

Ethereum protocol

以太坊協議

Classroom

- <https://classroom.google.com/> (請以 gmail 信箱登入)
- 加入課程 **fxrxtx9**



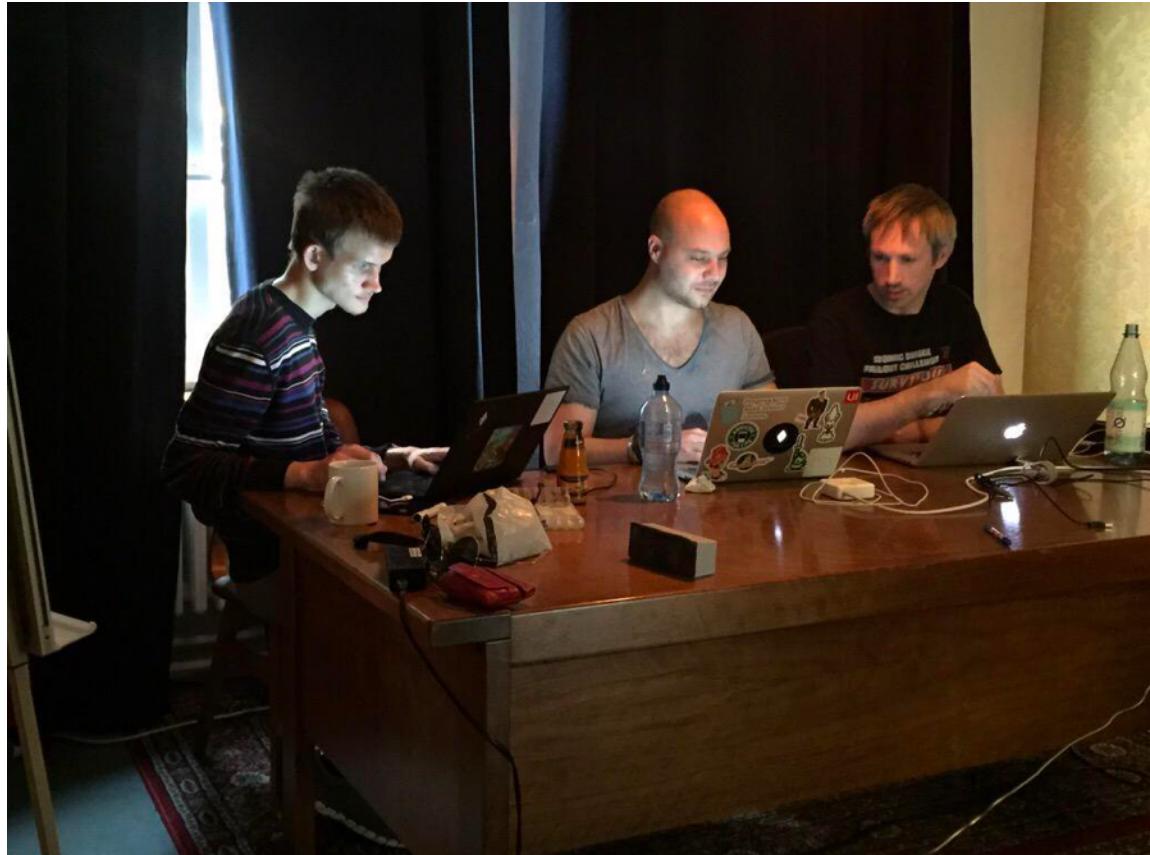
etherium

Co-Founder

- Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer.

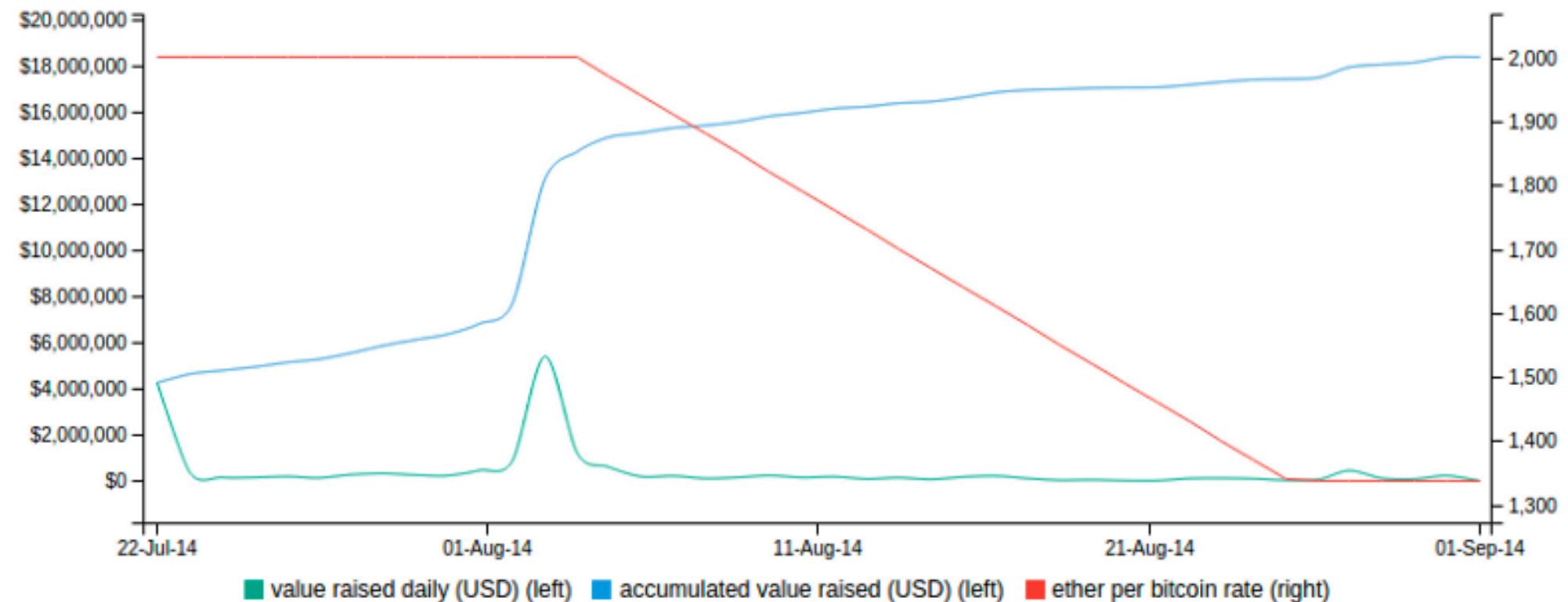


The Ethereum Launch Process



Crowdsale

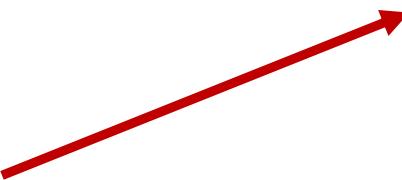
- Run for 42 days, between Jul-Sep in 2014.
- The sale price was 2000 ETH for 1 BTC for the first 14 days, and then started increasing linearly, finishing at 1337 ETH for 1 BTC.



Ethereum

- The system went live on 30 July 2015

Version	Code name	Release date
0	Olympic	May, 2015
1	Frontier	30 July 2015
2	Homestead	14 March 2016
3	Metropolis (vByzantium)	16 October 2017
3.5	Metropolis (vConstantinople)	TBA ^[25]
4	Serenity	TBA

 A red arrow points from the left towards the row containing the version number 3 and its code name Metropolis (vByzantium).

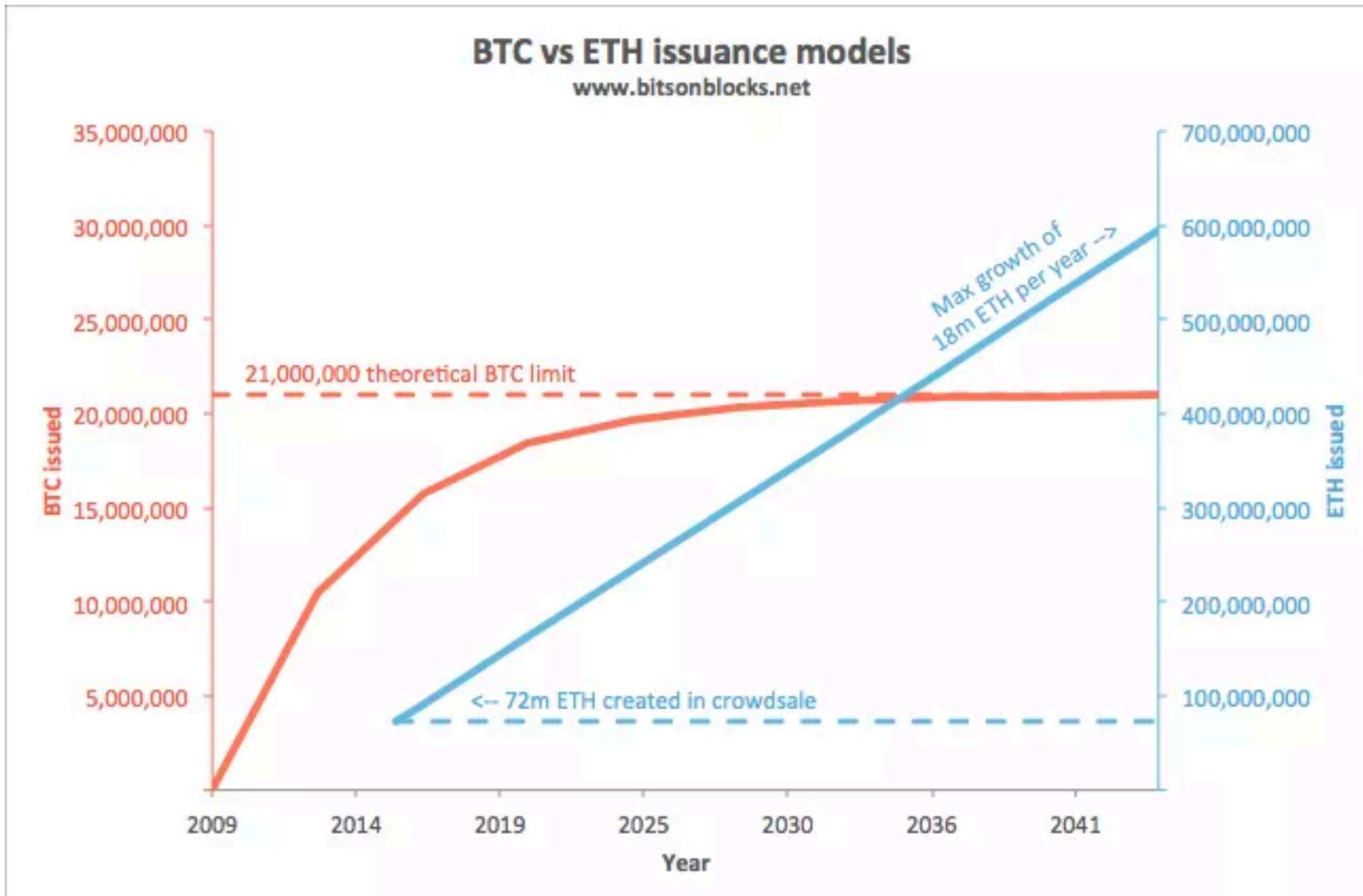

Old version **Latest version** Future release

Ethereum

- 以太坊基金會, 瑞士
- 柏林, 新加坡

Cryptocurrency	Ether
Ticker symbol	ETH
Timestamping scheme	Proof-of-work (Ethash)
Hash function	Keccak
Issuance	Block and Uncle/Ommer reward
Block reward	3 ETH → 2 ETH
Block time	14-15 seconds on average
Block explorer	https://etherscan.io/ https://www.etherchain.org/

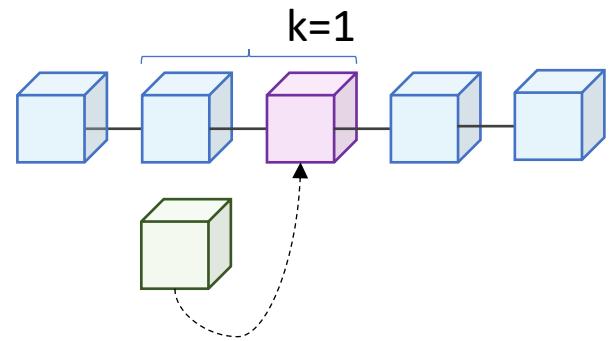
ETH issuance model



ETH issuance model (Early stage)

Total ETH = Pre-mine + Block rewards + Uncle rewards + Uncle inclusion reward

- Pre-mine: 以太坊正式運營之間，預先產出7200萬個以太幣，之後限制每年的生成以不超過四分之一的預先發行量，即1800萬個以太幣
- Block reward: 目前每一個區塊獎勵是5個以太幣，一個區塊的生成速度約14秒，換言之，一年相當於有225萬個區塊 ($365 \times 24 \times 60 \times 60 / 14$)，1125萬個以太幣生成
- Uncle reward: 在以太坊中，有些區塊在同一時間被其他礦工所發現，但卻不是接在主鏈上，稱之為Uncle區塊，相當於比特幣中的孤兒區塊(Orphan block)。這類區塊可能被之後的區塊所參照，此外這類區塊的獎勵為正常獎勵的八分之七，即 $5 \times (7/8) = 4.375$ 個以太幣。依據Uncle區塊的產生速率，一年約有接近700萬個以太幣生成
- Uncle inclusion reward: 打包 Uncle block 的礦工，可得現有以太幣的 1/32。



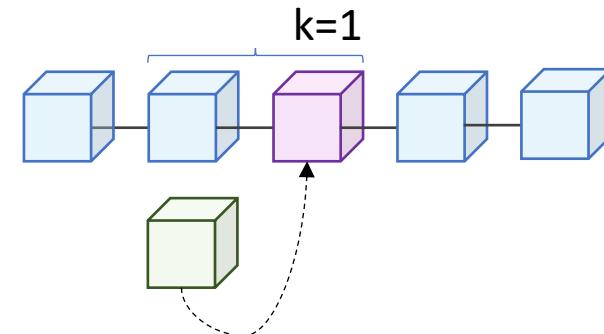
Current issuance

- Total ETH = Block rewards + Uncle rewards + Uncle inclusion reward
- Block reward: 目前每一個區塊獎勵是 2 個以太幣，一個區塊的生成速度約 12 秒
- Uncle reward: 沒進入到主鏈的合法區塊
 - $k = \text{block_number} - \text{uncle_number}$
 - $\text{new_uncle_reward} = (8 - k) * \text{block_reward} / 8$
 - Uncle inclusion reward = $\text{block_reward} / 32$
 - Example: <https://etherscan.io/block/8570623>
 - 2.2401790918 Ether (**2 + 0.1776790918 + 0.0625**)
 - Block_reward + tx fee + 1 Uncle inclusion reward (最多 2 個 Uncle inclusion reward)
- Uncle inclusion reward: 打包 Uncle block 的礦工，可得現有以太幣的 $2*1/32$

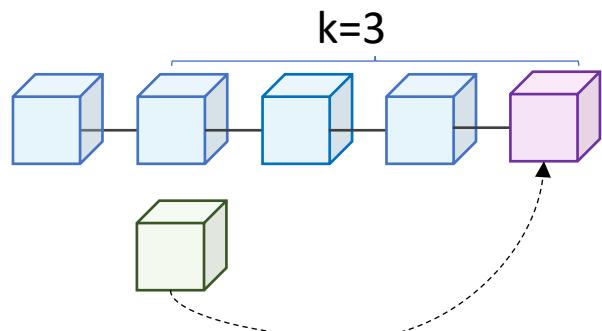
- 我是礦工，我可以打包盡可能多的 uncle block 嗎？
- 為什麼會有 uncle block？
- 我什麼時候會收到 reward？

Current issuance

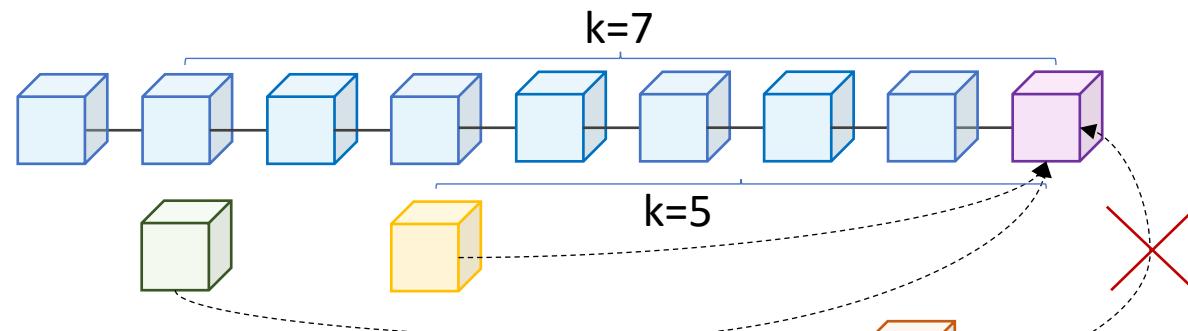
- $k = \text{block_number} - \text{uncle_number}$
- $\text{new_uncle_reward} = (8 - k) * \text{block_reward} / 8$
- Uncle inclusion reward = $\text{block_reward} / 32$



粉綠色礦工獎勵: $(8-1) * R / 8$
粉紫色礦工獎勵: $1/32 * 1 * R$



粉綠色礦工獎勵: $(8-3) * R / 8$
粉紫色礦工獎勵: $1/32 * 1 * R$



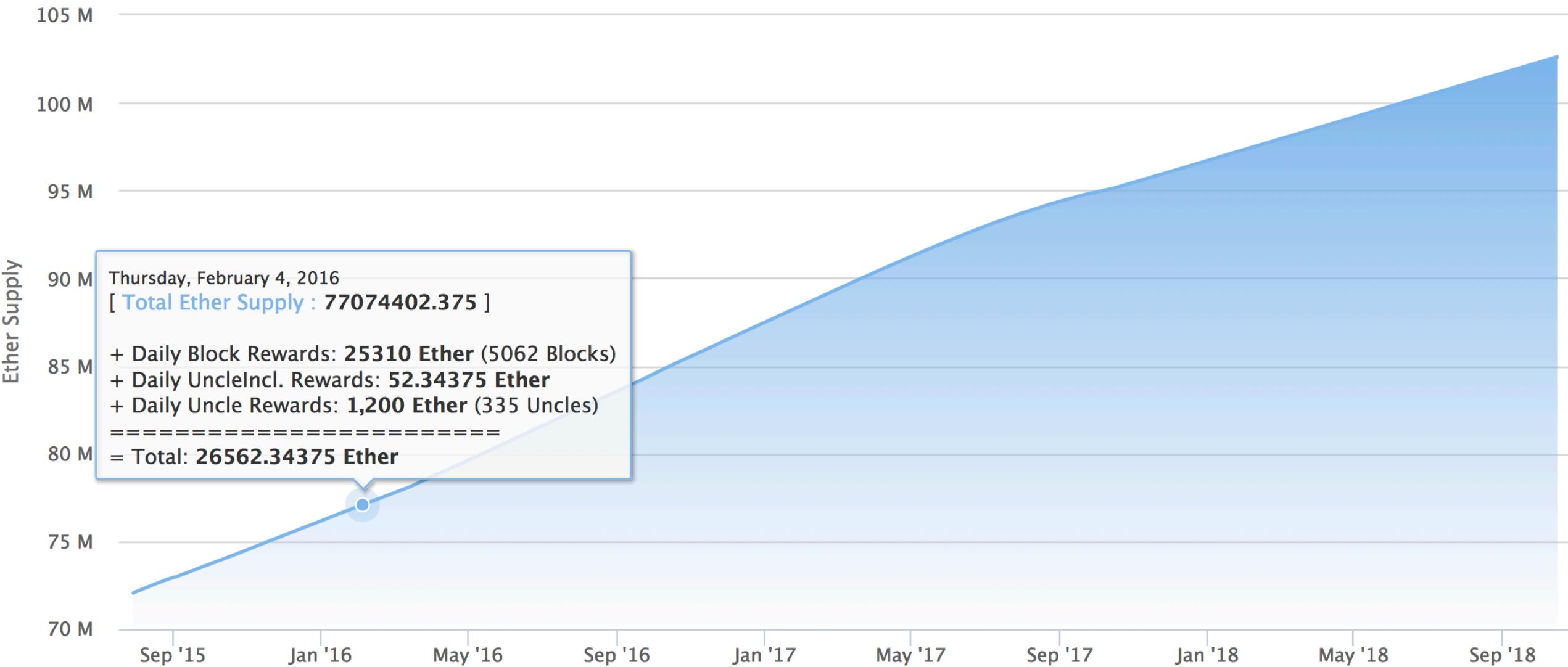
粉綠色礦工獎勵: $(8-7) * R / 8$
粉黃色礦工獎勵: $(8-5) * R / 8$
粉紫色礦工獎勵: $1/32 * 2 * R$

一個塊最多只能包兩個 uncle block
如果之後有其他礦工也可以收

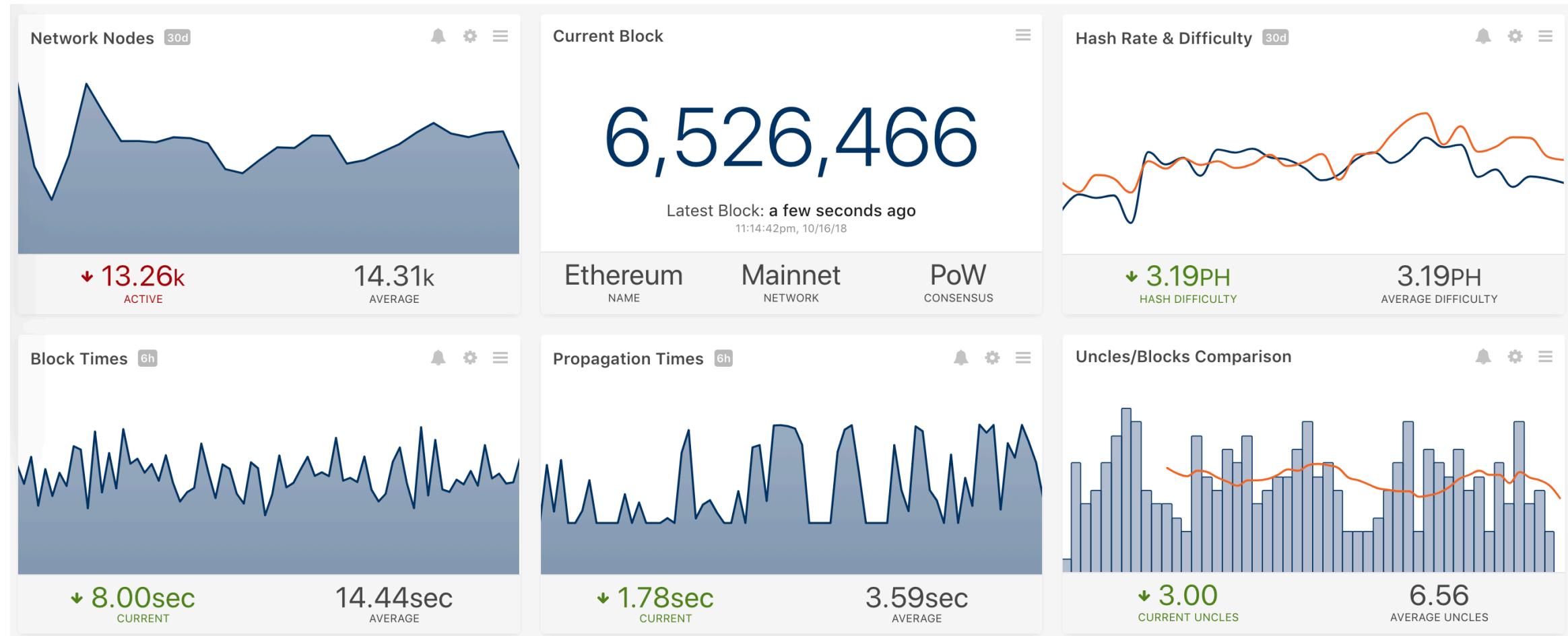
Ether Supply Growth Chart

Source: Etherscan.io

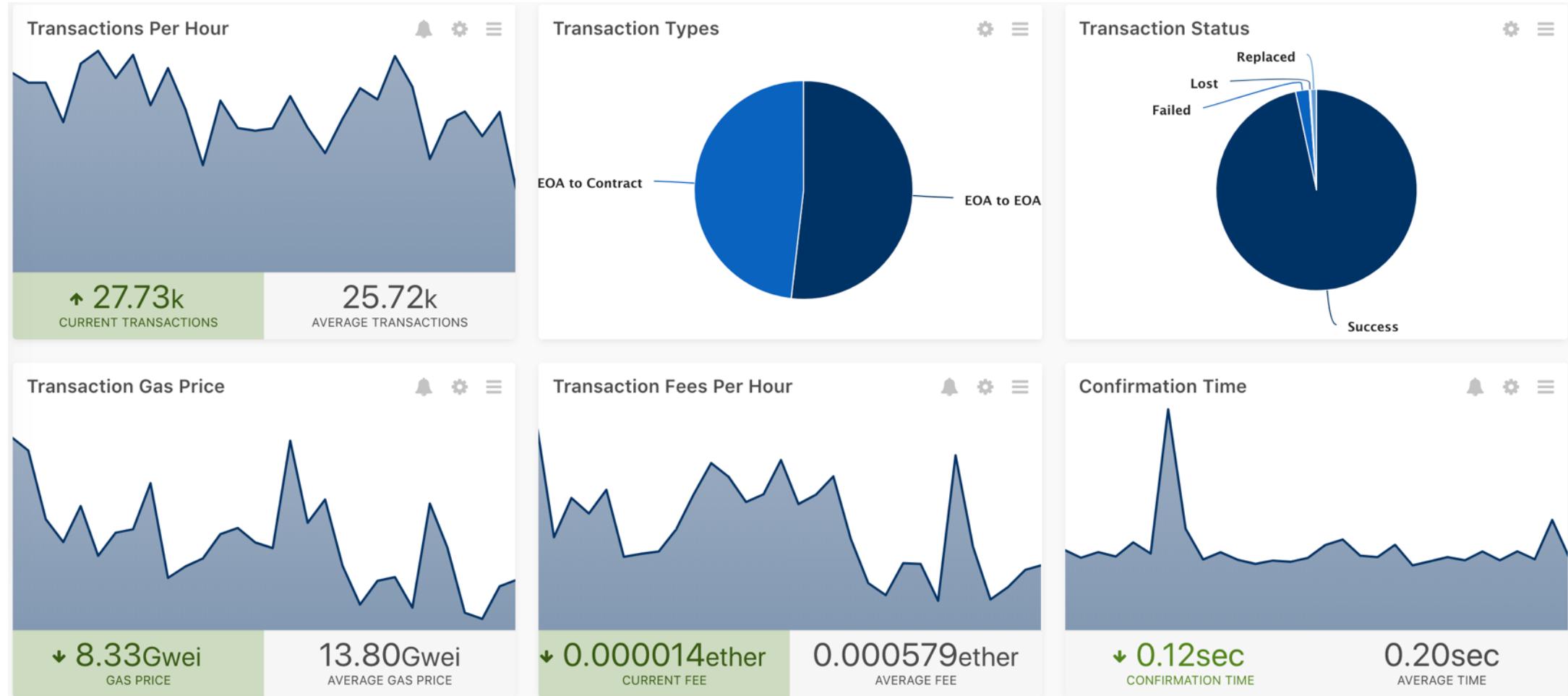
Click and drag in the plot area to zoom in



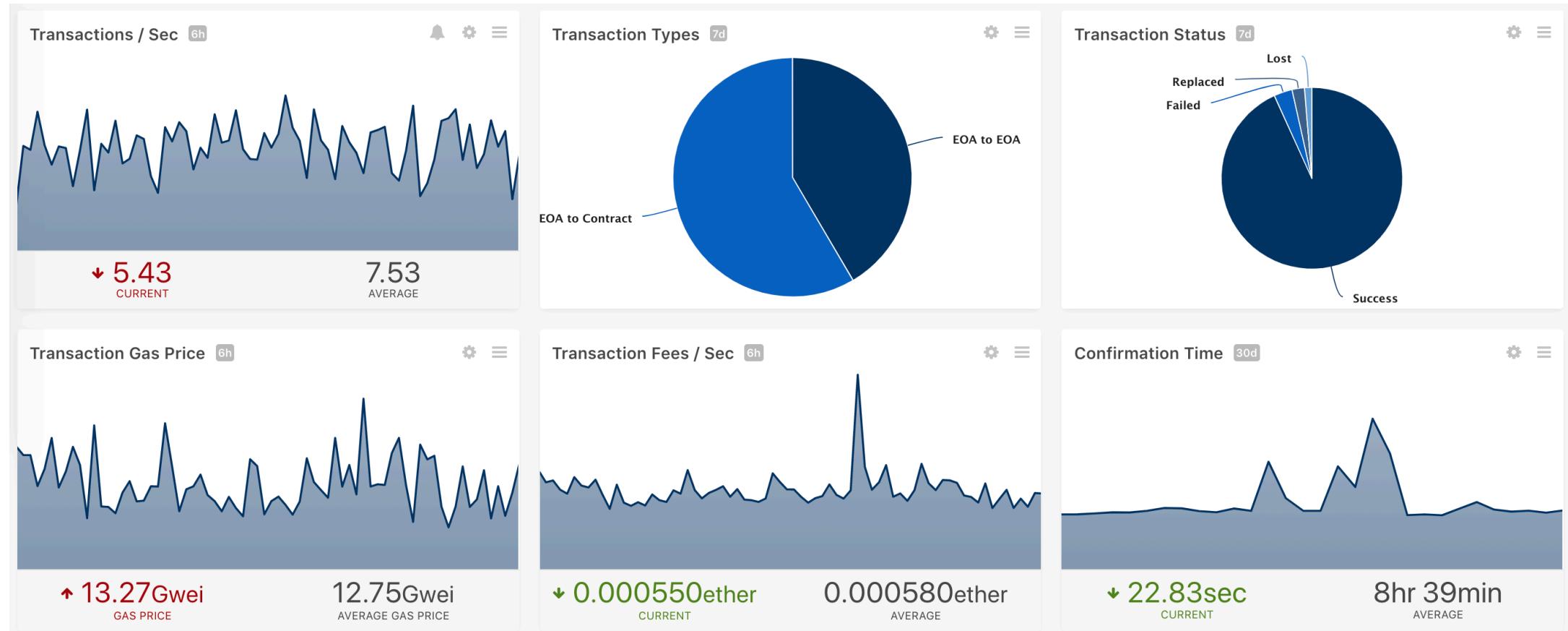
Real-time chart



Real-time chart (04/13)



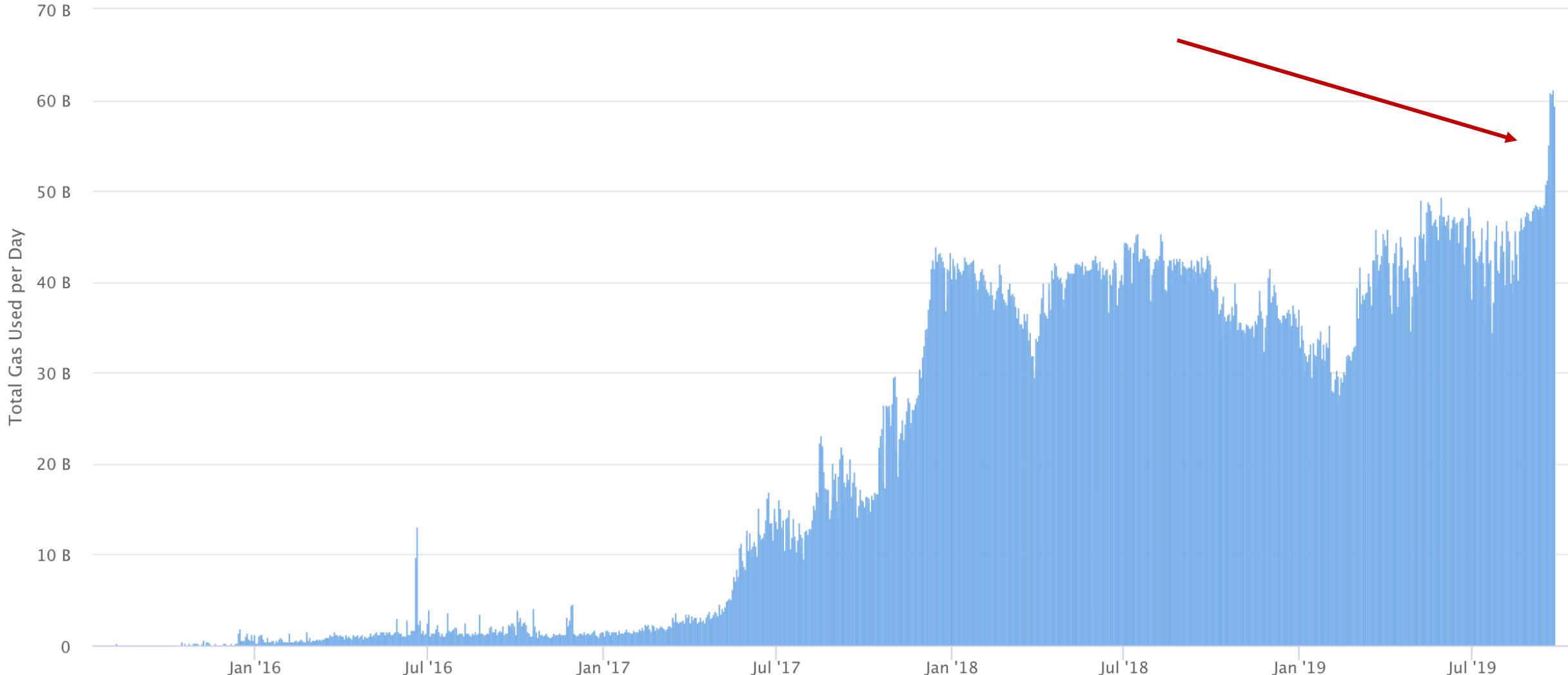
Real-time chart (10/16)



Ethereum Total Daily Gas Used Chart

Source: Etherscan.io

Click and drag in the plot area to zoom in



Market Cap (04/13)

Rank	Coin	Total Market Cap	Price	Circulating Supply	24h Change	1h Price Chart	
1	Bitcoin	\$128,855,294,369	\$7,591.63	\$8,128,550,000	16,973,337 BTC	9.46%	
2	Ethereum	\$45,827,548,286	\$463.96	\$2,223,630,000	98,775,209 ETH	10.17%	
3	Ripple	\$21,559,650,761	\$0.551475	\$1,003,880,000	39,094,520,623 XRP *	10.66%	
4	Bitcoin Cash	\$12,047,639,672	\$705.81	\$377,630,000	17,069,288 BCH	7.84%	
5	EOS	\$6,888,240,014	\$8.73	\$2,449,500,000	788,650,607 EOS *	22.26%	
6	Litecoin	\$6,792,943,416	\$121.20	\$488,687,000	56,049,238 LTC	5.20%	
7	Cardano	\$4,946,599,861	\$0.190789	\$417,519,000	25,927,070,538 ADA *	19.50%	
8	Stellar	\$4,105,206,958	\$0.221290	\$94,621,700	18,551,253,819 XLM *	8.48%	
9	NEO	\$3,941,782,000	\$60.64	\$299,360,000	65,000,000 NEO *	9.57%	

Market Cap (10/16)



1	Bitcoin	\$114,120,630,871	\$6,586.94	\$4,262,774,091	17,325,300 BTC	-0.95%		...
2	Ethereum	\$21,541,732,106	\$209.94	\$1,671,918,175	102,607,647 ETH	0.13%		...
3	XRP	\$18,158,558,751	\$0.453991	\$579,573,353	39,997,634,397 XRP *	2.44%		...
4	Bitcoin Cash	\$7,945,305,505	\$456.48	\$317,342,590	17,405,463 BCH	-0.70%		...
5	EOS	\$4,909,679,793	\$5.42	\$447,487,941	906,245,118 EOS *	-0.68%		...
6	Stellar	\$4,253,582,997	\$0.225163	\$42,737,692	18,891,162,191 XLM *	0.26%		...
7	Litecoin	\$3,225,043,903	\$54.89	\$289,043,006	58,750,702 LTC	-0.31%		...
8	Tether	\$2,210,951,893	\$0.979849	\$2,880,043,971	2,256,421,736 USDT *	1.54%		...
9	Cardano	\$1,957,754,417	\$0.075510	\$27,064,310	25,927,070,538 ADA *	1.11%		...

