ارائه طرحی برای رای‌گیری الکترونیکی با استفاده از امضای کور و فناوری بلاک چین

الهه مهربان*[۱]، رضا ابراهیمی آتانی [۲]

۱- دکتری ریاضی محض، دانشکده ریاضی، دانشگاه گیلان ، گیلان، رشت

۲- دانشیار گروه مهندسی کامپیوتر، دانشگاه گیلان،گیلان، رشت

چکیده

امروز با توسعه خدمات دولت الکترونیکی بسیاری از خدمات عمومی از طریق دفاتر پیشخوان الکترونیکی شده اند. بر این اساس عامه جامعه بدون نیاز به حضور فیزیکی در ادارات و دفاتر می توانند با استفاده از خدمات احراز هویت برخط مجاز شماری شوند و سرویس های لازم را بصورت الکترونیکی دریافت نمایند. یکی از خدمات الکترونیکی مهم در جامعه رای گیری الکترونیکی است که بعلت محدودیت زمانی برای ارایه خدمات و همچنین حذف محدودیت های مکانی میتواند کمک شایانی به مشارکت حداکثر آحاد جامعه در تصمیم گیری های عمومی داشته باشد. اصولا طرح های رای گیری الکترونیکی با استفاده از الگوریتم‌های مختلف رمزنگاری عمل می‌کند و طراحی پروتکل های رای گیری یکی از پیچیده ترین سیستم ها رمزنگاری می باشد. علی‌رغم مزیت‌های زیاد رای گیری الکترونیکی به علت اینکه اختیار کامل در دست مدیر یا ادمین سامانه رای گیری است و مدیر ناصادق می تواند صحت رای گیری را دچار چالش نماید. برای حل این مشکل، از فناوری نوظهور بلاک چین استفاده می‌شود. بلاک چین قابلیت اطمینان و یکپارچگی داده‌ها را فراهم می‌آورد. در این مقاله، با استفاده از امضای کور جمعی کوانتومی و بلاک چین طرحی در رای گیری الکترونیکی پیشنهاد شده است که می‌تواند حریم خصوصی و سایر ویژگی های امنیتی رای گیری الکترونیکی را تضمین کند.

کلمات کلیدی: بلاک چین، امضای کور جمعی کوانتومی، رای گیری الکترونیکی.

۱. مقدمه

در سال‌های اخیر، با محبوبیت رایانه‌ها و تلفن‌های هوشمند رای گیری الکترونیکی موردتوجه بسیاری از کشورهای توسعه یافته قرارگرفته است. رای گیری سنتی (کاغذی) مشکلاتی مانند زمان‌بر بودن و پرهزینه بودن دارد. باوجود

* **Corresponding author**
Email: e.mehraban.math@gmail.com

مزیت‌های رای گیری الکترونیکی که محدودیت مکان حذف نموده و صرفه‌جویی زمانی خوبی ایجاد می نماید، ممکن است در یک سیستم الکترونیکی رای گیری مدیران ناصادق، مشکل جعل یا دست‌کاری داده‌ها بوجود بیاورند و صحت رای گیری زیر سوال برود. اگرچه پیشنهاد های زیادی برای حل این مشکل ارایه شده است [۱، ۳] اما استفاده از بلاکچین با توجه به ویژگی‌های ذاتی آن راه‌حل جایگزین مناسبی است. رای گیری الکترونیکی مبتنی بر بلاک چین ویژگی‌های چشم‌گیری برای غلبه بر مشکلات حریم خصوصی و صحت آرا موردتوجه بسیار قرارگرفته است. فناوری بلاکچین نخستین بار در سال ۲۰۰۸ ظهور کرد [۹، ۱۰] با افزودن یک امضای حلقه به سیستم رای گیری الکترونیکی بیت کوین، حریم خصوصی را اضافه کرد. در پژوهش [۶] رای گیری الکترونیکی با استفاده از قراردادهای هوشمند ارائه‌شده است. در [۴] با استفاده از دو بلاک چین طرحی پیشنهاد داده شده است که یکی برای ذخیره اطلاعات رای دهندگان (بلاک چین رای دهندگان) مشارکت می نماید و دیگری برای ذخیره جزئیات رأی (بلاک چین رای) می باشد. در ادامه، طرحی مبتنی بر امضای کور و قرارداد هوشمند در بلاک چین عمومی پیشنهاد داده خواهد شد که باعث حفظ حریم خصوصی رای دهنده گردیده و صداقت، واجد شرایط بودن، انصاف را نیز در رای گیری حفظ می‌کند.

۲. ویژگی‌های رای گیری الکترونیکی

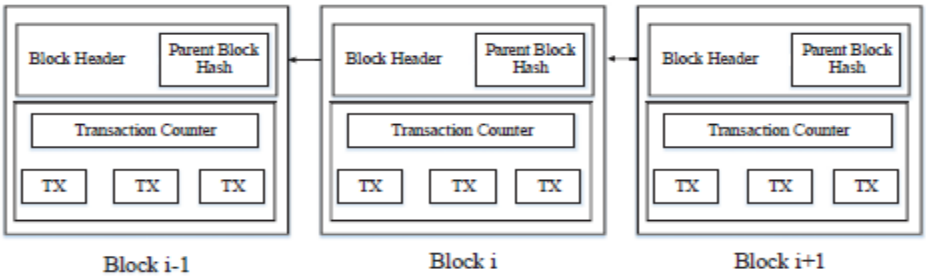
در این مقاله ویژگی‌های اصلی یک سامانه رای گیری الکترونیکی را با توجه به توصیه های طرح [5] در نظر گرفته‌شده است.

