科技產業技術實務系列課程

區塊鏈的原理與版權管理的應用

曲建仲
台灣大學電機工程學系博士
政治大學科技管理與智慧財產研究所兼任助理教授
中華民國九十六年度全國優秀青年工程師獎章並獲總統召見訓勉

Ansforce
www.ansforce.com

內容大綱

- ⇨ 比特幣(Bitcoin)
- ⇨ 基礎密碼學(Cryptography)：公開金鑰加密(Public key encryption)
- ⇨ 比特幣帳本(BTC ledger)：雜湊演算法(Hash algorithm)
- ⇨ 區塊(Block)與鏈結(Chain)
- ⇨ 比特幣的採礦(Mining)與礦工(Miner)
- ⇨ 節點資料同步：工作量證明(POW)
- ⇨ 區塊鏈的分叉：軟分叉(Soft fork)與硬分叉(Hard fork)
- ⇨ 首次代幣發行(ICO)：以太坊(Ethereum)與以太幣(ETH)
- ⇨ 區塊鏈的應用
- ⇨ 區塊鏈在版權管理上的應用
- ⇨ 結論與建議

Ansforce
www.ansforce.com

❒ 比特幣的起源

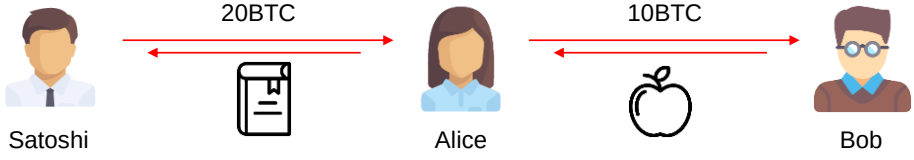
⇨ Satoshi自己創造比特幣(BTC：Bitcoin)並且給自己50BTC。
⇨ Satoshi支付Alice金額20BTC購買一本書籍，並且記錄在比特幣帳本內。
⇨ Alice的疑問？你給我的比特幣(BTC)我要怎麼用呢？

比特幣帳本
(BTC ledger)

付款人	收款人	交易金額
N/A	Satoshi	50BTC
Satoshi	Alice	20BTC

❒ 比特幣的交易流程

⇨ 解決方式：讓使用者能夠以比特幣(BTC)交易。
⇨ Alice支付Bob金額10BTC購買一顆蘋果，並且記錄在帳本內。
⇨ Alice與Bob的疑問？帳本都在你那裡，都是你說了算，我們有什麼保障？



比特幣帳本
(BTC ledger)

付款人	收款人	交易金額
N/A	Satoshi	50BTC
Satoshi	Alice	20BTC
Alice	Bob	10BTC

❒ 比特幣帳本應該放在那裡？

➪ 解決方式：將比特幣帳本複製給使用者Alice和Bob。

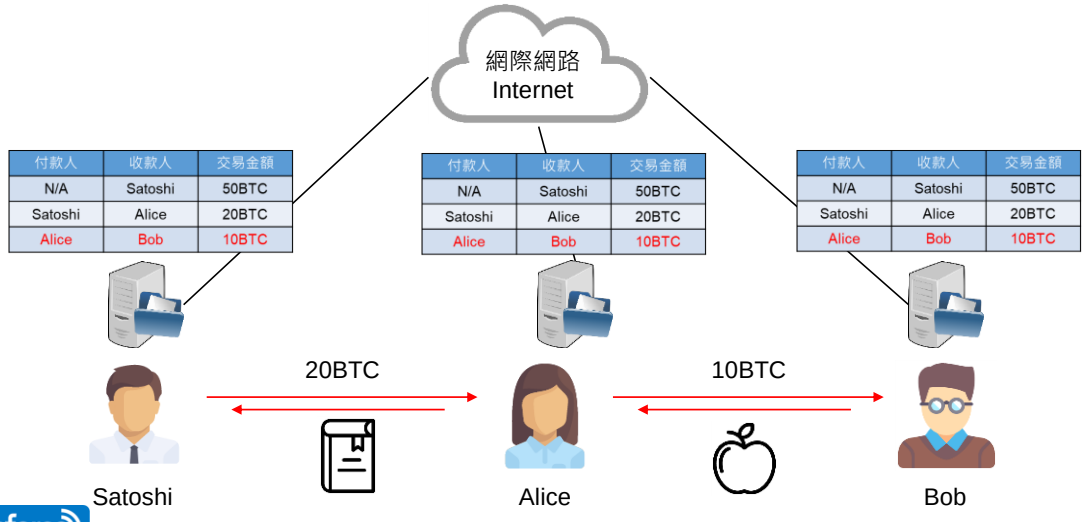
➪ Alice與Bob的疑問？

1.將比特幣帳本複製給所有使用者，那電腦記憶體要多少才夠？

2.每一筆交易都要通知所有使用者，那網路的反應夠快嗎？

3.使用者未必熟悉電腦操作，如何使用電腦進行交易？

❒ 比特幣帳本應該放在那裡？

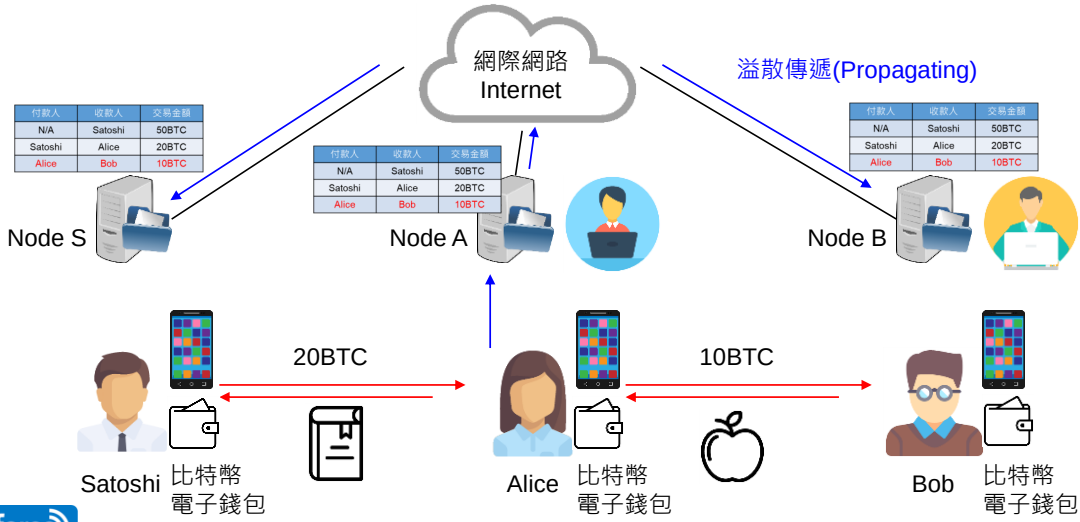


 資料來源：杜宏毅博士，Blockchain的前世今生與未來，台灣網路認證公司。

❒ 比特幣的工作原理：如何付款與收款？

- ⇨ 由Satoshi發起建位第一個節點(Node)，節點指的是在伺服器(Server)內安裝「節點軟體(Node software)」與「比特幣帳本(BTC ledger)」。
- ⇨ 號召網際網路上熟悉電腦操作的自願者在世界各地建立節點(Node)，同時在伺服器(Server)內安裝節點軟體與比特幣帳本。
- ⇨ 節點與節點之間經由「對等式網路連線(Peer to peer network connection)」軟體進行資料交換。
- ⇨ 使用者安裝手機應用程式(APP)「比特幣電子錢包(BTC wallet)」，並且以手機付款與收款，使用非常簡單。
- ⇨ 手機應用程式(APP)將交易內容回傳至節點(Node)，節點(Node)再將交易內容「溢散傳遞(Propagating)」給所有的節點(Node)。

