



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

پایان نامه کارشناسی ارشد مهندسی کامپیوتر - گرایش نرم افزار
تحت عنوان:

ارائه ی یک روش رای گیری امن مبتنی بر بلاک چین

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: ارائه‌ی یک روش رای‌گیری امن مبتنی بر بلاک‌چین

استاد راهنما: دکتر مقصود عباس‌پور

اینجانب شروین حاجی اسمعیلی 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 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
۲	۱.۱ نیازمندی‌های رای‌گیری ایده‌آل	۲
۳	۲.۱ سیستم‌های رای‌گیری سنتی	۳
۴	۳.۱ مشکلات و چالش‌های رای‌گیری الکترونیک	۴
۵	۴.۱ انگیزه و هدف	۵
۷	۲ تعریف مفاهیم	۷
۸	۱.۲ زنجیره‌ی قالبی	۸
۸	۱.۱.۲ پیاده‌سازی زنجیره‌ی قالبی	۸
۸	۲.۱.۲ انواع زنجیره‌ی قالبی	۸
۱۰	۲.۲ اثبات‌های بی‌دانش	۱۰
۱۰	۱.۲.۲ مثال شهودی	۱۰
۱۱	۲.۲.۲ اثبات‌های بی‌دانش بدون تعامل	۱۱
۱۱	اثبات بی‌دانش ZK-SNARK	۱۱
۱۳	اثبات بی‌دانش ZK-STARK	۱۳
۱۴	۳ کارهای پیشین	۱۴
۱۵	۱.۳ رای‌گیری الکترونیک	۱۵

۱۶	رای گیری الکترونیک متمرکز	۱.۱.۳
۱۷	رای گیری الکترونیک توزیع شده	۲.۱.۳
۱۷	رای گیری بدون زنجیره ی قالبی	
۱۷	رای گیری با زنجیره ی قالبی عمومی	
۱۸	رای گیری با زنجیره ی قالبی خصوصی	
۱۹	اعتماد	۲.۳
۱۹	روش توافق	۱.۲.۳
۲۰	توافق در ارزش های دیجیتال	
۲۰	اثبات سهم	
۲۰	Ripple Consensus Protocol	
۲۱	Stellar Consensus Protocol	
۲۱	اثبات های بی دانش	۳.۳
۲۲	کاربردها	۱.۳.۳
۲۲	پرداخت ناشناس	
۲۴	روش پیشنهادی	۴
۲۵	تعریف نقش ها	۱.۴
۲۵	شرایط مسئله ی رای گیری الکترونیکی	۲.۴
۲۷	فرضیات مسئله	۳.۴
۲۷	مثال شهودی	۴.۴
۲۸	فرایند رای گیری از نگاه کاربر	۵.۴
۲۸	قبل از رای گیری	۱.۵.۴
۲۹	در حوزه ی رای گیری	۲.۵.۴
۲۹	فرایند رای گیری از دید حوزه	۶.۴

۲۹	تراکنش‌ها	۱.۶.۴
۲۹	تراکنش ثبت	
۳۰	تراکنش شمارش	
۳۰	فرایند ثبت رای کاربر	۲.۶.۴
۳۱	شمای کلی	۷.۴
۳۲	اضافه شدن بلوک	۱.۷.۴
۳۳	مقادیر اولیه برای ZK-SNARK	۲.۷.۴
۳۳	توافق	۳.۷.۴
۳۳	قضیه‌ی CAP	
۳۵	Practical Byzantine Fault Tolerance	

۵ تحلیل و ارزیابی ۳۷

۳۸	پیاده سازی	۱.۵
۳۹	نزدیکی به رای گیری ایده آل	۲.۵
۴۰	مقایسه با کارهای مشابه	۳.۵
۴۰	روش‌های رای گیری دیگر	۱.۳.۵
۴۱	اطمینان از شمارش درست	۲.۳.۵
۴۲	حریم خصوصی	۳.۳.۵
۴۳	هزینه برگزاری	۴.۳.۵
۴۳	هزینه برای کاربر	
۴۴	هزینه انتخابات برای مجری	
۴۴	توانایی ردگیری خطا	۵.۳.۵

۶ نتیجه‌گیری و کارهای آتی ۴۷

۱.۶ نتیجه‌گیری ۴۸

۲.۶ کارهای آتی ۴۸

مراجع ۴۹

فهرست تصاویر

۹	یک درخت مرکب	۱.۲
۱۲	یک نمونه مدار محاسباتی	۲.۲
۳۱	فرایند ثبت رای در حوزه	۱.۴
۳۲	شمای منطقی سیستم	۲.۴
۳۶	روش PBFT	۳.۴

فهرست جداول

۹	انواع زنجیره‌ی قالبی	۱.۲
۳۵	روش توافق	۱.۴
۳۹	تنظیمات libsnark	۱.۵
۴۶	مقایسه‌ی روش‌های رای‌گیری	۲.۵

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 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: بلاک چین، 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 مسئله 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 دقیقاً 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 رای دادن 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.

احراز 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 نسبتاً 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 ۲۰۱۵^۱ 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^۲ کردن هستند که می‌تواند باعث کندی فرایند و حتی گاهی 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

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

^۲ crash

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

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

۴.۱ انگیزه و هدف

هدف این تحقیق، طراحی یک سیستم رای گیری الکترونیک است که شرایط رای گیری ایده‌آل را تا جای ممکن بدون نیاز به اعتماد به شخص ثالث ارضا 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)، پلتفرمی برای رای گیری الکترونیک ایجاد شدند که امنیت شمارش آرا را با عمومی ساختن فرایند رای گیری 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 امنیت 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 رای گیری به دلیل بی‌نام بودن برگه‌های رای بعد از اتمام فرایند رای گیری راهی برای اطمینان حاصل کردن از نتیجه‌ی رای فرد نیست. از طرفی به دلیل امنیت حوزه‌های رای گیری راهی برای اطمینان از نتیجه‌ی رای یک نفر در حین فرایند رای گیری هم نیست. پس راهی برای مجبور کردن یک نفر که به یک کاندیدای خاص رای بدهد وجود ندارد. اما در سیستم‌های مبتنی بر زنجیره‌ی قالبی هر رای داده شده با امضای الکترونیکی فرد امضا شده است و این موضوع می‌تواند با عمومی شدن زنجیره‌ی قالبی بعد از رای گیری باعث لو رفتن نتیجه‌ی رای آن فرد شود.

این مشکلات مانع بزرگی برای استفاده‌ی فراگیر این سیستم‌ها خواهد بود. هدف ما در این تحقیق این است که سیستمی ارائه کنیم که امنیت شمرده شدن آرا را بمانند این سیستم‌ها ارائه کند و در عین حالت حریم خصوصی رای‌دهنده را به طور کامل حفظ کند.

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

را کاهش خواهد داد. در عین حال کمترین تغییر برای رای دهندگان خواهد داشت که باعث افزایش دسترس پذیری این سیستم خواهد شد. همچنین تمامی آرا رای دهندگان در قبال یک مهاجم خارجی و حتی خود برگزار کننده ی انتخابات ناشناس خواهند ماند.