۱- کامل بودن: تمام اطلاعات جمع‌آوری‌شده در رأی باید به‌درستی مورداستفاده قرار گیرد.
۲- صداقت: رای نباید توسط رای دهندگان ناعادلانه قطع شود.
۳- حریم خصوصی: هیچ‌کس دیگر نباید بداند رای دهنده به چه چیزی رای داده است.
۴- غیرقابل استفاده بودن: رای دهندگان باید فقط یک‌بار بتوانند رای دهند.
۵- واجد شرایط بودن: رأی‌دهندگان تنها در صورتی می‌توانند رای بدهند که دارای قدرت رای دادن باشند.
۶- انصاف: مهم نیست که چه اتفاقی می‌افتد، شما نباید بر رأی خود تأثیر بگذارید.
۷- قابلیت اطمینان: هرکسی باید بتواند نتایج رأی گیری را تأیید کند.

رای گیری الکترونیکی باوجود مزیت‌هایی مانند محدودیت زمان، مکان و هزینه کمتر و شمارش سریع آرا دارد اکثر کشورها به دلیل عدم قابلیت اطمینان سیستم، مشکلات جعل و تعدیل داده‌ها حاضر به استفاده از آن نیستند. ازجمله راه‌حل‌هایی برای حفظ امنیت آن می‌توان به بلاک چین و امضای کور اشاره کرد.

۳. آشنایی با بلاک چین

درسال ۲۰۰۸[9]، با ظهور بیت کوین توسط ناکاموتو فناوری بلاک چین ظهور کرد. بلاک چین، یک زنجیر دارای مهر زمانی از تراکنش‌های تغییرناپذیر است که توسط دسته‌ای از گره‌ها با استفاده از الگوریتم ویژه‌ای، مدیریت می‌شود. این تراکنش تغییرناپذیر، در یک دفتر کل ذخیره می‌شوند که متعلق به هیچ موجودیت احدی نیست. بلاک چین از سه قسمت قالب (بلوک)، زنجیر و شبکه تشکیل‌شده است. شکل ۱ مثالی از دنباله بلوک‌ها در بلاک چین است.



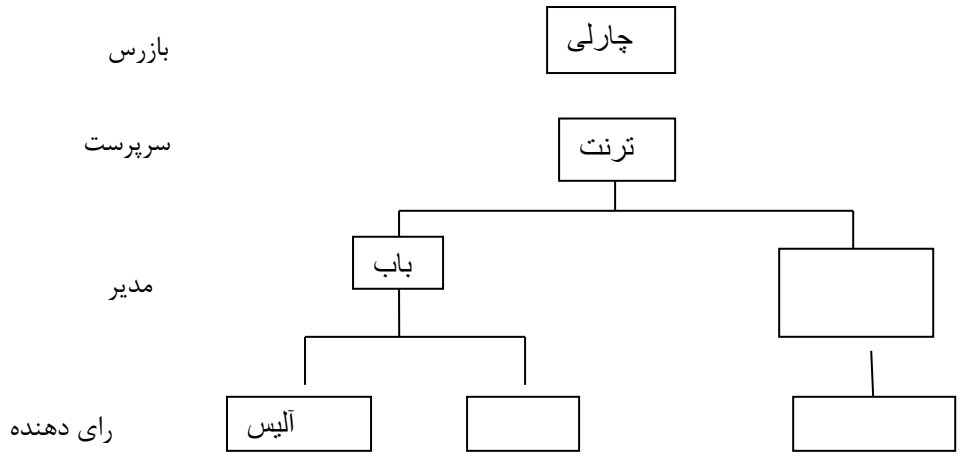
شکل ۱: مثالی از بلاک چین که از دنباله‌ای از بلوک‌ها که تشکیل‌شده است.

از مزایای امنیتی آن می‌توان به حفظ حریم خصوصی، گمنامی بازیابی خرابی‌ها، جلوگیری از دست‌کاری داده‌ها، ایجاد اعتماد در شبکه نام برد. انواع شبکه‌های بلاک چین شامل شبکه عمومی، خصوصی و شبکه مجاز است. بلاک چین دارای ویژگی غیرمتمرکز بودن است و بدون نیاز به شخص ثالث، نقش‌ها را با استفاده از الگوریتم اجماع (توافق) تائید می‌کند. از مهم‌ترین این‌ها می‌توان الگوریتم رقابتی شامل کار (PoW) و اثبات سهام (POS) نام برد.
در ادامه و در جدول ۱ پارامترهایی که در این مقاله برای طراحی پروتکل رای گیری مورداستفاده قرار می‌گیرد تشریح خواهد شد.

در مقاله [11]، با استفاده از امضای کور جمعی گروه کوانتومی ، طرحی برای رای گیری الکترونیکی ارائه داده‌شده است. در اینجا خلاصه‌ای از آن را بیان می‌کنیم. این طرح از چهار بخش رأی دهنده، مدیر، سرپرست و بازرس تشکیل‌شده است. شکل ۲ ساختار این رأی گیری نشان می‌دهد.

