دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

پروپوزال پروژه مهندسی نرم‌افزار، سال تحصیلی ۱۴۰۳-۱

سیستم رأی‌گیری الکترونیکی امن

گروه نرمینو

اعضای گروه:

محمدرضا ماجد
نگین دشتی
محمدصالح ناصح
سیدرضا موسوی

استاد راهنما:

امیرارسلان یاوری

۱۸ مهر ۱۴۰۳

فهرست مطالب

۱ معرفی پروژه

سیستم رأی‌گیری الکترونیکی امن[۱]، سیستمی برای انجام رأی‌گیری الکترونیکی آنلاین با تمرکز بر یکپارچگی[۲]، امنیت[۳]، دقت، شفافیت[۴]، قابل تأیید بودن[۵] (یا راستی‌آزمایی) و حفظ حریم خصوصی[۶] است. این اپلیکیشن به کاربران اجازه می‌دهد تا در انتخابات و نظرسنجی‌ها به راحتی و با اطمینان رأی خود را ثبت کنند. هدف از این نرم‌افزار ایجاد یک بستر امن و قابل اعتماد برای فرایندهای دموکراتیک است.

سیستم رأی‌گیری الکترونیکی امن، امکان ثبت‌نام و احراز هویت کاربران، امکان شرکت در رأی‌گیری‌های مجاز ارائه شده در سیستم برای واجدین شرایط با حفظ امنیت، شفافیت و حریم خصوصی را می‌دهد. همچنین کاربر می‌تواند در تمامی مراحل رأی خود را راستی‌آزمایی کند و گزارش‌های و تحلیل نتایج را در سیستم مشاهده کند.

برخی از ویژگی‌های مهم سیستم رأی‌گیری الکترونیکی امن ارائه شده در این پروژه به شرح زیر است:

طراحی رابط کاربر پسند: رابط کاربری برای همه افراد ساده و آسان و بدون پیچیدگی خواهد بود. همچنین این رابط اولویت را به دسترسی عادلانه و ثابت رأی‌دهندگان می‌دهد و تضمین می‌کند که صرف نظر از روند رأی‌گیری، همه رأی‌دهندگان از حقوق و فرصت‌های رأی برابر برخوردار هستند و اطلاعات و فرصت‌های یکسانی را دریافت می‌کنند.

احراز هویت و واجد شرایط بودن: قبل از رأی دادن کاربر در سیستم باید ثبت نام کند و احراز هویت[۷] شود. احراز هویت در سیستم با استفاده روش‌های احراز هویت چندعاملی[۸] (مانند OTP[۹]، اثر انگشت یا شناسایی چهره) انجام می‌گیرد. OTP (یا پسورد یک‌بار مصرف) توسط سیستم به شماره موبایل ثبت‌شده از کاربر مجاز ارسال می‌شود و همزمان با این عامل، شناسایی چهره و یا اثر انگشت نیز اعمال می‌گردد.

- اصالت رأی دهنده: سیستم نیاز به شناسایی رأی‌دهندگان بر اساس پایگاه داده ثبت‌نام رأی‌دهندگان دارد و تضمین می‌کند که فقط رأی‌دهندگان واجد شرایط رأی خود را ثبت می‌کنند.
- منحصربه‌فرد بودن: رأی‌دهنده فقط یک بار می‌تواند رأی بدهد و نتیجه نهایی آن رأی هرگز تغییر نمی‌کند.
- واجد شرایط بودن: تضمین می‌کند که فقط رأی دهندگان قانونی می‌توانند رأی دهند و هویت آنها دقیقاً تأیید می‌شود.

