیره‌ی قالبی‌های خصوصی اضافه کردن بلوک صرفا توسط افراد خاص ممکن است.

روش دیگر تقسیم‌بندی ما باز یا بسته بودن زنجیره‌ی قالبی است که این دسته‌بندی در مورد دسترسی خواندن اطلاعات از زنجیره‌ی قالبی است. در زنجیره‌ی قالبی‌های بسته خواندن اطلاعات توسط عموم آزاد نیست و در زنجیره‌ی قالبی‌های خصوصی تمام اطلاعات زنجیره‌ی قالبی برای خواندن، در دسترس عموم است.

با توجه به کاربرد زنجیره‌ی قالبی مورد نظر هر زنجیره‌ی قالبی می‌تواند در هر کدام از این دسته‌بندی‌ها قرار بگیرد، جدول ۱.۲ یک کاربرد ممکن برای هر کدام از این دسته‌بندی‌ها را نشان می‌دهد.

جدول ۱.۲: انواع زنجیره‌ی قالبی

	باز	بسته
عمومی	ارزهای دیجیتال	بعضی رای‌گیری‌ها
خصوصی	سامانه‌ی مدیریت اطلاعات مالیات	اطلاعات خصوصی یک شرکت

۲.۲ اثبات‌های بی‌دانش

اثبات بی‌دانش [1] روشی است که یک «اثبات‌کننده» می‌تواند به یک «بررسی‌کننده» نشان دهد که او یک راز - مثلا خروجی یک عملیات کامپیوتری - را می‌داند، بدون این که به بررسی‌کننده هیچ اطلاعات اضافه‌ای، مانند خروجی عملیات، بدهد. به عبارت دیگر اثبات‌های بی‌دانش، صرفا داشتن اطلاعات را اثبات می‌کنند و خود اطلاعات را محفوظ نگه می‌دارند.

یک اثبات بی‌دانش باید ۳ شرط زیر را داشته باشد:

- کامل‌بودن: اگر گزاره‌ی مورد اثبات صحیح باشد، بررسی‌کننده‌ای که پروتکل را رعایت کند، باید از درستی گزاره مطمئن شود.
- درستی: اگر گزاره مورد اثبات غلط باشد، هیچ اثبات‌کننده‌ای نتواند اثباتی ارائه کند که گزاره درست است.
- بی‌دانش: اگر اثبات درست باشد، بررسی کننده هیچ اطلاعاتی فراتر از این که گزاره درست است دریافت نکند.

اثبات‌های بی‌دانش، اثبات‌های احتمالاتی هستند و در واقع احتمال کمی وجود دارد که بتوان یک اثبات نادرست ارائه کرد. به بیان دیگر شرط درستی این است که احتمال تولید یک اثبات نادرست بسیار کم باشد.

۱.۲.۲ مثال شهودی

سناریویی را در نظر می‌گیریم که یک توپ سبز و یک توپ قرمز روی یک میز قرار دارد و آلیس می‌خواهد به باب که کوررنگ سبز و قرمز است ثابت کند که که این دو توپ با هم تفاوت دارند. برای اثبات آلیس چشمش را می‌بندد و باب یا دو توپ را جابجا می‌کند و یا جابجا نمی‌کند. در ادامه آلیس می‌گوید که آیا جای توپ‌ها با هم عوض شده‌اند یا نه. با یک پاسخ درست باب می‌فهمد که آلیس با احتمال ٪۵۰ درست می‌گوید. این فرایند را برای بار دوم نیز تکرار می‌کنند و در صورتی درستی جواب آلیس، باب می‌داند که با احتمال ٪۷۵ آلیس تفاوتی بین دو توپ می‌بیند. این فرایند آنقدر تکرار می‌کنند که باب با احتمال دلخواه خود از ادعای آلیس اطمینان پیدا کند.

[1] Zero knowledge proofs

یک نکته‌ی مهم در مثال بالا این است که حتی اگر باب این فرایند را ضبط کرده باشد، نمی‌تواند به کس دیگری اثبات کند که آلیس تفاوت این دو توپ را می‌داند چون که راهی برای اثبات این که سوال و جواب از قبل هماهنگ نشده بوده است ندارد.

این یکی از نیازمندی‌های بی‌دانش بودن اثبات است. اگر در فرایند برای تصمیم‌گیری در تعویض توپ‌ها باب از شیر یا خط کردن یک سکه استفاده می‌کرد، دیگر این اثبات بی‌دانش نبود، چرا که باب می‌توانست با ضبط کردن این فرایند به یک شخص ثالث اثبات کند که آلیس تفاوت این دو توپ را می‌داند.

برای داشتن شرط بالا یک اثبات بی‌دانش همواره تعامل از سمت بررسی‌کننده نیاز دارد. اما با ریلکس کردن این شرط و استفاده از یک ورودی غیرقابل پیشبینی برای تولید سوال‌های یک اثبات بی‌دانش - مثلا هش ریشه‌ی یک درخت مرکل - می‌توان اثبات‌های بی‌دانش بدون نیاز به تعامل بررسی‌کننده ساخت.

۲.۲.۲ اثبات‌های بی‌دانش بدون تعامل

منظور از اثبات بدون تعامل، اثباتی است که در آن نیازی به فرستادن پیامی از سمت بررسی‌کننده به اثبات‌کننده نباشد. با این روش‌ها اثبات‌کننده می‌تواند اثبات را مستقل از بررسی‌کننده بسازد و ارسال کند، در ادامه‌ی این تحقیق اثبات‌های بی‌دانش و بی‌تعامل را **شاهد** می‌نامیم. در ادامه دو روش تولید یک شاهد بی‌دانش را بررسی می‌کنیم. این روش‌ها می‌توانند برای خروجی هر محاسبات کامپیوتری شاهد ایجاد کنند.

اثبات بی‌دانش ZK-SNARK

یکی از پرکاربردترین روش‌های ایجاد شاهد ZK-SNARK [۱] است. شاهدهای این روش علاوه بر بی‌دانش بودن ویژگی‌های زیر را دارند:

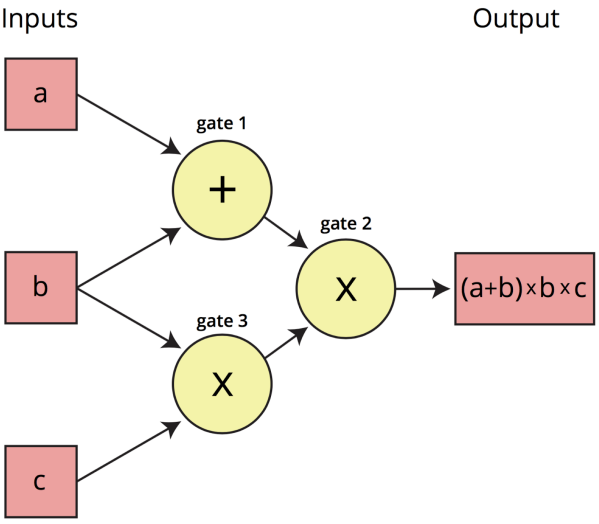
- مختصر [۲] : تولید و بررسی شاهد از انجام خود محاسباتی که اثبات می‌شود کوتاه‌تر (معمولا از مرتبه‌ی زمانی $((\log N)^2)$ است.
- بی‌تعامل [۳] : نیازی به پیامی از بررسی‌کننده برای ایجاد شاهد نیست.

[1] Zero-Knowledge Succint Non-Interactive Argument of Knowlege

[2] Succinct

[3] Non-Interactive

- ادعای دانش [۱] : اثبات ارائه شده در این روش درست [۲] است و نمی‌شود بدون داشتن اطلاعات آن را در زمان محدود ساخت.



شکل ۲.۲: یک نمونه مدار محاسباتی

برای ساختن یک شاهد به این روش ابتدا محاسبات لازم را به یک مدار محاسباتی ریاضی تبدیل می‌کنیم به طوری که اثبات را به عنوان تعدادی شرط روی این مدار نشان دهیم، سپس به کمک یک elliptic curve مقدار مدار را در چند نقطه‌ی تصادفی به عنوان اثبات ارائه می‌کنیم، با صادق بودن شرط‌ها در این نقاط شاهد را بررسی می‌کنیم.

برای انتخاب یکسان این نقاط تصادفی بین اثبات‌کننده و بررسی‌کننده نیاز به تعدادی نقطه‌ی توافق شده روی elliptic curve داریم که باید در قبل از تولید اثبات انتخاب شده باشند. در این فاز آماده‌سازی تعدادی عدد تصادفی برای انتخاب این نقاط تولید می‌شوند که بعد از تولید نقاط باید بلافاصله پاک شوند. کسی که این اعداد (در واقع نقطه‌ی شروع روی منحنی) را داشته باشد می‌تواند شاهدهای تقلبی ایجاد کند. برای تولید شاهد واقعی نیازی به دانستن این نقاط نیست و بنابراین بعد از فاز آماده‌سازی این اعداد باید پاک شوند.

[1] Argument of Knowledge
[2] Sound

اثبات بی‌دانش ZK-STARK

از روش‌های دیگر ایجاد شاهد بی‌دانش روش ZK-STARK [1] [۳۴] است. مهم‌ترین وجه تمایز این روش در مقایسه با ZK-SNARK «شفافیت» [2] است، به این معنی که نیازی به فاز آماده‌سازی ندارد. عدم نیاز به آماده‌سازی و نداشتن زباله‌ی سمی (اطلاعاتی که باید پاک شوند تا امنیت سیستم تامین شود) این روش را برای کاربردهای حساس مناسب‌تر می‌کند اما در ازای این امنیت، حجم شاهدها از چند صد بایت به چند صد هزار بایت تغییر می‌کند.

ار مزیت‌های دیگر این روش استفاده نکردن از Elliptic curveها است. نیازهای کم این روش باعث می‌شود که حتی با کامپیوترهای کوانتمی [3] راهی برای شکستن این اثبات‌ها وجود نداشته باشد.

برای ساختن یک شاهد با این روش، برنامه‌ی مورد نظر را تبدیل به یک چندچمله‌ای درجه بالا می‌کنند، سپس از مقادیر این چندجمله‌ای یک درخت مرکل ساخته می‌شود که مقادیر مختلف خروجی را نشان می‌دهد. سپس بررسی‌کننده چند شاخه از این درخت را به طور تصادفی انتخاب و بررسی می‌کند. برای غیرتعاملی کردن این اثبات می‌توان از هش ریشه‌ی درخت مرکل به عنوان ورودی یه تابع شبه‌تصادفی [4] استفاده می‌شود که مشخص می‌کند خروجی کدام شاخه‌ها باید در شاهد بیاید.

[1] Zero-Knowledge Scalable Transparent ARguments of Knowledge

[2] Transparency

[3] Quantum computers

[4] Pseudo random

فصل ۳

کارهای پیشین

برای ساخت یک رای‌گیری امن

در این بخش ابتدا به بررسی تحقیقاتی می‌پردازیم که به مسئله‌ی حذف اعتماد از سیستم‌های مبتنی بر اعتماد پرداخته‌اند، در ادامه به کارهای مربوط به رای‌گیری الکترونیک و در نهایت به اثبات‌های بی‌دانش می‌پردازیم.

۱.۳ اعتماد

مسئله‌ی حذف نیاز به یک شخص معتمد را از طریق عمومی ساختن کل اطلاعات مورد نیاز می‌توان حل کرد. اگر تمامی اطلاعات شفاف و عمومی باشد هر کسی می‌تواند برای خود درستی تراکنش‌ها را بررسی کند. مسئله‌ای که باقی می‌ماند زمانیست که بین چند شخص اختلاف پیش می‌آید که نسخه‌ی درست اطلاعات کدام است. مثلا زمانی که چند نسخه‌ی صحیح از نظر فرمت وجود دارند اما نتایج مختلفی را می‌رسانند.

