دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

بررسی کارایی و امنیت بلاک‌چین در قراردادهای هوشمند

گزارش سمینار کارشناسی ارشد مهندسی کامپیوتر
گرایش نرم‌افزار

نگارش

شروین حاجی‌اسمعیلی

استاد راهنما

دکتر مقصود عباس‌پور

تابستان ۹۷

دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

گزارش سمینار کارشناسی ارشد مهندسی کامپیوتر - گرایش نرم‌افزار

تحت عنوان:

بررسی کارایی و امنیت بلاک‌چین در قراردادهای هوشمند

در تاریخ پایان‌نامه دانشجو، ، توسط کمیته تخصصی داوران مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنما اول:	نام و نام خانوادگی	امضا
۲- استاد راهنما دوم:	نام و نام خانوادگی	امضا (در صورت نیاز)
۳- استاد مشاور:	نام و نام خانوادگی	امضا (در صورت نیاز)
۴- استاد داور (داخلی):	نام و نام خانوادگی	امضا
۵- استاد داور (خارجی):	نام و نام خانوادگی	امضا
۶- نماینده تحصیلات تکمیلی:	نام و نام خانوادگی	امضا

با سپاس و قدردانی از

پدران و مادرانی که خود را فدای تربیت فرزاندان 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 حاجی‌اسمعیلی

عنوان پایان‌نامه: بررسی کارایی و امنیت بلاک‌چین در قراردادهای هوشمند

استاد راهنما: دکتر مقصود عباس‌پور

اینجانب شروین حاجی‌اسمعیلی تهیه‌کننده گزارش سمینار 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 حاجی‌اسمعیلی

تاریخ و امضا:

تقدیم به

رهجویان علم و فناوری و دوست‌داران علم و دانش

آوردن این صفحه اختیاریست.

فهرست مطالب

۱ مقدمه **۱**

۲ تعریف مفاهیم **۵**

۳ معرفی قابلیت‌های قالب **۹**

۱.۳ نگارش ۱۰

۲.۳ بخش‌بندی ۱۱

۱.۲.۳ یک زیر بخش ۱۱

زیر بخشی در زیر بخش ۱۱

دومین زیربخش در زیربخش ۱۲

۲.۲.۳ زیر بخشی دیگر ۱۲

۳.۳ ارجاعات ۱۳

۴.۳ نمایه‌ها ۱۳

۱.۴.۳ فرمول‌نویسی ۱۳

۲.۴.۳ تصاویر ۱۴

۳.۴.۳ جداول ۱۶

مراجع **۱۷**

فهرست تصاویر

۱.۳ یک نمونه تصویر ۱۵

فهرست جداول

۱.۳ نمونه‌ای جدول ۱۶

چکیده

لورم ایپسوم (به انگلیسی lorem ipsum) متنی بی مفهوم است که تشکیل شده از کلمات معنی دار یا بی معنی کنار هم. کاربر با دیدن متن لورم ایپسوم تصور میکند متنی که در صفحه مشاهده میکند این متن واقعی و مربوط به توضیحات صفحه مورد نظر است واقعی است. حالا سوال اینجاست که این متن « لورم ایپسوم » به چه دردی میخورد و اساسا برای چه منظور و هدفی ساخته شده است؟ پیش از بوجود آمدن لورم ایپسوم ، طراحان وب سایت در پروژه های وب سایت و طراحان کرافیک در پروژه های طراحی کاتولوگ ، بروشور ، پوستر و ... همواره با این مشکل مواجه بودند که صفحات پروژه خود را پیش از آنکه متن اصلی توسط کارفرما ارائه گردد و در صفحه مورد نظر قرار گیرد چگونه پر کنند؟؟ اکثر طراحان با نوشتن یک جمله مانند «این یک متن نمونه است» ویا «توضیحات در این بخش قرار خواهند گرفت» و کپی آن به تعداد زیاد یک یا چند پاراگراف متن میساختند که تمامی متن ها و کلمات ، جملات و پاراگراف ها تکراری بود و از این رو منظره خوبی برای بیننده نداشت و ضمنا به هیچ وجه واقعی به نظر نمیرسید تا بتواند شکل و شمایل تمام شده پروژه را نشان دهد. از این رو متنی ساخته شد که با دو کلمه (به فارسی : لورم ایپسوم) آغاز میشد وبا همین نام در بین طراحان وب و گرافیک شناخته و به سرعت محبوب شد. وب سایت های سازنده لورم ایپسوم میتوانند هر تعداد کلمه و پاراگراف که بخواهید به صوورت تکراری یا غیر تکراری برایتان بسازند و تحویلتان بدهند تا از آنها در پروژه هایتان استفاده کنید. (لورم ایپسوم فارسی) متن های لورم ایپسوم را به زبان فارسی و علاوه بر زبان فارسی به انگلیسی ، عربی ، ترکی استانبولی و ... برایتان میسازد. زبان های دیگر نیز رفته رفته به بانک اطلاعاتی لورم ایسپوم فارسی اضافه خواهند شد.

