دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر

پروژه درس مهندسی نرم‌افزار

گروه نرمینو

سیستم رأی‌گیری الکترونیکی امن

داستان کاربر و فرآیندها

اعضای گروه:

نگین دشتی
محمدرضا ماجد
سید رضا موسوی
محمدصالح ناصح

استاد راهنما:

امیرارسلان یاوری

۷ آذر ۱۴۰۳

فهرست مطالب

۱ داستان کاربر (User Story)

۱.۱ کاربر رأی‌دهنده (Voter)

یک کاربر رأی‌دهنده با استفاده از برنامه‌ای که روی گوشی یا کامپیوتر خانگی خود نصب کرده است و یا مرورگر وب باید موارد زیر برای او به نمایش گذاشته شود تا بتواند در تعامل کارآمد با مدیران سیستم، پشتیبانی و بلاک‌چین باشد.

۱.۱.۱ صفحه ورود و ثبت‌نام

(۱) نمایش توضیحات مختصر در مورد انتخابات و لینک وبلاگ برای توضیحات در مورد برنامه رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین، امنیت آن و سودمندی‌های آن.

(۲) تعبیه مکانی برای وارد کردن شماره ملی و شماره موبایل (که به نام فرد با شماره ملی وارد شده باشد) و همچنین مکانی برای وارد کردن یک کد CAPTCHA و امکان تأیید آنها توسط کاربر و ارسال درخواست ثبت‌نام (registeration).

(۳) دریافت خطای مفهوم و واضح در صورت عدم موفقیت ثبت‌نام یا بروز مشکلات دیگر (مانند صاحب صلاحیت نبودن کاربر در انتخابات از سوی مدیران سیستم، عدم تعلق شماره موبایل به کد ملی و غیره).

(۴) در صورت تأیید صلاحیت رأی‌دهنده و موفقیت‌آمیز بودن ثبت‌نام، نمایش دادن مکان ورود یک رمز پویا (OTP[1]) و یک زمان انقضا برای وارد کردن رمز پویای ارسالی به شماره موبایل وارد شده

(۵) امکان وارد کردن رمز پویای ارسالی به شماره موبایل در صفحه ورود و تأیید آن توسط کاربر

(۶) در صورت درست نبودن رمز پویای وارد شده یا انقضای زمان وارد کردن آن، خطای واضح نمایش داده شود و امکان دریافت دوباره رمز پویا برای یک تعداد محدود دفعات داده شود.

(۷) امکان تماس آنلاین با پشتیبانی برای دریافت کمک در مورد فرآیند ثبت‌نام

۲.۱.۱ صفحه اصلی

در صورت درست بودن رمز پویای ارسالی، کاربر وارد صفحه اصلی برنامه می‌شود که دارای امکانات زیر است:

(۱) نمایش اطلاعات عمومی فرد رأی‌دهنده (برخی اطلاعات شناسنامه‌ای)

[1] One Time Password

(۲) مشاهده اطلاعات مختصر در مورد انتخاباتی که کاربر در آن شرکت کرده است.

(۳) مشاهده لینک وبلاگ برای راهنمایی در مورد کلیه مراحل فرآیند انتخابات و یا تماس آنلاین با پشتیبانی در مورد فرآیند انتخابات

(۴) مشاهده گام‌های انتخابات و رأی‌دهی به صورت پشت سر (یعنی گام‌های (الف) احراز هویت، (ب) دریافت توکن، (ج) رأی دادن و ارسال توکن رأی، (د) مشاهده نتایج، و در نهایت (ه) راستی‌آزمایی). گام‌های انتخابات باید به ترتیب با انتخاب کاربر فعال شوند و موفقیت‌آمیز به اتمام برسند تا گام بعدی فعال شود.

۳.۱.۱ گام احراز هویت

در این مرحله تنها گام احراز هویت فعال است که کاربر با کلیک روی آن امکانات زیر را باید مشاهده کند:

(۱) نمایش قوانین نحوه احراز هویت، مثل چگونگی دادن مجوز دسترسی برنامه به دوربین، روش خواندن یک متن در حالی که دروبین روشن است (برای راستی‌آزمایی ربات نبودن فرد)، زمان مورد نیاز برای ضبط ویدیو، نحوه قرارگیری کاربر در تصویر و غیره.

(۲) امکان تأیید قوانین و رفتن به صفحه‌ای که در آن دوربین روشن می‌شود.

