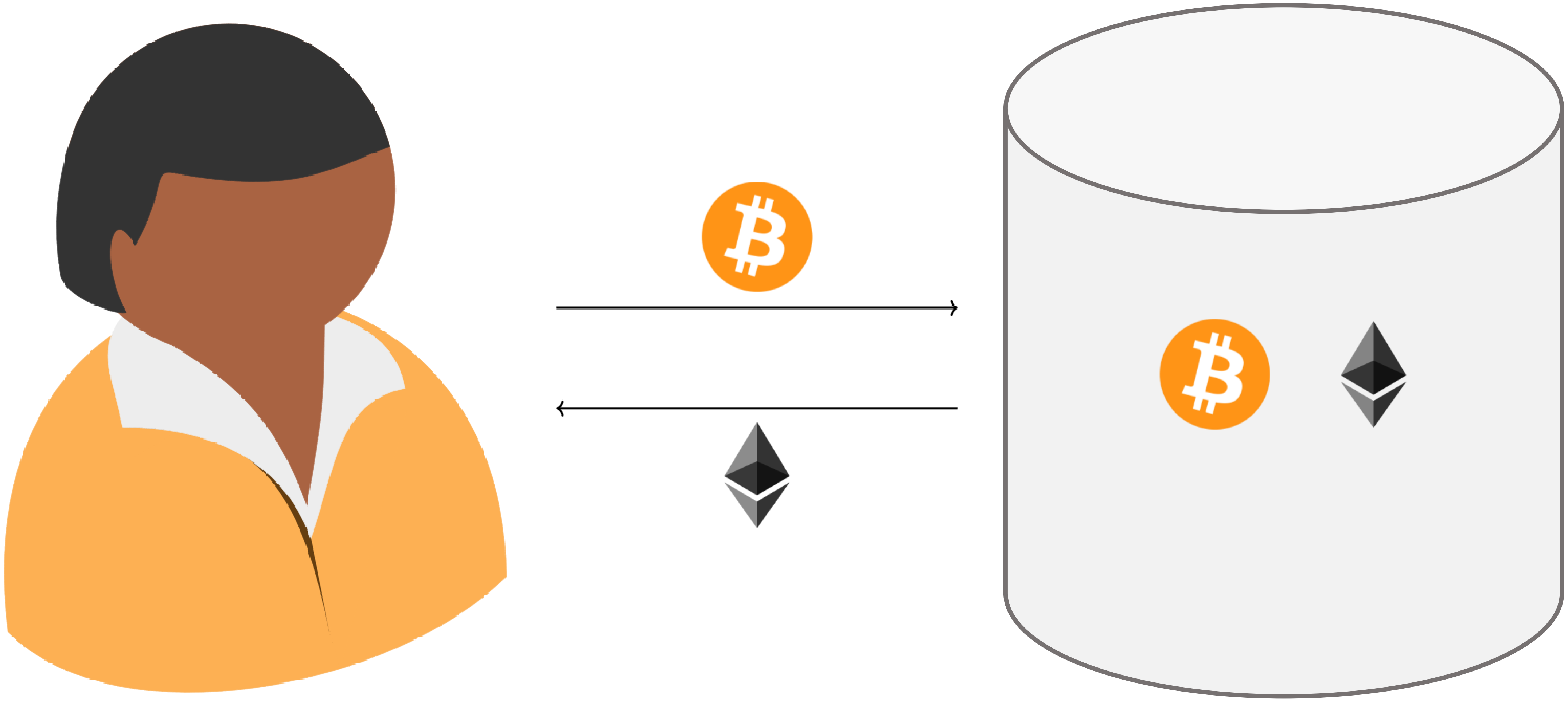
Eliminating Sandwich Attacks with the Help of Game Theory

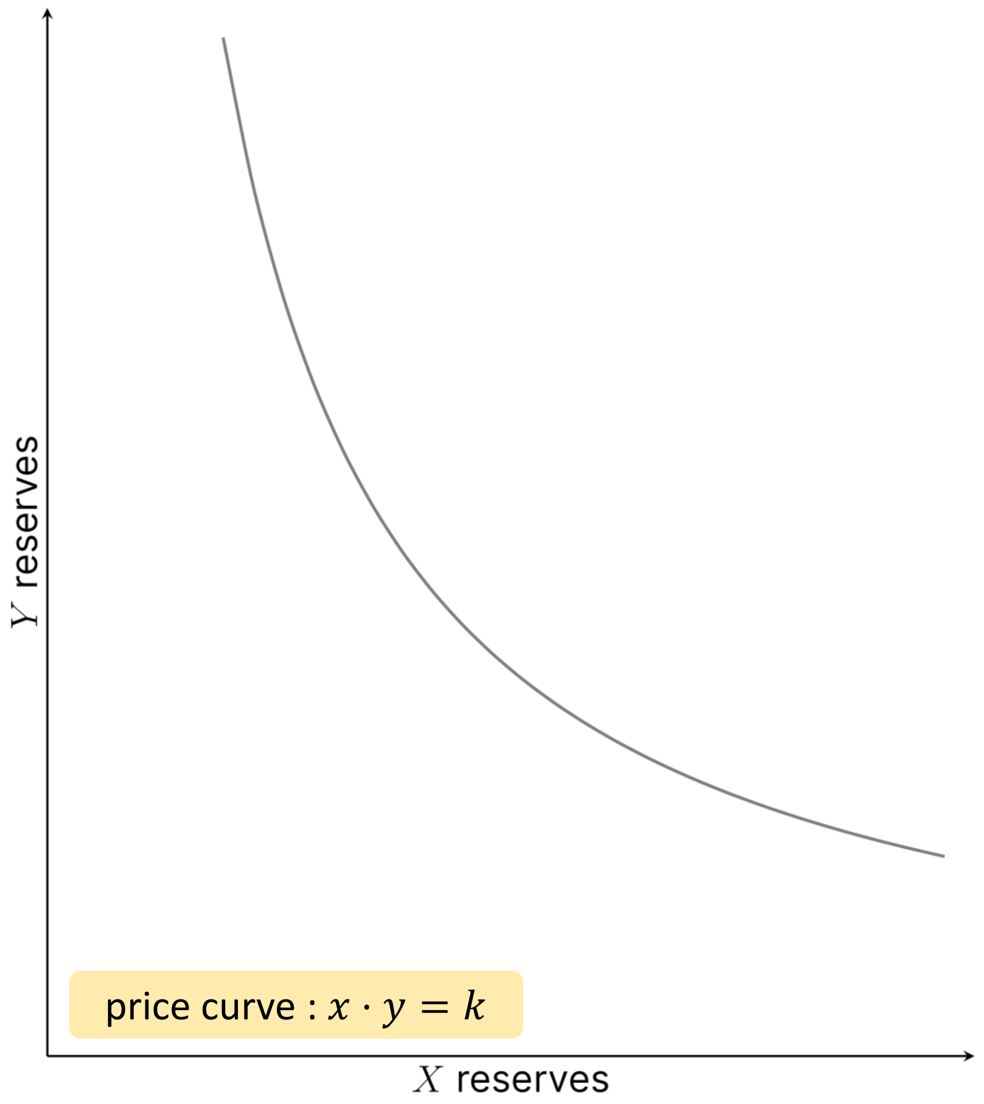
Lioba Heimbach, Roger Wattenhofer
ETH Zurich – Distributed Computing – www.disco.ethz.ch

Decentralized exchanges (DEXes)

Decentralized exchanges (DEXes)

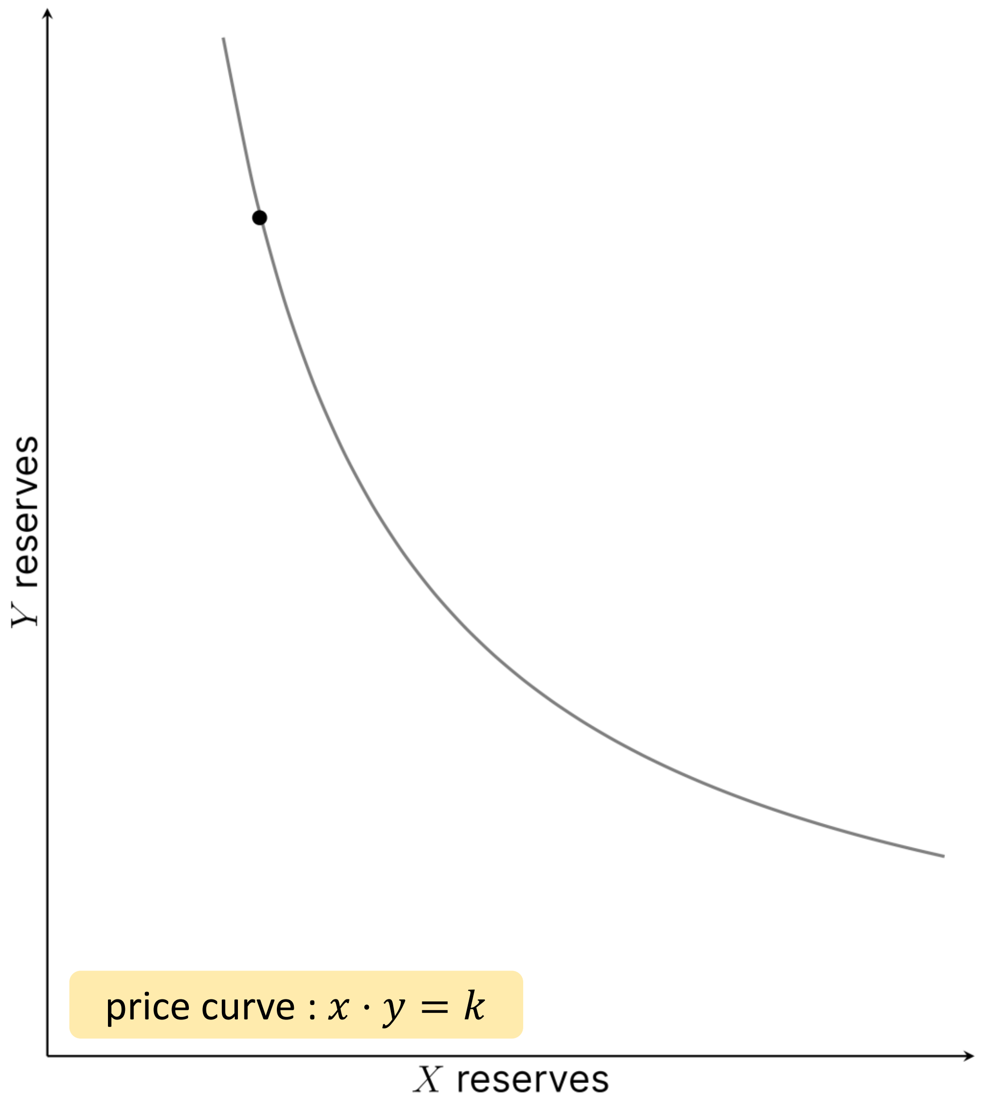


Constant product market makers (CPMMs)



