Towards a theory of Decentralized Finance

IFIP WG 2.2 Meeting, Münster/Online, Sept. 20-21, 2021

James Hsin-yu Chiang
Technical University of Denmark

Massimo Bartoletti
University of Cagliari

Alberto Lluch-Lafuente
Technical University of Denmark

DTU Compute

Decentralized Finance: Examples

1 Lending Pools

Crypto-asset Lending
- Borrowers borrow against collateral
- Algorithmic interest rate
- Current deposits in Compound: **$13.2B**

2 Automatic Market Makers

Crypto-asset Swaps
- Asset swaps without matching orders
- Algorithmic exchange rate
- Current deposits in Uniswap: **$7.7B**

3 (Algorithmic) Stable Coins

Crypto-asset with pegged price
- Price stability via algorithmic supply
- Useful as stable collateral
- Current deposits in MakerDAO: **$9.3B**

DeFi algorithms are managing >$100B worth of funds (~500% yoy)

DeFi: Examples of Vulnerabilities

Slock.It	Parity Wallet	Synthetix	MakerDAO	UniSwap	Lendf.me	PolyNetwork
Fundraising Contract	Wallet Library	Synthetic Assets	Stable Coin	AMM	Lending	Cross-chain DeFi
$ 60 M	**$310M**	**$37M**	$8M	$0.3M	$25M	**$600M**
2016	2017	2019	2020	2020	2020	**2021**
Smart Contract Vulnerability	**Smart Contract Vulnerability**	**Pricing Oracle Vulnerability**	Pricing Oracle Vulnerability	Smart Contract Vulnerability	Smart Contract Vulnerability	**Smart Contract Vulnerability**

Towards a Formal Theory of DeFi

An overview of our approach

1 Formal Executable Semantics

$\Gamma_i = A[100:\tau_0] \mid B[100:\tau_1] \mid (50:\tau_0) \mid (50:\tau_1) \mid (100:\tau_0, 100:\tau_1) \mid P$

$$\frac{(1)\ \sigma_A(\tau) \geq v \quad (2)\ \tau' := \begin{cases} \text{fresh} \notin \mathbb{T}_f & \text{if } \tau \notin \operatorname{dom} \pi_m \\ \pi_m(\tau) & \text{otherwise} \end{cases} \quad (3)\ v' := v/ER_\pi(\tau) \quad (4)\ \pi'_f := \pi_f + v:\tau \quad (5)\ \pi'_m := \begin{cases} \pi_m\{(\tau',v')/\tau\} & \text{if } \tau \notin \operatorname{dom} \pi_m \\ \pi_m\{(\tau',v''+v')/\tau\} & \text{if } \pi_m(\tau) = (\tau', v'') \end{cases}}{\sigma \mid \pi \mid p \xrightarrow{\mathsf{Dep}_A(v:\tau)} \sigma\{\sigma_A - v:\tau + v':\tau'/A\} \mid (\pi'_f, \pi_l, \pi'_m) \mid p} \text{[Dep]}$$

$$\frac{(1)\ \pi_f(\tau) \geq v > 0 \quad (2)\ f_A = \begin{cases} \pi_l A + v:\tau & \text{if } A \in \operatorname{dom} \pi_l \\ \{v/\tau\} & \text{otherwise} \end{cases} \quad (3)\ \pi' := (\pi_f - v:\tau,\ \pi_l\{f_A/A\},\ \pi_m) \quad (4)\ C_{\sigma|\pi'|p}(A) \geq C_{min}}{\sigma \mid \pi \mid p \xrightarrow{\mathsf{Bor}_A(v:\tau)} \sigma\{\sigma_A + v:\tau/A\} \mid \pi' \mid p} \text{[Bor]}$$

$$\frac{\pi'_l(A) := f'_A \ \text{ if } A \in \operatorname{dom} \pi_l, \text{ where } f'_A(\tau) := (I_\pi(\tau)+1) \cdot (\pi_l A)\tau \ \text{ if } \tau \in \operatorname{dom}(\pi_l A)}{\sigma \mid \pi \mid p \xrightarrow{\mathsf{Int}} \sigma \mid (\pi_f, \pi'_l, \pi_m) \mid p} \text{[Int]}$$

$$\frac{(1)\ \sigma_A(\tau) \geq v > 0 \quad (2)\ (\pi_l A)\tau \geq v \quad (3)\ \pi'_l = \pi_l\{\pi_l A - v:\tau/A\}}{\sigma \mid \pi \mid p \xrightarrow{\mathsf{Rep}_A(v:\tau)} \sigma\{\sigma_A - v:\tau/A\} \mid (\pi_f + v:\tau,\ \pi'_l,\ \pi_m) \mid p} \text{[Rep]}$$

$$\frac{\begin{array}{l}(1)\ \sigma_A(\tau) \geq v > 0 \quad v' := v \cdot ER_\pi(u_\pi(\tau)) \quad (2)\ \pi_f(u_\pi(\tau)) \geq v' \\ (3)\ (\exists \tau'.(\pi_l A)\tau' > 0) \Rightarrow C_{\sigma'|\pi'|p}(A) \geq C_{min} \quad \sigma'_A := \sigma_A - v:\tau + v':u_\pi(\tau) \\ \pi'_f := \pi_f - v':u_\pi(\tau) \quad \pi'_m := \pi_m\{(\tau, v''-v)/u_\pi(\tau)\} \text{ where } (\tau, v'') := \pi_m(u_\pi(\tau))\end{array}}{\sigma \mid \pi \mid p \xrightarrow{\mathsf{Rdm}_A(v:\tau)} \sigma\{\sigma'_A/A\} \mid (\pi'_f,\ \pi_l,\ \pi'_m) \mid p} \text{[Rdm]}$$

$$\frac{\begin{array}{lll}(1)\ \sigma_A(\tau) \geq v & (2)\ (\pi_l B)\tau \geq v & (3)\ \tau' \in \mathbb{T}_\pi \\ (4)\ \sigma_B(\tau') \geq v' & (5)\ v' = v \cdot \frac{p(\tau)}{p(u_\pi(\tau'))} \cdot r_{liq} & \\ (6)\ C_{\sigma|\pi|p}(B) < C_{min} & (7)\ C_{\sigma'|\pi'|p}(B) \leq C_{min} & \\ (8)\ \pi'_l := \pi_l B - v:\tau & (9)\ \sigma'_A := \sigma_A - v:\tau + v':\tau' & (10)\ \sigma'_B := \sigma_B - v':\tau'\end{array}}{\sigma \mid \pi \mid p \xrightarrow{\mathsf{Liq}_A(B, v:\tau, v':\tau')} \sigma\{\sigma'_A/A\}\{\sigma'_B/B\} \mid (\pi_f, \pi'_l, \pi_m) \mid p} \text{[Liq]}$$

$$\frac{\sigma_A(\tau) \geq v \quad \tau \in \mathbb{T}_\pi \quad \sigma' = \sigma\{\sigma_A - v:\tau/A\}\{\sigma_B + v:\tau/B\} \quad C_{\sigma'|\pi|p}(A) \geq C_{min}}{\sigma \mid \pi \mid p \xrightarrow{\mathsf{Mtrf}_A(B, v:\tau)} \sigma' \mid \pi \mid p} \text{[Mtrf]}$$