واژگان کلیدی: بلاک‌جین، اتریوم، امنیت، رای‌گیری

فصل ۱

مقدمه

با معرفی بیت‌کوین به عنوان یک ارز دیجیتال بدون پشتوانه و ارزش ذاتی در سال ۲۰۰۸ و فراگیر شدن استفاده‌ی از این بستر برای تراکنش‌های مالی مطالعات بسیاری در مورد دلیل موفقیت آن شد. اما با گذشت زمان توجه‌ها بیشتر به تکنولوژی مورد استفاده‌ی این ارز دیجیتال و به طور خاص بلاک‌چین جلب شد. از استفاده‌های دربلاک‌چین بیت کوین برای تولید ابزارهای مالی جدید می‌توان به سکه‌های رنگی به عنوان ارزهای جدید و Namecoin برای بستر خرید و فروش دامنه‌ی وب‌سایت اشاره کرد.

استفاده از بلاک‌چین به عنوان یک لیست تغییرناپذیر به کمک اثبات کار یک راه‌حل توزیع‌شده برای مسئله‌ی ژنرال‌های بیزنتین را ایجاد کرد که خود باعث تولید ارزهای جدید به روی بسترهای مستقل شده و برای کاربردهای جدید شد. یکی از بلندپروازانه‌ترین ایده‌هایی که تا به امروز دیده شده اتریوم است. تراکنش‌های بیت‌کوین توانایی ثبت اسکرپت‌هایی که قواعدی برای تراکنش ثبت کنند را دارند ولی تعدادی از خصوصیت‌های معمول زبان‌های برنامه‌نویسی turing-complete مانند حلقه را پشتیبانی نمی‌کنند. هدف از ساخت اتریوم ساخت یک زبان برنامه نویسی turing-complete برای این بستر است.

فلسفه‌ی ساخت پروتکل اتریوم رو می‌توان در این ۵ پایه خلاصه کرد:

- سادگی: پروتکل باید برای برنامه‌نویسان ساده و دردسترس باشد حتی به قیمت از کم شدن بهره‌وری کل سیستم.
- کامل بودن: اتریوم باید یک زبان turing-complete داشته باشد و هر مدل ریاضی را بتوان با آن پیاده کرد.
- بخش‌پذیری: قسمت‌های اتریوم باید از هم جدا باشند و توانایی عوض کردن الگوریتم‌های و ساختارداده‌های سیستم مانند درخت پاتریشا وجود داشته باشد، بدون این که قسمت‌های دیگر سیستم از این تغییر باخبر شوند
- چابکی: جزییات پروتکل اتریوم باید قابل تغییر باشند.
- برابری: سیستم نباید فعلانه جلوی یک دسته از کاربردها رو بگیرد یا آن‌ها رو محدود کند.

با بوجود آمدن اتریوم به عنوان یک بستر کامل، بی‌اعتماد و توزیع‌شده برای قراردادهای هوشمند کاربردهای اشاره شده در بالا را می‌توانن به سادگی با نوشتن چند خط کد پیاده کرد. این سادگی در پیاده‌سازی باعث جذب

بسیاری از توسعه‌دهندگان می‌شود که می‌توانند کاربردهای جدیدی پیاده کنند که به عنوان یک کارپرداز خودکار در این بستر فعالیت کنند. تغییرناپذیری قراردادهایی که در بستر بلاک‌چین نوشته می‌شوند باعث اعتماد مشتریان آن‌ها به آن قرارداد می‌شود ولی این تغییرناپذیری به معنی این است که اگر قرارداد «اشتباهی» در این بستر نوشته شود راهی برای تصحیح آن نیست. برای مثال در سال ۲۰۱۶ به اندازه‌ی ۵۰ میلیون دلار اتر از یک سازمان کرودفاندینگ در اثر یک باگ امنیتی از بک قرارداد آن‌ها دزدیده شد. با توجه به تغییر ناپذیر بودن بلاک‌چین هیچ راهی جز تغییر پروتکل برای بازگرداندن پول وجود نداشت و در نهایت با یک انشعاب سخت از این بستر پول به آن مجموعه بازگردانده شد. این تصمیم برای تغییر سیستم باعث شد کاربران اتریوم به دو دسته تقسیم شوند، دسته‌ی اول کسانی که از بازگردانده شدن پول به سازمان حمایت می‌کردند و بلاک‌چین جدید رو به عنوان بلاک‌چین اصلی اتریوم قبول کردند و دسته‌ی دوم که با این استدلال که قانون اتریوم کد قراردادهاست و چون قرارداد به درستی اجرا شده باید آن مبلغ به هکرها تعلق بگیرد، بلاک‌چین جدید را قبول نکرده و بلاک‌چین قبلی را ادامه دادند. از نمونه‌های دیگر این مسئله می‌توان به قفل شدن ۳۰۰ میلیون دلار اتر متعلق به شرکت parity در نوابر ۲۰۱۷ اشاره کرد.

