

دانشکده مهندسی کامپیوتر

**پروژه مقطع کارشناسی مهندسي کامپیوتر**

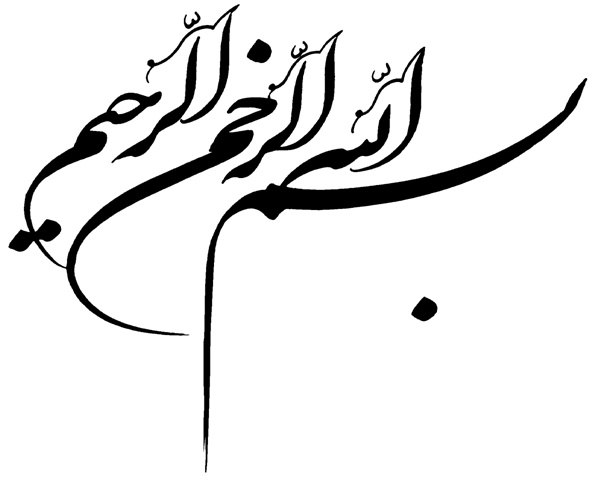
Smart contract generation on Elearn

ایمان عباسی‌زاده

**استاد راهنما:**

دکتر علائیان

**[تاریخ دقیق روز، ماه و سال دفاع]**



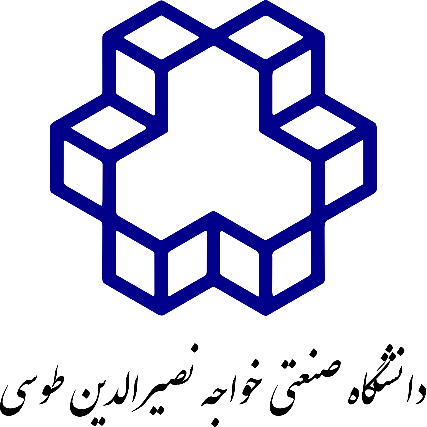
# تأييديّه هيات داوران

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[[13]](#footnote-14) لزوم استفاده از دوره های آنلاین[[14]](#footnote-15) در جهان به مسئله جدی تبدیل شد و پلتفرم[[15]](#footnote-16) 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.

1. **تحقق 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 اصل جز اساسی ترین انگیزه ها برای شکل‌گیری این پلتفرم می‌باشد.
2. **ایجاد انگیزه در کاربر[[16]](#footnote-17) برای تکمیل دوره های آنلاین اخذ کرده:** در شرایطی که فراگیر دوره آنلاین به صورت خودخواسته دوره[[17]](#footnote-18) 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[[18]](#footnote-19) که در این پلتفرم طراحی شده امکان تعیین موعد ‌‌مقرر ‌زمانی[[19]](#footnote-20) برای انجام ، تنبیه و تشویق مالی توسط خود کاربر برای دوره هایش، چه دورهای ارائه شده توسط پلتفرم و چه دوره های دیگر کاربر، درصورت عدم تکمیل دوره در زمان مقرر را فراهم نموده.
3. **ناشناس بودن کاربران و حفظ حریم شخصی :** در دنیای امروز که اکثر شرکت ها و موسسات در تلاش برای کسب اطلاعات هرچه بیشتر کاربران خود در جهت استفاده های تبلیغاتی، جامعه شناختی، تحلیلی و ... می‌باشند، پلتفرم smartlearn در خلاف جهت این موج سعی بر حفظ هویت افراد و آزادی عمل کاربران خود با بهره گیری از تکنولوژی بلاکچین[[20]](#footnote-21) دارد. این جهت‌گیری از انگیزه های مهم شکل‌گیری این پلتفرم و همچنین از دلایل استفاده smartlearn از بلاکچین برای ذخیره‌سازی اطلاعات کاربران خود است.

## تبیین مسئله

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

1. ارائه دوره های آنلاین ترجمه شده به صورت رایگان و قابل دسترس برای تمامی کاربران
2. ارائه امکانی برای ثبت دوره‌ها، تعیین موعد مقرر زمانی و تنبیه و تشویق مالی و مدیریت دوره های برای انجام به کمک قرارداد هوشمند

بخش اول این پلتفرم به مانند سایت ها و بسترهای فعال در زمینه آموزش آنلاین اما با رویکرد تحقق آرمان آموزش بدون تبعیض، دوره هایی ترجمه شده به زبان مقصد کاربر، در حال حاضر به زبان فارسی، 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 انگیزشی[[21]](#footnote-22) از نوع مالی در جهت اتمام دوره های اخذ شده کاربر می‌باشد. به کمک قرارداد هوشمندی که در این بخش طراحی شده کاربر 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 موعد مقرر زمانی و جایزه[[22]](#footnote-23) 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[[23]](#footnote-24) داشته که برای پاسخ به این نیاز یک سازوکار[[24]](#footnote-25) پایا[[25]](#footnote-26) 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[[26]](#footnote-27) توسط ساتوشی ناکاموتو[[27]](#footnote-28) بر پایه فناوری بلاکچین در سال ۲۰۰۸ میلادی نگاه جدی‌تری به سیستم های غیرمتمرکز و بهره‌‌وری از این سیستم‌ها شد، تا در سال ۲۰۱۵ بلاکچین اتریوم[[28]](#footnote-29) توسط ویتالیک بوترین[[29]](#footnote-30) و کوین وود[[30]](#footnote-31) 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 سیستم‌های غیر متمرکز به صورت جدی‌تری دنبال شد، پلتفرم smartlearn نیز هم‌جهت 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 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 پایگاه داده[[31]](#footnote-32) 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 نیازمندی‌های پروژه[[32]](#footnote-33)، نمودار های کلاس دیاگرام[[33]](#footnote-34) و بلاک دیاگرام[[34]](#footnote-35) و نمودار رابطه-موجودیت[[35]](#footnote-36) 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

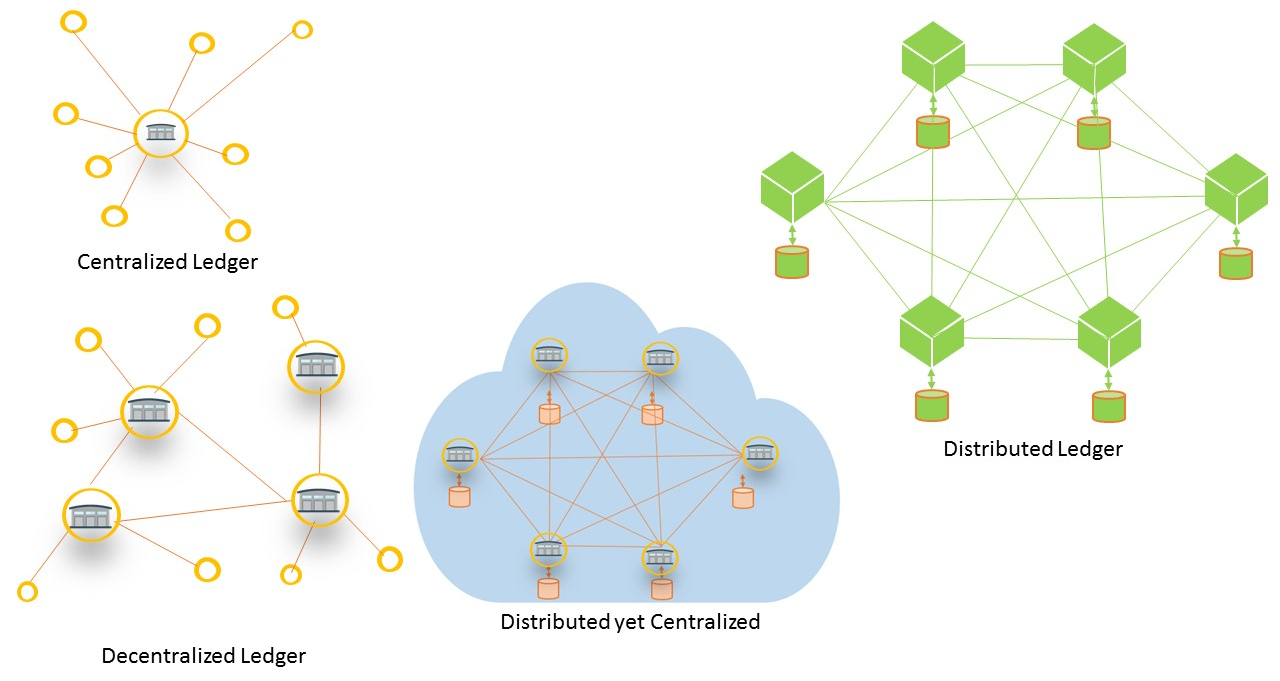
## مقدمه

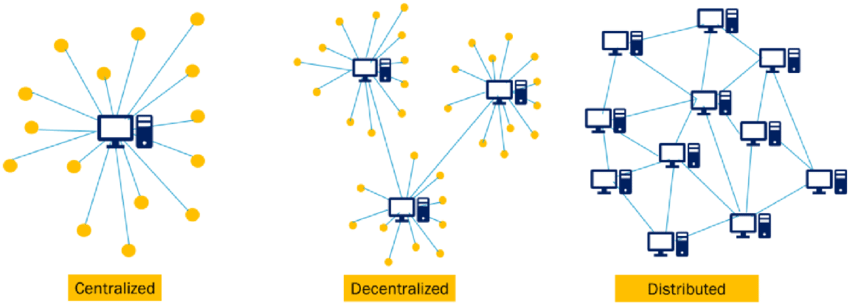
ثبت اطلاعات[[36]](#footnote-37) جهت دسترسی و ماندگاری اطلاعات از زمان آشنایی انسان با علم در حدود 3000 سال پیش از میلاد مسیح بر روی لوح های رسی/گلی انجام می‌گرفت [1]، با پیشرفت علم وسیله و شیوه ذخیره‌سازی[[37]](#footnote-38) داده[[38]](#footnote-39) تغییر و بهبود یافت تا با اختراع کامپیوتر در سال 1871 توسط چارلز بابیج[[39]](#footnote-40) مسیری جدید به روی انسان گشوده شد [2]، مسیری که دنیای امروز وام‌دار آن است و مسئله ذخیره‌سازی و واکشی[[40]](#footnote-41) 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[[41]](#footnote-42) به معنای کنترل اطلاعات به شکل واحد زیر نظر و حاکمیت یک شخص یا شرکت و همچنین مشترک یا توزیع نشده[[42]](#footnote-43) 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[[43]](#footnote-44) 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[[44]](#footnote-45)ی مثل آپاچی[[45]](#footnote-46) نمونه ای از یک سیستم غیرمتمرکز[[46]](#footnote-47) ولی توزیع نشده است که به صورت غیرمتمرکز و با کمک جمیع افراد توسعه‌دهنده[[47]](#footnote-48) سراسر جهان توسعه داده می‌شود ولی همچنان معضلات یک سیستم توزیع نشده را به همراه دارند از سوی دیگر سیستم‌های خدمات دهنده ابری[[48]](#footnote-49) مانند کلودفلر[[49]](#footnote-50) توزیع شده[[50]](#footnote-51) بوده و دارای سرور[[51]](#footnote-52)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[[52]](#footnote-53) به عنوان اولین رمزارز[[53]](#footnote-54) جهان بر پایه تکنولوژی بلاکچین[[54]](#footnote-55) که یک نوع دفتر کل حساب توزیع شده[[55]](#footnote-56) 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.





gg

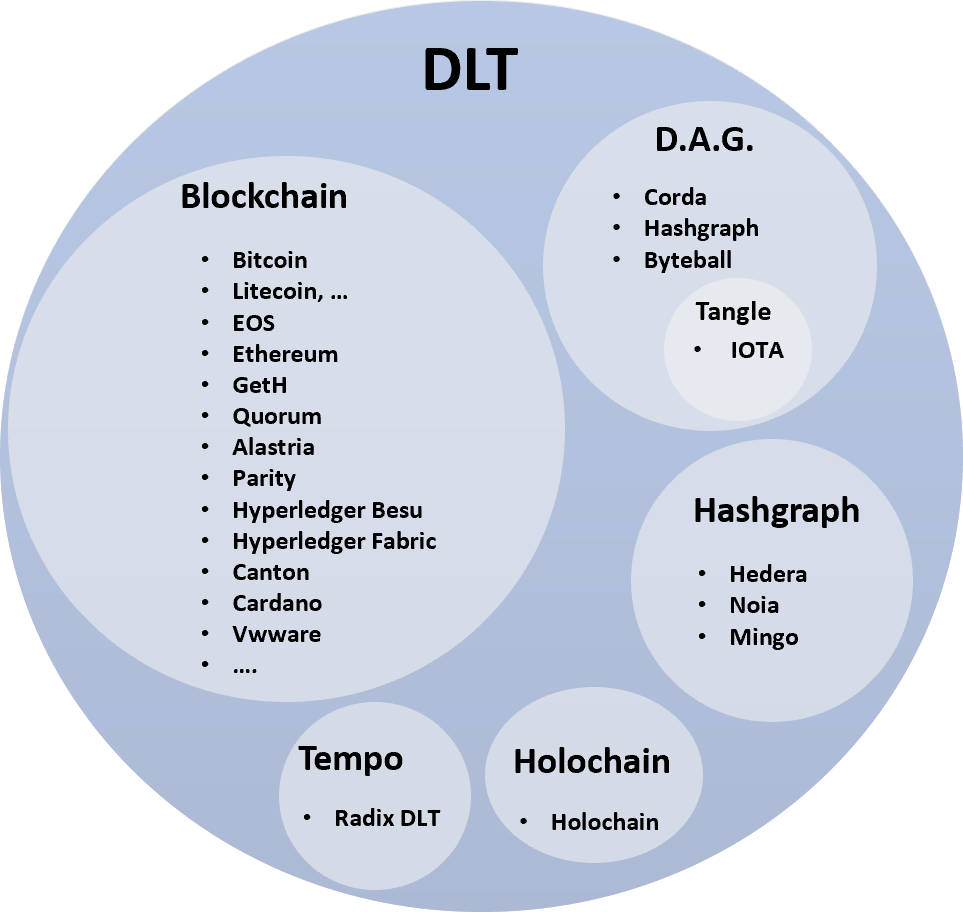
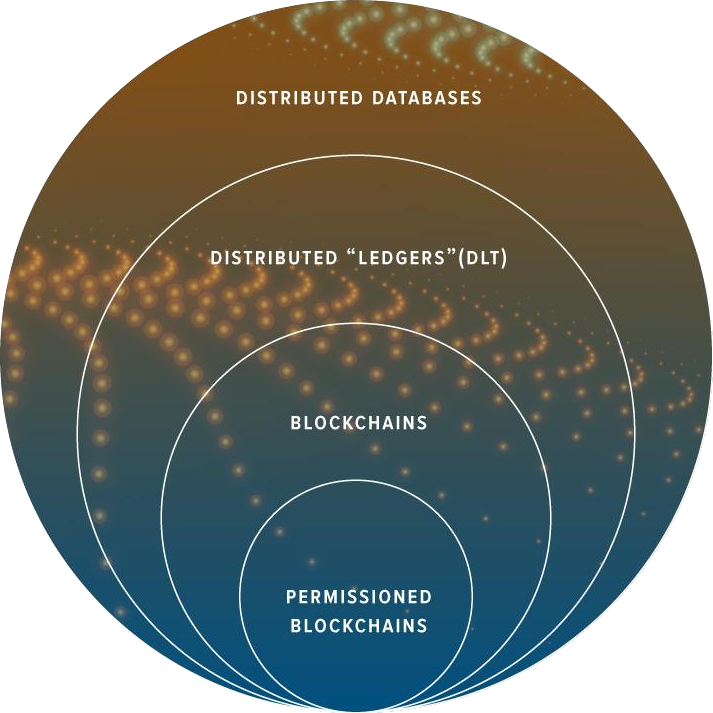
## دفتر کل حساب توزیع شده

دفتر کل حساب توزیع شده یک نمونه خاص از پایگاه داده توزیع شده است که تراکنش‌ها[[56]](#footnote-57) در آن به صورت توزیع شده ثبت می‌شوند، در یک دفتر کل حساب توزیع شده تمامی نودها[[57]](#footnote-58) باید یک نسخه یکسان از دفتر حساب داشته باشند و برای تغییر یا ثبت اطلاعات جدید، نودها باید روی حالت[[58]](#footnote-59) جدید توافق کنند.

