Smart Contracts: A Brief Introduction

政大資科系教授兼電算中心主任
陳 恭 博士
2016/05/28
What are Smart Contracts?

• Is a smart contract a “contract” in law?

• Are smart contracts smart?

No... Not Really!!!
Smart Contracts

• Concept pioneered by Nick Szabo in early 1990s.

“A smart contract is a computerized transaction protocol that executes the terms of a contract. ...”

一個智能合約是一個電腦化的交易協議，執行合約條款。

簡單範例：自動販賣機
Smart Contracts

- From **text contracts** written in **legal languages**
- To code contracts in **computer languages**

---

**contract Escrow { //第三方履約保證**

```solidity
address buyer;
address seller;
address agent;

function Escrow(address _agent, address _seller) {
...
}

function release() {
    if (msg.sender == agent)
        suicide(seller); // Send all funds to seller
    else throw;
}

function cancel() {
    if (msg.sender == agent)
        suicide(buyer);
    // Cancel escrow and return all funds to buyer
    else throw;
}
```

---

I (The **Buyer**) hereby deposit $10,000 with Bob (the **Agent**) who will store it securely in his bank account until such a time that the Buyer verifies that he has received delivery of a 1996 Mazda Protegé (the **Car**) from Alice (the **Seller**) at which point he authorizes the Agent to disburse the entirety of the funds to the Seller. If the Seller does not deliver the Car to the Buyer by April 1st the Agent will return the entirety of his funds to the Buyer.
Today's Topic

- Blockchain-Based Smart Contracts
- Decentralized App on a blockchain

Blockchain Platform

Contarct#1

```
Contract {
    Owner_address
    User_address
    deposit
    price
    open()
    close()
    rent()
    returnLock()
}
```

Contarct#2

```
Contract {
    Owner_address
    User_address
    deposit
    price
    open()
    close()
    rent()
    returnLock()
}
```

... (continues)

Contarct#n

```
Contract {
    Owner_address
    User_address
    deposit
    price
    open()
    close()
    rent()
    returnLock()
}
```

Blockchain

```
Block #1
Block #2
Block #3
```

Time

源自Bitcoin Blockchain
Bitcoin智能合約

• 用戶要動用比特幣時須滿足”支付條件”
• 延伸”支付條件”的功能，實現合約條款

例：當B要動用比特幣支付給C時

延伸:
以Bitcoin Script
製作合約條款的程式邏輯，但不夠一般化。

addr_B = 1BvBMSEYstWetq...

預設條件：B必須出示公鑰與數位簽章才能使用（支付條件）

signed by B
Pay to addr_C: 1BC
The Bitcoin Blockchain

區塊鍊

特色

1. 不可竄改 (Immutability)
2. 有效性 (Validity)
3. 一致共識 (Consensus)
4. 真實性 (Authentication)
5. 去中心化 (Decentralized)
6. 程式化 (Programmable)

Bitcoin script

獨一性 (Uniqueness)
Blockchain Smart Contracts

- Cost reduction 降低成本
- Disintermediation 去中間人
- ...

Traditional Transaction Model
Intermediaries & Custodians

Blockchain Model
Smart Contracts & Automation
Smart Contract範例1

- 數位音樂版稅合約

http://ujomusic.com/

REBUILDING THE MUSIC INDUSTRY ON THE BLOCKCHAIN

購買後版稅自動轉帳給相關人士
Smart Contract範例2

- 班機延誤或取消時，理賠自動化

http://insureth.mkvd.net/
Types of Smart Contracts

• Self-contained (Deterministic) smart contracts
  • 合約程式有足夠資訊自動執行

• Non-deterministic smart contracts
  • 需要從外部取得可信任的資料。例如：航班資訊
More Examples of Smart Contracts

應用範圍廣
智能租約：Slock.it (1/2)

• 透過智能鎖，方便出租物品
智能租約：Slock.it (2/2)

1. sets deposit and price

2. pays deposit

3. open/close

4. returns (deposits – cost)

5. receive payment

User

Owner
The BlockCharge PoC


• The BlockCharge PoC by RWE and Slock.it
• 電動車充電站 的合約
Many Smart Contract Platforms

- 目前有許多不同的智能合約平台在發展中，也有許多 Proof-of-Concepts 完成與進行中
  - Ethereum, Chain.com, Hyperledger, Corda, Ripple, ...

- 基於不同的區塊鍊平台技術
  - 使用：Public vs. Private (含 Consortium)
  - 記帳：Anyone (unpermissioned) vs. Some (permissioned)
    - 可再細分為 read/submit 交易，以及 mining 的權限
  - 不同的共識演算程序
  - 發展中的特色
    - 資料隱私性
    - 用戶的識別性 (KYC)
    - ...