۱.۱.۳ توافق

توصیف رسمی این مسئله، مسئله‌ی ژنرال‌های بیزنتین [۱] [۱] است. در این مسئله چند ژنرال که می‌توانند یک به یک با هم صحبت کنند، در تلاشند تا به توافق برسند که آیا باید حمله کنند یا نکنند، تعدادی از ژنرال‌ها خائن هستند و در تلاشند که نتیجه‌ی توافق ژنرال‌ها را تغییر دهند. ژنرال‌های خائن می‌توانند با جواب ندادن یا جواب غلط دادن تلاش کنند که نتیجه‌ی توافق را تغییر دهند. در ساده‌ترین حالت و بدون استفاده از امضاهای دیجیتال ثابت می‌شود که برای $3k+1$ ژنرال، با رای‌گیری می‌توان تا k خائن را تحمل کرد.

راه‌حل‌های متعددی برای توافق [۲] در بستر زنجیره‌ی قالبی داده شده که در ادامه به تعدادی از آن‌های می‌پردازیم.

توافق در ارزهای دیجیتال

روشی که S.Nakomoto [۲] برای رفع این مسئله در بیت‌کوین استفاده کرده است، اثبات کار [۳] نام دارد. این روش که بر پایه‌ی روش استفاده شده در hashcash [۳] است. در این روش برای اضافه شدن هر بلوک به زنجیره‌ی

[1] The Byzantine genarals problem

[2] کار اثبات

[3] Proof of work

قالبی باید یک مسئله‌ی سخت (که نیاز به توان پردازشی بالا دارد) حل شود ولی بررسی درستی جواب ساده است. این روش روش بسیار فراگیری در ارزهای دیجیتال است. از مشکلات این روش می‌توان به توان مصرفی بالا و کندی نسبی آن اشاره کرد. برای مثال حداکثر توان تئوری بیت‌کوین، ۷ تراکنش بر ثانیه است.

اثبات سهم

در روش اثبات سهم [1] [۴] برای ساخت بلوک‌های جدید باید یک فاکتور مقدار سکه‌های در اختیار ماینتر و سن آن‌هاست. به این صورت که می‌تواند در ازای سن سکه‌های در اختیارش (با زدن یه تراکنش به خود) هش ساده‌تری برای بلوک بعدی اعمال کند. مزیت اصلی این روش توان مصرفی پایین‌تر آن به نسبت اثبات کار است. معمولا در زنجیره‌ی قالبی‌ها در بلوک‌های ابتدایی ار روش اثبات کار استفاده می‌شود و بعد از مدتی برای کاهش هزینه‌های اضافه کردن بلوک چدید و مقیاس‌پذیری می‌توان از این روش یا ترکیب این روش‌ها استفاده کرد.

Ripple Consensus Protocol

در این روش [۵] [۶] تعدادی شخص مورد اعتماد وجود دارند که برای اضافه‌شدن بلوک به زنجیره‌ی قالبی باید درصدی از آن‌ها درستی تراکنش را تایید کنند. این اشخاص در دسته‌های مختلف قرار می‌گیرند و برای تایید باید یک زیردسته‌ی کامل تراکنش‌ها را تایید کنند.

با وجود سرعت نسبتا بالای این روش - تا ۱۰۰۰ تراکنش در ثانیه - منتقدین آن از نیاز به اشخاص مورد اعتماد می‌گویند. این روش تا $n/5$ خطا در نودهای مورد اعتماد را می‌تواند تحمل کند.

Stellar Consensus Protocol

روش SCP [۷] مبتنی بر ایجاد افراد مورد اعتماد، به صورت طبیعی و خودجوش، در شبکه است. در این روش با افزایش تراکنش‌های درست توسط هر شخصی، آن شخص به عنوان فرد مورد اعتماد شناخته می‌شود و هر تراکنش را باید تعداد افراد مورد اعتماد تایید کنند. این افراد توسط پرداخت‌کننده‌ی تراکنش انتخاب می‌شوند اما دسته‌بندی آن‌ها در شبکه به گونه‌ای است که خطا در تایید تراکنش باعث حذف شدن فرد از لیست افراد مورد اعتماد شود. تفاوت اصلی این روش با Ripple در توانایی انتخاب تاییدکنندگان تراکنش است و فرض‌های اعتماد

[1] proof of stake

کمتر این روش باعث می‌شود که تا $n/3$ خطا در نودهای مورد اطمینان را بتواند تحمل کند.

۲.۱.۳ کاربردهای زنجیره‌ی قالبی

ارز دیجیتال

اولین کاربرد زنجیره‌ی قالبی، بیت‌کوین بود که با موفقیت آن چندین مجصول دیگر هم تولید شدند. در بستر بیت‌کوین اثبات کار به صورت زیر استفاده می‌شود.:

هر بلوک جدید شامل تعدادی تراکنش، برای ثبت در زنجیره‌ی قالبی است. اما برای پذیرفته شدن این بلوک توسط دیگر دیگران، باید در این بلوک یک رشته‌ي بی‌معنی [۱] قرار گیرد به صورتی که هش بلوک از 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 یک بلوک ۱۰ دقیقه از کل شبکه زمان ببرد. از آنجایی که تنها راه یافتن همچین رشته‌ای بروت‌فورس [۲] است، توان محاسباتی بالاتر احتمال یافتن بلوک بعدی را افزایش خواهد داد.

در پروتکل بیت‌کوین طولانی‌ترین زنجیره‌ی قالبی - یعنی زنجیره‌ی قالبیی که بیشترین توان محاسباتی برای آن صرف شده - به عنوان نسخه‌ی درست در نظر گرفته می‌شود. در نتیجه فرض می‌کنیم شخص A یک بیت‌کوین را به B منتقل کرده، این تراکنش در زنجیره‌ی قالبی ثبت شده و در ازای آن کالایی دریافت کرده‌است، حال قصد دارد این تراکنش را از زنجیره‌ی قالبی 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 $(\frac{A's\ computational\ power}{Bitcoin\ network's\ computational\ power})^2$ است. اگر توان محاسباتی A از دیگر قسمت‌های شبکه کمتر باشد، این کسر عددی کوچک‌تر از 0.5 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 [۳] نام دارد که نشان داده می‌شود در آن در طول زمان احتمال موفقت مهاجم به صورت

[1] Nounce

[2] Bruteforce

[3] Gambler's Ruin

نمایی کاهش پیدا می‌کند.

از پرکاربردترین‌های این محصولات می‌توان به LiteCoin و z-cash [۸] اشاره کرد. مزیت لایت‌کوین نسبت به بیت‌کوین در هزینه‌ی کمتر اضافه کردن بلوک و زمان تراکنش‌های کمتر است و زی‌کش امنیت بیشتری در زمینه‌ی حریم خصوصی و ناشناس ماندن ارائه می‌کند.

از نمونه‌های دیگر می‌توان به Ripple اشاره کرد، که برای تراکنش‌های بانک‌ها طراحی شده و همانطوری که بررسی کردیم از اثبات کار برای توافق استفاده نمی‌کند.

۳.۱.۳ سازمان‌های توزیع‌شده‌ی خودکار

دسته‌ی بعدی کاربردهای زنجیره‌ی قالبی ایجاد سازمان‌های توزیع‌شده‌ی خودکار [۱] است. این مفهوم بر اساس مفهوم قرارداد هوشمند [۲] [۹] ساخته شده است. این سازمان‌ها برنامه‌هایی هستن که به طور خودکار و بی‌اعتماد در بستر زنجیره‌ی قالبی ایجاد می‌شوند و می‌توانند کاربردهای بسیاری داشته باشند. اتریوم [۳] [۱۰] که یک ارز دیجیتال است، یک بستر مناسب برای تولید قراردادهای هوشمند هم هست که در سال‌های اخیر کاربردهای بیشتری پیدا کرده‌اند. با این وجود یک دغدغه‌ای که همچنان در این بستر وجود دارد خطر اشتباه‌های برنامه‌نویسی در این سازمان‌هاست، از آن‌جا که تغییر کد اینگونه سازمان‌ها به دلیل خودکار بودن، همواره قابل تغییر نیست، اشتباهات امنیتی می‌تواند تاثیر مخرب عظیمی داشته باشند. atezi [۱۱] به بررسی مشکلات امنیتی معمول قراردادهای در بستر اتریوم و تله‌ی معمول این زبان برنامه‌نویسی و روش‌های تصحیح آن‌ها پرداخته است.

یک مسئله‌ی دیگر که ناشی از ناشناسی ذاتی این بسترهاست ایجاد شدن سازمان‌های مچرمانه در آن‌هاست. تحقیقات بسیاری [۱۲] [۱۳] در این زمینه شده، و از مثال‌های قراردادهای مخرب ممکن می‌توان به افشای اطلاعات خصوصی و یا حتی دزدین کلیدهای رمزنگاری اشاره کرد. به دلیل عدم وجود نظارت مرکزی در این سیستم‌ها، راهی برای جلوگیری از اینگونه قراردادها وجود ندارد.

[1] Decentralized autonomous organization (DAO)

[2] Smart contract

[3] Ethereum

۴.۱.۳ شناسایی

از کاربردهای دیگر بلاک‌چین ساخت روش‌های شناسایی [۱] است. ویژگی تغییر ناپذیری بلوک‌های قدیمی در یک زنجیره‌ی قالبی، باعث می‌شود که ساختارداده‌ی ایده‌آلی برای شناسایی باشد. از این نمونه کاربردها می‌توان به namecoin اشاره کرد. هدف این محصول کاهش نیاز به اعتماد در DNS [۲] است. این محصول که روی زنجیره‌ی قالبی بیت‌کوین ساخته شده است، در متن نوشته‌شده در تراکنش اطلاعات مربوط به نام دامنه‌ها را زخیره می‌کند.

از تحقیقات دیگر در این زمینه می‌توان به امنیت در داکر [۳] [۱۴] اشاره کرد. در این تحقیق با استفاده از زنجیره‌ی قالبی یک بستر توزیع‌شده برای به اشتراک‌گذاری فایل‌های امضا شده ساخته شده است. در این سیستم می‌توان از یک زنجیره‌ی قالبی خصوصی و یا یه زنجیره‌ی قالبی عمومی استفاده کرد.

۲.۳ رای‌گیری الکترونیک

رای‌گیری الکترونیک را به طور کلی می‌توانیم به دو دسته‌ی رای‌گیری تماما الکترونیک و رای‌گیری به کمک ابزارهای الکترونیکی تقسیم کرد. روش‌های دسته‌ی دوم مبتنی بر رای‌گیری سنتی هستند و از ابزاری‌های الکترونیکی صرفا برای کاهش هزینه و افزایش دسترسی پذیری استفاده می‌کنند. از این روش‌ها می‌توان به ابزارهای شمارش رای خودکار و یا دستگاه‌های ثبت رای‌الکترونیکی که خروجی آن‌ها یک برگه‌ی رای کاغذی [۴] است اشاره کرد. در این تحقیق این ابزارها را بررسی نمی‌کنیم و منظور از رای‌گیری الکترونیک، دسته‌ی اول یا رای‌گیری تماما الکترونیک است.

سیستم‌های رای‌گیری الکترونیک را می‌توان به دو دسته‌ی کلی توزیع‌شده و متمرکز تقسیم کرد. سیستم‌های مرکزی نیازمند یک ارتباط امن از رای‌دهنده تا سرویس مرکزی هستند. همچنین نیازمند اعتماد کامل به همان یک سرویس برای درستی انتخابات است. در سیستم‌های توزیع‌شده تلاش می‌کنند تا این دو مسئله را کمرنگ‌تر کنند.

