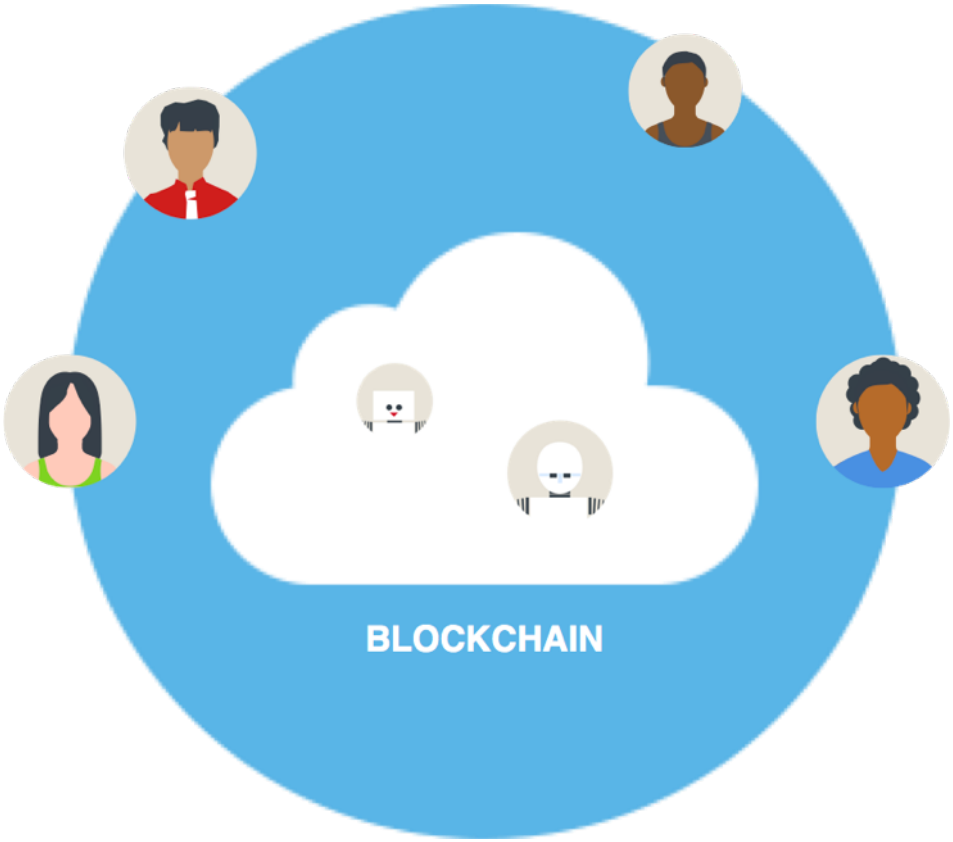
智能合約與應用

DApp

- 智能合約 (DApp)
  - ERC20 token
  - ERC721 token

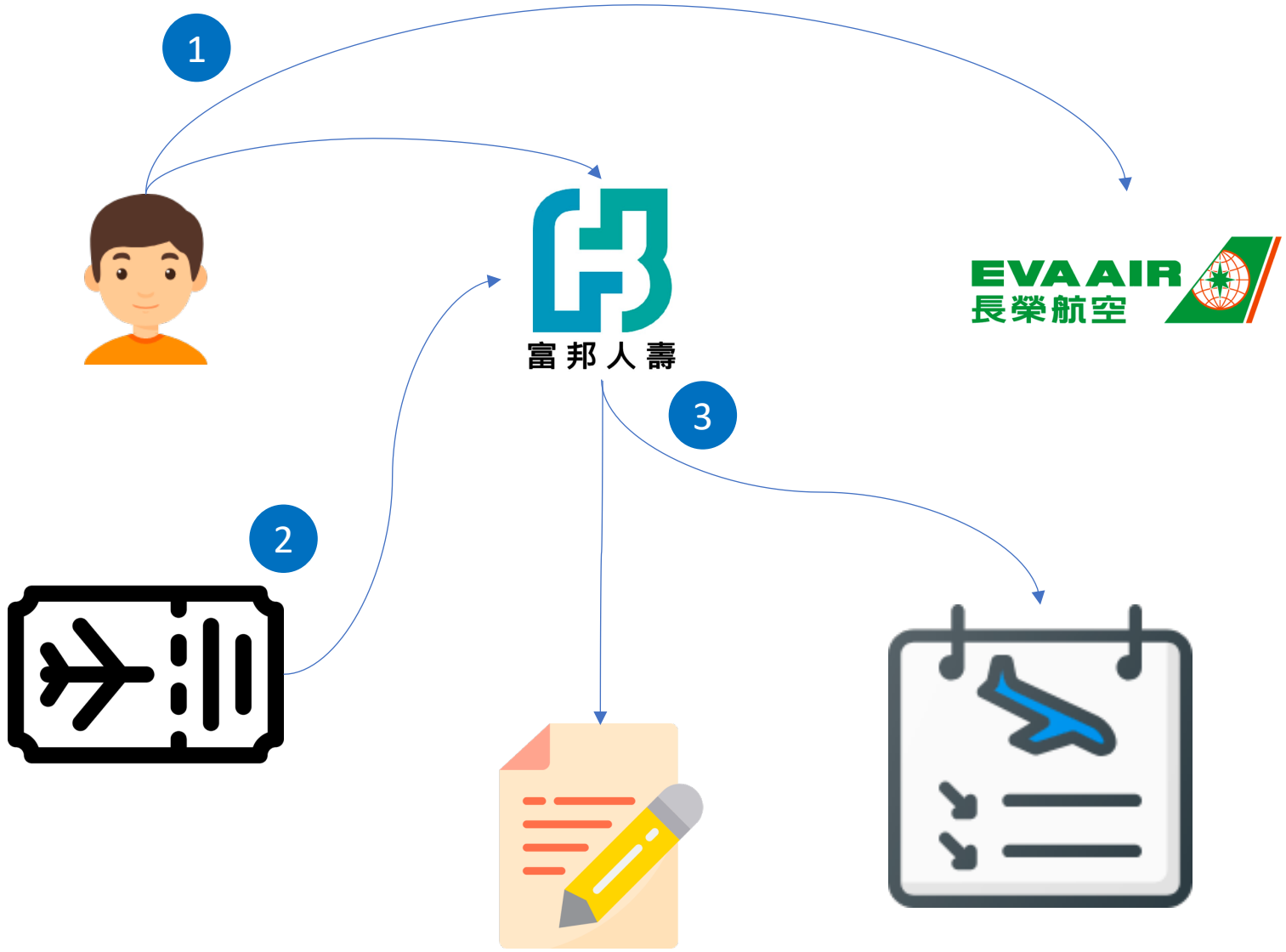


Why DApp?

- Non-custodial
- Trust
- Shared database
- Consensus
- Value transfer
- Transparent
- Tamper resistance

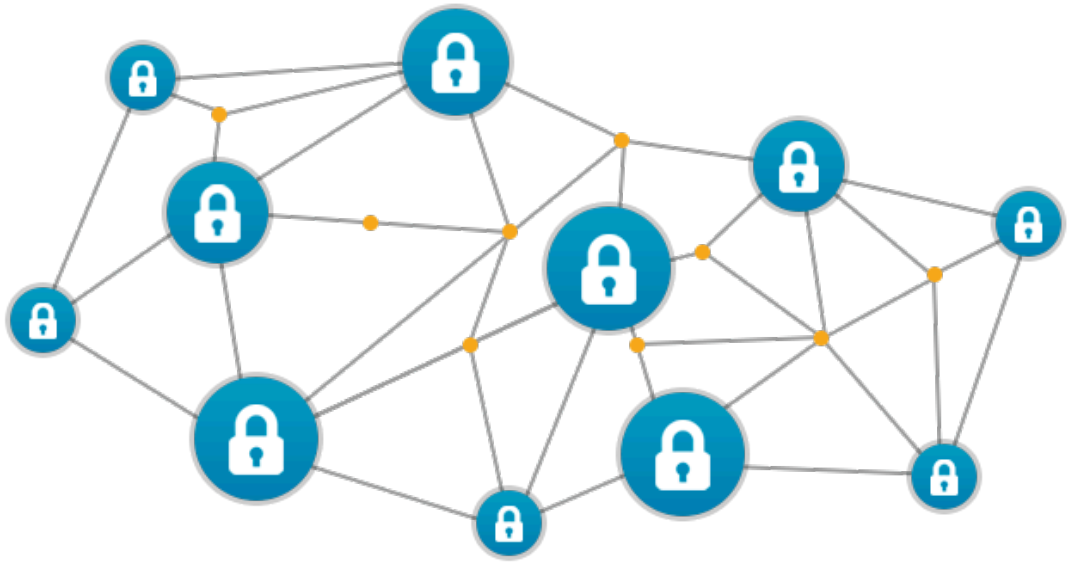
Why DApp?

- Non-custodial
- Trust
- Shared database
- Consensus
- Value transfer
- Transparent
- Tamper resistance



Why DApp?

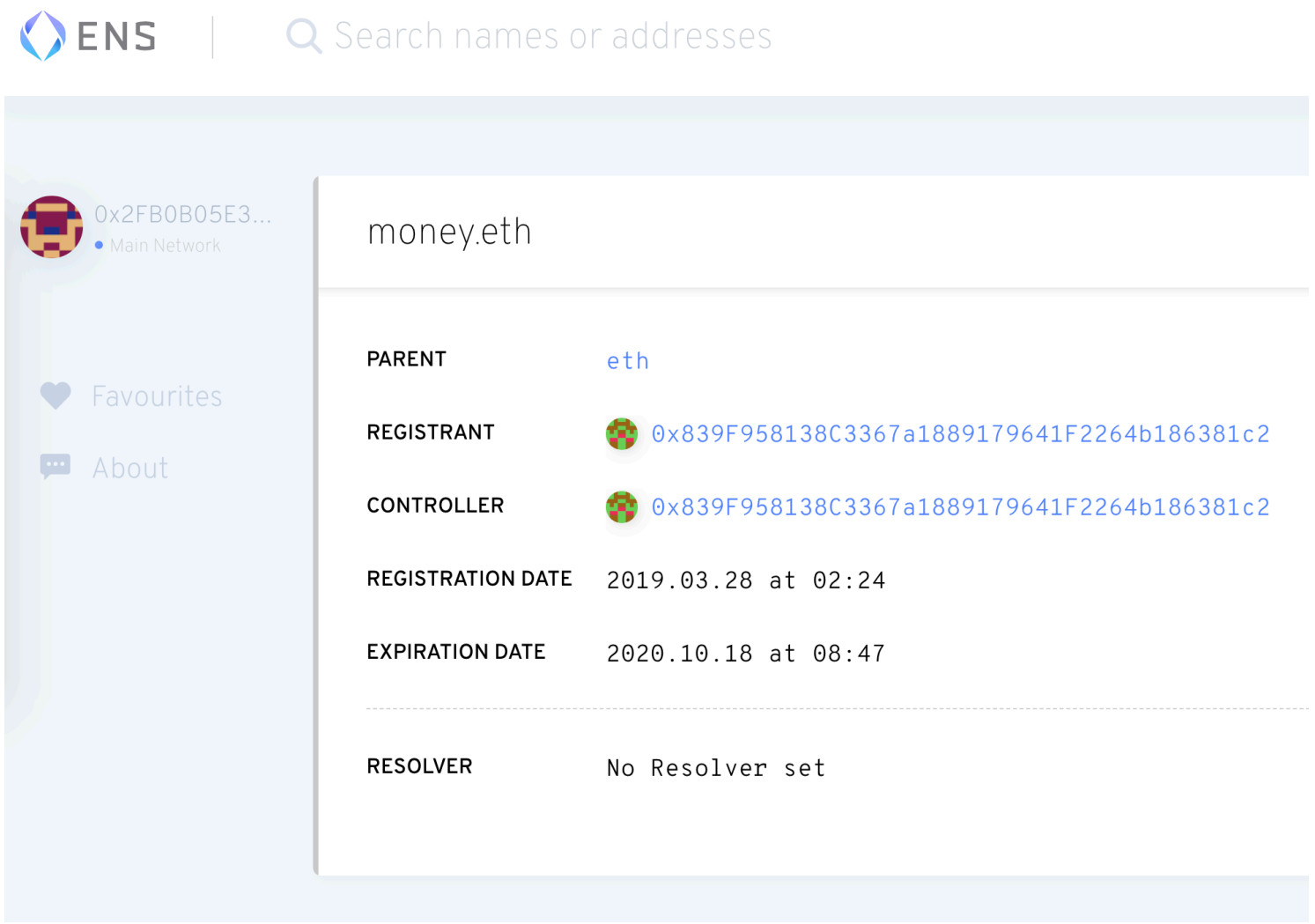
- Non-custodial
- Trust
- Shared database
- Consensus
- Value transfer
- Transparent
- Tamper resistance



Distributed Ledger Technology

Why DApp?

- Non-custodial
- Trust
- Shared database
- Consensus
- Value transfer
- Transparent
- Tamper resistance



Why DApp?