لازم به ذکر است که هیچ کدام از مشکلات امنیتی نام برده شده مشکل خود بستر اتریوم نبوده و مسئله استفاده‌ی اشتباه از زبان برنامه‌نویسی آن و قابلیت‌های آن‌ها بوده است. با این وجود توجه به مسائل امنیتی در این بستر ناآشنا و جدید با توجه به طرز فکر متفاوت از برنامه‌نویسی عادی بسیار مهم است.

در ادامه‌ی این تحقیق به بررسی دقیق‌تر بعضی از این مشکلات امنیتی خواهیم پرداخت.

یک سوال مهم در زمینه‌ی قراردادهای هوشمند اتریوم کاربردهای ممکن و یا مناسب این بستر است. از کاربرداهای معروف این بستر به کاربردهای زیر می‌توان اشاره کرد:

- ارزهای جدید
- سیستم‌های هویت
- فایل‌سیستم‌های توزیعشده
- سازمان‌های خودکار توزیع‌شده

در ادامه‌ی این تحقیق ابتدا به تعریف مفاهیم پرکاربرد آن می‌پردازیم و در ادامه ...

فصل ۲

تعریف مفاهیم

در این بخش تعریف مفاهیم مورد استفاده در این تحقیق می‌پردازیم.

- **بلاک‌چین:** بلاک‌چین یک ساختارداده متشکل از بلوک‌های پشت‌سرهم که هر بلوک شامل هشی از خودش بلوک قبلی هم هست. در نتیجه به تغییر یک بلوک باید تمام بلوک‌های بعد از آن را تغییر داد تا ساختار درست باشد.

- **اثبات کار:** روش اثبات کار بر اساس hashcash که یک روش برای جلوگیری از حملات DDoS طراحی شده بود ساخته شده است. روش کار hashcash به شکل زیر است:

برای این که یک ایمیل توسط سرور ارسال شود همراه متن ایمیل کلاینت باید که رشته‌ای ارسال کند که اگر هش SHA-1 آن از آن گرفته شود ۲۰ بیت اول آن صفر خواهند بود. به دلیلی تصادفی بودن هش رشته باید با امتحان کردن رشته‌های مختلف به یک رشته‌ی مناسب برسد. زمان حل این مسئله برای کامپوترهای 1 GHZ آن زمان حدود یک ثانیه بود و زمان بررسی درست بودن آن هش تنها ۲ میکروثانیه است.

برای یک کاربر عادی که قصد ارسال یک ایمیل را دارد زمان یک ثانیه‌ای قابل‌قبول است اما اگر یک مهاجم قصد spam کردن توسط این سرویس را داشته باشد زمان یک ثانیه برای هر ایمیل هزینه‌ی بسیار بالایی خواهد بود.

در بستر بیت‌کوین از این روش برای توافق بر بلوک‌های بعدی بلاک‌چین به صورت زیر استفاده می‌شود: هر بلوک جدید حاوی تعدادی تراکنش برای ثبت در بلاک‌چین توسط ماینترها به یک بلوک تبدیل می‌شود. ولی برای این که این بلوک توسط بقیه پذیرفته شود باید در این بلاک یک nounce قراردهند به صورتی که هش بلاک از یک عددی که توسط پروتکل بیت‌کوین انتخاب می‌شود کمتر باشد. این شرط در طول زمان به صورت خودکار به روزرسانی می‌شود به طوری که در هر لحظه به صورت میانگین اضافه کردن بلاک ۱۰ دقیقه از کل شبکه زمان ببرد. از آنجایی که تنها راه پیدا کردن همچین رشته‌ای بروت‌فورس است، توان محاسباتی بالاتر باعث شانس بیشتر برای پیدا کردن بلاک بعدی خواهد شد.