شناسه عمومی و خصوصی: به هر فرد دو شناسه داده می‌شود. یک شناسه عمومی که باید برای سوابق عمومی استفاده شود. این شناسه قرار نیست به طور تصادفی تولید شود، بلکه باید به عنوان راهی برای شناسایی منحصر به

[1] Secure Electronic Voting (E-Voting) System [2] Integrity [3] Security [4] Transparency [5] Verifiability [6] Privacy
[7] Authentication [8] multi-factor authentication [9] One-time password

فرد یک شخص ارائه شود. به عنوان مثال می‌توان از ترکیب شماره ملی و یک شماره موبایل از فرد برای شناسایی او بهره برد. شناسه دیگر، شناسه خصوصی است و برای زمانی مفید است که کسی بخواهد بررسی کند که رأی او در نظر گرفته شده است و صحت آن را به آنچه رأی داده است تأیید کند.

رمزنگاری داده‌ها: تمامی ارتباطات بین کلاینت و سرور سیستم رأی‌گیری الکترونیکی امن به صورت انتها به انتها[1] با استفاده از الگوریتم‌های رمز اثبات شده رمزنگاری می‌شود. همچنین تمامی داده‌های کاربران در سمت سرور برای حفاظت از حریم خصوصی و جلوگیری از دسترسی غیرمجاز به داده‌ها با استفاده از الگوریتم‌های امن رمزنگاری می‌شوند.

قابل تأیید بودن رأی‌گیری: قابل تأیید بودن[2] برای سیستم رأی‌گیری الکترونیکی قابل اعتماد امری ضروری است و معمولاً تحت سه دیدگاه مختلف در این سیستم در نظر گرفته می‌شود:

- تأیید فردی[3]: راستی‌آزمایی فردی به رأی‌دهندگان اجازه می‌دهد تا بررسی کنند که آرای فردی آنها به درستی شمارش شده است.
- تأیید عمومی[4]: راستی‌آزمایی عمومی به رأی دهندگان و اشخاص ثالث اجازه می‌دهد تا بررسی کنند که نتایج انتخابات با آرای ریخته‌شده مطابقت داشته باشد.
- تأیید انتها به انتها[5]: هدف از راستی‌آزمایی E2E این است که یک شخص اطمینان حاصل کند که رأی او به درستی ریخته شده و در شمارش نهایی نیز شمارش شده است و در نتیجه کل فرایند رأی‌گیری به درستی انجام شده است. این امر به نوبه خود منجر به نتایج قابل اعتماد انتخابات می‌شود.

توجه داشته باشید که ویژگی راستی‌آزمایی E2E در سیستم های رأی‌گیری سنتی به سختی قابل پشتیبانی است، زیرا رأی‌دهنده پس از رأی دادن تعامل خود را با سیستم رأی‌گیری از دست می‌دهد و دیگر قادر به راستی‌آزمایی رأی خود در شمارش نهایی نیست.

نظارت و حسابرسی شفاف: امکان پیگیری و حسابرسی آرا با ثبت شفاف تمامی مراحل رأی‌گیری، به طوری که ناظران مستقل بتوانند صحت فرآیند را تأیید کنند.

رأی‌گیری ناشناس: تضمین ناشناس بودن[6] رأی‌دهنده و رأی او به طوری که رأی‌دهندگان بتوانند بدون هیچ فشاری رأی خود را ثبت کنند و همچنین رأی‌ها به صورت راز باقی بمانند و حتی ادمین سیستم نیز نتواند آن را متوجه شود.

[1] end to end (E2E) [2] verifiability [3] individual verification [4] universal verification [5] end to end verification [6] Anonymity

- ناشناس بودن: هویت رأی‌دهنده با رأی او ارتباطی ندارد و اطلاعات شخصی یا هویت باید پنهان بماند.
- محرمانه بودن: حصول اطمینان از اینکه هیچ کس درگیر در فرآیند رأی‌گیری نمی‌تواند یک رأی خاص را به یک رأی‌دهنده خاص مرتبط کند. علاوه بر این، محتوای رأی آنها محرمانه باقی می‌ماند.

تمرکززدایی: تمرکززدایی به معنی توزیع اختیارات، مسئولیت و عملیات سیستم رأی‌گیری در یک شبکه در مقایسه با یک نهاد مرکزی اشاره دارد. این ویژگی برای افزایش اعتماد شهروندان با به حداقل رساندن کنترل یک شخص یا گروه ثالث بسیار اهمیت دارد.