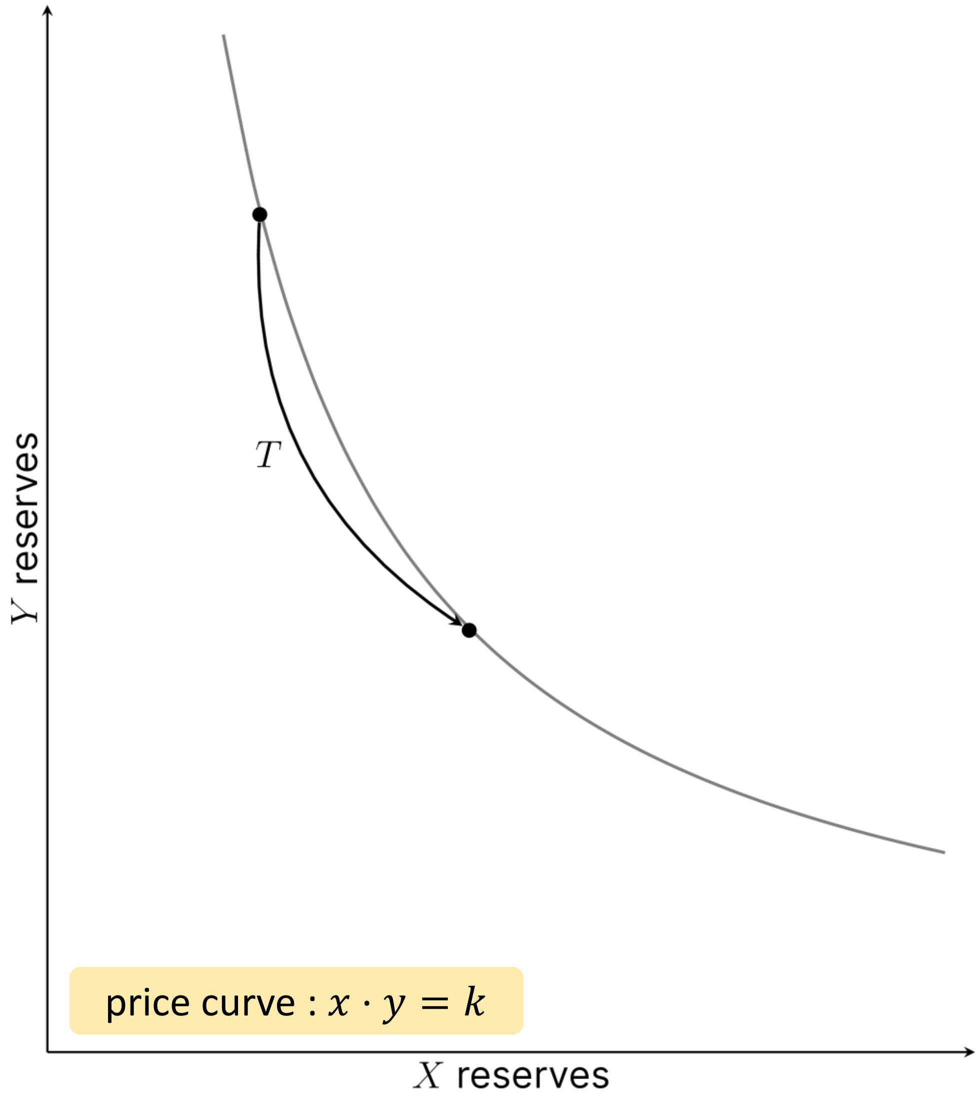
trading along price curve

Constant product market makers (CPMMs)



trading along price curve

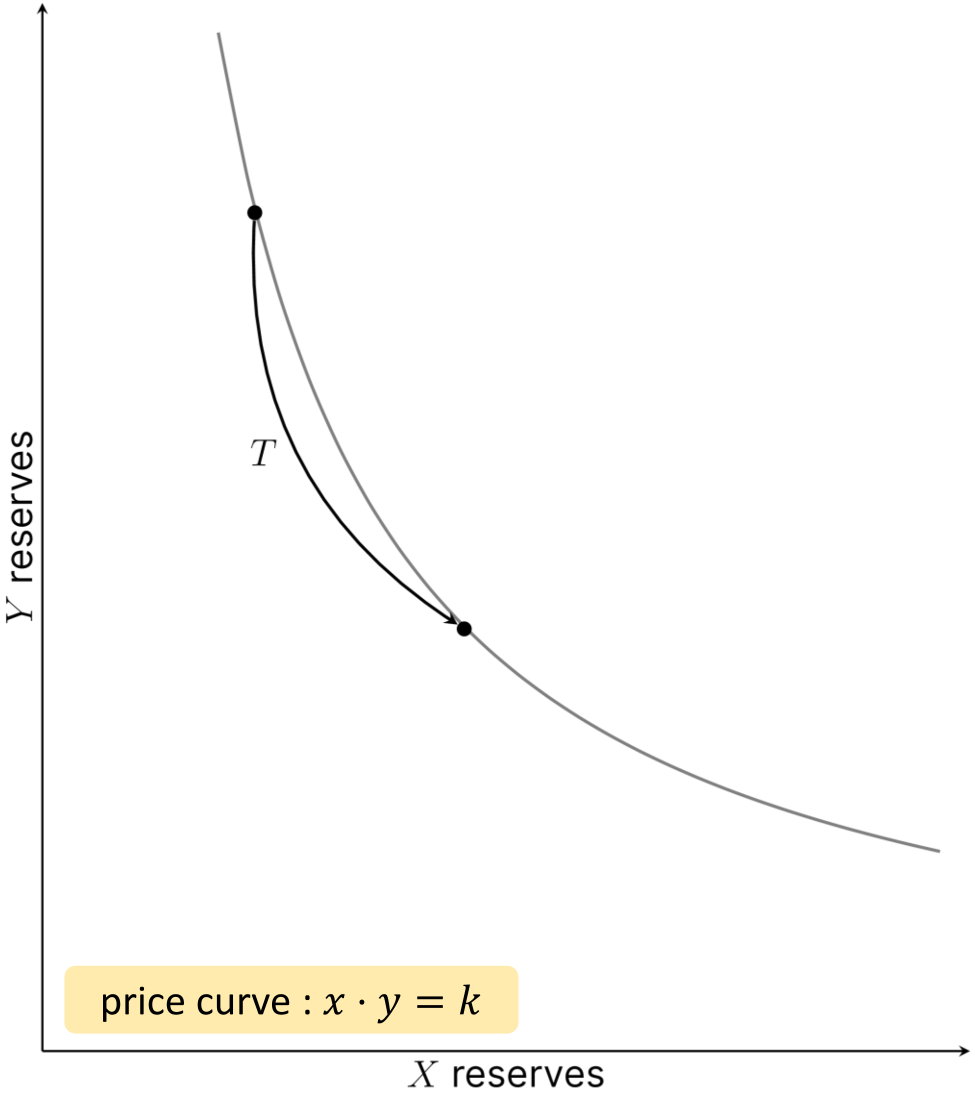
Constant product market makers (CPMMs)



trading along price curve

T: trade X → Y

Constant product market makers (CPMMs)

