 **پروژه­ی دوم درس ارزهای رمزگذاری­شده**

**استاد درس: دکتر بهرک**

**مهلت تحویل:**

**دستیار مربوطه: محمد محمودیان** [**mahmoodian@ut.ac.ir**](mailto:mahmoodian@ut.ac.ir)

در این تمرین کامپیوتری هدف این است که شما با زبان برنامه­نویسی Solidity و همچنین یک API[[1]](#footnote-1) به نام web3.js آشنا شوید به طوریکه بتوانید یک نرم­افزار غیرمتمرکز[[2]](#footnote-2) ساده را پیاده سازی کنید. در نرم­افزار­های غیرمتمرکز نیز، همانند سایر نرم­افزارها، لازم است یک قسمت سمت کاربر[[3]](#footnote-3) و یک قسمت سمت سرور[[4]](#footnote-4) پیاده سازی شود، که در این تمرین شما با پیاده سازی هر دو سمت آشنا می­شوید.

1. **دفترچه­حساب زنجیره­ی بلوکی[[5]](#footnote-5)**

هدف این است که یک سیستم غیرمتمرکز طراحی شود که بتواند بدهی­ و طلب افراد را ثبت کند؛ درواقع نمونه­ی غیرمتمرکز از یک دفترچه­ حساب. برای شفاف شدن بیشتر، یک مثال از نحوه­ی کار این سیستم در ادامه آورده می­شود.

فرض کنید که علیرضا، الهام و شبنم سه دوست هستند که معمولا با یکدیگر بیرون می­روند و غذا می­خورند. آخرین بار که علیرضا و الهام با یکدیگر ناهار خورده­اند، هزینه آن را الهام پرداخت کرده است. بنابراین علیرضا 30 هزار تومان به الهام بدهی دارد. همچنین یک بار که الهام و شبنم برای شام بیرون رفته­اند شبنم هزینه آن را پرداخت کرده است، پس الهام 30 هزار تومان به شبنم بدهکار است.

حال فرض کنید که شبنم به پول نیاز دارد و مبلغ 30 هزار تومان از علیرضا قرض بگیرد؛ در این لحظه هر سه نفر می­توانند توافق کنند که هیچ یک از آن­ها به دیگری بدهی­ ندارد و از تبادل پول خودداری کنند. درواقع هر زمانی که یک دور[[6]](#footnote-6) از بدهی­ها وجود داشته باشد می توان آن دور را حذف کرد و از جابجا شدن پول جلوگیری کرد.

ما قرار است که یک سیستم غیرمتمرکز طراحی و پیاده سازی کنیم که مشخص کند هر شخص به چه کسی و چه مبلغی بدهکار است، بدون اینکه نیاز باشد یک سازمان سومی[[7]](#footnote-7) در میان باشد. به صورتی­که مثلا وقتی الهام هزینه ناهار علیرضا را پرداخت می­کند از او بخواهد که در شبکه زنجیره­ی بلوک بدهکار بودنش را تصدیق کند. نحوه­ی تصدیق کردن بدین شکل است که فرد بدهکار یک تابع را صدا می­زند و در آن شخص طلبکار و مبلغ بدهی را مشخص می­کند؛ در کدِ برنامه این تصدیق­نامه(تاییدیه) را IOU[[8]](#footnote-8) می­نامیم. فضای موجود و عمومی و همچنین قابل دسترسِ شبکه­ی زنجیره­ی بلوک می­تواند به عنوان محل ذخیره سازی و یا به عبارتی سمت سرور برای لیست بدهی­های هر شخص استفاده شود. برای راحتی کار با این سرور لازم است که یک محیط کاربری نیز طراحی شود که جلوتر در مورد آن صحبت خواهیم کرد. ☺