جدول ۱. پارامترهای رای گیری طرح پیشنهادی

پارامترهای سیستم	تعریف پارامتر
i-- امین رای دهنده	V_i
i- امین بلوک متصل به بلاک چین	$Block_i$
i- امین کاندیدا	M_i
کلید جلسه i-- امین رای دهنده	K^i_m
شماره سریالi-- امین رای دهنده	SN^i
کلید اولیه مکان رای گیری به رای دهنده	K_{pv}
رمزگذاری K^i_m با K_{pv}	$E_{K_{pv}}\left(K^i_m\right)$
رمزگذاری SN^i با K_{pv}	$D\left(E_{K_{pv}}\left(SN^i\right)\right)$
رمزگشایی K^i_m با K_{pv}	$D\left(E_{K_{pv}}\left(K^i_m\right)\right)$
رمزگشایی SN^i با K_{pv}	$D\left(E_{K_{pv}}\left(SN^i\right)\right)$
شناسه رای i- امین رای دهنده	id^i



شکل ۲: ساختار رای گیری الکترونیکی امضای کور جمعی

ابتدا سرپرست کلید اولیه بازرس(K_{Tc}) و کلید اولیه مدیر (K_{TB})را به اشتراک می گذارد. و زمانی که رای دهنده(آلیس) درخواست پیام امضای رای به مدیر داد کلید (K_{AB})از طرف مدیر(باب) به او داده می‌شود. تمام این کلیدهای اولیه دنباله‌های بیتی به طول n است. بازرس کلید جلسه و شماره سریال آن را به‌صورت زوج $\left\{\left(K_{SV}{}^{1},SN^{1}\right),\cdots,\left(K_{SV}{}^{j},SN^{j}\right),\cdots\right\}$تولید می‌کند. چارلی با کلید K_{Tc}، K_{SV} و SNرا به‌صورت $E_{K_{Tc}}\left(K_{SV}\right)$ و $E_{K_{Tc}}\left(SN\right)$رمزگذاری می‌کند وبرای ترنت می‌فرستد. ترنت با رمزگشایی آن‌ها به K_{SV} و SN دست می‌یابد. و به‌طور تصادفی توزیع می‌کند. به‌عنوان‌مثال سرپرست (ترنت) $E_{K_{Tc}}\left(K_{SV}{}^{j}\right)$ و $E_{K_{Tc}}\left(SN^{j}\right)$را برای باب می‌فرستد. باب پس از رمزگشایی به $K_{SV}{}^{j}$ و شماره سریال SN^{j}برای تائید آن دستیابی پیدا می‌کند. ترنت شماره سریال SN^{j} را برای امضای باب یادداشت می‌کند. در مرحله آماده‌سازی پیام رای دهنده رای را به‌صورت دنباله $m^{j}=\left\{m^{j}(1),m^{j}(2),\cdots,m^{j}(i),\cdots\right\}$آماده کرده و با به‌کارگیری تابع هش $H(.):\{0,1\}\to\{0,1\}^{n}$، $M^{j}=H\left(m^{j}\right)$ آماده و به مدیر برای گرفتن امضا درخواست می‌دهد. مدیر پس از دریافت درخواست، تابع‌های رمزگذاری $E_{K_{AB}}\left(K_{SV}{}^{j}\right)$ و $E_{K_{AB}}\left(SN^{j}\right)$ را از کانال کوانتومی به رای دهنده می‌فرستد. رای دهنده پس از رمزگشایی $K_{SV}{}^{j}$ و SN^{j}را به دست می‌آورد و با رمزگذاری پیام M^{j} با استفاده از $K_{SV}{}^{j}$امضای $\left[S^{j}\right)=E_{K_{SV}{}^{j}}\left(M^{j}\right)$را به دست می‌آورد. همچنین برای m^{j}یک شناسه پیام به‌صورت id^{j}تولید می‌کند. مجموعه ۴-تایی $\left(id^{j},m^{j},S^{j},SN^{j}\right)$را به بازرس می‌فرستد. بازرس با استفاده از SN^{j}کلید $K_{SV}{}^{j}$را جستجو می‌کند. اگر موجود نباشد رد می‌کند. در غیر این صورت M^{j}را با رمزگشایی S^{j}به دست آورده و $M^{j}=H\left(m^{j}\right)$ را محاسبه می‌کند اگر $M^{j}==M^{j}$باشد امضا را قبول و در غیر این صورت رد می‌کند. در صورت قبول امضا m^{j}و id^{j}را در جدولی منتشر می‌کند و رای دهنده با مراجعه به جدول می‌تواند از صحت رای خود مطلع شود. بازرس $\left(S^{j},SN^{j}\right)$را به سرپرست می‌فرستد و در صورت تخلف می‌تواند موردبررسی قرار گیرد.