- Non-custodial
- Trust
- Shared database
- Consensus
- Value transfer
- Transparent
- Tamper resistance

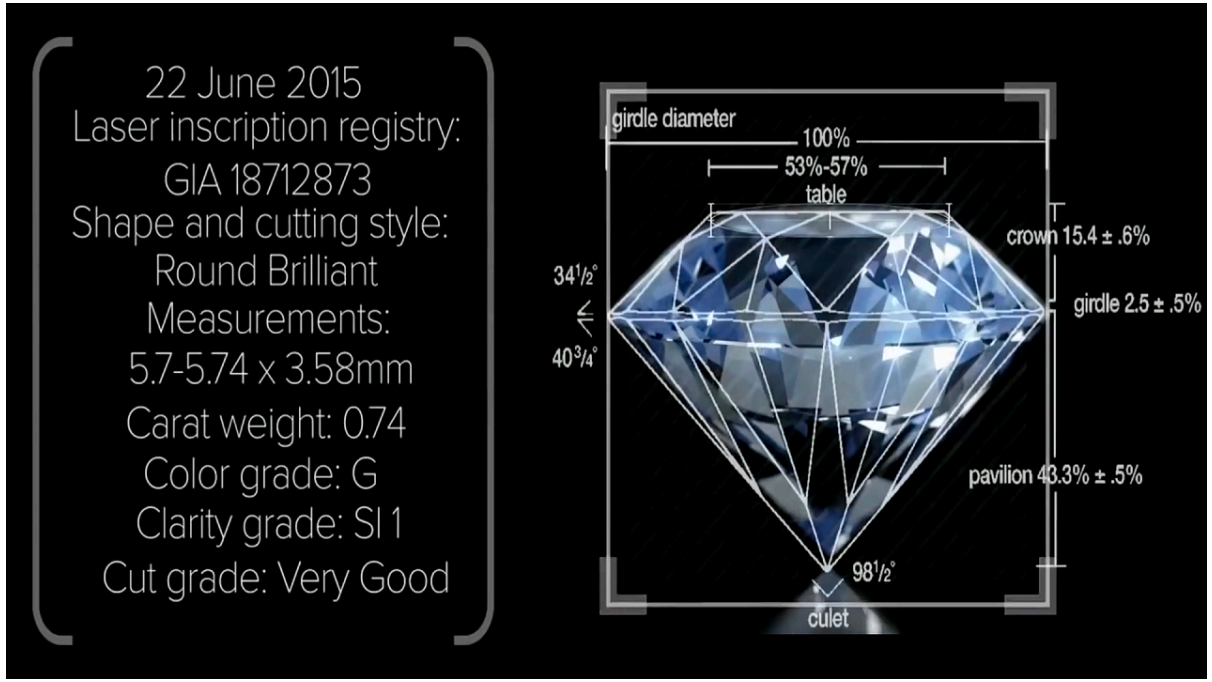
Ticket

But

- 低效高成本的信任機器
- 絕多數的時候，應用不需要區塊鏈
- 與機器學習比較，看哪個方案好
- 何時會需要
  - 明顯改善
  - 換取信任

Traceable

- Diamond ledger
- Food service resume



Traceable

- Diamond ledger
- Food service resume

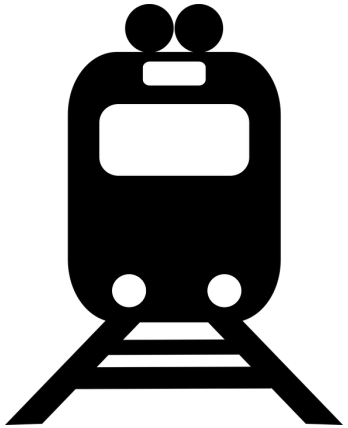
區塊鏈無法保證真相，只是將真相和謊言都以無法篡改的方式保留下來，
允許後人客觀地分析這些內容，從而更有信心揭露謊言。

- Nick Szabo

Money

Tool

DApp
Infrastructure



存在工具


Vitalik Buterin
@VitalikButerin
Following
Another day, another blockchain use case.
Block 3,930,000
=
0xe2f1fc56dald...
Retweets
446
Likes
1,656
5:01 pm - 25 Jun 2017

新聞工具

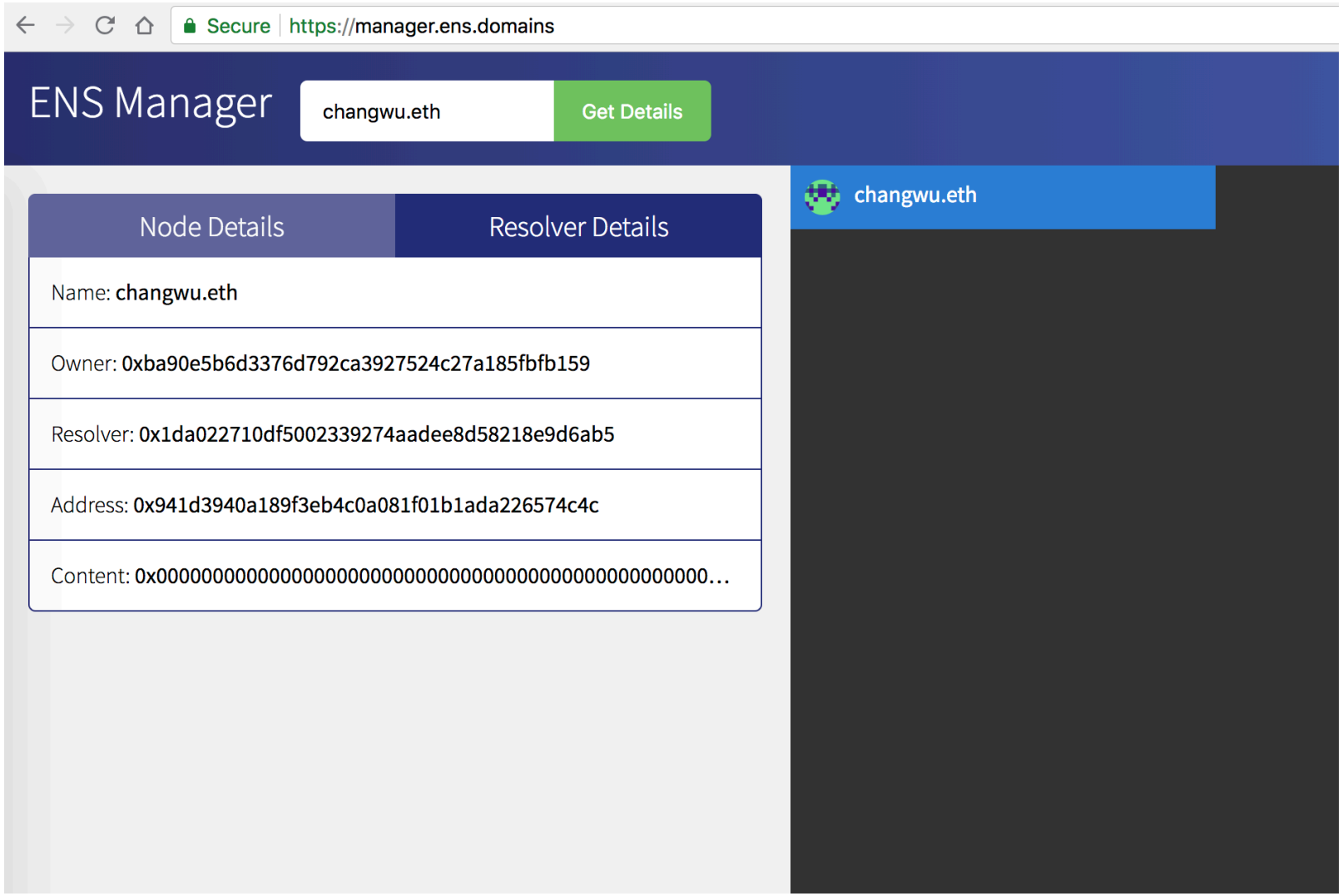
Actual Tx Cost/Fee:	0.0007787 Ether ($0.23)
Nonce & {Position}:	0 | {107}
Input Data:	

```
5. The School of Foreign Languages of Peking University should make a clear written response
to the appeal and give it to everyone concerned.
I will retain all legal rights to further investigate the responsibilities of relevant
individuals and units, including but not limited to reporting to Peking University and
higher authorities the serious violation of school regulations by the Foreign Language
Institute.
Peking University School of Foreign Languages
April 23, 2018

北京大学的老师和同学：
你们好！
我是2014级外国语学院的岳昕，是4月9日早上向北京大学递交《信息公开申请表》的八位到场同学之一。我拖着极疲惫的身躯
写下这段文字，说明近来发生在我身上的一些事情。
一
4月9日之后，我不断被学院学工老师、领导约谈，并两次持续到凌晨一点甚至两点。在谈话中，学工老师多次提到“能否顺利
毕业”、“做这个你母亲和姥姥怎么看”、“学工老师有权不经过你直接联系你的家长”。而我近期正在准备毕业论文，频繁的打
扰和后续的心理压力严重影响了我的论文写作。
二
4月20日中午，我收到了校方的回复。外国语学院党委书记、学工老师、班主任在场，党委书记向我宣读了学校对于本次信息
公开申请的答复：
1、讨论沈阳师德的会议级别不够记录
2、公安局调查结果不在学校的管理范围里
3、沈阳公开检讨的内容因中文系工作失误也没有找到
这样的回复结果令我失望。但毕业论文提交即将截止，我只能先将心思放在论文写作上。
```

View Input As

網域工具


Secure
https://manager.ens.domains
ENS Manager
changwu.eth
Get Details
Node Details
Resolver Details
Name: changwu.eth
Owner: 0xba90e5b6d3376d792ca3927524c27a185fbfb159
Resolver: 0x1da022710df5002339274aadee8d58218e9d6ab5
Address: 0x941d3940a189f3eb4c0a081f01b1ada226574c4c
Content: 0x0000000000000000000000000000000000000000000000000000...
changwu.eth

證書

Block Certs

研討會	TANet 2018 - 臺灣網際網路研討會
地點	國立中央大學
啟迄日	2018-10-24 至 2018-10-26
活動網站	http://tanet2018.ncu.edu.tw/
公鑰 (ECDSA Public Key)	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAED7XnIIapG21HJykOgFZ10GvUFmflX9DeTTUdn9l6sQfXnP5cMWpdCF__Qzt5ySwQh2WRqWAHq7Jzs-0BB82jMg
Previous Bundle	RQPBZCECSSQVCZEAGJJDTLJZSIAPZAYIKATVWABIYCZORSCAGXBGEISRMJJJLDOPAKCVEFQXKDZSVXYCY

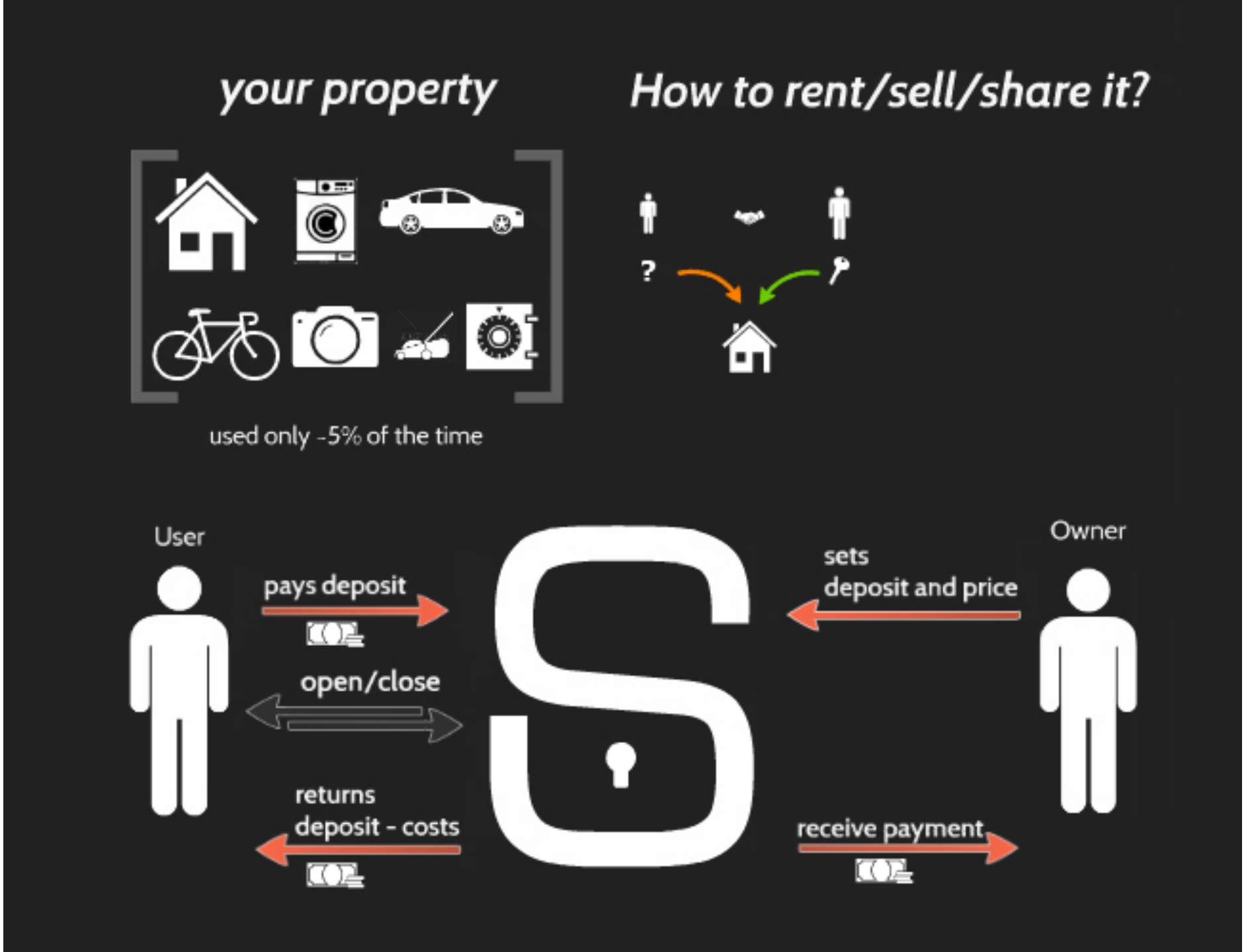
區塊鏈上的原始資料


```
{
  "type": "Conference",
  "prevBundle": "RQPBZCECSSQVCZEAGJJDTLJZSIAPZAYIKATVWABIYCZORSCAGXBGEISRMJJJLDOPAKCVEFQXKDZSVXYCY",
  "prevHash": "9714895b1999b09799a1710cd162b8ba6fe507c75502a31d047ccde22f9d4a6a",
  "name": "TANet 2018 - 臺灣網際網路研討會",
  "location": "國立中央大學",
  "startDate": "2018-10-24",
  "endDate": "2018-10-26",
  "url": "http://tanet2018.ncu.edu.tw/",
  "publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAED7XnIIapG21HJykOgFZ10GvUFmflX9DeTTUdn9l6sQfXnP5cMWpdCF__Qzt5ySwQh2WRqWAHq7Jzs-0BB82jMg"
}
```

