DeFi 與你的距離

MEV 入門指南

探索區塊鏈中的隱藏價值

Reyer Chu (瞿孝洋)

2023/8/14

deFintek

主講者　Reyer Chu 瞿孝洋

軟體 + 資安 + 金融

- 區塊鏈經歷：
  - 2017 年開始研究區塊鏈，2020 年創立 DeFi 讀書會及柢法科技，專注於投資及孵化 DeFi 及 Fintech 團隊及解決方案
  - 清大創業車庫業師
  - 英威康等公司區塊鏈顧問
  - CYBAVO 區塊鏈資安新創策略長

- 軟體及 IC 設計業經歷：
  - 物聯網 IC 設計公司總經理
  - 聯發科技軟體開發部門主管
  - 趨勢科技掃毒引擎開發軟體工程師

- 金融業經歷：
  - 金融證照：CFP 國際認證高級理財規劃顧問等 10 餘張
  - 金融交易：1996 年開始接觸程式交易

ReyerChu

柢法科技 deFintek

Telegram: t.me/reyerchu
LinkedIn: www.linkedin.com/in/reyerchu/

CYBAVO　MEDIATEK　TREND MICRO　deFintek

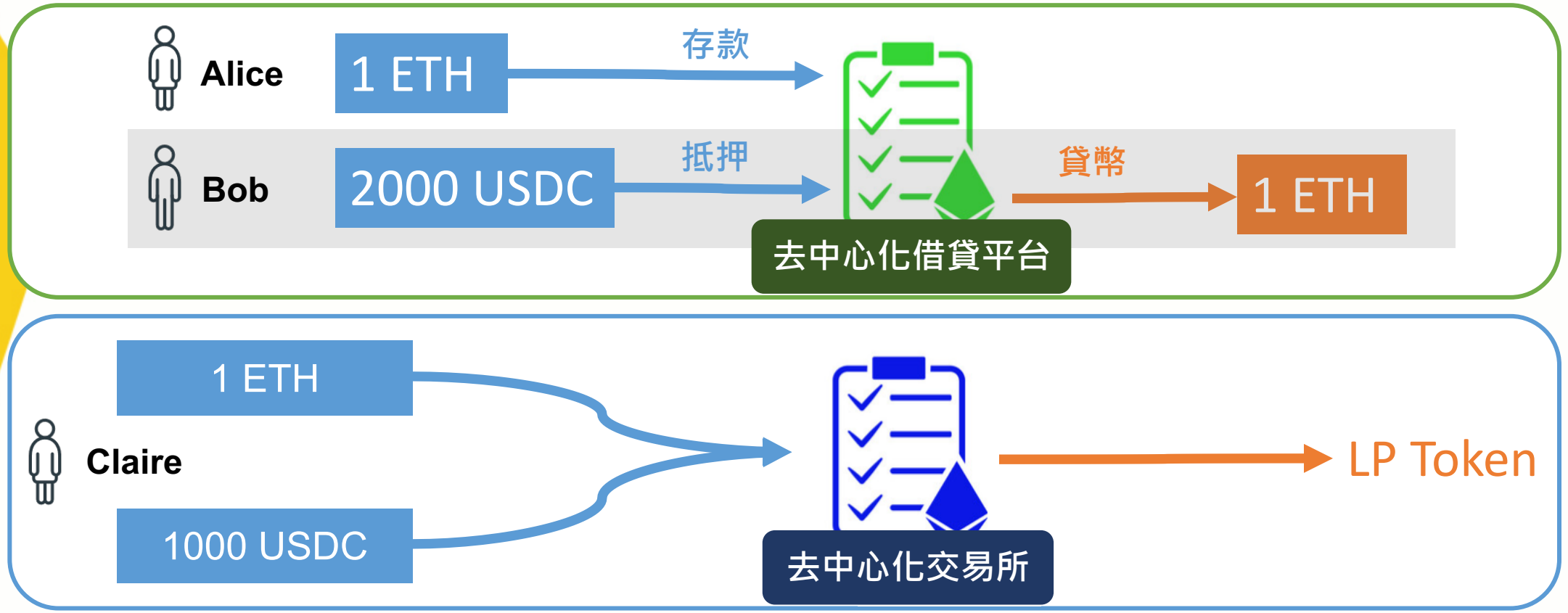
MEV 入門指南

- 背景
  - DeFi 去中心化金融平台：借貸平台、交易所
  - 搬磚套利、閃電貸、內存池（mempool）
  - 搶先交易、緊跟交易、三明治攻擊、清算

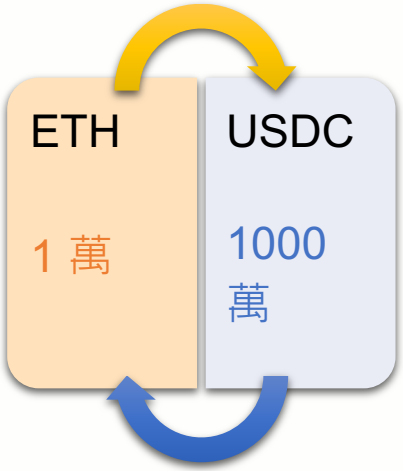
- 何謂 MEV
- MEV 影響
- MEV 解法與相關研究
  - Flashbots：Tx-based ➡ Bundle-based
  - In-protocol ePBS：Tx-based ➡ Block-based

DeFi 去中心化金融平台範例

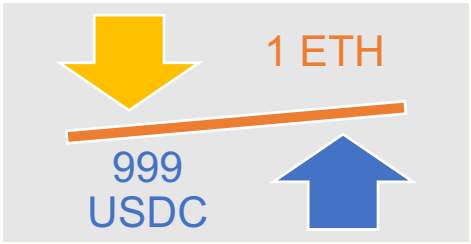
* 若 1 ETH = 1000 USDC

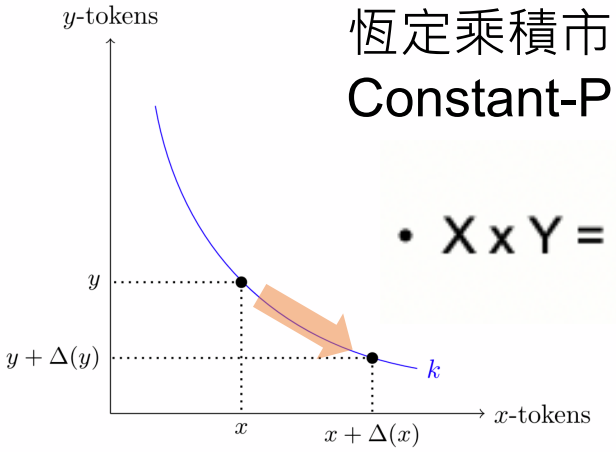


DEX 去中心化交易所



* 若初始 1 ETH = 1000 USDC





恆定乘積市場造市商模型 CPMM
Constant-Product Market-maker Model

- X x Y = Const

$$\prod_{i=0}^{n} x_i = K$$

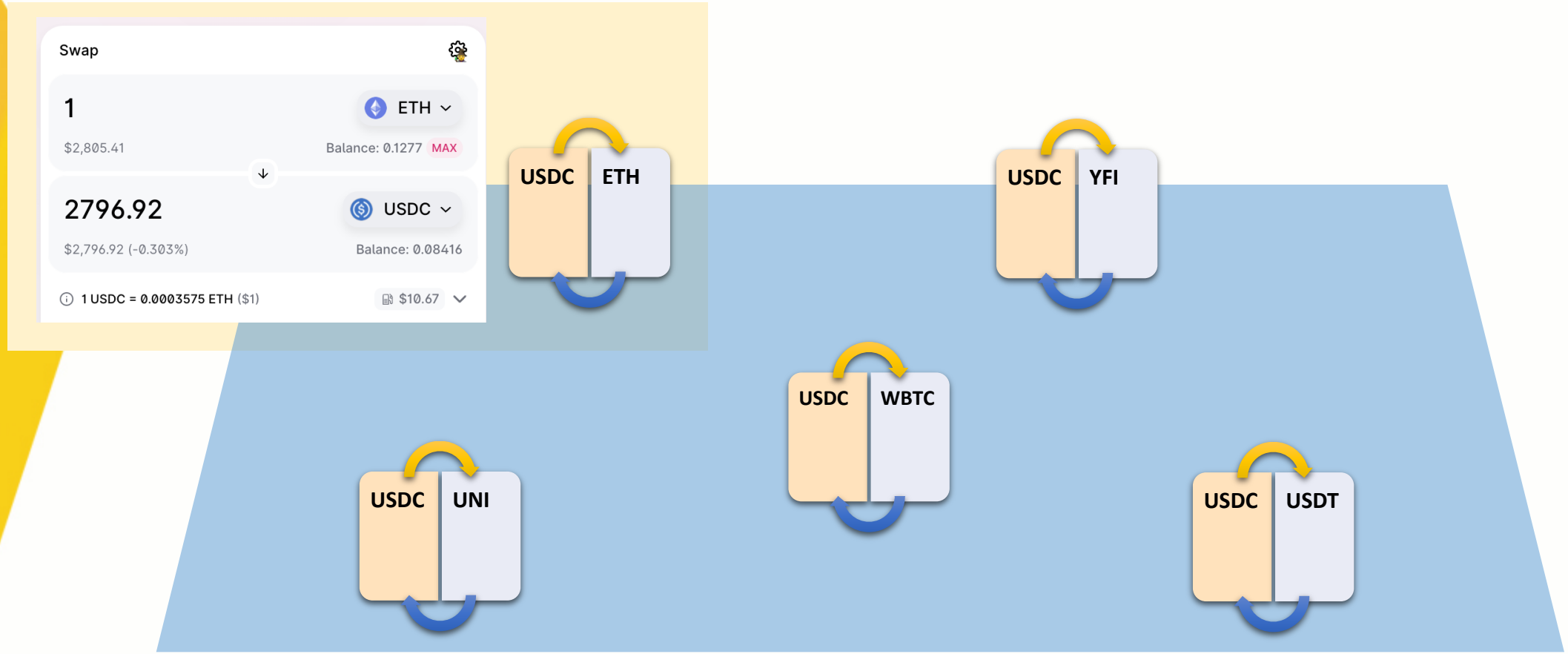
$$XY = K = (X + dX)\ (Y - dY)$$

$$dY = \frac{Y\ dX}{(X + dX)}$$

1 x 1000 = (1 + 1) (1000 - dY)
➔ dY = 500

deFintek

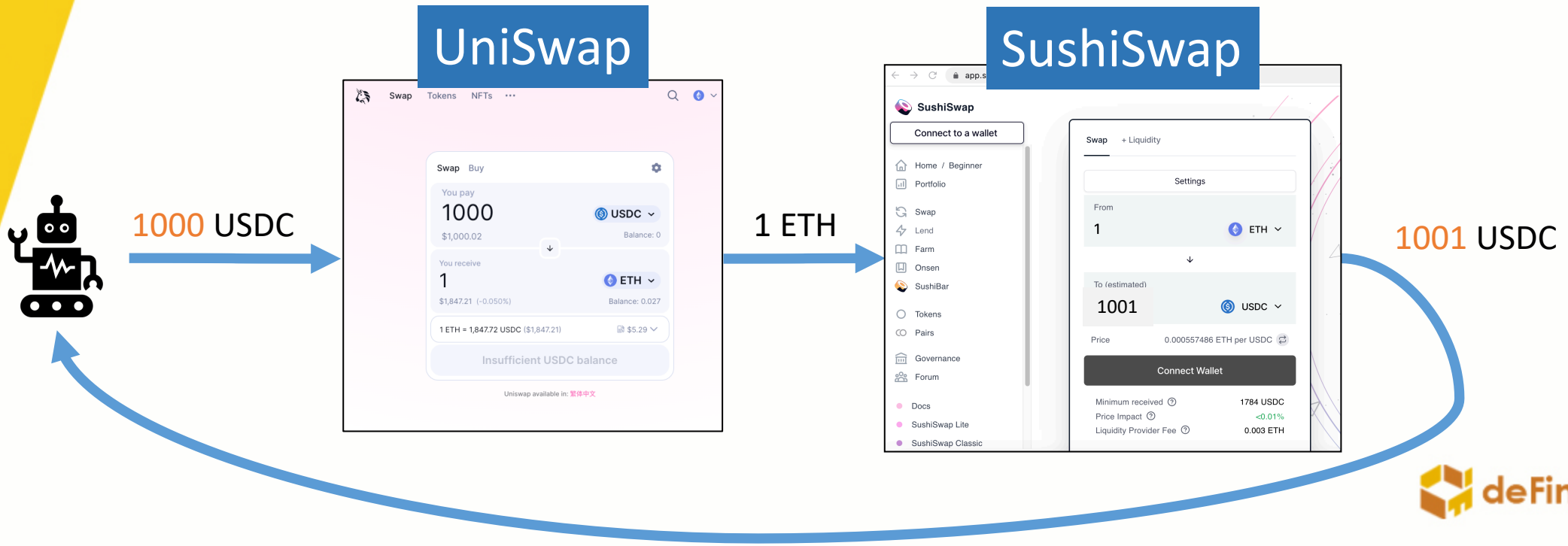
DEX 平台：Uniswap



https://app.uniswap.org

搬磚套利

- 同一種幣在不同交易所價格可能不同
- **搬磚**：低買高賣（在便宜的交易所買，在貴的交易所賣）
  - 若都在 DEX，可用 smart contract 達到所有交易結合是 atomic
  - 若其中有 CEX，要有不同套資金同時操作，避免價格跑掉或做半套
- 進階：三角套利，eg. USDC ➡ ETH ➡ LINK ➡ USDC