با این وجود این سیستم یک رد الکترونیک غیر قابل انکار از تمام آرا، در قالب یک زنجیره ی قالبی، ارائه خواهد کرد که با وجود حفظ حریم خصوصی به هر ناظر ثالثی اثبات کند که آرا درست شمرده شده است. همچنین تمامی این قابلیت ها بدون نیاز اعتماد به برگزارکننده ی انتخابات خواهد بود و هرگونه تخطی از پروتکل ارائه شده توسط حوزه های رای گیری از طریق اطلاعات ثبت شده در زنجیره ی قالبی قابل ردیابی خواهد بود.

فصل ۲

تعريف مفاهيم

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 ساختمان داده‌ایست 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 صرفاً 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 معمولاً 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 نگه‌می‌دارند. 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 پیش‌بینی 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 اضافه کردن بلوک به زنجیره‌ی قالبی دسترسی خاصی نمی‌خواهد

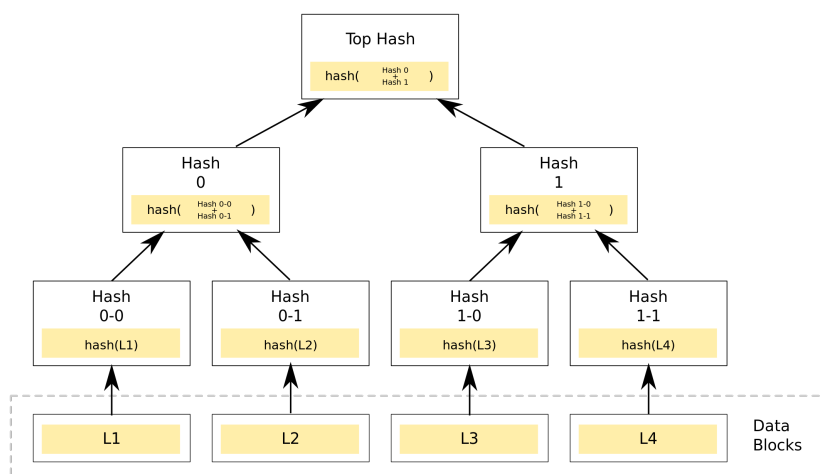
^۱ Linked list

^۲ Hash

^۳ Append only

^۴ Merkle tree

^۵ Binary tree



شکل ۱.۲: یک درخت مرکل

و هر کسی می‌تواند در آن‌ها بنویسد ولی در زنجیره‌ی قالبی‌های خصوصی اضافه کردن بلوک صرفاً 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

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

۲.۲ اثبات‌های بی‌دانش

اثبات بی‌دانش^۱ روشی است که یک «اثبات‌کننده» می‌تواند به یک «بررسی‌کننده» نشان دهد که او یک راز - مثلاً خروجی یک عملیات کامپیوتری - را می‌داند، بدون این که به بررسی‌کننده هیچ اطلاعات اضافه‌ای، مانند خروجی عملیات، بدهد. به عبارت دیگر اثبات‌های بی‌دانش، صرفاً داشتن اطلاعات را اثبات می‌کنند و خود اطلاعات را محفوظ نگه می‌دارند.

یک اثبات بی‌دانش باید ۳ شرط زیر را داشته باشد:

- کامل بودن: 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، بررسی‌کننده 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 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.

^۱ 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 - مثلاً هش ریشه‌ی یک درخت مرکب - 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 [۱] است. شاهد‌های این روش علاوه بر بی‌دانش بودن ویژگی‌های زیر را دارند:

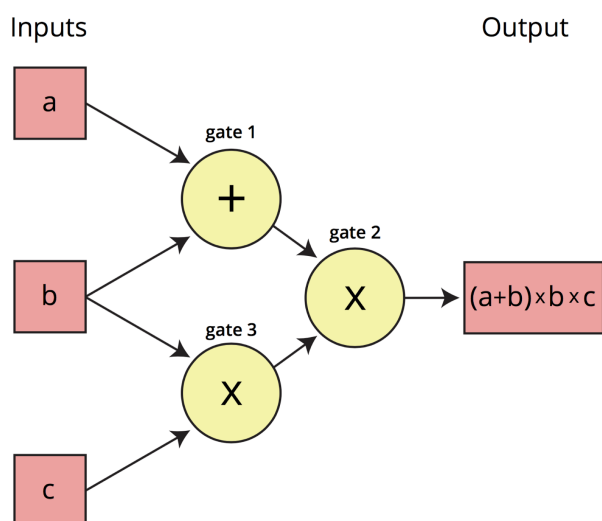
- مختصر^۲: تولید و بررسی شاهد از انجام خود محاسباتی که اثبات می‌شود کوتاه‌تر (معمولاً از مرتبه‌ی زمانی $(\log N)^2$) است.
- بی‌تعامل^۳: نیازی به پیامی از بررسی‌کننده برای ایجاد شاهد نیست.

^۱ Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

^۲ Succinct

^۳ 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^۱ [۲] است. مهم‌ترین وجه تمایز این روش در مقایسه با ZK-SNARK «شفافیت»^۲ 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.

از مزیت‌های دیگر این روش استفاده نکردن از Elliptic curveها است. نیازهای کم این روش باعث می‌شود که حتی با کامپیوترهای کوانتومی^۳ راهی برای شکستن این اثبات‌ها وجود نداشته باشد. برای ساختن یک شاهد با این روش، برنامه‌ی مورد نظر را تبدیل به یک چندجمله‌ای درجه بالا می‌کنند، سپس از مقادیر این چندجمله‌ای یک درخت مرکب 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 هاش ریشه‌ی درخت مرکب به عنوان ورودی به تابع شبه‌تصادفی^۴ استفاده می‌شود که مشخص می‌کند خروجی کدام شاخه‌ها باید در شاهد بیاید.

^۱ Zero-Knowledge Scalable Transparent ARguments of Knowledge

^۲ Transparency

^۳ Quantum computers

^۴ Pseudo random

فصل ۳

کارهای پیشین

از آن جایی که مهمترین فاکتورهای یک سیستم رای گیری مناسب امنیت شمارش آرا و حفظ حریم خصوصی رای دهنده است، این دو موضوع پایه های طراحی سیستم ما خواهند بود. سیستم های رای گیری الکترونیک قبل از تکنولوژی زنجیره ی قالبی از روش های متعددی برای تحقق این هدف استفاده می کردند اما تقریباً در تمامی این روش ها نیاز به اعتماد به مجری انتخابات وجود دارد.

طراحی زنجیره های قالبی همراه به کمک روش های توافق خلاقانه باعث ایجاد ارزش های دیجیتال بدون نیاز به یک شخص (بانک) مورد اعتماد شد. در ادامه این ساختار داده ی اکیدا افزایشی برای حذف نیاز به اعتماد در کاربرهای دیگر نیز استفاده شده است. زنجیره ی قالبی در این تحقیق نیز به عنوانی ابزاری که با ایجاد شفافیت نیاز به اعتماد را کاهش می دهند استفاده می شود.