---

[1] Authentication

[2] Domain Name Service

[3] Docker

[4] Direct-recording electronic voting systems or DRE

۱.۲.۳ رای‌گیری الکترونیک متمرکز

در این سیستم‌ها یک سامانه‌ی مرکزی وجود دارد که تمامی آرا در آن زخیره می‌شند. در این سیستم‌ها حوزه‌های رای‌گیری می‌توانند وجود داشته باشند اما حوزه‌ها صرفا وظیفه‌ی احراز هویت و ارائه‌ی درگاه امن برای ثبت رای در سامانه‌ی مرکزی را دارند. حریم خصوصی کاربران در این سیستم‌ها مبتی بر استفاده از کانال‌های ارتباطی ناشناس [1] بین حوزه‌های رای‌گیری و سامانه‌ی مرکزی است.

اولین تحقیق در رابطه با استفاده از کانال‌های ارتباطی ناشناس برای رای‌گیری در سال ۱۹۸۵ توسط Chaum [۱۵] بود که در آن برای ساخت کانال‌های ارتباطی ناشناس از امضای کورکورانه [2] [۱۶] برای ایجاد یک ارز دیجیتل استفاده می‌شد. در امضای کورکورانه، برای حفظ حریم خصوصی فردی که باید اطلاعاتی را تایید کند، رمزشده‌ی اطلاعات را امضا می‌کند، به این صورت از اطلاعات پیام باخبر نمی‌شود. اولین تلاش برای ایجاد یک پروتکل رای‌گیری الکترونیک با امضای کورکورانه در سال ۱۹۹۲ [۱۷] بود و در ادامه در سال ۱۹۹۷ [۱۸] نسخه‌ی کامل‌تری از آن ارائه شد. این روش‌ها مبتنی بر وجود یک شمارنده و یک حوزه هستند، حوزه احراز هویت را انجام می‌دهد و برگه رای‌های ناشناس صادر می‌کند و سپس از طریق یک کانال ارتباطی ناشناس رای‌دهنده رای را به شمارنده می‌دهد. از مشکلات این روش می‌توان به نیاز به اعتماد به حوزه اشاره کرد. حوزه می‌تواند که با ارائه رای‌های اشتباه بدون توانایی پیگیری، رای‌گیری را خراب کند، برای حل این مشکل تحقیقاتی [۱۹] در راستای استفاده از چند حوزه انجام شده است. مشکل بزرگ دیگر این روش‌ها [۲۰] سختی ناشناس نگه‌داشتن کانال‌های ارتباطی ناشناس است.

۲.۲.۳ رای‌گیری الکترونیک توزیع‌شده

رای‌گیری الکترونیک توزیع‌شده را به دو دسته‌ی رای‌گیری‌های بدون زنجیره‌ی قالبی و با زنجیره‌ی قالبی عمومی و با زنجیره‌ی قالبی خصوصی تقسیم می‌کنیم. با توجه به این که در رای‌گیری احرازهویت یک مسئله‌ی مهم است همه‌ي این سیستم‌ها از زنجیره‌ی قالبی‌های بسته استفاده می‌کنند.

[1] Anonymous communication channel

[2] Blind signature

رای‌گیری بدون زنجیره‌ی قالبی

بعضی سیستم‌های طراحی شده برای رای‌گیری الکترونیک [۲۱] [۲۲] [۲۳] از روش‌های تقسیم راز [1] استفاده می‌کنند. در این روش‌ها فرایند ثبت رای باید به تایید تعدادی از حوزه‌ها برسد که باعث کاهش نیاز به اعتماد می‌شود. در این روش‌ها می‌توان اثبات کرد که برای ردیابی یک رمز حداقل k حوزه باید تبانی کنند. مشکل بزرگ این روش‌ها وجود نداشتن یک الگوریتم مقیاس‌پذیر برای تقسیم راز است.

روش دیگری که برای رای‌گیری توزیع‌شده استفاده شده است، استفاده از بردار بررسی [2] [۲۴] است. در این روش‌ها بررسی درستی رای‌ها کاملا توزیع‌شده است اما نیاز به ارتباط دو به دوی تمامی رای‌دهنده‌ها دارد که در یک انتخابات واقعی شدنی نیست. ترکیبی از این روش و تقسیم راز باعث ایجاد پروتکل‌هایی [۲۵] [۲۶] شد که با سطح‌بندی حوزه‌ها و تقسیم رای‌ها و مخلوط کردن آن‌ها از حریم خصوصی حمایت می‌کنند. اما این روش‌ها به حوزه‌ها و رای‌دهندگان توانایی بررسی درستی برگه رای‌ها را نمی‌دهد و امکان ایجاد رای‌های اشتباه و جلوگیری از رای‌دادن یک فرد خاص را ایجاد می‌کنند.

رای‌گیری با زنجیره‌ی قالبی عمومی

با فراگیر شدن تکنولوژی زنجیره‌ی قالبی [۲۷] ، محصولاتی در زمینه‌ی رای‌گیری الکترونیک به کمک این تکنولوژی ساخته شدند. تعدادی از این سیستم‌های رای‌گیری در قالب قراردادهای هوشمند ساخته شده‌اند که از آن‌ها می‌توان به وتریم [3] [۲۸] و یا کار E.Yavuz [۲۹] در بستر اتریوم اشاره کرد. مزیت اینجور رای‌گیری‌ها هزینه‌ی اولیه کم استفاده از آن‌هاست، اما همچنان ریسک اشتباه برنامه‌نویسی در این سبک کارها بسیار بالاست. همچنین هزینه اجرای قراردادهای هوشمند به تعداد بالا برای یک رای‌گیری هزینه‌ی بالایی خواهد داشت که در طول زمان باعث افزایش هزینه‌ی رای‌گیری خواهد شد. مسئله‌ی دیگر در بستر اتریوم هم وابستگی سیستم رای‌گیری، به پهنای باند نودهای اتریوم و میزان بار روی شبکه‌ی آن است. این موضوع می‌تواند باعث کند شدن یا حتی در مواردی حذف شدن تعدادی از آرا شود.

---

[1] Secret sharing

[2] Check vector

[3] Votereum

رای‌گیری با زنجیره‌ی قالبی خصوصی

از سیستم‌های رای‌گیری با زنجیره‌ی قالبی خصوصی می‌توان به VoteBook [۳۰] 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 زنجیره‌ی قالبی 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. اینگونه طراحی سیستم، خطرات امنیتی در قالب بدافزار ایجاد می‌کند. همچنین با نبود یک حوزه‌ی رای‌گیری امن راهی برای تامین امنیت رای‌دهندگان و اطمینان حاصل کردن از این که کسی مجبور به رای دادن نشده، نیست.
یکی از موفق‌ترین سیستم‌های رای‌گیری مبتنی بر زنجیره‌ی قالبی 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 زنجیره‌ی قالبی است. طبق وب‌سایت این محصول تاکنون بیش از صدهزار رای در بیشتر از ۲۰ رای‌گیری مختلف توسط این سیستم شمارش شده‌است.
مدل اسفاده‌ی VoteWatcher به سیستم VoteBook بسیار شبیه است و تفاوت رفتاری زیادی با مدل‌های رای‌گیری الکترونیکی فعلی برای کاربران ندارد. در این محصول طبق نیاز رای‌گیری می‌توان از یک زنجیره‌ی قالبی عمومی یا خصوصی استفاده کرد.
از موارد دیگر می‌توان به پیاده‌سازی‌های به کمک قراردادهای هوشمند ولی با استفاده از زنجیره‌ی قالبی خصوصی [۳۱] که توانایی ردگیری بالاتری از پیاده‌سازی‌های دیگر ارائه می‌کنند، اما به دلیل کندی نسبی، نیاز به تقسیم رای‌گیری به چند رای‌گیری کوچک‌تر دارند.

۳.۳ اثبات‌های بی‌دانش

اثبات‌های بی‌دانش اولین بار در سال ۱۹۸۵ [۳۲] به عنوان روشی ساخت یک روش رمزنگاری متقارن با کلید عمومی استفاده شد. با پیشرفت تکنولوژی اثبات‌های بی‌دانش، روش‌های جامع اثبات بی‌دانش مانند ZK-

SNARK[۳۳] و ZK-STARK[۳۴] بوجود آمدند. این روش‌ها توانایی اثبات هر محاسباتی را به صورت بی‌دانش دارند و این موضوع باعث استفاده‌ی آن‌ها در کاربردهای بیشتری شد.

۱.۳.۳ کاربردها

با فراگیری ارزهای دیجیتال، مسئله‌ی حریم خصوصی در آن‌ها پررنگ‌تر شد. در ابتدا یکی از بزرگ‌ترین کاربردهای بیت‌کوین پرداخت‌های مجرمانه بود که ناشناسی نسبی در این بستر باعث می‌شد برای این سبک پرداخت‌ها ایده‌آل باشند. اما به دلیل عمومی بودن زنجیره‌ی قالبی و تمامی تراکنش‌ها در آن دنبال کردن رد پرداخت بسیار ساده است.

برای جلوگیری از این ردگیری در کاربردهای مجرمانه از یک شخص مورد اعتماد برای «مخلوط کردن» سکه‌های افراد استفاده می‌شود. در این روش چندین نفر به یک نفر پرداخت می‌کنند و آن فرد به کلیدهای عمومی که از قبل تعیین شده با سکه‌های جدید پرداخت می‌کند اما در این روش همگی به شخص مخلوط کننده اعتماد می‌کنند که به اندازه پرداخت کند و رد واقعی سکه‌ها را جایی ثبت نکند. این روش برای کاربردهای مجرمانه تا حد بسیار خوبی پاسخگو است اما برای افراد عادی که صرفا دغدغه‌ی حریم خصوصی خود را دارند خطرها و هزینه‌ي این روش معقول نیست، به همین دلیل کارهای مختلفی در زمینه‌ی پرداخت ناشناس انجام شده است.

پرداخت ناشناس

از این تحقیقات می‌توان به بستر HAWK[۳۵] اشاره کرد. در این تحقیق به کمک یک تعریف کلی از زنجیره‌ی قالبی به عنوان سیستمی که همواره در دسترس است و هیچ اطلاعات اشتباه نمی‌پذیرد اما حریم خصوصی را حفظ نمی‌کند یک بستر قرارداد هوشمند ساخته شده است که در آن به ازای کد قرارداد هوشمند، یک کد برای حفظ حریم خصوصی به کمک اثبات‌های بی‌دانش ساخته می‌شود. روش کار این سیستم مبتنی بر ایجاد آدرس‌های مقصد یکتا به ازای هر تراکنش است.

مونرو [1] که یک ارز دیجیتال است که بر اساس الگوریتم Cryptonote [۳۶] کار می‌کند، به مانند HAWK با یکتا سازی آدرس‌های مقصد و امضای حلقه‌ای [2] کار می‌کند. در ادامه این ارز دیجیتال با همین روش مدلی [۳۷] برای

[1] Monero

[2] Ring Signature

مخفی کردن پرداخت‌کننده‌ی سکه نیز ارائه کرد.

از کارهای دیگر در این زمینه می‌توان به zerocoin [۳۸] که روش پرداخت ناشناس بر بستر بیت‌کوین به کمک ZK-SNARK ارائه کرد اشاره کرد. روش استفاده شده در آن با بهبود در ارز دیجیتال z-cash [۸] استفاده شد. این ارز دیجیتال دو مدل سکه‌ی قابل ردگیری و غیرقابل ردگیری دارد و هر کسی می‌توان طی یک تراکنش سکه‌های خود را به سکه‌های ناشناس تبدیل کند.

.

۲.۳.۳ فاز آماده‌سازی

با توجه به این که ZK-SNARK ها، به طور خاص خاص پروتکل پینوکیو [1] فراگیرترین روش برای ایجاد اثبات‌های بی‌دانش است. تحقیقات زیاد در مورد فاز آماده‌سازی و ایجاد پارامترهای عمومی این مدل اثبات شده است. همانطور که قبلا اشاره کردیم ورودی‌های این فاز اگر بعد از این فاز پاک نشوند می‌توانند برای ایجاد اثبات‌های تقلبی استفاده شوند.

