以太坊原理與應用開發

Ethereum DApp Development

http://ethereum.org/

以太坊原理與應用開發

- 授課教師
  - 陳昶吾 - changwu@nccu.edu.tw
- 課程
  - 時間: 星期三 (13:10-16:00)
  - 地點: 大仁 200102 教室
  - Office hours: Anytime on slack
- 課程大綱
  - 網址: http://bit.ly/nccu-eth-108

協作平台

- Moodle
- Slack
  - https://nccu-eth-slack.herokuapp.com/
  - 輸入你的 Email
  - 輸入 invite token: nccu

Syllabus

Week	Topic*	Lecture Hours	Outside of Class Hours
1	09/11: Introduction to Blockchain	3	3
2	09/18: Ethereum I (Protocol)	3	3
3	09/25: Ethereum II (Protocol) **(Forming teams for group project)**	3	3
4	10/02: Wallet, Key & Node Management **(Homework 1)**	3	3
5	10/09: Solidity Programming	3	3
6	10/16: Truffle & Ganache **(Homework 2)**	3	3
7	10/23: Contract Applications & Token model	3	3
8	10/30: Smart Contract Security Best Practices	3	3
9	**11/06: Midterm**	3	3

Syllabus

Week	Topic*	Lecture Hours	Outside of Class Hours
10	**11/13: Project Proposal Presentation**	3	3
11	11/20: Oracle, Proxy Contract, Random Number **(Homework 3)**	3	3
12	11/27: Auction, Ethereum Name Service	3	3
13	12/04: Decentralized Exchange	3	3
14	12/11: Stablecoin & DeFi Applications **(Homework 4)**	3	3
15	12/18: Privacy-Preserving Applications & DAO	3	3
16	12/25: Ethereum 2.0	3	3
17	**01/01: New Year's Day**	0	0
18	**01/08: Final Project Presentation**	3	3

Tickets

EDU	Early Bird	Regular
NT512	NT1024	NT1200
Oct 18 - Aug 26 Requires valid student/lecturer ID	Save 15% today Aug 26 - Sep 15	Sep 16 - Oct 18
BUY TICKET	BUY TICKET	BUY TICKET

*Tickets grant access to all conference sections, coffee breaks, lunch and party. Accommodation is NOT included in the ticket price.

https://crosslink.taipei/

課程目標

- 了解區塊鏈
- 認識以太坊協定
- 撰寫智能合約應用
- 區塊鏈挑戰與限制

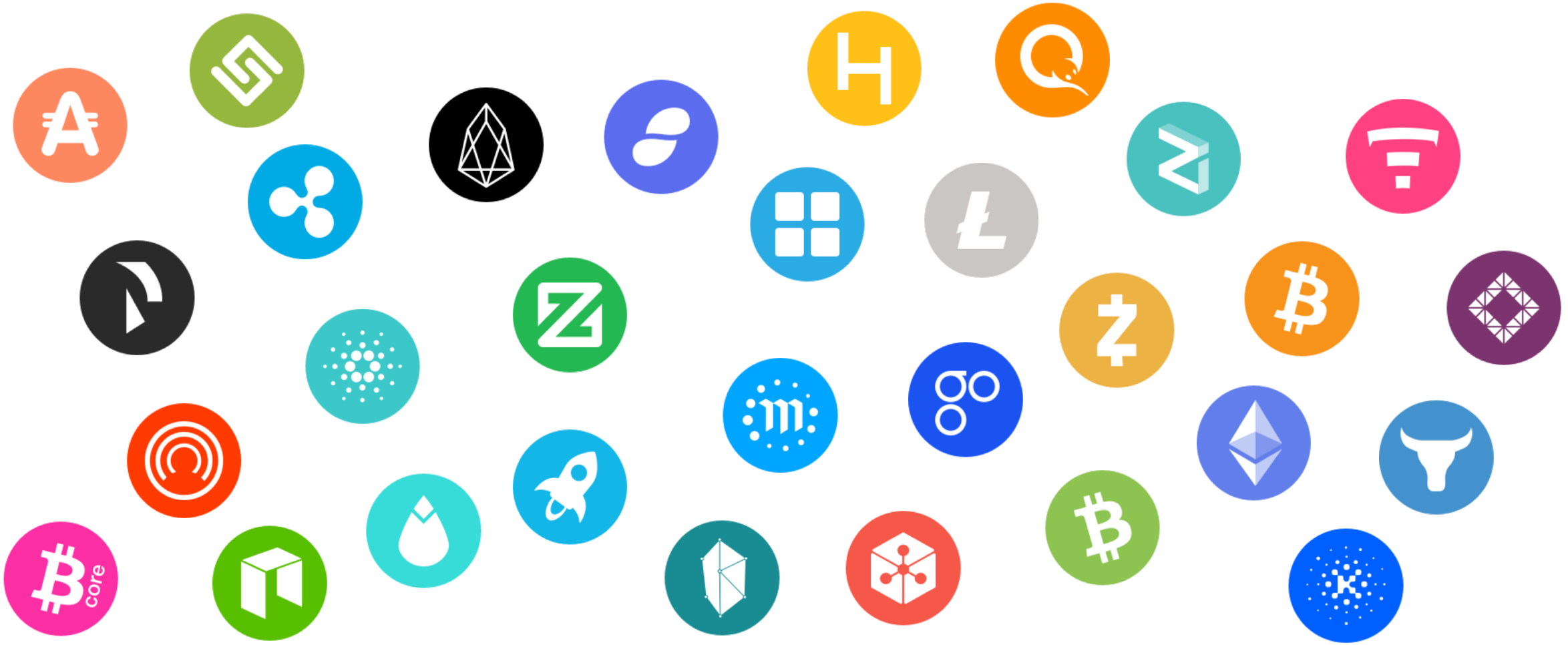
評分標準

- (10%) Class participation
- (40%) Programming assignments
- (20%) Midterm
- (30%) Final project
  - (20%) Implementation
  - (10%) Presentation

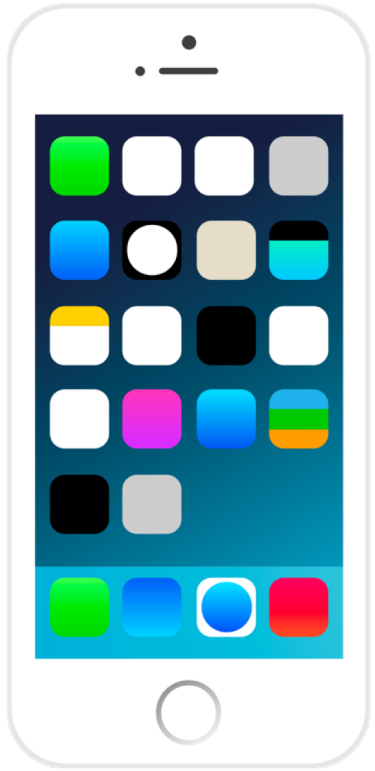
預備知識

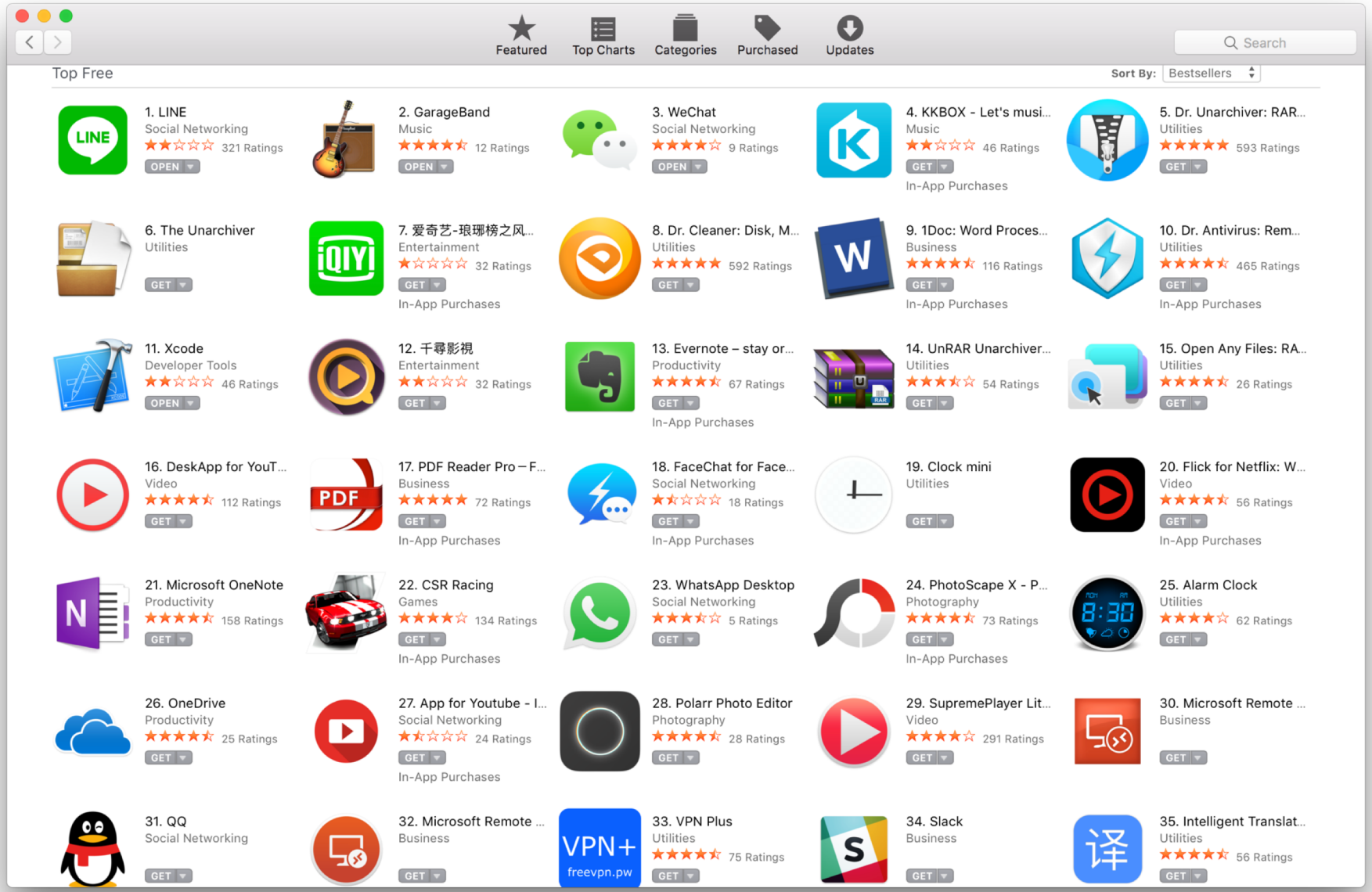
- 密碼學
- 分散式系統
- P2P 網路
- 熟稔一門程式語言 (Golang, Python, Java etc.)

Cryptocurrency (加密貨幣/密碼貨幣)



App Store




Featured
Top Charts
Categories
Purchased
Updates
Search
Top Free
Sort By: Bestsellers
1. LINE
Social Networking
321 Ratings
OPEN
2. GarageBand
Music
12 Ratings
OPEN
3. WeChat
Social Networking
9 Ratings
OPEN
4. KKBOX - Let's musi...
Music
46 Ratings
GET
In-App Purchases
5. Dr. Unarchiver: RAR...
Utilities
593 Ratings
GET
6. The Unarchiver
Utilities
GET
7. 爱奇艺-琅琊榜之风...
Entertainment
32 Ratings
GET
In-App Purchases
8. Dr. Cleaner: Disk, M...
Utilities
592 Ratings
GET
9. 1Doc: Word Proces...
Business
116 Ratings
GET
In-App Purchases
10. Dr. Antivirus: Rem...
Utilities
465 Ratings
GET
In-App Purchases
11. Xcode
Developer Tools
46 Ratings
OPEN
12. 千尋影視
Entertainment
32 Ratings
GET
13. Evernote – stay or...
Productivity
67 Ratings
GET
In-App Purchases
14. UnRAR Unarchiver...
Utilities
54 Ratings
GET
15. Open Any Files: RA...
Utilities
26 Ratings
GET
16. DeskApp for YouT...
Video
112 Ratings
GET
17. PDF Reader Pro – F...
Business
72 Ratings
GET
In-App Purchases
18. FaceChat for Face...
Social Networking
18 Ratings
GET
In-App Purchases
19. Clock mini
Utilities
GET
20. Flick for Netflix: W...
Video
56 Ratings
GET
In-App Purchases
21. Microsoft OneNote
Productivity
158 Ratings
GET
22. CSR Racing
Games
134 Ratings
GET
In-App Purchases
23. WhatsApp Desktop
Social Networking
5 Ratings
GET
24. PhotoScape X - P...
Photography
73 Ratings
GET
In-App Purchases
25. Alarm Clock
Utilities
62 Ratings
GET
26. OneDrive
Productivity
25 Ratings
GET
27. App for Youtube - I...
Social Networking
24 Ratings
GET
In-App Purchases
28. Polarr Photo Editor
Photography
28 Ratings
GET
29. SupremePlayer Lit...
Video
291 Ratings
GET
30. Microsoft Remote ...
Business
GET
31. QQ
Social Networking
GET
32. Microsoft Remote ...
Business
GET
33. VPN Plus
Utilities
75 Ratings
GET
34. Slack
Business
GET
35. Intelligent Translat...
Utilities
56 Ratings
GET

Top 100 Cryptocurrencies By Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$112,902,556,502	$6,559.79	$4,778,625,083	17,211,300 BTC	8.14%	
2	Ethereum	$30,707,104,525	$303.00	$1,919,670,181	101,343,286 ETH	17.19%	
3	XRP	$11,790,741,661	$0.299467	$321,666,561	39,372,399,467 XRP *	15.18%	
4	Bitcoin Cash	$9,258,875,705	$535.37	$378,266,882	17,294,413 BCH	10.22%	
5	EOS	$4,398,457,819	$4.85	$676,318,559	906,245,118 EOS *	12.10%	
6	Stellar	$4,287,214,056	$0.228386	$88,792,978	18,771,749,250 XLM *	7.81%	
7	Litecoin	$3,397,925,872	$58.73	$285,153,629	57,858,159 LTC	13.73%	
8	Cardano	$2,584,812,664	$0.099696	$84,247,959	25,927,070,538 ADA *	10.46%	
9	Tether	$2,410,238,602	$1.00	$3,074,803,898	2,407,140,346 USDT *	-0.17%	
10	Monero	$1,526,847,712	$93.56	$25,261,244	16,319,775 XMR	15.29%	

Blockchain Primitives

起源

Bitcoin (比特幣)

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 (201?)**
- 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

信任的基礎

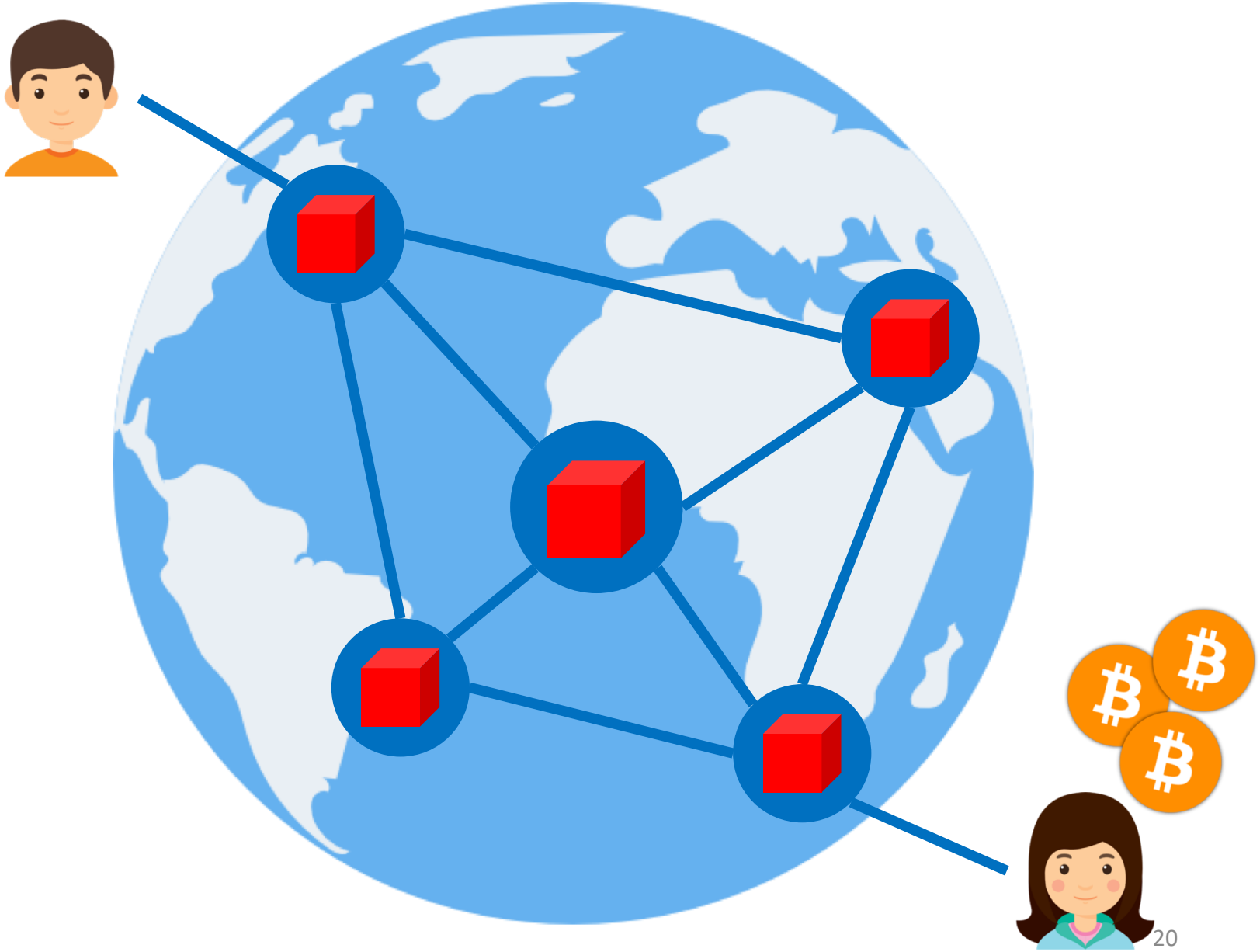
人類社會

社會信任 (制度); 商業信任 (契約); 政府背書

資訊系統

區塊鏈(?)