شفافیت در انتخابات خود باعث ایجاد مشکلاتی برای امنیت رای دهندگان می شود. عدم حفظ حریم خصوصی رای دهنده در یک انتخابات می تواند باعث شود رای دهنده نتواند به کاندیدای دلخواهش رای دهد یا تحت فشار مجبور به رای دادن شود. برای رفع این مسئله از اثبات های بی دانش استفاده می کنیم. اثبات های بی دانش این امکان را ما می دهند تا بتوانیم حتی با وجود حفظ حریم خصوصی کاربر، درستی شمارش انتخابات را اثبات کنیم.

۱.۳ رای گیری الکترونیک

رای گیری الکترونیک را به طور کلی می توانیم به دو دسته ی رای گیری تماماً الکترونیک و رای گیری به کمک ابزارهای الکترونیکی تقسیم کرد. روش های دسته ی دوم مبتنی بر رای گیری سنتی هستند و از ابزارهای الکترونیکی صرفاً برای کاهش هزینه و افزایش دسترسی پذیری استفاده می کنند. از این روش ها می توان به ابزارهای شمارش رای خودکار و یا دستگاه های ثبت رای الکترونیکی که خروجی آن ها یک برگه ی رای کاغذی^۱ است اشاره کرد. در این تحقیق این ابزارها را بررسی نمی کنیم و منظور از رای گیری الکترونیک، دسته ی اول یا رای گیری تماماً الکترونیک است.

سیستم های رای گیری الکترونیک را می توان به دو دسته ی کلی توزیع شده و متمرکز تقسیم کرد. سیستم های مرکزی نیازمند یک ارتباط امن از رای دهنده تا سرویس مرکزی هستند. همچنین نیازمند اعتماد کامل به همان

^۱ Direct-recording electronic voting systems or DRE

یک سرویس برای درستی انتخابات است. در سیستم‌های توزیع شده تلاش می‌کنند تا این دو مسئله را کم‌رنگ‌تر کنند.

۱.۱.۳ رای‌گیری الکترونیک متمرکز

در این سیستم‌ها یک سامانه‌ی مرکزی وجود دارد که تمامی آرا در آن ذخیره می‌شوند. در این سیستم‌ها حوزه‌های رای‌گیری می‌توانند وجود داشته باشند اما حوزه‌ها صرفاً وظیفه‌ی احراز هویت و ارائه‌ی درگاه امن برای ثبت رای در سامانه‌ی مرکزی را دارند. حریم خصوصی کاربران در این سیستم‌ها مبتنی بر استفاده از کانال‌های ارتباطی ناشناس^۱ بین حوزه‌های رای‌گیری و سامانه‌ی مرکزی است.

اولین تحقیق در رابطه با استفاده از کانال‌های ارتباطی ناشناس برای رای‌گیری در سال ۱۹۸۵ توسط Chaum [۳] بود که در آن برای ساخت کانال‌های ارتباطی ناشناس از امضای کورکورانه^۲ [۴] برای ایجاد یک ارز دیجیتال استفاده می‌شد. در امضای کورکورانه، برای حفظ حریم خصوصی فردی که باید اطلاعاتی را تایید کند، رمز شده‌ی 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 [۵] بود و در ادامه در سال ۱۹۹۷ [۶] 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 [۷] در راستای استفاده از چند حوزه انجام شده است. مشکل بزرگ دیگر این روش‌ها [۸] سختی ناشناس نگه‌داشتن کانال‌های ارتباطی ناشناس است.

^۱ Anonymous communication channel

^۲ Blind signature

۲.۱.۳ 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 همه‌ی این سیستم‌ها از زنجیره‌ی قالبی‌های بسته استفاده می‌کنند.

رای‌گیری بدون زنجیره‌ی قالبی

بعضی سیستم‌های طراحی شده برای رای‌گیری الکترونیک [۹][۱۰][۱۱] از روش‌های تقسیم‌راز^۱ 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 تقسیم‌راز است.

روش دیگری که برای رای‌گیری توزیع‌شده استفاده شده است، استفاده از بردار بررسی^۲ [۱۲] است. در این روش‌ها بررسی درستی رای‌ها کاملاً توزیع‌شده است اما نیاز به ارتباط دو به دوی تمامی رای‌دهنده‌ها دارد که در یک انتخابات واقعی شدنی نیست. ترکیبی از این روش و تقسیم‌راز باعث ایجاد پروتکل‌هایی [۱۳][۱۴] 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 [۱۵]، محصولات در زمینه‌ی رای‌گیری الکترونیک به کمک این تکنولوژی ساخته شدند. تعدادی از این سیستم‌های رای‌گیری در قالب قراردادهای هوشمند^۳ [۱۶] ساخته شده‌اند که از آن‌ها می‌توان به وتریوم^۴ [۱۷] و یا کار E.Yavuz [۱۸] در بستر اتریوم^۵ [۱۹] - که یک ارز دیجیتال

^۱ Secret sharing

^۲ Check vector

^۳ Smart contract

^۴ Votereum

^۵ Ethereum

و یک بستر قرارداد هوشمند است - اشاره کرد. مزیت اینجور رای گیری ها هزینه ی اولیه کم استفاده از آن هاست، اما همچنان ریسک اشتباه برنامه نویسی [۲۰] [۲۱] [۲۲] در این سبک کارها بسیار بالاست. همچنین هزینه اجرای قراردادهای هوشمند به تعداد بالا برای یک رای گیری هزینه ی بالایی خواهد داشت که در طول زمان باعث افزایش هزینه ی رای گیری خواهد شد. مسئله ی دیگر در بستر اتریوم هم وابستگی سیستم رای گیری، به پهنای باند نودهای اتریوم و میزان بار روی شبکه ی آن است. این موضوع می تواند باعث کند شدن یا حتی در مواردی حذف شدن تعدادی از آرا شود.

رای گیری با زنجیره ی قالبی خصوصی

از سیستم های رای گیری با زنجیره ی قالبی خصوصی می توان به VoteBook [۲۳] توسط شرکت Kaspersky که یک شرکت پیشرو در زمینه ی امنیت است اشاره کرد. فلسفه ی ساخت این سیستم به صورتی است که تلاش می کند برای کاربرانی که از سیستم هایی رای گیری فعلی استفاده می کنند کمترین تغییر در رفتار نیاز باشد. از مثال های دیگر سیستم های رای گیری مبتنی بر زنجیره ی قالبی می توان به استارت آپ Follow My Vote اشاره کرد. نحوه ی کار این سیستم با سیستم VoteBook تفاوت اساسی دارد و برای رای دادن احتیاج دارد که نرم افزاری برای رای دادن به روی کامپیوتر و یا تلفن همراه کاربران نصب شود. اینگونه طراحی سیستم، خطرات امنیتی در قالب بدافزار ایجاد می کند. همچنین با نبود یک حوزه ی رای گیری امن راهی برای تامین امنیت رای دهندگان و اطمینان حاصل کردن از این که کسی مجبور به رای دادن نشده، نیست.