* LP transition rules shown

2 Foundational Properties

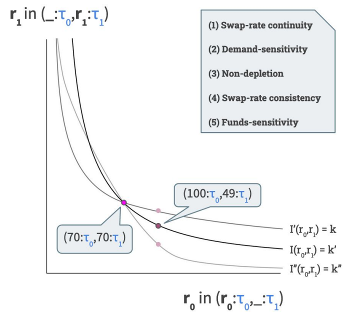
Lending Pools

- Increasing exchange rate $ER_\Gamma(\{\tau\})$
- Preservation of token supply
- ε-collateralization (loan recoverability)

AMMs

- Concurrency theory
- Preservation of supply, net-wealth
- Liquidity of deposited funds
- Game-based value extraction & incentives

* AMM: Incentive-consistent funds invariant



3 … and more coming

Current and future Work

- Composed security/vulnerabilities
- New designs with less vulnerabilities, e.g. MPC to mitigate front-running
- A DSL for DeFi

Related papers

SoK: Lending Pools in Decentralized Finance
- https://arxiv.org/abs/2012.13230

A theory of Automated Market Makers in DeFi
- https://arxiv.org/abs/2102.11350

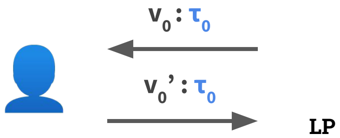
Maximizing Extractable Value from Automated Market Makers
http://arxiv.org/abs/2106.018700

DeFi as a Labeled Transition System (LTS)

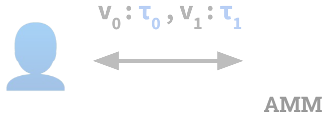
$$\Gamma_i = \overbrace{A[100:\tau_0]}^{\text{User A Wallet}} \mid \overbrace{B[100:\tau_1]}^{\text{User B Wallet}} \mid \overbrace{(50:\tau_0) \mid (50:\tau_1)}^{\text{LP Contract}} \mid \overbrace{(100:\tau_0, 100:\tau_1)}^{\text{AMM Contract}} \mid \overbrace{P}^{\text{Token prices}}$$

$$\Gamma_i \xrightarrow{\text{User : action}(\ \ldots\ )} \Gamma_{i+1}$$

Lending (LP)

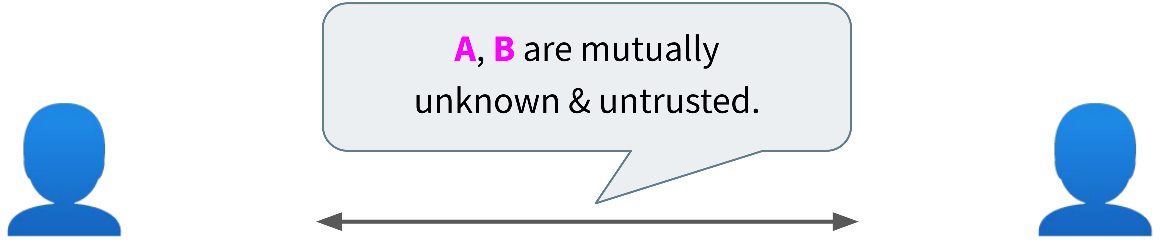


Swaps (AMM)



Composition?
(e.g. AMM as price oracle for LP)

LP: A Disintermediated Loan Market



Γ_0 : A[125:τ_0] B[100:τ_1]

LP: Deposits

Γ_0 :	A[125: τ_0]	-	B[100: τ_1]
Γ_1 :	A[25: τ_0, **100**:{τ_0}]	(100: τ_0)	B[100: τ_1]

A receives units of <u>minted</u> {τ_i} to represent deposit.

A new LP pool (_: τ_i)

LP: Borrows

Γ_0 : A[125:τ_0] - B[100:τ_1]

Γ_1 : A[25:τ_0, **100**:{τ_0}] (100:τ_0) B[100:τ_1]

❌ **Invalid Action**: What incentivizes **B** to repay?

LP: Borrows

B: dep$(100{:}\tau_1)$

B : bor$(50{:}\tau_0)$

LP

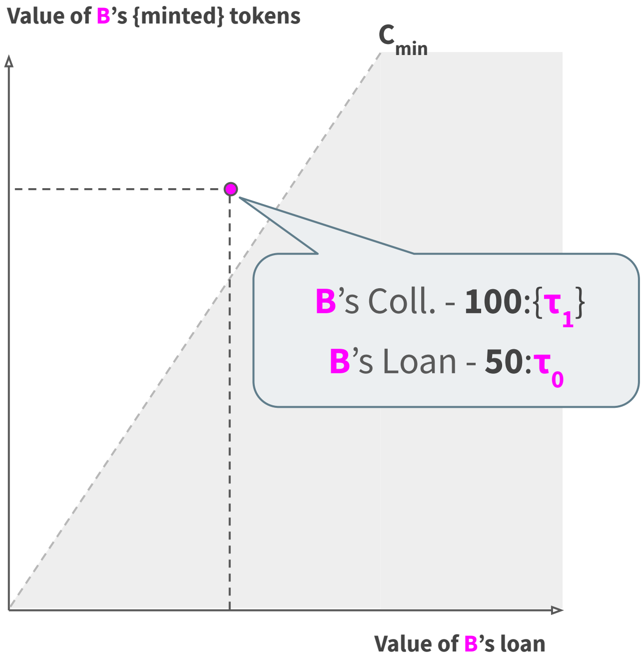
Γ_1 :	$A[25{:}\tau_0,\ 100{:}\{\tau_0\}]$	$(100{:}\tau_0)$	$B[100{:}\tau_1]$
Γ_2 :	$A[25{:}\tau_0,\ 100{:}\{\tau_0\}]$	$(100{:}\tau_0) \mid (\mathbf{100}{:}\tau_1)$	$B[\mathbf{100}{:}\{\tau_1\}]$
Γ_3 :	$A[25{:}\tau_0,\ 100{:}\{\tau_0\}]$	$(\mathbf{50}{:}\tau_0,\{B{:}\mathbf{50}\}) \mid (100{:}\tau_1)$	$B[\mathbf{50}{:}\tau_0,100{:}\{\tau_1\}]$

(**#loan**)

(**#held**)

