

دانشکده مهندسی کامپیوتر

**پروژه مقطع کارشناسی مهندسي کامپیوتر**

Smart contract generation on Elearn

ایمان عباسی‌زاده

**استاد راهنما:**

دکتر علائیان

**[تاریخ دقیق روز، ماه و سال دفاع]**



# تأييديّه هيات داوران

اعضاي هيئت داوران، نسخه نهائي پروژه خانم / آقاي: [نام دانشجو]

را با عنوان: [عنوان پروژه]

از نظر شکل و محتوي بررسي نموده و پذيرش آن را براي تکميل درجه کارشناسی تأييد مي‏کنند.

|  |  |  |  |
| --- | --- | --- | --- |
| **اعضاي هيئت داوران** | **نام و نام خانوادگي** | **رتبه علمي** | **امضاء** |
| 1. استاد راهنما |  |  |  |
| 1. استاد داور |  |  |  |

**دانشگاه صنعتی خواجه نصیرالدین طوسی**

|  |
| --- |
| **اظهارنامه دانشجو** |
| اینجانب **ایمان عباسی‌زاده** دانشجوی مقطع کارشناسی رشته **مهندسی کامپیوتر** گواهی می‌نمایم که مطالب ارائه شده در این پروژه با عنوان:  **Smart Contract Generation on E-learn**  با راهنمایی استاد محترم **دکتر علائیان** توسط شخص اینجانب انجام شده است. صحت و اصالت مطالب نوشته شده در این پروژه تأیید می‌شود و در تدوین متن پروژه قالب مصوب دانشگاه را به طور کامل رعایت کرده‌ام.  **امضاء دانشجو:**  **تاریخ:** |

**حق طبع، نشر و مالکیت نتایج**

1- حق چاپ و تکثیر این پروژه متعلق به نویسنده و استاد راهنمای آن است. هرگونه تصویربرداری از کل یا بخشی از پروژه تنها با موافقت نویسنده یا استاد راهنما یا کتاب‌خانه دانشکده‌های مهندسی برق و کامپیوتر دانشگاه صنعتی خواجه نصیرالدین طوسی مجاز است.

2- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی خواجه نصیرالدین طوسی است و بدون اجازه کتبی دانشگاه قابل واگذاری به شخص ثالث نیست.

3- استفاده از اطلاعات و نتایج موجود پروژه بدون ذکر مرجع مجاز نیست.

###### تقديم به:

###### تشکر و قدرداني

###### چکيده

نیاز به آموزش آنلاین[[1]](#footnote-2) و غیر حضوری در سال های اخیر و به‌ویژه در دوره همه‌گیری کوید-۱۹[[2]](#footnote-3) تبدیل به یکی از نیازهای مهم و غیر قابل انکار شده، از طرفی دیگر ایجاد یک انگیزه موثر برای به پایان رساندن دوره[[3]](#footnote-4)های آنلاینی که شخص به صورت خودمختار اخذ کرده و هیچ الزام بیرونی نظیر دانشگاه ، استاد و ... برای اتمام دوره‌های اخذ کرده ندارد و همچنین داشتن لیستی از این دوره ها به همراه تاریخ اخذ و موعد مقرر[[4]](#footnote-5) مورد نظر برای به پایان رساندن و از سوی دیگر تحقق هرچه کامل‌تر آرمان آموزش بدون تبیعض برای همه با در دسترس قرار دادن دوره‌های ترجمه شده به صورت رایگان و در آخر ایجاد یک ساز و کار مالی پایا برای تحقق اهداف ذکر شده، ایده ساخت پلتفرم[[5]](#footnote-6) آنلاین Smartlearn را به کمک تکنولوژی بلاکچین[[6]](#footnote-7) و قراردادهای‌‌هوشمند[[7]](#footnote-8) بوجود آورد.

کليد واژه: بلاکچین ، اتریوم[[8]](#footnote-9) ، آموزش آنلاین ، مشوق مالی[[9]](#footnote-10) ، جنگو[[10]](#footnote-11) ، **VueJS** ، متامسک[[11]](#footnote-12) ، سالیدیتی[[12]](#footnote-13)

###### فهرست مطالب

عنوان صفحه

[تأييديّه هيات داوران ‌ه](#_Toc531381831)

[فهرست شکل‏ها ‌ه](#_Toc531381832)

[فهرست جدول‏ها ‌ز](#_Toc531381833)

[فهرست علامت‏ها و نشانه‏ها ‌ط](#_Toc531381834)

[فصل 1- مقدمه... 1](#_Toc531381835)

[1-1- پيشگفتار 1](#_Toc531381836)

[1-2- هدف از اين قالب و شیوه‏نامه 1](#_Toc531381837)

[فصل 2- ساختار بيان مطالب 3](#_Toc531381838)

[2-1- بخش‏هاي گزارش و ترتيب آنها 3](#_Toc531381839)

[2-2- فصل‏های متن اصلي گزارش 4](#_Toc531381840)

[2-3- نكته‏های كلّي در روش بيان 6](#_Toc531381841)

[فصل 3- سبك نگارش 9](#_Toc531381842)

[3-1- مقدمه..... 9](#_Toc531381843)

[3-1-1- ديدن سبك‏هاي تعريف شده 9](#_Toc531381844)

[3-1-2- اعمال سبك مورد نظر روي متن 9](#_Toc531381845)

[3-1-3- توليد يك سبك جديد 10](#_Toc531381846)

[3-2- سبك نگارش متن 10](#_Toc531381847)

[3-2-1- شروع پاراگراف 10](#_Toc531381848)

[3-2-2- ادامه يک پاراگراف 10](#_Toc531381849)

[3-2-3- تصحيح سبك پاراگراف‏هاي از قبل تايپ شده 11](#_Toc531381850)

[3-3- قلم 11](#_Toc531381851)

[3-4- صفحه‏بندي 12](#_Toc531381852)

[3-4-1- حاشيه صفحه‏ها 12](#_Toc531381853)

[3-4-2- سربرگ و شماره‏دهی صفحه‏ها 13](#_Toc531381854)

[3-4-3- مشخصات جلد پایان‏نامه 15](#_Toc531381855)

[3-5- فصل‏بندي 16](#_Toc531381856)

[3-5-1- شماره‏گذاري بخش‏ها و زيربخش‏ها 16](#_Toc531381857)

[3-6- روش تهيه فهرست مطالب 16](#_Toc531381858)

[3-7- جدول‏ها و شکل‏ها 18](#_Toc531381859)

[3-7-1- شماره‏گذاري خودكار شکل‏ها و جدول‏ها 20](#_Toc531381860)

[3-7-2- ارجاع به يک شکل و يا جدول 22](#_Toc531381861)

[3-7-3- مزاياي استفاده از Caption 23](#_Toc531381862)

[3-7-4- روش تهيه فهرست شکل‏ها و جدول‏ها 23](#_Toc531381863)

[3-8- توضيحات متن با استفاده از پانِوِشت 24](#_Toc531381864)

[3-8-1- درج نکردن واژه‏های انگليسي در متن فارسي 25](#_Toc531381865)

[3-9- رابطه‏ها و معادله‏های رياضي 26](#_Toc531381866)

[3-10- روش بازسازي شماره‏ها بصورت خودكار 27](#_Toc531381867)

[فصل 4- مرجع دهی 29](#_Toc531381868)

[4-1- روش مرجع‏دهي در متن با استفاده از مرجع‌دهی خودکار word 29](#_Toc531381869)

[پیوست ‌أ- سبك‏هاي تعريف شده 33](#_Toc531381870)

[پیوست ‌ب- روش انتقال سبك‏ها به فايل ديگر 35](#_Toc531381871)

[پیوست ‌ج- روش مناسب توليد فايل pdf 37](#_Toc531381872)

[پیوست ‌د- معادل فارسی تعدادی از واژه‏های بیگانه 39](#_Toc531381873)

[پیوست ‌ه- واژه‏نامه فارسي-انگليسي 41](#_Toc531381874)

[پیوست ‌و- واژه‏نامه انگليسي-فارسي 43](#_Toc531381875)

[پیوست ‌ز- نكته‏های قابل توجه در ارائه شفاهي 45](#_Toc531381876)

[فهرست مرجع‏ها 46](#_Toc531381877)

فهرست شکل‏ها

عنوان صفحه

[شکل ‏3‑1 اندازه و حالت‏دهی چینش صفحه (الف) حاشیه‏ها، (ب) کاغذ، و (ج) طرح برای کل فایل 15](#_Toc530263777)

[شکل ‏3‑2 پنجره توليد فهرست مطالب. 17](#_Toc530263778)

[شکل ‏3‑3 پنجره به‌هنگام کردن محتواي جدول فهرست مطالب. 18](#_Toc530263779)

[شکل ‏3‑4 تنظيمات لازم در MATLAB برای انتقال شکل به MS-Word. 19](#_Toc530263780)

[شکل ‏3‑5 شکل با فضای خالی در راست و بالای آن (الف) و شکل با حذف فضای خالی (ب) 20](#_Toc530263781)

[شکل ‏3‑6 پنجره دادن خودکار شرح شکل و عنوان جدول. 21](#_Toc530263782)

[شکل ‏3‑7 پنجره Cross-reference برای ارجاع به شکل یا جدول در متن 22](#_Toc530263783)

[شکل ‏3‑8 تنظيمات لازم براي تهيه فهرست شکل‏ها و جدول‏ها. 24](#_Toc530263784)

[شکل ‏3‑9 تنظيمات پانِوِشت. 25](#_Toc530263785)

فهرست جدول‏ها

عنوان صفحه

[جدول ‏1‑1 سبك‏هاي تعريف شده و موارد استفاده آنها 33](#_Toc530720185)

فهرست علامت‏ها و نشانه‏ها

عنوان علامت اختصاري

ثابت انتشار *γ*

ثابت پلانک *h*

ثابت فاز *β*

دمای مطلق (معمولا بر حسب کلوین) 

ضریب رسانایی الکتریکی *σ*

ضریب گذردهی الکتریکی *ε*

ضریب نفوذپذیری مغناطیسی *μ*

فرکانس پلاسما *ωp*

# مقدمه

## انگیزه

با همه گیری کووید-۱۹ لزوم استفاده از دوره های آنلاین و غیر حضوری در جهان به مسئله جدی تبدیل شد و پلتفرم های مختلفی جهت رفع این نیاز ایجاد و یا پلتفرم های قبلی با جدیت بیشتری توسعه پیدا کردند.

پلتفرم smartlearn نیز در جهت رفع این نیاز و با ۳ انگیزه مهم جهت بهبود شرایط آموزش آنلاین بوجود آمد.

۱. تحقق و تکمیل آرمان آموزش بدون تبیعض برای همه :

وجود این مدل فکری برای هر سازمان، موسسه، پلتفرم و هر کسی که در زمینه آموزش فعالیت می‌کند یک اصل بسیار مهم باید باشد تا فردی به علت محدودیت هایی که خود عاملش نبوده از یادگیری و توسعه فردی باز نماند. در جهت همین خط فکری پلتفرم smartlearn سیاست های کلی خود را بر دو اصل رایگان بودن تمامی دوره ها و ترجمه دوره ها به زبان مقصد کاربر ( در ابتدا به زبان فارسی) بنا نهاده و تحقیق این دو مورد جز اساسی ترین انگیزه ها برای شکل‌گیری این پلتفرم می‌باشد.

2. فراهم کردن امکانی برای ایجاد انگیزه در کاربر برای تکمیل دوره های آنلاین اخذ کرده :

در شرایطی که فراگیر دوره آنلاین به صورت خودخواسته دوره ای را اخذ میکند و شخص یا سازمانی مانند استاد یا دانشگاه جهت نظارت خارجی و ایجاد الزام بیرونی برای اتمام و به سرانجام رساندن دوره اخذ شده وجود ندارد لزوم وجود انگیزه مالی-تنبهی برای نتیجه‌گیری هرچه بهتر کاربر احساس می‌شود.

