دانشگاه تهران
پردیس دانشکده‌های فنی
دانشکده مهندسی برق و کامپیوتر

تمرین کامپیوتری اول

درس ارزهای رمزگذاری شده

مهلت تحویل: 1 خرداد 1402

مقدمه

در این تمرین قصد داریم تا با شبکه‌ی بیت‌کوین به صورت عملی تعامل کنید و در آن تراکنش انجام دهید و سایر مکانیزم‌های بیت‌کوین مانند استخراج بلوک را آزمایش کنید. با توجه به اینکه در شبکه‌ی اصلی بیت‌کوین (Mainnet)، برای انجام تراکنش نیاز به صرف هزینه‌ی واقعی و پرداخت بیت‌کوین (به عنوان کارمزد تراکنش) می‌باشد، موارد خواسته شده را در شبکه‌ی آزمایشی (Testnet) انجام می‌دهید. شبکه‌ی آزمایشی از نظر فنی کاملا مشابه شبکه‌ی اصلی بیت‌کوین است و در صورتی که بتوانید عملیات مد نظر را در این شبکه به طور صحیح به انجام رسانید، این عملیات در شبکه‌ی اصلی نیز قابل اجراست. تفاوت جدی شبکه‌ی آزمایشی و شبکه‌ی اصلی در این است که شبکه‌ی آزمایشی به گونه‌ای طراحی شده است که بیت‌کوین‌های استخراج شده در آن هیچ ارزشی ندارند و ارزش آن‌ها تقریبا برابر صفر است. از این رو توسعه‌دهندگان بیت‌کوین برای طراحی، ساخت و توسعه‌ی امکانات جدید، از شبکه‌ی آزمایشی برای تست کردن این امکانات بدون نیاز به صرف هزینه استفاده می‌کنند. شبکه‌ی آزمایشی، زنجیره‌ی بلوکی منحصر به خود را دارد و مستقل از شبکه‌ی اصلی به کار خود ادامه می‌دهد و هیچ ارتباطی بین این دو زنجیره وجود ندارد و تنها از نظر فنی مشابه یکدیگر می‌باشند.

برای دریافت پول در شبکه‌ی آزمایشی، برخی از وب‌سایت‌ها که Faucet نامیده می‌شوند، با ارائه‌ی آدرس خود در شبکه‌ی آزمایشی به آن‌ها، به شما بیت‌کوین می‌دهند و می‌توانید با آن‌ها موارد خواسته شده در این تمرین را انجام دهید. برخی از Faucet های شناخته شده در بیت‌کوین عبارتند از:

1) https://coinfaucet.eu/en/btc-testnet
2) https://bitcoinfaucet.uo1.net/
3) https://testnet-faucet.mempool.co/
4) https://kuttler.eu/en/bitcoin/btc/faucet/

برای مشاهده‌ی زنجیره‌ی بلوکی شبکه‌ی آزمایشی بیت‌کوین، می‌توانید از مرورگرهای زنجیره‌ی بلوکی زیر استفاده کنید:

1) https://www.blockchain.com/explorer?view=btc-testnet
2) https://blockchair.com/bitcoin/testnet
3) https://live.blockcypher.com/btc-testnet/
4) https://blockstream.info/testnet/

قسمت اول: تولید آدرس

اولین قدم در شروع کار با شبکه‌ی آزمایشی بیت‌کوین، تولید یک آدرس معتبر است. زیرا برای دریافت پول ابتدا می‌بایست یک آدرس معتبر تولید کنید و سپس از آن استفاده کرده و تراکنش‌های لازم را انجام دهید. در بیت‌کوین آدرس با فرمت مشخصی تولید می‌گردد که در آن از توابع رمزنگاری درهم‌ساز SHA-256 و RIPEMD-160 استفاده می‌گردد.

سوال ۱) کدی به زبان پایتون بنویسید تا برای شبکه‌ی آزمایشی، آدرس تولید کند. خروجی این کد می‌بایست یک آدرس به صورت Base58 و کلید خصوصی متناظر با آن به فرم WIF باشد. چه تفاوتی میان آدرس‌های شبکه‌ی اصلی و آزمایشی وجود دارد؟

سوال ۲) کدی بنویسید که یک آدرس ویژه (Vanity Address) تولید کند. این کد با دریافت ۳ کاراکتر، باید آدرسی تولید کرده که با این ۳ کاراکتر شروع شود (با توجه به اینکه کاراکتر اول آدرس مطابق با فرمت بیت‌کوین دارای مقادیر مشخصی است، ۳ کاراکتر دریافت شده باید در جایگاه‌های دوم تا چهارم در آدرس ظاهر شوند). خروجی این کد می‌بایست یک آدرس به صورت Base58 و کلید خصوصی متناظر با آن به فرم WIF باشد.