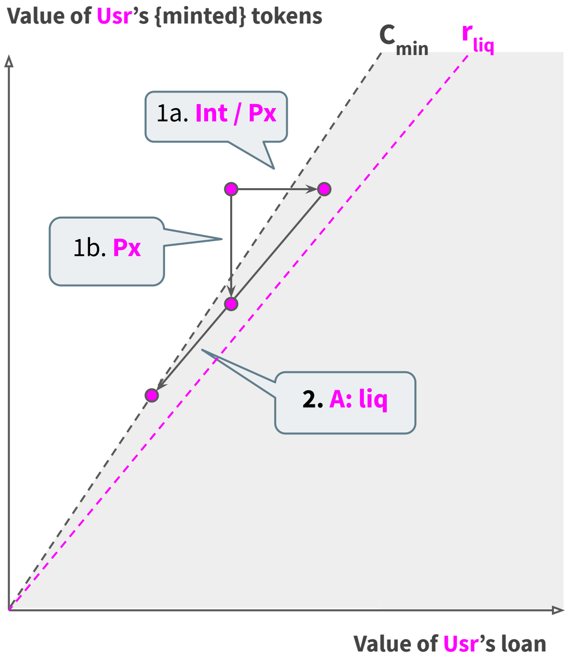
B's minted tokens **100:{**τ_1**}** serve as collateral. They are not free!

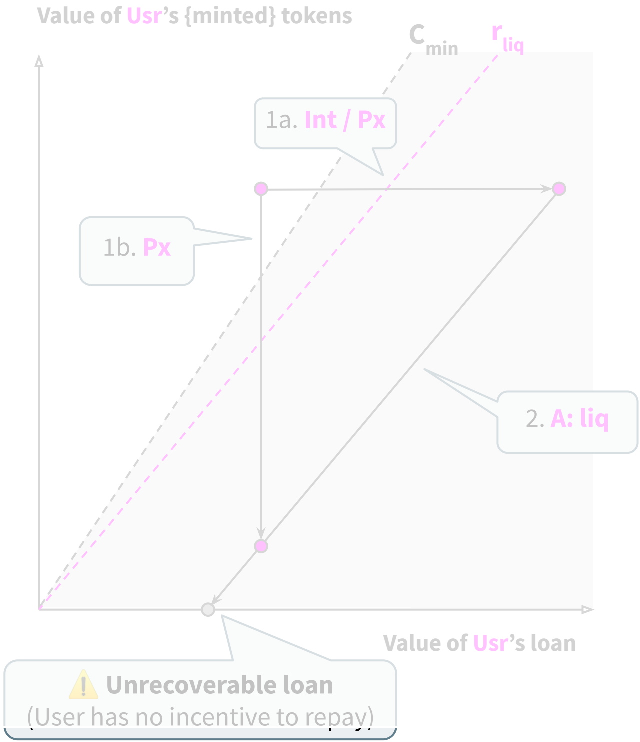
Collateralization of Loans



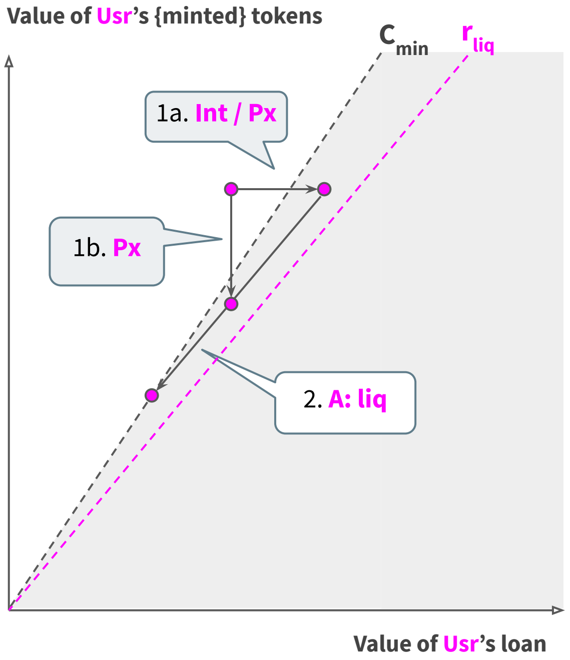
$$\text{Collateralization}_{\Gamma}(B) = \frac{\text{Value of \{minted\} tokens of } B}{\text{Value of borrowed tokens of } B}$$

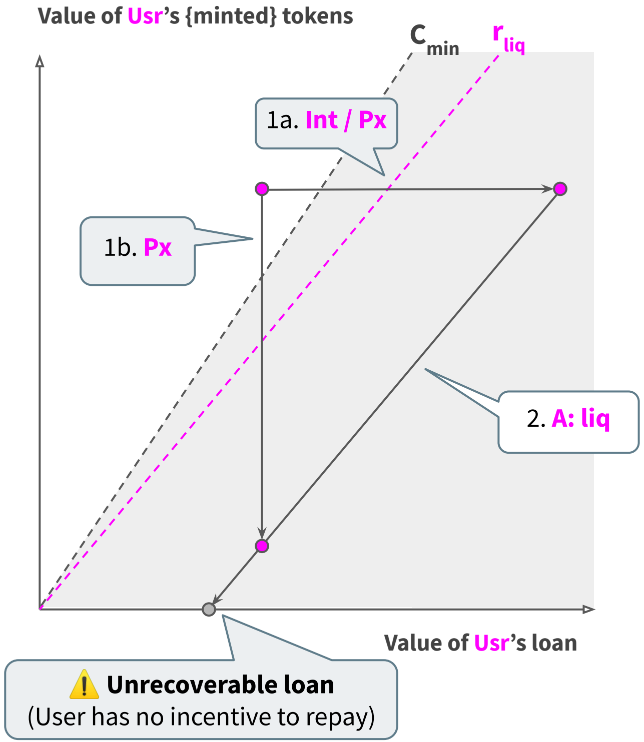
Collateralization Safety



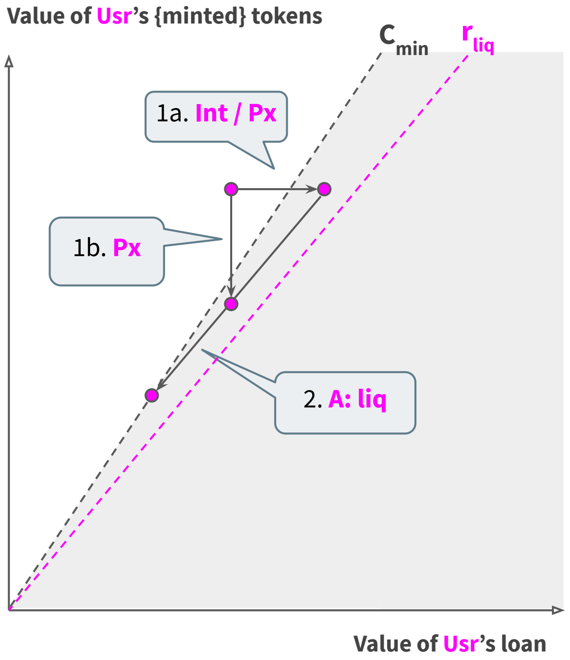


LP: Collateralization Safety





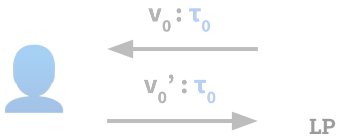
LP: Collateralization Safety



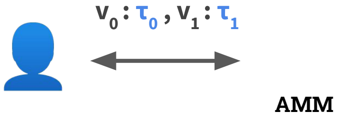
Collateralization safety depends on

- Price stability: e.g. Stable-coins
- Effectiveness of liquidation incentive
- **Trusted price oracle**

Lending (LP)



Swaps (AMM)



Composition?
(e.g. AMM as price oracle for LP)

AMM: A Disintermediated Market Marker

A, B are mutually unknown & untrusted.