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

1. **اتمیک[[59]](#footnote-60) :** به معنی انجام تمامی عملیات یک تراکنش است که درصورت انجام نشدن یک عملیات کل تراکنش انجام نشده تلقی می‌شود
2. **با ثبات[[60]](#footnote-61) :** 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[[61]](#footnote-62) مالی بانک ثابت می‌ماند
3. **پایا[[62]](#footnote-63) :** 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 [[63]](#footnote-64) نامیده می‌شود خود شامل انواع تکنولوژی‌های مختلفی است که شناخته شده‌ترین آن تکنولوژی بلاکچین است.



jk

## بلاکچین

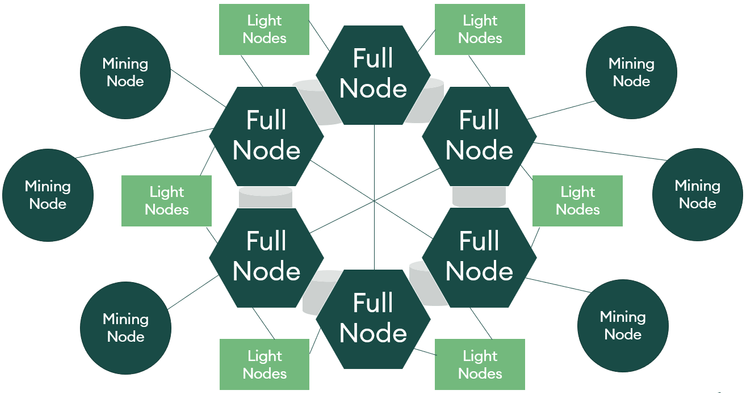
بلاکچین به عنوان مطرح‌ترین نوع دفتر کل حساب توزیع شده, زنجیره ای از بلوک‌[[64]](#footnote-65)ها است که هر بلوک حاوی تعدادی تراکنش و داده می‌باشد که به بلوک قبلی اشاره دارد، این زنجیره ادامه پیدا می‌یابد تا به اولین بلوک ایجاد شده به نام بلوک پیدایش[[65]](#footnote-66) برسد.

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[[66]](#footnote-67) و اسکات استورنتا[[67]](#footnote-68) پایه‌ریزی شد و بلاکچین را به عنوان یک راه حل عملی محاسباتی برای زدن برچسب زمانی[[68]](#footnote-69) 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[[69]](#footnote-70) یا اتصال به آن سخت‌افزار خاصی نیاز است. [3]

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[[70]](#footnote-71) و یا در حالت جدی‌تر به ایجاد یک بلاکچین جدید می‌انجامد.



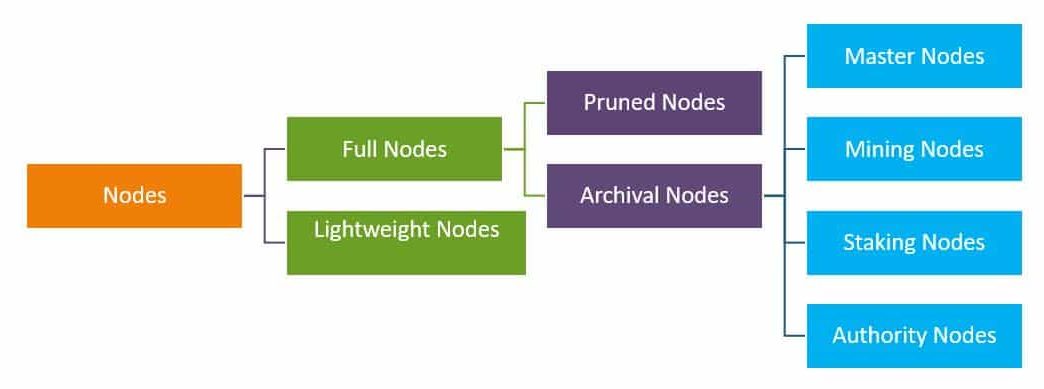
kk

گره‌ها به دو دسته کلی تقسیم می‌شوند :

1. **گره‌های کامل[[71]](#footnote-72) :** 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[[72]](#footnote-73) و گره‌های بایگانی[[73]](#footnote-74) تقسیم‌بندی می‌شوند و تفاوت این دو گره در میزان ذخیره‌سازی آن‌ها است[[74]](#footnote-75)، گره‌های هرس شده ابتدا باید کل بلاکچین را از ابتدا طی کند و تمام بلوک‌های قبلی را تایید کند تا بتواند تراکنش‌های جدید را از نظر مقادیر ورودی، امضا فرستنده و موجودی کافی جهت انجام تراکنش اعتبارسنجی نماید.

* گره استخراج[[75]](#footnote-76) یک گره کامل از نوع گره بایگانی است که امکان تایید و استخراج بلوک از طریق اجماع اثبات کار[[76]](#footnote-77) دارد.

1. **گره‌های سبک وزن[[77]](#footnote-78) :** 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[[78]](#footnote-79) تراکنش در شبکه امکان تعامل کاربر با بلاکچین را نظیر ارسال، دریافت و امضا تراکنش‌ها برقرار می‌کند.



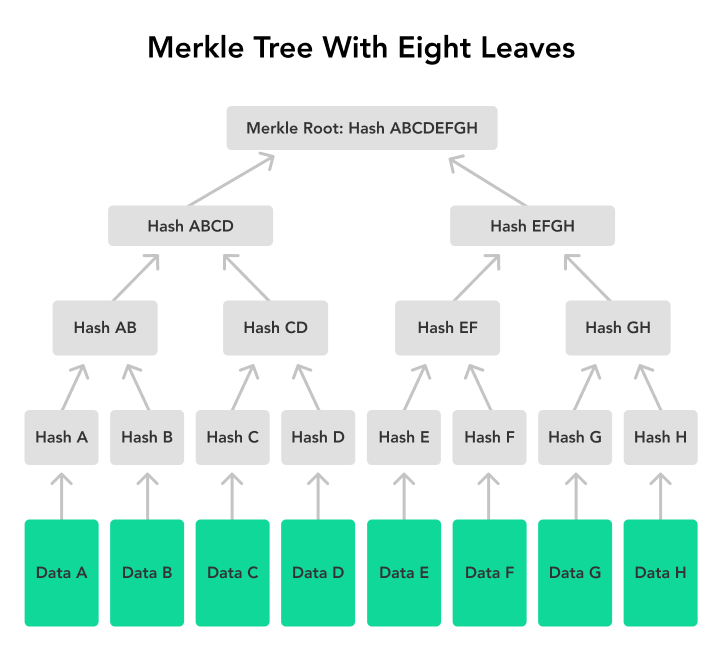
hh

### 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[[79]](#footnote-80) تشکیل می‌شوند:

* **بدنه :** بدنه هر بلوک شامل لیست تراکنش‌هایی است که هش[[80]](#footnote-81) هر یک با الگوریتم[[81]](#footnote-82) مخصوصی، در بیت‌کوین با الگوریتم SHA256، محاسبه شده و با ساختمان داده[[82]](#footnote-83) درخت مرکل[[83]](#footnote-84) ذخیره شده اند.

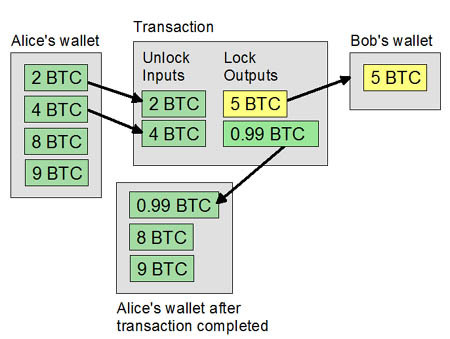


gg

هر تراکنش، که در شبکه بیت‌کوین منظور تراکنش صرفا مالی است، شامل آدرس فرستنده، آدرس گیرنده، تعداد ساتوشی[[84]](#footnote-85) و کارمزد تراکنش[[85]](#footnote-86) 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[[86]](#footnote-87) [4] جهت تایید میزان موجودی کافی برای انجام تراکنش و همچنین برای جلوگیری از خرج مجدد[[87]](#footnote-88) و افزایش امنیت استفاده می‌کند.

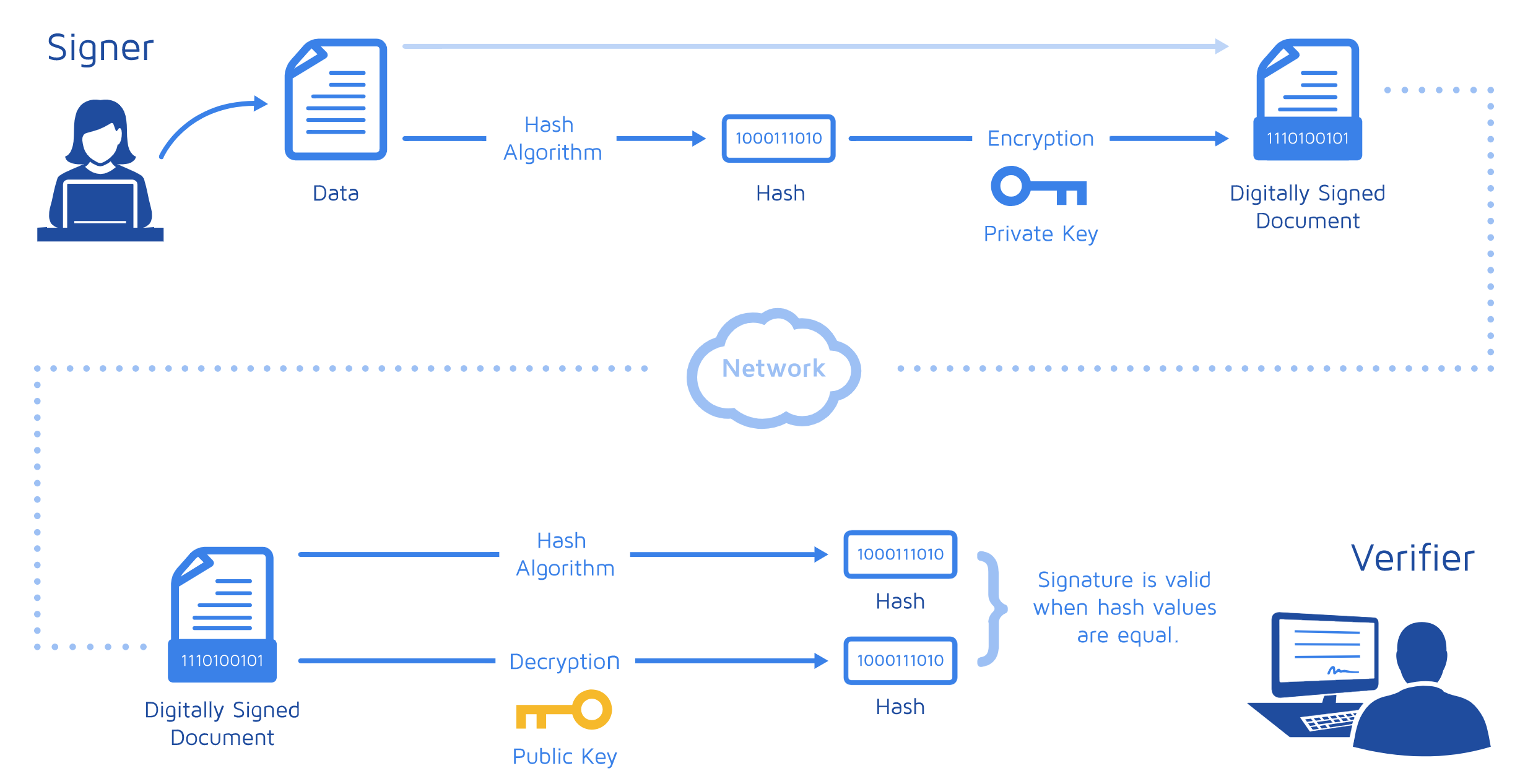
یک آدرس کیف پول از سه طریق موجودی بدست می‌آورد یا از طریق پاداشی است که از استخراج بلوک[[88]](#footnote-89) منتقل شده یا از آدرس دیگری انتقال صورت گرفته و یا به عنوان باقی مانده تراکنش به همان آدرس بازگردد، در هر صورت هر مقدار بیت‌کوین[[89]](#footnote-90) انتقال شده و موجود در آدرس کیف پول یک UTXO است، گره‌های شبکه زمان درخواست انجام یک تراکنش موجودی آدرس فرستنده تراکنش را بررسی می‌کنند تا مطمئن شوند UTXO کافی برای انجام تراکنش وجود دارد.



ff

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[[90]](#footnote-91) استفاده می‌کند، امضا دیجیتال توسط رمزنگاری نامتقارن[[91]](#footnote-92) پیاده‌سازی شده و غیرقابل انکار[[92]](#footnote-93) است و گره‌های شبکه مسئولیت صحت‌سنجی[[93]](#footnote-94) به عهده دارند.



dd

مطابق شکل بالا ابتدا هش تراکنش با کلید خصوص فرستنده تراکنش رمز می‌شود[[94]](#footnote-95) 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[[95]](#footnote-96) کرده و هش بدست آمده را با هش تراکنش مقایسه می‌کنند که در صورت یکی بودن این دو امضا تایید می‌شود.

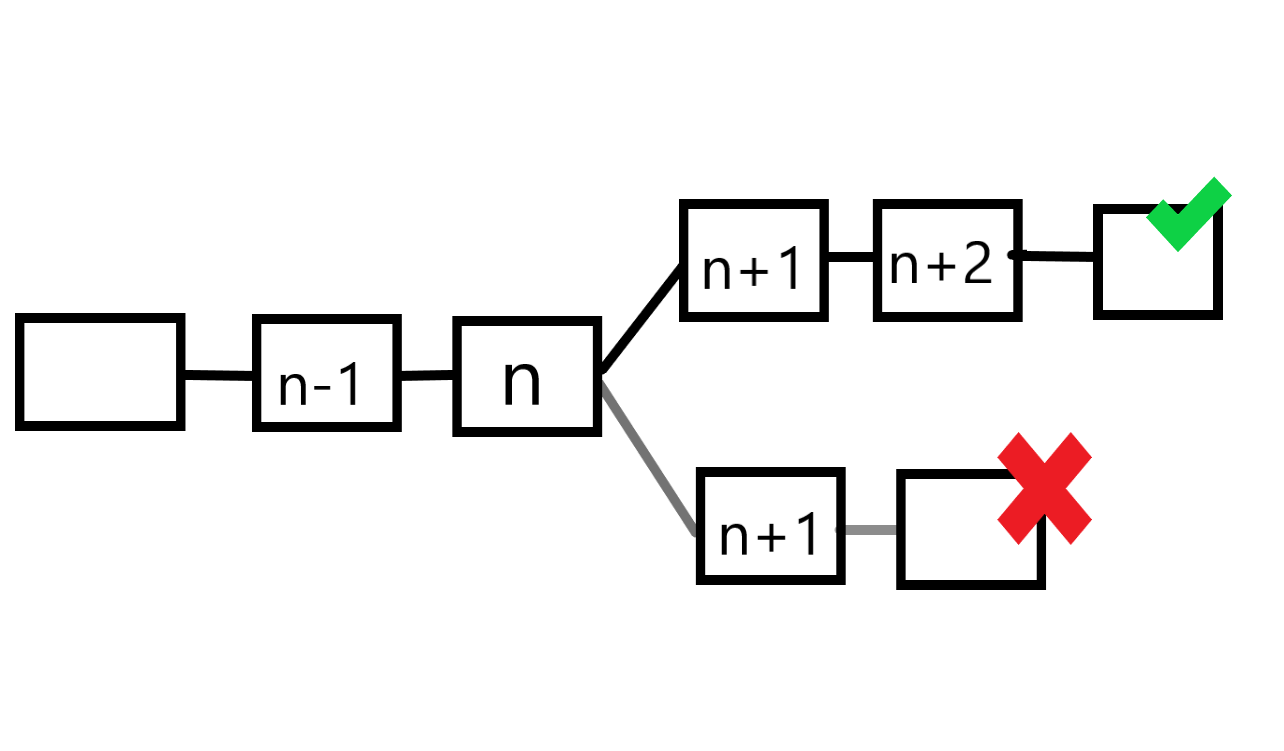
* **سربرگ :** سربرگ هر بلوک حاوی اطلاعاتی شامل سختی شبکه[[96]](#footnote-97)، عدد نانس[[97]](#footnote-98)، هش بلوک قبلی، هش خود بلوک، ریشه درخت مرکل تراکنش‌ها، مهر زمانی[[98]](#footnote-99)، نسخه بلاکچین[[99]](#footnote-100) و شماره بلوک است که در ادامه به توضیح دو مورد اول، سختی شبکه و عدد نانس می‌پردازیم اما قبل از آن باید شناختی نسبت به سازوکاری به نام اثبات کار[[100]](#footnote-101) پیدا کنیم.