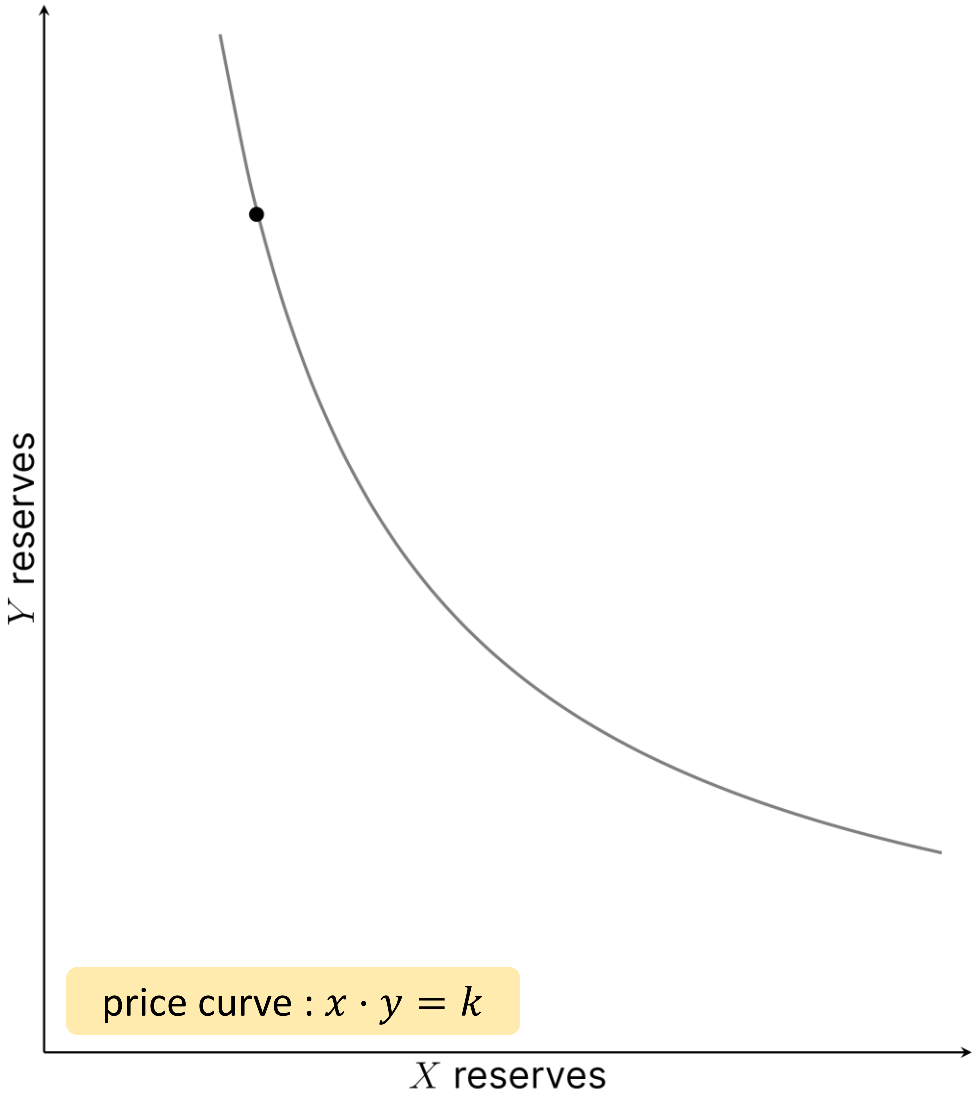


trading along price curve

T: trade X → Y

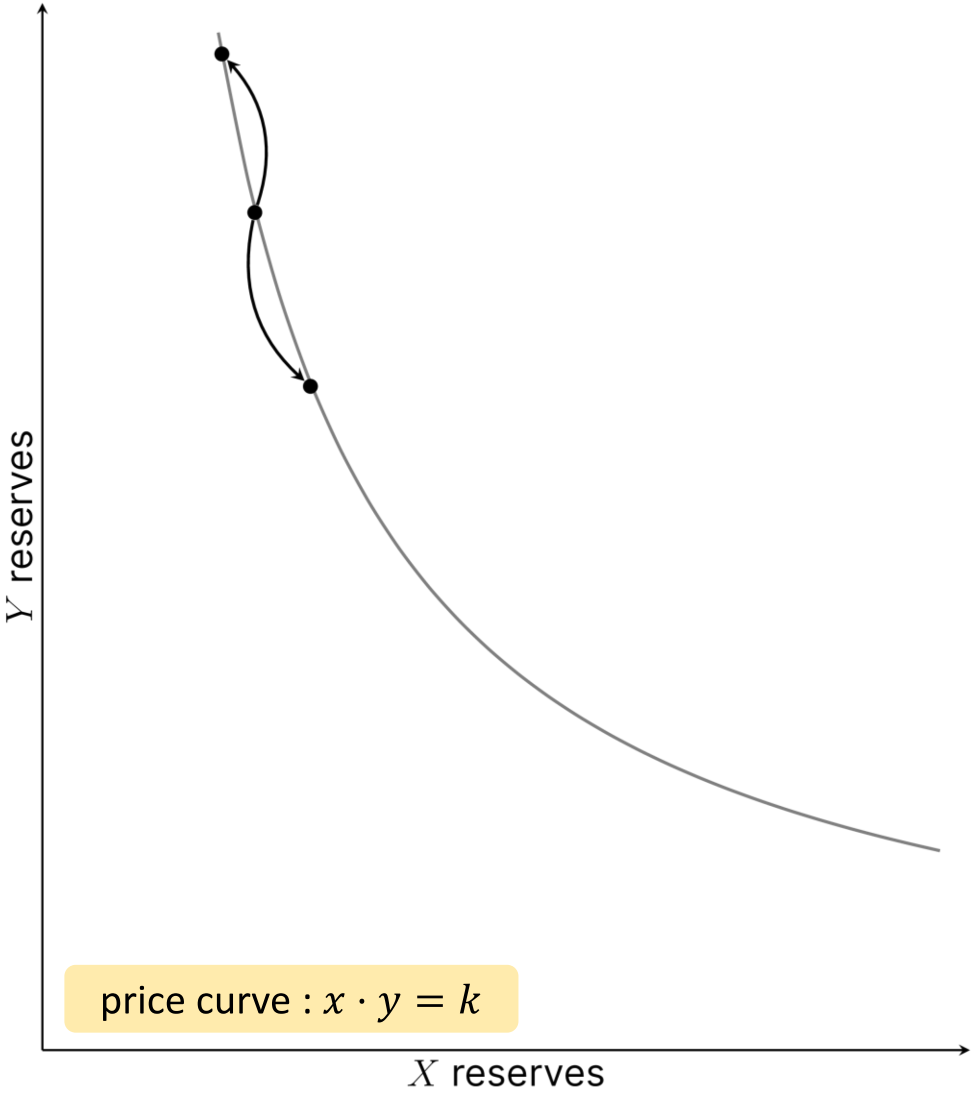
expected slippage
=
expected price decrease

Unexpected slippage



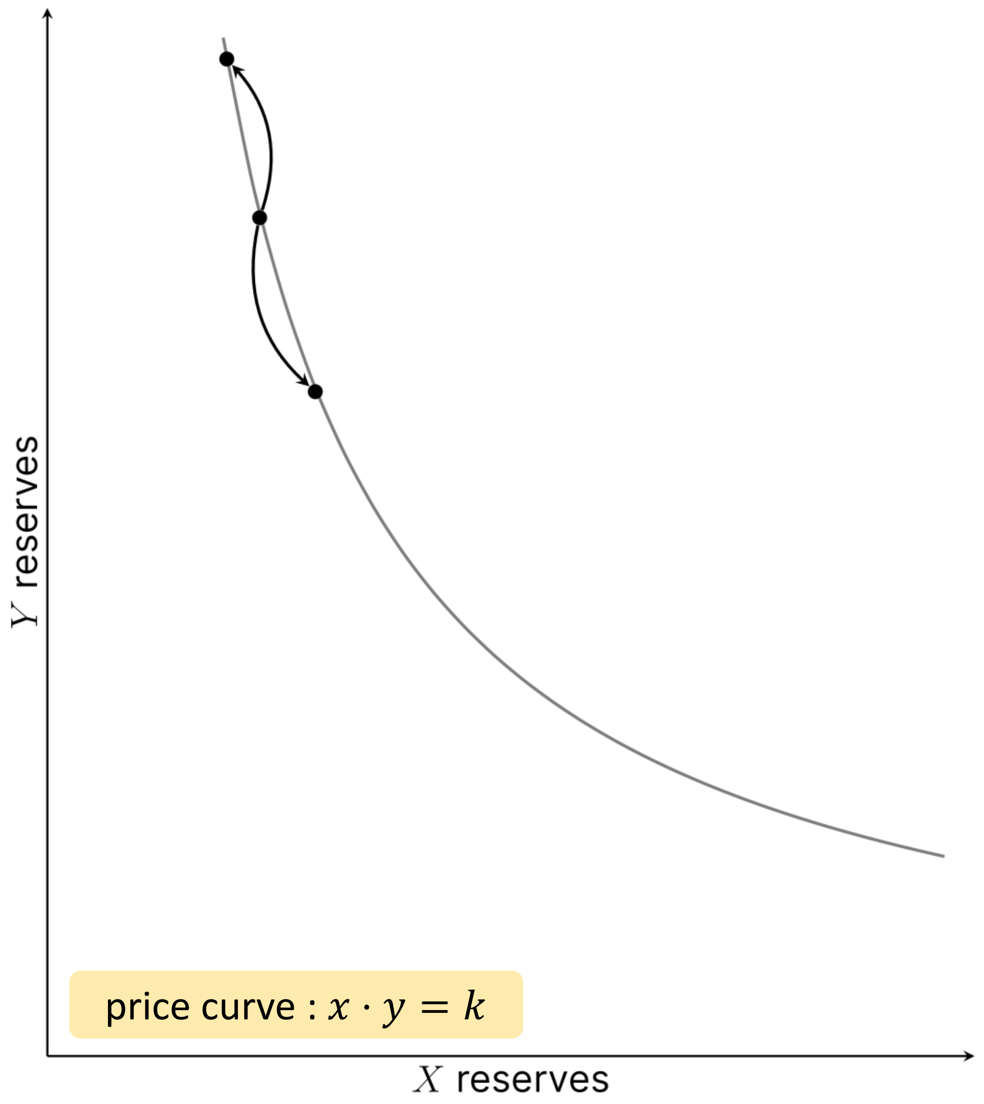
unexpected slippage
=
unexpected price increase/decrease