Γ_0 :

A[70:τ_0,70:τ_1]

B[30:τ_0,10:τ_1]

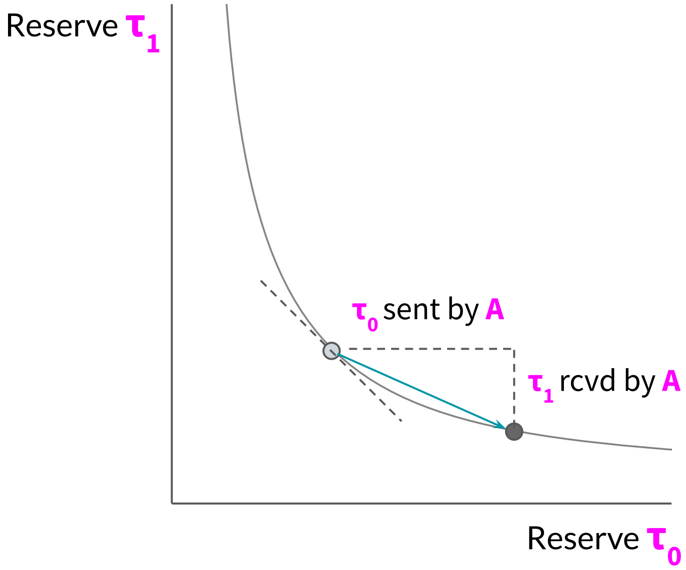
Depositing User
Would like to increase value of holdings (τ_0,τ_1)