1. **آماده­سازی جهت شروع**
2. نصب نرم­افزارهای پیشنیاز: لازم است که بر روی سیستم خود Node.js را نصب کنید. می توانید از این [لینک](https://nodejs.org/en/download/) استفاده کنید. لازم است که علاوه بر Node.js ، npm نیز بر روی سیستم شما نصب شود. به کمک npm می­توانید سایر پکیج­های مورد نیاز را نصب کنید. نسخه­ی ویندوز Node.js همراه خود npm را نیز دارد، اما در سیستم­عامل­های دیگر ممکن است لازم باشد آن را جداگانه نصب کنید.
3. نصب شبیه­ساز شبکه اتریوم و اجرای آن: برای اینکار در ترمینال خود از دستور npm install –g ganache-cli استفاده کنید. با این کار یک سرور به نام ganache بر روی سیستم شما نصب می شود که با اجرا شدن آن تعدادی اکانت اتریوم(پیشفرض 10 عدد) با موجودی های تعیین شده(100 اتر) ایجاد می شود که از آن­ها می­توانید برای انجام این تمرین کامپیوتری استفاده کنید. می­توان از طریق پروتکل http به این سرور وصل شد، آدرس پیشفرض آن localhost یا همان 127.0.0.1 است و پورت پیشفرض آن نیز 8545 است. برای اجرا شدن این سرور کافیست دستور ganache-cli را در ترمینال خود وارد کنید. برای متوقف کردن سرور نیز می­توانید از Ctrl+C استفاده کنید.
4. از صفحه­ی درس پوشه ItCProject2Starter را دانلود کنید.
5. در جستجوگر وب خود صفحه­ی مقابل را باز کنید. <https://remix.ethereum.org> . در قسمت ‘Run’ محیط اجرایی[[9]](#footnote-9) را بر روی ‘Web3 Provider’ تنظیم کنید. و آدرس آن را نیز بر روی <http://localhost:8545> که آدرس پیشفرض نیز هست، تنظیم کنید. محیطی که در آن هستید جایی است که لازم است شما قرارداد هوشمند[[10]](#footnote-10) خود را بنویسید و آن را کامپایل کنید. و در شبکه­ی شبیه­سازی شده مستقر(ثبت)[[11]](#footnote-11) کنید.
6. در پوشه ای که از سایت درس دانلود کرده اید یک فایل به نام index.html وجود دارد. آن را در مرورگر خود باز کنید. باید صفحه ای را تحت عنوان ‘Blockchain Splitwise’ بتوانید ببینید. توصیه می­شود که قسمت javascript console مرورگر خود را نیز باز کنید و خطاهای احتمالی را مشاهده کنید. ( برای نحوه­ی باز کردن این قسمت می­توانید از این [لینک](https://webmasters.stackexchange.com/questions/8525/how-do-i-open-the-javascript-console-in-different-browsers) کمک بگیرید) در صورتیکه همه چیز به خوبی پیش رفته باشد. شما نباید خطایی را مشاهده کنید. البته احتمالا هشدارهایی را می­بینید که می­توانید آن­ها را نادیده بگیرید.
7. فایل­های درون پوشه­ی دانلود شده را در محیط برنامه نویسی مورد علاقه خود باز کنید. (مانند Atom, Sublime,.. ) شما برای کامل شدن سمت کاربر لازم است که فایل script.js را کامل کنید. توصیه می­شود که سایر فایل های موجود را نیز بررسی کنید.
8. قبل از شروع توصیه می­شود که راجع به web3.js و برنامه نویسی solidity اطلاعات بیشتری کسب کنید. همچنین فکر کردن راجع به نحوه­ی کار سیستم کلی و همچنین نحوه ی ذخیره سازی اطلاعات و ساختارهای داده­ای که قرار است استفاده کنید، قبل از کدزنی می­تواند مفید باشد. درحال حاضر یک نسخه­ی تحت توسعه از web3.js وجود دارد(نسخه 1.0) که می­توانید راهنمای آن را از [اینجا](https://web3js.readthedocs.io/en/1.0/) ببینید، اما در این تمرین کامپیوتری از نسخه­های قدیمی­تر(0.x) استفاده می­شود که راهنمای آن را در این [لینک](https://github.com/ethereum/wiki/wiki/JavaScript-API) می­توانید ببیند.
9. در قسمت بعد کارهایی که قرار است انجام دهید با جزئیات بیشتری توضیح داده می­شود، بعد از اینکه قرارداد هوشمند خود را نوشتید و آن را بر روی شبکه ثبت کردید لازم است که آدرس[[12]](#footnote-12) آن و همچنین چکیده[[13]](#footnote-13) آن را در فایل script.js به­روزرسانی کنید. چکیده را می­توانید از قسمت ‘Compile’ و آدرس را نیز می­توانید از قسمت ‘Deployed Contracts’ در بخش ‘Run’ در صفحه Remix بیابید و کپی کنید.
10. **نیازمندی­ها**

