

Tezos

宋鴻明 王皓正 徐誌鴻

2022/3/10

Outline

- Tezos 與 akaSwap 介紹
- Tezos 智能合約範例
- API (Tezos RPC, TzKT, akaSwap)

Why Tezos?

Why Tezos

1. PoS 共識機制

- PoW vs. PoS

PoW (Proove of Work) 工作量證明機制 -

解題大賽, 誰先解出來就越有機會, ex. ETH, BTC

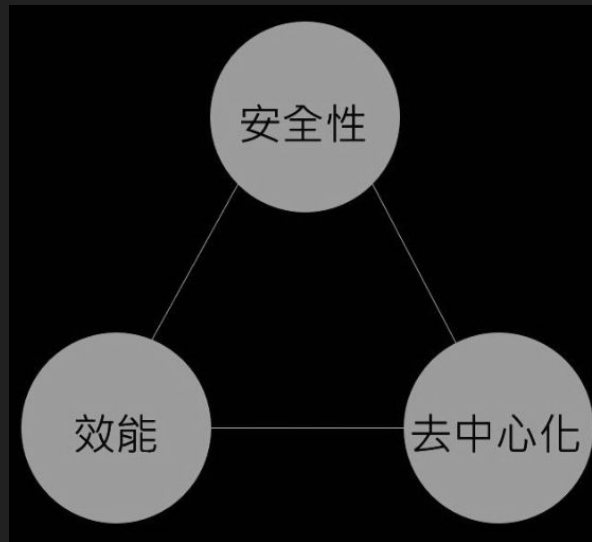
PoS (Proove of Stake) 持有量證明機制 -

彩票箱, 越大的就越多票 (8000xtz 一票)

=> 手續費低廉 (不到1台幣)

=> Energy-efficient (能源消耗約為PoW的200萬分之一)

<https://www.techbang.com/posts/93343-pow-pos-dpos>



Why Tezos

2. 自我更新機制 (Self-amendment)

- 協議升級機制

- 共同治理

提案階段



探索投票階段

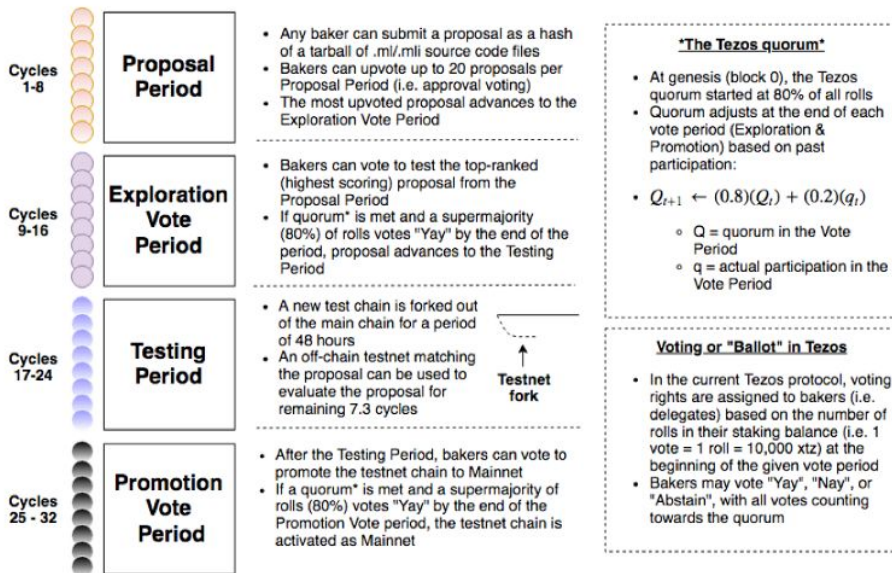


測試階段



升級投票階段

An Overview of the Tezos Governance Mechanism



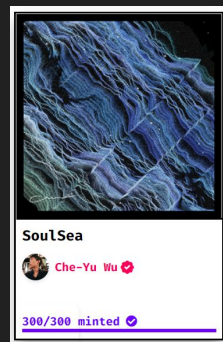
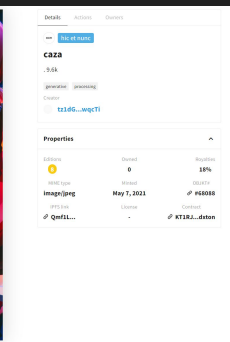
Why Tezos