- **مسئله‌ی جنرال‌های بیزنتین**

مسئله‌ی جنرال‌های بیزنتین یا تحمل خطای بیزنتین مدلی از تحمل خطا در سیستم‌های توزیع شده است. در این مسئله تعدادی جنرال یک ارتش با هم به صورت پیام‌های یک به یک صحبت می‌کنند و در ساده‌ترین

حالت در مورد حمله کردن یا عقب‌نشینی در یک نبرد تصمیم می‌گیرند. ولی تعدادی از این جنرال‌ها خائن بوده و تلاش می‌کنند که جمع به توافق غلطی برسد (توافق درست توافقی است که اگر هیچ خائنی وجود نداشت به آن می‌رسیدند) و یا با جواب ندادن مانع تصمیم‌گیری آن‌ها شوند. در ساده‌ترین حالت و بدون استفاده از امضاهای دیجیتال ثابت می‌شود که برای $3k + 1$ جنرال، با رای‌گیری می‌توان تا k خائن را تحمل کرد. راه‌حل خلاقانه‌ی بیت‌کوین برای حل این مسئله استفاده از بلاک‌چین برای ذخیره‌ی اطلاعات و استفاده از اثبات کار برای اضافه کردن بلوک به بلاک‌چین است.

برای نشان دادن نحوه‌ی حل این مسئله یک مثال را بررسی می‌کنیم. فرض می‌کنیم شخص A یک بیت‌کوین را به B منتقل کرده و این تراکنش در بلاک‌چین ثبت شده و در ازای آن کالایی دریافت کرده، حال قصد دارد که این تراکنش رو از بلاک‌چین بیت‌کوین حذف کند تا بتواند آن را ۲ بار خرج کند. از آنجایی که نودهای شبکه‌ی بیت‌ککوین اگر ۲ زنجیره از بلوک‌ها دریافت کنند زنجیره‌ی بلندتر را قبول خواهند کرد باید ۲ بلوک سالم بسازد قبل از این که کل شبکه یک بلوک به شبکه اضافه کنند.

احتمال موفقت حمله‌ی A مساوی $(\frac{A's\ computational\ power}{Bitcoin\ network's\ computational\ power})^2$ است. اگر توان محاسباتی A از بقیه‌ی شبکه کمتر باشد این کسر یک عدد کوچک‌تر از ۵.۰ است. اگر در این کار به موقع موفق نشود سه بلاک عقب می‌افتد و توان فرمول بالا تبدیل به سه می‌شود و احتمال موفقیتش کمتر از پیش نیز می‌شود. این مسئله مسئله‌ی قمارباز نام دارد که نشان داده می‌شود در آن در طول زمان احتمال موفقت مهاجم به صورت نمایی کاهش پیدا می‌کند.

- **انشعاب:** منظور از انشعاب در ارزهای دیجیتال تبدیل یک بلاک‌چین به دو بلاک‌چین است، گاها برای ساخت ارزهای جدید از بلاک‌چین موجود یک ارز دیگر مثل بیت‌کوین استفاده می‌شود، این کار باعث می‌شود که شروع بلاک‌چین آسان‌تر و امن‌تر شود. در روال عادی کار بیت‌کوین نیز ممکن است انشعابی رخ دهد اما هر ماینری که متوجه انشعابی شود به صورت خودکار بلندترین زنجیره را به عنوان زنجیره‌ی درست انتخاب می‌کند. در صورتی که یک انشعاب برای تولید بلاک‌چین جدید انجام گیرد و بلوک‌هایی قبلی که در آن وجود داشتند همچنان درست حساب شوند این انشعاب را انشعاب نرم و اگر بلوک‌های قبلی مورد قبول سیستم جدید نباشند انشعاب را انشعاب سخت می‌نامیم.

- **ماین‌کردن:** به عملیات پیدا ساختن بلوک‌های جدید روی بلاک‌چین به هدف پیدا کردن بلاک‌های درست و دریافت جایزه‌ی آن‌ها ماین‌کردن می‌گوییم.

- **ماینینگ پول:** از آن جایی که ماین کردن برای یک نفر با توجه به احتمال پایین این که بتوانند بلاک معتبر را زودتر از بقیه‌ی شبکه پیدا کنند بسیار پایین است، ماینینگ‌پول‌ها شکل گرفته‌اند. با تقسیم کردن کار بین چندین ماشین شانس پیدا کردن بلوک معتبر بیشتر می‌شود و جایزه‌ی ماین کردن به نسبت توان محاسباتی بین شرکت‌کنندگان تقسیم می‌شود. برای بدست آوردن توان محاسباتی که هر ماشین برای این کار مصرف کرده از تعداد بلوک‌هایی که هش آن‌ها به اندازه‌ی کافی برای درست بودن کوچک نیست ولی به جواب درست نزدیکند استفاده می‌شود.