از این تحقیق‌ها می‌توان به روش‌هایی [۳۹] [۴۰] که تلاش در کاهش نیاز به اعتماد در این فاز می‌کنند اشاره کرد. این روش‌ها باعث می‌شوند که برای لو رفت اطلاعات خطرناک احتیاج به تبانی تمامی اعضای موجود در فاز آماده‌سازی باشد.

از دیگر کارهای در این زمینه می‌توان به تلاش‌هایی برای حذف فاز آماده‌سازی به طور کلی اشاره کرد. این روش با تغییر اساسی در پروتکل و استفاده از چندجمله‌ای‌ها [۴۱] مرحله‌ي آماده‌سازی را حذف می‌کند

[1] Pinocchio

فصل ۴

روش پیشنهادی

در این بخش به بررسی روش پیشنهادی این تحقیق می‌پردازیم، در ابتدا شرایطی که در آن مسئله را حل کنیم بررسی می‌کنیم و شرط‌های لازم برای سیستم رای‌گیری خود را بررسی می‌کنیم، در ادامه به بررسی کلی روش رای‌گیری عناصر حاضر در آن می‌پردازیم و در نهایت الگوریتم‌ها و پروتکل دقیق را بررسی می‌کنیم.

۱.۴ تعریف نقش‌ها

در این بخش نقش‌های حاضر در سیستم رای‌گیری و انتظارات خود از آن‌ها را تعریف می‌کنیم:

- **ناظر انتخابات:** این سازمان مسئول بررسی درستی انتخابات و احراز هویت شرکت‌کنندگان در انتخابات است. به این سازمان اعتماد می‌شود تا کار احراز هویت را به درستی انجام دهد. همچنین این سازمان بررسی‌کننده‌ی نهایی درست بودن انتخابات است و باید بتواند از درستی انتخابات اطمینان حاصل کند.
- **رای‌دهنده:** فردی که حق رای به یک کاندیدا را دارد، این فرد می‌تواند از رایش استفاده بکند یا نکند، می‌تواند تلاش کند که چند بار رای‌دهد. باید بتواند از درستی انتخابات اطمینان حاصل کند. ممکن است توسط یک رقیب بدخواه برای رای‌دادن تحت فشار قرار بگیرد.
- **حوزه‌ی انتخابات:** محلی که در آن رای داده می‌شود، باید بتواند امنیت فیزیکی افراد را تامین کند. ممکن است برای خراب کردن انتخابات یا نقض حریم خصوصی کاربران تلاش کند.

۲.۴ شرایط مسئله‌ی رای‌گیری الکترونیکی

شروط لازم برای سیستم رای‌گیری ارائه شده عبارتند از:

۱. هر فرد واجد شرایط دقیقا یک بار بتواند رای دهد.

۲. هیچ کسی نتواند به جای فرد دیگری رای دهد.

۳. هیچ فردی مجبور به رای دادن نشود.

۴. هیچ فردی مجبور به رای دادن به کاندیدای خاصی نشود.

۵. در صورت نقض حریم خصوصی و یا شمرده نشدن بعضی رای‌ها ناظر انتخابات بتواند حوزه‌ي متخلف را شناسایی کند. حوزه‌ها به دلیل در اختیار داشتن سامانه‌های کامپیوتری رای‌گیری همواره می‌توانند با روش‌های phishing و یا استفاده از بدافزارها حریم خصوصی کاربر را زیر سوال ببرند یا رای او را ثبت نکنند. به همین دلیل قابل پیگیری بودن تخلفات حوزه‌ها یکی از مهم‌ترین شرایط یک انتخابات درست است. در صورت خطای حوزه، حوزه‌ی خطاکار باید مشخص شود.

۶. هر رای‌دهنده بتواند به کمک ابزارهای رمزنگاری اطمینان حاصل کند که رای او شمرده شده است. این شرط به این معنی است که هر کاربری که دانش کافی داشته باشد باید بتواند از درستی انتخابات - بدون نیاز به اعتماد به حوزه یا حتی ناظر انتخابات - اطمینان حاصل کند.

۷. رای‌دهنده نیازی به دانش یا توانایی خاصی برای رای‌دادن نداشته باشد. این نیازمندی برای دسترس‌پذیر نگه‌داشتن انتخابات لازم است.

۸. سیستم رای‌گیری نسبت به روش‌های فعلی رای‌گیری از دید کاربر تفاوت چندانی نداشته باشد. هر تغییر اساسی از نگاه رای‌هنده باعث سختی نسبی انتخابات خواهد شد و هزینه‌ی اولیه استفاده از این سیستم انتخاباتی را به شدت افزایش خواهد داد.

۹. بتوان نتایج انتخابات را در بازه‌های زمانی معین دید. هر سیستم انتخاباتی که نتایج لحظه‌ای نشان دهد همواره در خطر حمله‌های مبتنی بر زمان در رابطه با حریم خصوصی رای‌دهندگان خواهد بود، به همین منظور نتایج انتخابات را می‌توان در بازه‌های زمانی که حریم خصوصی را به خطر نیندازد نشان داد.

۱۰. بتوان از شمرده شدن تمامی آرا بعد از انتخابات اطمینان حاصل کرد. به دلیل الزام مخفی نگه‌داشتن زمان حدودی ارسال هر رای، نتایج نهایی انتخابات تنها بعد از اتمام رای‌گیری قابل اتکاست.

۳.۴ فرضیات مسئله

در این تحقیق هدف ارائه‌ی یک پروتکل رای‌گیری امن است و در این روش به جزییات پیاده‌سازی و مسائل

مسئله‌ی شناسایی یک مسئله‌ی مهم در هر انتخابات است، با توجه به این که افراد واجد شرایط بسته به هر انتخابات تغییر می‌کنند در این مسئله فرض می‌کنیم که هر رای‌دهنده یک جفت کلید خصوصی و عمومی دارد که قبل از فرایند انتخابات توسط ناظر انتخابات تایید شده است.

وظیفه‌ی حفظ امنیت کلید عمومی و خصوصی هر کاربر به عهده‌ی خود کاربر خواهد بود چرا نشانگر هویت کاربر در سیستم کلید عمومی او خواهد بود. هر چند که برای رای دادن در حوزه اطلاعات شناسایی کاربر با کلید عمومی او تطابق داده خواهد شد.

هر رای‌دهنده برای ثبت رای نیاز به یک دستگاه هوشمند دارد، از آن‌جایی که این دستگاه صرفا برای امضای کورکورانه استفاده می‌شود برای دسترس‌پذیری بالاتر می‌توان این دستگاه را در حوزه ارائه کرد و رای‌دهندگان تنها کلید خصوصی خود را در آن وارد کنند. بدیهیست که انجام این کار نیاز اعتماد به حوزه را بالاتر می‌برد چرا که رای‌دهنده راهی برای اطمینان حاصل کردن از این که دستگاه برنامه‌ی درستی را اجرا می‌کند ندارد.

۴.۴ مثال شهودی

برای بدست آوردن دید کلی در راه‌حل ابتدا یک مثال شهودی از یک مدل رای‌گیری متمرکز را بررسی می‌کنیم، سپس در ادامه از این روش برای ایجاد سیستم توزیع‌شده و الکترونیکی خود استفاده می‌کنیم.

یک رای‌گیری را فرض می‌کنیم که در آن به ازای هر رای‌دهنده یک کاغذ نام رای‌دهنده و یک برگه‌ی رای وجود دارد. همچنین یک صندوق به ازای هر کاندیدا وجود دارد و همه‌ی این اطلاعات در معرض دید عموم هستند.

آلیس برای رای‌دادن یکی از کاندیداها را انتخاب می‌کند، مسئول حوزه یک کاغذ رمز شده که در آن یک شماره‌ی تصادفی r و کاندیدای موردنظر خود، باب، نوشته شده را به آلیس می‌دهد تا امضا کند، آلیس پس از اطمینان حاصل کردن از درستی ثبت کاندیدا (ولی بدون فهمیدن r) آن را امضا می‌کند. ثبت مسئول حوزه این عبارت رمز شده و برگه‌ی رای مربوط به آلیس را به تخته می‌چسباند. این فرایند را ثبت رای می‌نامیم.

در ادامه پس از مدتی مسئول حوزه تخته مراجعه‌ی می‌کند و شاهدی بر تخته ثبت می‌کند که ثابت می‌کند او یک کلید رمزی می‌داند که یکی از کاغذهای روی تخته را باز می‌کند که نتیجه‌ی آن r و باب است. سپس یکی از رای‌های روی تخته را برمی‌دارد و به صندوق باب می‌اندازد. این فرایند را شمارش رای می‌نامیم.

شاهد آلیس در تخته ثبت شده و دیگر نمی‌توان اثباتی ارائه کرد که رای آلیس را دو بار بشمرد، چرا که عدد r آن تکراری خواهد بود.

از طرفی از آن‌جا که مسئول حوزه نشان نداده که کدام عبارت رمز شده به باب رای‌داده، در نتیجه حریم خصوصی آلیس محفوظ می‌ماند.

چون حوزه‌ی انتخابات محل امنی برای رای دادن است راهی برای مجبور کردن آلیس به رای دادن به کاندیدای خاصی نخواهد بود و با اضافه کردن صندوق رای ممتنع می‌توانیم اطمینان حاصل کنیم که کسی آلیس را مجبور به رای‌دادن نیز نکرده است.

۵.۴ فرایند رای‌گیری از نگاه کاربر

یکی از مهم‌ترین قسمت‌های طراحی یک سیستم رای‌گیری تاثیر آن بر رای‌دهنده است چرا که در انتخابات‌های بزرگ هزینه‌ی تغییر رفتار رای‌دهندگان یا سخت‌تر شدن فرایند رای‌گیری به هر نحوی می‌تواند باعث کاهش شرکت رای‌دهندگان و افزایش هزینه‌ی تغییر رای‌گیری شود.

فرایند رای‌گیری را به دو بخش قبل از رای‌گیری و در حوزه‌ی رای‌گیری تقسیم می‌کنیم.

۱.۵.۴ قبل از رای‌گیری

قبل از رای‌گیری هر فرد واجد شرایط باید از یک روش امن از ناظر انتخابات یک جفت کلید عمومی و خصوصی دریافت کند و یا کلید عمومی خود را در سامانه‌ی مربوط ثبت کند. این کلید می‌تواند در قالب یک فایل بر روی یک دستگاه هوشمند - مثلا تلفن همراه یا حتی یک کارت هوشمند - باشد. این مرحله می‌تواند در هر انتخابات تکرار شود یا یک فرایند ابتدایی باشد و برای انتخابات‌های بعدی نیز استفاده شود.

۲.۵.۴ در حوزه‌ی رای‌گیری

در حوزه‌ی رای‌گیری رای‌دهنده پس از ورود کارت شناسایی و کلید عمومی خود را ارائه می‌کند، در صورت تایید اطلاعات کاربر، کاربر با دستگاه هوشمند خود به سیستم حوزه متصل می‌شود و رای خود را از بین کاندیداهای ممکن و یا ممتنع وارد می‌کند و پیام تایید را دریافت می‌کند.

۶.۴ فرایند رای‌گیری از دید حوزه

در این بخش فرایند رای‌گیری را از نگاه حوزه بررسی می‌کنیم، در این بخش صرفا منطق پروتکل را بررسی می‌کنیم و جزییات زنجیره‌ی قالبی و عملیات توزیع شده نمی‌پردازیم.

برای ثبت رای یک نفر در ابتدا آن فرد با کارت شناسایی احراز هویت می‌شود و از طریق ارتباط با ناظر انتخابات درستی کلید عمومی آن فرد بررسی می‌شود. در مرحله‌ی بعدی با ارائه‌ی کلید خصوصی کاربر یک تراکنش ثبت با نتیجه‌ی مورد نظر ایجاد می‌کند و تراکنش ثبت توسط دستگاه هوشمند کاربر کوکورانه امضا می‌شود. در این مرحله تراکنش شمارش نیز ایجاد می‌شود و با تاخیر زمانی در زنجیره‌ی قالبی ذخیره می‌شود.