❒ 比特幣的工作原理：如何付款與收款？



❒ 比特幣全球節點(Node)分布

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Nov 18 2017 09:10:12 GMT+0800 (台北標準時間).

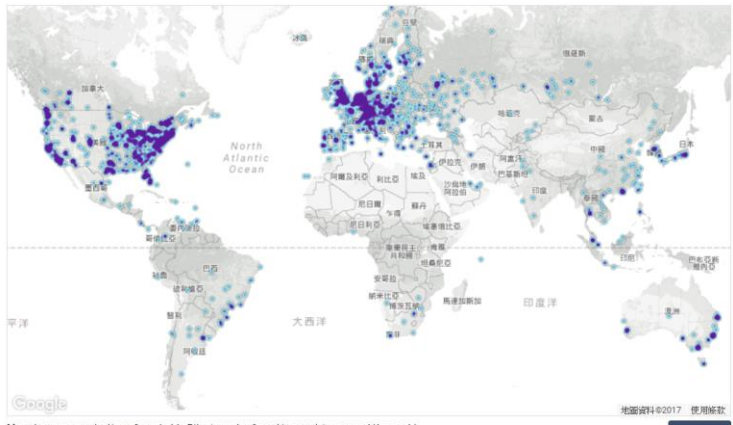
11018 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	3112 (28.24%)
2	Germany	1835 (16.65%)
3	China	753 (6.83%)
4	France	732 (6.64%)
5	Netherlands	526 (4.77%)
6	Canada	462 (4.19%)
7	United Kingdom	420 (3.81%)
8	n/a	409 (3.71%)
9	Russian Federation	342 (3.10%)
10	Singapore	234 (2.12%)

More (100) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

Ansforce www.ansforce.com 資料來源：https://bitnodes.earn.com/。

9

❒ 網路拓撲(Network topology)

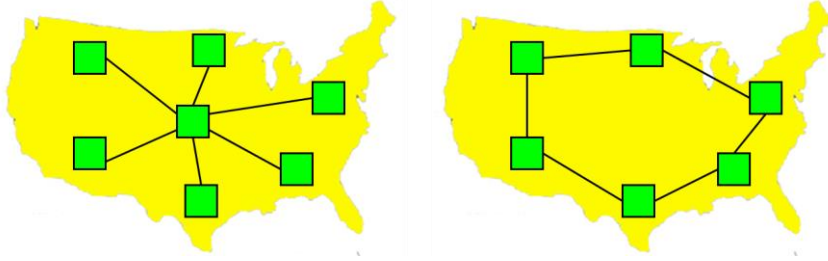
◈ 集中式拓撲(Centralized topology)

➪ 將網路上各節點主機的資料集中到一台固定的主機(超級電腦)處理。

◈ 分散式拓撲(Distributed topology)或非集中式拓撲(Decentralized topology)

➪ 將網路上各節點主機的資料分散到各主機處理，可以減少主機的負載。

➪ 通訊協定(Communication Protocol)：為了使所有通訊設備有共同的通訊規則可以交換資料，必須採用相同的通訊協定(例如：IEEE802.11)。



Ansforce www.ansforce.com

10

❒ 比特幣(Bitcoin)三大特性

◈ 交易識別確認

⇨ 使用公開金鑰驗證機制，確認這筆交易的真實性，使用者不可否認。

⇨ 屬於「可驗證的匿名制」，保留貨幣交易的特性。

◈ 資料無法篡改

⇨ 使用「區塊(Block)」與「鏈結(Chain)」確保交易資料無法篡改。

⇨ 使用「條件雜湊(Hash<Difficulty)」與「前區塊雜湊(Previousblockhash)」。

◈ 節點資料同步

⇨ 使用「工作量證明(POW：Proof of Work)」達到節點資料收斂同步。

⇨ 使用「分散式拓撲」，保留總困難指數高的分支，刪除總困難指數低的分支。

❒ 基礎密碼學(Cryptography)

◈ 密碼學的特性

⇨ 完整性(Integrity)：確保資訊與原來的一致，沒有被竄改或偽造。

⇨ 鑑別性(Authentication)：確認網路的使用者或資料傳送者的身份。

⇨ 不可否認性(Non-repudiation)：不可否認其傳送的資料或完成的交易行為。

⇨ 機密性(Confidentiality)：保護資料內容不讓非法使用者得知。

◈ 密碼學的原理

⇨ 明文(Plaintext)：是指加密前的原始資料。

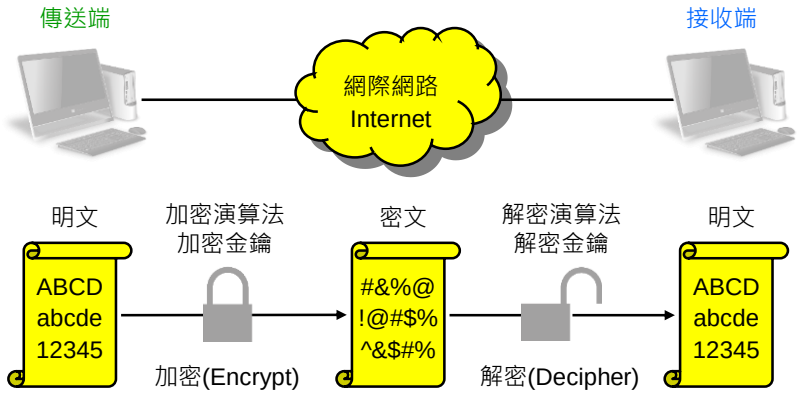
⇨ 加密演算法(Encryption algorithm)：對明文進行加密運算的數學公式(函式)。

⇨ 金鑰(Key)：用來和加密演算法產生特定密文的數字或符號字串。

⇨ 密文(Ciphertext)：是指加密後的資料。

⇨ 解密演算法(Decryption algorithm)：對密文進行解密運算的數學公式(函式)。

❒ 密碼學的原理



❒ 密碼學的種類

◈ 對稱加密(Symmetric encryption)