(۳) در صورت تأیید قوانین، دوربین فعال شود و متن تصادفی ارسالی سیستم بر روی گوشی به نمایش در می‌آید. پایین صفحه نمایش دکمه شروع ضبط قرار دارد که کاربر می‌تواند آن را فعال کند.

(۴) کاربر با اجازه دادن به فعال شدن ضبط دوربین، متن نمایش داده شده را با رعایت قوانین گفته شده می‌خواند و بعد از اتمام دکمه ارسال ویدیو را می‌زند.

(۵) احراز هویت ممکن است برای چند دقیقه تا یک ساعت طول بکشد. نتیجه احراز هویت از طریق پیامک و خود برنامه رأی‌گیری به اطلاع کاربر رسانیده می‌شود.

(۶) در صورت موفقیت‌آمیز نبودن احراز هویت و یا عدم تأیید مدیران، کاربر باید دوباره این مرحله را طی کند.

(۷) امکان تماس آنلاین با پشتیبانی برای دریافت کمک در مورد فرآیند احراز هویت.

(۸) در صورت موفقیت‌آمیز بودن احراز هویت و تأیید سیستم انتخابات، نتیجه از طریق پیامک به اطلاع کاربران می‌رسد و در برنامه رأی‌گیری الکترونیکی گام دریافت توکن (یا برگه رأی الکترونیکی امن) فعال می‌شود.

۴.۱.۱ گام دریافت توکن رأی

کاربر در صورت احراز هویت موفقیت‌آمیز می‌تواند روی گام دریافت توکن رأی در صفحه اصلی برنامه کلیک کند و باید امکانات زیر را مشاهده کند:

(۱) ارسال درخواست دریافت توکن برای مدیر سیستم.

(۲) در صورت موفقیت‌آمیز بودن و دریافت توکن توسط کاربر، مرحله بعد رأی‌گیری در صفحه اصلی برنامه فعال می‌شود.

(۳) در غیر این صورت پیغام خطای مناسب نمایش داده می‌شود.

(۴) امکان تماس آنلاین با پشتیبانی برای دریافت کمک در مورد فرآیند دریافت توکن رأی.

۵.۱.۱ گام ارسال توکن رأی یا به صندوق انداختن رأی

در صورت موفقیت‌آمیز بودن دریافت توکن رأی، گام رأی‌گیری الکترونیکی فعال می‌شود و کاربر با کلیک بر روی آن موارد زیر را مشاهده می‌کند:

(۱) مشاهده لیست کاندیداهای انتخابات به همراه یک گزینه دیگر با عنوان رأی سفید (رأی سفید به منزله این است که هیچ کاندیدی را انتخاب نمی‌کند). می‌توان گزینه‌های دیگر نیز به این موارد اضافه کرد.

(۲) انتخاب کاندید مدنظر توسط کاربر و ارسال توکن رأی (برای بلاک‌چین و نه مدیر سیستم)

(۳) در حین انجام این کار ساده توسط کاربر برنامه کارهای زیادی انجام می‌دهد که در بخش فرآیندها بحث می‌شود.

۶.۱.۱ گام مشاهده نتایج

بعد از ارسال رأی توسط کاربر تمامی مراحل رأی‌گیری غیرفعال می‌شوند. بعد از پایان شمارش آرا، گام مشاهده نتایج فعال می‌شود و کاربر می‌تواند آن را انتخاب کند. این کار به دلیل عدم تأثیرپذیری در نتیجه انتخابات صورت می‌گیرد که می‌تواند بسته به شرایط توسط مدیران سیستم در تنظیمات انتخابات تغییر کند. کاربر با کلیک روی مشاهده نتایج می‌تواند موارد زیر را مشاهده کند:

(۱) مشاهده نتایج انتخابات و آرای کاندیداها

(۲) مشاهده لینک وبلاگ برای آمارهای دیگر به صورت نموداری و گرافیکی

۷.۱.۱ گام راستی‌آزمایی

بعد از مشاهده نتایج انتخابات گام بعدی که راستی‌آزمایی است فعال می‌شود که کاربر می‌تواند با دسترسی به دفترکل توزیع‌شده بلاک‌چین رأی خود را راستی‌آزمایی کند. با کلیک روی این گام موارد زیر نمایش داده می‌شود:

(۱) گزینه دریافت و دانلود کل دفتر توزیع شده در بلاک‌چین و راستی‌آزمایی با استفاده از شناسه عمومی کاربر

(۲) گزینه راستی‌آزمایی بدون دانلود کل دفتر کل توزیع‌شده

(۳) نمایش راستی‌آزمایی در هر یک از موارد

۲.۱ مدیر انتخابات (Election Admin)

مدیران انتخابات یا به اصطلاح authorityها که در یک انتخاب ملی به عنوان نمونه می‌تواند وزارت کشور یا شورای نگهبان یا غیره باشد باید از طریق یک سامانه امکانات زیر را در اختیار داشته باشد.