یکپارچگی سیستم[1]**:** سیستم رأی‌گیری اکترونیکی امن، در برابر خرابی‌ها یا آسیب‌پذیری‌های امنیتی مقاومت دارد و عملکرد خود را با جلوگیری از پیکربندی مجدد در حین کار و استفاده از سطوح مختلف کنترل حفظ می‌کند.

قابلیت اطمینان[2]**:** اطمینان از عملکرد سیستم بدون از دست دادن هیچ رأیی، حتی در صورت وجود خرابی‌های متعدد، از جمله موارد مربوط سرورهای رأی‌گیری و ارتباطات شبکه.

گزارش‌دهی و تحلیل نتایج: ارائه گزارش‌های تحلیلی و بصری از نتایج انتخابات و نظرسنجی‌ها، به همراه امکان مشاهده روند رأی‌گیری به صورت زنده.

مدیریت و تنظیمات انتخابات: قابلیت تنظیم و مدیریت جزئیات انتخابات، از جمله زمان‌بندی، موضوعات رأی‌گیری و فهرست رأی‌دهندگان.

مقرون به صرفه بودن: این سیستم دررقابت با روش‌های رأی‌گیری سنتی اساساً مقرون به صرفه و قابل استفاده مجدد با هزینه‌های اجرا و نگهداری معقول است.

نوآوری اصلی این پروژه این است که با بکارگیری ویژگی‌های متمایز فناوری بلاک‌چین[3] مانند تمرکززدایی، امنیت، تغییرناپذیری و شفافیت، می‌تواند به ضعف‌ها و محدودیت‌های مربوط به سیستم‌های رأی‌گیری سنتی غلبه کند. این امر در نهایت منجر به افزایش اعتماد مردم به رویه‌های دموکراتیک خواهد شد.

۲ جامعه هدف

جامعه هدف این سیستم رأی‌گیری الکترونیک امن، طیف وسیعی از کاربران، نهادها و سازمان‌های دولتی و مردم‌نهاد هستند که مسئول برگزاری انتخابات و نظرسنجی‌های ملی و محلی هستند و می‌خواهند با فرآیندی دموکراتیک نظرات مردم و یا کارمندان خود را در مورد موضوعی خاص بدانند. همچنین سازمان‌هایی که می‌خواهند اعضای

[1] System integrity [2] Reliability [3] Blockchain

اصلی خود را با انتخابات تعیین کنند می‌توانند از این سیستم استفاده کنند. با استفاده از این سیستم می‌توان حتی بسیاری از چالش‌های موجود در کشور را نیز به صورت کاملاً امن به رأی مردم گذاشت و نظرات آنها را در این موارد جویا شد. استفاده از این سیستم باعث اعتماد بیشتر مردم خواهد شد.

علاوه بر این، سازمان‌های غیردولتی و خصوصی نیز می‌توانند از این سیستم برای برگزاری نظرسنجی‌های داخلی یا رأی‌گیری‌های مربوط به تصمیم‌گیری‌های گروهی استفاده کنند. این سیستم امکان تنظیم و مدیریت انتخابات را به راحتی فراهم می‌کند و قابلیت‌هایی نظیر گزارش‌دهی زنده و تحلیل نتایج را در اختیار کاربران قرار می‌دهد.

این سامانه می‌تواند برای نهادهای کوچکتر مانند شهرداری‌ها یا شوراهای شهر به کار گرفته شود و همچنین قادر است انتخابات بزرگ و گسترده‌تری، مانند انتخابات عمومی که شامل تمام افراد جامعه است، را مدیریت کند. با انعطاف‌پذیری و کارایی بالا، این سامانه می‌تواند در مقیاس‌های مختلف از رأی‌گیری‌های محلی تا ملی به طور مؤثر عمل کند.

