

民間區塊鏈2019區議 會選舉

[HTTP://HKDISTRICTELECTION.ONLINE/](http://HKDISTRICTELECTION.ONLINE/)

FIGHT FOR FREEDOM, STAND WITH HONG KONG

目錄

- 1) 為何設立這個選舉
- 2) 選舉系統設計
- 3) 如何投票
- 4) 如何成為票站
- 5) 如何幫助我們

為何設立這個選舉

自2019年6月起, 香港人為守護自己的權利和自由開始左反對《逃犯條例》修訂草案運動.

2019年11月24日是區議會選舉的日子, 表達民意的大好機會.

但香港有不少人擔心政府會取消區議會選舉, 或者延遲部分地區選舉, 保障建制派的議席.

我們利用以太幣為基礎的區塊鏈智能合約做了這個民間區塊鏈2019區議會選舉, 確保香港人, 特別是使用網絡的年輕人, 能夠表達對區議會以至政府的意見.

所有程式碼和運作都會公開透明, 又盡量確保結果公平公正.

選舉系統目標

- 1) 每人只能在一個選區投一票, 不能重覆投票
 - 如何認證一個選民?
 - 如何保證不會重覆投票?
 - 如何確保一個人不能被其他人代為投票?
- 2) 不能從選票得知是誰投票
- 3) 選舉期間能夠知道投票統計, 但只有選舉後才有可能知道結果
 - 所有選票均被加密, 選舉後才使用預設的解密鑰解密
 - 選舉期間沒有人能夠私自打開票站拿取選票解密