توجه کنید که فرآیند تولید آدرس می‌بایست به صورت کامل توسط شما پیاده‌سازی گردد استفاده از کدهای موجود در اینترنت مجاز نیست و تنها برای توابع رمزنگاری، تولید اعداد تصادفی، تبدیل مبناها و سایر نیازهای جانبی می‌توانید از کتابخانه‌های موجود استفاده کنید. برای هر سوال یک فایل پایتون ارائه دهید و توضیحات لازم را ارائه دهید.

قسمت دوم: انجام تراکنش

برای انجام تراکنش در شبکه‌ی آزمایشی بیت‌کوین، از کتابخانه‌ی python-bitcoinlib استفاده می‌کنیم. این کتابخانه دارای توابع مختلف برای ایجاد انواع تراکنش است. برای انجام این قسمت از تمرین، ابتدا با نحوه‌ی کار کردن ماشین پشته‌ای بیت‌کوین و Script ها و دستورات آن از روی منابعی که در انتها معرفی شده است و یا سایر منابع معتبر، آشنایی لازم را پیدا کنید. با توجه به اینکه برای انجام تراکنش در بیت‌کوین، نیاز به اتصال به شبکه‌ی توزیع شده‌ی آن است، برای راحتی کار در این تمرین، تراکنش‌ها به API هایی که توسط برخی از وب‌سایت‌های مرورگر زنجیره‌ی بلوکی ارائه شده است، ارسال می‌شود و آن‌ها به نیابت از شما، تراکنش را در شبکه Broadcast می‌کنند. برای شروع یک کد استارتر با عنوان transaction.py قرار داده شده است که با استفاده از آن می‌توانید یک تراکنش با یک ورودی و یک خروجی از نوع P2PKH ایجاد کنید. همچنین در کد util.py برخی توابع کاربردی ایجاد شده است که آدرس API مربوط به Push TX یکی از وب‌سایت‌های معروف نیز در آن قرار داده شده است که در صورت لزوم می‌توانید آن را تغییر داده و تراکنش‌ها را به سایر API های موجود ارسال کنید. در توابع مشخص شده در فایلtransaction.py ، قسمتهای مربوط به scriptSig و scriptPubKey را با داده‌ها و دستورات مناسب در قسمت return کامل کنید تا بتوانید یک تراکنش ساده با آن انجام دهید. با استفاده از کدهای قسمت اول تمرین و یا استفاده از تولیدکننده‌های آنلاین آدرس، برای شبکه‌ی آزمایشی بیت‌کوین آدرس ایجاد کرده (آدرس مورد استفاده را به همراه کلید خصوصی آن در گزارش خود ذکر کنید) و پس از دریافت پول از Faucet ها، تراکنش‌های زیر را انجام دهید (لازم است برای هر سوال، علاوه بر توضیحات لازم، ۲ فایل پایتون که در واقع نسخه‌هایی از فایل transaction.py هستند ارائه دهید که یکی برای تراکنش ایجاد UTXO های مورد نظر و دیگری برای تراکنش خرج کردن آن‌ها باشد):

سوال ۱) تراکنشی با یک ورودی و دو خروجی ایجاد کنید که خروجی اول آن توسط هیچکس قابل خرج شدن نباشد و خروجی دوم آن توسط هر شخصی قابل خرج شدن باشد. در تراکنشی دیگر خروجی قابل خرج این تراکنش را خرج کرده و به آدرس اصلی خود به صورت خروجی P2PKH بازگردانید.

سوال 2) سه آدرس جدید تولید کنید و مشخصات آن را در گزارش ذکر کنید. تراکنشی ایجاد کنید که یک ورودی و یک خروجی داشته باشد که خروجی آن از نوع P2MS یا Multisig بوده و توسط ۲ نفر از این ۳ آدرس آن قابل خرج شدن باشد. در تراکنشی دیگر این خروجی را خرج کرده و پول آن را به آدرس اصلی خود بازگردانید.

سوال 3) دو عدد اول مثال بزنید و آن دو را در گزارش خود درج کنید. حاصل جمع و حاصل تفریق آن‌ها را حساب کنید. یک تراکنش با یک ورودی و یک خروجی تولید کنید به گونه‌ای که در