➪ 加密與解密使用同一把秘密金鑰，所以稱為「對稱(Symmetric)」。

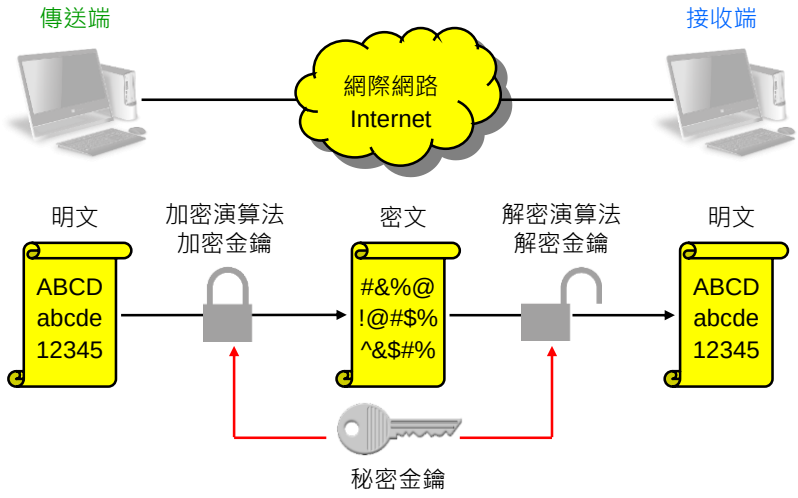
➪ 又稱為「秘密金鑰加密(Secret key encryption)」，是指傳送端與接收端雙方都擁有一把相同的「秘密金鑰(Secret key)」。

➪ 對稱加密與解密演算法通常比較簡單運算較快，秘密金鑰資料量很小，通常只有128位元(bit)或256位元(bit)，所以運算效率較佳。

➪ 傳送端如何將秘密金鑰「安全的」交給接收端而不被攔截？每一對傳送端與接收端都需要一把秘密金鑰，要準備多少金鑰？

➪ 常見的對稱加密技術包括：資料加密標準(DES)、三資料加密標準(TDES)、進階加密標準(AES)等。

❒ 秘密金鑰的加密流程(只有一把金鑰)



❒ 密碼學的種類

◈ 非對稱加密(Asymmetric encryption)

➪ 加密與解密使用不同的金鑰，所以稱為「非對稱(Asymmetric)」。

➪ 又稱為「公開金鑰加密(Public key encryption)」，每一位使用者自行產生一把「私有金鑰(Private key)」與一把「公開金鑰(Public key)」

➪ 使用者必須秘密地保存自己的私有金鑰，並且在網路上發佈公開金鑰，優點是公開金鑰可以公開傳送，同時提供機密性、鑑別性、不可否認性。

➪ 非對稱加密與解密演算法通常比較複雜運算速度較慢，私有金鑰與公開金鑰資料量很大，通常在1024位元(bit)以上，所以運算效率較差。

➪ 非對稱加密技術並不是要用來取代對稱加密技術，而是用來彌補對稱加密的不足以加強安全性，由於兩者各有優劣，實務上經常合併使用。

❒ 公開金鑰的加密與驗證流程(有兩把金鑰)

◈ 公開金鑰加密流程

⇨ 傳送端使用「接收端(對方)」的公開金鑰加密(加密文件)，接收端使用「自己」的私有金鑰解密(解密文件)。

◈ 公開金鑰驗證流程

⇨ 傳送端使用「自己」的私有金鑰加密(簽署文件)，接收端使用「傳送端」的公開金鑰解密(確認簽署者)。

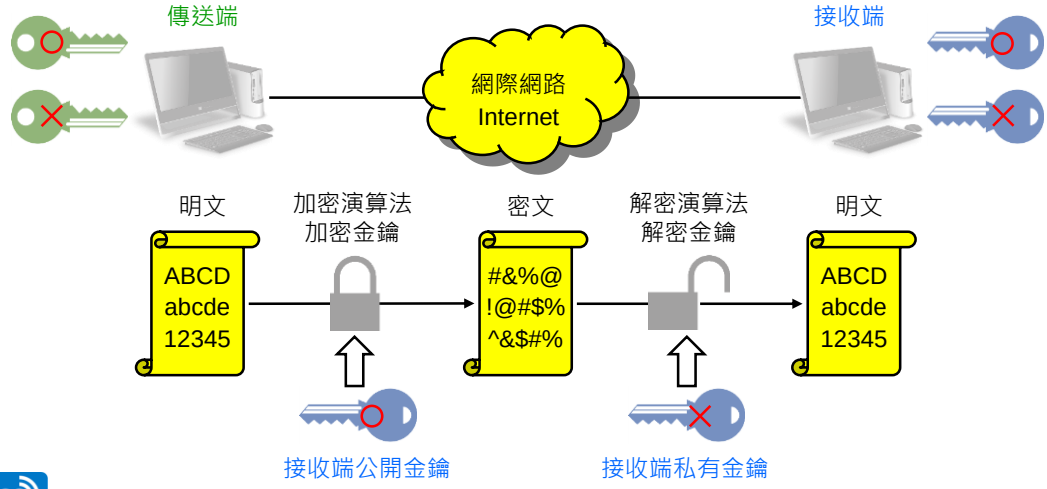
⇨ 接收端：可以確認這份文件是由傳送端發出。

⇨ 傳送端：不可否認曾經傳送這份文件。

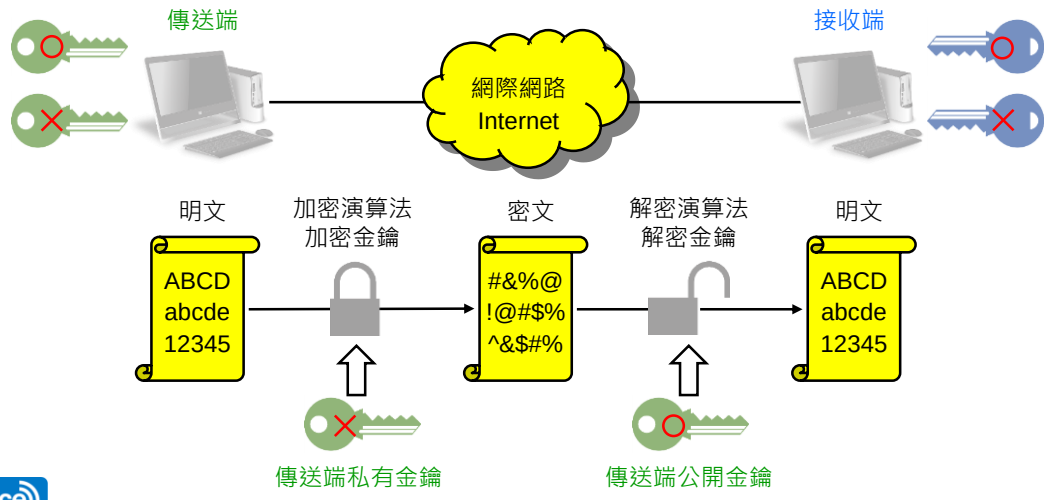
【備註】

⇨ 2015年圖靈獎(Turing Award)得主為昇陽前安全長Whitfield Diffie與史丹佛大學電子工程系的榮譽教授Martin E. Hellman。