閃電貸 & 原子性操作

- 原子性操作（**Atomic** operation）
  - 一起完成 “一手交錢一手交貨”
    - Eg. 房屋轉貸（B 銀行清償 A 銀行貸款 → 塗銷 A 銀行抵押 → 設定抵押給 B 銀行）
  - Ethereum transaction is atomic. => All or Nothing
    - Ethereum EVM is smart-contract-state-based atomic.
- 閃電貸（Flash Loan）
  - Day-trade（日內交易）→ “Block”-trade（塊內交易）
  - “Block”-based atomic (not only transaction-based)

Borrow
從 “銀行” 借 borrowAmount ETH

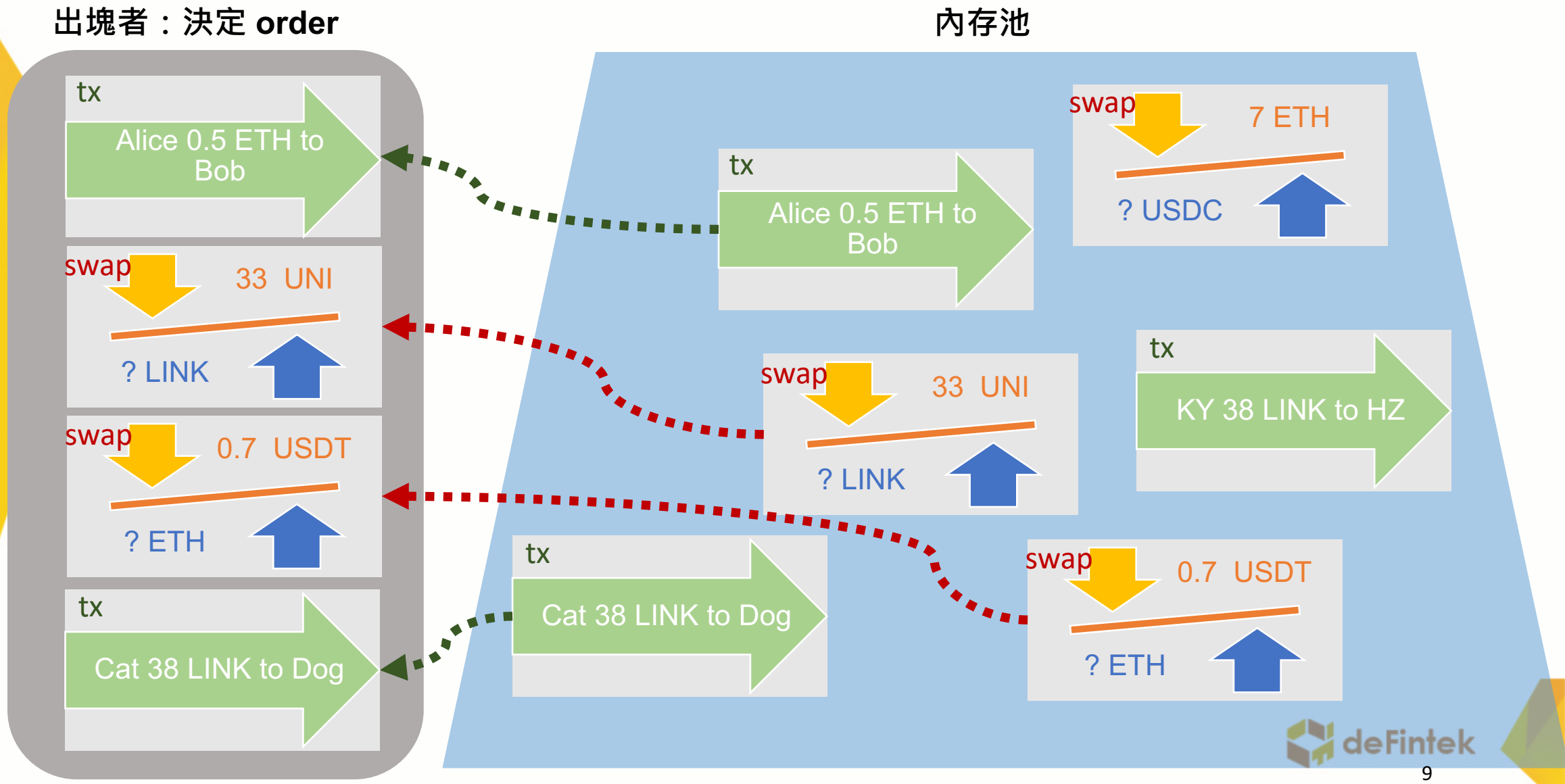
… (circuits)

Repay
還給 “銀行” borrowAmount ETH

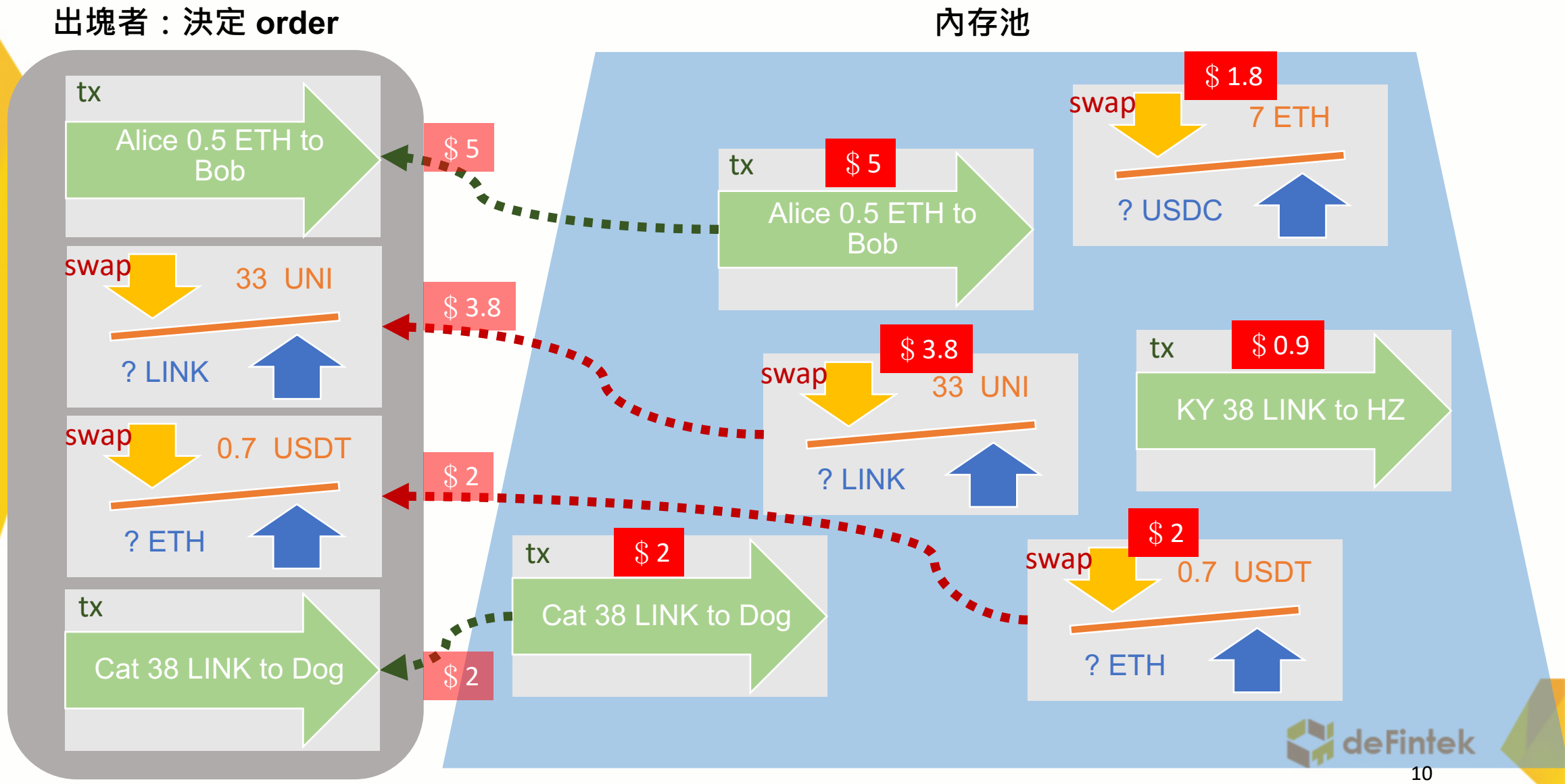
…
earnAmount = repayAmount – borrowAmount – fee
require(earnAmount > 0)