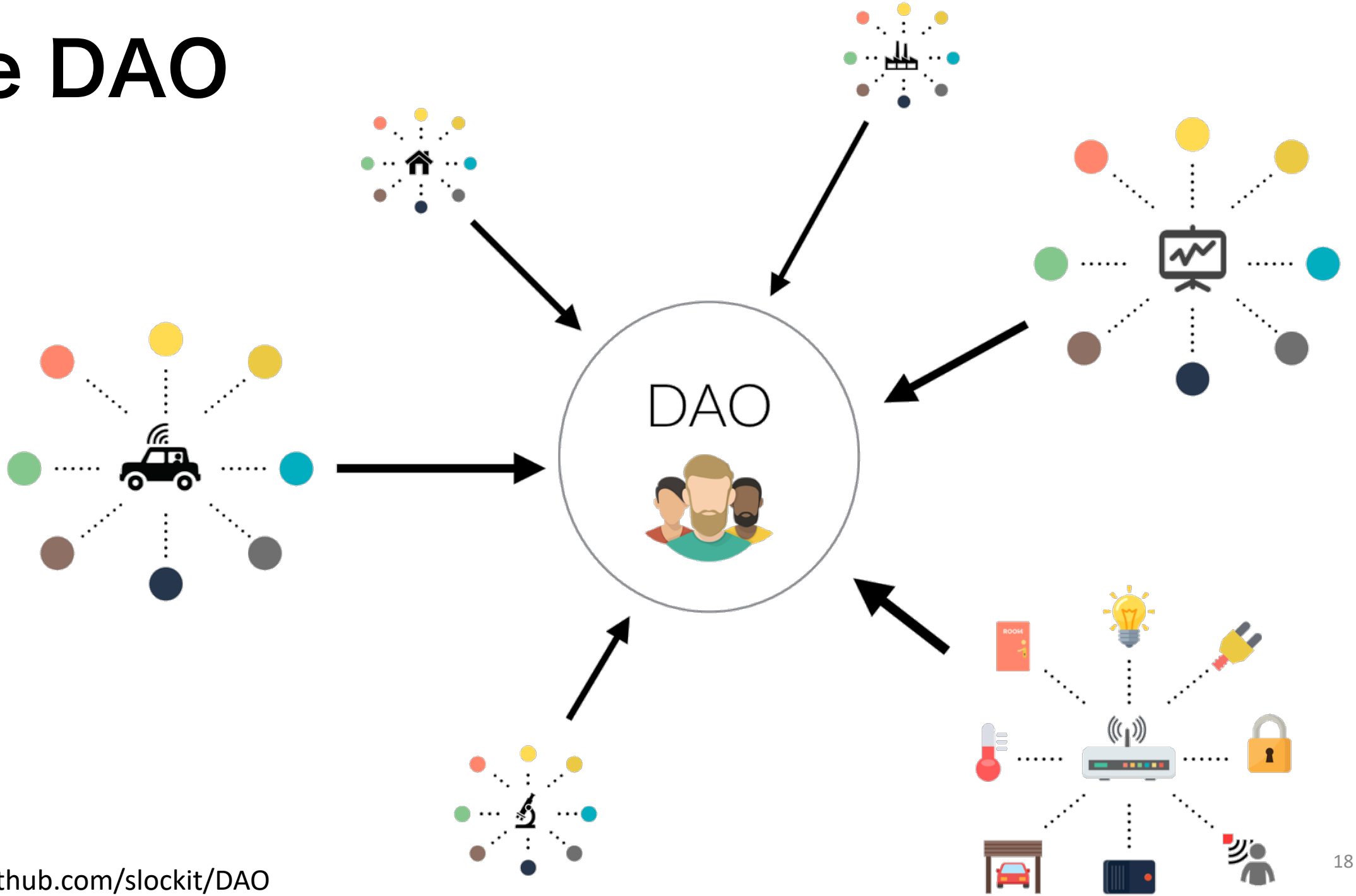
代幣模型

- Payment token (貨幣)
- Security token (股票)
- Utility token (代幣/車票)

Slock it


your property
How to rent/sell/share it?
used only ~5% of the time
User
Owner
pays deposit
sets
deposit and price
open/close
returns
deposit - costs
receive payment

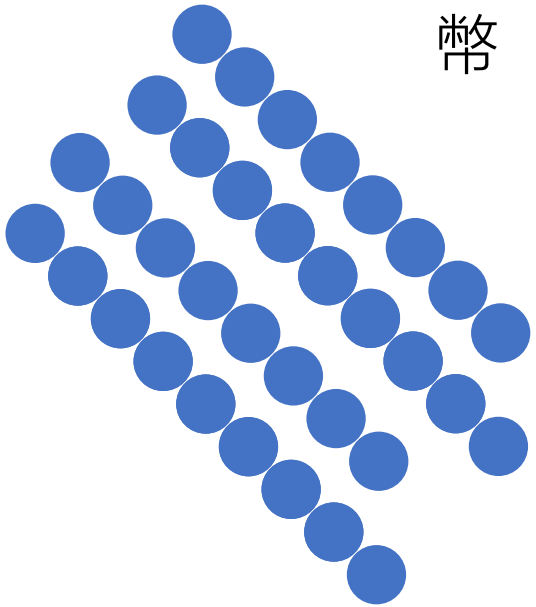
The DAO



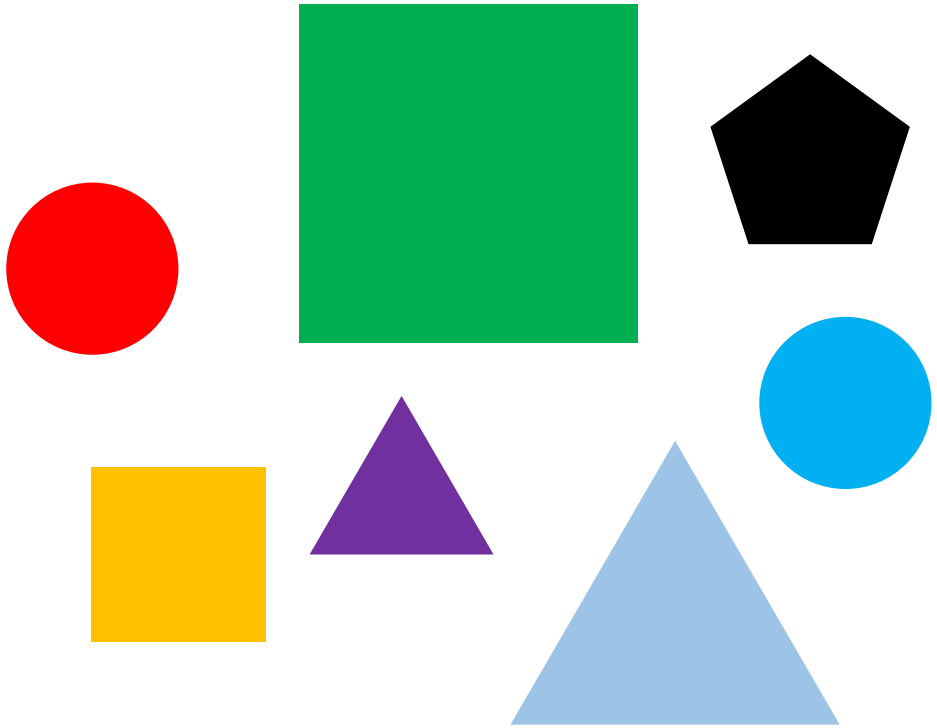
https://github.com/slockit/DAO

代幣

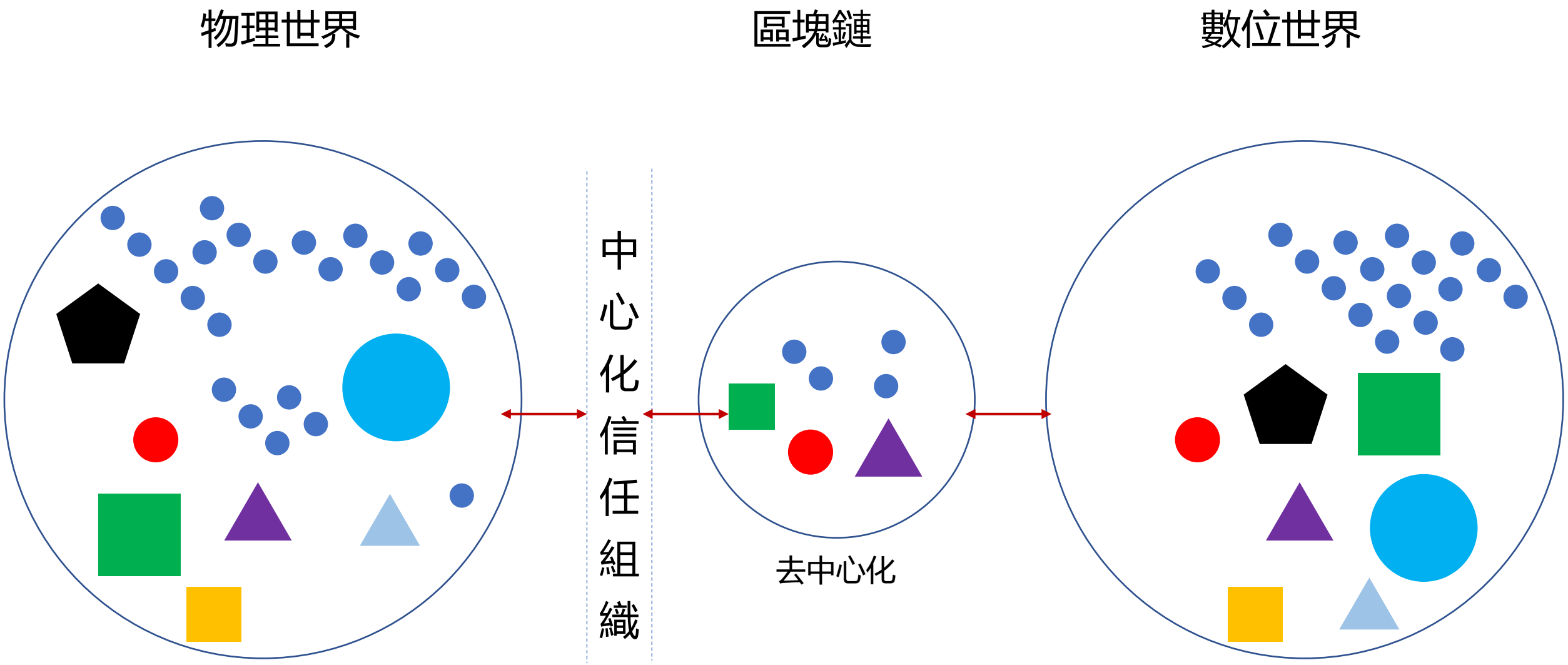
幣



人 / 事 / 物 / 權



Source: AlphaWallet



Source: AlphaWallet

應用

- 票卷系統
- 捐款
- 政治獻金
- 會員點數系統

未來生活

- 小明上網訂了一箱紅酒
  - Identity token
  - Payment token
  - Tracking token
  - Order token
  - Reward points
  - Food traceability