❒ 公開金鑰加密流程(有兩把金鑰)



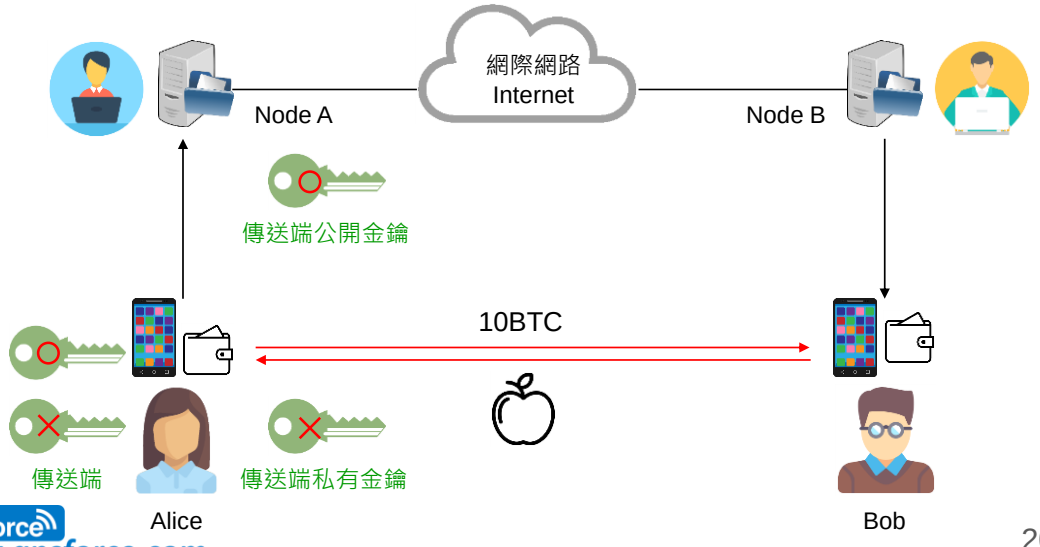
❒ 公開金鑰驗證流程(有兩把金鑰)



Ansforce
www.ansforce.com

19

❒ 交易識別確認：公開金鑰驗證流程



Ansforce
www.ansforce.com

20

❒ 比特幣帳本(BTC ledger)

➪ 比特幣帳本是由一個一個的「區塊(Block)」連接而成的「鏈結(Chain)」，因此這種技術又稱為「區塊鏈(Blockchain)」。

付款人	收款人	交易金額
N/A	01100110	50BTC
00010101	01111001	30BTC
01000100	00011010	20BTC
01100101	00000001	10BTC
00011010	01010101	40BTC
01010101	00001111	15BTC
01111001	00011001	25BTC
01100110	01100110	35BTC

Block 0

付款人	收款人	交易金額
N/A	01100110	50BTC
00010101	01111001	30BTC

Block 1

01000100	00011010	20BTC
01100101	00000001	10BTC

Block 2

00011010	01010101	40BTC
01010101	00001111	15BTC

Block 3

01111001	00011001	25BTC
01100110	01100110	35BTC

❒ 區塊(Block)的意義

◈ 條件雜湊(Conditional hash)

➪ 我們不只需要「資料篡改可以檢查出來」，更需要「資料無法篡改」。

➪ 「雜湊(Hash)」必須小於「困難指數(Difficulty)」，讓雜湊很難重新計算，而保護「交易(Transaction)」的內容不被篡改。

❒ 比特幣的「採礦(Mining)」

◈ 比特幣的採礦步驟

⇨ 猜測一個nonce值。

⇨ 用安全雜湊演算法(SHA)計算「雜湊(Hash)」。

⇨ 如果計算出「雜湊(Hash)」小於「困難指數(Difficulty)」則成功建立一個「區塊(Block)」，可以獲得50BTC做為獎勵。

⇨ 如果計算出「雜湊(Hash)」大於「困難指數(Difficulty)」則重複上述步驟。

⇨ 可能要猜幾十億次才能成功建立一個「區塊(Block)」，因此並不容易。

【名詞解釋】

⇨ 猜測nonce值，計算雜湊(Hash)的動作稱為「採礦(Mining)」，而我們所要採的「礦」就是計算出「雜湊(Hash)」小於「困難指數(Difficulty)」。

❒ 比特幣的「採礦(Mining)」

◈ 比特幣礦工的酬勞

⇨ 進行採礦的人稱為「礦工(Miner)」，計算出一個區塊可以獲得50BTC的酬勞，如果其他支付交易有給手續費，則礦工還會獲得手續費。

⇨ 大約每10分鐘採出一個區塊，每採出21萬個區塊(大約4年)酬勞減半，因此比特幣總數不超過2100萬個BTC，總數固定可以提升比特幣的價值。

$$\text{比特幣總數} = 210{,}000 \times \left(\frac{50}{2^0} + \frac{50}{2^1} + \frac{50}{2^2} + \cdots + \frac{50}{2^n}\right) = 210{,}000 \times 50 \times \left(\frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \cdots + \frac{1}{2^n}\right)$$

$$= 210{,}000 \times 50 \times \left[\left(\frac{1}{2}\right)^0 + \left(\frac{1}{2}\right)^1 + \left(\frac{1}{2}\right)^2 + \cdots + \left(\frac{1}{2}\right)^n\right] = 210{,}000 \times 50 \times \sum_{n=0}^{\infty}\left(\frac{1}{2}\right)^n$$

$$= 210{,}000 \times 50 \times \left(\frac{1}{1-\frac{1}{2}}\right) = 210{,}000 \times 50 \times 2 = 21{,}000{,}000$$