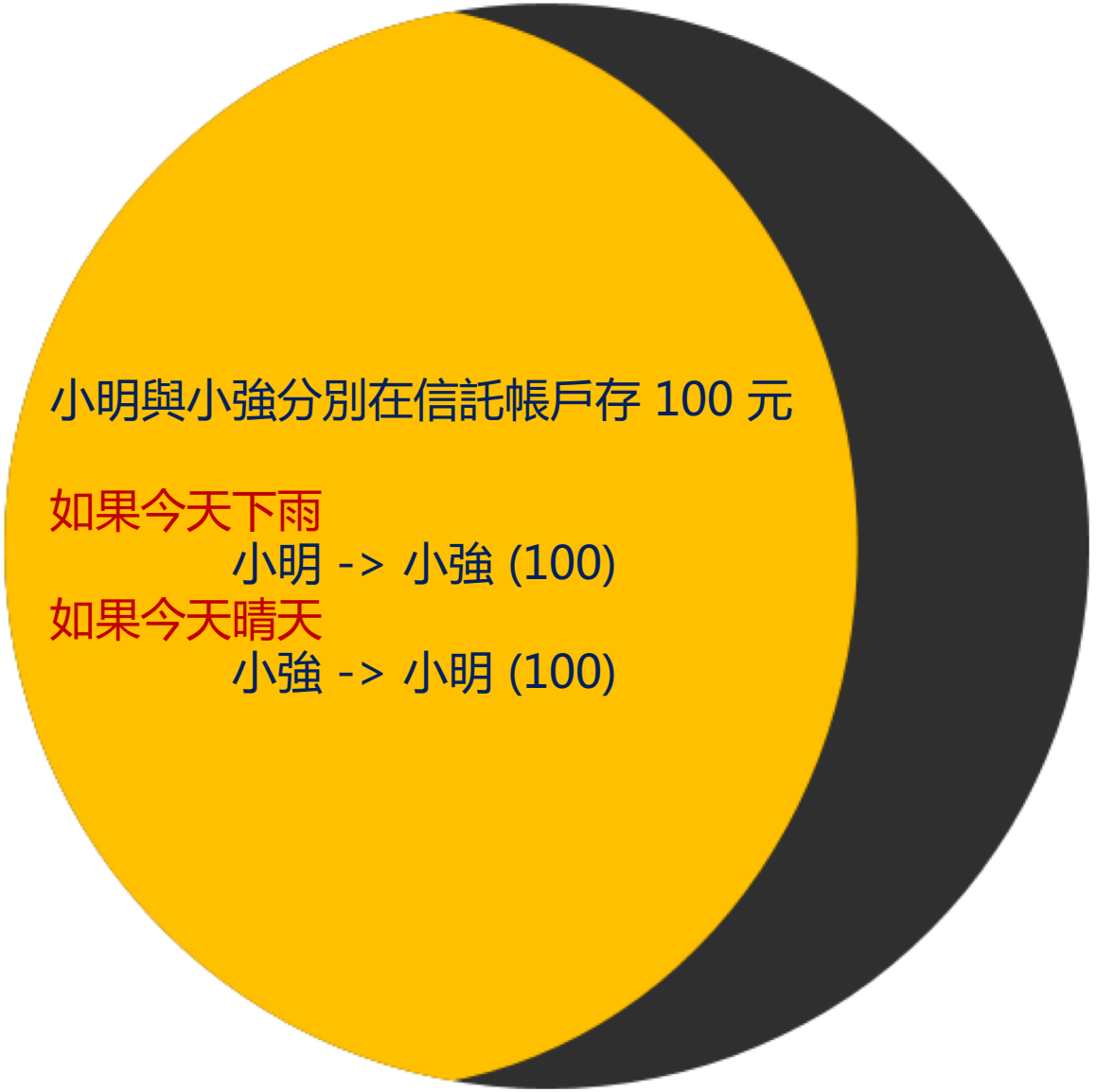
分散式帳本



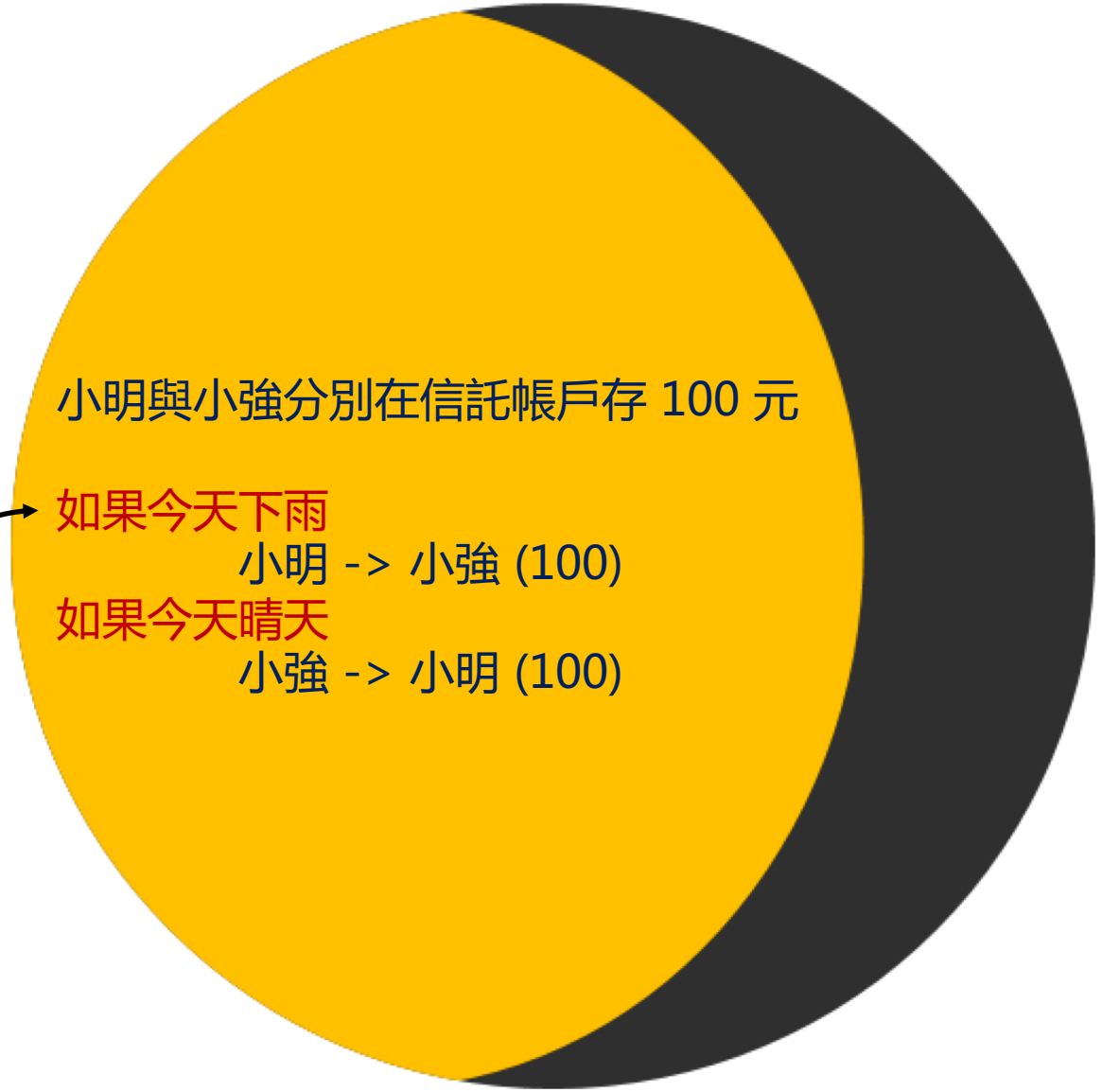
信任媒介 (區塊鏈)

分散式系統、密碼學、機制設計

智能合約



智能合約

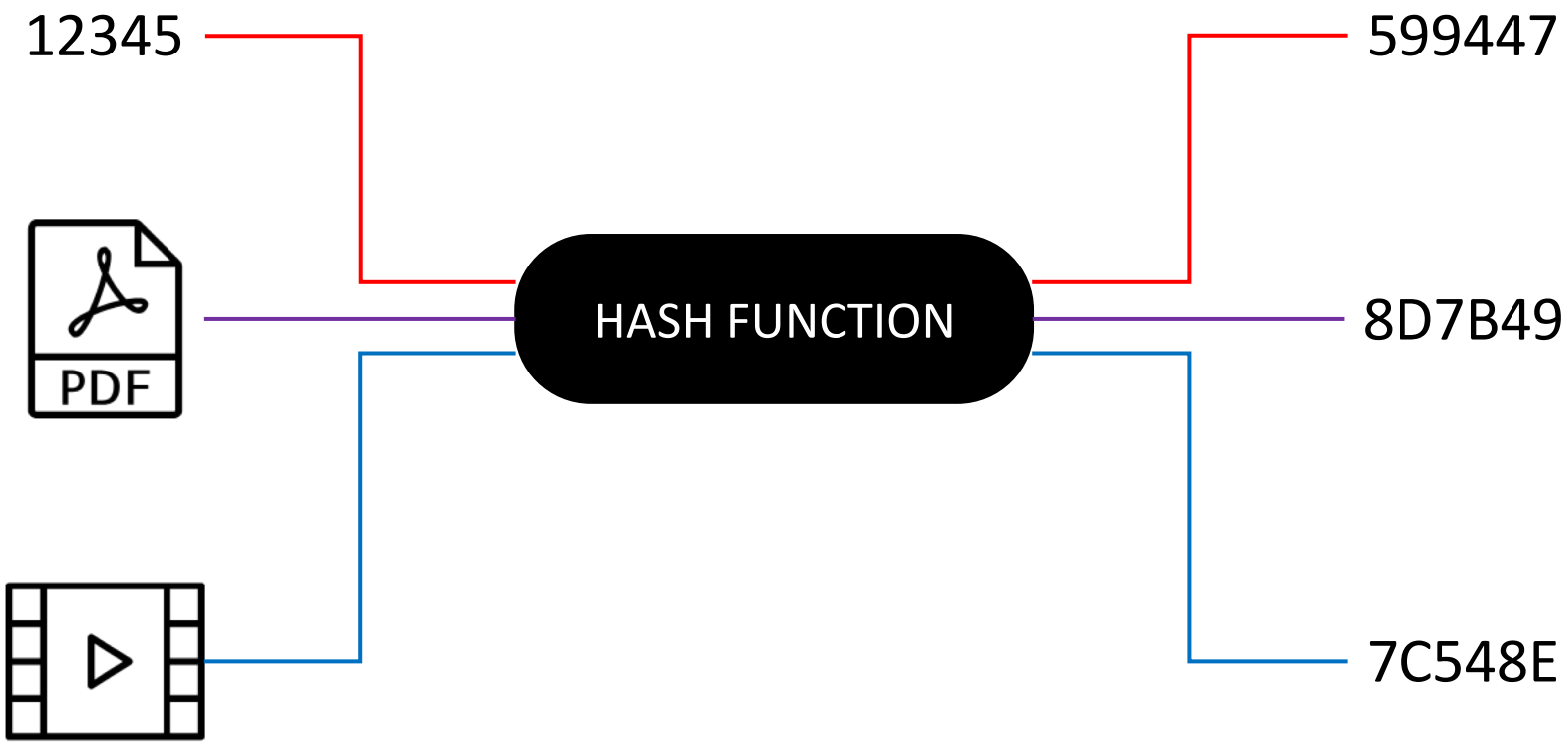


資訊來源?