همانطور که قبلا توضیح داده شد، این تمرین کامپیوتری از دو بخش مهم تشکیل می­شود: قرارداد هوشمند که به زبان solidity نوشته می­شود و در شبکه­ی آنلاین زنجیره­ی بلوک ثبت می­شود و قسمت سرور شما را تشکیل می­دهد و همچنین یک محیط کاربری که به زبان JavaScript نوشته می­شود و درمرورگر شما اجرا می­شود و از طریق web3.js به سرور شما وصل می­شود و اطلاعاتی را که میخواهید نمایش می­دهد.

1. **توابع سمت کاربر**
2. getUsers() : این تابع یک لیست از آدرس­های شبکه­ی اتریوم را برمی­گرداند. شما می­توانید آدرس تمام افراد موجود در شبکه را برگردانید و یا اینکه فقط افرادی را برگردانید که تا به حال فعالیت مالی­(طلب یا بدهی) داشته­اند. این تابع می­تواند به عنوان تابع کمکی در دیگر توابع مورد استفاده قرار بگیرد.
3. getTotalOwed(user) : این تابع آدرس یک کاربر را می­گیرد و کل مبلغی را که آن کاربر بدهکار است برمی­گرداند.
4. getLastActive(user) : این تابع زمان آخرین فعالیت کاربر را برمی­گرداند. منظور از آخرین فعالیت، فرستادن IOU و یا ذکر شدن به عنوان بستانکار در یک IOU توسط یک کاربر دیگر است. فرمت زمانی باید به صورت ثانیه­های گذشته از مبداِ تاریخ ( 1 ژانویه 1970) باشد.
5. add\_IOU(creditor, amount) : این تابع به عنوان تاییدیه فرستاده می­شود که نشان می­دهد شخصی که آن را صدا می­زند مبلغی معادل amount را به فرد creditor بدهکار است. این تابع چیزی را برنمی­گرداند. در این تابع لازم است که مشکل وجود حلقه نیز برطرف شود که جلوتر در مورد آن توضیح خواهیم داد.
6. **توابع سمت سرور**

یک فایل به نام BlockchainSplitwise.sol در پوشه­ی starter وجود دارد که لازم است همه­ی آن را خودتان بنویسید و شامل توابع زیر باشد.

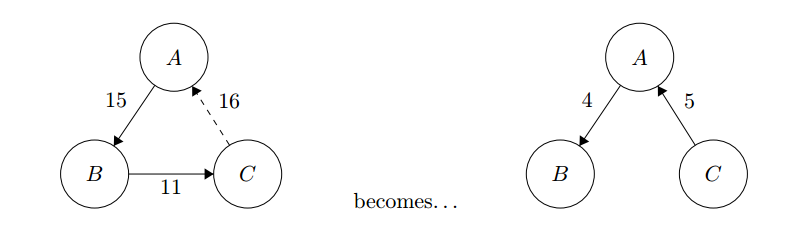
1. lookup(address debtor, address creditor) public view returns (unit32 ret) : این تابع مبلغی را که فرد debtor به شخص creditor بدهکار است، برمی­گرداند. برای این کار کافی است که در بدنه­ی تابع متغیر ret را مقداردهی کنید و نیازی به نوشتن return در انتهای تابع نیست. کلمه view یعنی اینکه این تابع قرار نیست متغیرهای موجود در شبکه را تغییر دهد، بلکه صرفا قرار است مقادیر این متغیرها را بخواند.
2. add\_IOU(address creditor, uint32 amount, …) : این تابع تاییدیه نهایی در سرور را انجام می­دهد و نشان می­دهد که msg.sender مبلغ amount را به فرد creditor بدهکار است. amount لازم است که عدد مثبتی باشد. شما می­توانید بسته به نیازتان آرگومان های دیگری برای این تابع تعریف کنید.