همانطور که در قسمت گره‌ها بیان شد گره استخراج وظیفه تایید و استخراج بلوک برای قرارگیری در بلاکچین را دارد که با انجام این کار گره استخراج کننده پاداش دریافت می‌کند برای تعیین این که به کدام گره پاداش تعلق می‌گیرد نیاز به یک توافق یا اجماع میان گره‌ها داریم.

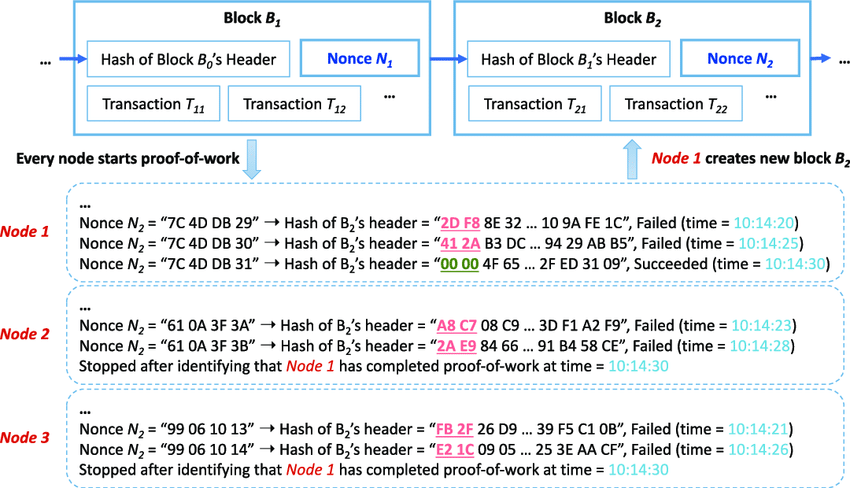
از آنجایی که ماهیت بلاکچین غیرمتمرکز و توزیع شده بوده و هر گره استقلال و آزادی عمل خود را دارد سازوکار اجماع[[101]](#footnote-102) بکارگرفته شده باید قابلیت تحمل خطای بیزانسی[[102]](#footnote-103) را نیز داشته باشد.

با توجه به مطالب بیان شده و نیاز به یک سازوکار اجماع، بلاکچین بیت‌کوین از سازوکار اثبات کار استفاده می‌کند و این شبکه را در مقابل خطای بیزانسی درصورتی که حداکثر یک سوم از گره‌ها غایب و یا خائن باشند مقاوم می‌کند.

سازوکار اثبات کار در سال ۱۹۹۳ و برای جلوگیری از ارسال هرزنامه‌ها[[103]](#footnote-104) با درگیر کردن پردازنده[[104]](#footnote-105) ارسال- کننده جهت هزینه‌بر کردن ارسال ایمیل[[105]](#footnote-106) بوجود آمد ولی مطرح شدن آن به واسطه بلاکچین انجام گرفت، در بلاکچین به این گونه است؛ شبکه بلاکچین تحت عنوان سختی شبکه تعیین میکند که هش بلوکی که مجاز است به بلاکچین اضافه شود باید شرایط خاصی داشته باشد، به طور مثال ۴ کاراکتر[[106]](#footnote-107) اول آن صفر باشد[[107]](#footnote-108)، سپس گره‌های استخراج برای اضافه کردن این بلوک باید عددی تحت عنوان عدد نانس حدس بزنند[[108]](#footnote-109) که هش بلوک طبق آن شرایط بدست بیاید، اولین گره‌ای که بتواند این عدد را به درستی بدست آورد آن بلوک را استخراج کرده و به بلاکچین اضافه می‌شود و همچنین پاداش به همراه کارمزدهای تراکنش‌های موجود در ان بلوک را بدست می‌اورد، در صورتی که دو گره همزمان دو گره دو بلوکی را استخراج که هر دو به بلوک قبلی اشاره می‌کنند، هر دو به بلاکچین اضافه می‌شوند که در اینجا یک انشعاب موقت[[109]](#footnote-110) رخ می‌دهد و آن بلوکی در شبکه میماند که بلوک‌های بیشتری به آن متصل شوند به عبارتی طولانی‌ترین زنجیر[[110]](#footnote-111) در شبکه ادامه پیدا می‌کند و به بلوک یا بلوک‌های در زنجیر ادامه نیافته به اصطلاح بلوک یتیم[[111]](#footnote-112) گفته می‌شود [5].

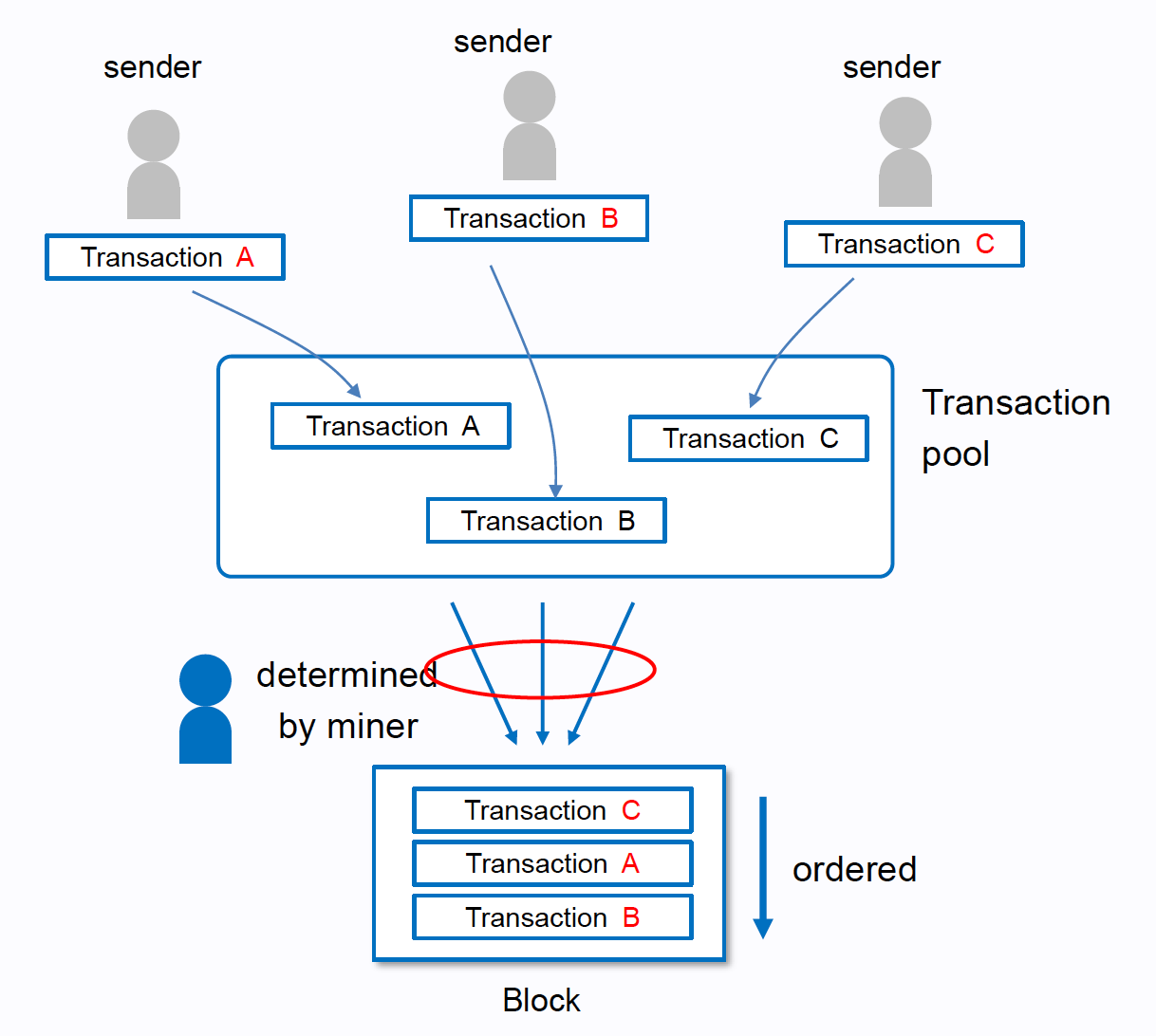
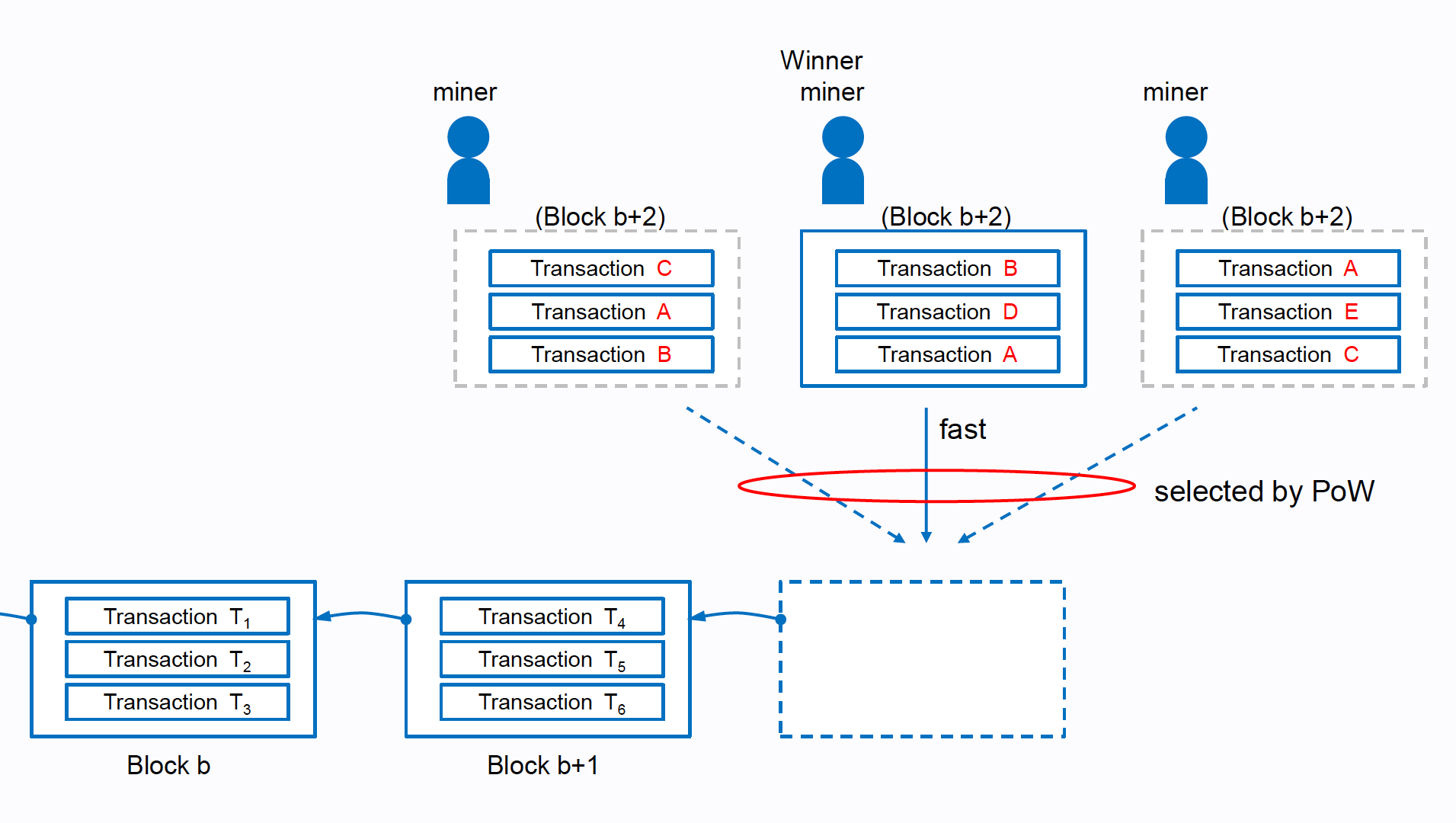


kj



Dd

در هر بلوک که گره‌های استخراج سعی در اضافه کردن آن به بلاکچین دارند تعدادی تراکنش وجود دارد؛ این تراکنش‌ها بعد از ایجاد در جایی به نام استخر تراکنش‌ها[[112]](#footnote-113) قرار می‌گیرند و گره‌های استخراج از آنجا تراکنش‌ها را با توجه به میزان کارمزد هر تراکنش و مسائل دیگر به بلوکی که قصد اضافه کردن آن به بلاکچین را دارند اضافه می‌کنند.



Kk

سرعت اضافه شدن بلوک به بلاکچین در هر بلاکچینی متفاوت است به طور مثال در بیت‌کوین متوسط زمان اضافه شدن هر بلوک باید ۱۰ دقیقه باشد که برای تنظیم آن از سختی شبکه استفاده می‌شود، سختی شبکه با توجه به سرعت استخراج کنندگان هر چند مدت تغییر می‌کند که برای بیت کوین هر ۲۰۱۶ بلوک که ۲ هفته می‌شود[[113]](#footnote-114) بررسی می‌شود و سختی شبکه کم یا زیاد می‌شود.

### ویژگی‌ها

یک شبکه بلاکچین به علت غیرمتمرکز و توزیع شده بودن آن علاوه بر مزایای این نوع سیستم‌ها که امنیت و استقلال شبکه را به ارمغان می‌اورد به علت سازوکار ویژه ای که در بلاکچین تعبیه شده است ویژگی‌های کارآمد و خاصی را برای کاربرانش خواهد داشت

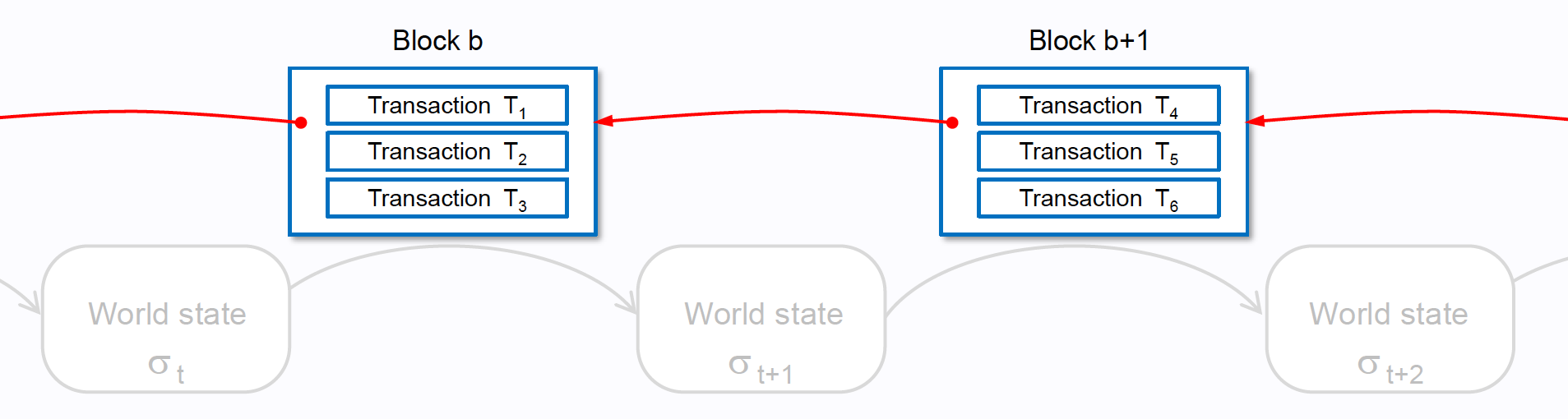
## اتریوم و قراردادهای هوشمند

آنچه تا اینجا بیان شد مربوط به بلاکچین بیت‌کوین بود که اکثر مطالب و منطق کلی آن بین تمام بلاکچین‌ها یکسان است، در این قسمت قصد داریم بلاکچین اتریوم[[114]](#footnote-115) را به عنوان مهمترین بلاکچین بعد از بیت‌کوین با قابلیت تعریف و اجرای قراردادهای هوشمند بررسی کنیم ولی قبل از آن یک تعریف جامع از بلاکچین اتریوم داشته باشیم به این شکل است که در اصل اتریوم تلفیق دو تکنولوژی بلاکچین و ماشین مجازی محاسباتی[[115]](#footnote-116) بوده که قادر به اجرای بدون وقفه[[116]](#footnote-117) و تغییرناپذیر[[117]](#footnote-118) هر برنامه کامپیوتری است [5].