<table>
<thead>
<tr>
<th>Public/Anyone</th>
<th>Private/Anyone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>?</td>
</tr>
<tr>
<td>Public/Some</td>
<td>Private/Some</td>
</tr>
<tr>
<td>Ripple, ...</td>
<td>Bankchain, ...</td>
</tr>
</tbody>
</table>
案例一: Ethereum以太坊智能合約平台

- Public/Unpermissioned chain, Open-source platform,
- 以太幣(Ether)· Proof-of-Work mining (目前)
- 提供功能強大的“合約程式語言”來撰寫合約邏輯
- Blockchain-as-a-Service on MS Azure

兩種帳戶: (1) 一般帳戶(以太幣) (2)智能合約帳戶
• 合約語言:
  • **Serpent**: Python-like
  • **Solidity**: JavaScript-like, now supported by MS Visual Studio

```solidity
contract Escrow {
  address buyer;
  address seller;
  address agent;

  function Escrow(address _agent, address _seller) {
    ...
  }

  function release() {
    if (msg.sender == agent)
      suicide(seller); // Send all funds to seller
    else throw;
  }

  function cancel() {
    if (msg.sender == agent)
      suicide(buyer);
      // Cancel escrow and return all funds to buyer
    else throw;
  }
}
```
Ethereum 以太坊架構

- Smart contracts 佈署於 blockchain 上
- 每次執行合約程式就是一次 交易。
- 眾多交易經 mining 後成為 block
案例二: The Corda Platform

- 私有認許制(Private/Permissioned)
- 不發行虛擬貨幣
- 交易資料並非全面共享
- 交易驗證有僅由相關成員驗證
- 提供多種共識機制
- 提供監管單位特殊查帳功能
- 提供智能合約與文字合約間之對照與關聯
- ...
A Recent Case (April 2016)

- How Barclays Used R3's Tech to Build a Smart Contracts Prototype
  - Based on R3's Corda platform
  - Barclays' Smart Contract Templates
  - ISDA master agreements for Interest Rate Swap

http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/
Case Study

Interest Rate Swap

SMART CONTRACT Creator

1. creates

SMART CONTRACT Couterparty

2. agrees & enters

SMART CONTRACT template

R3 Corda

3. computation (execution)

OUTCOME

Outside Data
1. 選取Templates
2.設定Template參數 (1/2)

Credit Support Annex 1995 - England and Wales

determined for each relevant currency and calculated for each day in that Interest Period on the principal amount of the portion of the Credit Support Balance comprised of cash in such currency, determined by the Valuation Agent for each such day as follows:

(x) the amount of cash in such currency on that day; multiplied by:
(y) the relevant Interest Rate in effect for that day; divided by:
(z) 360 (or, in the case of pounds sterling, 365).

"Interest Period" means the period from (and including) the date on which the amount has yet been transferred, the Local Business Day on which the transfer was transferred to or received by the Transferee) to (but excluding) the Local Business Day on which the relevant Credit Amount is transferred.

"Interest Rate" means, with respect to an Eligible Currency, the rate specified in Paragraph 11(f)(i) for that currency.

"Local Business Day", unless otherwise specified in Paragraph 11(h), means:

(ii) in relation to a transfer of cash or other property (other than securities) under this Annex, a day on which commercial banks are open for business (including dealings in foreign exchange and foreign currency deposits) in the place where the relevant account is located and, if different, in the principal financial centre, if any, of the currency of such payment.

Source: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/

Reproduced with permission of ISDA
2. 設定 Template 參數 (2/2)

Source: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/
3. 設定協議參數

Source: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/

Reproduced with permission of ISDA
4. 設定交易參數

Source: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/
5. 交易對手確認合約

Source: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/
6. 合約檢視

<table>
<thead>
<tr>
<th>Template Editor</th>
<th>Agreement Editor</th>
<th>Trade Entry</th>
<th>Trade Affirmation</th>
<th>Trade Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trade ID: TRADE102</td>
<td>Date: 2017-03-30</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Confirmation & Agreements

<table>
<thead>
<tr>
<th>Fixed Leg</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed Rate Payer</td>
<td>Bank A</td>
</tr>
<tr>
<td>Notional</td>
<td>USD 15,900,000</td>
</tr>
<tr>
<td>Payment Frequency</td>
<td>SemiAnnual</td>
</tr>
<tr>
<td>Effective Date</td>
<td>2016-04-04</td>
</tr>
<tr>
<td>Effective Date Adjustment</td>
<td>None</td>
</tr>
<tr>
<td>Termination Date</td>
<td>2026-03-16</td>
</tr>
<tr>
<td>Termination Date Adjustment</td>
<td>None</td>
</tr>
<tr>
<td>Fixed Rate</td>
<td>1.677%</td>
</tr>
<tr>
<td>Day Count Basis Day</td>
<td>D30</td>
</tr>
<tr>
<td>Day Count Basis Year</td>
<td>Y360</td>
</tr>
<tr>
<td>Roll Convention</td>
<td>ModifiedFollowing</td>
</tr>
<tr>
<td>Day In Month</td>
<td>10</td>
</tr>
<tr>
<td>Payment Rule</td>
<td>InArrears</td>
</tr>
<tr>
<td>Payment Delay</td>
<td>0</td>
</tr>
</tbody>
</table>

### Floating Schedule

- **Base Currency**: USD
- **Eligible Currency**: USD
- **Eligible Credit Support**: Cash in an Eligible Currency
- **Threshold**: USD 0
- **Independent Amounts**: USD 0
- **Minimum Transfer Amount**: USD 250,000
- **Rounding**: USD 1,000,000
- **Valuation Date**: Every Local Business Day
- **Notification Time**: 2:00pm London
- **Resolution Time**: 2:00pm London time on the first
- **Interest Rate**: EONIA
- **Address For Transfers**: -
- **Local Business Day**: London, New York

Moving Forward: Issues and Challenges

• Legal and Regulatory issues
• Technological challenges
  – **Scalability** of the underlying blockchain platforms
  – **Safe and correct** contracts (verification)
  – Large yet modular contracts
  – Development/Testing tools
  – ...

2016/05/28 National Chengchi University
Thanks

謝謝聆聽