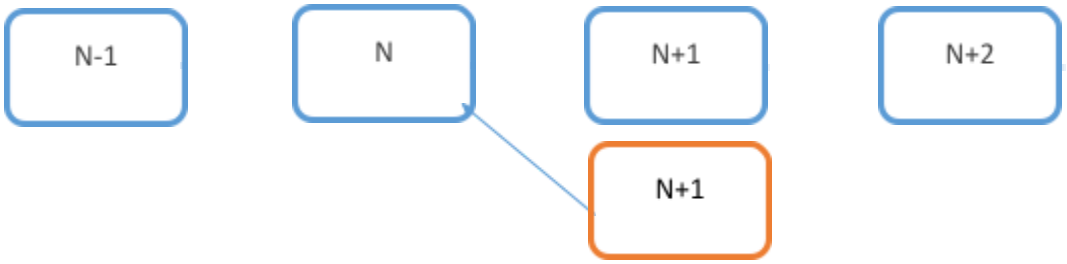
خروجی آن، حاصل جمع و حاصل تفریق این دو عدد به همراه دستورهای لازم در scriptPubKey قرار گرفته باشد به گونه‌ای که تنها فردی بتواند این UTXO را خرج کند که هر دوی این اعداد را داشته باشد. سپس یک تراکنش دیگر ایجاد کنید که در ورودی آن در قسمتscriptSig ، با ارائه‌ی این دو عدد اول، بتواند UTXO را خرج کند و پول دوباره به حساب اصلی شما برگردد.

سوال 4) یک تراکنش ایجاد کنید که یک ورودی و دو خروجی داشته باشد که یکی از آن خروجی‌ها توسط هیچ فردی به هیچ عنوان قابل خرج کردن نباشد و یکی از این خروجی‌ها توسط تمامی اشخاص قابل خرج کردن باشد.

لازم است که در تمامی سوالات مشخصات کامل آدرس‌های استفاده شده شامل کلید خصوصی آن‌ها به فرم WIF و شناسه‌ی تراکنش‌ها را به طور کامل در گزارش خود ذکر کنید.

قسمت سوم: استخراج بلوک

در این بخش با فرآیند استخراج بلوک و ساختار بلوک به صورت عملی آشنا می‌شوید. با توجه به اینکه فرآیند استخراج احتیاج به تجهیزات محاسباتی بسیار قوی دارد، این کار را به صورت متفاوتی انجام خواهید داد. این بخش می‌بایست بر روی یکی از بلوک‌های قدیمی در بیت‌کوین، یک انشعاب (Fork) ایجاد کنید.



ابتدا بلوک n را در نظر بگیرید. این بلوک یکی از بلوک‌های قدیمی روی زنجیره‌ی بلوکی شبکه‌ی **اصلی** بیت‌کوین است. شماره‌ی بلوک انتخابی میبایست، ۴ رقم سمت راست شماره‌ی دانشجویی شما می‌باشد.به طور مثال اگر شماره‌ی دانشجویی شما 810198765 است، بلوک 8765 را انتخاب کنید. حال باید بلوک n+1 (بلوک 8766) را طوری بر روی این بلوک بنا کنید که دارای شرایط زیر باشد:

- دارای تنها یک تراکنش باید که آن تراکنش همان تراکنش coinbase است که پاداش بلوک را به شما تخصیص می‌دهد.
- در متنcoinbase data که در تراکنش coinbase قرار دارد، باید شماره‌ی دانشجویی خود را به همراه نام و نام خانوادگی خود به صورت ASCII درج کنید. به طور مثال شماره‌ی دانشجویی 810198765 با نام امیر امیری به صورت ASCII و Hex به این صورت می‌باشد:

0x383130313938373635416d6972416d697269

که معادل متن زیر است:

810198765AmirAmiri

- تراکنش coinbase که حاوی پاداش استخراج است، تنها شامل یک خروجی باشد که به یک آدرس معتبر در شبکه‌ی اصلی بیت‌کوین اختصاص داده شود. برای تولید آدرس می‌توانید از کدهای قسمت اول تمرین و یا سایت‌های آنلاین تولید آدرس بیت‌کوین استفاده کنید. (مقدار پاداش باید مطابق پروتکل بیت‌کوین تعیین گردد)
- سایر بخش‌های بلوک مانند هش بلوک قبلی و هش درخت مرکل باید به درستی تنظیم گردد. در واقع بلوک باید به صورت صحیح ایجاد شده و توسط سایر miner ها قابلیت validate شدن داشته باشد.

- با تنظیم nonce به گونه ای بلوک را استخراج کنید که هش بلوک در فرمت hex با ۴ صفر (۱۶ صفر به صورت بیتی) شروع شود.

کدی بنویسید که با دریافت بلوک n، مطابق شرایط گفته شده در بالا، بلوک n+1 را استخراج کرده و اطلاعات بلوک استخراج شده شامل:

- تمامی اطلاعات و فیلدهای ذخیره شده در بلوک به صورت human readable (مشابه سایت‌های مرورگر زنجیره‌ی بلوکی)
- هش بلوک به صورت hex
- کل بلوک به صورت raw و به فرمت hex

را نمایش دهد. برای دریافت بلوک n (مطابق شماره دانشجویی که در بالا توضیح داده شد)، می‌توانید از سایت‌های مرورگر زنجیره‌ی بلوکی استفاده کرده و بلوک را به صورت hex و به طور دستی دریافت کنید و hex آن را صورت دستی به عنوان ورودی به برنامه‌ی خود بدهید. برای آشنایی با ساختار بلوک به لینک مراجع کنید.