Oracle

Hash function

```
2. changwu@changwu-mbp: ~ (zsh)
(⎈ |ws:ws)sha256 12345
5994471ABB01112AFCC18159F6CC74B4F511B99806DA59B3CAF5A9C173CACFC5
(⎈ |ws:ws)sha256 /Users/changwu/Desktop/Screen\ Shot\ 2018-09-03\ at\ 11.26.20\ AM.png
8D7B49815818A27ED1F9B5F71B53AF9AB9104CF1EF51A340FA6D6763036FF6E4
(⎈ |ws:ws)sha256 /Users/changwu/An_Overview_Of_Governance_In_Blockchains.webm
7C548EBA8675AE0970D688C394C286A06A67D8D79ACAC33378208076BC2C0EC1
(⎈ |ws:ws)_
```

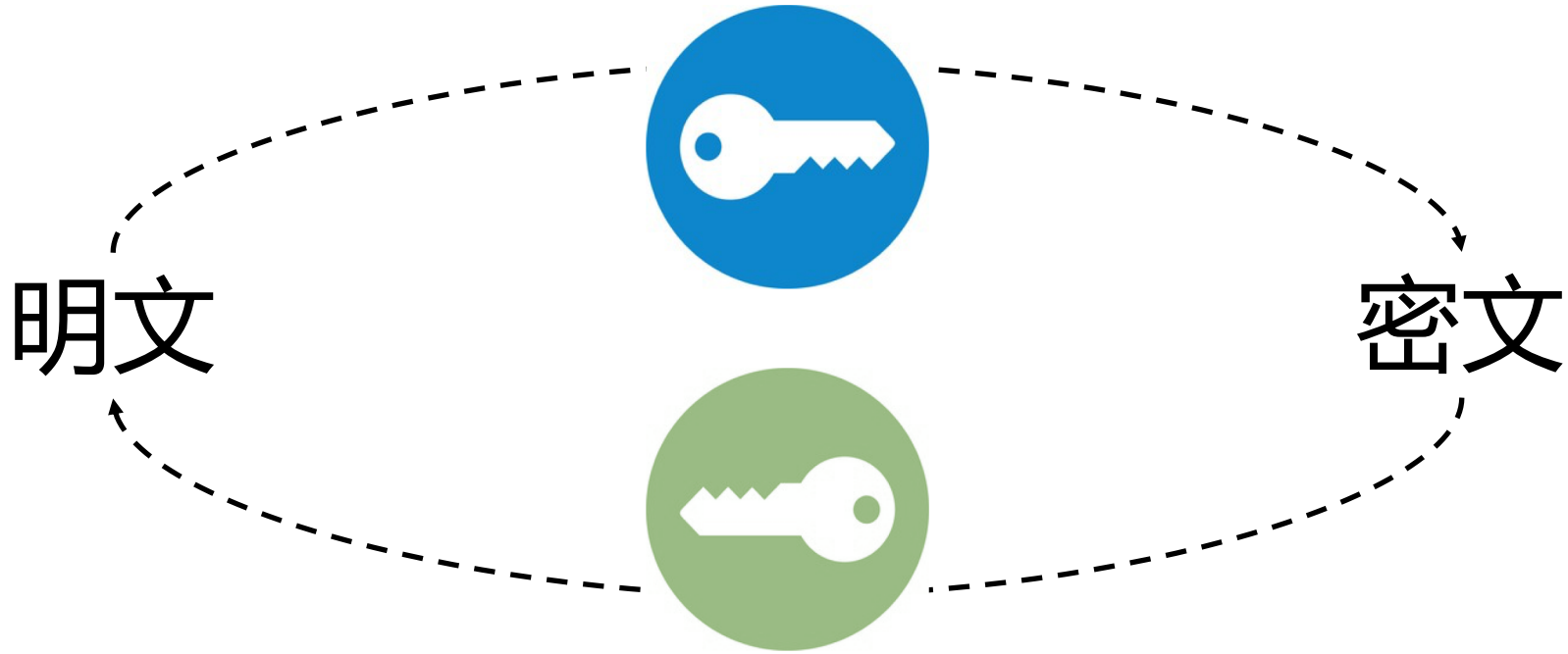


- Deterministic
- Fast
- Irreversibility
- Randomness
- Collision resistant

Hash function

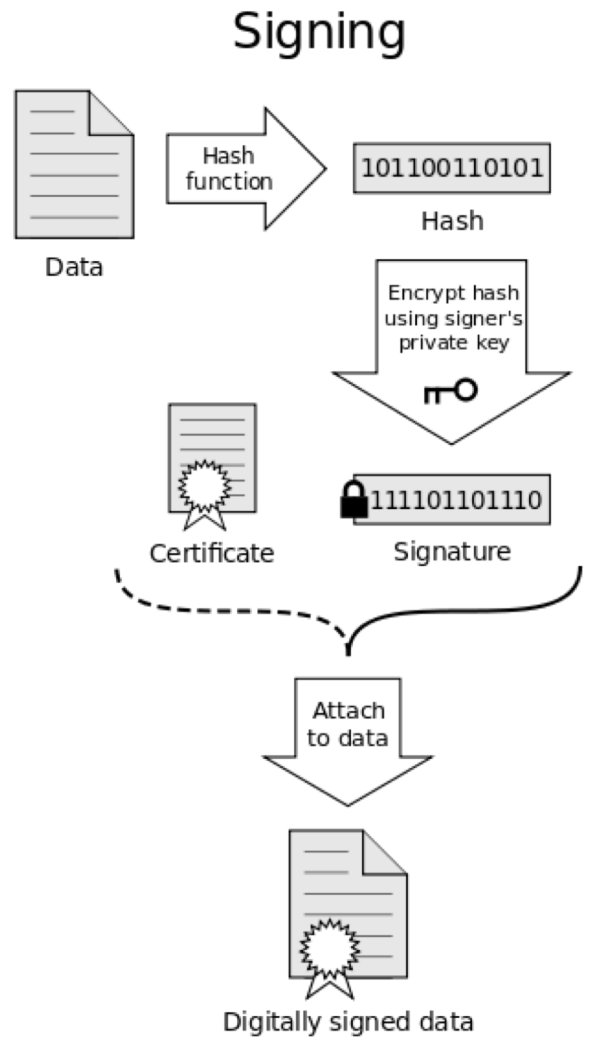
- 資料完整性
  - Checksums
  - Password hashing
- Proof of Work
  - Mathematical puzzle
- 資料身份性
  - Hash table
  - P2P networks
  - TX ID

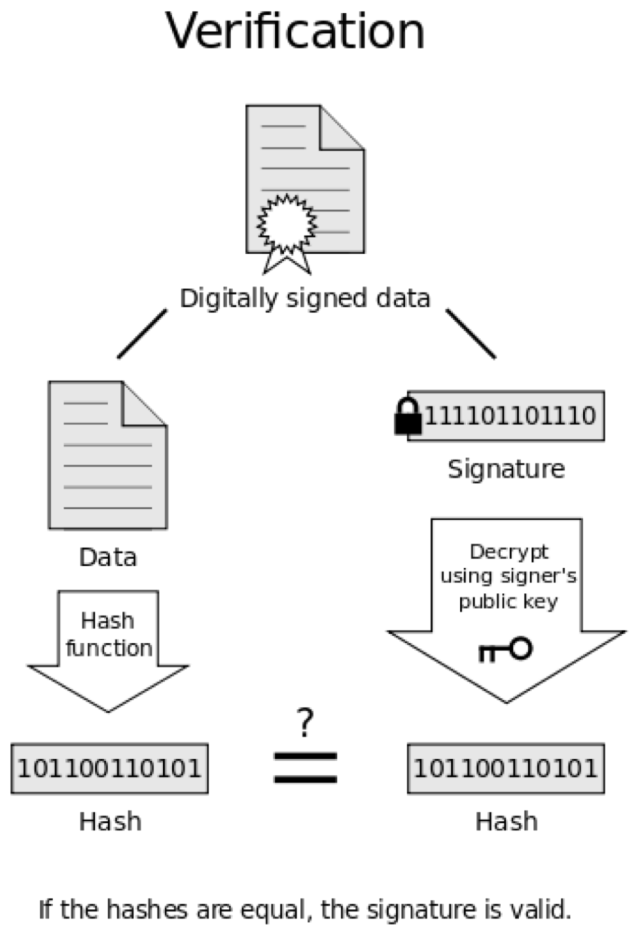
Public Key Cryptography



私鑰簽名
公鑰加密
→
公鑰驗證
私鑰解密

Digital signature

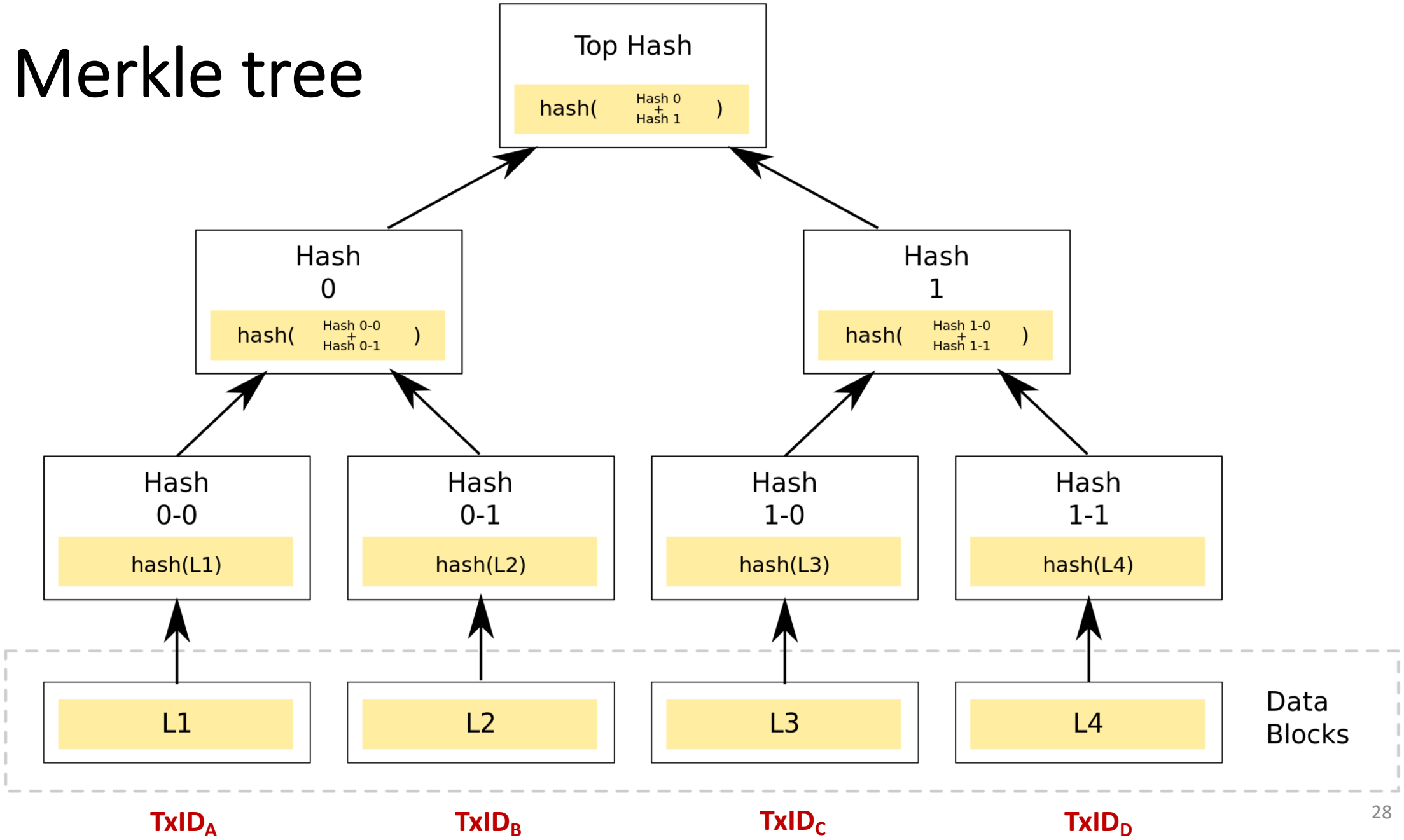




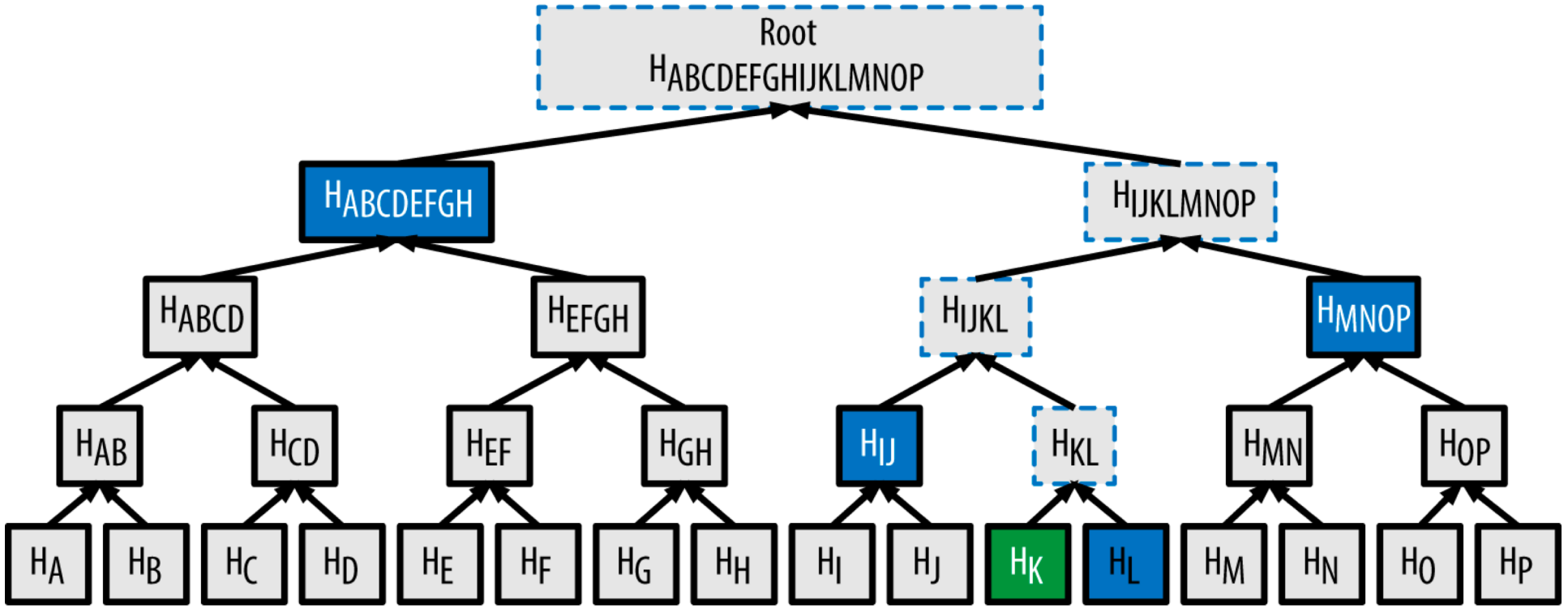
Source: https://en.wikipedia.org/wiki/Electronic_signature

Source: https://en.bitcoinwiki.org/wiki/Merkle_tree

Merkle tree

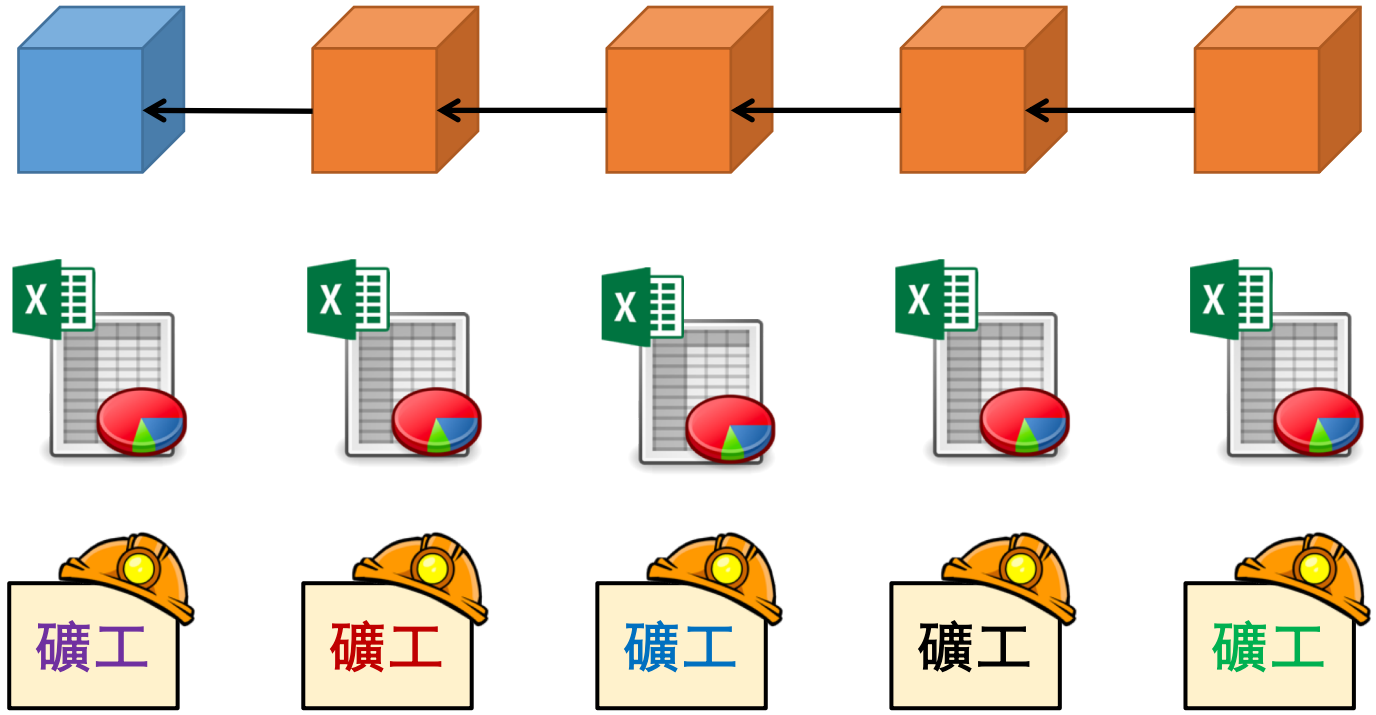


Merkle branch



Source: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html

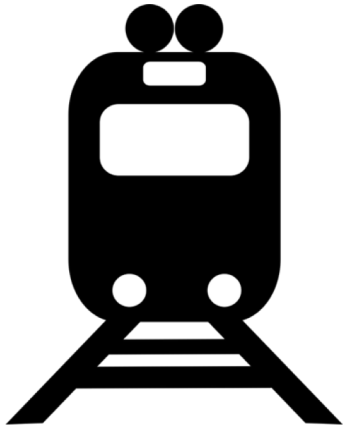
Blockchain (區塊鏈)



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

證書

Mateo Nakach

Alumnus

MIT Global Entrepreneurship Bootcamp

Cambridge, Massachusetts, August 18-22, 2014

This certificate identifies you as an alumnus of the MIT Global Entrepreneurship Bootcamp and verifies your membership in the the bootcamp alumni community.

