به نام خدا

تمرین کامپیوتری اول مبانی رمزارزها

محمدحسین ارسلان

سروش یوسفی

ابتدا به بررسی کلیت کد سالیدیتی ارائه شده برای قرارداد هوشمند طراحی شده برای این سوال می‌پردازیم و پس از بررسی و معرفی متغیرها و توابع به‌کار رفته در کد یک اجرا و دیپلوی از آن روی شبکه بلاکچین خواهیم دید.

متغیرها

```
uint number_of_voters = 0;
    uint maximun_number_of_voters;
    // uint number_of_candidates = 100;
    uint date_of_start;
    uint date_of_end;
    uint number_of_registered;
    string title;
    string[] candidates;
    mapping (address => Voter) voters;
    mapping (string => uint) votes; // candidates must be
added to this map too
    address public Abbas;
```

بیشینه تعداد افراد مجاز برای رای دادن. تاریخ شروع و پایان رای گیری که بصورت عددی است و به کمک Timestamp تعیین می‌شود. تعداد ثبتنامی‌ها و آرایه‌ای از جنس رشته حاوی نام کاندیدها است. دو مپ در این تمرین استفاده کرده‌ایم یکی آدرس ولت هر رای‌دهنده را به رای دهنده مپ می‌کند (رای دهنده خود دارای یک struct مجزا است)، مپ دیگری هم داریم که نام هر کاندید را به تعداد آراء کسب کرده‌اش مپ می‌کند. همچنین مسئول انتخابات طبق صورت تمرین عباس می‌باشد و یک آدرس ولت به‌نام او خواهیم داشت.

در Structیی که برای voterها داریم، نام منتخب رای دهنده، بولینی برای دانستن این که فرد ثبتنام شده است یا خیر توسط مسئول و همچنین یک عدد که بیانگر تعداد آرای قابل ثبت توسط voter است (این مورد برای سهولت در انتقال حق رای تعیین شده است) قرار دارند.

یکسری تابع اضافه که در طول پیشرفت تمرین برای دیباگ ایجاد کردیم در تمرین هست که ترجیح دادیم بمانند. یک تابع به ما تعداد آرای ثبت شده تا لحظه فراخوانی را می‌دهد، یک تابع اتمام یا عدم اتمام زمان را به ما می‌دهد و ...

از توابع اصلی تمرین می‌توان به move_vote_right اشاره کرد که به‌عنوان ورودی، یک آدرس ولت می‌گیرد و اگر فرد صدازننده تابع حق رای داشته باشد و همچنین فرد مقصد هم اجازه رای داشته باشد، این حق رای به فرد مقصد اهدا می‌شود.

تابع ثبت‌نام رای دهندگان هم توسط مسئول انتخابات (عباس) قابل صدا زدن است. محدودیت‌هایی که موجب ملغی شدن رای‌گیری می‌شود به کمک require در این تابع هندل شده است.

تابع ثبت رای نیز در ورودی خود نام فرد منتخب را می‌گیرد و بعد از بررسی حق رای صدا زننده (msg.sender) و همچنین تعداد رای‌های باقی‌مانده آن فرد، رای او را ثبت می‌کند.

تابع اعلام نتیجه هم با یک for بررسی می‌کند رای بیشینه از آن چه کسی است و همچنین تعداد رای‌های ثبت شده را می‌شمارد و بعد از بررسی مشروعیت انتخابات نام برنده را اعلام می‌کند.

نکات جانبی

رای باطله هم امکان‌پذیر است و می‌توان به هر نام دلخواه رای دهد اما اگر آن فرد کاندید نباشد رای شمرده نمی‌شود، انتخاباتی که مشارکت حداقل ۵۰ درصدی را داشته باشد (حتی اگر باطله‌ها بیشتر از رای‌های صحیح باشند) مشروع است و اعلام نتیجه صورت می‌پذیرد.