$$\sum_{n=0}^{\infty}\left(\frac{1}{r}\right)^n = \frac{1}{1-r}$$

❒ 比特幣的「採礦(Mining)」

◈ 比特幣礦工的酬勞

⇨ 比特幣2009年發行礦工酬勞50BTC，2012年12月第一次減半酬勞25BTC，2016年7月第二次減半酬勞12.5BTC，酬勞下降使手續費成為採礦動機。

⇨ 為了維持大約每10分鐘採出一個區塊，產生新區塊的難度會定期調整，每採出2016個區塊(大約兩週)會自動調整接下來2016個區塊的採礦難度。

⇨ 比特幣的區塊大約1MB，一筆交易大約256B，一個區塊大約儲存4096筆交易，平均每秒最多只能處理7筆交易(4096筆交易/600秒=6.82)。

⇨ 比特幣礦工最早使用Intel或AMD的CPU產品來採礦，2013年礦工開始使使用GPU、FPGA，甚至ASIC大量投入使得個人礦工已經沒有收益。

 資料來源：http://www.bitcoin-tw.com/bitcoin-stats.html。

❒ 鏈結(Chain)的意義

◈ 區塊鏈(Blockchain)的「鏈結(Chain)」

⇨ 將不同的區塊以「 雜湊(“hash”)與前區塊雜湊(“previousblockhash”)」給「鏈結(Chain)」起來，可以大大增加資料的安全性。

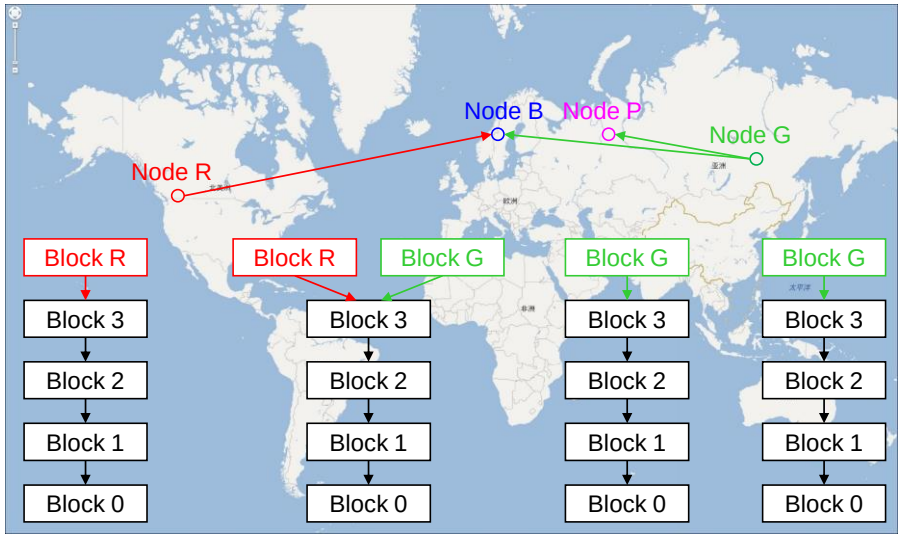
⇨ 區塊一(Block 1)：想要篡改「交易(Transaction)」，由於交易會影響表頭(Header)內的摘要(merkleroot)，必須重新計算區塊一的「雜湊(Hash)」。

⇨ 區塊二(Block 2)：區塊一的雜湊(Hash)儲存在「區塊二」表頭(Header)內的「 “previousblockhash”」，必須重新計算區塊二的「雜湊(Hash)」。

⇨ 假設這個區塊鏈有100個區塊(Block)，則篡改一個區塊的交易(Transaction)就必須重新計算100次雜湊(Hash)，在合理的時間內根本不可能。

⇨ 牽一髮而動全身，當區塊鏈(Blockchain)愈長，前面的區塊(Block)就被保護的愈安全，而且每個結點都有比特幣帳本，只篡改一個節點也沒有用。

❒ 節點資料同步



 資料來源：杜宏毅博士，Blockchain的前世今生與未來，台灣網路認證公司。27

❒ 節點資料同步

◈ 溢散傳遞(Propagating)

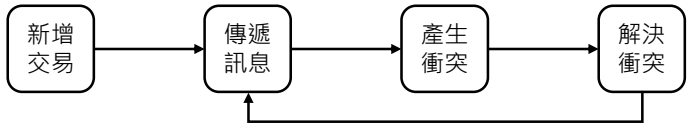
⇨ 節點(Node R)：已儲存區塊(Block 0/1/2/3)，採出新礦區塊(Block R)。

⇨ 節點(Node G)：已儲存區塊(Block 0/1/2/3)，採出新礦區塊(Block G)。

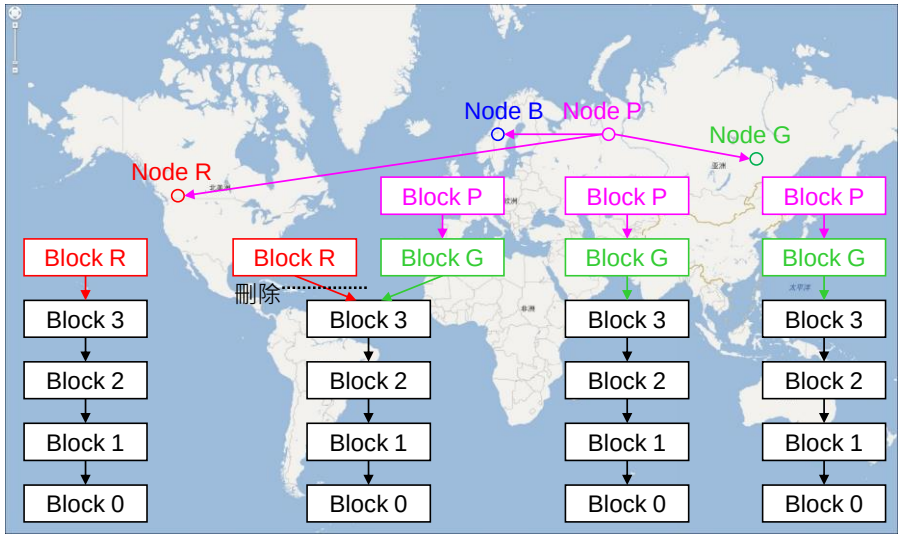
⇨ 區塊(Block R與Block G)分別經由「溢散傳遞(Propagating)」給所有節點，其中節點(Node B)同時收到區塊(Block R與Block G)。

⇨ 節點(Node B)不知道該鏈結那個區塊，因此同時將區塊(Block R與Block G)鏈結到區塊(Block 3)後面，形成「分岔(Fork)」。

⇨ 節點(Node P)：已儲存區塊(Block 0/1/2/3/G)，採出新礦區塊(Block P)。



❒ 節點資料同步



資料來源：杜宏毅博士，Blockchain的前世今生與未來，台灣網路認證公司。

❒ 節點資料同步

◈ 工作量證明(POW：Proof of Work)

⇨ 節點(Node B)：將區塊(Block P)鏈結在區塊(Block G)，並且計算區塊(Block R與Block G/P)兩個分支的「總困難指數(Difficulty)」。

⇨ 假設區塊(Block G/P)分支的總困難指數高，則保留總困難指數高的分支，刪除困難指數低的分支，稱為「工作量證明(POW：Proof of Work)」。

⇨ 如果被刪除區塊(Block R)內的「交易(Transaction)」已經包含在區塊(Block G與Block P)內則不做任可變動。

⇨ 如果被刪除區塊(Block R)內的「交易(Transaction)」沒有包含在其他區塊內，節點(Node B)將這些交易傳遞出去讓其他區塊將這些交易包含進去。