Chi-Chu Tschang

Co-founder, MIT Global Entrepreneurship Bootcamp

A project by the Media Lab Learning Initiative + MIT Global Entrepreneurship Bootcamp that critically explores notions of social capital and reputation, empathy and gift economies, and social behavior. Digital certificates are registered on the blockchain, cryptographically signed, and tamper proof.

Verify certificate

Public Key: 1GuqT4EpnhmA6GQvA3Fz5JWPjcZyXSQpFw

Blockchain Address: 00655ebd91dba1dc27acc0de66a90d270ab4297d631dcc0dc4ad24fbf5a5c78b

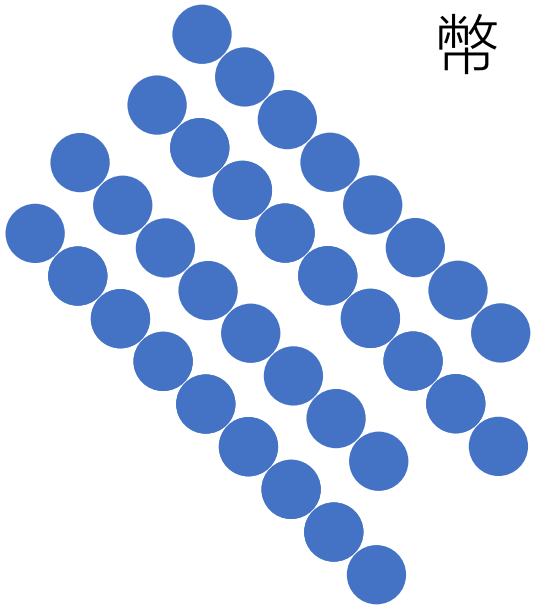
http://certificates-bootcamp.mit.edu/

代幣模型

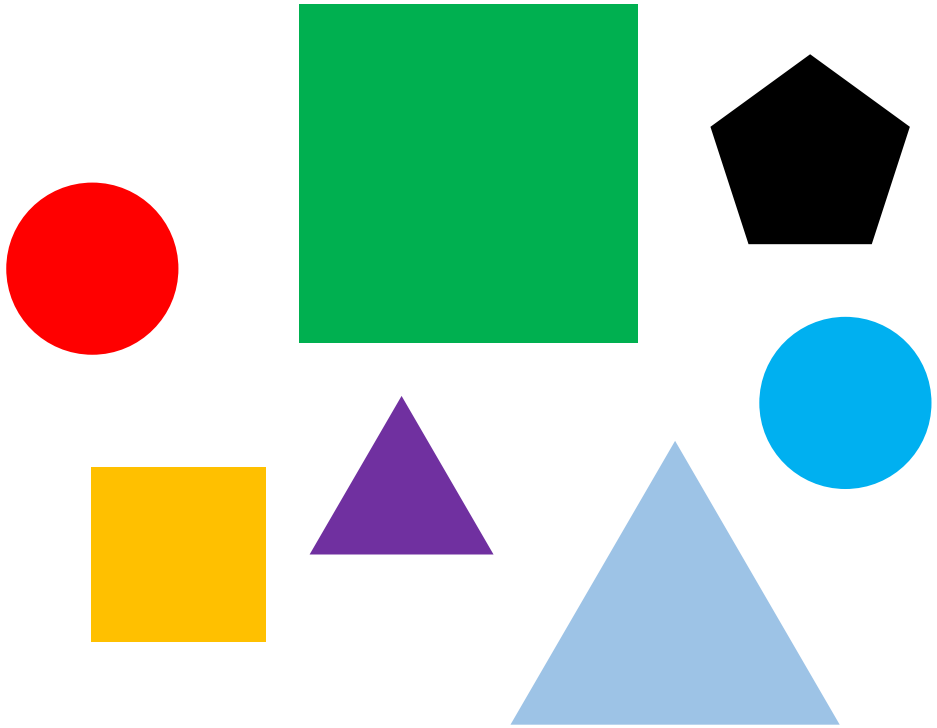
- Payment token (貨幣)
- Security token (股票)
- Utility token (代幣/車票)

