

區塊鏈應用實例

報告人 湯耀翔

區塊鏈是什麼

- 區塊鏈是一種透過**共識算法**實現**去中心化**的技術
- 區塊鏈可以用於**有價值的商品**上如：房子、汽車等
- 區塊鏈提供了在鏈上成員可以**即時檢閱、共享資訊**
- 區塊鏈的特性與技術增加了客戶的**信任度**。

共識機制

共識演算法是區塊鏈的核心制度之一，由於節點之間是分散且平行的，因此必須設計一套制度，來維護系統的運作順序與公平性，統一區塊鏈的版本。

- 工作量證明(Proof of Work, PoW)
- 權益證明(Proof of Stake, PoS)
- 權威證明(Proof of Authority, PoA)

創世區塊(Genesis Block)

區塊鏈上的第一個區塊，創建者可以自己設定創世區塊的所有值與參數，只要沒有人跟你設定相同的參數，那你的區塊鏈就是獨一無二的。

```
1  {}
2  {
3  .. "config": {
4  .. .. "chainId": 1997,
5  .. .. "homesteadBlock": 0,
6  .. .. "eip150Block": 0,
7  .. .. "eip155Block": 0,
8  .. .. "eip158Block": 0
9  .. },
10 .. "alloc": {},
11 .. "coinbase": "0x0000000000000000000000000000000000000000",
12 .. "difficulty": "0x20000",
13 .. "extraData": "0x74686520726f73657320696e206865722068616e642c2074686520666c61766f7220696e206d696e65",
14 .. "gasLimit": "0x44c747",
15 .. "nonce": "0x00000000c000ff59",
16 .. "mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000",
17 .. "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
18 .. "timestamp": "0x599DA33A"
19 }
```

創世區塊(Genesis Block)

參數的解釋

Name	Description
chainID	區塊鏈的識別ID
homesteadBlock	這是以太坊的第二個主要版本，第一個是 Frontier，這個值設為"0"表示目前正在使用 Homestead 版本
eip155Block	eip 是 ethereum improvement proposal 的縮寫，私有鏈不會因為這些提議分岔，因此設為"0"
eip158Block	eip 是 ethereum improvement proposal 的縮寫，私有鏈不會因為這些提議分岔，因此設為"0"
mixhash	與 nonce 配合用於挖礦，由上一個區塊的一部分產生的雜湊
nonce	一個 64 位隨機數，用於挖礦
difficulties	挖礦難度參數
alloc	預置帳號與該帳號內金額
coinbase	預設為第一個建立帳號的礦工
timestamp	設置創世區塊的時間戳
parentHash	上一個區塊的 Hash 值，因為是創世區塊所以為 0
extraData	附加信息
gasLimit	交易所使用到的 gas 總量限制，用來限制區塊能包含的交易信息總和，因為我們是私有鏈，所以填最大。

區塊鏈中的區塊

一個完整的區塊中所包含的內容會有兩個部分

- 1) 區塊頭 (Block Header)
- 2) 區塊體 (Block Body)

區塊頭位置

Block Size (4 bytes): 618.435 KB
Block Header (80 bytes)

Version (4 bytes): 0x20800000
Previous Block Hash (32 bytes):
00000000000000002590a68b9a13f218aa4542d775
21c69cbe83ed2744b8b41
Merkle Root (32 bytes):3e691438a38d879019bf99c17
68a8de0ff91712f85a19a272c6c9046ce83de50
Timestamp (4 bytes):1698765589
Difficulty (14 bytes):166851513282.7772
Nonce (4 bytes):4005464614

區塊體位置

Transaction Counter (1-9 bytes):1162
Transactions

這裡會記錄1162筆交易的Hash值
Tx1:1KFHE7w8Bha ENAsw)nryaoccDb6qcT6DbYY
Tx2:101hecyrKzinnaK592TTNudCKfBNbEhTaB7
....



Block Size (4 bytes) 129575 KB
Block Header (80 bytes)

