點數平台

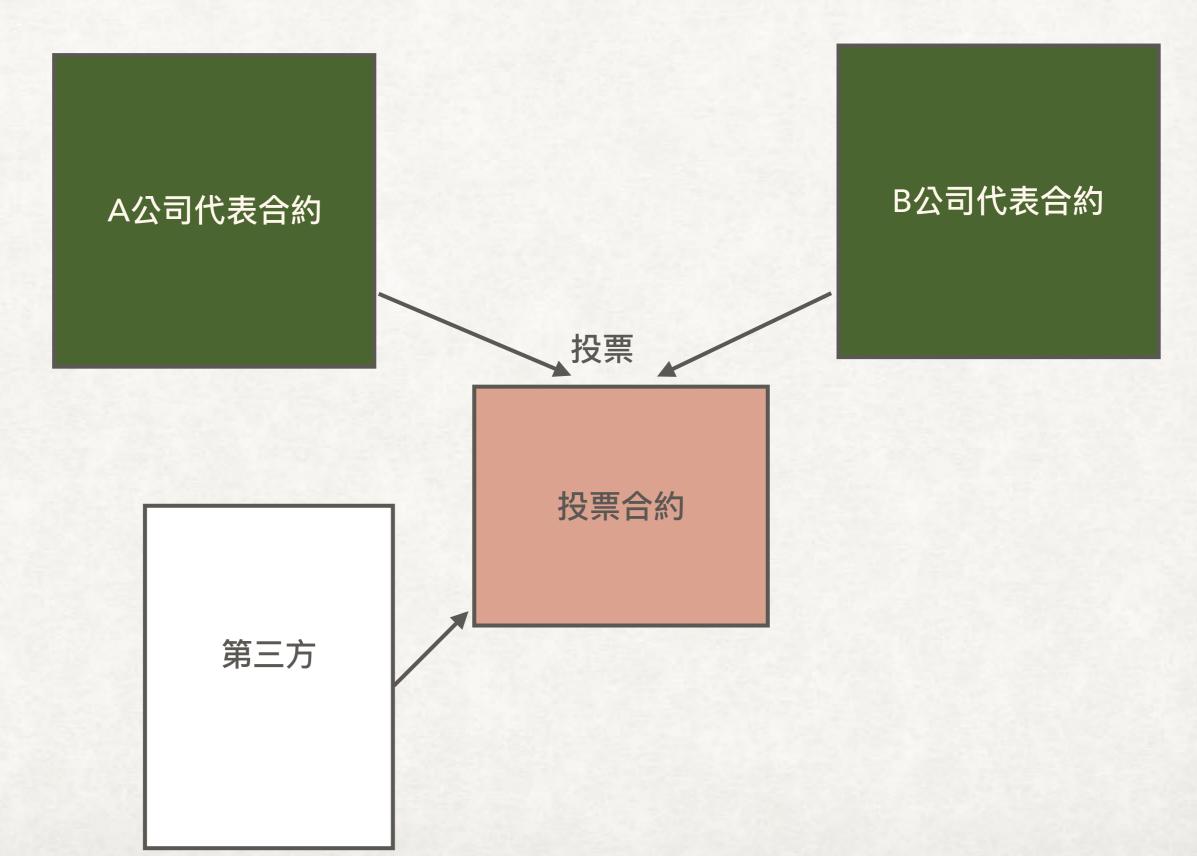
#### 點數管理

公司代表合約: 紀錄公司發行哪些點數 產生 點數合約A: 點數合約C: 紀錄該點數 紀錄該點數 發行狀況 發行狀況 點數合約B: 紀錄該點數 發行狀況

第三方: 可能是平台,etc

> 投票合約: 公司和第三方在此 合約進行投票,決 定是否產生新專案 合約

# 投票產生專案合約



## 產生專案合約

投票合約 通知新專案合約產生 通知新專案合約產生 產生 A公司的 B公司的 點數合約C 點數合約D 專案合約 呼叫權限限制: A公司及B公司

第三方

第三方 A公司代表合約 B公司代表合約 專案合約 呼叫權限限制: A公司及B公司 修改資料 B公司的 A公司的 點數合約D 點數合約C

## 合約名稱對應

公司代表合約 ॥ tokenManage 投票合約 II multiSig

點數合約 ॥ tokenInfo

專案合約 ॥ tokenExchange

## 公司代表合約

- tokenManage合約是公司所有,每個公司會有一個。
- · 這個合約記錄現在公司所發行的token。
- 目前紀錄的token資訊是
  - 1.名稱
  - 2.該token的合約address
  - 3.發行總數
  - 4.是否還在使用中