選舉系統目標

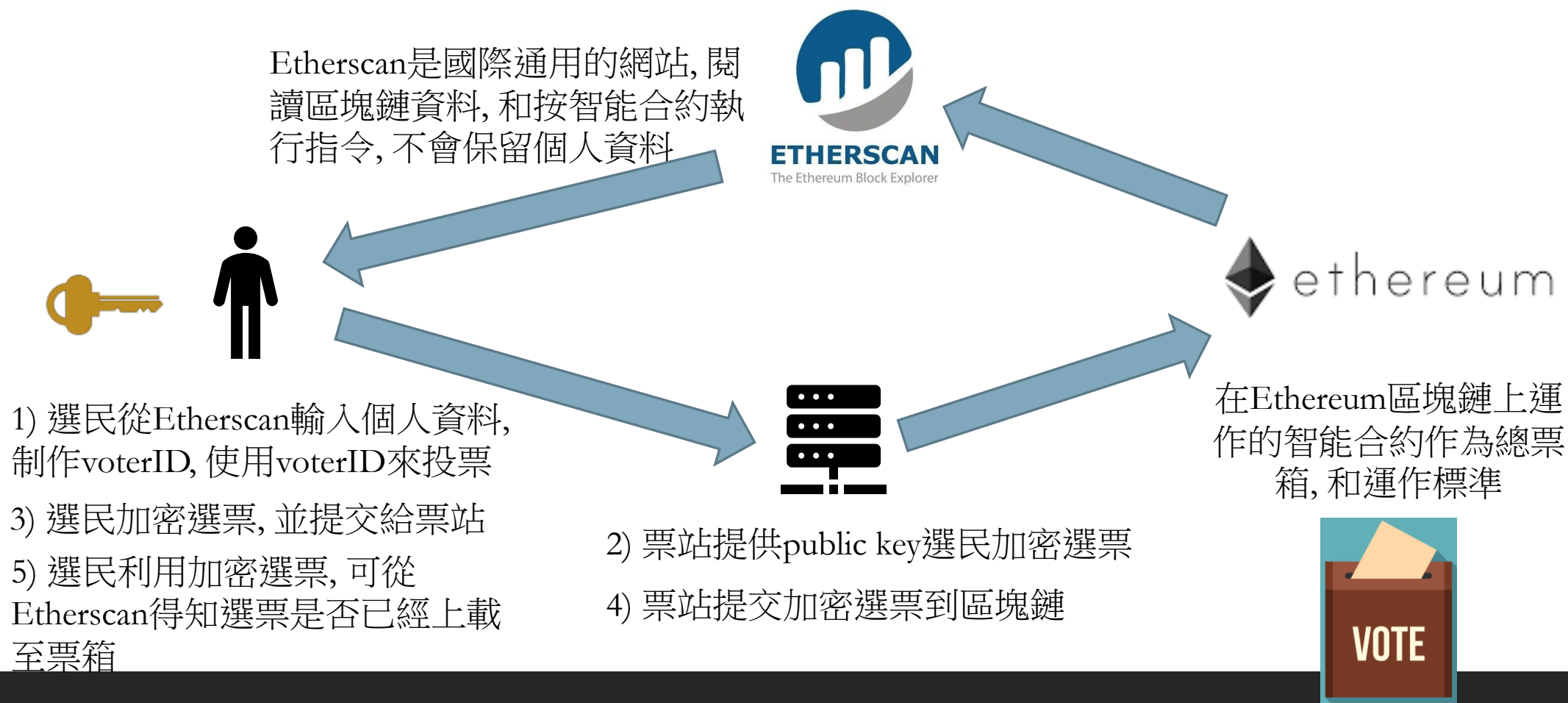
4) 執行選舉的人無力控制選舉

- 香港之前發生過整個票站的票消失, 只剩由職員的點票記錄
- 確保票站不能控制選票, 或刪除選票
- 如發現有票站做假, 可令票站的選票無效而要求選民在另一票站投票

5) 確保選舉能夠進行

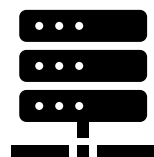
- 因不是政府所舉行, 非常有機會被中國政府為首的組織攻擊
- 從過去經驗可知, 攻擊力極強, 一般組織無可能對抗維持服務

選舉系統設計



選舉系統設計2

選舉private key公開,任何人都可以
解密區塊鏈資料,得知選舉結果



ethereum



ETHERSCAN
The Ethereum Block Explorer



選舉後票站打開,所有加
密選票公開予大眾



Etherscan是國際通用的網站,閱
讀區塊鏈資料,和按智能合約執
行指令,不會保留個人資料

為何使用區塊鏈?

完全公開運作, 無人能控制

- 由區塊鏈運行, 所有人得到的資訊都是一樣的, 包括選舉發起人

滿足要求 4

- 票站只能機械式地提交選票, 和提供公開資料, 選民也可以選擇在任意票站投票
- 票站不可能事先得知或修改選票, 也不能把獲得的選票隱瞞不上交票箱
- 選民隨時知道自己選了票沒有, 如有記錄加密選票更隨時有查閱選票是上交區塊鏈
- 大眾可以隨時從區塊鏈看到票站投票情況, 一旦某個票站有可疑可以把來自該站的票取消

滿足要求 5

- 只要Ethereum能夠運作, 香港人能上網, 選舉就能順利舉行
- 從最極端的情況, 就算所有票站網站被封, 人們也能直接聯絡票站負責人提交選票, 沒有私人資料外流, 選舉正常運作

如何滿足其他要求?

要求3 區塊鏈合約決定了只有選舉後才公開已加密的選票

- 同時實時提供選舉統計
- 選舉發起人只能被動地等待選舉完結然後公開所管有的private key, 該全世界能解密選舉結果

要求2 投票是使用voterID, 由選民資料 (身份證號碼) 和其他資料藉SHA256 hashing產生, 單從voterID不能得知選民資料

- 另一方面, 只有知道一個人的HKID才能投票

選舉限制: 要求1

今次選舉名冊保密, 一般人無需得知一個人是否選民, 和那一個選區

沒有辦法在電子世界認證一個人的身份

- 在香港沒有實行數碼個人身份 → 無法在電子世界認證一個人
- 就算在現實世界, 身份證的防偽特徵也只有政府部門能核實

只能假定得知有效身份證號碼的便是選民, 選區由選民決定

- 同一身份證的人會有同一voterID → 不能重複投票
- 當有人發現自己被人假借身份投票, 可聯絡票站把特定voterID的選票取消, 然後再投票
- 當有人發現自己的投票被取消, 也可要求重新投票
- 減少偽冒投票的機會, 但也增加工作量和票站權力, 和令選舉後人們有可能追查特定人士的投票