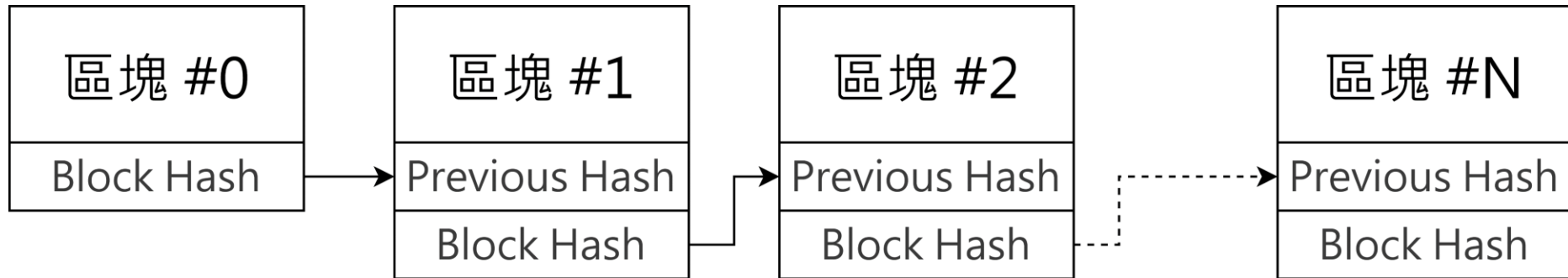
Version (4 bytes): 0x20800000
Previous Block Hash (32 bytes):
00000000000000000654120e44c08813da2091ec5d
5a95bf951865a047157ff9
Merkle Root (32 bytes)07889ba79c8ffd5f0502983521
3faa0e3e4f64b53c8d3c988db44d3febc977b6
Timestamp (4 bytes):1618752156
Difficulty (4 bytes):166851513282.7772
Nonce (4 bytes):154600755

Transaction Counter (1-9 bytes):226
Transactions

這裡會記錄226筆交易的Hash值
Tx1:eb68541ca32e6c4795dfd0fd28ea388b24880517
0eda920b4aa0c16f7a42121c
....

區塊+鏈

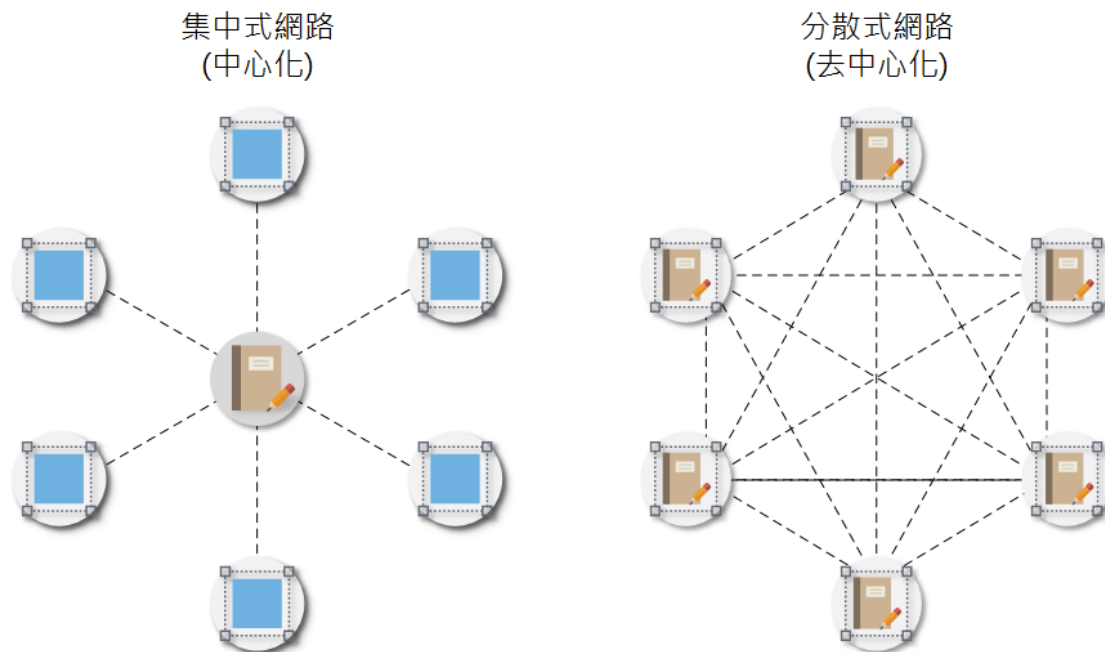
每個區塊中透過區塊頭裡面的Previous Hash來形成一個鏈結串連每一個區塊形成區塊鏈。