代幣

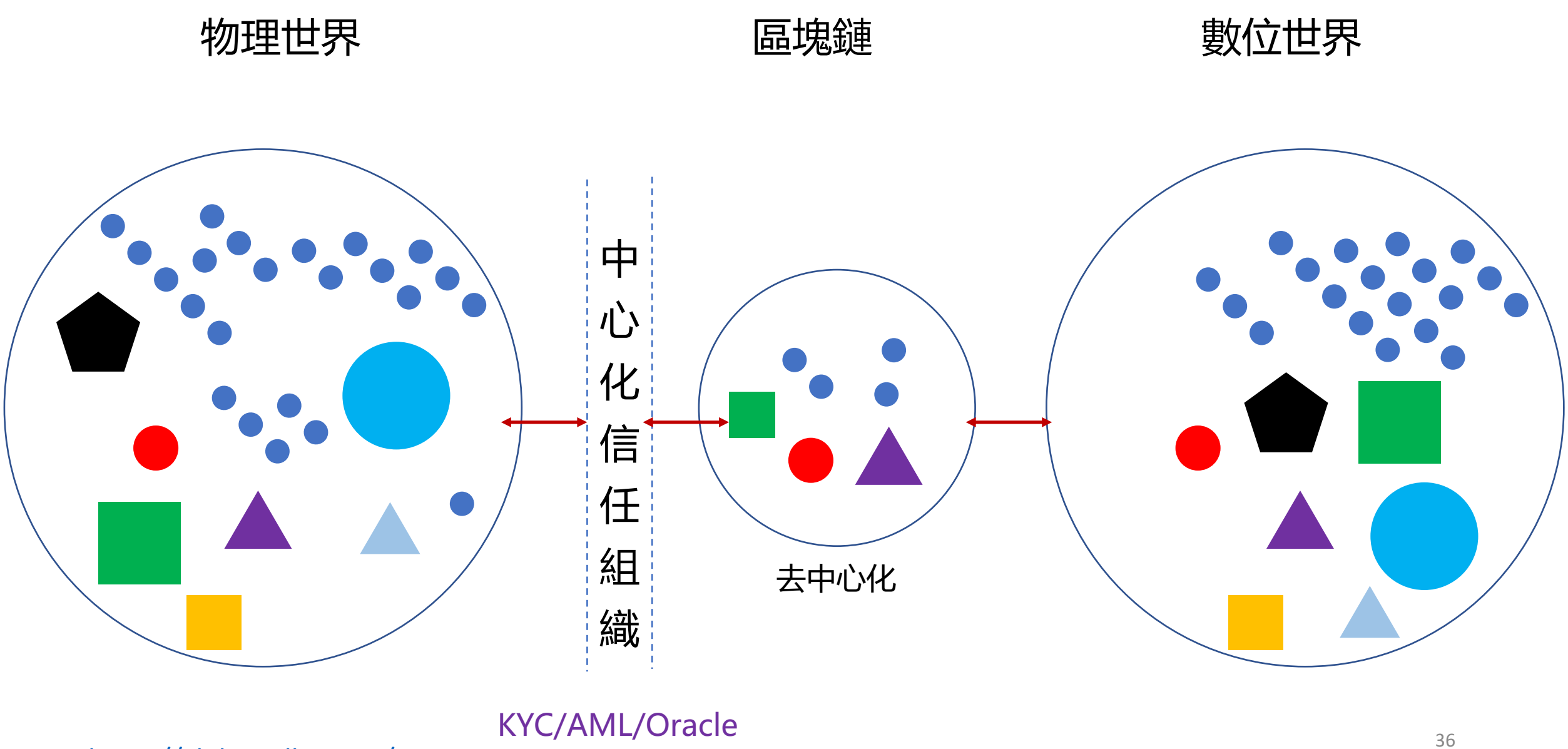
幣



人 / 事 / 物 / 權

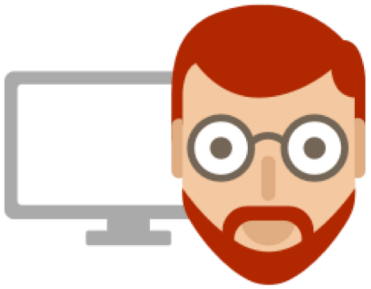


Source: https://alphawallet.com/



Source: https://alphawallet.com/

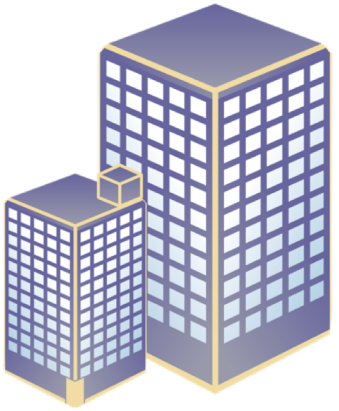
開發者/研究員



礦工

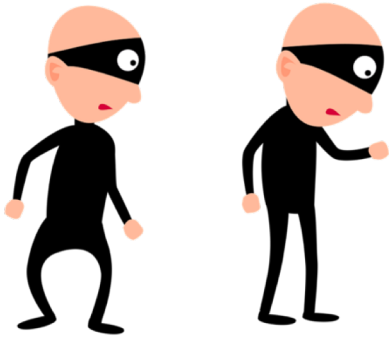
政府/監管單位

企業/組織

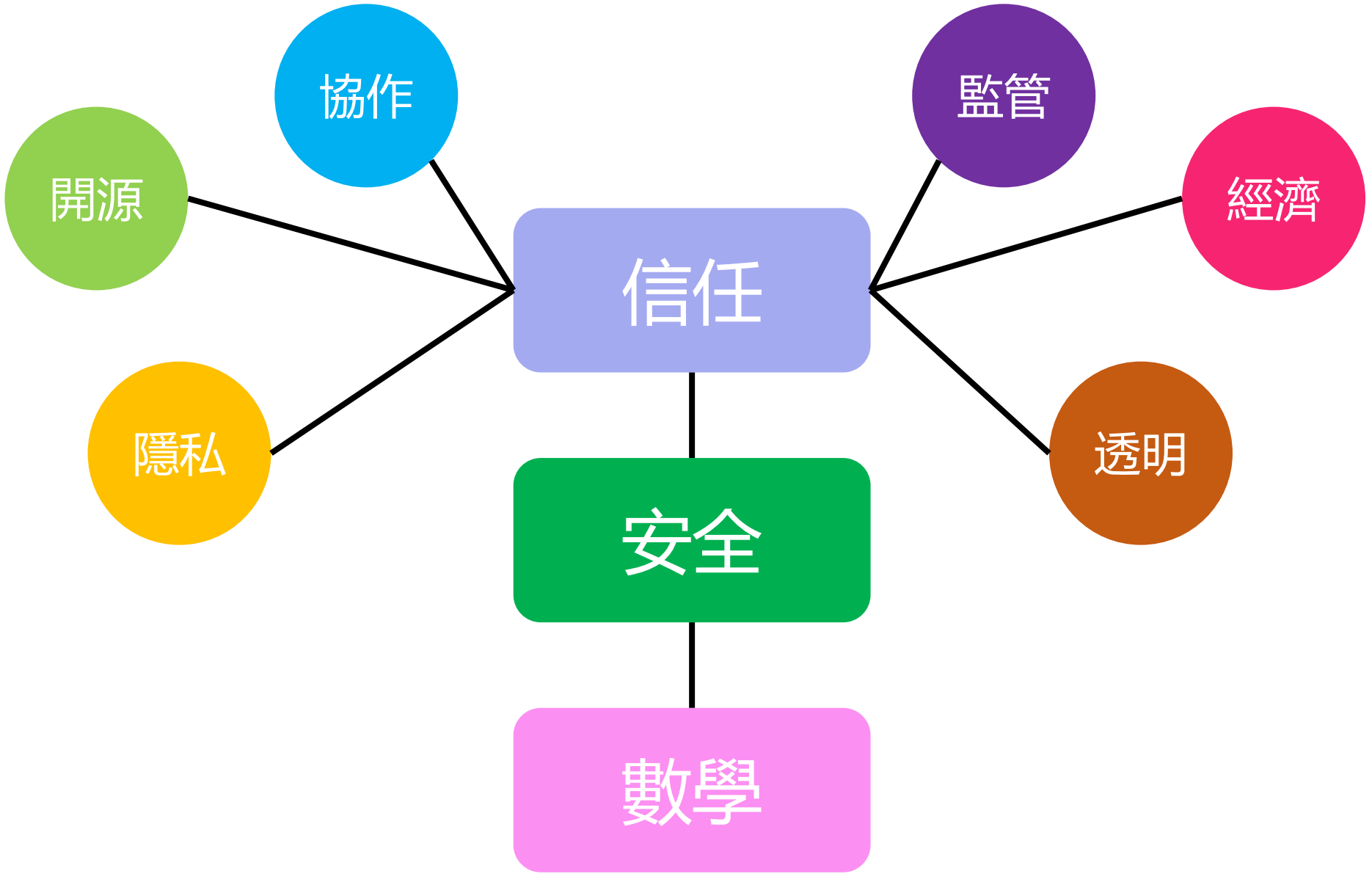


使用者/投資客

交易所



駭客/詐欺犯


協作
開源
監管
經濟
信任
隱私
透明
安全
數學

Decentralized Finance

DeFi

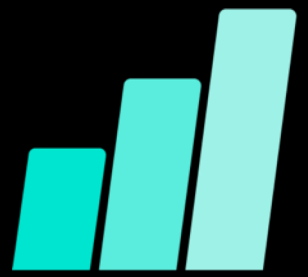
Finance

- 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/

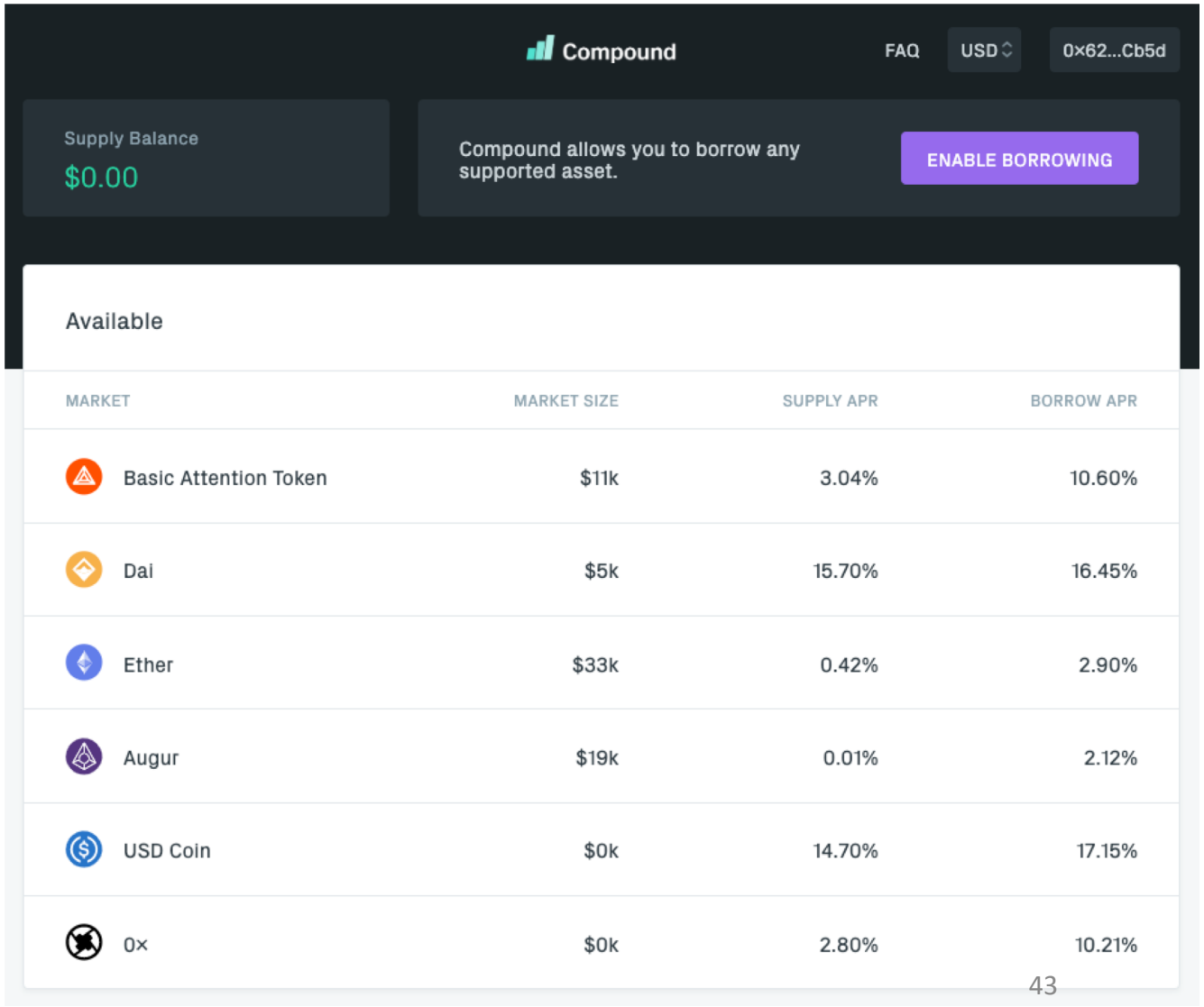


Compound

https://compound.finance/

Compound your Crypto

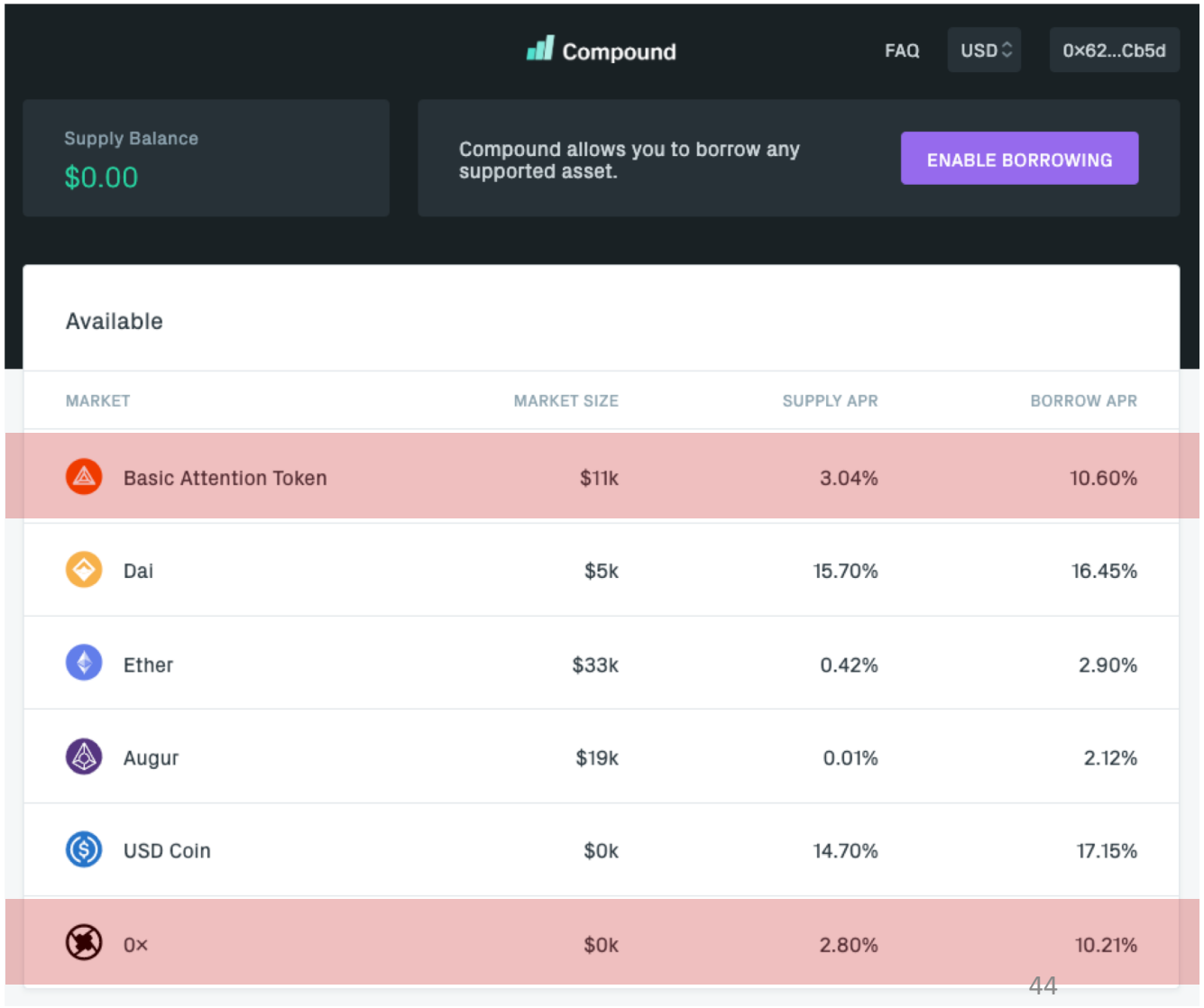
- An open-source protocol for algorithmic, efficient Money Markets on the Ethereum blockchain.



Compound your Crypto

- An open-source protocol for algorithmic, efficient Money Markets on the Ethereum blockchain.

放高利貸
借貸



Prepared

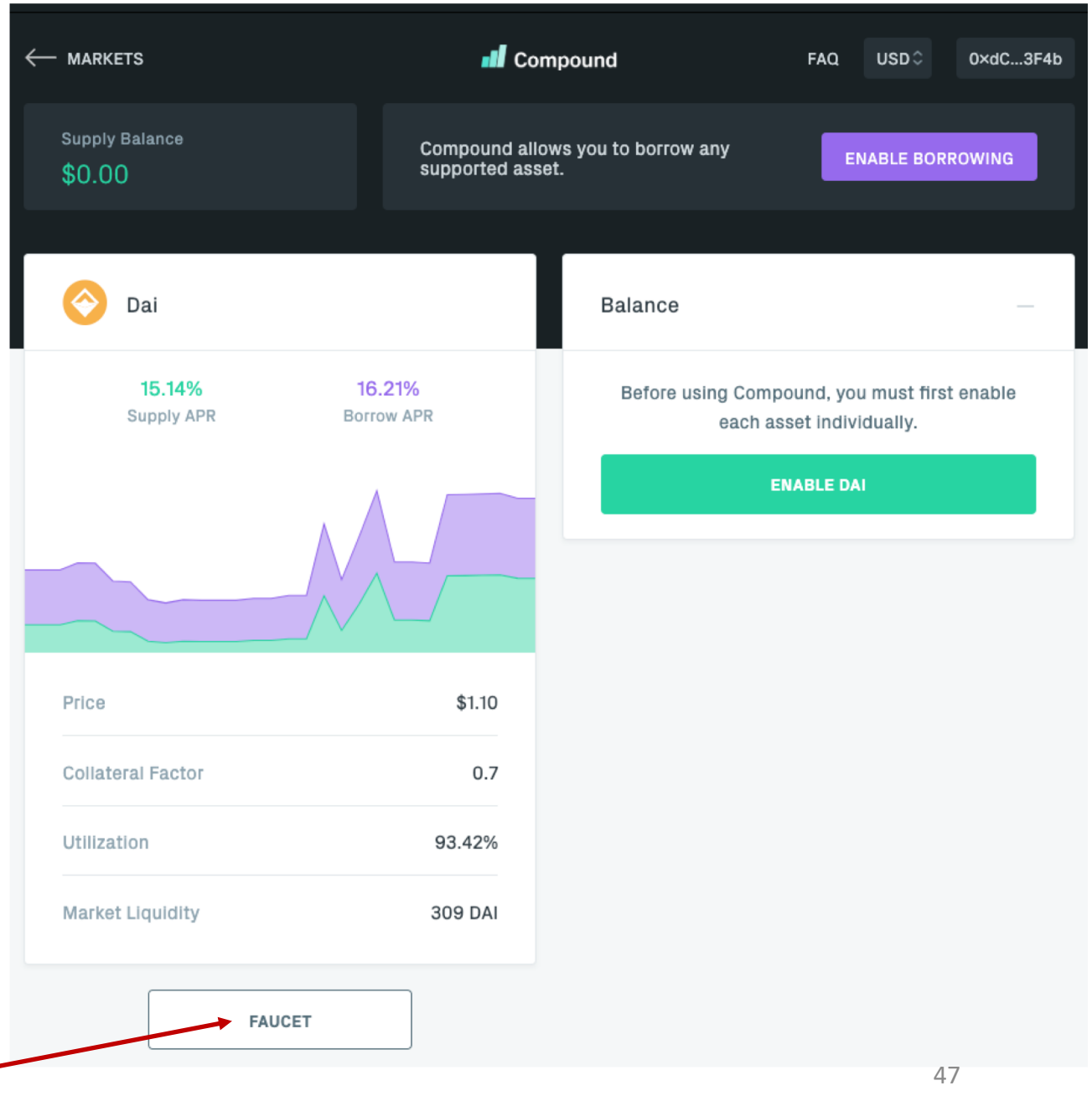
- Metamask
- Get some Ethers from faucet
  - http://rinkeby-faucet.com/
- Go to DApps
  - https://app.compound.finance/#Asset/cDAI

01. Get Ether (for gas fee)

- Get 0.001 ETH from faucet
  - http://rinkeby-faucet.com/

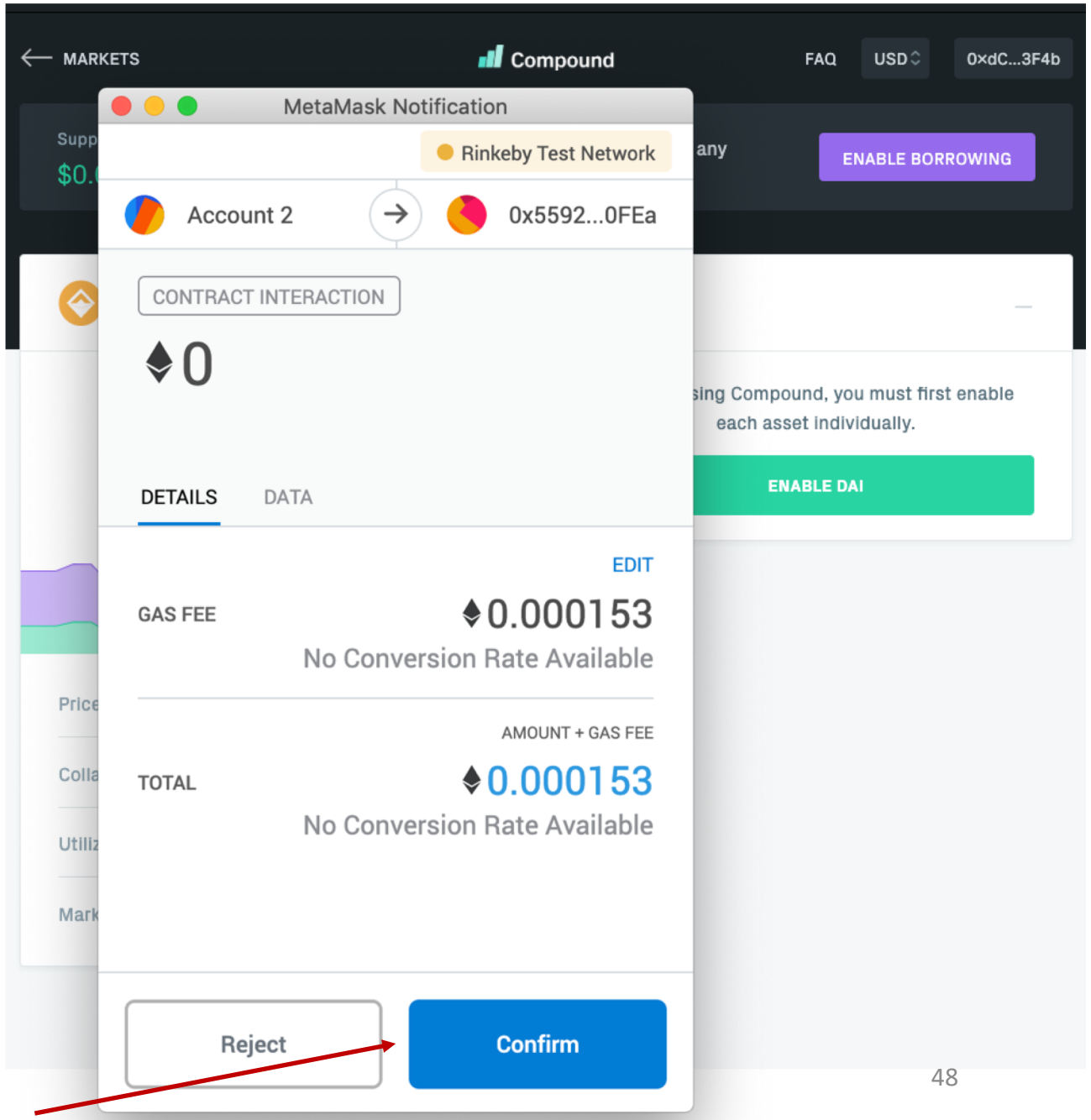
02. Get DAI (for test)

- Get test DAI
  - https://app.compound.finance/#Asset/cDAI



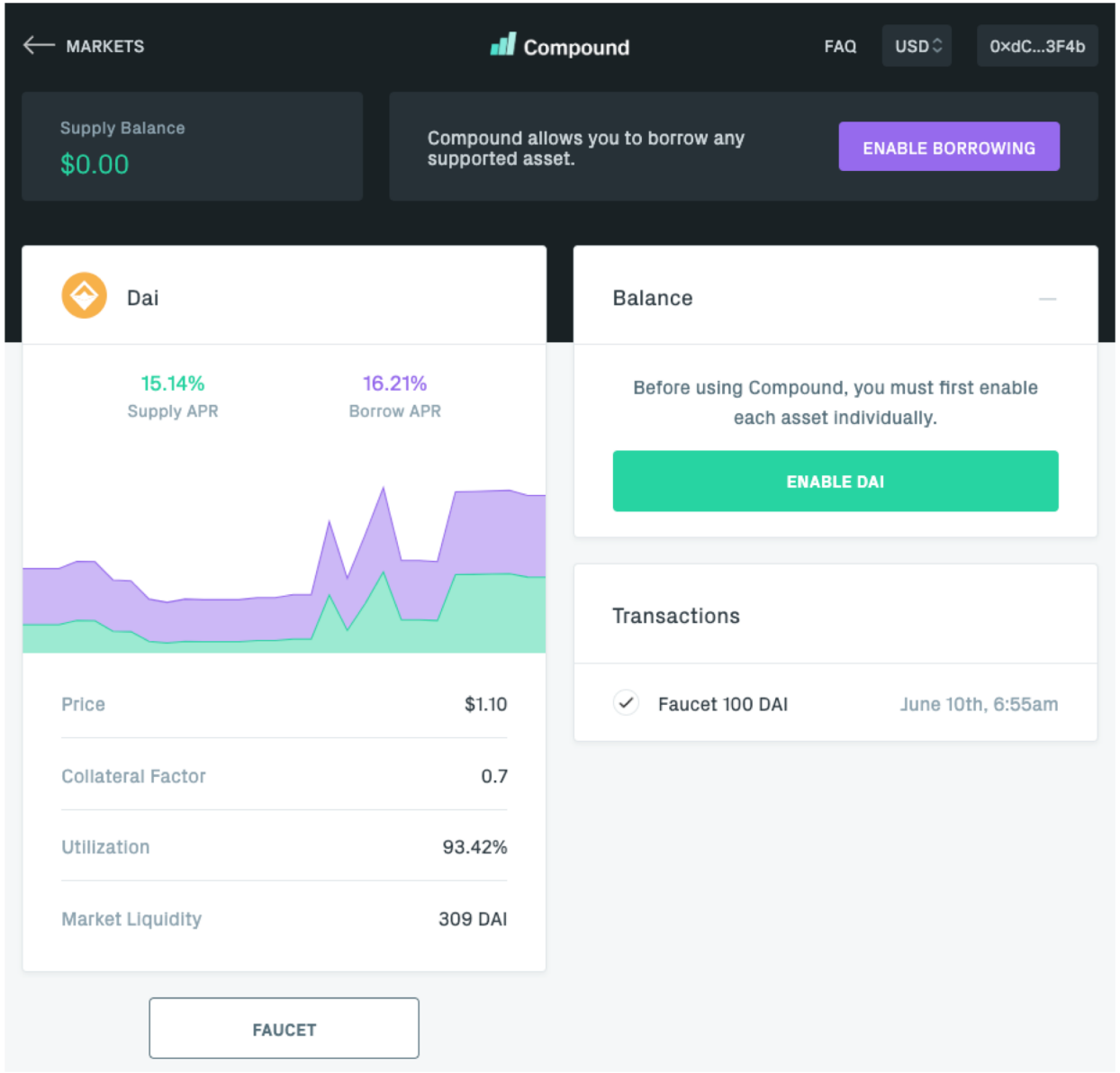
02. Get DAI (for test)