Unexpected slippage



unexpected slippage
=
unexpected price increase/decrease

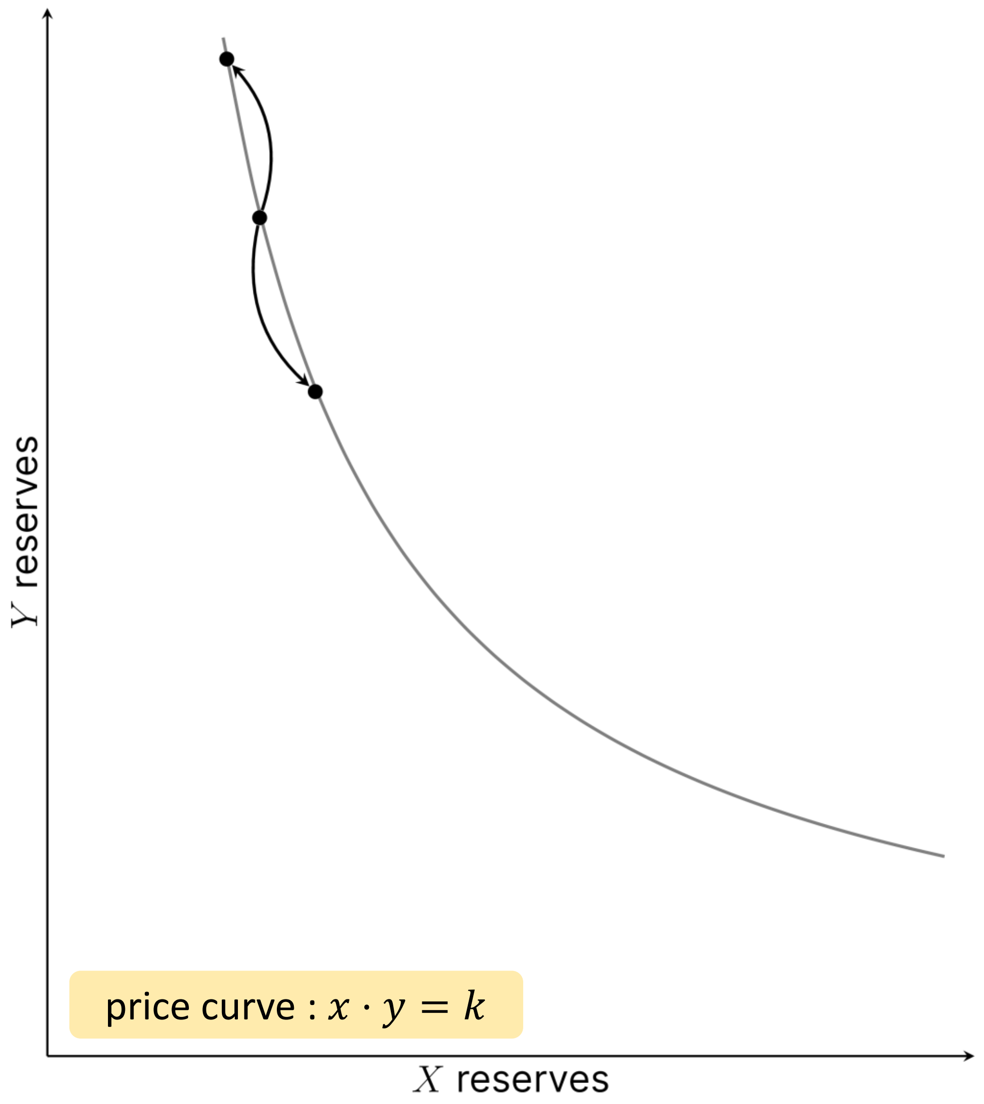
Unexpected slippage



unexpected slippage
=
unexpected price increase/decrease

slippage tolerance specifies
maximum price movement

Unexpected slippage

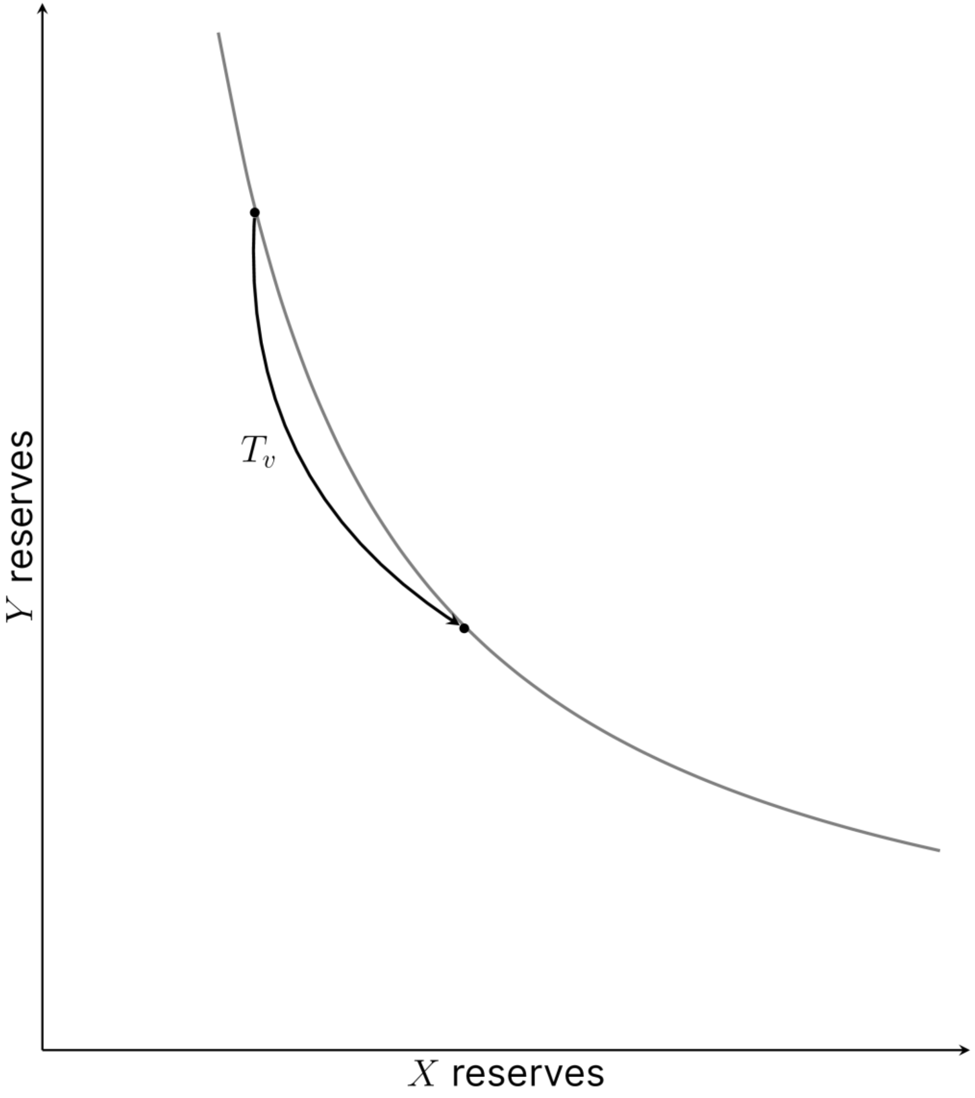


unexpected slippage
=
unexpected price increase/decrease

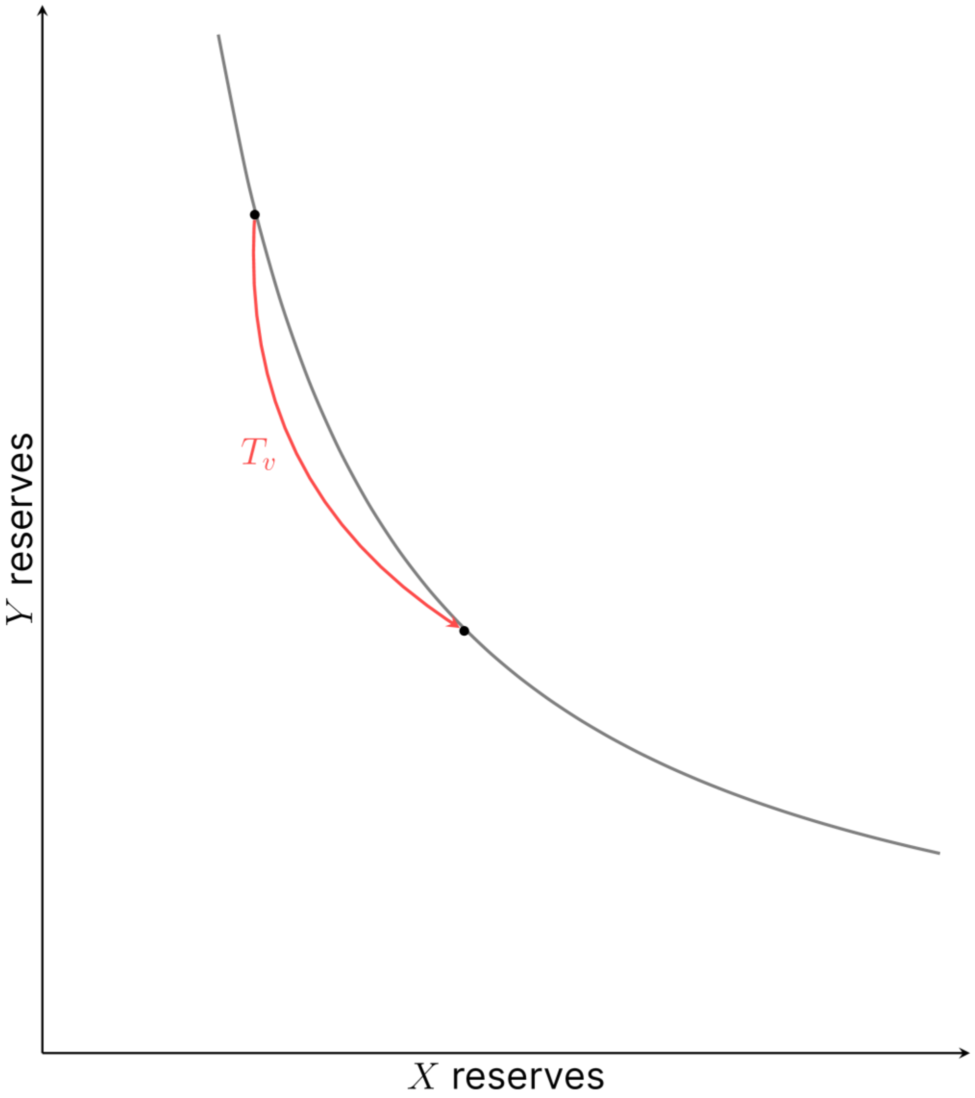
slippage tolerance specifies maximum price movement