۱.۲.۱ تنظیمات انتخابات

مدیر باید بتواند تنظیمات مورد نیاز برای یک انتخابات جدید را انجام بدهد.

(۱) تعریف نام انتخابات و وارد کردن اسامی کاندیداها

(۲) تولید کلید عمومی و خصوصی و ارسال کلید عمومی برای Boot Node

- کلید عمومی برای تأیید اصالت توکن رأی (برگه رأی کاربر) استفاده می‌شود و باید در اختیار ماینرها یا مشارکت‌کنندگان در شبکه بلاک‌چین قرار گیرد. این کار از طریق یک گره در شبکه به نام Boot Node انجام می‌شود.
- کلید خصوصی برای امضای دیجیتال توکن رأی استفاده می‌شود و باید در سمت مدیران انتخابات مخفی بماند.
- مشارکت‌کنندگان در بلاک‌چین با استفاده از این کلید عمومی می‌توانند از یک طرف جلوی مصرف دوباره توکن را بگیرند و از طرف دیگر قرارداد هوشمند توکن را در شبکه اجرا کنند تا با اجرای الگوریتم قرارداد هوشمند در هسته بلاک‌چین، یک رأی به آرای کاندید مد نظر توکن رأی اضافه شود و این توکن به دفتر کل توزیع‌شده اضافه شود.

(۳) تعریف تنظیمات مورد نیاز برای تولید توکن رمزنگاری شده با کلید خصوصی مدیر، توسط یک قرارداد هوشمند الکترونیکی، مثل لیست کاندیداها و تنظیمات مربوط به زمان شروع و پایان ارسال توکن توسط رأی‌دهنده و غیره.

(۴) تعاملاتی که در بخش کاربر رأی‌دهنده با مدیران سیستم گفته شد، در سمت مدیران سیستم به صورت خودکار و الگوریتمیک اجرا می‌شود و نیازی به کار یا عملی از سمت مدیران نیست. این موارد در بخش فرآیندها بحث می‌شوند.

۲.۲.۱ مدیریت مشارکت‌کنندگان در شبکه بلاک‌چین

مدیر انتخابات باید بتواند درخواست‌های مشارکت‌کنندگان در انتخابات به عنوان ماینر در بلاک‌چین را پاسخ بدهد و با توجه به سیاست‌های اعلامی در وبلاگ آنان را به شبکه بلاک‌چین اضافه کند.

(۱) مشاهده لیست درخواست‌ها برای مشارکت به عنوان ماینر در شبکه بلاک‌چین (که می‌تواند قبل از شروع انتخابات یا در حین آن باشد) و تأیید یا عدم تأیید آنها.

(۲) مشاهده وضعیت هر کدام از مشارکت‌کنندگان، قدرت سخت‌افزاری آنها و میزان مشارکت در شبکه در هر لحظه

(۳) ارسال لیست مشارکت‌کنندگان در شبکه بلاک‌چین برای Boot Node (که با استفاده از این گره بوت ارتباط مشارکت‌کنندگان در شبکه با یکدیگر حفظ می‌شود).

۳.۲.۱ مدیریت پشتیبان‌ها

مدیر انتخابات باید بتواند پشتیبان‌های انتخابات را مشاهده و پیگیری کند.

(۱) ثبت حساب جدید پشتیبانی

(۲) مشاهده لیست پشتیبان‌ها

(۳) مشاهده فعالیت‌های پشتیبان‌ها

(۴) مشاهده پیام‌های ارسالی از طرف پشتیبان‌ها

(۵) تغییر، حذف و ویرایش حساب‌های پشتیانی

۴.۲.۱ مدیریت وبلاگ

(۱) ارسال و ویرایش مطالب مفید در مورد رأی‌گیری الکترونیکی امن مبتنی بر بلاک‌چین و ویژگی‌های مهم آن

(۲) ارسال مطلب در مورد نحوه رأی‌گیری الکترونیکی و راهنمایی کاربران برای استفاده از برنامه رأی‌گیری