deFintek

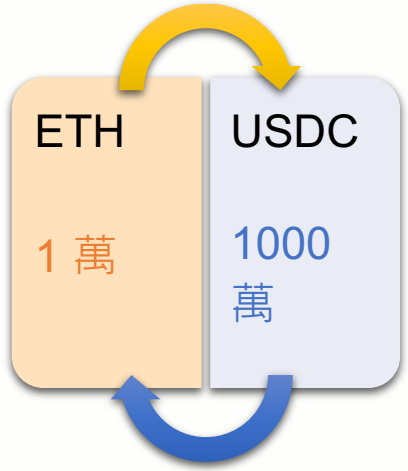
内存池：Tx-based 黑暗森林



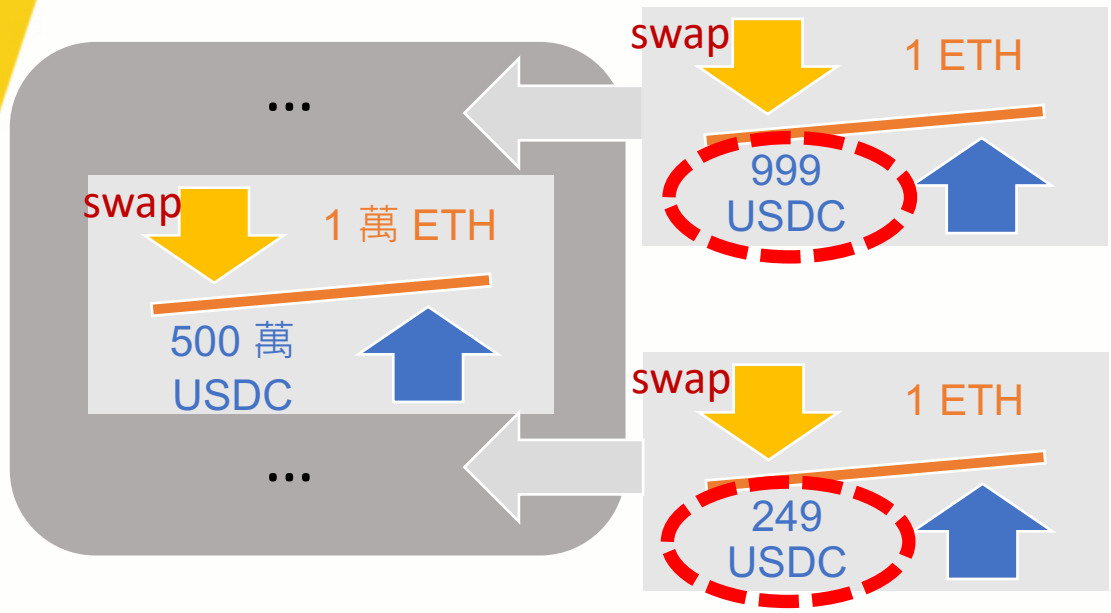
內存池：Tx-based 競標場？



Front-running 搶先交易

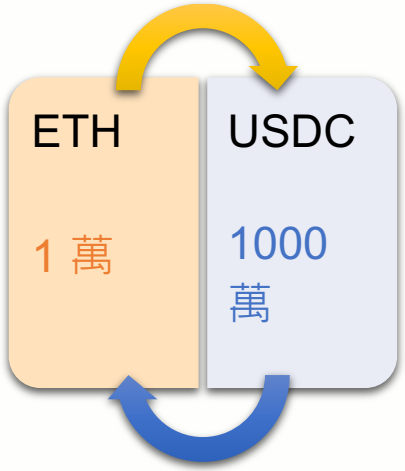


* 若初始 1 ETH = 1000 USDC

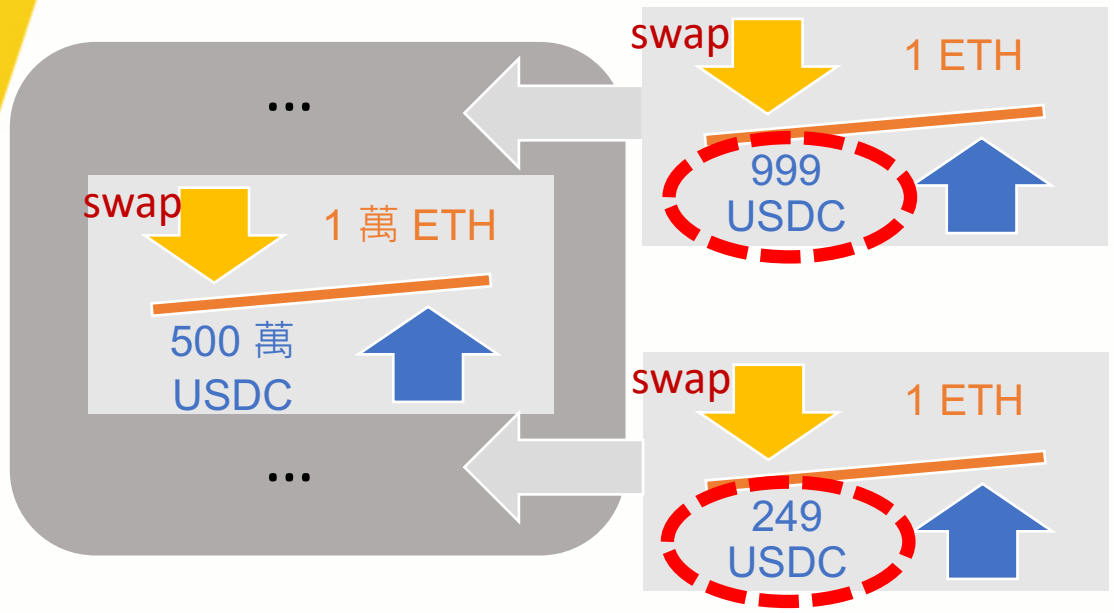


- 若要賣 ETH，可在大筆賣單（砸盤）之前搶先賣
- 礦工
  - 可決定 order
- 其他人（e.g. 套利機器人）
  - 用較高的 gas fee 吸引礦工優先選到
  - 風險：不是 atomic

Back-running 緊跟交易



* 若初始 1 ETH = 1000 USDC

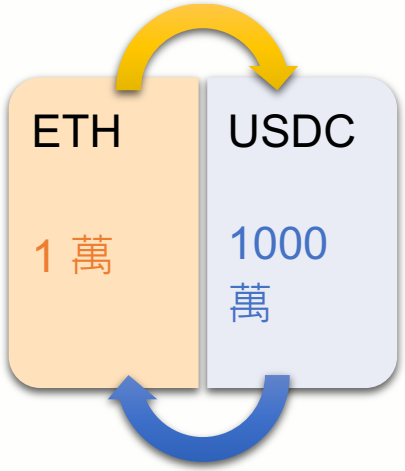


X

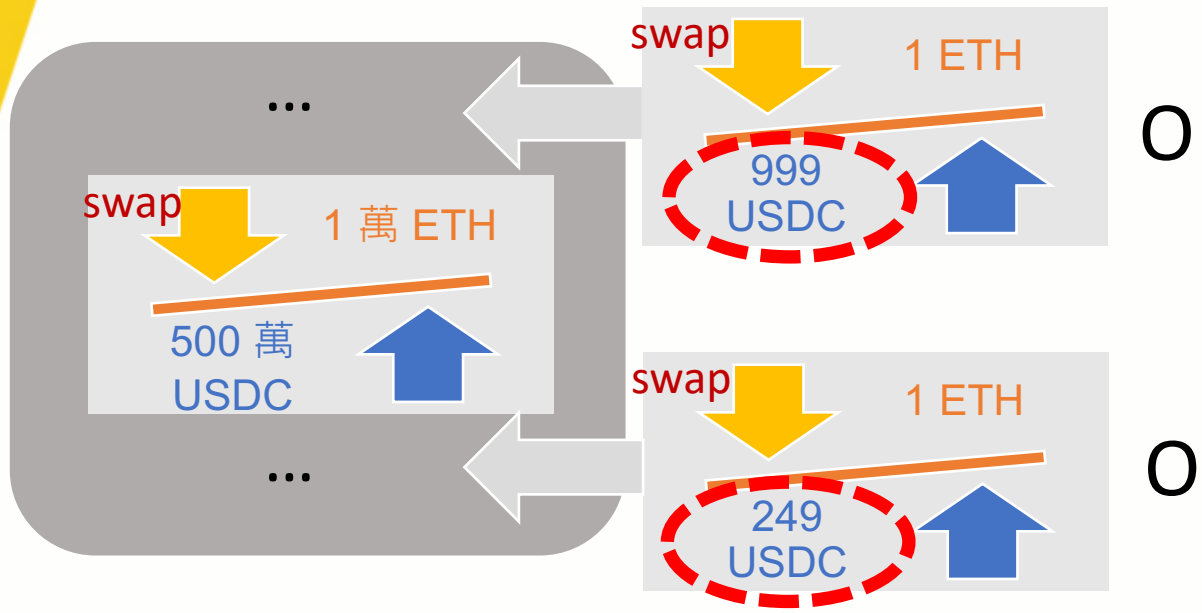
O

- 若要買 ETH，可在大筆賣單（砸盤）之後緊跟著買
- 礦工
  - 可決定 order
- 其他人（e.g. 套利機器人）
  - 用稍低的 gas fee 吸引礦工緊跟著選到
  - 風險：不是 atomic

Sandwich Attack 三明治攻擊



* 若初始 1 ETH = 1000 USDC



O

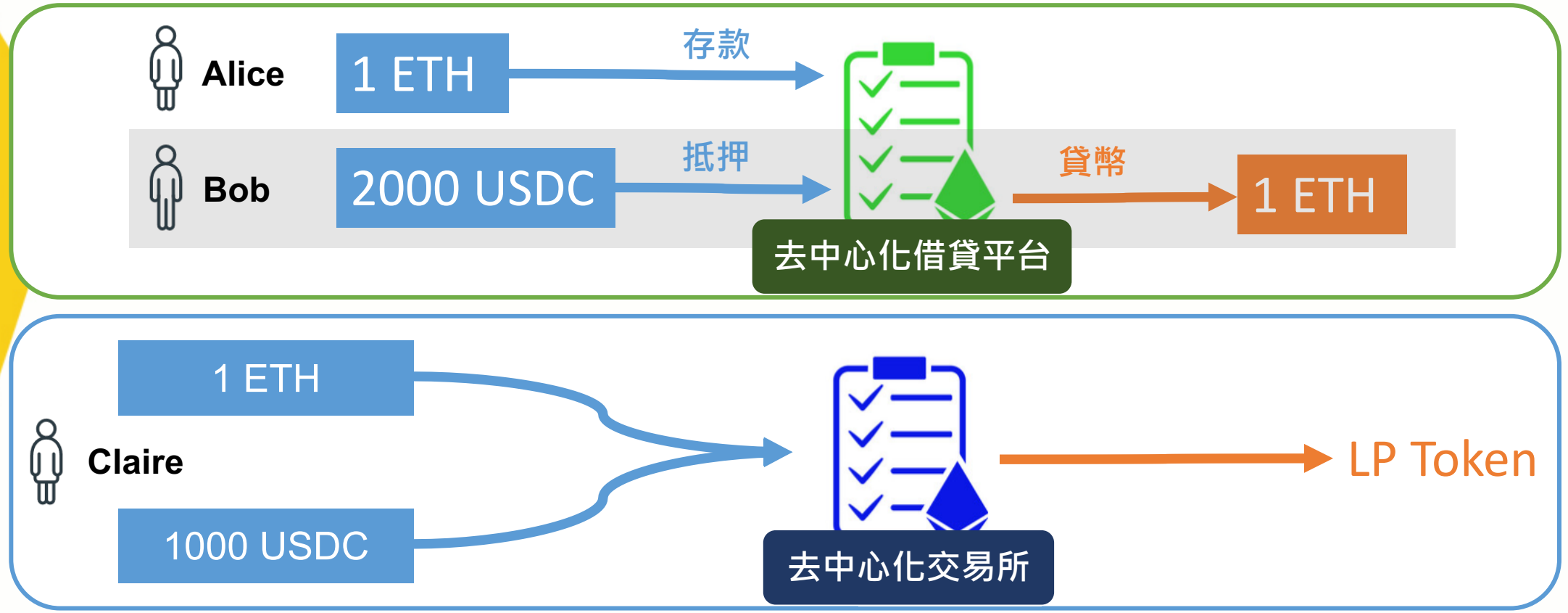
O

- 搶先 + 緊跟交易
  - 在大筆賣單（砸盤）之前搶先賣
  - 在大筆賣單（砸盤）之後緊跟著買回
  - 吃大筆賣單交易者的豆腐

- 礦工
  - 可決定 order
- 其他人（e.g. 套利機器人）
  - 風險：不是 atomic
    - 價格可能跑掉
    - 可能做半套（風險大）

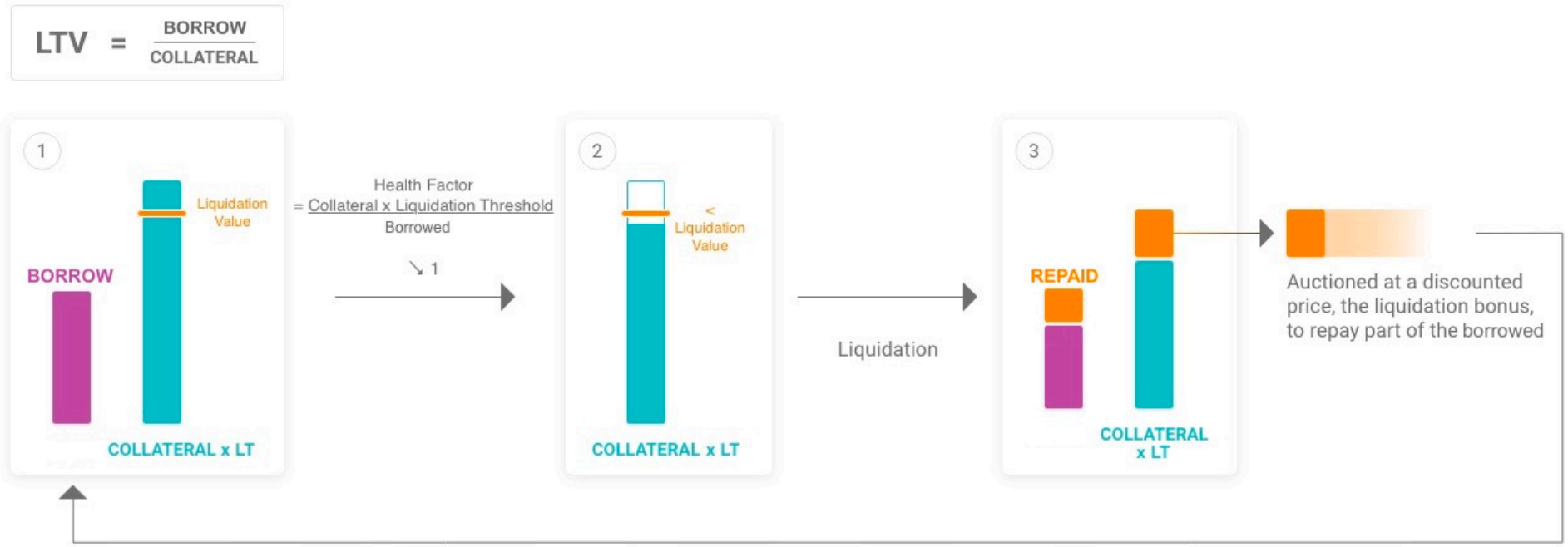
DeFi 去中心化金融平台範例

* 若 1 ETH = 1000 USDC



清算

- 超額抵押 -> 若資債比（LTV：Loan-to-Value）低於清算點（e.g. 120%）將進行清算，以避免 "資不抵債"
- 去中心化借貸平台
  - 一般由任意第三方的清算機器人進行清算
  - 清算人可得到清算獎勵



https://docs.aave.com/risk/asset-risk/risk-parameters

其他範例

- 搬磚
  - 在特地交易所有大筆交易發生時，立刻進場搬磚
- 緊跟交易
  - IDO 在 add liquidity 的時候，馬上進去買
  - NFT 在一開始發行時，馬上進去買
- 清算/緊跟交易
  - AMM 或 oracle 更新價格之後，清算機器人馬上進行清算
- 清算
  - （用閃點貸借幣）砸盤讓 oracle 價格達到清算點，再用清算機器人清算後（再還幣）
- 三明治攻擊
  - 在 DEX 急著交易時會設高 slippage（滑價）tolerance，攻擊者利用 slippage 的極值坑交易者