區塊鏈技術與特色

• 去中心化的分散式電子帳本

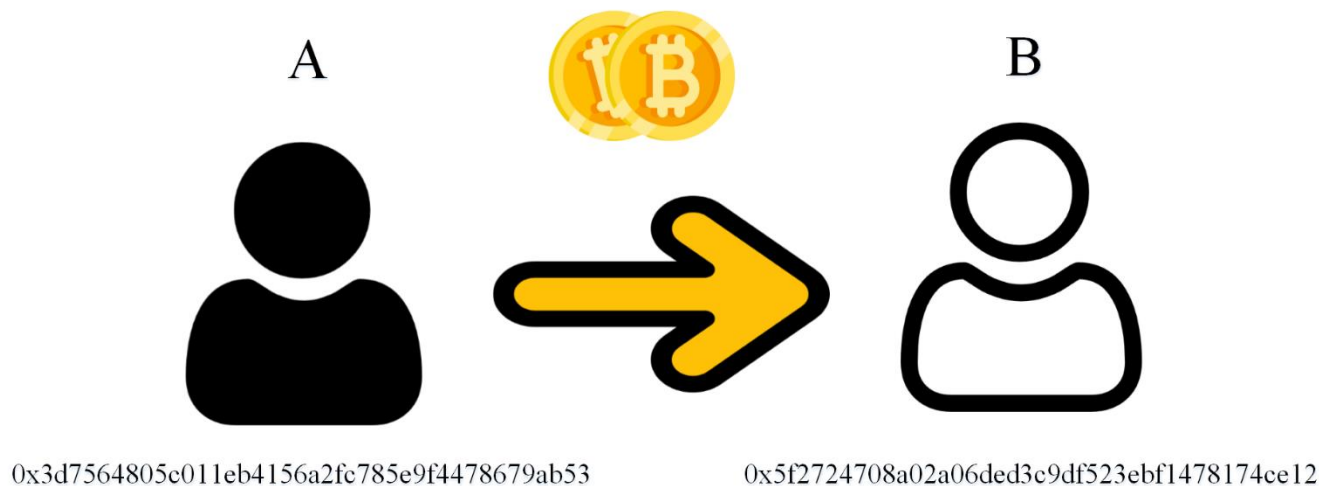
帳本是由**一群節點(電腦)**共同維護，而不是由一個類似銀行的中心機構來掌管，以此達到去中心化的概念。而每一個節點都會有一本相同的帳本，記錄著過去所有交易的內容。



區塊鏈技術與特色

- 所有節點都以匿名方式共同驗證整份帳簿

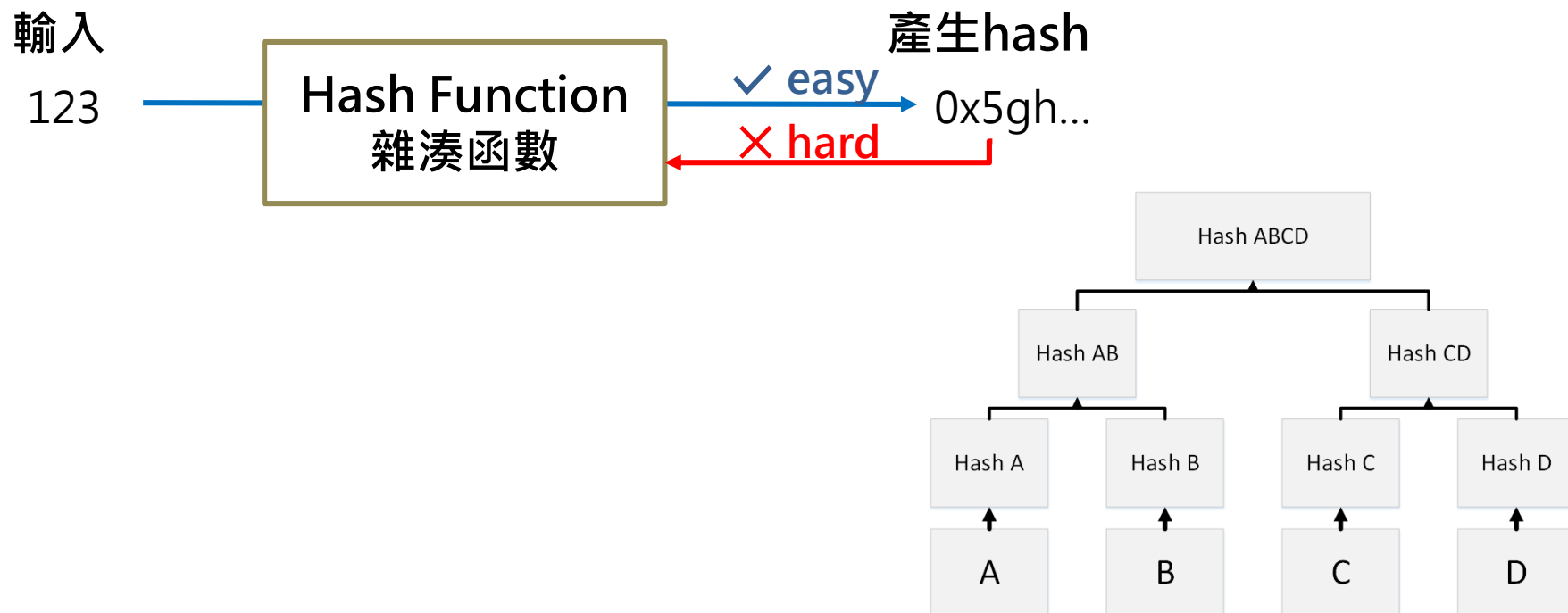
節點會使用一組「**英文+數字**」的代碼作為名稱，我們可以稱作為地址(Address) 可以不需要使用真實名字便可進行交易。