(۳) مشاهده نظرات و سؤالات پرسیده شده

(۴) ارسال سؤالات متداول و جواب‌های آنها

(۵) ارسال مشارکت‌کننده‌گان در شبکه بلاک‌چین به صورت لحظه‌ای در وبلاگ

(۶) انتشار آمار لحظه‌ای مربوط به انتخابات در هر لحظه، مثل تعداد رأی‌دهنده‌گان، تعداد ثبت‌نام کنندگان و غیره

(۷) انتشار نتایج انتخابات و آرای هر کاندید پس از اتمام انتخابات و همچنین آمارهای دیگر به صورت نموداری و گرافیکی

۵.۲.۱ مدیریت ارتباط با سرور ارسال رمز پویا

(۱) بررسی و مشاهده وضعیت امکان ارتباط سریع و امن با سرور ارسال رمز پویا

(۲) مشاهده جدول وضعیت پیام‌های ارسالی برای سرور رمز پویا و زمان پاسخگویی سرور و نتایج آن در ثبت‌نام کاربران

۶.۲.۱ مدیریت ارتباط با Boot Node

(۱) بررسی و مشاهده وضعیت امکان ارتباط سریع و امن با Boot Node

(۲) مشاهده جدول لحظه‌ای مشارکت‌کنندگان در شبکه بلاک‌چین و وضعیت آنها

۷.۲.۱ مدیریت ارتباط با سامانه ثبت‌احوال

(۱) بررسی امکان ارتباط سریع و امن با سامانه ثبت‌احوال یا دیتابیسی از افراد و تصاویر آنها

(۲) مشاهده جدول لحظه‌ای درخواست‌های ارسال شده برای ثبت‌احوال و زمان پاسخگویی و دیگر آمارهای مورد نیاز

۸.۲.۱ مدیریت بخش کاربران

(۱) مشاهده لیست کاربران ثبت‌نام شده و وضعیت آنها در برخی از گام‌های انتخابات (ثبت‌نام، احراز هویت و ارسال توکن).

(۲) مشاهده لیست کاربرانی که در هر یک از گام‌های رأی‌گیری به مشکل برخورده‌اند و دلایل و خطاهای این مشکل.

۹.۲.۱ مشاهده دفتر کل توزیع شده

(۱) مشاهده دفتر کل توزیع شده و آمار کاربرانی که رأی خود را به شبکه بلاک‌چین و دفتر کل توزیع شده داده‌اند و وضعیت آرای انتخابات

(۲) انتشار آمار لحظه‌ای مربوط به انتخابات در هر لحظه، مثل تعداد رأی‌دهنده‌گان، تعداد ثبت‌نام کنندگان و غیره

(۳) انشتار آمار نهایی پس از اتمام زمان انتخابات

۳.۱ تأییدکنندگان اثبات صلاحیت در شبکه بلاک‌چین

تأییدکنندگان اثبات صلاحیت (POA validators[1]) یا ماینرها می‌تواند هر یک از افراد، نهادها و احزاب در یک جامعه یا کشور باشند که با امکانات سخت‌افزاری خود به برگزاری روند انتخابات و غیرمتمرکز شدن آن کمک شایانی می‌کنند. آنها می‌توانند با ارسال درخواست برای مدیر سیستم رأی‌گیری (به عنوان نمونه از طریق سایت وزارت کشور یا ...) و فقط اجرا کردن هسته شبکه بلاک‌چین بر روی سیستم خود به برگزاری انتخابات و جمع‌آوری آرا کمک کنند.

۴.۱ Boot Node

گره Boot در شبکه بلاک‌چین سروری است که سعی می‌کند گره‌های مختلف شبکه را در هر لحظه از وجود هم باخبر کند تا دفتر کل توزیع شده بین آنها به اشتراک گذاشته شود و به صورت غیرمتمرکز بتوان قراردادهای هوشمند را در هسته شبکه بلاک‌چین اجرا نمود.

۵.۱ بخش پشتیبانی

۱.۵.۱ پروفایل

(۱) امکان مشاهده پروفایل کاربری و مشاهده اطلاعات حساب

(۲) مشاهده آمار سؤال‌های پاسخ داده شده در هر یک از بخش‌های انتخابات و آمار مربوط به سؤالاتی که بسته نشده‌اند.