شما می­توانید بسته به نیازتان توابع دلخواه دیگری را در هریک از دوسمت کاربر و سرور تعریف کنید و از آن­ها استفاده کنید. در سمت کاربر می­توانید توابع سمت سرور را به صورت BlockchainSplitwise.functionname(arguments) صدا بزنید.

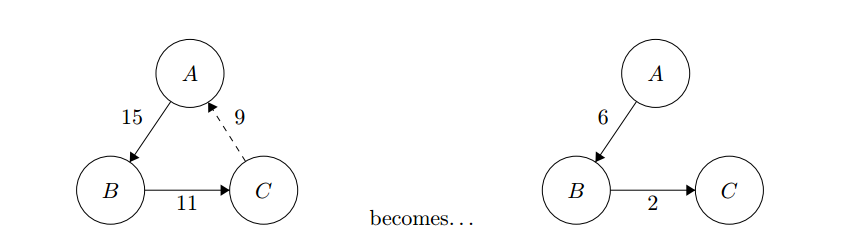
1. **حل مشکل وجود حلقه­ی بدهی­ها**

برای تحلیل راحت­تر، از مدل گرافِ جهت­دارِ وزندار برای مسئله­ی خود استفاده می­کنیم، بدین صورت که هر یک از کاربرها یک گره محسوب می­شوند و هریک از یال­ها وزنی دارد که مقدار وزن آن نشان­دهنده­ی مبلغ بدهی است. جهت یال ها از بدهکار به سمت بستانکار است. مثلا وقتی که شخص A مبلغ X را به شخص B بدهکار است آنگاه: . نرم­افزار ما لازم است به­گونه­ای کار کند که اگر حلقه­ای ایجاد شد آن را از بین ببرد برای این­کار لازم است که کوچکترین یال در حلقه پیدا شود و مقدار آن از تک­تک یال­ها کم شود به صورتیکه یکی از یال­ها به ارزش صفر برسد.

به عنوان مثال اگر و آنگاه اگر C بخواهد تراکنش را اضافه کند لازم است که نرم­افزار ما گراف را به صورت زیر تغییر دهد.



*به عنوان یک مثال دیگر اگر C بخواهد تراکنش را اضافه کند آنگاه گراف جدید به صورت زیر خواهد بود.*



لازمه­ی انجام این­کار این است که شما در تابع add\_IOU در قسمت کاربر قبل از فرستادن دستور به سمت سرور چک کنید که آیا با اضافه شدن این تراکنشِ جدید حلقه­ای به وجود می آید یا نه و درصورت وجود، حداقل یکی از آن­ها را حذف کنید. نگران موارد پیچیده نباشید و یا اینکه لازم نیست به دنبال پیدا کردن راه­های بهینه برای حذف حلقه باشید. بنابراین لازم است در توابع سمت سرور این فرض را درنظر بگیرید که هیچ حلقه­ای وجود ندارد و قسمت حذف حلقه در سمت کاربر انجام می­گیرید.