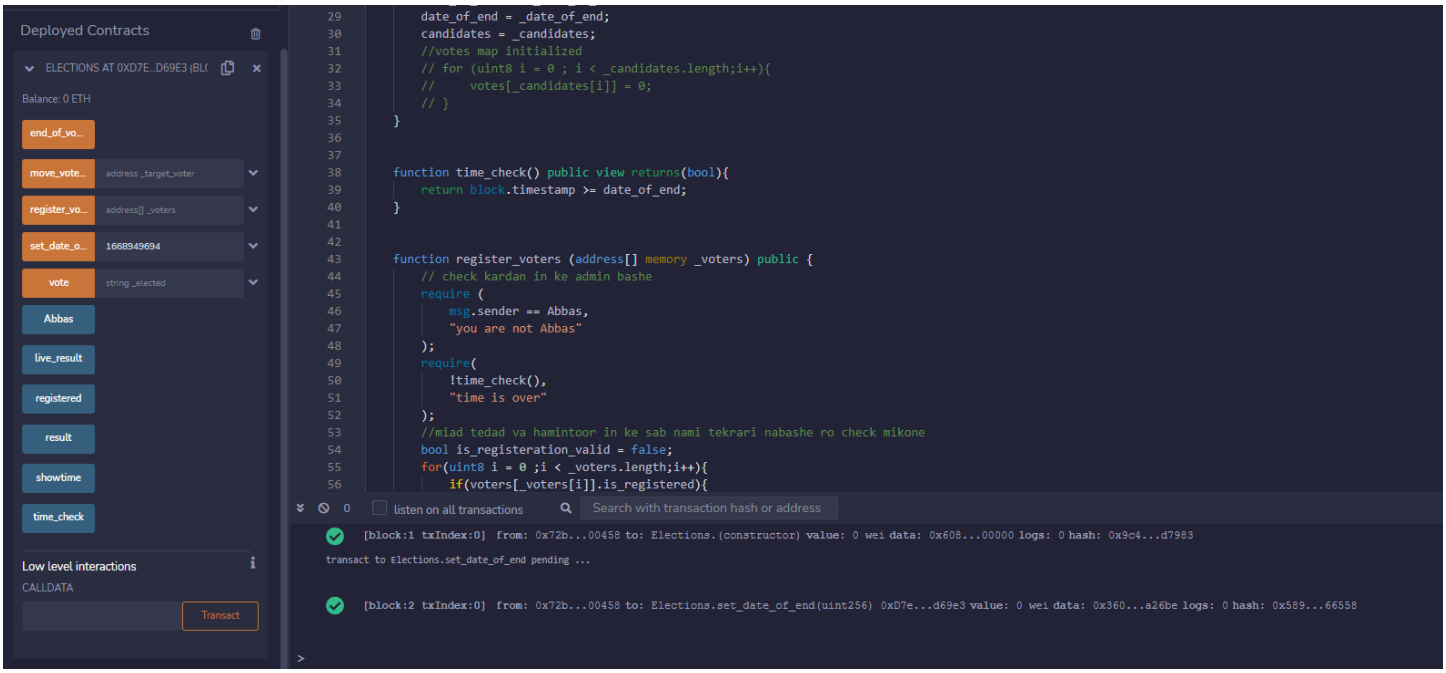
مشکل block.timestamp برای دریافت timestamp در لحظه این بود که زمان آخرین تغییر در بلاک را ارائه می‌کرد که خب این مورد در پایان رای‌گیری مشکل ایجاد می‌کرد از این رو با تابع end_of_voting که توسط مسئول قابل صدا زدن است، پایان رای‌گیری ثبت شده و از این رو timestamp هم بروز می‌شود و end_date هم برابر با timestamp می‌شود تا بتوانیم اعلام نتیجه را فراخوانی و مشاهده کنیم.