Not money

交易媒介 (x)
價值儲存 (x)
記帳單位 (x)

Community



Taipei Ethereum



A S S E T H



Enterprise Ethereum Alliance



- 與 Ethereum Foundation 沒有任何關係



Background

- Public chain, any one can become the miner (PoW)
 - Ethereum Foundation
 - Parity Technologies
 - ConsenSys
- Consortium chain, only the permissioned member can propose block
 - Enterprise Ethereum Alliance
 - <https://media.consensys.net/what-the-eea-and-hyperledger-collaboration-means-for-enterprise-blockchain-development-31580012cb2>

Why Ethereum?



Ultimate Scripting: A Platform for Generalized Financial Contracts on Mastercoin

0.1. Introduction

Perhaps the key advantage of Mastercoin over the raw Bitcoin protocol is the potential to include much more advanced transaction types, including transactions that specify behavior based on future information well off into the future. For example, Mastercoin joins Ripple in being one of the only two major cryptocurrency networks that include the ability for users to make binding exchange offers as a type of transaction. From there, the Mastercoin Foundation intends to integrate even more complex contracts, including bets, contracts for difference and on-blockchain dice rolls. However, up until this point Mastercoin has been taking a relatively unstructured process in developing these idea, essentially treating each one as a separate "feature" with its own transaction code and rules. This document outlines an alternative way of specifying Mastercoin contracts which follows an open-ended philosophy, specifying only the basic data and arithmetic building blocks and allowing anyone to craft arbitrarily complex Mastercoin contracts to suit their own needs, including needs which we may not even anticipate.

0.2. Specification

The underlying idea behind this specification is to allow anyone to create a contract which pays out according to an arbitrary formula. The formula will be defined in a Bitcoin-like stack-based scripting language, consisting of numbers and opcodes.

The evaluation algorithm is as follows:

```
dataStack = []
opStack = script
while len(opStack) > 0:
    var op = opStack.pop()
    if typeof(op) == 'opcode': eval(dataStack,op)
    else: dataStack.push(op)
return dataStack.pop()
```

Where `eval` is defined for each opcode below. Any error (eg. division by zero) will make the script return `FAIL`, and result in the entire transaction being treated as invalid by the Mastercoin network. All variables will be signed 64-bit integers, and all arithmetic operations wrap around (that is, if the underlying arithmetic operation returns `R`, the value pushed is $((R + 2^{63}) \% 2^{64}) - 2^{63}$.

For simplicity, we define `ds[-1]` to be the topmost value on the `dataStack`, `ds[-2]` the second topmost, etc. The opcodes are in two categories: arithmetic operations and data operations. Arithmetic operations are:

- **SWAP**: Swaps `ds[-1]` and `ds[-2]` in place
- **DUP**: Pushes a copy of `ds[-1]` onto the stack, thereby duplicating it
- **DROP**: Pops `ds[-1]` and does nothing
- **ADD**: Pops `ds[-1]` and `ds[-2]` and pushes `ds[-1] + ds[-2]`

區塊鏈

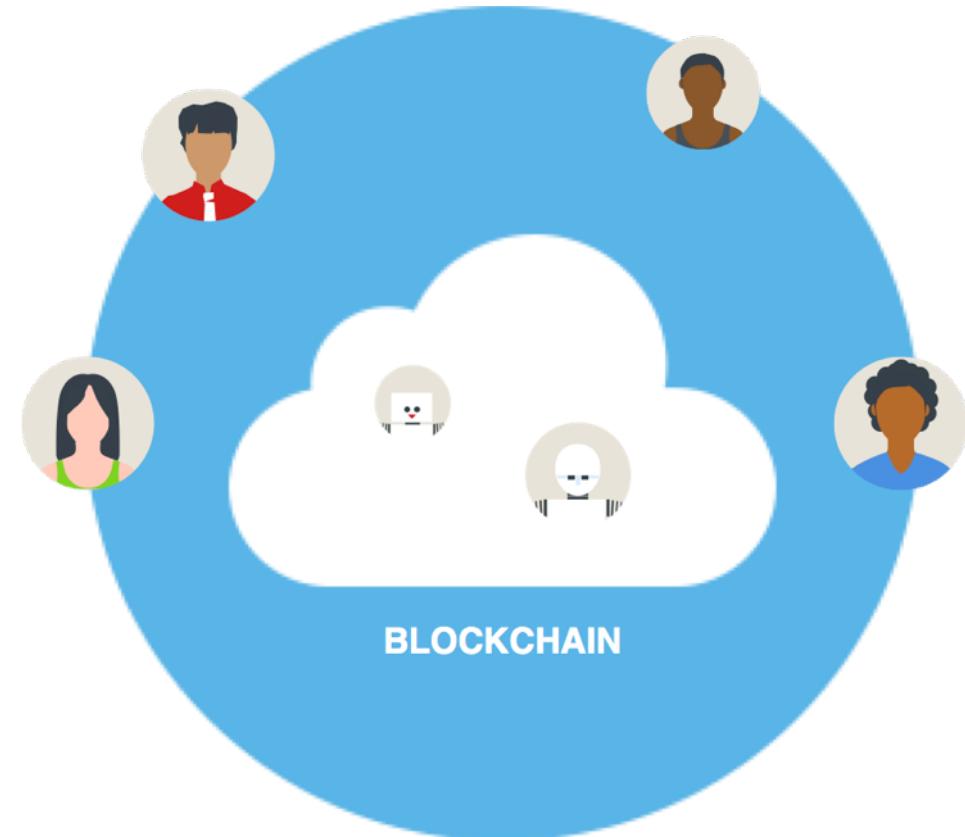
- 起於中本聰的白皮書 (2008)
- 比特幣系統上線，被設計作為電子貨幣 (2009)
- 白皮書中沒有區塊鏈一詞
- 區塊鏈 (Blockchain) 技術被提出 (201X)
- 以太坊 (Ethereum) 被提出 (2013)
- 以太坊 ICO (Initial Coin Offering) (2014)
- 以太坊上線，智能合約的概念 (2015)
- ICO 盛行 (2017)



以太幣

Why Ethereum?

- 受比特幣啟發 (電子貨幣)
- 提供一個分散式應用平台 (區塊鏈為底)
- 智能合約 (DApp)
 - Token is one of the DApp



什麼是智能合約

- 由程式碼直接控制數字資產或業務流程
 - 程式碼對合約具有相同理解
 - 不因合約多次更迭而有所混淆
 - 對外部資料看法一致 (油價或股價等)
- 智能不是指人工智能
- 智能合約(目前)不是法律合約
- 程式碼僅執行複雜的規則和條件，不具有學習能力
 - 電梯
 - 販賣機

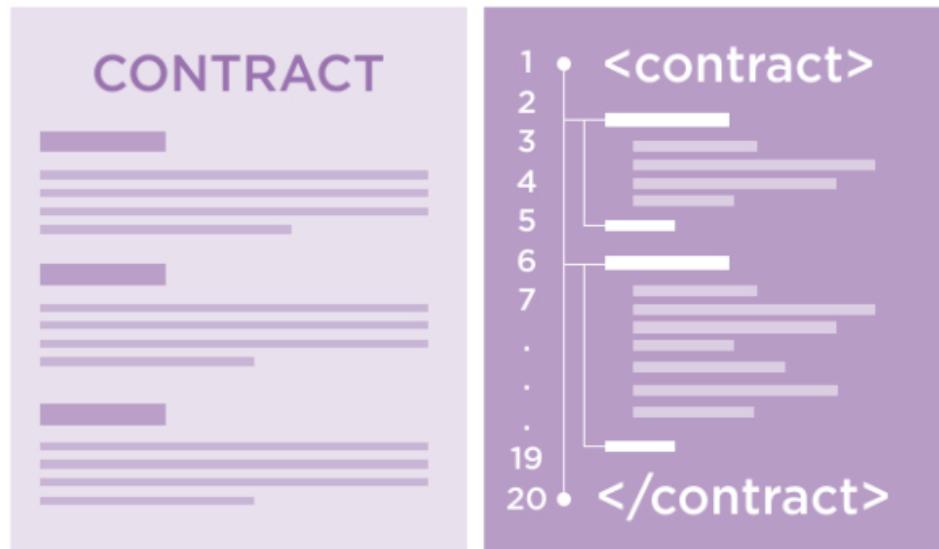
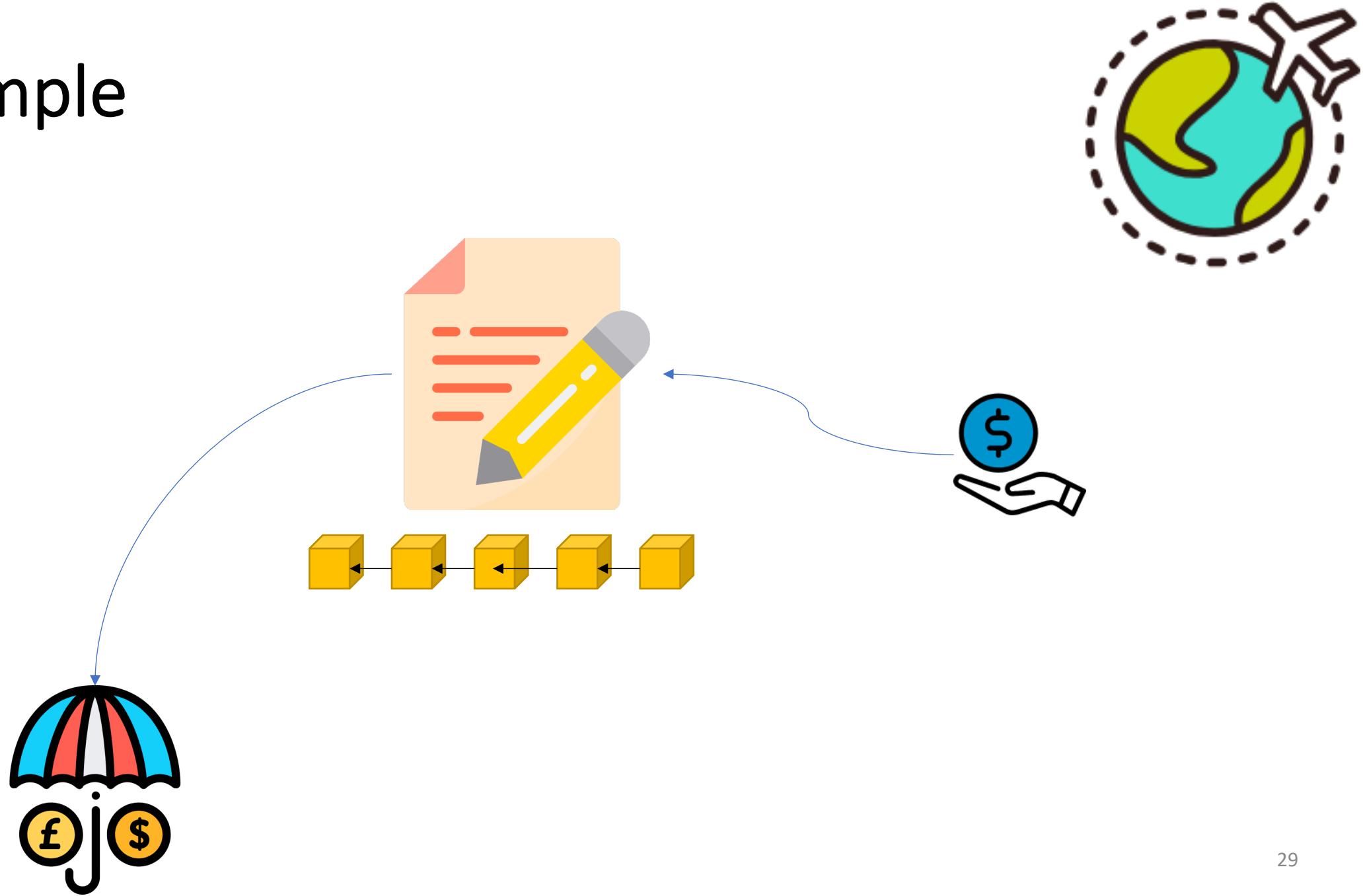


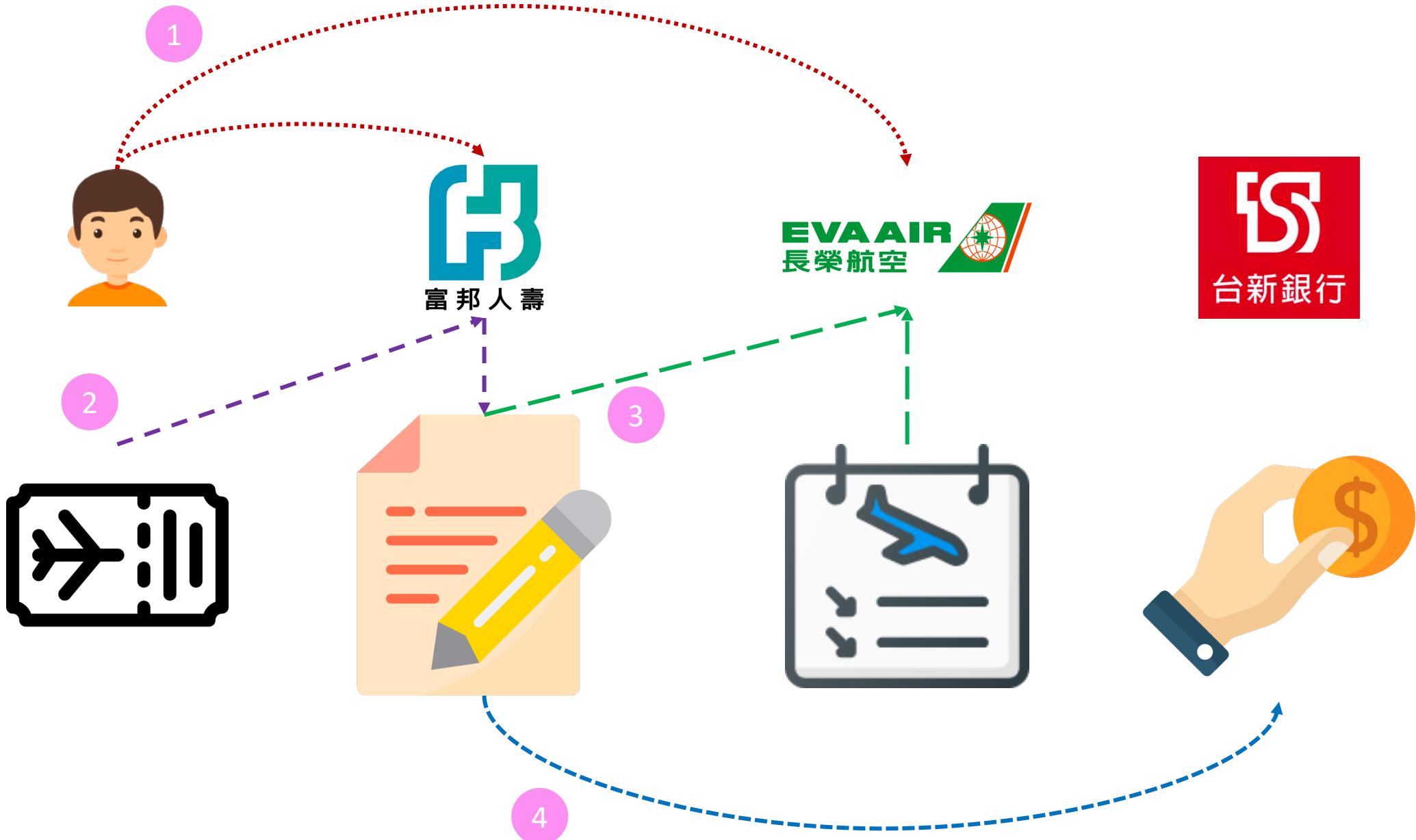
Image: <https://bitsonblocks.net>

Example



Example



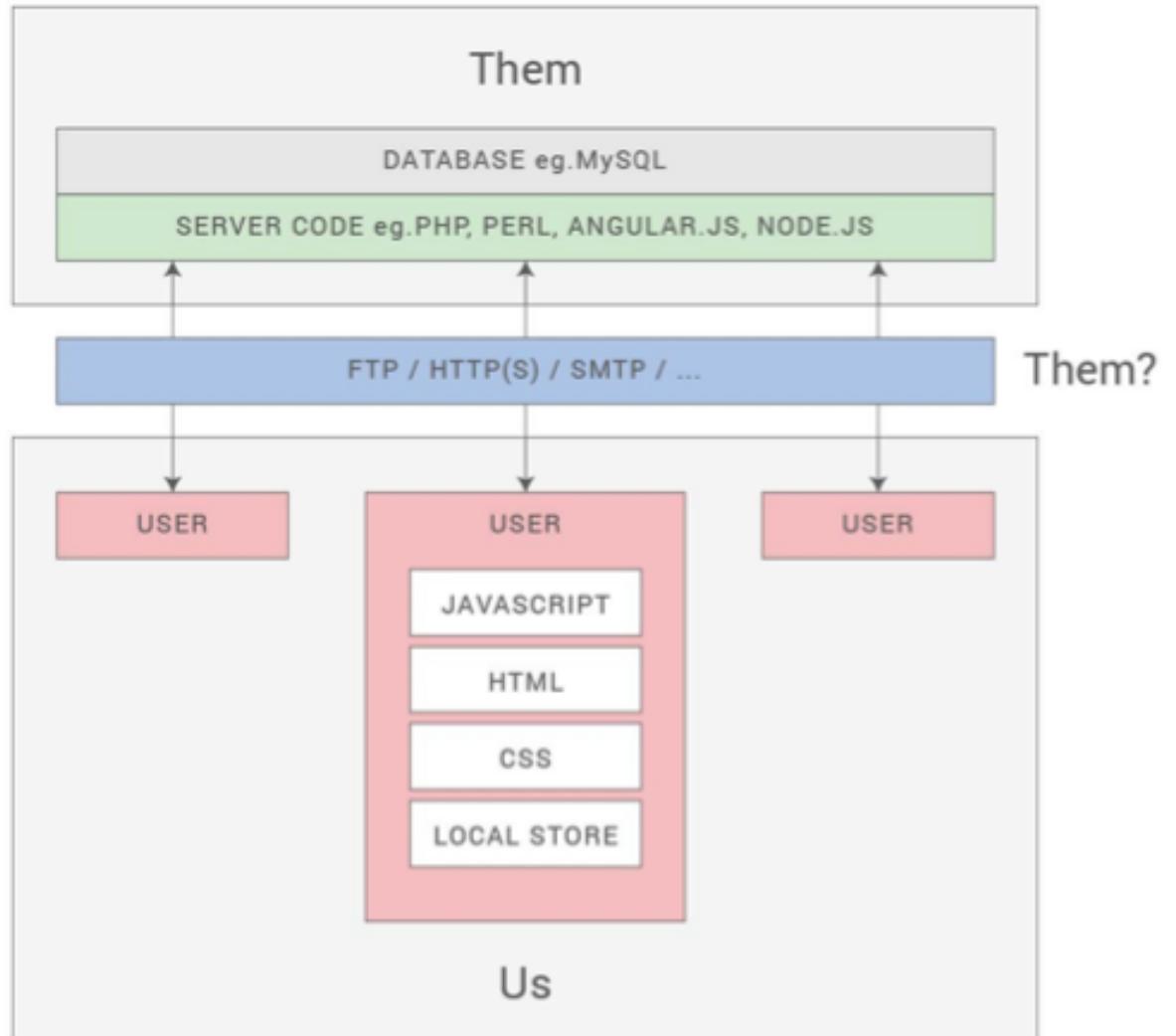


Web 2.0

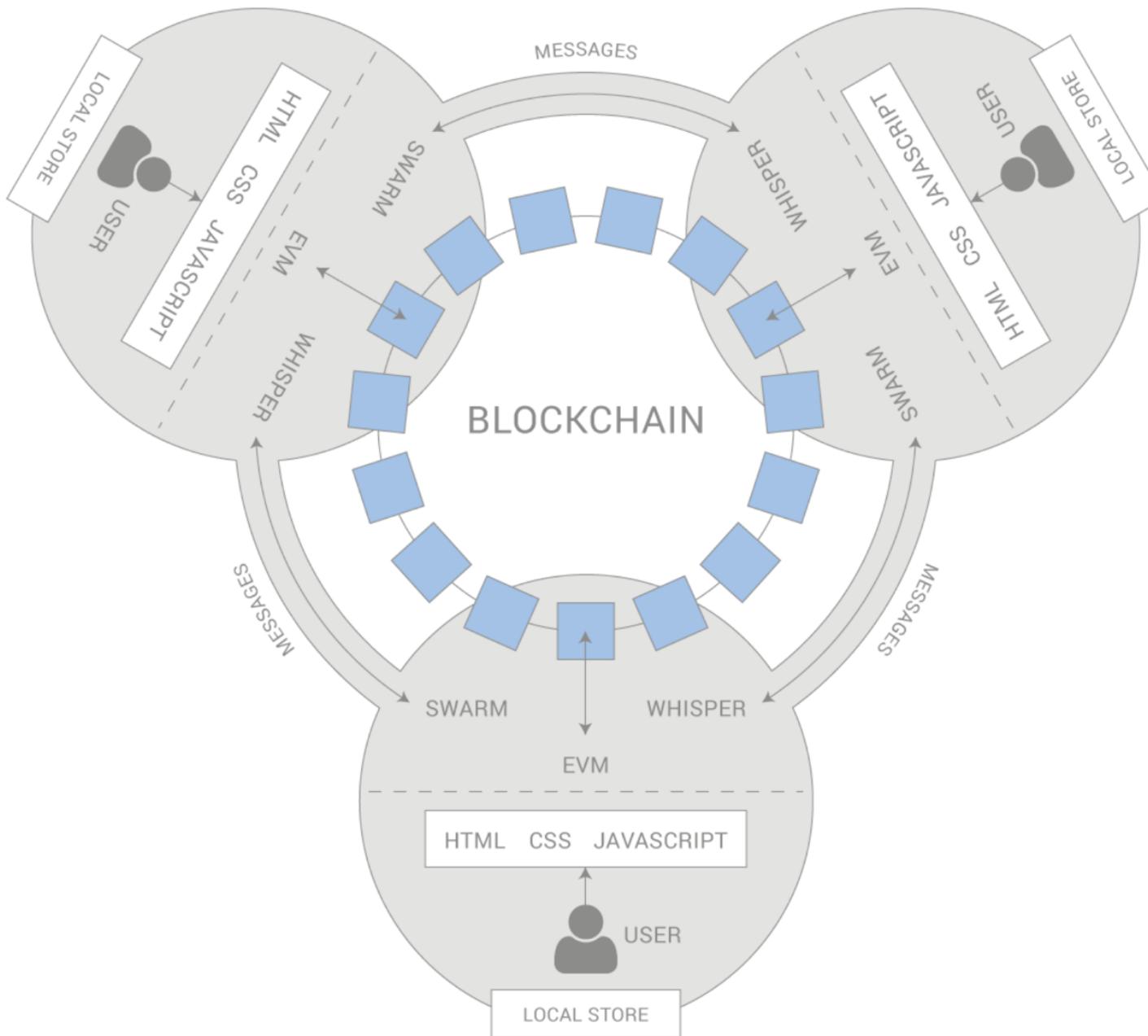


Web 2.0, How it is

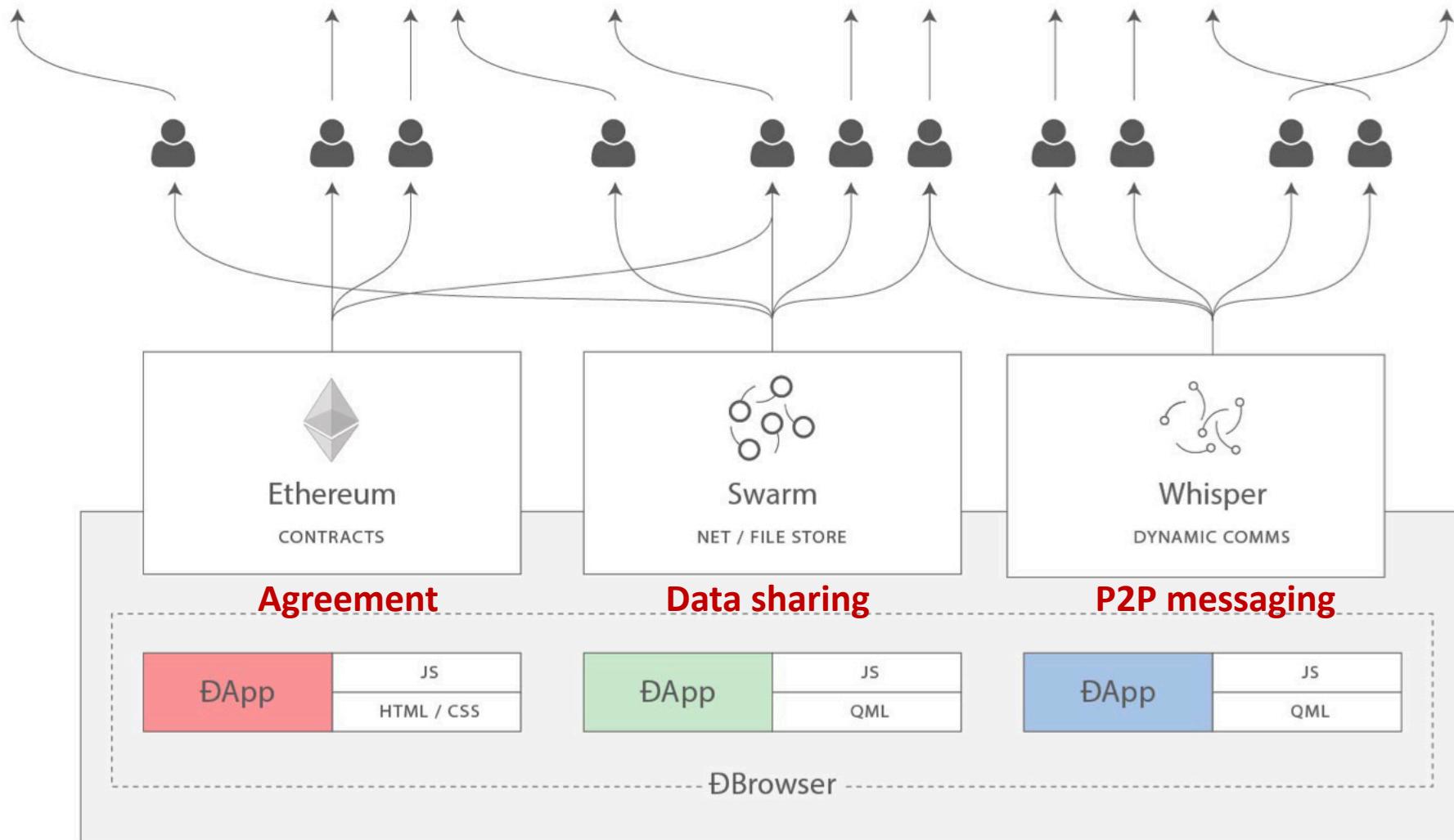
The Ethereum Experience with Dr. Gavin Wood, CTO



DApp



Web 3.0



比特幣有何限制？

- Bitcoin
 - UTXO
 - OP_RETURN
 - Pricing and Fairness
 - Bitcoin script





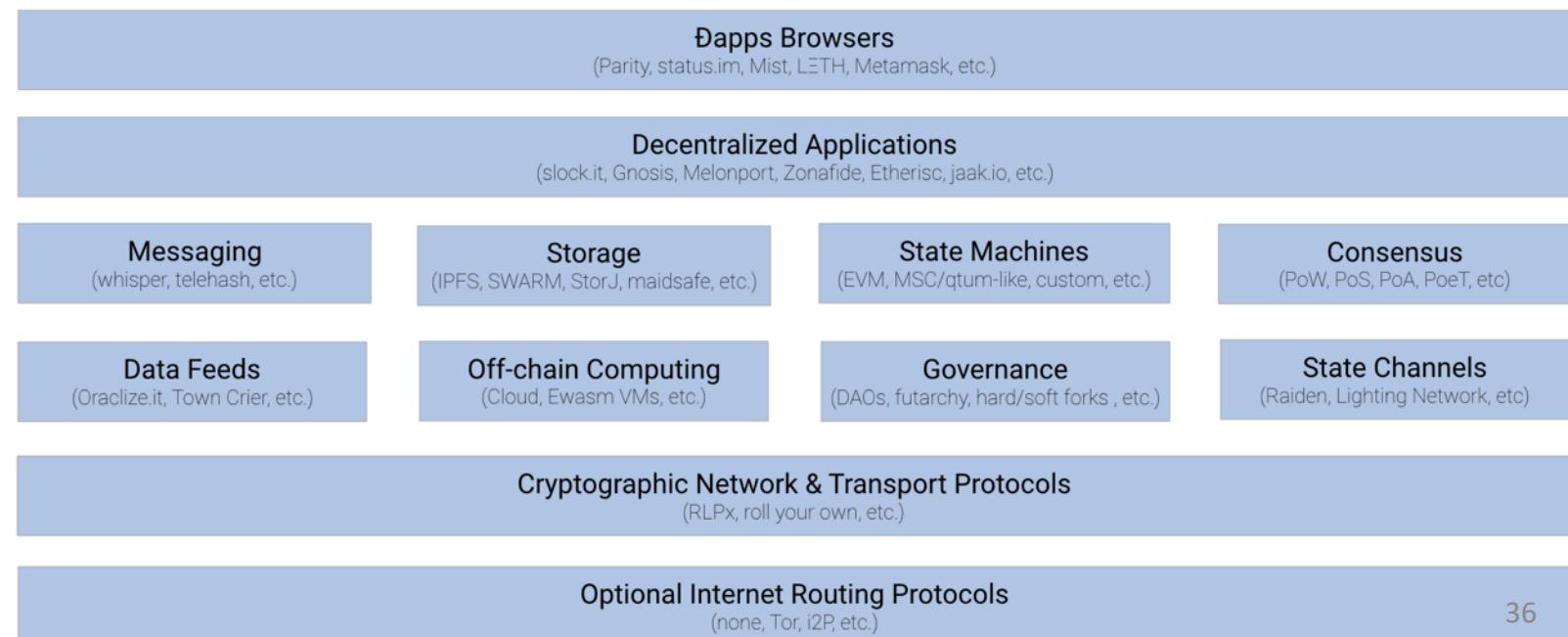
協議設計原則

- 三明治模型

- 應用層的介面設計對使用者要儘可能簡單 (Language, Interface)
- 複雜的系統設計放在中間層
- 核心共識

The Web 3.0 Abstracted Stack

Diagram v.1.0 by @stephantual - 26 May 2017



協議設計原則

- **自由度**

- 不限制使用者如何使用以太坊協議
- 保持網路中立，對交易或合約一視同仁
- 透過設置手續費來課徵污染稅 (Pigouvian tax)

- <https://medium.com/cryptocow/ethereum-transaction-fee-economics-8214242d5024>
- <https://github.com/ethereum/research/blob/master/papers/pricing/ethpricing.pdf>
- <https://www.youtube.com/watch?v=7vuTtvshR34>



