



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 بلاک چین

استاد راهنما: دکتر مقصود عباس پور

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 روش‌های 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
۲۰	روش توافق	۱.۲.۳
۲۰	توافق در ارزش های دیجیتال	
۲۰	اثبات سهم	
۲۱	روش Ripple Consensus Protocol	
۲۱	روش Stellar Consensus Protocol	
۲۱	روش Aura	
۲۲	روش Clique	
۲۲	روش Practical Byzantine Fault Tolerance	
۲۳	اثبات های بی دانش	۳.۳
۲۳	پروتکل های مبتنی بر اثبات بی دانش	

۲۵	روش پیشنهادی	۴
۲۷	تعریف نقش ها	۱.۴
۲۷	شرایط مسئله ی رای گیری الکترونیک	۲.۴
۲۸	مفروضات مسئله	۳.۴
۲۹	پروتکل ثبت رای	۴.۴
۲۹	مثال شهودی	۱.۴.۴
۳۱	فرایند رای گیری از نگاه کاربر	۲.۴.۴

۳۱	قبل از رای گیری	
۳۱	در حوزه ی رای گیری	
۳۲	فرایند رای گیری از دید حوزه	۳.۴.۴
۳۲	تراکنش ها	
۳۳	فرایند ثبت رای کاربر	
۳۵	ناشناسی رای گیری	
۳۵	فرایندهای توزیع شده	۵.۴
۳۶	شمای کلی	۱.۵.۴
۳۶	اضافه شدن بلوک	۲.۵.۴

۵ تحلیل و ارزیابی ۳۸

۳۹	پیاده سازی	۱.۵
۴۰	معیارهای رای گیری مناسب	۲.۵
۴۱	نزدیکی به رای گیری ایده آل	۳.۵
۴۲	مقایسه با کارهای مشابه	۴.۵
۴۲	روش های رای گیری دیگر	۱.۴.۵
۴۳	موارد حذف شده از مقایسه	
۴۴	هزینه ی اطمینان از شمارش درست	۲.۴.۵
۴۴	حریم خصوصی	۳.۴.۵
۴۵	هزینه برگزاری	۴.۴.۵
۴۵	هزینه برای کاربر	
۴۶	هزینه انتخابات برای مجری	
۴۷	توانایی ردگیری خطا	۵.۴.۵
۴۹	احتمال ناهمخوانی در زنجیره ی قالبی	۵.۵

۴۹ قضیه‌ی CAP

۵۲ نتیجه‌گیری و کارهای آتی ۶

۵۳ نتیجه‌گیری ۱.۶

۵۳ کارهای آتی ۲.۶

۵۴ مراجع

فهرست تصاویر

۹	یک درخت مرکب	۱.۲
۱۲	یک نمونه مدار محاسباتی	۲.۲
۲۲	روش PBFT	۱.۳
۲۶	شمای منطقی سامانه	۱.۴
۳۰	شمای شهودی	۲.۴
۳۳	تراکنش ثبت	۳.۴
۳۳	تراکنش شمارش	۴.۴
۳۴	فرایند ثبت رای در حوزه	۵.۴
۳۶	شمای منطقی سامانه	۶.۴

فهرست جداول

۹ انواع زنجیره‌ی قالبی	۱.۲
۴۰ تنظیمات libsnark	۱.۵
۴۸ مقایسه‌ی روش‌های رای‌گیری	۲.۵
۵۱ روش توافق	۳.۵

چکیده

رای گیری یکی از حساس ترین از سال ۲۰۰۹ تاکنون، با فراگیری بیت کوین شاهد افزایش کاربردهای بلاک چین و سیستم های توزیع شده و بدون نیاز به اعتماد بوده ایم. بعد از انتشار بستر اتریوم تا به امروز قراردادهای هوشمند توزیع شده در این بستر رشد قابل توجهی داشته اند. به همین دلیل بررسی امنیتی قراردادهای این بستر اهمیت ویژه ای دارد. همچنین با ساخت این بستر فرصت مناسبی است تا سرویس های بیشمار مبتنی بر اعتماد فعلی خود و راه های جایگزین آن ها را در بستر بلاک چین بررسی کنیم. در این تحقیق ابتدا به معرفی ارزهای دیجیتال و نحوه ی کارکرد آن ها می پردازیم، سپس تحقیقات امنیتی خود بسترها و کاربردهای آن ها را بررسی کرده و در نهایت به کاربرد آن ها برای رای گیری دیجیتال و چالش های این کار اشاره خواهیم کرد.

واژگان کلیدی: بلاک چین، رای گیری الکترونیک، امنیت

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 سامانه‌ی 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 روش‌های 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 روش‌های 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 رای‌گیری امنیت و حریم خصوصی است. مخالفین رای‌گیری الکترونیک از کم هزینه بودن تقلب و تغییر رای‌های ثبت شده در انتخابات الکترونیک می‌گویند و رد کاغذی در یک انتخابات را یک فاکتور مهم برای امنیت آن می‌دانند. هزینه تغییر میلیون‌ها رای در یک سامانه‌ی 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 سامانه‌ی 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 سامانه‌ی 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 سامانه‌های رای‌گیری الکترونیک اعلام شده است.

برای مثال یک تحقیق معروف از دانشگاه NYU در سال ۲۰۱۵^۱ توضیح داد که ماشین‌های رای‌گیری الکترونیک 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 سامانه‌های 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 سامانه‌های رای گیری کاملاً الکترونیکی برای انتخابات‌های مهم و بزرگ هستند که یک سامانه رای گیری مناسب باید آن‌ها را تا جای ممکن رفع کند.

۴.۱ انگیزه و هدف

هدف این تحقیق، طراحی یک سامانه‌ی 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 سامانه‌های توزیع شده بدون نیاز به اعتماد (برای مثال بیت کوین به عنوان یک ارز دیجیتال بدون نیاز به اعتماد)، پلتفرم‌هایی برای رای گیری الکترونیک ایجاد شدند که امنیت شمارش آرا را با عمومی ساختن فرایند رای گیری تامین می‌کردند. با وجودی که راه حل ارائه شده‌ی این روش‌ها مسئله‌ی اطمینان از شمارش رای‌ها را حل می‌کرد، مسئله‌ی حریم شخصی در این روش‌ها حل نشده است و انتخابات‌های برگزار شده با این سامانه‌ها 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 روش‌های 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 سامانه‌های 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 روش‌ها خواهد بود. هدف ما در این تحقیق این است که سامانه‌ای ارائه کنیم که امنیت شمرده شدن آرا را، مانند این سامانه‌ها ارائه کند و در عین حالت حریم خصوصی رای‌دهنده را به طور کامل حفظ کند.

نتیجه‌ی این تحقیق یک روش رای گیری الکترونیک است که قیاس با روش‌های سنتی انتخابات هزینه‌ها را

کاهش خواهد داد. در عین حال کمترین تغییر برای رای دهندگان خواهد داشت که باعث افزایش دسترس پذیری این سامانه 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 سامانه یک رد الکترونیک غیرقابل 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 پایه‌ی به کار برده شده در این تحقیق می‌پردازیم. در ابتدا با مفاهیم زنجیره‌ی قالبی، انواع و کاربردهای آن آشنا می‌شویم و در ادامه به بررسی اثبات‌های بی‌دانش می‌پردازیم. این دو تکنولوژی ابزارهای تئوری لازم برای ساخت سامانه 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 نگه می‌دارد. 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 نگه داشته 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. با توجه به این نوع ساختار درخت مرکل، هر تغییری در درخت باعث تغییر هش در ریشه‌ی آن خواهد شد و به دلیل تصادفی بودن خروجی یک هش خوب، هش ریشه‌ی درخت مرکل هیچ ویژگی قابل پیشبینی ندارد.

۲.۱.۲ انواع زنجیره‌ی قالبی

در این تحقیق زنجیره‌های قالبی را از دو نظر دسته‌بندی می‌کنیم. زنجیره‌های قالبی می‌توانند عمومی یا خصوصی باشند، در زنجیره‌های قالبی عمومی اضافه کردن بلوک به زنجیره‌ی قالبی نیاز به دسترسی خاصی ندارد

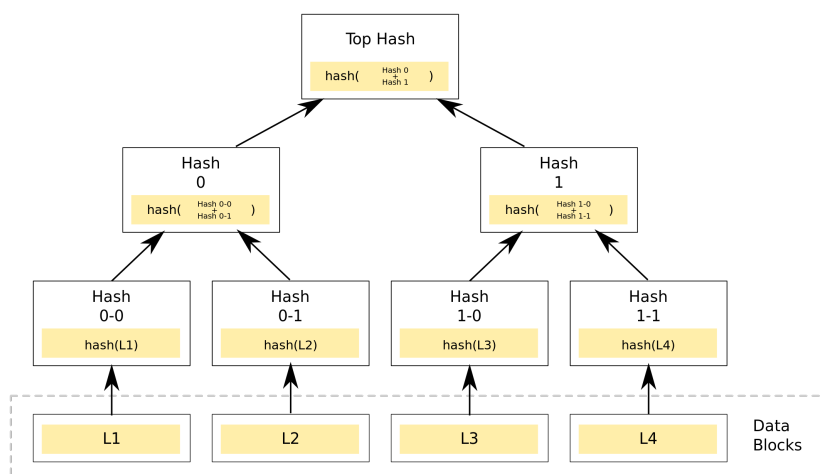
^۱ Linked list

^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 زنجیره‌های قالبی خصوصی اضافه کردن بلوک تنها توسط افراد خاص ممکن است.