MEV 入門指南

- 背景
  - DeFi 去中心化金融平台：借貸平台、交易所
  - 搬磚套利、閃電貸、內存池（mempool）
  - 搶先交易、緊跟交易、三明治攻擊、清算

- 何謂 MEV
- MEV 影響
- MEV 解法與相關研究
  - Flashbots：Tx-based ➡ Bundle-based
  - In-protocol ePBS：Tx-based ➡ Block-based

何謂 MEV？

- ~~Miner~~ Maximal Extractable Value
  - 在生成 block 時，對交易（tx：transaction）進行
    - 安插（insertion）
    - 排除（censorship）
    - 改變順序（reordering）

    所能得到的 “非常規 block reward 和 gas fee” 的最大價值
  - 常規：內存池中 gas fee 高的 tx 優先處理
    - PGA：Priority Gas Auction
- 最早由 Flash Boys 2.0 中提出，在 Flashbots
  - Miner → Searcher/Miner
- The Merge 之後
  - Miner → Validator

BEV：Blockchain Extractable Value

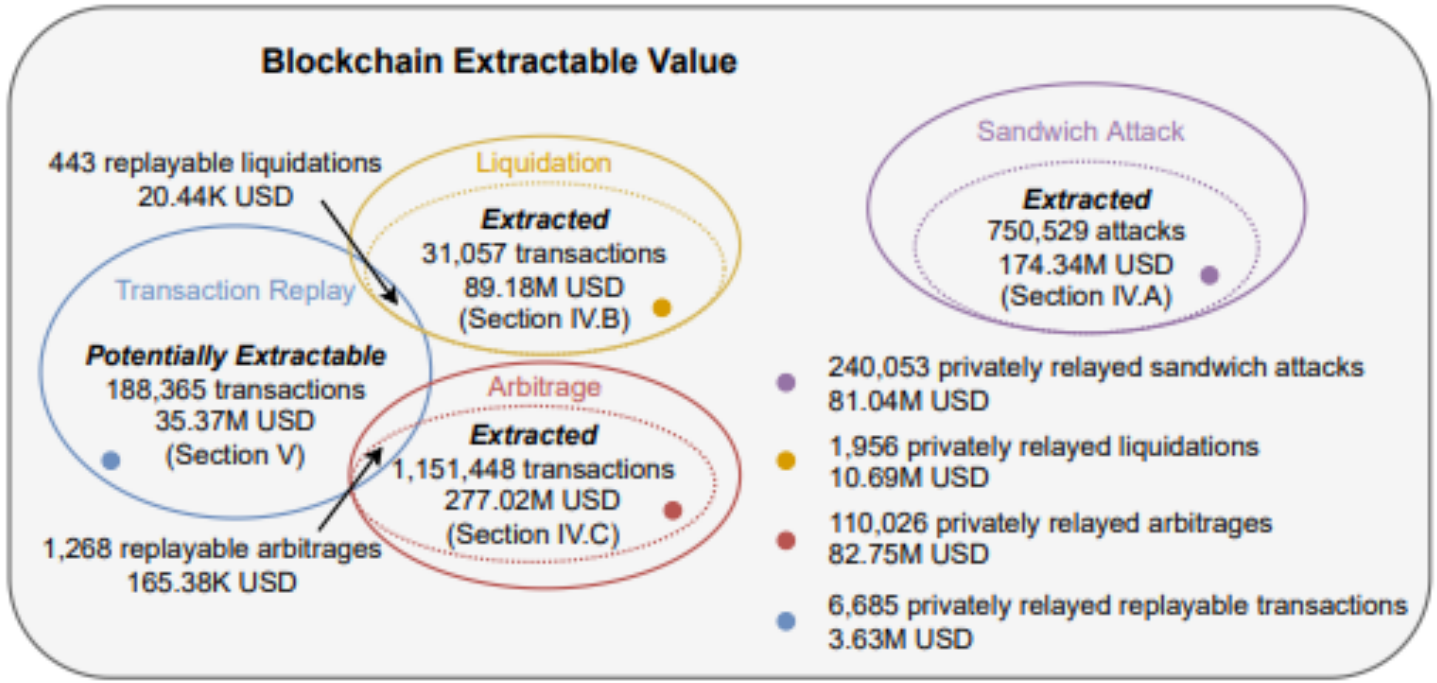


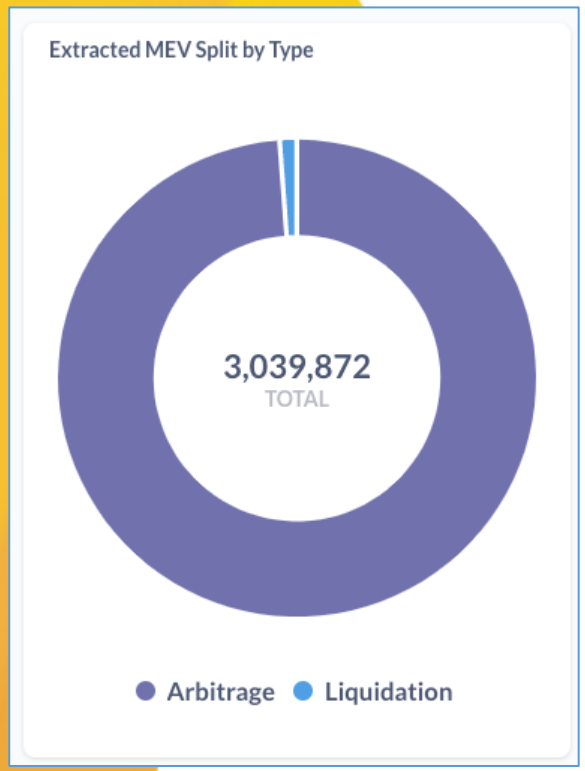
Fig. 1: Overview of various sources of blockchain extractable value. We find that sandwich attacks, liquidations and arbitrage yield 540.54M USD of BEV over 32 months. We further evaluate a novel application-agnostic transaction replay algorithm, which could have extended BEV by 35.18M USD.