۲.۵.۱ مشاهده لیست سؤالات جدید

(۱) امکان پاسخ‌دهی به به سؤالات دریافتی

[1] Proof of Authority validators

(۲) امکان فوروارد کردن مشکلات و سؤالات اساسی به مدیر

۲ فرآیندها

۱.۲ فرآیندهای کاربر رأی‌دهنده

۱.۱.۲ فرآیند ثبت‌نام

(۱) رأی‌دهنده برنامه رأی‌گیری الکترونیکی امن (نرمینو) را بر روی گوشی موبایل یا کامپیوتر خود نصب می‌کند و یا از طریق مروگرهای وب و آدرس سایت به آن دسترسی می‌گیرد.

(۲) کاربر رأی‌دهنده شماره ملی و شماره موبایلی که به نام خود او باشد را در اینترفیس login برنامه وارد می‌کند، و درخواست ثبت‌نام را به صورت رمزنگاری انتها به انتها[1] برای سیستم رأی‌گیری الکترونیکی ارسال می‌کند.

(۳) در صورت صحیح بودن شماره ملی و شماره موبایل، تعلق شماره موبایل به شماره ملی و از طرف دیگر قانونی بودن رأی‌دهنده (با چک شدن شرایطی مثل آیا اصلاً این فرد مجاز به شرکت در این انتخابات هست یا نه) یک رمز پویا یا OTP به شماره موبایل ثبت‌شده ارسال می‌شود و کاربر آن را در برنامه و در جای مناسب وارد می‌کند و آن را برای سیستم ارسال می‌کند.

(۴) در صورت صحیح نبودن شماره ملی یا شماره موبایل یا هر گونه مشکل دیگر مثل قانونی نبودن رأی‌دهنده و غیره، خطای مناسب بر روی برنامه به کاربر نمایش داده می‌شود.

(۵) در صورت صحیح بودن رمز پویای ارسال شده توسط کاربر، او وارد برنامه می‌شود و اطلاعات مختصری در مورد مشخصات انتخاباتی که در آن شرکت کرده است و برخی از مشخصات شناسنامه‌ای کاربر نمایش داده می‌شوند.

(۶) در صورت صحیح نبودن رمز پویای وارد شده توسط کاربر، پیغام خطای مناسب برای او نمایش داده می‌شود و امکان درخواست ارسال مجدد رمز پویا به تعداد مشخص شده و محدود به او داده می‌شود.

(۷) در صورت بروز مشکلات در فرآیند ثبت‌نام و یا عدم اطلاع از فرآیندهای انتخابات کاربر می‌تواند با کلیک بر روی مشاهده وبلاگ وارد وبلاگ انتخابات شود تا راهنمایی‌های نوشتاری و ویدیویی مورد نیاز را مشاهده کند.

(۸) در صورت بروز مشکلات در فرآیند ثبت‌نام کاربر با کلیک بر روی تماس با پشتیبانی وارد فرآیند تعامل آنلاین با پشتیبانی می‌شود.

[1] end-to-end encryption

۲.۱.۲ فرآیند احراز هویت

(۱) رأی‌دهنده بعد از ورود به اینترفیس برنامه و مشاهده مشخصات انتخابات مورد نظر و مشخصات خود از طریق کلیک بر روی گزینه گام احراز هویت وارد فرآیند احراز هویت می‌شود.

(۲) در اینترفیس احراز هویت، کاربر راهنمایی‌های موجود در اینترفیس مانند فعال کردن دوربین گوشی یا وب‌کم کامپیوتر را می‌خواند و سیاست‌های مرتبط با ضبط و ارسال ویدیوی زنده از خود را مشاهده می‌کند.

(۳) با تأیید سیاست‌های نوشته شده درخواست احراز هویت برای سیستم ارسال می‌شود.

(۴) در صورت دریافت تأیید درخواست احراز هویت، دوربین کاربر فعال شده و متنی تصادفی بر روی اینترفیس احراز هویت مشاهده می‌شود.

(۵) کاربر در حالی که دوربین روشن است، متن مشاهده شده را با توجه به سیاست‌های اعلامی می‌خواند و ویدیو را ارسال می‌کند.

(۶) کاربر منتظر می‌ماند تا فرآیند احراز هویت کامل شود و پیام تأیید احراز هویت برای او پیامک شود و در برنامه گام بعدی (دریافت توکن رأی) فعال شود. این فرآیند ممکن است تا حداکثر ۱ ساعت طول بکشد.

(۷) در صورت بروز خطا یا مناسب نبودن کیفیت ویدیو یا هر گون مشکل احتمالی در فرآیند احراز هویت از سمت مدیران و مقامات انتخابات، به کاربر از طریق برنامه و پیامک اطلاع‌رسانی می‌شود تا دوباره فرآیند را تکرار کند.

