My個運彩!

使用智能合約管理運彩販售系統

陳敬翔 劉有楷 神黃咸恆



期中Proposal時我們想這麼做

- 1. ERC721--NFTs:
- a.彩券紀錄不能被竄改
- b.智能合約使得獎金自動支付。
- c.模彷 FOMO3D, 最後購買者將獲巨額獎金。(一場比賽兩個賭局)
- d.彩券可在交易前在告示板上自由搓合。
- e.開獎紀錄儲存於區塊鏈內。
- 2.智能合約:
- a.在比賽前一個小時結束販賣(鎖定賠率)。
- b.比賽結束後, 比賽結果觸發合約, 獎金自動支付。
- 3.使用爬蟲抓取比賽結果(or Orcale Machine, if possible)



但是....

- 原本要建立兩個市場 一個是一級市場 買家可以向莊家購買彩票; 還有一個二級市場 買家之間可以自由交易直到比賽開始前一小時⇒發現太複雜到期末前來不及完成
- 2.因為對於Orcal Machine不夠熟悉不敢貿然使用⇒這次我們使用網頁爬蟲搭配 Web3.py跟合約溝通
- 3. 原計畫是設計一個系統使買家可以直接跟系統互動, 購買彩券⇒ 我們將多數時間 花在智能合約編寫, 前端投入少量時間使得前端比較陽春, 這次proposal不會呈現

期末Proposal 修正為

1.有兩種合約 Hub跟 TicketSale; 使用 母合約Hub 來為當日比賽的 隊伍建立 TicketSale 子合約, 其 Host 為 Hub 合約地址、以及建立 Hub 合約的人。

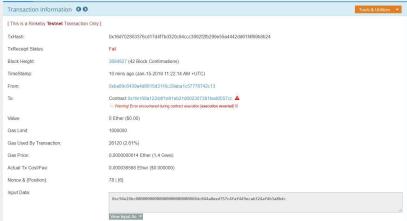


Write Contract	[Reset]
1. createEvent	
name (string)	
波士頓塞爾提克	
startTime (uint256)	
1545696000	
dueTime (uint256)	
1546246200	
price (uint256)	
10000000000	
Write	

期末Proposal 修正為

2.勝負的判定由爬蟲搭配web3.py, 先從Hub合約中取得兩方的 TicketSale合約地址, 得知比賽結果後分別呼叫兩個TicketSale合約 裡面的Win函數, 將勝隊位址傳入





Demo

Bitbucket: https://bitbucket.org/Starfine/nccu10/src

HackMD:

https://hackmd.io/ZOnV7mGcT5i3x-plXgsBjw?view



執行中我們面臨哪些問題

- 1.因為智能合約無法直接 Print 變數, 所以 Debug 很困難, 而且部署之後也還是無法直接從 TX 上看到變數⇒只能不斷的 Try 和 Error 到成功為止, 或是用 Event(但 Event 要花更多時間去額外寫 WSS 去監聽, 所以就作罷)
- 2. Web3.py 在把勝隊位址餵進ticketsale合約的時候會有一個error, 似乎是因為web3.py 合約不在TicketSale這張合約的Host列表中
- ⇒ 透過共用private key解決這個問題

3. 只有勝隊的合約會交易成功, 敗隊的會被reverted, why?

My個運彩!

使用智能合約管理運彩販售系統

陳敬翔 劉有容 楊立辉 神鐸 黄咸恆