⇨ 重複上面步驟，使所有節點的資料收斂(Convergence)達到同步而一致。

❒ 軟分叉(Soft fork)與硬分叉(Hard fork)

◈ 軟分叉(Soft fork)

➪ 當新共識規則發布後，未升級的節點會因為不知道新共識規則，而產生不合法的區塊，通常就會產生的臨時分叉。

➪ 區塊鏈的資料結構發生改變時，未升級的節點可以驗證已升級的節點採出的區塊，而且已升級的節點也可以驗證未升級的節點採出的區塊。

◈ 硬分叉(Hard fork)

➪ 區塊鏈發生永久性分叉，在新的共識規則發布後，部分沒有升級的節點無法驗證已經升級的節點所產生的區塊，通常就會發生硬分叉。

➪ 區塊鏈的區塊格式或交易格式發生改變時，未升級的節點拒絕驗證已升級的節點採出的區塊，但是已升級的節點可以驗證未升級的節點採出的區塊，然後大家各自延續自己認為正確的鏈，所以分成兩條鏈。

❒ 比特幣(Bitcoin)三大特性

◈ 交易識別確認

➪ 使用公開金鑰驗證機制，確認這筆交易的真實性，使用者不可否認。

➪ 屬於「可驗證的匿名制」，保留貨幣交易的特性。

◈ 資料無法篡改

➪ 使用「區塊(Block)」與「鏈結(Chain)」確保交易資料無法篡改。

➪ 使用「條件雜湊(Hash<Difficulty)」與「前區塊雜湊(Previousblockhash)」。

◈ 節點資料同步

➪ 使用「工作量證明(POW：Proof of Work)」達到節點資料收斂同步。

➪ 使用「分散式拓撲」，保留總困難指數高的分支，刪除總困難指數低的分支。

❒ 首次公開發行(IPO)與首次代幣發行(ICO)

◈ 首次公開發行(IPO：Initial Public Offering)

➪ 經由證券交易所，公司首次將它的股票(Stock)賣給投資人(個人或法人)來募集公司營運所需要的資金，私人公司經由這個過程轉化為上市公司。

➪ 投資人以法定貨幣(例如：新台幣或美金)來交換私人公司的股票，通俗的說就是「印股票換鈔票」。

◈ 首次代幣發行(ICO：Initial Coin Offering)

➪ 經由區塊鏈平台，公司首次將它的代幣(Token)賣給投資人(個人或法人)來募集公司營運所需要的資金，私人公司經由這個過程轉化為？？？？。

➪ 投資人以其他加密貨幣(例如：比特幣或以太幣)來交換私人公司的代幣，，通俗的說就是「以代幣換代幣」。

❒ 以太坊(Ethereum)與以太幣(Ether)

◈ 以太坊平台(Ethereum platform)

➪ 不同應用必須分別定義自己的區塊鏈協定(共識規則)，造成只有少數區塊鏈應用相容，與其他區塊鏈應用無法相容的問題。

➪ 以太坊創始人Vitalik希望讓區塊鏈技術應用在加密貨幣以外的領域，讓開發者建立可擴展、易開發、可相容的各種區塊鏈應用。

➪ 提供很好的智能合約建立通用的區塊鏈協定，讓程式設計師在以太坊區塊鏈協定上撰寫程式語言，可以快速開發應用，與其他區塊鏈應用相容。

➪ 開發者可以在以太坊平台上創造一個全新的加密貨幣(例如：科學幣)，投資人再以其他加密貨幣(例如：比特幣或以太幣)來交換科學幣。

➪ 2014年7月以太坊就是用這個方法募集了31,591個比特幣(當時市值1,840萬美元)，隨著加密貨幣的膨脹吸引更多開發者、投資者、投機者投入。

❒ 比特幣與其他資產比較

資產種類	貴金屬	法定貨幣	比特幣
資產實例	黃金、白銀等	美元、歐元等	比特幣、乙太幣
存放成本	每年0.15%到1%	由存放款利差所補貼	免費
交易成本	昂貴	中等	僅需極低廉手續費
防偽	無法複製或人工合成	防偽技術、法律	密碼學
運送	昂貴且有安全問題	不方便且有安全問題	安全、方便、便宜、迅速
存放方式	存放於機構	存放於機構	密碼學及區塊鏈
發行方式	挖礦	政治(印鈔鑄幣)	演算法
信用媒介	物理的稀少性	國家政權	演算法及區塊鏈
記錄儲存	手動	手動	區塊鏈自動記入
支付結算	昂貴	集中式	分散式(非集中式)
稀有性	高	主觀的	演算法，最高2100萬個
鑑定	昂貴的化驗	信賴對方	區塊鏈
凍結	會被扣押	會被凍結	只要私鑰在，無法被扣押凍結
隱私	實名但保密	實名但保密	匿名但公開

 資料來源：維基百科。

❒ 比特幣(Bitcoin)的問題

- ⇨ 可驗證的匿名制：可驗證代表可以確認這筆交易的真實性，匿名制代表並不知道發動這筆交易的人是誰，因此容易造成交易追蹤斷線。
- ⇨ 分散式拓撲：沒有中央控管機制會造成交易不確定性、究責與賠償困難、服務提供者(節點或電子錢包)技術落差等問題。
- ⇨ 比特幣(Bitcoin)的目標明確，就是要取代傳統貨幣扮演貨幣支付的角色，但是仍然有許多困難必須克服，重複支付、結算確認、交易同步等。
- ⇨ 比特幣在法規上存有疑義難以被主管機關接受，因此有人將比特幣的部分技術抽離出來尋找新的應用，並且取了新名字：區塊鏈(Blockchain)。
- ⇨ 區塊鏈落實困難，無法直接套用到現用的其他應用上，因此開始演化並且出現新名字，例如：分散式帳本(Distributed ledger)、分享式帳本(Shared ledger)、超級帳本(Hyper ledger)等。

❒ 區塊鏈的種類

◈ 公共區塊鏈(Public blockchain)

➪ 全世界任何人都可讀取、任何人都能發送交易、交易能獲得有效確認的、任何人都能參與其中共識過程的區塊鏈，通常被視為「完全去中心化」。

◈ 聯盟區塊鏈(Consortium blockchain)