<https://medium.com/cryptocow/cryptocow-submit-rules-a62b9ccc1efc>

協議設計原則

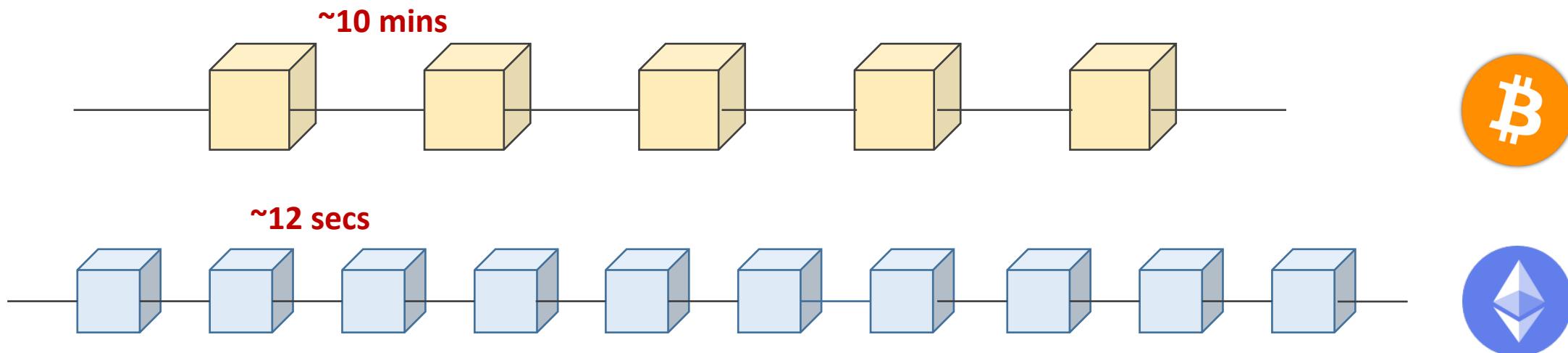
- 一般化
 - 協議的特性與操作碼要能最大限度地體現底層的概念
 - 以便功能能隨意被組合

協議設計原則

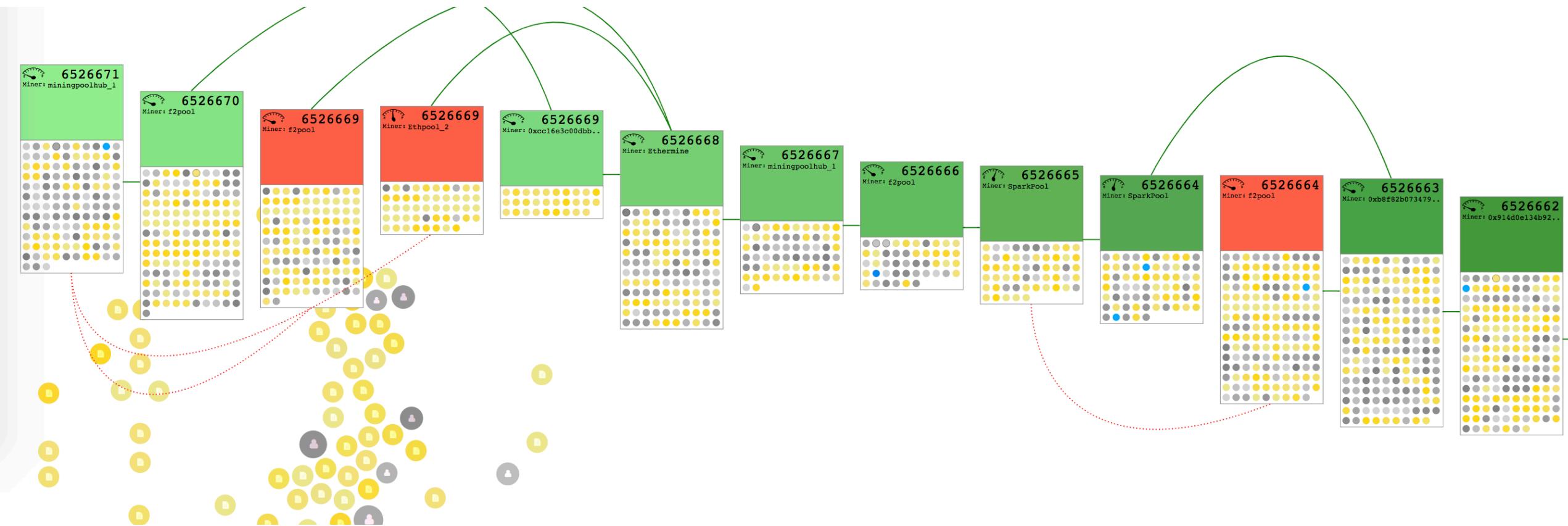
- 不具任何特色
 - 為了遵循一般化原則，拒絕在協議中提供某種高階功能
 - 反之，使用者可以在合約中建立任何 sub-protocol
 - 例如：沒有 TimeLock, Multisig 功能

協議設計原則

- 不排斥承擔風險
 - 如果風險增加提供更多好處，願意承擔更多風險
 - 例如
 - 一般的狀態轉換
 - 50 倍快的區塊生成時間
 - 高效的共識



Fork

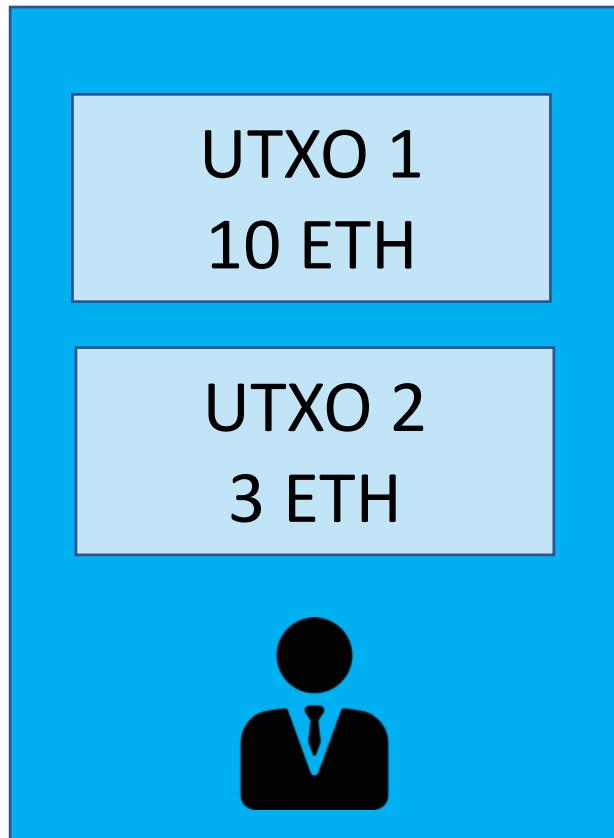


Blockchain-level protocol

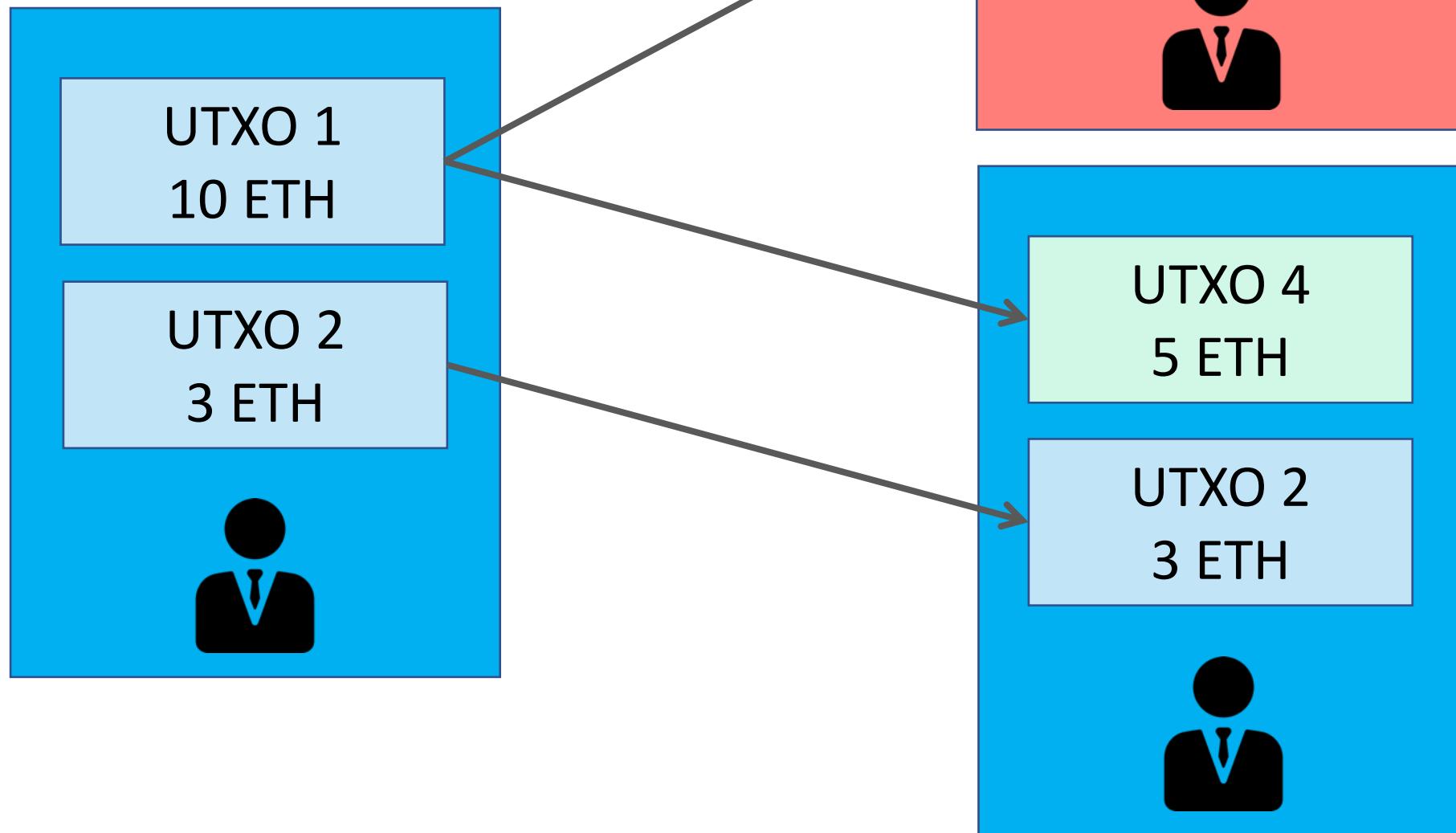
新的設計

- Account
- Merkle Patricia tree/trie (MPT)
- Recursive Length Prefix (RLP)
- Ether/gas/fee
- EVM

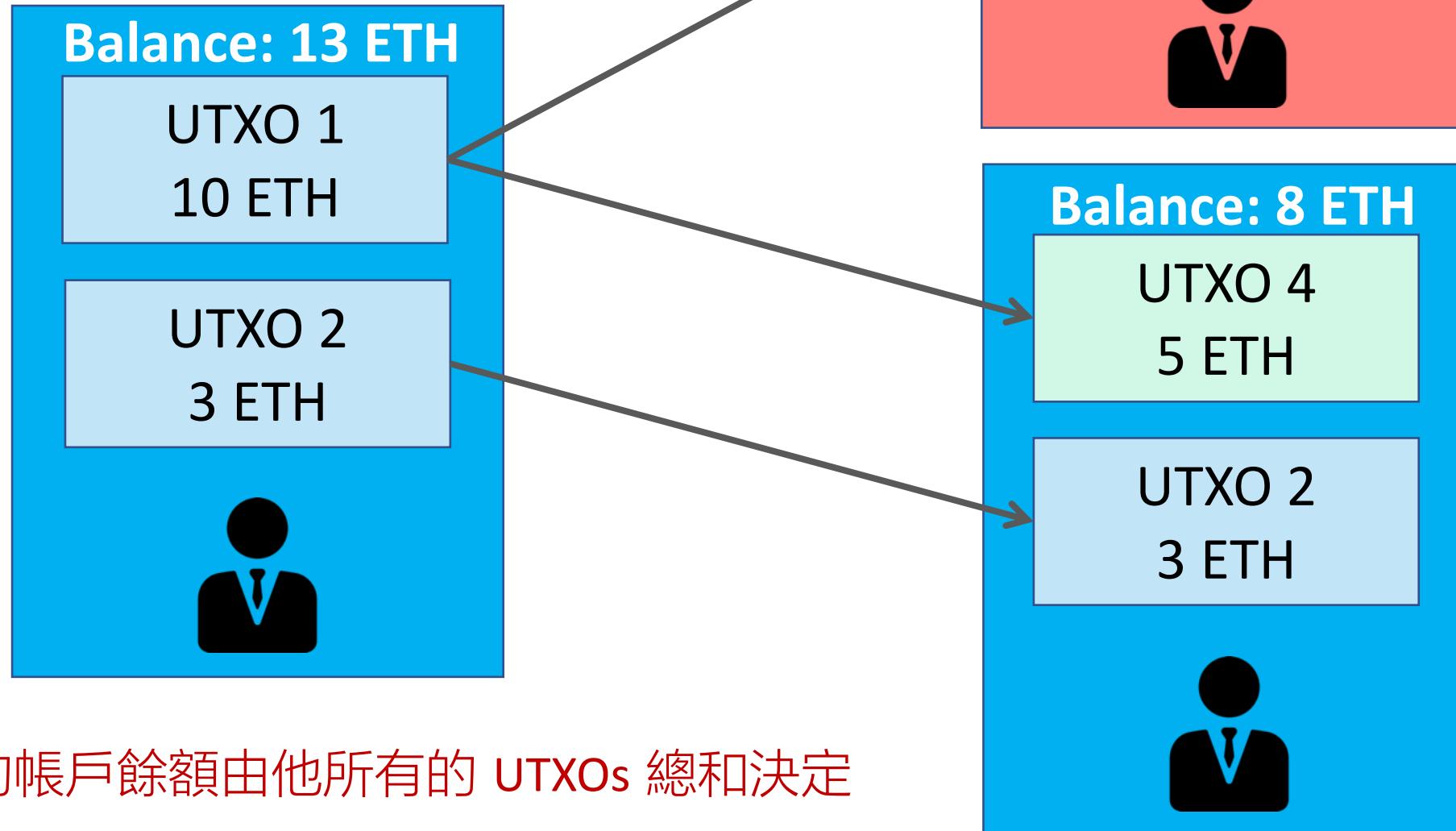
UTXOs



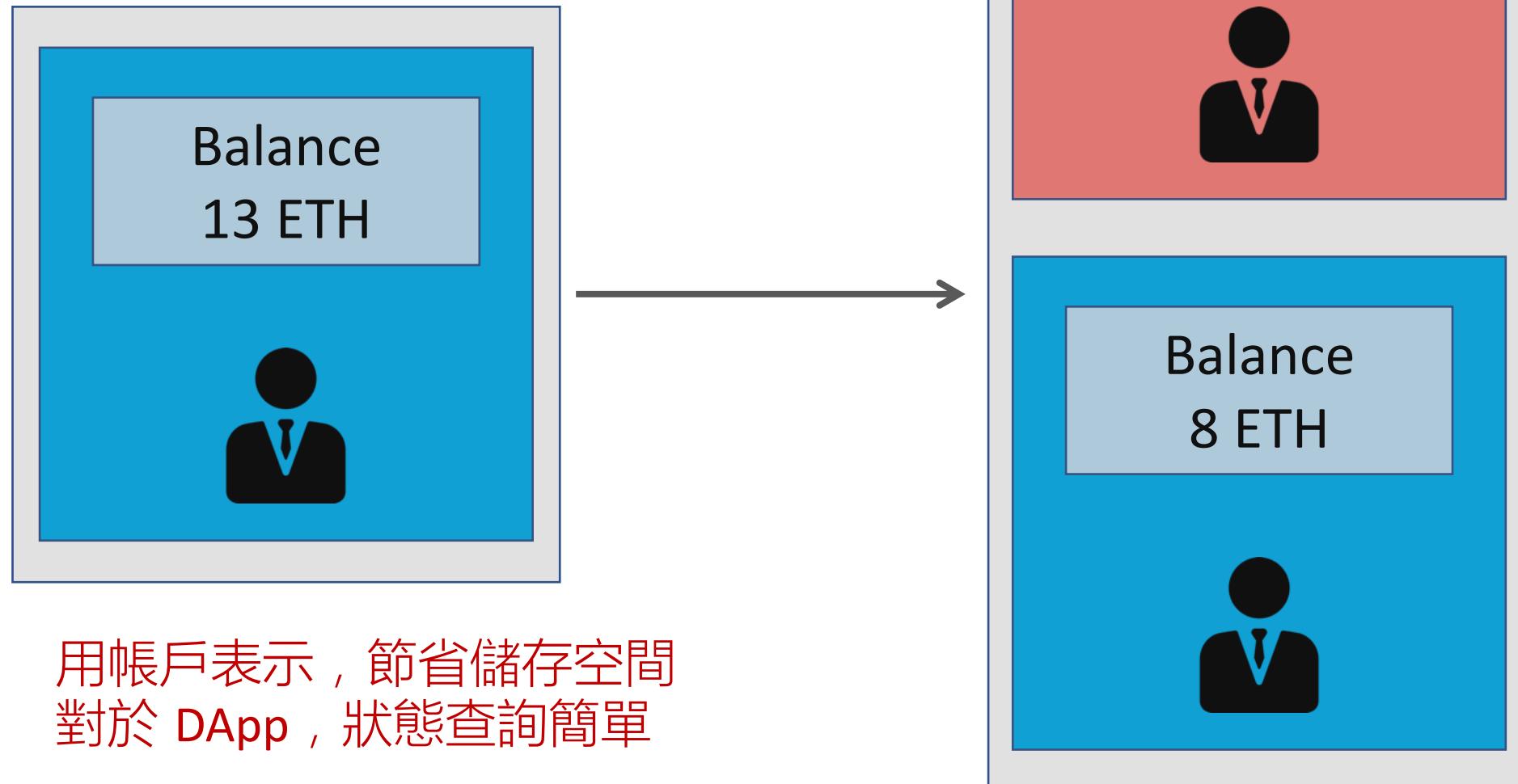
UTXOs



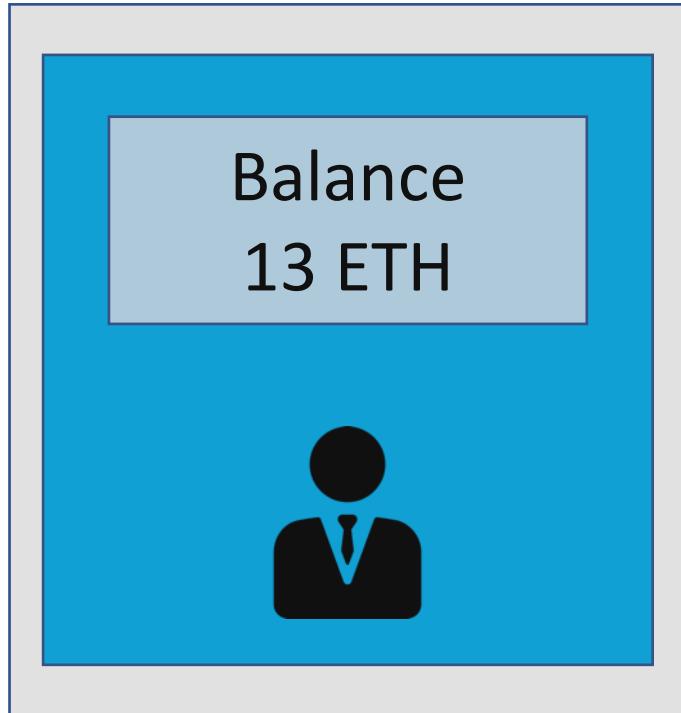
UTXOs



Accounts



Accounts



用帳戶表示，節省儲存空間
對於 DApp，狀態查詢簡單
隱私性相對較差
擴展性差

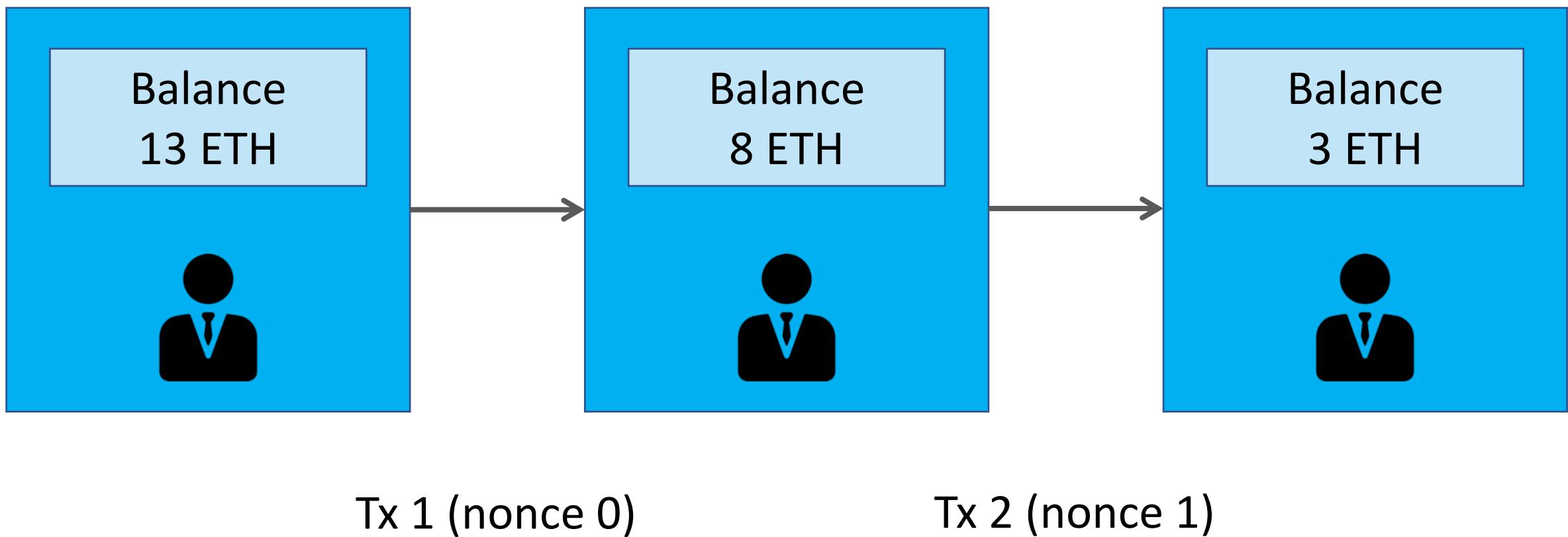
Accounts



有 replay attack 的風險
回想一下，之前提過交易的流水號

Accounts

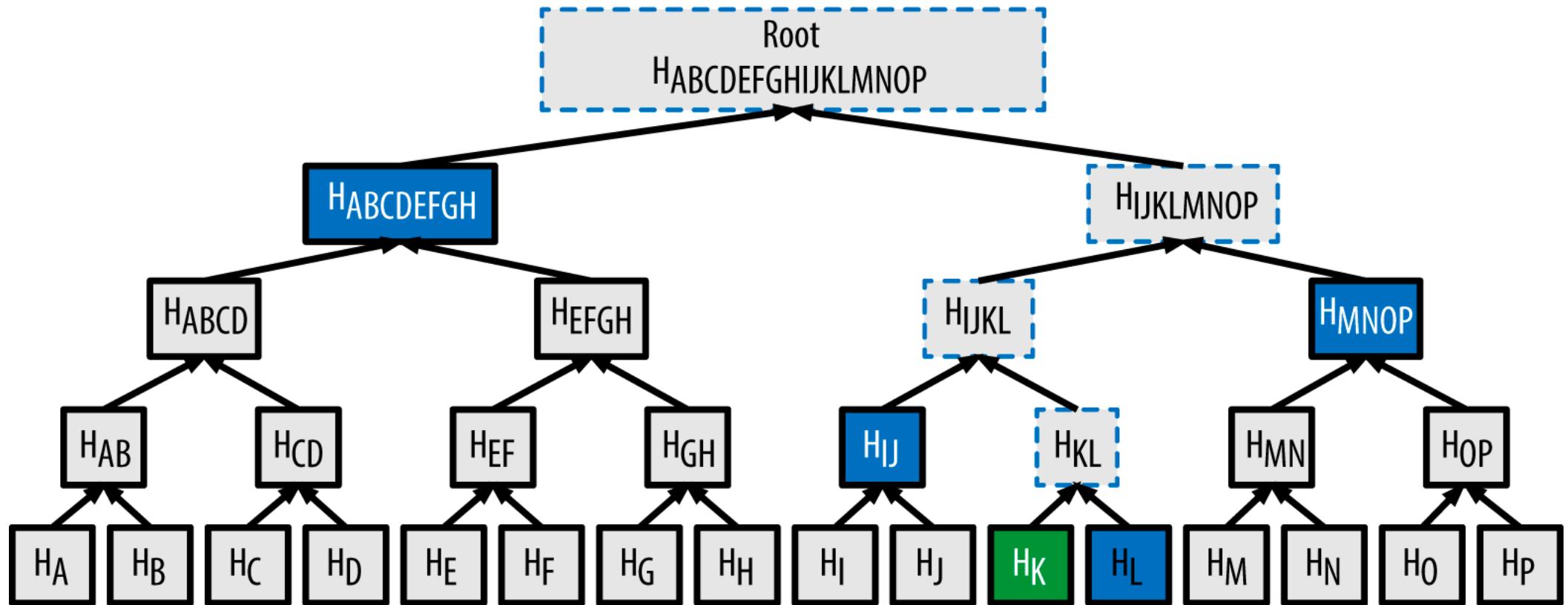
透過 nonce 來防止 replay attack
不可跳號，nonce 依序執行



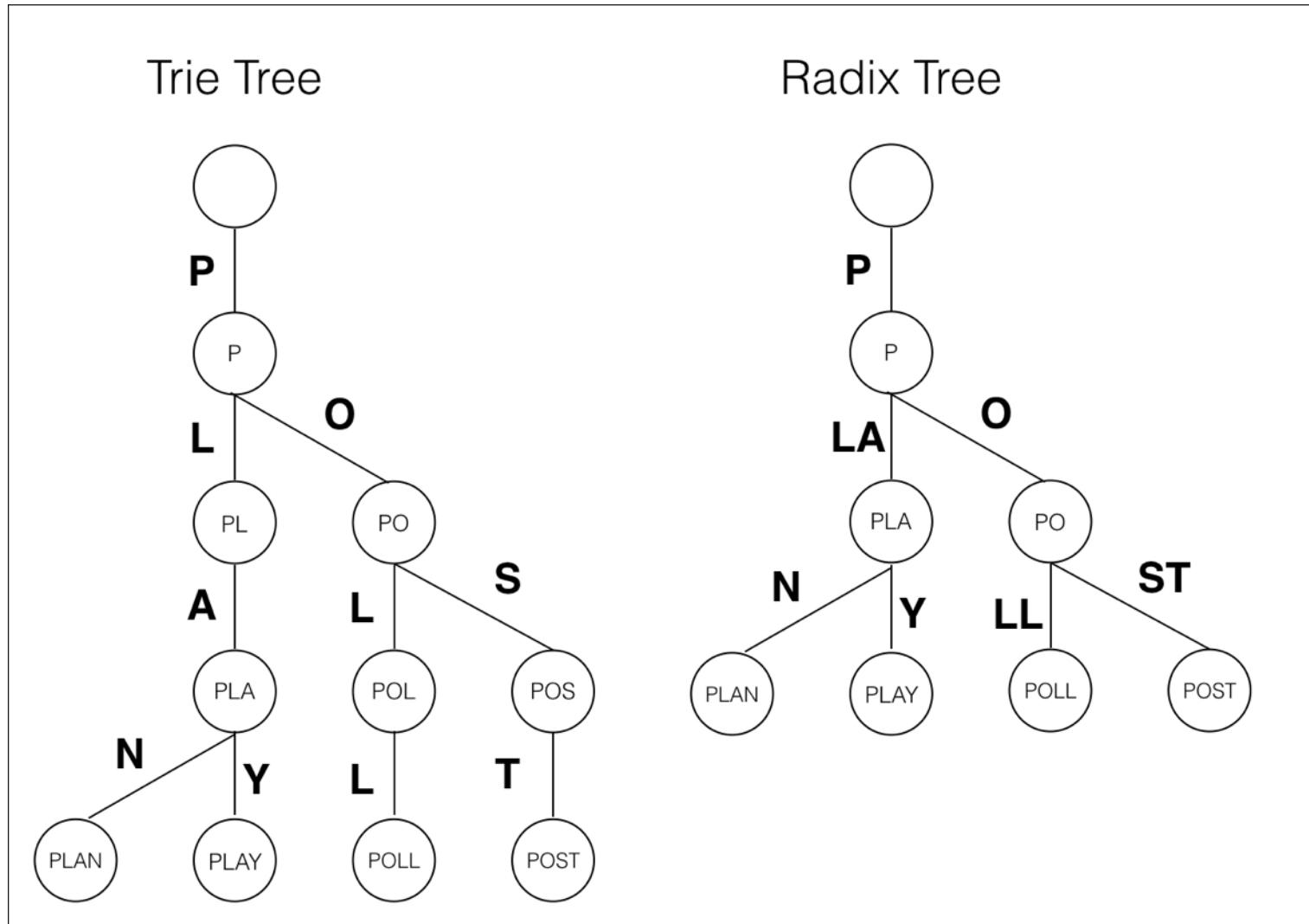
Merkle Patricia tree/trie

- 結合兩種樹狀結構，對 key/value 搜尋優化
 - Radix tree
 - Merkle tree

Merkle tree



Radix tree



How does Ethereum work, anyway?

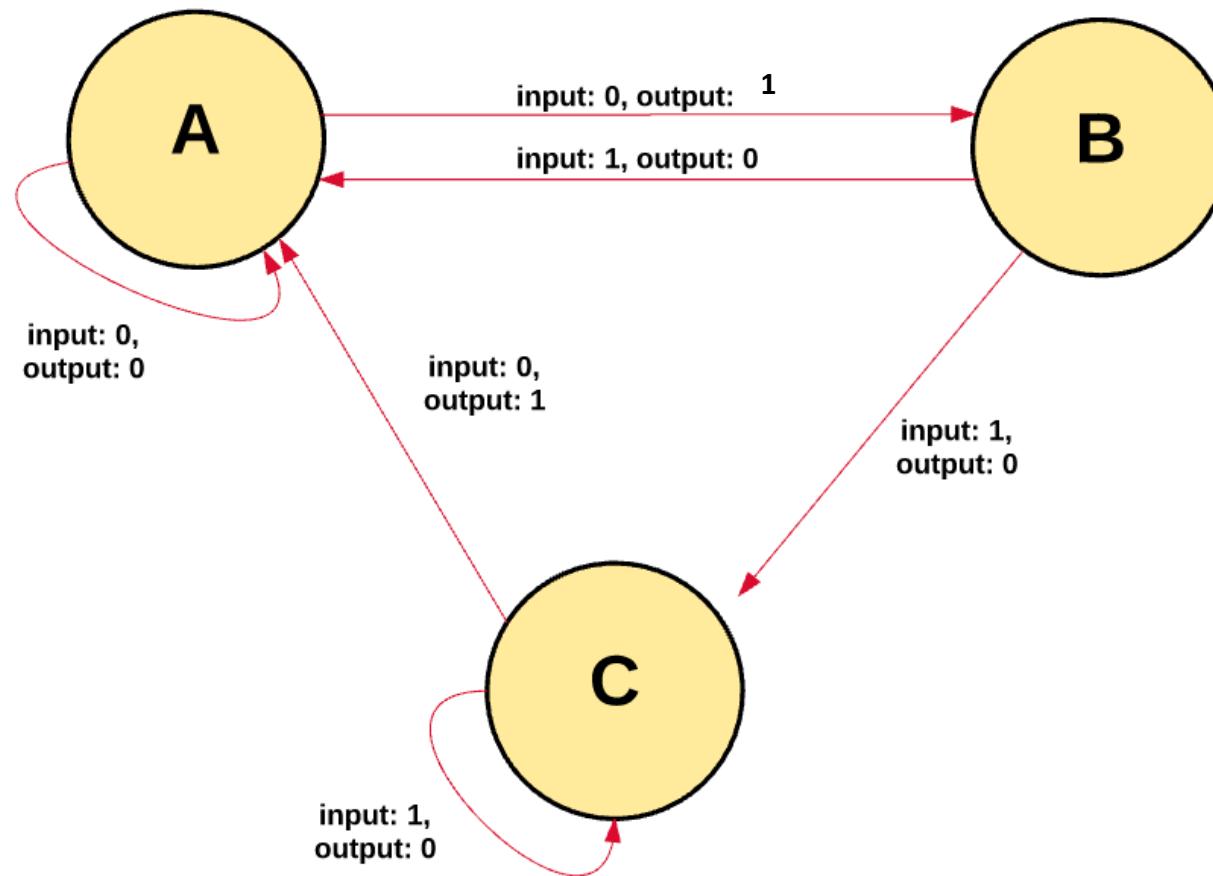
Author: Preethi Kasireddy

<https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369>

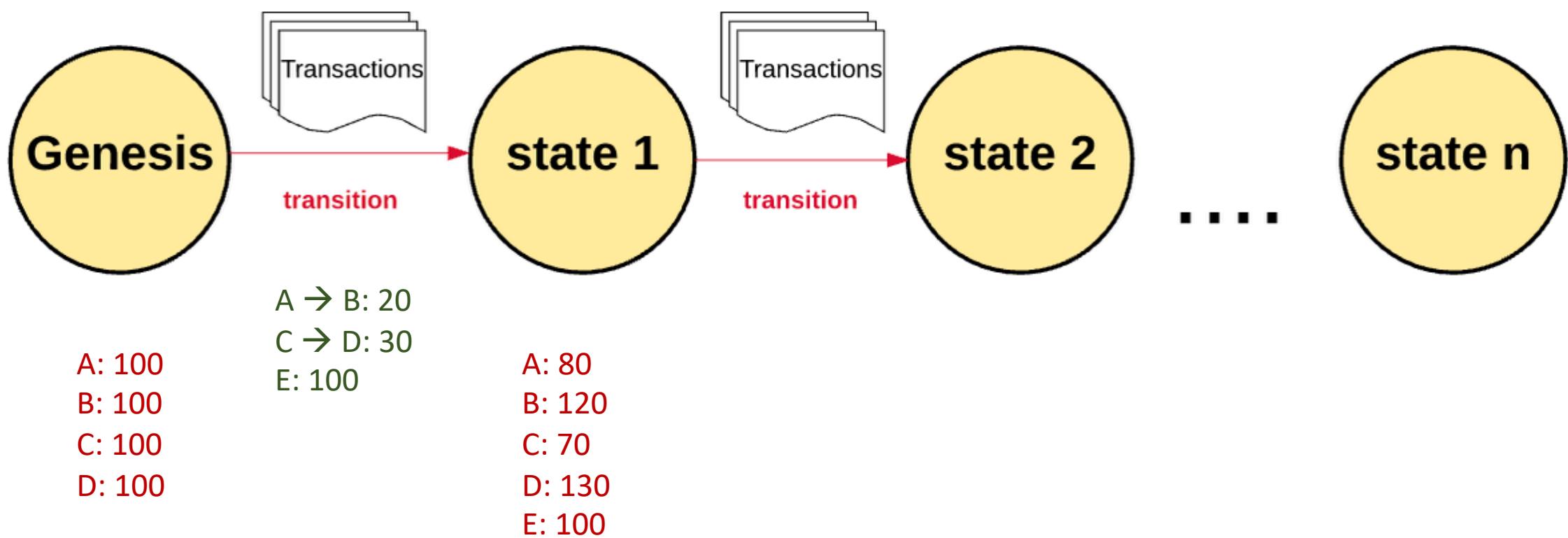
Blockchain

- A blockchain is a “cryptographically secure transactional singleton machine with shared-state.”
 - cryptographically secure
 - transactional singleton machine
 - with shared-state.