روش دیگر تقسیم‌بندی ما باز یا بسته بودن زنجیره‌ی قالبی است که در رابطه با دسترسی خواندن اطلاعات در این زنجیره می‌باشد. در زنجیره‌های قالبی بسته خواندن اطلاعات توسط عموم آزاد نیست. در حالی که دو نوع باز آن تمام اطلاعات زنجیره برای خواندن در دسترس عموم است.

با توجه به کاربرد زنجیره‌ی قالبی مورد نظر هر زنجیره می‌تواند در هر یک 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 در آن «اثبات‌کننده» می‌تواند به «بررسی‌کننده» نشان دهد که او یک راز - مثلاً خروجی یک عملیات کامپیوتری - را می‌داند، بدون این که به او 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 در رابطه با درست بودن گزاره ارائه کند.

- بی‌دانش: اگر اثبات درست باشد، بررسی‌کننده هیچ اطلاعاتی فراتر از درست بودن گزاره 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 درست بودن جواب آلیس، باب می‌داند که با احتمال ۷۵٪ او تفاوتی بین دو توپ می‌بیند. این فرایند آنقدر تکرار می‌شود تا باب با احتمال دلخواه خود از ادعای آلیس اطمینان حاصل کند.

^۱ Zero knowledge proofs

نکته‌ی مهم در مثال بالا این است که حتی اگر باب این فرایند را ضبط کرده باشد، نمی‌تواند به کس دیگری ثابت 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 طول فرایند باب برای تصمیم‌گیری در تعویض کردن یا نکردن توپ‌ها 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 به 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 پیام 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. همچنین 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:

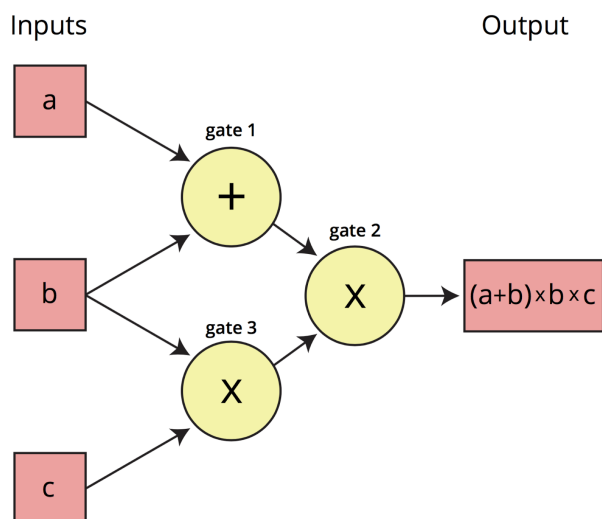
- مختصر^۲: تولید و بررسی شاهد از انجام محاسباتی که اثبات می‌شود کوتاه‌تر (معمولاً از مرتبه‌ی زمانی $(\log N)^2$) است.
- بی‌تعامل^۳: نیازی به پیامی از بررسی‌کننده برای تولید شاهد نیست.

^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 نمی‌توان 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 و 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 قبل از تولید اثبات انتخاب شده باشند. در این فاز آماده‌سازی تعدادی عدد تصادفی برای انتخاب این نقاط تولید می‌شوند که بعد از آن 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. 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 سامانه 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 خروجی این چندجمله‌ای یک درخت مرکب ساخته می‌شود که خروجی‌های چندجمله‌ای را به ازای ورودی‌های مختلف 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 مرکب به عنوان ورودی به تابع شبه‌تصادفی^۴ استفاده می‌شود که مشخص می‌کند خروجی کدام شاخه‌ها باید در شاهد ظاهر شود.

^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 خصوصیت‌های یک سامانه رای گیری مناسب امنیت شمارش آرا و حفظ حریم خصوصی رای‌دهنده است، این دو موضوع پایه‌های طراحی یک سامانه رای گیری امن خواهند بود. سامانه‌های رای گیری الکترونیک قبل از تکنولوژی زنجیره‌ی قالبی از روش‌های متعددی برای تحقق این هدف استفاده می‌کردند اما تقریباً در تمامی این روش‌ها نیاز به اعتماد به مجری انتخابات وجود دارد.

طراحی زنجیره‌های قالبی همراه به کمک روش‌های توافق خلاقانه باعث ایجاد ارزش‌های دیجیتال بدون نیاز به یک شخص (بانک) مورد اعتماد شد. در ادامه این ساختار داده‌ی اکیدا افزایشی برای حذف نیاز به اعتماد در کاربردهای دیگر نیز استفاده شده است. زنجیره‌ی قالبی در این تحقیق نیز به عنوانی ابزاری که با ایجاد شفافیت نیاز به اعتماد را کاهش می‌دهند استفاده می‌شود.

شفافیت در انتخابات خود باعث ایجاد مشکلاتی برای امنیت رای‌دهندگان می‌شود. عدم حفظ حریم خصوصی رای‌دهنده در یک انتخابات می‌تواند باعث شود رای‌دهنده نتواند به کاندیدای دلخواهش رای دهد یا تحت فشار مجبور به رای دادن شود. برای رفع این مسئله از روش‌هایی مانند اثبات‌های بی‌دانش استفاده می‌شود. اثبات‌های بی‌دانش این امکان را ایجاد می‌کنند تا حتی با حفظ حریم خصوصی کاربر، درستی شمارش انتخابات اثبات گردد. در این بخش ابتدا روش‌های مختلف رای گیری الکترونیک را بررسی می‌کنم و روش‌های استفاده شده برای حفظ امنیت و حریم خصوصی را تحلیل می‌کنیم. در ادامه تکنولوژی زنجیره‌ی قالبی را به عنوان ابزاری برای کاهش نیاز به اعتماد و ایجاد شفافیت بررسی می‌کنیم و در نهایت اثبات‌های بی‌دانش را به هدف ناشناس نگه داشتن رای گیری بررسی می‌کنیم.

۱.۳ رای‌گیری الکترونیک

رای‌گیری الکترونیک را به طور کلی توانیم به دو دسته‌ی رای‌گیری تماماً الکترونیک و رای‌گیری به کمک ابزارهای الکترونیکی تقسیم کرد. روش‌های دسته‌ی دوم مبتنی بر رای‌گیری سنتی هستند و از ابزارهای الکترونیکی صرفاً برای کاهش هزینه و افزایش دسترسی‌پذیری استفاده کنند. از این روش‌ها توان به ابزارهای شمارش رای خودکار و یا دستگاه‌های ثبت رای الکترونیک که خروجی آن‌ها یک برگه‌ی رای کاغذی^۱ است اشاره

^۱ Direct-recording electronic voting systems (DRE)

کرد. در این تحقیق این ابزارها را بررسی ن‌کنیم و منظور از رای‌گیری الکترونیک، دسته‌ی اول یا رای‌گیری تماماً الکترونیک است.

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

۱.۱.۳ رای‌گیری الکترونیک متمرکز

در این روش‌ها یک سامانه‌ی مرکزی وجود دارد که تمامی آرا در آن ذخیره می‌شوند. در این روش‌ها 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 سامانه‌ها 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 تاییدکننده‌ی اطلاعات، 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 [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

^۱ Anonymous communication channel

^۲ Blind signature

ناشناس است.

۲.۱.۳ رای گیری الکترونیک توزیع شده

رای گیری الکترونیک توزیع شده را به سه دسته ی رای گیری های بدون زنجیره ی قالبی، با زنجیره ی قالبی عمومی و با زنجیره ی قالبی خصوصی تقسیم می کنیم. با توجه به این که در رای گیری احراز هویت یک مسئله ی مهم است همه ی این سامانه ها از زنجیره ی قالبی های بسته استفاده می کنند.

رای گیری بدون زنجیره ی قالبی

بعضی سامانه های طراحی شده برای رای گیری الکترونیک [۹][۱۰][۱۱] از روش های تقسیم راز^۱ استفاده می کنند. در این روش ها فرایند ثبت رای باید به تایید تعدادی از حوزه ها برسد که باعث کاهش نیاز به اعتماد می شود. در این روش ها می توان اثبات کرد که برای ردیابی یک رمز حداقل k حوزه باید تبانی کنند. مشکل بزرگ این روش ها عدم وجود یک الگوریتم مقیاس پذیر برای تقسیم راز است.

روش دیگری که برای رای گیری توزیع شده استفاده شده است، استفاده از بردار بررسی^۲ [۱۲] است. در این روش ها بررسی درستی رای ها کاملاً توزیع شده است، اما نیاز به ارتباط دو به دوی تمامی رای دهنده ها دارد که در یک انتخابات واقعی شدنی نیست. ترکیبی از این روش و تقسیم راز باعث ایجاد پروتکل هایی [۱۳][۱۴] شد که با سطح بندی حوزه ها و تقسیم رای ها و مخلوط کردن آن ها از حریم خصوصی حمایت می کنند، اما این روش ها به حوزه ها و رای دهندگان توانایی بررسی درستی برگه رای ها را نمی دهد و امکان ایجاد رای های اشتباه و جلوگیری از رای دادن یک فرد خاص را ایجاد می کنند.