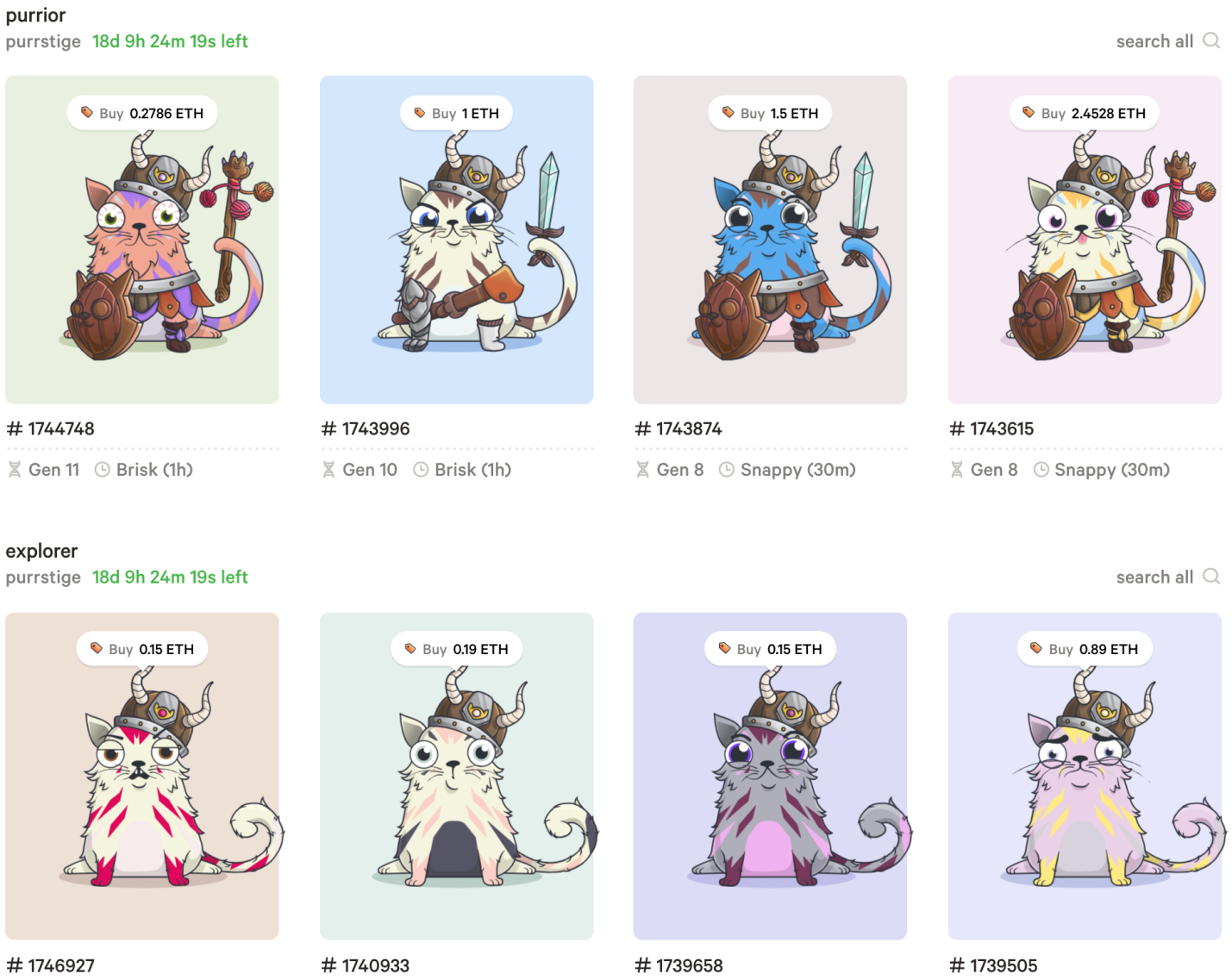
區塊鏈投票 (計票，選票)

- Enforced secrecy
  - 秘密投票
  - 不受干擾
- Individual verifiability
  - 每個人的票都被忠實的記錄
  - 每張票可計數
- Global verifiability
  - 開票紀錄正確
  - 沒有人可作票

MLB Crypto Baseball

https://www.mlbcryptobaseball.com/marketplace

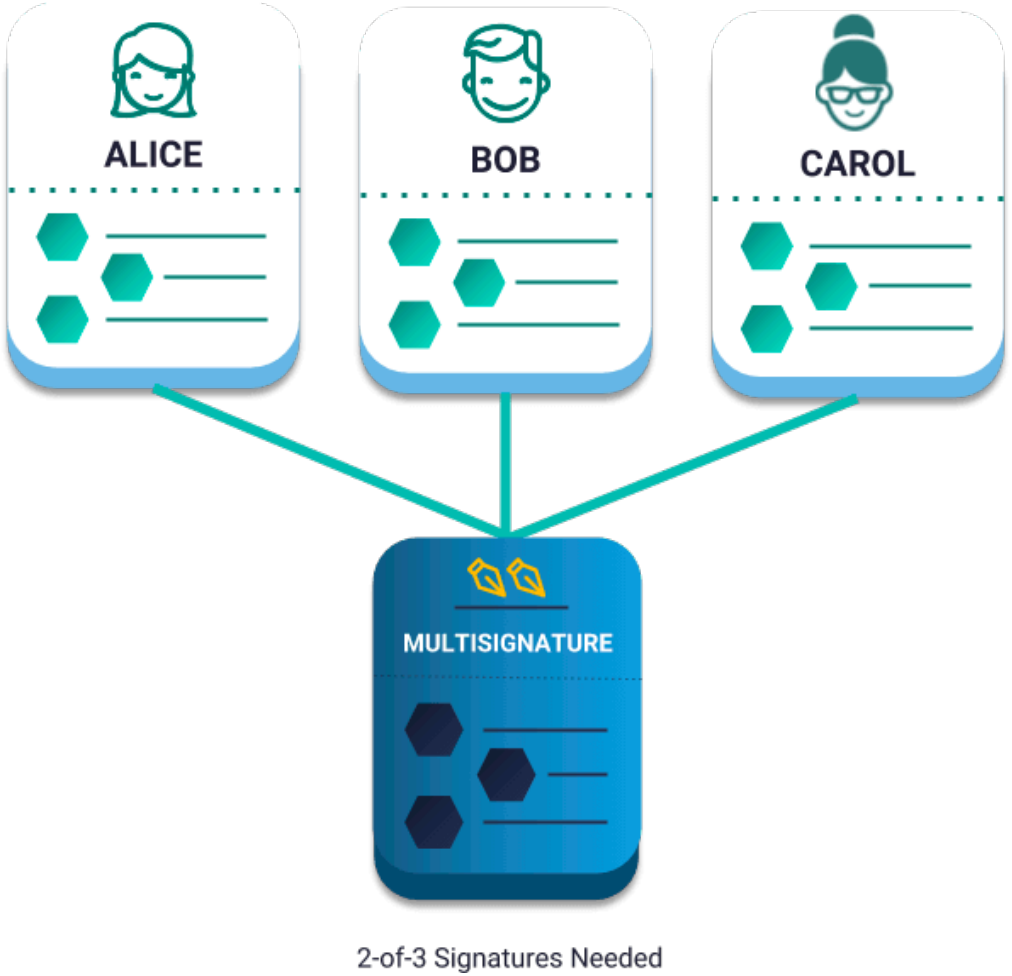
CryptoKitties



https://www.cryptokitties.co/

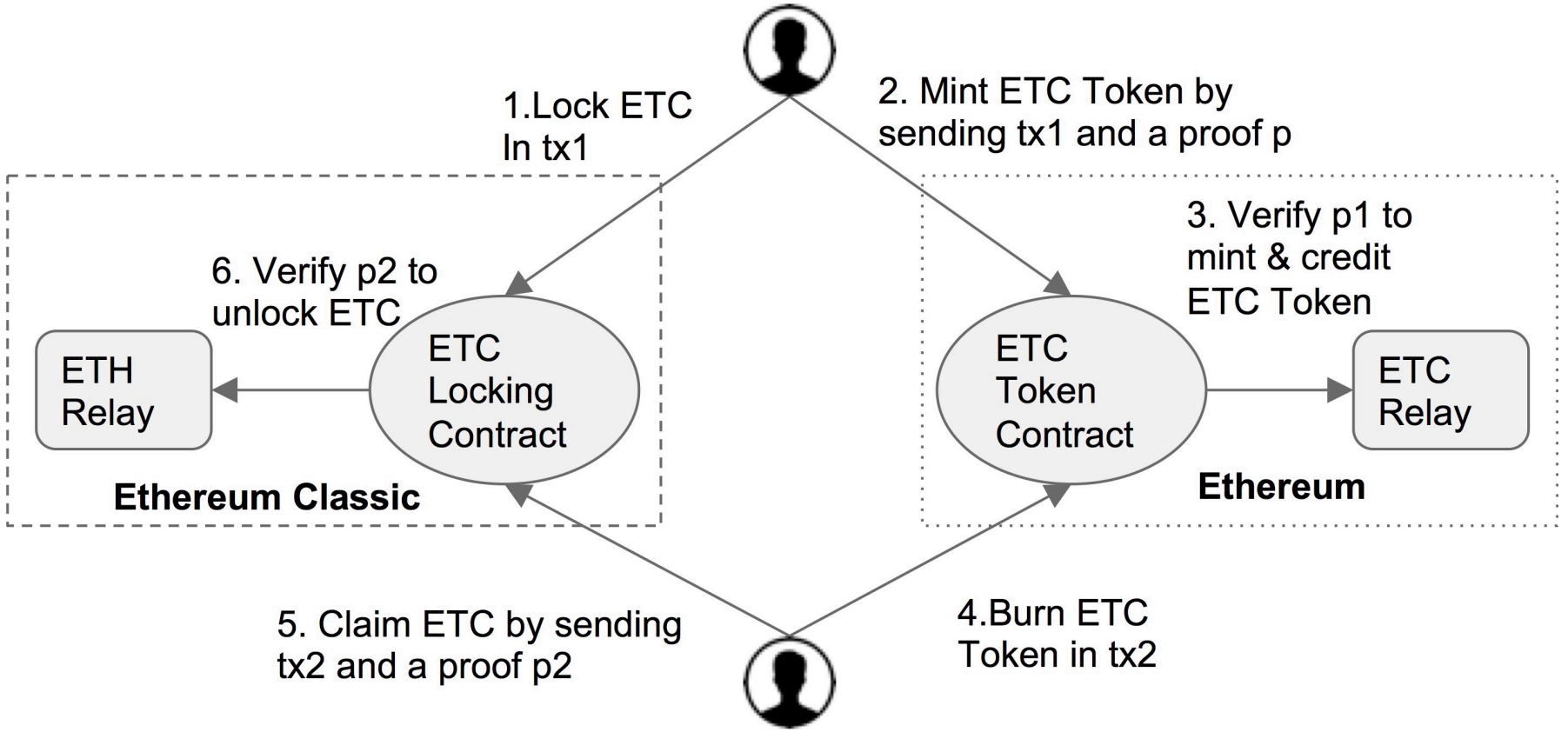
Ethereum Multisignature Wallet

Figure: https://nemtech.github.io/concepts/multisig-account.html



https://github.com/gnosis/MultiSigWallet

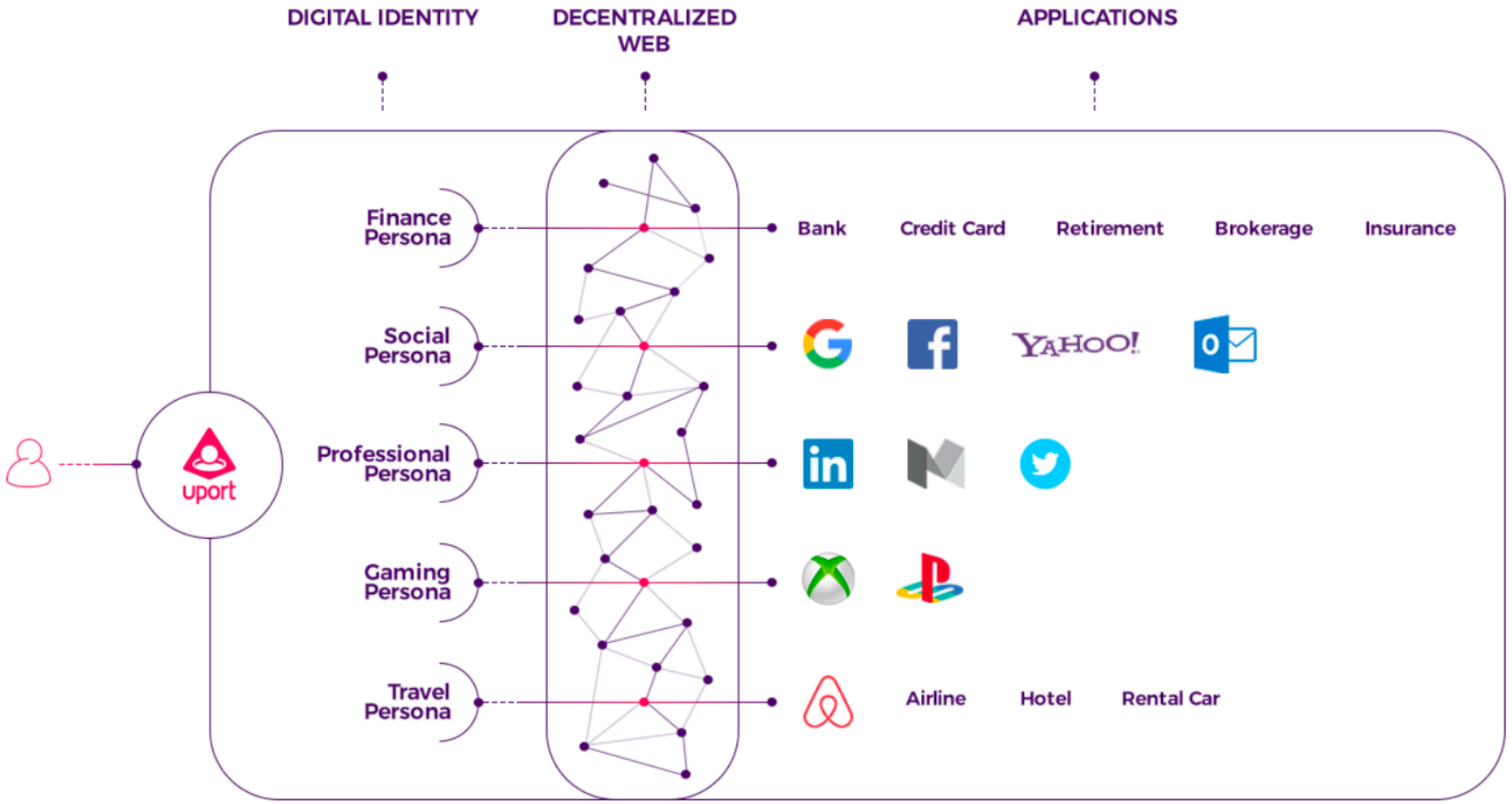
Atomic swap (cross-chain)



https://medium.com/@loiluu/peacerelay-connecting-the-many-ethereum-blockchains-22605c300ad3