Exchanging User
Would like to swap between τ_0 and τ_1

Token Swaps: Automatic Market Makers

A: swapL

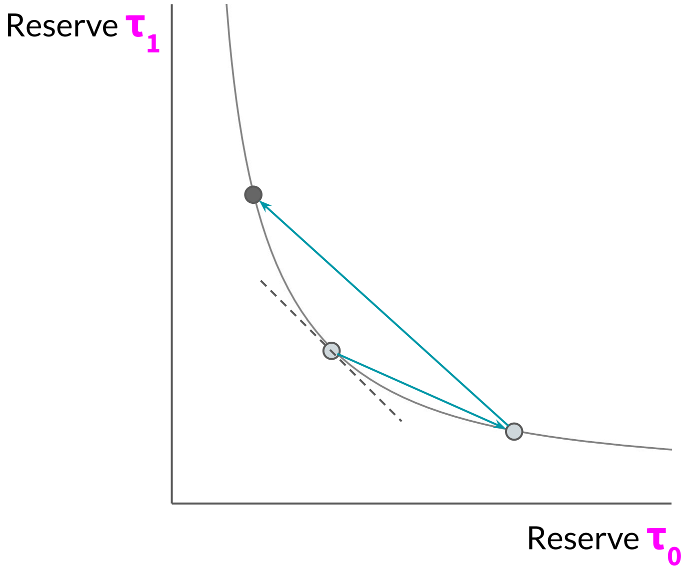
r_0 * r_1 = k = r’_0 * r’_1



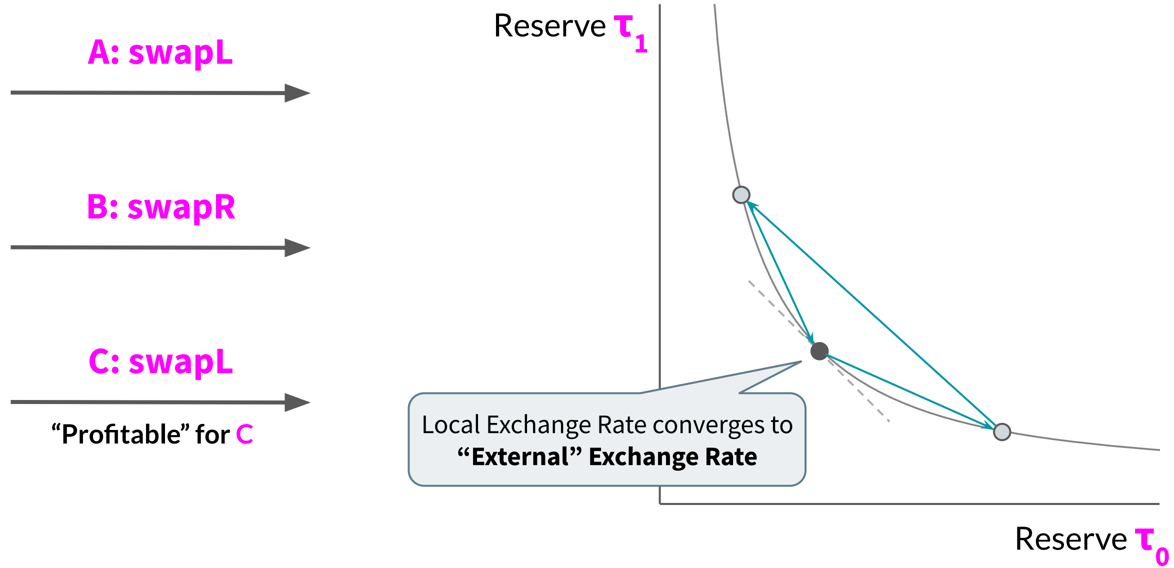
Token Swaps: Automatic Market Makers

A: swapL

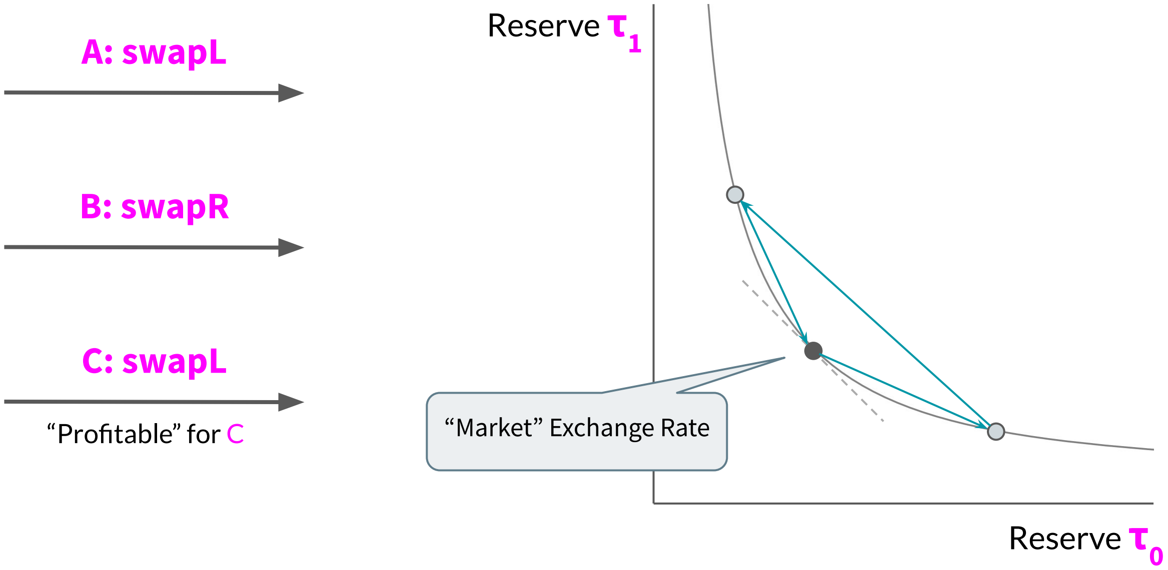
B: swapR



Token Swaps: Automatic Market Makers



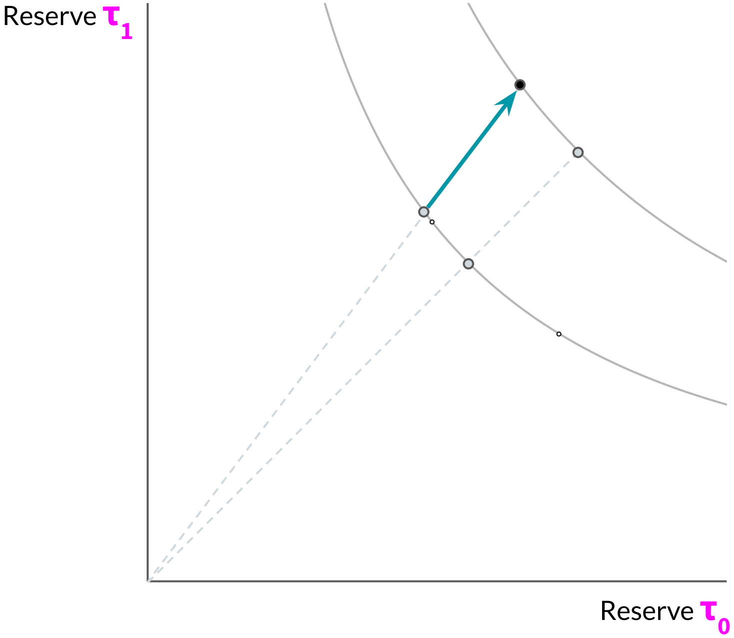
Token Swaps: Automatic Market Makers



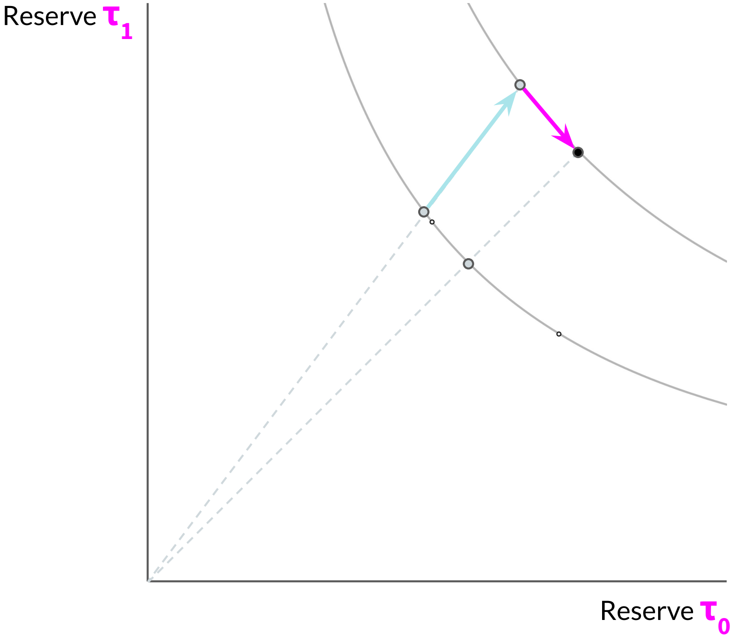
AMM offers swap without counter-party

Price Oracle: Tends towards market exchange rate

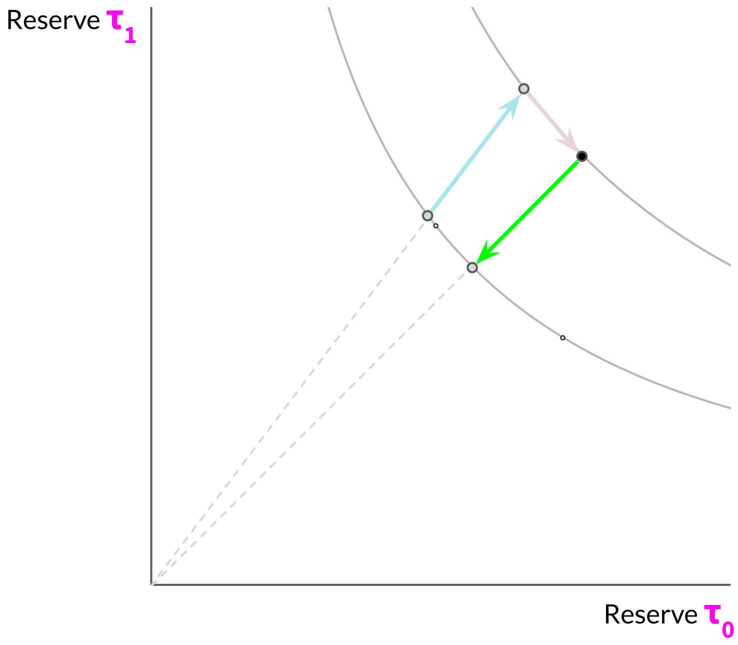
An example trace: deposit



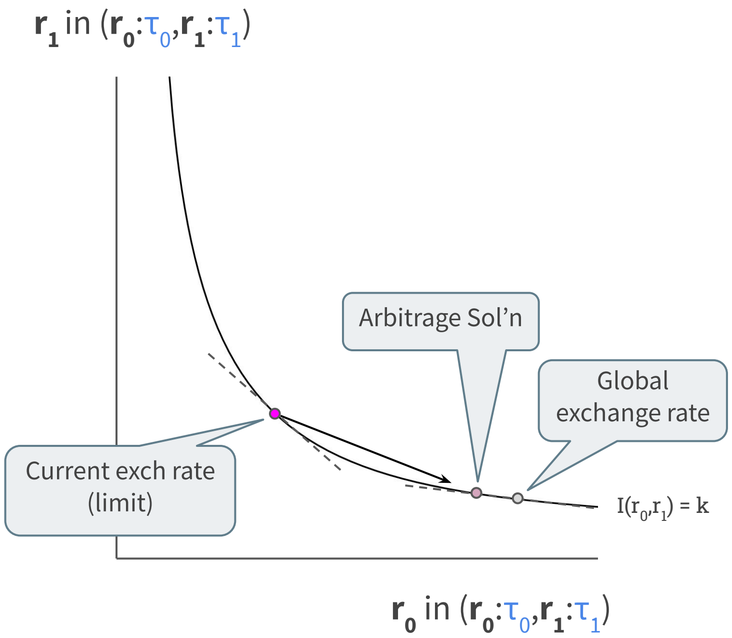
An example trace: swap



An example trace: redeem