۱.۶.۴ تراکنش‌ها

در این بخش تراکنش‌ها ثبت و شمارش را تعریف می‌کنیم.

تراکنش ثبت

در تراکنش ثبت یک رای از یک کلید عمومی به دسته‌ی رای‌های منتظر شمارش منتقل می‌شود. هر تراکنش ثبت شامل یک رای و یک رشته [1] رمز شده است که حاوی یک عدد تصادفی s و حساب مقصد d است که با کلید تصادفی k رمزشده است. این عبارت رمزشده رای CM می‌نامیم. سپس CM (نه خود s) در زنجیره‌ی قالبی به همراه رای ثبت می‌شود.

$$CM = enc_k(r, d) \tag{۱.۴}$$

تراکنش شمارش

مدل دیگر تراکنش ممکن تراکنش شمارش است که در آن شاهدی برای شمارش رای ارائه می‌شود. برای این تراکنش رای‌دهنده اثبات بی‌دانشی برای دو موضوع ارائه می‌کند: یک C می‌شناسد به طوری که $C \in$

[1] string

$C_1, C_2, ..., C_n$ و یک رشته‌ای r می‌داند که C را به s و d باز می‌کند. در نتیجه‌ی این اثبات یکی از رای‌های ثبت‌شده به d منتقل می‌شود.

لازم به ذکر است که از آنجایی که در تراکنش شمارش C و r نشان داده نشده‌اند، راهی برای فهمیدن این که رای متعلق به چه کسی است وجود ندارد.

۲.۶.۴ فرایند ثبت رای کاربر

در این بخش پروتکل ثبت رای حوزه را به طور دقیق بررسی می‌کنیم، در این بخش منظور از کاربر دستگاه هوشمند اوست.

۱. کاربر گزینه‌ی مورد نظر خود را انتخاب می‌کند، حوزه به تعداد n تا CM می‌سازد که رای کاربر به کاندیدای مورد نظر را نشان می‌دهند، هر کدام را با یک کلید تصادفی رمز می‌کند و برای تایید به کاربر می‌دهد.

۲. یکی از از عبارات رمزشده به طور تصادفی توسط کاربر CM_c انتخاب می‌شود و به حوزه اعلام می‌شود.

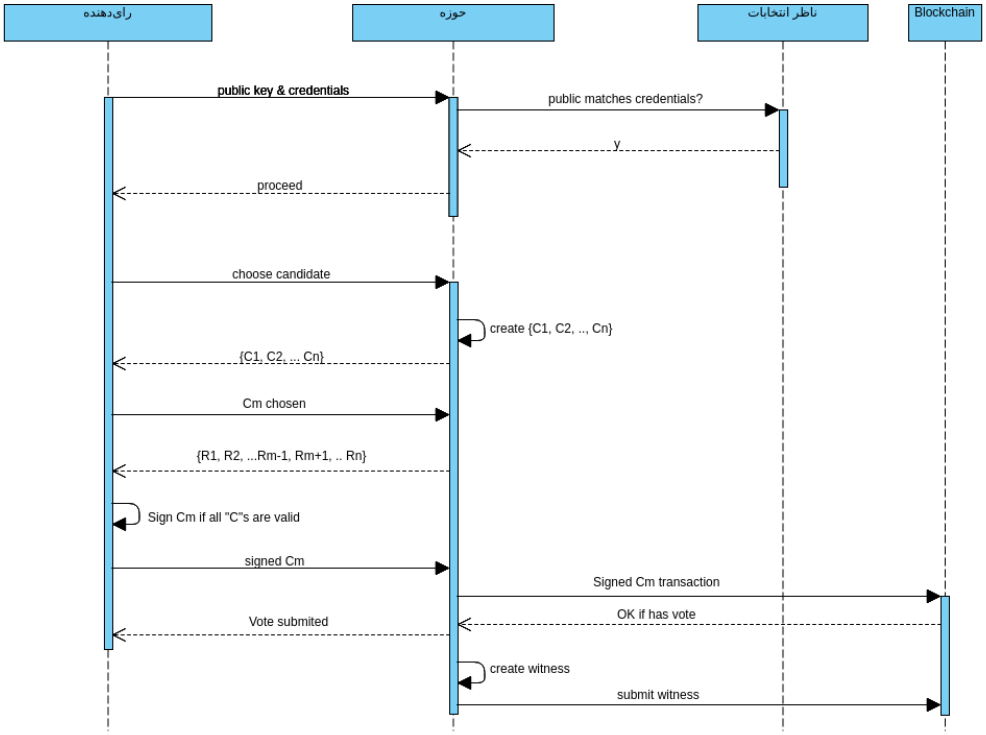
۳. حوزه کلید مربوط به تمامی CMهای دیگر را به کاربر ارائه می‌کند.

۴. کاربر همه‌ی CMها را باز می‌کند و چک می‌کند که در همه‌ی آن‌ها رای به نام کاندیدای مورد نظر او ثبت شده باشند. با این روش کاربر با احتمال $\frac{n-1}{n}$ از درستی رای در CM_c مطمئن می‌شود. سپس کاربر CM_c را با کلید خصوصی خود امضا می‌کند و به حوزه می‌دهد. در نتیجه‌ی این کار کاربر راهی برای فهمیدن عدد تصادفی در CM_c، که آن را s می‌نامیم، ندارد.

۵. حوزه CM_c را به همراه رای موجود در حساب کاربر به عنوان یک تراکنش ثبت در زنجیره‌ی قالبی ذخیره می‌کند. در صورتی که رای کاربر قبلا ثبت شده باشد در این مرحله خطا رخ می‌دهد و رای ثبت نمی‌شود.

۶. حوزه یک شاهد برای شمارش رای کاربر می‌سازد و هر دوی این تراکنش‌ها در بلوک بعدی زنجیره‌ی قالبی ذخیره می‌شوند.

شکل ۱.۴ این توالی فرایند را نشان می‌دهد.

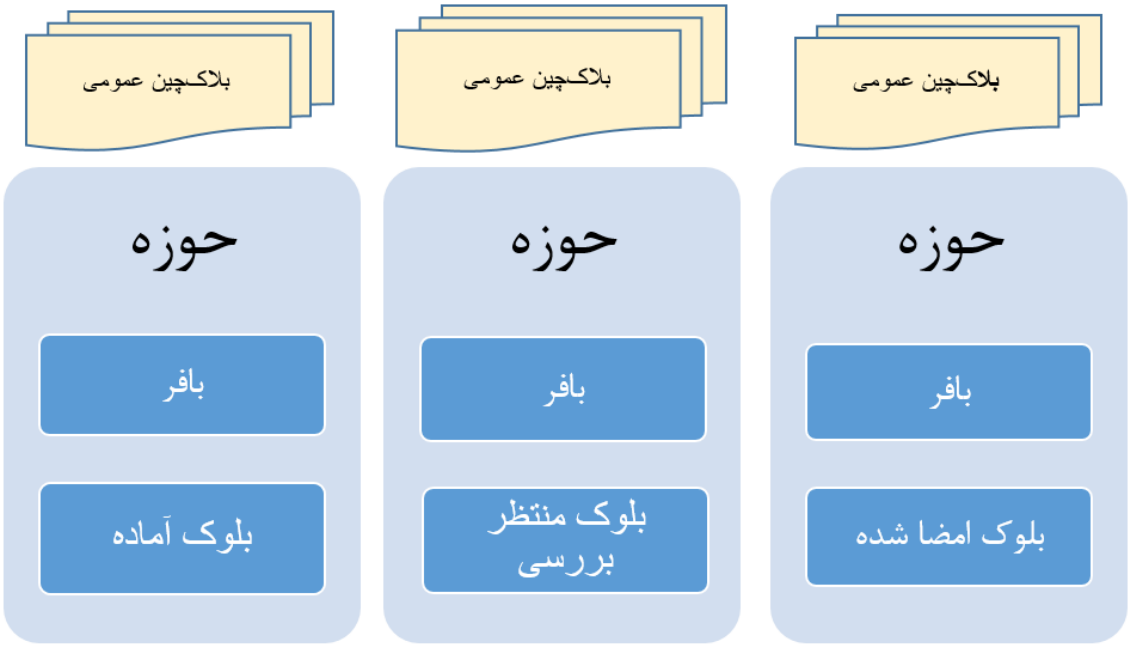


شکل ۱.۴: فرایند ثبت رای در حوزه

۷.۴ شمای کلی

به طور کلی سیستم از تعدادی حوزه تشکیل می‌شود که روی یک زنجیره‌ی قالبی توافق می‌کنند. همچین هر حوزه ممکن است بلوک آماده شده و منتظر گرفتن تایید از بقیه‌ی حوزه‌ها داشته باشد، یا این که بلوکی از حوزه‌ی دیگری گرفته باشد که باید بررسی و امضا کند، شکل ۲.۴ شمای کلی درشت‌دانه‌ی سیستم را نشان می‌دهد.

بلوک ابتدایی این زنجیره‌ی قالبی به ازای هر فرد واجد شرایط یک کلید عمومی و یک رای‌دارد. همچنین یک آدرس خروجی به ازای هر کاندیدا وجود دارد که تعداد رای‌هایی که به آن آدرس فرستاده شده باشند رای‌های آن کاندیداست.



شکل ۲.۴: شمای منطقی سیستم

۱.۷.۴ اضافه شدن بلوک

می‌دانیم که در هر بلوک ثبت‌شده در زنجیره‌ی قالبی تعدادی از دو مدل تراکنش‌های ثبت و شمارش داریم، همچنین هش بلوک قبلی را نیز برای اطمینان از تغییر نکردن بلوک‌های قبلی نگه‌می‌داریم. مسئله‌ای که در اینجا باقی می‌ماند نحوه‌ی توافق روی یک زنجیره‌ی قالبی است. در این تحقیق از یک زنجیره‌ی قالبی عمومی و بسته استفاده می‌کنیم.

هر حوزه یک بافر برای نگه‌داری تراکنش‌های مربوط به آرا دارد که قبل از ثبت در زنجیره‌ی قالبی که آن را تبدیل به یک بلوک می‌کند. برای اضافه شدن هر تراکنش روی زنجیره‌ی قالبی باید حداقل نصف به علاوه‌ی یکی از حوزه‌ها روی آن توافق کنند. هر حوزه برای توافق بررسی می‌کند که که تراکش‌های مربوط به رای دادن و شاهدهای ثبت شده در بلوک جدید درست باشند و هش بلوک قبلی نیز در بلوک صحیح باشد. هر حوزه‌ی زنجیره‌ی قالبی را با امضای دیجیتال خود تایید می‌کند.

۲.۷.۴ مقادیر اولیه برای ZK-SNARK

همانطور که قبلا اشاره کردیم برای استفاده از روش ZK-SNARK برای ایجاد شاهدهای بی‌دانش احتیاج به توافق روی نقاط اولیه‌ای روی یک elliptic curve داریم. برای انجام این کار از روش ارائه شده در تحقیق [۴۰] استفاده می‌کنیم. در این روش برای ایجاد نقاط اولیه از تقسیم مسئله بین افراد توافق‌کننده استفاده می‌شود، به صورتی که حاصل ضرب اطلاعات همه‌ی افراد نقاط اولیه را تشکیل می‌دهند و برای لو رفتن آن باید تمامی حوزه‌ها تبانی کنند. در این روش خود برای ایجاد پارامترها از یک حالت خاص اثبات‌های بی‌دانش استفاده می‌شود.