۴. طرح پیشنهادی

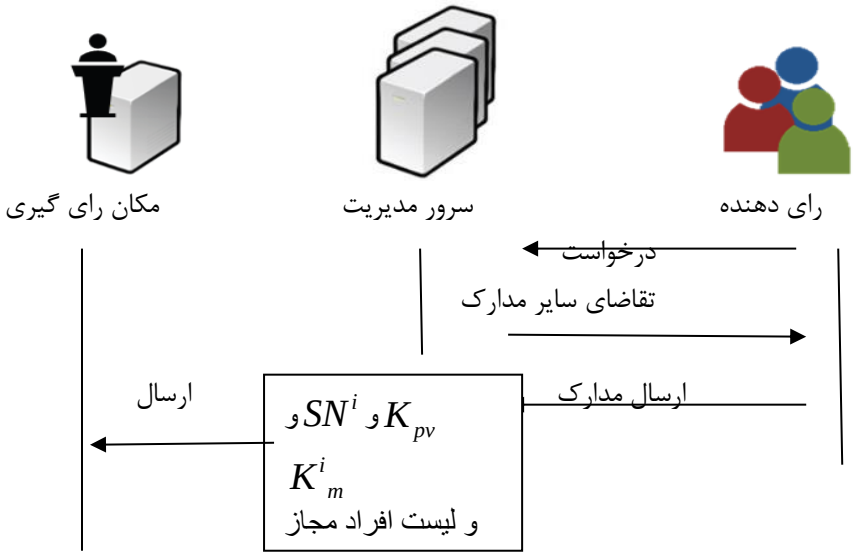
برای پیاده‌سازی این طرح پیشنهادی از طرح امضای کور جمعی گروه کوانتومی در [11] استفاده‌شده است. با تغییراتی سعی در بهبود امنیت رای ها و حفظ کامل حریم خصوصی داریم. در اینجا، برخلاف[11] بازرس و سرپرست مجزا نیستند. طرح پیشنهادی شامل چهار قسمت رای دهنده، سرور مدیریت، سرور مکان رای گیری، سرور شمارش آرا. در این طرح، می توان از بلاک چین عمومی مانند اتریم استفاده کرد که قرارداد هوشمند روی آن قرار دارد. اتریم یک پلتفرم محاسباتی غیرمتمرکز مبتنی بر به بلاک چین است که مکانیسم توافق روی آن (POW) است و برای ایجاد یک بلوک جدید و تائید تراکنش‌ها از آن استفاده می‌شود.

مراحل الگوریتم رای گیری شامل مراحل زیر است:

۱- **ثبت‌نام**: ثبت‌نام شامل رای دهنده‌ها و کاندیداهای انتخاباتی است که توسط سرور مدیریت انجام می‌شود.

ثبت‌نام رای دهندگان:

- رای دهنده درخواست خود را به سرور مدیریت می‌دهد.
- سرور مدیریت درخواست را بررسی می‌کند و در صورت پذیرفتن از وی تقاضای دادن سایر مشخصات می کند.
- رای دهنده مشخصات دیگر مانند آدرس مکان زندگی، محل کار، شماره همراه... را به سرور ارسال می‌کند.
- سرور مدیریت برای هر رای دهنده ثبت‌نام‌شده یک کلید جلسه K^i_m و یک شماره سریال آن SN^i تولید می‌کند.
- سرور مدیریت $\{(K^1_m, SN^1),(K^1_m, SN^1),\cdots,(K^i_m, SN^i),\cdots\}$ را به مکان رای گیری می فرستد.
- سرور مدیریت یک کلید اولیه برای محل رای گیری که به رای دهنده می‌فرستد K_{pv} تولید می‌کند.
- لیست افراد مجاز به مکان رای گیری می‌فرستد.



شکل۳:ثبت‌نام رای دهندگان

ثبت‌نام کاندیدا:

- کاندیدا درخواست خود را به سرور مدیریت می‌دهد.
- سرور مدیریت درخواست را بررسی می‌کند و در صورت پذیرفتن تقاضای دادن سایر مشخصات می‌کند.
- کاندیدا مشخصات دیگر مانند آدرس مکان زندگی، محل کار، شماره همراه... را به سرور ارسال می‌کند.
- سرور مدیریت لیست تمام افراد ثبت‌نام‌شده را به مکان رای گیری می‌فرستد.

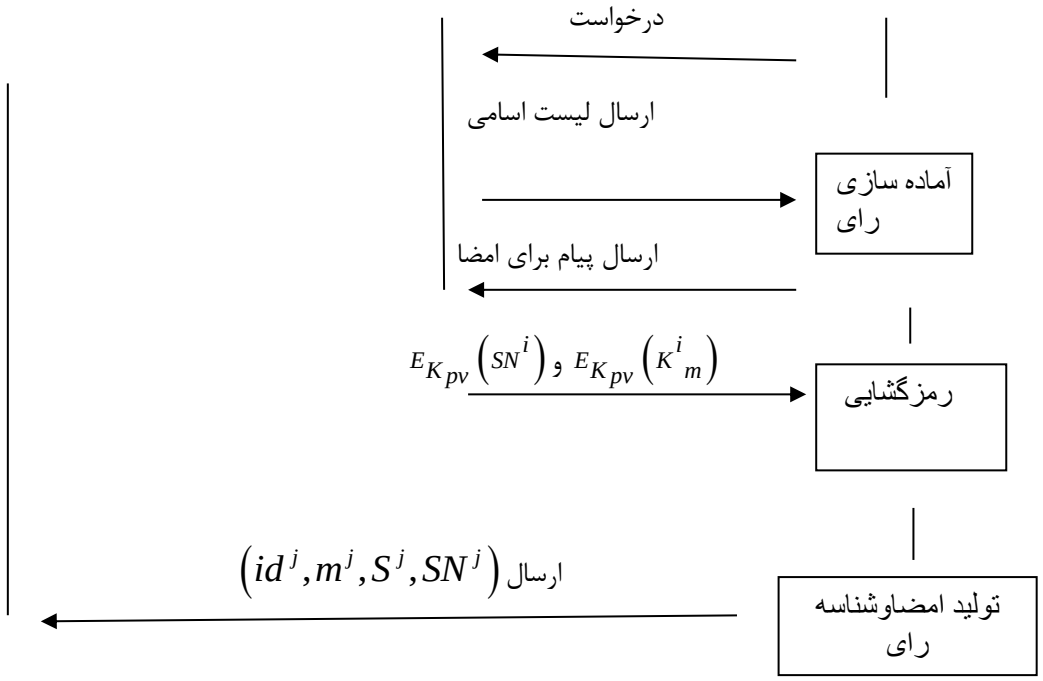
۲- رای دادن:

- رای دهنده درخواست رای دادن می‌کند. در صورت مجاز بودن لیست کاندیدا برای آن ارسال می‌شود.
- در مکان رای گیری اسم کاندیدا موردنظر خود را انتخاب می‌کند.
- رای دهنده ، رای خود را به‌صورت $m^j=\{m^j(1),m^j(2),\cdots,m^j(i),\cdots\}$ و به کار بردن تابع هش $H(.):\{0,1\}\to\{0,1\}^n$ [11]، به‌صورت $M^j=H(m^j)$ آماده و مکان رای گیری را برای امضا مطلع می‌نماید.
- مکان رای گیری پس از دریافت پیام رای دهنده، $E_{K_{pv}}(K^i{}_m)$ و $E_{K_{pv}}(SN^i)$ را برای رای دهنده از کانال کوانتومی می‌فرستد.
- رای دهنده با رمزگشایی $D(E_{K_{pv}}(K^i{}_m))$ و $D(E_{K_{pv}}(SN^i))$ مقادیر $K^i{}_m$ و SN^i را برای امضای خود به دست می‌آورد.
- رای دهنده با رمزگذاری M^j با کلید $K^i{}_m$، امضای $[S^j)=E_{K^i{}_m}(M^j)$ را تولید می‌کند.
- رای دهنده شناسه رای خود را نیز id^j را تولید می‌کند.
- رای دهنده (id^j,m^j,S^j,SN^j) به مدیریت می‌فرستد.