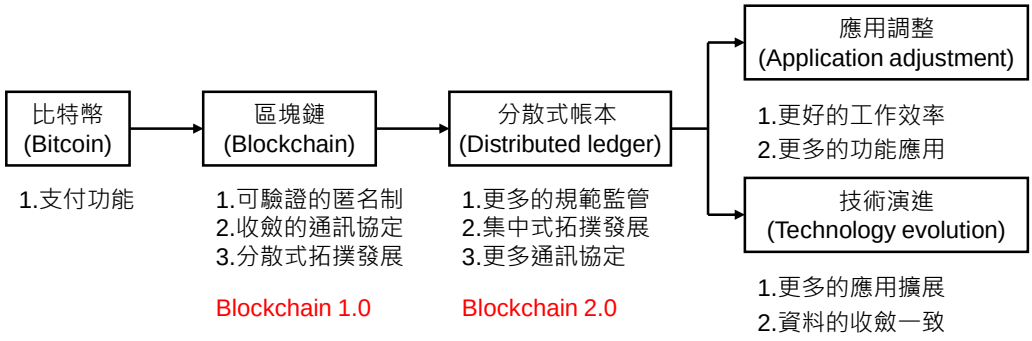
➪ 共識過程受到預先設定節點控制的區塊鏈，假設有一個由10家銀行組成的區塊鏈，每個銀行設定一個節點，通常被視為「部分去中心化」。

◈ 私有區塊鏈(Private blockchain)

➪ 所有權限掌握在一個公司或組織的區塊鏈，因此規則可能也由該公司或組織決定，讀取權限可能對外開放，也可能會有所限制。

➪ 系統仍保留區塊鏈真實性和部分去中心化的特性，規則改變容易，交易成本便宜，節點連接容易、隱私保護較佳，因此適合金融機構使用。

❒ 區塊鏈(Blockchain)的演化過程



 資料來源：杜宏毅博士，Blockchain的前世今生與未來，台灣網路認證公司。

❒ 區塊鏈(Blockchain)的應用

- ⇨ 加密數位貨幣(Cryptocurrency)：必須考量主管機關接受程度，例如：比特幣(Bitcoin)、美國郵政貨幣(Postcoin)；考量是否適合應用在高頻交易，Ripple將其應用在非即時的跨國金融機構外匯交換業務可能更合適。
- ⇨ 價值登錄機制(Value registry)：Factom、SmartContract將分散式帳本應用在所有權與存在證明(POEAP：Proof of Existence and Possession)。
- ⇨ 價值型聯網(Value web)：進行有價資產登錄(Value registry)、智慧型合約(Smart contract)、國內支付(Domestic payment)、國際支付(International payment)、貿易金融(Trade finance)、資本市場(Capital market)。
- ⇨ 價值生態系(Value ecosystem)：應用在非金融服務，Ethereum將其應用在公開帳本(Public ledger)提供各種商業應用；R3CEV將其應用在私密帳本(Private ledger)提供各種金融應用。

❒ 信任機器 / 信任機制(Trust machine)

◈ 我們的世界是建立在信任機制上

- ⇨ 我們將個人財產交給銀行來保管 ➔ 基於對金融體制的信任
- ⇨ 我們將個人資訊交給政府來保管 ➔ 基於對政府機構的信任

◈ 舊有的信任機制保護不足

- ⇨ 完全依賴第三方信任機構提供價值證明與所有權證明
- ⇨ 舊有的證明方式有許多缺點：不易傳遞、容易偽造、沒有效率、法規限制
- ⇨ 銀行服務的便利性可以再提升嗎？政府服務的效率可以再提升嗎？

◈ 區塊鏈是信任機制的基礎建設

- ⇨ 加密保護的共享帳本確保資料無法篡改
- ⇨ 去中心化不需要依賴第三方信任機構
- ⇨ 可以提供各種改變與創新的應用

❒ 區塊鏈(Blockchain)的應用

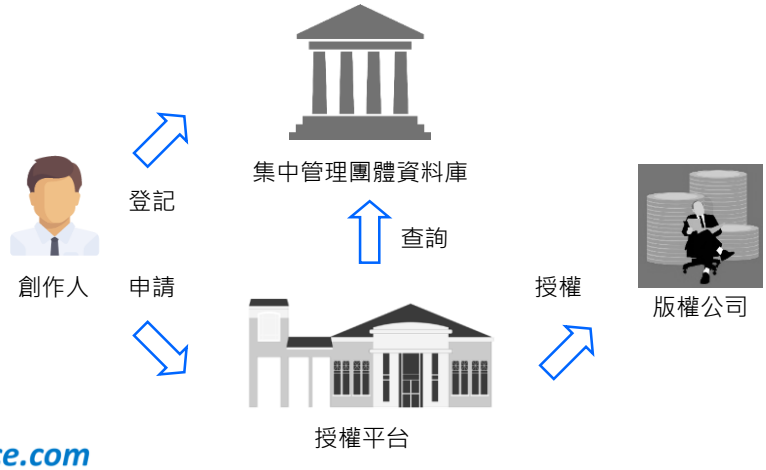
- ⇨ 電子商務：透過支付平台需要佣金對雙方都不利、如果B寄出不良商品？
- ⇨ 學歷證明：申請耗時耗力、資料可能篡改
- ⇨ 旅館民宿：安全、評價、價格無法公開透明，共享經濟抽取高額佣金
- ⇨ 醫療保健：向醫生隱瞞病、病歷無法自由存取、病歷可能被惡意運用
- ⇨ 民意調查：中間人偏好影響結果、統計錯誤、資料做假
- ⇨ 能源交易：私下交易、付錢後不供電、中間人抽取高額費用
- ⇨ 生產履歷
- ⇨ 專利與著作權

❒ 傳統版權管理方式

- ⇨ 直接到政府版權管理部門申請登記著作權，保護效果最好，但是發證時間長、登記費用高，而且不適合目前追求時效與低成本的網路創作。
- ⇨ 直接在圖片或影片加上浮水印或文字商標，但是去浮水印技術簡單，往往要確定創作權歸屬不易，很難確定誰的創作產出時間更早。
- ⇨ 音樂銷售從發行公司、版權公司、音樂平台、金融機構最後到的使用者，中間人的層層媒介不透明，複雜的權利分潤成本高且效率低。
- ⇨ 分潤過程不透明，創作人不確定自己的創作被點閱次數與相關資訊，中間人掌握了大部分控制權，實際到創作者手中的分潤偏低。