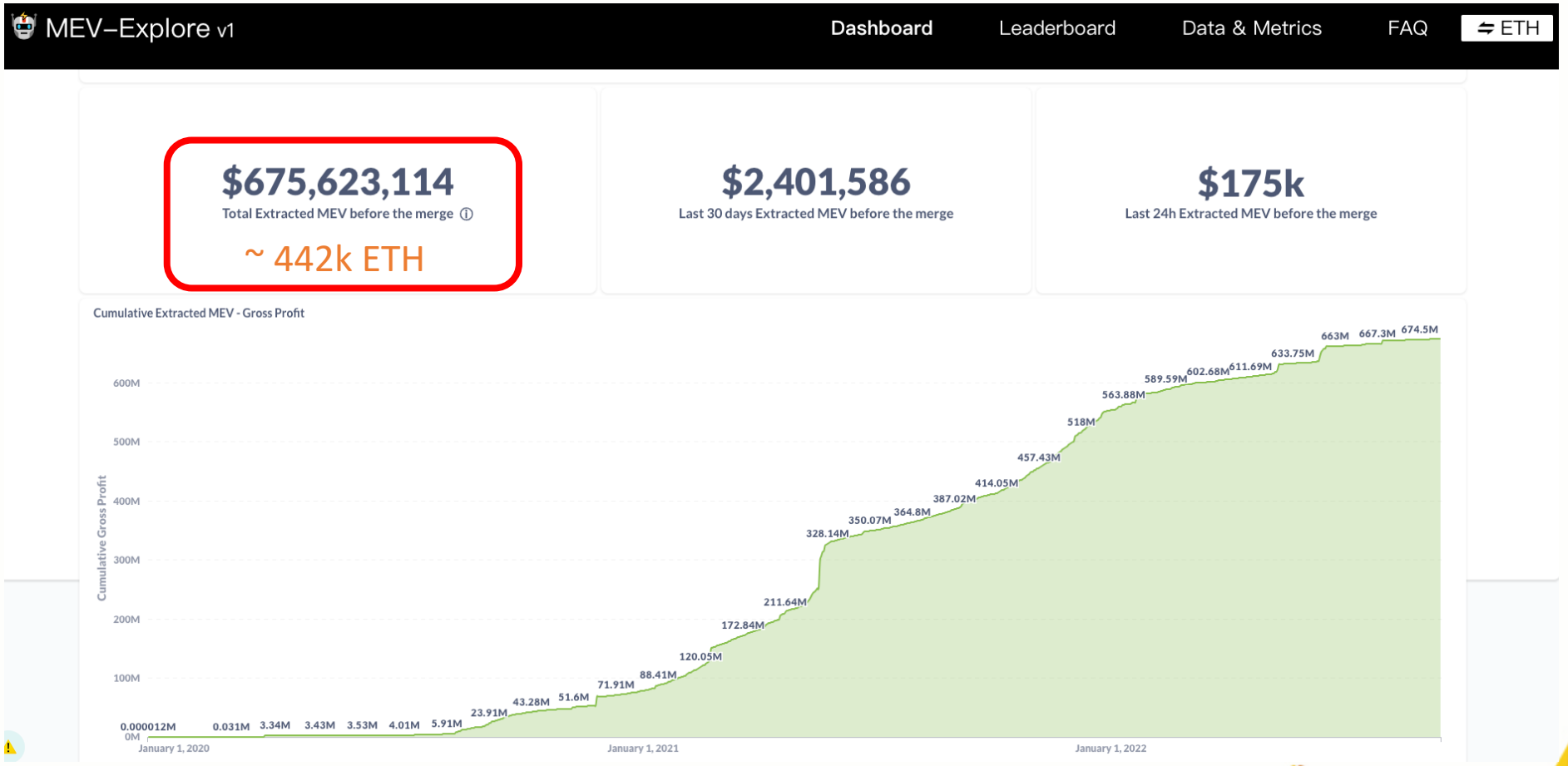
https://arxiv.org/pdf/2101.05511.pdf

deFintek

MEV 統計：Pre-Merge

- 2019/12/14 ~ 2022/9/15



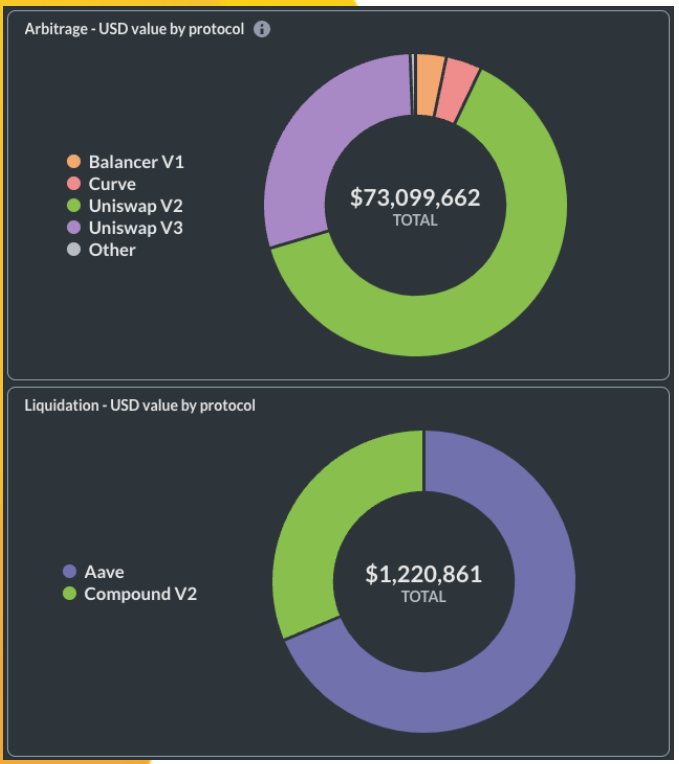


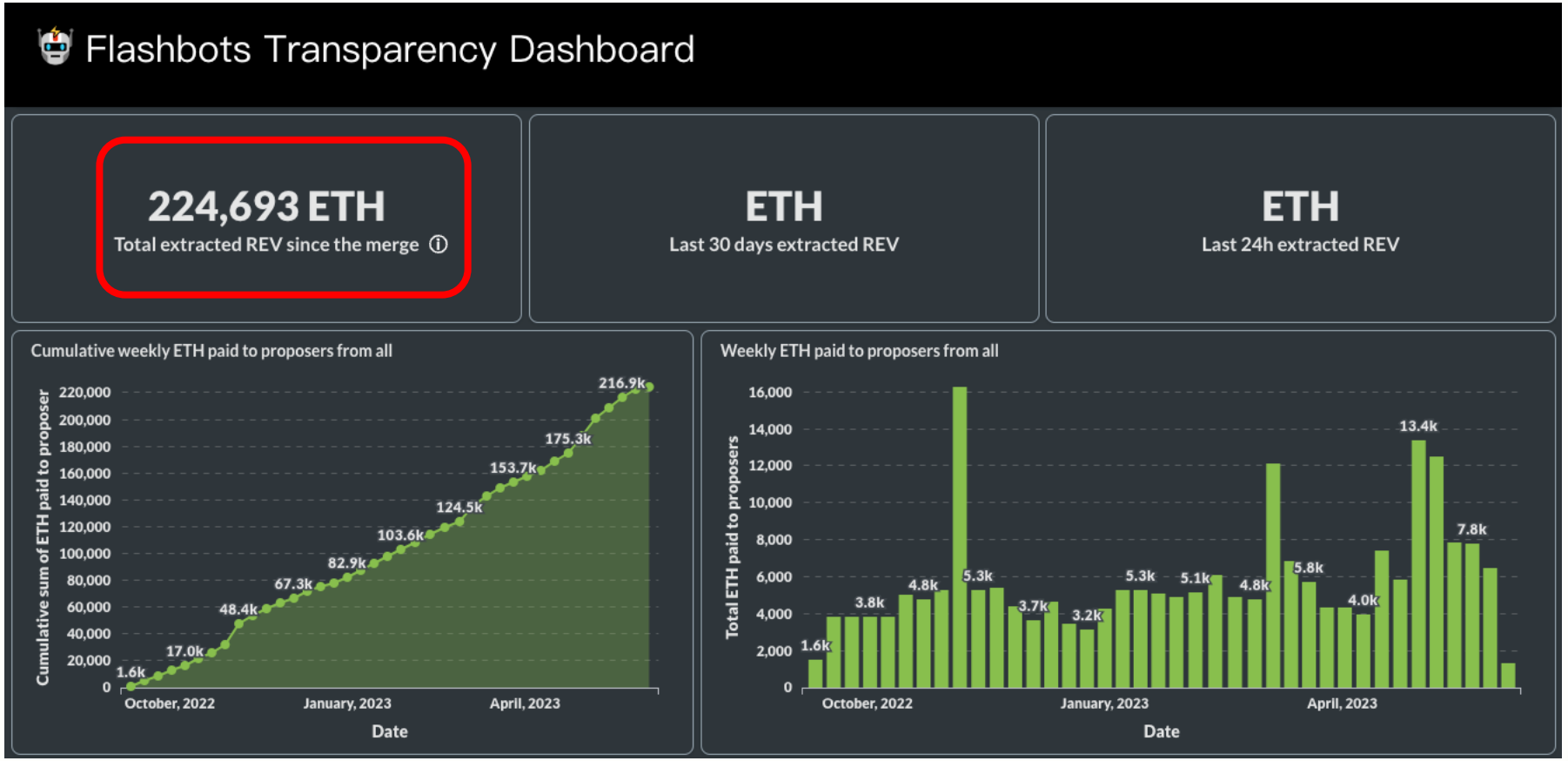
https://explore.flashbots.net/

deFintek

MEV 統計：Post-Merge

- 2022/9/15 ~ 2023/8/14 REV（Realised EV）





https://transparency.flashbots.net/

deFintek

MEV 影響

- 好
  - 同一種幣在各交易所的價格更趨於一致
  - 借貸清算更有效率，減少 "資不抵債" 發生機率
  - 創造出更多角色參與生態（e.g. searcher）

- 壞：負外部性（negative externalities）
  - 用戶體驗變差
  - 太多 MEV 競爭者 ➡ 網路壅塞
  - 提高 gas fee 來爭取 MEV ➡ gas fee 升高
  - 鼓勵 validator 重組 block 來得到 MEV ➡ 出塊不穩定
    - 當 block reward 小於 MEV 時
  - 影響去中心化程度
    - 鼓勵 validator 更中心化：經濟規模使得大者恆大
    - 鼓勵 "暗池" - permissioned mempool

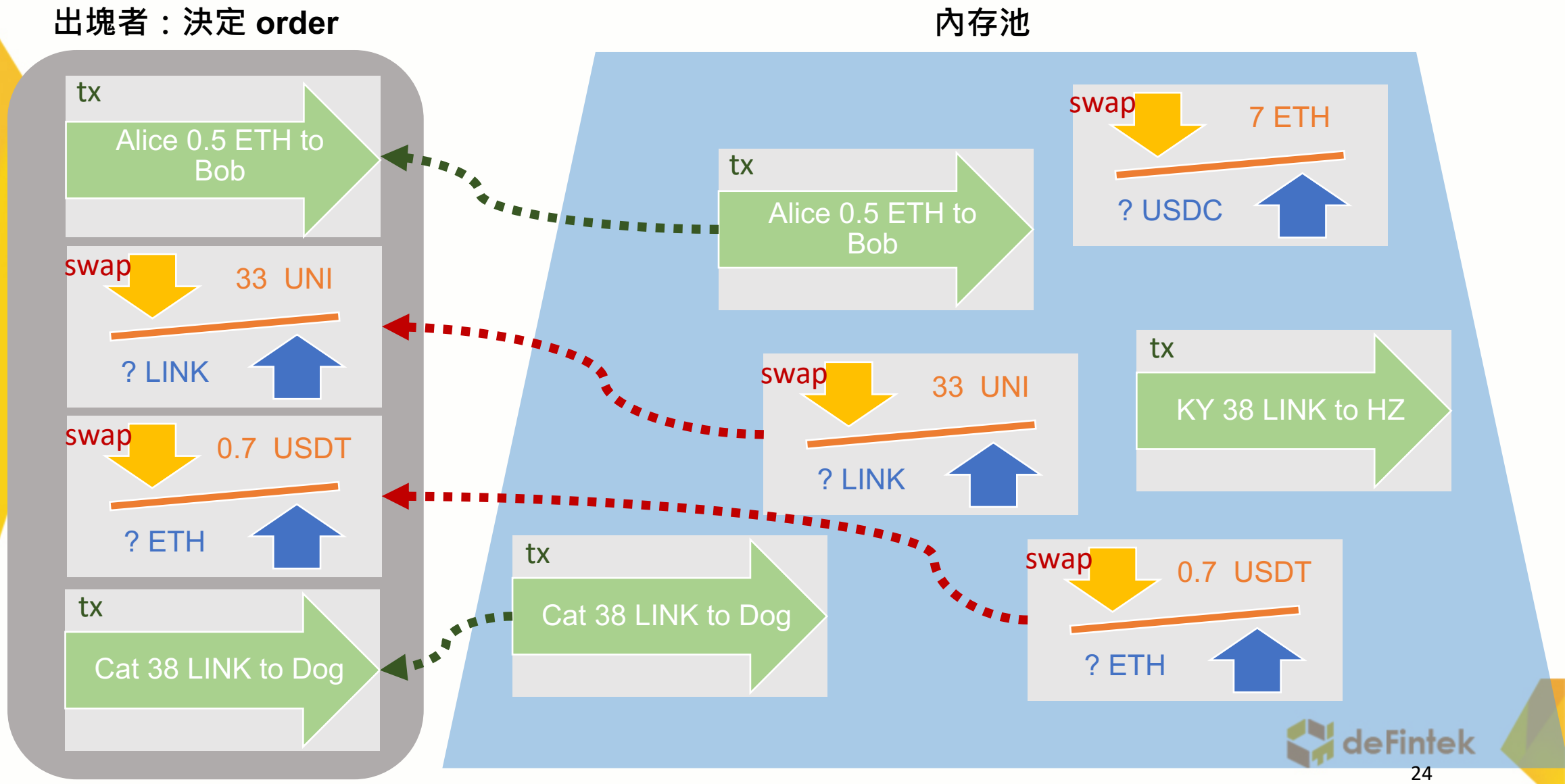
MEV 解法

- 黑暗森林 ➡ 公開競標場
- Tx-based ➡ Bundle-based ➡ Block-based

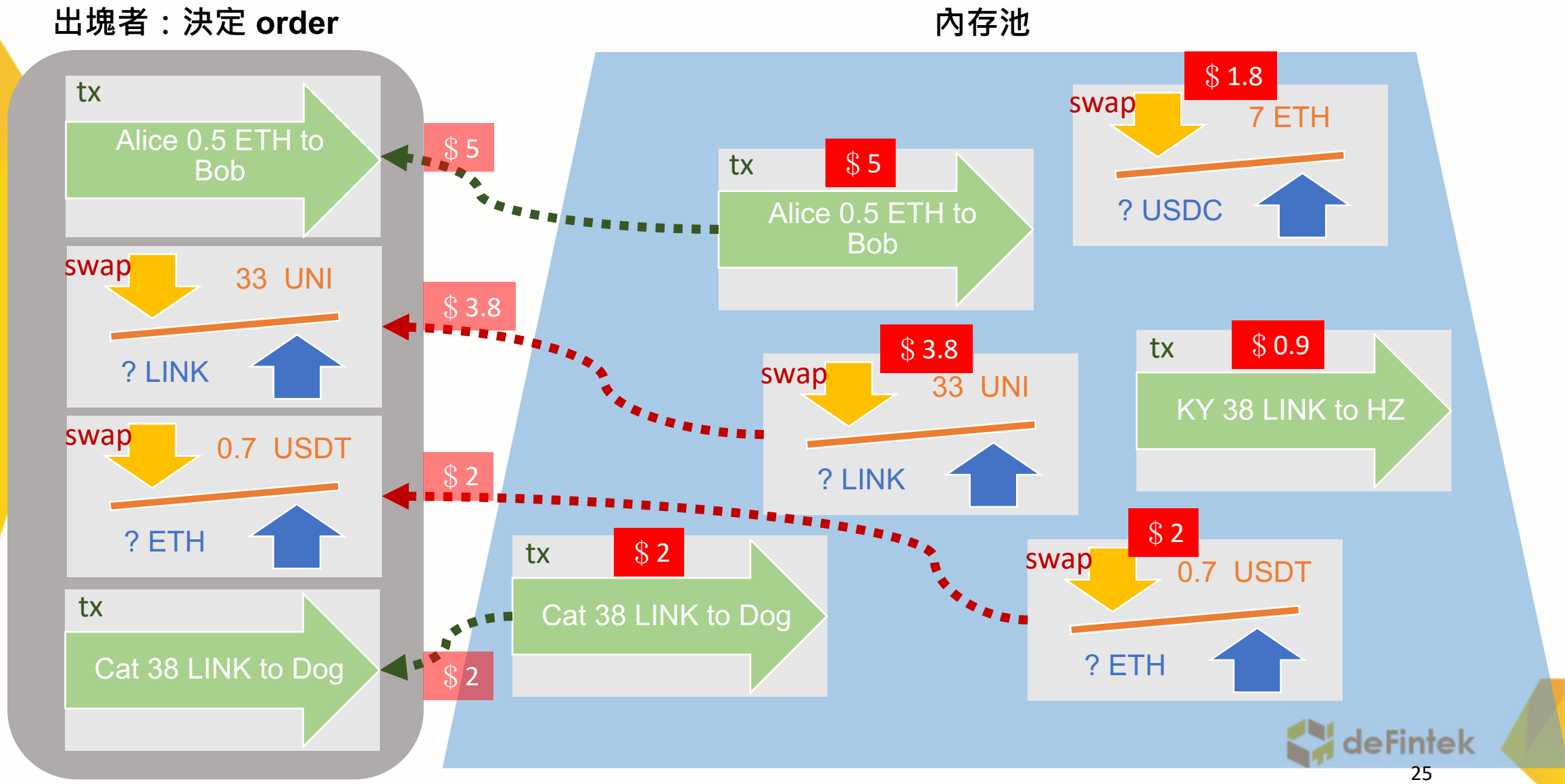
- Flashbots：Bundle-based 競標場
  - 照亮黑暗森林
  - 將「MEV 搜尋」去中心化
  - 重新分配 MEV 利益

- In-protocol：Block-based 競標場在共識層
  - ePBS：Enshrined Proposer-Builder Separation
  - Builder API