### 點數合約

- tokeInfo合約對應到一個token,裡面記錄
  - 持有這個token的人及其持有數量。公司本身自己也會持有(發行的意思即是無中生有生出一筆點數給公司自己)。
  - 目前發行token的權限是給公司合約,所以公司可以任意發行。
  - 如果發行等等的權限要改成第三方(multisig等),修改modifier 即可。

### 投票合約

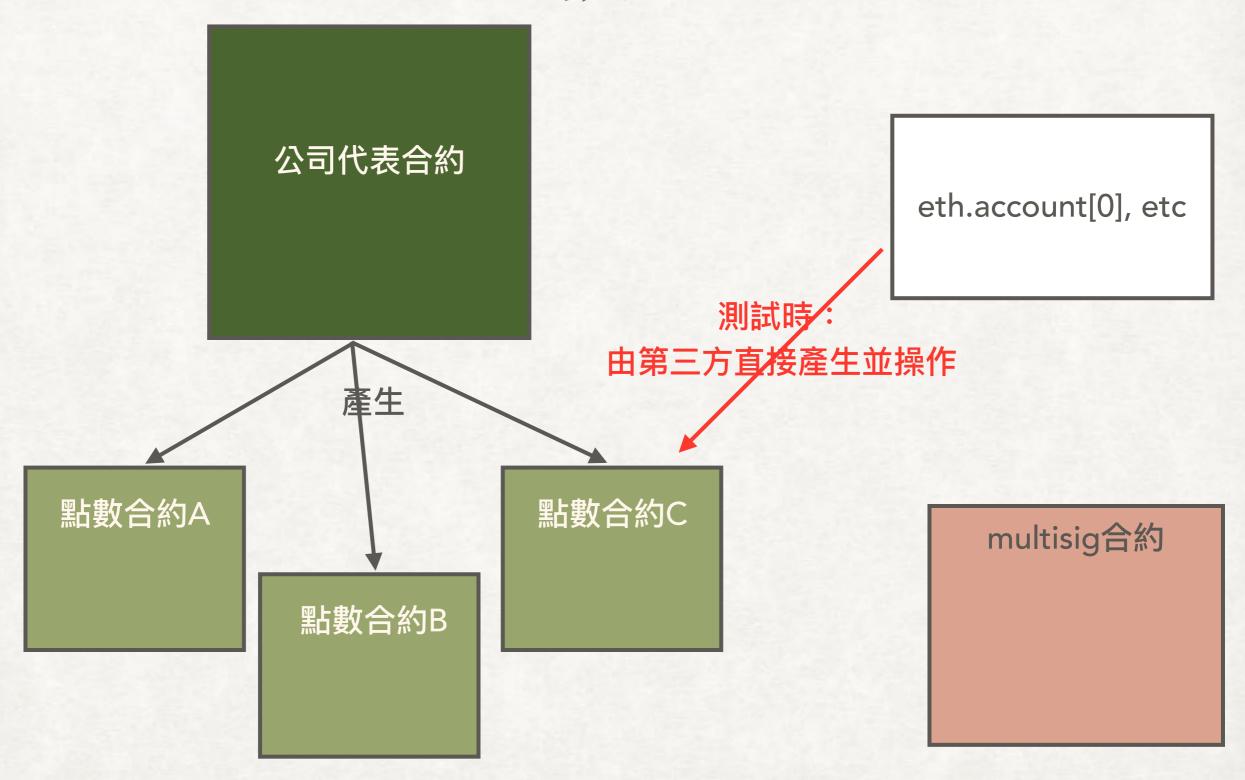
- MultiSig合約是用來產生專案合約的合約,由雙方公司和第三方共同投票決定一個專案是否產生。
- 合約裡會紀錄專案合約的相關資訊,如雙方公司及欲交換點數相關資訊,到時候在產生專案合約時要將這些資訊傳入。
- 用32 byte的hash值來當作每一個投票的識別, hash值可以是 sha3(time || comanyA || tokenA || companyB || tokenB) 之類的。
- · 當雙方公司和第三方都投票了,就會產生新的專案合約並通知 tokenInfo合約。