### ساختار داده و انواع حساب در اتریوم

سازوکار بلاکچین اتریوم به طور کلی مانند سازوکار بلاکچین بیت‌کوین است ولی تفاوت‌های مهمی بین این دو بلاکچین وجود دارد که هر یک را متمایز از دیگری می‌کند یکی از این تمایزها استفاده اتریوم از ساختارداده‌ای از ترکیب دو ساختمان داده درخت مرکل و درخت پیشوندی[[118]](#footnote-119) و الگوریتم عملی برای بازیابی اطلاعات کدشده به صورت الفبای عددی[[119]](#footnote-120) است که به آن [[120]](#footnote-121)Merkle Patricia Trie می‌گویند و امکان جستجو و یافتن سریع اطلاعات را می‌دهد، پایگاه داده مورد استفاده اکثر گره‌های شبکه برای ذخیره‌سازی این ساختار داده پایگاه داده Level DB است که از نوع کلید/مقدار[[121]](#footnote-122) است [6] [7].

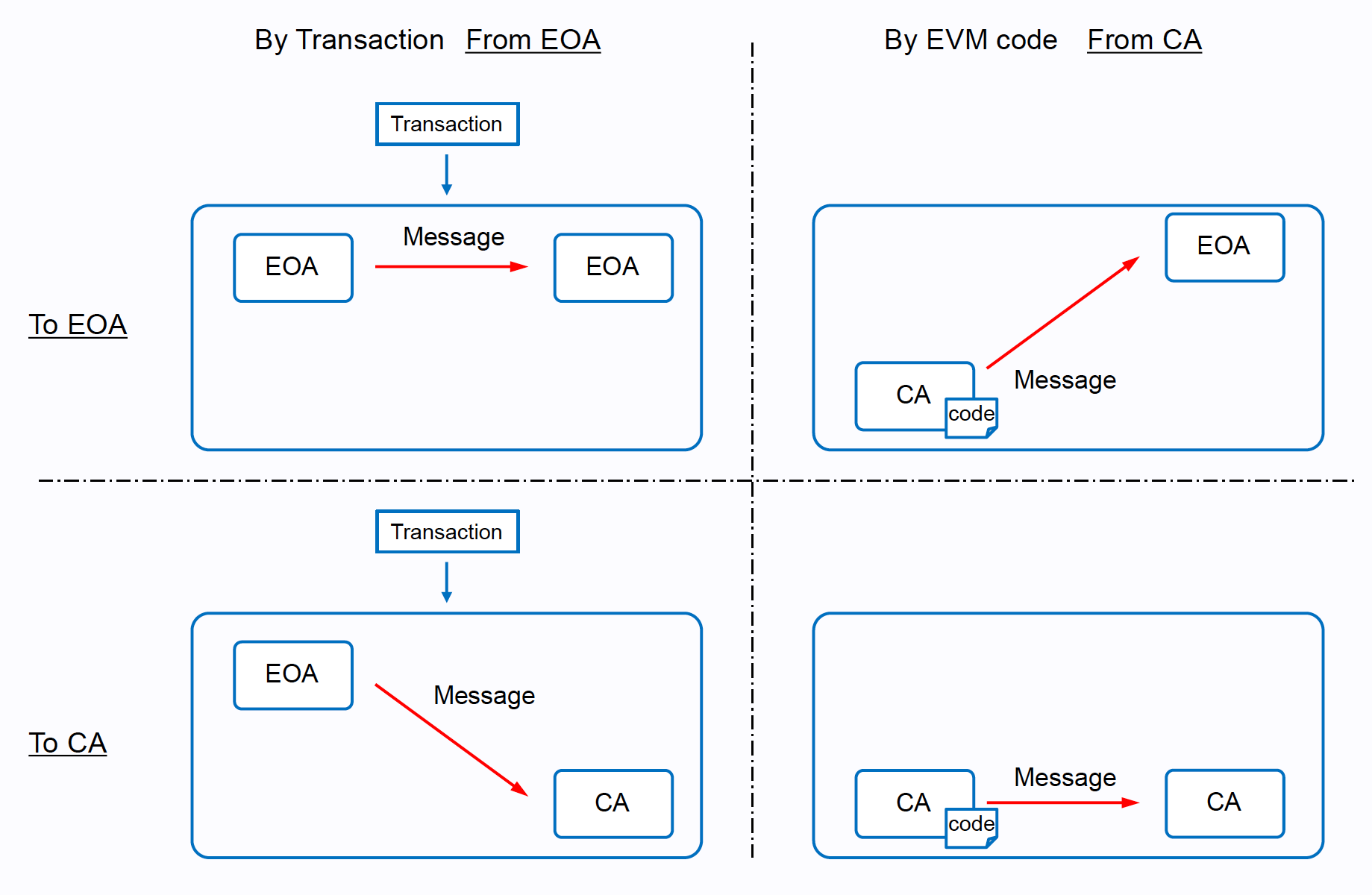
بلاکچین اتریوم بجای یک دفتر کل توزیع شده یک ماشین حالت توزیع شده[[122]](#footnote-123) است که این مدل ساختاری با استفاده از ساختارداده Merkle Patricia Trie امکان ایجاد قرارداد‌های هوشمند و ذخیره سازی حساب‌ها و موجودی هر حساب و اطلاعات مربوط به قرارداد هوشمند را می‌دهد، اگر از دید وضعیت به اتریوم نگاه کنیم می‌توان گفت که اتریوم زنجیره ای از وضعیت‌ها[[123]](#footnote-124) است.



kh

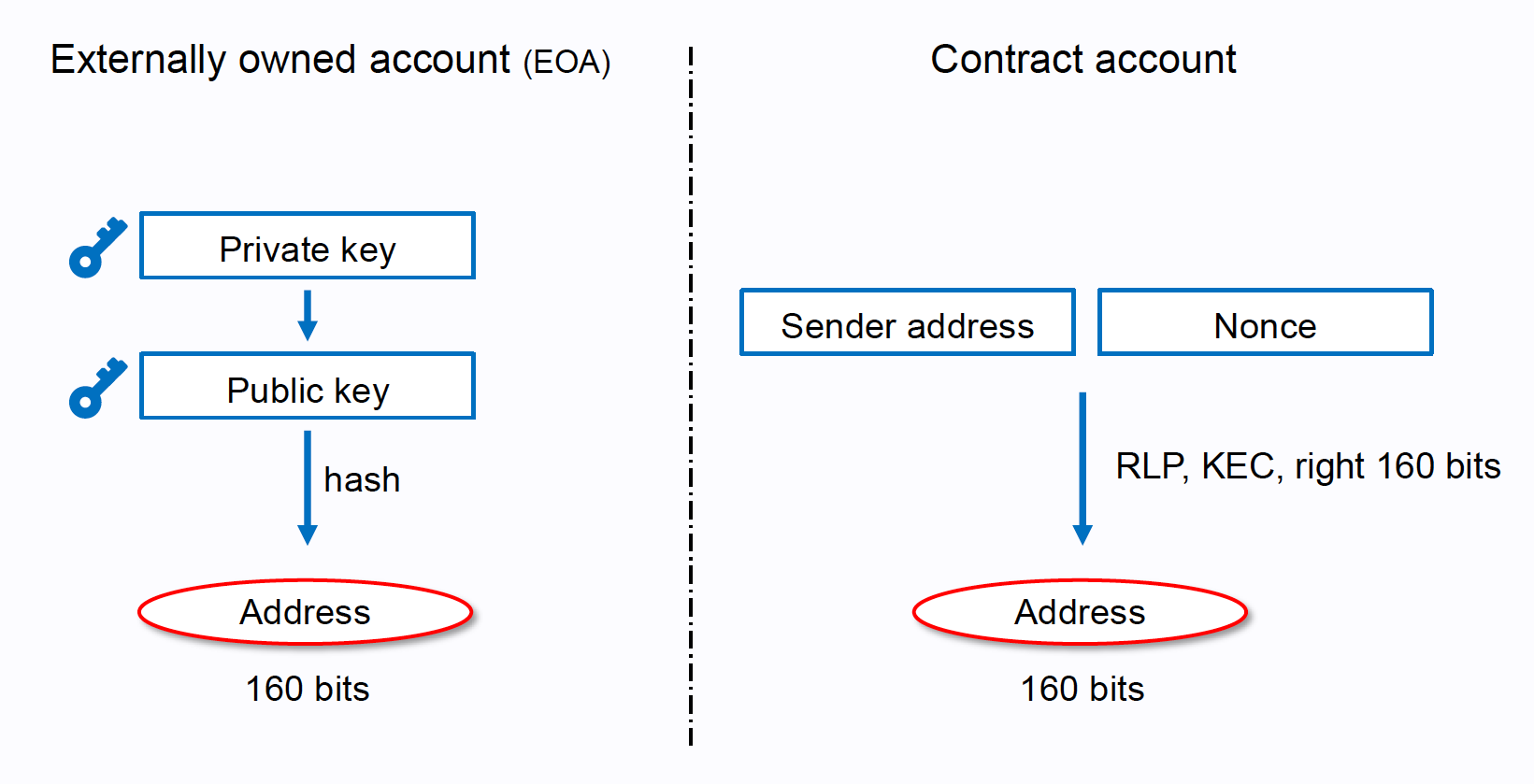
در بلاکچین اتریوم دو نوع آدرس حساب داریم :

1. **حساب‌های با مالکیت خارجی[[124]](#footnote-125) :** این نوع حساب‌ها از همان نوع آدرس کیف پول است که شامل کلید خصوصی جهت امضا تراکنش‌ها، تراکنش مالی ویا فعال کردن و تعامل با کد قرارداد ، می‌باشد. این حساب توسط کاربر مدیریت شده و می‌تواند به هر دو نوع حساب تراکنش ارسال کند و همچنین می‌توان از طریق این نوع حساب با قرار دادن آدرس صفر[[125]](#footnote-126) به عنوان آدرس گیرنده حساب‌های مبتنی بر قرارداد ایجاد کرد.
2. **حساب‌های مبتنی بر قرارداد[[126]](#footnote-127) :** این حساب دارای کلید خصوصی نبوده و توسط کد قرارداد هوشمند کنترل می‌شود، اجرا این نوع حساب توسط EOA و یا قرارداد دیگری با انجام می‌گیرد همچنین می‌تواند به هر دو نوع حساب تماس پیام[[127]](#footnote-128) ارسال کند.



jj

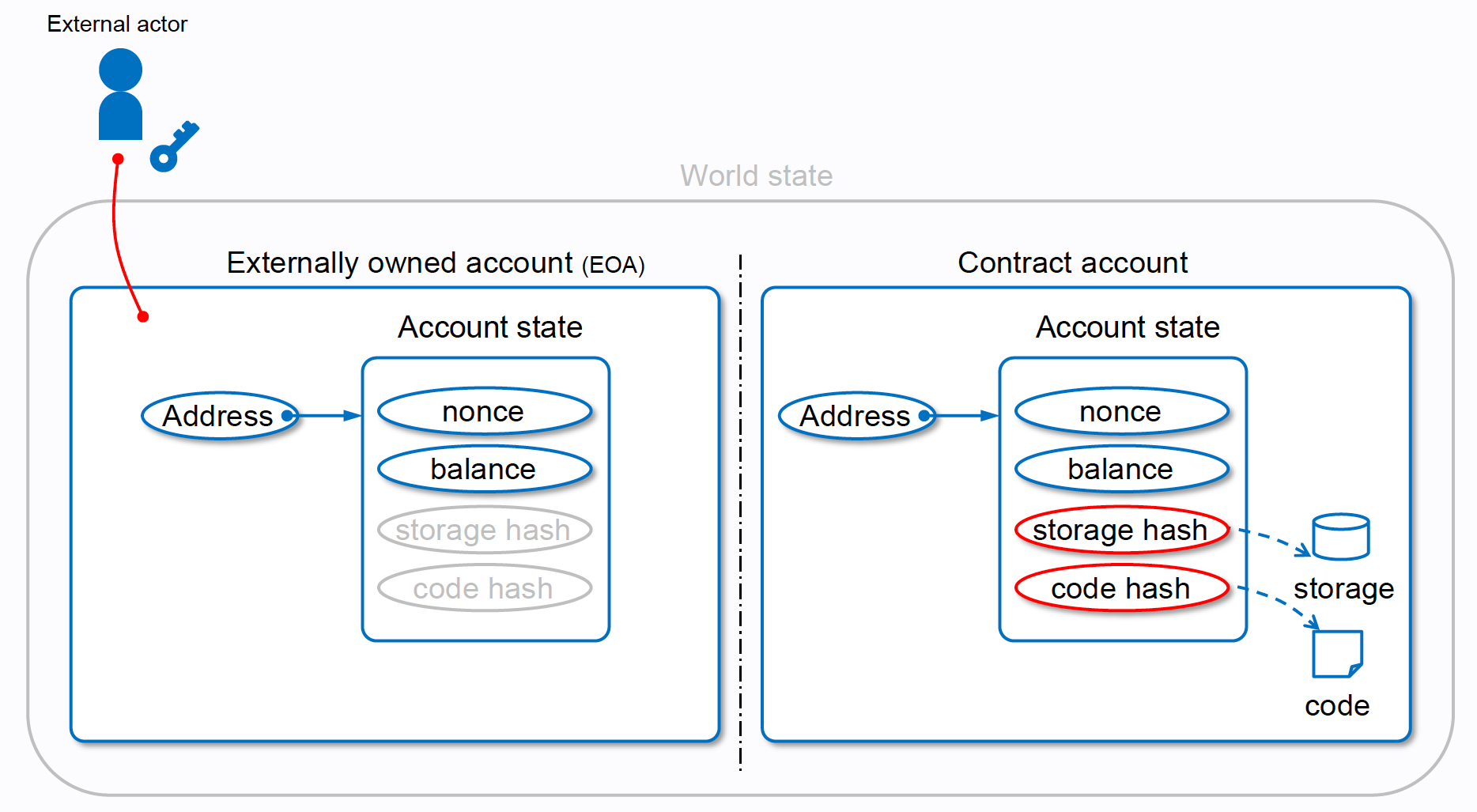
هر دو حساب دارای آدرس با طول ثابت ۲۰ بایت[[128]](#footnote-129) یا ۴۲ نیبل[[129]](#footnote-130) هستند ولی طریقه بدست آوردن هر یک متفاوت است، آدرس EOA ۲۰ بایت از هش کلید عمومی حساب است در اصل زمان درخواست ساخت کیف پول یک داده تصادفی[[130]](#footnote-131) تولید می‌شود سپس با الگوریتم مخصوص هر کیف پول کلید عمومی و خصوصی استخراج می‌شود و ۲۰ بایت از هش کلید عمومی به عنوان آدرس EOA در نظر گرفته می‌شود، آدرس حساب میتنی بر قرارداد از روی آدرس EOA سازنده آن و یک عدد نانس بدست می‌آید.