سرور


مکان رای گیری

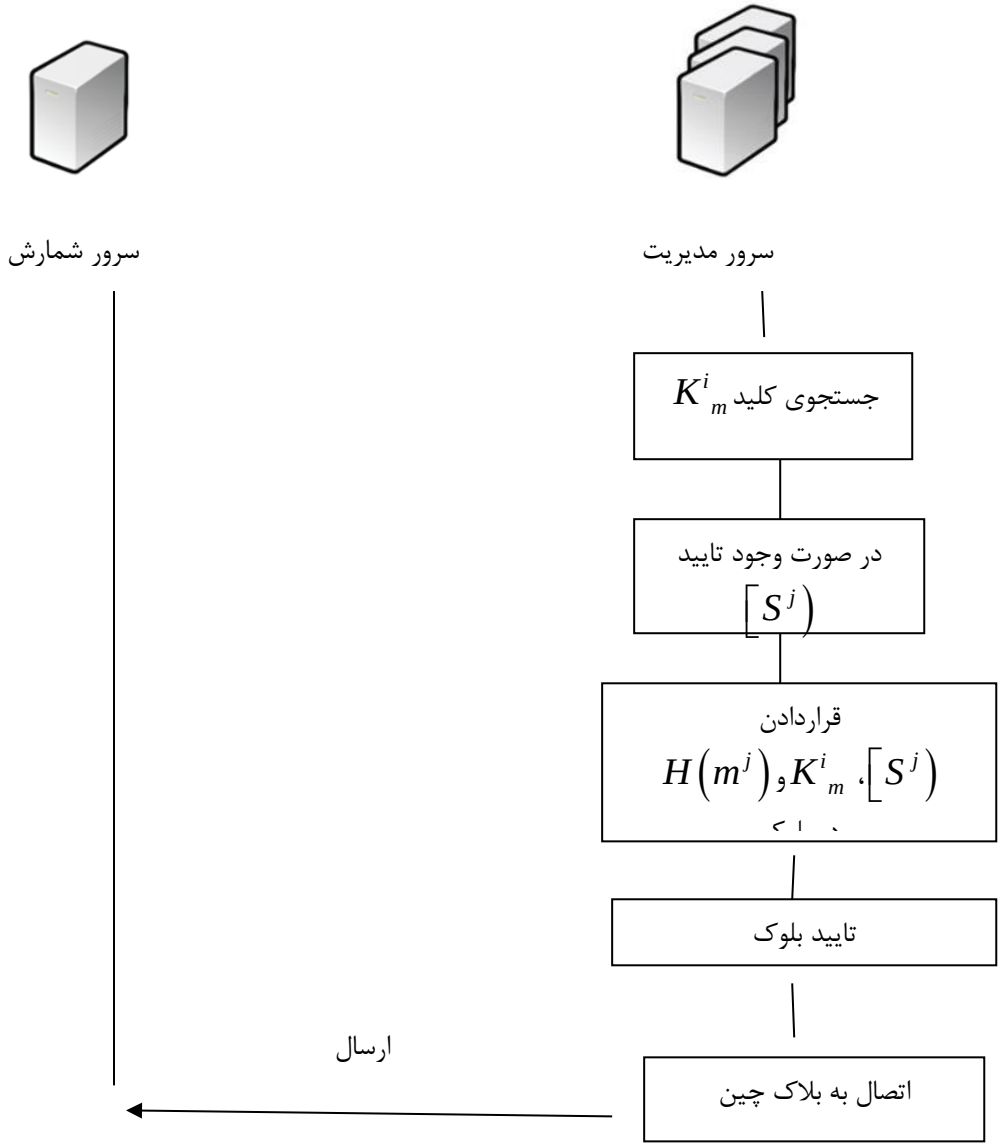

رای دادن



شکل۴: رای دادن

۳-جمع‌آوری رای ها در بلاک چین

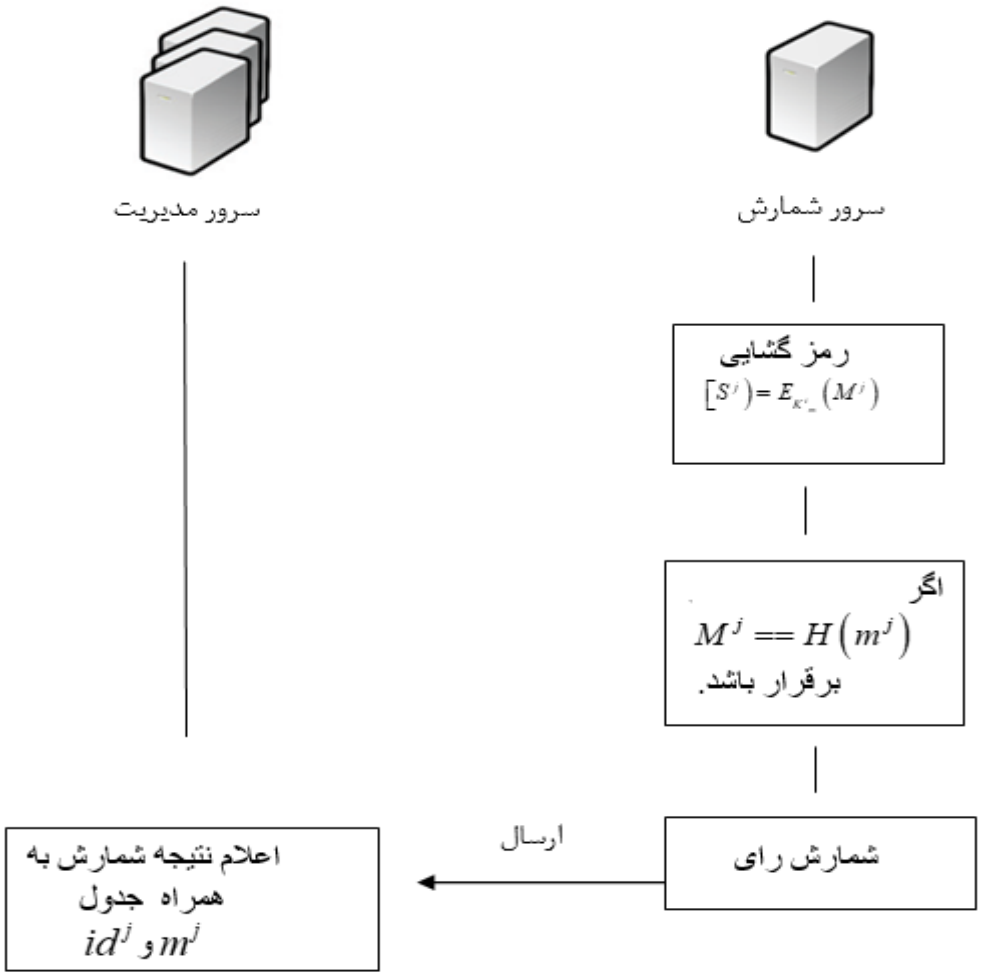
- مدیریت (id^j, m^j, S^j, SN^j) بدون اطلاع از نام شخص فرستنده دریافت می‌کند.
- با استفاده از SN^j کلید $K^i{}_m$ را جستجو می‌کند.
- اگر وجود داشته باشد $[S^j)$ را تائید و در غیر این صورت رد می‌کند.
- $[S^j)$ تائید شده به همراه $K^i{}_m$ و $H(m^j)$ را بلوک قرار داده و پس از تائید به بلاک چین متصل می‌کند.
- پس از پایان رای گیری بلاک چین به سرور شمارش فرستاده می‌شود.



شکل۵: مرحله جمع‌آوری رای ها در بلاک چین

۴ – شمارش آرا:

- بیرون آوردن معاملات از بلوک در بلاک چین.
- رمزگشایی‌شده $\lceil S^j \rfloor = E_{K^i_m}(M^j)$ و M^j به دست می‌آید.
- اگر $M^j == H(m^j)$ باشد آنگاه رای شمارش می‌شود. در غیر این صورت رد می‌شود.
- آرا پس از شمارش به مدیریت فرستاده می‌شود.
- مدیریت نتیجه نهایی را اعلام می‌کند. و در جدولی m^j و id^j را منتشر می‌کند.



شکل۶: الگوی شمارش آرا در طرح رای گیری الکترونیکی

۵. اعتبار سنجی در طرح پیشنهادی

- درخواست تائید کننده تمام بلوک‌ها از بلاک چین.
- بررسی $M^j == H(m^j)$.
-شمارش آرا و تائید نتایج.