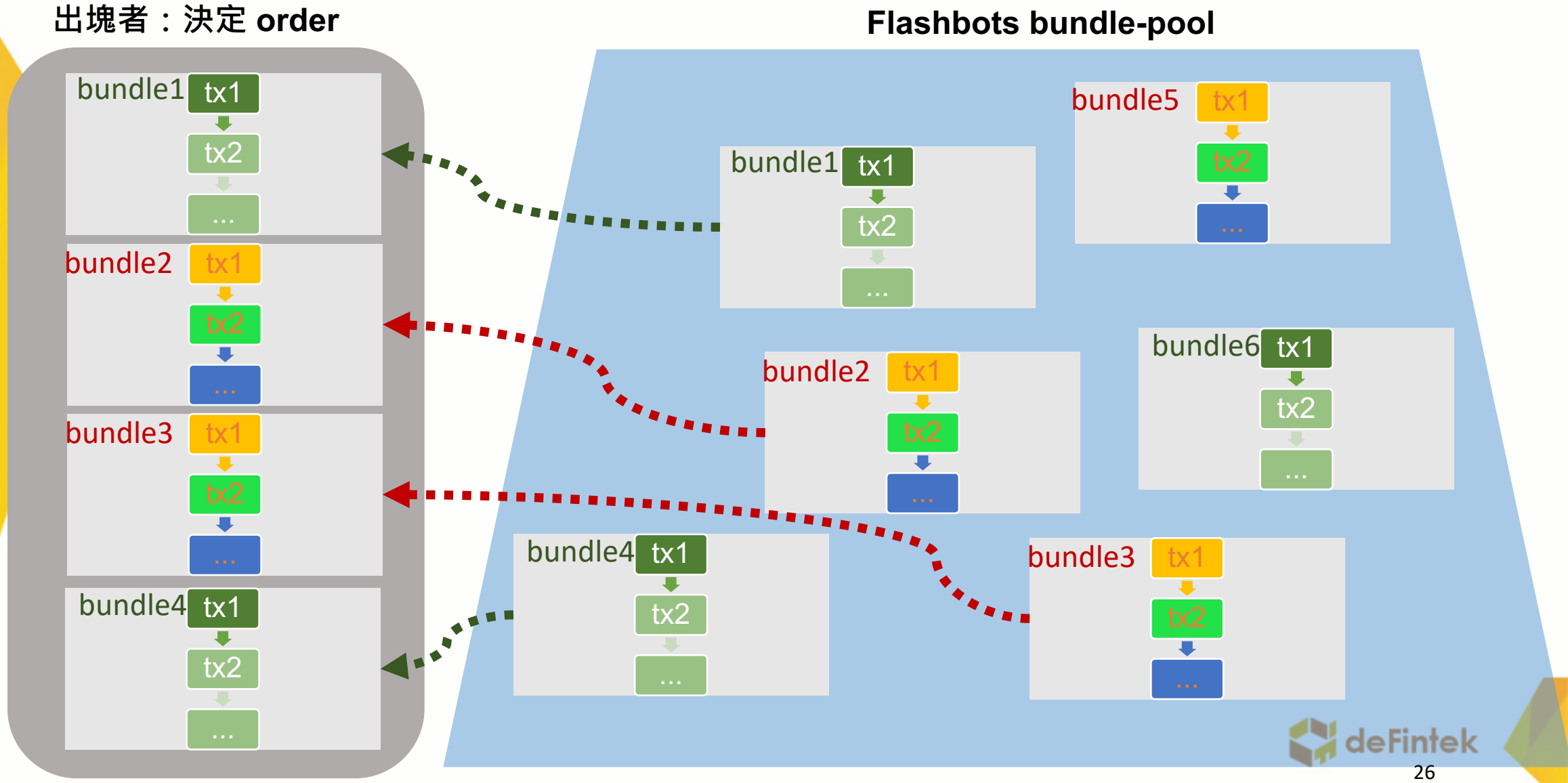
内存池：Tx-based 黑暗森林



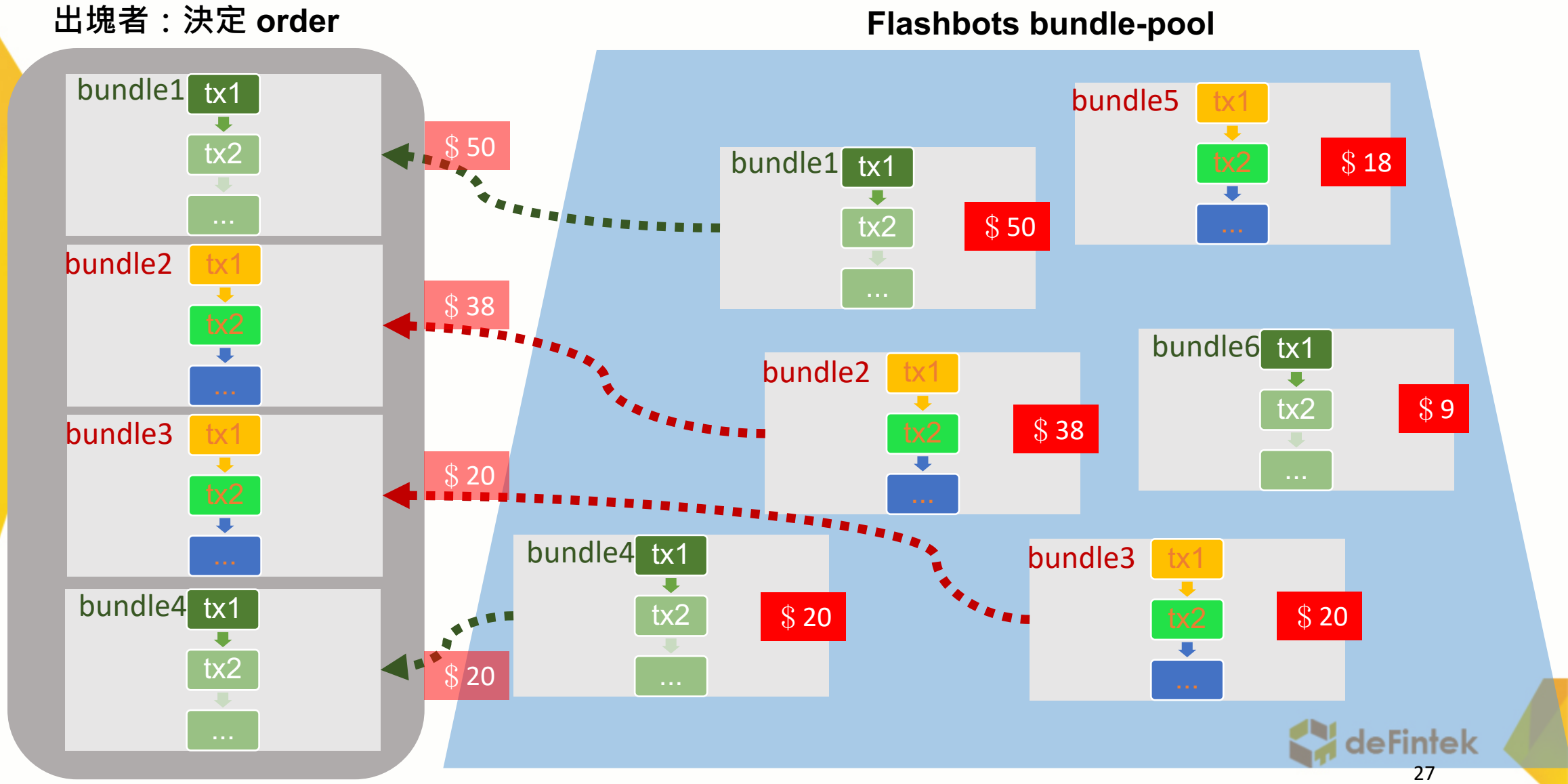
內存池：Tx-based 競標場？



Flashbots：Bundle-based Pool

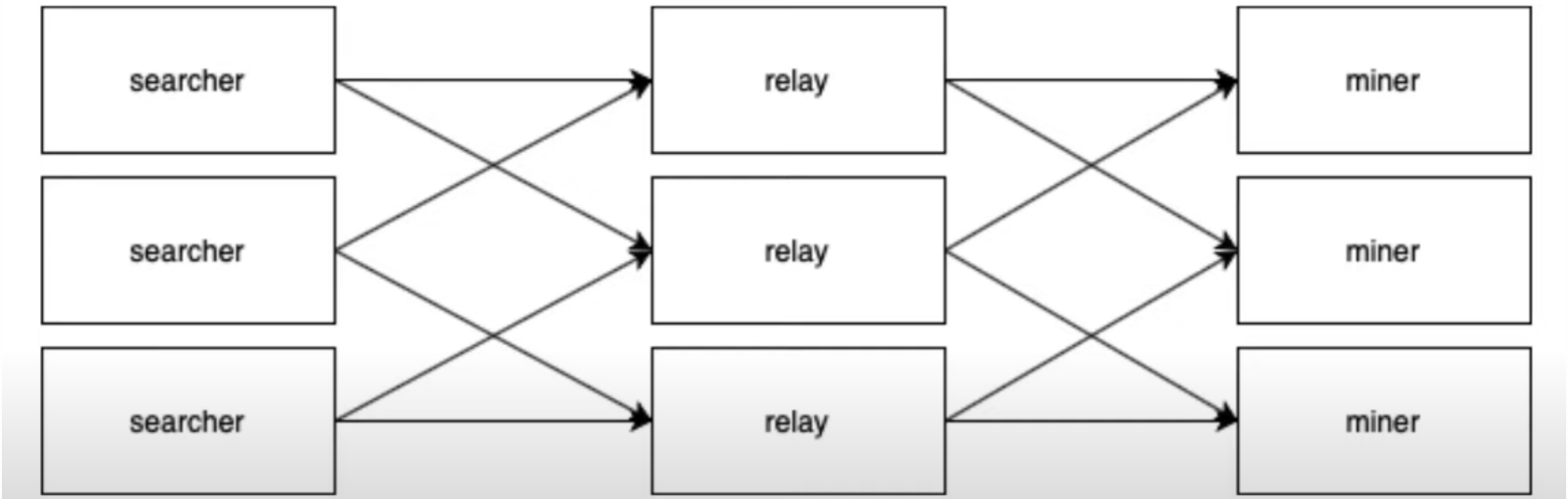


Flashbots：Bundle-based 競標場



Flashbots：私有的 Bundle 競標場

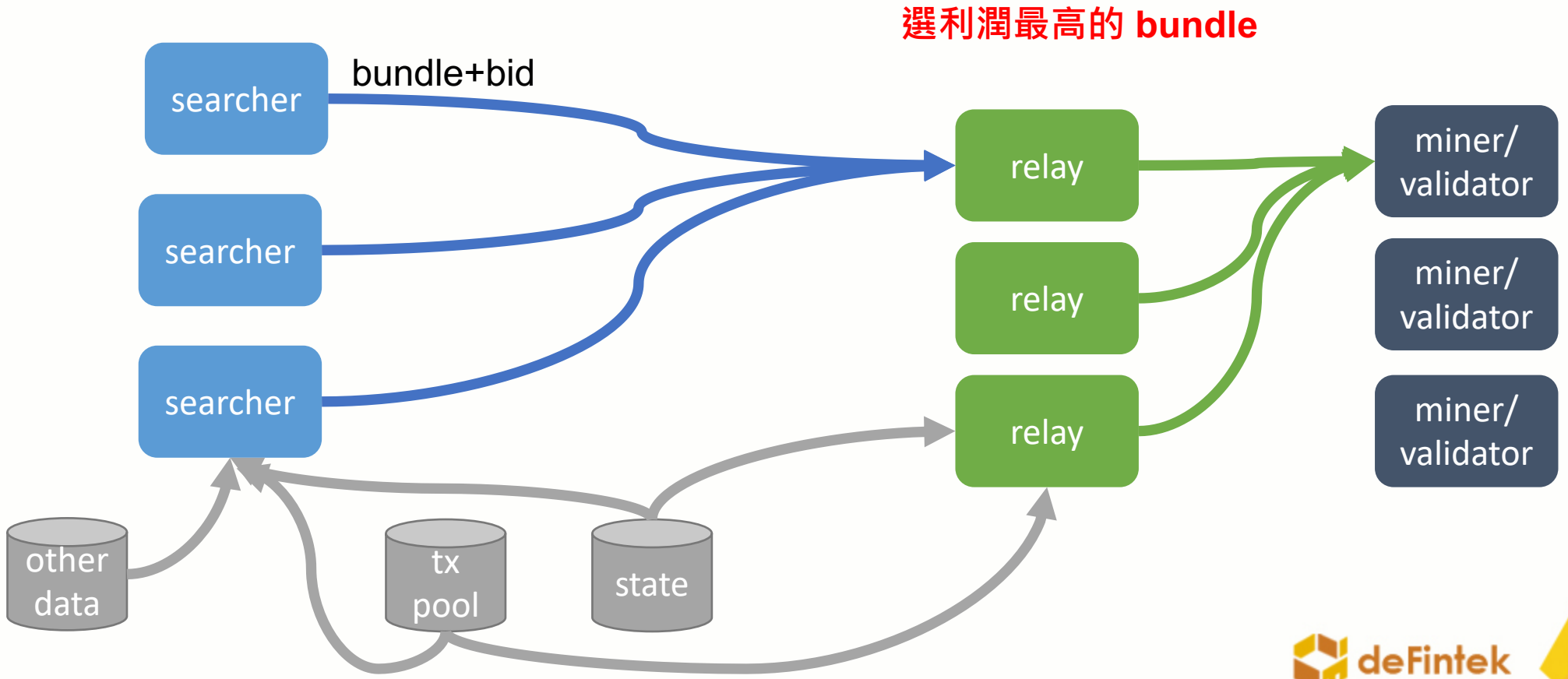
- mev-geth：密封的區塊空間競標場
  - 一個新的 RPC endpoint
- mev-relay：私有交易池
- mev-boost：更新的 Flashbots 架構 for PoS