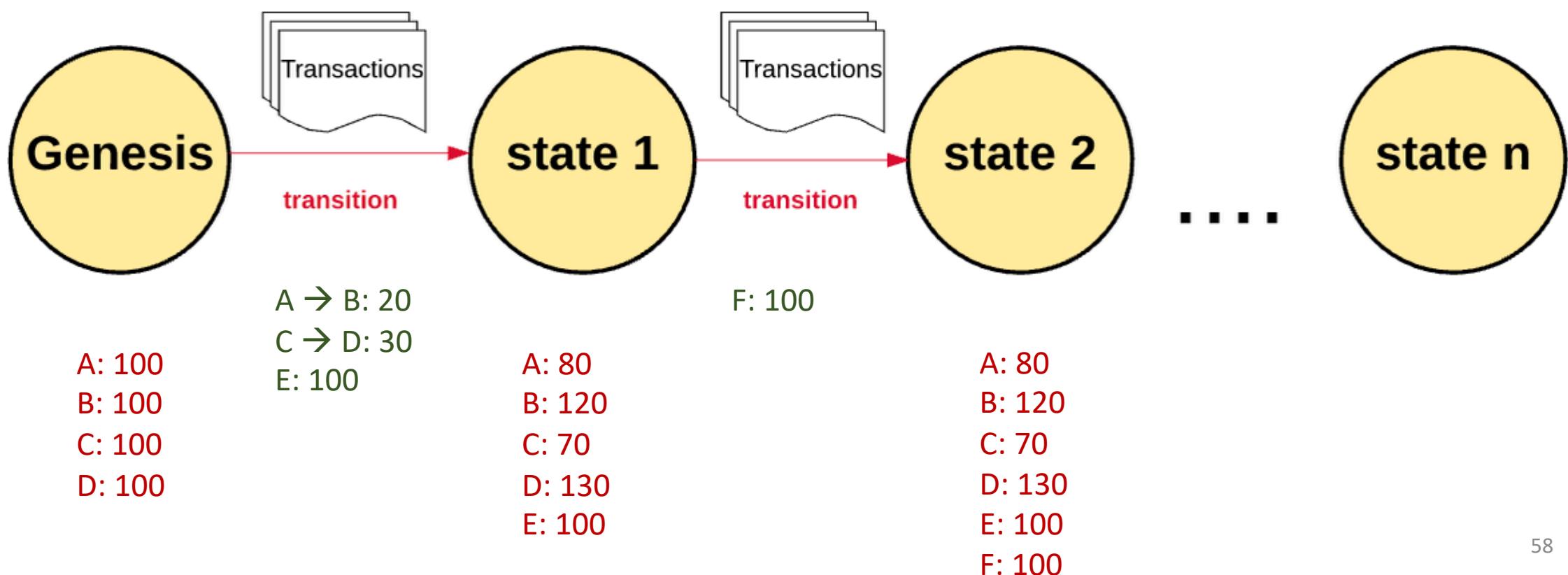
Transaction-based state machine



From genesis state to current state

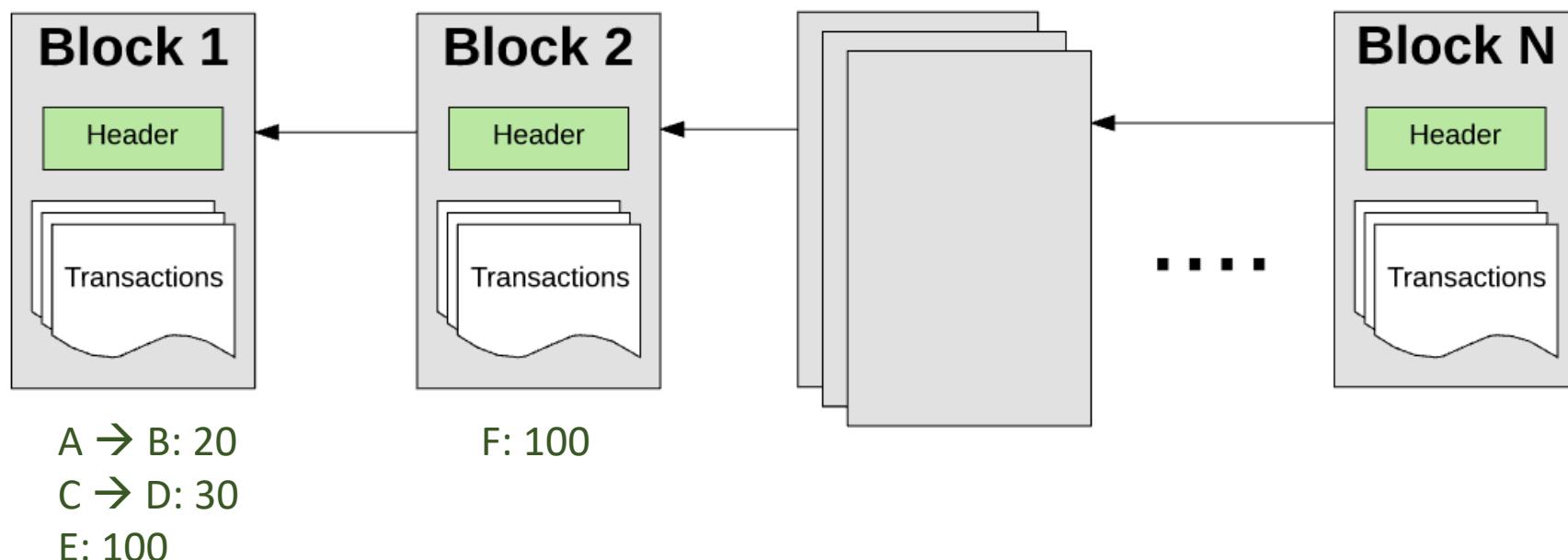


Global state



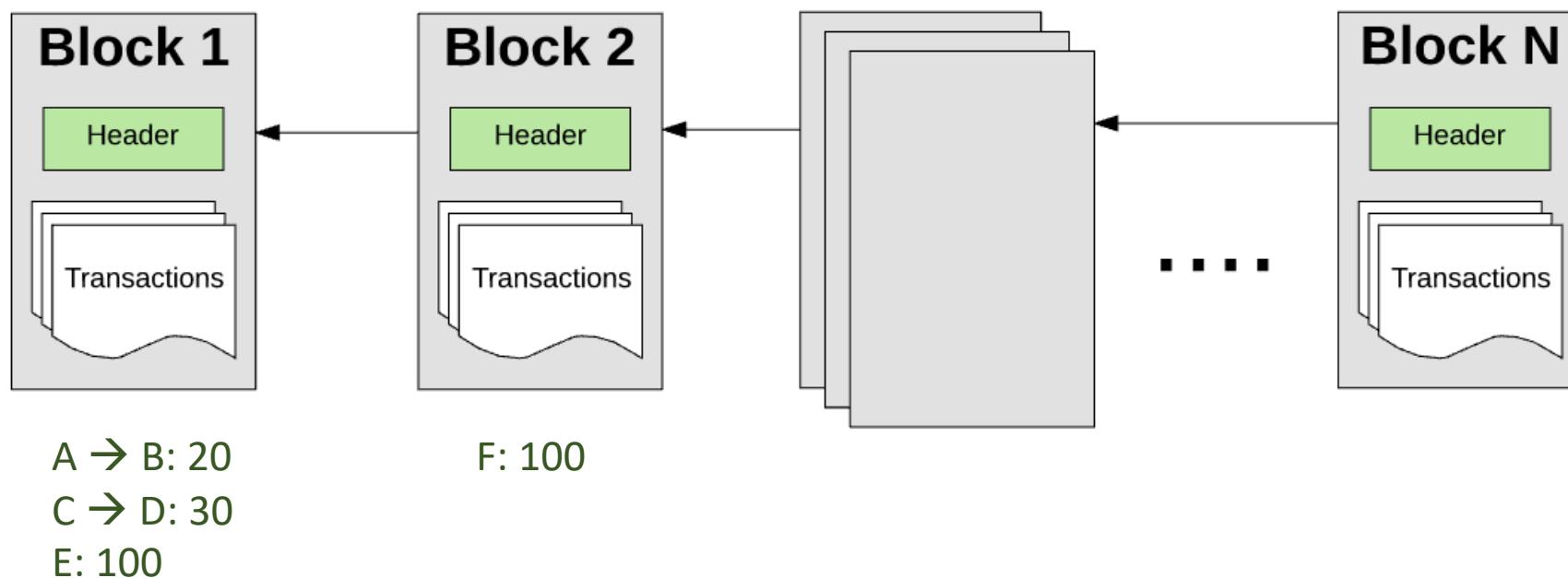
Storage

A: 100	A: 80	A: 80
B: 100	B: 120	C: 70
C: 100	C: 70	D: 130
D: 100	D: 130	E: 100
	E: 100	F: 100



Mining

- 驗證交易合法, 透過 Proof of Work
- 從上一個狀態轉換成下一個狀態

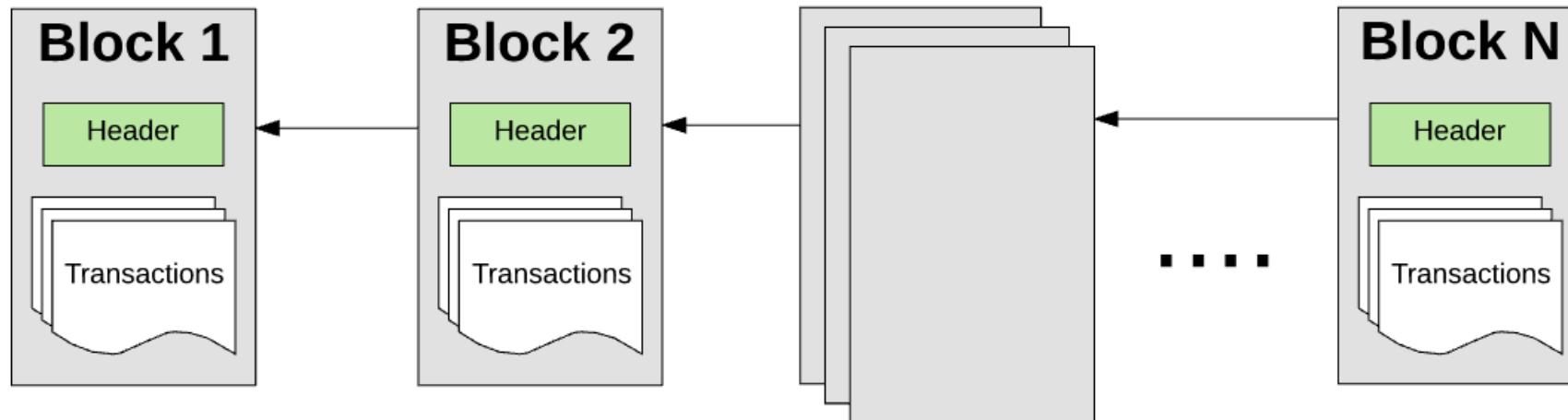


Block reward

- 驗證交易並形成新區塊的礦工，會得到獎勵
- 獲得以太幣 (Ether) 做為獎賞

Block size (Gas)

~8,000,029 gas

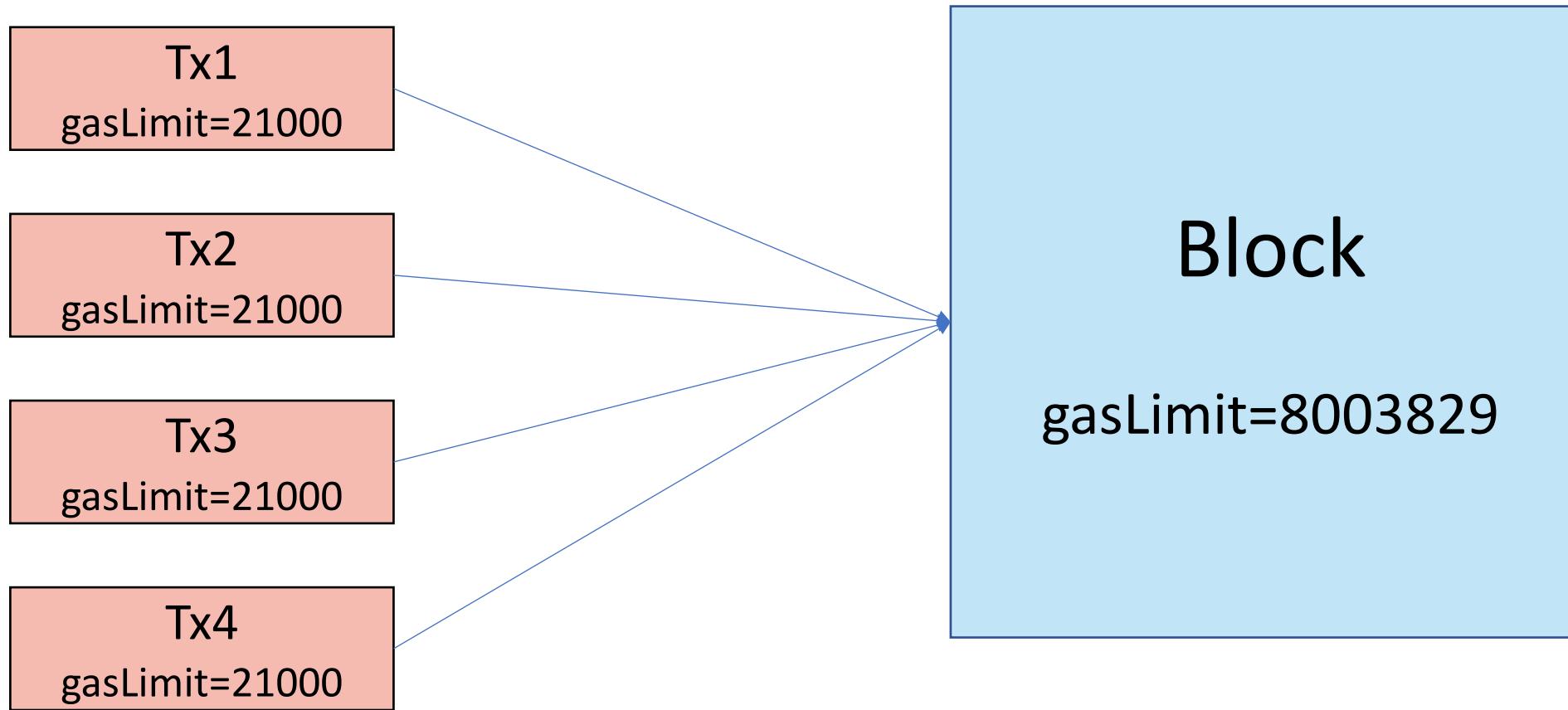


EVM (opcode - gas cost)

Value	Mnemonic	Gas Used	Subset	Removed from stack	Added to stack	Notes
0x00	STOP	0	zero	0	0	Halts execution.
0x01	ADD	3	verylow	2	1	Addition operation
0x02	MUL	5	low	2	1	Multiplication operation.
0x03	SUB	3	verylow	2	1	Subtraction operation.
0x04	DIV	5	low	2	1	Integer division operation
0x05	SDIV	5	low	2	1	Signed integer division o
0x06	MOD	5	low	2	1	Modulo remainder operat
0x07	SMOD	5	low	2	1	Signed modulo remaind
0x08	ADDMOD	8	mid	3	1	Modulo addition operati
0x09	MULMOD	8	mid	3	1	Modulo multiplication op
0xa	EXP	(exp == 0) ? 10 : (10 + 10 * (1 + log256(exp)))		2	1	Exponential operation.

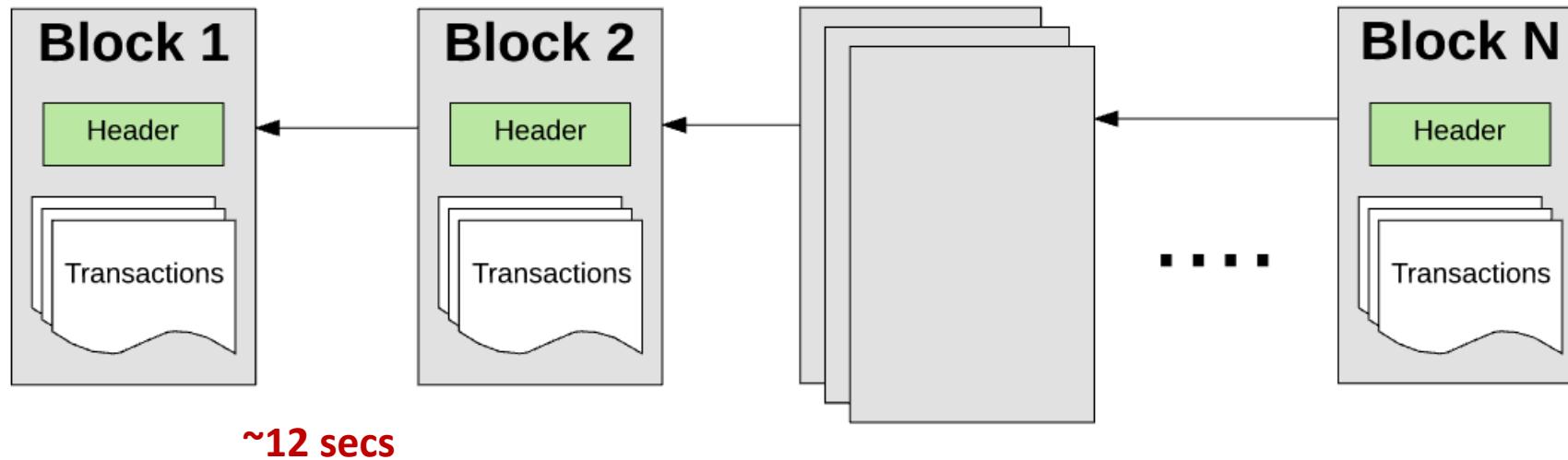
Block & gasLimit

Block 可容納的交易最大數不可超過 Block 的 gasLimit
ex: $8003829/21000 \approx 381$



Block time

~8,000,029 gas



CalcDifficulty

- Avg block time 13 seconds
 - $(9+17)/2 = 13$
 - Advanced reading: <https://blog.cotten.io/ethereums-eip-2-4-15-second-block-target-98d4c11017e1>

// https://github.com/ethereum/EIPs/issues/100.

```
diff = (
    parent_diff +
    (parent_diff / 2048 * max((2 if len(parent.uncles) else 1) - ((timestamp - parent.timestamp) // 9), -99)) +
    2^(periodCount - 2)
)

new_diff = (
    parent_diff +
    parent_diff * scalar +
    difficulty_bomb
)
```

Ethereum's Ice Age

- Difficulty bomb
 - <https://eips.ethereum.org/EIPS/eip-1234>

```
int(2**((block.number // 100000) - 2))
```

Ethereum Block Difficulty Growth Chart

Source: Etherscan.io

Click and drag in the plot area to zoom in



[Home](#)[Blockchain](#) ▾[Tokens](#) ▾[Resources](#) ▾[More](#) ▾[Sign In](#)

Going to Devcon 5? Check out more events during the week [Find out more!](#)



Ethereum Blockchain Explorer

Quick links: [ERC-20 Tokens](#) [ERC-721 Tokens](#)

[All Filters](#) ▾Search

ETHER PRICE
\$177.85 @ 0.0213 BTC (-0.91%)

LATEST BLOCK
8657267 (13.3s)

TRANSACTIONS
552.51 M (8.4 TPS)

ETHEREUM TRANSACTION HISTORY IN 14 DAYS



MARKET CAP
\$19,202,377,525.623

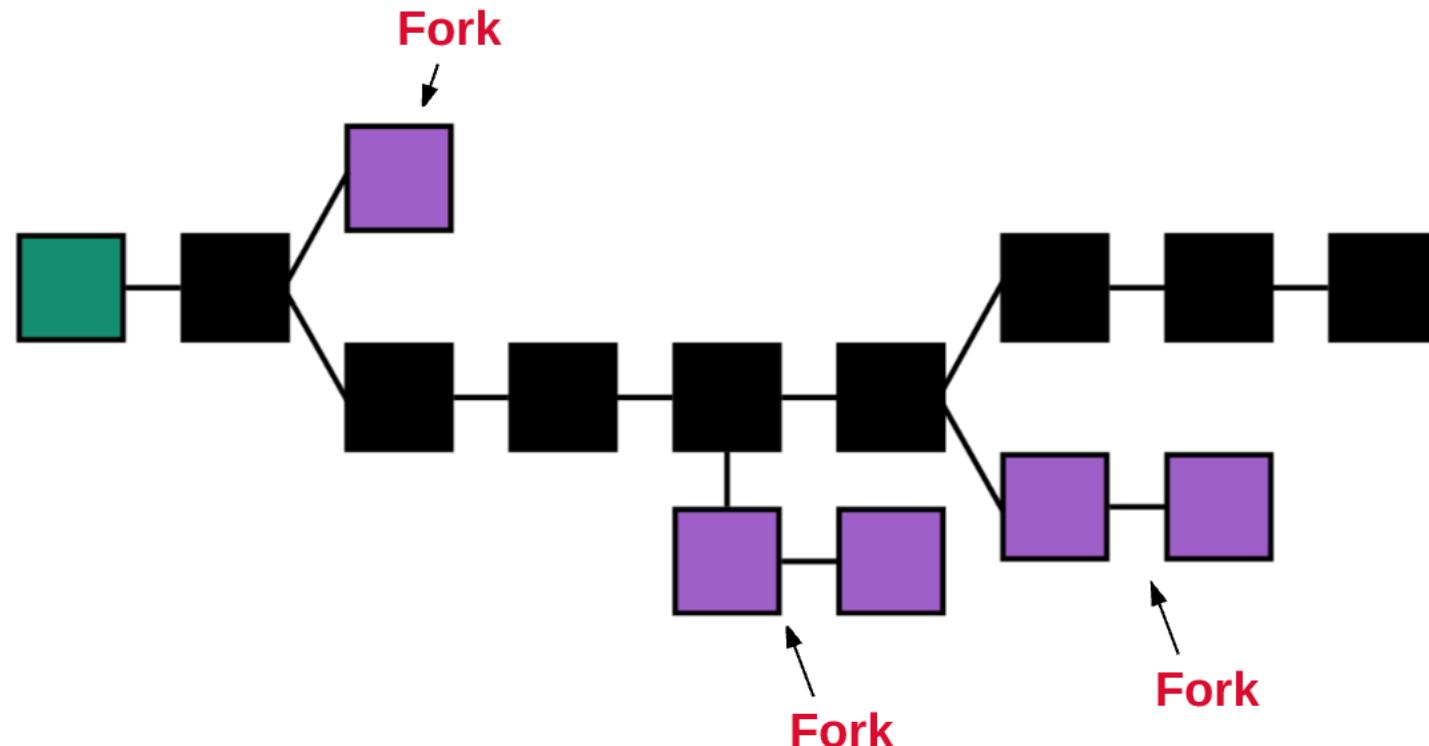
DIFFICULTY
2,457.88 TH

HASH RATE
194,266.88 GH/s

Height	Age	txn	Uncles	Miner	GasUsed	GasLimit	Avg.GasPrice	Reward
6526910	28 secs ago	61	0	MiningPoolHub_1	7990649 (99.88%)	8000029	5.24 Gwei	3.04186 Ether
6526909	37 secs ago	138	1	SparkPool	7996442 (99.96%)	8000029	3.23 Gwei	3.11961 Ether
6526908	38 secs ago	24	0	Ethermine	1466444 (18.33%)	8000029	37.42 Gwei	3.05487 Ether
6526907	54 secs ago	67	0	Ethermine	7981592 (99.77%)	8000029	3.72 Gwei	3.02967 Ether
6526906	1 min ago	23	1	MinerallPool	1124849 (14.05%)	8003875	34.56 Gwei	3.13262 Ether
6526905	1 min ago	82	0	Ethermine	7983629 (99.80%)	7999992	3.24 Gwei	3.02587 Ether
6526904	1 min ago	89	0	DwarfPool_1	3872901 (48.46%)	7992222	15.36 Gwei	3.05948 Ether
6526903	1 min ago	65	0	MiningPoolHub_1	7999898 (100.00%)	8000029	6.17 Gwei	3.04938 Ether
6526902	1 min ago	104	0	SparkPool	7979635 (99.75%)	8000029	1.77 Gwei	3.01414 Ether
6526901	1 min ago	103	0	SparkPool	4421679 (55.27%)	8000029	15.84 Gwei	3.07004 Ether
6526900	1 min ago	103	0	SparkPool	7992210 (99.90%)	8000029	4.27 Gwei	3.03414 Ether
6526899	1 min ago	83	0	Ethermine	7991895 (99.90%)	8000029	8.42 Gwei	3.06729 Ether
6526898	2 mins ago	135	1	MiningPoolHub_1	7987068 (99.84%)	8000029	6.05 Gwei	3.14205 Ether
6526897	2 mins ago	181	0	Nanopool	7986851 (99.84%)	8000029	18.83 Gwei	3.15041 Ether

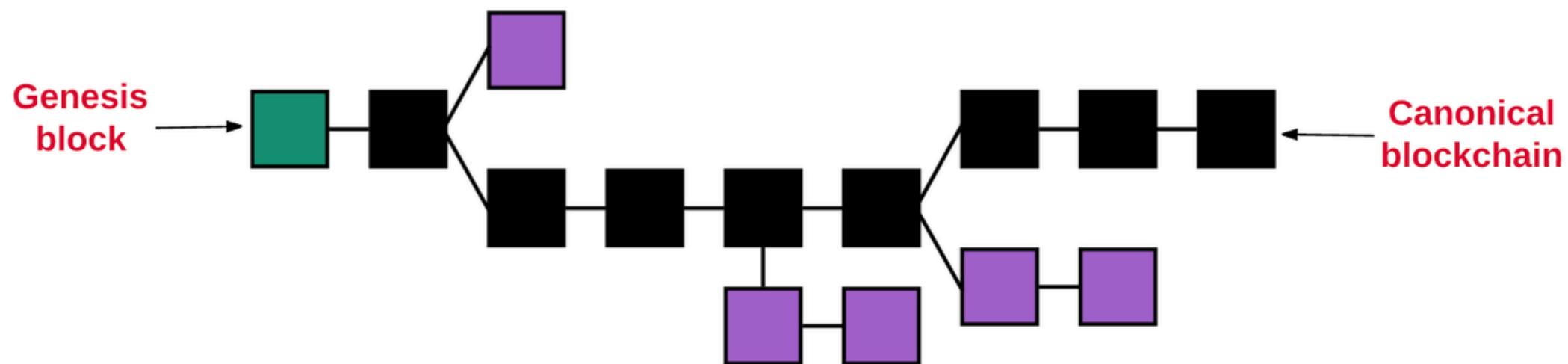
鏈的一致性

- GHOST = Greedy Heaviest Observed Subtree protocol



GHOST

Ethereum uses only uses longest chain, instead of the actual heaviest chain proposed in GHOST.