AMM: Arbitrage Game



For any *incentive-consistent I*

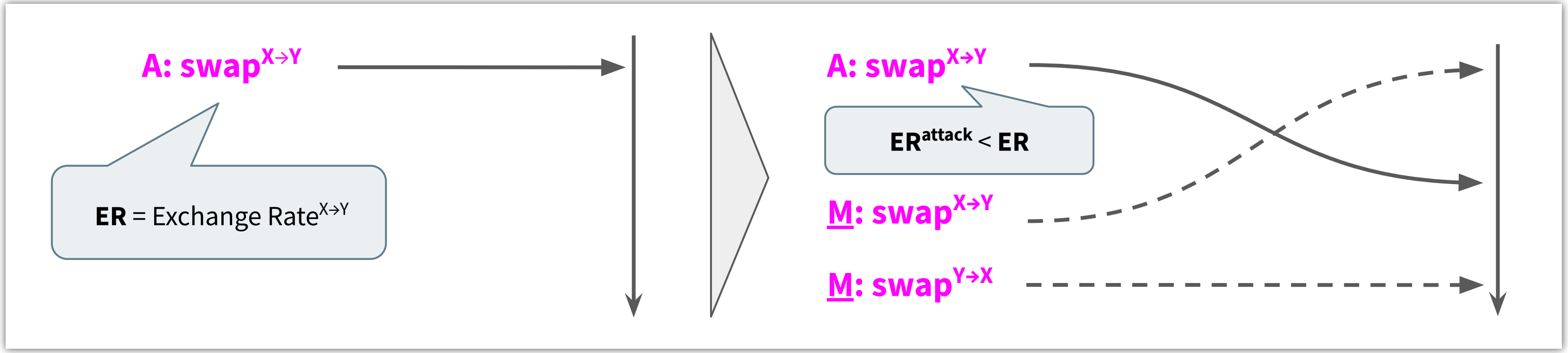
- There exists a unique arbitrage sol'n
- … consisting of a swap action
- … at any global price

⇒ AMM trails global exchange rate

Can we use AMM as price oracles?

(No trusted third party)

AMM: Miner Extractable Value



Adversarial Miner finalizes action sequence

- Can select user actions from tx-pool
- Can inject miner actions
- Also known as "front-running" by miner

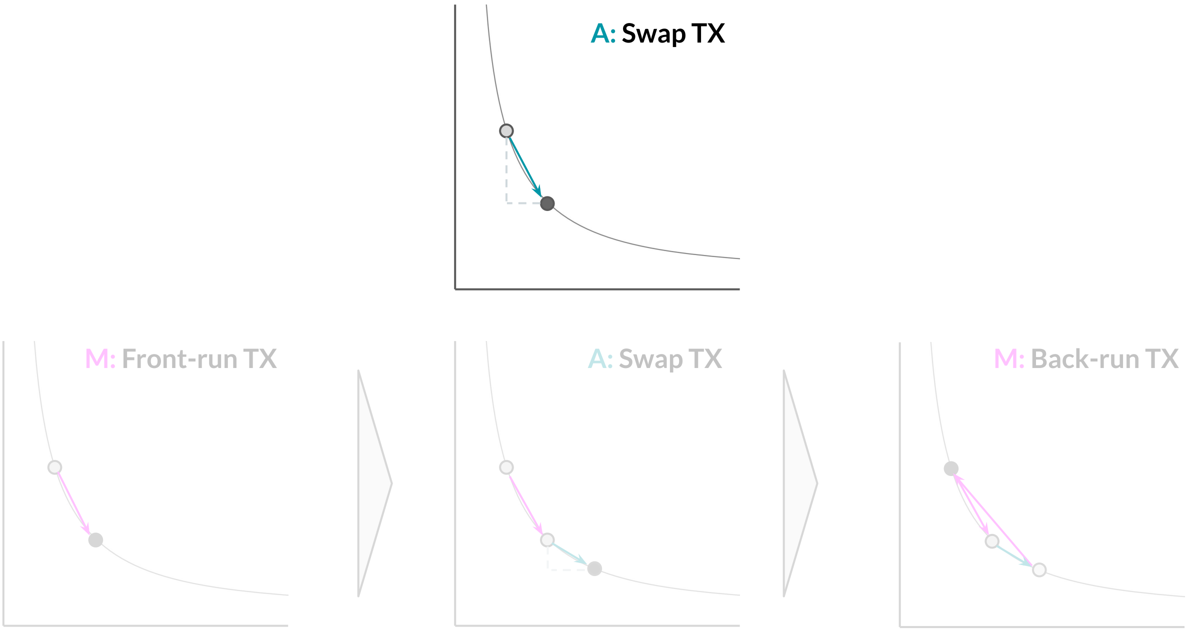
"Sandwich" attack transfers user value to miner

- Miner actions alter algorithmic exchange rate
- Rational miner is incentivized to extract value
- However, current descriptions are incomplete!