trade fails if slippage tolerance exceeded

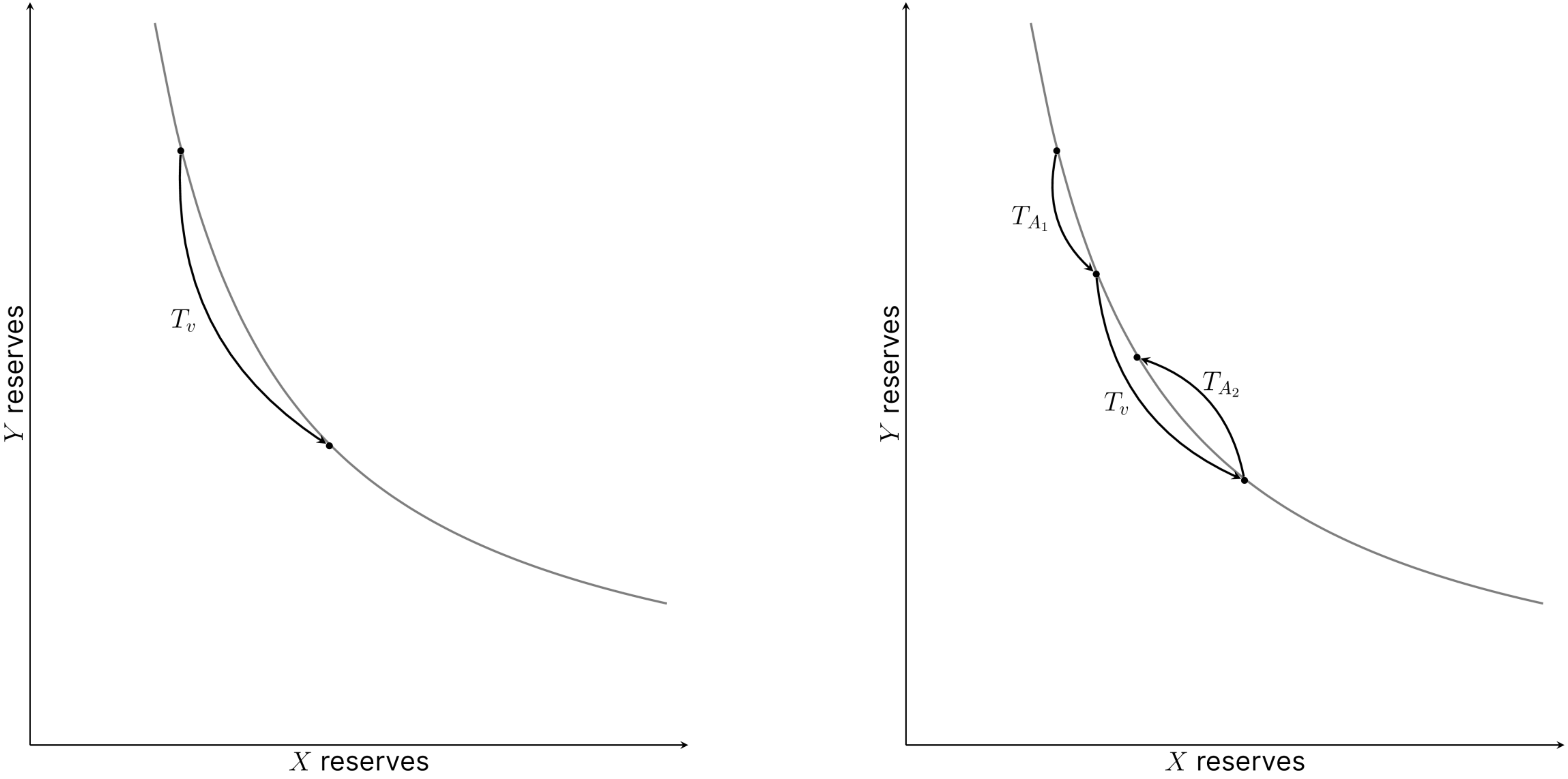
Sandwich attack mechanism



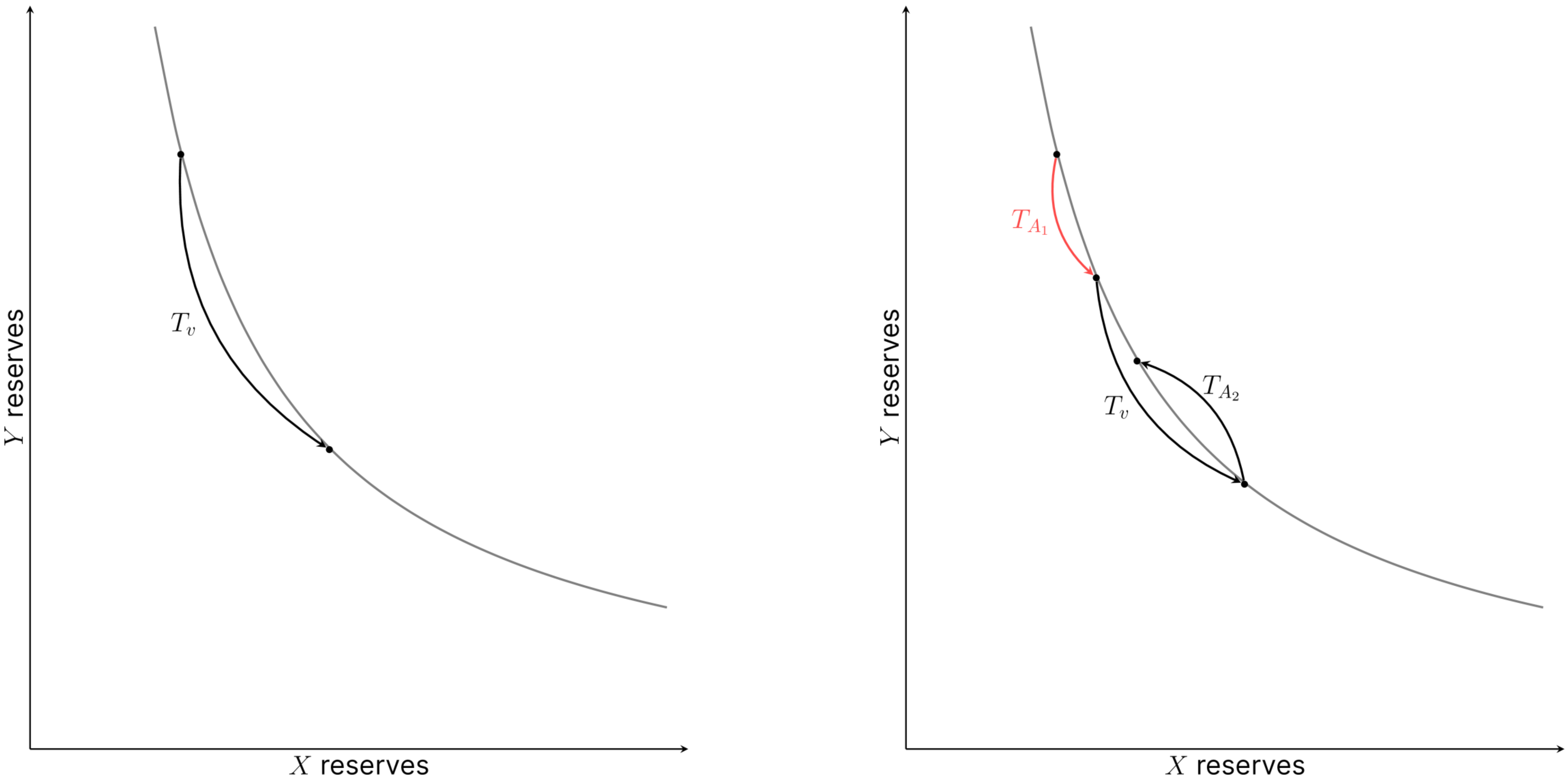
Sandwich attack mechanism



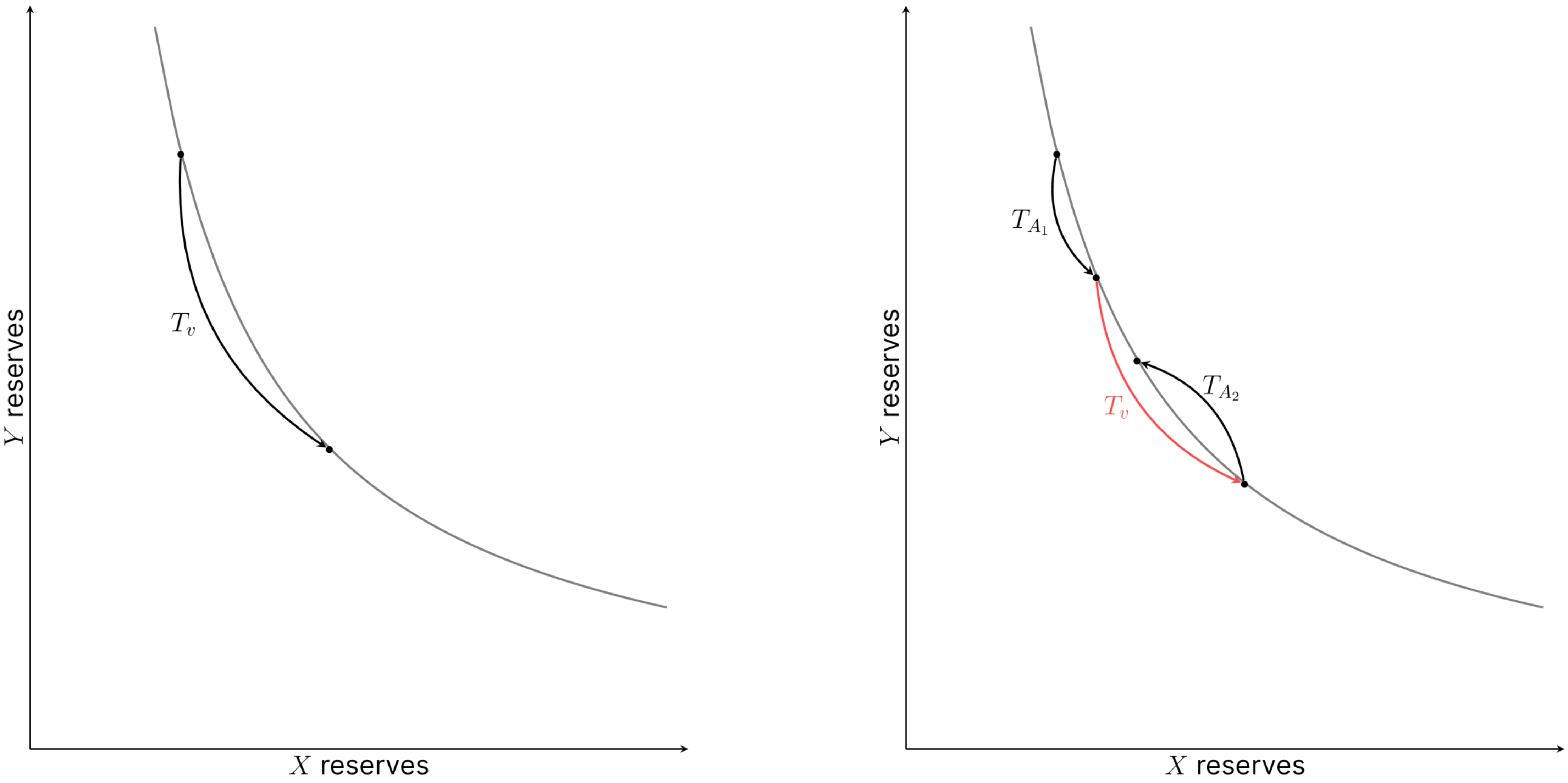
Sandwich attack mechanism



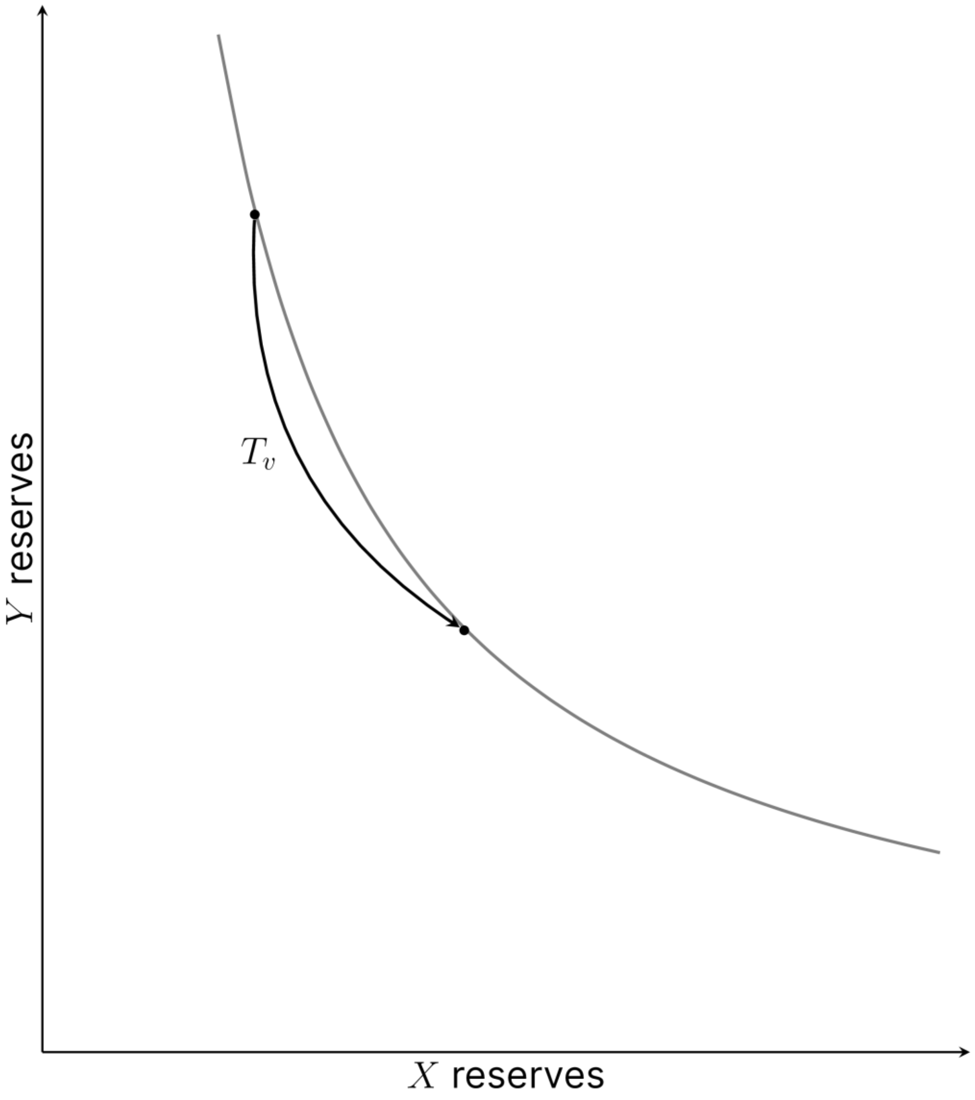
Sandwich attack mechanism

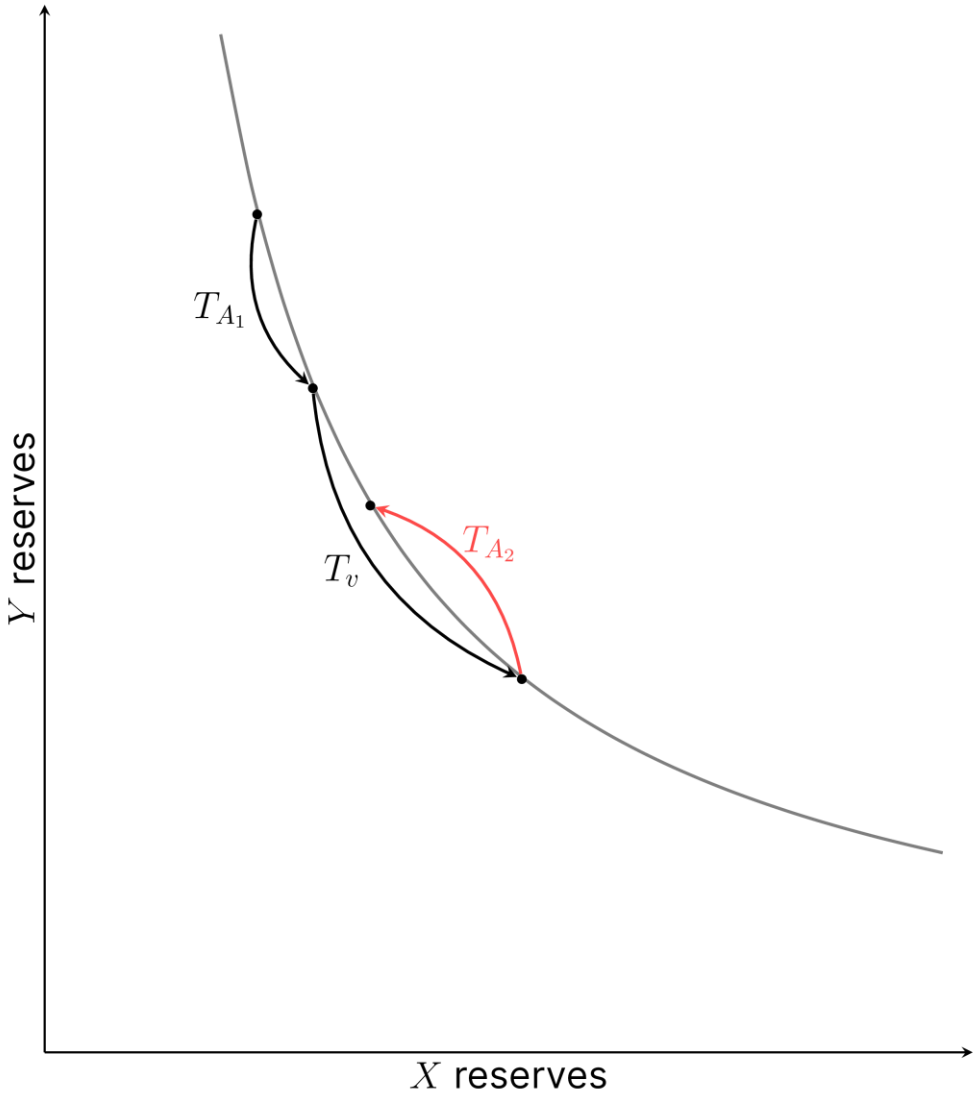


Sandwich attack mechanism

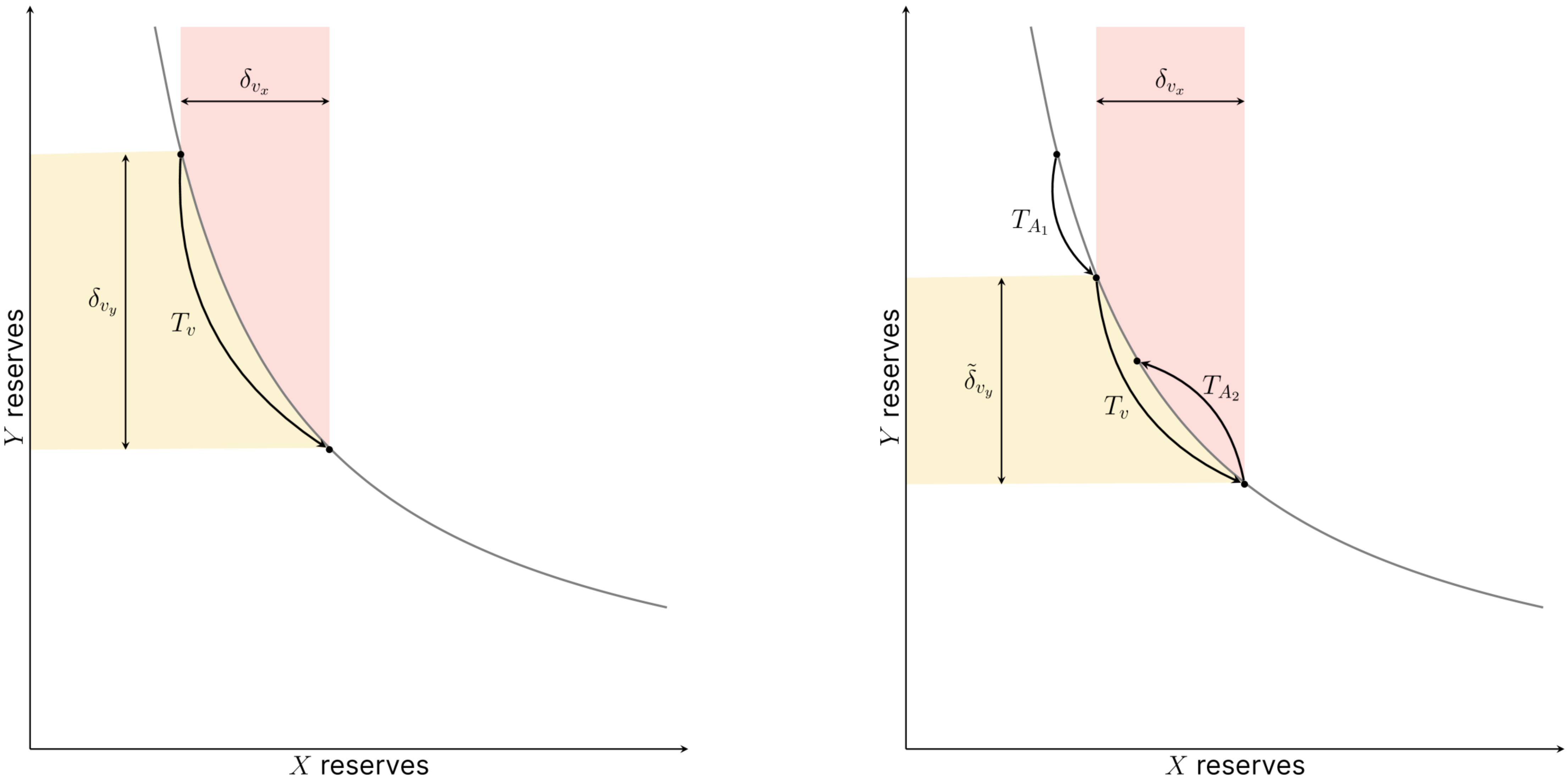