در این طرح بدون دانستن هویت رای دهنده امضا و ناشناس بودن فرد حفظ می‌شود. همچنین اعتبار امضا با $M^j == H(m^j)$ در محل شمارش تائید می‌شود. و با فرستادن رای دهنده (id^j, m^j, S^j, SN^j) نمی‌تواند محل رای گیری منکر امضا شود و تخلف کند. رای دهنده با لیست m^j و id^j می‌تواند بررسی کند که رای وی درستکاری شده است یا خیر.

۶. تحلیل طرح:

در این بخش الزامات امنیتی طرح پیشنهادی را تجزیه‌وتحلیل می‌کنیم:

۱. کامل بودن: با استفاده از بلاک چین یکپارچگی داده‌های سیستم را فراهم می‌کند و رای کامل فراهم می شود (قرار دادن $H(m^j)$ و K^i_m، $[S^j)$ در بلوک).
۲. صداقت: در امضای کور جمعی کوانتومی هیچ‌کس به‌جز رای دهنده نمی تواند امضای معتبر ایجاد کند.
۳. حریم خصوصی: حریم خصوصی اطلاعات رای با تابع رمزگذاری و حریم خصوصی کاربر با استفاده از امضای کور جمعی گروه کوانتومی حفظ می‌شود.
۴. غیرقابل استفاده بودن: وقتی رای داده می‌شود. مدیریت با دریافت ۴-تایی (id^j, m^j, S^j, SN^j) می تواند تائید کند چه کسانی رای داده‌اند. و امضای معتبر را با استفاده از کلید K^i_m تائید کند.
۵. واجد شرایط بودن:سرور مدیریت لیست رای دهندگان را ایجاد می‌کند و از با امضا تائید می‌کند. بنابراین کسی جز لیست رای دهندگان نمی‌تواند رای دهد.
۶. انصاف: محتویات رای به‌صورت رمزگذاری منتقل می‌شود. بنابراین فاش نمی‌شود.
۷. قابلیت اطمینان: رای دهنده می‌تواند با استفاده از شناسه رای خود را بررسی کند .آیا دست‌کاری شده است یا خیر؟

مقایسه طرح با طرح‌های پیشین

در اینجا، برای نمونه چند طرح پیشین را ازنظر ویژگی‌های رای گیری مورد تحلیل قرار می‌دهیم. درمقاله [4]،سیستم بلاک چین از الگوریتم SHA-256 استفاده می‌شود. این الگوریتم متن ساده را به‌عنوان ورودی می‌گیرد. و مقدار دودویی ۲۵۶ بیتی را به‌عنوان خروجی می‌دهد و کاملاً یک‌طرفه است یعنی فقط فرآیند رمزگذاری بدون رمزگشایی دارد. در این سیستم، رای دادن توسط رای دهنده به‌صورت یک معامله در نظر گرفته می شود و بلاک چین با اطلاعات رای دهندگان و همچنین رای به‌روز می‌شود. جزییات که باید به بلاک چین ارسال شوند به‌صورت (کلید، مقدار) وارد می‌شود. ابتدا از تمام افراد یک هفته قبل از انتخابات ثبت‌نام می‌شود. به‌منظور ثبت‌نام باید شناسه ملی خود را ارائه دهد . در صورت معتبر بودن یک پین در نظر گرفته می‌شود .شخص پس از وارد شدن با پین به پایگاه رای گیری، با کلیک کردن روی اسامی کاندیدا ، می تواند شخص مورد نظر خود را انتخاب کند. پس از انتخاب پین جدیدی برای رای ایجادشده و این پین با رای انتخابی به بلاک چین دوم ارسال می‌شوند .پس از اتمام انتخابات آرا از بلاک چین شمارش می‌شوند. در این مدل فقط مدیر حق مشاهده نتیجه را دارد. اطلاعات رای دهندگان و آرا در دو بلاک چین مجزا ذخیره می‌شود. در این طرح واجد شرایط بودن افراد با اختصاص پین به آن‌ها حفظ می‌شوند.

در مقاله [7]، از بلاک چین و سایر ویژگی‌های رمزگذاری و TPP(شخص ثالث مورد اعتماد)برای رای دادن استفاده‌شده است.این طرح از چهار قسمت سازمان، شخص ثالث مورد اعتماد، رای دهنده و بلاک چین مورداستفاده قرارگرفته است. در این طرح فرض بر این است که احراز هویت توسط سازمان ثبت‌شده و لیست افراد مجاز مشخص است. رای دهنده رای خود را به سازمان به‌صورت هش می‌دهد این باید منحصربه‌فرد باشد و وقتی هش به سازمان ارسال می‌شود آنگاه پیام هش به شناسه آن در سازمان می پیوند. با استفاده از شخص ثالث مورد اعتماد ، رای تائید می‌شود بدون آنکه هویت رای دهنده فاش شود. استفاده از بیت کوین، از دست‌کاری آن‌ها جلوگیری می‌شود. با استفاده از بیت کوین و استفاده از رمزنگاری و شخص ثالث مورد اعتماد طرحی در مورد رای گیری الکترونیکی پرداخته‌شده است که کامل بودن، غیرقابل استفاده بودن، واجد شرایط بودن و قابلیت اطمینان را حفظ می‌کند.اما چون داده‌ها را رمزنگاری نمی کندنمی تواند عدالت را تضمین کند.
مقاله[8]، از امضای کور و بلاک چین برای رای گیری استفاده می‌کند. از سه بخش رای دهنده، سازمان و بازرس تشکیل‌شده است. انتقال پیام در بلاک چین به این صورت است که هر کاربر یک کلید خصوصی و عمومی وجود دارد. فرستندگان با استفاده از کلید خصوصی خود برای امضای پیام و ارسال آن استفاده می‌کند. شبکه P2P بلاک چین این تنظیمات، پیام جمع‌آوری و بسته‌بندی می‌کند. و در یک دوره زمانی وارد بلوک می‌شود و به‌عنوان پیام در سراسر شبکه