یکی از موفق ترین سیستم های رای گیری مبتنی بر زنجیره ی قالبی موجود در حال حاضر VoteWatcher ساخته شده توسط یک شاخه از شرکت blockchain Technologies Corporation است که یک شرکت بزرگ برای ارائه ی سرویس های مبتنی بر زنجیره ی قالبی است. طبق وبسایت این محصول تاکنون بیش از صد هزار رای در بیشتر از ۲۰ رای گیری مختلف توسط این سیستم شمارش شده است.

مدل اسفاده ی VoteWatcher به سیستم VoteBook بسیار شبیه است و تفاوت رفتاری زیادی با مدل های رای گیری الکترونیکی فعلی برای کاربران ندارد. در این محصول طبق نیاز رای گیری می توان از یک زنجیره ی قالبی عمومی یا خصوصی استفاده کرد.

از موارد دیگر می توان به پیاده سازی های به کمک قراردادهای هوشمند ولی با استفاده از زنجیره ی قالبی خصوصی

[۲۴] که توانایی ردگیری بالاتری از پیاده‌سازی‌های دیگر ارائه می‌کنند، اما به دلیل کندی نسبی، نیاز به تقسیم رای‌گیری به چند رای‌گیری کوچک‌تر دارند.

۲.۳ اعتماد

همانطور که اشاره کردیم برای ایجاد یک رای‌گیری خوب تا جای ممکن باید نیاز به وجود شخص معتمد را حذف یا حداقل کم‌رنگ کنیم. ساده‌ترین راه حل برای حذف نیاز به اعتماد ایجاد شفافیت و عمومی ساختن تمامی اطلاعات است؛ در صورتی که همه بتوانند تمامی اطلاعات را بررسی کنند و از درستی آن‌ها اطمینان حاصل کنند، دیگر نیازی اعتماد کردن به شخص دیگر ندارند.

با استفاده از زنجیره‌ی قالبی می‌توانیم برای بررسی درستی اطلاعات همواره با بررسی بلوک آخر از درستی کل زنجیره اطمینان حاصل کنیم اما با توجه این که چندین نفر می‌توانند به آن بلوک اضافه کنند ممکن است سناریویی پیش بیاید که در آن دو یا چند نسخه‌ی درست از زنجیره‌ی قالبی وجود داشته باشد. برای حل این مسئله باید پروتکلی داشته باشیم که یا اجازه‌ی پیش آمدن این شرایط را ندهد و یا روشی برای حذف تعدادی از آن‌ها ارائه کند و کاری کند که در طول زمان پس از مدتی فقط یک نسخه‌ی درست از زنجیره‌ی قالبی باقی بماند. این پروتکل را روش توافق می‌نامیم.

۱.۲.۳ روش توافق

توصیف رسمی این مسئله، مسئله‌ی ژنرال‌های بیزنتین^۱ [۲۵] 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

^۱ The Byzantine generals problem

^۲ کار اثبات

می‌پردازیم.

توافق در ارزهای دیجیتال

روشی که S.Nakamoto [۲۶] برای رفع این مسئله در بیت‌کوین استفاده کرده است، اثبات کار^۱ نام دارد. این روش که بر پایه‌ی روش استفاده شده در hashcash [۲۷] است. در این روش برای اضافه شدن هر بلوک به زنجیره‌ی 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^۲ [۲۸] 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 به تراکنش به خود) هش ساده‌تری برای بلوک بعدی اعمال کند. مزیت اصلی این روش توان مصرفی پایین‌تر آن به نسبت اثبات کار است. معمولاً در زنجیره‌ی قالبی‌ها در بلوک‌های ابتدایی از روش اثبات کار استفاده می‌شود و بعد از مدتی برای کاهش هزینه‌های اضافه کردن بلوک جدید و مقیاس‌پذیری می‌توان از این روش یا ترکیب این روش‌ها استفاده کرد.

Ripple Consensus Protocol

در این روش [۲۹][۳۰] تعدادی شخص مورد اعتماد وجود دارند که برای اضافه شدن 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 نسبتاً 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.

^۱ Proof of work

^۲ proof of stake

Stellar Consensus Protocol

روش SCP [۳۱] 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 کمتر این روش باعث می‌شود که تا $n/3$ خطا در نودهای مورد اطمینان را بتواند تحمل کند.

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 [۱] و ZK-STARK [۲] بوجود آمدند. این روش‌ها توانایی اثبات هر محاسباتی را به صورت بی‌دانش دارند و این موضوع باعث استفاده‌ی آن‌ها در کاربردهای بیشتری شد.

با توجه به این که ZK-SNARK، به طور خاص خاص پروتکل پینوکیو^۱، فراگیرترین روش برای ایجاد اثبات‌های بی‌دانش است. تحقیقات زیادی در مورد فاز آماده‌سازی و ایجاد پارامترهای عمومی این مدل انجام شده است. همانطور که قبلاً اشاره کردیم ورودی‌های این فاز اگر پس از استفاده‌ی اولیه پاک نشوند می‌توانند برای ایجاد اثبات‌های تقلبی استفاده شوند.

از این تحقیق‌ها می‌توان به روش‌هایی [۳۳] [۳۴] 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 [۳۵] مرحله‌ی آماده‌سازی را حذف می‌کند

^۱ Pinocchio

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 صرفاً دغدغه‌ی حریم خصوصی خود را دارند خطرهای هزینه‌ی 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 [۳۶] 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^۱ که یک ارز دیجیتال است که بر اساس الگوریتم Cryptonote [۳۷] کار می‌کند، به مانند HAWK با یکتا سازی آدرس‌های مقصد و امضای حلقه‌ای^۲ کار می‌کند. در ادامه این ارز دیجیتال با همین روش مدلی [۳۸] برای مخفی کردن پرداخت‌کننده‌ی سکه نیز ارائه کرد.

از کارهای دیگر در این زمینه می‌توان به zerocoin [۳۹] که روش پرداخت ناشناس بر بستر بیت‌کوین به کمک

^۱ Monero

^۲ Ring Signature

ZK-SNARK ارائه کرد اشاره کرد. روش استفاده شده در آن با بهبود در ارز دیجیتال z-cash [۴۰] 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.

فصل ۴

روش پیشنهادی

روش پیشنهادی ما سه هدف کلی دارد، هر رای دهنده از شمارش درست رای خود اطمینان حاصل کند، حریم خصوصی حفظ شود و هر خطا در فرایند رای گیری قابل تشخیص باشد. برای رسیدن به این اهداف نیازمند باید فرایند به گونه ای طراحی شود که هیچ فردی معتمد فرض نشود. برای این کار ابتدا شرایط و فرضیات مسئله را به طور دقیق تر بررسی می کنیم، در ادامه روش رای گیری را به صورت کلی و بدون در نظر گرفتن توزیع شده بودن سیستم ارائه می کنیم و در نهایت با یک روش توافق مناسب امنیت پروتکل در حالت توزیع شده را فراهم می کنیم.