Sandwich attack mechanism

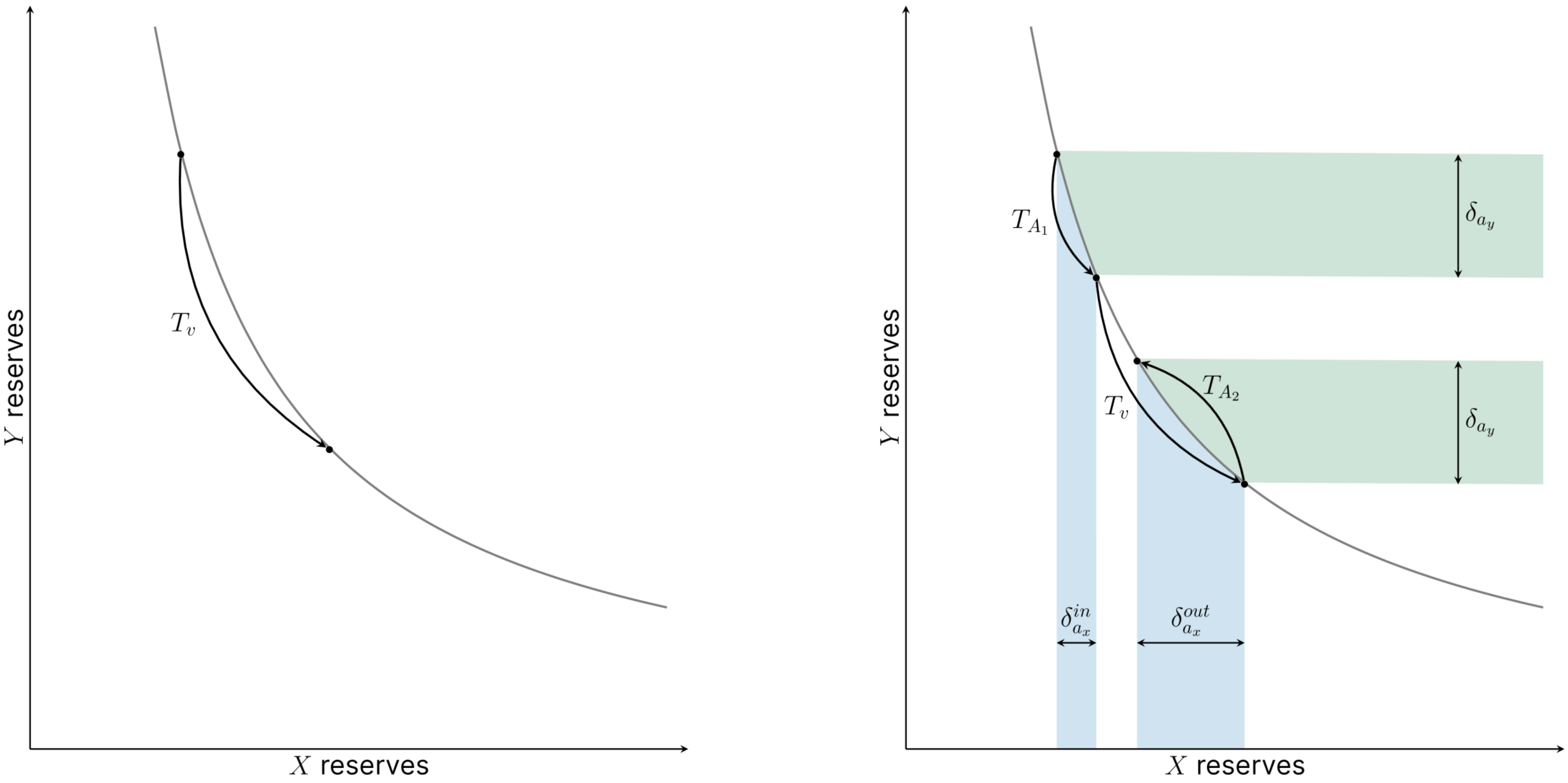




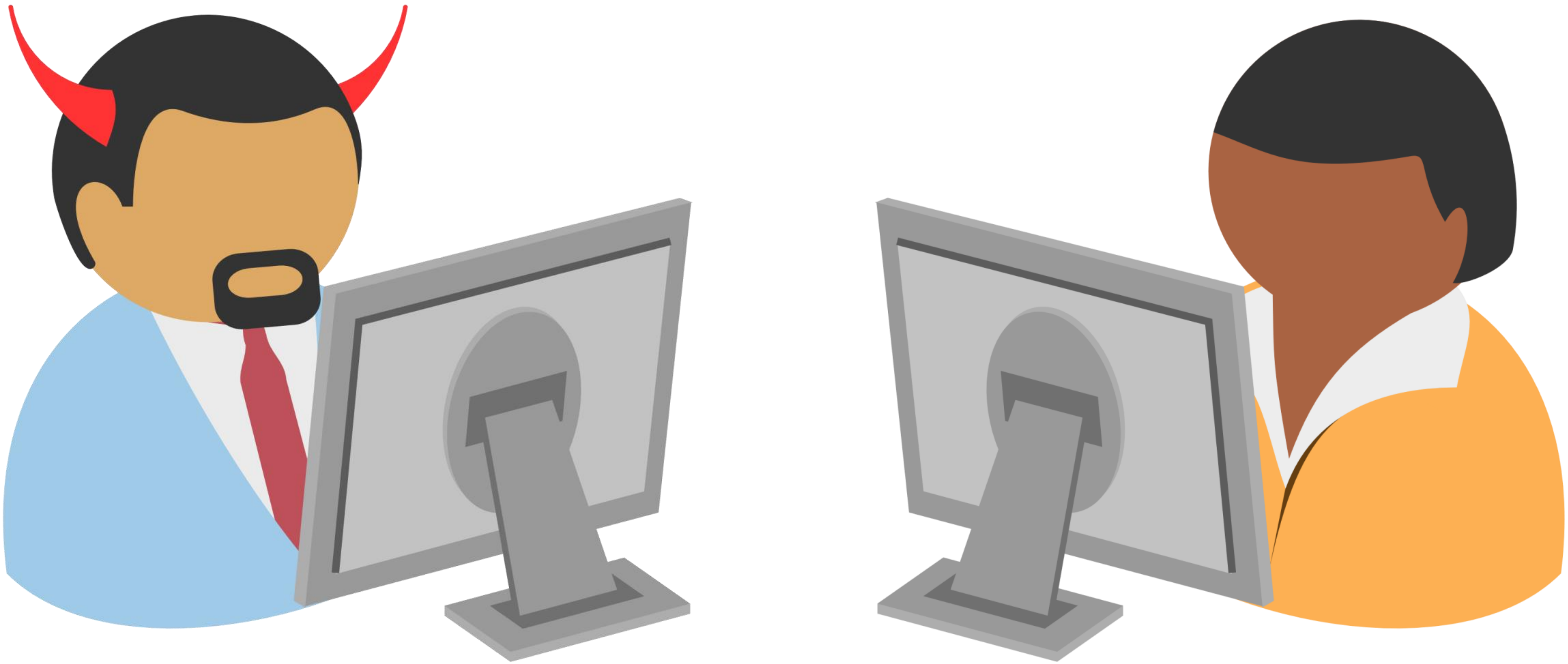
Sandwich attack mechanism



Sandwich attack mechanism



Sandwich attack game



Optimal sandwich attack

Optimal sandwich attack

maximize profit

Optimal sandwich attack

Optimal sandwich attack

victim transaction

Optimal sandwich attack

victim transaction

transaction size (δ_{v_x})