當有辦法有效認證一個人, 便能取消重複投票機制, 更保證選票和選民完全分離



選舉流程

<http://hkdistrictelection.online/>

試運 2019年11月17日晚上10點開始至22日晚上10點 Test polling from 10pm 17th to 10pm 21th Nov 2019

公佈試運投票結果22日晚上11點 Announce the test polling result at 11pm 21th Nov 2019

正式投票 2019年11月24日早上7點半開始至24日晚上10點半 Real polling from 7:30am 24th to 10:30pm 24th Nov 2019

公佈正式投票結果25日晚上12點01分 Announce the election result at 12:01am 25th Nov 2019

<http://hkdistrictelection.online/>

如何投票?

1) 到Etherscan.io 使用選舉智能合約, 輸入中文全名和身份證號碼以得到選民號碼 (VoterID)

<https://etherscan.io/address/0x63ae1FC0907d8BaBFB1E4015655C3ED09f3d8C7a#readContract>

2) 到 <http://hkdistrictelection.online/voting.html>, 或任意一個票站網站, 填寫 voterID和電郵, 得到電郵驗證碼, 填寫選票得到加密選票

3) 記錄加密選票, 並按上載, 上載選票

4) 利用加密選票在選舉智能合約檢查選票情況

如何投票

10. getVoterID

name (string)

陳大文

HKID (string)

G123456A

Query

↳ uint256

[getVoterID method Response]

» uint256 : 24622587317983017394856615978927968013939490922389582995549819146417565083864

如何投票

2) 輸入電郵. 我們將發送一個驗證碼到你的電郵. 確保你是真人和沒有投過票. Input email, we will send you a verification code to make sure you are real person and have not been voted before.

Put your email here
發送驗證碼 Send verification code

3) 填寫選票並加密 Fill-in the vote and encrypt

輸入VoterID Input VoterID

輸入VoterID Input VoterID

輸入驗證碼 Input verification code

輸入驗證碼 Input verification code

選擇選區 Select the council to vote

選擇候選人 Select candidate

加密 Encrypt

加密選票號碼. 如保留此號在Etherscan查證選票是否有效. 和有問題時追查用. 因存有你的投票選擇. 勿把此號分享給他人. Encrypted vote, please keep this vote to check if your vote is submitted on Etherscan and problem tracing. As this vote contains your voting choice, please this vote private.

4) 提交選票 Submit the vote to blockchain

提交選票 Submit the vote

提交選票交易記錄. 當顯示成功即你的選票已經成功繳交. Vote submission transaction. When the transaction is confirmed. Your vote has been submitted.

如何投票

Email verification code for Folk Hong Kong 2019 District Council Election

收件箱 x



non-reply@hkdistrictelection.online

收件者：secondphoneJune2019 ▾

下午11:52 (0 分鐘前)



🇺🇸 英文 ▾ > 中文(繁體) ▾ 翻譯郵件

關閉以下語言的翻譯功能：

Dear sir or madam,

Thank you for using our service. Your code is **57836081**

Please copy this code into the verification code field when encrypt and submit the vote.

Folk Hong Kong 2019 District Council Election



回覆



轉寄

如何投票, 得到加密選票

2) 輸入電郵, 我們將發送一個驗證碼到你的電郵, 確保你是真人和沒有投過票. Input email, we will send you a verification code to make sure you are real person and have not been voted before.

secondphoneJune2019@gmail.com
發送驗證碼 Send verification code

3) 填寫選票並加密 Fill-in the vote and encrypt
輸入VoterID Input VoterID

78267797985477011236300365729907352616284657272517151278402105028539

輸入驗證碼 Input verification code

57836081

選擇選區 Select the council to vote

中環

選擇候選人 Select candidate

許智峯

加密 Encrypt

加密選票號碼, 如保留此號在Etherscan查證選票是否有效, 和有問題時追查用. 因存有你的投票選擇, 勿把此號分享給他人. Encrypted vote, please keep this vote to check if your vote is submitted on Etherscan and problem tracing. As this vote contains your voting choice, please this vote private.