رای گیری با زنجیره ی قالبی عمومی

با فراگیر شدن تکنولوژی زنجیره ی قالبی [۱۵]، محصولات در زمینه ی رای گیری الکترونیک به کمک این تکنولوژی ساخته شدند. تعدادی از این سامانه های رای گیری در قالب قراردادهای هوشمند^۳ [۱۶] ساخته

^۱ Secret sharing

^۲ Check vector

^۳ Smart contract

شده‌اند که از آن‌ها می‌توان به‌ترتیب^۱ [۱۷] و یا سامانه‌ی ارائه شده توسط E.Yavuz [۱۸] در بستر اتریوم^۲ [۱۹] - که یک ارز دیجیتال و یک بستر قرارداد هوشمند است - اشاره کرد. مزیت این نوع رای‌گیری‌ها هزینه‌ی اولیه کم برای استفاده از آن‌هاست، اما همچنین خطر اشتباه برنامه‌نویسی [۲۰][۲۱][۲۲] 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 هزینه‌های رای‌گیری خواهد شد. مسئله‌ی دیگر در بستر اتریوم هم وابستگی سامانه‌ی 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.

رای‌گیری با زنجیره‌ی قالبی خصوصی

از سامانه‌های رای‌گیری با زنجیره‌ی قالبی خصوصی می‌توان به‌توبوک^۳ [۲۳] توسط شرکت Kaspersky که یک شرکت پیشرو در زمینه‌ی امنیت است اشاره کرد. فلسفه‌ی ساخت این سامانه به‌صورتی است که تلاش می‌کند برای کاربرانی که از روش‌های رای‌گیری فعلی استفاده می‌کنند کمترین تغییر در رفتار نیاز باشد. برای رای دادن در به کمک این سامانه رای‌دهندگان باید برای رای دادن یک شناسه برای احراز هویت - مانند شماره‌ی کارت ملی - و محل رای دادن خود را مشخص کنند. در ادامه در محل رای‌گیری به کمک شناسه‌ی ثبت شده رای خود را ثبت می‌کنند و یک شماره‌ی رای برای پیگیری درستی رای دریافت می‌کنند. هر کسی با داشتن این دو عدد می‌تواند نتیجه‌ی رای را بررسی کند و از درستی آن آگاه شود.

از مثال‌های دیگر سامانه‌های رای‌گیری مبتنی بر زنجیره‌ی قالبی می‌توان به استارت‌آپ Follow My Vote اشاره کرد. نحوه‌ی کار این سامانه با‌توبوک تفاوت اساسی دارد و برای رای دادن احتیاج است که نرم‌افزاری به‌روی کامپیوتر و یا تلفن همراه کاربر نصب شود. این روش طراحی سامانه، 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 سامانه‌های رای‌گیری مبتنی بر زنجیره‌ی قالبی موجود در حال حاضر VoteWatcher ساخته

^۱ Votereum

^۲ Ethereum

^۳ VoteBook

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 سامانه شمارش شده است.

مدل اسفاده‌ی VoteWatcher به روش VoteBook بسیار شبیه است و تفاوت رفتاری زیادی با مدل‌های رای‌گیری الکترونیک فعلی برای کاربران ندارد. در این محصول طبق نیاز رای‌گیری می‌توان از یک زنجیره‌ی قالبی عمومی یا خصوصی استفاده کرد.

تلاش‌های دیگری نیز در این حوزه برای افزایش توانایی ردگیری در انتخابات شده است [۲۴] اما به دلیل کندی نسبی، این روش‌های رای‌گیری نیاز به تقسیم رای‌گیری به چند رای‌گیری کوچک‌تر دارند و قابل استفاده در رای‌گیری‌های واقعی نیستند.

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 به 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 آن‌ها می‌پردازیم.

توافق در ارزهای دیجیتال

روشی که S.Nakamoto [۲۶] برای رفع این مسئله در بیت‌کوین استفاده کرده است، اثبات کار^۳ 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^۴ [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.

^۱ The Byzantine generals problem

^۲ کار اثبات

^۳ Proof of work

^۴ proof of stake

روش 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.

روش 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.

روش Aura

یکی از روش‌هایی که معمولاً در زنجیره‌های قالبی خصوصی استفاده می‌شود Aura [۴۴] نام دارد. در این روش یک نود رهبر برای اضافه کردن بلوک‌های جدید انتخاب می‌شود و در طول زمان در دوره‌های مشخصی رهبر تغییر می‌کند. برای انتخاب زمان تغییر از ساعت unix استفاده می‌شود که می‌تواند در اثر همگام^۱ نبودن ساعت نودهای حاضر در شبکه در یک لحظه دو رهبر وجود داشته باشد. این باعث از بین رفتن همخوانی در سامانه می‌شود ولی سامانه همواره در دسترس خواهد بود.

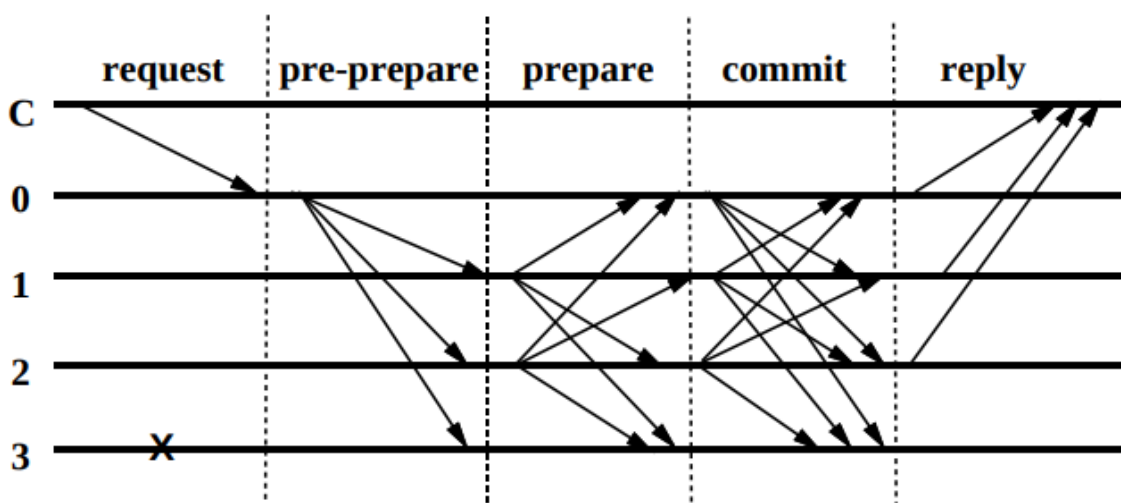
^۱ sync

روش Clique

از روش‌های پرکاربرد دیگر در زنجیره‌های قالبی خصوصی می‌توان به Clique [۴۵] اشاره کرد. 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.

روش Practical Byzantine Fault Tolerance

در این روش [۳۲] نودهای حاضر در زنجیره‌ی قالبی به ترتیب اولویت چیده می‌شوند و برای ثبت هر بلوک جدید، بلوک آماده‌شده را به رهبر (نودی با بیشترین اولویت) داده می‌شود و نود رهبر آن را به تمامی حوزه‌های دیگر ارسال می‌کند. سپس تمامی نودهای دیگر بعد از تایید نتیجه را برای هم ارسال می‌کنند و در صورت موفقیت آن را ثبت می‌کنند، بعد از تایید نتایج برای نودی ابتدایی ارسال شده و ثبت نهایی می‌شود. همچنین بعد از اضافه شدن هر بلوک حوزه‌ی رهبر تغییر می‌کند و به نفر بعدی در زنجیره‌ی اولویت می‌رسد. همچنین در صورت جواب ندادن حوزه‌ی رهبر در مدت زمان مشخص یا جواب‌های غلط دادن مسئولیت به نفر بعدی منتقل می‌شود.



شکل ۱.۳: روش PBFT

در این روش حداکثر تعداد تعداد نودهایی که باید خطا کار باشند تا بلوک اشتباهی در زنجیره‌ی قالبی ثبت شود برای $1 + 3f$ نود f نوداست.

۳.۳ اثبات‌های بی‌دانش

اثبات‌های بی‌دانش اولین بار در سال ۱۹۸۵ [۳۳] 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 [۳۴][۳۵] 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 [۳۶] مرحله‌ی آماده‌سازی را حذف می‌کند

پروتکل‌های مبتنی بر اثبات بی‌دانش

از این تحقیقات می‌توان به بستر HAWK [۳۷] اشاره کرد. در این تحقیق به کمک یک تعریف کلی از زنجیره‌ی قالبی به عنوان سامانه که همواره در دسترس است و هیچ اطلاعات اشتباهی 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 سامانه، مبتنی بر ایجاد آدرس‌های

^۱ Pinocchio

مقصد یکتا به ازای هر تراکنش است.

مونرو^۱ که یک ارز دیجیتال است که بر اساس الگوریتم Cryptonote [۳۸] 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 [۳۹] برای مخفی کردن پرداخت‌کننده‌ی سکه نیز ارائه کرد.