در کدهای سمت کاربر یک تابع کمکی به نام doBFS(start, end, getNeigbors) برای شما قرار داده شده است که الگوریتم bread-first search را انجام می­دهد و خروجی آن لیستی از گره­ها ایست که گره start را به گره end وصل می­کنند، البته درصورتیکه مسیری بین این دو گره وجود داشته باشد. دقت شود که آرگومان سوم، خود یک تابع است که یک گره را می­گیرد و همسایه­های آن را به صورت یک لیست برمی­گرداند و لازم است خودتان آن را بنویسید. در صورتیکه مسیری بین دوگره وجود نداشته باشد، خروجی تابع یک لیست خالی خواهد بود. استفاده از این تابع اختیاری است و شما می­توانید از هر الگوریتم دیگری برای پیدا کردن مسیر استفاده کنید.

آخرین چیزی که به نظر می­رسد باید انجام دهیم، پرداخت بدهی است به این صورت که فرض کنید آخرین بار علیرضا مبلغ 40 هزار تومان به شبنم بدهکار است حال اگر پول خود را به شبنم پرداخت کند لازم است که شبنم در شبکه یک تاییدیه بفرستد که مبلغ 40 هزار تومان به علیرضا بدهکار است با این کار یک حلقه­ی کوچک به وجود می­آید که انتظار می­رود نرم­افزار ما آن را تشخیص دهد و حذف کند و نتیجه­ی آن این باشد که هیچ یک از علیرضا و شبنم به دیگری بدهکار نیست. در واقع برای این حالت خاص لازم نیست که شما کار خاصی را انجام دهید، درصورتیکه قسمت قبل را به خوبی پیاده­سازی کرده باشید، این حالت نیز خودبه­خود انجام می­شود.

1. **توصیه های نهایی**
2. دست شما باز است که هر طور که می­خواهید قراداد هوشمند خود را بنویسید فقط لازم است که توابع خواسته شده را حتما پیاده­سازی کنید. همچنین سعی کنید قرارداد هوشمند شما کمترین میزان حافظه و کمترین میزان انجام محاسبات را به خود اختصاص دهد، چرا که اینکار باعث می­شود که استفاده از قرارداد شما ارزان­تر تمام شود.
3. از بدهی منفی حتما خودداری کنید زیرا این­کار پیچیدگی را افزایش می­دهد.
4. توصیه می­شود که ابتدا قرارداد هوشمند خود را کامل کنید، سپس سراغ بخش کاربری بروید. در سایت Remix می­توانید تمام توابع قرارداد را صدا بزنید و آن­ها را تست کنید. (از طریق پنل سمت راست و پایین صفحه) و همچنین می­توانید از قسمت ‘Accounts’ بین آدرس­های مختلف جابجا شوید. برای کپی کردن هریک از آدرس­هایی که فکر می­کنید لازم دارید، می­توانید از آیکن کنار آن­ها استفاده کنید. همچنین از طریق قسمت ‘debug’ می­توانید تراکنش­های انجام شده را دیباگ کنید و با جزئیات بیشتری اتفاقات درون آن را ببینید.(توجه کنید که برای استفاده از این قسمت لازم است که از قسمت Environment اتصال خود به سرور محلی اتریوم را قطع کنید و به JavaScript VM وصل شوید)
5. هر بار که سرور شبیه­ساز شبکه اجرا می­شود اکانت­های متفاوتی ساخته می­شود، در صورتیکه علاقه دارید هربار اکانت­های یکسانی ساخته شود می­توانید از دستور ganache-cli -d استفاده کنید.
6. برای انجام این تمرین کامپیوتری به حجم زیادی از کدزنی نیاز ندارید. کد نوشته شده­ی ما شامل حدود 40 خط در سمت سرور و 70 خط در سمت کاربر است.
7. در قسمت سمت کاربر هنگامی­که شما از تابع lookup استفاده می­کنید مقدار بازگشتی آن به فرمت BigNumber است که به فرم استاندارد با سه پارامتر c, e, s است، برای تبدیل آن به عدد معمولی می­توانید از دستور bn.toNumber() و یا از عملگر + قبل از bn استفاده کنید که منظور از bn مقدار بازگشتی از تابع lookup است.
8. برای دیباگ کردن سمت کاربر می­توانید از تابع آماده­ی log و یا از تابع console.log استفاده کنید که تابع اول خروجی را در صفحه­ی اصلی سایت نشان می­دهد و تابع دوم خروجی را در قسمت console مرورگرتان نشان می­دهد.
9. در صورت مشاهده­ی خطایی مبنی بر عدم اتصال به localhost:8545 ، از درحال اجرا بودن شبیه­ساز شبکه اتریوم (ganache-cli) مطمئن شوید.
10. در زبان solidity یک تابع کارآمد به نام require وجود دارد که می­تواند برای چک­کردن­های مربوط به قسمت­های امنیتی از آن استفاده کنید.
11. **بخش امتیازی**