به عنوان نمونه تمامی انجمن‌های علمی و شرکت‌های بورسی و ... می‌توانند اعضای اصلی خود را بر این اساس انتخاب کنند. همچنین سازمان‌هایی مثل مرکز آمار، روزنامه‌ها و ... می‌توانند درباره موضوعات مهم نظرسنجی بین طیف‌های مختلف مردم برگزار کنند. حتی دولت می‌تواند در برخی از موارد نظرات مردم را در مورد تصمیمات خود جویا شود. در صورت موفقیت این پروژه و جذب سرمایه، حتی می‌توان از این سیستم در انتخابات‌های مهم کشوری مثل انتخابات شورا، مجلس، دولت و ... نیز استفاده کرد. این پروژه در صورت پیاده‌سازی و موفقیت در تست‌های امنیتی و همچنین بعد از ارائه مناسب، به علت اهمیت و ضرورت آن در دموکراسی و نظرسنجی می‌تواند پتانسیل زیادی برای سوددهی داشته باشد و هدف مناسبی برای سرمایه‌گذاری خواهد بود. همچنین جدای از جنبه اقتصادی، این پروژه می‌تواند بستر مناسبی برای تحقیقات در زمینه رأی‌گیری الکترونیکی امن و حفاظت از حریم خصوصی رأی‌دهندگان باشد.

۳ میزان تأثیر پروژه

در این پروژه، با رویکردی نوآورانه و توجه ویژه به مباحث امنیت، دقت، و شفافیت، قادر است تحولی عمیق در فرآیندهای رأی‌گیری الکترونیکی ایجاد کند و این فرآیند را به خوبی تسریع و آسان کند. سیستم با بهره‌گیری از روش‌های احراز هویت چندعاملی از امنیت اطلاعات و صحت رأی کاربران اطمینان حاصل می‌کند. علاوه بر این، استفاده از رمزنگاری داده‌ها در این سیستم، از هرگونه دسترسی غیرمجاز به داده‌های حساس و خصوصی جلوگیری می‌کند. این ویژگی نه تنها برای رأی‌دهندگان اطمینان‌بخش است، بلکه به ارتقای سطح امنیت و سلامت در انتخابات کمک می‌کند. شفافیت و امکان حسابرسی نیز در این سیستم به شکل دقیق و کاملی فراهم شده است، به نحوی که تمامی مراحل رأی‌گیری ثبت و ذخیره می‌شوند و امکان بررسی و تأیید توسط ناظران مستقل فراهم می‌شود. قابلیت رأی‌گیری ناشناس نیز بخش مهم دیگری از این پروژه است. با تضمین محرمانگی آرای ثبت‌شده،

رأی‌دهندگان از این جهت که رأی آن‌ها تحت هیچ شرایطی شناسایی نخواهد شد، احساس امنیت می‌کنند و با آزادی بیشتری در رأی‌گیری مشارکت خواهند کرد. چنین پروژه‌ای در عین حال که به امنیت و محرمانگی رأی‌دهندگان اهمیت می‌دهد، همچنین به افزایش اعتماد عمومی نسبت به فرآیندهای انتخاباتی کمک خواهد کرد.

این پروژه می‌تواند به شکل قابل توجهی کیفیت و سلامت فرآیندهای رأی‌گیری را ارتقا دهد و همچنین هزینه‌های مربوط به برگزاری انتخابات را کاهش دهد. به دلیل انعطاف‌پذیری بالا، این سامانه برای انواع مختلف رأی‌گیری، از انتخابات ملی گرفته تا نظرسنجی‌های داخلی و رأی‌گیری‌های گروهی، با ویژگی‌ها و نیازهای متنوع قابل استفاده است.

پروژه ارائه شده با توجه به جنبه‌های مختلف و ویژگی‌های ارائه شده در بخش ۱ می‌تواند تأثیرات زیادی در حیطه توسعه دموکراسی در جامعه و افزایش اعتماد مردم به سیستم داشته باشد. همچنین از لحاظ علمی می‌تواند تحقیقات بسیاری را در زمینه استفاده از سیستم‌های امن و غیرمتمرکز دیگر در مواردی مثل زنجیره‌های تأمین و توزیع کالا، بهداشت، و ... مطرح کند.