به طور مثال بلوک 8765 از طریق آدرس زیر به صورت raw hex قابل دریافت است:

https://blockchain.info/block/8765?format=hex

در این بخش می‌توانید از تمامی کتابخانه‌های موجود استفاده کنید. اما فرآیند ساخت درخت مرکل و استخراج بلوک می‌بایست به صورت کامل توسط شما پیاده‌سازی شود. همچنین ساخت بلوک به صورت local کفایت کرده و نیازی به ثبت آن در شبکه نیست.

برای اطلاعات بیشتر در مورد فرم WIF به لینک زیر مراجعه کنید:

https://learnmeabitcoin.com/technical/wif

برای اطلاعات بیشتر در مورد آدرسهای بیت‌کوین به لینک زیر مراجعه کنید:

https://en.bitcoin.it/wiki/Address

برای اطلاعات بیشتر در مورد پیشوند آدرس در بیت‌کوین به لینک زیر مراجعه کنید:

https://en.bitcoin.it/wiki/List_of_address_prefixes

برای آشنایی بیشتر با دستورات بیت‌کوین و نحوه‌ی کار کردن ماشین پشته‌ای آن به لینک زیر مراجعه کنید:

https://en.bitcoin.it/wiki/Script

برای اطلاعات بیشتر در مورد ساختار بلوک به لینک زیر مراجعه کنید:

https://en.bitcoin.it/wiki/Block

نکات تمرین

1. مهلت انجام این تمرین تا **روز دوشنبه اول خرداد** است.
2. **در این تمرین، گزارش کتبی شما ملاک اصلی نمره‌دهی می‌باشد.** از این رو تمامی موارد شامل توضیحات لازم و موارد خواسته شده، روند انجام، نتایج حاصل، آدرس‌های به کار رفته به همراه کلید خصوصی آن‌ها و شناسه‌ی تراکنش‌ها را در گزارش ارائه دهید. **در کنار گزارش کتبی، ارسال کدها نیز الزامی می‌باشد.**
3. برای ثبت تراکنش در زنجیره‌ی بلوکی، باید مبلغی مناسبی را به عنوان کارمزد تراکنش بپردازید. لذا در تنظیم مقادیر ورودی و خروجی تراکنش، این مساله را لحاظ کنید تا تراکنش شما با موفقیت در زنجیره‌ی بلوکی شبکه‌ی آزمایشی بیت‌کوین درج گردد. اختلاف مجموع مقادیر ورودی و خروجی تراکنش به عنوان کارمزد تراکنش برای استخراج کننده‌ی آن در نظر گرفته می‌شود.
4. نمره‌ی سوالاتی که مربوط به انجام تراکنش است، تنها در صورت ثبت تراکنش‌های خواسته شده در زنجیره‌ی بلوکی شبکه‌ی آزمایشی بیت‌کوین تعلق می‌گیرد و در صورت عدم ثبت شدن تراکنش

در زنجیره‌ی بلوکی و یا عدم استخراج آن، نمره‌ای دریافت نمی‌کنید. **از این رو از ثبت شدن کامل تراکنش‌ها در زنجیره‌ی بلوکی و استخراج آن توسط ماینرها و پایدار شدن آن (سپری شدن ۶ بلوک) اطمینان حاصل نمایید و شناسه‌ی تراکنش‌ها را در گزارش خود ارائه دهید.**

5. در سوالاتی که مربوط به انجام تراکنش است، **ارائه کلید خصوصی به صورت WIF برای آدرس‌هایی که در انجام تراکنش‌ها از آن استفاده کردید الزامی می‌باشد**، زیرا نشان‌دهنده‌ی آن است که این آدرس‌ها متعلق به شماست. **در غیر این صورت تراکنش متعلق به فرد دیگری تلقی گردیده و نمره‌ای بابت آن دریافت نخواهید کرد.**
6. فایل نهایی خود را شامل گزارش کامل به صورت PDF و همچنین کدهای خود به صورت جداگانه برای هر سوال را در قالب یک فایل فشرده‌ی zip با درج شماره‌ی دانشجویی به صورت StudentID.zip ارسال کنید.
7. در صورت داشتن هر گونه سوال، پرسش و یا ابهام، از طریق ایمیل shayanhamidi2000@gmail.com پرسش‌های خود را مطرح کنید.