3. NFT 生態系豐富

- NFT 交易平台
 - Hic Et Nunc
 - OBJKT
 - FxHash
 - akaSwap

1	 OpenSea ETH · Polygon	Marketplaces	\$96.47k	36.32k +1.69%	\$55.49M	
2	 Magic Eden SOLANA	Marketplaces	\$9.02k	31.71k -2.91%	\$15.55M	
3	 Axie Marketplace ETH · RONIN	Marketplaces	\$532.47	27.86k -14.76%	\$0	
4	 AtomicMarket WAX · EOS	Marketplaces	\$21.28k	16.56k -0.43%	\$1.14k	
5	 Radio Caca Market BSC	Marketplaces	\$0.01	4.09k -5.65%	\$0	
6	 objkt.com TEZOS	Marketplaces	\$400.49k	3.42k +16.87%	\$519.96k	
7	 Hic et Nunc TEZOS	Marketplaces	\$67.36	2.37k +5.24%	\$16.09k	
🔗 Enabling Decentralized Finance for Metaverse Join us NOW!						
8	 Paras 2.0 NEAR	Marketplaces	\$217.63k	2.34k -7.82%	\$0	
9	 NeftyBlocks WAX	Marketplaces	\$0	2.09k +8.71%	\$42.07k	
10	 Solanart SOLANA	Marketplaces	\$6.2k	1.83k -13.68%	\$235.95k	