۳.۷.۴ توافق

در زنجیره‌ی قالبی‌های عمومی معمولا یک مسئله در توافق حالت‌هاییست که زنجیره‌ی قالبی دو شاخه می‌شود، یعنی دو مدل از زنجیره‌ی قالبی وجود داشته باشد که هر کدام را قسمتی از شبکه به عنوان زنجیره‌ی قالبی درست بشناسند. در بسیاری از ارزهای دیجیتال طولانی‌ترین زنجیره‌ی قالبی از نظر تعداد بلوک‌ها همواره به عنوان نسخه‌ی درست شناخته می‌شود اما در یک سیستم رای‌گیری این کار باعث کم شدن رای می‌شود و این ریسک قابل قبولی نیست.

قضیه‌ی CAP

این قضیه‌ی معروف [۴۲] اثبات می‌کند که در یک دیتابیس توزیع‌شده - مانند یک زنجیره‌ی قالبی - در هر بازه‌ای حداکثر می‌توان دو شرط از سه شرط همخوانی [۱] ، دردسترس بودن [۲] و تحمل قسمت‌شدن [۳] را می‌توانند داشته باشند.با توجه به این که هیچ زمانی نمی‌توانیم روی درستی شبکه حساب کنیم سیستم ما در حال CP عمل می‌کند. معمولا در سیستم‌ها مبتنی بر زنجیره‌ی قالبی از روش‌های که گارانتی می‌کنند که همه‌ی نودها در نهایت به همخوانی می‌رسند [۴]. اما در یک سیستمی که برای رای‌گیری استفاده می‌شود این مسئله می‌تواند خطر گم شدن تعدادی از آرا ایجاد کند و این خطر معقولی برای یک سیستم رای‌گیری الکترونیکی نیست.

[1] Consistency
[2] Availability
[3] Partition tolerance
[4] Eventual consistency

در زنجیره‌ی قالبی‌های عمومی معمولا از روش‌های اثبات کار و اثبات سهم استفاده می‌شود که دسترس پذیری و تحمل قسمت‌شدن را به خوبی ارائه می‌کنند اما ممکن است شاخه‌های [1] لحظه‌ای پیش بیاید و چند نسخه از زنجیره‌ی قالبی درست وجود داشته باشد، معمولا در این روش‌ها طولانی‌ترین زنجیره‌ی قالبی نسخه‌ی درست در نظر گرفته می‌شود و زنجیره‌ی قالبی‌های کوتاه‌تر حذف می‌شوند. از آن‌جایی که این کار در سیستم ما باعث از بین رفتن رای می‌شود باید در روش دیگری استفاده کنیم.

در این تحقیق سه روش برای تفاوق را بررسی می‌کنیم. روش اول Aura [۴۳] نام دارد. در این روش نود یک نود رهبر بلوک‌های جدید ارائه می‌کند و در طور زمان در دوره‌های مشخصی رهبر تغییر می‌کند. برای انتخاب زمان تغییر از ساعت unix استفاده می‌شود که می‌تواند در اثر همگام sync نبودن ساعت نودهای حاضر در شبکه در یک لحظه دو رهبر وجود داشته باشد. این باعث از بین رفتن همخوانی در سیستم می‌شود ولی سیستم همواره در دسترس خواهد بود.

روش دیگر Clique [۴۴] نام دارد. این روش شبیه Aura عمل می‌کند با این تفاوت که برای همگامی نودها به جای استفاده از ساعت، از تعداد بلوک ثبت شده در زنجیره‌ی قالبی استفاده می‌شود، همچنین در این روش، نودهایی غیر از نود رهبر نیز می‌توانند بلوک جدید پیشنهاد کنند. این کار می‌تواند باعث ایجاد شاخه در زنجیره‌ی قالبی شود اما در طول زمان با تغییر رهبر یکی از دو شاخه حذف خواهد شد. این روش نیز در نهایت به همخوانی می‌رسد اما ریسک حذف شدن رای را سیستم وارد می‌کند.

راه‌حلی در در پروتکل ارائه شده در این تحقیق برای این موضوع استفاده کردیم PBFT [2] [۴۵] نام دارد. این روش هزینه‌ی محاسباتی بسیار کمتری از روش‌های مبتنی بر اثبات کار دارد و از نظر مقیاس پذیری [۴۶] نیز بسیار بهتر عمل می‌کند.

Practical Byzantine Faul Tolerance

در این روش در ابتدای رای‌گیری حوزه‌ها در یک زنجیره‌ی اولویت چیده می‌شوند و برای ثبت هر بلوک جدید، بلوک آماده‌شده را به رهبر (حوزه‌ای با بیشترین اولیت) داده می‌شود و حوزه آن را به تمامی حوزه‌های دیگر ارسال

[1] fork

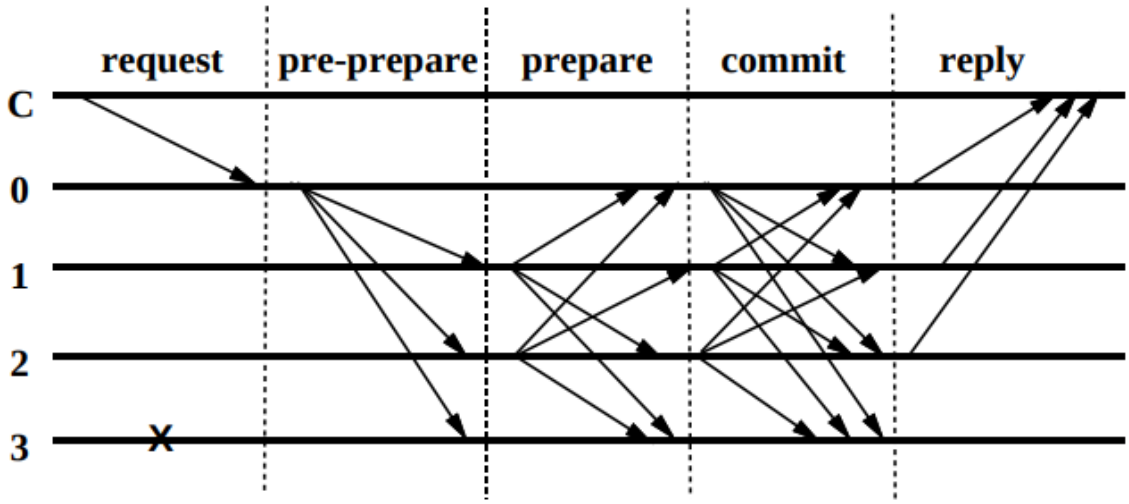
[2] Practical Byzantine fault tolerance

جدول ۱.۴: روش توافق

	هم‌خوانی	دردسترس بودن	تحمل تقسیم شدن
اثبات کار	همخوانی در نهایت	دارد(اما ممکن است بلوک حذف شود)	دارد
اثبات سهم	همخوانی در نهایت	دارد(اما ممکن است بلوک حذف شود)	دارد
Aura	گارانتی نمی‌کند	دارد	دارد
Clique	همخوانی در نهایت	دارد(اما ممکن است بلوک حذف شود)	دارد
PBFT	دارد	در صورت تقسیم شدن ندارد	دارد

می‌کند. سپس تمامی حوزه‌های دیگر بعد از تایید نتیجه را برای هم ارسال می‌کنند و در صورت موفقت آن را ثبت می‌کنند، بعد از تایید نتایج برای حوزه‌ی ابتدایی ارسال شده و ثبت نهایی می‌شود.

همچنین بعد از اضافه شدن هر بلوک حوزه‌ی رهبر تغییر می‌کند و به نفر بعدی در زنجیره‌ی اولیت می‌رسد. همچنین در صورت جواب ندادن حوزه‌ی رهبر در مدت زمان مشخص یا جواب‌های غلط دادن مسئولیت به نفر بعدی منتقل می‌شود.



شکل ۳.۴: روش PBFT

در این روش حداکثر تعداد تعداد حوزه‌ای که باید خطاکار باشند تا بلوک اشتباهی در زنجیره‌ی قالبی ثبت

شود برای $3f + 1$ حوزه f حوزه‌است. این تعداد حوزه‌ی خراب‌کار می‌توانند بلوک‌های اشتباهی ثبت کنند اما به دلیل استفاده از امضای دیجیتال بعد از اتمام رای‌گیری با بررسی درستی بلوک‌های ثبت شده در زنجیره‌ی قالبی بلوک‌های خطا به سادگی قابل شناسایی هستند. در همچین شرایطی چون نمی‌توان از تعداد رای‌دهندگانی که رای آن‌ها ثبت نشده اطمینان پیدا کرد نتایج رای‌گیری باید مردود محسوب شود.

در روش PBFT اثبات می‌شود [۴۷] تا زمانی که کمتر از یک سوم حوزه‌ها خطاکار باشند هیچ زمانی دو نسخه‌ی مستقل از زنجیره‌ی قالبی توسط حوزه‌ها تایید نمی‌شود. به عبارت دیگر این روش به طور کامل هم‌خوانی و توانایی قسمت‌شدن را دارد.

لازم به ذکر است که در این حالت سیستم همواره دردسترس نیست. به این معنی که ممکن است موقعیتی پیش بیاید که یک حوزه به دلیل قطع شدن شبکه از بقیه‌ی حوزه‌ها نتواند بلوک جدید ثبت کند، اما می‌تواند در بافر خود اطلاعات آرا را نگه دارد و زمان اتصال به شبکه بلوک جدید را بسازد و ثبت کند.

فصل ۵

تحلیل و ارزیابی

۱.۵ پیاده سازی

برای ساخت اثبات‌های بی‌دانش از کتاب‌خانه‌ی libsnark[1] استفاده شده است. این کتاب‌خانه از الگوریتم پینوکیو برای ساخت اثبات استفاده می‌کند و توسط Zcash نیز برای ساخت اثبات استفاده شده است. همچنین برای بالا آوردن سیستم از docker استفاده شده است.

در فرایند کامپایل این کتاب‌خانه از تنظیمات زیر استفاده شده است:

جدول ۱.۵: تنظیمات libsnark

نام متغیر	مقدار	توضیحات
CURVE	ALT_BN128	مدل خم مورد استفاده با ۱۲۸ بیت امنیت
MULTICORE	ON	استفاده از چند هسته برای موازی سازی
USE_PT_COMPRESSION	OFF	سرعت بالاتر در ازای حجم شاهدهای بزرگتر
PROFILE_OP_COUNTS	OFF	شمارش تعداد فعالیت روی خم

بقیه‌ی تنظیمات کتاب‌خانه در حالت پیش‌فرض استفاده شده است.

برای زنجیره‌ی قالبی و حوزه‌ها از hyperledger fabric [2] که یک بستر قراردادهای هوشمند است استفاده شده است. hyperledger fabric توسط شرکت IBM طراحی شده و توسط Linux Foundation نگهداری می‌شود. این پروژه یک زنجیره‌ی قالبی خصوصی ارائه می‌کند که قسمت‌های مختلف آن مانند روش توافق به سادگی قابل تغییرند.

۲.۵ مقایسه با کارهای مشابه

در این بخش به مقایسه‌ی روش رای‌گیری ارائه شده با تحقیقات دیگر در این زمینه می‌پردازیم . این مقایسه را از چند جنبه‌ی نحوه‌ی اطمینان از ثبت رای، ناشناسی آرا، سطح اعتماد مورد نیاز و هزینه‌ی انتخابات بررسی

[1] https://github.com/scipr-lab/libsnark

[2] https://www.hyperledger.org/projects/fabric

می‌کنیم.