پلتفرم smartlearn به کمک قرارداد هوشمندی که در این پلتفرم طراحی شده امکان تعیین ددلاین و جایزه برای دوره های کاربر(چه دورهای ارائه شده توسط پلتفرم و چه دوره های دیگر کاربر) و همچنین امکان تنبیه مالی کاربر درصورت عدم تکمیل دوره در زمان مقرر را فراهم نموده.

3. ناشناس بودن کاربران و حفظ حریم شخصی با عدم دریافت و ثبت اطلاعات شخصی کاربر :

در دنیای امروز که اکثر شرکت ها و موسسات در تلاش برای کسب اطلاعات هرچی بیشتر از کاربران برای استفاده های مفید یا مضر تبلیغاتی، جامعه شناختی، تحلیلی و ... می‌باشند، پلتفرم smartlearn در خلاف جهت این موج سعی دارد برای حفظ هویت افراد و آزادی عمل کاربران با بهره گیری از تکنولوژی بلاکچین محیطی امن برای کاربرانش فراهم کند. این جهت‌گیری از انگیزه های مهم شکل‌گیری این پلتفرم و همچنین از دلایل استفاده smartlearn از بلاکچین برای ذخیره سازی اطلاعات دوره های برای انجام کاربر به صورت ناشناس می‌باشد.

## تبیین مسئله

پلتفرم smartlearn از نظر ساختاری به دو بخش کلی تقسیم بندی می‌شود:

۱.ارائه دوره های آنلاین ترجمه شده به صورت رایگان و قابل دسترس برای تمامی کاربران

۲. ارائه امکانی برای ثبت دوره ها،تعیین ددلاین و جایزه و مدیریت دوره های برای انجام به کمک قرارداد هوشمند

بخش اول این پلتفرم به مانند سایت ها و بستر های فعال در زمینه آموزش آنلاین (E-lear) اما در جهت تحقق آرمان آموزش بدون تبعیض، دوره هایی ترجمه شده به زبان مقصد کاربر (زبان فارسی) - در حال حاضر و ابتدای شروع کار پلتفرم -  و به صورت کاملا رایگان فراهم آورده که تمامی کاربران امکان بهره‌وری از این دوره ها را دارا می‌باشند.

بخش دوم مربوط به ارائه امکان مدیریت دوره های کاربران و تعیین و تعریف خود-انگیزش مالی در جهت اتمام دوره های اخذ شده کاربر می‌باشد. به کمک قرارداد هوشمندی که در این بخش طراحی شده کاربر ویژه ( کاربری که دارای یک کیف پول متصل به متامسک بوده و همچنین افزونه متامسک را در مرورگر خود نصب شده دارد) میتواند دوره های ارائه شده در سایت و یا هر دوره دیگری که اخذ نموده است را به لیست دوره های برای انجام خود با تعیین ددلاین( حداکثر موعد اتمام دوره اخذ کرده) و جایزه و انتخاب گزینه های اضافی موجود اضافه نماید و با در کنار هم داشتن تمامی دوره های اخذ کرده به صورت یکجا امکان مدیریت و برنامه ریزی دوره ها را در محیطی امن، غیر قابل تغییر و ناشناس داشته باشد.

این پلتفرم برای امتداد حیات خود و توانایی ارائه دوره ها به صورت ترجمه شده و رایگان نیاز به یک چرخه حیات مالی داشته که برای پاسخ به این نیاز یک ساز و کار پایا با تعیین کارمزد برای اضافه کردن دوره در بخش دوم و استفاده از مجموع دریافتی ها از کاربران ویژه برای تعریف و ترجمه دوره ها در بخش اول طراحی شده که این چرخه عامل ارتباطی بین این دو بخش می‌باشد.

همچنین به جهت تشویق کاربران برای مشارکت در این چرخه مکانیزمی طراحی شده تا کاربران ویژه بتواند در صورتی که مجموع مشارکت مالی آن ها به میزان از قبل تعیین شده ای( مبلغ کافی جهت انجام امور ترجمه و تولید دوره مورد نظر کاربر) رسید دوره ای را برای ترجمه از هر زبانی به زبان مورد تقاضا کاربر به سایت ارائه میدهد که براساس تاریخ ارائه و گذشت زمان مورد نیاز جهت ترجمه و تولید دوره به صورت ترجمه شده و رایگان در اختیار تمامی کاربران قرار می‌گیرد.

## هدف

با خلق اولین رمزارز توسط ساتوشی ناکاموتو بر پایه فناوری بلاکچین در سال ۲۰۰۸ میلادی نگاه جدی‌تری به سیستم های غیرمتمرکز و بهر‌وری از این سیستم‌ها شد، تا در سال ۲۰۱۵ بلاکچین اتریوم توسط ویتالیک بوترین جهت توسعه و برطرف سازی کاستی هایی که در بیت کوین وجود داشت بوجود آمد، اتریوم توانست امکان ایجاد قراردادهای هوشمند را برای تمام پروژه‌ها عملی کرده و گام نوینی در جهت هوشمند‌سازی جهان بردارد.

در ادامه این روند پیشرو،  تولید پروژه های کاربردی جهت نهادینه کردن و استفاده هرچه بیشتر از سیستم های غیر متمرکز به صورت جدی‌تری دنبال شد.

پلتفرم smartlearn نیز هم جهت با این روند ایجاد شد.

هدف اصلی خلق پلتفرم smartlearn استفاده از تکنولوژی نوین بلاکچین و قراردادهای هوشمند برای ایجاد یک برنامه کاربردی در فضای غیرمتمرکز بوده تا بتواند سهمی هرچند خیلی کوچک در ساخت و توسعه جهان هوشمند و آزاد و غیرمتمرکز آینده داشته باشد.

## نوآوری

پیاده سازی پلتفرم smartlearn به طور کلی از سه بخش فنی تشکیل شده که ابزارهای بکار گرفته شده در هر بخش از حیث سرعت، قدرت و به‌روز بودن در سطح یک بوده و هریک در زمینه تخصصی خود پیشرو و نوآور به حساب می‌آیند :

1. **سمت سرور :** جهت ثبت و واکشی اطلاعات دوره های ارائه شده در سایت نیازمند یک دیتابیس به شکل متمرکز و زبانی برای تعامل با این دیتابیس (backend) می‌باشیم، برای پاسخ به این نیاز از زبان قدرتمند پایتون و چهارچوب جنگو ستفاده شده است و دیتابیس مرکزی پلتفرم sqlite می‌باشد
2. **سمت بلاکچین :** نوآوری اصلی بکارگرفته شده در این پلتفرم بهری‌گیری از فناوری بلاکچین و استفاده از قراردادهای هوشمند می‌باشد، ثبت و واکشی اطلاعات دوره های برای انجام کاربران ویژه و میزان مشارکت مالی آنها، در بلاکچین اتریوم انجام میشود و قسمت منطق و اجرای دستورات از قبل نوشته شده و همچنین ارتباطات بین کاربر ویژه و سایت و برقراری تمامی شروطی و تفاهماتی که به مانند یک قرارداد فی مابین کاربر ویژه و سایت وجود دارد توسط قراردادهوشمند طراحی شده با زبان سالیدیتی انجام می‌گیرد.
3. **سمت کاربر :** جهت نمایش اطلاعات ذخیره شده و برقراری تعامل پویا با کاربران (frontend) نیاز به یک زبان برنامه نویسی سمت کاربر وجود دارد، در پاسخ به این نیاز پلتفرم smartlearn از زبان قدرتمند جاوااسکریپ و چهارچوب ویو و همچنین از کتابخانه‌ای به نام drizzle برای اتصال بین قراردادهوشمند و frontend استفاده نموده است.

## ساختار پایان نامه

روند ساختاری این پایان نامه در ادامه بدین شکل خواهد بود؛ ما بعد از ارائه یک چشم انداز کلی از انگیزه ها، نوآوری های بکار گرفته شده و هدف شکل‌گیری پروژه و همچنین بیان ساختار کلی آن در فصل اول و در مقدمه، قصد داریم در فصل دوم به تعریف بلاکچین و قراردادهای هوشمند به عنوان هسته اصلی و نوآورانه این پروژه بپردازیم تا با شناخت هرچه بیشتر این فناوری درک جامع‌تری نسبت به پتانسیل سیستم‌های غیرمتمرکز و جایگاه کاربردهای آن در دنیای امروز کسب کنیم.

در فصل سوم به بیان کارهایی که پیش از این در زمینه آموزش آنلاین با رویکرد استفاده از بلاکچین و قراردادهای هوشمند انجام گرفته می‌پردازیم.

فصل چهارم توضیح جامعی از تحلیل و طراحی پروژه و جزئیات بکار رفته در آن ارائه خواهد شد و همچنین جدول نیازمندی های پروژه، نمودار کلاس، نمودار بلاک و نمودار پکیج در این فصل رسم شده و نمایی از رابط کاربری پروژه را خواهیم داشت.

فصل پنجم به توضیح کامل جزئیات ابزار‌های بکار رفته در پروژه ،که در بخش نوآوری فصل اول به صورت تیتروار بیان شد، اختصاص دارد همچنین نحوه دانلود و نصب این ابزارها و نسخه استفاده شده از هریک در پروژه توضیح داده خواهد شد.

در فصل ششم و پایانی این پایان‌نامه جمع‌بندی، نتیجه‌گیری، پیشنهادات و ایده‌هایی که در آینده جهت توسعه پروژه در نظر داریم را ارائه خواهیم کرد.