۱.۴ تعریف نقش ها

در این بخش نقش های حاضر در سیستم رای گیری و انتظارات خود از آن ها را تعریف می کنیم:

- **ناظر انتخابات:** این سازمان مسئول بررسی درستی انتخابات و احراز هویت شرکت کنندگان در انتخابات است. به این سازمان اعتماد می شود تا کار احراز هویت را به درستی انجام دهد. همچنین این سازمان بررسی کننده ی نهایی درست بودن انتخابات است و باید بتواند از درستی انتخابات اطمینان حاصل کند.
- **رای دهنده:** فردی که حق رای به یک کاندیدا را دارد، این فرد می تواند از رایش استفاده نکند یا نکند، می تواند تلاش کند که چند بار رای دهد. باید بتواند از درستی انتخابات اطمینان حاصل کند. ممکن است توسط یک رقیب بدخواه برای رای دادن تحت فشار قرار بگیرد.
- **حوزه ی انتخابات:** محلی که در آن رای داده می شود، باید بتواند امنیت فیزیکی افراد را تامین کند. ممکن است برای خراب کردن انتخابات یا نقض حریم خصوصی کاربران تلاش کند.

۲.۴ شرایط مسئله ی رای گیری الکترونیکی

شروط لازم برای سیستم رای گیری ارائه شده عبارتند از:

۱. هر فرد واجد شرایط دقیقاً 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 حوزه‌ی 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 رای دادن نداشته باشد. این نیازمندی برای دسترس‌پذیر نگه داشتن انتخابات لازم است.
۸. سیستم رای‌گیری نسبت به روش‌های فعلی رای‌گیری از دید کاربر تفاوت چندانی نداشته باشد. هر تغییر اساسی از نگاه رای‌دهنده 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 نگه داشتن 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 مربوط به مقایسه‌پذیری در یک محصول کامل نمی‌پردازیم. برای مثال برای بهینه‌سازی حجم شاهدهای بی‌دانش در محیط واقعی باید از تجمیع گره‌های یک طرفه^۱ که اولین بار در سال ۱۹۹۳ [۴۱] ارائه شدند و یا روش‌های مشابه استفاده کرد.

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 آن جایی که این دستگاه صرفاً 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 راه حل ابتدا یک مثال شهودی از یک مدل رای‌گیری متمرکز را بررسی می‌کنیم، سپس در ادامه از این روش برای ایجاد سیستم توزیع شده 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 رای دادن یکی از کاندیداها را انتخاب می‌کند، مسئول حوزه یک کاغذ رمز شده که در آن یک

^۱ One-way accumulator

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 شاهده‌ی 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 رای داده، 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 رای دادن 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 - مثلاً 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 صرفاً منطق پروتکل را بررسی می‌کنیم و جزئیات 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 کوکورانده 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 رای از یک کلید عمومی به دسته‌ی رای‌های منتظر شمارش منتقل می‌شود. هر تراکنش ثبت شامل یک رای و یک رشته^۱ رمز شده است که حاوی یک عدد تصادفی s و حساب مقصد d است که با کلید تصادفی k رمز شده است. این عبارت رمز شده رای CM می‌نامیم. سپس CM (نه خود s) در زنجیره‌ی قالبی به

^۱ string

همراه رای ثبت می‌شود.

$$CM = enc_k(r, d) \quad (۱.۴)$$

تراکنش شمارش

مدل دیگر تراکنش ممکن تراکنش شمارش است که در آن شاهدهی برای شمارش رای ارائه می‌شود. برای این تراکنش رای دهنده اثبات بی‌دانشی برای دو موضوع ارائه می‌کند: یک C می‌شناسد به طوری که $C \in C_1, C_2, \dots, C_n$ 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.

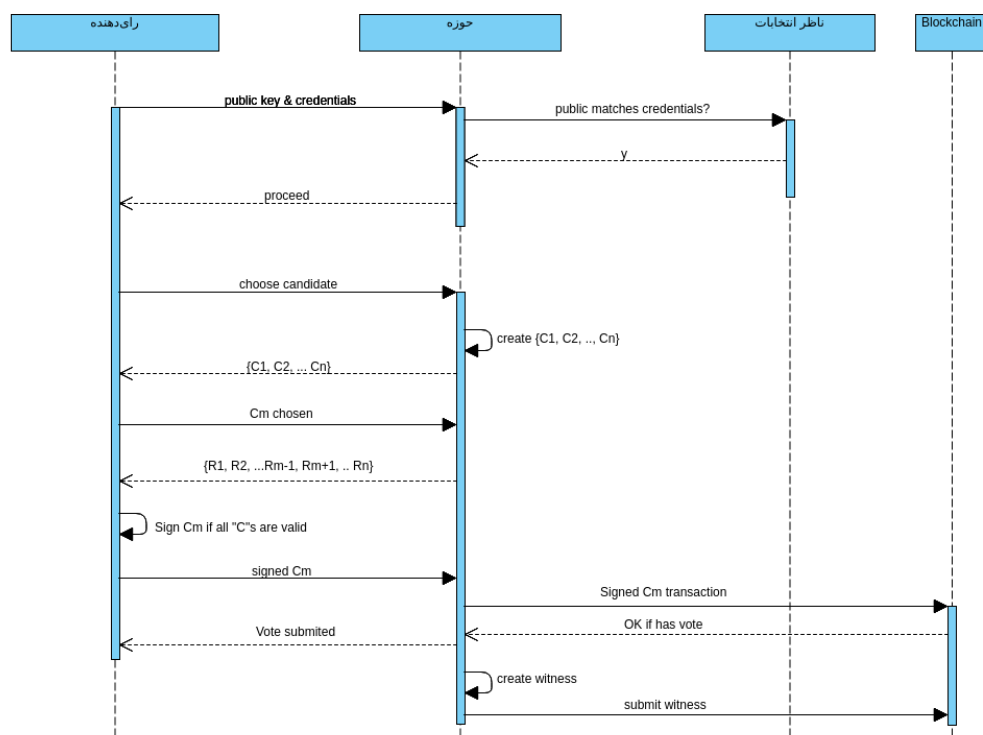
لازم به ذکر است که از آنجایی که در تراکنش شمارش C و r نشان داده نشده‌اند، راهی برای فهمیدن این که رای متعلق به چه کسی است وجود ندارد.

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 عبارات رمز شده به طور تصادفی توسط کاربر CM_c انتخاب می‌شود و به حوزه اعلام می‌شود.
۳. حوزه کلید مربوط به تمامی CM های دیگر را به کاربر ارائه می‌کند.

۴. کاربر همه‌ی CM ها 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.