Optimal sandwich attack

victim transaction

transaction size (δ_{v_x})

slippage tolerance (s)

Optimal sandwich attack

victim transaction

transaction size (δ_{v_x})

slippage tolerance (s)

attacker fees

Optimal sandwich attack

victim transaction

transaction size (δ_{v_x})

slippage tolerance (s)

attacker fees

transaction fee (f)

Optimal sandwich attack

victim transaction

transaction size (δ_{v_x})

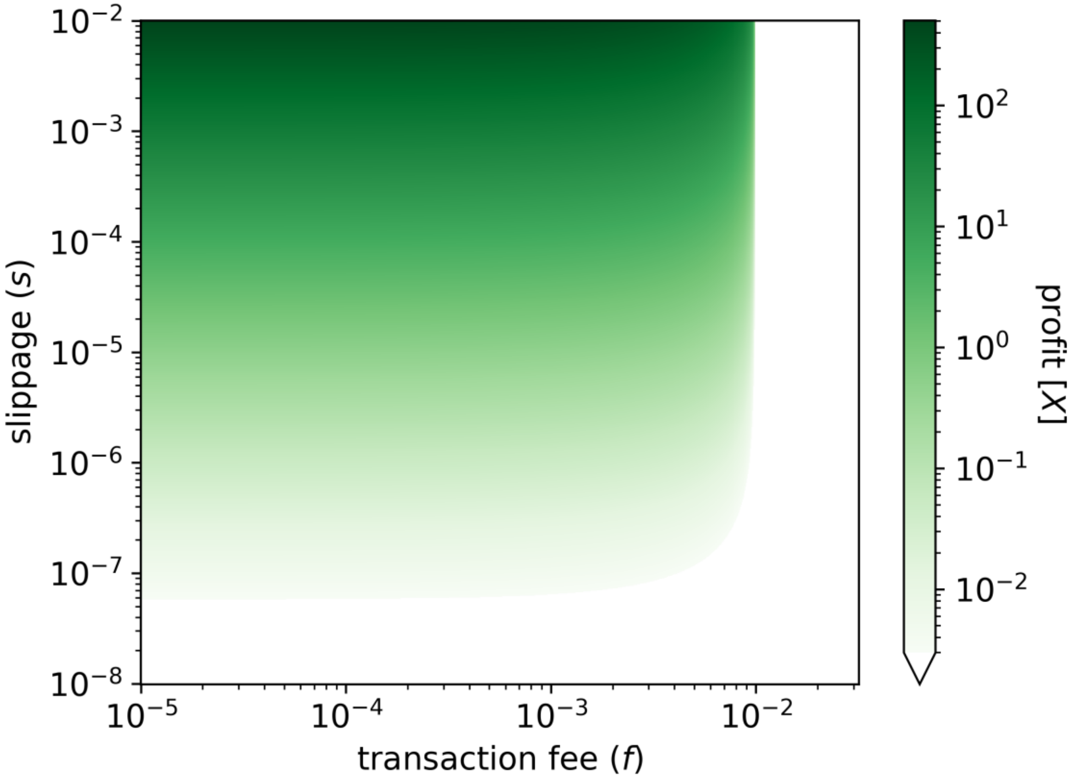
slippage tolerance (s)

attacker fees

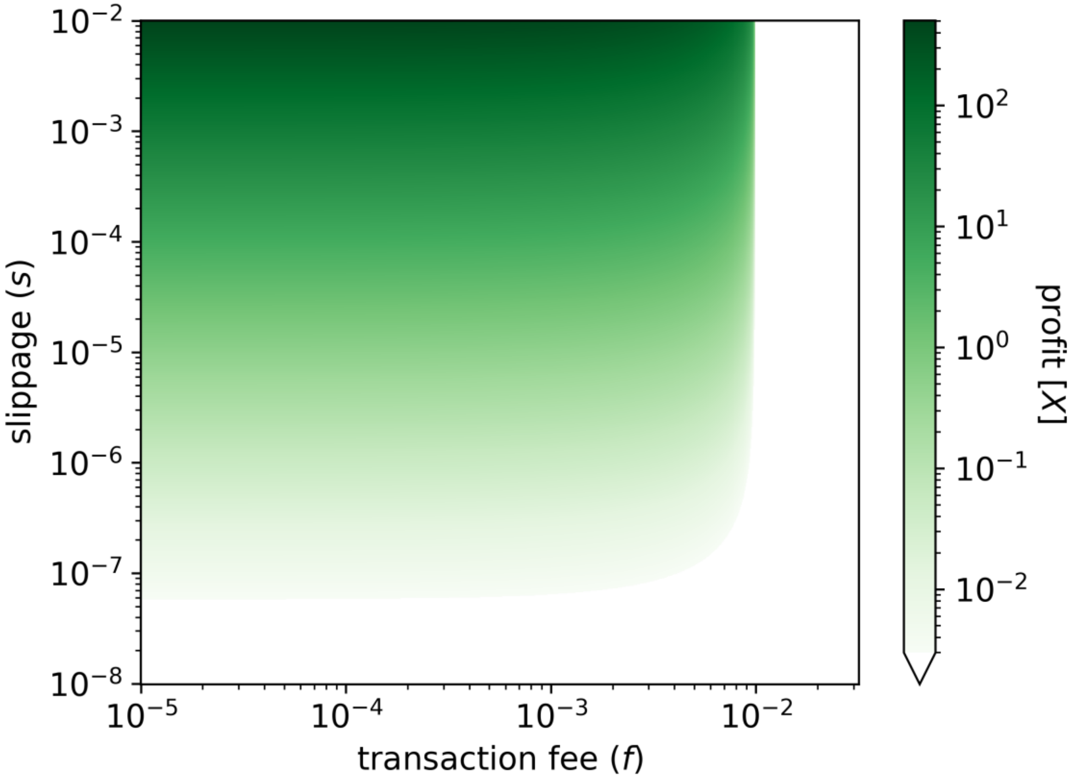
transaction fee (f)

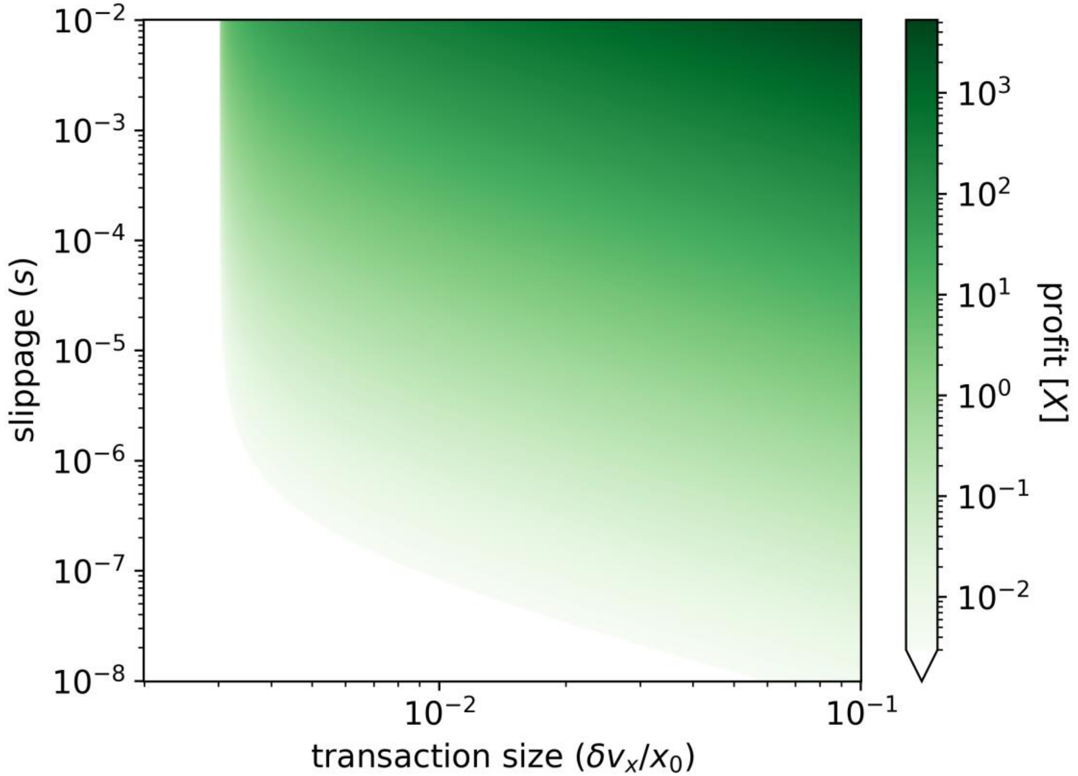
block fee (b)

Optimal sandwich attack

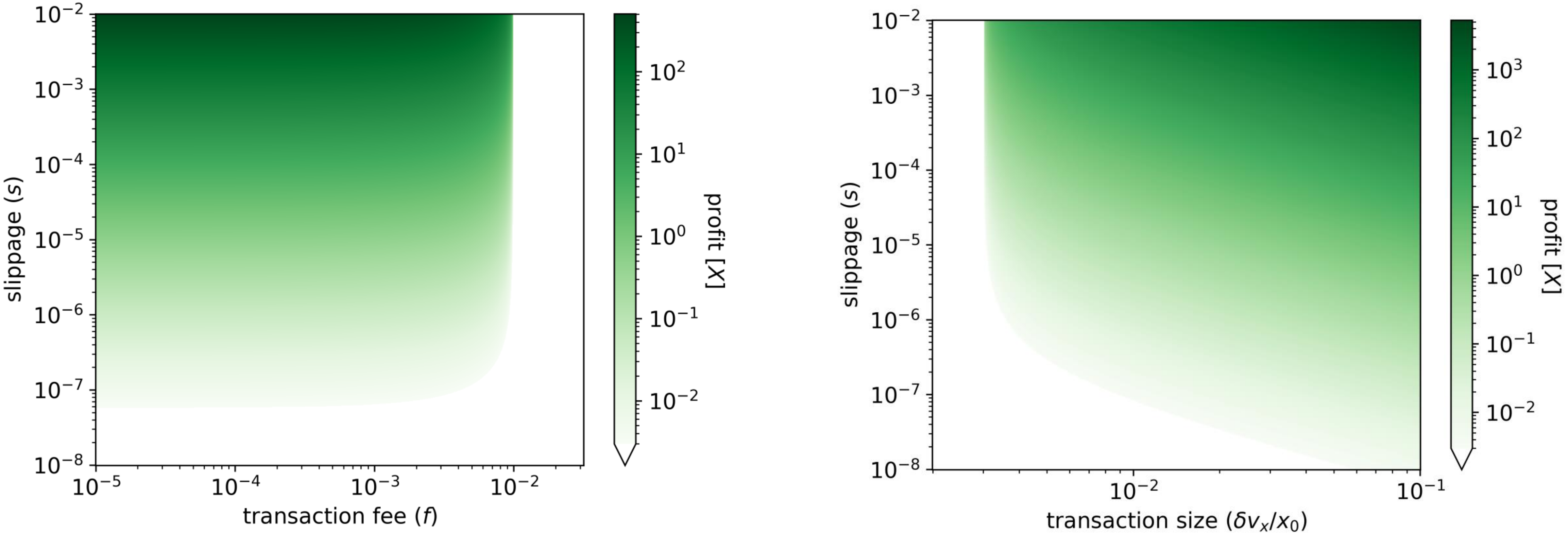


Optimal sandwich attack





Optimal sandwich attack



the attacker's profit cannot exceed the victim's loss

Setting slippage

Setting slippage

avoid sandwich attack

Setting slippage

avoid sandwich attack

avoid transaction failure

Setting slippage

Setting slippage

unattackable trade

Setting slippage

unattackable trade

$s < s_a$ to ensure transaction is unattackable

Setting slippage

unattackable trade

$s < s_a$ to ensure transaction is unattackable

expected transaction re-sending cost

Setting slippage

unattackable trade

$s < s_a$ to ensure transaction is unattackable

expected transaction re-sending cost

$s_r < s$ expected transaction re-sending
cost does not exceed sandwich attack cost