# بلاکچین و قراردادهای هوشمند

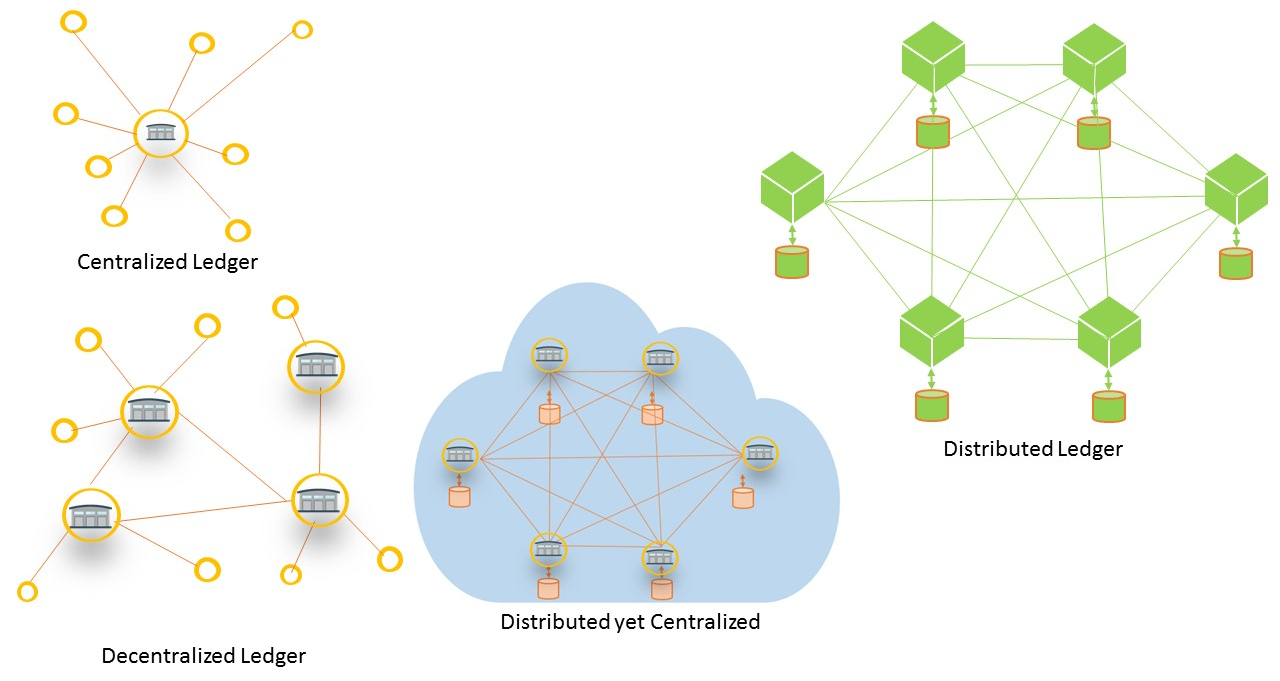
## مقدمه

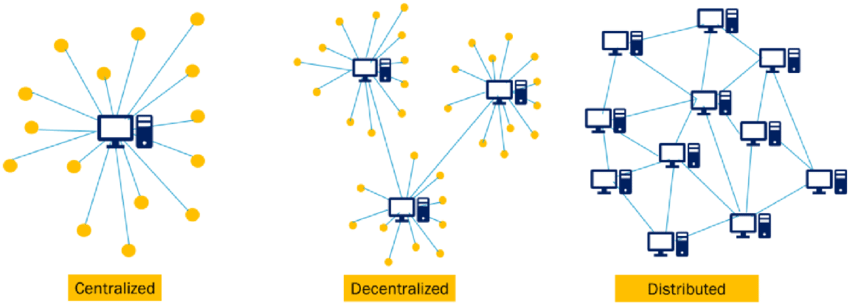
ثبت اطلاعات[[13]](#footnote-14) جهت دسترسی و ماندگاری اطلاعات از زمان آشنایی انسان با علم در حدود 3000 سال پیش از میلاد مسیح بر روی لوح های رسی/گلی انجام می‌گرفت [1]، با پیشرفت علم وسیله و شیوه ذخیره‌سازی[[14]](#footnote-15) داده[[15]](#footnote-16) تغییر و بهبود یافت تا با اختراع کامپیوتر در سال 1871 توسط چارلز بابیج[[16]](#footnote-17) مسیری جدید به روی انسان گشوده شد [2]، مسیری که دنیای امروز وام‌دار آن است و مسئله ذخیره‌سازی و واکشی[[17]](#footnote-18) داده را به یک مسئله بسیار جدی و مهم‌ تبدیل کرده است.

در طی این مسیر جدید و با پیشرفت تکنولوژی بخصوص با ظهور اینترنت به عنوان شبکه‌ای از کامپیوتر‌ها ذخیره‌سازی داده به شکل سیستمی درآمد و ساختاریافته دنبال شد، ذخیره‌سازی داده بر روی کامپیوترها در ابتدا به شکل سیستم های متمرکز[[18]](#footnote-19) به معنای کنترل اطلاعات به شکل واحد زیر نظر و حاکمیت یک شخص یا شرکت و همچنین مشترک یا توزیع نشده[[19]](#footnote-20) به معنای استقرار تمامی اجزای سیستم در یک مکان فیزیکی یکجا بود که این دو ویژگی متمرکز و توزیع نشده هر یک معضلاتی را در مسیر پیشرفت و گسترش تکنولوژی قرار میداد، از سویی متمرکز بودن یک سیستم کنترل داده ها را در اختیار کامل شخص یا شرکت قرار می‌دهد که این امر در دراز مدت عامل فساد و سوء استفاده از داده های ذخیره شده می‌شود همچنین به علت تحت کنترل بودن سیستم توسط افراد محدود باعث کندی پیشرفت تکنولوژی می‌شود و از سوی دیگر عدم توزیع سیستم، خطراتی از جمله خرابی و یا هک[[20]](#footnote-21) سرور مرکزی که باعث از دست رفت یا صدمه به داده‌ها می‌باشد را در پی خواهد داشت.

در ادامه روند پیشرفت سیستم های ذخیره‌سازی داده و در پی رفع معضلات بیان شده ایده‌ها و سیستم هایی بوجود آمدند؛ ارائه‌دهنده‌های متن باز[[21]](#footnote-22)ی مثل آپاچی[[22]](#footnote-23) نمونه ای از یک سیستم غیرمتمرکز[[23]](#footnote-24) ولی توزیع نشده است که به صورت غیرمتمرکز و با کمک جمیع افراد توسعه‌دهنده[[24]](#footnote-25) سراسر جهان توسعه داده می‌شود ولی همچنان معضلات یک سیستم توزیع نشده را به همراه دارند از سوی دیگر سیستم‌های خدمات دهنده ابری[[25]](#footnote-26) مانند کلودفلر[[26]](#footnote-27) توزیع شده[[27]](#footnote-28) بوده و دارای سرور[[28]](#footnote-29)های متعددی در اقصی نقاط جهان می‌باشند اما به صورت متمرکز بوده و کنترل مرکزی دارند.

در جهت فراهم شدن سیستمی غیرمتمرکز و توزیع شده رویکردی نوین با ظهور بیت‌کوین[[29]](#footnote-30) به عنوان اولین رمزارز[[30]](#footnote-31) جهان بر پایه تکنولوژی بلاکچین[[31]](#footnote-32) که یک نوع دفتر کل حساب توزیع شده[[32]](#footnote-33) است و صرفا جهت ثبت تراکنش‌های مالی استفاده می‌گردد شکل گرفت و با گسترش این رویکرد نوین، تکنولوژی‌های جدیدی جهت ذخیره‌سازی و واکشی اطلاعات بوجود آمدند.





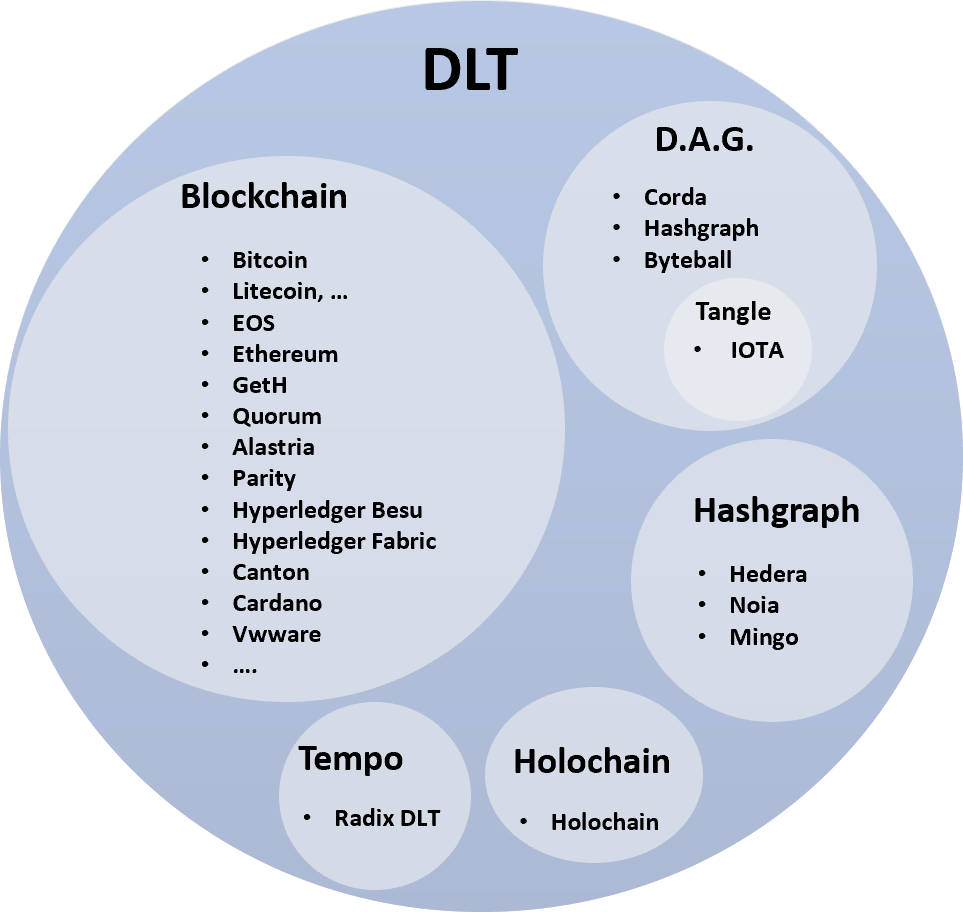
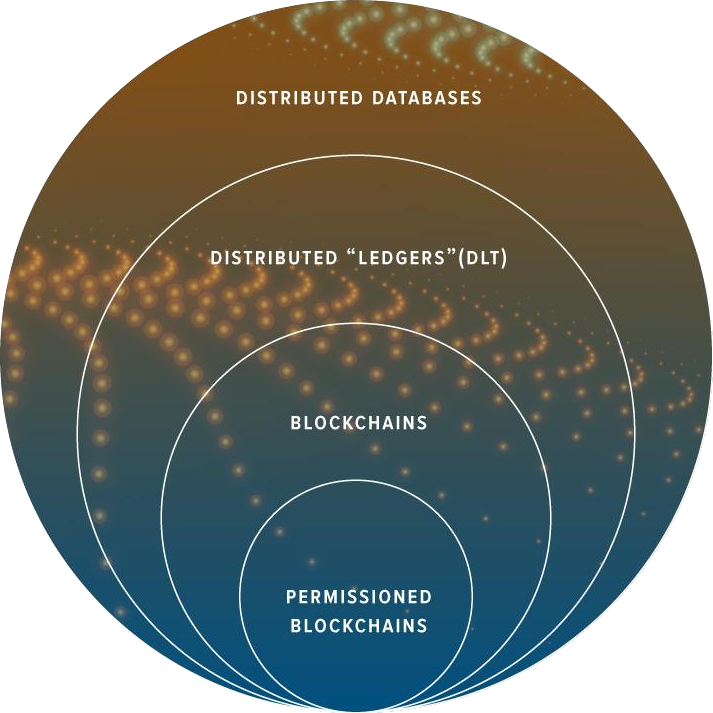
## دفتر کل حساب توزیع شده

دفتر کل حساب توزیع شده یک نمونه خاص از پایگاه داده توزیع شده است که تراکنش‌ها[[33]](#footnote-34) در آن به صورت توزیع شده ثبت می‌شوند، در یک دفتر کل حساب توزیع شده تمامی نودها[[34]](#footnote-35) باید یک نسخه یکسان از دفتر حساب داشته باشند و برای تغییر یا ثبت اطلاعات جدید، نودها باید روی حالت[[35]](#footnote-36) جدید توافق کنند.

تراکنش های ثبت شده روی دفتر کل حساب باید دارای سه ویژگی به شرح ذیل باشند :

1. **اتمیک[[36]](#footnote-37) :** به معنی انجام تمامی عملیات یک تراکنش است که درصورت انجام نشدن یک عملیات کل تراکنش انجام نشده تلقی می‌شود
2. **با ثبات[[37]](#footnote-38) :** به این معنا که تراکنش صورت گرفته ثبات کل جریان دفتر حساب را حفظ کند، به طور مثال در تراکنش انتقال پول در یک بانک کل بالانس[[38]](#footnote-39) مالی بانک ثابت می‌ماند
3. **پایا[[39]](#footnote-40) :** تراکتش در صورت انجام و قرارگیری در پایگاه داده باید به طور دائم وجود داشته باشد و قابل دسترس باشد

تکنولوژی دفتر کل حساب توزیع شده که به اختصارDLT [[40]](#footnote-41) نامیده می‌شود خود شامل انواع تکنولوژی‌های مختلفی است که شناخته شده‌ترین آن تکنولوژی بلاکچین است.