از کارهای دیگر در این زمینه می‌توان به zerocoin [۴۰] 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 [۴۱] استفاده شد. این ارز دیجیتال دو مدل سکه‌ی قابل ردگیری و غیرقابل ردگیری دارد و هر کسی می‌تواند طی یک تراکنش سکه‌های خود را به سکه‌های ناشناس تبدیل کند.

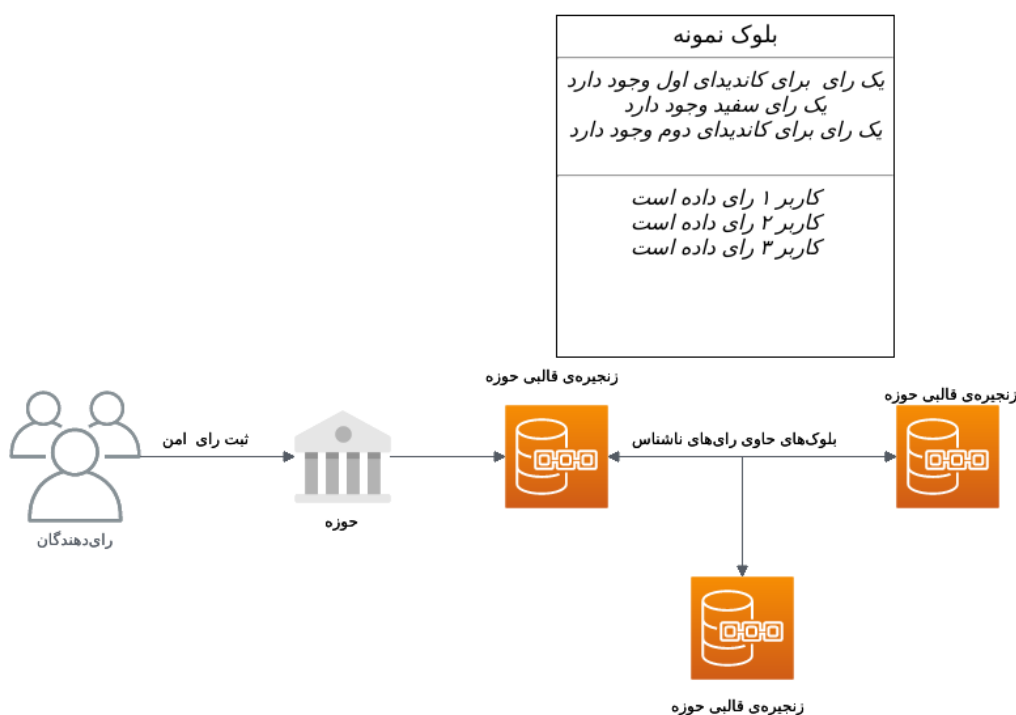
^۱ Monero

^۲ Ring Signature

فصل ۴

روش پیشنهادی

در این بخش یک روش برای رای گیری الکترونیک توزیع شده و مبتنی بر زنجیره ی قالبی ارائه می شود. در این روش برخلاف تلاش های مشابه برای ایجاد روش های رای گیری امن، ناشناسی آرا به صورت کامل حفظ می شود. برای حل این مسئله به دو پروتکل امن نیاز داریم: یکی بین کاربر و حوزه ی رای گیری و دیگری برای به اشتراک گذاری اطلاعات بین حوزه ها. شکل ۱.۴ شمای منطقی سامانه را نشان می دهد، دو پروتکل ارائه شده با استفاده از زنجیره ی قالبی، نیاز به یک شخص مورد اعتماد را در رای گیری حذف می کنند.



شکل ۱.۴: شمای منطقی سامانه

روش پیشنهادی ما سه هدف کلی دارد: ۱- هر رای دهنده از شمارش درست رای خود اطمینان حاصل کند ۲- حریم خصوصی حفظ شود ۳- هر خطا در فرایند رای گیری قابل تشخیص باشد. برای رسیدن به این اهداف باید فرایند به گونه ای طراحی شود که هیچ فردی معتمد فرض نشود. برای این کار ابتدا شرایط و مفروضات 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 سامانه ارائه می کنیم و در نهایت با استفاده از یک روش توافق مناسب امنیت پروتکل در حالت توزیع شده را فراهم می کنیم.

۱.۴ تعریف نقش‌ها

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

- **ناظر انتخابات:** این سازمان مسئول بررسی صحت انتخابات و احراز هویت شرکت‌کنندگان در انتخابات است. به این سازمان فقط در حوزه‌ی احراز هویت اعتماد می‌شود. همچنین این سازمان بررسی‌کننده‌ی نهایی درست بودن انتخابات است و باید بتواند از آن اطمینان حاصل کند.
- **رای‌دهنده:** فردی که حق رای به یک کاندیدا را دارد، این فرد اختیار استفاده کردن یا نکردن از رأی خورا داشته و می‌تواند تلاش کند که چند بار رای دهد. باید بتواند از درستی انتخابات اطمینان حاصل کند زیرا ممکن است توسط یک رقیب بدخواه برای رای دادن تحت فشار قرار بگیرد.
- **حوزه‌ی انتخابات:** محلی که در آن رای داده می‌شود، باید به گونه‌ای باشد که امنیت فیزیکی افراد را تامین کند. در عین حال ممکن است برای خراب کردن انتخابات یا نقض حریم خصوصی کاربران تلاش کند.

۲.۴ شرایط مسئله‌ی رای‌گیری الکترونیک

شروط لازم برای روش رای‌گیری ارائه شده عبارت‌اند از:

۱. هر فرد واجد شرایط دقیقاً یک بار بتواند رای دهد.
۲. هیچ‌کسی 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 نقض کنند یا او را ثبت نکنند.

لذا از آنجا که 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 حفظ دسترس‌پذیری انتخابات لازم است.

۸. سامانه 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 استفاده از این روش انتخاباتی را به شدت افزایش خواهد داد.

۹. بتوان نتایج انتخابات را در بازه‌های زمانی معین دید. هر سامانه‌ی انتخاباتی که نتایج را به صورت 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 مفروضات مسئله

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 که نشانگر هویت کاربر در سامانه 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 تا رای‌دهندگان تنها کلید خصوصی خود را در آن وارد کنند. 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.

هر حوزه یک جفت کلید عمومی و خصوصی دارد که برای امضا کردن بلوک‌های زنجیره‌ی قالبی استفاده می‌شود، همه‌ی حوزه‌ها و ناظر انتخابات قبل از رای‌گیری از طریق یک کانال امن کلیدهای عمومی خود را به اشتراک می‌گذارند در نتیجه هر حوزه و ناظر انتخابات کلید عمومی تمامی حوزه‌ها را می‌شناسد.

۴.۴ پروتکل ثبت رای

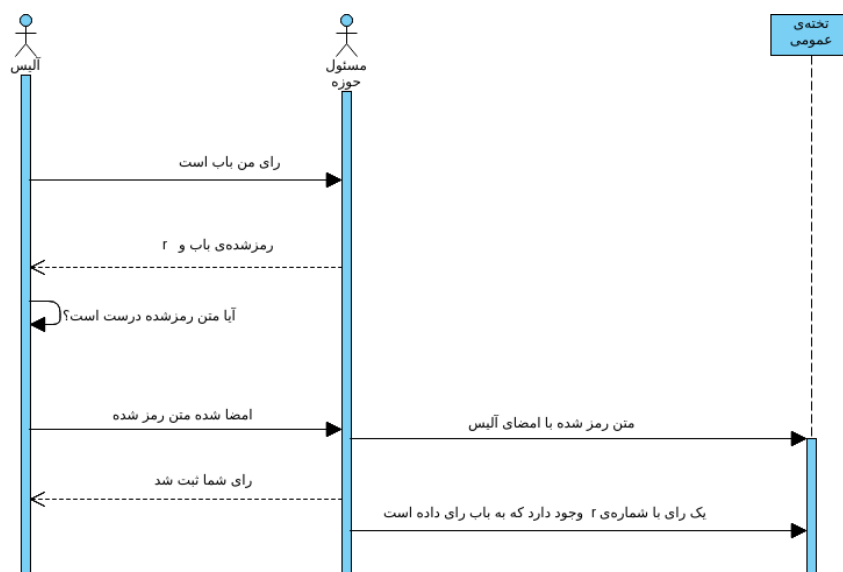
۱.۴.۴ مثال شهودی

برای به‌دست 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 سامانه‌ی توزیع‌شده و الکترونیک خود استفاده می‌کنیم. به طور کلی این روش مانند شکل ۲.۴ عمل می‌کند.

فرض می‌کنیم در یک رأی‌گیری به ازای هر رای‌دهنده یک کاغذ نام رای‌دهنده، یک برگه‌ی رای و 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 شماره‌ی تصادفی r و کاندیدای موردنظر آلیس، 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 مراجعه می‌کند و شاهی بر تخته ثبت می‌کند که ثابت می‌کند او کلید



شکل ۲.۴: شمای شهودی

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. از آن جایی که شاهد ارائه شده یک شاهد بی‌دانش خواهد بود هیچ راهی برای فهمیدن این موضع که شاهد برای رای آلیس ساخته شده وجود ندارد. حتی خود آلیس چون عدد r را به صورت رمز شده دریافت کرده است، نمی‌تواند شاهد مربوط به خود را پیدا کند. پس می‌دانیم که حریم خصوصی آلیس حفظ شده است. 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.