❒ 傳統版權管理方式

➪ 台灣音樂著作財產權授權平台：使用傳統的中心化架構，以集中管理團體資料庫作為中心，創作人要將一筆音樂著作專屬授權給版權公司。



Ansforce
www.ansforce.com

43

❒ 區塊鏈版權管理方式

➪ 創作人直接將著作的身份資訊與時間、內容等資訊寫入區塊鏈確定版權歸屬，由於區塊鏈去中心化與不可篡改的特性，版權就有了唯一性。

➪ 區塊鏈雖然無法防止轉載、抄襲，但是發生糾紛時可以立即經由區塊鏈裡確定版權歸屬，達到快速取證的作用。

➪ 創作人直接將著作的身份資訊與時間、內容等資訊寫入區塊鏈，再把檔案利用存放在分散式儲存平台供使用者戶付費存取。

➪ 在區塊鏈建位的數位版權管理架構，中間人不再扮演「價值傳遞」的角色，而應該轉變為「價值創造」，協助創作人利用作品創造更多的價值。

➪ 中間人應該投入更多資源在產品、內容、創意、行銷等實際創造價值的事務，而將更多的收益分潤給創作人。

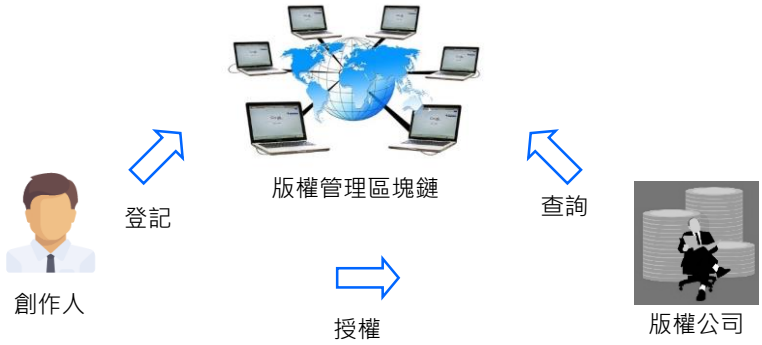
Ansforce
www.ansforce.com

44

❒ 區塊鏈版權管理方式

➪ 版權管理區塊鏈：使用區塊鏈去中心化架構，創作人直接將著作資訊寫入區塊鏈，創作人要將一筆音樂著作專屬授權給版權公司。

➪ 交易雙方都可以直接在公開的區塊鏈上查詢相關資訊，去中心化與不可篡改的特性免除了中間人為操控的問題。



❒ 影音產業區塊鏈應用實例

➪ Dotblockchain Music：從檔案格式到對應之APP和區塊鏈的技術框架

➪ Ujo Music：基於以太坊區塊鏈技術提供音樂授權服務

➪ Musicoin：基於以太坊區塊鏈核心技術修改而成的一種計次播放服務

➪ MUSE Blockchain：針對著作權登記和版稅結算所設計的區塊鏈架構

➪ PeerTracks：基於MUSE Blockchain 所架構的音樂播放平台

 資料來源：http://www.pochang.com/blog/，Pochang Wu 2017。

❒ 影音產業區塊鏈應用實例

◈ 介面(Interface)

➪ 使用者透過區塊鏈軟體取得服務，可能網頁、手機或電腦應用程式等，包括：著作權登記、查詢、交易、授權、管理、播放、智能合約開發等。

◈ 智能合約(Smart contract)

➪ 第二代區塊鏈(Blockchain 2.0)提供的服務，例如：乙太坊(Ethereum)、超級帳本(Hyperledger)等，是以程式撰寫的自動執行合約。

➪ 使用者經由介面執行智能合約，產生交易與訊息，並且在交易完成後記錄在帳本上，可以用來建立和管理授權的相關約定，可以自動執行。

➪ 創作登記、讓與、授權、使用、分潤結算，其中授權包括：類型、範圍、地區、時間、分潤、合約延展或終止等。

❒ 影音產業區塊鏈應用實例

◈ 紀錄(Record)

➪ 由智能合約產生的各項紀錄，包括：著作權(Copyright)、著作權人位址、著作名稱、後設資料(Metadata)、權利人分配比例等。

➪ 登記和讓與紀錄(Registration & Transfer)、授權紀錄(License)、利用與使用報酬結算紀錄(Exploitation & Payment)等。

◈ 帳本(Ledger)

➪ 帳本用來保存智能合約、紀錄、和其他狀態。

❒ 影音產業區塊鏈應用實例

Interface	Web browser	Mobile APP	Desktop APP		
	Consumer service	Business service	Application service		
Smart contract	Registration	Transfer	Licensing	Exploitation	Payment
Record	Copyright	License	Registration & Transfer	Exploitation & Payment	
Ledger	Blockchain data structure	Consensus protocol	Privacy	Security	

Ansforce www.ansforce.com 資料來源：http://www.pochang.com/blog/，Pochang Wu 2017。

❒ 影音產業區塊鏈相關參與者

- ⇨ 著作人：詞曲作者、音樂製作人、獨立音樂人。
- ⇨ 著作關係人：表演者、製作相關工作者、收益分配人、其他著作關係人。
- ⇨ 著作財產權人：著作人、音樂廠牌、投資人。
- ⇨ 著作財產權代理人：音樂版權公司、錄音代理發行公司。
- ⇨ 開發者：系統開發團隊、應用服務商、學術研究單位、其他獨立開發者。
- ⇨ 集中管理團體：錄音著作集管團體、音樂著作集管團體。
- ⇨ 主管機關：智慧財產局、國家圖書館、文化部影視及流行音樂產業局。
- ⇨ 著作財產權代理人：數位音樂平台、影音媒體、影音製作單位、音樂活動主辦單位、播放音樂之營業場所、個人用戶等。

Ansforce www.ansforce.com 資料來源：http://www.pochang.com/blog/，Pochang Wu 2017。

❒ 結論與建議

◈ 比特幣(Bitcoin)

➪ 比特幣已經佔有一席之地，未來不會消失，利用區塊鏈可以創造各種加密貨幣(例如：乙太幣)，各種加密貨幣競爭將使比特幣回到合理價位。

◈ 以太坊平台(Ethereum platform)

➪ 提供智能合約建立通用的區塊鏈協定，讓程式設計師在以太坊區塊鏈協定上撰寫程式語言，可以快速開發應用，與其他區塊鏈應用相容。

◈ 區塊鏈(Blockchain)

➪ 區塊鏈可以說是一種「規範網路上分散的節點儲存資料與交換資料的通訊協定或技術」，可以應用在各種重要資料與價值資產記錄。

➪ 區塊鏈是一種可以創新應用的技術，的確具有發展潛力，但是不應該將這種技術神化為「凡事皆區塊鏈」，才不會重蹈「凡事皆奈米」的覆轍。

❒ 結論與建議

➪ 所有權證明：如何證明創作人擁有所有權？仍然必須經由權威公證機構來證明。可能的做法是在所有權登記時附加外部連結認證。

➪ 金流問題：加密貨幣與現金的交換必須經由交易所，因此當使用者想要支付費用時仍然必須經由一般銀行匯款或信用卡支付，處理完畢後再由金流節點呼叫智能合約完成整個結算手續，不符合區塊鏈去中心化的原則。

➪ 交易費用：智能合約在技術上可以做到使用即結算，例如：使用者每次播放歌曲時就支付播放費用給權利人，但是必須考慮支付給礦工的手續費問題，所以可行性有待評估。

➪ 目前大多數區塊鏈版權管理都是想要跳過大部份產業參與者，直接連結創作人與使用者，但是目前數位影音產業發展相當成熟，因此讓產業內的所有參與者都找到加入的誘因，與加入後所能扮演的角色才能成功。