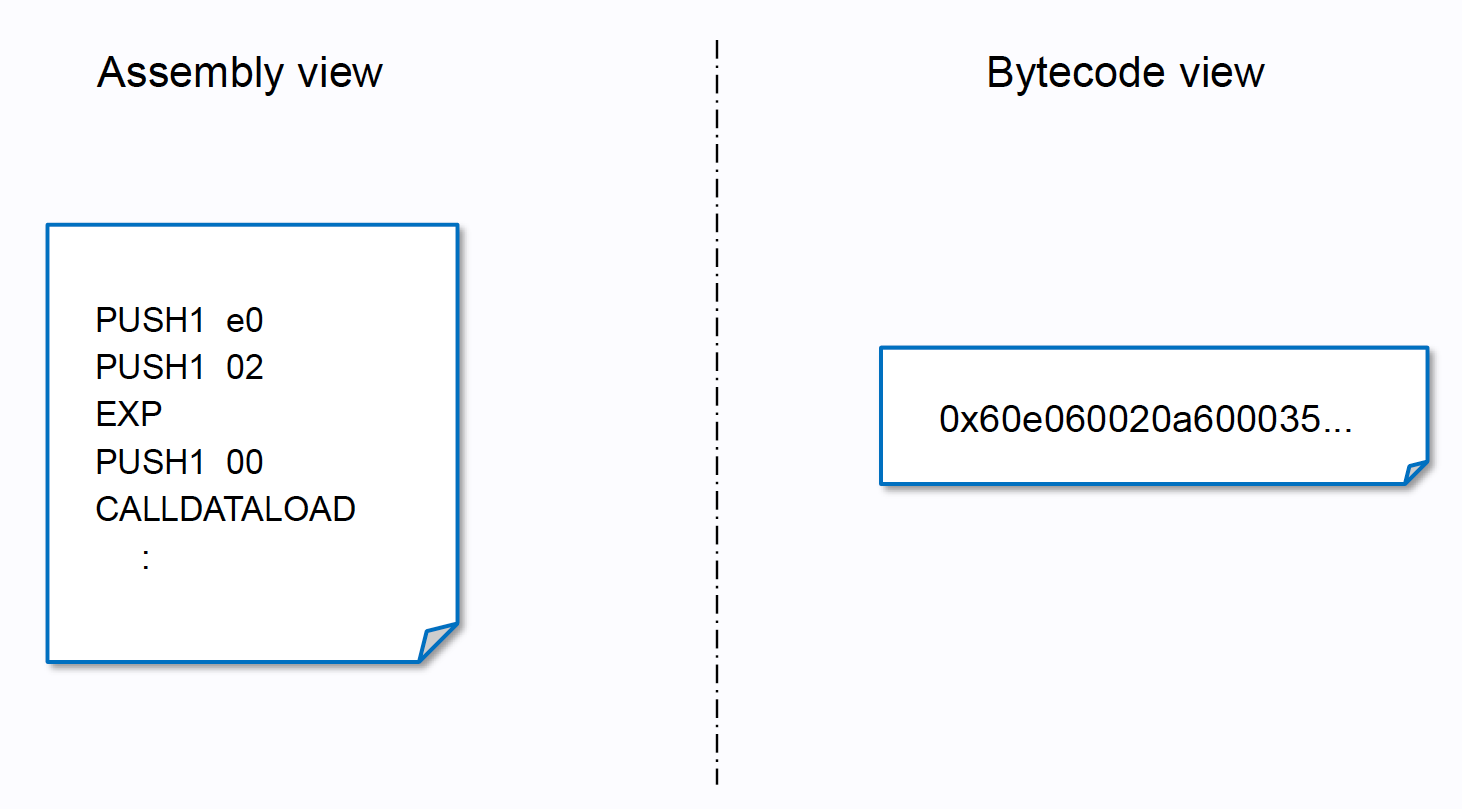
yy

هر دو نوع حساب از چهار قسمت تشکیل شده :

1. **عدد نانس :** عدد نانس در اینجا با عدد نانسی که گره‌های استخراج باید حدس بزنند متفاوت است، این عدد از صفر شروع شده و برای جلوگیری از خرج مجدد برای هر حساب تعریف شده اما برای هر حساب معنای متفاوتی دارد، این عدد برای یک EOA به این صورت است که به ازای هر تراکنش ارسالی یک واحد به آن اضافه می‌شود ولی برای حساب‌های مبتنی بر قرارداد به ازای هر تماس پیام به قرارداد دیگر یک واحد اضافه می‌گردد
2. **موجودی :** موجودی حساب را به wei[[131]](#footnote-132) نمایش می‌دهد
3. **هش ریشه انبارش[[132]](#footnote-133) :** اطلاعات قرارداد شامل ورودی ها و متغییر‌های وضعیت[[133]](#footnote-134) در این قسمت نگهداری می‌شوند و این قسمت برای EOAها خالی است
4. **هش کد[[134]](#footnote-135)‌ :** هش بایت کد[[135]](#footnote-136) ماشین مجازی اتریوم[[136]](#footnote-137) مربوط به قرارداد است و این قسمت برای EOAها خالی است



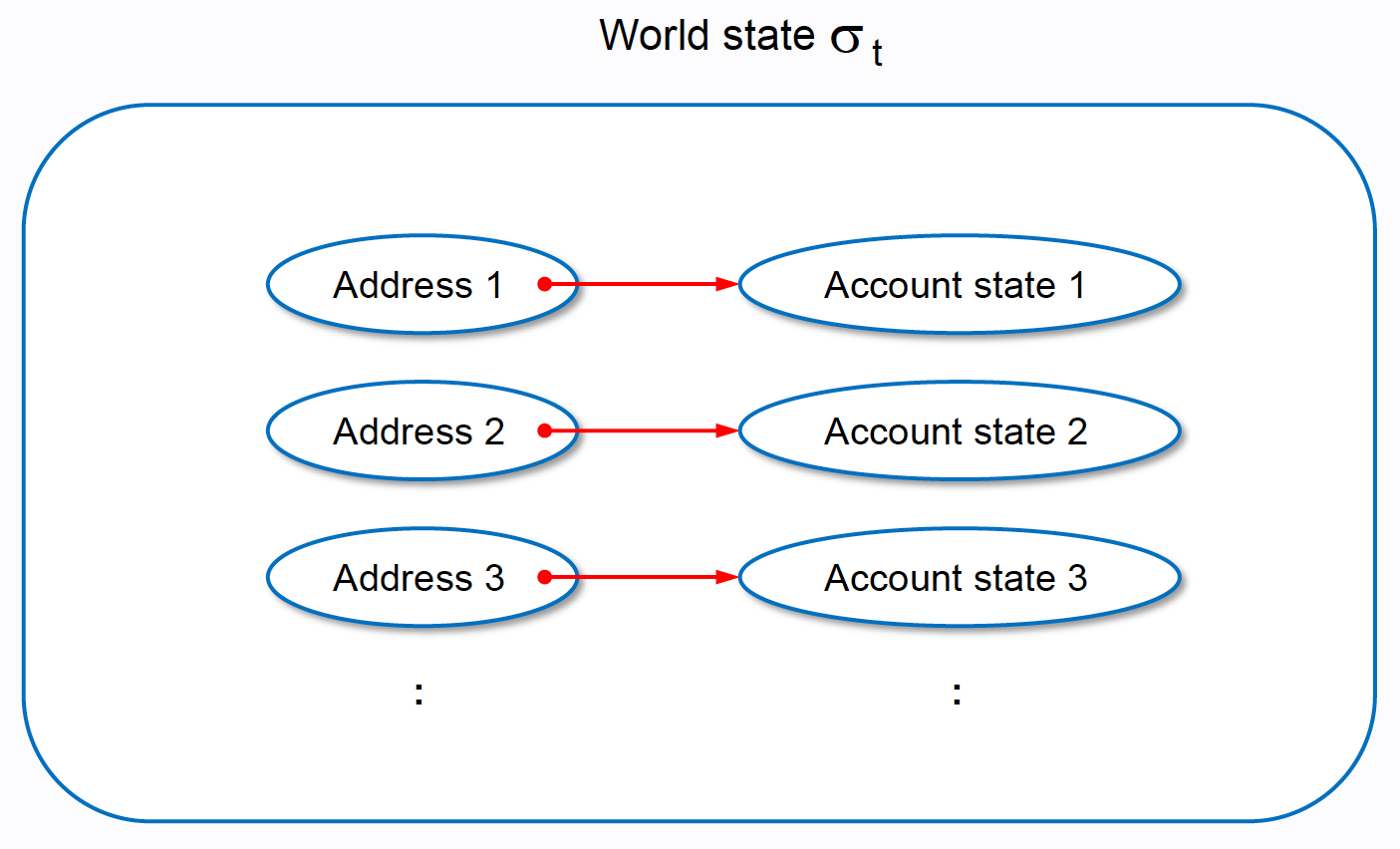
Kk



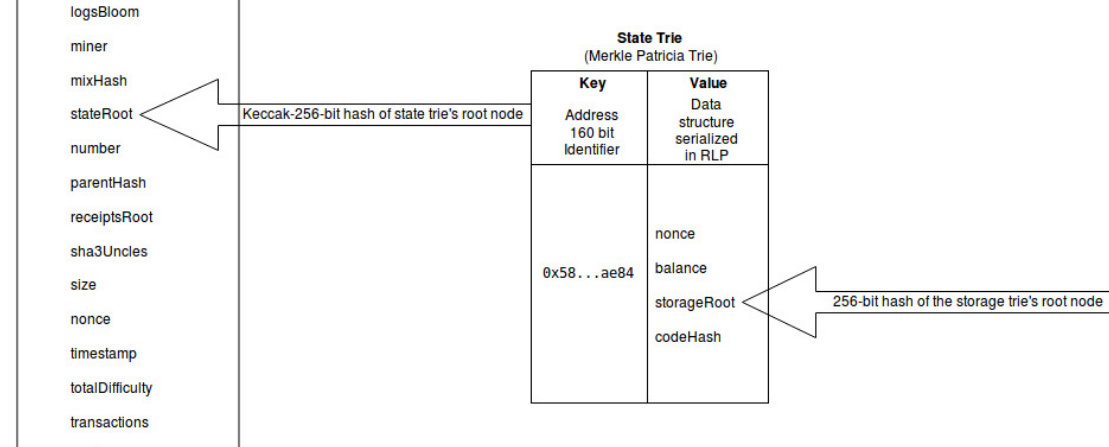
Kj

اجزای تشکیل دهنده بلوک در بلاکچین اتریوم نیز متفاوت‌تر، بیشتر و پیچیده‌تر از بلوک‌‌های بیت‌کوین است، سربرگ بلوک اتریوم علاوه بر موارد ذکر شده در عموم بلاکچین‌ها دارای چهار مورد مفهومی است:

1. **Uncles** **Hash :** اتریوم به استخراج کننده بلوک‌های یتیم جهت تشویق برای کمک به شبکه درصدی از پاداش و کارمزد‌های آن بلوک را می‌دهد و هش ستخراج کنندگان این بلوک‌ها را در سربرگ خود و لیستی از آن‌ها را در بلوک ثبت می‌کند.
2. **هش ریشه وضعیت جهانی[[137]](#footnote-138) :** وضعیت جهانی یکی از مهمترین مفاهیم در اتریوم است و همانطور که قبل بیان شد اتریوم را می‌توان زنجیره‌ای از وضعیت‌ها در نظر گرفت و حتی می‌توان گفت که پروتکل[[138]](#footnote-139) اتریوم صرفا به منظور حفظ عملکرد مداوم، بدون وقفه و تغییر ناپذیر این ماشین حالت[[139]](#footnote-140) ویژه وجود دارد [6]، منظور از وضعیت جهانی وضعیت و حالتی از کل شبکه است که تمام گره‌های سراسر شبکه یک نسخه یکسان از آن را دارند، وضعیت جهانی طبق ساختارداده Merkle Patricia Trie شکل می‌گیرد و هش ریشه آن در سربرگ بلوک ذخیره می‌شود، وضعیت جهانی به صورت کلید/مقدار در Merkle Patricia Trie ذخیره می‌شود که کلیدها حساب‌ها هستند و مقدار‌ها همان چهار قسمتی است که قبل بیان شد.