R = 3 ETH

Uncle reward

$$\bullet (U_n + 8 - B_n) * R \div 8$$

Maximum of 2 Uncles is allowed per block

Block Height	UncleNumber	Age	Miner	Reward
6526925	6526923	2 mins ago	Nanopool	(23-25+8)*3/8
6526917	6526916	3 mins ago	0xd4383232c8d1db...	2.625 Ether
6526916	6526915	4 mins ago	SparkPool	2.625 Ether
6526914	6526912	4 mins ago	SparkPool	2.25 Ether
6526909	6526908	5 mins ago	Nanopool	2.625 Ether
6526906	6526905	6 mins ago	MiningPoolHub_1	2.625 Ether
6526898	6526895	7 mins ago	SparkPool	(95-98+8)*3/8

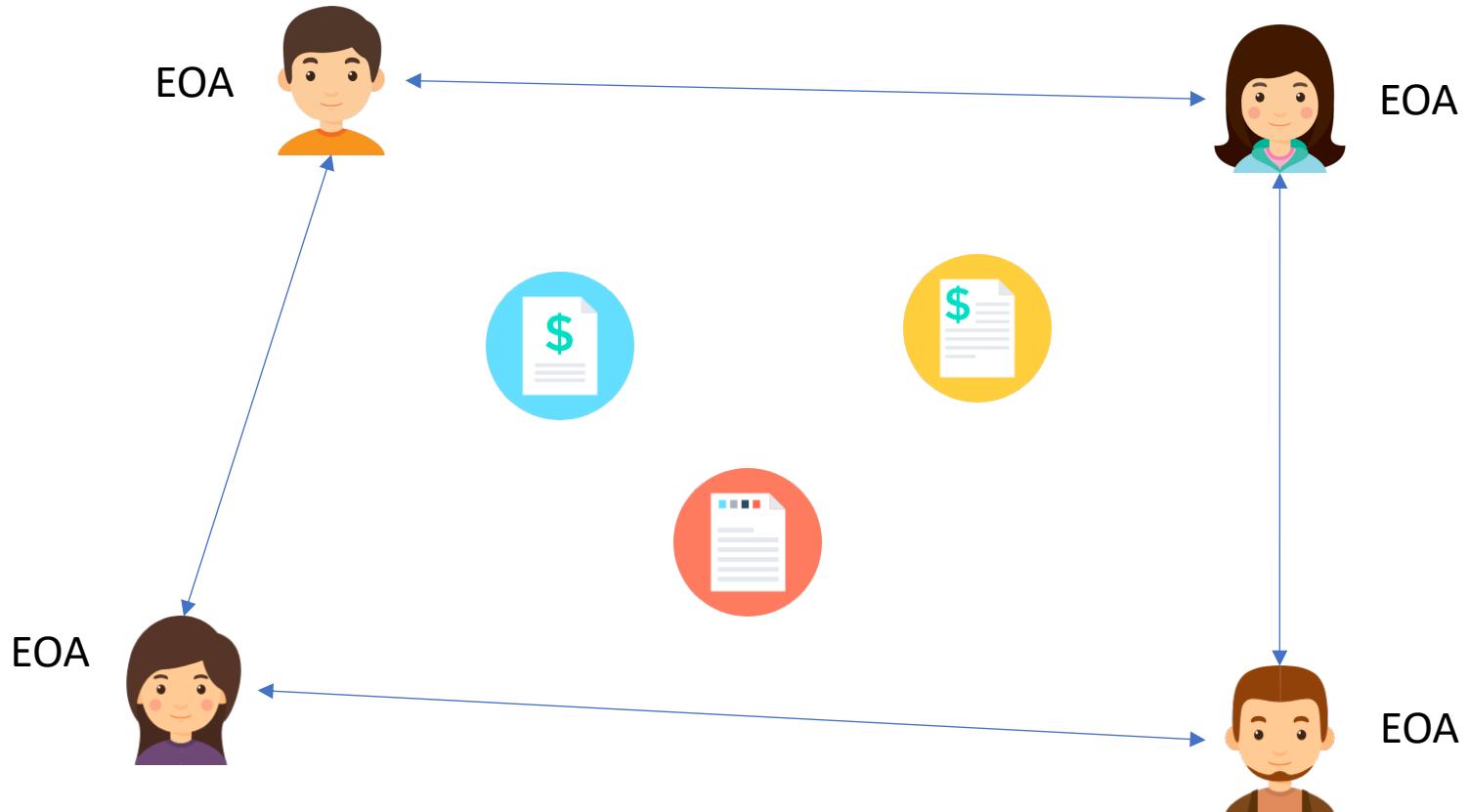
名詞

- 帳戶 (accounts)
- 狀態 (state)
- gas 和手續費 (gas and fees)
- 交易 (transactions)
- 區塊 (blocks)
- 交易執行 (transaction execution)
- 挖礦 (mining)
- 工作量證明 (proof of work)

角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯

0xA473768422AB71D0D2dC60F6cBB8C6bC0811F7c3

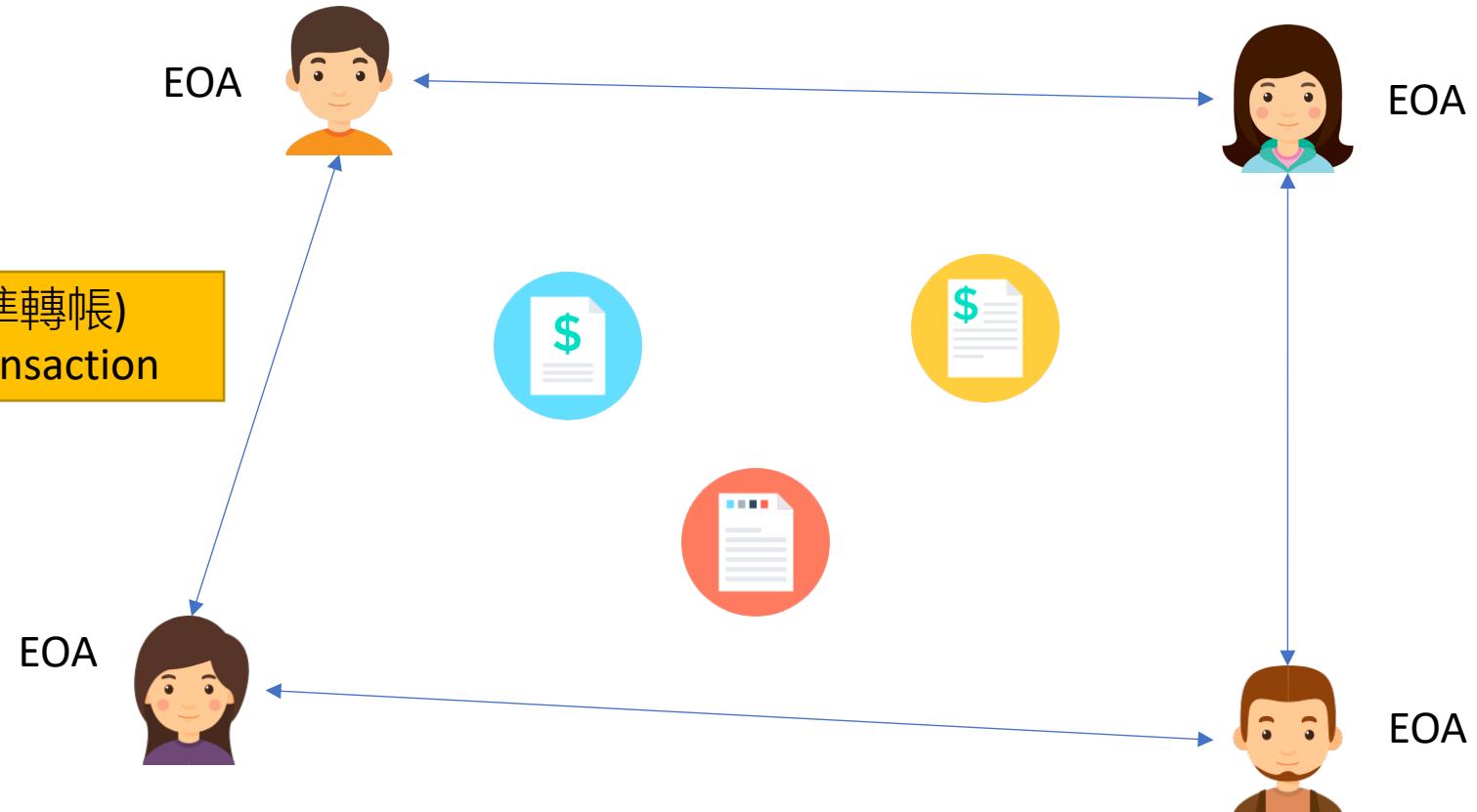


角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯

0xA473768422AB71D0D2dC60F6cBB8C6bC0811F7c3

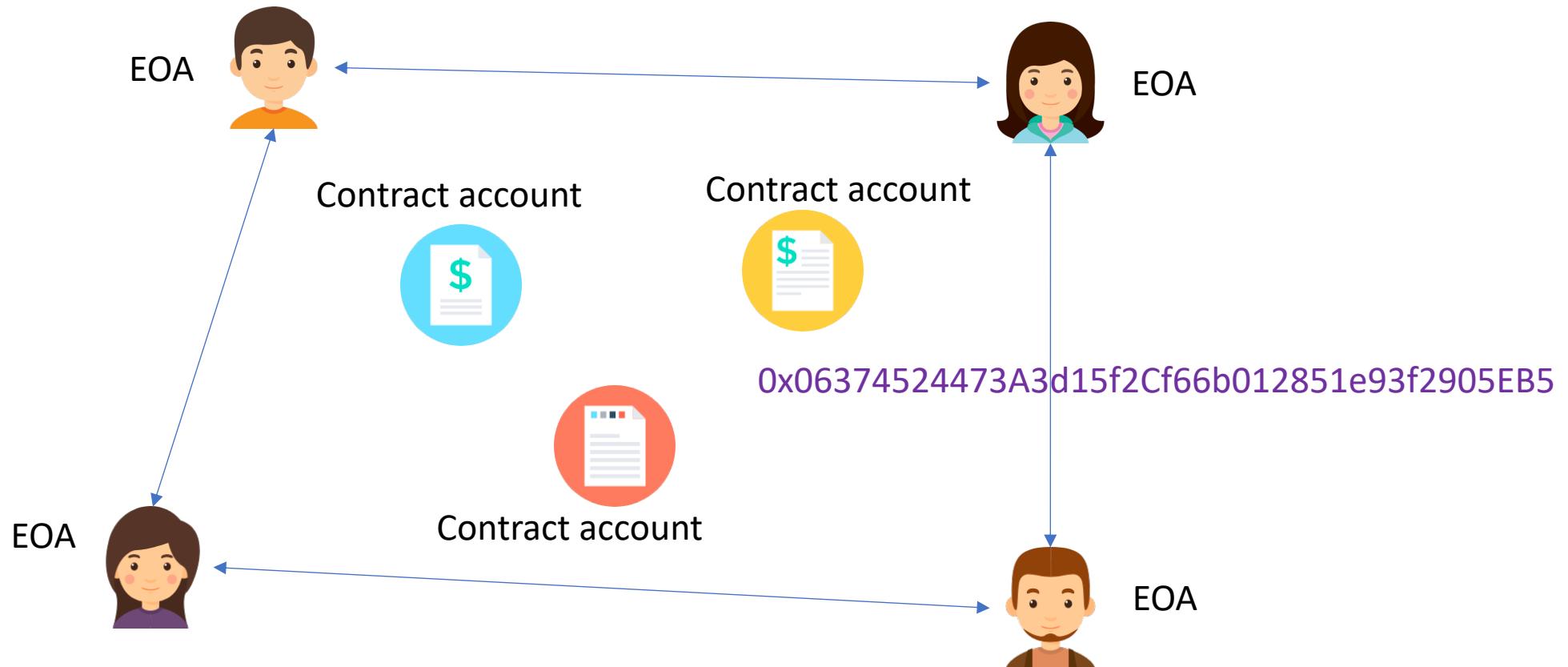
0x3441781fc5f9619c53336861f4fb08b273125F4F



角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯

0xA473768422AB71D0D2dC60F6cBB8C6bC0811F7c3

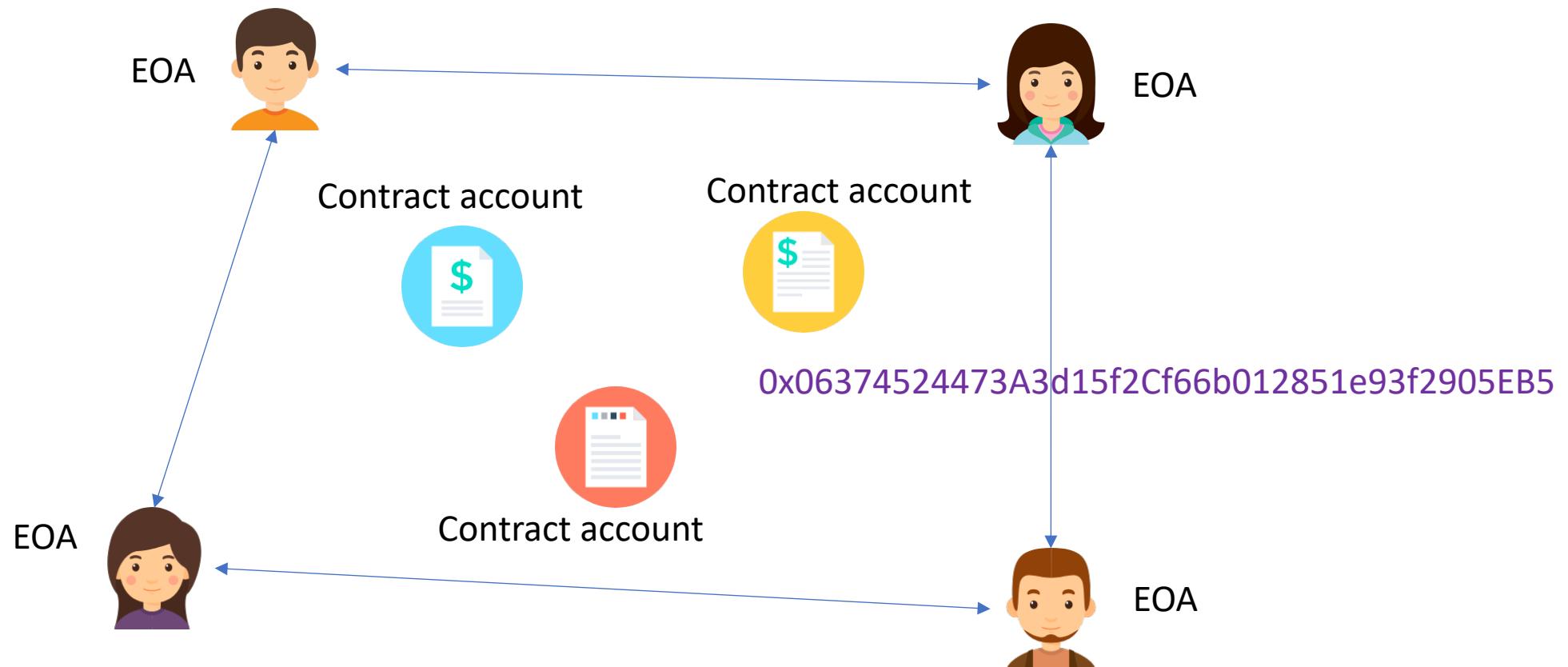


角色

- 外部帳戶 (External owned account, EOA), 由私鑰進行控制
- 合約帳戶 (Contract account), 與合約程式碼相關聯

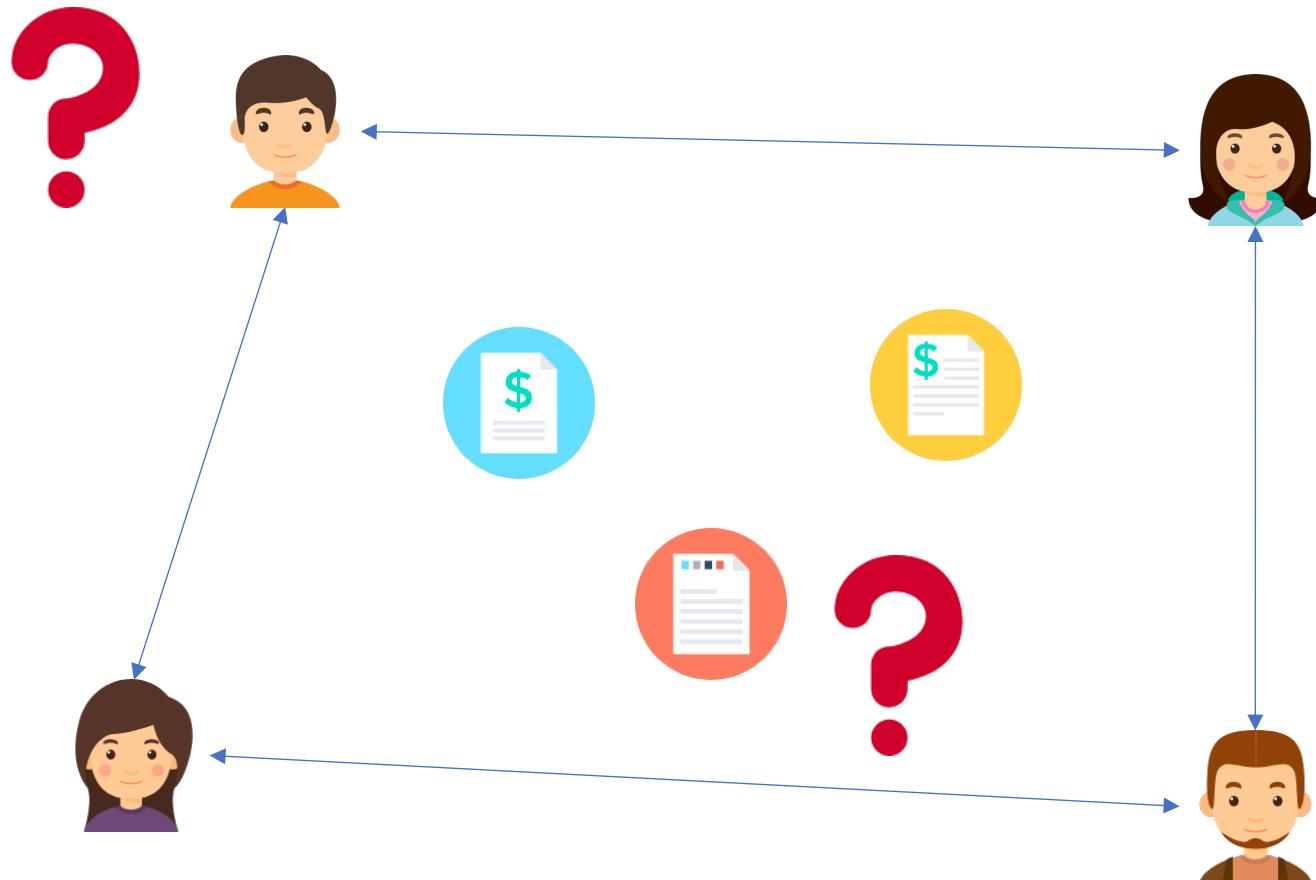
0xA473768422AB71D0D2dC60F6cBB8C6bC0811F7c3

肉眼分不出地址是 EOA
還是 Contract account



角色

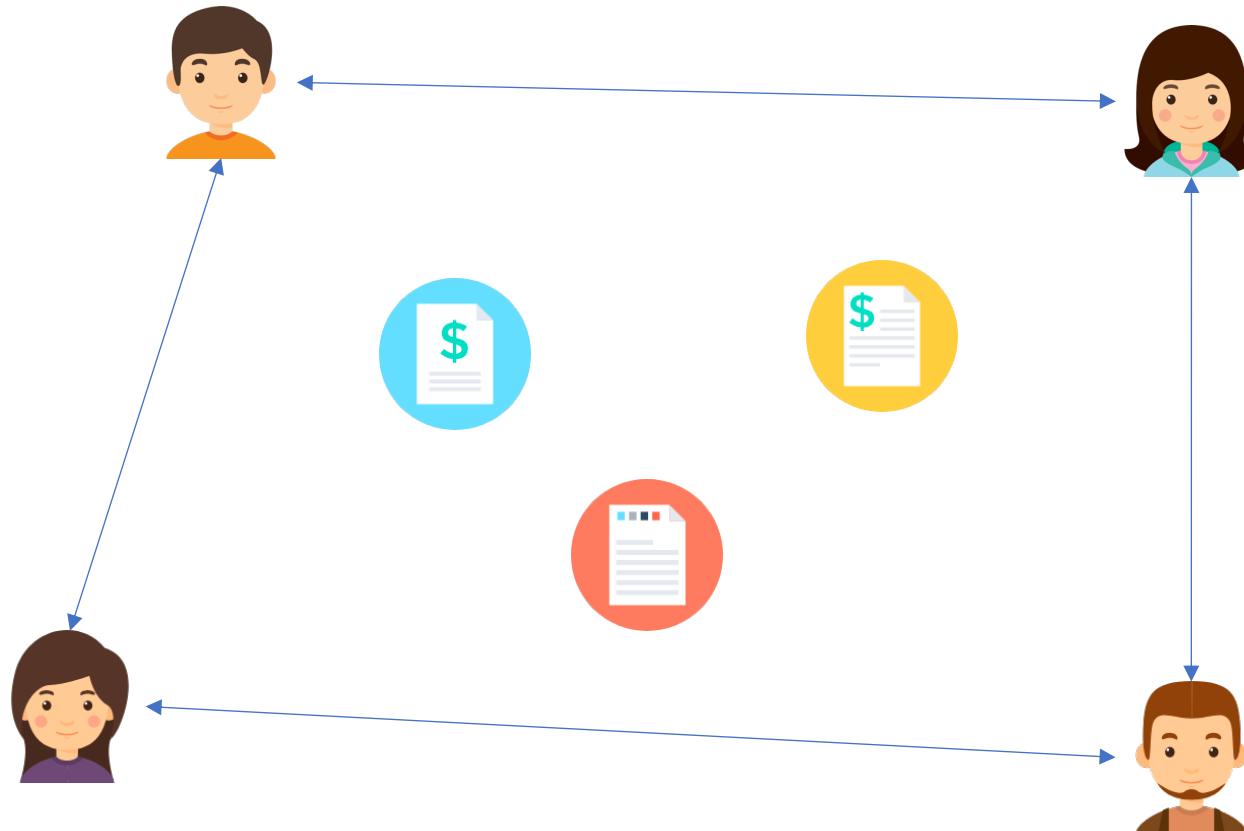
1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



角色

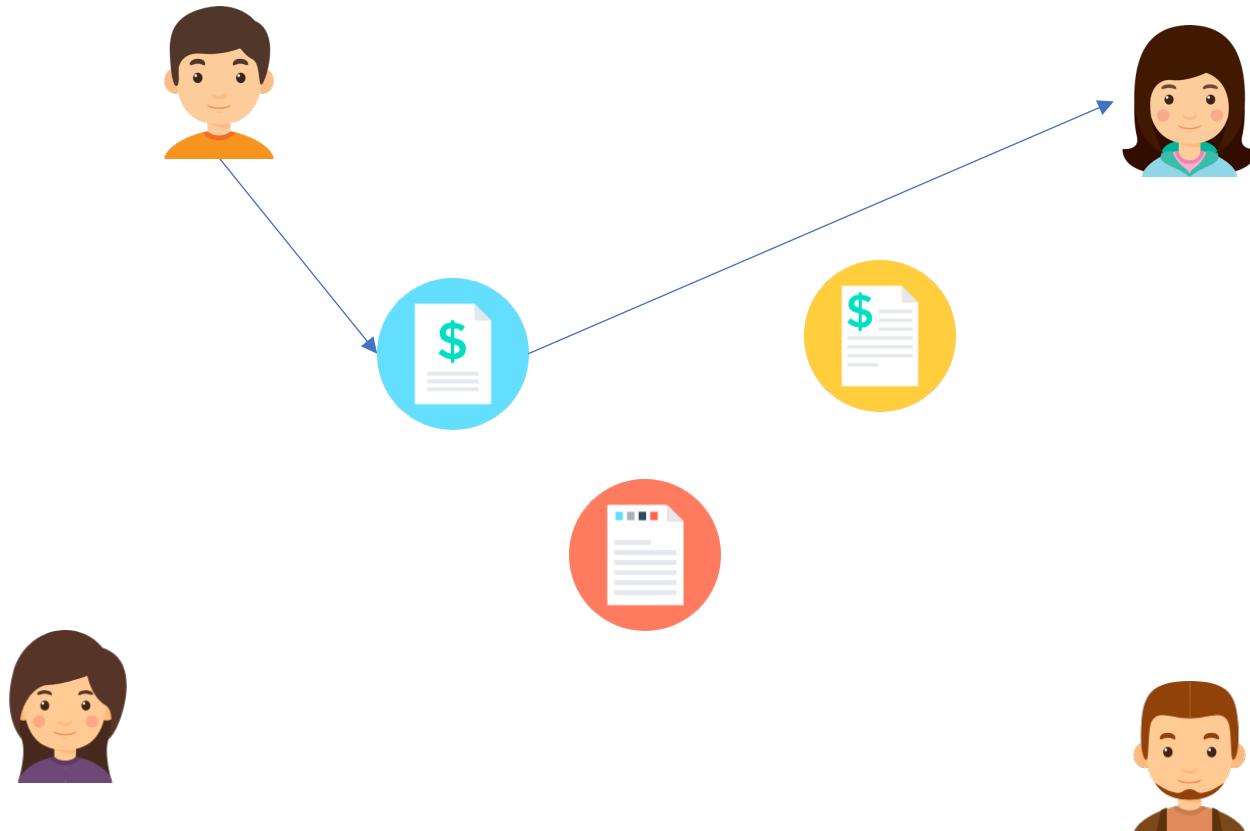
1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯

既然 Contract account 沒有私鑰，就無法發起交易



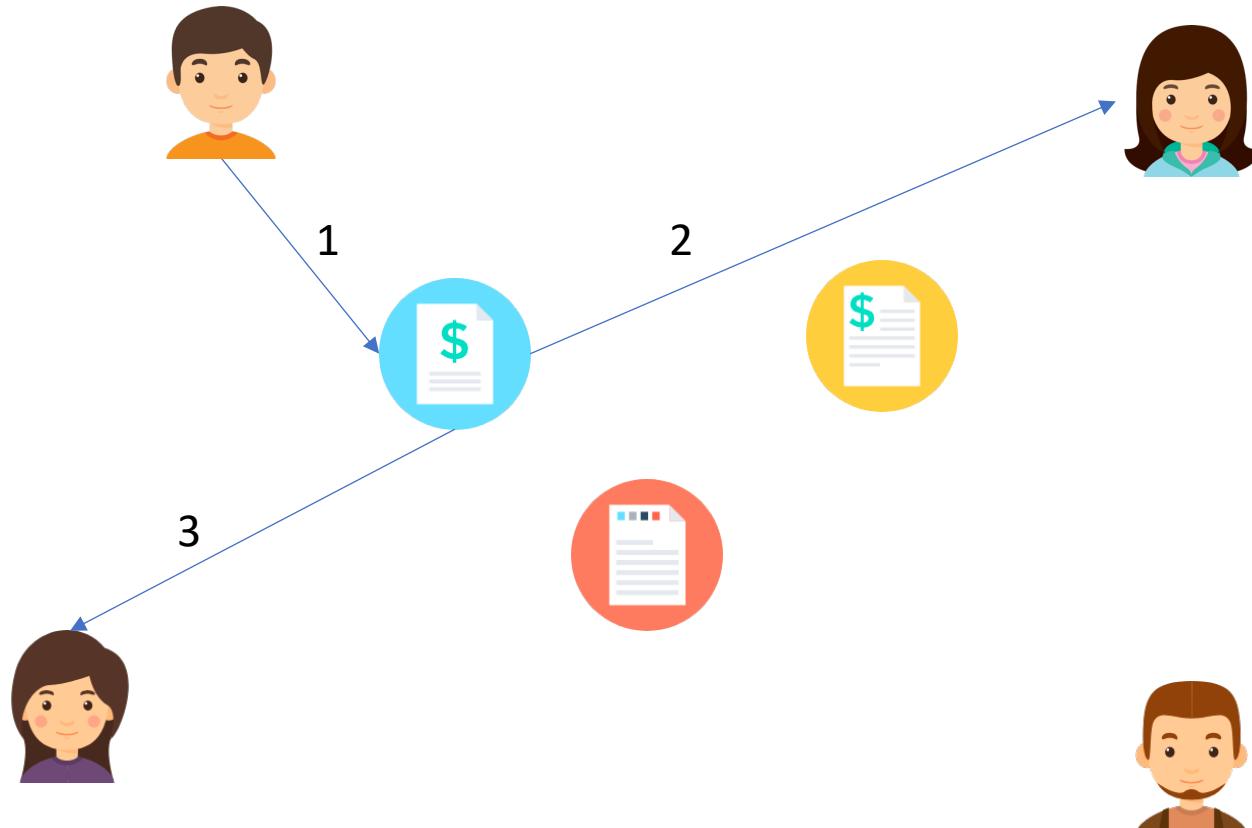
角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



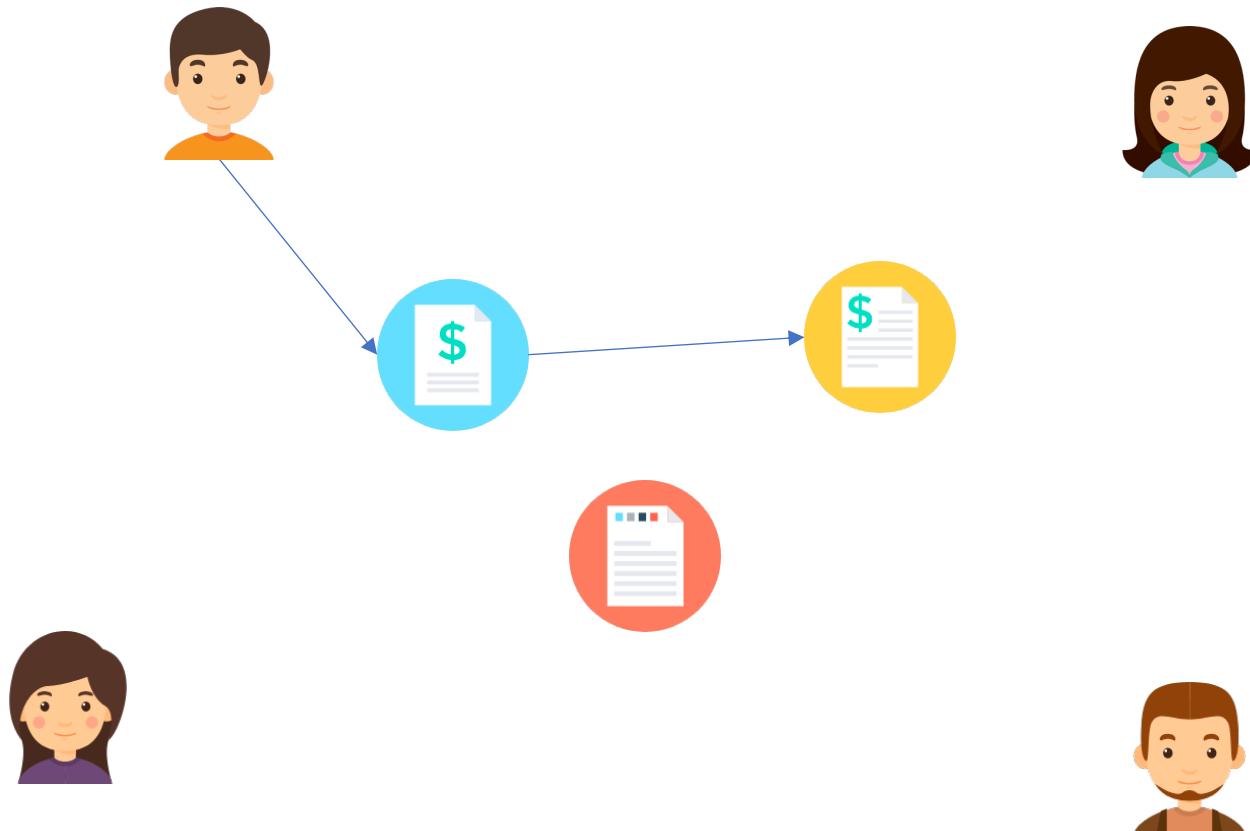
角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



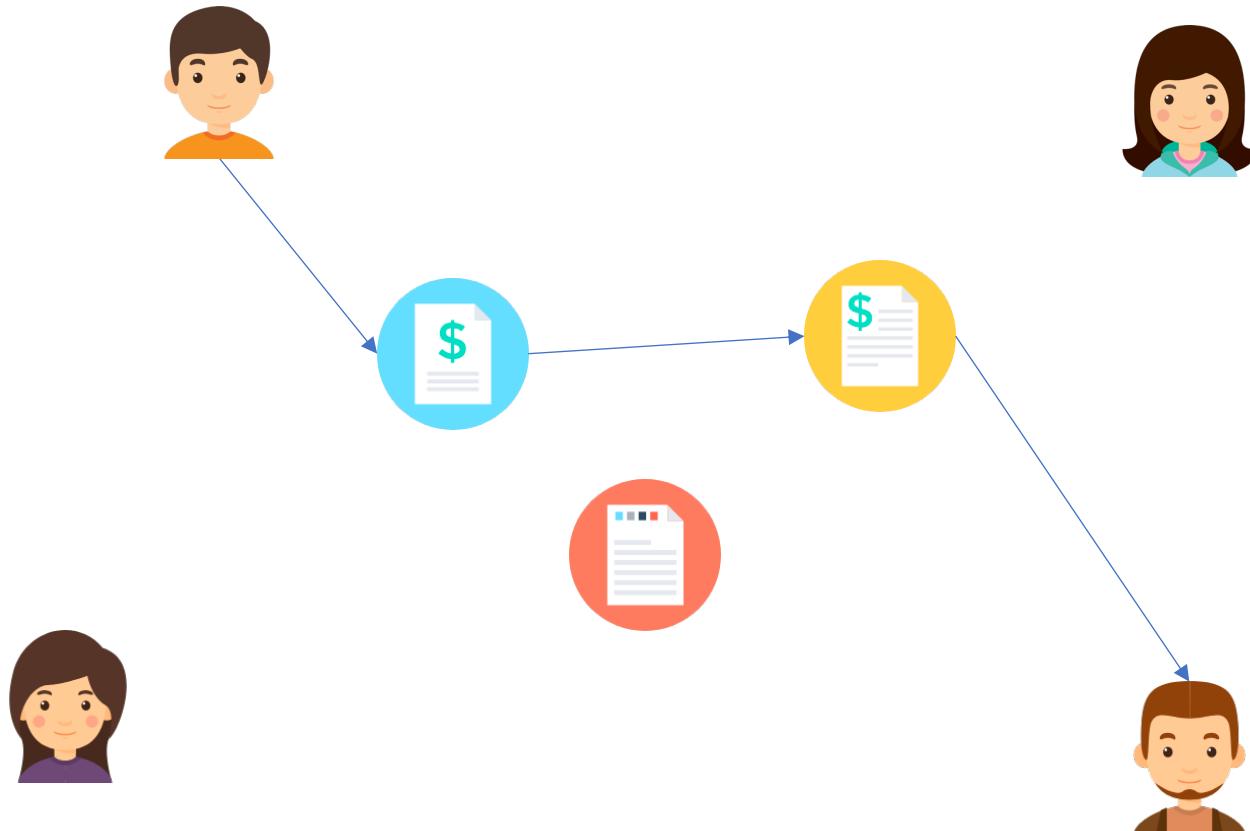
角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



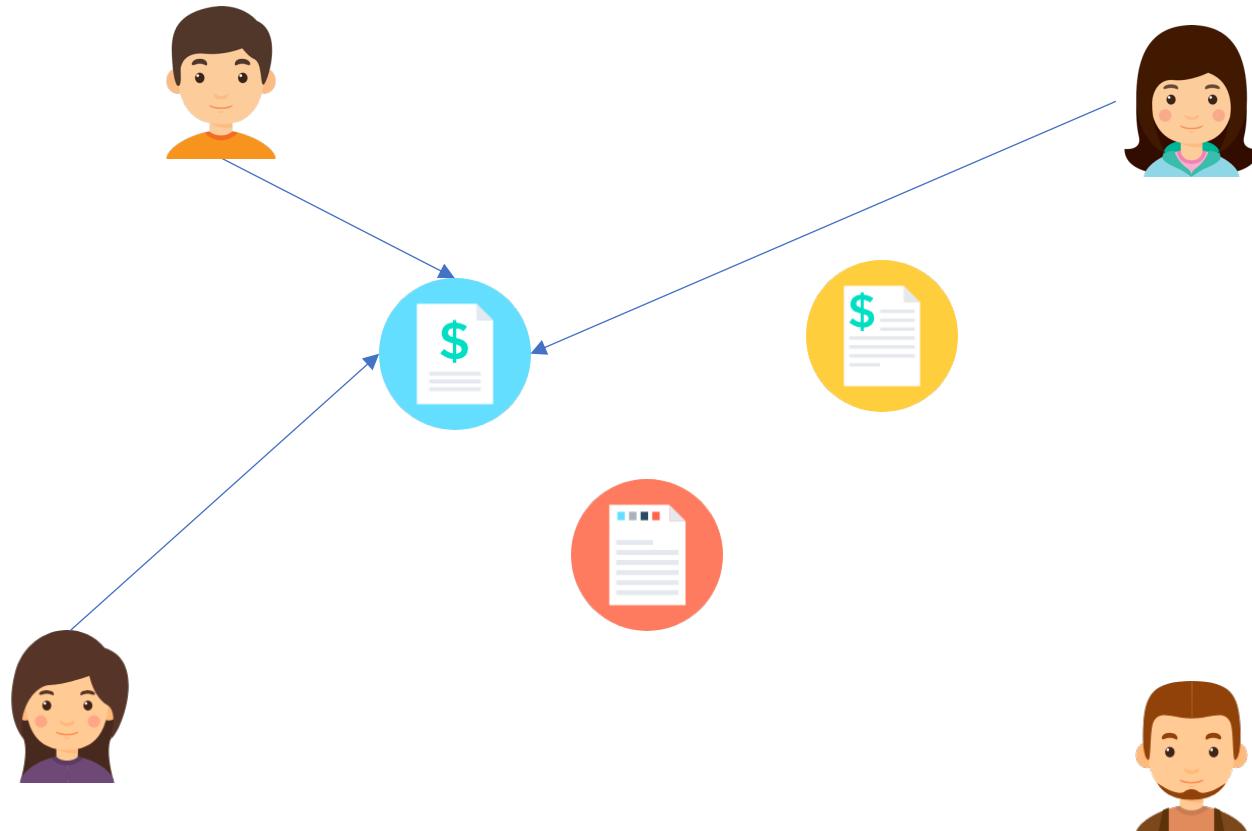
角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