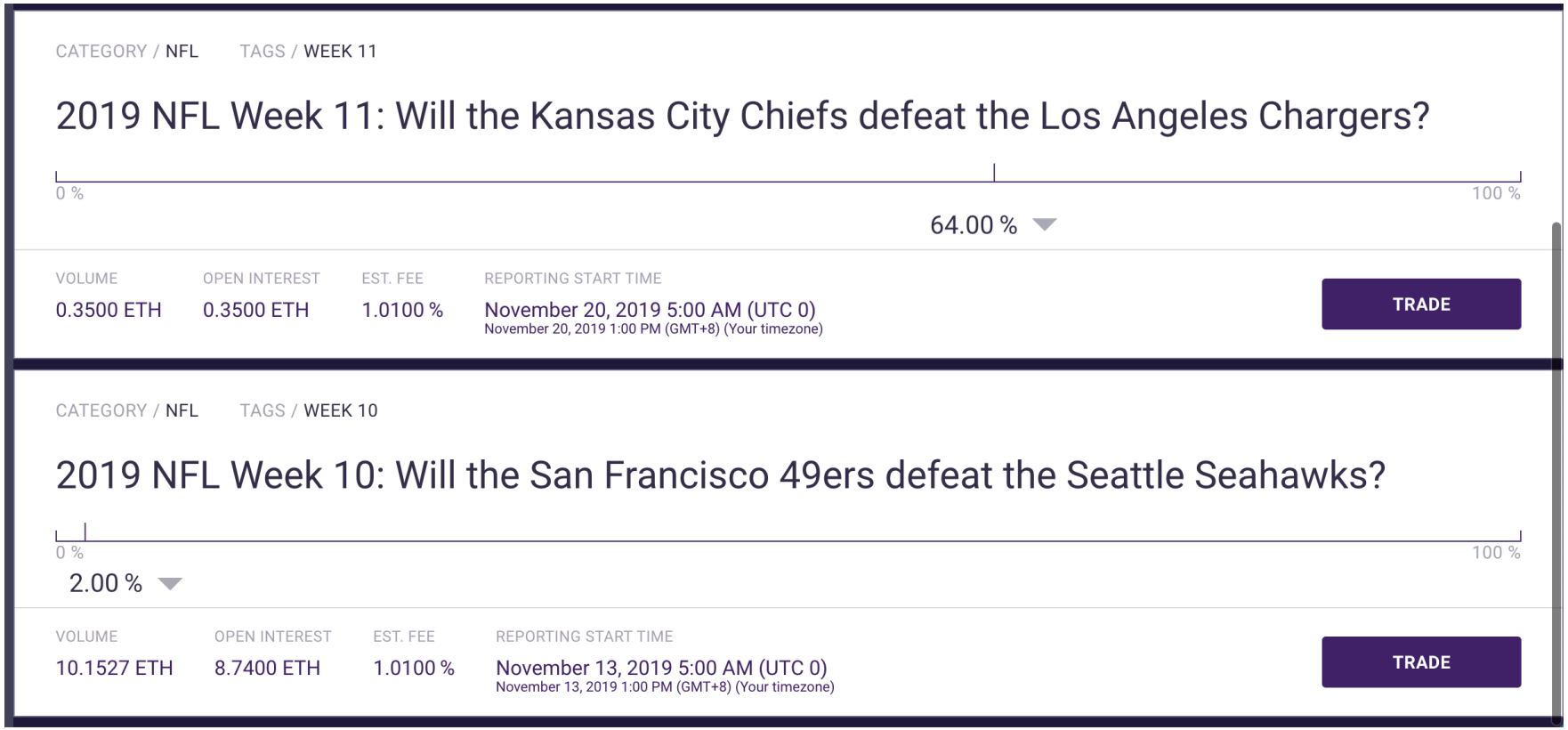
uPort

- Digital identity



Augur

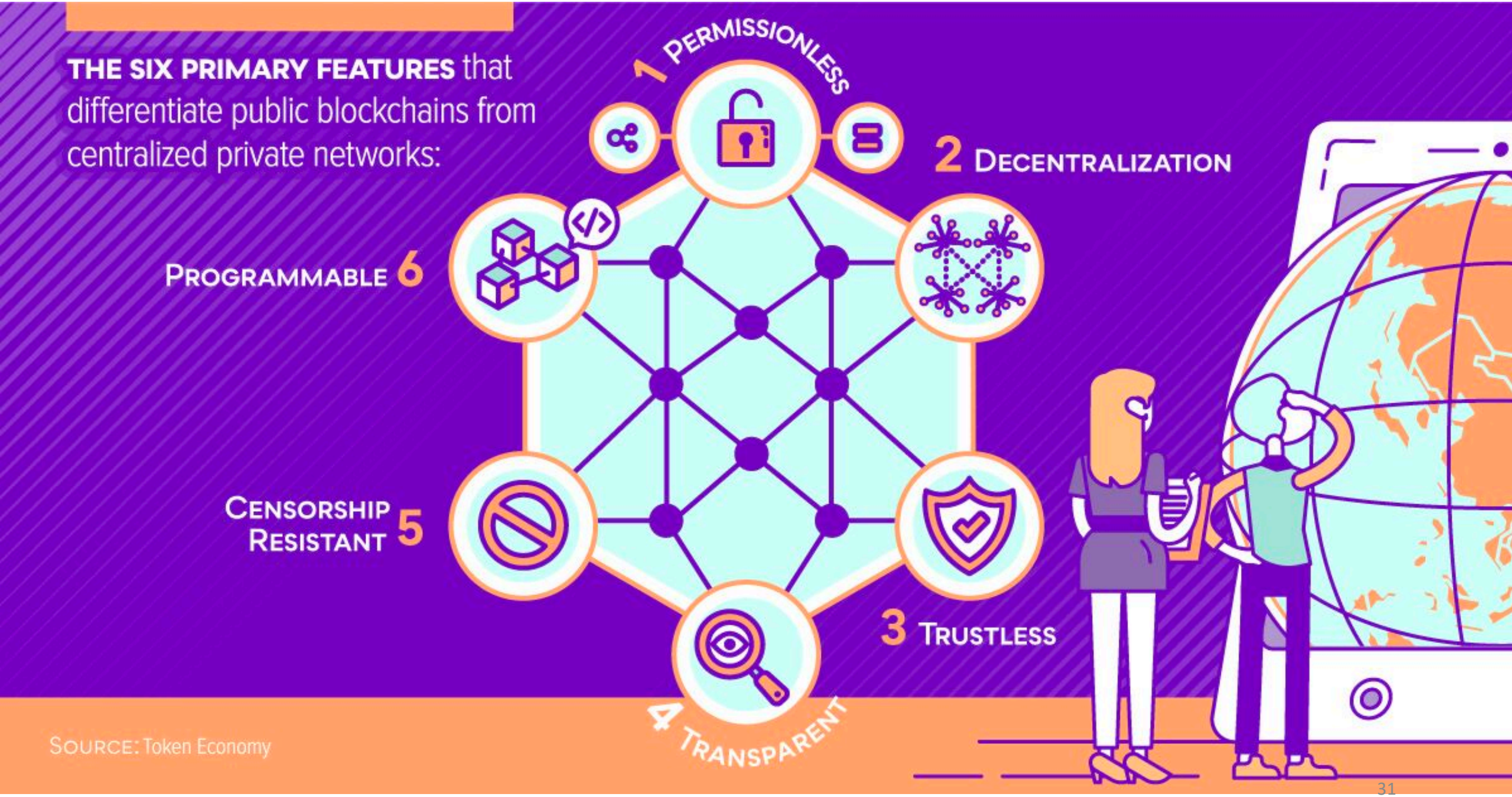
- Prediction market



https://cloudflare-ipfs.com/ipfs/Qmf9Rf7bVoaN47ph8A8TXNv7WTPz28ZB53zHn54AY2skfo/?ethereum_node_http=https%3a%2f%2feth-mainnet.alchemyapi.io%2fjsonrpc%2f7sE1TzCIRIQA3NJPD5wg7YRiVjhxuWAE&augur_node=wss%3a%2f%2faugur-node.augur.casino#!/markets

Decentralized Finance

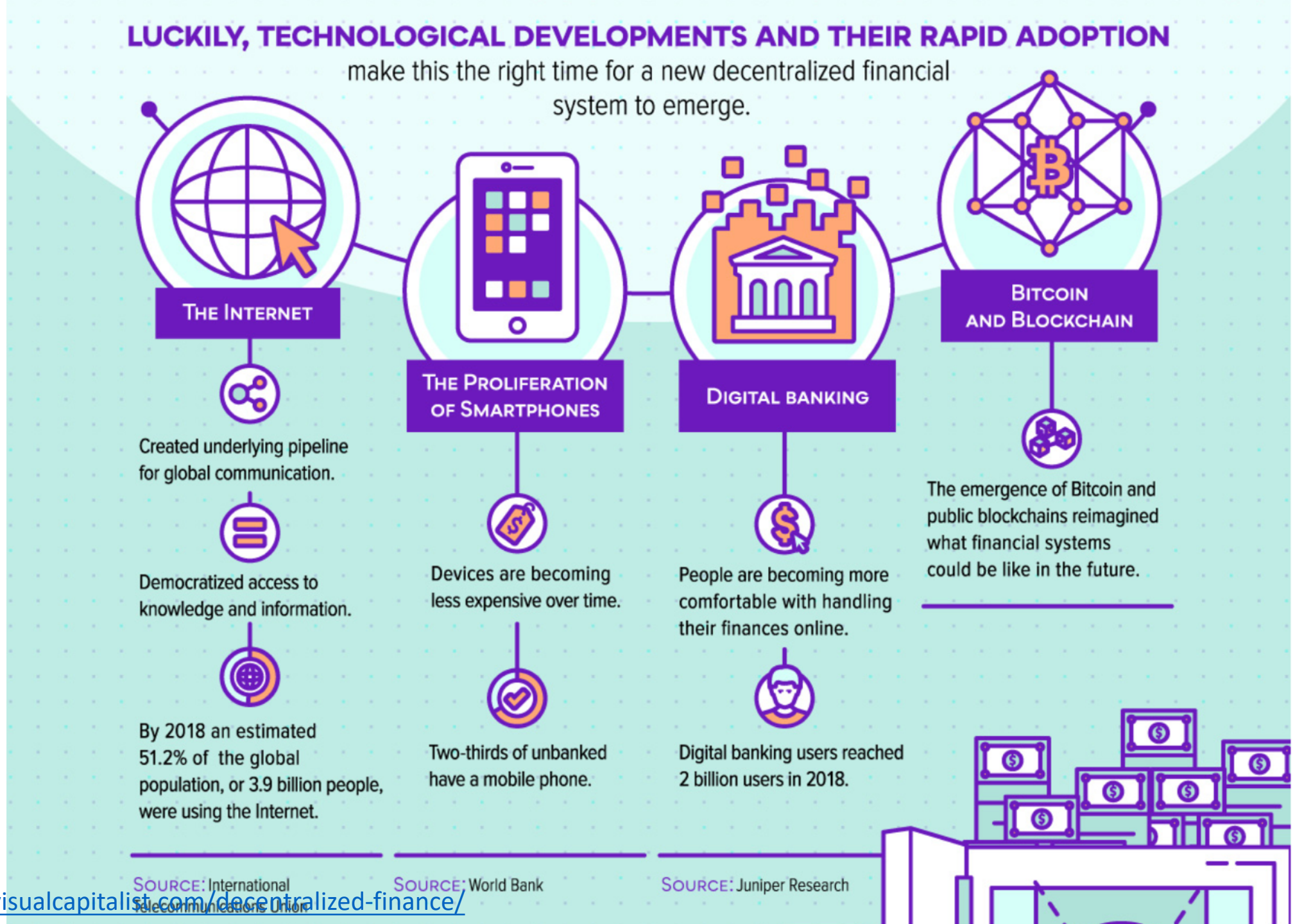
DeFi



https://www.visualcapitalist.com/decentralized-finance/

Blockchain

- Decentralize everything
- Tokenize everything



https://www.visualcapitalist.com/decentralized-finance/

Finance

- FinTech
- Conventional financial tools built on a blockchain
  - DeFi
  - BlockFi
  - Open Finance

Benefits

- Monetary policy not controlled by a central bank
- Lowers the barrier to create new products vs. traditional banking system
- Serves as a release valve for overaggressive government regulations
- Transparency
- Can be audited
- Fairness
- Eliminates rent seeking middlemen
- Open 24 hours a day
- No credit checks
- I don't have to ask permission from a financial intermediary

https://www.reddit.com/r/ethereum/comments/by2u15/defi_user_studies_research_some_of_my_findings/

Technical Risk vs Trust DApps

- Trustless
- Smart contract audits
  - Compound v2 announcement
    - Contract source code
      - https://etherscan.io/address/0xf5dce57282a584d2746faf1593d3121fcac444dc#contracts
    - Audited by Trail of Bits
      - https://drive.google.com/file/d/1w-xIxeC5Awl5C2rPrayW3OFgL379mlHB/view
    - Formally verified by Certora
  - MakerDAO
    - https://medium.com/makerdao/the-code-is-ready-2aee2aa62e73
- Social proof
  - Compound v1, launched in September 2018
- Aligns with the ethos of crypto

DEFI PULSE

Total Value Locked (USD)	Maker Dominance	
$511.2M	75.67%	Lending: $451M DEX: $28.1M Derivatives: $22.8M Payments: $7.4M Assets: $2M