چون پلیس یا نظران انتخابات امنیت فیزیکی رای‌دهنده در محل رای‌گیری را تضمین می‌کنند، 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.

تنها مسئله‌ای که به ظاهر حل نشده، این است که آلیس چون یک عبارت رمز شده دریافت کرده نمی‌تواند از درست شمردن رای خود مطمئن شود، برای حل این مسئله از امضای کورکورانه استفاده کرده‌ایم. این روش به آلیس اجازه می‌دهد که بدون فهمیدن r مطمئن شود که داخل متن رمز شده باب نوشته شده است. در انتهای این فرایند تعداد رای موجود در صندوق باب، تعداد رای‌های او خواهد بود.

لازم به ذکر است که در پیاده‌سازی واقعی تخته را با یک زنجیره‌ی قالبی مدل می‌کنیم و مسئول حوزه برنامه‌ی در حال اجرا در حوزه خواهد بود. همچنین صندوق و برگه‌های رای نیز به طور شفاف به عنوان حساب‌هایی در زنجیره‌ی قالبی محسوب می‌شوند.

۲.۴.۴ فرایند رای‌گیری از نگاه کاربر

یکی از مهم‌ترین جنبه‌های طراحی یک سامانه‌ی رای‌گیری تأثیر 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.

در بعضی روش‌های رای‌گیری مانند Follow my vote کاربر رای‌دهنده به دسترسی اینترنت نیاز دارد و یا در بعضی روش‌های روش و تبوک کاربر باید محل رای‌دادن خود را پیش از انتخابات تعیین کند. این تغییرات در انتخابات‌هایی با مقیاس بزرگ قابل قبول نیستند. در روش ما کاربر جدا از مرحله‌ی شناسایی اولیه که می‌تواند یک بار به ازای چندین انتخابات انجام شود نیازمند تغییری در رفتار خود نیست. برای تشریح فرایند رای‌دادن کاربر، آن را به دو بخش قبل از رای‌گیری و در حوزه‌ی رای‌گیری تقسیم می‌کنیم.

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.

در حوزه‌ی رای‌گیری

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

۳.۴.۴ فرایند رای گیری از دید حوزه

در این بخش فرایند رای گیری را از نگاه حوزه بررسی می کنیم اما صرفاً منطق پروتکل را مورد بررسی قرار می دهیم و جزئیات زنجیره ی قالبی و عملیات توزیع شده نمی پردازیم.

برای ثبت رای یک نفر در ابتدا آن فرد با کارت شناسایی احراز هویت شده و از طریق ارتباط با ناظر انتخابات درستی کلید عمومی آن فرد بررسی می شود. در مرحله ی بعدی با ارائه ی کلید خصوصی کاربر یک تراکنش ثبت با نتیجه ی مورد نظر ایجاد می کند و تراکنش ثبت توسط دستگاه هوشمند کاربر کوکورا نه امضا می شود. در این مرحله تراکنش شمارش نیز ایجاد شده و با تاخیر زمانی در زنجیره ی قالبی ذخیره می شود.

تراکنش ها

در این بخش تراکنش های ثبت و شمارش را تعریف می کنیم.

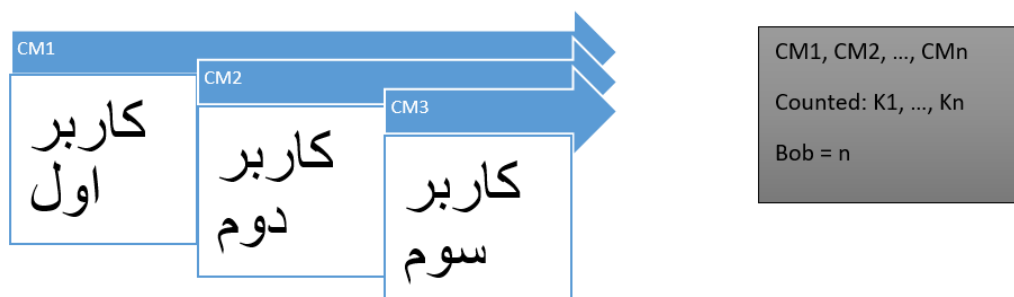
در تراکنش ثبت یک رای از یک کلید عمومی به دسته ی رای های منتظر شمارش منتقل می شود. هر تراکنش ثبت شامل یک رای و یک رشته ^۱ رمز شده است که حاوی یک عدد تصادفی s و حساب مقصد d بوده و با کلید تصادفی k رمز شده است. این عبارت رمز شده را CM می نامیم. سپس CM (نه خود s) در زنجیره ی قالبی به همراه رای ثبت می شود.

$$CM = enc_k(r, d) \quad (۱.۴)$$

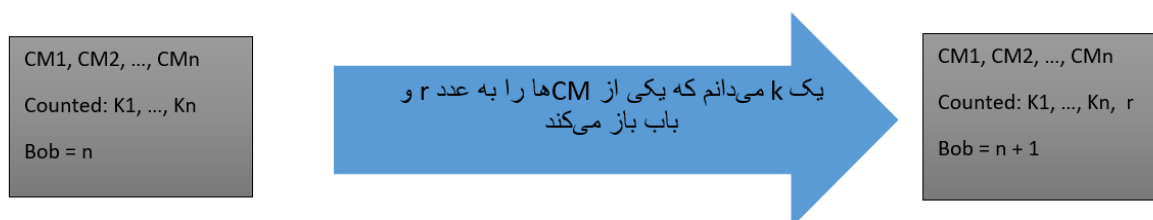
مدل دیگر تراکنش ممکن تراکنش شمارش است که در آن شاهی برای شمارش رای ارائه می شود. برای این تراکنش رای دهنده اثبات بی دانشی برای دو موضوع ارائه می کند: یک C می شناسد به طوری که $C \in$ C_1, C_2, \dots, C_n و یک رشته ای r می داند که C را به s و d باز می کند. در نتیجه ی این اثبات یکی از رای های ثبت شده به d منتقل می شود.

برای تحلیل این امنیت این روش یک بلوک را تصور می کنیم که دارای n تراکنش ثبت و به همین تعداد تراکنش شمارش است و می خواهیم از درستی شمارش آگاه شویم. هر تراکنش شمارش یک شاهد بی دانش ثبت کرده

^۱ string



شکل ۳.۴: تراکنش ثبت



شکل ۴.۴: تراکنش شمارش

است که نشان می‌دهد در آن بلوک یک C_i وجود دارد که شماره‌ی آن r_i است. با توجه به این که هر کسی می‌تواند شاهدها را بررسی کند می‌دانیم که هر شاهد ثبت شده درست است. چون رای‌ها در تراکنش ثبت رمز شده ثبت می‌شوند راهی برای یافتن رای‌دهنده‌ی هر شاهد نداریم و با توجه به تکراری نبودن r ها می‌دانیم که هیچ رای دوبار شمرده نشده است.

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.

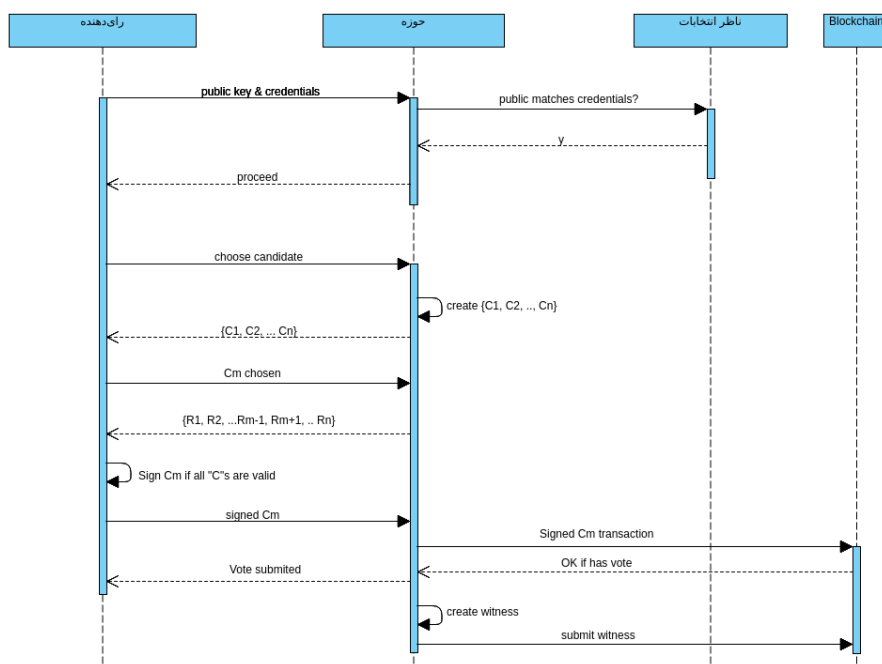
۳. حوزه کلید مربوط به تمامی CM های دیگر را به کاربر ارائه می کند.