در صورت نیاز این سیستم می‌تواند منبع باز باشد تا عملکرد سیستم برای شهروندان شفاف باشد و متخصصان بتوانند نحوه عملکرد سیستم را درک و بررسی کنند.

۴ نحوه‌ی ارائه پروژه

برای آشنایی کاربران با این سیستم و جمع‌آوری بازخوردهای اولیه، پیشنهاد می‌شود پروژه در فاز آزمایشی (بتا) به صورت رایگان در اختیار دانشگاه‌ها و مؤسسات دولتی قرار گیرد. این امر نه تنها به توسعه‌دهندگان کمک می‌کند تا از بازخورد کاربران برای بهبود سیستم بهره ببرند، بلکه امکان بررسی عملکرد سیستم در محیط‌های واقعی را نیز فراهم می‌سازد. همچنین با این کار می‌توان از امنیت نیز تا حدودی اطمینان پیدا کرد.

در مرحله بعدی، با استفاده از تبلیغات هدفمند و همکاری با رسانه‌های معتبر و شناخته‌شده، می‌توان این پروژه را به مخاطبان گسترده‌تری معرفی کرد. همکاری با دانشگاه‌ها، مؤسسات تحقیقاتی، و نهادهای نظارتی می‌تواند به اعتبار و اعتماد به این پروژه افزوده و آن را به یک ابزار استاندارد و معتبر در سطح ملی و بین‌المللی برای رأی‌گیری الکترونیکی و نظرسنجی تبدیل کند. علاوه بر این، این سامانه می‌تواند به طور اختصاصی در جلسات برای سازمان‌ها و شرکت‌های مختلف معرفی شود.

همچنین، امکان ارتقاء سیستم به کمک اشتراک‌های ویژه و سرویس‌های اضافی، می‌تواند در آینده به عنوان منبع درآمد و حفظ پایداری پروژه در نظر گرفته شود. از سوی دیگر، با ایجاد ارتباطات مؤثر با جامعه آکادمیک، این پروژه می‌تواند به عنوان یک پروژه تحقیقاتی شناخته شود که از منظر توسعه امنیت سایبری و رمزنگاری، می‌تواند به نفع جامعه علمی و محققان حوزه‌های مرتبط باشد.

۵ نحوه پیاده‌سازی

۱.۵ تحلیل نیازمندی‌ها

- جمع‌آوری نیازمندی‌ها: شناسایی نیازهای کاربران شامل امنیت، سهولت استفاده و قابلیت دسترسی و نیازمندی‌های دیگری که در بخش ۱ به آنها اشاره شد.
- بررسی الزامات قانونی: اطمینان از رعایت قوانین و مقررات مربوط به رأی‌گیری

۲.۵ طراحی معماری سیستم

- معماری کلاینت-سرور: سیستم شامل یک (یا چند) سرور مرکزی و کلاینت‌های مختلف (وب، موبایل)
- استفاده از بلاک‌چین: انتخاب پلتفرم بلاک‌چین مناسب برای ثبت رأی‌ها
- مدل دیتابیس: طراحی پایگاه داده برای ذخیره‌سازی اطلاعات کاربران و رأی‌ها (به صورت رمزنگاری شده)

۳.۵ توسعه نرم‌افزار

- پیاده‌سازی بلاک‌چین
  - قراردادهای هوشمند: توسعه قراردادهای هوشمند برای مدیریت فرآیند رأی‌گیری (ثبت رأی، تأیید رأی، و محاسبه نتایج)
  - سیستم رمزنگاری: استفاده از الگوریتم‌های رمزنگاری برای امنیت رأی‌ها و احراز هویت کاربران
- توسعه بک‌اند
  - فریم‌ورک‌های مناسب: انتخاب فریم‌ورک‌های سرور
  - طراحی API: APIهای RESTful برای ارتباط بین سرور و کلاینت
- توسعه فرانت‌اند
  - طراحی UX/UI: طراحی رابط کاربری کاربرپسند برای ثبت‌نام، ثبت رأی و مشاهده نتایج و ...
  - فریم‌ورک‌های فرانت‌اند