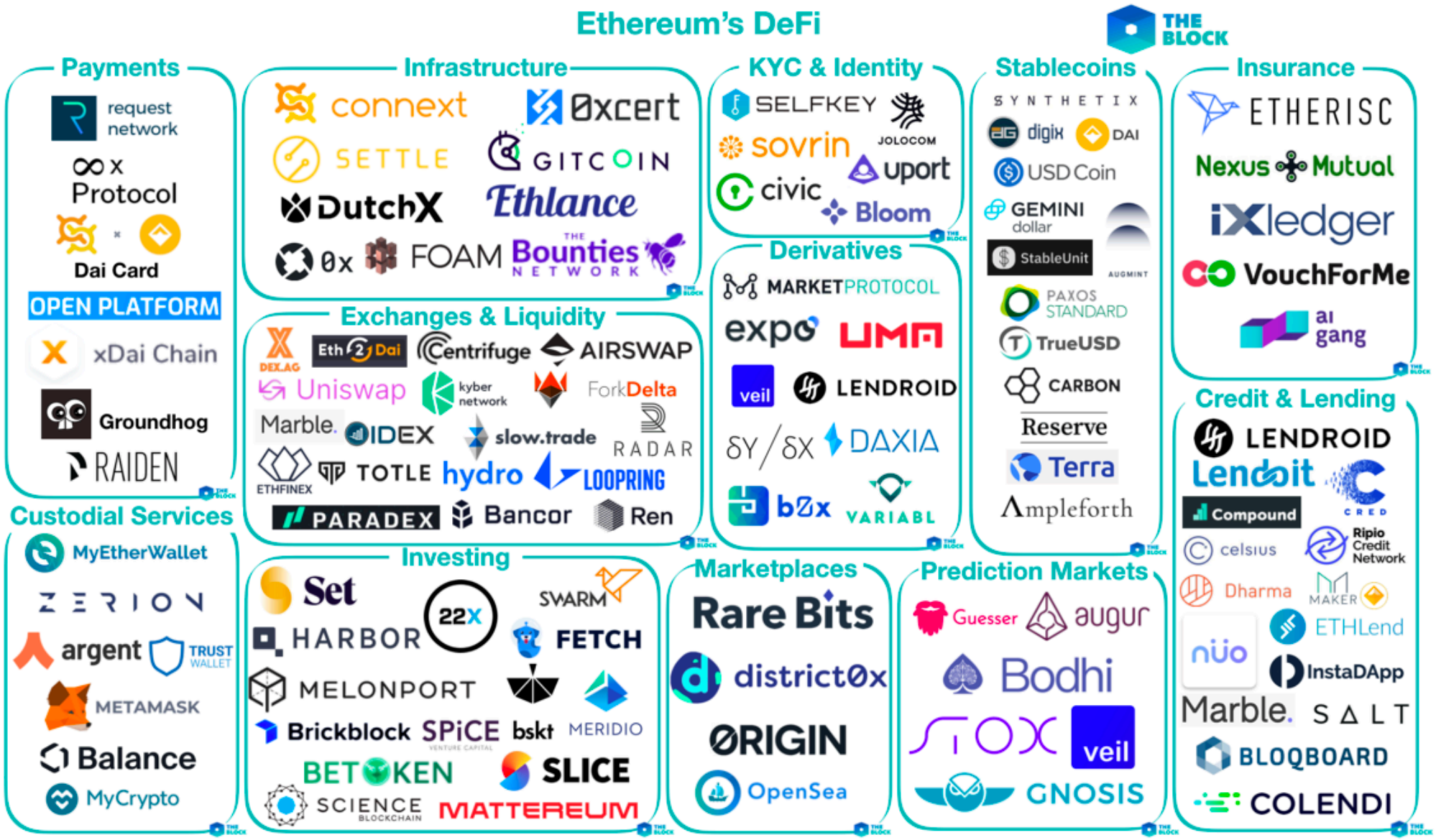
ALL | LENDING | DEX | DERIVATIVES | PAYMENTS | ASSETS

DEFI PULSE	Name	Chain	Category	Locked (USD)	1 Day %
1.	Maker	Ethereum	Lending	$386.8M	-2.9%
2.	Compound	Ethereum	Lending	$29.4M	5.6%
3.	Synthetix	Ethereum	Derivatives	$21.7M	5.8%
4.	Dharma	Ethereum	Lending	$20.3M	-2.9%
5.	Uniswap	Ethereum	DEX	$16.8M	-1.8%
6.	Bancor	Ethereum	DEX	$10.1M	-0.8%
7.	Nuo Network	Ethereum	Lending	$7.9M	-0.7%
8.	Lightning Network	Bitcoin	Payments	$7.3M	-3.7%
9.	dYdX	Ethereum	Lending	$6.4M	-0.2%
10.	InstaDApp	Ethereum	Lending	$2M	-6.2%

https://defipulse.com/

DeFi Applications

- Open Lending/borrowing Protocols
  - Compound Finance (Liquidity pool)
  - Dharma (P2P protocol)
- Decentralized Prediction Markets
  - Augur
  - Gnosis
- Exchanges and Open Marketplaces
  - Radar Relay
  - EtherDelta
  - Uniswap
- Stablecoins
  - MakerDAO



https://www.theblockcrypto.com/2019/03/14/mapping-out-ethereums-defi/

Token types

- Payment token (貨幣)
  - Stablecoins
- ~~Utility token (代幣/車票)~~
  - ~~Ticket~~
- ~~Security token (股票)~~
  - ~~STO~~

Functions of Money

- Medium of Exchange (MoE)
- Store of Value (SoV)
- Unit of Account

檢視比特幣

- 貨幣三大功能
  - 交易媒介 (x)
  - 價值儲存 (x)
  - 記帳單位 (x)
- 原因
  - 價格具波動性

穩定幣 (Stablecoin)

- 與法幣 1:1 錨定 (USDT)

- 發行模式，大致分三類
  - 法幣抵押型穩定幣
  - 鏈上資產抵押型穩定幣
  - 鏈上無資產抵押型穩定幣

法幣抵押型穩定幣

- 由中心機構托管用戶的美元存款，發行 1:1 的法幣兌換卷 (消費卷)
  - ex: USDT, TUSD, GUSD
- 優點
  - 機制設計簡單
  - 法幣穩定
- 缺點
  - 中心化
  - 透明性和監管難度
  - 監管審批
  - 流動性
  - 難以規模化

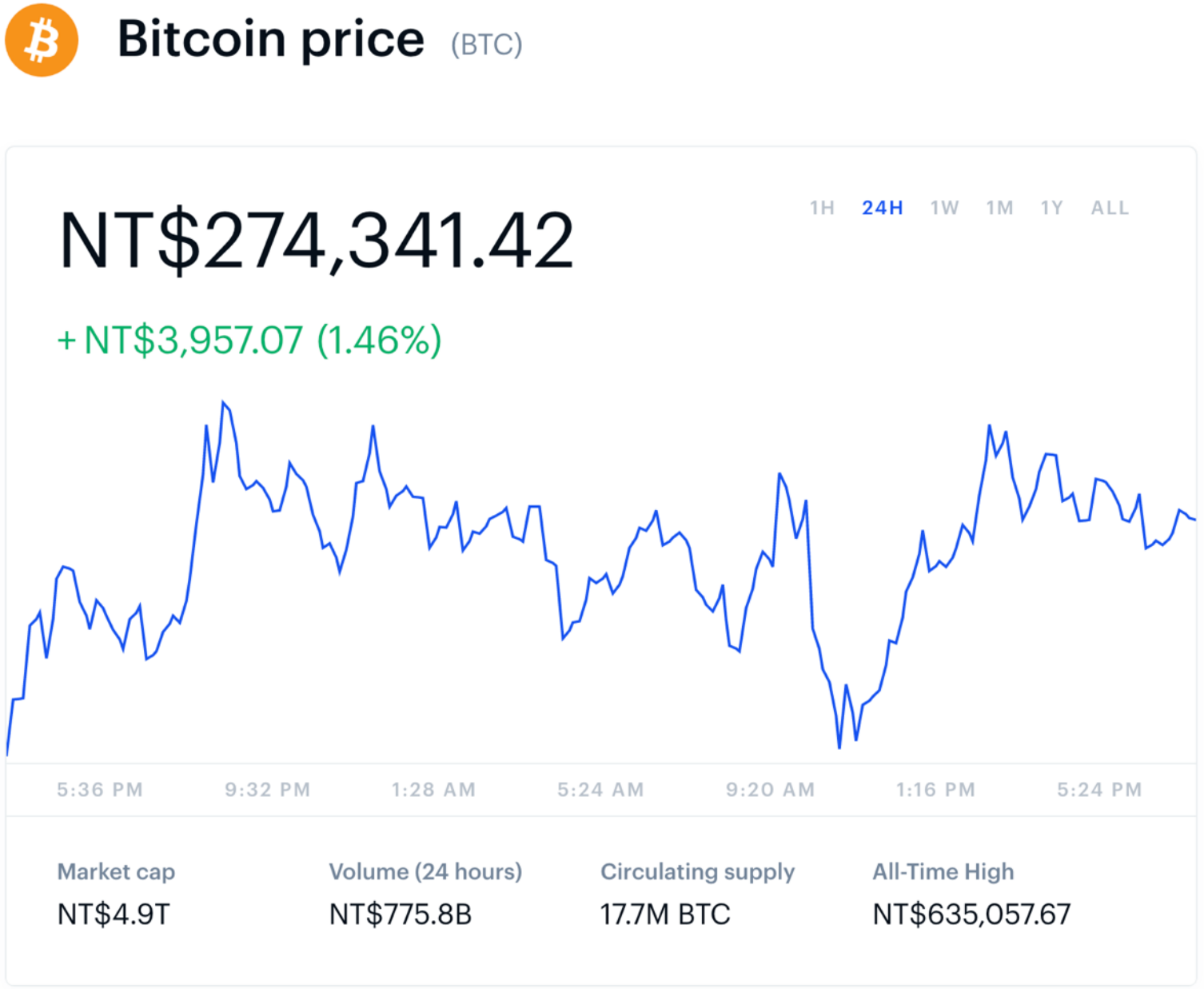
鏈上資產抵押型穩定幣

- 用戶將鏈上資產，送到智能合約進行超額抵押，以生成穩定幣
  - ex: DAI
- 公開透明
- 無需審批
- 機制設計複雜

MakerDAO

https://www.youtube.com/watch?v=J9q8hkyy8oM

Fluctuation



MAKER

Products Learn Foundation Community

Stability for the blockchain

Dai is an asset-backed, hard currency for the 21st century.
The first decentralized stablecoin on the Ethereum blockchain.

Buy DAI ▷ How it works

With Dai, anyone, anywhere has the freedom to
choose a money they can place their confidence in.
A money that maintains its purchasing power.