۱.۲.۵ روش‌های رای‌گیری دیگر

برای مقایسه سیستم‌های رای‌گیری زیر را بررسی می‌کنیم:

- **رای‌گیری سنتی:** این روش به عنوان خط مبنای تحقیق بررسی می‌شود، در این روش از سیستم‌های الکترونیکی برای رای‌گیری استفاده نمی‌شود. این روش در بخش ۲.۱ توصیف شده است.
- **رای‌گیری الکترونیک بدون زنجیره‌ی قالبی:** در این روش، رای‌گیری الکترونیک متمرکز را بررسی می‌کنیم، چرا که سیستم‌های رای‌گیری توزیع‌شده‌ی بدون زنجیره‌ی قالبی به به کاربرد عمومی نرسیدند. در این سیستم‌ها اطلاعات رای‌دهندگان و نتیجه‌ی رای آن‌ها به دلیل نیاز به روش ردگیری به طور کامل ثبت می‌شود اما در فرایند ثبت رای تفاوت چندانی با سیستم‌های سنتی ندارند.
- **VoteBook** این سیستم را به عنوان مصداقی از سیستم‌های رای‌گیری با زنجیره‌ی قالبی خصوصی بررسی می‌کنیم. در این سیستم از یک زنجیره‌ی قالبی که می‌توان در حالت خصوصی یا عمومی از استفاده کرد برای ثبت آرا استفاده می‌شود.

سیستم معروف VoteWatcher نیز فعالیت‌های بسیاری در این زمینه داشته اما به دلیل عمومی نبودن اطلاعات پیاده‌سازی این سیستم، از مقایسه‌ی آن خودداری می‌کنیم.

همچنین از آن‌جایی که روش‌های رای‌گیری به کمک یک زنجیره‌ی قالبی عمومی و یا روش‌های توزیع‌شده بدون زنجیره‌ی قالبی به دلیل مشکلات مقیاس‌پذیری توانایی استفاده شدن در انتخابات‌های بزرگ(بیش از چند هزار نفر) را ندارند از بررسی این نوع سیستم‌ها صرف نظر می‌کنیم.

همچنین روش مورد استفاده در Follow my Vote از لحاظ روش پیاده‌سازی شباهت زیادی به VoteBook دارد ولی به جای حوزه‌ی رای‌گیری از یک برنامه در کامپیتور شخصی یا تلفن هوشمند استفاده می‌کند. این تصمیم باعث سادگی فرایند رای‌گیری برای بعضی از رای‌دهندگان می‌شود اما دو مشکل بزرگ ایجاد می‌کند که باعث شده از مقایسه‌ی آن خودداری کنیم. اولین مشکل کاهش دسترسی‌پذیری این سیستم برای افرادی که دسترسی

به اینترنت ندارند است و دومین مشکل این است که بدون وجود یک حوزه‌ی امن، راهی وجود ندارد تا اطمینان حاصل کنیم که رای‌دهنده مجبور به رای‌دادن به کاندیدای خاصی نشده است.

۲.۲.۵ اطمینان از شمارش درست

شاید مهمترین شرط برگذاری یک انتخابات میزان اطمینان از شمارش درست آرا در آن باشد. در این بخش به بررسی نجوه‌ی شمارش آرا در روش‌های مختلف می‌پردازیم.

در روش سنتی برای شمارش آرا بعد از اتمام انتخابات برگه‌های رای موجود در صندوق‌ها به مکانی منتقل می‌شوند و در آن جا یا به روش انسانی و یا با استفاده از دستگاه‌های الکترونیکی شمارش می‌شوند. طبیعتا این مدل شمارش به دلیل دخالت انسانی احتمال خطای نسبتا بالایی دارد. همچنین برای اطمینان درستی شمارش یک حوزه، تنها روش شمارش کامل برگه‌های رای آن حوزه است که هزینه‌ی آن معادل هزینه شمارش اولیه می‌باشد.

در روش‌های رای‌گیری بدون زنجیره‌ی قالبی برای ثبت رای، اطلاعات کاربر به طور رمزشده به همراه نتیجه‌ی رای او ثبت می‌شود. دلیل نگه‌داشتن اطلاعات رای‌دهنده توانایی ردگیری و بررسی درستی شمارش آرا است. در این سیستم‌ها شمارش رای‌گیری به صورت آنلاین اتفاق می‌افتد و هزینه‌ی چندانی ندارد، همچنین بررسی ناظر انتخابات هزینه ناچیزی خواهد داشت.

در سیستم VoteBook و سیستم پیشنهادی این تحقیق نیز روال شمارش آرا تفاوت چندانی ندارد و هزینه‌ی اضافه‌ای برای شمارش آرا اضافه نمی‌کنند. اما در این دو روش با عمومی شدن زنجیره‌ی قالبی قبل یا در حین رای‌گیری رای‌دهندگان نیز می‌توانند از درستی شمارش آرا و شمرده شدن رای خود اطمینان حاصل کنند.

۳.۲.۵ حریم خصوصی

در روش سنتی برگزاری انتخابات با توجه به ناشناس بودن برگه‌های رای در صندوق رای‌گیری راهی برای فهمیدن نتیجه‌ی رای یک فرد خاص نیست. البته با توجه به این که حوزه‌ی رای‌گیری برگه‌های رای را از قبل از انتخابات در دسترس دارد، این گزاره در صورتی صحیح است که حوزه یا شماره یا علامتی ناشناسی برگه‌های رای را از بین نبرده باشد.

در روش‌های رای‌گیری الکترونیک بدون زنجیره‌ی قالبی، با توجه به عمومی نشدن اطلاعات رای‌گیری اطلاعات محفوظ می‌مانند. در این روش نیز حوزه‌ی انتخابات که مسئولیت رمزکردن اطلاعات شخصی کاربر را دارد می‌تواند به حریم خصوصی آسیب بزند. همچینین برای جلوگیری از دو بار رای دادن یک کاربر باید مرکز مستقلی که اطلاعات رای‌گیری را ذخیره می‌کند نیز توانایی بازگشایی اطلاعات کاربر را داشته باشد در نتیجه این مرکز و تمامی افرادی که به اطلاعات آن دسترسی دارند نیز می‌توانند حریم خصوصی را نقض کنند.

در روش VoteBook هر رای‌دهنده یک «شماره‌ی رای‌دهنده» دارد و بعد از رای دادن نیز یک «شماره‌ی رای» دریافت می‌کند. در ادامه هش شماره‌ی رای و شماره‌ی راه‌دهنده در زنجیره‌ی قالبی به عنوان رای‌دهنده ثبت می‌شود. در این روش علاوه بر حوزه، هر کسی که شماره‌ی رای و شماره‌ی رای‌دهنده را داشته باشد می‌تواند از نتیجه‌ی رای آن فرد آگاه شود. شماره‌های رای‌دهندگان در یک زنجیره‌ی قالبی خصوصی مستقل نگهداری می‌شود و هیچ وقت عمومی نمی‌شوند در نتیجه جدا از حوزه‌ی رای‌گیری فقط خود فرد (یا کسی که اطلاعات خصوصی او را از خودش دریافت کند) می‌تواند نتیجه‌ی رای فرد را بررسی کند.

در روش پیشنهادی ما برای از بین بردن ریسک لو رفتن اطلاعات درست ثبت شدن رای در خود حوزه به کاربر اثبات می‌شود و چون خود کاربر تراکنش ثبت را کورکورانه امضا می‌کند بعد از فرایند ثبت رای راهی برای پیدا کردن نتیجه‌ی رای فرد وجود ندارد. در این روش نیز مانند همه‌ی روش‌های ممکن در رای‌گیری حوزه‌ی خطاکار می‌تواند در حین دریافت رای نتیجه‌ی آن را جداگانه ثبت کند و از این روش به حریم خصوصی آسیب بزند اما با توجه به این که تمامی بلوک‌ها توسط حوزه‌ها امضا شده‌اند در صورت نقض حریم خصوصی به سادگی حوزه‌ی خطاکار مشخص می‌شود.

۴.۲.۵ هزینه برگزاری

در این بخش هزینه‌ی برگزاری انتخابات با هر کدام از روش‌ها را از دید کاربر و از دید مجری انتخابات بررسی می‌کنیم.

هزینه برای کاربر

فرایند رای‌دادن کاربر در روش‌هایی که بررسی می‌کنیم به سه حالت خواهد بود:

- در روش سنتی و رای‌گیری بدون زنجیره‌ی قالبی کاربر برای رای‌دادن صرفا نیاز کارت شناسایی دارد. کاربر با ارائه‌ی کارت شناسایی و بعد از بررسی شدن این که کاربر دو بار رای نداده رای خود را ثبت می‌کند.

- در رای‌گیری با زنجیره‌ی قالبی با هدف افزایش شفافیت و ایجاد اطمینان از شمارش درست آرا برای کاربر، هر کابری نیاز به ثبت یک «هویت یکتا» در سامانه‌ی مربوط به انتخابات دارد. در VoteBook این کار با شماره‌ی رای‌دهنده اتفاق می‌افتد و همچنین کاربر باید قبل از رای دادن حوزه‌ی مد نظر خود را برای رای‌دادن مشخص کند. دلیل مشخص کردن حوزه این است که شماره‌ی رای‌دهندگان ممکن از قبل در حوزه ذخیره شده باشند.

- در سیستم ما نیز کاربر باید قبل از رای‌گیری یک کلید عمومی ثبت کند که برای فرایند رای‌گیری استفاده می‌شود. همچنین کاربر برای اطمینان از درست شمرده شدن رای خود می‌تواند از یک دستگاه هوشمند برای عمل امضای کورکورانه استفاده کند. کاربر می‌تواند از دستگاه‌های درون حوزه استفاده کند ولی با این کار باید اعتماد کند که حوزه رایش را به درستی ثبت کرده چرا که راهی برای اثبات درستی برنامه‌ی موجود در حوزه وجود ندارد. در ادامه فرایند مانند روش‌های

هزینه انتخابات برای مجری

در روش سنتی انتخابات هزینه‌ی اولیه‌ای برای مجری ایجاد نمی‌شود اما در هر انتخابات جدا از هزینه‌ی ایجاد حوزه، هزینه‌ی تولید برگه‌ی رای فیزیکی و شمارش را باید تحمل کند.

در روش‌های رای‌گیری الکترونیک متمرکز جدا از حوزه هزینه‌ی اضافی معنی‌داری به مجری تحمیل نمی‌شود، اما دستگاه‌های الکترونیکی نیازمند بررسی و ارتقا در طول زمان هستند.

در VoteBook یک سامانه‌ای برای ثبت و نگهداری اطلاعات محل رای‌گیری و شماره رای‌دهنده برای هر کابر وجود دارد که خود این مسئله نیز نیازمند بررسی امنتی مداوم و ارتقا است.

در سیستم پیشنهادی ما نیز در هر انتخابات، مجری انتخابات باید توانایی عوض کردن یا ثبت کلید عمومی جدید را به رای‌دهندگان بدهد که خود این مسئله یک هزینه‌ی نگهداری به مجری اضافه می‌کند.

۵.۲.۵ توانایی ردگیری خطا

برای درستی انتخابات نیاز است که برای ناظر انتخابات راهی وجود داشته باشد تا از درستی برگزاری انتخابات اطمینان حاصل کند. با توجه به این که یک حوزه‌ی انتخابات خطاکار همواره می‌تواند بعضی رای‌ها را شمارش نکند و یا تلاش کند که رای جعلی تولید کند، در این بخش توانایی ردگیری همچین حملاتی را بررسی می‌کنیم. در روال سنتی رای‌گیری با توجه به کاغذی بودن آرا و وصل نبودن برگه‌ی رای به کاربر، فراتر از بررسی تعداد آرا و مقایسه‌ی آن‌ها با تعداد برگه‌ی ثبت رای راهی برای بررسی درستی نتایج حوزه وجود ندارد. ایجاد برگه رای‌های غلط هزینه‌ی اندکی ندارد ولی در انتخابات‌های حساس ممکن است به صرفه باشد و در صورت اتفاق افتادن همچین مسئله‌ای، راه‌حل سیستمی برای پیدا کردن مشکل وجود ندارد. همچینین در صورتی که بخشی از آرا توسط حوزه دور ریخته شود، ناظر انتخابات هیچ راهی برای فهمیدن این عمل ندارد و رای‌دهندگان عادی نیز روش برای فهمیدن این موضوع که رای آن‌ها شمرده نشده ندارند.

