

Tezos

smart contract and web dapps sample

2023/3/22

Outline

- Tezos 與 akaSwap 介紹
- Tezos 智能合約範例
- Web dapps 範例

Why Tezos?

Tezos 於 2018 年正式上線，為凝聚全球開發者與藝術創作者的著名區塊鏈Tezos 採用綠色節能的 LPoS 演算法，擁有無縫更新區塊鏈協議的先進機制，吸引如嬌蘭(Guerlain)、育碧(Ubisoft)、GAP 等國際大型企業相繼使用，並且受大量藝術工作者青睞，包括Teia、objkt、fxhash、akaSwap 等平台在內，持續發展出蓬勃且橫跨鏈上鏈下的成熟生態系。



實現去中心化群眾治理

用戶可透過提案和投票參與決策，不斷將 Tezos 與最新科技接軌

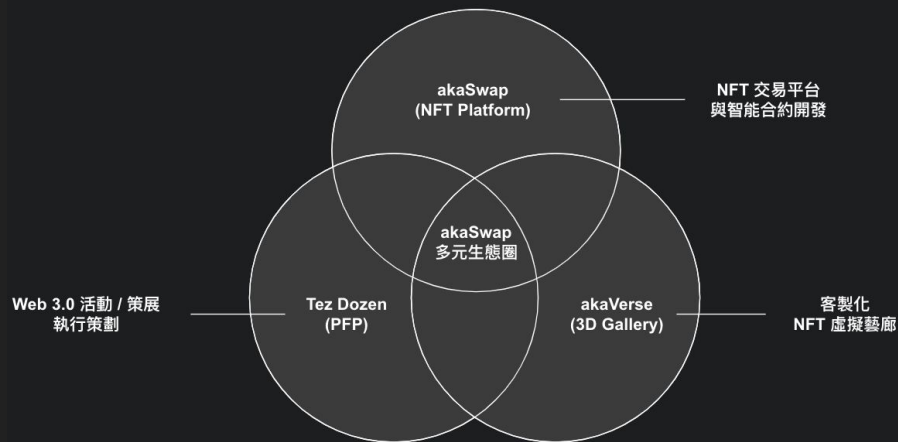
無縫，無分叉，無中斷的升級能力

Tezos 採用自我更新協議機制，定期於區塊速度、功能升級

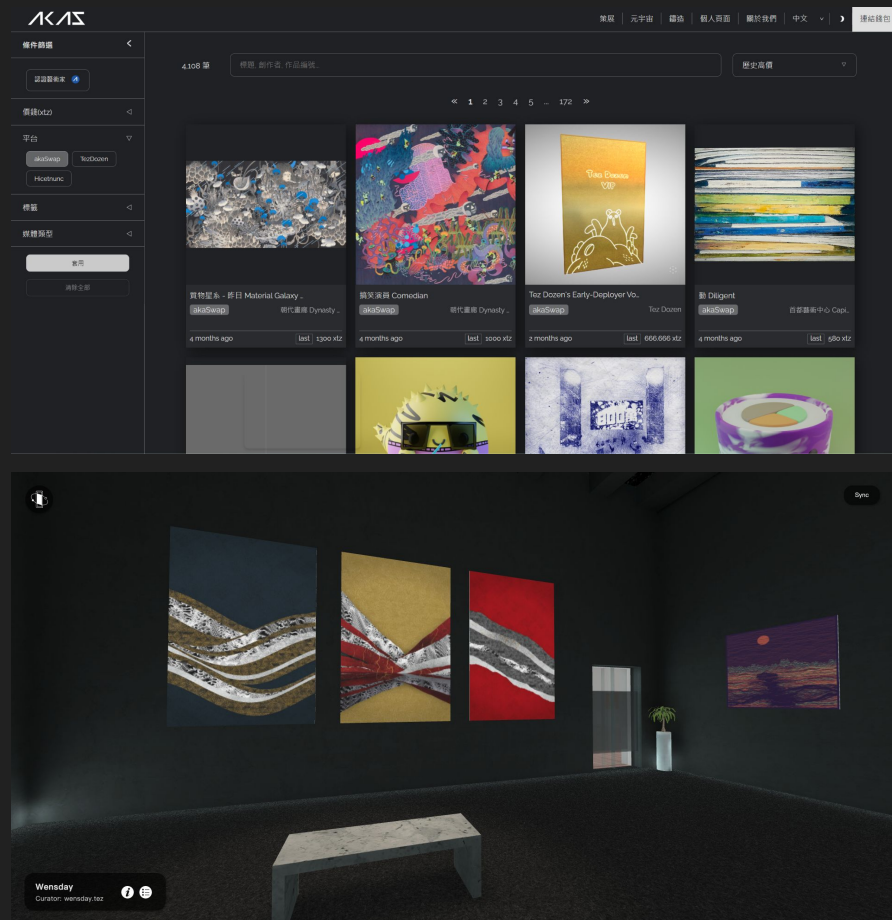
綠色節能演算法

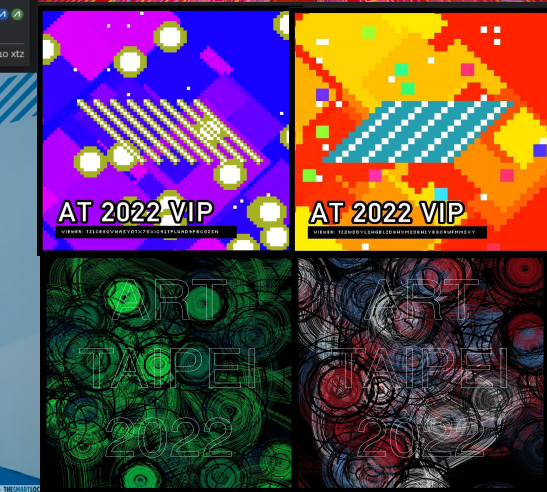
POS 共識機制能顯著減少能源消耗，兼顧Web 3.0 理念與永續發展之目的。

akaSwap



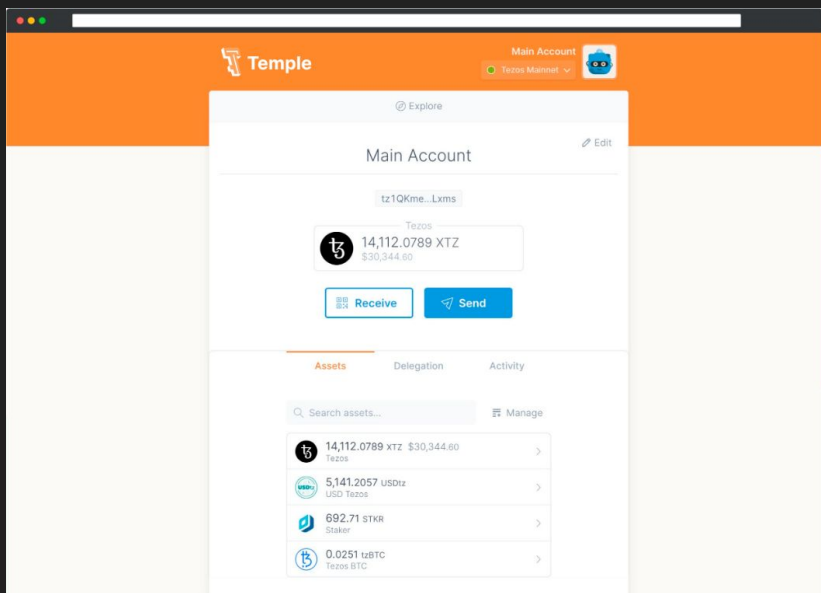
<https://akaswap.com>
<https://testnets.akaswap.com>
<https://tezdozen.xyz>
<https://akaverse.app>