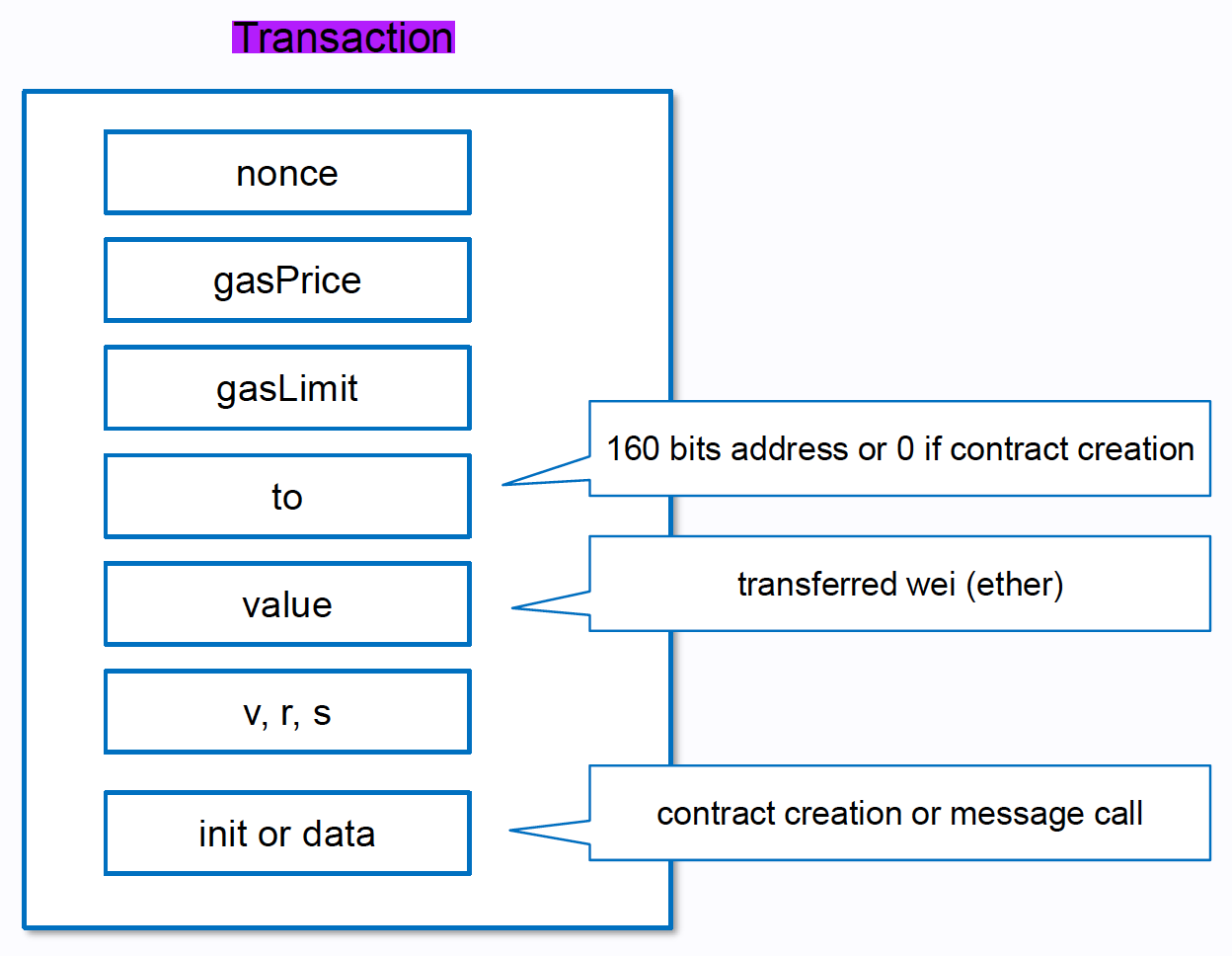


gg



gj

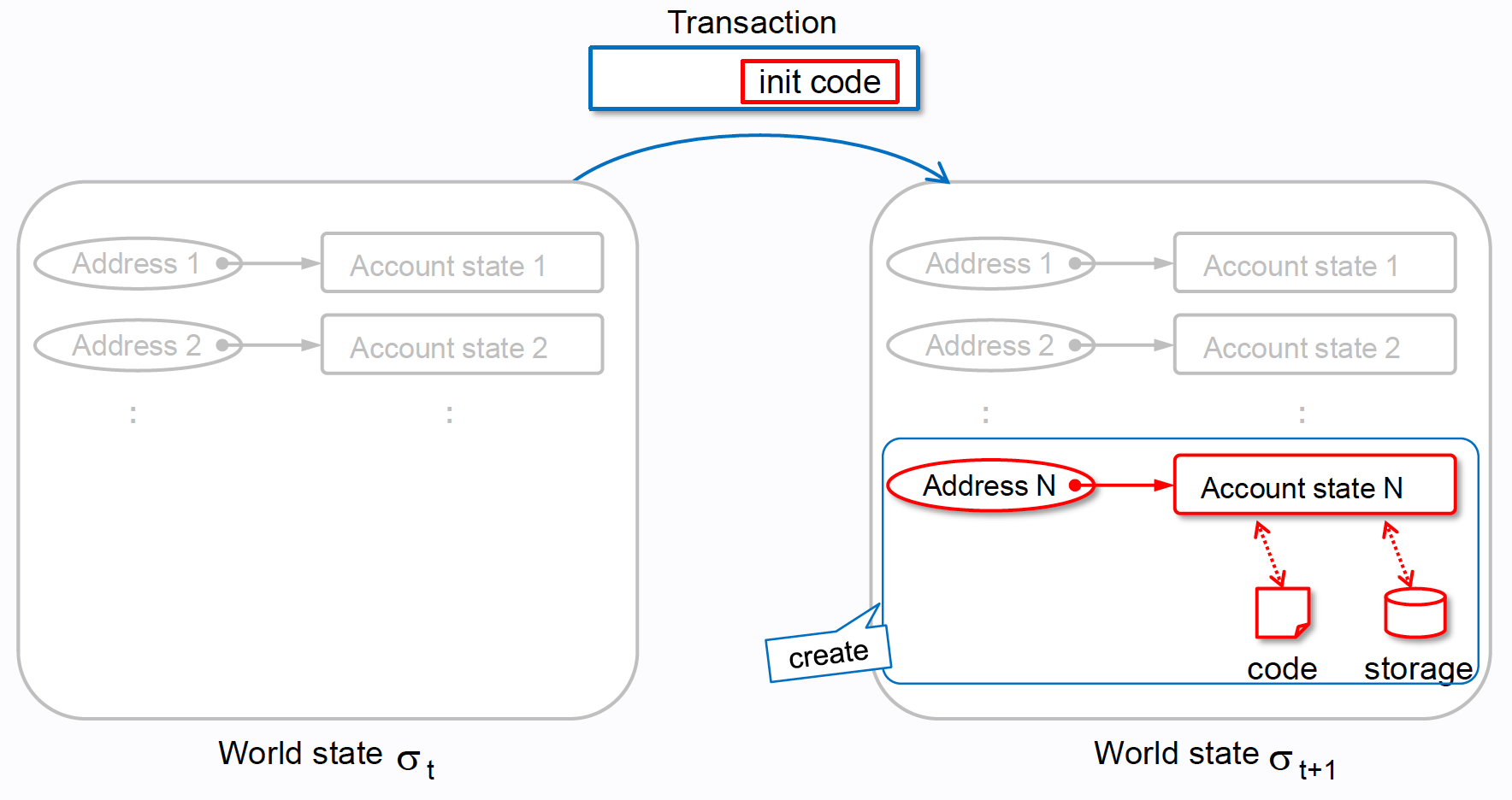
1. **هش ریشه تراکنش‌ها :** تراکنش**‌**ها در اتریوم نیز از ساختارداده Merkle Patricia Trie استفاده می‌کنند و هش ریشه تمام تراکنش‌ها در سربرگ بلوک ذخیره می‌شود، هر تراکنش ذخیره شده از بخش‌های یکسانی مانند شکل ذیل تشکیل می‌شود :



hh

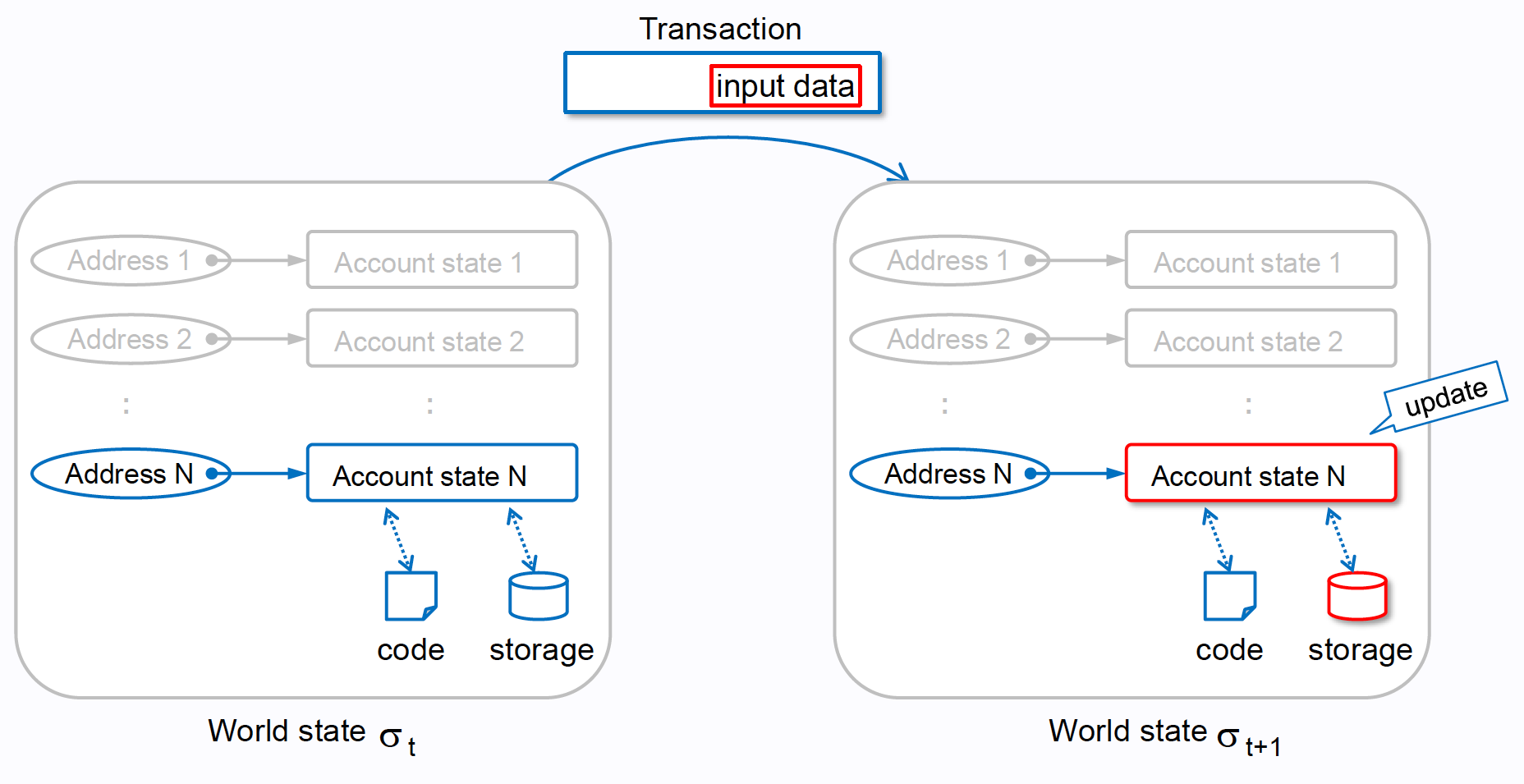
طبق شکل بالا هر تراکنش از اجزای مهمی تشکیل شده که در ادامه به توضیحی از هر یک خواهیم پرداخت

* **Nonce :** عدد نانس در اینجا هم معنی نانس در حساب‌ها است و مشخص می‌کند که حساب ارسال‌ کننده قبلا چند تراکنش موفق و تایید شده ارسال کرده است
* **گاز[[140]](#footnote-141) :**
* **v, r,** **s :** این مقادیر برای امضا رمزنگاری مورد استفاده قرار می‌گیرد جهت تعیین فرستنده تراکنش
* **init or data :** در صورتی که یک حساب EOA تراکنشی مبنی بر ساخت یک قرارداد هوشمند ارسال کند مقدارcode init که کد سازنده[[141]](#footnote-142) کد قرارداد در این بخش نوشته می‌شود و یک قرارداد در وضعیت جهانی ایجاد می‌شود



Ff

در صورتی که حساب EOA یا حساب قرارداد ورودی به قراردادی داشته باشد مقادیر آن در data ذخیره می‌شود و انبارش وضعیت جهانی را تغییر می‌دهد که این به‌روزرسانی طبق کد قرارداد یا همان کد ماشین مجازی اتریوم، که در ادامه به آن می‌پردازیم، توسط ماشین مجازی اتریوم انجام می‌شود.



Kj

1. **هش ریشه رسید تراکنش‌ها :** در این قسمت رسید تراکنش‌های موفق و به طور کامل انجام شده طی همان ساختارداده مطرح شده در اتریوم ذخیره شده و هش ریشه آن در سربرگ بلوک ثبت می‌شود.

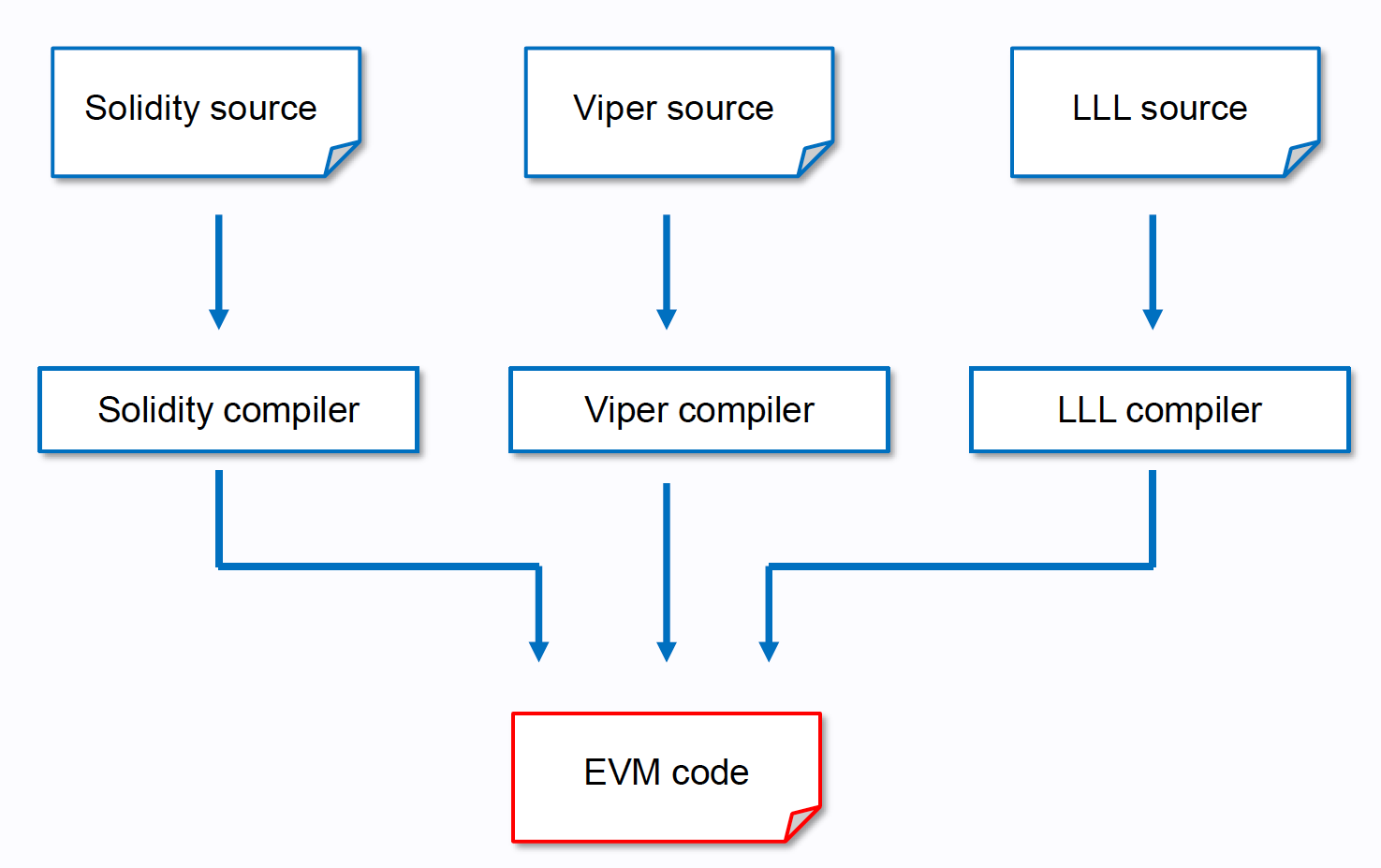
### ماشین مجازی اتریوم

قرارداد هوشمند یک قرارداد خوداجرا شونده[[142]](#footnote-143) است که شرایط قرارداد طرفین در یک کد برنامه نویسی شده و در سراسر شبکه بلاکچین غیرمتمرکز و توزیع شده قرار می‌گیرد، قراردادهای هوشمند اجازه می‌دهند تا معاملات و توافقات قابل اعتماد بین طرف‌های ناهمگون و ناشناس بدون نیاز به یک مرجع مرکزی، سیستم قانونی یا مکانیزم اجرایی خارجی انجام شود.

تعریف قرارداد هوشمند به این شکل با کمک بلاکچین اتریوم و ماشین مجازی آن تحقق یافت اگرچه ایده اولیه قرارداد‌های هوشمند توسط دانشمند کامپیوتر و رمزنگاری، نیک سابو[[143]](#footnote-144) در سال ۱۹۹۴ مطرح شد اما در آن زمان فضای مناسب برای تحقق این ایده‌ وجود نداشت.

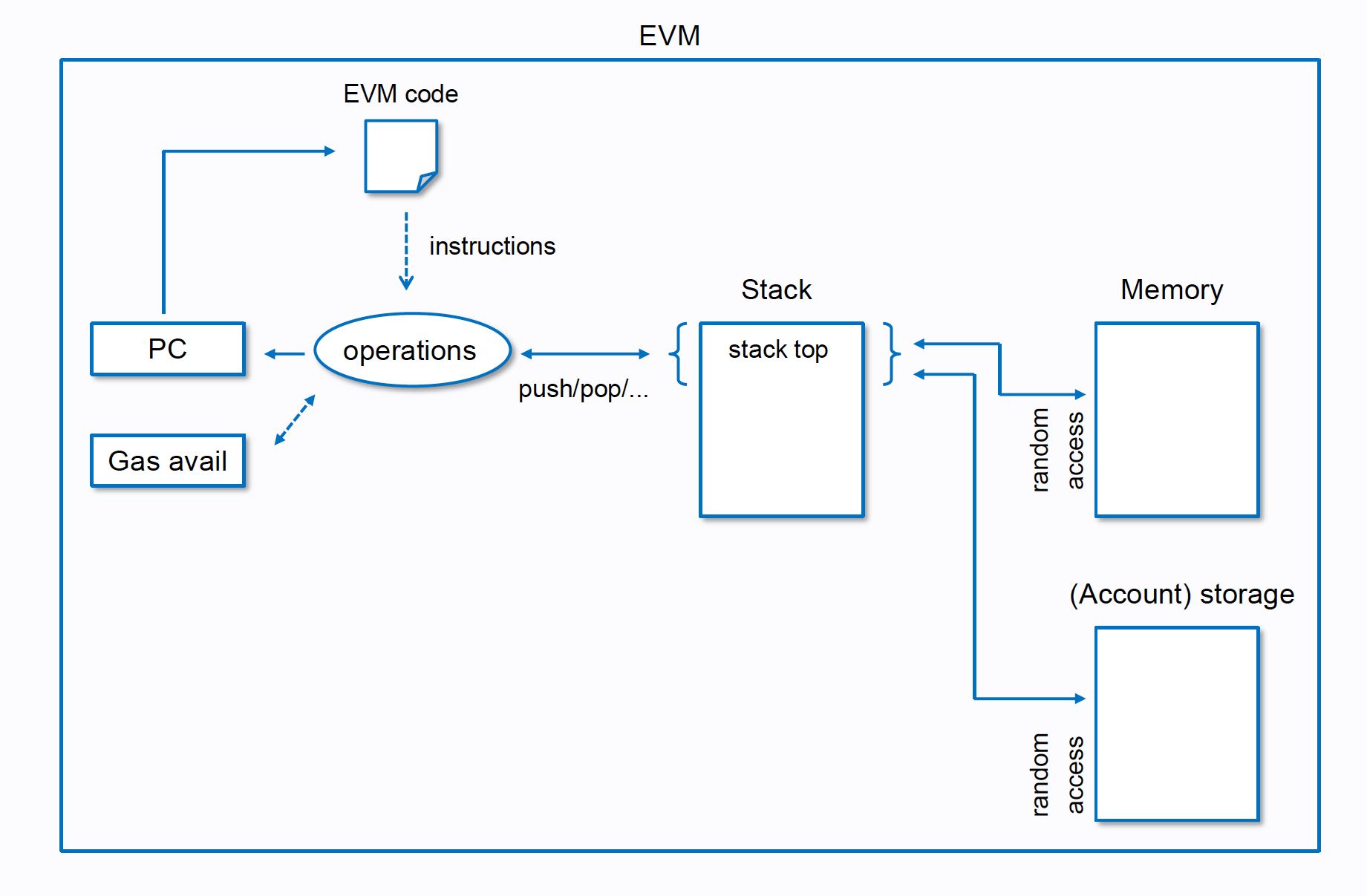
کد قراردادهای هوشمند اتریوم توسط ماشین مجازی اتریوم روی همه گره‌های موجود در بلاکچبن اتریوم اجرا می شوند که کار اجرای کد به عنوان بخشی از وظیفه گره‌ها برای تایید بلاک های جدید محسوب می شود، به همین علت کد قرارداد هوشمند را کد EVM نیز می‌نامند و از این رو شناخت ماشین مجازی اتریوم بسیار مهم است.