۴. کاربر همه ی CM ها را باز می کند و چک می کند که در همه ی آن ها 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 می شود. سپس کاربر CM_c را با کلید خصوصی خود امضا می کند و به حوزه می دهد. در نتیجه ی این کار کاربر راهی برای فهمیدن عدد تصادفی در CM_c ، که آن را s می نامیم، ندارد.

۵. حوزه CM_c را به همراه رای موجود در حساب کاربر به عنوان یک تراکنش ثبت در زنجیره ی قالبی ذخیره می کند. در صورتی که رای کاربر قبلاً ثبت شده باشد در این مرحله خطا رخ می دهد و رای ثبت نمی شود.

۶. حوزه یک شاهد برای شمارش رای کاربر می سازد و هر دوی این تراکنش ها در بلوک بعدی زنجیره ی قالبی ذخیره می شوند.

شکل ۵.۴ این توالی فرایند را نشان می دهد.



شکل ۵.۴: فرایند ثبت رای در حوزه

ناشناسی رای گیری

یکی از اهداف اصلی طراحی این پرتوکل حفظ حریم شخصی کاربر، حتی در شرایطی که تمامی اطلاعات او لو رفته باشد، بوده است. این مسئله معادل این است که باب که در رای گیری شرکت کرده بخواهد اثبات کند به یک کاندیدای خاص، T ، رای داده است. اطلاعاتی که باب برای این کار دارد کلید خصوصی خود و تمامی اطلاعات موجود روی زنجیره‌ی قالبی است.

باب برای این کار دو روش دارد، یا باید بتواند اثبات کند که در تراکنش ثبت اون T ثبت شده است و یا به روشی تراکنش شمارش مربوط به رای خود را پیدا کند. ابتدا روش اول را بررسی می‌کنیم. پیدا کردن تراکنش ثبت مربوط به باب کار ساده‌ایست چرا که با کلید خصوصی او امضا شده. اما از با توجه به این که این تراکنش را کورکورانه امضا کرده کلید مربوط را ندارد. بهترین شانس باب حمله‌ی با دانستن متن^۱ است چرا که می‌داند در متن باید عبارت T نوشته شده باشد ولی با توجه کوتاه بودن عبارت رمز شده پیدا کردن کلید این روش نیز ممکن نیست. روش دوم پیدا کردن تراکنش شمارش مربوط به رای باب است که برای این کار شماره سریال مربوط به تراکنش ثبت را نیاز دارد و این شماره سریال تنها در تراکنش ثبت به صورت رمز شده ذخیره شده است پس این روش نیز نیازمند حل روش اول است و قابل اجرا نیست.

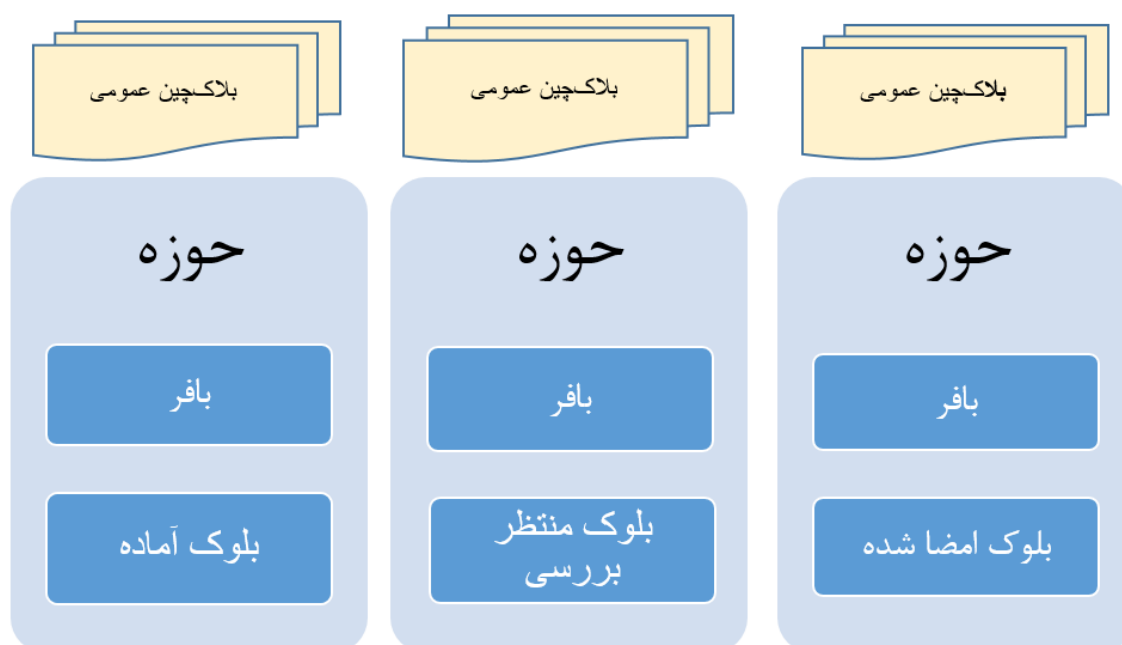
۵.۴ فرایندهای توزیع شده

در بخش‌های قبل یک پروتکل ثبت رای ارائه کردیم و در این بخش قصد داریم پروتکل ارائه شده را به صورت توزیع شده در تعدادی حوزه، بدون ایجاد خطری در ثبت رای اجرا کنیم. در ادامه شمای کلی سامانه و روش اضافه کردن بلوک به زنجیره‌ی قالبی را ارائه می‌کنیم و در نهایت به نحوه‌ی استفاده از اثبات‌های بی‌دانش در یک محیط توزیع شده می‌پردازیم.

^۱ Known-plaintext attack

۱.۵.۴ شمای کلی

به طور کلی سامانه 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 ۶.۴ شمای کلی درشت‌دانه‌ی سامانه 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 کاندیدا است.



شکل ۶.۴: شمای منطقی سامانه

۲.۵.۴ اضافه شدن بلوک

می‌دانیم که در هر بلوک ثبت‌شده در زنجیره‌ی قالبی تعدادی از دو مدل تراکنش‌های ثبت و شمارش داریم، همچنین هشت بلوک قبلی را نیز برای اطمینان از تغییر نکردن بلوک‌های قبلی نگاه می‌داریم. 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.

برای توافق نیز از روش PBFT استفاده می‌کنیم. این روش به ما اجازه می‌دهد که با در دسترس بودن بیش از یک سوم حوزه‌ها انتخابات را به درستی اجرا کنیم و خطری گم شدن بلوک (و در نتیجه گم شدن رای) نداشته باشیم. با استفاده از این روش در هر زمان یک حوزه‌ی رهبر داریم که می‌تواند بلوک جدید به زنجیره‌ی قالبی اضافه کند، هر حوزه‌ای که قصد اضافه کردن بلوک جدید داشته باشد، آن را برای حوزه‌ی رهبر می‌فرستد و رهبر برای بقیه‌ی حوزه‌ها ارسال می‌کند تا بررسی و امضا شود.

رهبر در طول زمان تغییر می‌کند و این مسئولیت بین حوزه‌ها می‌چرخد اما با توجه به این که در هر زمان دقیقاً یک رهبر وجود دارد هیچ زمانی دو بلوک تایید شده، توسط حوزه‌ها تایید نمی‌شوند و ممکن نیست در زنجیره‌ی قالبی آن‌ها شاخه‌ای ایجاد شود. برای تضمین کردن این موضوع که حتی در صورت پیش آمدن قطعی در شبکه‌ی بین حوزه‌ها، دو رهبر همزمان تایید نمی‌شوند، هر حوزه‌ای که ارتباطش با نیمی از حوزه‌های دیگر قطع شود دیگر بلوکی برای تایید ارسال نمی‌کند و رهبر نیز نمی‌شود. این موضوع به این معنی است که ممکن است در بعضی بازه‌های زمانی، یک حوزه‌ی خاص نتواند بلوک خود را ثبت کند و باید رای‌ها را در بافر خود تا زمانی که ارتباط او با حوزه‌های دیگر متصل شود، نگهداری 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. لازم به ذکر است که در این تحقیق هدف ارائه‌ی یک پروتکل رای‌گیری امن است و در این روش به سرعت اجرا در یک محصول کامل نمی‌پردازیم. برای مثال برای بهینه‌سازی حجم شاهد‌های بی‌دانش در محیط واقعی باید از تجمیع‌گرهای یک طرفه^۱ که اولین بار در سال ۱۹۹۳ [۴۲] ارائه شدند و یا روش‌های مشابه استفاده کرد. این روش‌ها در پروتکل‌های مشابه مانند زی‌کش در مقیاس بزرگ استفاده شده‌اند و می‌دانیم که مسئله‌ی سرعت و مقیاس‌پذیری چالشی بزرگی در استفاده از این محصول نخواهد بود.

۱.۵ پیاده‌سازی

در پیاده‌سازی این کار نیازمند ابزاری برای ایجاد یک زنجیره‌ی قالبی خصوصی با روش توافق PBFT هستیم. برای این کار از hyperledger fabric^۲ 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^۳ به سادگی تعدادی نود با یک بلاک‌چین خصوصی ارائه می‌کند. همچنین به کمک نوشتن قراردادهای هوشمند بر روی این بستر حوزه‌های مورد نیاز را ایجاد کردیم.