- Get test DAI
  - https://app.compound.finance/#Asset/cDAI



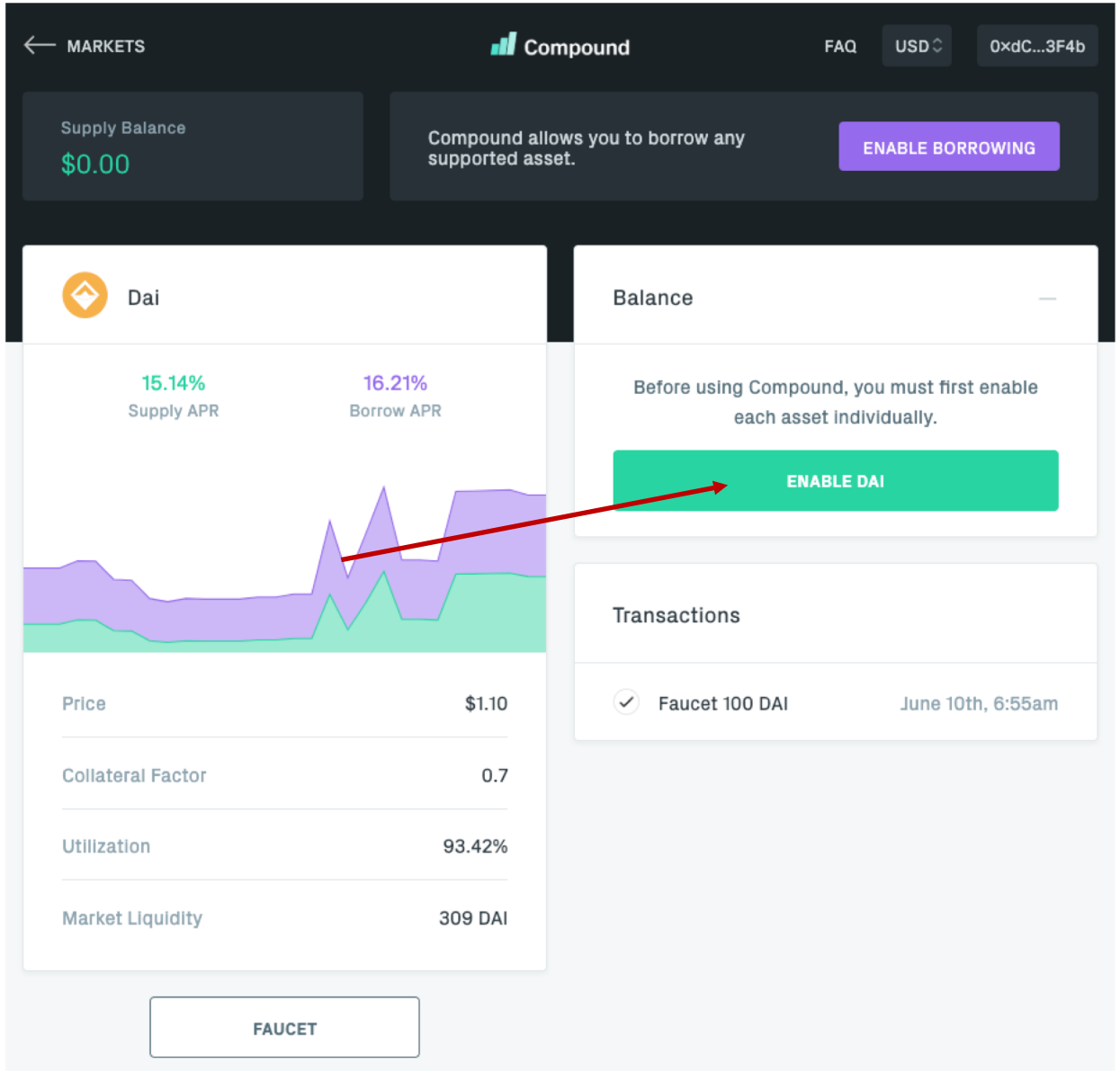
02. Get DAI (for test)

