

راهنمای بارگذاری قرارداد هوشمند توکن سیتکس

در بلاک چین اتریوم

## - بسته های نرم افزاری مورد نیاز:

ابتدا پس از راه اندازی سیستم عامل اوبونتو دستورات ذیل را در ترمینال اجرا نمایید:

```
sudo apt-get update
```

```
sudo apt-get install build_essential
```

سپس جهت نصب و راه اندازی این پروژه ابتدا بایستی بسته های نرم افزاری node.js که یک پلتفرم اجرای کدهای زبان جاوا اسکریپت در سمت سرور می باشد و همچنین npm یا node package manager را نصب نمود. جهت نصب بسته های نرم افزاری یاد شده لطفا به وبسایت اصلی آن [www.nodejs.org](http://www.nodejs.org) مراجعه نمایید. همچنین در نظر داشته باشید که پروژه پیش رو بر مبنای v-8 nodejs و نسخه v-6 npm توسعه یافته و توصیه می گردد از نسخه های مشابه استفاده گردد.

علاوه بر این لازم می باشد تا نرم افزار git نیز نصب گردد:

```
sudo apt-get update
```

```
sudo apt-get install git
```

همچنین جهت مشاهده و بررسی بهتر کدها نصب نرم افزار vscode توصیه می گردد. برای این کار ابتدا از لینک زیر نسخه deb. را دانلود نمایید

<https://code.visualstudio.com/Download>

و با دستور زیر آنرا نصب نمایید:

```
sudo dpkg -i ~/path/to/code_xxx.deb
```

## - دریافت فایل پروژه و نصب بسته های اختصاصی:

جهت دریافت فایل مربوط به پروژه ابتدا ترمینال را گشوده و در مسیر مورد نظر با استفاده از دستور زیر فایل های پروژه را از مخزن آن در سایت گیت هاب دریافت نمایید:

```
git clone git@github.com:CitexCo/Julia-SmartContract-persian.git
```

در صورت دریافت موفقیت آمیز فایل های پروژه با هدایت ترمینال خود به مسیر پروژه با استفاده از دستور زیر بسته های استفاده شده در این پروژه را نصب نمایید:

```
npm install
```

## - کامپایل پروژه:

پیش از بارگذاری قرارداد هوشمند بر روی بلاک چین اتریوم ابتدا باید کدهای مرتبط را کامپایل نمود. برای این کار ابتدا نرم افزار `vscode` را باز کرده و از منوی `File > Open Folder` فولدر پروژه را باز نمایید سپس در ترمینال یا در واقع `power shell` نرم افزار `vscode` با استفاده از بسته نرم افزاری `truffle` و با از طریق دستور ذیل پروژه را کامپایل نمایید:

```
truffle compile
```

## - بار گذاری قرارداد هوشمند بر روی شبکه بلاک چین اتریوم:

بطور کلی سه حالت مختلف جهت بار گذاری قرارداد هوشمند بر روی بلاک چین اتریوم وجود دارد. بار گذاری بر روی شبکه آزمایشی محلی یا عمومی و بلاک چین اصلی.

## - بارگذاری در شبکه بلاک چین آزمایشی محلی:

منظور از شبکه آزمایشی محلی ساخت یک بلاک چین آزمایشی بر روی ماشین محلی می باشد. این کار از طریق نرم افزارهایی چون `testrpc`, `ganache`, `geth`, ... قابل اجرا می باشد. هر یک از بسته های یاد شده به سادگی می توان با استفاده از `npm` قابل نصب می باشد. بطور مثال جهت نصب بسته `ganache-cli` از دستور زیر می توان استفاده نمود:

```
npm i -g ganache-cli
```

جهت بارگذاری قرارداد هوشمند بر روی شبکه آزمایشی ابتدا یکی از بسته های نصب شده بر روی ماشین را اجرا نمایید. بطور مثال برا راه اندازی شبکه آزمایشی `ganache` دستور زیر را اجرا نمایید:

```
ganache-cli
```

در صورت اجرای موفق شبکه آزمایشی 10 حساب اتریوم آزمایشی ساخته می شود که کلید عمومی و خصوصی آنها در بلافاصله چاپ می گردد. ضمناً هر حساب دارای 100 اتر می باشد.