- **قرارداد هوشمند** لفظ قراردادهای هوشمند اولین بار در سال ۱۹۹۳ توسط N.Szabo به عنوان یک پروتکل تراکنش کامپیوتری که شروط یک قرارداد را اجرا می‌کند. در اولین مثال معروف قراردادهای هوشمند یک وندینگ ماشین را مثال زد که در ازای سکه‌ی به طور اتوماتیک کالای مورد نظر را به مشتری می‌دهد، همینطور از آنجایی که بدون پول دادن هرگز کالایی نمی‌دهد و امنیت سکه‌ها را از طریق صندوق خود تا حد معقولی تامین می‌کند قرارداد مناسبی بین مشتری و تولیدکننده‌ی کالا محسوب می‌شود. هدف نهایی قراردادهای هوشمند کاهش نیاز به اعتماد کردن و افراد میانی در یک قرارداد است و با بوجود آمدن بسترهای ارز دیجیتال و راه‌حل‌های جدید مسئله‌ی جنرال‌های بیزنتین بستر مناسبی برای ساخت قراردادهای هوشمند و توزیع‌شده بدون نیاز به اعتماد به شخص ثالث بوجود آمده است. با وجودی که به کمک زبان اسکریپتینگ بیت‌کوین می‌توان مدل‌های مختلفی از قراردادهای هوشمند را تولید کرد، با اتریوم به به کمک زبان برنامه‌نویسی turing-complete آن در تئوری می‌توان هر قرارداد هوشمند ممکن را تولید کرد.

فصل ۳

معرفی قابلیت‌های قالب

در این بخش با آوردن یک متن ساده به نمایش ظاهر و ساختار قالب و همچنین معرفی برخی دستورات لازم برای کار با آن قالب پرداخته می‌شود. این توضیحات بسیار مختصر بوده و صرفاً برای معرفی قالب می‌باشد و چنانچه با LaTeX آشنایی ندارید، بهتر است پیش از آغاز تدوین پایان‌نامه مختصری در مورد نحوه کار با LaTeX مطالعه بفرمایید.

۱.۳ نگارش

رعایت تمامی اصول نگارش در هنگام تدوین پایان‌نامه الزامیست، بسیاری از نکات نگارشی توسط قالب رعایت می‌شوند. در ادامه این بخش به معرفی برخی دستورات کاربردی برای این کار پرداخته می‌شود.

به طور پیش‌فرض هر پاراگراف به صورت خودکار با فاصله از کنار آغاز می‌شود. چنانچه در حالت خاصی، نیاز به حذف این فاصله باشد می‌توانید از دستور

```
\noindent
```

استفاده کنید.

برای نوشتن متون انگلیسی لازم است آن‌ها را داخل تگ \lr{} قرار دهید. به عنوان مثال با نوشتن \lr{word} کلمه word به درستی داخل متن قرار می‌گیرد.

با نوشتن \\می‌توانید خط جدیدی را آغاز کنید و نوشتن \par نیز باعث ایجاد یک پاراگراف جدید خواهد شد. با قرار دادن متن در داخل تگ \textbf{} متن به صورت **ضخیم** و با قرار دادن نوشته در داخل تگ \textit{} نوشته کج خواهد شد. امکان استفاده هم‌زمان از این تگ‌ها نیز وجود دارد. برای آشنایی بیشتر با دستورات، پیشنهاد می‌شود به آموزش‌های LaTeX مراجعه کنید.

پانوشت‌ها یکی از بخش‌های اصلی در هر نوشته‌ای می‌باشد. در این قالب شماره‌های پانوشت در هر صفحه، مجدداً از ۱ آغاز می‌شود. با نوشتن

```
\LTRfootnote{footnote}
```

می‌توان یک پانوشت لاتین[1] اضافه نمود.

[1] footnote

برای افزودن پانوشت‌های فارسی[۱] نیز از دستور زیر استفاده می‌شود.

\RTLfootnote{پانوشت}

نمونه‌های افزودن پانوشت نیز در همین قسمت وجود دارد.

۲.۳ بخش‌بندی

برای ساخت یک فصل جدید کافیست از دستور

\cchapter{عنوان}

استفاده شود. با نوشتن این دستور به صورت خودکار یک فصل جدید اضافه شده و عنوان آن در یک صفحه مجزا قرار می‌گیرد. هر بخش می‌تواند شامل تعدادی Section باشد. شماره‌های آن مانند آنچه در بالا نیز مشاهده می‌کنید با . از یک‌دیگر جدا شده و به صورت خودکار شماره‌گزاری شده و به فهرست اضافه می‌شوند. کافیست برای ساخت بخش دستور

\section{عنوان}

را وارد کنید. همچنین با دستورات زیر می‌توانید زیربخش و حتی زیر زیر بخش، ایجاد کنید.