۴.۵ آزمایش و تست

- آزمایش امنیتی: انجام تست‌های نفوذ[1] برای شناسایی آسیب‌پذیری‌ها
- آزمایش کارایی: ارزیابی عملکرد سیستم تحت بارهای مختلف و اطمینان از پاسخ‌گویی در زمان واقعی
- آزمایش کاربری: انجام تست‌های کاربری برای جمع‌آوری بازخورد و بهبود رابط کاربری

۵.۵ انتشار نسخه بتا

- انتشار آزمایشی: ارائه نسخه بتا به گروهی از کاربران برای تست و جمع‌آوری بازخورد
- بهبود و رفع اشکالات: بر اساس بازخورد کاربران، رفع اشکالات و بهبود عملکرد سیستم

۶.۵ نظارت و بهبود مستمر

- نظارت بر عملکرد: پیگیری عملکرد سیستم و جمع‌آوری داده‌ها برای تحلیل‌های بعدی
- به‌روزرسانی‌های امنیتی: اجرای به‌روزرسانی‌های منظم برای حفظ امنیت و کارایی سیستم

۶ برنامه زمانی اجرای پروژه

برنامه زمانی (یا گانت) اجرای پروژه به صورت جدول زیر است.

فاز پروژه	فعالیت‌ها	زمان مورد نیاز
فاز اول	تحلیل نیازمندی‌ها و طراحی اولیه	۱ ماه
فاز دوم	طراحی معماری سیستم و توسعه بلاک‌چین	۱۵ ماه
فاز سوم	توسعه بک‌اند و فرانت‌اند	۲ ماه
فاز چهارم	آزمایش‌های امنیتی و کارایی	۱ ماه
فاز پنجم	انتشار نسخه بتا و جمع‌آوری بازخورد	۱ ماه
فاز ششم	بهبود و به‌روزرسانی مستمر	۱ ماه (مداوم)

۷ تیم توسعه‌دهنده، هزینه‌ها و منابع مورد نیاز

تیم توسعه‌دهنده این پروژه شامل چهار نفر با تقسیم وظایف زیر است:

[1] Penetration testing

- **محمدرضا ماجد**: توسعه‌دهنده قراردادهای هوشمند و متخصص بلاک‌چین
- **نگین دشتی**: توسعه‌دهنده بک‌اند و مهندس DevOps
- **سیدرضا موسوی**: توسعه‌دهنده فرانت‌اند و طراح UX/UI
- **محمدصالح ناصح**: مهندس امنیت و رمزنگاری

برای پیاده‌سازی سیستم رأی‌گیری الکترونیکی امن بر پایه بلاک‌چین، نیاز به منابع و زیرساخت‌های زیر است:

(۱) **پیاده‌سازی بلاکچین**: به دلیل نیازهای خاص این پروژه، یک بلاک‌چین سفارشی طراحی و پیاده‌سازی خواهد شد. این بلاکچین باید به گونه‌ای طراحی شود که امنیت، شفافیت، تغییرناپذیری، و مقیاس‌پذیری لازم برای سیستم رأی‌گیری را تضمین کند. توسعه این بلاک‌چین نیاز به برنامه‌ریزی دقیق برای معماری، الگوریتم‌های اجماع و توسعه قراردادهای هوشمند دارد.

(۲) **سرورهای پردازش و ذخیره‌سازی**: برای توسعه و آزمایش بلاک‌چین سفارشی و سیستم رأی‌گیری، نیاز به سرورهای پردازشی و ذخیره‌سازی با امنیت بالا داریم. هزینه تخمینی برای اجاره این سرورها در ابتدا ماهانه حدود ۳ میلیون تومان خواهد بود. با افزایش تعداد کاربران و حجم تراکنش‌ها، استفاده از سرورهای قوی‌تر و مطمئن‌تر ضرورت خواهد داشت.