شکل ۱.۴: فرایند ثبت رای در حوزه

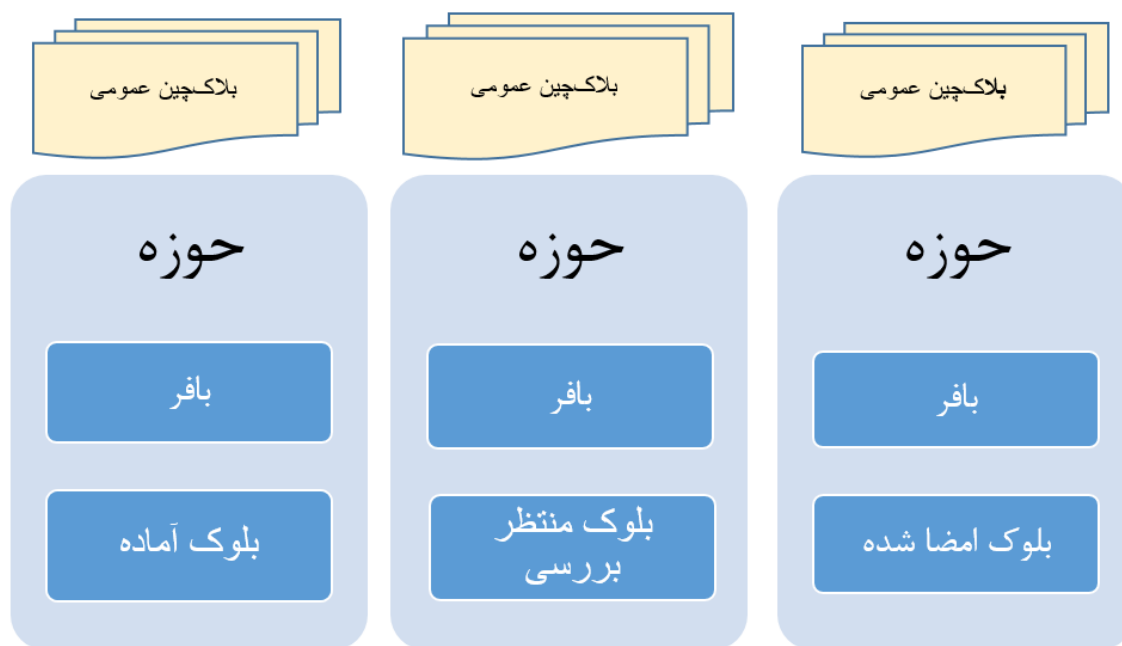
۵. حوزه CM_c را به همراه رای موجود در حساب کاربر به عنوان یک تراکنش ثبت در زنجیره‌ی قالبی ذخیره می‌کند. در صورتی که رای کاربر قبلاً ثبت شده باشد در این مرحله خطا رخ می‌دهد و رای ثبت نمی‌شود.
۶. حوزه یک شاهد برای شمارش رای کاربر می‌سازد و هر دوی این تراکنش‌ها در بلوک بعدی زنجیره‌ی قالبی ذخیره می‌شوند.

شکل ۱.۴ این توالی فرایند را نشان می‌دهد.

۷.۴ شمای کلی

به طور کلی سیستم از تعدادی حوزه تشکیل می‌شود که روی یک زنجیره‌ی قالبی توافق می‌کنند. همچنین 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 رای دارد. 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 تراکنش‌های 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 قبلاً 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 [۳۴] 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 لورفتن آن باید تمامی حوزه‌ها تباری کنند. در این روش خود برای ایجاد پارامترها از یک حالت خاص اثبات‌های بی‌دانش استفاده می‌شود.

۳.۷.۴ توافق

در زنجیره‌ی قالبی‌های عمومی معمولاً 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. معمولاً 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

^۱ Consistency

^۲ Availability

^۳ Partition tolerance

^۴ Eventual consistency

شدن تعدادی از آرا ایجاد کند و این خطر معقولی برای یک سیستم رای گیری الکترونیکی نیست.

در زنجیره‌ی قالبی‌های عمومی معمولاً از روش‌های اثبات کار و اثبات سهم استفاده می‌شود که دسترس پذیری و تحمل قسمت‌شدن را به خوبی ارائه می‌کنند اما ممکن است شاخه‌های^۱ لحظه‌ای پیش بیاید و چند نسخه از زنجیره‌ی قالبی درست وجود داشته باشد، معمولاً در این روش‌ها طولانی‌ترین زنجیره‌ی قالبی نسخه‌ی درست در نظر گرفته می‌شود و زنجیره‌ی قالبی‌های کوتاه‌تر حذف می‌شوند. از آن جایی که این کار در سیستم ما باعث از بین رفتن رای می‌شود باید در روش دیگری استفاده کنیم.

در این تحقیق سه روش برای تفاوت را بررسی می‌کنیم. روش اول Aura [۴۳] نام دارد. در این روش نود یک نود رهبر بلوک‌های جدید ارائه می‌کند و در طول 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.

راه حلی در در پروتکل ارائه شده در این تحقیق برای این موضوع استفاده کردیم PBFT^۲ [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.

^۱ fork

^۲ Practical Byzantine fault tolerance

جدول ۱.۴: روش توافق

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

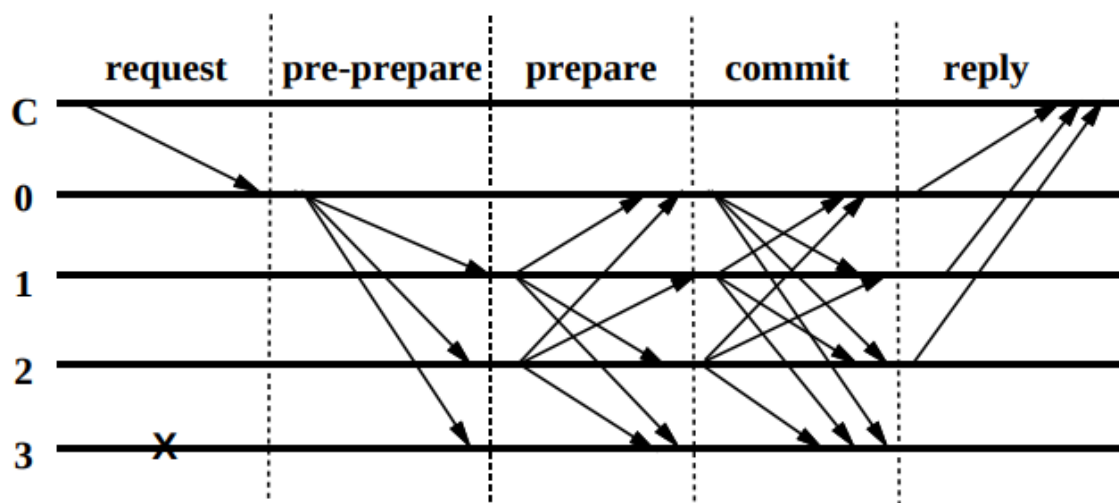
Practical Byzantine Fault Tolerance

در این روش در ابتدای رای گیری حوزه ها در یک زنجیره ی اولویت چیده می شوند و برای ثبت هر بلوک جدید، بلوک آماده شده را به رهبر (حوزه ای با بیشترین اولویت) داده می شود و حوزه آن را به تمامی حوزه های دیگر ارسال می کند. سپس تمامی حوزه های دیگر بعد از تایید نتیجه را برای هم ارسال می کنند و در صورت موفقیت آن را ثبت می کنند، بعد از تایید نتایج برای حوزه ی ابتدایی ارسال شده و ثبت نهایی می شود.

همچنین بعد از اضافه شدن هر بلوک حوزه ی رهبر تغییر می کند و به نفر بعدی در زنجیره ی اولویت می رسد. همچنین در صورت جواب ندادن حوزه ی رهبر در مدت زمان مشخص یا جواب های غلط دادن مسئولیت به نفر بعدی منتقل می شود.