deFintek

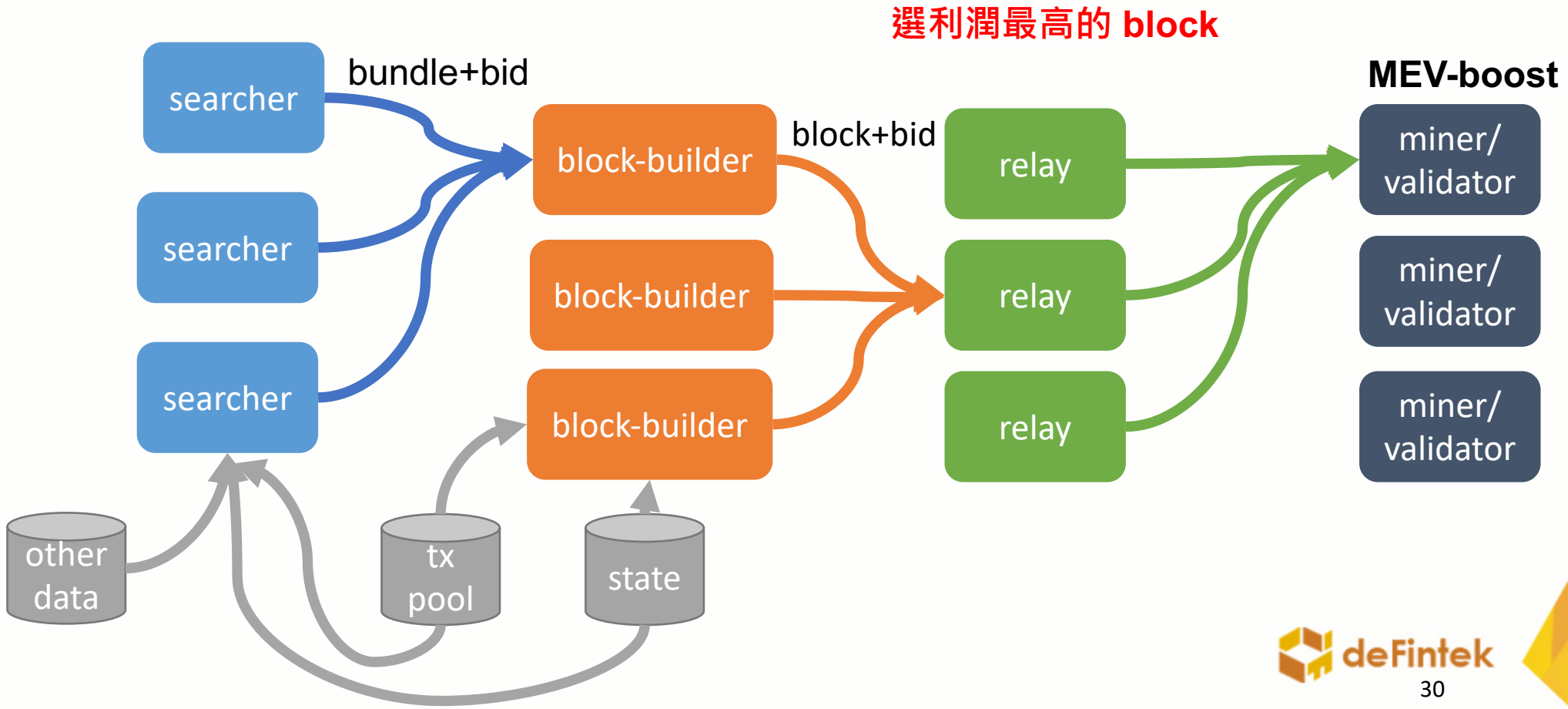
Pre-Merge Flashbots：Technical Architecture

- tx pool ➡ searcher ➡ relay ➡ miner/validator



Flashbots & PBS：Technical Architecture

- tx pool ➡ searcher ➡ block-builder ➡ relay ➡ miner/validator



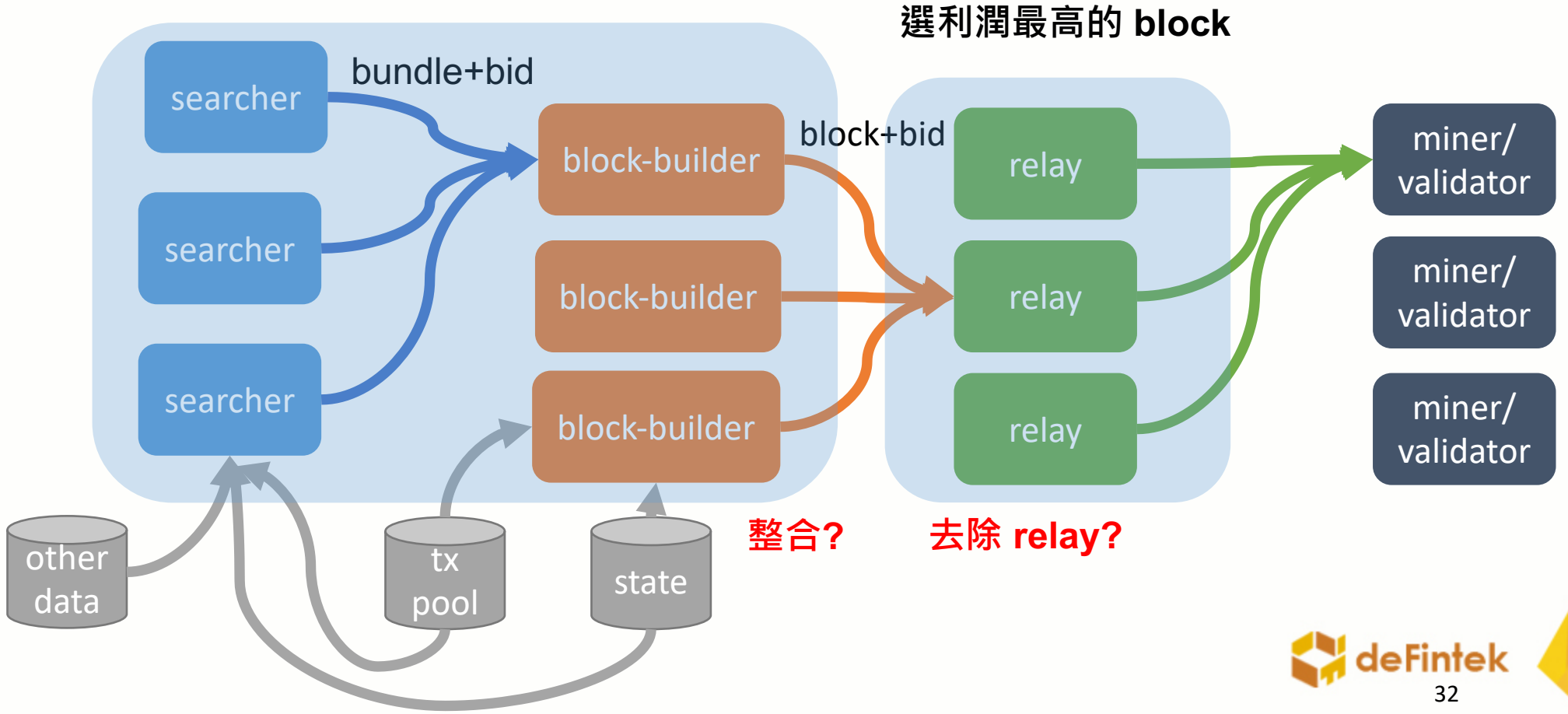
ePBS：Enshrined Proposer-Builder Separation

- In-protocol
  - 將 Flashbots 競標場的做法引進共識層
  - Tx-based ➡ Block-based
  - 共識層引入新角色：Block-builder
  - 將 proposer（validator） 與 builder 的角色分開，可增進以太坊的公平透明競爭、去中心化和抗審查性

- Builder API：
  - E.g. MEV-boost：Open source middleware run by validators

ePBS：Technical Architecture

- tx pool ➡ searcher ➡ block-builder ➡ relay ➡ miner/validator



ePBS：Block-builder vs. Validator

- Block-builder
  - 決定 tx order 組成 Beacon-Chain block（i.e. execution payload）
    - Block + bid
  - 可用特製硬體找尋 MEV 來最大化收益
  - Commit-reveal scheme
    - Block-builder 只提供 block-header + bid 給 validator
  - PEPC：Protocol Enforced Proposer Commitments
- Validator
  - 不需找尋 MEV，只要專注找最高 bid 的 block
    - 讓 solo staker 也能得到 MEV 好處，減少暗池及中心化可能性

MEV 相關研究

- Gas golf 技術（for searcher）
  - 用 programming tx 來減少 gas fee 的技術
  - E.g. 使用 prefix 有很多 0 的地址 0x0000000000C521824EaFf97Eac7B73B084ef9306
- "螳螂捕蟬，黃雀在後"
  - 廣義的 front-running：監控內存池裡 front-runner 的 tx，將其地址改成自己的
- 其他鏈的 MEV
- MEV job (bot) board by Flashbots
  - https://github.com/flashbots/mev-job-board

MEV 機會：Job Board by Flashbots

MEV opportunities

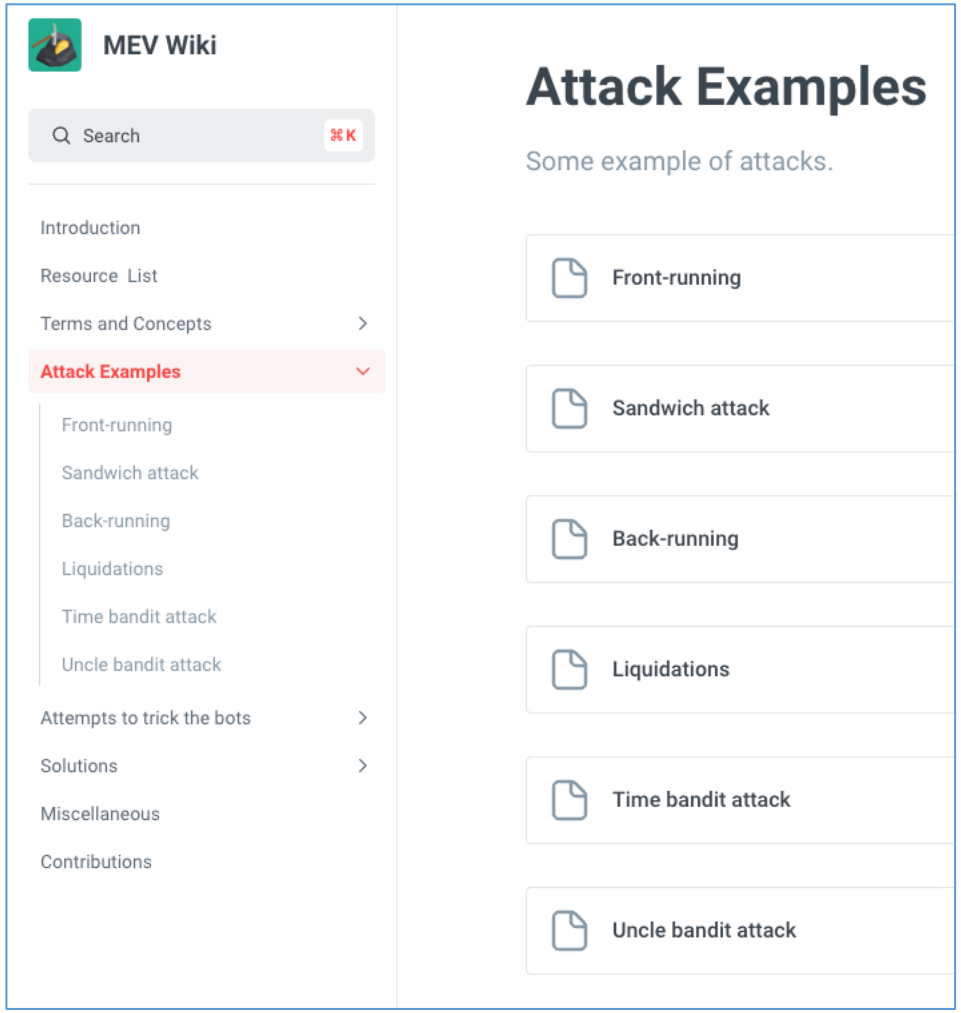
Protocol	Category	Reoccurring or one-off	Description
Template	Template	Template	An example MEV job spec that can be used by protocol teams
Synthetix	Arbitrage	Reoccurring	Arbitrage between sLINK minted at parity and trading at premium
Rari Capital's Fuse	Liquidations	Reoccurring	Compound-style liquidations on multiple small lending pools
Aave 👻	Liquidations	Reoccurring	Liquidate bad debt positions to earn liquidation bonus
Wild Credit	StakingFees	Reoccurring	Distribute pending fees to xWILD stakers
Gro Protocol	LP pool	Reoccurring	Arbitrage between pool exchange rate & pegs to underlying stables
Gro Protocol - new	LP pool	Reoccurring	Arbitrage between pool exchange rate & pegs to underlying stables - new PWRD pool
DPI Arbitrage	Arbitrage	Reocurring	Arbitrage between the DPI index token and underlying tokens
Maker wstETH liquidations	Liquidations	Reocurring	Liquidate bad wstETH debt positions on Maker to earn liquidation bonus
Vesper VUSD Arbitrage	Arbitrage	Reocurring	Arbitrage between the VUSD and USDC/DAI
Liquity	Liquidations	Reocurring	Liquidate undercollateralized Troves to earn liquidation bonus

https://github.com/flashbots/mev-job-board

deFintek

MEV 進階

- Attack Examples
  - https://www.mev.wiki/attack-examples
  - Time-Bandit Attack 時間強盜攻擊
    - https://www.mev.wiki/attack-examples/time-bandit-attack
  - Uncle-Bandit Attack 叔塊強盜攻擊
    - https://www.mev.wiki/attack-examples/uncle-bandit-attack
- Salmonella Attack 沙門桿菌攻擊
  - https://github.com/Defi-Cartel/salmonella