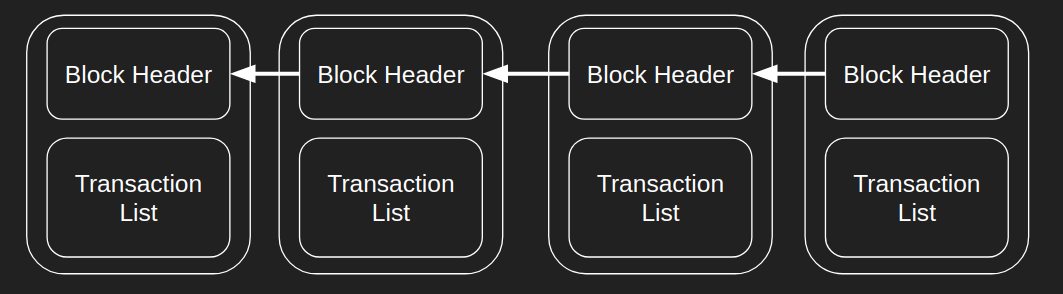


شکل 2-1 هنت

## بلاکچین

بلاکچین به عنوان مطرح‌ترین نوع دفتر کل حساب توزیع شده, زنجیره ای از بلوک‌[[41]](#footnote-42)ها است که هر بلوک حاوی تعدادی تراکنش و داده می‌باشد که به بلوک قبلی اشاره دارد، این زنجیره ادامه پیدا می‌یابد تا به اولین بلوک ایجاد شده به نام بلوک پیدایش[[42]](#footnote-43) برسد.

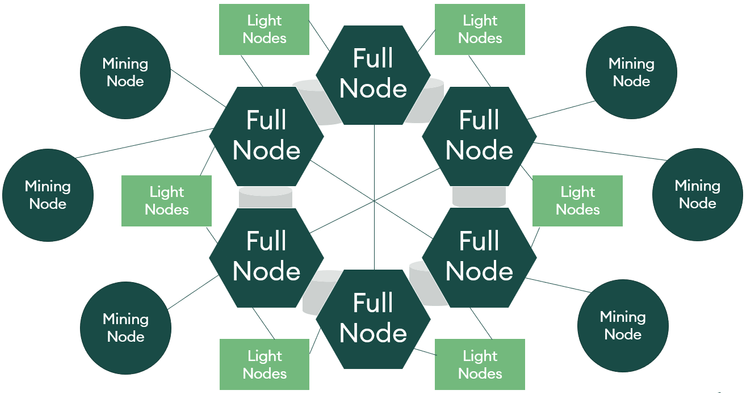
تعریف بلاکچین به شکل امروزی‌ که بیان شد متعلق به بعد از عرضه بیت‌کوین در سال ۲۰۰۸ است اما ایده اولیه شکل‌گیری بلاکچین در سال ۱۹۹۱ و با تلاش های استوارت هابر[[43]](#footnote-44) و اسکات استورنتا[[44]](#footnote-45) پایه‌ریزی شد و بلاکچین را به عنوان یک راه حل عملی محاسباتی برای زدن برچسب زمانی[[45]](#footnote-46) به اسناد دیجیتال معرفی کردند که این کار از برگرداندن زمان و دست‌کاری اسناد جلوگیری می‌کرد.



### گره‌ها

توزیع و غیرمتمرکز بودن شبکه بلاکچین به علت وجود گره‌ها در این شبکه است، به طور کلی هر شرکت کننده در شبکه بلاکچین یک گره است، أنواع مختلفی گره در شبکه وجود دارد که هر یک دارای ویژگی مخصوصی هستند و برای میزبانی[[46]](#footnote-47) یا اتصال به آن سخت‌افزار خاصی نیاز است.

هر گره در شبکه بلاکچین مستقل بوده و برای خود تصمیم گیرنده است به این معنا که با داشتن یک نسخه کامل از کل شبکه می‌تواند در هر لحظه تصمیم بگیرد در صورت ایجاد تغییر در شبکه و به‌روزرسانی در الگوریتم‌ها از تغییرات پیروی کند یا نه و یا تصمیم بر ایجاد تغییر در شبکه بگیرد و یا حتی می‌تواند به صورت موقت یا دائم بلوک‌ای به زنجیره بلوک‌هایش اضافه نکند و از شبکه خارج شود که نتیجه این تصمیمات در صورت همکاری و موافقت دیگر گره‌های شبکه به ایجاد انشعاب[[47]](#footnote-48) و یا در حالت جدی‌تر به ایجاد یک بلاکچین جدید می‌انجامد.

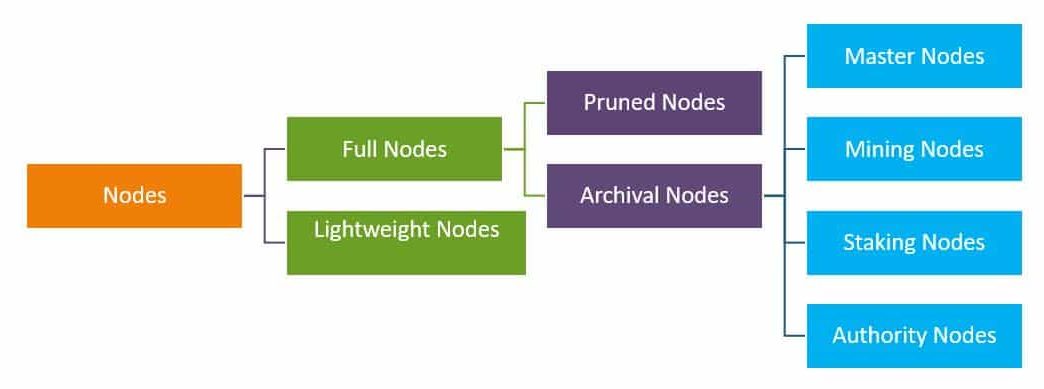


گره‌ها به دو دسته کلی تقسیم می‌شوند :

1. **گره‌های کامل[[48]](#footnote-49) :** گره‌های کامل یک کپی از بلاکچین را ذخیره می‌کنند که در نتیجه امنیت و صحت داده‌ها بر روی بلاکچین با اعتبارسنجی داده‌ها تضمین می‌شود، این دسته از گره خود به دو دسته گره‌های هرس شده[[49]](#footnote-50) و گره‌های بایگانی[[50]](#footnote-51) تقسیم‌بندی می‌شوند و تفاوت این دو گره در میزان ذخیره‌سازی آن‌ها است[[51]](#footnote-52)، گره‌های هرس شده ابتدا باید کل بلاکچین را از ابتدا طی کند و تمام بلوک‌های قبلی را تایید کند تا بتواند تراکنش‌های جدید را اعتبارسنجی نماید و همچنین تعداد محدودی در حدود ۱۲۸ بلوک آخر را ذخیره میکند درحالی که در یک گره بایگانی کل بلوک‌ها ذخیره می‌شوند.

* گره استخراج[[52]](#footnote-53) یک گره کامل از نوع گره بایگانی است که امکان تایید و استخراج بلوک از طریق اجماع اثبات کار[[53]](#footnote-54) دارد.

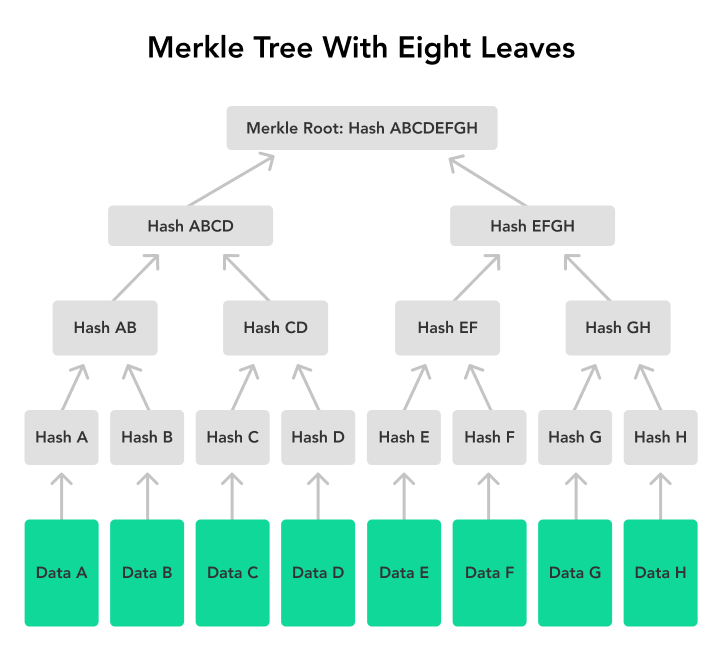
1. **گره‌های سبک وزن[[54]](#footnote-55) :** در گره سبک وزن فقط سربرگ بلوک‌ها ذخیره می‌شوند، این گره به امنیت شبکه کمکی نمی‌کند و برای استفاده کاربر بوجود آمده، این گره با تکیه بر یک نود کامل و پخش[[55]](#footnote-56) تراکنش در شبکه امکان تعامل کاربر با بلاکچین را نظیر ارسال، دریافت و امضا تراکنش‌ها برقرار می‌کند.



### ساز و کار بلاکچین

در این بخش قصد داریم با بررسی بلاکچین بیت‌کوین به عنوان مهم‌ترین و معروف‌ترین بلاکچین، شناخت کامل‌تری نسبت به ساز و کار بلاکچین بدست آوریم.

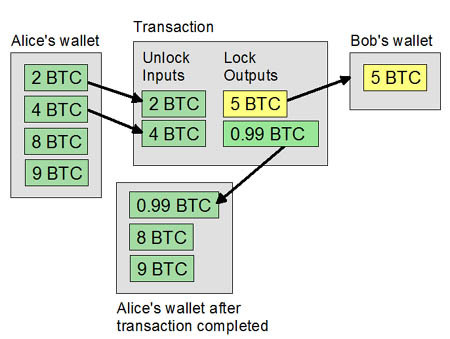
بلوک‌های بلاکچین از دو بخش سربرگ و بدنه[[56]](#footnote-57) تشکیل می‌شوند:

* **بدنه :** بدنه هر بلوک شامل لیست تراکنش‌هایی است که هش[[57]](#footnote-58) هر یک با الگوریتم مخصوصی، در بیت‌کوین با الگوریتم SHA256، محاسبه شده و با ساختمان داده[[58]](#footnote-59) درخت مرکل[[59]](#footnote-60) ذخیره شده اند.

هر تراکنش، که در شبکه بیت‌کوین منظور تراکنش صرفا مالی است، شامل آدرس فرستنده، آدرس گیرنده، تعداد ساتوشی[[60]](#footnote-61) و کارمزد تراکنش[[61]](#footnote-62) است و جهت ارسال و تایید نیازمندی‌هایی دارد که بخشی از آن توسط کاربر ایجاد کننده تراکنش مرتفع می‌شود و بخش دیگر آن به کمک مفاهیم تعریف شده داخل شبکه انجام می‌گیرد.