Miner-Extractable-Value (Sandwich Attack)

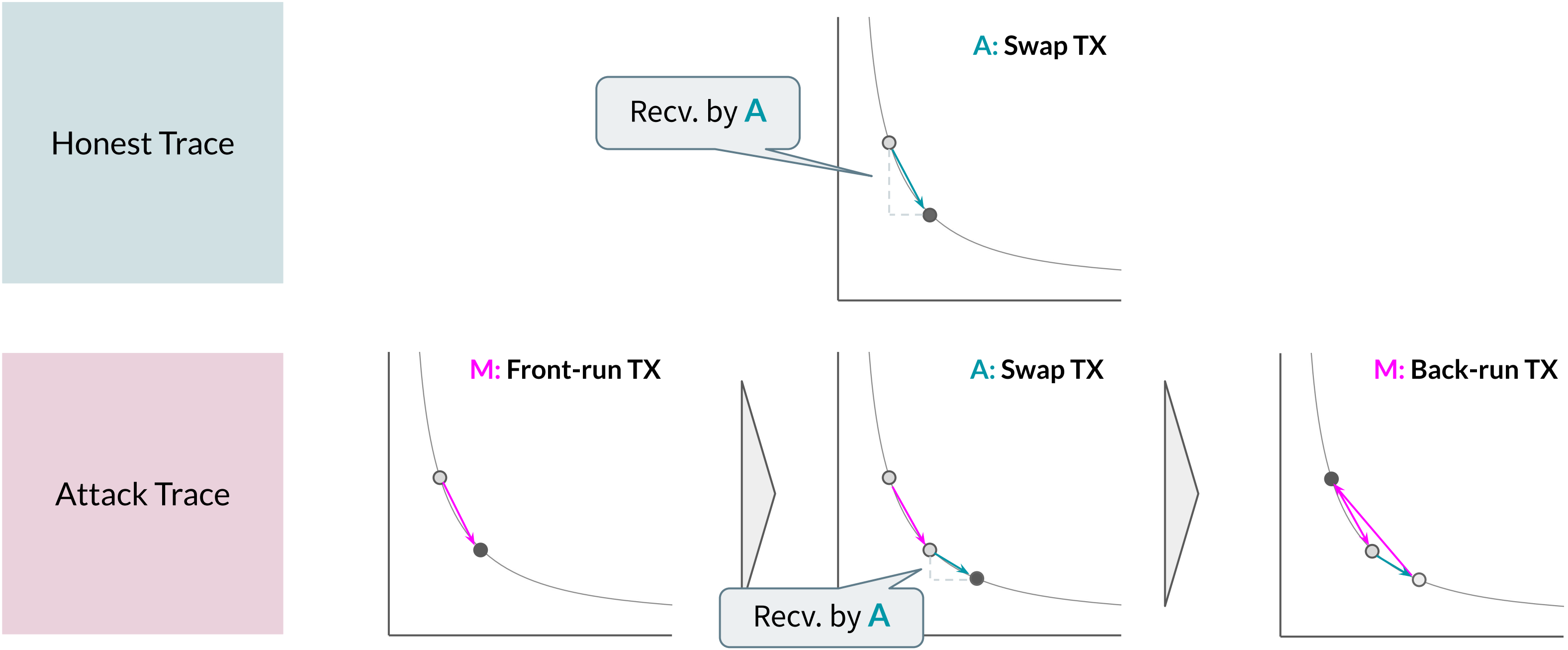
Honest Trace

Attack Trace



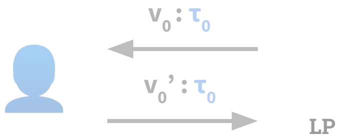
User obtains a lower exchange rate
(Miner earns profit)

Miner-Extractable-Value (Sandwich Attack)

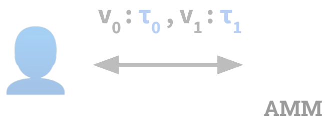


User obtains a lower exchange rate
(Miner earns profit)

Lending (LP)

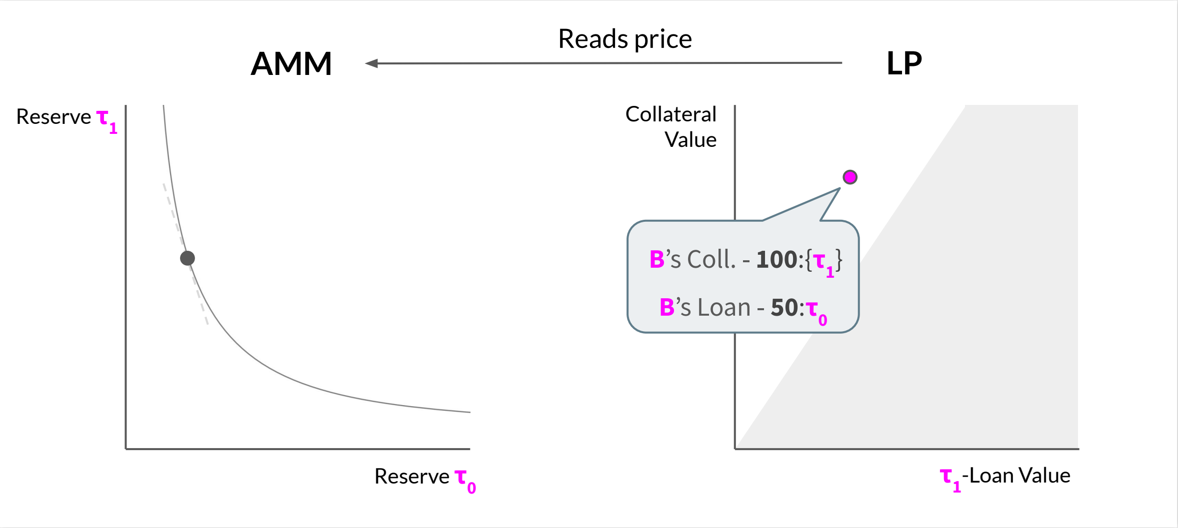


Swaps (AMM)

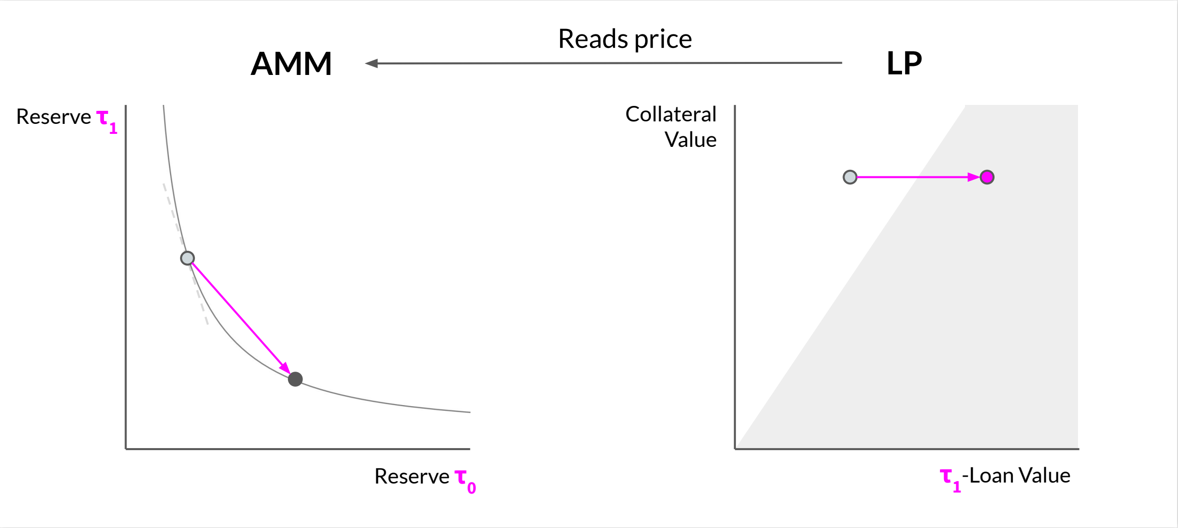


Composition?
(e.g. AMM as price oracle for LP)