區塊鏈技術與特色

• 每份歷史記錄都不易被篡改

區塊鏈中的每一筆資料一旦寫入就不能再更改，只要資料被驗證完後就會永久的寫入區塊中，其中的技術是透過 Hash Function 對其內容進行加密動作。



以太坊 - 智能合約

智能合約是一個運行於區塊鏈上的一串代碼，在以太坊的網路中有許多節點，這些節點除了挖礦外，也要負責運行以太坊上的智能合約，這項工作運行在每一個礦工的**以太坊虛擬機**(Ethereum Virtual Machine, EVM)上。

其智能合約經過編譯後會產生Bytecode與ABI兩個部分

- 1) ABI: 在部署智能合約的時候，需要藉由ABI當作媒介傳遞Data
- 2) Bytecode: 讓虛擬機可以運行的程式碼

以太坊 - 智能合約

智能合約編譯完成後，可以連接自己所建立的私有鏈，並且完成部署。

```

1 pragma solidity ^0.4.25;
2 pragma experimental ABIEncoderV2;
3 contract International {
4     enum Station { Fishingboat,Wholesale,Processingplant,LogisticsCenter,Massmerchandise }
5     //訂單位置
6     struct transportpath {
7         uint index;//訂單順序
8         Station state;//
9     }
10
11     //transportpath[] public Path;
12     mapping (uint => transportpath) public Path;
13     //漁產品履歷
14     struct data{
15         string transName;//魚的名稱
16         string[5] reason;//特殊原因; string[5]預設5站
17         uint[5] transTime;
18         uint weight;//重量
19         string Location;//產地
20         //string enterLocationTime;//進站時間
21         //string leaveLocationTime;//出站時間
22         Station state;
23     }
24     mapping (uint => data) public datas;
25     uint[] internal fishList;
26
27     //event A1(data a1);
28     event LogFish(uint _number, string transName, string reason, uint weight, string Location);
29     event LogShipping(uint _number, Station state, uint time);
30
31     function get_datas(uint _number) public view returns(string[5],uint[5]) {
32         return (datas[_number].reason, datas[_number].transTime);
33     }
34     function goto_Fishingpost(uint _number, string _transName, string _reason, uint _weight, string _Location) public{
35         transportpath storage entry = Path[_number];
36         if(entry.index > 0){
37             return;
38         }else{
39             fishList.push(_number);
40             entry.index = fishList.length;
41             entry.state = Station.Fishingboat;
42
43             datas[_number].transName = _transName;
44             datas[_number].reason[uint(Station.Fishingboat)] = _reason;
45             datas[_number].transTime[uint(Station.Fishingboat)] = now;
46             datas[_number].weight = _weight;
47             datas[_number].Location = _Location;
48             //LogFish(_number,_transName,now,_weight,_Location);
49         }
50     }

```



ENVIRONMENT

Web3 Provider

ACCOUNT

0x5B3...eddC4 (100 ether)

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

International - 產品履歷.sol

Deploy

Publish to IPFS

OR

At Address Load contract from Address:

Transactions recorded 0

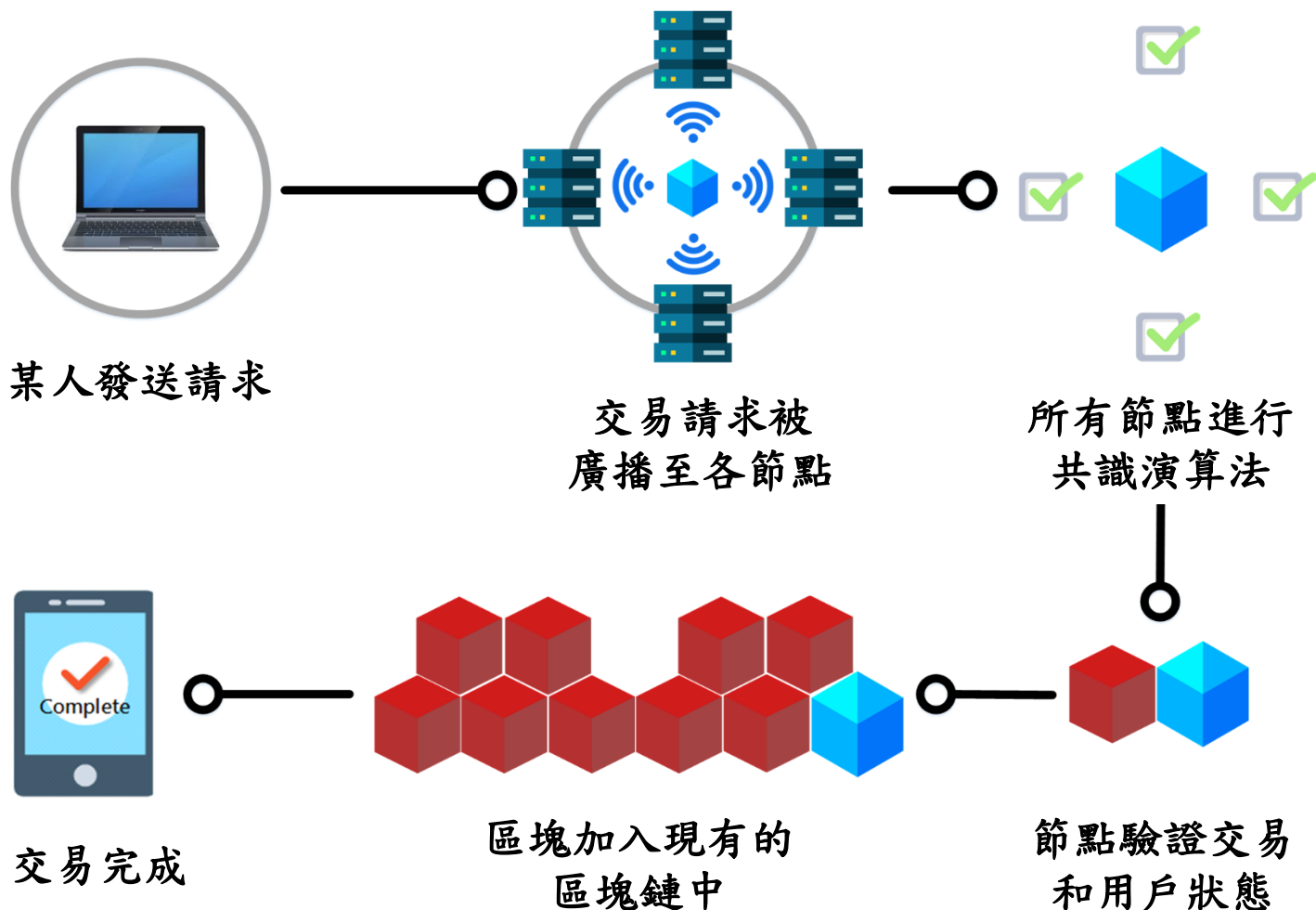
Deployed Contracts

Currently you have no contract instances to interact with.