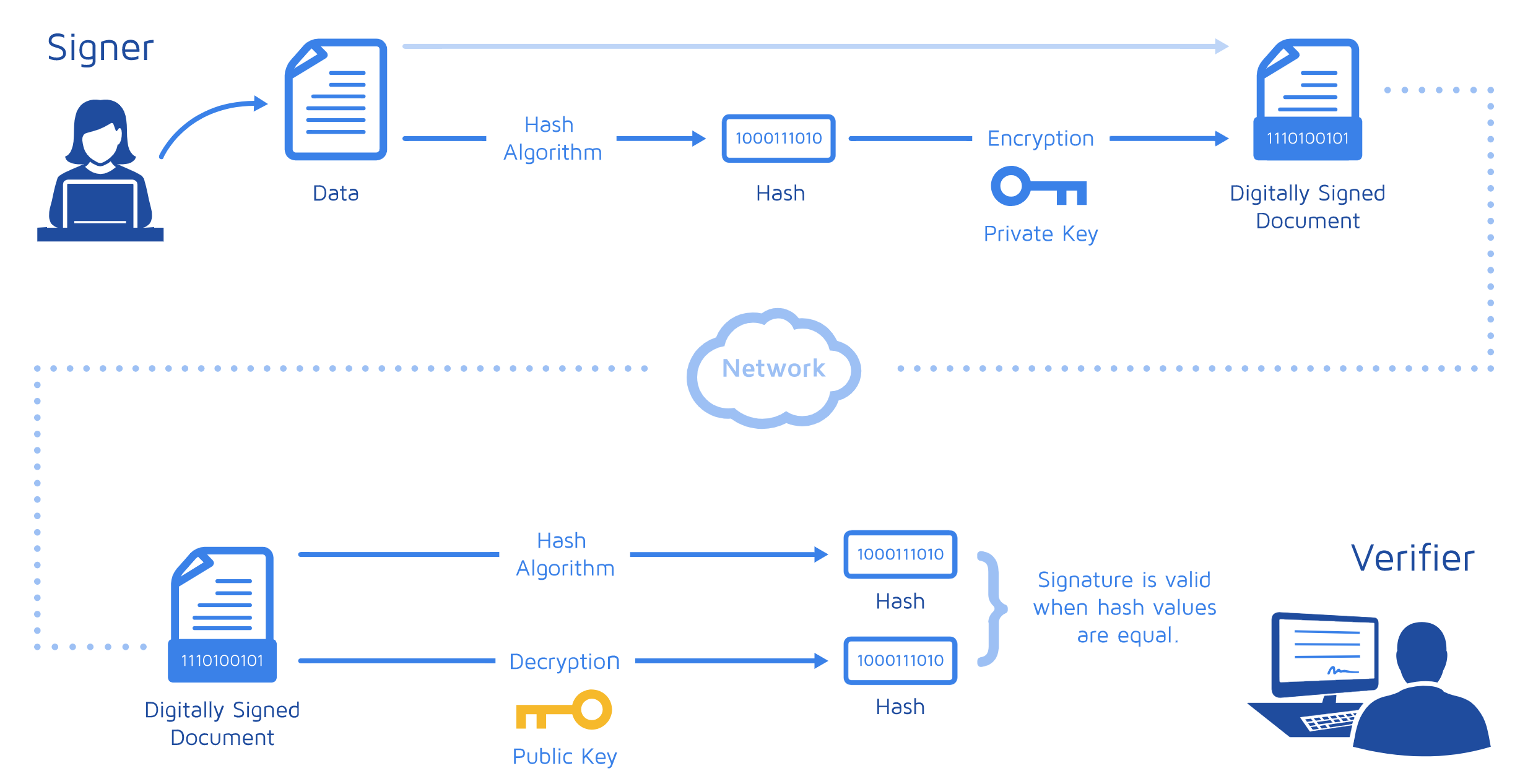
مهترین نیازمندی جهت تایید تراکنش، محاسبه میزان موجودی ارسال کننده تراکنش است؛ بیت‌کوین موجودی آدرس کیف پول‌ها را در شبکه نگهداری نمی‌کند و از مفهومی به نام خروجی خرج نشده تراکنش[[62]](#footnote-63) [3] جهت تایید میزان موجودی کافی برای انجام تراکنش و همچنین برای جلوگیری از خرج مجدد[[63]](#footnote-64) و افزایش امنیت استفاده می‌کند.

یک آدرس کیف پول از سه طریق موجودی بدست می‌آورد یا از طریق پاداشی است که از استخراج بلوک[[64]](#footnote-65) منتقل شده یا از آدرس دیگری انتقال صورت گرفته و یا به عنوان باقی مانده تراکنش به همان آدرس بازگردد، در هر صورت هر مقدار بیت‌کوین[[65]](#footnote-66) انتقال شده و موجود در آدرس کیف پول یک UTXO است، گره‌های شبکه زمان درخواست انجام یک تراکنش موجودی آدرس فرستنده تراکنش را بررسی می‌کنند تا مطمئن شوند UTXO کافی برای انجام تراکنش وجود دارد.



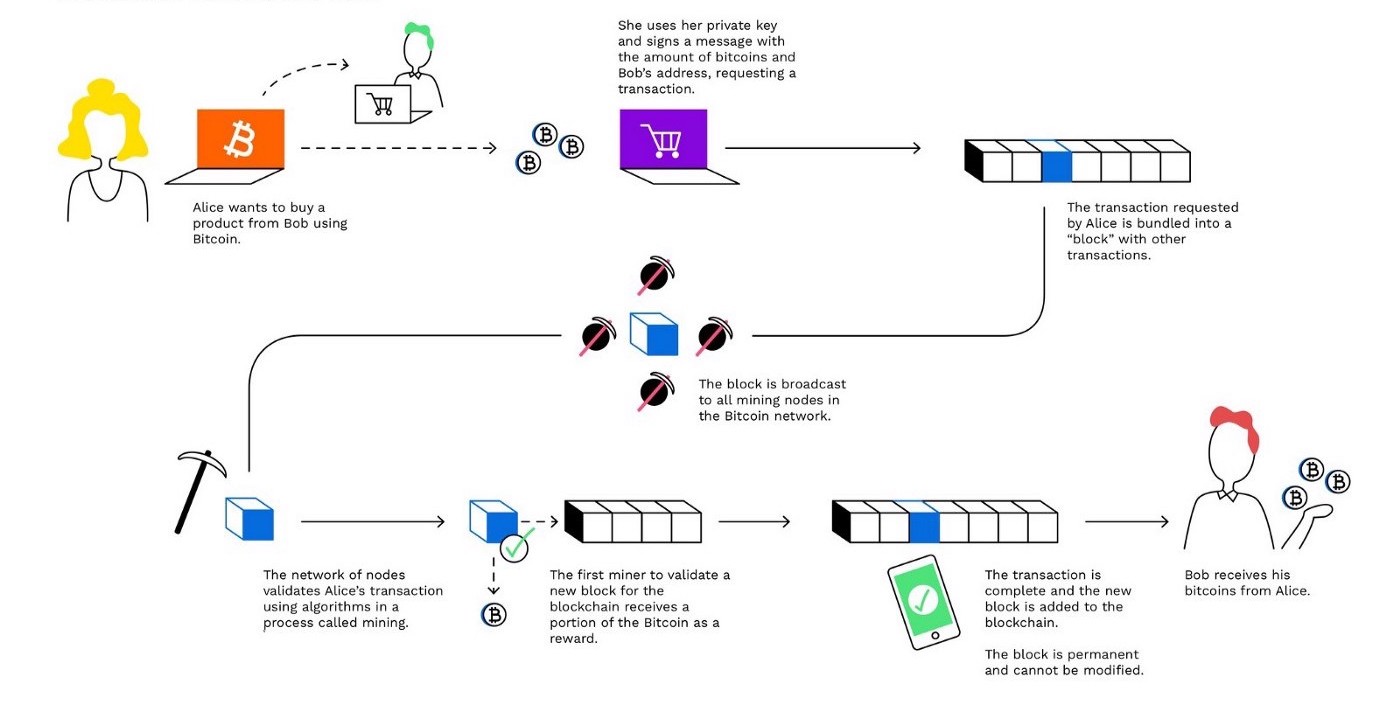
همان‌طور که در شکل بالا مشاهده می‌کنید برای انجام این تراکنش 5 بیت‌کوین لازم است جهت تامین این میزان از دو UTXO حاوی 2 و 4 بیت‌کوین از آدرس کیف پول فرستنده استفاده شده که مجموعا 6 بیت‌کوین است که از این میزان 5 بیت‌کوین منتقل می‌شود و 0.01 کارمزد تراکنش کسر میشود و 0.99 بیت‌کوین به عنوان یک UTXO جدید به آدرس کیف پول فرستنده منتقل می‌شود.

نیازمندی مهم دیگر تایید ارسال تراکنش است که از مفهوم امضا دیجیتال[[66]](#footnote-67) استفاده می‌کند، امضا دیجیتال توسط رمزنگاری نامتقارن[[67]](#footnote-68) پیاده‌سازی شده و غیرقابل انکار[[68]](#footnote-69) است و گره‌های شبکه مسئولیت صحت‌سنجی[[69]](#footnote-70) به عهده دارند.



مطابق شکل بالا ابتدا هش تراکنش با کلید خصوص فرستنده تراکنش رمز می‌شود[[70]](#footnote-71) و سند رمز شده به همراه هش تراکنش برای صحت سنجی فرستاده می‌شود و گره‌های شبکه با استفاده از کلید عمومی سنده رمز شده را رمزگشایی[[71]](#footnote-72) کرده و هش بدست آمده را با هش تراکنش مقایسه می‌کنند که در صورت یکی بودن این دو امضا تایید می‌شود.

* **سربرگ :**



## قراردادهاي هوشمند

# بلاکچین در آموزش آنلاین

## مقدمه

از ابتدای حضور انسان در این کره خاکی همواره نیاز به آموزش از نیازهای حیاتی بشر بوده، گونه انسان از ابتدای وجودی خود به واسطه بهروی از مغزش و ساخت ابزارالات توانسته گونه خود را حفظ نماید و تسلط و شناختش بر جهان را گسترش دهد.

مطالعات بر روی انسان نشان می‌دهد که این گونه در حدود ۳.۳ میلیون سال قبل و در دوران قبل از تاریخ، دوره ای قبل از توانایی مکتوب کردن تاریخ، موضوع آموزش وجود داشته.

آموزش؛ این عضو جدایی‌ناپذیر از انسان در هر دوره از سیر تکاملی بشر نقش مهم و کلیدی داشته و در نقاط عطف تاریخی همگام با اختراعات نوآورانه و جدید بشر خود را به روز کرده است. [3]

بهره‌وری از تکنولوژی روز هر دوره برای آموزش در ابتدا با هدف بهبود و تسهیل فرآیند آموزش بوده و از نظر تاریخی از دوره غارنشینی انسان با استفاده از ابزار اولیه مانند نقاشی روی دیواره‌های غار شروع شده [4] رفته رفته در هر دوره با ظهور تکنولوژی جدید، فرآیند آموزش به‌روزتر و کارآمدتر شده و با رشد انسان به واسطه مجموعه آموزش‌ها، هدف و آرمانی جدید در کنار هدف تسهیل آموزش تعریف شد؛ آرمان آموزش برای همه فارغ از موقعیت جغرافیایی، وضعیت مالی و حتی زبان دوره آموزشی آرمانی است که در قرن اخیر و با درک این موضوع که انسان با دانش قوی‌تر است و دنیای قدرتمند نیازمند انسان‌های قوی است شکل گرفت.

در حال حاضر جدیدترین تکنولوژی پیش روی انسان تکنولوژی بلاکچین بوده و افراد مختلف در سراسر جهان سعی دارند با مطرح کردن ایده‌های نوآورانه جهت استفاده از پتانسیل‌های این تکنولوژی در زمینه آموزش و به خصوص آموزش آنلاین اهداف مطرح شده را تحقق بخشند.