Flashbots Plan

- SUAVE：Single Unifying Auction for Value Expression
  - 獨立一條區塊鏈，只做特定用途，不與 L1/L2 競爭
  - 泛用型的解決方案 vs. ePBS 只存在以太坊
  - https://www.youtube.com/watch?v=1NzsfmAqbck

- MEV-Garden
  - Cross-domain markets w/ PBS and SUAVE
  - https://www.youtube.com/watch?v=XYg_0rt9pv8

Takeaway

- 背景
  - DeFi 去中心化金融平台：借貸平台、交易所
  - 搬磚套利、閃電貸、內存池（mempool）
  - 搶先交易、緊跟交易、三明治攻擊、清算

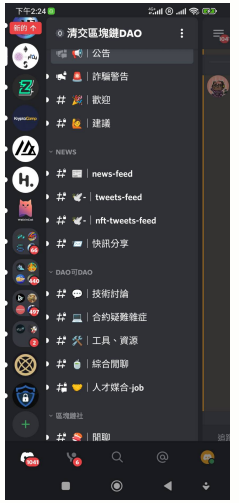
- 何謂 MEV
- MEV 影響
- MEV 解法與相關研究
  - Flashbots：Tx-based ➡ Bundle-based
  - In-protocol ePBS：Tx-based ➡ Block-based

歡迎加入「清交區塊鏈 DAO」

Web3 職涯讀書會

https://t.me/defistudy

清交區塊鏈 Discord



https://discord.com/invite/rpQy37a8tk

ReyerChu

https://t.me/reyerchu

清交區塊鏈 YouTube

https://www.youtube.com/@defi

deFintek

Thank You

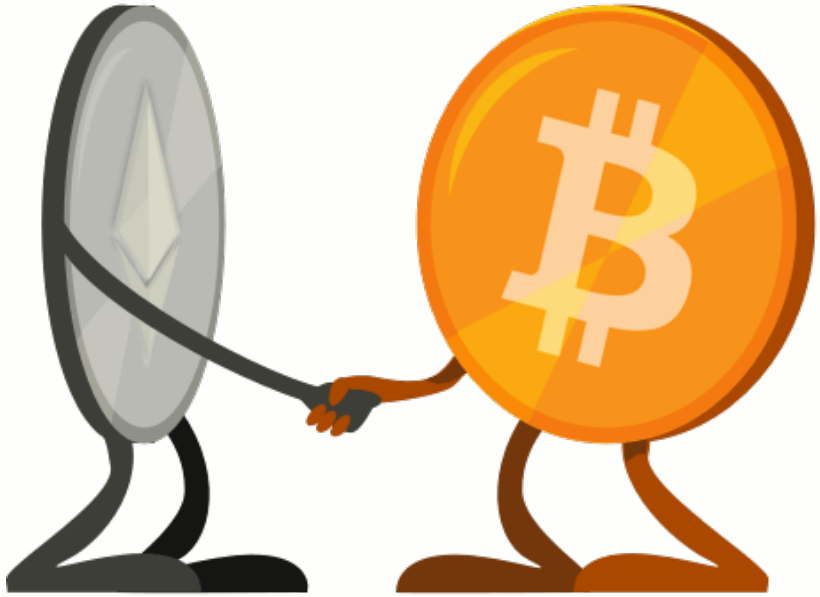


Image Courtesy https://www.ethereum.org/ether

deFintek

參考資料

- Charlie Noyes, https://research.paradigm.xyz/MEV
- Raphael Auer, Jon Frost and Jose Maria Vidal Pastor (2022): “Miners as intermediaries: extractable value and market manipulation in crypto and DeFi”. https://www.bis.org/publ/bisbull58_appendix.pdf
- Qin, K, L Zhou and A Gervais (2021): “Quantifying blockchain extractable value: How dark is the forest?”, arXiv:2101.05511. https://arxiv.org/pdf/2101.05511.pdf
- Daian, P, S Goldfeder, T Kell, Y Q Li, X Y Zhao, I Bentov, L Breidenbach and A Juels (2020): “Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability”, 2020 IEEE Symposium on Security and Privacy (SP), vol 1, pp 910–27. https://arxiv.org/pdf/1904.05234.pdf
- Flashbots Docs: https://docs.flashbots.net/
- MEVboost.org: https://www.mevboost.org/
- Blocknative: https://docs.blocknative.com/mev-relay-instructions-for-ethereum-validators
- MEV.wiki: https://www.mev.wiki/

附錄

CoW Protocol

- CoW：Coincidence of Wants 需求的巧合
- CoW Protocol
  - https://cow.fi/
  - 匹配可能的點對點交易，省去中間商
  - 搜索 1inch、Uniswap 等 DEX 及聚合器，獲得最佳價格
  - MEV 保護
  - 失敗的交易無需付費
  - 用出售代幣來收取費用，不需使用 ETH
  - 不需等到一筆交易完成後再進行另一筆交易
  - 由 Gnosis 孵化，由透明且值得信賴的工程師社區構建，將安全放在首位

CoW Protocol 運作方式

1

Batch

CoW Protocol collects orders into "batches" every 30 seconds. This is done off-chain, which has a few benefits – you won't pay if your trade fails, and the fees are collected in your sell token, not ETH.

2

Match

CoW Protocol's network of solving algorithms ("solvers") scans each batch for Coincidences of Wants (i.e. traders who want what each other has). These "CoWs" are matched peer-to-peer, so everyone gets a better price and no one pays unnecessary AMM fees.

3

Search

CoW Protocol's solvers compete to find the best liquidity source for your trade across all decentralized exchanges and aggregators. So the worst price you'll get with CoW Protocol is the best price available elsewhere.

4

Settle

CoW Protocol submits the batches on-chain and hides them from the public mempool, so your trade is protected from manipulation (frontrunning and other forms of MEV) by miners and bots.

Flashbots 統計：Registered Validators

- ~2022/9
- **The Flashbots MEV-Boost Relay has 160,651 registered validators of 434,499 total validators (36.9% adoption) as of September 23, 2022.** The Flashbots Builder has delivered over 10,000 payloads https://www.mevboost.org/ 🙌🥳

https://boost.flashbots.net/mev-boost-status-updates/mev-boost-status-update-sep-9-sept-22-2022

deFintek

Flashbots 現況：~89% by MEV-Boost

- https://www.mevboost.org/ 2022/12/16

mevboost.org

Tracking MEV-Boost relays and block builders. A quick hack by Anish. Design inspired by file.app. API documentation.

Network participation (24h)
89.08%
% of MEV-Boost blocks relayed in last 24h.

Flashbots dominance
74.69%
% of MEV-Boost blocks relayed by Flashbots.

Active relays
10
Relays that relayed at least one block (Flashbots, BloXroute Max Profit, Blocknative, Eden, BloXroute Regulated, BloXroute Ethical, Manifold, Relayooor, Agnostic Relay, ultra sound relay).

Top relays
Relays sorted by number of relayed blocks.

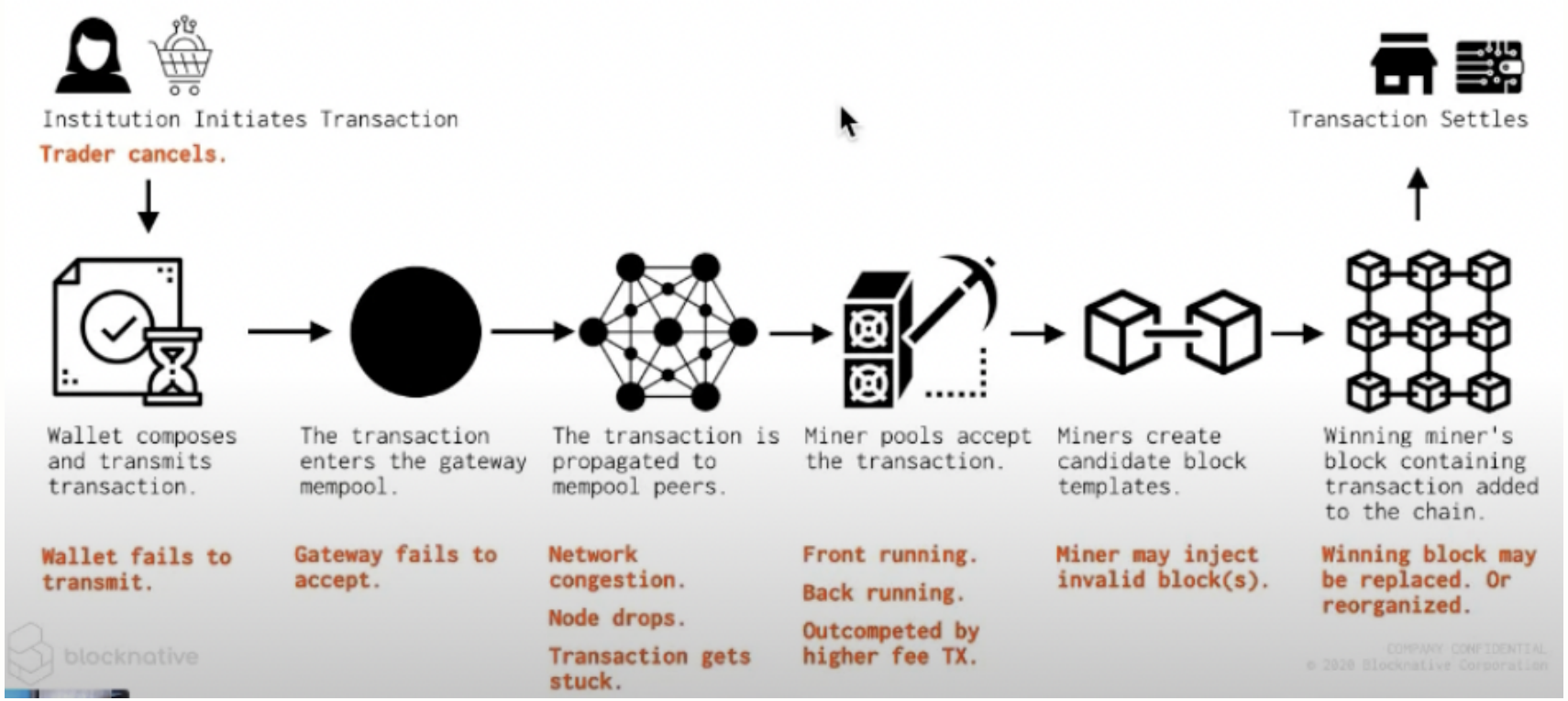
RELAY	# BLOCKS	TOTAL VALUE (ETH)	AVERAGE BLOCK VALUE (ETH)
Flashbots	335,396	50,412.535	0.15
BloXroute Max Profit	55,077	6,003.259	0.109
Blocknative	18,683	1,861.076	0.1
Eden	13,175	2,471.537	0.188
BloXroute Regulated	9,260	1,002.232	0.108
BloXroute Ethical	8,134	648.542	0.08
Manifold	5,087	517.449	0.102
Relayooor	2,077	233.682	0.113
Agnostic Relay	1,587	229.371	0.145
ultra sound relay	578	137.263	0.237

Top builders
Block builders sorted by number of built blocks.

BUILDER	# BLOCKS	TOTAL VALUE (ETH)	AVERAGE BLOCK VALUE (ETH)	LAST USED RELAY

ETH tx 發送流程

- Wallet -> Gateway mempool
  -> mempool peers -> Miner pools -> Block -> Blockchain



https://www.youtube.com/watch?v=aZPx7K8XI68