# سیستم رأی‌گیری الکترونیکی امن

پروپوزال پروژه مهندسی نرم‌افزار

**گروه نرمینو**

محمدرضا ماجد، نگین دشتی، محمدصالح ناصح، و سیدرضا موسوی

مشاور: امیرارسلان یاوری

دانشکده مهندسی برق و کامپیوتر
دانشگاه صنعتی اصفهان

۲۱ مهر ۱۴۰۳

# فهرست


۱ معرفی پروژه

۲ جامعه هدف

۳ میزان تأثیر پروژه

۴ نحوه‌ی ارائه پروژه

۵ نحوه پیاده‌سازی

۶ برنامه زمانی اجرای پروژه

۷ تیم توسعه‌دهنده، هزینه‌ها و منابع مورد نیاز

۸ ریسک‌های احتمالی

قسمت ۱

# معرفی پروژه

# سیستم رأی‌گیری الکترونیکی امن

سیستم رأی‌گیری الکترونیکی امن، سیستمی برای انجام رأی‌گیری الکترونیکی آنلاین با تمرکز بر یکپارچگی، امنیت، دقت، شفافیت، قابل تأیید بودن (یا راستی‌آزمایی) و حفظ حریم خصوصی 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.

## برخی از ویژگی‌های مهم

- طراحی رابط کاربر پسند
- تضمین راستی‌آزمایی فردی رأی‌گیری
- تضمین اصالت رأی‌دهنده
- تضمین راستی‌آزمایی عمومی رأی‌گیری
- تضمین منحصربه‌فرد بودن رأی‌دهنده
- تضمین راستی‌آزمایی E2E رأی‌گیری
- تضمین واجد شرایط بودن رأی‌دهنده
- نظارت و حسابرسی شفاف
- رمزنگاری داده‌ها به صورت E2E
- تمرکززدایی

# برخی از ویژگی‌های مهم

- رأی‌گیری ناشناس
- محرمانه بودن رأی
- یکپارچگی سیستم
- قابلیت اطمینان
- گزارش‌دهی و تحلیل نتایج
- مدیریت و تنظیمات انتخابات
- مقرون به صرفه بودن
- مبتنی بر فناوری بلاک‌چین

قسمت ۲

# جامعه هدف

# جامعه هدف

کاربران، نهادها و سازمان‌های دولتی و مردم‌نهاد

سازمان‌هایی که می‌خواهند اعضای اصلی خود را با انتخابات تعیین کنند

نهادهای کوچکتر مانند شهرداری‌ها یا شوراهای شهر

رأی‌گیری‌های محلی تا ملی

انجمن‌های علمی و شرکت‌های بورسی و ...

مراکز نظرسنجی مثل مرکز آمار، روزنامه‌ها و ...

انتخابات شورا، مجلس، دولت و ...

قسمت ۳

# میزان تأثیر پروژه

# تأثیر پروژه

ایجاد تحولی عمیق در فرآیندهای رأی‌گیری الکترونیکی

ارتقای سطح امنیت و سلامت در انتخابات

اطمینان‌بخشی به رأی‌دهندگان

افزایش اعتماد عمومی نسبت به فرآیندهای انتخاباتی

کیفیت و سلامت فرآیندهای رأی‌گیری

قسمت ۴

# نحوه‌ی ارائه پروژه

## نحوه‌ی ارائه پروژه

پروژه در فاز آزمایشی (بتا) به صورت رایگان در اختیار دانشگاه‌ها و مؤسسات دولتی قرار گیرد

تبلیغات هدفمند و همکاری با رسانه‌های معتبر و شناخته‌شده

همکاری با دانشگاه‌ها، مؤسسات تحقیقاتی، و نهادهای نظارتی

ارائه اختصاصی برای سازمان‌ها و شرکت‌های مختلف

ارتقاء سیستم به کمک اشتراک‌های ویژه و سرویس‌های اضافی

ارتقاء سیستم به کمک اشتراک‌های ویژه و سرویس‌های اضافی

ایجاد ارتباطات مؤثر با جوامع آکادمیک

قسمت ۵

# نحوه پیاده‌سازی

# تحلیل نیازمندی‌ها

## جمع‌آوری نیازمندی‌ها

شناسایی نیازهای کاربران شامل امنیت، سهولت استفاده و قابلیت دسترسی و نیازمندی‌های دیگری که در مقدمات به آنها اشاره شد.

## بررسی الزامات قانونی

اطمینان از رعایت قوانین و مقررات مربوط به رأی‌گیری

# طراحی معماری سیستم

## معماری کلاینت ـ 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)

# 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

# آزمایش و تست

## آزمایش امنیتی

انجام تست‌های نفوذ (Penetration testing) 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

# 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

## 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

قسمت ۶

# برنامه زمانی اجرای پروژه

# برنامه زمانی اجرای پروژه

| 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) |

قسمت ۷

# تیم توسعه‌دهنده، هزینه‌ها و منابع مورد نیاز

## تیم توسعه‌دهنده

- **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

# منابع و زیرساخت‌ها

| | |
|---|---|
| پیاده‌سازی بلاکچین | رمزنگاری و احراز هویت |
| سرورهای پردازش و ذخیره‌سازی | نیازمندی‌های توسعه |

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.

قسمت ۸

# ریسک‌های احتمالی

# ریسک‌های احتمالی

خروج یکی از اعضای تیم توسعه

مشکلات در پیاده‌سازی بلاک‌چین

محدودیت‌های منابع و سرورها

مشکلات در پیاده‌سازی الگوریتم‌های رمزنگاری

عدم جمع‌آوری داده‌های کافی برای بهبود سیستم

تأخیر در تکمیل پروژه

# پایان