AMM & LP: Insecure Composition



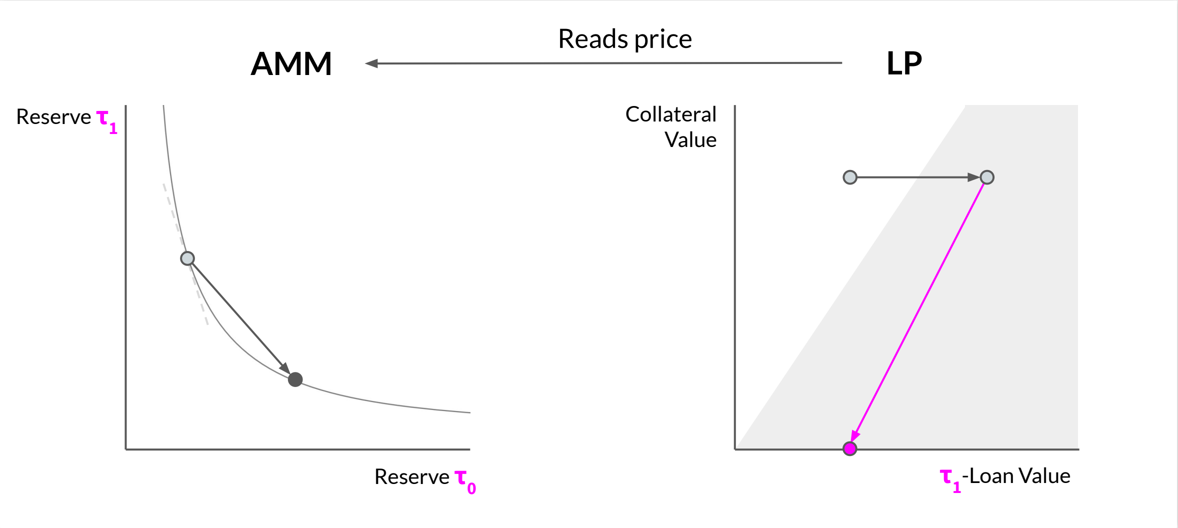
AMM & LP: Insecure Composition



Attack Trace

M: swapL

AMM & LP: Insecure Composition



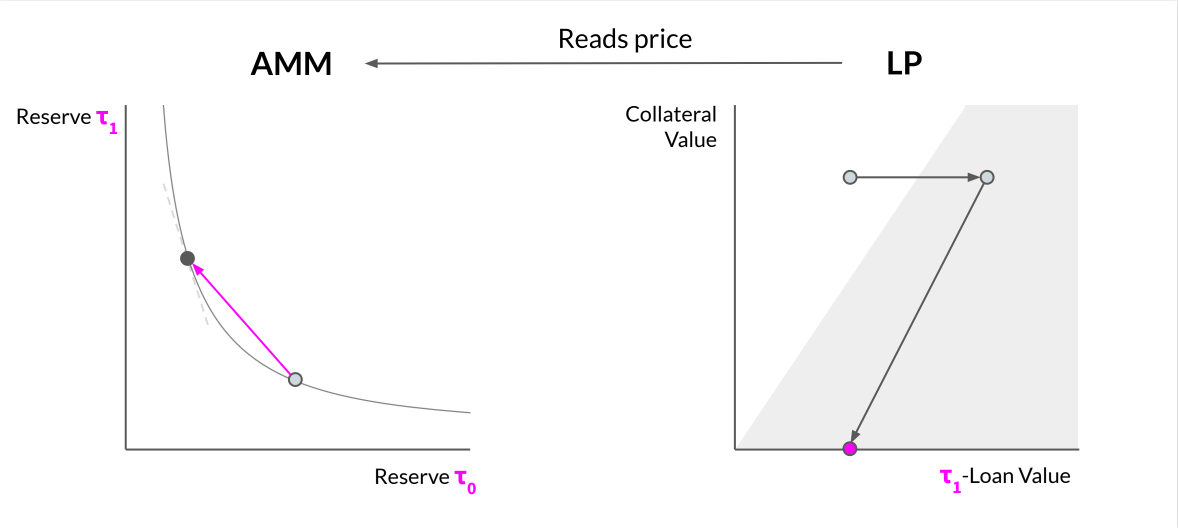
Attack Trace

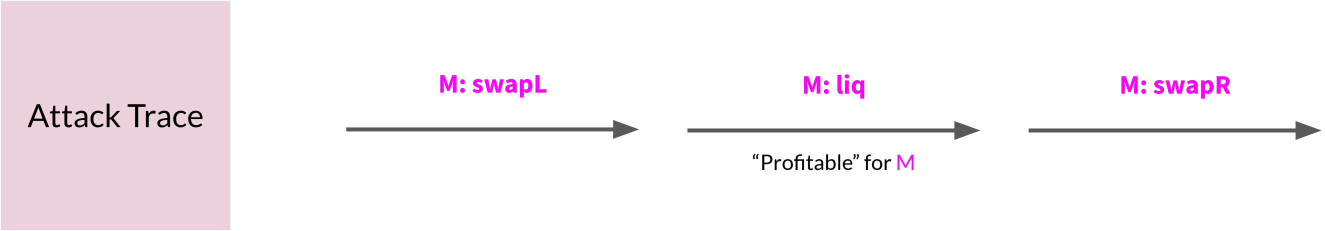
M: swapL

M: liq

“Profitable” for M

AMM & LP: Insecure Composition





DeFi: Open Challenges

1 Agent Strategies

Concurrency of DeFi actions

- MEV: Miner-extractable value
- Miner exploits TX ordering privileges

2 Cryptographic Composition

Privacy protocols

- DeFi with secure computation (MPC)

3 Domain Specific Languages

A formal DeFi Calculus?

- Abstract away implementation details
- Composed of common DeFi semantics
- Towards a formal theory of DeFi

Related work

1. **SoK: Lending Pools in Decentralized Finance [WTSC'21]**
   - M. Bartoletti, J. Hsin-yu Chiang, A. Lluch-Lafuente
   - https://arxiv.org/abs/2012.13230

2. **A theory of Automated Market Makers in DeFi [COORDINATION'21]**
   - M. Bartoletti, J. Hsin-yu Chiang, A. Lluch-Lafuente
   - https://arxiv.org/abs/2102.11350

3. **Maximizing Extractable Value from Automated Market Makers**
   - M. Bartoletti, J. Hsin-yu Chiang, A. Lluch-Lafuente
   - http://arxiv.org/abs/2106.01870