در این روش حداکثر تعداد تعداد حوزه ای که باید خطا کار باشند تا بلوک اشتباهی در زنجیره ی قالبی ثبت شود برای $3f + 1$ حوزه f حوزه است. این تعداد حوزه ی خراب کار می توانند بلوک های اشتباهی ثبت کنند اما به دلیل استفاده از امضای دیجیتال بعد از اتمام رای گیری با بررسی درستی بلوک های ثبت شده در زنجیره ی قالبی بلوک های خطا به سادگی قابل شناسایی هستند. در همچین شرایطی چون نمی توان از تعداد رای دهندگانی که رای آن ها ثبت نشده اطمینان پیدا کرد نتایج رای گیری باید مردود محسوب شود.

در روش PBFT اثبات می شود [۴۷] تا زمانی که کمتر از یک سوم حوزه ها خطا کار باشند هیچ زمانی دو نسخه ی مستقل از زنجیره ی قالبی توسط حوزه ها تایید نمی شود. به عبارت دیگر این روش به طور کامل همخوانی



شکل ۳.۴: روش PBFT

و توانایی قسمت شدن را دارد.

لازم به ذکر است که در این حالت سیستم همواره در دسترس 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

تحليل و ارزیابی

در این فصل به تحلیل و بررسی روش ارائه شده و مقایسه‌ی این روش با روش‌های دیگر رای‌گیری می‌پردازیم. در ابتدا با بررسی جزئیات پیاده‌سازی تست شده در روش می‌پردازیم و بعد از بررسی نحوه‌ی ارضای شرایط رای‌گیری ایده‌آل، این روش را در قیاس با روش‌های دیگر از نظر هزینه و میزان اعتماد مورد نیاز بررسی می‌کنیم.

۱.۵ پیاده‌سازی

در پیاده‌سازی این کار نیازمندی ابزاری برای ایجاد یک زنجیره‌ی قالبی خصوصی با روش تفاوت PBFT هستیم. برای این کار از hyperledger fabric^۱ 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. این ابزار به کمک NodeJS نوشته شده است و به کمک داکر^۲ به سادگی تعدادی نود با یک بلاک‌چین خصوصی ارائه می‌کند. همچنین به کمک نوشتن قراردادهای هوشمند بر روی این بستر می‌توانیم حوزه‌های مورد نیاز را ایجاد کنیم.

مسئله‌ی بعدی روش ایجاد اثبات‌های بی‌دانش است. برای ایجاد تراکنش‌های شمارش نیاز به اثبات‌های بی‌دانش داریم. برای برای ساخت اثبات‌های بی‌دانش از کتابخانه‌ی libsnark^۳ استفاده شده است. این کتابخانه از الگوریتم پینوکیو با زبان C++ پیاده کرده است و توسط Zcash - یکی از بزرگ‌ترین ارزهای دیجیتال با توانایی تراکنش ناشناس - نیز برای ساخت اثبات استفاده شده است.

در فرایند کامپایل این کتابخانه از تنظیمات موجود در جدول ۱.۵ استفاده شده است.

بقیه‌ی تنظیمات کتابخانه در حالت پیش‌فرض استفاده شده است.

^۱ <https://www.hyperledger.org/projects/fabric>

^۲ Docker

^۳ <https://github.com/scipr-lab/libsnark>

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

۲.۵ نزدیکی به رای گیری ایده آل

در این بخش نیازمندی های رای گیری ایده آل را دوره می کنیم و می بینیم که سیستم ارائه شده چگونه هر کدام از نیازمندی ها را رفع می کند.

- می دانیم که هر شخصی حداکثر یک رای می تواند بدهد چون که در حساب کلید عمومی آن فرد دقیقاً یک رای در ابتدای رای گیری وجود دارد. از طرفی می دانیم که سیستم مانع رای دادن فردی نمی شود چرا که رای دهنده می تواند بررسی کند که رای او در زنجیره ی قالبی مصرف شده باشد.
- می دانیم کسی نمی تواند به جای دیگری رای دهد، چرا که برای رای دادن هم نیاز به دسترسی به کلید خصوصی دارد و هم کلید عمومی فرد با اطلاعات شناسایی او در حوزه مقایسه می شود.
- با اضافه شدن گزینه ی ممتنع و حفظ امنیت فیزیکی حوزه ی رای گیری می توانیم اطمینان حاصل کنیم که کسی مجبور به رای دادن نمی شود.
- هیچ کسی مجبور به رای دادن به شخص خاصی نمی شود چرا که راهی برای چک کردن رای فرد بعد از فرایند رای گیری وجود ندارد، در نتیجه به دلیل امن بودن حوزه ی رای گیری، رای دهنده همواره می تواند به کاندیدای دلخواه خود رای دهد ولی این عمل را انکار کند.
- در انتهای انتخابات می توانیم به سادگی با بررسی تعداد تراکنش های ثبت و شمارش از درستی شمارش آرا

اطمینان حاصل کنیم. هر شخصی نیز با بررسی این که عمل ثبتي برای او در زنجیره‌ی قالبی وجود دارد می‌تواند از شماره‌دهی شدن رای خود اطمینان حاصل کند.

- نتیجه‌ی آرا ناشناس باقی می‌ماند چرا 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.
- در هر زمانی که یک بلوک جدید در زنجیره‌ی قالبی ثبت شود می‌توان با استناد به حساب‌های کاندیداها از نتیجه‌ی آن لحظه‌ی انتخابات مطلع شد. در صورتی هم که مجری انتخابات نخواهد که نتایج لحظه‌ای را منتشر کند می‌تواند زنجیره‌ی قالبی را تا پایان انتخابات بسته نگه دارد.

۳.۵ 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 می‌کنیم.

۱.۳.۵ 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 آن جایی 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 کامپیوتر 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.

۲.۳.۵ اطمینان از شمارش درست

شاید مهمترین شرط برگزاری یک انتخابات میزان اطمینان از شمارش درست آرا در آن باشد. در این بخش به بررسی نحوه‌ی 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. طبیعتاً این مدل شمارش به دلیل دخالت انسانی احتمال خطای نسبتاً 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 رمز شده 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 هزینه‌ی 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.

۳.۳.۵ 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. همچنین 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 خطا کار 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 خطا کار مشخص می‌شود.

۴.۳.۵ 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 رای دادن کاربر در روش‌هایی که بررسی می‌کنیم به سه حالت خواهد بود:

- در روش سنتی و رای‌گیری بدون زنجیره‌ی قالبی کاربر برای رای دادن صرفاً 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 کاربری 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 رای دادن 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 کاربر وجود دارد که خود این مسئله نیز نیازمند بررسی امنیتی 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.