۳.۱.۲ فرآیند دریافت توکن رأی

در صورت موفقیت‌آمیز بودن گام احراز هویت، گام دریافت توکن در اینترفیس رأی‌گیری الکترونیکی برای کاربر فعال می‌شود.

(۱) کاربر با انتخاب گام دریافت توکن درخواست دریافت توکن را برای سیستم ارسال می‌کند.

(۲) در صورت تأیید درخواست توسط سیستم یک توکن رأی برای کاربر ارسال می‌شود و کاربر پیغام دریافت توکن را دریافت می‌کند و گام بعدی انتخابات برای او فعال می‌شود.

- این توکن با استفاده از کلید خصوصی مدیران انتخابات ساخته شده است.
- توکن رمزگذاری شده رابطی برای تعامل کاربر با بلاک‌چین برای رأی دادن و حسابرسی است. توکن فقط یک بار قابل استفاده است و نمی‌توان آن را بین کیف پول‌ها انتقال داد یا فروخت.
- قرارداد هوشمند انتخابات شامل موارد زیر است:

- تنظیمات پارامترهای انتخابات مثل شروع و پایان امکان ارسال رأی و عدم استفاده دوباره از توکن
- لیستی از اعضای POA[1] یا ماینرها برای ارسال رأی به آنها در شبکه بلاک‌چین
- لیست نامزدهای انتخابات و امکان انتخاب یک یا چند تا از آنها بر اساس سیاست‌های مدیران

(۳) در صورت عدم تأیید پیغام کاربر پیغام خطای مناسب دریافت می‌کند.

۴.۱.۲ فرآیند ارسال توکن رأی برای بلاک‌چین یا به صندوق انداختن رأی

در صورت موفقیت‌آمیز بودن گام دریافت توکن، اینترفیس رأی‌دهی، گام رأی‌گیری الکترونیکی برای کاربر فعال می‌شود.

(۱) با انتخاب گام رأی‌دهی توسط کاربر، لیست کاندیداها در اینترفیس نمایش داده می‌شوند.

(۲) کاربر با انتخاب کاندید مورد نظر و انتخاب دکمه تأیید رأی خود را به سمت دفتر کل توزیع‌شده در بلاک‌چین و برای یکی از ماینرها ارسال می‌کند.

(۳) در ضمن انتخاب دکمه تأیید چندین کار در اینتفرفیس برنامه رخ می‌دهد که به شرح زیر هستند:

- تولید کلیدهای عمومی و خصوصی برای کاربر که در آن کلید خصوصی به منزله شناسه خصوصی او و کلید عمومی به منزله شناسه عمومی او در بلاک‌چین است.
- رمزگذاری توکن (برگه رأی) با استفاده از یک الگوریتم رمزگذاری مانند ZKP رمزگذاری می‌شود، که با استفاده از کلید عمومی کاربر برای اثبات رأی بدون افشای آن در شبکه بلاک‌چین مورد استفاده است.
- توکن رمگذاری شده به همراه ZKSMP[2] آن به سمت دفتر کل توزیع‌شده در بلاک‌چین ارسال می‌شوند.

۵.۱.۲ فرآیند مشاهده نتایج و اطلاعات راجع به انتخابات

(۱) بعد از اتمام انتخابات و اعلام نتایج کاربر می‌تواند با ورود به برنامه، نتایج انتخابات و آمارهای مربوط به آن را مشاهده کند.

۶.۱.۲ فرآیند راستی‌آزمایی رأی کاربر در انتخابات

(۱) ZKSMP تولید شده توسط کاربر نشان می‌دهد که قرارداد موجود در دفترکل توزیع‌شده متعلق به کاربر مدنظر با شناسه عمومی او است و راستی‌آزمایی فردی در انتخابات و شمرده شدن رأی او را تأیید می‌کند.

[1] Proof Of Authority [2] Zero Knowlege Set Membership Proof

۷.۱.۲ فرآیند درخواست پشتیبانی

(۱) در هر مرحله از گام‌های انتخابات کاربر با ارسال درخواست پشتیبانی می‌تواند سؤالات خود را با پشتبان‌های انتخابات در میان بگذارد و به صورت آنلاین با آنها در ارتباط باشد.