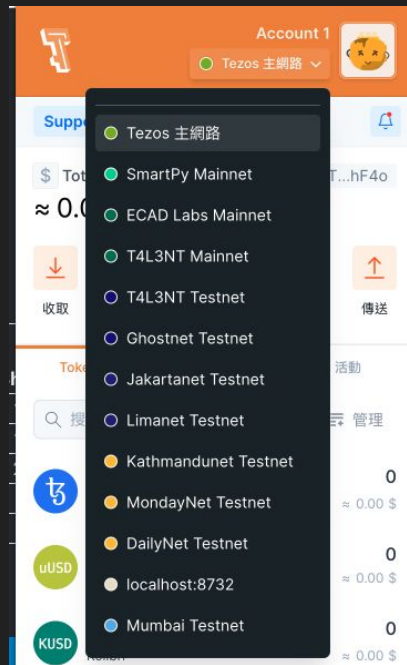


Tezos wallet - Temple

Installation: <https://templewallet.com>



https://youtu.be/Kf_9WpJYnsY



Mumbainet Testnet 測試網

Smart Contract on Tezos

About me...

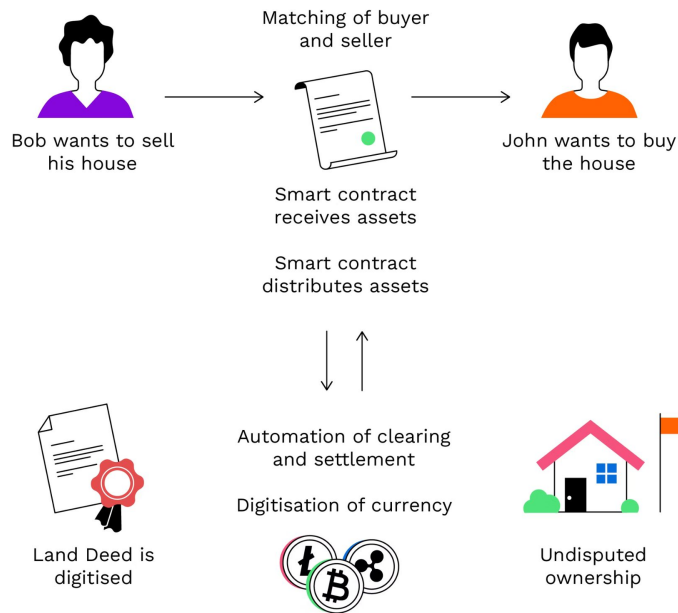
- NakoOn
 - 奈子丸
 - 奈子老公
 - 奈子腦公
- 智能合約工程師
 - akaSwap
 - Tez Dozen
 - BlockTrain
 - akaVerse



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
 - helloworld.c
- 智能合約: 錢包 ≈ 法人: 自然人

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 parameter (or (unit %default)
2             (or (List %update_share (pair (address %addr) (nat %share)))
3                 (unit %withdraw)));
4 storage (pair (pair (address %admin) (big_map %metadata string bytes))
5             (pair (map %shares address nat) (nat %shares_total)));
```

```
6 code { UNPAIR ;
7       IF_LEFT
8       { NIL operation ;
9         DUP 3 ;
10        GET 3 ;
11        ITER { PUSH mutez 0 ;
12              DUP 5 ;
13              GET 4 ;
14              DUP 3 ;
15              CDR ;
16              AMOUNT ;
17              MUL ;
18              EDIV ;
19              IF_NONE { PUSH int 24 ; FAILWITH } {} ;
20              CAR ;
21              COMPARE ;
22              GT ;
23              IF
24              { DUP ;
25                DUG 2 ;
26                CAR ;
27                CONTRACT unit ;
28                IF_NONE { PUSH int 26 ; FAILWITH } {} ;
29                DUP 5 ;
30                GET 4 ;
31                DIG 3 ;
32                CDR ;
33                AMOUNT ;
34                MUL ;
35                EDIV ;
36                IF_NONE { PUSH int 24 ; FAILWITH } {} ;
37                CAR ;
38                UNIT ;
39                TRANSFER_TOKENS ;
40                CONS }
41              { DROP } } ;
42        SWAP ;
43        DROP }
44      { IF_LEFT
45        { SWAP ;
46          DUP ;
47          DUG 2 ;
48          CAR ;
49          CAR ;
50          SENDER ;
51          COMPARE ;
52          EQ ;
53          IF {} { PUSH string "NOT_ADMIN" ; FAILWITH } ;
54          DUP ;
55          ITER { DUP 3 ;
```



Smart Contract on Tezos

- High-level languages
 - LIGO
 - **SmartPy**
 - Archetype