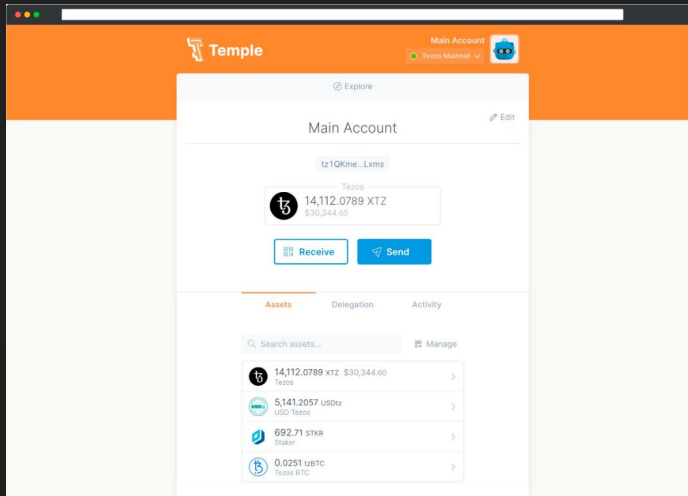
- 大咖演算藝術家
- 藝術氣息濃厚
- 社群關係緊密



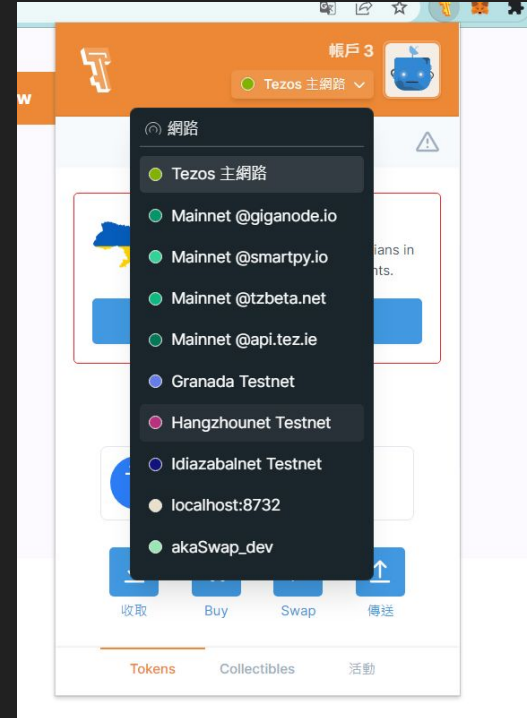
Tezos wallet - Temple

Installation: <https://templewallet.com>

XTZ Airdrop: <https://tinyurl.com/GiveMeTezos>



https://youtu.be/Kf_9WpJYnsY



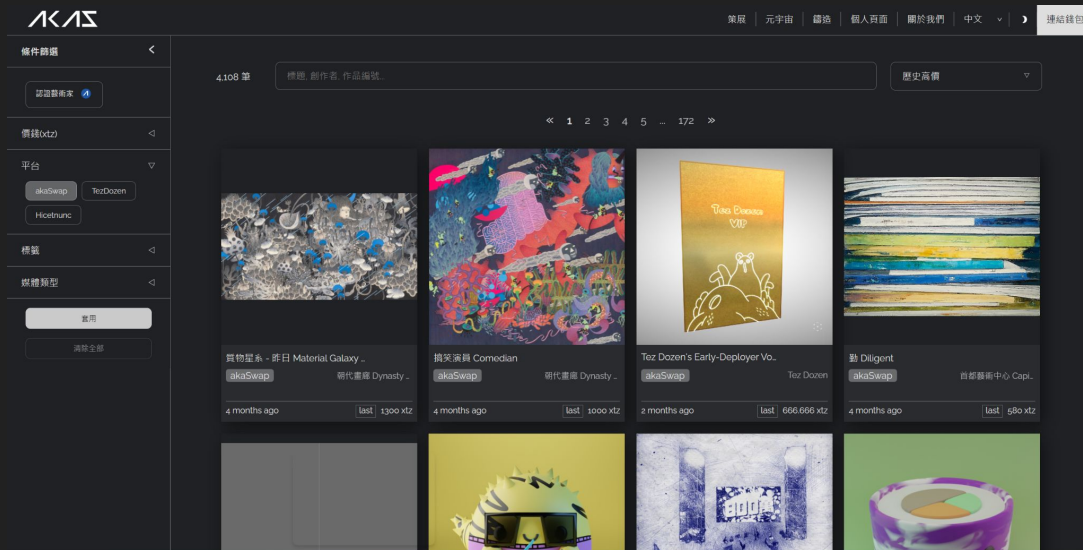
Hangzhounet Testnet 測試網

akaSwap

- 台灣唯一的 Tezos NFT 交易平台
- 知名台灣藝術家如 Aluan Wang, 川貝母, 阿爆...
- 最後賞、策展、創作者分潤...

<https://akaswap.com>

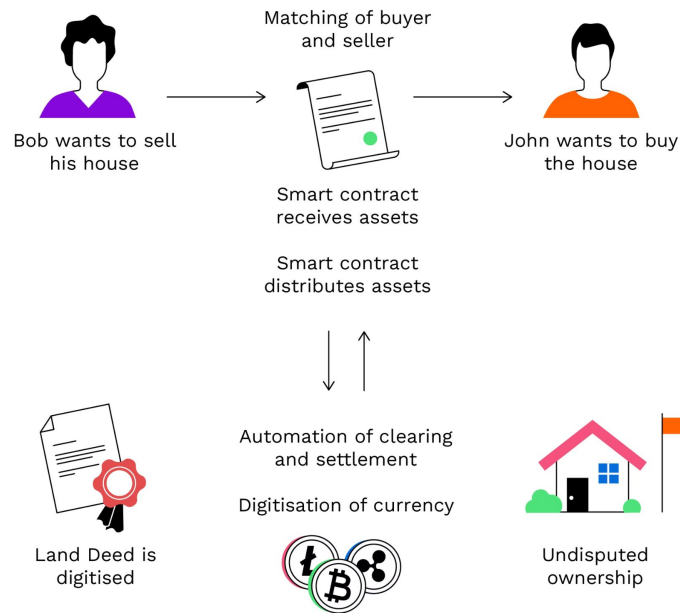
<https://testnets.akaswap.com>



Smart Contract

- Smart Contract
 - They're Not Smart And They're Not Contracts
- 智能合約
 - 其實就是一段程式碼
- Language
 - Bitcoin: (no smart contract)
 - Ethereum: Solidity
 - Solana: Rust, C, C++
 - Tezos: michelson