۲.۲ فرآیندهای مدیران انتخابات

۱.۲.۲ فرآیند راه‌اندازی و تنظیمات انتخابات

(۱) تولید کلید خصوصی و عمومی با استفاده از یک الگوریتم کلید عمومی امن مثل خم‌های بیضوی یا RSA و ارسال کلید عمومی برای تمامی تأییدکنندگان POA در شبکه بلاک‌چین از طریق Boot Node.

- قراردادهای هوشمند توکن در سمت مدیران سیستم با استفاده از کلید خصوصی امضا می‌شوند. کلید خصوصی باید مخفی بماند.
- تأییدکنندگان POA در شبکه بلاک‌چین می‌توانند با استفاده از این کلید عمومی قراردادهای ارسالی توسط هر رأی‌دهنده به سمت دفترکل توزیع‌شده را تأیید و راستی‌آزمایی کنند و از مصرف مجدد آن جلوگیری کنند و غیره.

(۲) مقداردهی اولیه سیاست‌های انتخابات و قرار دادن لیست کاندیداها و ضوابط رأی‌دهی در قراردادهای هوشمند

(۳) برقراری ارتباط با سرعت بالا و امن از طریق یک API با سامانه ثبت احوال یا یک دیتابیسی از کاربران که شامل مشخصات و تصاویر آنها باشد.

(۴) برقراری ارتباط با سرعت بالا و امن از طریق یک API با سامانه هوش مصنوعی تشخیص زنده بودن ویدیوهای ارسالی کاربران.

(۵) برقراری ارتباط با سرعت بالا و امن از طریق یک API با سامانه ارسال پیام کوتاه

۲.۲.۲ فرآیند ثبت‌نام رأی‌دهندگان

(۱) در صورت دریافت درخواست ثبت‌نام از سمت یک کلاینت، شماره ملی و شماره موبایل را در دیتابیس و یا از طریق API با سامانه ثبت‌احوال چک می‌کند.

(۲) در صورتی که شماره موبایل به نام شماره ملی ثبت شده باشد و سیاست‌های کلی انتخابات مثل سن و واجدشرایط بودن و غیره رعایت شده باشند، یک کد OTP تصادفی تولید و به همراه شماره موبایل کاربر برای سامانه ارسال پیامک می‌فرستد. در غیر این صورت یک پیغام خطا را به سمت کلاینت مورد نظر ارسال می‌کند.

(۳) در صورتی که در زمان مناسب و تعیین شده کاربر کد ارسالی را برای سیستم ارسال کند، برخی از اطلاعات در مورد مشخصات انتخابات و مشخصات خود کاربر برای کلاینت ارسال می‌شود. در این صورت کاربر اطلاعات را دریافت کرده و login می‌شود.

۳.۲.۲ فرآیند احراز هویت رأی‌دهندگان

(۱) در صورت دریافت درخواست احراز هویت از سمت یک کلاینت، سیستم رأی‌گیری برای او درخواست ارسال ویدیو را به همراه یک متن تولید شده به صورت تصادفی را ارسال می‌کند.

(۲) در صورت ارسال ویدیو از سمت کلاینت، ویدیو و متن تولید شده را برای دو سامانه تشخیص هویت فرد (مثل ثبت‌احول) و سامانه تشخیص زنده بودن ویدیو (سامانه‌ای بر اساس هوش مصنوعی که می‌تواند تشخیص بدهد که فرد به صورت زنده در حال خواندن متن مورد نظر است) ارسال می‌کند.

(۳) در صورت تأیید ویدیو از سمت دو سامانه، پیام تأیید هویت برای کاربر از طریق اینترنت و از طریق پیامک ارسال می‌شود.

۴.۲.۲ فرآیند تولید توکن رمزنگاری شده

(۱) به محض تأیید هویت در سامانه رأی‌گیری الکترونیکی یک توکن در قالب قرارداد هوشمند الکترونیکی با استفاده از کلید خصوصی سیستم تولید می‌شود که کاربردهای زیر را دارد:

- اثبات اینکه که کاربر مجاز به رأی‌دادن هست و بیش از یک بار نتواند از توکن برای رأی دادن استفاده کند. کلید عمومی سیستم رأی‌دهی قبلاً برای تمامی مشارکت‌کنندگان در بلاک‌چین ارسال شده است که با استفاده از آن می‌توانند تراکنش‌ها (در اینجا مجاز بودن رأی‌دهنده) را اثبات کنند.
- تنظیم پارامترهایی برای انجام انتخابات مثل زمان شروع استفاده کاربر از توکن برای انتخاب و زمان پایان آن.
- همچنین لیست کاندیداها و لیست اعضای تأییدکننده POA یا مشارکت‌کنندگان در بلاک‌چین در این قرارداد الکترونیکی قرار دارد که کاربر رأی‌دهنده باید انتخاب خود را بر اساس لیست کاندیداها در قرارداد هوشمند انجام دهد و برای بلاک‌چین ارسال کند.