در بخش قبل برای کامپایل کردن و ثبت کردن قرارداد بر روی شبکه­ی بلاک­چین از سایت remix استفاده کردیم، در این بخش قرار است ابزاری را معرفی کنیم که این کار را هوشمندانه­تر و کاربردی­تر انجام دهد. پکیجی به نام truffle. برای نصب آن کافیست که در ترمینال خود دستور روبرو را وارد کنید. npm install –g truffle . سه تا از دستور­های ترافل که در این بخش از آن استفاده می­کنیم، عبارتند از:

* truffle compile
* truffle migrate
* truffle test

نحوه­ی کار ترافل بدین شکل است که لازم است سه پوشه با نام­های contracts، migrations و test در پوشه­ی اصلی که پروژه ما در آن است موجود باشد. در پوشه اول(contracts) کدهای solidity قرار می­گیرد، قرارداد­های اصلی که لازم است کامپایل و ثبت شوند. در پوشه دوم و سوم فایل­های به فرمت .js قرار می­گیرند که اصطلاحا اسکریپت نام دارند و به زبان Node.js هستند که شباهت زیادی به JavaScript دارد. فایل­های پوشه­ی migrations لازم است به صورتی باشند که اسم آن­ها با عدد شروع شود.

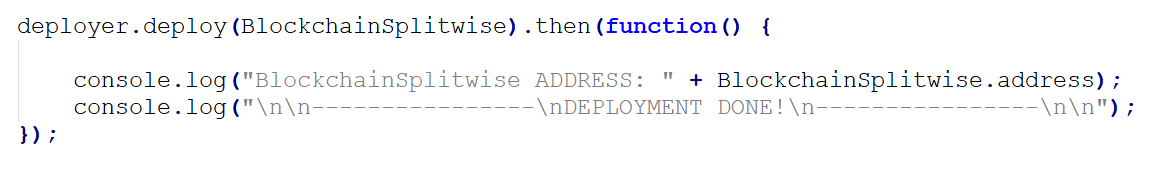
با اجرای دستور اول، قراردادهای موجود در پوشه اول کامپایل می­شوند و یک پوشه به نام build ساخته می­شود و چکیده­ی قراردادها به فرمت .json در آن ثبت می­شود، می­توانید abi هر قرارداد را آن­جا ببینید و درصورت لزوم آن را کپی کنید.

با اجرای دستور دوم، اسکریپت­های موجود در پوشه دوم به ترتیب اسم توسط Node.js کامپایل و اجرا می­شوند، این اسکریپت­ها به نحوی نوشته می­شوند که با اجرا شدن آن­ها، قراردادهای اصلی(موجود در پوشه اول) کامپایل و درصورت درستی در شبکه ثبت شوند. درواقع هدف اسکریپت­های موجود در پوشه دوم انجام کاری است که ما تا الان با remix انجام می­دادیم.

اجرای دستور سوم باعث می­شود که تمام فایل های موجود درپوشه تست کامپایل و اجرا شوند. هدف از فایل­های موجود در این پوشه این است که قراردادهای اصلی ما را در شبکه ثبت کند و سپس توابع آن­ها را صدا بزند و خروجی های آن­ها را نمایش دهد، در واقع با این کار به راحتی می­توان چک کرد که آیا توابعی که ما در قراردادمان نوشته­ایم به درستی کار می­کنند یا نه.