مسئله‌ی بعدی روش ایجاد اثبات‌های بی‌دانش است. برای ایجاد تراکنش‌های شمارش نیاز به اثبات‌های بی‌دانش داریم. برای این ساخت اثبات‌های بی‌دانش از کتابخانه‌ی libsnark^۴ 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.

همانطور که قبلاً اشاره کردیم برای استفاده از روش ZK-SNARK برای ایجاد شاهد‌های بی‌دانش احتیاج

^۱ One-way accumulator

^۲ <https://www.hyperledger.org/projects/fabric>

^۳ Docker

^۴ <https://github.com/scipr-lab/libsnark>

به توافق روی نقاط اولیه‌ای روی یک elliptic curve داریم. رد کتابخانه‌ی libsnark برای انجام این کار از روش ارائه شده در تحقیق [۳۵] استفاده شده است. برای این کار حوزه‌ها در یک زنجیره چیده می‌شوند و هر کدام قسمتی از محاسبات لازم برای ایجاد نقطه‌های اولیه را انجام می‌دهند، به صورتی که حتی با حذف یکی از آن‌ها نیز محاسبات ناتمام بماند. سپس با یک حالت خاص از اثبات‌های بی‌دانش انجام محاسبات را به یکدیگر اثبات می‌کنند. با این روش برای این که بتوان به نقاط اولیه برای ایجاد شاهدهای تقلبی دسترسی داشت، باید نتیجه‌ی محاسبات تمامی حوزه‌ها را داشته باشیم؛ به عبارت دیگر برای ایجاد شاهدهای تقلبی، تمامی حوزه‌ها باید در فاز آماده‌سازی تبانی کرده و اطلاعات خصوصی خود را به اشتراک بگذارند

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

۲.۵ معیارهای رای‌گیری مناسب

هر روش رای‌گیری خوب باید بتواند شروط رای‌گیری ایده‌آل را ارضا کند. شروط ارائه شده نیازمندی‌های اصلی یک رای‌گیری هستند و در صورت ارضا نشدن آن‌ها روش رای‌گیری قابل استفاده در کاربردهای مهم و بزرگ نیست.

در رای‌گیری‌های مهم، برنده شدن در انتخابات می‌تواند سود بسیار زیادی برای یک کاندیدا داشته باشد، به همین دلیل همواره انگیزه برای هزینه کردن برای تخلف در انتخابات وجود دارد و برای اطمینان از یک انتخابات

امن باید تا جای ممکن نیازی به اعتماد به هیچ شخصی نباشد و هر گونه تخلف قابل ردیابی باشد. فاکتور مهم بعدی هزینه‌ی برگزاری انتخابات است. یک روش انتخابات که امنیت را به خوبی تامین کند ولی هزینه‌ی گزافی برای رای‌دهنده یا مجری انتخابات داشته باشد، در عمل استفاده نخواهد شد بنابراین یکی از مهم‌ترین معیارهای ارزیابی روش رای‌گیری، هزینه‌ی آن است.

مسئله‌ی دیگری که در هر سامانه‌ی توزیع‌شده‌ای نیازمند بررسی دقیق است، نحوه‌ی نگهداری داده‌هاست. در سامانه‌های توزیع شده به دلیل مشکلات ذاتی شبکه از قبیل گم شدن پیام و یا تاخیر رسیدن پیام‌ها، همواره احتمال ایجاد ناهمخوانی بین داده‌های قسمت‌های مختلف شبکه وجود دارد. به همین دلیل در بخش پایانی این فصل به بررسی روش توافق استفاده شده در این روش و تاثیر آن در همخوان نگه‌داشتن اطلاعات حوزه‌ها می‌پردازیم.

به دلیل اهمیت بالای نیازمندی‌های رای‌گیری ایده‌آل در ابتدا بررسی می‌کنیم که روش پیشنهادی این تحقیق چگونه هر کدام از نیازمندی‌ها را برطرف می‌کند. در ادامه در مقایسه با تحقیقات دیگری که توانسته‌اند این شروط را ارضا کنند نحوه‌ی اطمینان شمارش درست، خطر از بین رفتن ناشناسی رای‌ها، هزینه‌ی برگزاری، هزینه‌ی تغییر برای کاربر و در نهایت توانایی پیدا کردن خطاهای حوزه‌ها را بررسی می‌کنیم.

۳.۵ نزدیکی به رای‌گیری ایده‌آل

در این بخش نیازمندی‌های رای‌گیری ایده‌آل را دوره می‌کنیم و می‌بینیم که روش ارائه شده چگونه هر کدام از نیازمندی‌ها را رفع می‌کند.

- می‌دانیم که هر شخصی حداکثر یک رای می‌تواند بدهد چون که در حساب کلید عمومی آن فرد دقیقاً یک رای در ابتدای رای‌گیری وجود دارد. از طرفی می‌دانیم که سامانه 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 کلید خصوصی 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 کسی مجبور به رای دادن به شخص خاصی نمی‌شود چرا که راهی برای چک کردن رای فرد بعد از فرایند رای‌گیری وجود ندارد، در نتیجه به دلیل امن بودن حوزه‌ی رای‌گیری، رای‌دهنده همواره می‌تواند به کاندیدای دلخواه خود رای دهد ولی این عمل را انکار کند.
- در انتهای انتخابات می‌توانیم به سادگی با بررسی تعداد تراکنش‌های ثبت و شمارش از درستی شمارش آرا اطمینان حاصل کنیم. هر شخصی نیز با بررسی این که عمل ثبتی برای او در زنجیره‌ی قالبی وجود دارد می‌تواند از شماره 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.

۴.۵ 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.

۱.۴.۵ روش‌های رای‌گیری دیگر

برای مقایسه سامانه‌های رای‌گیری زیر را بررسی می‌کنیم:

• **رای گیری سنتی:** این روش به عنوان خط مبنای تحقیق بررسی می شود، روش های رای گیری الکترونیکی ساخته شده تاکنون همواره با وجود کاهش هزینه ها برای شمارش رای ها، در زمینه های امنیت و حریم خصوصی خطرهایی ایجاد کرده اند به همین دلیل همچنان در کاربردهایی ممکن است که رای گیری سنتی بهتر از روش های دیگر عمل کند و روش های جدید رای گیری باید با این روش مقایسه شوند. نحوه ی برگزاری انتخابات در این روش در بخش ۲.۱ توصیف شده است.

• **رای گیری الکترونیک بدون زنجیره ی قالبی:** در این روش، رای گیری الکترونیک متمرکز را بررسی می کنیم، چرا که سامانه های رای گیری توزیع شده ی بدون زنجیره ی قالبی به به کاربرد عمومی نرسیدند. در این سامانه ها اطلاعات رای دهندگان و نتیجه ی رای آن ها به دلیل نیاز به روش ردگیری به طور کامل ثبت می شود اما در فرایند ثبت رای تفاوت چندانی با سامانه های سنتی ندارند.

• **وت بوک** این روش را به عنوان مصداقی از سامانه های رای گیری با زنجیره ی قالبی خصوصی بررسی می کنیم. در این روش از یک زنجیره ی قالبی که می توان در حالت خصوصی یا عمومی از استفاده کرد برای ثبت آرا استفاده می شود.

موارد حذف شده از مقایسه

روش معروف Vote Watcher نیز فعالیت های بسیاری در این زمینه داشته اما به دلیل عمومی نبودن اطلاعات پیاده سازی این سامانه، از مقایسه ی آن خودداری می کنیم.

همچنین از آن جایی که روش های رای گیری به کمک یک زنجیره ی قالبی عمومی و یا روش های توزیع شده بدون زنجیره ی قالبی به دلیل مشکلات مقیاس پذیری توانایی استفاده شدن در انتخابات های بزرگ (بیش از چند هزار نفر) را ندارند از بررسی این نوع سامانه ها صرف نظر می کنیم.

همچنین روش مورد استفاده در Follow my Vote از لحاظ روش پیاده سازی شباهت زیادی به وت بوک دارد ولی به جای حوزه ی رای گیری از یک برنامه در رایانه ی شخصی یا تلفن هوشمند استفاده می کند. این تصمیم باعث سادگی فرایند رای گیری برای بعضی از رای دهندگان می شود اما دو مشکل بزرگ ایجاد می کند که باعث شده از مقایسه ی آن خودداری کنیم. اولین مشکل کاهش دسترسی پذیری این روش 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 رای دادن به کاندیدای خاصی نشده است.

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

در روش وب‌توک و روش 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.

۳.۴.۵ 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 وت‌بوک 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.

۴.۴.۵ 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 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 وب‌بک 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. بنابراین به روال رای‌گیری کاربر در روش سنتی، یک مرحله‌ی آماده‌سازی اضافه می‌کند که باید در مدت زمان کوتاهی قبل از انتخابات انجام شود، چرا که رای‌گیری نیاز دارد تمامی رای‌دهندگان حوزه‌ی خود را مشخص کرده باشند.