## پروژه‌های انجام گرفته

یکی از اولین ایده‌های شکل گرفته جهت بهره‌وری از بلاکچین در آموزش ذخیره‌سازی و اشتراک‌گزاری مدارک و سوابق تحصیلی-آموزشی است، این ایده از ویژگی‌ تغییرناپذیری بلاکچین

# تحلیل نیازمندی‌ها و طراحی

## مقدمه

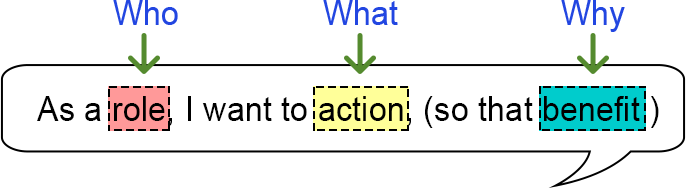
پروژه طراحی و ساخته شده پیش روی شما که با عنوان پلتفرم smartlearn در سراسر این پایان‌نامه شناخته می‌شود حاصل ماه‌ها تلاش شبانه‌روزی انفرادی بوده و سعی داشته هم‌جهت با هدف والای آموزش که تحقق آرمان آموزش بدون تبعیض برای همه می‌باشد توسعه یابد، در این فصل از پایان‌نامه در ابتدا با بیان خواست کاربران در قالب داستان‌های کاربر[[72]](#footnote-73) به نیازسنجی یک فرد استفاده کننده از دوره های آنلاین آموزشی پرداختیم و در ادامه با تبیین سند نیازمندی‌های این پلتفرم[[73]](#footnote-74)، نیازمندی‌های سیستم جهت پیاده سازی پروژه و نیازهای کاربران به شکل جدول در سه بخش سمت کاربر، سمت سرور و سمت بلاکچین ارائه میشود که هر یک از نیازمندی های مطرح شده جزء به جزء مورد بررسی قرار میگیرد سپس با ارائه نمودار های کلاس دیاگرام و بلاک دیاگرام و همچنین نمودار رابطه-موجودیت برای مدل‌سازی پایگاه داده نمایش بهتر و کامل‌تری از کل بخش های پروژه خواهیم داشت.

## داستان‌های کاربر

در قدم‌های ابتدایی شروع توسعه هر نرم افزاری نیازسنجی مهمترین بخش می‌باشد تا بر اساس هدف و انگیزه‌های شکل‌گیری یک سیستم نیازهای استفاده کنندگان حوزه مورد توسعه شناسایی و باتوجه به این نیازها توسعه نرم‌ افزار انجام شود.

روش نیازسنجی کاربران در رویکرد توسعه نرم افزار چابک[[74]](#footnote-75)، داستان‌های کاربر می‌باشد تا از زبان کاربران سندی جهت نیازسنجی برای ارائه به تیم فنی فراهم شود.

قالب اصلی داستان‌های کاربر به شکل ذیل می‌باشد:



* من به عنوان 《 یک شخص 》، میخواهم 《کاری را انجام دهم》[نیازی دارم]، (تا《به هدفی برسم》[کاری برایم آسان شود])[[75]](#footnote-76)

در ادامه می‌توان داستان‌های کاربری که منجر به پیاده‌سازی پلتفرم smartlearn شد را مشاهده کرد:

* من به عنوان یک فرد می‌خواهم هیچ اطلاعات شخصی برای استفاده از دوره‌های آموزی آنلاین و دیگر خدماتی که در این حوزه ارائه می‌شود را ارائه نکنم و به صورت ناشناس فعالیت کنم
* من به عنوان یک فرد می‌خواهم دوره‌های آموزشی رایگان و ترجمه شده به زبان خودم را در دسترس داشته باشم
* من به عنوان یک فرد می‌خواهم دسترسی آسان به دوره‌های آموزشی آنلاین داشته باشم
* من به عنوان یک فرد می‌خواهم بتوانم برای دوره‌های آنلاینی که اخذ کرده ام محدودیت زمانی و جایزه قرار دهم تا انگیزه ام برای تمام کردن تمام دوره‌هایم در زمان مقرر بیشتر شود
* من به عنوان یک فرد می‌خواهم لیستی از تمام دوره‌های آنلاینی که اخذ کرده ام را داشته باشم
* من به عنوان یک فرد می‌خواهم بتوانم تنبیه مالی در صورت به پایان نرساندن دوره‌ای که اخذ کرده ام داشته باشم تا الزام و فشار بیشتری برای تمام کردن دوره در زمان معین داشته باشم
* من به عنوان یک فرد می‌خواهم بتوانم درصورت دلخواه فرد دیگری را با انگیزه مالی تشویق به اتمام دوره آموزشی اش در زمان مقرر کنم
* من به عنوان یک فرد می‌خواهم بتواتم دوره‌هایی را جهت ترجمه به زبان خودم درخواست تولید دهم
* من به عنوان یک فرد می‌خواهم تراکنش های مالی‌ام بر بستر بلاکچین و با رمز ارز[[76]](#footnote-77) اتر[[77]](#footnote-78) انجام گیرد تا تراکنش هایم مورد تحریم یا هر نوع محدودیت دیگری قرار نگیرد
* من به عنوان یک فرد می‌خواهم بتوانم درصورت دلخواه حمایت مالی از سایت ارائه دهنده خدمات آموزشی داشته باشم

## سند نیازمندی‌های نرم‌افزار

در ادامه سند نیازمندی‌های پلتفرم smartlearn را به صورت جدول خواهیم داشت ولی قبل از آن لازم است تعریف شفافی از کاربران این پلتفرم ارائه شود؛ کاربران این پلتفرم به دو دسته تقسیم می‌شوند:

**۱. کاربران ویژه :** کاربری که کیف پول رمزارزی[[78]](#footnote-79)متامسک داشته و کیف پولش حاوی مقداری اتر جهت انجام تراکنش بوده و همچنین کاربر افزونه متامسک در مرورگرهای مورد پوشش متامسک[[79]](#footnote-80) داشته باشد و اتصال کیف پول به سایت انجام گرفته باشد.

**۲. کاربر معمولی :** کاربر معمولی که ما در این پایان‌نامه جهت سهولت به اسم کاربر از آن یاد می‌کنیم به هر فردی که به اینترنت دسترسی داشته و به پلتفرم smartlearn مراجعه می‌کند اطلاق می‌شود.

|  |  |  |
| --- | --- | --- |
|  |  | **Client Side** |
| کد ویژگی | عنوان ویژگی | توضیحات |
| C01 | مشاهده صفحه دوره‌های ارائه شده | کاربر می‌تواند لیست دوره‌های تهیه شده سایت را در صفحه مربوطه مشاهده کند |
| C02 | مشاهده جزئیات دوره‌های ارائه شده در سایت | کاربر می‌تواند جزئیات مربوط به هر دوره را مشاهده نماید |
| C03 | مشاهده ویدئو‌های دوره‌های ارائه شده | کاربر می‌تواند ویدئو‌ دوره‌ ارائه شده را از طریق youtube مشاهده نماید |
| C04 | مشاهده صفحه خانه | کاربر می‌تواند صفحه خانه را مشاهده کند |
| C05 | امکان ارسال نظر و پیشنهاد | کاربر می‌تواند به شکل کاملا ناشناس پیشنهادات خود را جهت بهبود سایت ارسال کند |
| C06 | مشاهده صفحه اضافه کردن دوره به لیست دوره‌های برای انجام | کاربر می‌تواند صفحه مربوط به اضافه کردن دروس برای انجام را مشاهده نماید |
| C07 | مشاهده پیام نیاز اتصال به متامسک | کاربر جهت بهره‌وری کامل از سایت پیام اتصال به متامسک را مشاهده می‌کند |
| C08 | اتصال کیف پول کاربر به سایت | از طریق افزونه Metamask اتصال کیف پول کاربر به سایت انجام می‌شود و کاربر به کاربر ویژه تغییر می‌یابد |
| C09 | امکان حمایت مالی سایت | کاربر ویژه می‌تواند به میزان دلخواه با انتقال اتر به آدرس کیف پول سایت حمایت مالی انجام دهد و به همان میزان به مشارکت کلی کاربر ویژه اضافه شود |
| C10 | مشاهده لیست دوره‌های برای انجام | کاربر ویژه می‌تواند لیستی از دروسی که برای انجام ثبت کرده را با جزئیات هر درس مشاهده نماید |
| C11 | اضافه کردن دوره‌ به لیست دوره‌های برای انجام | کاربر ویژه می‌تواند دوره های اخذ کرده خود را؛ چه این دوره از دوره‌های ارائه شده سایت باشد و چه هر دوره دیگری که اخذ نموده است را با پر کردن موارد مربوطه به لیست دوره‌های برای انجام خود اضافه نماید |
| C12 | امکان اضافه کردن دوره‌های ارائه شده به لیست دوره‌های برای انجام | کاربر ویژه‌ می‌تواند از قسمت جزئیات هر دوره ارائه شده در سایت دوره انتخاب کرده را به لیست دوره‌های برای انجام اضافه کند |
| C13 | امکان تعیین تشویق مالی برای دیگر افراد | کاربر ویژه می‌تواند آدرس کیف پول فرد دیگری و یا حتی آدرس دیگر کیف پول خودش را به عنوان ادرس مقصد جهت تراکنش پرداخت جایزه قرار دهد |
| C14 | امکان تعیین تنبیه مالی دوره‌های در حال انجام | کاربر ویژه‌ می‌تواند تعیین نماید در صورت عدم تکمیل دوره ثبت شده برای انجام در زمان مقرر شده، میزان اتر از قبل تعیین شده به عنوان جایزه، جهت تنبیه به آدرس کیف پول سایت منتقل شود و به همان میزان به مشارکت کلی کاربر ویژه اضافه شود |
| C15 | تکمیل دوره برای انجام | کاربر ویژه‌ای که دوره ای برای انجام دارد می‌تواند دوره برای انجامش را به حالت تکمیل شده تغییر دهد |
| C16 | مشاهده زمان دقیق کامل شدن دوره برای انجام | کاربر ویژه‌ای که دوره برای انجامش را به حالت کامل شده تغییر می‌دهد می‌تواند زمان دقیق کامل شدنش را مشاهده نماید |
| C17 | کشتن دوره برای انجام | کاربر ویژه‌ای که دوره ای برای انجام دارد می‌تواند دوره برای انجامش را به حالت کشته شده که به معنای عدم تکمیل دوره است تغییر دهد |
| C18 | حذف دوره برای انجام | کاربر ویژه‌ای که دوره ای برای انجام دارد می‌تواند دوره برای انجامش را در صورتی که تکمیل شده و یا kill شده باشد به طور کامل حذف نماید |
| C19 | مشاهده میزان کل مشارکت | کاربر ویژه‌ می‌تواند میزان کل مشارکتش با سایت را به اتر مشاهده نماید |
| C20 | مشاهده تعداد دفعات پیشنهاد دوره | کاربر ویژه‌ می‌تواند تعداد دفعاتی را که میتواند دوره‌ای را برای ترجمه پیشنهاد دهد را مشاهده کند |
| C21 | امکان درخواست یک دوره برای ترجمه | کاربر ویژه‌ می‌تواند در صورتی که مجاز باشد با پر کردن موارد مربوطه دوره‌ای را برای ترجمه درخواست دهد |
| C22 | برقراری ارتباط با قرارداد هوشمند |  |
| C23 | برقراری ارتباط با پایگاه داده |  |
| C24 | بررسی و محاسبه به روز وضعیت و شرایط مربوط به هر دوره برای انجام |  |
| C25 | بررسی موارد مجاز ورودی‌ها |  |
| C26 | دریافت ورودی‌ها |  |

|  |  |  |
| --- | --- | --- |
|  |  | **Blockchain Side** |
| کد ویژگی | عنوان ویژگی | توضیحات |
| B01 | Push کردن اطلاعات دوره‌های برای انجام |  |
| B02 | واکشی آرایه ای از دوره‌های برای انجام |  |
| B03 | حذف (pop) کردن دوره‌ای از آرایه دوره‌های برای انجام |  |
| B04 | اعمال تغییر وضعیت دوره‌های برای انجام |  |
| B05 | محاسبه تعداد دفعات مجاز برای پیشنهاد دوره | تعداد دفعات مجاز هر کاربر ویژه |
| B06 | محاسبه میزان کل مشارکت | میزان کل مشارکت کاربر ویژه بر حسب wei محاسبه می‌شود |
| B07 | انجام تراکنش‌ها | انتقال اتر از یک آدرس به آدرس دیگری |
| B08 | واکشی میزان کل مشارکت |  |
| B09 | واکشی تعداد دفعات مجاز برای پیشنهاد دوره |  |
| B10 | ثبت تعداد دفعات مجاز برای پیشنهاد دوره |  |
| B11 | ثبت میزان کل مشارکت |  |
| B12 | محاسبه و کسر کارمزد |  |
| B13 | اعمال محاسبات و شروط دوره‌های برای انجام |  |
| B14 | بررسی زمان مجاز برای تعیین ضرب الاجل دوره های برای انجام |  |
| B15 | چک کردن انقضا ضرب الاجل دوره های برای انجام |  |
| B16 | بررسی امکان حذف |  |
| B17 | بررسی حداقل میزان جایزه |  |

|  |  |  |
| --- | --- | --- |
|  |  | **Server Side** |
| کد ویژگی | عنوان ویژگی | توضیحات |
| S01 | ثبت اطلاعات دوره‌های تهیه و آماده شده | اطلاعات دوره‌های تهیه و آماده شده توسط ادمین در پایگاه داده متمرکز ذخیره و ثبت می‌شود |
| S02 | واکشی اطلاعات دوره‌های سایت | اطلاعات دوره‌های تهیه و آماده شده جهت نمایش به کاربر از پایگاه داده متمرکز واکشی می‌شود |
| S03 | ثبت اطلاعات دوره‌های پیشنهادی | اطلاعات دوره‌های پیشنهادی از طرف کاربر ویژه در پایگاه داده متمرکز ذخیره و ثبت می‌شود |