۵.۳.۵ 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 همچنین 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 برگه‌ی رای‌های غلط هزینه‌ی اندکی ندارد ولی در انتخابات‌های حساس ممکن است به صرفه باشد و در صورت اتفاق افتادن همچنین مسئله‌ای، راه حل سیستمی برای پیدا کردن مشکل وجود ندارد. همچنین 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 آن جایی 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 هزینه‌ی زیاد	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

فصل ۶

نتیجه‌گیری و کارهای آتی

۱.۶ نتیجه‌گیری

تحقیقات در راستای ایجاد رای‌گیری امن قبل از فراگیری تکنولوژی زنجیره‌ی قالبی بسیار نادر بود اما با فراگیری این تکنولوژی و کاربردهای آن تحقیقات جدید و خلاقانه‌ای در این زمینه انجام شده است. در این تحقیق روش‌های استفاده شده در رای‌گیری‌های الکترونیکی را بررسی کردیم. سپس زنجیره‌ی قالبی را به عنوان یک ابزار برای کاهش نیاز به شخص مورد اعتماد در رای‌گیری استفاده کردیم تا یک رای‌گیری با توانایی ردگیری خطا از مجری انتخابات و حوزه‌ها بسازیم. همینطور نشان دادیم که کم کردن نیاز به اعتماد لزوماً به معنی کاهش حریم خصوصی نیست و با استفاده از اثبات‌های بی‌دانش پروتکل امنی برای شمارش رای بدون به خطر انداختن حریم خصوصی رای‌دهنده ارائه دادیم.

با استفاده از این روش رای‌گیری می‌توان یک رای‌گیری الکترونیکی امن برگزار کرد که علاوه بر هزینه‌ی بسیار کمتر از روش‌های سنتی، باعث افزایش اطمینان رای‌دهندگان و ناظران انتخابات به درستی آن نیز می‌شود.

۲.۶ کارهای آتی

روش توافق استفاده شده در این تحقیق به ما اطمینان می‌دهد که زنجیره‌ی قالبی موجود در حوزه‌ها همواره با هم همخوان می‌ماند. این ویژگی برای کاربرد ما بسیار مناسب است اما باعث می‌شود که در صورت خطا کار بودن بیش از یک سوم حوزه‌ها کل فرایند رای‌گیری - حتی برای حوزه‌های درست کار - متوقف شود. استفاده از روش‌هایی مانند Clique که در نهایت همخوان می‌شوند یا تغییر در ساختار زنجیره‌ی قالبی مورد استفاده به گونه‌ای که بتواند چند زنجیره‌ی درست را با هم تبدیل به یک زنجیره کند باعث می‌شود حتی در صورتی که حتی نیمی از حوزه‌ها خطا کار باشند رای‌گیری برای بقیه‌ی حوزه‌ها درست انجام شود. این تغییر می‌تواند به امنیت و مقیاس‌پذیری روش انتخابات کمک شایانی کند.

مراجع

- [1] Y. E. Ben-Sasson, I. Bentov and M. Riabzev, "Pinocchio : nearly practical verifiable computation," *IEEE Symposium on Security and Privacy*, pp.238-252, 2013.
- [2] Y. E. Ben-Sasson, I. Bentov and M. Riabzev, "Scalable zero knowledge with no trusted setup," *Annual International Cryptology Conference*, pp.701-732, 2019.
- [3] D. Chaum, "Security without identification : Transaction systems to make big brother obsolete," *Communication of the ACM*, vol.28, no.1, pp.1030-1044, 1985.
- [4] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology Proceedings of Crypt*, vol.82, no.3, pp.199-203, 1983.
- [5] 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.
- [6] L. F. Cranor and R. K. Cytron, "Sensus : A security-conscious electronic polling system for the internet," *Proceedings of the Hawaii International Conference on System Sciences*, 1997.
- [7] B. W. DuRette, "multiple administrators for electronic voting," *B.Sc thesis, MIT*, 1999.
- [8] B. N. L. M. Wright, M. Adler and C. Shields, "an analysis of the degradation of anonymous protocols," *In Proceedings of Network and Distributed System Security Symposium*, 2002.
- [9] B. S. R. Cramer, M. Franklin and M. Yung, "Multi-authority secret-ballot elections with linear work," *LNCS 1070, Advances in Cryptology - EUROCRYPT*, pp.72-83, 1996.
- [10] 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.
- [11] 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.
- [12] N. L. R. DeMillo and M. Merritt, "Cryptographic protocols," *Proceedings of the 14th Annual Symposium on the Theory of Computing*, pp.383-400, 1984.

- [13] D. Malkhi and E. Pavlov, "Anonymity without 'cryptography'," *Proceedings of Financial Cryptography*, pp.117-135, 2001.
- [14] O. D.Malkhi and E.Pavlov, "E-voting without 'cryptography'," *In International Conference on Financial Cryptography*, pp.1-15, 2002.
- [15] R. Osgood, "The future of democracy: Blockchain voting," *COMP116: Information Security*, 2016.
- [16] N. Szabo, "Smart contracts," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Lecture/01_16_SmartContracts.html, 1993.
- [17] C.-L.-B. L.Vo-Cao-Thuy, K.Cao-Minh and T.A.Nguyen, "Votereum: An ethereum-based e-voting system," *IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*, pp.1-6, 2019.
- [18] 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.
- [19] "Ethereum foundation, ethereum whitepaper, a next-generation smart contract and decentralized application platform,"" <https://github.com/ethereum/wiki/wiki/White-Paper>", 2014.
- [20] 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.
- [21] 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.
- [22] 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.
- [23] 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.
- [24] 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.
- [25] 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.

- [26] S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system," 2008.
- [27] A. beck, "Hashcash : a denial of service counter-measure," 2008.
- [28] S. S.King, "Ppcoin : Peer-to-peer crypto-currency with proof-of-stake.,", *self-published paper*, 2012.
- [29] N. D.Schwartz and A.Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, 2014.
- [30] B.Chase and E.MacBrough, "Analysis of the xrp ledger consensus protocol," *Ripple Labs Inc White Paper*, 2018.
- [31] D.Mazieres, "The stellar consensus protocol : A federated model for internet-level consensus," 2015.
- [32] S. Z.Galil and M.Yung, "Symmetric public-key encryption," *Conference on the Theory and Application of Cryptographic Techniques. Springer,*, 1985.
- [33] 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.
- [34] 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.
- [35] 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.
- [36] 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.
- [37] N. Saberhagen, "Cryptonote v 2.0," <https://cryptonote.org/whitepaper.pdf>, 2013.
- [38] B.Goodell1 and S.Noether2, "Thring signatures and their applications to spender-ambiguous digital currencies," *Monero Research Lab*, 2018.
- [39] 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.
- [40] C. M. I. E. E.B.Sasson, A.Chiesa and M.Virza, "Zerocash : Decentralized anonymous payments from bitcoin," *2014 IEEE Symposium on Security and Privacy*, pp.459-474, 2014.
- [41] J. Benaloh and M. de Mare, "One-way accumulators : a decentralized alternative to digital signatures," *Advances in Cryptology — EUROCRYPT*, pp.274-285, 1993.

-
- [42] E. Brewer, "Cap twelve years later : How the "rules" have changed," *Computer*, vol.45, no.2, pp.23-29, 2012.
- [43] "Aura," <https://wiki.parity.io/Aura>.
- [44] "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. Maghsoud Abbaspour

2018