(۳) **رمزنگاری و احراز هویت**: مهندس امنیت وظیفه‌ی طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری و پروتکل‌های احراز هویت چندعاملی را برعهده دارد. این بخش نیازمند هزینه‌های مربوط به کتابخانه‌های نرم‌افزاری و ابزارهای امنیتی است.

(۴) **نیازمندی‌های توسعه**: ابزارها و کتابخانه‌های توسعه نرم‌افزار شامل ابزارهای برنامه‌نویسی قراردادهای هوشمند، توسعه رابط کاربری، و توسعه APIهای RESTful برای ارتباط بین کلاینت و سرور.

در مجموع، تخمین می‌زنیم که هزینه‌های اولیه برای پیاده‌سازی بلاک‌چین سفارشی و اجاره زیرساخت‌های سرور ماهانه حدود ۵ میلیون تومان باشد. با افزایش کاربران و حجم تراکنش‌ها، این هزینه‌ها قابل افزایش خواهند بود.

۸ ریسک‌های احتمالی

در فرآیند توسعه سیستم رأی‌گیری الکترونیکی امن بر پایه بلاکچین، چندین ریسک احتمالی وجود دارد که باید به آن‌ها توجه شود:

(۱) خروج یکی از اعضای تیم توسعه: در صورت خروج یکی از اعضای تیم در طول پروژه، می‌توان با توزیع مجدد وظایف بین اعضای باقی‌مانده و همچنین برون‌سپاری برخی از تسک‌ها، از بروز اختلالات جدی در روند توسعه جلوگیری کرد. برای مثال، وظایف مربوط به توسعه بک‌اند یا امنیت می‌تواند به پیمانکاران متخصص واگذار شود.

(۲) مشکلات در پیاده‌سازی بلاک‌چین: با توجه به اینکه پیاده‌سازی بلاکچین پیچیدگی‌های زیادی دارد، احتمال بروز مشکلات فنی در مراحل مختلف توسعه وجود دارد. در چنین مواردی، می‌توان با کاهش پیچیدگی‌های اولیه و اجرای پروژه در مقیاس کوچک‌تر، مشکلات فنی را به مرور زمان حل کرد.

(۳) محدودیت‌های منابع و سرورها: در صورت مواجهه با محدودیت‌های سخت‌افزاری یا مشکلات در زیرساخت‌های سرور، ممکن است نیاز به افزایش هزینه‌ها برای ارتقاء منابع پردازشی و ذخیره‌سازی باشد. به‌منظور مدیریت این ریسک، باید از ابتدا برنامه‌ریزی دقیقی برای مقیاس‌پذیری سرورها و منابع انجام شود.

(۴) مشکلات در پیاده‌سازی الگوریتم‌های رمزنگاری و امنیتی: در صورت بروز مشکلات امنیتی یا ناکارآمدی برخی از الگوریتم‌های رمزنگاری، می‌توان به طور موقت از روش‌های جایگزین استفاده کرد و به مرور زمان با به‌روزرسانی‌های مستمر سیستم، الگوریتم‌های پیشرفته‌تر را پیاده‌سازی کرد.

(۵) عدم جمع‌آوری داده‌های کافی برای بهبود سیستم: اگر در مراحل اولیه داده‌های کافی برای ارزیابی عملکرد سیستم جمع‌آوری نشود، می‌توان نسخه اولیه سیستم را به‌طور محدود در اختیار گروهی از کاربران قرار داد تا با دریافت بازخوردهای آنان، داده‌های بیشتری برای بهبود و ارتقاء سیستم جمع‌آوری شود.

(۶) تأخیر در تکمیل پروژه: در صورت بروز تأخیر در توسعه برخی از بخش‌ها، می‌توان با افزایش تعداد نیروهای پشتیبان یا افزایش ساعت کاری تیم، این تأخیرات را جبران کرد.