در نهایت جهت بارگذاری قرارداد هوشمند در power shell نرم افزار vscode دستور زیر را اجرا نمایید:

```
truffle migrate --reset
```

در صورتی که بارگذاری با موفقیت اجرا گردد هش ترنزکشن و آدرس قرارداد در خروجی چاپ خواهد شد.

### - بار گذاری قرارداد هوشمند در شبکه آزمایشی عمومی:

شبکه های بلاک چین آزمایشی عمومی متعددی موجود می باشد که مهم ترین آنها شبکه های ropsten, rinkeby و kovan می باشند. این شبکه های آزمایشی هم چنین در صورت درخواست اتر آزمایشی به حساب اتریومی ارسال می نمایند.

جهت استفاده از این شبکه ها ابتدا بر روی یکی از وبسایت های معتبر همچون mist, myetherwallet و یا با استفاده از برخی افزونه ها مانند Metamask یک کیف پول اتریومی ایجاد نمایید و برای یکی از حساب های متصل به آن از شبکه بلاک چین آزمایشی مورد نظر درخواست اتر آزمایشی نمایید.

همانطور که می دانید هنگام ساخت کیف پول اتریومی تعدادی کلمه بعنوان کد یادآوری یا mnemonic code تولید می گردد که در واقع مشخصه یکتای کیف پول بوده و از طریق یک تابع هش به یک کد باینری که همان کلید خصوصی می باشد نگاشت می یابد. برای ارسال یک تراکنش به شبکه بلاک چین باید آن تراکنش را امضا نمود که این کار از طریق کلید خصوصی انجام می پذیرد. بنابراین جهت بارگذاری یک قرارداد هوشمند در بلاک چین باید کلید خصوصی یا کد یادآوری را بسته به API مورد استفاده فراهم نمود. با توجه به اینکه وارد کردن این کدها در کد به لحاظ امنیتی اشتباه می باشد این کار از طریق یک فرایند config انجام شده است. در این روش ابتدا در power shell نرم افزار vscode کد یادآوری کیف پول بصورت متغیر محیطی یا environment variable ذخیره می گردد. سپس این متغیر توسط برنامه فراخوانی شده و توسط آن عملیات بارگذاری انجام می گیرد. بدین ترتیب کد یادآوری کیف پول توسط کاربر هنگام اجرای عملیات بارگذاری وارد شده و به هیچ وجه در کد ثبت نمی گردد. از طرف دیگر در صورت بسته شدن power shell کد وارد شده از حافظه پاک می گردد.

نهایتاً فرایند بارگذاری قرارداد در بلاک چین بصورت زیر می باشد:

```
$evn: Julia_ropsten_passphrase= “...”
```

```
$evn: Julia_rinkeby_passphrase= “...”
```

که دستور اول جهت وارد کردن کد یادآوری کیف برای بارگذاری در شبکه ropsten و دستور دوم برای شبکه rinkeby می باشد.

سرانجام برای بارگذاری قرارداد در شبکه بلاک چین مورد نظر از دستورهای زیر به ترتیب برای بارگذاری در شبکه های ropsten و rinkeby استفاده می شود:

```
truffle migrate --network ropsten
```

```
truffle migrate --network rinkeby
```

#### - باگذاری قرارداد هوشمند در شبکه بلا چین اصلی:

فرایند بارگذاری در شبکه اصلی هوشمند همانند فراین یاد شده در شبکه های آزمایشی عمومی می باشد. برای این کاری باید دستورهای زیر به ترتیب اجرا گردند:

```
$evn: Julia_mainnet_passphrase= “...”
```

```
truffle migrate --network production
```