- Get test DAI
  - https://app.compound.finance/#Asset/cDAI



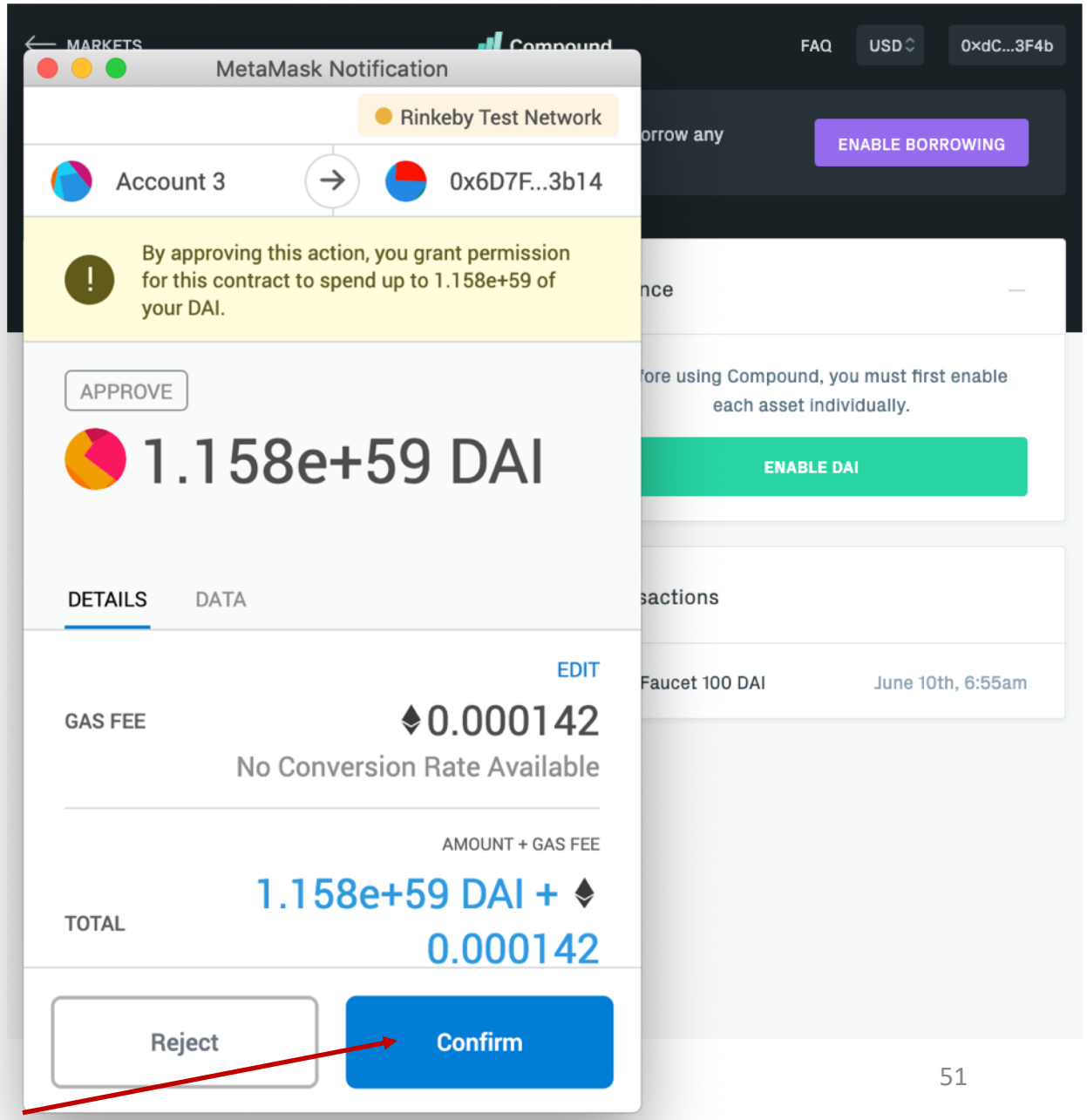
03. Enable DAI

- Approve a contract to move fund



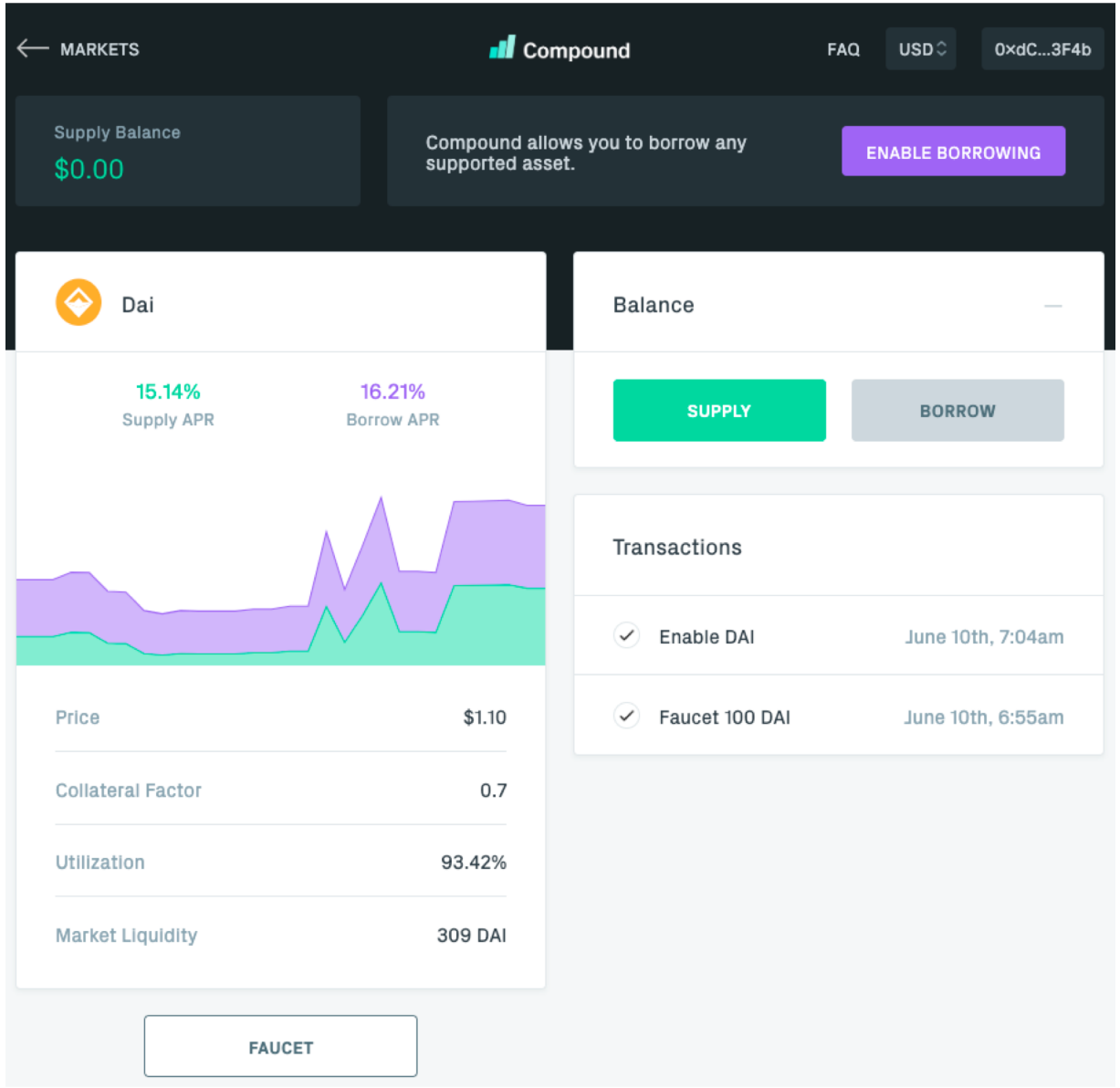
03. Enable DAI

- Approve a contract to move fund



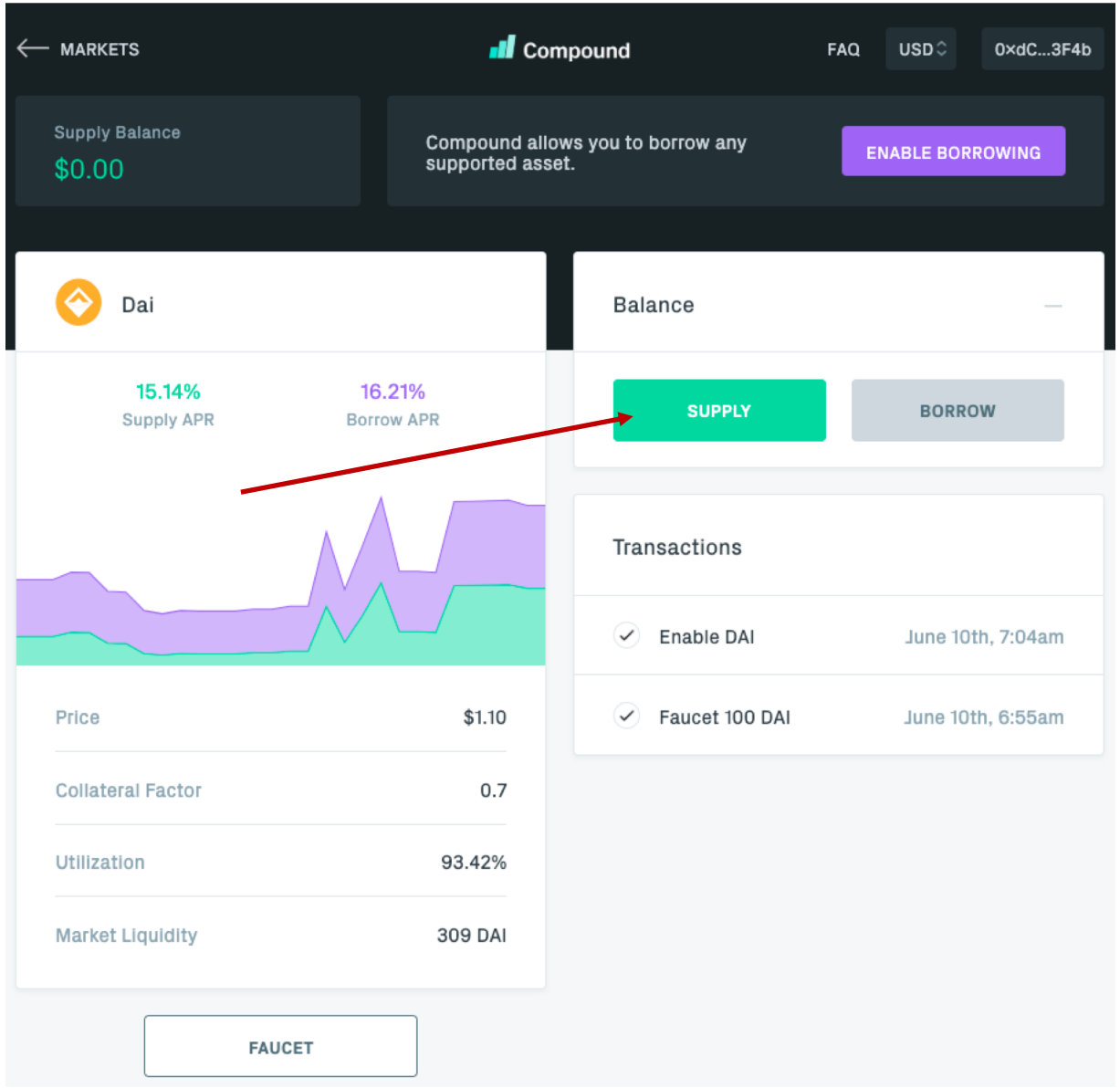
03. Enable DAI

- Approve a contract to move fund



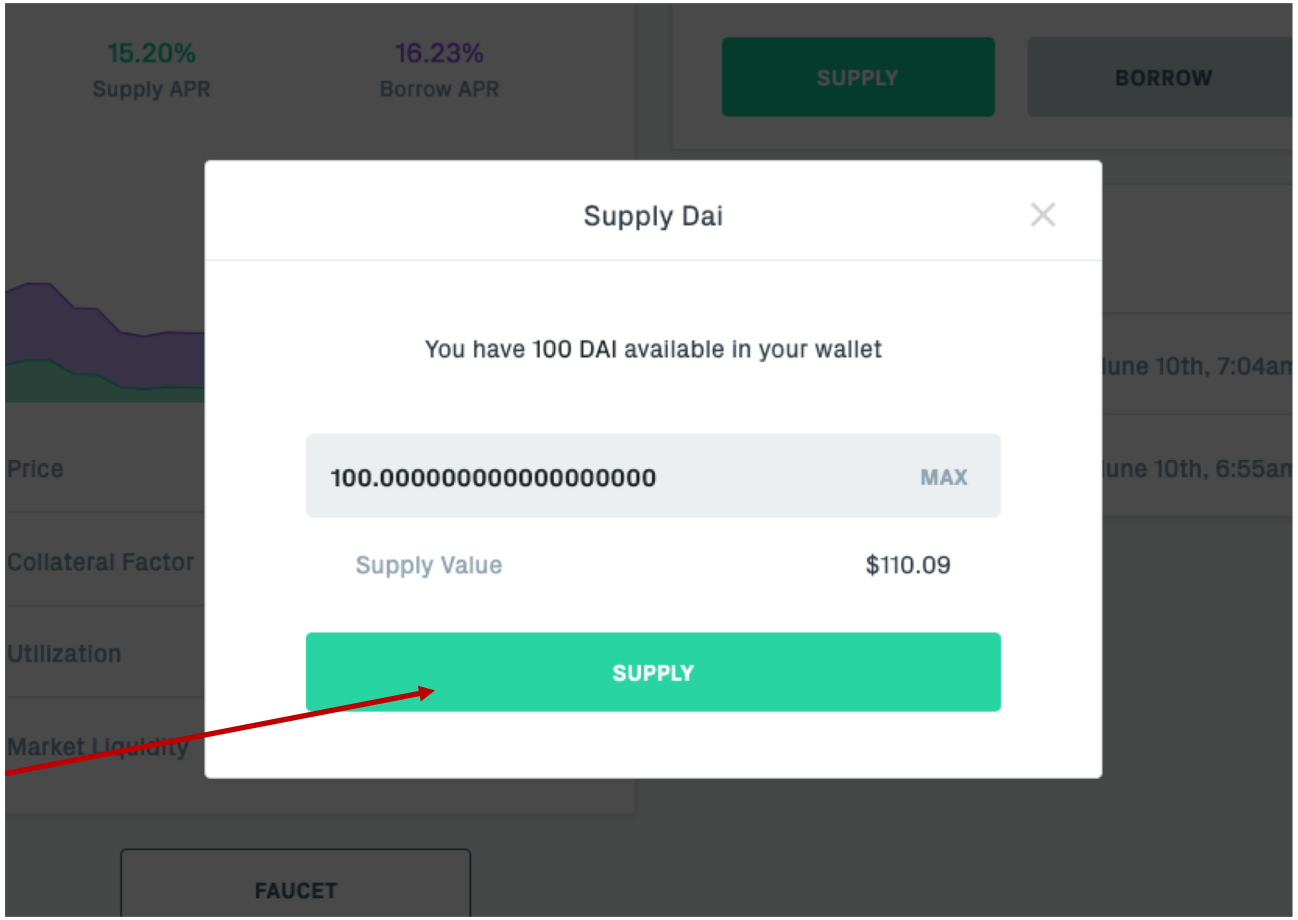
04. Supply

- Supply DAI



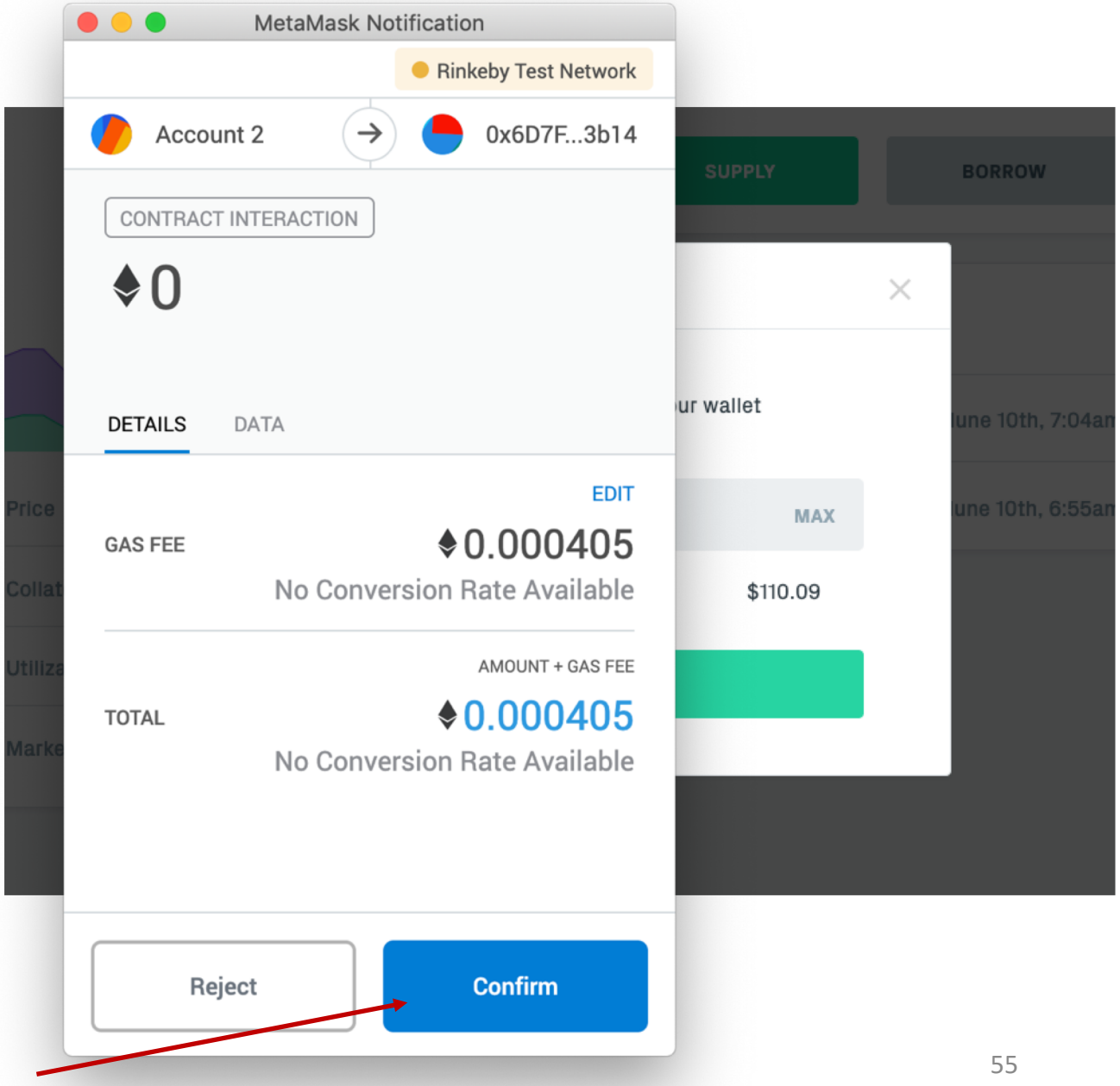
04. Supply

- Supply DAI



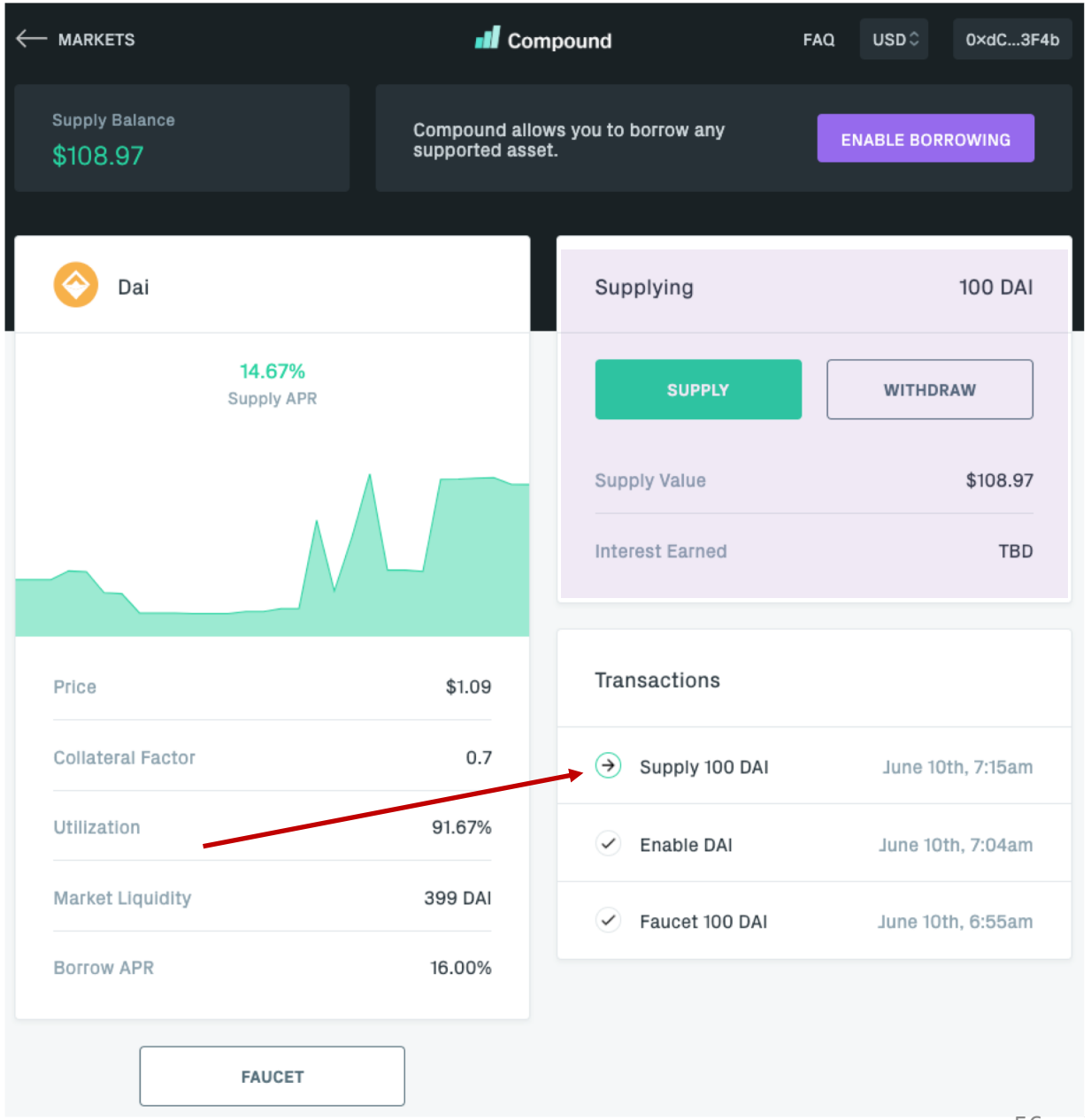
04. Supply

- Supply DAI

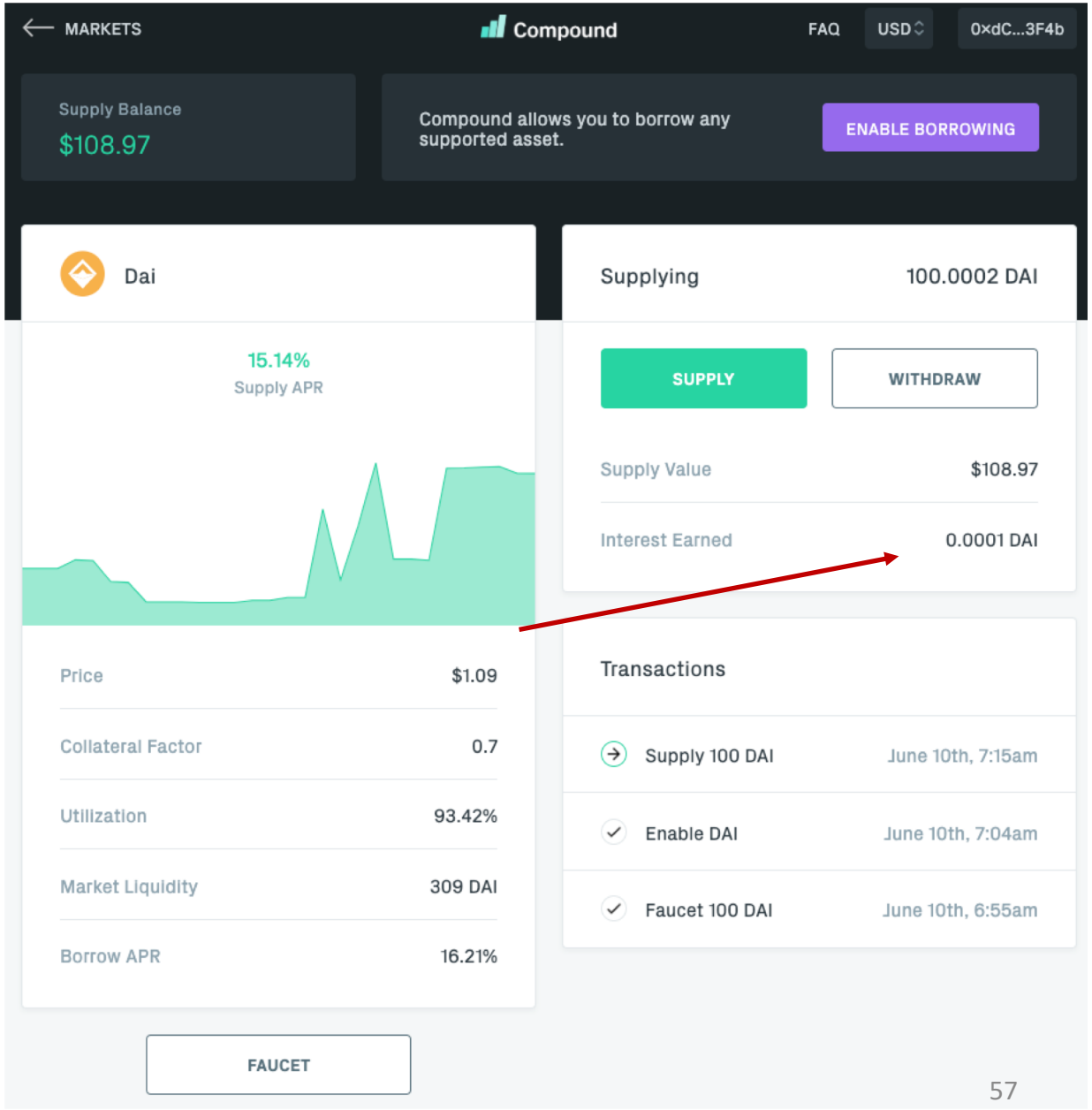


04. Supply

- Supply DAI

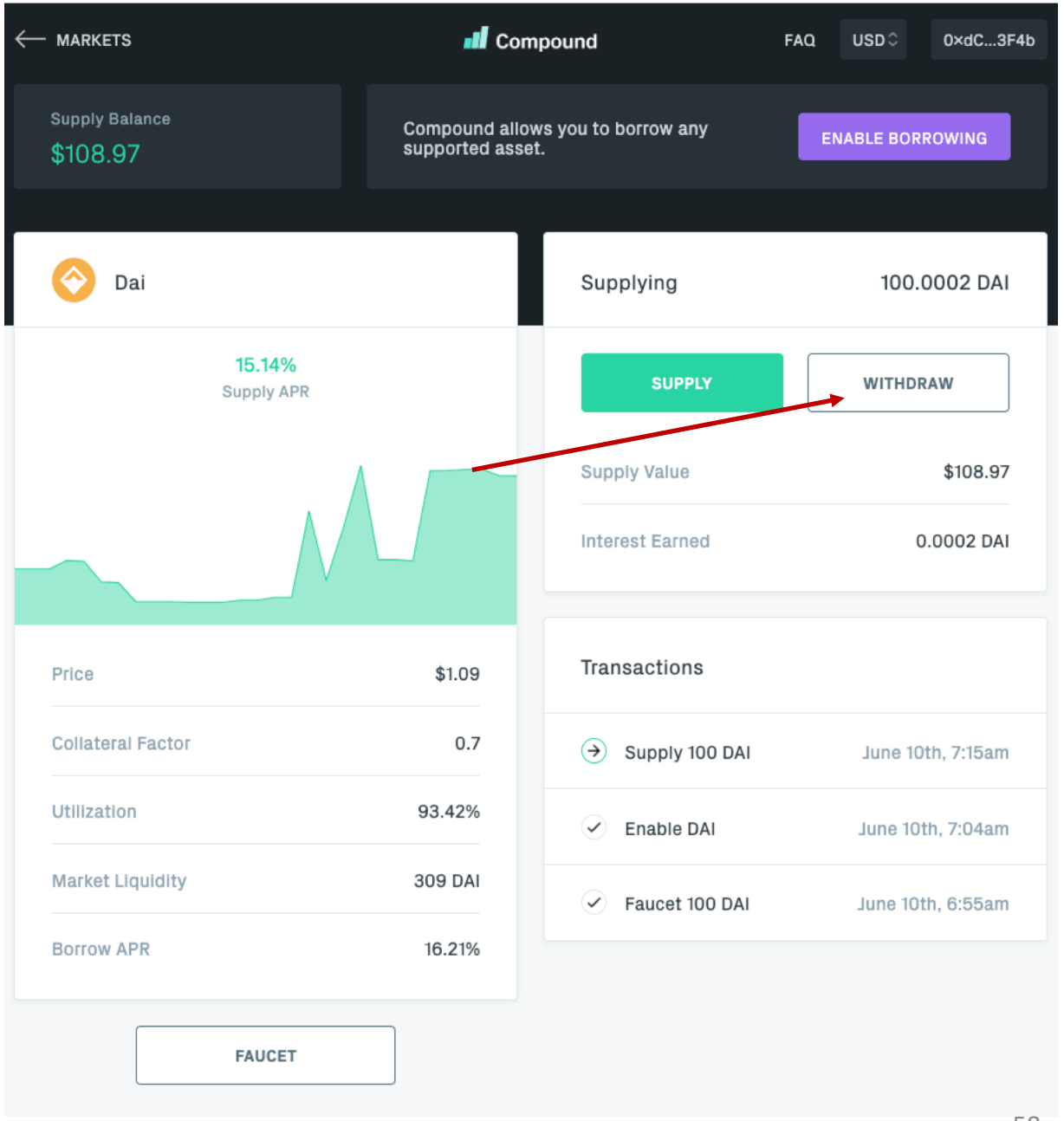