\subsection{عنوان}

\subsubsection{عنوان}

به عنوان مثال بخش زیر را در نظر بگیرید : (متون این زیربخش‌ها بی‌معنا و برای پر کردن صفحه می‌باشد.)

۱.۲.۳ یک زیر بخش

اگر زیر بخش‌ها به سطح سوم برسند شماره‌گذاری نمی‌شوند ولی در فهرست مطالب قرار می‌گیرند، به عنوان مثال:

زیر بخشی در زیر بخش

متن

[۱] یک پانوشت فارسی

دومین زیربخش در زیربخش

متنی دیگر

۲.۲.۳ زیر بخشی دیگر

لورم ایپسوم (به انگلیسی lorem ipsum) متنی بی مفهوم است که تشکیل شده از کلمات معنی دار یا بی معنی کنار هم. کاربر با دیدن متن لورم ایپسوم تصور میکند متنی که در صفحه مشاهده میکند این متن واقعی و مربوط به توضیحات صفحه مورد نظر است واقعی است. حالا سوال اینجاست که این متن « لورم ایپسوم » به چه دردی میخورد و اساسا برای چه منظور و هدفی ساخته شده است؟ پیش از بوجود آمدن لورم ایپسوم ، طراحان وب سایت در پروژه های وب سایت و طراحان کرافیک در پروژه های طراحی کاتولوگ ، بروشور ، پوستر و ... همواره با این مشکل مواجه بودند که صفحات پروژه خود را پیش از آنکه متن اصلی توسط کارفرما ارائه گردد و در صفحه مورد نظر قرار گیرد چگونه پر کنند؟؟ اکثر طراحان با نوشتن یک جمله مانند «این یک متن نمونه است» ویا «توضیحات در این بخش قرار خواهند گرفت» و کپی آن به تعداد زیاد یک یا چند پاراگراف متن میساختند که تمامی متن ها و کلمات ، جملات و پاراگراف ها تکراری بود و از این رو منظره خوبی برای بیننده نداشت و ضمنا به هیچ وجه واقعی به نظر نمیرسید تا بتواند شکل و شمایل تمام شده پروژه را نشان دهد. از این رو متنی ساخته شد که با دو کلمه (به فارسی : لورم ایپسوم) آغاز میشد وبا همین نام در بین طراحان وب و گرافیک شناخته و به سرعت محبوب شد. وب سایت های سازنده لورم ایپسوم میتوانند هر تعداد کلمه و پاراگراف که بخواهید به صوورت تکراری یا غیر تکراری برایتان بسازند و تحویلتان بدهند تا از آنها در پروژه هایتان استفاده کنید. (لورم ایپسوم فارسی) متن های لورم ایپسوم را به زبان فارسی و علاوه بر زبان فارسی به انگلیسی ، عربی ، ترکی استانبولی و ... برایتان میسازد. زبان های دیگر نیز رفته رفته به بانک اطلاعاتی لورم ایسپوم فارسی اضافه خواهند شد. لورم ایپسوم (به انگلیسی lorem ipsum) متنی بی مفهوم است که تشکیل شده از کلمات معنی دار یا بی معنی کنار هم. کاربر با دیدن متن لورم ایپسوم تصور میکند متنی که در صفحه مشاهده میکند این متن واقعی و مربوط به توضیحات صفحه مورد نظر است واقعی است. حالا سوال اینجاست که این متن « لورم ایپسوم » به چه دردی میخورد و اساسا برای چه منظور و هدفی ساخته شده است؟ پیش از بوجود آمدن لورم ایپسوم ، طراحان وب سایت در پروژه های وب

سایت و طراحان کرافیک در پروژه های طراحی کاتولوگ ، بروشور ، پوستر و ... همواره با این مشکل مواجه بودند که صفحات پروژه خود را پیش از آنکه متن اصلی توسط کارفرما ارائه گردد و در صفحه مورد نظر قرار گیرد چگونه پر کنند؟؟ اکثر طراحان با نوشتن یک جمله مانند «این یک متن نمونه است» ویا «توضیحات در این بخش قرار خواهند گرفت» و کپی آن به تعداد زیاد یک یا چند پاراگراف متن میساختند که تمامی متن ها و کلمات ، جملات و پاراگراف ها تکراری بود و از این رو منظره خوبی برای بیننده نداشت و ضمنا به هیچ وجه واقعی به نظر نمیرسید تا بتواند شکل و شمایل تمام شده پروژه را نشان دهد. از این رو متنی ساخته شد که با دو کلمه (به فارسی : لورم ایپسوم) آغاز میشد وبا همین نام در بین طراحان وب و گرافیک شناخته و به سرعت محبوب شد. وب سایت های سازنده لورم ایپسوم میتوانند هر تعداد کلمه و پاراگراف که بخواهید به صوورت تکراری یا غیر تکراری برایتان بسازند و تحویلتان بدهند تا از آنها در پروژه هایتان استفاده کنید. (لورم ایپسوم فارسی) متن های لورم ایپسوم را به زبان فارسی و علاوه بر زبان فارسی به انگلیسی ، عربی ، ترکی استانبولی و ... برایتان میسازد. زبان های دیگر نیز رفته رفته به بانک اطلاعاتی لورم ایسپوم فارسی اضافه خواهند شد.