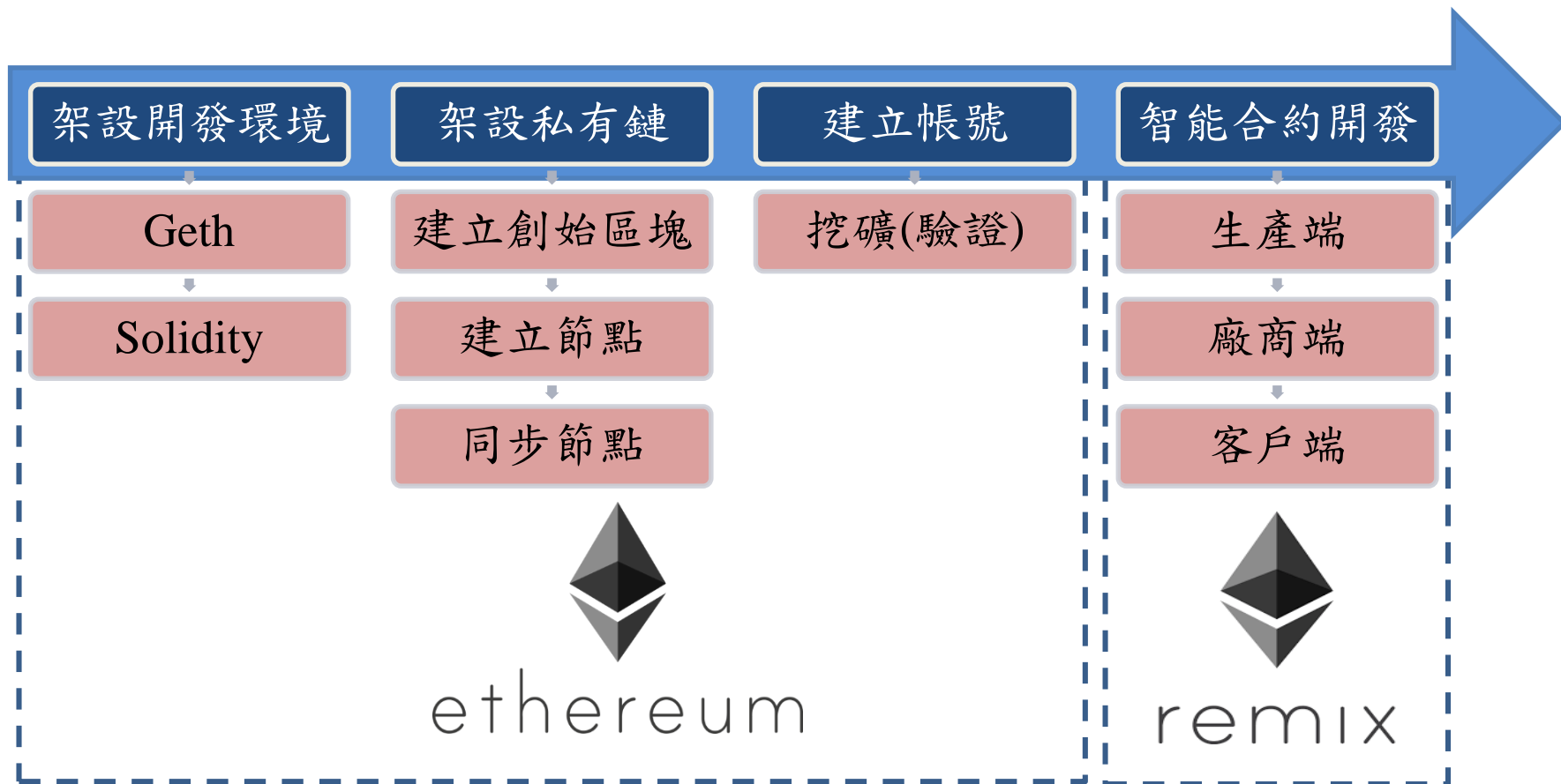
本機端

部署的帳戶

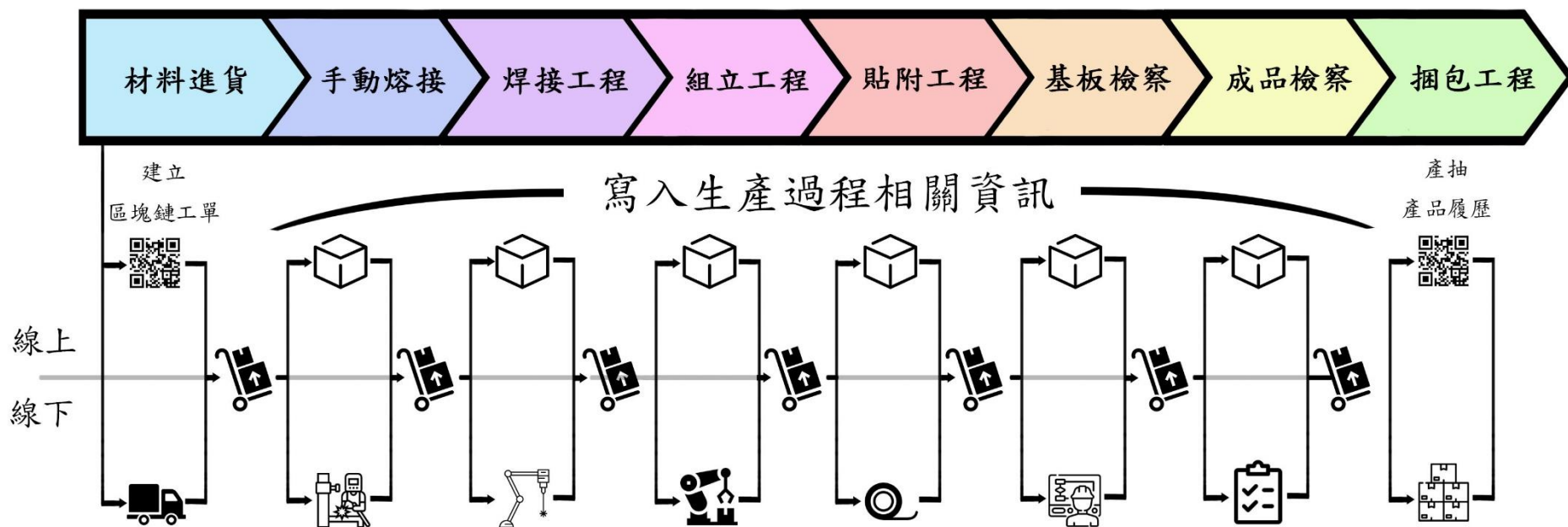
區塊鏈運作流程



區塊鏈的開發流程



廠內生產線流程置入區塊鏈示意圖



作業員紀錄之生產資訊

紀錄生產
訊息識別
編號



交易編號 NO.2566

作業員(Operator): 0xb79b3fd5fb02b5a8fde434422f521667c64b7f1e

時間戳(Timestamp): Jan 14 2020 11:17:20

訊息(Data): OK! 生植物料無誤, 準備進站生產。

生產線狀態

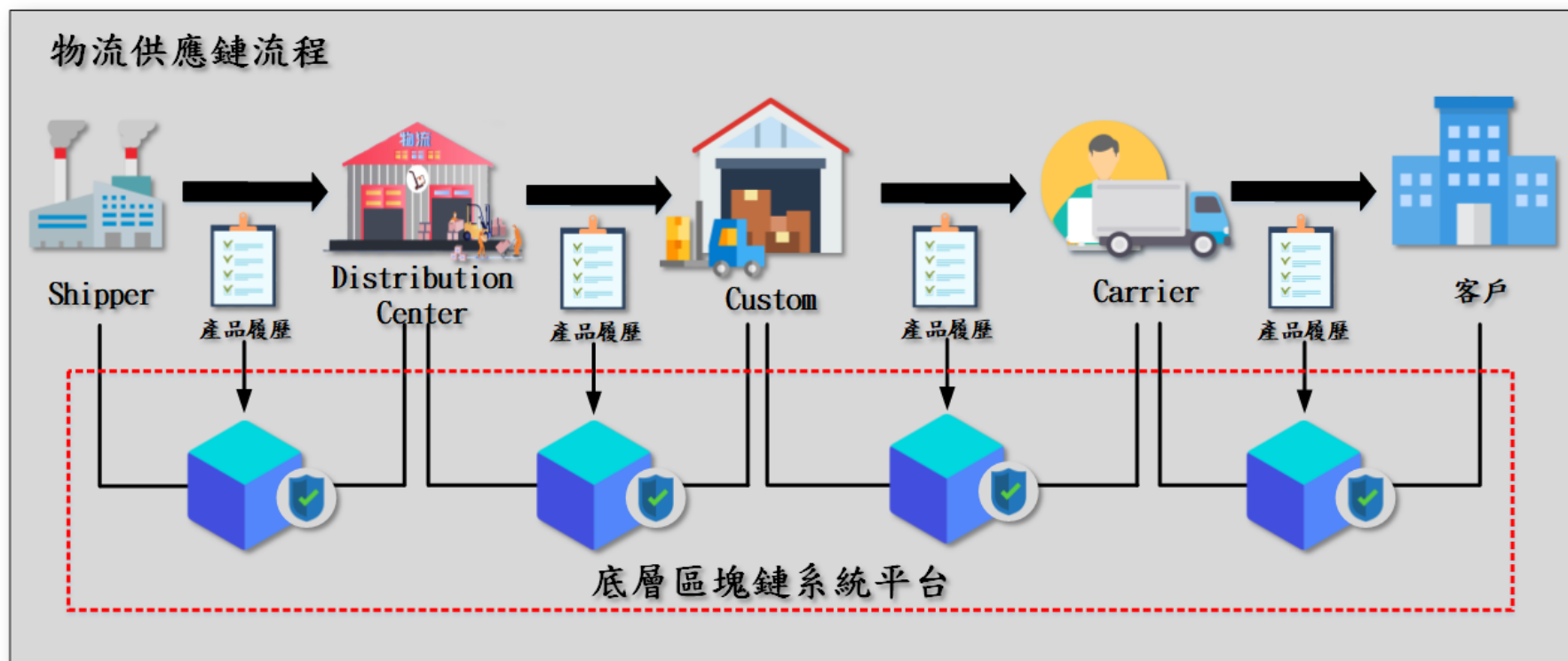


進站	工站B In	工站B Out	工站C In	工站C Out	工站D In	工站D Out	工站E In	工站E Out	出站

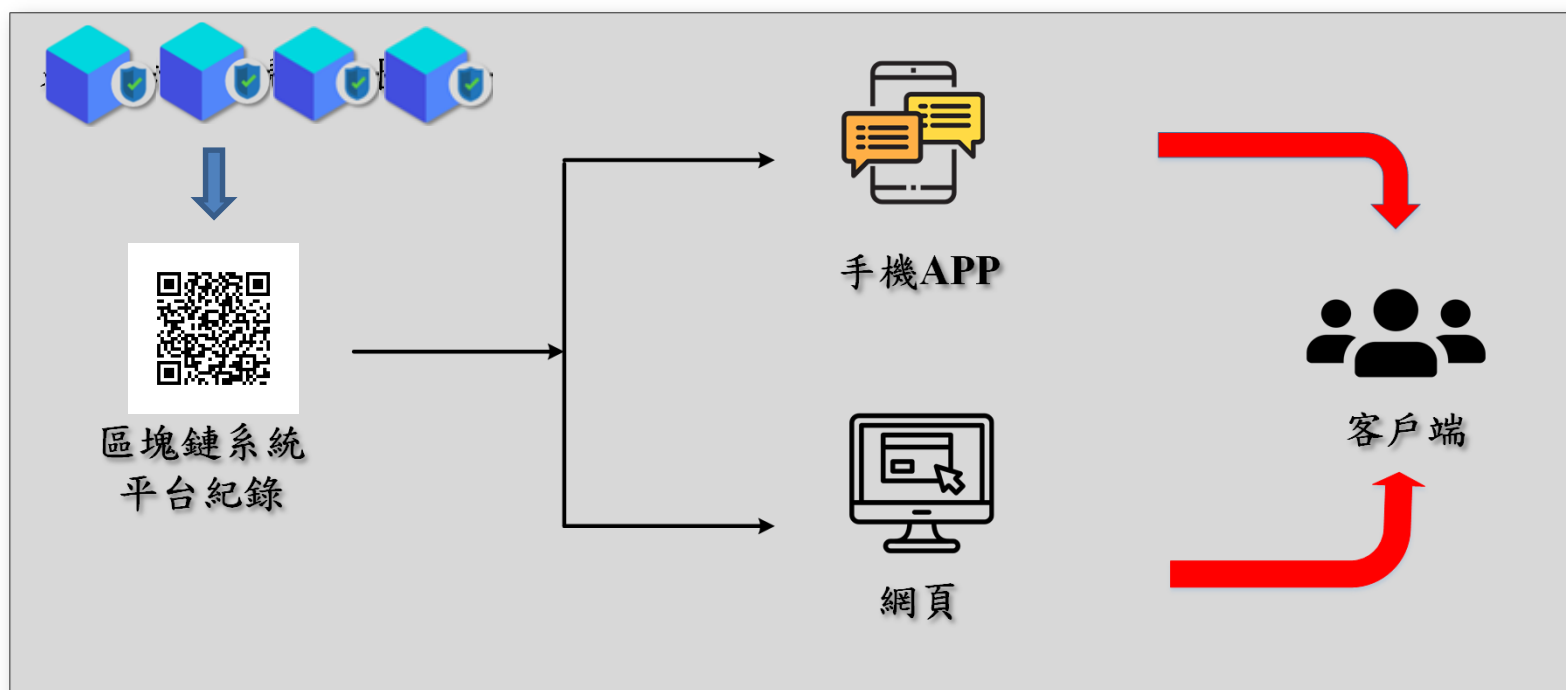
產品生產履歷實測



國際物流導入區塊鏈示意圖



區塊鏈系統透過使用者介面將資訊傳遞給客戶端示意圖



國際物流供單建立

建立國際物流智能合約履歷

工單建立在區塊鏈上的國際物流模擬