How a smart contract works



Interaction with Smart Contract

- Normal Transaction

- source
- destination
- amount

internal transaction APPLIED		
SENDER	DESTINATION	AMOUNT
akaMetaverse V2	tz1NgXN...S5TR	5 ₮

- Transaction to Smart Contract

- source
- destination
- amount
- parameters

transfer APPLIED		
SOURCE	DESTINATION	AMOUNT
tz1NgXN...S5TR	akaNFTContract	0 ₮
PARAMETERS		
0: 2 items		
from_: tz1NgXNo9K46BAsgFP829ZRXCkXmc7XwS5TR		
txs: 1 items		
0: 3 items		
to_: tz1hPN9mfsaASSHLjzZRYFG9vbc6oj758KgW		
token_id: 62		
amount: 10		

Tezos: michelson

```
1 storage (pair (pair (address %admin) (address %leader))
2           (pair
3             (big_map %member address
4               (pair (pair (mutez %donation) (bool %isMale))
5                     (pair (nat %lucky_number) (string %name))))
6             (pair (big_map %metadata string bytes) (mutez %min_price))));
7 parameter (or
8   (or (or (unit %add_donation) (unit %default))
9     (or
10       (pair %join_family (bool %isMale)
11         (pair (nat %luck_number) (string %name)))
12       (address %kick_member)))
13   (or (or (address %update_admin) (address %update_leader))
14     (or (pair %update_metadata (string %k) (bytes %v))
15       (or (mutez %update_min_price) (mutez %withdraw)))));
```

```
16 code { UNPAIR ;
17   IF_LEFT
18     { IF_LEFT
19       { IF_LEFT
20         { DROP ;
21           DUP ;
22           GET 3 ;
23           SENDER ;
24           MEM ;
25           IF {} { PUSH string "YOU_ARE_NOT_FAMILY" ; FAILWITH } ;
26           PUSH mutez 0 ;
27           AMOUNT ;
28           COMPARE ;
29           GT ;
30           IF {} { PUSH string "NEED_DONATION" ; FAILWITH } ;
31           DUP ;
32           GET 3 ;
33           DUP ;
34           SENDER ;
35           DUP ;
36           DUG 2 ;
37           GET ;
38           IF_NONE { PUSH int 81 ; FAILWITH } {} ;
39           UNPAIR ;
40           UNPAIR ;
41           AMOUNT ;
42           ADD ;
43           PAIR ;
44           PAIR ;
45           SOME ;
46           SWAP ;
47           UPDATE ;
48           UPDATE 3 ;
49           NIL operation }
50       { DROP ;
51         NIL operation ;
52         SENDER ;
53         CONTRACT unit ;
54         IF_NONE { PUSH int 24 ; FAILWITH } {} ;
55         AMOUNT ;
56         UNIT ;
57         TRANSFER_TOKENS ;
```



Smart Contract on Tezos

- High-level languages
 - LIGO
 - SmartPy
 - Morley/Lorentz

```
def __init__(self, admin, leader, metadata):
    self.init(
        admin = admin,
        leader = leader,
        metadata = metadata,
        member = sp.big_map(
            tkey = sp.TAddress,
            tvalue = sp.TRecord(
                name = sp.TString,
                isMale = sp.TBool,
                lucky_number = sp.TNat,
                donation = sp.TMutez
            )
        ),
        min_price = sp.mutez(1)
    )
```



```
1 storage (pair (pair (address %admin) (address %Leader))
2           (pair
3             (big_map %member address
4               (pair (pair (mutez %donation) (bool %isMale))
5                 (pair (nat %Lucky_number) (string %name))))
6             (pair (big_map %metadata string bytes) (mutez %min_price))));
```

Let's Try it!