در سیستم‌های رای‌گیری الکترونیک بدون زنجیره‌ی قالبی نیز رای‌دهنده راهی برای اطمینان حاصل کردن رای‌دهنده از شمارش رایش وجود ندارد. همچنین راهی برای ناظر انتخابات برای تشخیص دادن رای‌هایی که فرستاده نشده‌اند وجود ندارد. با توجه به این که کاربر برای ارسال رای هیچ راه شناسایی مستقل از حوزه‌ای هم ندارد، ایجاد رای دروغین توسط حوزه هم ممکن است.

در سیستم VoteBook برای ایجاد اطمینان از شمارش آرا تمامی رای‌ها شفاف ذخیره می‌شوند و هر کسی که با اطلاعات خصوصی خود می‌تواند بررسی کند که رای او به درستی ثبت شده است. ناظر انتخابات نیز می‌تواند رای‌های ثبت شده را با اطلاعات کاربرانی که باید در آن حوزه رای می‌دادند بررسی کند و به این صورت هیچ رای اشتباهی نمی‌تواند ثبت شود. اما یک حمله‌ای که حوزه‌ی خراب‌کار می‌تواند انجام دهد این است که رای کاربر را به عنوان رای ممتنع ثبت کند. در فرایند رای‌گیری با VoteBook از کاربر پرسیده می‌شود که تحت فشار مجبور به رای دادن شده یا خبر، در صورت پاسخ بله کاربر شماره‌ی رای کاربر به عنوان رای ممتنع ثبت می‌شود و اطلاعات آرا ممتنع هیچ‌وقت به صورت عمومی منتشر نمی‌شوند اما با توجه به این که این اطلاعات در اختیار ناظر انتخابات خواهد بود حمله‌ی بزرگ به این روش به سادگی قابل تشخیص خواهد بود.

در سیستم رای‌گیری ما نیز کاربر از درستی شمارش رای ثبت‌شده‌ی خود در فرایند امضای کورکورانه آگاه

می‌شود همچنین بعد از فرایند رای‌گیری نیز می‌تواند با بررسی زنجیره‌ی قالبی از ثبت رای خود (ولی نه نتیجه‌ی آن) مطمئن شود. از آن‌جایی که تمامی رای‌ها نیازمند امضای دیجیتال رای‌دهندگان هستند راهی برای ایجاد رای‌های دروغین توسط یک حوزه نیز وجود ندارد. از طرفی ناظر انتخابات می‌تواند با بررسی تساوی تعداد تراکنش‌ها ثبت و شمارش ثبت شده در زنجیره‌ی قالبی رفتار حوزه را تحلیل کند. در صورت پیدا کردن خطا از یک حوزه راهی برای پیدا کردن کاربری که رای او شمرده نشده و نتیجه‌ی رای او نخواهد بود.

جدول ۲.۵: مقایسه‌ی روش‌های رای‌گیری

معیار	روش سنتی	بدون زنجیره‌ی قالبی	VoteBook	روش پیشنهادی
شمارش درست	احتمال خطای انسانی و پرهزینه	کم هزینه	کم هزینه	کم هزینه
خطر نقض حریم خصوصی	حوزه	حوزه و مرکز	حوزه و رسید رای	حوزه
هزینه‌ی برگزاری	زیاد	کم	متوسط	متوسط
هزینه‌ی کاربر	کم	کم	متوسط	متوسط
ردگیری خطای حوزه	ناممکن	ناممکن	ممکن	ممکن

۳.۵ نزدیکی به رای‌گیری ایده‌آل

در این بخش به بررسی نزدیکی پروتکل رای‌گیری ارائه شده با رای‌گیری ایده‌آل می‌پردازیم.

- می‌دانیم که هر شخصی حداکثر یک رای می‌تواند بدهد چون که در حساب کلید عمومی آن فرد دقیقا یک

رای در ابتدای رای‌گیری وجود دارد. از طرفی می‌دانیم که سیستم مانع رای دادن فردی نمی‌شود چرا که رای‌دهنده می‌تواند بررسی کند که رای او در زنجیره‌ی قالبی مصرف شده باشد.

- می‌دانیم کسی نمی‌تواند به جای دیگری رای دهد، چرا که برای رای دادن هم نیاز به دسترسی به کلیدخصوصی دارد و هم کلید عمومی فرد با اطلاعات شناسایی او در حوزه مقایسه می‌شود.

- با اضافه شدن گزینه‌ی ممتنع و حفظ امنیت فیزیکی حوزه‌ی رای‌گیری می‌توانیم اطمینان حاصل کنیم که کسی مجبور به رای دادن نمی‌شود.

- هیچ فردی مجبور به رای دادن به کاندیدای خاصی نشود. با توجه به امنیت فیزیکی رای‌گیری و ناشناسی آرا می‌توانیم مطمئن باشیم که کسی مجبور به انتخاب گزینه‌ی خاصی نمی‌شود.

- در انتهای انتخابات می‌توانیم به سادگی با بررسی تعداد تراکنش‌های ثبت و شمارش از درستی شمارش آرا اطمینان حاصل کنیم. در صورت شمرده نشدن یک رای می‌توان فرد رای دهنده و حوزه را پیدا کرد اما راهی برای فهمیدن نتیجه‌ی رای فرد وجود ندارد.

- نتیجه‌ی آرا ناشناس باقی بماند. از آن‌جایی که تراکنش‌های ثبت کورکورانه امضا می‌شوند حتی خود رای‌دهنده با وجود از اطمینان از نتیجه‌ی رای راهی برای چک کردن نتیجه‌ی برگه‌ی رایش بعد از انتخابات ندارد.

- بسته به نیاز بتوان نتایج لحظه‌ای انتخابات را (بدون آسیب به شرط‌های قبلی) دید.

۴.۵ معیارهای مقایسه

برای مقایسه این روش رای گیری با روش‌های دیگر جنبه‌های زیر را بررسی می‌کنیم:

- هزینه‌ی زیرساخت

- هزینه‌ی هر رای‌گیری

- توانایی ردگیری درستی رای‌گیری
- هزینه برای کاربر
- درصد اطمینان از درست شمرده شدن رای
- توانایی بررسی ناظر انتخابات
- سختی مجبور کردن یک کاربر برای رای دادن به یک کاندیدای خاص

مراجع

[1] R. L.Lamport and M.Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems* (*TOPLAS*), vol.4, no.3, pp.382-401, 1982.

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

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

[4] S. S.King, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake.," *self-published paper*, 2012.

[5] N. D.Schwartz and A.Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, 2014.

[6] B.Chase and E.MacBrough, "Analysis of the xrp ledger consensus protocol," *Ripple Labs Inc White Paper*, 2018.

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

[8] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," *2014 IEEE Symposium on Security and Privacy*, pp.459-474, 2014.

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

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

[11] M. N.Atzei 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] 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.

[13] 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.

[14] M. F. B. M. R. B. Q.Xu, C.Jin and K.M.M.Aung, "Blockchain-based decentralized content trust for docker images," *Multimedia Tools and Applications*, vol.77, no.14, 2018.

[15] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communication of the ACM*, vol.28, no.1, pp.1030-1044, 1985.

[16] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Advances in Cryptology Proceedings of Crypt*, vol.82, no.3, pp.199-203, 1983.

[17] T. O. B. Fujioka and K. Ohta, "A practical secret voting scheme for large scale elections," *LNCS 718, Advances in Cryptology - ASIACRYPT*, pp.244-251, 1992.

[18] L. F. Cranor and R. K. Cytron, "Sensus: A security-conscious electronic polling system for the internet," *Proceedings of the Hawai i International Conference on System Sciences*, 1997.

[19] B. W. DuRette, ""multiple administrators for electronic voting," *B.Sc thesis, MIT*, 1999.

[20] B.N.L.C.S.M. Wright, M. Adler, ""an analysis of the degradation of anonymous protocols," *In Proceedings of Network and Distributed System Security Symposium*, 2002.

[21] B. S. R. Cramer, M. Franklin and M. Yung, "Multi-authority secret-ballot elections with hnear work," *LNCS 1070, Advances in Cryptology - EUROCRYPT*, pp.72-83, 1996.

[22] R. G. R. Cramer and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," *LNCS 1233, Advances in Cryptology - EUROCRYPT*, pp.103-118, 1997.

[23] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," *LNCS 1666, Advances in Cryptology - CRYPTO*, pp.148-164, 1999.

[24] N. L. R. DeMillo and M. Merritt, "Cryptographic protocols," *Proceedings of the 14th Annual Symposium on the Theory of Computing*, pp.383-400, 1984.

[25] D. Malkhi and E. Pavlov, "Anonymity without 'cryptography'," *Proceedings of Financial Cryptography*, pp.117-135, 2001.

[26] O. D.Malkhi and E.Pavlov, "E-voting without 'cryptography'," *In International Conference on Financial Cryptography*, pp.1-15, 2002.

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

[28] C.-L.-B. L.Vo-Cao-Thuy, K.Cao-Minh and T.A.Nguyen, "Security without identification: Transaction systems to make big brother obsolete," *IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*, pp.1-6, 2019.

[29] U. . G. E.Yavuz, A.Kaan Koç, "Towards secure e-voting using ethereum blockchain," *6th International Symposium on Digital Forensic and Security (ISDFS)*, pp.1-7, 2019.

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

[31] M. F.Hjalmarsson, G.Hrei arsson and G.Hjalmtysson, "Blockchain-based e-voting system.," *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp.983-986, 2018.

[32] S. Z.Galil and M.Yung, "Symmetric public-key encryption," *Conference on the Theory and Application of Cryptographic Techniques. Springer,*, 1985.

[33] Y. E.Ben-Sasson, I.Bentov and M.Riabzev, "Pinocchio: nearly practical verifiable computation," *IEEE Symposium on Security and Privacy*, pp.238-252, 2019.

[34] Y. E.Ben-Sasson, I.Bentov and M.Riabzev, "Scalable zero knowledge with no trusted setup," *Annual International Cryptology Conference*, pp.701-732, 2019.

[35] E. Z. A.Kosba, A.Miller and C.Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," *IEEE Symposium on Security and Privacy*, pp.839-858, 2016.

[36] N. Saberhagen, "Cryptonote v 2.0," *https:|| cryptonote.org| whitepaper.pdf*, 2013.

[37] B.Goodell1 and S.Noether2, "Thring signatures and their applications to spender-ambiguous digital currencies," *Monero Research Lab*, 2018.

[38] M. I.Miers, C.Garman and A.D.Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," *IEEE Symposium on Security and Privacy*, pp.397-411, 2013.

[39] A. S.Bowe1 and M.D.Green, "A multi-party protocol for constructing the public parameters of the pinocchio zk-snark," *International Conference on Financial Cryptography and Data Security*, pp.64-77, 2018.

[40] M. E. M. V. E.Ben-Sasson, A.Chiesa, "Secure sampling of public parameters for succinct zero knowledge proofs," *EEE Symposium on Security and Privacy*, pp.287-304, 2015.

[41] A. J. R.S.Wahby, I.Tzialla and M.Walfish, "Doubly-efficient zksnarks without trusted setup," *IEEE Symposium on Security and Privacy (SP)*, pp.926-943, 2018.

[42] E. Brewer, "Cap twelve years later: How the "rules" have changed," *Computer*, vol.45, no.2, pp.23-29, 2012.

[43] "Clique," *https://github.com/ethereum/EIPs/issues/225*.

[45] M.Castro and B.Liskov, "Practical byzantine fault tolerance," *OSDI*, pp.173-186, 1999.

[46] X. K. H.Sukhwani, J.M.Martinez and A.Rindos, "Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric)," *36th Symposium on Reliable Distributed Systems (SRDS)*, pp.253-255, 2017.

[47] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *CM Transactions on Computer Systems (TOCS)*, vol.20, no.4, p.398-461, 2002.

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. Maghsood Abbaspour

2018