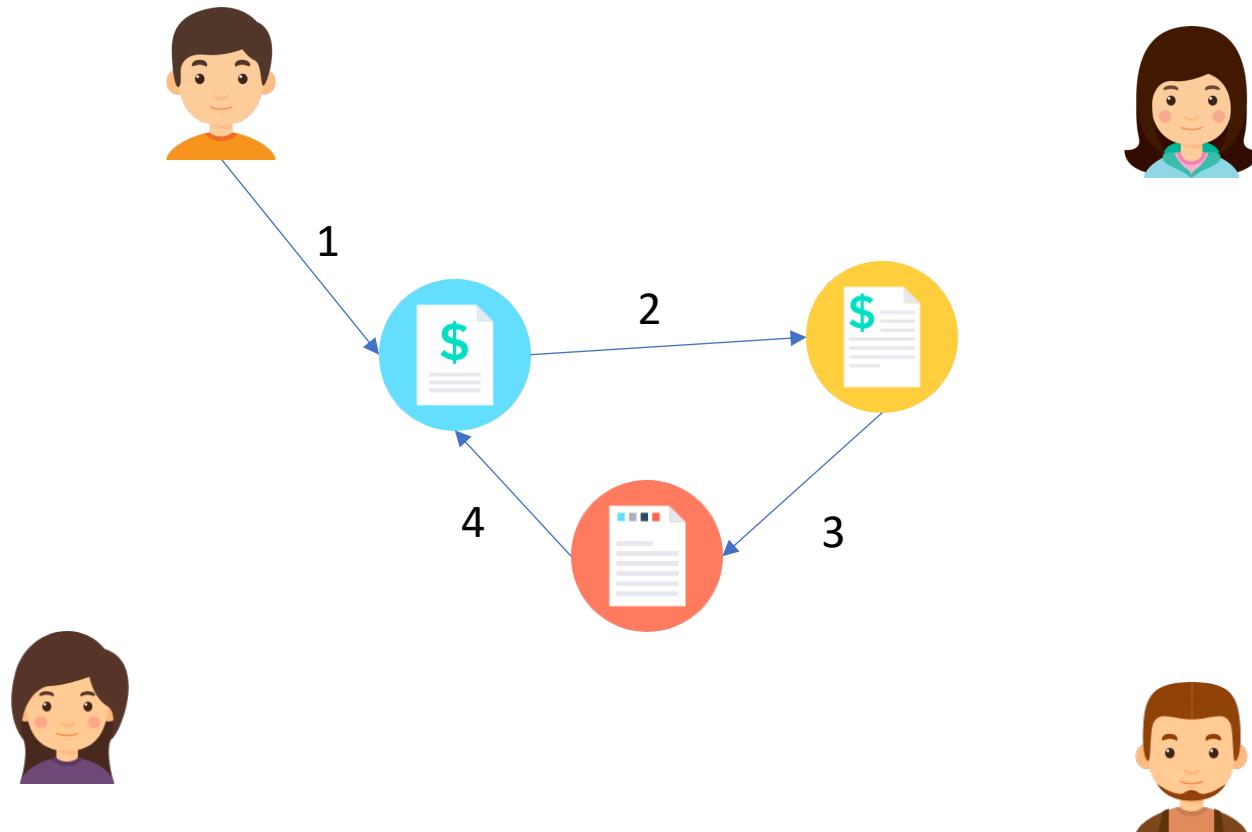
角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



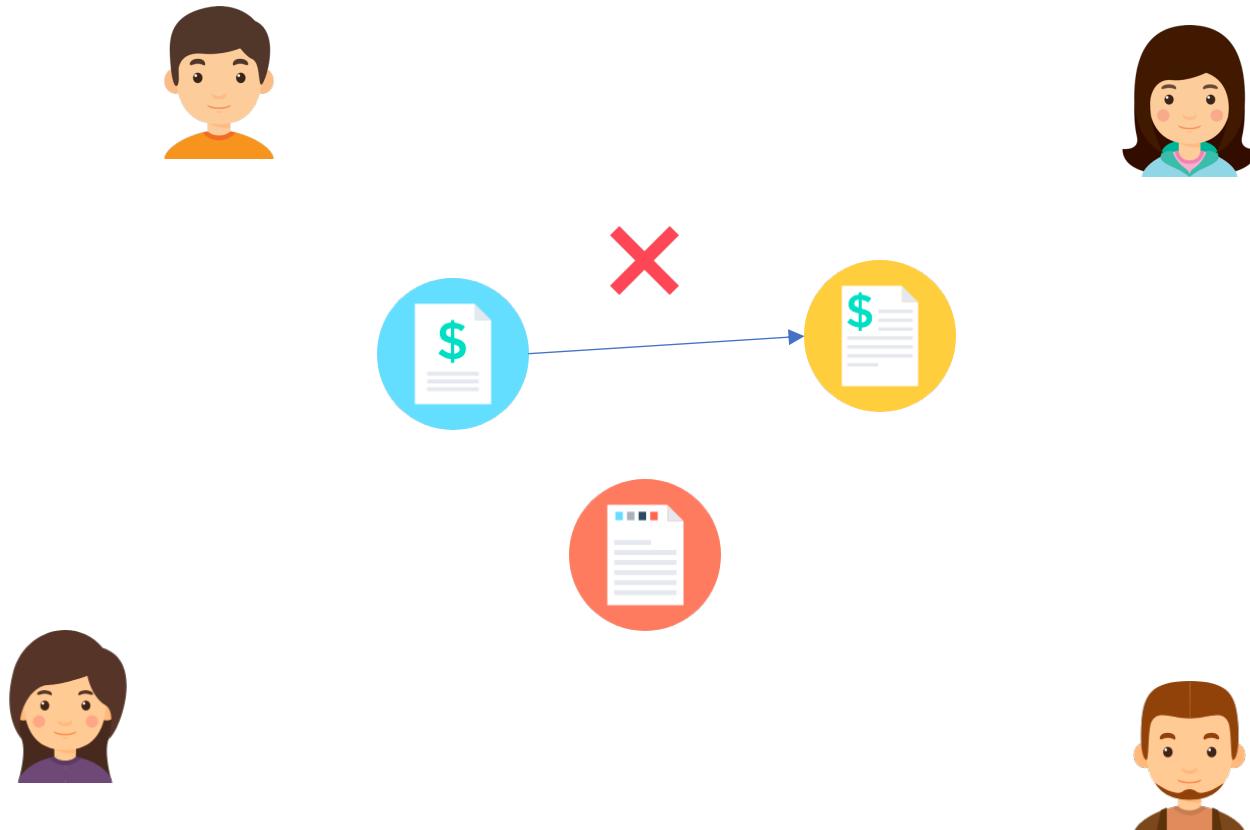
角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



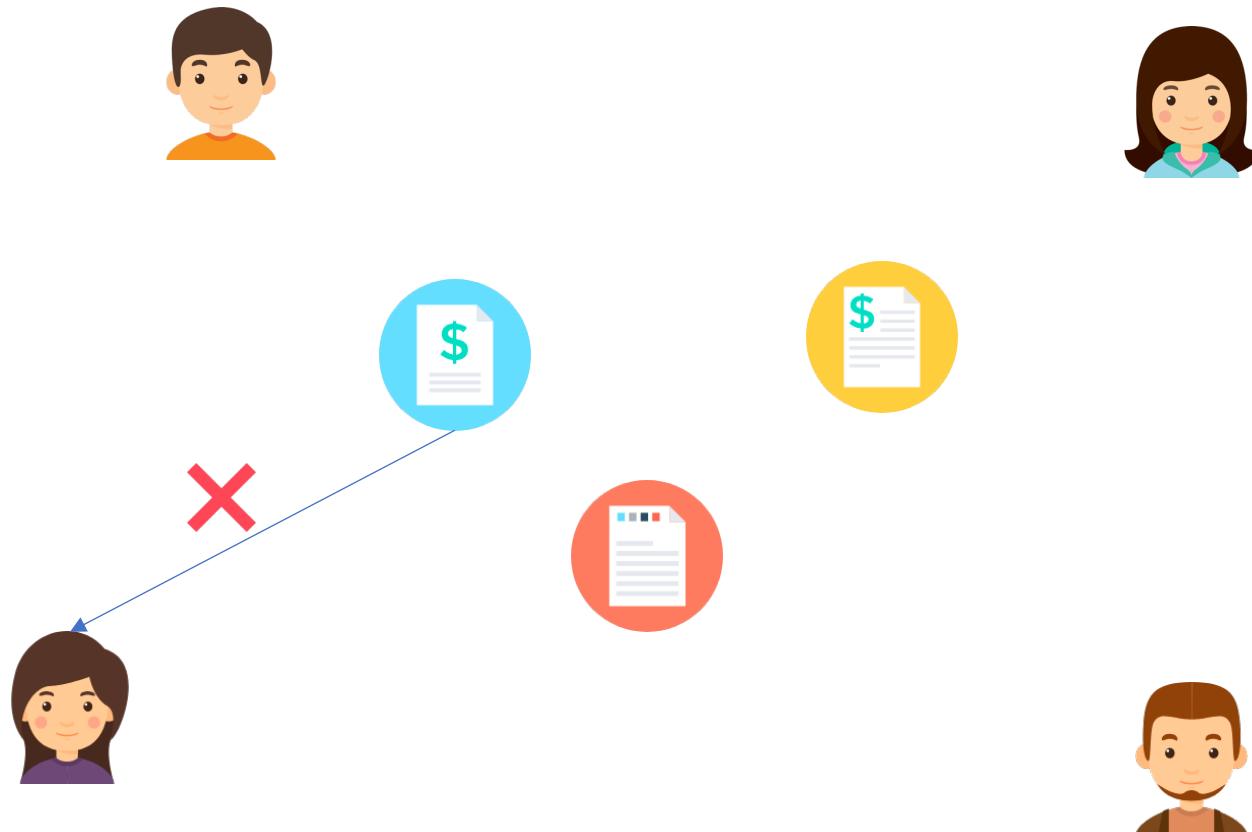
角色

1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



角色

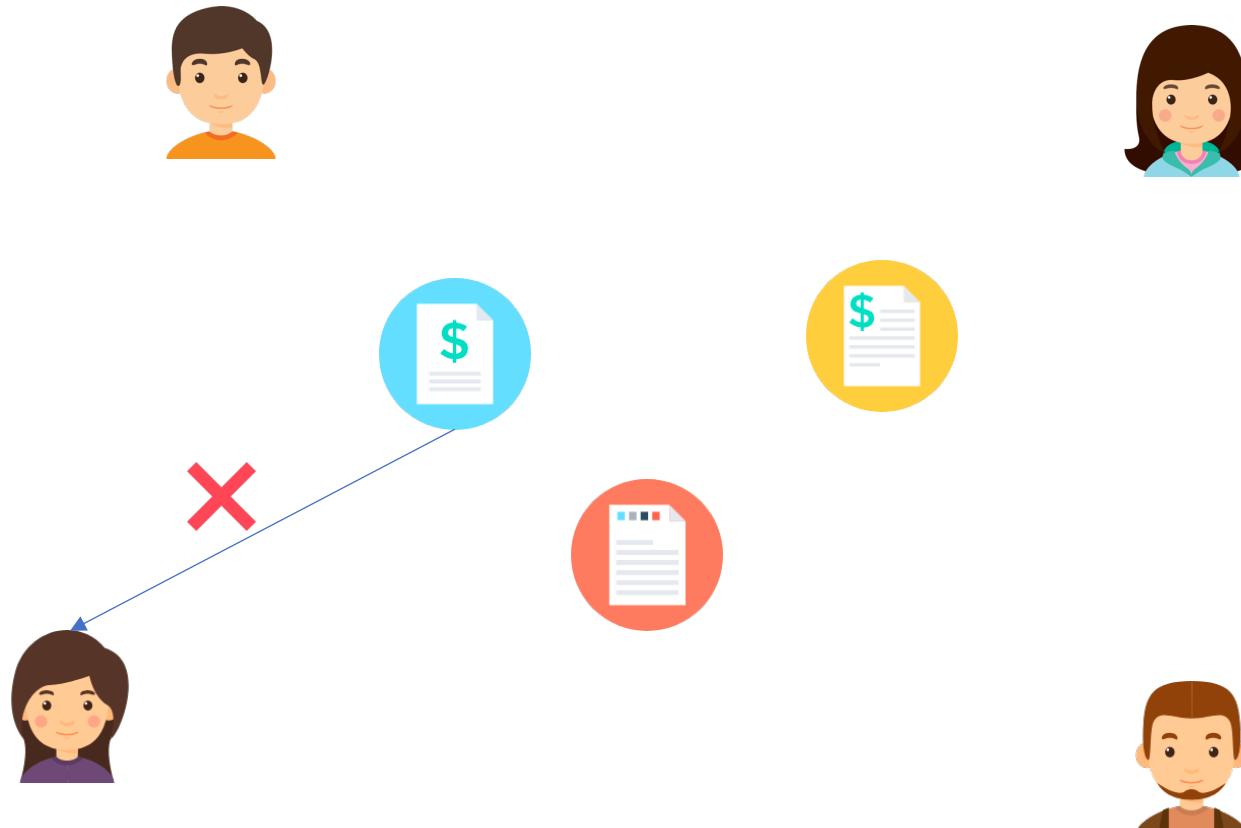
1. 外部帳戶 (External owned account, EOA), 由私鑰進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯



角色

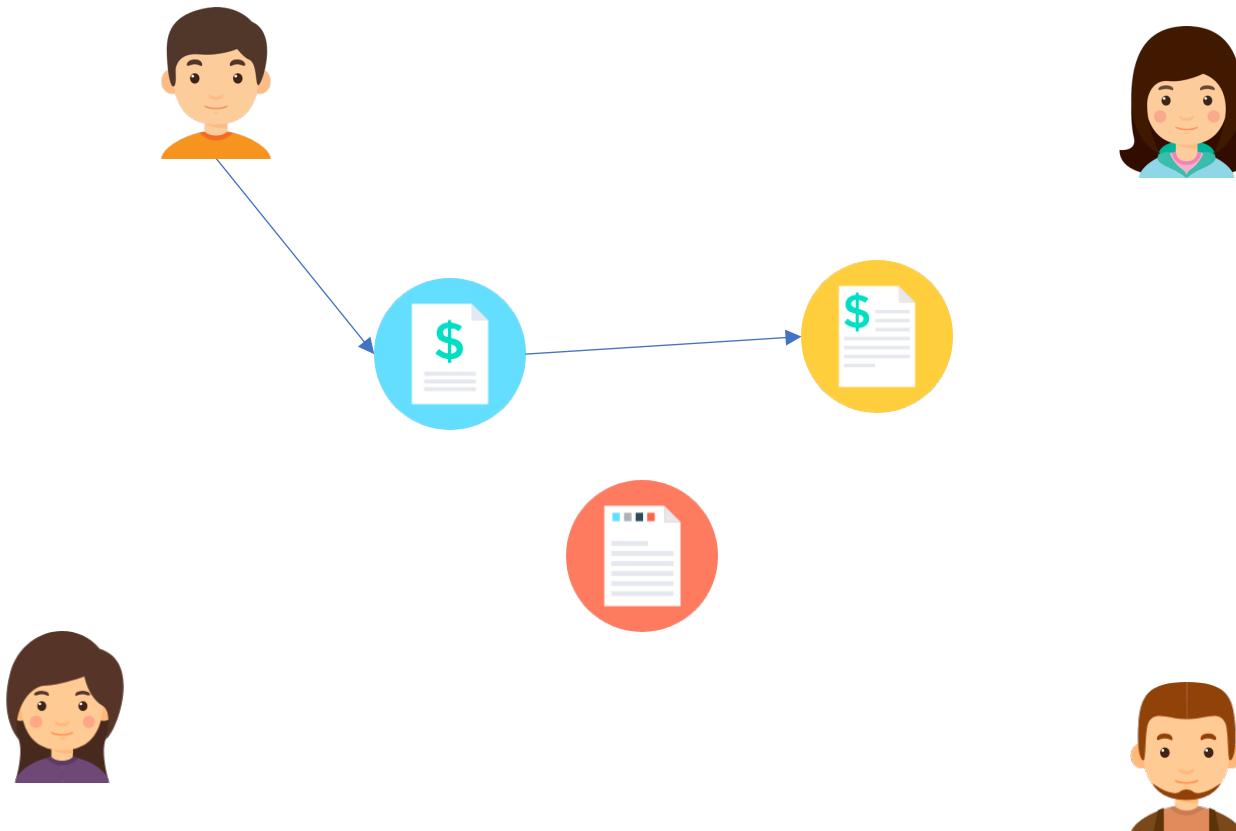
1. 外部帳戶 (External owned account, EOA), 由**私鑰**進行控制
2. 合約帳戶 (Contract account), 與合約程式碼相關聯

擁有私鑰的外部帳戶
才能主動發起交易或訊息



交易

- 標準交易 (EOA to EOA)
- 合約交易 (EOA 與 Contract account 有互動的交易)



交易

- 標準交易 (EOA to EOA)
- 合約交易 (EOA 與 Contract account 有互動的交易)
 - Contract creation
 - Contract invocation (Message calls)