## 專案合約

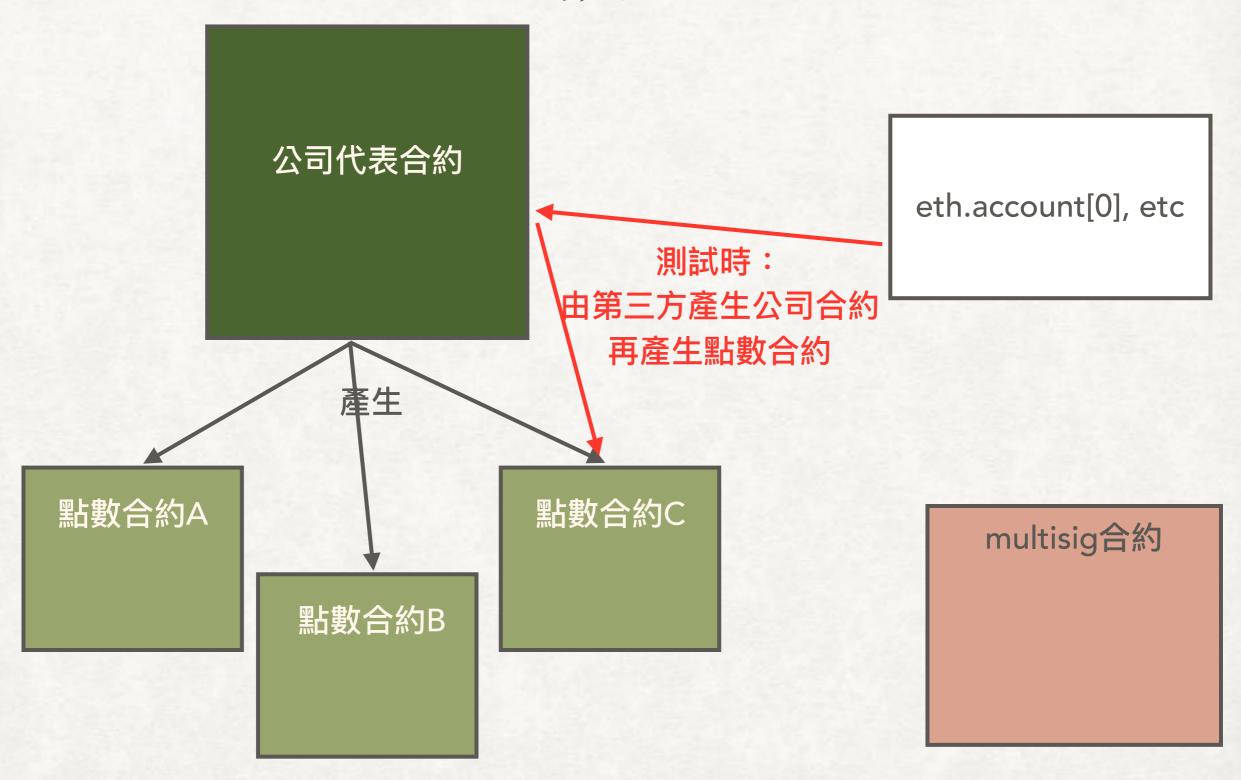
- tokenExchange是專案合約,由投票合約產生,只有兩家相關公司能操作。
- 如果A公司收到客戶的請求要換成B公司的D點數時,便呼叫專案合約,專案合約將客戶在A公司的C點數轉給B公司(表示B公司將持有A公司的C點數),並將B公司的D點數從B公司轉給客戶(客戶會持有B公司的D點數)。
- 其中因為小數點的問題,客戶要換的數量未必能全數兌換, exchange 函式在轉換成功後會回傳成功兌換到的點數數量。