۳.۳ ارجاعات

دادن ارجاعات با افزودن BibTeX مرجع به فایل thesis.bib و سپس آوردن نام آن انجام می‌شود. مانند همین ارجاعی که در این صفحه وجود دارد. ارجاعات می‌تواند به منابع انگلیسی [۱] یا فارسی [۲] باشد.

۴.۳ نمایه‌ها

در این بخش به نحوه افزودن فایل‌های خارجی و جداول به متن پرداخته می‌شود.

۱.۴.۳ فرمول‌نویسی

نگارش فرمول‌ها در LaTeX به صورتی که مشاهده می‌کنید انجام می‌شود، در ادامه چند فرمول به عنوان نمونه نوشته می‌شود. تمامی قواعد و قوانین فرمول‌نویسی در LaTeX بدون نیاز به هیچ‌گونه تغییری در این قالب

قابل استفاده می‌باشد.

$$MAP(Q) = \frac{1}{|Q|} \sum_{j=1}^{|Q|} \frac{1}{m_j} \sum_{k=1}^{m_j} Precision(R_j k) \tag{۱.۳}$$

$$MI(sa, w) = \sum_{A_{sa}=0,1} \sum_{A_w=0,1} p(A_{sa}, A_w) \log \frac{p(A_{sa}, A_w)}{p(A_{sa})p(A_w)} \tag{۲.۳}$$

برای ارجاع به فرمول‌ها می‌توان از دستور \ref{label}\ استفاده کرد. به عنوان مثال: معادله ۱.۳ از معادلات مهم است.

۲.۴.۳ تصاویر

برای افزودن تصاویر می‌توانید از فایل‌های برداری مانند PDF و یا تصاویر پیکسلی مانند PNG و JPG استفاده کنید. افزودن این تصاویر مانند تصویر زیر انجام می‌شود و به راحتی می‌توان برای آنها توضیح نوشت و به طور خودکار در فهرست تصاویر قرار می‌گیرند. این تصاویر به طور خودکار در مکان مناسب قرار می‌گیرند.

آوردن نام تصاویر در متن نیز مانند فرمول‌ها می‌باشد به عنوان مثال: تصویر ۱.۳ لوگو دانشگاه را نشان می‌دهد.

متنی که در ادامه این بخش آمده فقط برای پرکردن فضا می‌باشد: لورم ایپسوم (به انگلیسی lorem ipsum) متنی بی مفهوم است که تشکیل شده از کلمات معنی دار یا بی معنی کنار هم. کاربر با دیدن متن لورم ایپسوم تصور میکند متنی که در صفحه مشاهده میکند این متن واقعی و مربوط به توضیحات صفحه مورد نظر است واقعی است. حالا سوال اینجاست که این متن « لورم ایپسوم » به چه دردی میخورد و اساسا برای چه منظور و هدفی ساخته شده است؟ پیش از بوجود آمدن لورم ایپسوم ، طراحان وب سایت در پروژه های وب سایت و طراحان کرافیک در پروژه های طراحی کاتولوگ ، بروشور ، پوستر و ... همواره با این مشکل مواجه بودند که صفحات پروژه خود را پیش از آنکه متن اصلی توسط کارفرما ارائه گردد و در صفحه مورد نظر قرار گیرد چگونه پر کنند؟؟ اکثر طراحان با نوشتن یک جمله مانند «این یک متن نمونه است» ویا «توضیحات در این بخش قرار خواهند گرفت» و کپی آن به تعداد زیاد یک یا چند پاراگراف متن میساختند که تمامی متن ها و کلمات ، جملات و پاراگراف ها تکراری بود و از این رو منظره خوبی برای بیننده نداشت و ضمنا به هیچ وجه واقعی به نظر نمیرسید تا بتواند شکل

