Overview

- nodes
- transcation (tx)
- Smart Contract (flexable txs, ERC20 造幣 token, ERC721 非同質化代幣 NFT)
  - read, write
  - Verfy s.c code need Flatten.
  - bytcode to EVM.

"Full node" store blockchain

→□→□→□→□→□→□→

tx

read: 1o token

write: burn 1 token

有沒有改變合約狀態？

Blockchain Award

浪費電

- Bitcoin: Proof-of-Work, H(pre_hash, tx's root, nonce) < t
- Proof-of-Stake, (tx's root) 不用 Nonce

願意放多少幣，就有多少機會賺更多幣

石破：水

1. Blockchain 中 Smart Contract 代表什麼？

   Ans. Token 表達的一種形式。

2. 為什麼要做 Flatten?

   Ans. 減少依賴，確保合約獨立運行。

3. 100% 在 POS 的機率分配，顏色相同要一樣分四已

A	B	C	D	E	F	G
7	10	11	10	15	20	3
4	14	14	14	35	25	4

使用先拆單分配

4. 為什麼省電？

   Ans. 加入質押，要過效期才可取回

   大戶(交易所)一起質押，交易所一起控

5. 隨機哪裡來(用來決定誰挖到，不可預測)

   Ans. 使用 node 產生時間毫秒值，看數值的接近

Digital Signature

1. tx generation by (address) who hold coins.

2. verification of tx really from (address)

m : msg
σ : signature

Syntax of Digital Signature.

- Gen(1^λ) → sk, vk → verification key
  sec parameter ↓ signing key
- Sig(sk, m) → σ
- Vrfy(vk, m, σ) → accept / reject

sk ⟷ vk ⟷ address

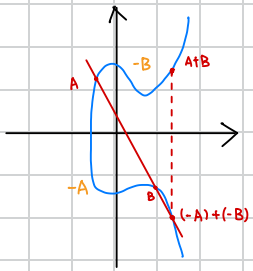
Signature
- Authentication : Verify m from S.
- Integrity : m is not modified.
- Non-repudiation : cannot withdraw the sig.

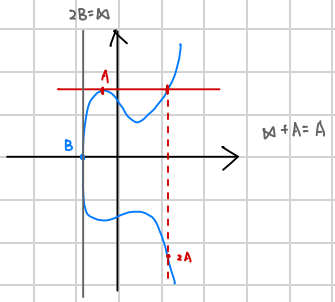
下週四考

Signature 橢圓曲線密碼學

$y^2 = x^3 + ax + b \mod P$

$x, y \in Z_p$
a, b
$\{0, \dots, P-1\}$





$y^2 = x^3 + ax + b \mod q$

P, Q : a point in E (group defind by a EC)

- P is generator $E = \{P, 2P, \dots, (q-1)P\}$
- Give a pairrt Q in E, $Q = \alpha P$

EC hardness : Give (P, Q) (public / generator), hard to find $\alpha \in Z_q$ s.t. $Q = \alpha P$

Elliptic Curve Digital Signature Algrithm (ECDSA)

- Gen(n) : Let q is a prime, E is EC over mod q
  P is the generator of E, $sk = \alpha \in Z_p$, $vk (E, q, P, Q = \alpha P)$
- Sign(sk, m) : → (σ_1, σ_2)
  1. random $r \in Z_q$
  2. compute $\sigma_1 = rP$
  3. compute $u = H(\sigma_1, \alpha P, m)$
  $\sigma_2 = r^{-1}(H(m) + \alpha \cdot u)$

  $(\sigma_1, \sigma_2) \rightarrow \sigma$
- Vrfy(vk, m, σ) : $\sigma_2(\sigma_1) = r^{-1}(H(m) + \alpha \cdot u) \cdot (rP)$
  $= (H(m) + \alpha u) P$
  $= H(m) P + u(\alpha P)$ (αP → vk)