(۲) در صورت دریافت درخواست رأی‌دهی از سمت کلاینتی که احراز هویت شده است، سیستم توکن رمزگذاری شده (برگه رأی) را برای او ارسال می‌کند.

(۳) همزمان با ارسال توکن، لیست کاندیداها نیز برای کلاینت ارسال می‌شوند که در اینترفیس کلاینت نمایش داده شوند.

(۴) همچنین مهلت استفاده از توکن رأی‌گیری نیز برای کلاینت ارسال می‌شود تا به او نمایش داده شود.

۵.۲.۲ فرآیند مشاهده نتایج انتخابات

(۱) با اجرای قراردادهای هوشمند در ماشین مجازی شبکه بلاک‌چین توسط مشارکت‌کنندگان (ماینرها)، توکن مانند یک نرم‌افزار اجرا می‌شود و همه مشارکت‌کنندگان می‌توانند بروزرسانی‌ها را ببینند. با اجرای قرارداد شمارش آرا نیز در شبکه بلاک‌چین انجام می‌شود.

(۲) چون شبکه بلاک‌چین و دفتر کل توزیع‌شده می‌تواند در دسترس همه باشد، مدیران انتخابات نیز می‌توانند نتایج را مشاهده کنند.

۶.۲.۲ ارسال نتایج نهایی و آمارهای مرتبط

(۱) با اتمام فرآیند شمارش آرا مدیران سیستم نتایج و آمار مربوطه را در وبلاگ بروزرسانی می‌کنند.

۳.۲ فرآیندهای تأییدکنندگان POA در شبکه بلاک‌چین

تأییدکنندگان اثبات صلاحیت (POA validators[1]) یا مشارکت‌کننده‌گان در شبکه بلاک‌چین، مانند ماینرها در سیستم بلاک‌چین بیت‌کوین عمل می‌کنند. آنها تراکنش‌ها را تأیید می‌کنند و در مرحله رأی‌گیری آنها را به بلاک‌چین اضافه می‌کنند. ماینرها مشارکت‌کنندگان در شبکه بلاک‌چین هستند که در یک فرآیند انتخاباتی می‌تواند افراد یا احزاب یا نهادها باشند. هر کس بخواهد به عنوان مشارکت‌کننده سخت‌افزار خود را در اختیار سیستم انتخابات قرار دهد می‌تواند با ثبت‌نام در سایت انتخابات، ماشین مجازی شبکه بلاک‌چین را دریافت نموده و بر روی سیستم سرور خود نصب کند و به عنوان یک ماینر به فرآیند انتخابات و غیرمتمرکز شدن آن کمک کند.

در یک قرارداد هوشمند[2]، توافقات مستقیماً در کد برنامه در یک عبارت if-when نوشته می‌شود. هنگامی که الزامات عبارات if-when برآورده می‌شود، کد برنامه شرایط قرارداد هوشمند را اجرا می‌کند.

تأییدکنندگان اثبات صلاحیت یا مشارکت‌کنندگان در شبکه بلاک‌چین، توکن رأی‌گیری رمزنگاری شده و شامل قرارداد هوشمند را دریافت می‌کنند و سپس آن را به داخل یک ماشین مجازی (VM[3]) منتقل می‌کند. این ماشین مجازی، قرارداد هوشمند را به عنوان ورودی می گیرد و آن را مانند نرم‌افزاری اجرا می‌کند که در آن همه مشارکت‌کنندگان در شبکه می‌توانند بروزرسانی‌ها را تماشا کنند.

۴.۲ فرآیندهای Boot Node

BootNode (یا سرویس کشف) گره‌ای است که توسط اعضایی با امکان دسترسی به سیستم میزبانی می‌شوند. آنها

[1] Proof of Authority validators [2] smart contract [3] virtual machine

به سایر نودها در کشف کمک می‌کنند و با فراهم کردن یک IP ثابت یا اندپوینت API داده که حاوی مجموعه‌ای از اطلاعات اتصال است، به سایر گره ها کمک می‌کنند تا همدیگر را کشف کنند و سهولت اتصال فراهم شود.