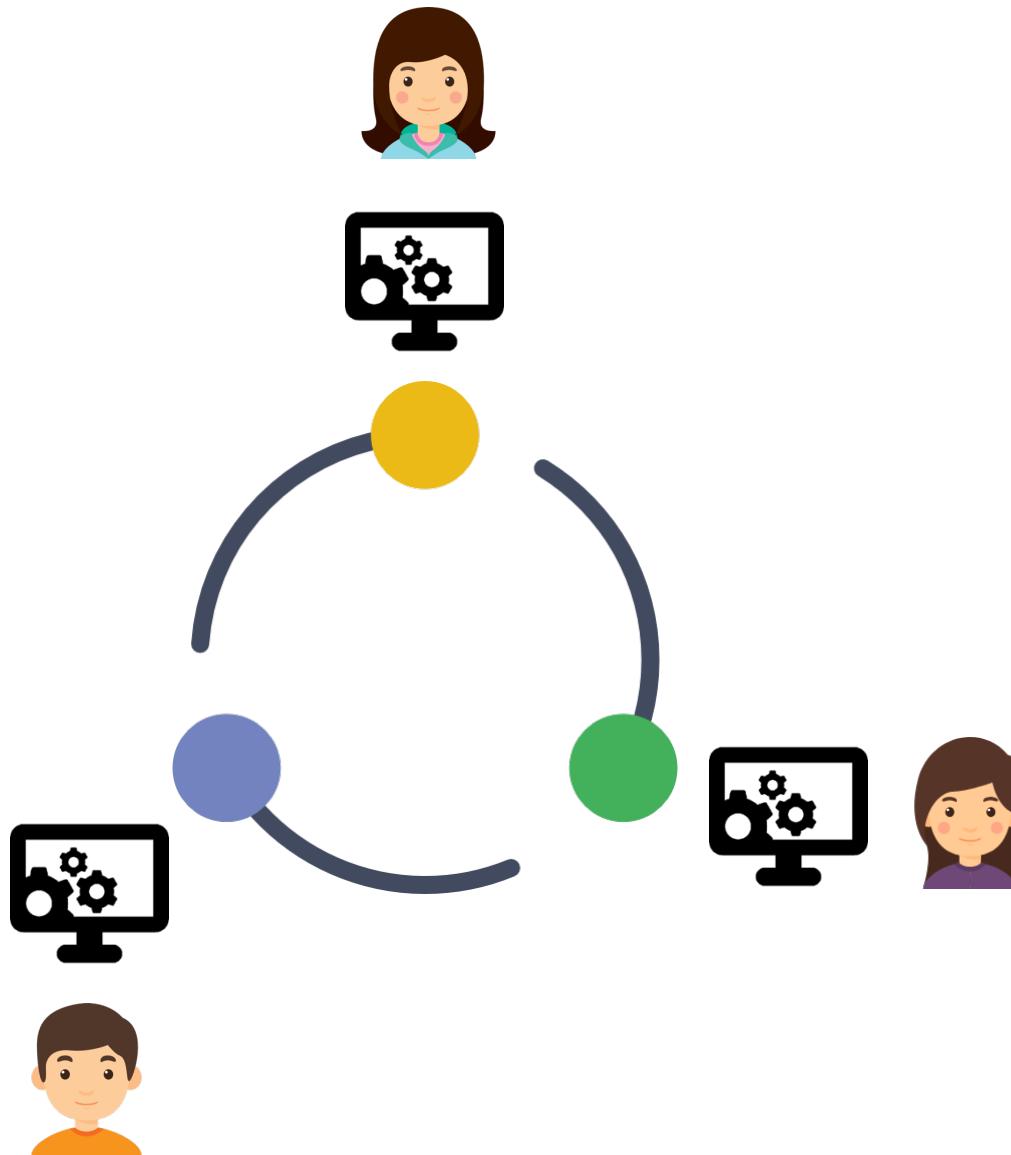
網路



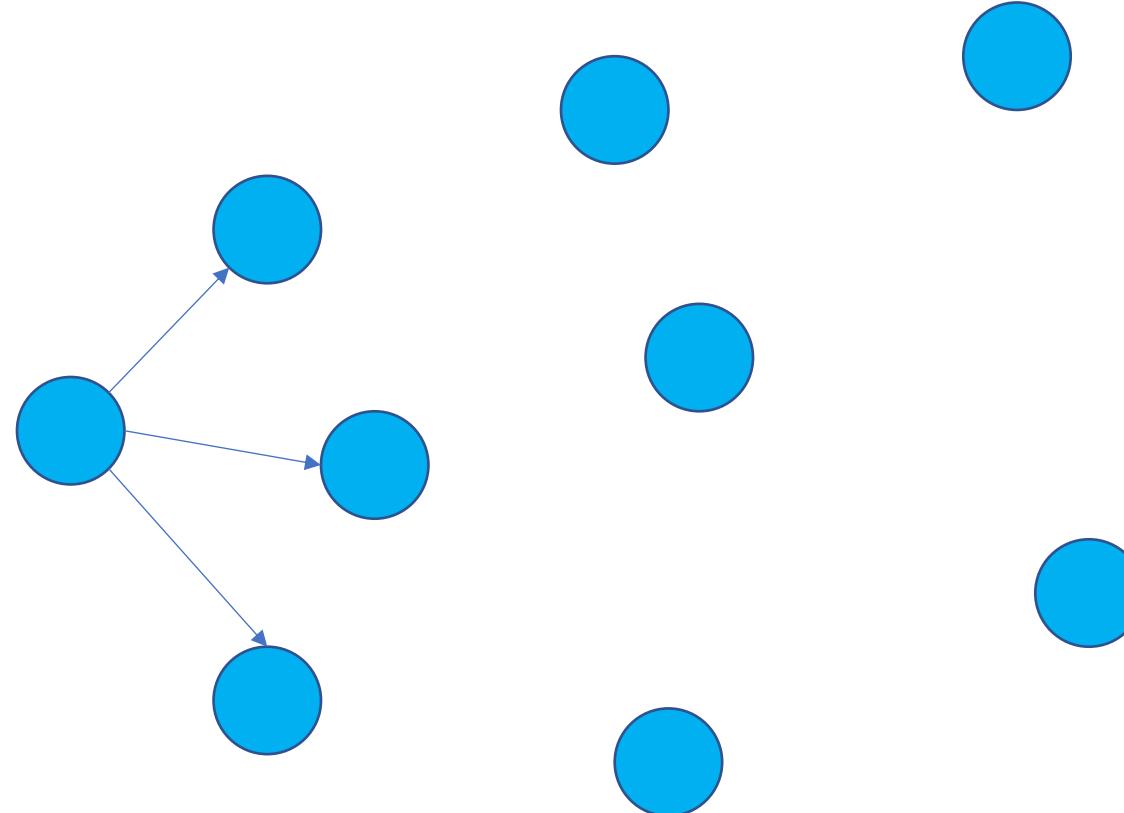
標準交易



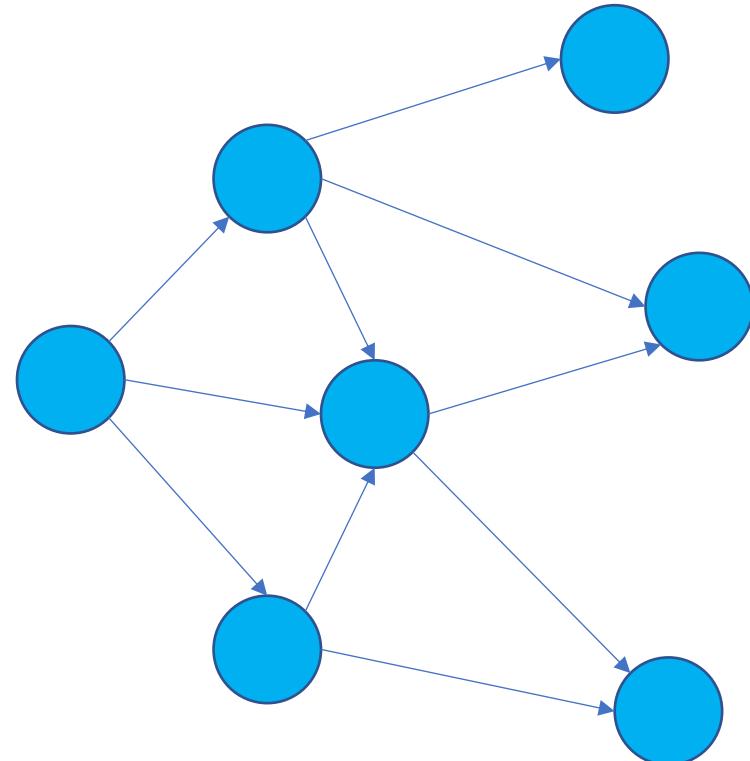
合約交易



廣播交易

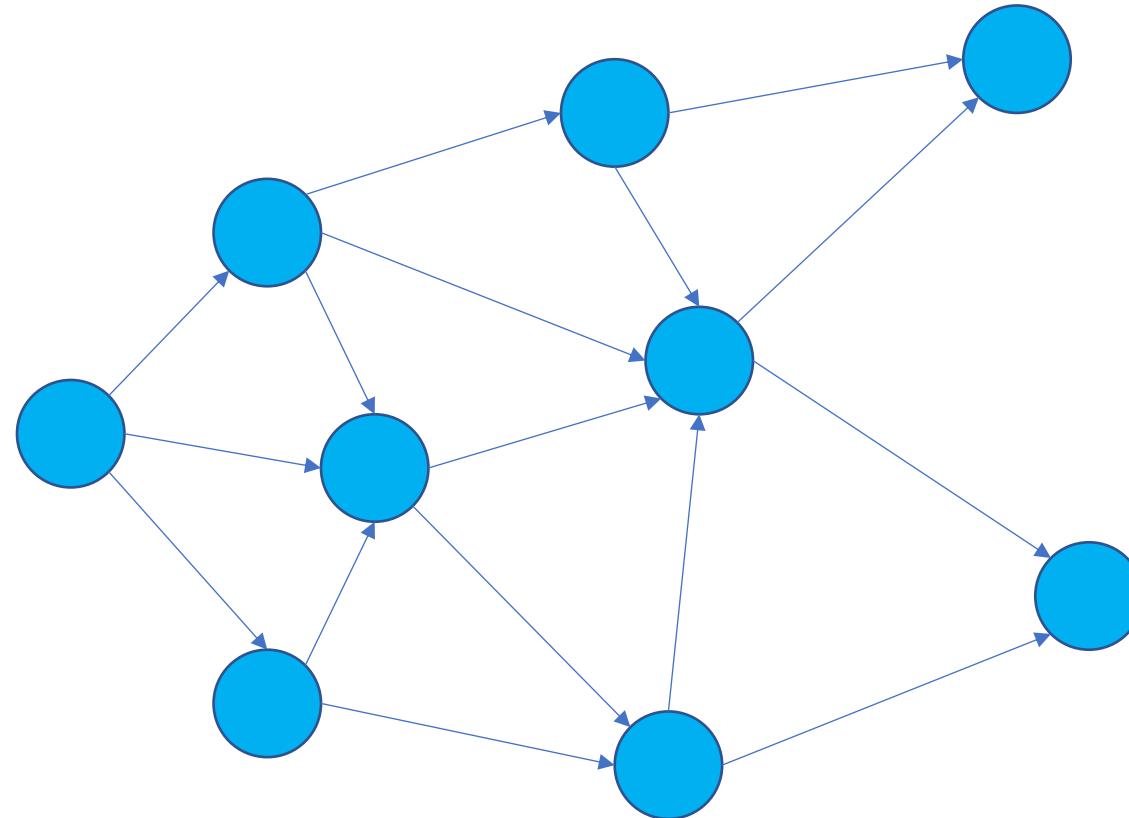


廣播交易

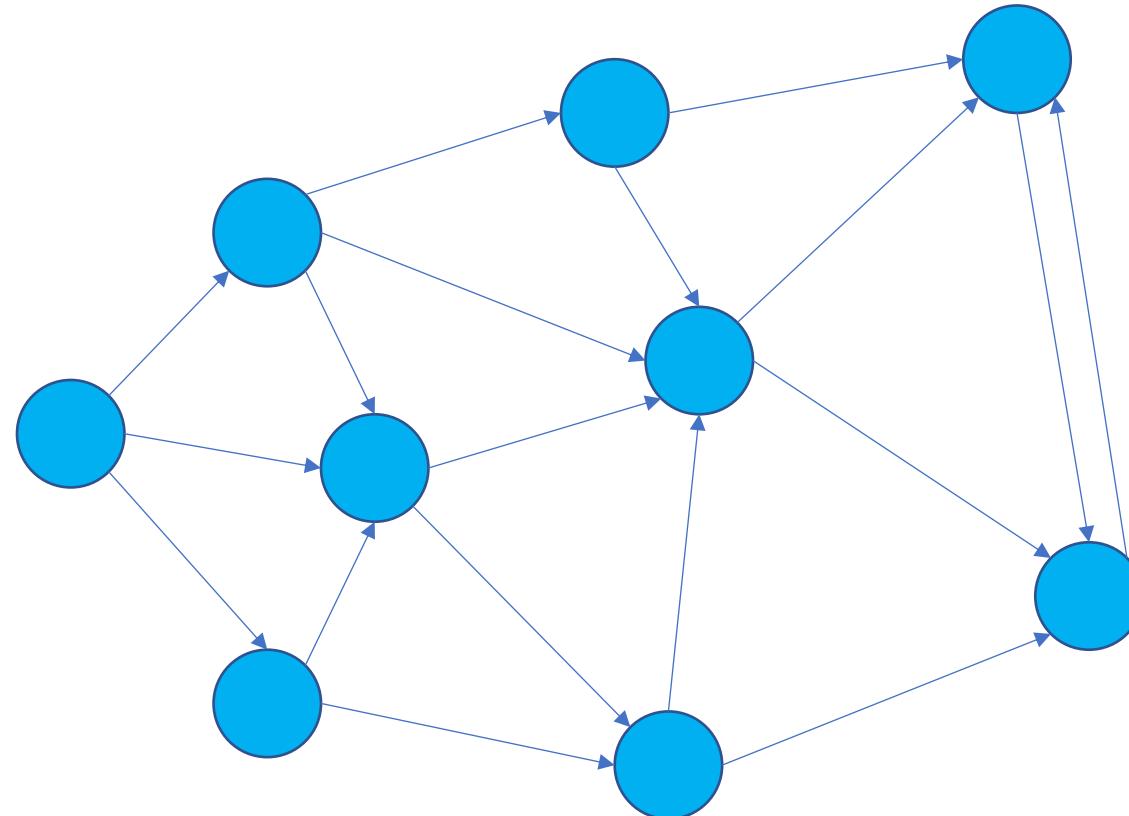


將交易送給與自己連接的電腦，若相同的交易收過就不
再收

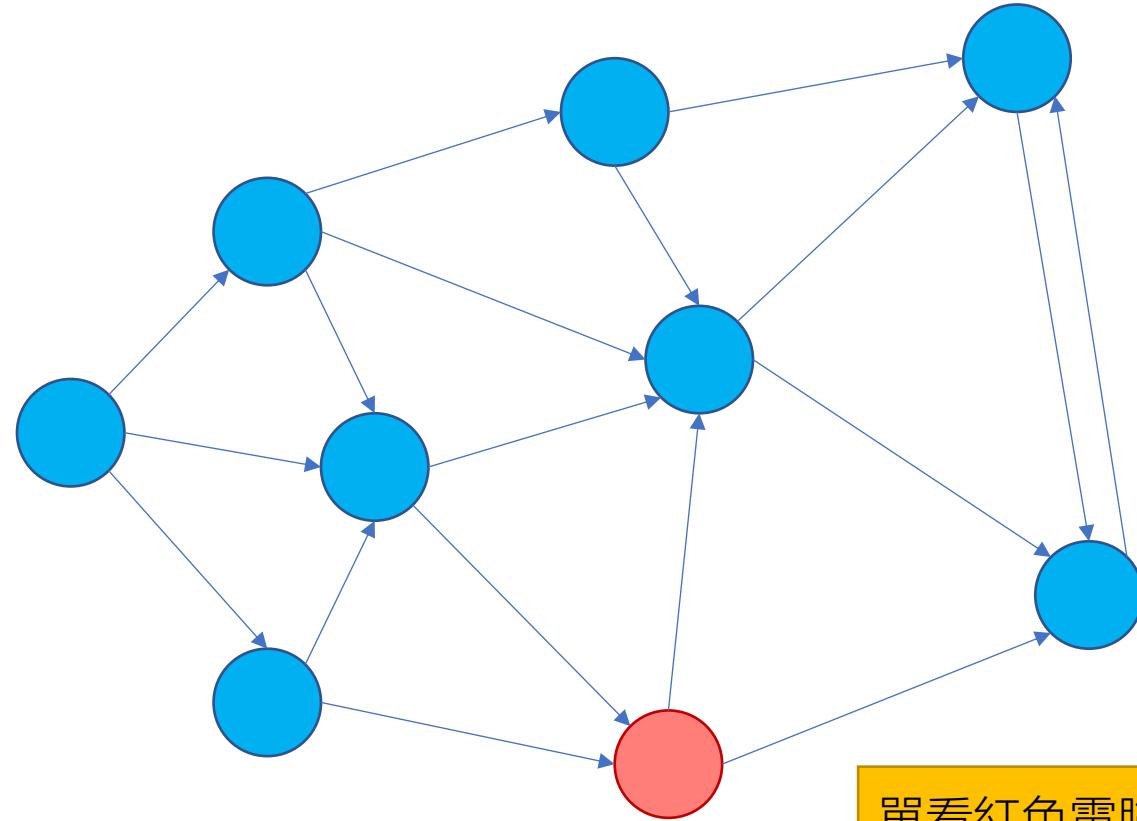
廣播交易



廣播交易



廣播交易



單看紅色電腦裡面，收到交易的情況，一般程式裡會有一塊記憶體專門收廣播來的交易

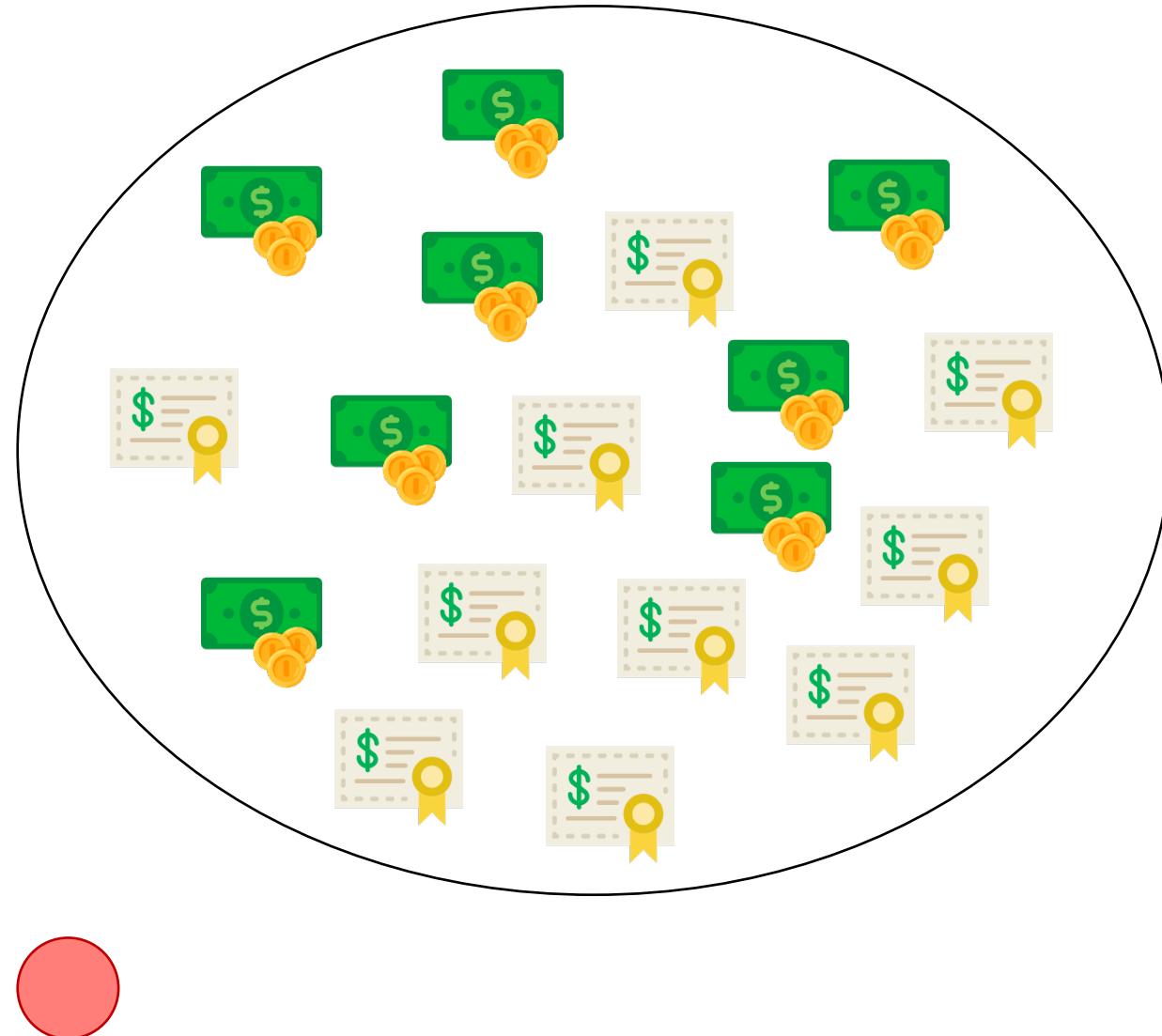
Transaction pool



標準交易

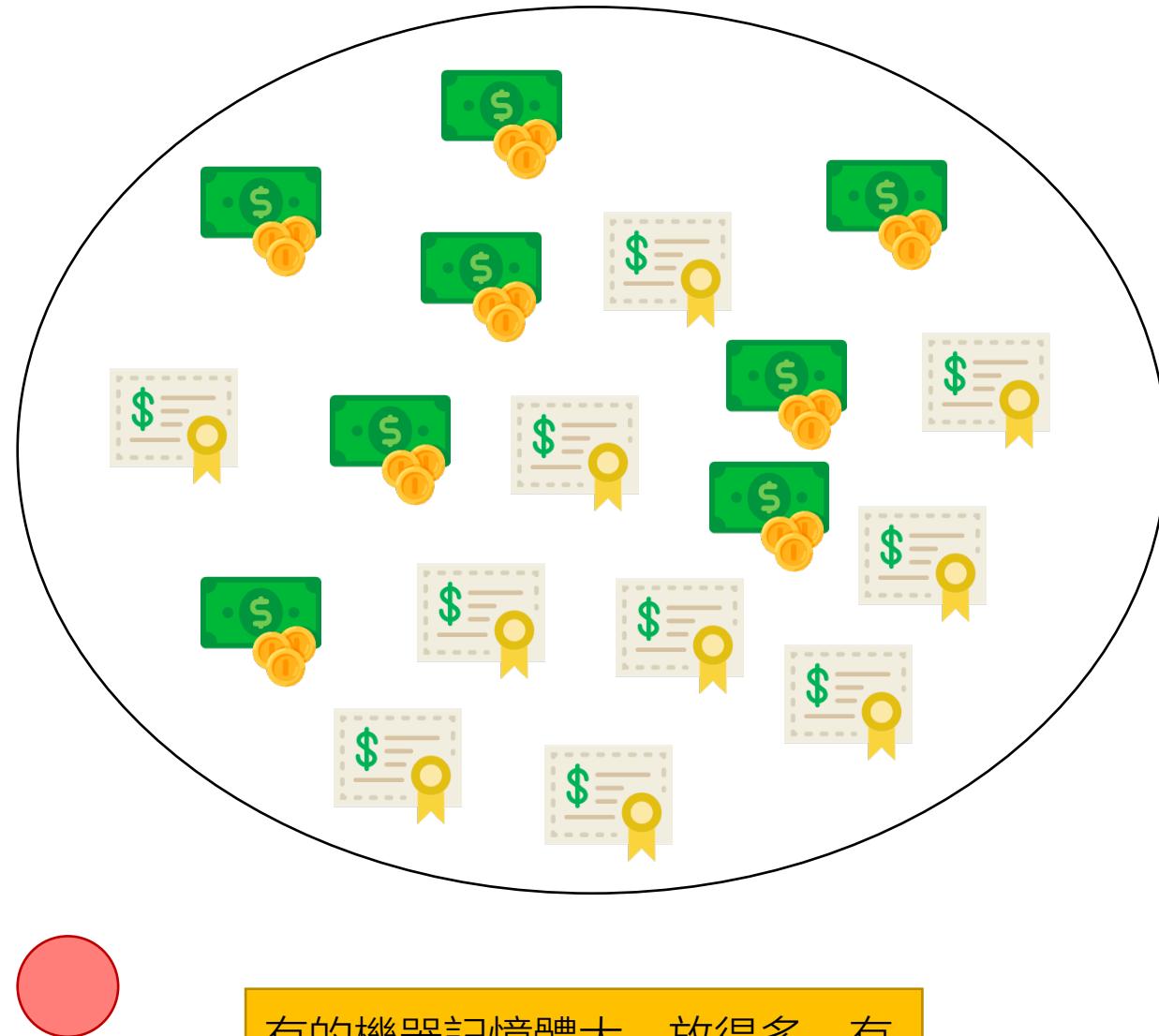


合約交易



Transaction pool

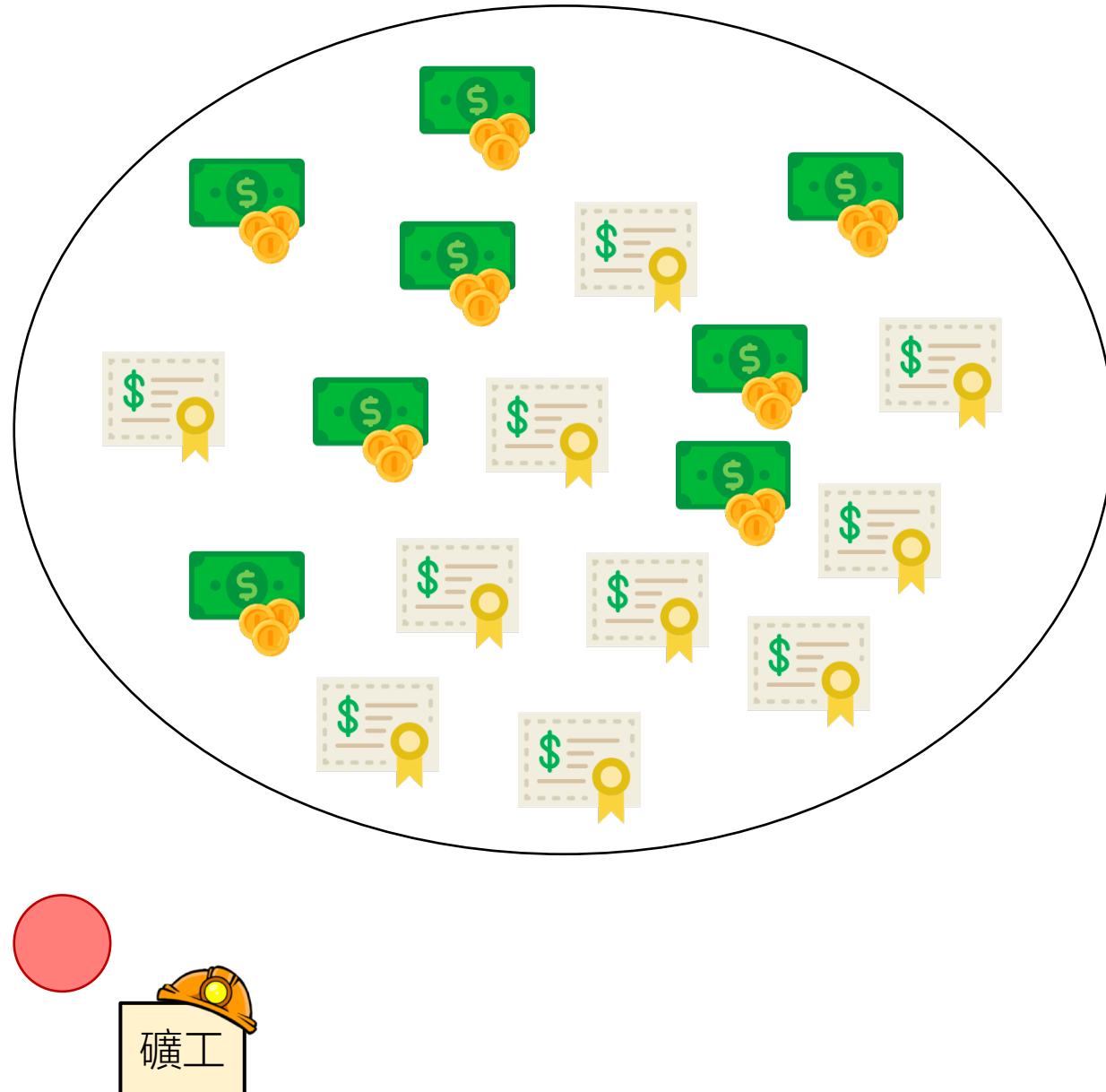
- Pending transaction
 - 等待礦工來確認並完成交易



有的機器記憶體大，放得多，有的放得少，所以不是大家 txpool 都具有相同的 view

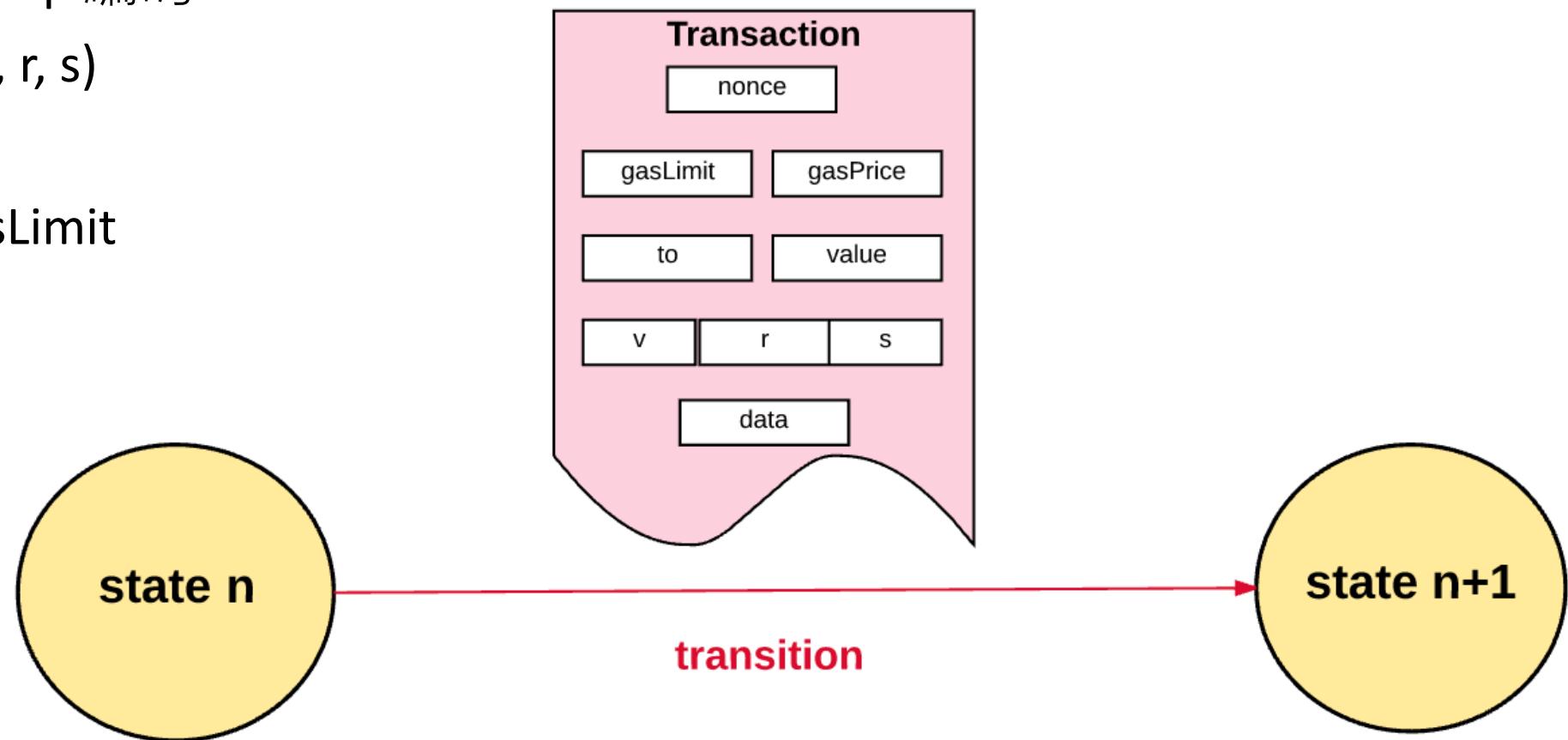
打包規則

- Pending transaction
 - 等待礦工來確認並完成交易
- 紳工怎麼挑？
 - 區塊有容量限制，怎麼挑對我划算？
 - 可以挑多少個？
 - 交易是正確的 rlp 編碼？
 - 有效的簽名 (v, r, s)
 - 有效的 nonce
 - $\text{gasUsed} \leq \text{gasLimit}$



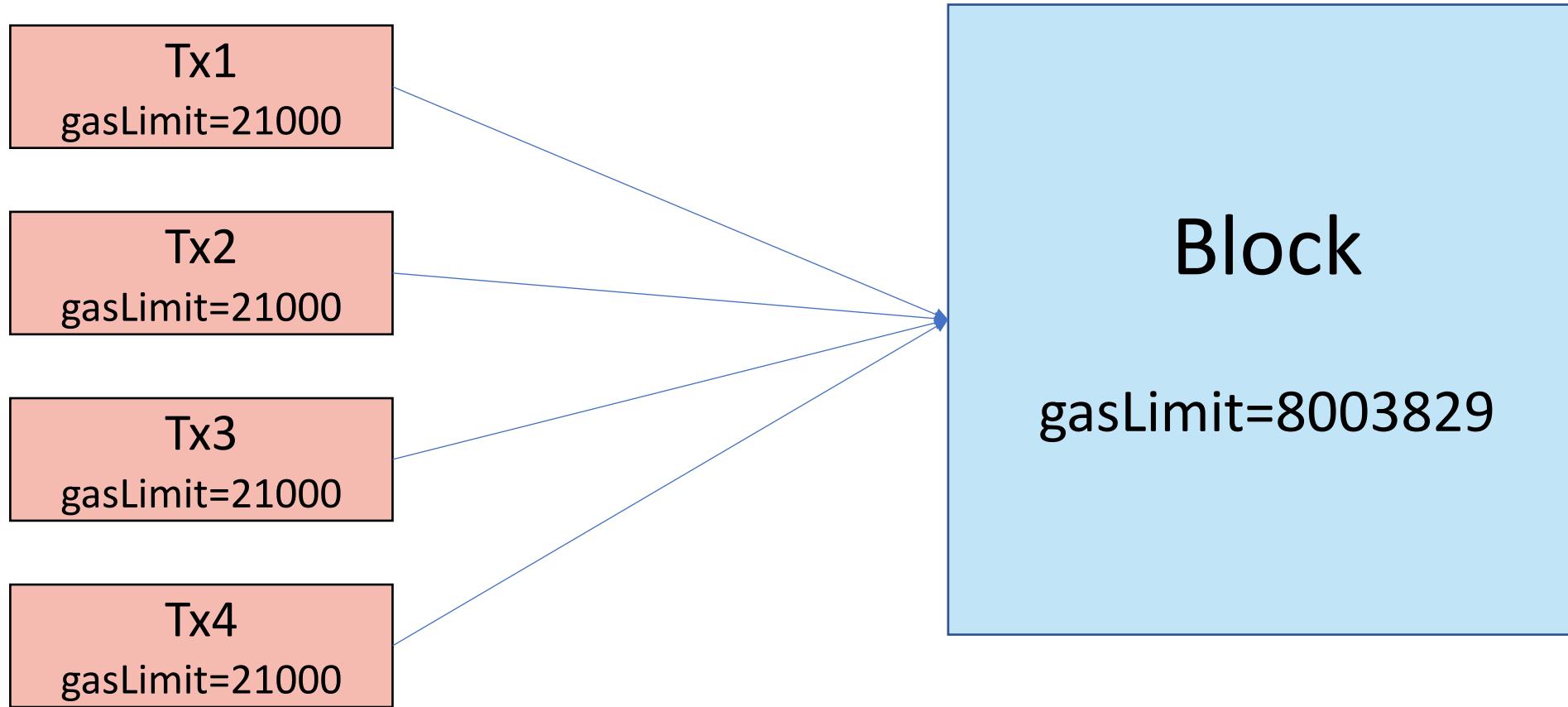
Transaction Execution

- 交易是正確的 rlp 編碼
- 有效的簽名 (v, r, s)
- 有效的 nonce
- $\text{gasUsed} \leq \text{gasLimit}$



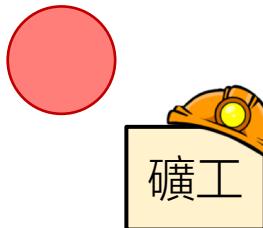
Block & gasLimit

Block 可容納的交易最大數不可超過 Block 的 gasLimit
ex: $8003829/21000 \approx 381$



打包規則

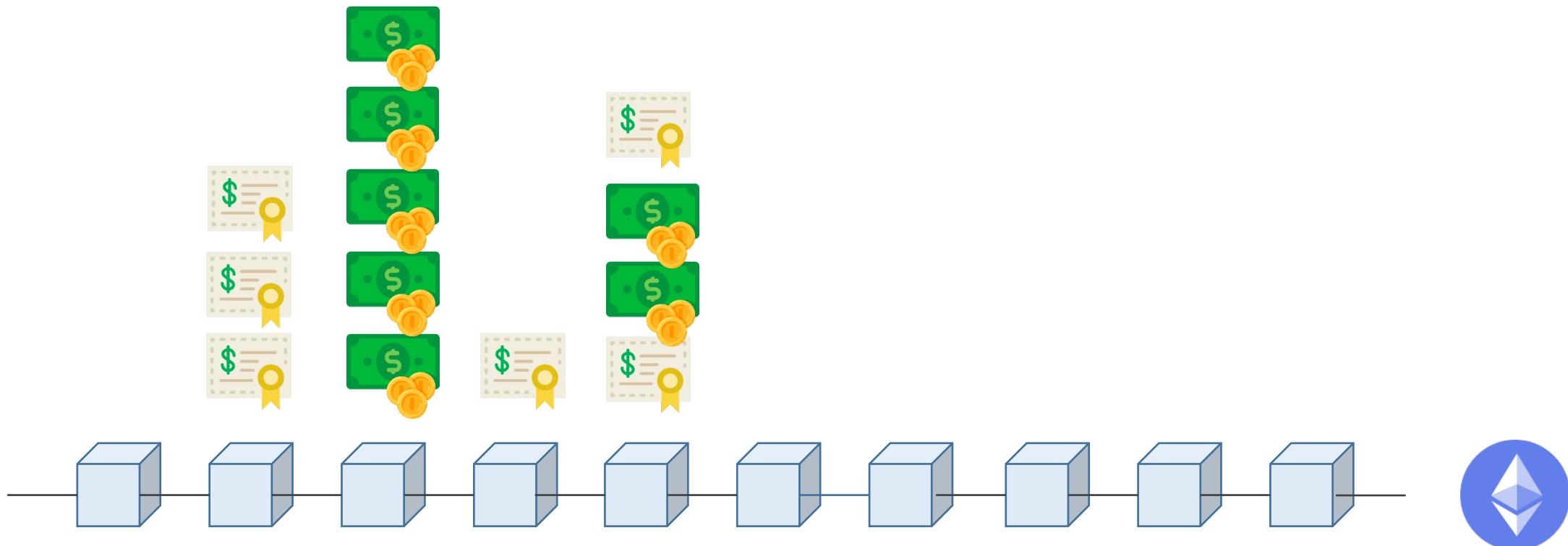
- Pending transaction
 - 等待礦工來確認並完成交易
- 紳工怎麼挑？
 - 區塊有容量限制，怎麼挑對我划算？
 - 可以挑多少個？
 - 如果交易簽名或內容有錯，要捨棄



礦工要把區塊塞滿，他的自由
礦工不想放任何交易，他的自由
礦工任意挑交易，他的自由
只要他能夠解 PoW，挖到礦

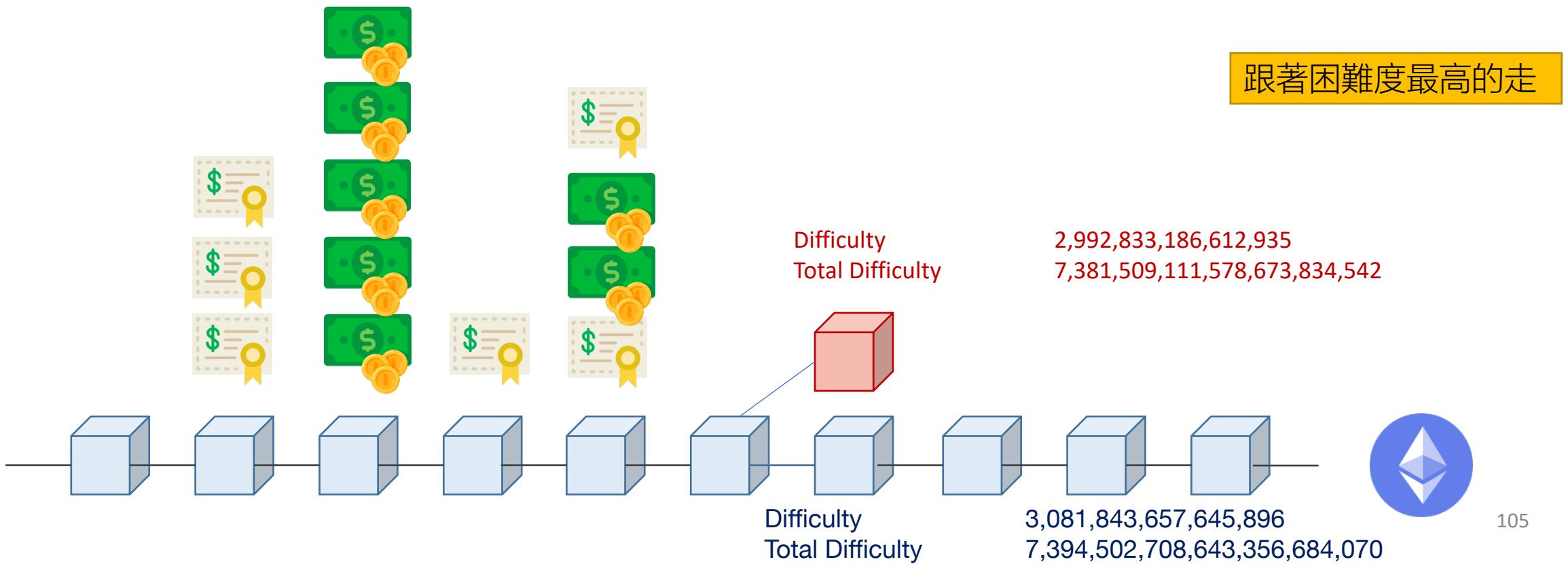
交易被打包入塊

- Transaction (status: Success)



分叉

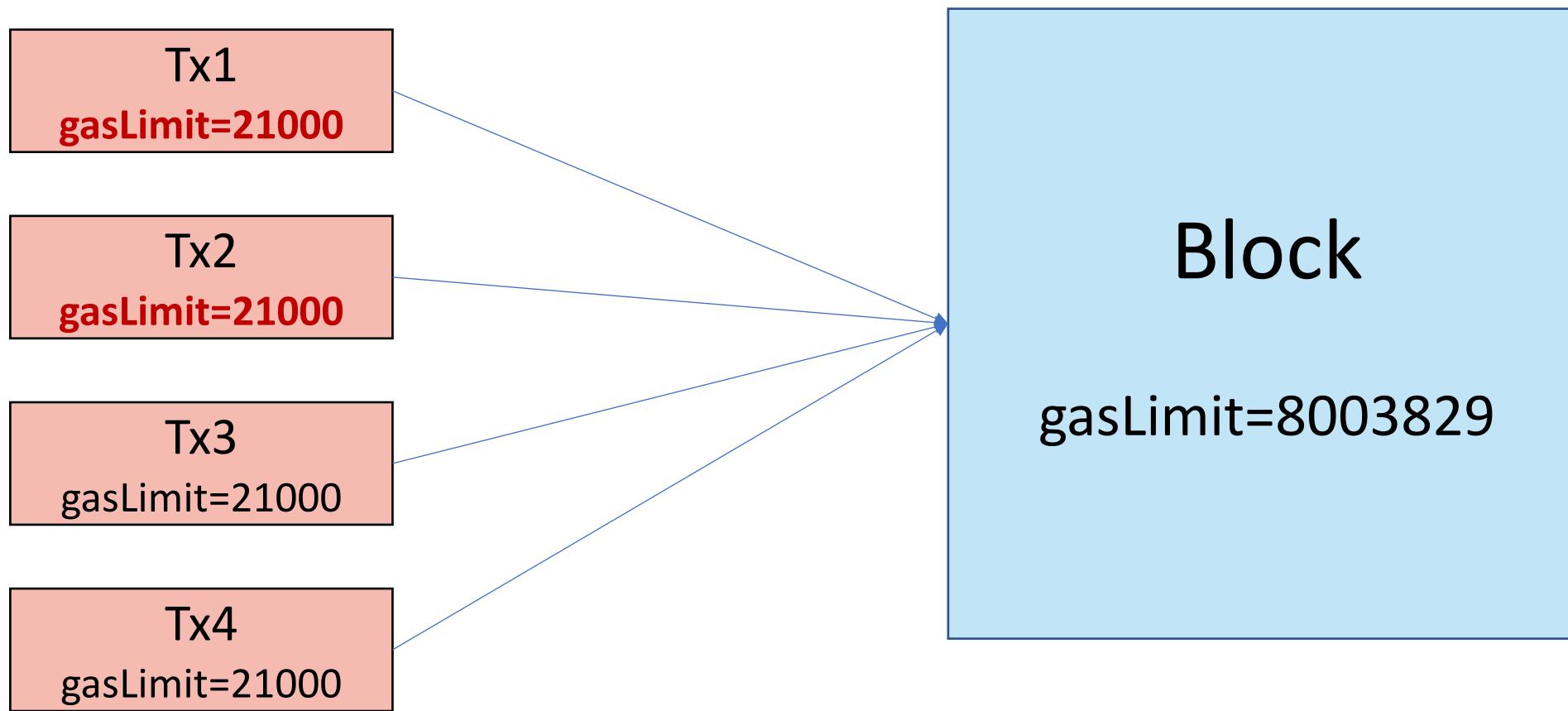
- Transaction (status: Success)



Fork



Block & gasLimit

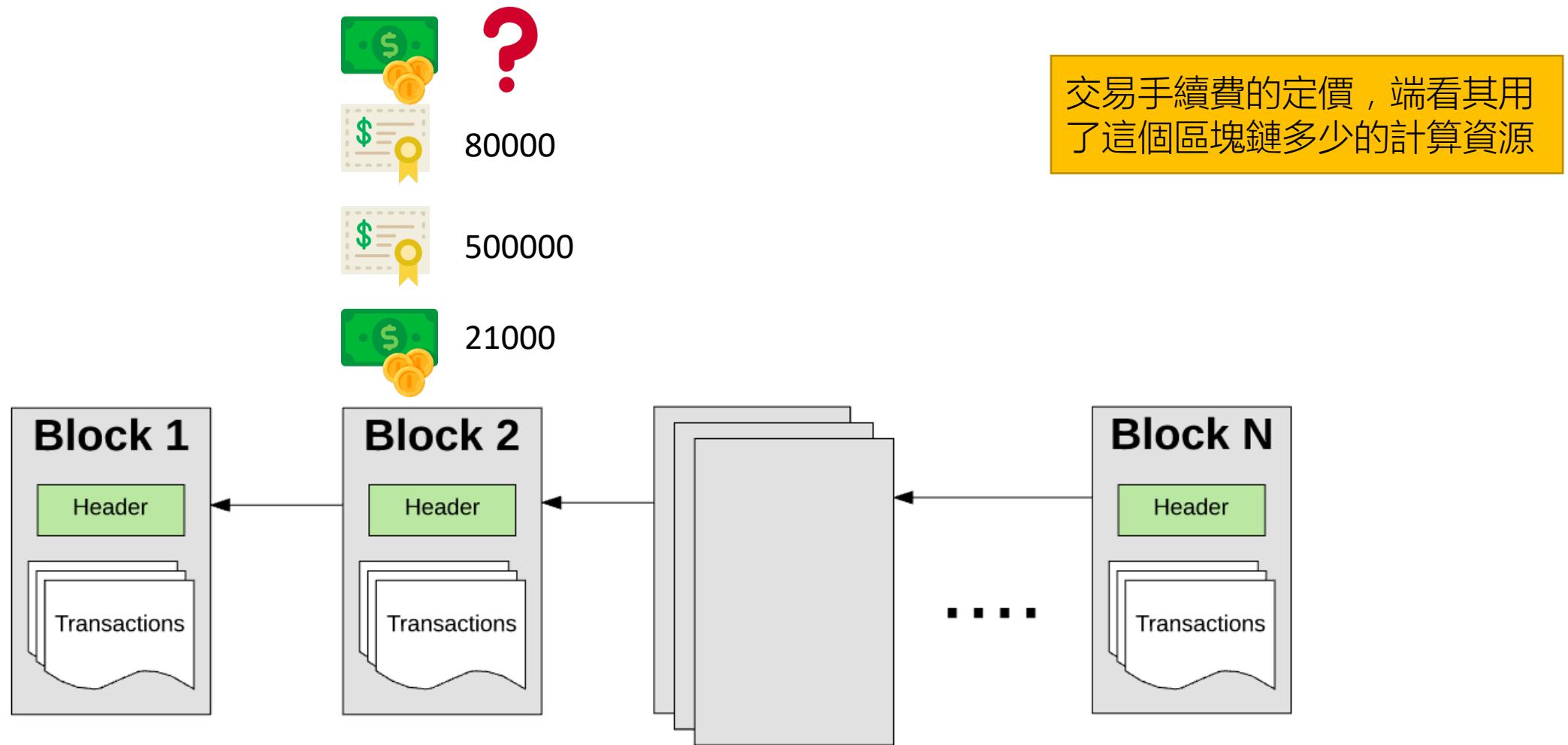


計算單價 (gas)