- 合約: We are family
- Storage
 - 一位admin
 - 一位leader
 - 紀錄家人的資訊
 - 名字
 - 性別
 - 幸運數字
 - 捐款
 - 最低捐款額

- Entrypoint (function)

- 加入家庭
- 增加捐款額
- 踢除家人*
- 提領捐款*
- 更換leader*
- 更換admin**
- 更新最低捐款額**
- 更新合約資訊**

*leader或admin有權限

**僅admin權限



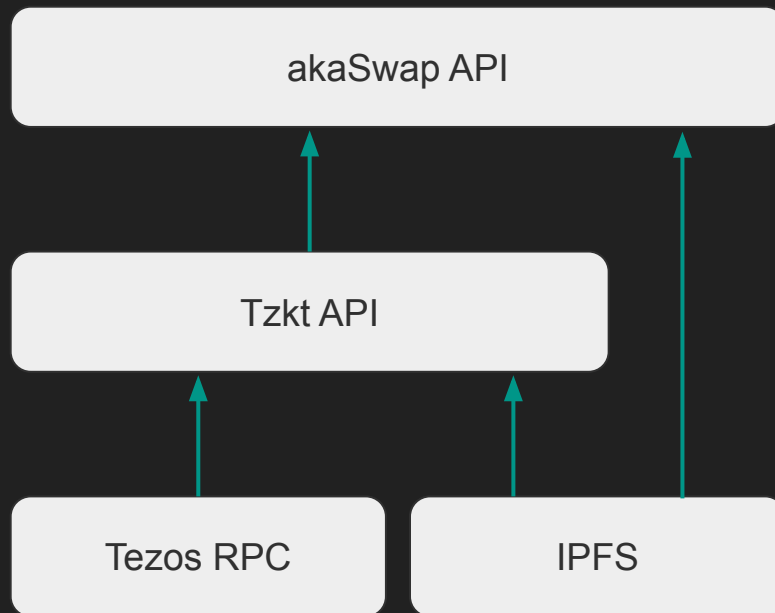
Let's Try it!

- 合約資訊
 - [metadata](#)
- 基礎
 - `sp.sender` : 呼叫人
 - `sp.amount` : 傳入金額(單位mutez)
 - `sp.verify(statement)` : 驗證statement是否成立, 否則回溯
 - `self.data.XXX` : storage中的某資料
- <https://tinyurl.com/TezosZanZan>



API

- Tezos RPC
 - Tzkt API
 - akaSwap API
-
- IPFS (InterPlanetary File System)
[Token Metadata \(akaOBJ#4587\)](#)



Tezos RPC

- 直接使用 Tezos node 提供的 RPC(Remote Procedure Call)
 - 第一手資料
 - 查詢資料較不方便
-
- 文件:
 - <https://tezos.gitlab.io/shell/rpc.html>
 - 範例:
 - <https://tezos.gitlab.io/active/rpc.html>
 - https://hangzhounet.api.tez.ie/chains/main/blocks/head/context/big_maps/178236
(/chains/<chain_id>/blocks/<block_id>/context/big_maps/<big_map_id>)

Tzkt API

- 透過 Tezos RPC 讀取鏈上資料，整理後存入資料庫
- 提供方便查詢的 API
- 文件:
 - <https://api.hangzhou2net.tzkt.io>
- 範例:
 - <https://api.hangzhou2net.tzkt.io/v1/bigmaps/178236/keys>
 - <https://api.hangzhou2net.tzkt.io/v1/contracts/KT1GbRhFAYQ6ytHytwEKoxAWNWPPhSfqNYCCc/bigmaps/member/keys>
 - <https://api.hangzhou2net.tzkt.io/v1/operations/transactions?target=KT1GbRhFAYQ6ytHytwEKoxAWNWPPhSfqNYCCc>

akaSwap API

- 透過 Tzkt API 讀取鏈上資料, 整理後存入資料庫
- 整合相關資訊 (如: 交易價格、時間)
- 文件:
 - <https://akaswap.com/api/v2/doc/index.html>
- 範例:
 - <https://akaswap.com/api/v2/fa2tokens/KT1AFq5XorPduoYyWxs5gEyrFK6fVjJVbtCj/4587>

Demo

- 利用 akaSwap API 查詢作品擁有者

感謝大家