UQZnKzch5mHjM98dqEMJk/5LnZgOgRem8E3cQlhbCGuQy/wKDZ8h5jIXpYql59e6wAb
oXEqbKdmJrSnT6iyeuQ==

如何投票, 發送加密選票和查看發送情況

vote private.

UQZnKzch5mHjM98dqEMJk/5LnZgOgRem8E3cQlhbCGuQy/wKDZ8h5jIXpYql59e6wAb
oXEqbKdmJrSnT6iyeuQ==


4) 提交選票 Submit the vote to blockchain

提交選票 Submit the vote

提交選票交易記錄. 當顯示成功即你的選票已經成功繳交. Vote submission transaction. When the transaction is confirmed. Your vote has been submitted. [Check the upload status.](#)

如何投票, 發送加密選票和查看發送情況

← → ↺ etherscan.io/tx/0x0b856f0ab448dcaff30c20b59638884f3178294e38d132e853adbc59f0ffee29

 All Filters ▾ Search by Address / Txn Hash / Block / Token / Ens







Eth: \$176.74 (+0.90%) Home Blockchain ▾ Tokens ▾ Resources ▾ More ▾

Transaction Details

Buy ▾ Earn Interest ▾

💡 Feature Tip: 💰 DEFI - Track your [Compound & Maker loans](#) on Etherscan! 🔍

Overview State Changes Comments

Transaction Hash:	0x0b856f0ab448dcaff30c20b59638884f3178294e38d132e853adbc59f0ffee29 
Status:	 Success
Block:	8969007 31 Block Confirmations
Timestamp:	🕒 7 mins ago (Nov-20-2019 03:01:31 PM +UTC)
From:	0x0fe7c97d52d49a6249ac4ffab6e8e700b1c7e22d 
To:	Contract 0x63ae1fc0907d8babfb1e4015655c3ed09f3d8c7a  
Value:	0 Ether (\$0.00)
Transaction Fee:	0.0004894764 Ether (\$0.09)
Click to see More	
Private Note:	To access the Private Note feature, you must be Logged In

如何投票, 發送加密選票和查看發送情況

Block:

8969007 31 Block Confirmations

Timestamp:

7 mins ago (Nov-20-2019 03:01:31 PM +UTC)

From:

0x0fe7c97d52d49a6249ac4ffab6e8e700b1c7e22d

To:

Contract 0x63ae1fc0907d8babfb1e4015655c3ed09f3d8c7a

Value:

0 Ether (\$0.00)

Transaction Fee:

0.0004894764 Ether (\$0.09)

Gas Limit:

450,000

Gas Used by Transaction:

407,897 (90.64%)

Gas Price:

0.0000000012 Ether (1.2 Gwei)

Nonce

Position

14 124

Input Data:

Function: registerAndVote(uint256 voterID, uint256 hashedEmail, string council, string singleVote)

MethodID: 0xfc1372d5

[0]: dd87b5db8e617a9bca1a69021089b5fe4ae720ebd5bd6d291ef4cfbfb2bc1063

[1]: f0224f243c1a3b1aa41b6101afe913edc6057f77a9c3c928da35bc554a88ba2c

[2]: 00

[3]: 00

[4]: 0009

[5]: e79fh3e5a198e5928000

View Input As

Decode Input Data

[Click to see Less](#)

如何投票, 發送加密選票和查看發送情況

etherscan.io/tx/0x0b856f0ab448dcaff30c20b59638884f3178294e38d132e853adbc59f0fee29

Status: Success

Block: 8969007 31 Block Confirmations

Timestamp: 7 mins ago (Nov-20-2019 03:01:31 PM +UTC)

From: 0x0fe7c97d52d49a6249ac4ffab6e8e700b1c7e22d

To: Contract 0x63ae1fc0907d8babfb1e4015655c3ed09f3d8c7a

Value: 0 Ether (\$0.00)

Transaction Fee: 0.0004894764 Ether (\$0.09)

Gas Limit: 450,000

Gas Used by Transaction: 407,897 (90.64%)

Gas Price: 0.0000000012 Ether (1.2 Gwei)

Nonce: 14 Position 124

Input Data:

#	Name	Type	Data
0	voterID	uint256	100200919025958488839831908808408670094900968802416560410757543616027071090787
1	hashedEmail	uint256	108615702675035403005075036635956616240558963782079244732105312965567487457836
2	council	string	石塘咀
3	singleVote	string	HEoHDhx3k0qmsgJ1Sb9bw8tica+2p2hXuFL90+uBfVUETspRc+sK8ia2u3rbAe16/L7AWHdwUn9TA6kDIGuhQg==

Decoded input inspired by Canoe Solidity

Switch Back

Click to see Less

如果投票不成功 (Failed), 如何尋找原因

OverviewState ChangesComments

Transaction Hash:

0xcc2208892e64614d252d8a932d9965fb1e501a9f683cfb917bd55f39afa1afa8

Status:

✖ Fail

Block:

8968331

987 Block Confirmations

Timestamp:

🕒 3 hrs 45 mins ago (Nov-20-2019 12:29:21 PM +UTC)

From:

0x0fe7c97d52d49a6249ac4ffab6e8e700b1c7e22d

To:

Contract 0x63ae1fc0907d8babfb1e4015655c3ed09f3d8c7a

⚠️

⚠️ Warning! Error encountered during contract execution [Reverted] 😞

Value:

0 Ether (\$0.00)

Transaction Fee:

0.000040614 Ether (\$0.01)

Click to see More

⬇️

Private Note:

To access the Private Note feature, you must be [Logged In](#)

如果投票不成功 (Failed), 如何尋找原因

如isVoted輸入你的 voterID得到結果為 true, 即你已經投過票, 不能再投了

如usedPhoneNumber非零, 即你所使用的電郵已經被Response所寫的voteID的人登記使用過, 需要使用其他電郵. 而這function的input可藉把電郵輸入getEmailHash function得到

The screenshot shows the etherscan.io interface for a contract at address 0x63ae1fc0907d8babfb1e4015655c3ed09f3d8c7a. It displays two query results:

- 14. isVoted**
 - Query: bool
 - voterID (uint256): 78267797985477011236300365729907352616284657272517151278402105028539288750140
 - Query: bool
 - [isVoted method Response]
 - bool: false (indicated by a red arrow)
- 15. owner**
 - 0x0fe7c97d52d49a6249ac4ffab6e8e700b1c7e22d address
- 16. usedPhoneNumber**
 - <input> (uint256): 77256736397751460561018738909395331600461740202332280299138220922560350786094
 - Query: uint256
 - [usedPhoneNumber method Response]
 - uint256: 0 (indicated by a red arrow)

如果投票不成功 (Failed), 如何尋找原因

如voterList輸入你的voterID得到結果為true, 即你已經登記了, 需要聯絡票站人手輸入加密選票

17. voterList

<input> (uint256)

49392759923783406634712035798837259781009158783488393147850236186714509637035

Query

↳ bool

[voterList method Response]

» bool: false



如何成為票站

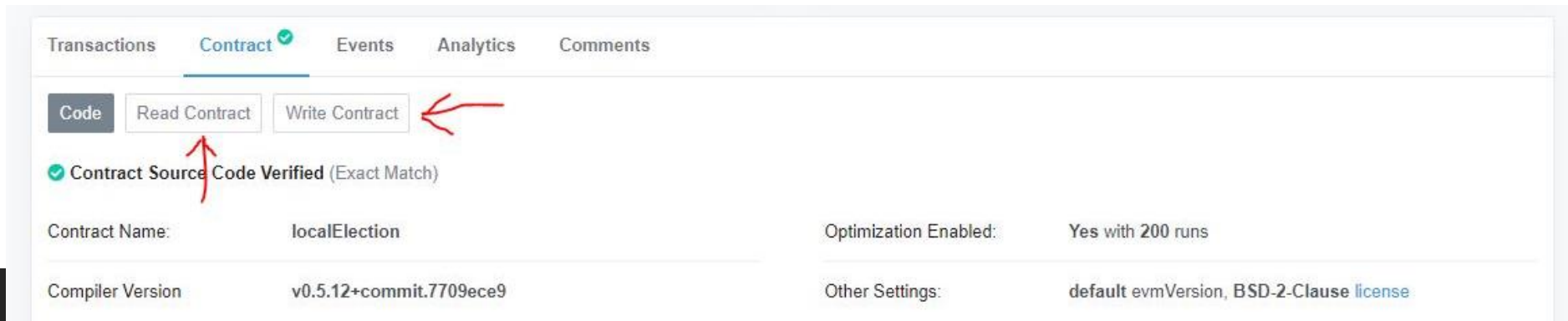
- 1) 在Chrome安裝Metamask, 申請一個Ethereum戶口, 放入一些Ethereum (1 ETH大約能處理二千張選票)
- 2) 把address發給@secondphonejune (Telegram), 該他把你加入為票站
這是人工輸入選票的要求, 如果想設立票站網站, 該選民自動投票, 你還要
- 3) 設立電郵帳戶來發送電郵驗證碼
- 4) 設立Infura帳戶和project link
- 5) 設立Node.js 網站, source code可從GitHub下載
- 6) 在credentials.js 和public-html/config.json填寫資料
- 7) public-html/voteboxes.json加入網站資料, 然後push到GitHub上