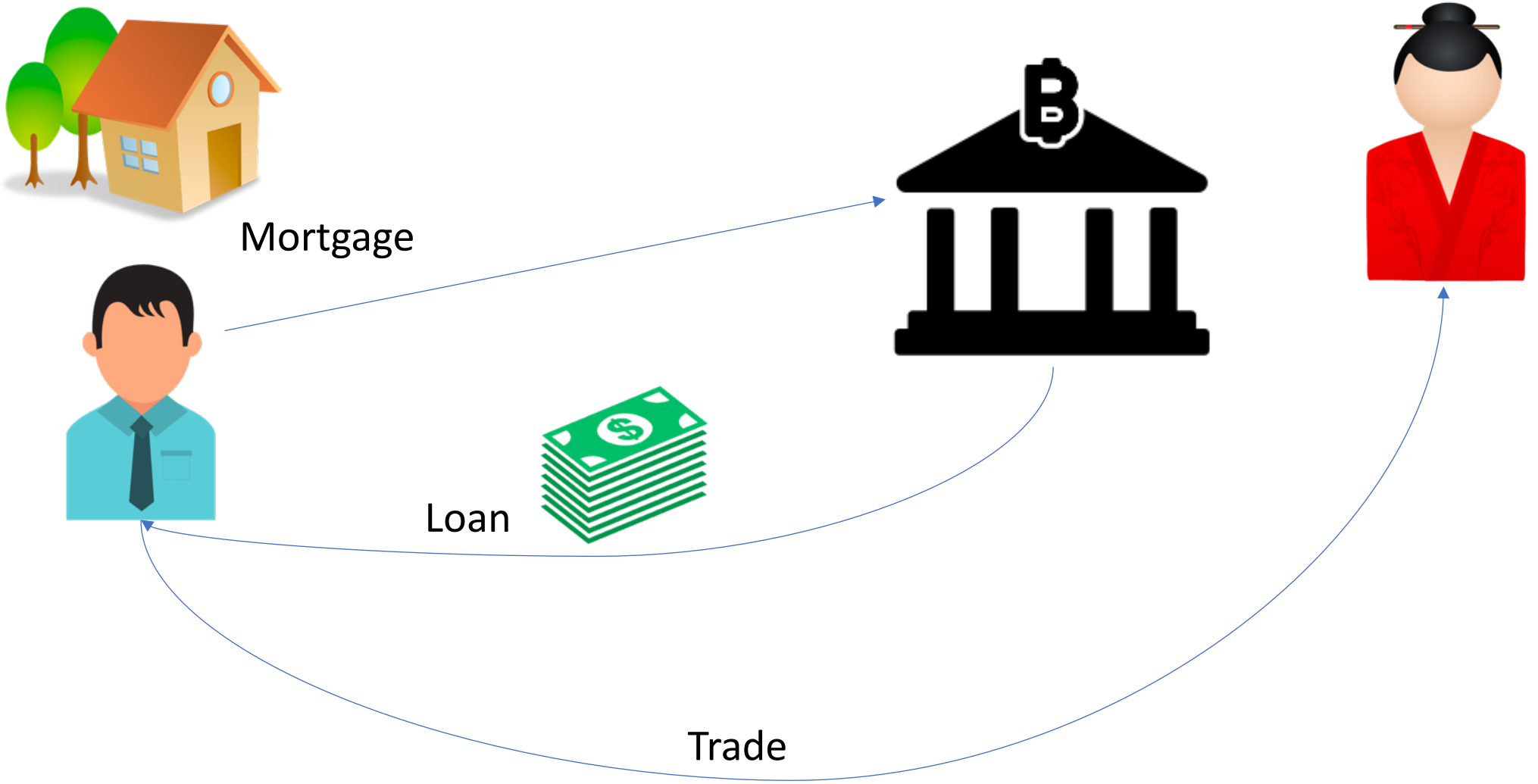
https://makerdao.com/en/

Stablecoin

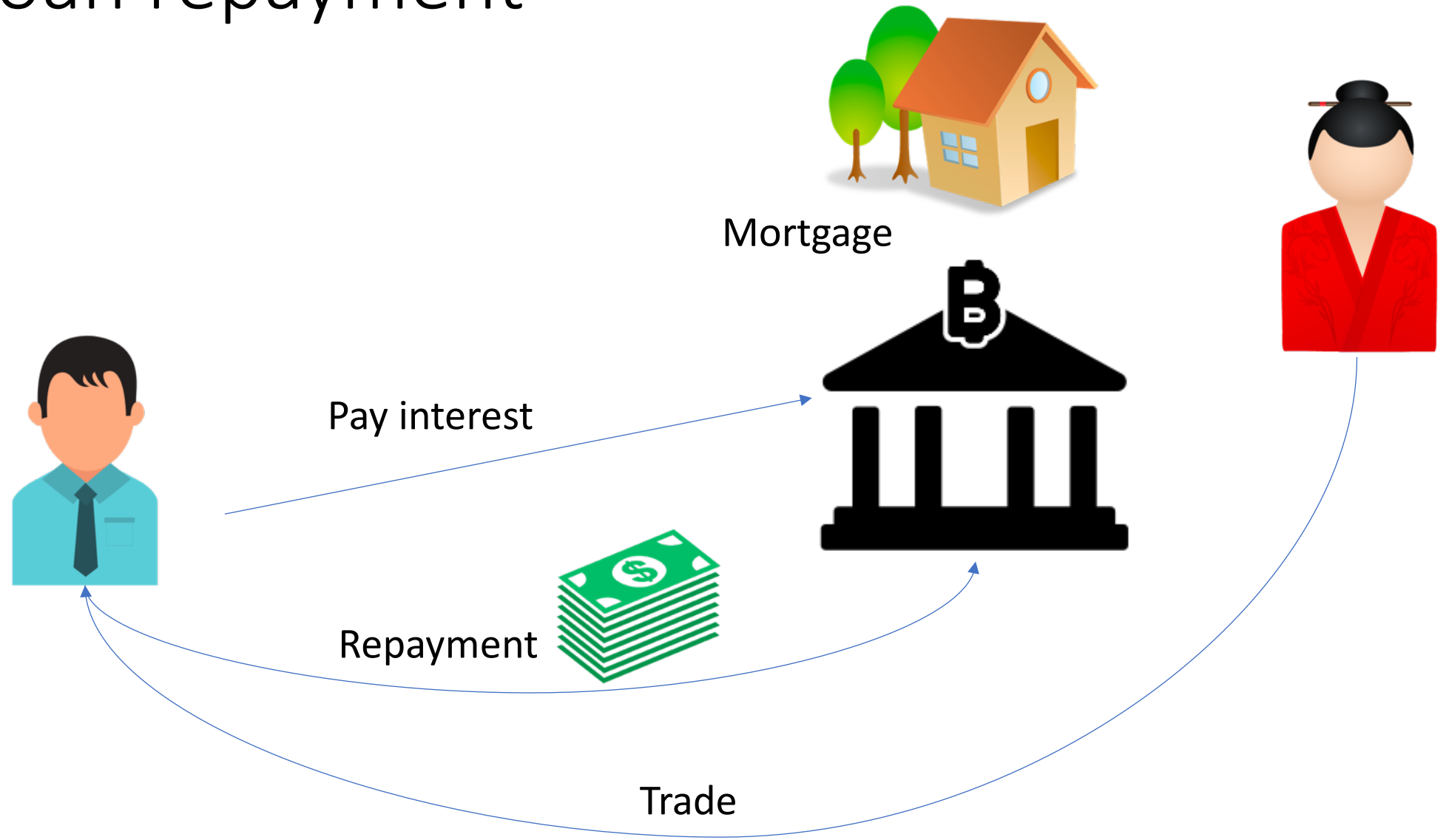
- Pegged 1 : 1 with USD
- Crypto-collateralized
  - A stable peg with an outside asset (e.g., ETH, BTC)
- Dai (借貸)

https://jpkoning.blogspot.com/2019/05/revisiting-stablecoins.html

Borrowing



Loan repayment

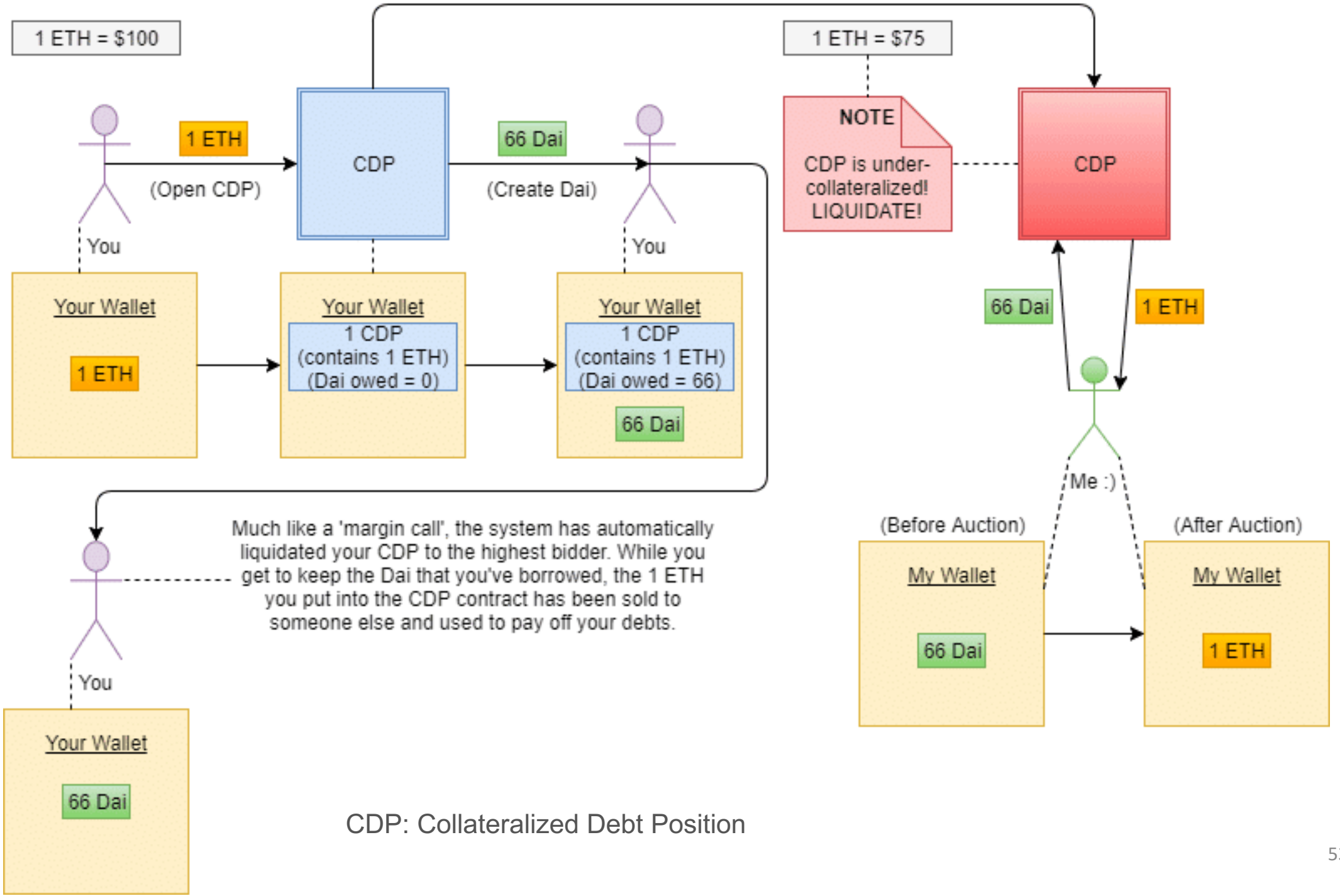


Liquidation

Auction

Pay interest

Trade

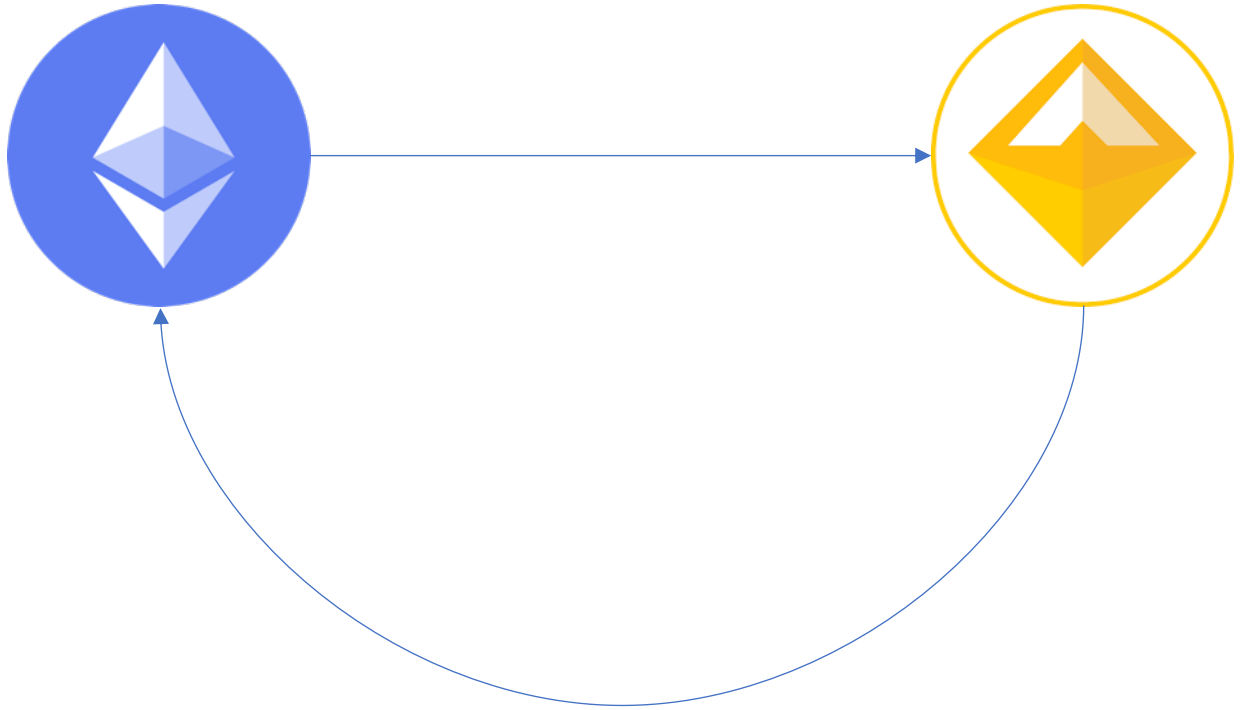


CDP: Collateralized Debt Position

經濟模型

- 抵押 Ether 產生穩定幣
- 抵押率 75% (1 ETH = $100 貸出 $75)
- 貸款利率 (10%)
- 還款，銷毀 DAI
  - 歸還等額 DAI + 利息
- 價格即將低於貸出 DAI 價格時，啟動清算
- 拍賣 Ether

槓桿



差異 (優勢)

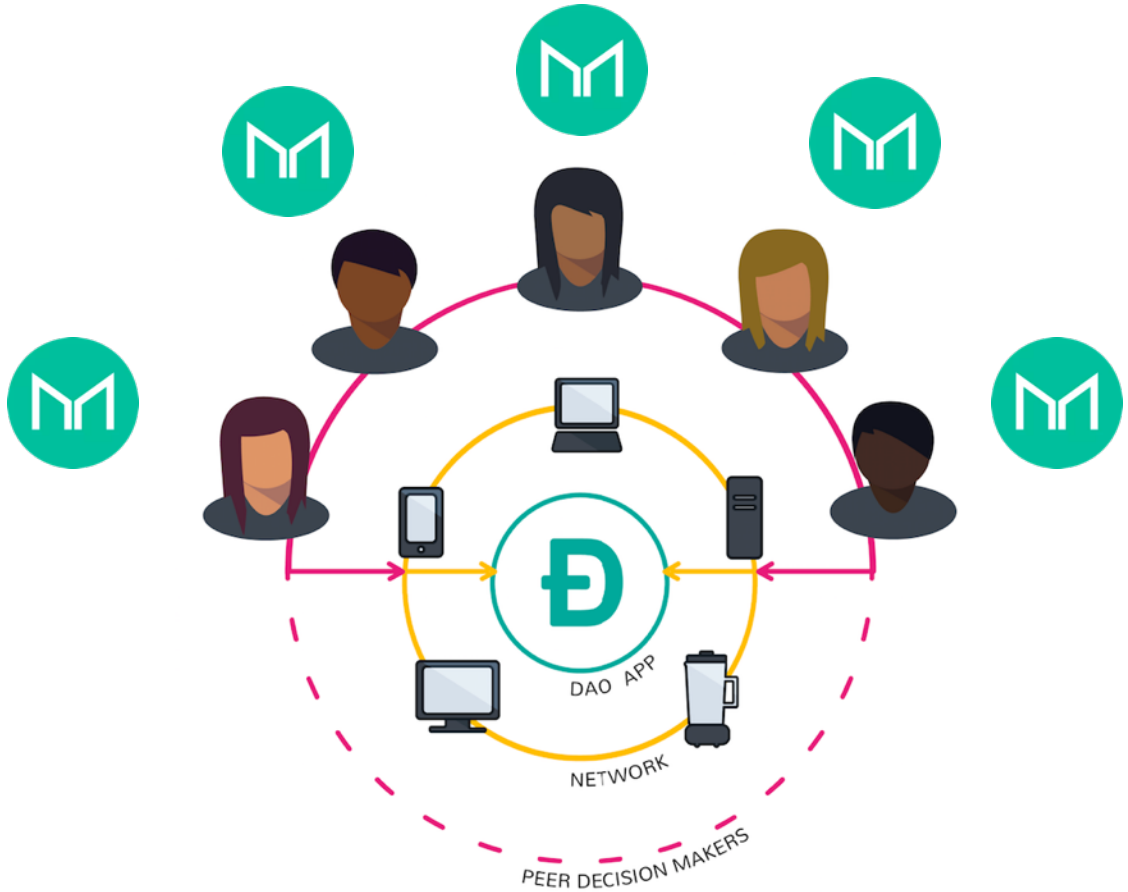
- 即借即貸
- 不用擔心 KYC 或是信貸問題
- 不用擔心被特別審查
- 不用擔心銀行倒
- 不用走審批流程
- 無人管理系統
- 自動化