05. Interest Earned



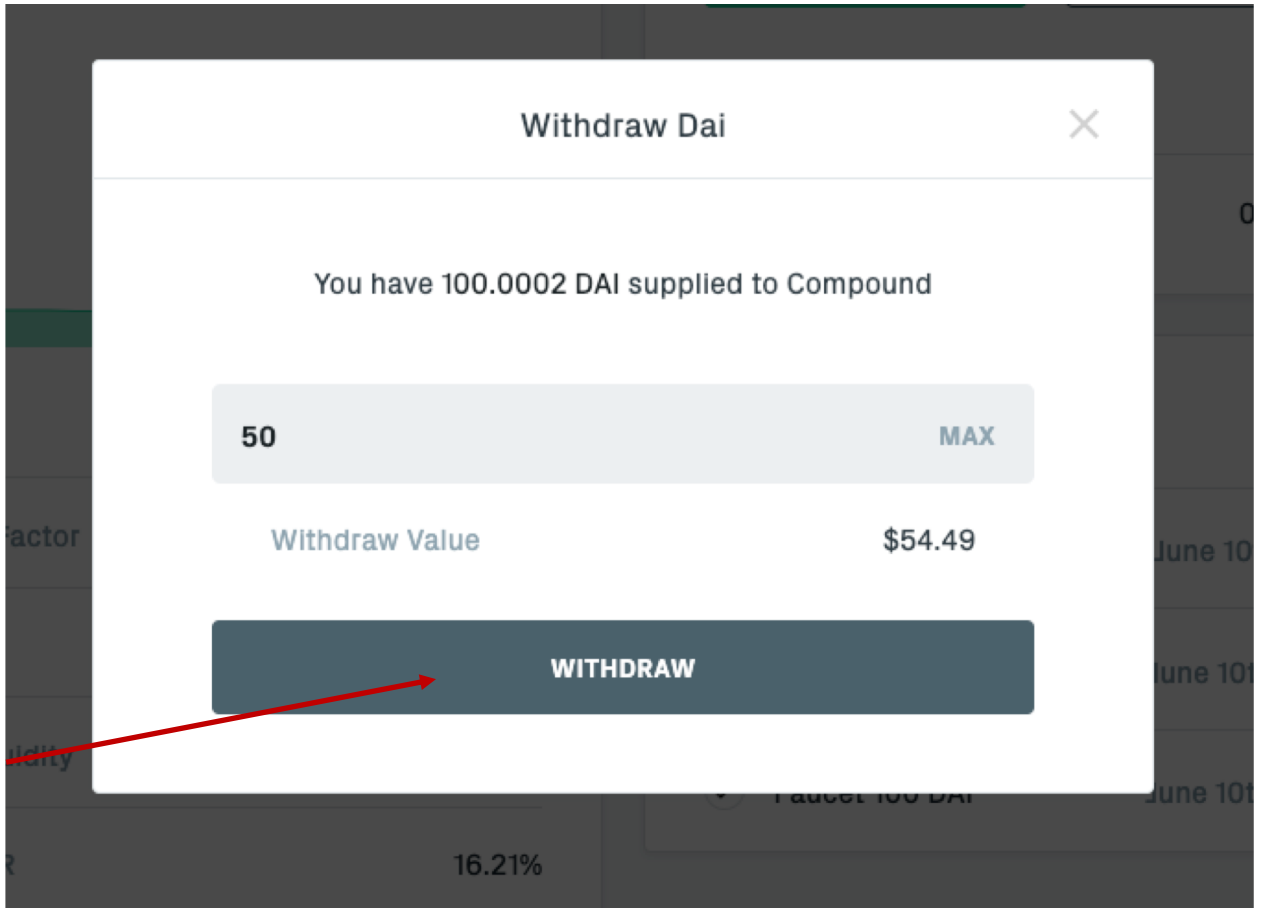
06. Withdraw

- Withdraw DAI



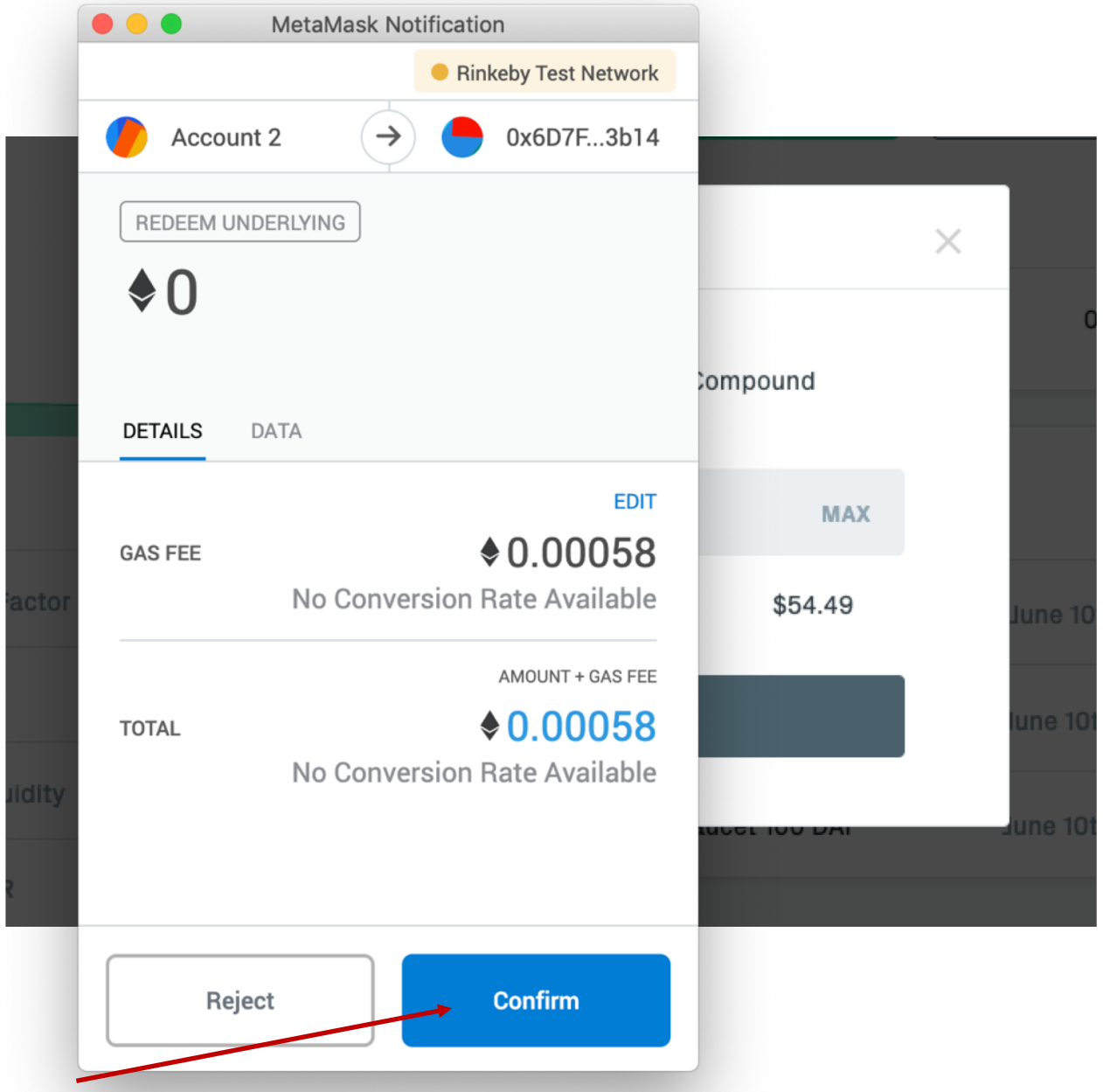
06. Withdraw

- Withdraw DAI



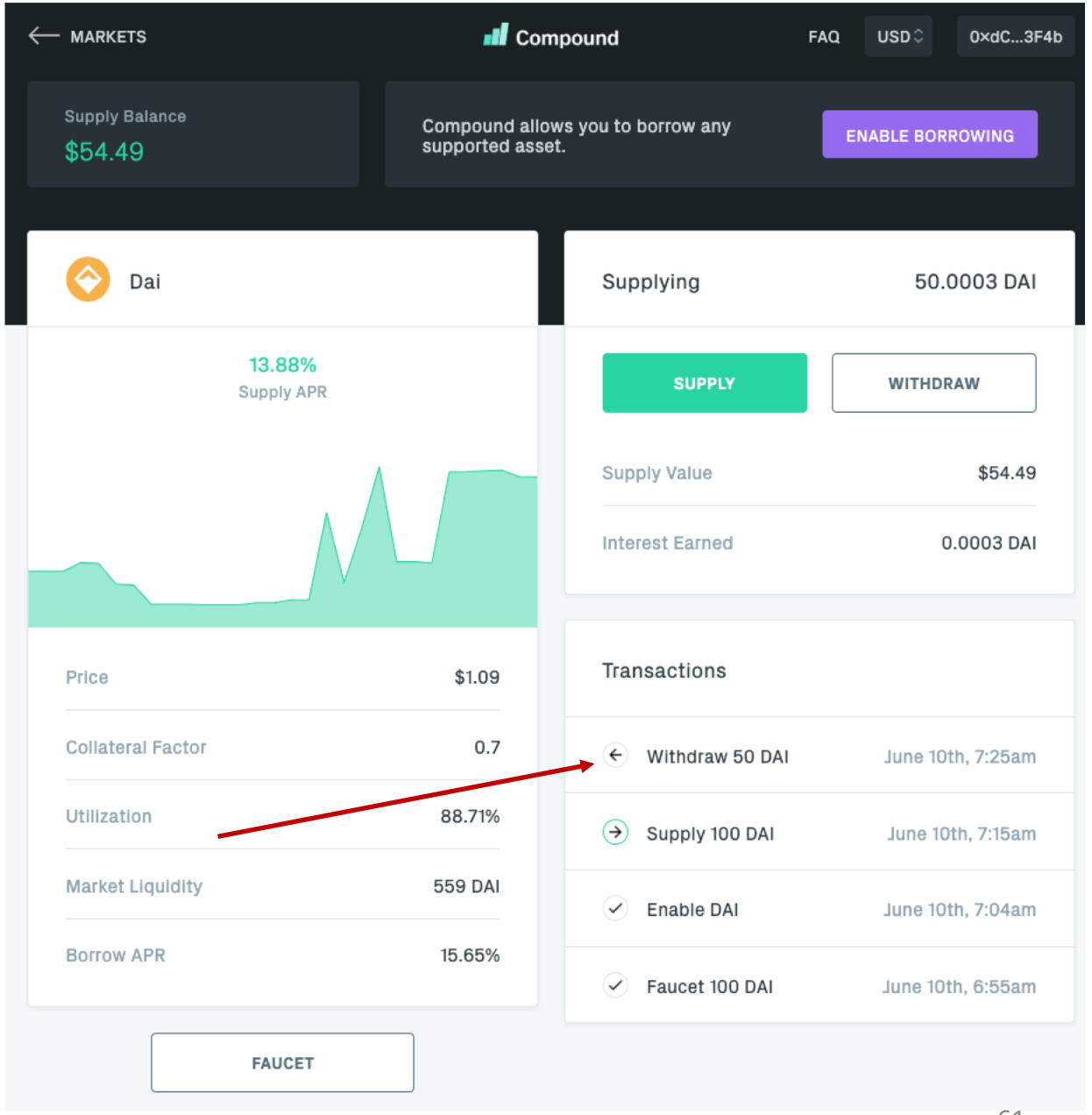
06. Withdraw

- Withdraw DAI



06. Withdraw

- Withdraw DAI



Resources

Weekly news

- Week in Ethereum News
  - http://www.weekinethereum.com/
- Seeking Yield
  - https://staked.substack.com/
- Blockchain Threat Intelligence
  - https://blockthreat.substack.com/

Podcast

- epiCenter
  - https://epicenter.tv/
- Zero Knowledge
  - https://www.zeroknowledge.fm/

Your Action

- 考慮清楚是否選修此課
- 找期末專題組員
- 加入 Slack