```
def __init__(self):
    self.init(
        admin = ADMIN,
        shares = sp.map(
            tkey = sp.TAddress,
            tvalue = sp.TNat
        ),
        shares_total = sp.nat(0),
        metadata = sp.utils.metadata_of_url(MetadataUrl)
    )
```



```
storage (pair (pair (address %admin) (big_map %metadata string bytes))
             (pair (map %shares address nat) (nat %shares_total)));
```

Let's Try it!

- 分錢合約:Fen Chian
- Storage
 - 一位admin
 - shares (map)
 - key: 錢包位址
 - value: 股份
 - shares_total
 - 總股份
 - metadata
- Entrypoint (function)
 - 匯錢(分錢)
 - 更換admin**
 - 更新股份**
 - 領錢**

**僅admin權限



在Try 之前...

- 合約資訊

- metadata

- 基礎

- `sp.sender` : 呼叫人
- `sp.amount` : 傳入的金額(單位mutez)
- `sp.balance` : 合約中剩餘金額(單位mutez)
- `sp.verify(statement)` : 驗證statement是否成立, 否則回溯
- `sp.send(target, amount)` : 發錢給指定地址(單位mutez)
- `self.data.XXX` : storage中的某資料



Let's Go!

- 合約原始碼
 - <https://tinyurl.com/FenChianSC>
- 領取測試幣
 - <https://tinyurl.com/IWantGhostMoney>
- 呼叫合約(better-call-dev)
 - <https://tinyurl.com/???>



Web dapps

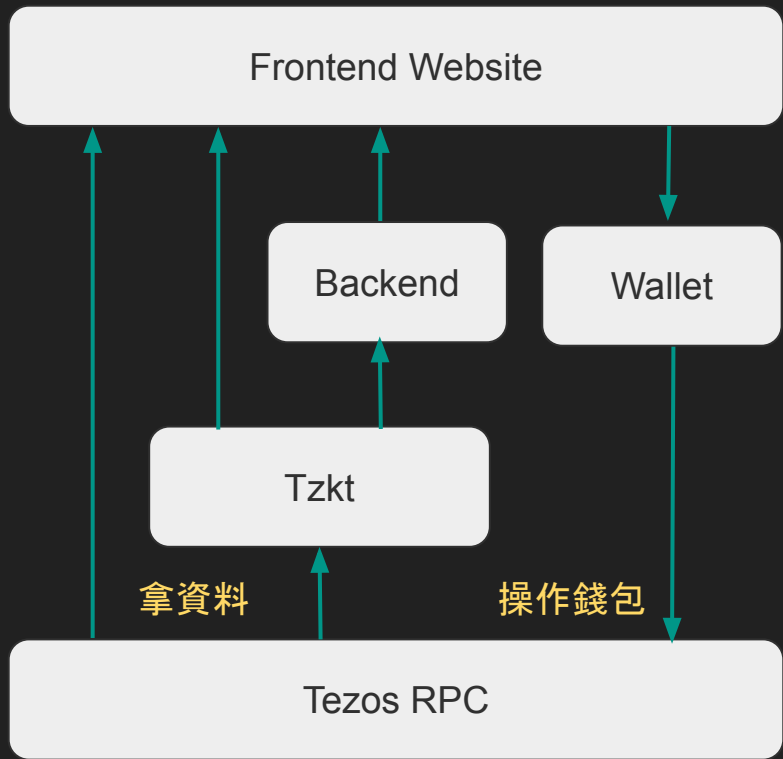
Dapps Sample

- 直接使用 Tezos node 提供的 RPC (Remote Procedure Call) 查詢資料較不方便
- Tzkt - 透過 Tezos RPC 讀取鏈上資料, 提供方便查詢的 API

<https://werwesrwerwer>

<https://tezos.gitlab.io/shell/rpc.html>

<https://ghostnet.tzkt.io/>



API - Demo

- 利用 akaSwap API 查詢作品擁有者

API - TzKT

- 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>

API - akaSwap

- 透過 TzKT 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>

感謝大家