**چند نکته.**

1. لازم است در هنگام استفاده از truffle سرور ganache-cli درحال اجرا باشد.
2. برای آشنایی بیشتر با truffle می­توانید از دستور truffle --help استفاده کنید و با سایر قابلیت­های آن آشنا شوید از جمله می­توان به truffle console اشاره کرد که برای استفاده­ی developers مناسب است.
3. اگر در یک پوشه خالی دستور truffle unbox را اجرا کنید یک نمونه از یک پروژه انجام شده را همراه با سه پوشه اصلی و فایل های درون آن می­توانید مشاهده کنید. حتما توصیه می­شود که از این فایل­ها کمک بگیرید.
4. با انجام نکته سوم خواهید دید که در پوشه migrations دوفایل با نام­های 1\_initial\_migration.js و 2\_deploy\_contracts.js وجود دارد فایل اول را می­توانید دقیقا به همان صورت استفاده کنید اما لازم است که در فایل دوم تغییراتی ایجاد کنید که با قرارداد هوشمند شما سازگار باشد. همچنین برای دیدن آدرس قرارداد ثبت شده ( که در مراحل قبل آدرس آن را از remix کپی می­کردید و به فایل script.js انتقال می­دادید) می­توانید از قطعه کد زیر کمک بگیرید.



1. با انجام قسمت سوم همچنین خواهید دید که در پوشه­ی contracts سه فایل موجود است، لازم است که فایل Migrations.sol را به همان شکل به پوشه­ی متناظر در پروژه­ی خود انتقال دهید.
2. در آخر نیز اگر بعداز انجام قسمت سوم محتویات پوشه test را ببینید. دو فایل وجود دارد که شما تنها لازم است فایلی همانند فایل metacoin.js در پروژه خود بسازید. توجه شود که در این اسکریپت از مفهومی به نام promise که یکی از مفاهیم کدنویسی به زبان nodejs است، استفاده­ی زیادی دارد، همچنین از دستور it() استفاده می­شود، توصیه می­شود برای درک بهتر کدها، مقداری با این مفاهیم آشنا شوید.

در این قسمت از شما خواسته می­شود که سه پوشه اصلی را بسازید و فایل­های لازم را در آن بنویسید. در مورد فایل موجود در پوشه تست، لازم است که یک فایل به نام test.js بسازید و آن را کامل کنید در این فایل لازم است که کلیه توابعی که در قرارداد خود آورده اید تست شوند و از صحت اجرای آن­ها اطمینان حاصل شود. میزان پیچیدگی تست ها به خودتان بستگی دارد، اما انتظار می­رود که تست­ها هوشمندانه و قابل اطمینان باشند. از آنجاییکه این بخش به صورت امتیازی است، نمره­ی اختصاص داده شده به آن به صورت نسبی و در مقایسه با عملکرد بقیه دانشجویان خواهد بود.

1. **بارگزاری فایل ها**

کلیه فایل­ها و پوشه­های خود را در قالب یک فایل فشرده به صورت StudentID1-StudentID2.zip آپلود کنید، یکی از افراد گروه آپلود کند، کافیست.

1. Application Protocol Interface [↑](#footnote-ref-1)
2. Decentralized Application(DApp) [↑](#footnote-ref-2)
3. Client side [↑](#footnote-ref-3)
4. Server side [↑](#footnote-ref-4)
5. Blockchain Splitwise [↑](#footnote-ref-5)
6. Cycle [↑](#footnote-ref-6)
7. Third party [↑](#footnote-ref-7)
8. I Owe You [↑](#footnote-ref-8)
9. Environment [↑](#footnote-ref-9)
10. Smart contract [↑](#footnote-ref-10)
11. Deploy [↑](#footnote-ref-11)
12. Contract address [↑](#footnote-ref-12)
13. ABI [↑](#footnote-ref-13)