شکل ۱.۳: یک نمونه تصویر

و شمایل تمام شده پروژه را نشان دهد. از این رو متنی ساخته شد که با دو کلمه (به فارسی : لورم ایپسوم) آغاز میشد وبا همین نام در بین طراحان وب و گرافیک شناخته و به سرعت محبوب شد. وب سایت های سازنده لورم ایپسوم میتوانند هر تعداد کلمه و پاراگراف که بخواهید به صوورت تکراری یا غیر تکراری برایتان بسازند و تحویلتان بدهند تا از آنها در پروژه هایتان استفاده کنید. (لورم ایپسوم فارسی) متن های لورم ایپسوم را به زبان فارسی و علاوه بر زبان فارسی به انگلیسی ، عربی ، ترکی استانبولی و ... برایتان میسازد. زبان های دیگر نیز رفته رفته به بانک اطلاعاتی لورم ایسپوم فارسی اضافه خواهند شد. لورم ایپسوم (به انگلیسی lorem ipsum) متنی بی مفهوم است که تشکیل شده از کلمات معنی دار یا بی معنی کنار هم. کاربر با دیدن متن لورم ایپسوم تصور میکند متنی که در صفحه مشاهده میکند این متن واقعی و مربوط به توضیحات صفحه مورد نظر است واقعی است. حالا سوال اینجاست که این متن « لورم ایپسوم » به چه دردی میخورد و اساسا برای چه منظور و هدفی ساخته شده است؟ پیش از بوجود آمدن لورم ایپسوم ، طراحان وب سایت در پروژه های وب سایت و طراحان کرافیک در پروژه های طراحی کاتولوگ ، بروشور ، پوستر و ... همواره با این مشکل مواجه بودند که صفحات پروژه خود را پیش از آنکه متن اصلی توسط کارفرما ارائه گردد و در صفحه مورد نظر قرار گیرد چگونه پر کنند؟؟ اکثر طراحان با نوشتن

یک جمله مانند «این یک متن نمونه است» ویا «توضیحات در این بخش قرار خواهند گرفت» و کپی آن به تعداد زیاد یک یا چند پاراگراف متن میساختند که تمامی متن ها و کلمات ، جملات و پاراگراف ها تکراری بود و از این رو منظره خوبی برای بیننده نداشت و ضمنا به هیچ وجه واقعی به نظر نمیرسید تا بتواند شکل و شمایل تمام شده پروژه را نشان دهد. از این رو متنی ساخته شد که با دو کلمه (به فارسی : لورم ایپسوم) آغاز میشد وبا همین نام در بین طراحان وب و گرافیک شناخته و به سرعت محبوب شد. وب سایت های سازنده لورم ایپسوم میتوانند هر تعداد کلمه و پاراگراف که بخواهید به صوورت تکراری یا غیر تکراری برایتان بسازند و تحویلتان بدهند تا از آنها در پروژه هایتان استفاده کنید. (لورم ایپسوم فارسی) متن های لورم ایپسوم را به زبان فارسی و علاوه بر زبان فارسی به انگلیسی ، عربی ، ترکی استانبولی و ... برایتان میسازد. زبان های دیگر نیز رفته رفته به بانک اطلاعاتی لورم ایسپوم فارسی اضافه خواهند شد.

۳.۴.۳ جداول

ساخت جداول در این قالب مانند بقیه متون نوشته شده توسط LaTeX می‌باشد. ابزارهای مختلفی نیز برای ساخت خودکار این جداول موجود می‌باشد که می‌توانید از آنها برای ساخت جداول پیچیده‌تراستفاده کنید. در ادامه نمونه‌ای جدول آورده می‌شود. برای ارجاع به نام جداول در متن نیز مانند تصاویر عمل می‌شود. به عنوان مثال در ادامه جدول ۱.۳ را مشاهده می‌کنید.

جدول ۱.۳: نمونه‌ای جدول

روش	دقت	صحت	حساسیت	معیار اِف
روش اول	۹۸/۷۰ %	۰/۸۸۲۱	۰/۸۸۱۷	۰/۸۸۱۹
روش دوم	۹۸/۱۵ %	۰/۷۴۶۴	۰/۴۷۷۲	۰/۶۱۱۸

مراجع

[1] K. Balog, Y. Fang, M. de Rijke, P. Serdyukov, and L. Si, "Expertise retrieval," *Foundations and Trends® in Information Retrieval*, vol.6, no.2-3, pp.127-256, 2012.

[۲] مصطفی واحدی، "درختان پوشای کمینه دورنگی مسطح،" مجله فارسی نمونه، جلد ۱، صفحات ۲۲-۳۰، آبان ۱۳۸۷.

Abstract:

This is Abstract in English.

Keywords: Blockchain, ethereum, security, voting

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. Maghsood Abbaspour

2018