建立國際物流智能合約帳戶：0x69525f82343477a8e39003f01f5bc1d6734fe836

Distribution Center帳戶地址

Custom帳戶地址

Carrier帳戶地址

Sales帳戶地址

驗證密碼(Address pass)

建立產品履歷

確認

供應鏈人員在食品進出各站確認機制模擬

確認人員(From):

履歷編號(To)

訊息(Message)

驗證密碼(Address pass)

發送

國際物流資訊紀錄

國際物流智能合約帳戶：0x3486cc177af3e949df3413ce038f39e872fc1614

Transaction Address:

0xa8c3ce7d7c771229f56d4a38d659aa0f12a59800abb26e94ee05989ca8a365b

合約地址: 0xa8c3ce7d7c771229f56d4a38d659aa0f12a59800abb26e94ee05989ca8a365b

合約帳戶: 0x3486cc177af3e949df3413ce038f39e872fc1614

區域位置: 2899

shipper: 0xb79B3FD5fb02B5A8Fde434422F521667c64B711E

Distribution Center: 0x7140b11a729b6d9594b6a4fb1b0cf386665431ff

Custom: 0x129a6b8f381a312b425da4078bb22dc617ece509

Carrier: 0x44c600c7a8d897410e51d2d00499482b05a1948b

sales: 0x69525f82343477a8e39003f01f5bc1d6734fe836

- 交易編號 NO.2902
- 交易編號 NO.2904
- 交易編號 NO.2906
- 交易編號 NO.2909
- 交易編號 NO.2911
- 交易編號 NO.2913
- 交易編號 NO.2916
- 交易編號 NO.2918
- 交易編號 NO.2921
- 交易編號 NO.2923

國際物流資訊紀錄

每個站別紀錄訊息並寫入區塊鏈中



交易編號 NO.2902



工作人員(Operator): 0xb79b3fd5fb02b5a8fde434422f521667c64b7f1e



時間戳(Timestamp): Oct 23 2020 13:27:58



訊息(Data): 檢查產品原料品質

把資訊寫入QR code中



實測

- 將產銷履歷訊息寫入 json server 再利用 QR code 的方式呈現，藉由我們自己開發的 APP 來讀取資料。