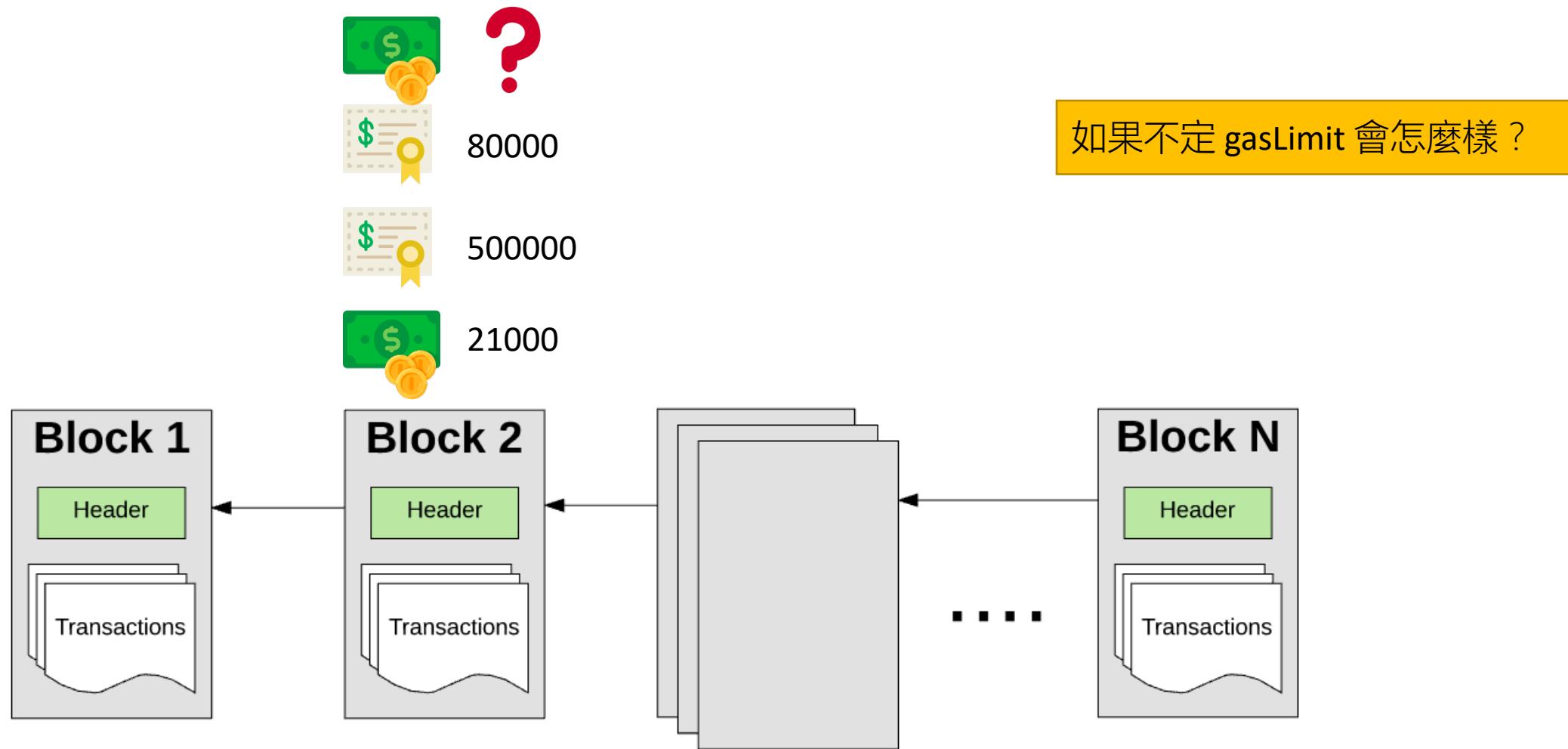
1+2=3

value	mnemonic	price	description
0x00	STOP	0	Halts execution.
0x01	ADD	3	Addition operation.
0x02	MUL	5	Multiplication operation.
0x03	SUB	3	Subtraction operation.
0x04	DIV	5	Integer division operation.
0x05	SDIV	5	Signed integer division operation (truncated).
0x06	MOD	5	Modulo remainder operation.
0x07	SMOD	5	Signed modulo remainder operation.
0x08	ADDMOD	8	Modulo addition operation.
0x09	MULMOD	8	Modulo multiplication operation.
0x0a	EXP	(exp == 0) ? 10 : (10 + 10 * (1 + log256(exp)))	Exponential operation.
0x0b	SIGNEXTEND	5	Extend length of two's complement signed integer.
0x10	LT	3	Less-than comparison.
0x11	GT	3	Greater-than comparison.
0x12	SLT	3	Signed less-than comparison.
0x13	SGT	3	Signed greater-than comparison.
0x14	EQ	3	Equality comparison.
0x15	ISZERO	3	Simple not operator.

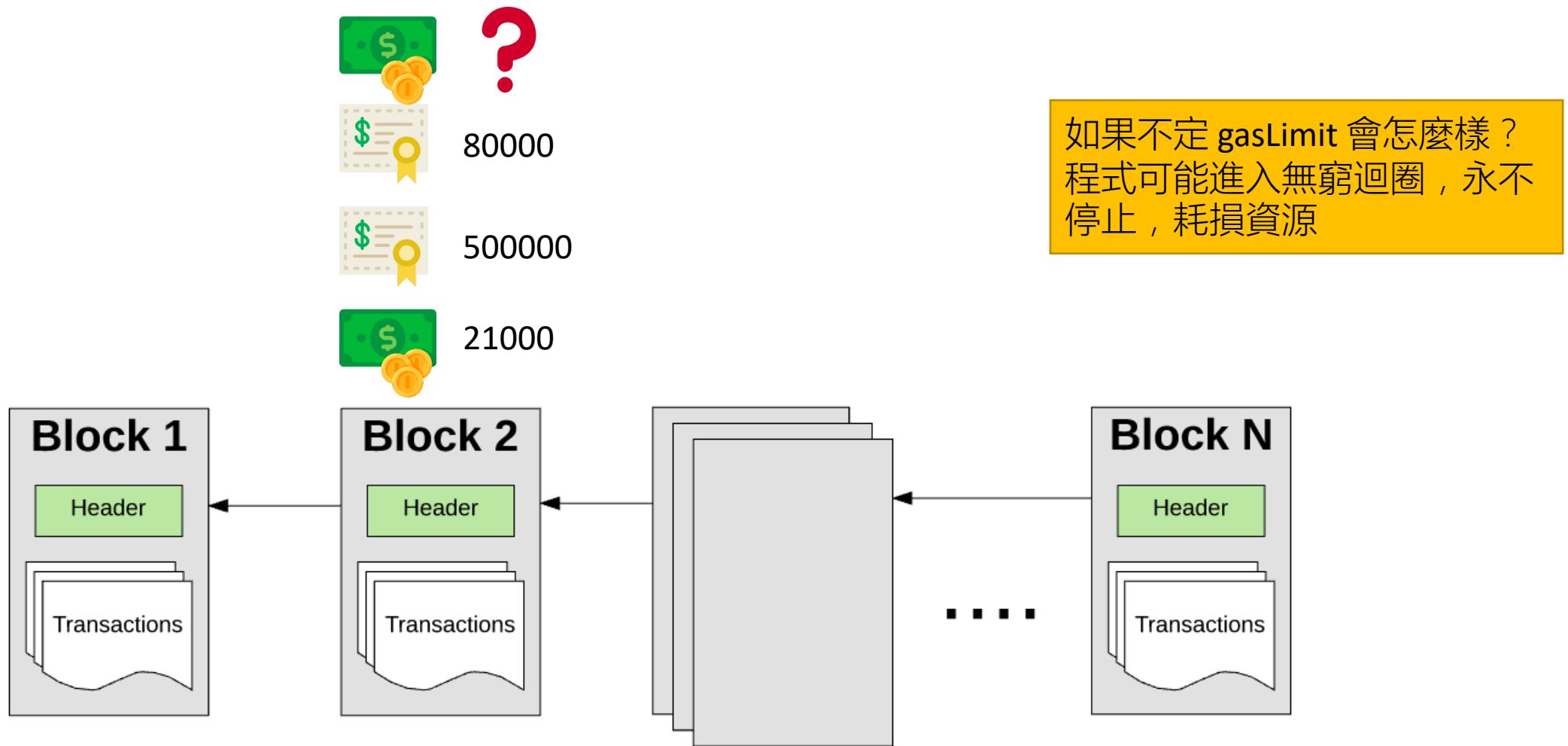
gasLimit



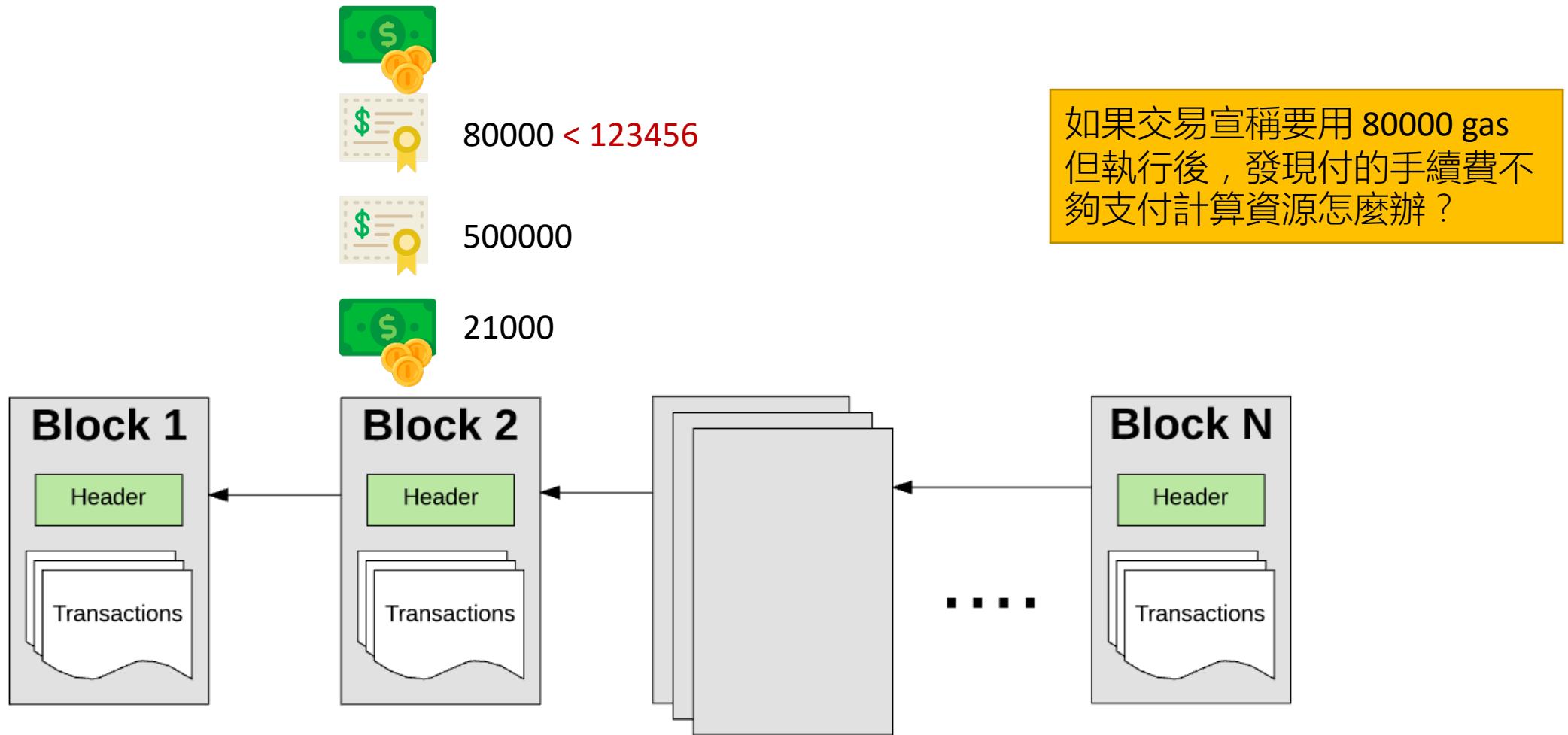
gasLimit



gasLimit



gasLimit



Gas & fee

- gas limit: 50000
- gas price: 20gwei

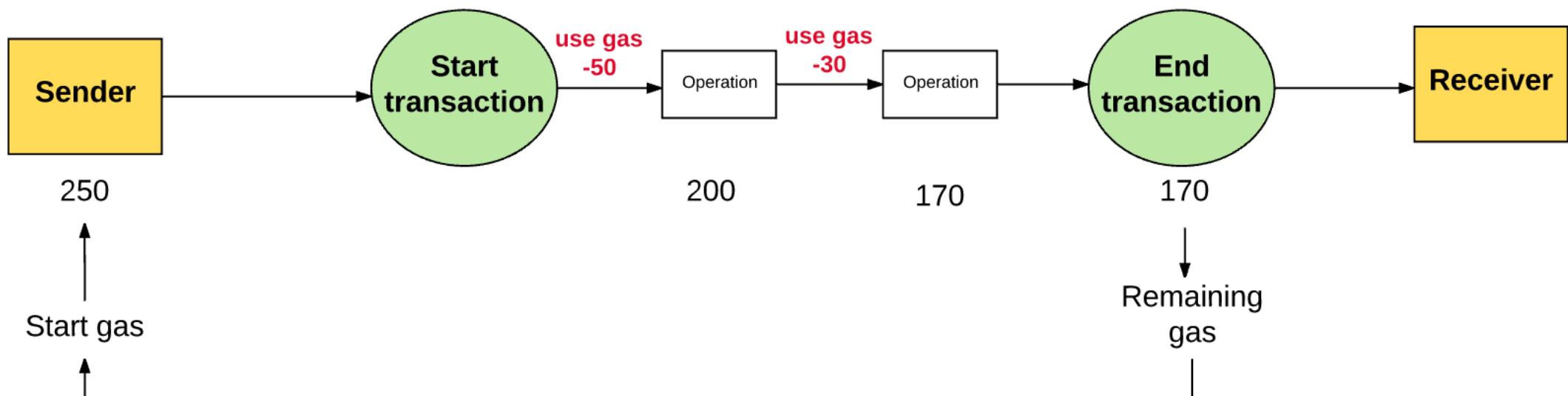
$$\begin{array}{c|c|c} \text{Gas Limit} & \times & \text{Gas Price} \\ 50,000 & & 20 \text{ gwei} \\ \hline & = & \text{Max transaction fee} \\ & & 0.001 \text{ Ether} \end{array}$$

單位

Transaction execution

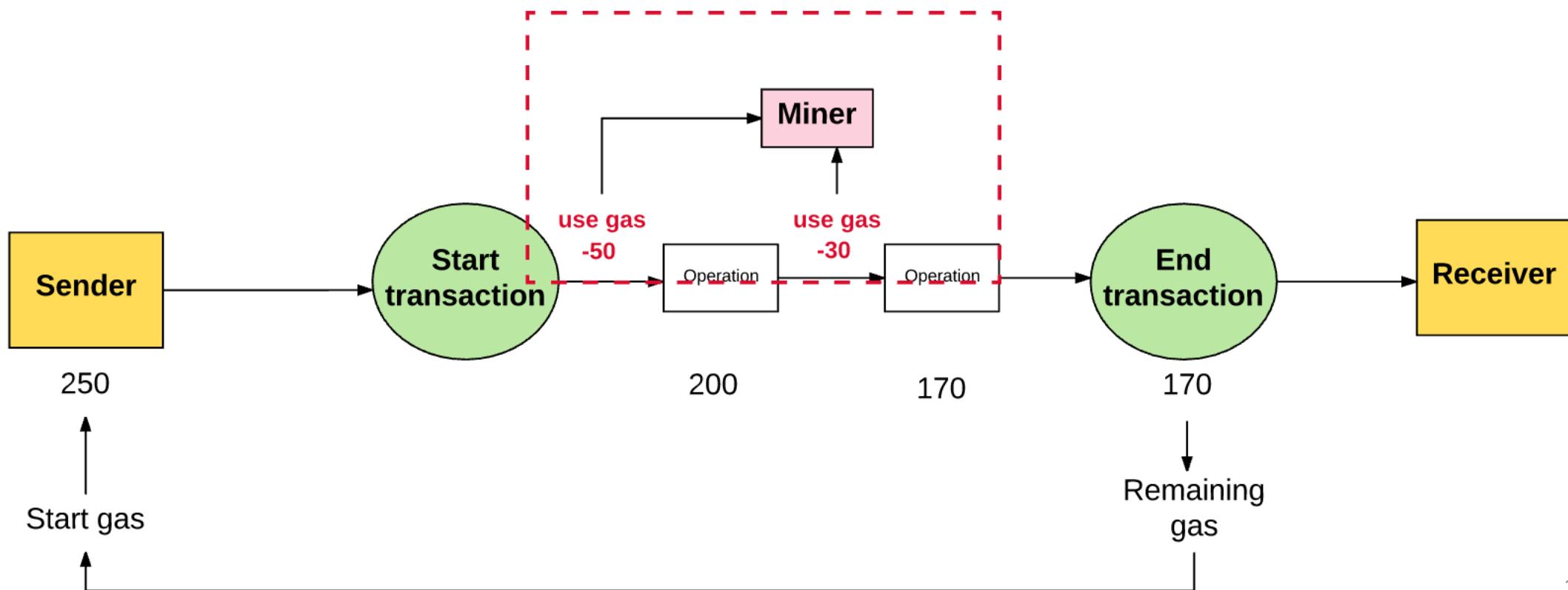
ex: $1+2=3$

Add
Equal

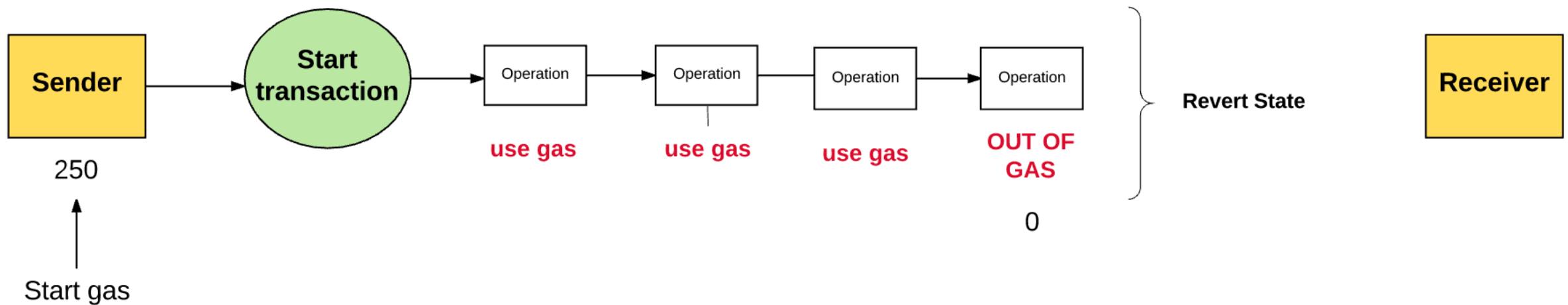


Fee

- Beneficiary address, which is the miner's address



Out of gas



Out of gas

Overview	Comments
Transaction Information	
TxHash:	0x71e3cdd6c9f393655f19cf820d454300aa9ffdbf6b290ff3aad402273208bed4
Block Height:	4154614 (1266212 block confirmations)
TimeStamp:	240 days 10 hrs ago (Aug-14-2017 12:09:03 AM +UTC)
From:	0x9c67e141c0472115aa1b98bd0088418be68fd249 (HitBtc)
To:	Contract 0x03985e1e158e28192ec2b37e6e598d30f386574c ⚠ ... Warning! Error encountered during contract execution [Out of gas] ☹
Value:	20.10635272 Ether (\$8,373.29) - [CANCELLED] ⓘ
Gas Limit:	21026

Ether & Gas

- Ether: 原生貨幣
- Gas: 工作單位
- 以太坊上的“交易”像是執行一段小程序，這段程式會幫忙驗證“錢是否正確被轉出去”
- 因為是一段小程序，需要大家(礦工)幫你驗證，為了不失公平性，gas 是這段小程序需要耗費的工作量
- 因為礦工不是無償幫忙驗證，需要收點手續費

Ether & Gas

- 驗證一筆交易需要耗費工作量, 而 gas 是工作量的最小單位,
- 計價公式
 - 工錢(手續費) = 工作量 \times 每單位的計價
- 假設 $\text{gasPrice} = 0.00000001 \text{ Ether} = 10\text{gwei}$ (每單位的計價)
- 假設交易總耗費 21000 gas (工作量)
- 手續費
 - $21000(\text{gas}) * 0.00000001(\text{Ether/gas}) = 0.00021 \text{ Ether}$ (手續費)
 - 按匯率算, 若 Ether ≈ 400 USD, $0.00021 * 400 = 0.084$ USD (手續費)
- 若指定的 gas 量太少 ?
- 若 gasPrice 太低會如何 ?

Ether & Gas

- Ether: 是貨幣單位
- Gas: 是工作量的計價單位
- 那為什麼有 Ether , 還要定義 gas ? 還有 gasPrice ?
 - 因為如果不把兩個參數解耦 , 當 Ether 大漲時 , 手續費會變得不合理

Gas Limit (startgas)

- 每筆交易在執行後會耗費工作量 (gasUsed)
- 在使用者提交交易前，需要設定 gasPrice 與 gasLimit
- 假設設定 gasLimit=35000，但實際用量 gasUsed=21000 (程式真正消耗的工作量)
- 這個 gasLimit 是個系統保護機制，因為在電腦科學上，很難保證或衡量一段程式，執行後一定會終止，如果不能終止就會造成電腦卡住。又或是如果駭客發現一個漏洞，本來一段程式碼是在做轉錢的動作，因為沒有設定終止的條件，最終可被利用將錢無止盡的轉出
- 假設 21000 的工作量是將你的錢轉出 5 ETH，假設想再次轉帳 5 ETH，第二次會被擋下，因為需要額外 21000 的工作量，因為起初指定的 gasLimit 只有 35000。(實際上轉兩次 5 ETH 的工作量很小，這裡只是舉例)

Gas Limit (startgas)

- 如果交易在執行過程，耗費的工作量超過指定的 `gasLimit=35000`
- 這筆交易會視為無效，並回復到之前的狀態
- 另外，礦工會收走手續費， $35000(\text{gas}) * 0.00000001(\text{Ether/gas}) = 0.00035 \text{ Ether}$
- 錯誤訊息: **transaction is out of gas**

Ether & Gas

- 手續費: $(\text{startgas} - \text{gas_remaining}) * \text{gasprice}$
- `gas_remaining`: 退回給使用者
- 基本的轉帳交易: 21000 gas
- 複雜的合約交易會用掉較多 gas
- 一筆交易的 `gasLimit` 可能會接近一個 Block 的 `gasLimit`
- 但是若交易的 `gasLimit` 高於 Block 的 `gasLimit`，則該交易不會進到區塊

Transaction pool

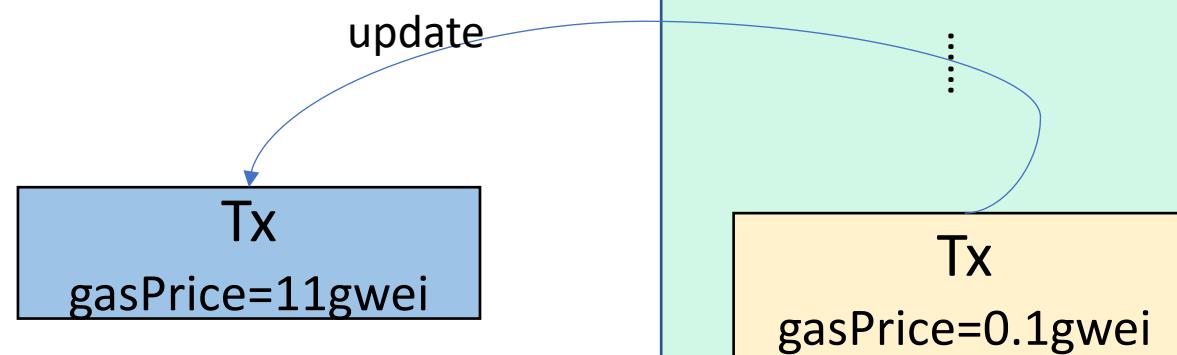
- Pending transaction
 - 等待礦工來確認並完成交易



手續費太少，礦工都不理怎麼辦？

交易卡住

- 交易使用過低的 gasPrice，造成交易無法被打包
- 解決
 - 重新送出原交易，調整 gasPrice 欄位
 - 手續費必須高於原交易手續費的 10%
- [x] 10GWei → 10.5GWei
- [o] 10GWei → 11GWei



Transaction pool

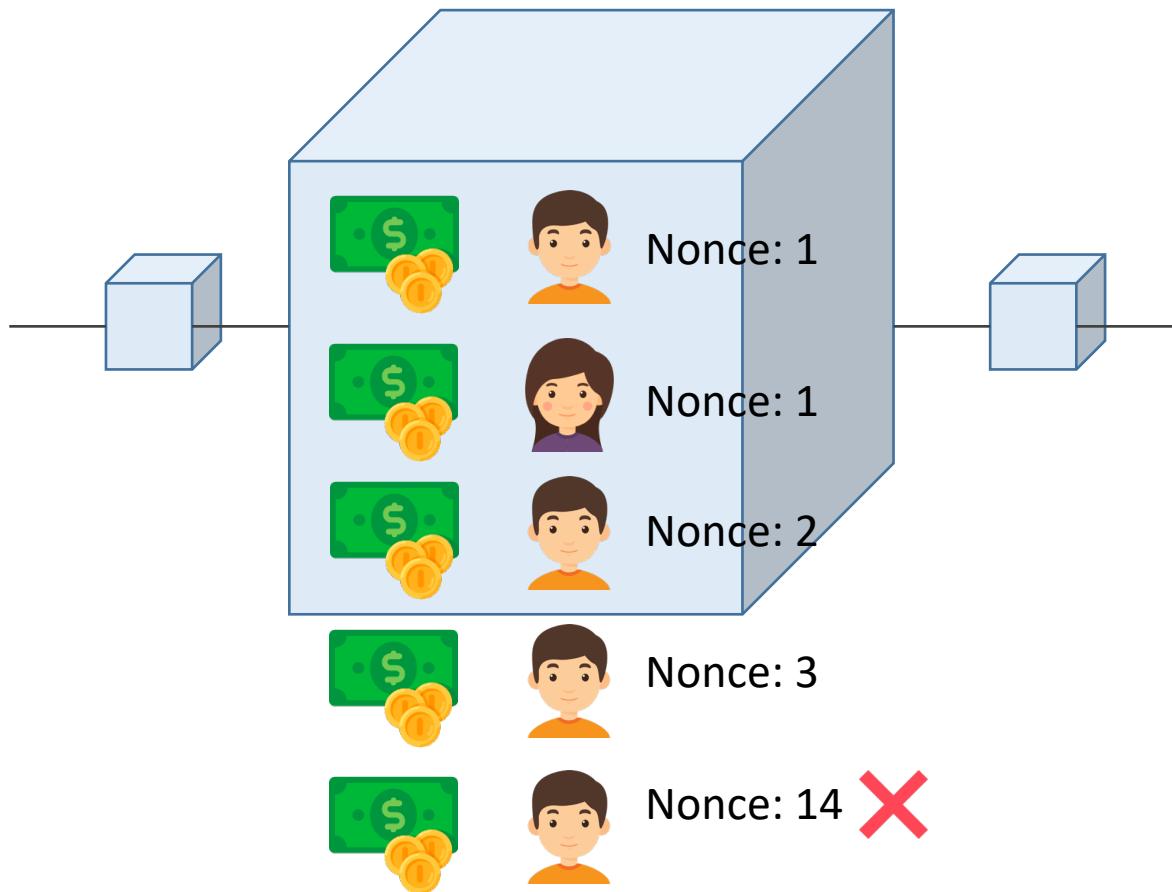
Tx
gasPrice=20gwei

Tx
gasPrice=15gwei

Tx
gasPrice=10gwei

Tx
gasPrice=0.1gwei

nonce

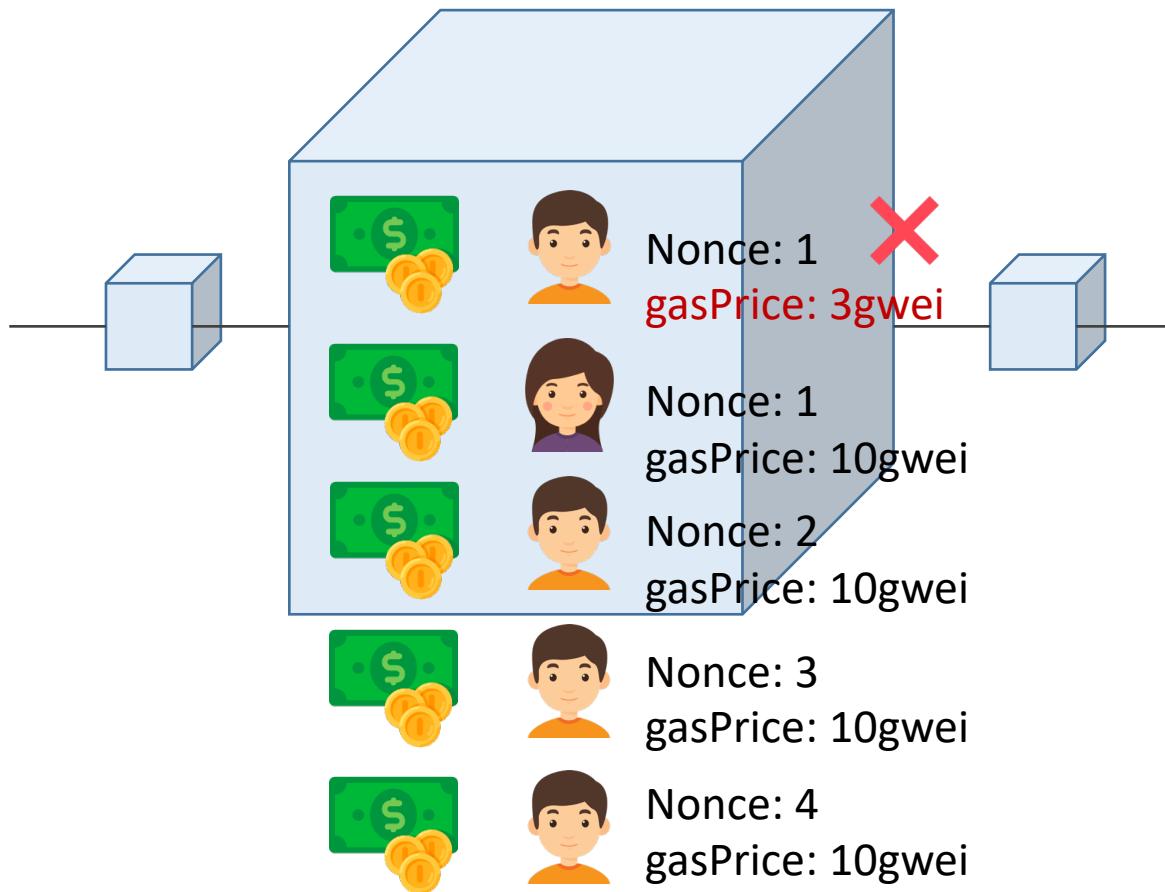


假設礦工挑了 5 筆交易
礦工執行交易時會有一個順序

同一個帳號，交易的執行順序跟
nonce 有關，一定要遞增且連號執行

nonce

假設目前網路上礦工平均收交易的手續費
gasPrice: 10gwei



同一個帳號，交易的執行順序跟
nonce 有關，一定要遞增且連號執行

如果 nonce 1 的手續費不提高
後面的交易是會被卡住的

<https://ethgasstation.info/>

ETH Gas Station | Consumer

Estimates over last 1,500 blocks - Last update: Block 6569245

Change Currency

Std Cost for Transfer: \$0.017 | Gas Price Std (Gwei): 4.1 | SafeLow Cost for Transfer: \$0.015 | Gas Price SafeLow (Gwei): 3.6 | Median Wait (s): 31 | Median Wait (blocks): 2

Gas-Time-Price Estimator: For transactions sent at block: 6569245

Adjust confirmation time

Avg Time (min)	260.11	Gas Used*	21000
95% Time (min)	650.28	Avg Time (blocks)	1000
Gas Price (Gwei)*	4.1	95% Time (blocks)	2500
Tx Fee (Fiat)	\$0.017	Tx Fee (ETH)	0.00009

Real Time Gas Use: % Block Limit (last 10)

Last Block: 6569245

Transaction Count by Gas Price

Confirmation Time by Gas Price

Recommended Gas Prices (based on current network conditions)

Speed	Gas Price (gwei)
SafeLow (<30m)	3.6
Standard (<5m)	4.1
Fast (<2m)	20

Note: Estimates not valid when multiple transactions are batched from the same address or for transactions sent to addresses with many (e.g. > 100) pending transactions

Misc Stats (Last 1,500 blocks)

Main Page | Tx Calculator | TxPool Vision | Low Gas Price Watch List | Gas Burners | FAQ | External Links

<https://www.etherchain.org/api/gasPriceOracle>

<https://ethgasstation.info/json/ethgasAPI.json>

Internal transaction