- در سامانه ما نیز کاربر باید قبل از رای‌گیری یک کلید عمومی ثبت کند که برای فرایند رای‌گیری استفاده می‌شود. همچنین کاربر برای اطمینان از درست شمردن رای خود باید از یک دستگاه هوشمند برای عمل امضای کورکورانه استفاده کند. بنابراین نیاز به یک دستگاه هوشمند نیز به هزینه‌های رای‌دهنده اضافه می‌شود.^۱

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 سامانه‌های کامپیوتری حاضر در حوزه هزینه‌ای به مجری تحمیل نمی‌شود، اما دستگاه‌های الکترونیکی نیازمند بررسی و ارتقا در طول زمان هستند. در وب‌بک علاوه بر سامانه‌های موجود در حوزه‌ها، یک سامانه 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 و این مسئله هزینه‌ی نگهداری در طول زمان این روش را افزایش می‌دهد.

^۱ لازم به ذکر است که کاربر می‌تواند از دستگاه‌های درون حوزه استفاده کند ولی با این کار باید اعتماد کند که حوزه رای او را به درستی ثبت کرده است چرا که راهی برای اثبات درستی برنامه‌ی موجود در حوزه وجود ندارد. یعنی می‌توان هزینه‌ی کاربر را در فرایند رای‌گیری کمتر کرد ولی این عمل باعث می‌شود که یک حوزه‌ی خطاکار بتواند رای کاربر را از طریق حمله‌ی phishing تغییر دهد.

در روش پیشنهادی ما نیز علاوه بر سامانه‌ی موجود در حوزه، در هر انتخابات مجری انتخابات باید توانایی عوض کردن یا ثبت کلید عمومی جدید را به رای‌دهندگان بدهد که خود این مسئله هزینه‌ی نگهداری به مجری اضافه می‌کند.

۵.۴.۵ 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 خطا کار 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 مناسبی 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 روش‌های 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 روش وت‌بوک 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 خراب کار می‌تواند انجام دهد این است که رای کاربر را به عنوان رای ممتنع ثبت کند. در فرایند رای‌گیری با وت‌بوک 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

ممنوع هیچ وقت به صورت عمومی منتشر نمی شوند اما با توجه به این که این اطلاعات در اختیار ناظر انتخابات خواهد بود حمله ی بزرگ به این روش به سادگی قابل تشخیص خواهد بود.

در روش رای گیری ما نیز کاربر از درستی شمارش رای ثبت شده ی خود در فرایند امضای کورکورانه آگاه می شود همچنین بعد از فرایند رای گیری نیز می تواند با بررسی زنجیره ی قالبی از ثبت رای خود (ولی نه نتیجه ی آن) مطمئن شود. از آن جایی که تمامی رای ها نیازمند امضای دیجیتال رای دهندگان هستند راهی برای ایجاد رای های دروغین توسط یک حوزه نیز وجود ندارد. از طرفی ناظر انتخابات می تواند با بررسی تساوی تعداد تراکنش ها ثبت و شمارش ثبت شده در زنجیره ی 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 نتیجه ی رای او نخواهد بود.

جدول ۲.۵: مقایسه ی روش های رای گیری

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

۵.۵ احتمال ناهمخوانی در زنجیره‌ی قالبی

در زنجیره‌ی قالبی‌های عمومی معمولاً یک مسئله در توافق حالت‌هایست 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 ارزش‌های دیجیتالی طولانی‌ترین زنجیره‌ی قالبی از نظر تعداد بلوک‌ها همواره به عنوان نسخه‌ی درست شناخته می‌شود اما در یک سامانه رای‌گیری این کار باعث کم شدن رای می‌شود و این خطر قابل قبولی نیست.

قضیه‌ی CAP

برای تحلیل روش توافق استفاده شده در این تحقیق از قضیه‌ی CAP استفاده می‌کنیم. این قضیه‌ی معروف [۴۳] اثبات می‌کند که در یک دیتابیس توزیع شده - 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 ثبات شبکه حساب کنیم سامانه‌ی ما در حالت CP عمل می‌کند. به عبارت دیگر توانایی همخوانی برای از دست ندادن رای و تحمل تقسیم‌شدن برای عدم ثبات شبکه را نیاز داریم. معمولاً در سامانه‌های مبتنی بر زنجیره‌ی قالبی از روش‌های که تضمین می‌کنند که همه‌ی نودها در نهایت به همخوانی می‌رسند^۴. اما در یک سامانه که برای رای‌گیری استفاده می‌شود این مسئله می‌تواند خطر گم شدن تعدادی از آرا ایجاد کند و این خطر معقولی برای یک روش رای‌گیری الکترونیک نیست.

در زنجیره‌ی قالبی‌های عمومی معمولاً از روش‌های اثبات کار و اثبات سهم استفاده می‌شود که دسترس‌پذیری و تحمل قسمت‌شدن را به خوبی ارائه می‌کنند اما ممکن است شاخه‌های^۵ 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 آنجایی که این کار در سامانه‌ی ما باعث از

¹ Consistency

² Availability

³ Partition tolerance

⁴ Eventual consistency

⁵ fork

بین رفتن رای می‌شود باید در روش دیگری استفاده کنیم.

روش دیگری که برای مقایسه بررسی می‌کنیم Aura [۴۴] است. از آن جایی که این روش از ساعت unix استفاده می‌کند ممکن است در اثر ناهمگامی ساعت‌های حوزه‌ها در یک زمان دو رهبر بوجود بیاید که هر کدام تعدادی بلوک اضافه می‌کنند. این مسئله باعث دو شاخه شدن زنجیره‌ی قالبی می‌شود و این روش توافق راه‌حلی برای حل این موضوع ارائه نمی‌کند. در کاربردی مانند رای‌گیری که ثبت درست تمامی رای‌ها یک نیازمندی اساسی است، این روش توافقی مناسبی نخواهد بود.

مورد مقایسه‌ی بعدی Clique [۴۵] است. این روش به برای حل مشکلات Aura به جای استفاده از ساعت برای تغییر رهبر، از تعداد بلوک ثبت شده استفاده می‌کند. این تصمیم مسئله‌ی بوجود آمدن دو رهبر در یک زمان را حل می‌کند. اما برای کارایی و سرعت بالاتر در این روش علاوه بر رهبر حوزه‌های دیگر نیز می‌تواند بلوک جدید ارائه کنند و در صورتی که رهبر از بخشی از شبکه قطع شده باشد، این بلوک‌های جدید می‌توانند باعث ایجاد شاخه در زنجیره‌ی قالبی شوند. در این روش نسخه‌ی مورد تایید بیشترین حوزه به عنوان نسخه‌ی درست زنجیره در نظر گرفته می‌شود و شاخه‌ی دیگر حذف می‌شود که این رفتار نیز برای استفاده در یک سیستم انتخاباتی مناسب نیست.

روش انتخابی ما در این تحقیق PBFT^۱، هزینه‌ی محاسباتی بسیار کمتری از روش‌های مبتنی بر اثبات کار دارد و از نظر مقیاس پذیری [۴۶] نیز بسیار بهتر عمل می‌کند.

می‌دانیم در این روش حداکثر تعداد تعداد حوزه‌ای که باید خطا کار باشند تا بلوک اشتباهی در زنجیره‌ی قالبی ثبت شود برای $3f + 1$ حوزه f حوزه است. این تعداد حوزه‌ی خراب کار می‌تواند 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 همچنین شرایطی چون نمی‌توان از تعداد رای‌دهندگان 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 خطا کار باشند هیچ زمانی دو نسخه‌ی مستقل از زنجیره‌ی قالبی توسط حوزه‌ها تایید نمی‌شود. به عبارت دیگر این روش به طور کامل هم‌خوانی

^۱ Practical Byzantine fault tolerance

جدول ۳.۵: 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

و توانایی قسمت شدن را دارد.

لازم به ذکر است که در این حالت سامانه 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 اما این مسئله به سادگی با یک بافر به اندازه‌ی کافی بزرگ حل می‌شود و مانع عملکرد درست حوزه‌ی انتخاباتی نمی‌شود.

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 الکترونیک 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 الکترونیک 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/03_SmartContracts/03-01_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.Hjalmtýsson, "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] M.Castro and B.Liskov, "Practical byzantine fault tolerance," *OSDI*, pp.173-186, 1999.
- [33] S. Z.Galil and M.Yung, "Symmetric public-key encryption," *Conference on the Theory and Application of Cryptographic Techniques. Springer*, 1985.
- [34] 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.
- [35] 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.
- [36] 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.
- [37] 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.
- [38] N. Saberhagen, "Cryptonote v 2.0," <https://cryptonote.org/whitepaper.pdf>, 2013.
- [39] B.Goodell1 and S.Noether2, "Thring signatures and their applications to spender-ambiguous digital currencies," *Monero Research Lab*, 2018.
- [40] 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.
- [41] 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.

- [42] J. Benaloh and M. de Mare, "One-way accumulators : a decentralized alternative to digital signatures," *Advances in Cryptology—EUROCRYPT*, pp.274-285, 1993.
- [43] E. Brewer, "Cap twelve years later : How the "rules" have changed," *Computer*, vol.45, no.2, pp.23-29, 2012.
- [44] "Aura," <https://wiki.parity.io/Aura>.
- [45] "Clique," <https://github.com/ethereum/EIPs/issues/225>.
- [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, E-voting, Security



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