کد قرارداد به بایت‌کد بوده و نوشتن آن به این صورت برای برنامه‌ نویسان تقریبا غیر ممکن است به همین جهت زبان‌های برنامه نویسی سطح بالایی مثل سالیدیتی[[144]](#footnote-145) ، وایپر[[145]](#footnote-146)، LLL [[146]](#footnote-147) و ... بوجود امدند.



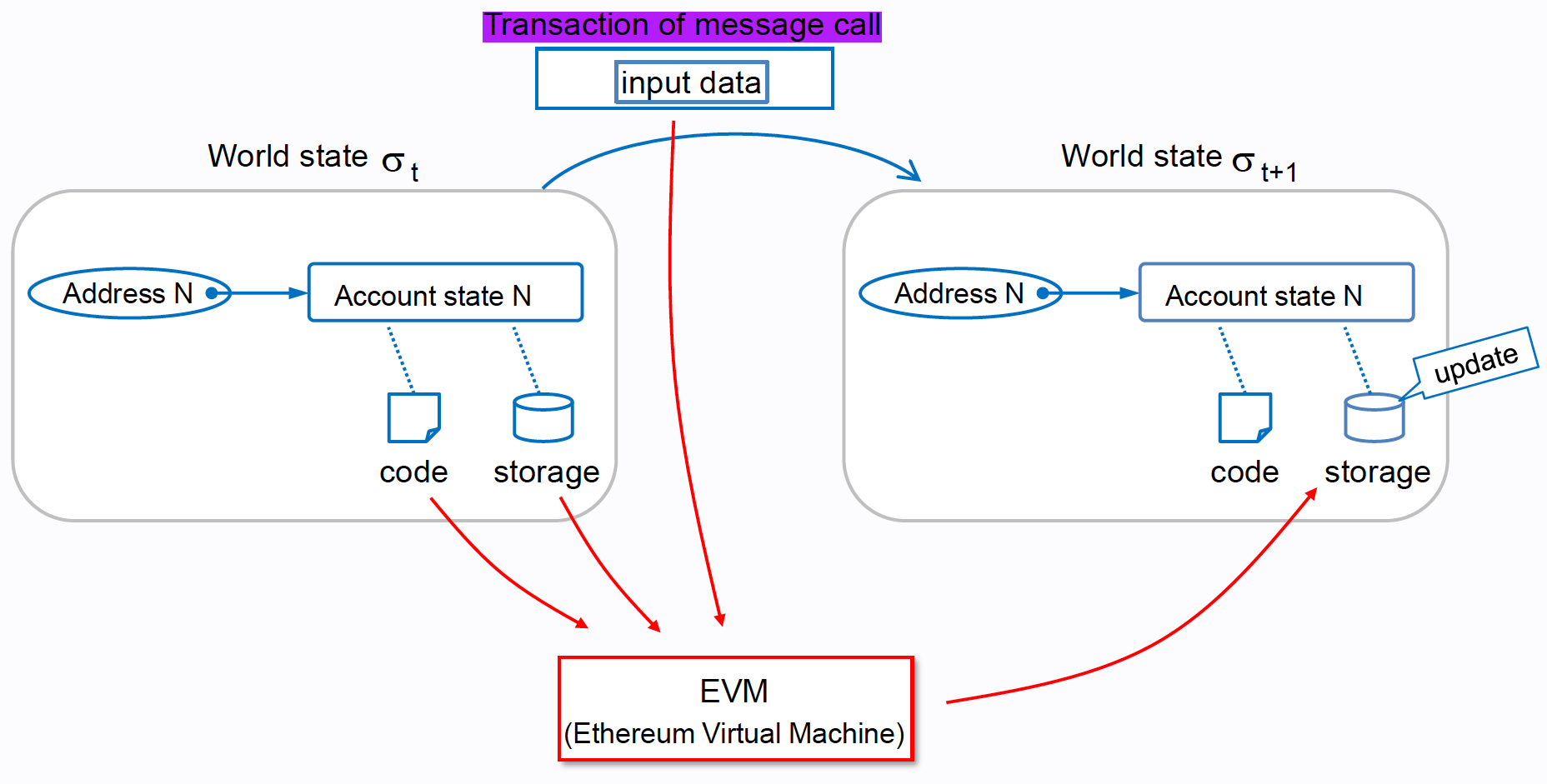
Jj

بایت‌ کد قرارداد کامپایل[[147]](#footnote-148) شده به صورت تعدادی از آپ‌کد[[148]](#footnote-149)های EVM مانند XOR، AND، ADD، SUB و ... اجرا می شود، از این رو ماشین مجازی اتریوم یک ماشین تورینگ کامل[[149]](#footnote-150) بوده و می‌تواند عملکردی مانند یک کامپیوتر داشته باشد به همین جهت و به واسطه وجود EVM در اتریوم، این بلاکچین را یک کامپیوتر جهانی به حساب می‌آورند



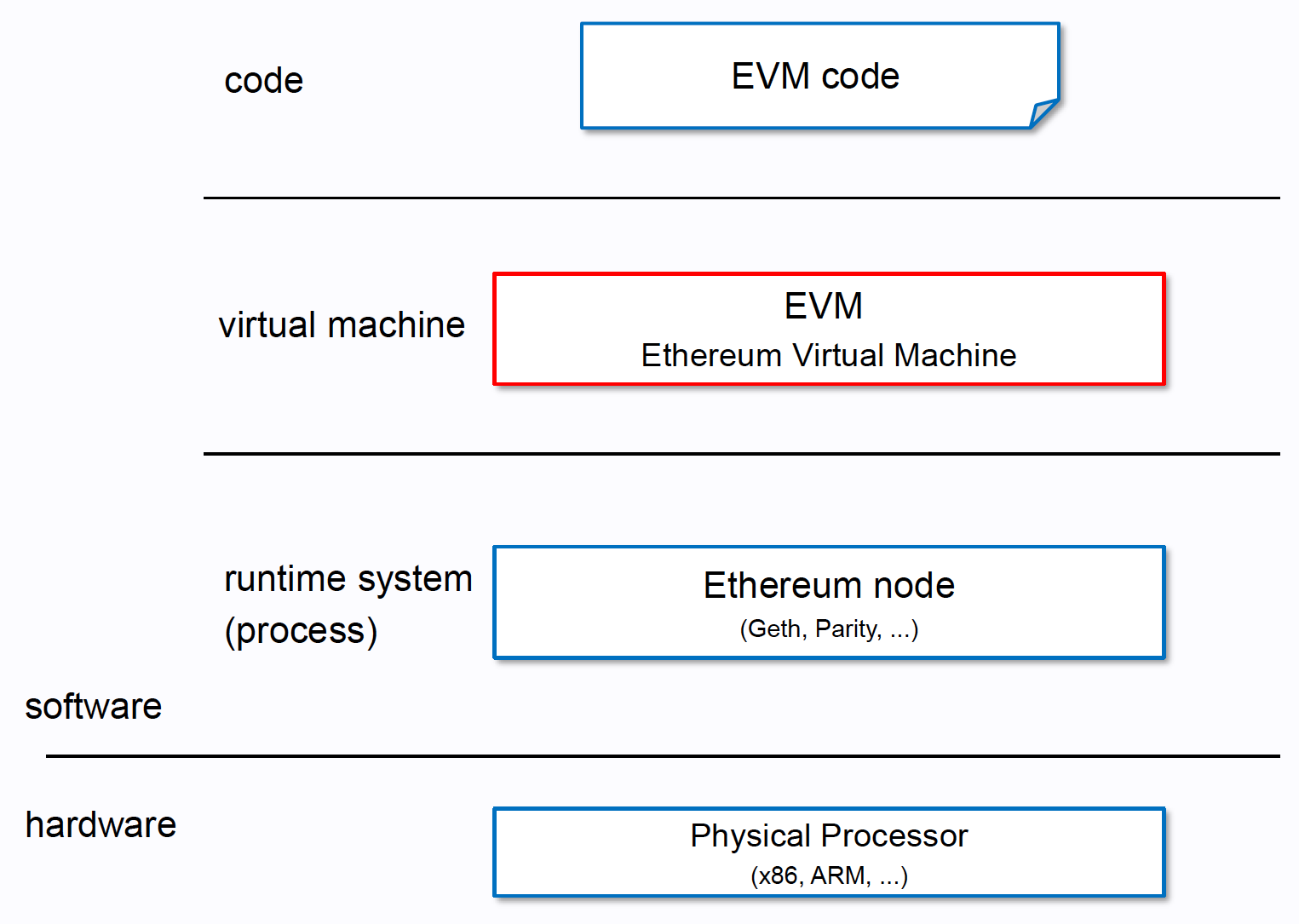
Hh

وظیفه اصلی ماشین مجازی اتریوم تغییر از یک حالت جهانی به یک حالت جهانی است که این کار طبق کد‌های قرارداد است که بر روی آن نوشته شده و EVM آن‌ها را اجرا می‌کند، در اصل EVM مثل یک تابع انتقال حالت قطعی[[150]](#footnote-151) نامید که وضعیت جهانی معتبر قبلی را به همراه مجموعه ای جدید از تراکنش‌های معتبر را به عنوان ورودی تابع می‌گیرد و حالت جهانی معتبر جدید را به عنوان خروجی تولید می‌کند.



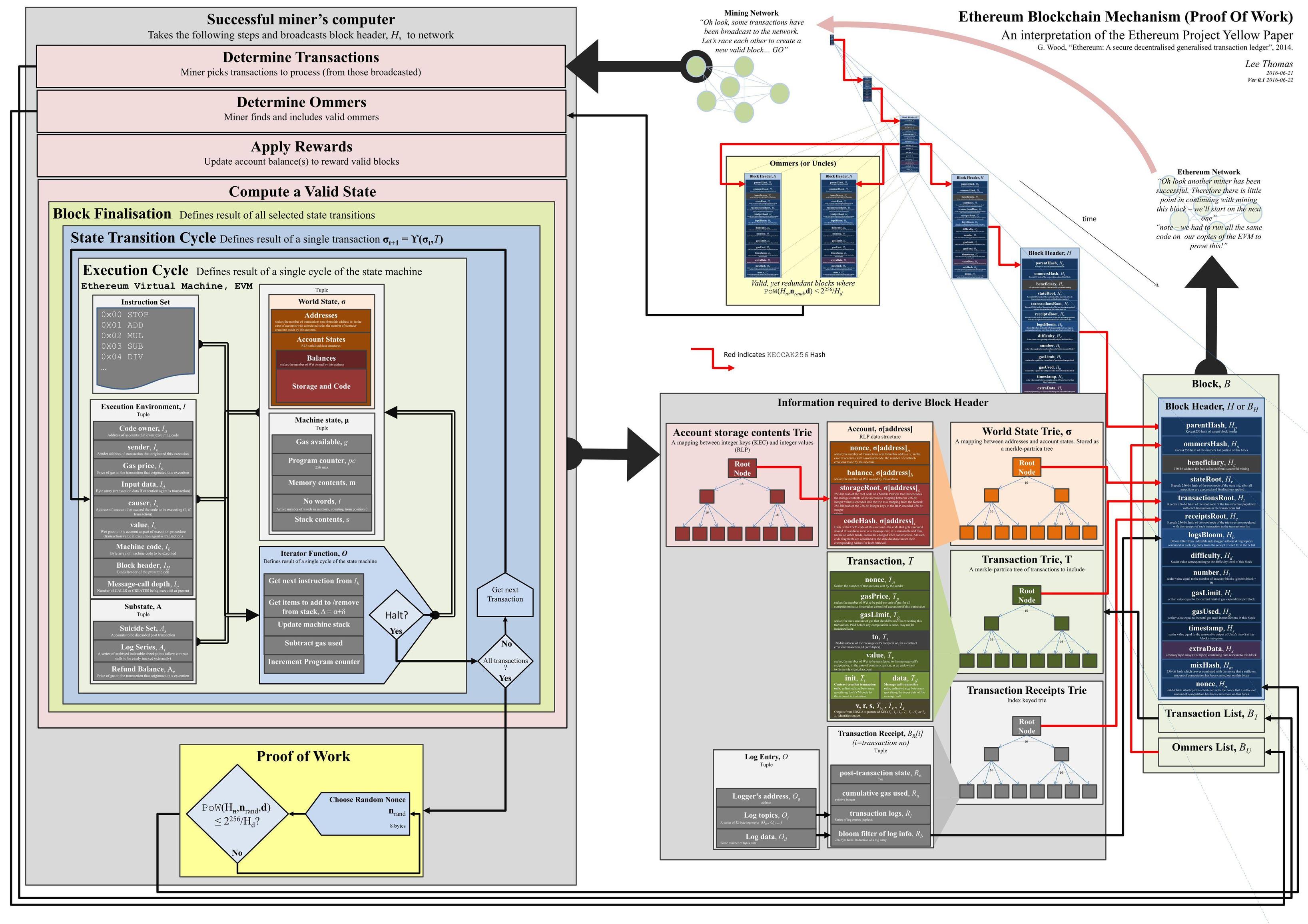
hh

از نظر ساختاری وضعیت کدهای قرارداد و EVM به شکل ذیل بوده و گره‌های شبکه موظف به اجرا کردن نرم‌افزار مخصوص جهت پیاده سازی EVM هستند.



Hh

در پایان این بخش قصد داریم یک نمای کاملی از کل شبکه بلاکچین اتریوم با توجه به مطالب بیان شده در شکل ذیل داشته باشیم :



guj

# 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. [8]

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 [9] 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

به علت نوپا بودن این تکنولوژی پروژه‌های انجام گرفته در زمینه آموزش بر پایه بلاکچین عموما با رویکرد استفاده از ویژگی اصلی این شبکه یعنی غیرقابل تغییر بودن اطلاعات ثبت شده بوده و تمرکز بر روی این ویژگی پروژه‌های متعددی را پدید آورده که در ادامه به نقل مستقیم از یک مقاله

به بیان چند پروژه تحقیقاتی-عملی مطرح شده در مقاله‌های مختلف می‌پردازیم.