* **کد ویژگی :** C01 **|** **بازیگران :** کاربر - پایگاه داده متمرکز (سرور)

**عنوان نیازمندی :** مشاهده صفحه دوره‌های ارائه شده

**توضیح نیازمندی :** کاربر با کلیک بر روی دکمه[[80]](#footnote-81) Courses واقع در سربرگ[[81]](#footnote-82) و یا دکمهExplore courses در صفحه خانه وارد صفحه دوره‌های ارائه شده می‌شود و لیست دوره‌های تهیه شده سایت مشاهده می‌کند.

**توضیح فنی به همراه تکه کد :** با استفاده از کتابخانه axios اطلاعات تمام دوره‌های تهیه شده از پایگاه داده متمرکز (سرور) جهت نمایش به کاربر واکشی می‌شود و این اطلاعات به صورت یک آرایه[[82]](#footnote-83) به سمت frontend فرستاده می‌شود

courses: []

async created() {

try {

const response = await axios.get(`http://127.0.0.1:8000/api/v1/courses`);

this.courses = response.data;

} catch (e) {

this.errors.push(e);

}

}

* **کد ویژگی :** C03 **|** **بازیگران :** کاربر - پایگاه داده متمرکز (سرور)

**عنوان نیازمندی :** مشاهده ویدئو‌های دوره‌های ارائه شده

**توضیح نیازمندی :** کاربر می‌تواند در صفحه جزئیات دوره انتخابی‌اش ویدئو دوره را از طریق yotube مشاهده نماید

**توضیح فنی به همراه تکه کد :** آدرس ویدئو ذخیره در یوتوب به عنوان ویدئو در پایگاه داده ذخیره می‌شود و با کد زیر به کاربر نمایش داده می‌شود

<b-embed type="iframe" width="640" height="360"

:src="`https://www.youtube.com/embed/${course.video}`"

allowfullscreen></b-embed>

* **کد ویژگی :** C02 **|** **بازیگران :** کاربر - پایگاه داده متمرکز (سرور)

**عنوان نیازمندی :** مشاهده جزئیات دوره‌های ارائه شده در سایت

**توضیح نیازمندی :** کاربر با کلیک بر روی دکمه GO در باکس[[83]](#footnote-84) مربوط به هر دوره ارائه شده در سایت وارد صفحه جزئیات آن دوره می‌شود که این جزئیات شامل { نام دوره – توضیحات دوره – ویدئو دوره - مدت زمان مقرر برای اتمام دوره – زبان دوره (ترجمه شده) – دکمه اضافه کردن دوره به لیست دوره‌های برای انجام } می‌باشد.

**توضیح فنی به همراه تکه کد :** با استفاده از کتابخانه axios اطلاعات جزئیات مربوط به دوره انتخاب شده از پایگاه داده متمرکز (سرور) جهت نمایش به کاربر واکشی می‌شود و این اطلاعات به صورت یک شی[[84]](#footnote-85) به سمت frontend فرستاده می‌شود

course: {}

async created() {

try {

const response = await axios.get(

`http://127.0.0.1:8000/api/v1/courses/${this.courseId}`

);

this.course = response.data;

} catch (e) {

this.errors.push(e);

}

}

هر دوره از روی آیدی منحصر به فردش شناخته می‌شود و با کد زیر آیدی مربوط به دوره‌ای که کاربر انتخاب کرده جهت واکشی اطلاعات استخراج و ذخیره می‌شود

courseId: this.$route.params.id

* **کد ویژگی :** C04 **|** **بازیگر :** کاربر

**عنوان نیازمندی :** مشاهده صفحه خانه

**توضیح نیازمندی :** این صفحه، صفحه ورودی هر کاربر می‌باشد و شامل دکمه های ورود به صفحه لیست دوره‌های ارائه شده و دکمه ورود به صفحه اضافه کردن دوره به لیست دوره‌های برای انجام می‌باشد

**توضیح فنی به همراه تکه کد :** کد‌های این قسمت فنی نبوده و صرفا طراحی می‌باشد

* **کد ویژگی :** C05 **|** **بازیگر :** کاربر

**عنوان نیازمندی :** امکان ارسال نظر و پیشنهاد

**توضیح نیازمندی :** در قسمت سربرگ سایت دکمه Any Offer وجود دارد که کاربر می‌تواند با کلیک کردن آن پیشنهادات خود را به شکل کاملا ناشناس ارسال کند

**توضیح فنی به همراه تکه کد :** با استفاده از کتابخانه EmailJS ارسال ایمیل انجام می‌گیرد.

sendEmail() { if (this.message.length >= 10)

{emailjs.sendForm("service\_9sjxu8w",

"template\_cut3mh7", this.$refs.form,

"Hmqsuup3nMwM\_91eK");}}

* **کد ویژگی :** C06 **|** **بازیگر :** کاربر

**عنوان نیازمندی :** مشاهده پیام نیاز اتصال به متامسک

**توضیح نیازمندی :** در صورت متصل نبودن کیف پول کاربر از طرق متامسک به سایت، کاربر امکان استفاده از امکانات سایت را نداشته و فقط می‌تواند بدون اتصال کیف پولش دوره‌های تهیه شده را مشاهده نماید در این صورت پیامی به این شکل برای کاربر نمایش داده می‌شود :

**Is [MetaMask](https://metamask.io/" \t "_blank) extension installed on your browser?**

**Is proper network selected in MetaMask?**

**(Rinkeby Test Network or Localhost on port 8545)**

**توضیح فنی به همراه تکه کد :** کد‌های این قسمت فنی نبوده و صرفا طراحی می‌باشد

* **کد ویژگی :** C07 **|** **بازیگر :** کاربر

**عنوان نیازمندی :** اتصال کیف پول کاربر به سایت

**توضیح نیازمندی :** در قسمت سربرگ سایت دکمه Any Offer وجود دارد که کاربر می‌تواند با کلیک کردن آن پیشنهادات خود را به شکل کاملا ناشناس ارسال کند

**توضیح فنی به همراه تکه کد :** با استفاده از کتابخانه EmailJS ارسال ایمیل انجام می‌گیرد

# ابزارها

# جمع‌بندی و نتیجه‌گیری

1. معادل فارسی تعدادی از واژه‏های بیگانه

|  | **واژه بيگانه** | **معادل فارسي** |
| --- | --- | --- |
|  | Associative | انجمني |
|  | Buffer | ميانگير |
|  | Cable | بافه |
|  | Chip | تراشه |
|  | Conductor | رسانا |
|  | Data Sheet | برگه‏ي راهنما |
|  | Flash | درخش |
|  | Gain | بهره |
|  | Global | سراسري، سرتاسري |
|  | Heat sink | گرماخور |
|  | Monitoring | پايش |
|  | Offline | بادرنگ |
|  | Online | بي‏درنگ |
|  | Overhead | فزون‏كاري - سربار |
|  | Pager | پي‏جو |
|  | Paging | پي‏جويي |
|  | Pin | پايه |
|  | Port | درگاه |
|  | Process | فرآيند |
|  | Semiconductor | نيمه‏رسانا |
|  | Soft Computing | رايانش نرم |
|  | Switching | كليدزني، سودهي |
|  | System | سامانه |
|  | Tolerance | رواداري، رواداشت |
|  | Vector | بردار |
|  | اتوماتيك | خودكار |
|  | اخيراً | به‏تازگي |
|  | اكثر(يت) | بيشتر |
|  | اكسترمم | فرينه |
|  | المان (ماتريس) | درايه |
|  | انتخاب | گزينه |
|  | بعضي | برخي |
|  | پالس | تپ |
|  | پروژه، تز | پایان‏نامه، رساله |
|  | پروسسور | پردازنده، پردازشگر |
|  | ترمينال | پايانه |
|  | تست | آزمون، كارآزمايي |
|  | تكامل | فرگشت |
|  | جواب | پاسخ |
|  | خاصيت | ويژگي |
|  | خروجي | برونداد |
|  | خيلي | بسيار |
|  | درحين | هنگام |
|  | راحت | آسان |
|  | راه حل | راهكار |
|  | سمپوزيوم | نشست |
|  | سمينار | هم‏انديشي |
|  | سوال | پرسش |
|  | شروع | آغاز |
|  | ضميمه | پيوست |
|  | فارغ‏التحصيل | دانش‏آموخته |
|  | فركانس | بسامد |
|  | فقط | تنها |
|  | فلوچارت | روندنما |
|  | فيلتر | پالايه |
|  | كامپيوتر | رايانه |
|  | كنگره | همايش |
|  | ماكزيمم | بيشينه |
|  | مالتي پروسسور | چند پردازنده |
|  | المان(ماتريس) | درايه |
|  | متنوع | گوناگون |
|  | مجدداً | دوباره، ازنو |
|  | مدرك | دانش‏نامه |
|  | مقدمه | ديباچه |
|  | ميكروپروسسور | ريزپردازنده |
|  | مينيمم | كمينه |
|  | نويز | نوفه (ف) |
|  | ورودي | درونداد (ف) |

1. واژه‏نامه فارسي-انگليسي

تمامي واژه‏های پانويسي شده در متن بايد يكبار در واژه‏نامه فارسي-انگليسي به ترتيب حروف الفباي فارسي بصورت جدول زير از راست به چپ آورده شود. براي انجام اين‏كار مي‏توانيد از منوي View⇨DocumentView آيكون Draft را انتخاب كرده و سپس از منوي References⇨Footnotes آيكون ShowNotes را انتخاب نماييد تا بتوانيد كليّه پانِوِشت‏ها را يكجا ببينيد. با فشردن ماوس بر روي هر پانِوِشت، معادل فارسي آن در متن در پنجره اصلي قابل رؤيت است و مي‏توانيد عبارت‏ها را تك تك كپي نماييد. سپس مي‏توانيد با برنامه اِكسل آنها را به ترتيب حروف الفباي فارسي مرتب سازي نماييد، و در نهايت، بصورت يك جدول به نرم افزار مايكروسافت ورد بازگردانيد. برای این­که واژه‏نامه کامل باشد، باید در متن پابان­نامه دقت داشته باشید که پانوشت­ها کامل باشند، تا به همان صورت به واژه­نامه منتقل شوند. برای صرفه‏جویی می‏توانیم واژه‏نامه را به صورت دوستونی بنویسیم. برای این کار بعد از اتمام این متن یک Section Break (Continuous) گذاشته و فرمت بعد از آن را به صورت دو ستونی تعریف می‏کنیم. باید دقت کنیم که عرض دو ستون و فاصله بین آن‏ها نباید از عرض متن نوشته اصلی بیشتر شود.