پخش می‌شود. رای دهنده، پس از آماده‌سازی رای آن را برای سازمان می‌فرستد. سازمان با امضای کور رای را تائید می‌کند بدون آنکه از محتویات آن آگاه باشد.همچنین رای دهنده رای خود را به بازرس ارسال کرده و از آن امضای کور می‌گیرد. در آخر رای و امضای کور سازمان و بازرسان را برای سازمان می‌فرستد.پس از پایان رای گیری، سازمان رای های معتبر را تائید و پس از شمارش آرا نتیجه را اعلام می کند. حریم خصوصی رای دهندگان با استفاده از امضای کور حفظ می‌شود.

جدول ۲: بررسی عملکردهای طرح‌های رای گیری پیشین

طرح	کامل بودن	صداقت	حریم خصوصی اطلاعات رای	حریم خصوصی رای دهنده	غیرقابل استفاده بودن	واجد شرایط بودن	انصاف	قابلیت اطمینان
[4]	بلاک چین	-	-	با استفاده از کلید خصوصی	قرارداد هوشمند	لیست رای دهندگان	-	بلاک چین
[7]	بلاک چین	-	-	-	جدول hash	جدول hash	-	بلاک چین
[8]	بلاک چین	-	-	امضای کور	قرارداد هوشمند	قرارداد هوشمند	-	بلاک چین
[11]	-	-	-	امضای کور جمعی کوانتومی	امضای کور جمعی کوانتومی	-	-	با انتشار جدول m^j و id^j

۷. نتیجه گیری:

با پیاده‌سازی فناوری بلاک چین و استفاده از امضای کور جمعی کوانتومی می‌توان اطمینان حاصل کنیم روند رای گیری به شیوه‌ای مطمئن و دقیق انجام شود. در این طرح رای گیری، شخص امضاکننده نمی‌تواند از محتویات متن مطلع شود. ضمنا جز امضاکننده قانونی فرد دیگری قادر به ایجاد امضا نخواهد بود. در ادامه تائید امضا بدون شناسایی از هویت شخص امضاکننده خواهد بود که حریم خصوصی رای دهنده حفظ خواهد شد. از دیگر ویژگی‌های این امضا می‌توان به غیرقابل‌انکار بودن امضاکننده، ناشناس بودن صاحب پیام، و در آخر صاحب پیام می‌تواند بررسی کند آیا پیامش دست‌کاری شده است یا خیر. همچنین با استفاده از بلاک چین حریم خصوصی و سایر ویژگی‌های رای گیری حفظ می‌شود و اطمینان از صحت نتایج به دست می‌آید.

۸. مراجع

[1] A. A. Abu Aziz, H. N. Qunoo and A. A. Abu Samra, “Using homomorphic cryptographic solutions on Evoting Systems”, **(2018)**.

[2] D. Chaum: Blind signatures for untraceable payments. In Chaum, D., Rivest, R.L., Sherman, A.T., eds.: Advances in Cryptology: Proceedings of CRYPTO '82 Santa Barbara, California, USA, Aguset 23-25, 1982., Plenum Press, New York (1982) 199-203.

[3] V. Cortier, G. Fuchsbauer and D. Galindo, “BeleniosRF: A Strongly Receipt-Free Electronic Voting Scheme”, IACR Cryptology ePrint Archive 2015, **(2015)**, pp. 629.

[4] D. Dwijesh Kumar, D. V. Chandini, B. Dinesh Reddy, Debnath Bhattacharyya and Tai-hoon Kim, Secure Electronic Voting System using Blockchain Technology, International Journal of Advanced Science and Technology, Vol.118 , 2018, pp.13-22

[5] A. Fujioka. T. Okamoto, and K. Ohta, “A practical secret voting scheme for large scale elections,” in Advances in Cryptology – AUSCRYPT’92. Heidelberg: Springer, 1992, pp. 244-251.

[6] F. P. Hjalmarsson, G. K. Hreidarsson, M. Hamdaqa, and G. Hjalmtysson, “Blockchain-based e-voting system,” in Proceedings of 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986.

[7] K. Lee, J. I. James, T. G. Ejeta, and H. J. Kim, “Electronic voting service using block-chain,” Journal of Digital Forensics, Security and Law, vol. 11, no. 2, article no. 8, 2016.

[8] Y. Liu and Q. Wang, “An e-voting protocol based on Blockchain,” 2017; https://eprint.iacr.org/2017/1043.pdf.

[9] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, **2008**.

[10] D. Springall, “Security analysis of the Estonian internet voting system”, Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, ACM, **2014**.

[10] Y. Wu, “An e-voting system based on Blockchain and ring signature,” M.S. thesis, University of Birmingham, UK, 2017.

[11] R. Xu, L. Huang, W. Yang, L. He, Quantum group blind signature scheme without entanglement, Optics Communications 284, 2011, 3654–3658.