### ثبت دیپلم

## نتیجه‌گیری

# تحلیل نیازمندی‌ها و طراحی

## مقدمه

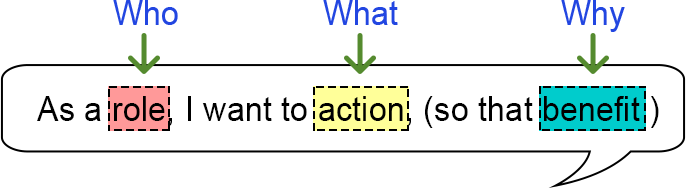
پروژه طراحی و ساخته شده پیش روی شما که با عنوان پلتفرم smartlearn در سراسر این پایان‌نامه شناخته می‌شود حاصل ماه‌ها تلاش شبانه‌روزی انفرادی بوده و سعی داشته هم‌جهت با هدف والای آموزش که تحقق آرمان آموزش بدون تبعیض برای همه می‌باشد توسعه یابد، در این فصل از پایان‌نامه در ابتدا با بیان خواست کاربران در قالب داستان‌های کاربر[[151]](#footnote-152) به نیازسنجی یک فرد استفاده کننده از دوره های آنلاین آموزشی پرداختیم و در ادامه با تبیین سند نیازمندی‌های این پلتفرم[[152]](#footnote-153)، 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 گیرد.

روش نیازسنجی کاربران در رویکرد توسعه نرم افزار چابک[[153]](#footnote-154)، 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])[[154]](#footnote-155)

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[[155]](#footnote-156) اتر[[156]](#footnote-157) 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[[157]](#footnote-158)متامسک داشته و کیف پولش حاوی مقداری اتر جهت انجام تراکنش بوده و همچنین کاربر افزونه متامسک در مرورگرهای مورد پوشش متامسک[[158]](#footnote-159) 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.

gg

|  |  |  |
| --- | --- | --- |
|  |  | 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 |
| 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 |  |

gh

|  |  |  |
| --- | --- | --- |
|  |  | 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 |  |

ff

|  |  |  |
| --- | --- | --- |
|  |  | 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[[159]](#footnote-160) Courses واقع در سربرگ[[160]](#footnote-161) 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[[161]](#footnote-162) 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 [youtube](https://www.youtube.com/) 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[[162]](#footnote-163) 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[[163]](#footnote-164) 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 :** C08 **|** **بازیگر :** کاربر

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

**توضیح نیازمندی :** به محض ورود کاربر به سایت و نصب داشتن افزونه متامسک در مرورگرهای مورد پوشش به صورت خودکار صفحه متامسک برای اتصال کیف‌پول رمزارزی کاربر ظاهر می‌شود و کار می‌تواند با برقراری این اتصال از تمامی امکانات سایت استفاده نماید، در صورت عدم برقراری اتصال پیامی به شکل ذیل 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 :** با استفاده از چهارچوب[[164]](#footnote-165) Drizzle و متد[[165]](#footnote-166) isDrizzleInitialize تعریف شده در آن اتصال کیف پول کاربر بررسی می‌شود، استفاده از این چهارچوب نیازمند

<div v-if="isDrizzleInitialized" class="container py-1">

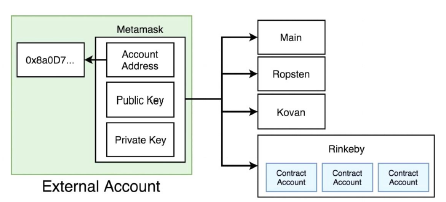
# ابزارها

## مقدمه

توسعه پلتفرم smartlearn از سه بخش سمت کاربر، سمت سرور و سمت بلاکچین تشکیل شده است که ابزار بکار گرفته شده هر بخش به صورت مجزا مورد بررسی قرار خواهند گرفت، در جدول ذیل یک لیست کاملی از تمام ابزار بکار گرفته شده به همراه نسخه مورد استفاده آن ارائه شده همچنین محیط برنامه نویسی استفاده شده در این پروژه ویرایشگر متن[[166]](#footnote-167) visual studio code محصول شرکت ماکروسافت[[167]](#footnote-168) است.

kk

|  |  |  |
| --- | --- | --- |
| سمت کاربر | Node JS | 16.15.0 |
| npm | 7.6.0 |
| Vue | 2.6.10 |
| Vuex | 3.1.1 |
| Vue-router | 3.5.4 |
| axios | 0.27.2 |
| moment | 2.29.3 |
| Bootstrap | 5.1.1 |
| Bootstrap-vue | 2.21.2 |
| EmailJS | 3.6.2 |
| Drizzle store | 1.5.3 |
| Drizzle vue plugin | 0.1.0 |
| سمت سرور | Python | 3.10.4 |
| pip | 22.1.1 |
| env |  |
| Django |  |
| Django rest framework |  |
| Django-cors-headers |  |
| Sqlite3 |  |
| سمت بلاکچین | Truffle | 5.5.13 |
| Ganache | 7.1.0 |
| Solidity | 0.5.16 |
| Solc | 0.8.11 |
| Hdwallet-provider | 2.0.8 |
| Openzeppline/contracts | 4.3.1 |
| Metamask | 10.18.3 |
| Infura |  |
| dotenv | 16.0.1 |



# 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) |

فهرست مرجع‏ها

|  |  |
| --- | --- |
| [1] | E. Grant, Ancient Egypt to Plato, New York: Cambridge University Press, 2007. |
| [2] | D. S. Halacy, Charles Babbage, Father of the Computer, Crowell-Collier Press, 1970. |
| [3] | J. Evans, "nodes," [Online]. Available: https://nodes.com. |
| [4] | M. Rajarshi , "medium," 25 5 2020. [Online]. Available: https://medium.com/bitbees/what-the-heck-is-utxo-ca68f2651819. |
| [5] | P. contribution, "ethereum.org," [Online]. Available: https://ethereum.org/en/developers/docs/evm/. |
| [6] | T. McCallum, "medium," 11 2 2018. [Online]. Available: https://medium.com/cybermiles/diving-into-ethereums-world-state-c893102030ed. |
| [7] | G. Wood, "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER," 2014. |
| [8] | Mialaret Gaston،Vial Jean, Histoire Mondiale de l'éducation, Paris: PUF, 1981. |
| [9] | David Jonassen, Michael J. Spector, Marcy Driscoll, M. David Merrill, Jeroen van Merrienboer, Marcy P. Driscoll, Handbook of Research on Educational Communications and Technology, New York: Routledge, 2007. |
| [10] | G. E. D. a. F. A. Paganini, A course in robust control theory: A convex approach, New York, NY: Springer, 2000. |
| [11] | T. Mendyk-Krajewska and Z. Mazur, "Problem of network security threats," *3rd International Conference on Human System Interaction,* pp. 436 - 443, 2010. |
| [12] | A. Galves, "Bezier Curve and Surface Fitting of 3D Point Clouds Through Genetic Algorithms, Functional Networks and Least-Squares Approximation," 2007. |
| [13] | 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. |
| [14] | R. Etges and K. McNeil, "Understanding data classification based on business and security," *ISACA Information Systems Control Journal,* vol. 5, 2006. |
| [15] | R. Etges and K. McNeil, "Understanding data classification based on business and security," *ISACA Information Systems Control Journal,* vol. 5, 2006. |
| [16] | E. Bergström and R.-M. Åhlfeldt, "Information classification issues," *Nordic Conference on Secure IT Systems,* pp. 27-41, Springer International Publishing, 2014. |
| [17] | 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. Coronavirus disease (COVID-19) [↑](#footnote-ref-14)
14. Online courses [↑](#footnote-ref-15)
15. Platform [↑](#footnote-ref-16)
16. User [↑](#footnote-ref-17)
17. Course [↑](#footnote-ref-18)
18. Smart contract [↑](#footnote-ref-19)
19. Deadline [↑](#footnote-ref-20)
20. Blockchain [↑](#footnote-ref-21)
21. Self-motivation [↑](#footnote-ref-22)
22. Prize [↑](#footnote-ref-23)
23. [↑](#footnote-ref-24)
24. [↑](#footnote-ref-25)
25. [↑](#footnote-ref-26)
26. Cryptocurrency [↑](#footnote-ref-27)
27. Satoshi Nakamoto [↑](#footnote-ref-28)
28. Ethereum [↑](#footnote-ref-29)
29. Vitalik Buterin [↑](#footnote-ref-30)
30. Gavin Wood [↑](#footnote-ref-31)
31. Data base [↑](#footnote-ref-32)
32. [↑](#footnote-ref-33)
33. [↑](#footnote-ref-34)
34. [↑](#footnote-ref-35)
35. [↑](#footnote-ref-36)
36. Information [↑](#footnote-ref-37)
37. Storage [↑](#footnote-ref-38)
38. Data [↑](#footnote-ref-39)
39. Charles Babbage [↑](#footnote-ref-40)
40. fetching [↑](#footnote-ref-41)
41. Centralized Systems [↑](#footnote-ref-42)
42. UnDistributed [↑](#footnote-ref-43)
43. Hack [↑](#footnote-ref-44)
44. Open Source [↑](#footnote-ref-45)
45. Apache [↑](#footnote-ref-46)
46. Decentralize [↑](#footnote-ref-47)
47. Developer [↑](#footnote-ref-48)
48. Cloud Service Provider [↑](#footnote-ref-49)
49. Cloudflare [↑](#footnote-ref-50)
50. Distributed [↑](#footnote-ref-51)
51. Server [↑](#footnote-ref-52)
52. Bitcoin [↑](#footnote-ref-53)
53. Crypto Currency [↑](#footnote-ref-54)
54. Blockchain [↑](#footnote-ref-55)
55. Distributed Ledger [↑](#footnote-ref-56)
56. 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-57)
57. Node [↑](#footnote-ref-58)
58. State [↑](#footnote-ref-59)
59. Atomic [↑](#footnote-ref-60)
60. Consistent [↑](#footnote-ref-61)
61. Balance [↑](#footnote-ref-62)
62. Durable [↑](#footnote-ref-63)
63. Distributed Ledger Technology [↑](#footnote-ref-64)
64. Block [↑](#footnote-ref-65)
65. Genesis block [↑](#footnote-ref-66)
66. Stuart Haber [↑](#footnote-ref-67)
67. w. scott stornetta [↑](#footnote-ref-68)
68. Timestamping [↑](#footnote-ref-69)
69. Host [↑](#footnote-ref-70)
70. Fork [↑](#footnote-ref-71)
71. Full node [↑](#footnote-ref-72)
72. Pruned nodes [↑](#footnote-ref-73)
73. Archival nodes [↑](#footnote-ref-74)
74. در گره هرس شده به حداقل یک ترابایت حافظه پر سرعت نیاز داریم و این گره حدود ۱۲۸ بلوک آخر را در خود ذخیره می‌کند ولی در گره بایگانی به حداقل دوازده ترابایت حافظه پر سرعت نیاز بوده و تمام شبکه بلاکچین را در خود ذخیره می‌کند [↑](#footnote-ref-75)
75. Mining node [↑](#footnote-ref-76)
76. Proof of work [↑](#footnote-ref-77)
77. Lightweight node [↑](#footnote-ref-78)
78. Broadcast [↑](#footnote-ref-79)
79. Body [↑](#footnote-ref-80)
80. Hash [↑](#footnote-ref-81)
81. Algorithm [↑](#footnote-ref-82)
82. Data structure [↑](#footnote-ref-83)
83. Merkle tree [↑](#footnote-ref-84)
84. Satoshi (1 satoshi = 0.00000001 BTC) [↑](#footnote-ref-85)
85. Transaction Fees [↑](#footnote-ref-86)
86. Unspent Transaction Output (UTXO) [↑](#footnote-ref-87)
87. double spending [↑](#footnote-ref-88)
88. Coinbase [↑](#footnote-ref-89)
89. BTC ( The Cryptocurrency of The Bitcoin Blockchain) [↑](#footnote-ref-90)
90. Digital signature [↑](#footnote-ref-91)
91. Asymmetric cryptography [↑](#footnote-ref-92)
92. non-repudiation [↑](#footnote-ref-93)
93. Validation [↑](#footnote-ref-94)
94. Encryption [↑](#footnote-ref-95)
95. Decryption [↑](#footnote-ref-96)
96. Network Difficulty [↑](#footnote-ref-97)
97. Nonce [↑](#footnote-ref-98)
98. Unix Timestamp ( From January 1st, 1970 ) [↑](#footnote-ref-99)
99. The Bitcoin Version Number [↑](#footnote-ref-100)
100. Proof of work [↑](#footnote-ref-101)
101. Consensus Mechanism [↑](#footnote-ref-102)
102. Byzantine fault tolerance [↑](#footnote-ref-103)
103. Spam [↑](#footnote-ref-104)
104. CPU [↑](#footnote-ref-105)
105. Email [↑](#footnote-ref-106)
106. Character [↑](#footnote-ref-107)
107. 0000f79349c800b2ef5ed40ba485e4abb75158f60f0fe7a962b5bd0fa6ccf1a0 [↑](#footnote-ref-108)
108. Hash rate or Hashing power (به تعداد حدس‌های گره‌ها برای تعیین هش با شرایط خواسته شده در یک ثانیه) [↑](#footnote-ref-109)
109. Temporary Fork [↑](#footnote-ref-110)
110. Longest Chain [↑](#footnote-ref-111)
111. Orphaned Block [↑](#footnote-ref-112)
112. Transaction Pool [↑](#footnote-ref-113)
113. 2\*7\*24\*60 = 20160 minutes [↑](#footnote-ref-114)
114. Ethereum [↑](#footnote-ref-115)
115. Virtual machine [↑](#footnote-ref-116)
116. Uninterrupted [↑](#footnote-ref-117)
117. Immutable [↑](#footnote-ref-118)
118. Trie [↑](#footnote-ref-119)
119. Practical Algorithm To Retrieve Information Coded In Alphanumeric (Patricia) [↑](#footnote-ref-120)
120. اتریوم در اصل از نسخه تغییریافته این ساختارداده استفاده می‌کند [↑](#footnote-ref-121)
121. Key/Value [↑](#footnote-ref-122)
122. Distributed State Machine [↑](#footnote-ref-123)
123. State Chain [↑](#footnote-ref-124)
124. Externally-Owned Account(EOA) [↑](#footnote-ref-125)
125. Zero Address (0x0000000000000000000000000000000000000000) [↑](#footnote-ref-126)
126. Contract Account [↑](#footnote-ref-127)
127. Message Call [↑](#footnote-ref-128)
128. Byte [↑](#footnote-ref-129)
129. Nibble [↑](#footnote-ref-130)
130. Random Data [↑](#footnote-ref-131)
131. One ether = 1,000,000,000,000,000,000 wei (1018) [↑](#footnote-ref-132)
132. Storage Root [↑](#footnote-ref-133)
133. State Variables [↑](#footnote-ref-134)
134. Code Hash [↑](#footnote-ref-135)
135. Byte code [↑](#footnote-ref-136)
136. Ethereum Virtual Machine (EVM) [↑](#footnote-ref-137)
137. World State Root [↑](#footnote-ref-138)
138. Protocol [↑](#footnote-ref-139)
139. State Machine [↑](#footnote-ref-140)
140. Gas [↑](#footnote-ref-141)
141. Constructor [↑](#footnote-ref-142)
142. Self-executing [↑](#footnote-ref-143)
143. Nick Szabo [↑](#footnote-ref-144)
144. Solidity [↑](#footnote-ref-145)
145. Viper [↑](#footnote-ref-146)
146. Low-level Lisp-like Language [↑](#footnote-ref-147)
147. Compile [↑](#footnote-ref-148)
148. Opcodes [↑](#footnote-ref-149)
149. Total Turing machine [↑](#footnote-ref-150)
150. Deterministic State Transition Function [↑](#footnote-ref-151)
151. User stories [↑](#footnote-ref-152)
152. Software Requirements Document [↑](#footnote-ref-153)
153. Agile software development [↑](#footnote-ref-154)
154. بخش انتهایی داستانه‌های کاربر اختیاری است [↑](#footnote-ref-155)
155. cryptocurrency [↑](#footnote-ref-156)
156. Ether (رمزارز شبکه اتریم) [↑](#footnote-ref-157)
157. Crypto wallet [↑](#footnote-ref-158)
158. Chrome – Firefox – Brave - Edge [↑](#footnote-ref-159)
159. Button [↑](#footnote-ref-160)
160. Header [↑](#footnote-ref-161)
161. Array [↑](#footnote-ref-162)
162. Box [↑](#footnote-ref-163)
163. Object [↑](#footnote-ref-164)
164. Framework [↑](#footnote-ref-165)
165. Method [↑](#footnote-ref-166)
166. Text Editor [↑](#footnote-ref-167)
167. Microsoft [↑](#footnote-ref-168)