預測

- 市場供需預測價格

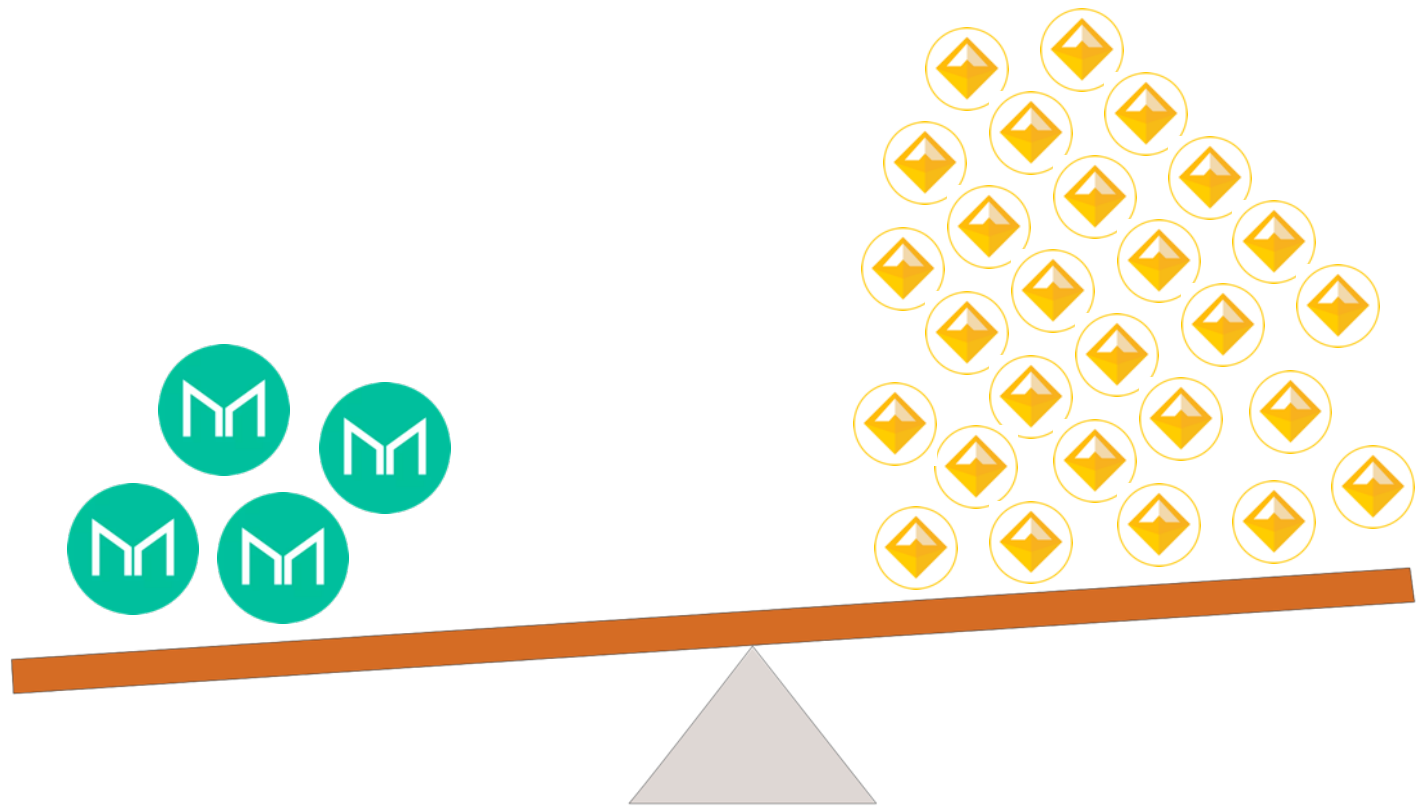
DAO

- Decentralized Autonomous Organization (DAO)



擔保

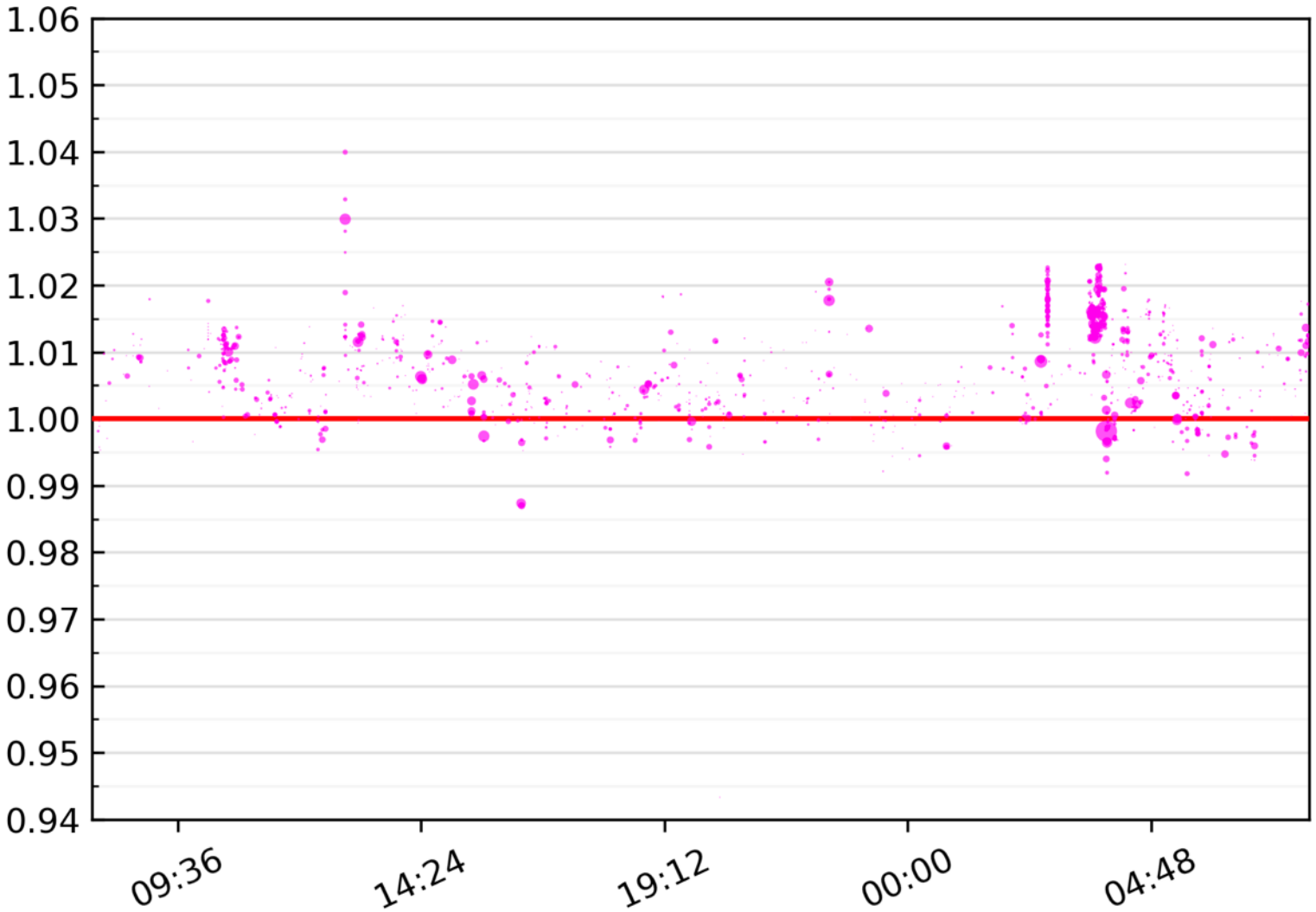
- 價格波動，誰來承擔
- 價格偏高
- 價格偏低
- 價格驟降



MKR

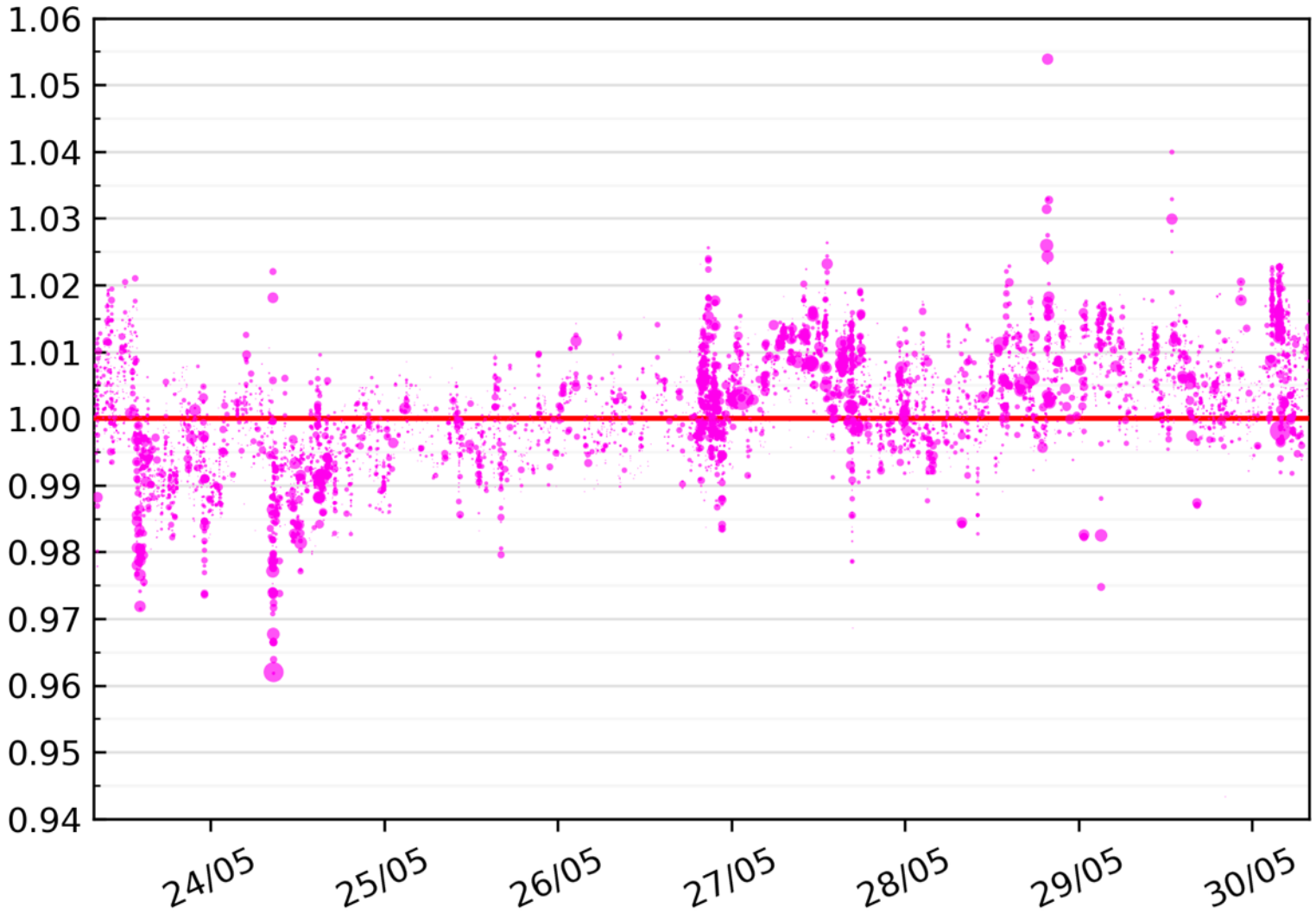
- 收益
- 價格驟降
- DAO (治理)

1 Day



https://dai.stablecoin.science/

1 Week



https://dai.stablecoin.science/

Dai Charts


Linear Scale
Log Scale
Zoom 1d 7d 1m 3m 1y YTD ALL
From Dec 27, 2017 To Jun 14, 2019
Market Cap
$100M
$75M
$50M
$25M
$0
Price (USD)
$1.04
$1.00
$0.960000
$0.920000
$0.880000
Price (BTC)
0.00048 BTC
0.00036 BTC
0.00024 BTC
0.00012 BTC
0 BTC
24h Vol
60M
0
Jan '18
Mar '18
May '18
Jul '18
Sep '18
Nov '18
Jan '19
Mar '19
May '19
Jan '18
Jul '18
Jan '19

Tether Charts

Thanks

Q & A