如何成為票站 1

<https://medium.com/publicaio/a-complete-guide-to-using-metamask-updated-version-cd0d6f8c338f>

如何人工幫選民提交選票, 或協助選民重新投票

- 1) 從選民得到voterID, 選區, 加密選票和電郵
- 2) 使用ReadContract ➔ getEmailHash得到電郵的hash value
- 3) 使用WriteContract ➔ register重新登記該選民, 並取消其過去選票
 - 需要花費ETH, 也需要等待transaction confirm
- 4) 使用WriteContract ➔ submitVote提交選票
 - 需要花費ETH, 也需要等待transaction confirm



如何人工幫選民提交選票, 或協助選民重新投票

7. getEmailHash

email (string)

secondphoneJune2019@gmail.com

Query

└─ uint256

[getEmailHash method Response]

➤ uint256 : 77256736397751460561018738909395331600461740202332280299138220922560350786094

如何人工幫選民提交選票, 或協助選民重新投票

← → ↺ etherscan.io/address/0x63ae1fc0907d8babfb1e4015655c3ed09f3d8c7a#writeContract

Ether Value: \$0.00 Contract Creator: 0x0fe

Transactions **Contract** Events Analytics Comments

Code Read Contract **Write Contract**

[Feature Tip: Etherscan Dapp Page](#) - A new front-end interface for any smart contract on Ethereum!

● Write Contract

1. addVoteBox

box (address)

box (address)

Write

2. register

voterID (uint256)

782677979854770112363003b5729907352616284657272517151278402105028539288750140

hashedEmail (uint256)

44405938424454268367946282980487408403504670053662657313238915285748000380617

council (string)

石塘咀

Write **View your transaction**

如何人工幫選民提交選票, 或協助選民重新投票

發送後按Write旁邊新出現的View your transaction, 便能從新分頁看到選票繳交情況, 可發給選民讓佢檢查選票上載到區塊鏈的情況

← → ↺ 🔒 etherscan.io/address/0x63ae1fc0907d8babfb1e4015655c3ed09f3d8c7a#writeContract

6. stopElection

Write

7. submitVote

voterID (uint256)

78267797985477011236300365729907352616284657272517151278402105028539288750140

hashedEmail (uint256)

77256736397751460561018738909395331600461740202332280299138220922560350786094

council (string)

中環

singleVote (string)

VlcrCMZYRNQOnsQ4siiN1dyVRbOZvTntkhro4SzxdYj+vvqVojXPqSDzva0LPylhlyTfFwXxlgrtZ2JAyVSRGwg==

Write

如何成為票站 4

The screenshot shows the Infura dashboard at the URL `infura.io/dashboard`. The interface features an orange header with the Infura logo and navigation links for 'DASHBOARD' and 'STATS'. A prominent orange banner at the top promotes 'INFURA+' with the message: 'Thanks for being a loyal Infura user, upgrade your account and receive a free 3 month trial!'. Below this, the 'YOUR PROJECTS' section displays a single project, 'MAIN ETHER NETWORK', which was created on July 2, 2019. To the right of the project list is a 'CREATE NEW PROJECT' button. The 'REQUESTS TODAY' section shows a progress bar indicating that 0 out of 100,000 requests have been used today, with a note that 0% of total daily requests have been used. At the bottom, the 'RESOURCES' section is partially visible, and the 'TOTAL REQUESTS' section shows a calendar for November 21. The interface includes various interactive elements like 'VIEW PROJECT' and 'VIEW STATS' buttons, and a 'DASHBOARD' tab is selected.