獨立測試步驟

## 點數管理



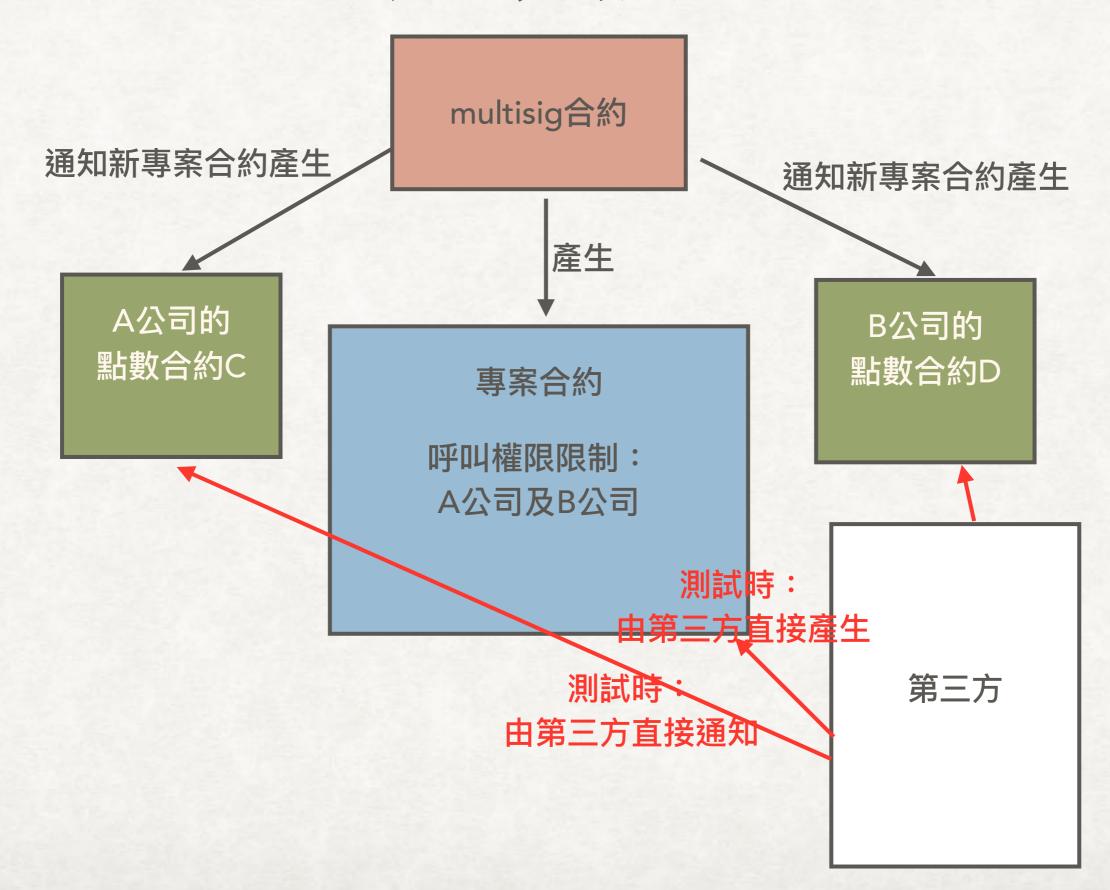
## 點數管理



# 投票產生專案合約

eth.account[2], etc eth.account[1], etc 投票 multisig合約 eth.account[0], etc

#### 產生專案合約



第三方 測試時: 由第三方直接呼叫 A公司代表合約 B公司代表合約 專案合約 呼叫權限限制: A公司及B公司 修改資料 B公司的 A公司的 點數合約D 點數合約C