تست و دیپلوی

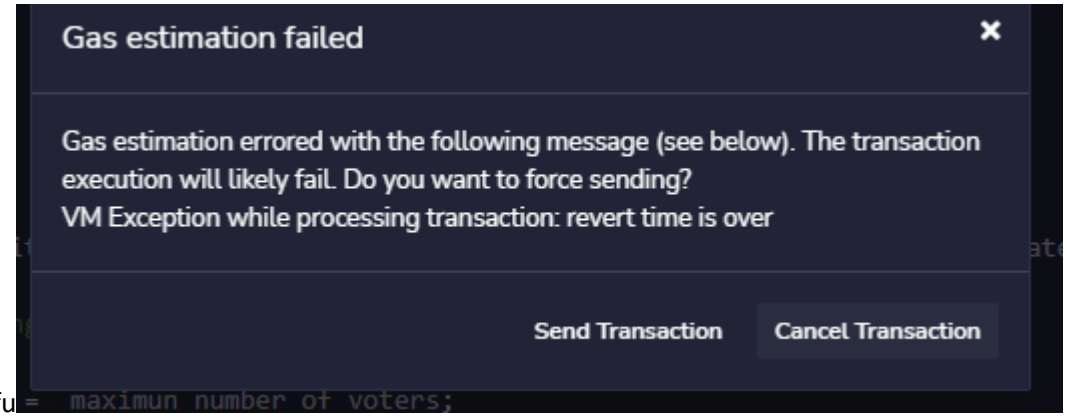
برای تست این اجرا روی پورت ۳۰۰۰ لوکال‌هاست کار می‌کنیم.

ابتدا باید مقدار آدرس را بر روی remix نیز تنظیم کنیم. در فایلی که همراه پروژه نیز هست ، مقادیر مناسب برای دیپلوی کد آورده شده است. کانستراکتور کد یک عنوان ، تعداد بیشینه رای دهندگان ، تاریخ شروع ، تاریخ پایان و همچنین آرایه کاندیدا ها را میگیرد و روی شبکه آن را دیپلوی می کند. برای مثال برای دیپلوی آن Abbas's Election,5,1668937682,1668943020,[A,B,C] مناسب است. تاریخ های داده شده به صورت یونیکس تایم استمپ است.

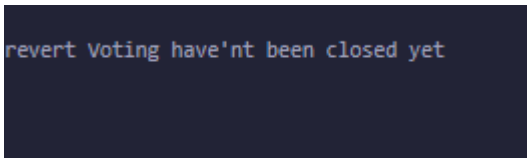
در این جا برای مثال اجرای تمدید انتخابات را که به صورت درست انجام شده است ، مشاهده می کنیم.



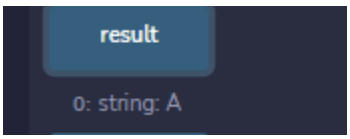
سپس اقدام به ثبت نام کردن تعدادی رای دهنده میکنیم. به دلیل تاخیر، باید با ارور مواجه شویم که برنامه ارور را به درستی شناسایی می کند.



بعد از ثبت نام کردن کاربران ، اقدام به رای دادن به تابع vote می کنیم. سپس اگر بر روی result برای مشاهده نتایج کلیک کنیم ، مشاهده می شود که ارور تمام نشدن زمان را می دهد که درست است.



سپس بر روی Abbas سوییچ می کنیم و بر روی end_of_vote میزنیم و نتایج را مشاهده می کنیم.



به دلیل این که تایم استمپ تاریخ آخرین تراکنش را بر میگرداند ، مجبور به استفاده از end_of_vote شدیم (در بالا توضیح داده شده است) .

در پایین نیز لیست والت ها را مشاهده می کنیم که به دلیل انجام تراکنش ، مقدار اولیه حساب عباس کم شده است. (اولین پابلیک کی)

ADDRESS	BALANCE	TX COUNT	INDEX	
0×72b7a6Bf4bf961Ea2Bc32c235F890e8599200458	99.92 ETH	7	0	
ADDRESS	BALANCE	TX COUNT	INDEX	
0×FA199Cf35fB5Eb8477476930A3f24513f52c5AC6	100.00 ETH	1	1	
ADDRESS	BALANCE	TX COUNT	INDEX	
0×97D0B67aD0a7fD7d136b589Ffc55C6838Df94f49	100.00 ETH	1	2	