← → ↻ infura.io/dashboard ☆ 🐱 👤

≡ DASHBOARD STATS INFURA UPGRADE

INFURA+
Thanks for being a loyal Infura user, upgrade your account and receive a free 3 month trial! UPGRADE

YOUR PROJECTS 2 remaining CREATE NEW PROJECT REQUESTS TODAY ⓘ

✓ MAIN ETHER NETWORK
Created on Jul 2, 2019
VIEW PROJECT
VIEW STATS

TOTAL 0 of 100,000
0% of total daily requests used

RESOURCES TOTAL REQUESTS ⓘ All times are in UTC
NOVEMBER 21

如何成為票站 4

得到Endpoint

infura.io/project/db573ee83e1b4983b484863612665ba0

INFURA

UPGRADE

NAME

main Ether network

SAVE CHANGES

KEYS

PROJECT ID

PROJECT SECRET ⓘ

ENDPOINT MAINNET ▼

mainnet.infura.io/v3/

SECURITY

如何成為票站 5

1) 安裝Node.js <https://www.runoob.com/nodejs/nodejs-install-setup.html>

2) GitHub project 網址:

<https://github.com/secondphonejune/hk2019distractelectionblockchain>

安裝Node.js ➔ 下載nodejs folder ➔ 填寫資料 (step 6) ➔ 執行 npm install
➔ 執行 node index.js ➔ Redirect 80 port 到 localhost:3000

如何成為票站 6

```
credentials.js - Notepad
File Edit Format View Help
var credentials = {
  email:{
    host: 'sg1-ls7.a2hosting.com',
    port: 465,
    secure: true, // true for 465, false for other ports
    user: 'non-reply@hkdistrictelection.online',
    password: '[REDACTED]'
  },
  privateKey:
    '[REDACTED]',
  infuraEndPoint:
    '[REDACTED]',
  senderAddress: "[REDACTED]",
  electionSmartcontractAddress: "0x63ae1FC0907d8BaBFB1E4015655C3ED09f3d8C7
a"
};
module.exports = credentials;
```

電郵登入資料

Metamask 戶口private key

Infura Endpoint

Metamask 戶口address

如何成為票站 6

config.json - Notepad

File Edit Format View Help

```
{
  "voteboxName": "http://www.hkdistrictelection.online 0xbe598e435D60eF83C6F474AE6E72A0812b2e8B50",
  "ProblemContact": "@secondphonejune (Telegram)",
  "electionSmartcontractAddress": "0x63ae1FC0907d8BaBFB1E4015655C3ED09f3d8C7a",
  "encryption_public_key": "MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAG168YGjhOGN10fR
+a5HwPCWQxdgbHoK/F50YyDi7PBQ0gUHorC5Ih+0vhhVcKqaMy2zn7ka/hnHJdWpMGBMdcCAwEAAQ=="
}
```

需要修改

如何成為票站 7



```
{
  "Available_votebox": {
    "http://localhost:3000": "0x0FE7C97d52D49a6249Ac4FFab6e8E700b1c7E22D",
    "http://www.hkdistrictelection.online": "0xbe598e435D60eF83C6F474AE6E72A0812b2e8B50"
  }
}
```

加入自己的網站, 然後push上GitHub

如何幫助我們

- 1) 幫忙測試投票系統
- 2) 幫忙做文宣, 給所有你認識的人知道
- 3) 幫助修改smartcontract/electionList_smartcontract_V1.sol和nodejs/public-html/councils.json 把所有區議會候選人資料放入
- 4) 成為其中一個票站
- 5) 幫助重新設計網站和這份介紹
- 6) 捐出ETH讓選舉能夠進行, 我們需要100 ETH, 目標處理二十萬選票, 多出的ETH會捐給星火

謝謝