| Equivalent English | واژه فارسی |
| --- | --- |
| Superscript | بالانويس |
| Footnote | پانِوِشت، پانویس |
| Endnote | پايان‏نِوِشت |
| Database | پايگاه داده |
| Subscript | پایین‏نویس، اندیس |
| Bold | پررنگ |
| Full Width at half Maximum | پهنای کامل نیم‏بیشینه |
| Link to previous | پیوند با قبل |
| Single line | تك سطر |
| Page Setup | چینش صفحه |
| Italic | خوابیده |
| Even | زوج |
| Sub-headings | زيرفصل‏ها |
| Style | سبك |
| Heading | سرفصل |
| Gutter | شيرازه |
| Template file | فايل قالب |
| Odd | فرد |
| Regular font | فونت عادی |
| Font | قلم |
| Border | مرز، سرحد |

1. واژه‏نامه انگليسي-فارسي

بطور مشابه واژه‏های پانويسي شده بايد در اينجا به ترتيب حروف الفباي انگليسي و از چپ به راست آورده شود. اگر بخواهید هر دو ستون به ترتیب هم نوشته گرفته و این‏طور نباشد که یک ستون پرشده و بعد در دومی مطلب نوشته شود. در خط بعد از جدول نیز یک Section Break (Continuous) بگذارید تا مطابق زیر دو ستون به طور موازی نوشته شوند.

| Equivalent English | واژه فارسی |
| --- | --- |
| Bold | پررنگ |
| Border | مرز، سرحد |
| Database | پايگاه داده |
| Database | پايگاه داده |
| Endnote | پايان‏نِوِشت |
| Endnote | پايان‏نِوِشت |
| English Word | معادل فارسی |
| Even | زوج |
| Font | قلم |
| Font | قلم |
| Footnote | پانِوِشت، پانویس |
| Footnote | پانِوِشت، پانویس |
| Full Width at half Maximum | پهنای کامل نیم‏بیشینه |
| Full Width at half Maximum | پهنای کامل نیم­بیشینه |
| Gutter | شيرازه |
| Gutter | شيرازه |
| Heading | سرفصل |
| Headings | فصل‏ها |
| Italic | خوابیده |
| Link to previous | پیوند با قبل |
| Odd | فرد |
| Page Setup | چینش صفحه |
| Regular font | فونت عادی |
| Single line | تك سطر |
| Single line | تك سطر |
| Style | سبك |
| Styles | سبك |
| Sub-headings | زيرفصل‏ها |
| Sub-headings | زيرفصل‏ها |
| Subscript | پایین‏نویس، اندیس |
| Superscript | بالانويس |
| Superscript | بالانويس |
| Template file | فايل قالب |
| Template file | فايل قالب |

1. نكته‏های قابل توجه در ارائه شفاهي

در جلسه ارائه سمينار يا دفاع از پایان‏نامه نكات زير را در نظر بگيريد:

1. مدّت زمان اعلام شده براي ارائه دقيقاً رعايت شود.
2. تعداد اسلايد‌ها حداكثر يك تا 2/1 برابر زمان داده شده به دقيقه باشد.
3. اسلايدها داراي عنوان در بالاي هر كدام و شماره اسلايد از كلّ اسلايدها در پايين (مثلاً  
   «6 از 25») باشد.
4. سعي شود از قلم‏هاي تا حد ممكن بزرگ استفاده شود و تلاش شود تعداد خطوط در يك اسلايد از 5 تا 6 خط تجاوز نكند.
5. بهتر است اسلايدها با زمينه روشن و قلم‏ها با رنگ تیره باشد. (براي تبديل رنگ متن معادله‏ها به رنگ دلخواه بايد از قابليّت recolor كه تنها در PowerPoint 2003 وجود دارد استفاده نماييد.)
6. بجاي جمله‏های كامل، از عبارت‏های ناقص كوتاه بصورت شماره‏دار يا گوی[[85]](#footnote-86)دار استفاده شود.
7. داراي فهرست مطالب و نتيجه‏گيري باشد.
8. فهرست راهكارهاي قابل انجام در ادامه تحقيقات در زمينه مورد بحث ارائه شود.

در دفاع پایان‏نامه، فهرست نوآوري­ها و مقاله‏های ارسال شده ارائه شود.

فهرست مرجع‏ها

|  |  |
| --- | --- |
| [1] | G. E. D. a. F. A. Paganini, A course in robust control theory: A convex approach, New York, NY: Springer, 2000. |
| [2] | T. Mendyk-Krajewska and Z. Mazur, "Problem of network security threats," *3rd International Conference on Human System Interaction,* pp. 436 - 443, 2010. |
| [3] | A. Galves, "Bezier Curve and Surface Fitting of 3D Point Clouds Through Genetic Algorithms, Functional Networks and Least-Squares Approximation," 2007. |
| [4] | Fibikova, Lenka, Müller, Roland and Pohlmann, Norbert, "A Simplified Approach for Classifying Applications," *ISSE 2010 Conference on Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe,* pp. 39-49, 2010. |
| [5] | R. Etges and K. McNeil, "Understanding data classification based on business and security," *ISACA Information Systems Control Journal,* vol. 5, 2006. |
| [6] | R. Etges and K. McNeil, "Understanding data classification based on business and security," *ISACA Information Systems Control Journal,* vol. 5, 2006. |
| [7] | E. Bergström and R.-M. Åhlfeldt, "Information classification issues," *Nordic Conference on Secure IT Systems,* pp. 27-41, Springer International Publishing, 2014. |
| [8] | J. L. Bayuk, "The utility of security standards," *44th Annual IEEE International Carnahan Conference on Security Technology,* pp. 1-6, 2010. |

**Abstract**

In this thesis, we …



**K. N. Toosi University of Technology**

**Faculty of** Choose an item. **Engineering**

**A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of** Choose an item.

**in** Choose an item. **Engineering -** Choose an item.

[Thesis Title]

**By:**

[student name]

**Supervisor:**

[supervisor name(s)]

**Advisor:**

[advisor name(s)]

Spring 2010

1. E-learn [↑](#footnote-ref-2)
2. Covid-19 [↑](#footnote-ref-3)
3. Course [↑](#footnote-ref-4)
4. Deadline [↑](#footnote-ref-5)
5. Platform [↑](#footnote-ref-6)
6. Blockchain [↑](#footnote-ref-7)
7. Smart Contracts [↑](#footnote-ref-8)
8. Ethereum [↑](#footnote-ref-9)
9. Financial Incentive [↑](#footnote-ref-10)
10. Django [↑](#footnote-ref-11)
11. Metamask [↑](#footnote-ref-12)
12. Solidity [↑](#footnote-ref-13)
13. Information [↑](#footnote-ref-14)
14. Storage [↑](#footnote-ref-15)
15. Data [↑](#footnote-ref-16)
16. Charles Babbage [↑](#footnote-ref-17)
17. fetching [↑](#footnote-ref-18)
18. Centralized Systems [↑](#footnote-ref-19)
19. UnDistributed [↑](#footnote-ref-20)
20. Hack [↑](#footnote-ref-21)
21. Open Source [↑](#footnote-ref-22)
22. Apache [↑](#footnote-ref-23)
23. Decentralize [↑](#footnote-ref-24)
24. Developer [↑](#footnote-ref-25)
25. Cloud Service Provider [↑](#footnote-ref-26)
26. Cloudflare [↑](#footnote-ref-27)
27. Distributed [↑](#footnote-ref-28)
28. Server [↑](#footnote-ref-29)
29. Bitcoin [↑](#footnote-ref-30)
30. Crypto Currency [↑](#footnote-ref-31)
31. Blockchain [↑](#footnote-ref-32)
32. Distributed Ledger [↑](#footnote-ref-33)
33. مجموعه‌ای از عملیات که مانند یک واحد منطقی عمل می‌کنند به طور مثال انتقال پول در بانک که شامل مجموعه عملیات{ کم شدن از یک حساب - انتقال - اضافه شدن به حساب دیگر } مجموعا یک تراکنش محسوب می‌شوند، تراکنش‌ها لزوما مالی نبوده، رای دادن و یا انتقال مالکیت و ... نیز تراکنش به حساب می‌آیند [↑](#footnote-ref-34)
34. Node [↑](#footnote-ref-35)
35. State [↑](#footnote-ref-36)
36. Atomic [↑](#footnote-ref-37)
37. Consistent [↑](#footnote-ref-38)
38. Balance [↑](#footnote-ref-39)
39. Durable [↑](#footnote-ref-40)
40. Distributed Ledger Technology [↑](#footnote-ref-41)
41. Block [↑](#footnote-ref-42)
42. Genesis block [↑](#footnote-ref-43)
43. Stuart Haber [↑](#footnote-ref-44)
44. w. scott stornetta [↑](#footnote-ref-45)
45. Timestamping [↑](#footnote-ref-46)
46. Host [↑](#footnote-ref-47)
47. Fork [↑](#footnote-ref-48)
48. Full node [↑](#footnote-ref-49)
49. Pruned nodes [↑](#footnote-ref-50)
50. Archival nodes [↑](#footnote-ref-51)
51. در گره هرس شده به حداقل یک ترابایت حافظه پر سرعت نیاز داریم و در گره بایگانی به حداقل دوازده ترابایت [↑](#footnote-ref-52)
52. Mining node [↑](#footnote-ref-53)
53. Proof of work [↑](#footnote-ref-54)
54. Lightweight node [↑](#footnote-ref-55)
55. Broadcast [↑](#footnote-ref-56)
56. Body [↑](#footnote-ref-57)
57. Hash [↑](#footnote-ref-58)
58. Data structure [↑](#footnote-ref-59)
59. Merkle tree [↑](#footnote-ref-60)
60. Satoshi (1 satoshi = 0.00000001 BTC) [↑](#footnote-ref-61)
61. Transaction Fees [↑](#footnote-ref-62)
62. Unspent Transaction Output (UTXO) [↑](#footnote-ref-63)
63. double spending [↑](#footnote-ref-64)
64. Coinbase [↑](#footnote-ref-65)
65. BTC ( The Cryptocurrency of The Bitcoin Blockchain) [↑](#footnote-ref-66)
66. Digital signature [↑](#footnote-ref-67)
67. Asymmetric cryptography [↑](#footnote-ref-68)
68. non-repudiation [↑](#footnote-ref-69)
69. Validation [↑](#footnote-ref-70)
70. Encryption [↑](#footnote-ref-71)
71. Decryption [↑](#footnote-ref-72)
72. User stories [↑](#footnote-ref-73)
73. Software Requirements Document [↑](#footnote-ref-74)
74. Agile software development [↑](#footnote-ref-75)
75. بخش انتهایی داستانه‌های کاربر اختیاری است [↑](#footnote-ref-76)
76. cryptocurrency [↑](#footnote-ref-77)
77. Ether (رمزارز شبکه اتریم) [↑](#footnote-ref-78)
78. Crypto wallet [↑](#footnote-ref-79)
79. Chrome – Firefox – Brave - Edge [↑](#footnote-ref-80)
80. Button [↑](#footnote-ref-81)
81. Header [↑](#footnote-ref-82)
82. Array [↑](#footnote-ref-83)
83. Box [↑](#footnote-ref-84)
84. Object [↑](#footnote-ref-85)
85. Bullet [↑](#footnote-ref-86)