Setting slippage

setting slippage algorithm

Calculate s_a and s_r
if $s_r < s_a$:
    set $s = s_a - \varepsilon$, where $\varepsilon \to 0^+$
else:
    set $s = s_r$

Setting slippage

setting slippage algorithm

Calculate s_a and s_r
if $s_r < s_a$:
    set $s = s_a - \varepsilon$, where $\varepsilon \to 0^+$
else:
    set $s = s_r$

Setting slippage

setting slippage algorithm

Calculate s_a and s_r
if $s_r < s_a$:
    set $s = s_a - \varepsilon$, where $\varepsilon \to 0^+$
else:
    set $s = s_r$

Setting slippage

setting slippage algorithm

Calculate s_a and s_r
if $s_r < s_a$:
    set $s = s_a - \varepsilon$, where $\varepsilon \to 0^+$
else:
    set $s = s_r$

Cost comparison

USDC ↔ ETH

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	0,000	$2{,}267 \cdot 10^{-4}$	∞
100	0,000	$3{,}545 \cdot 10^{-5}$	∞
1000	$3{,}554 \cdot 10^{-6}$	$1{,}632 \cdot 10^{-5}$	4.5924
10000	$1{,}434 \cdot 10^{-4}$	$5{,}103 \cdot 10^{-3}$	35.5718
100000	$3{,}178 \cdot 10^{-4}$	$5{,}013 \cdot 10^{-3}$	15.7735

BTC ↔ ETH

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	0,000	$7{,}440 \cdot 10^{-5}$	∞
100	$2{,}490 \cdot 10^{-6}$	$1{,}515 \cdot 10^{-5}$	6.0858
1000	$5{,}829 \cdot 10^{-6}$	$9{,}229 \cdot 10^{-6}$	1.5832
10000	$4{,}132 \cdot 10^{-5}$	$5{,}105 \cdot 10^{-3}$	123.5364
100000	$6{,}575 \cdot 10^{-5}$	$5{,}015 \cdot 10^{-3}$	76.2684

USDC ↔ USDT

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	0,000	$8{,}310 \cdot 10^{-5}$	∞
100	0,000	$1{,}335 \cdot 10^{-5}$	∞
1000	$2{,}086 \cdot 10^{-6}$	$6{,}381 \cdot 10^{-6}$	3.0588
10000	$2{,}612 \cdot 10^{-5}$	$5{,}101 \cdot 10^{-3}$	195.2647
100000	$4{,}150 \cdot 10^{-5}$	$5{,}011 \cdot 10^{-3}$	120.7390

LINK ↔ ETH

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	0,000	$5{,}707 \cdot 10^{-5}$	∞
100	$4{,}470 \cdot 10^{-6}$	$2{,}032 \cdot 10^{-5}$	4.5450
1000	$1{,}659 \cdot 10^{-5}$	$1{,}664 \cdot 10^{-5}$	1.0031
10000	$1{,}637 \cdot 10^{-5}$	$5{,}114 \cdot 10^{-3}$	312.3494
100000	$1{,}834 \cdot 10^{-5}$	$5{,}024 \cdot 10^{-3}$	273.9272

Cost comparison

USDC ↔ ETH

size [\$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$2{,}267 \cdot 10^{-4}$	∞
100	$0{,}000$	$3{,}545 \cdot 10^{-5}$	∞
1000	$3{,}554 \cdot 10^{-6}$	$1{,}632 \cdot 10^{-5}$	4.5924
10000	$1{,}434 \cdot 10^{-4}$	$5{,}103 \cdot 10^{-3}$	35.5718
100000	$3{,}178 \cdot 10^{-4}$	$5{,}013 \cdot 10^{-3}$	15.7735

BTC ↔ ETH

size [\$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$7{,}440 \cdot 10^{-5}$	∞
100	$2{,}490 \cdot 10^{-6}$	$1{,}515 \cdot 10^{-5}$	6.0858
1000	$5{,}829 \cdot 10^{-6}$	$9{,}229 \cdot 10^{-6}$	1.5832
10000	$4{,}132 \cdot 10^{-5}$	$5{,}105 \cdot 10^{-3}$	123.5364
100000	$6{,}575 \cdot 10^{-5}$	$5{,}015 \cdot 10^{-3}$	76.2684

USDC ↔ USDT

size [\$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$8{,}310 \cdot 10^{-5}$	∞
100	$0{,}000$	$1{,}335 \cdot 10^{-5}$	∞
1000	$2{,}086 \cdot 10^{-6}$	$6{,}381 \cdot 10^{-6}$	3.0588
10000	$2{,}612 \cdot 10^{-5}$	$5{,}101 \cdot 10^{-3}$	195.2647
100000	$4{,}150 \cdot 10^{-5}$	$5{,}011 \cdot 10^{-3}$	120.7390

LINK ↔ ETH

size [\$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$5{,}707 \cdot 10^{-5}$	∞
100	$4{,}470 \cdot 10^{-6}$	$2{,}032 \cdot 10^{-5}$	4.5450
1000	$1{,}659 \cdot 10^{-5}$	$1{,}664 \cdot 10^{-5}$	1.0031
10000	$1{,}637 \cdot 10^{-5}$	$5{,}114 \cdot 10^{-3}$	312.3494
100000	$1{,}834 \cdot 10^{-5}$	$5{,}024 \cdot 10^{-3}$	273.9272

Cost comparison

USDC ↔ ETH

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$2{,}267 \cdot 10^{-4}$	∞
100	$0{,}000$	$3{,}545 \cdot 10^{-5}$	∞
1000	$3{,}554 \cdot 10^{-6}$	$1{,}632 \cdot 10^{-5}$	4.5924
10000	$1{,}434 \cdot 10^{-4}$	$5{,}103 \cdot 10^{-3}$	35.5718
100000	$3{,}178 \cdot 10^{-4}$	$5{,}013 \cdot 10^{-3}$	15.7735

BTC ↔ ETH

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$7{,}440 \cdot 10^{-5}$	∞
100	$2{,}490 \cdot 10^{-6}$	$1{,}515 \cdot 10^{-5}$	6.0858
1000	$5{,}829 \cdot 10^{-6}$	$9{,}229 \cdot 10^{-6}$	1.5832
10000	$4{,}132 \cdot 10^{-5}$	$5{,}105 \cdot 10^{-3}$	123.5364
100000	$6{,}575 \cdot 10^{-5}$	$5{,}015 \cdot 10^{-3}$	76.2684

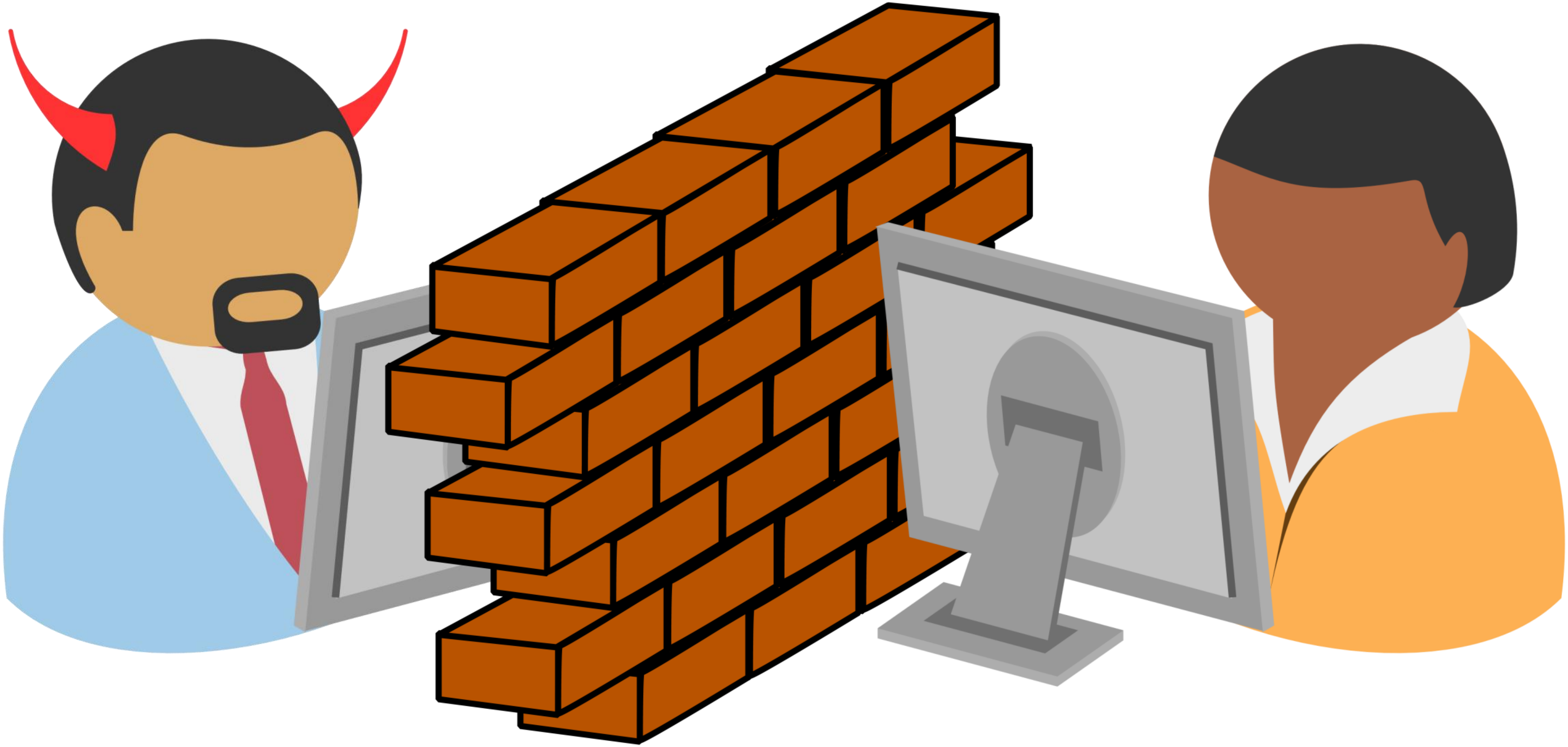
USDC ↔ USDT

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$8{,}310 \cdot 10^{-5}$	∞
100	$0{,}000$	$1{,}335 \cdot 10^{-5}$	∞
1000	$2{,}086 \cdot 10^{-6}$	$6{,}381 \cdot 10^{-6}$	3.0588
10000	$2{,}612 \cdot 10^{-5}$	$5{,}101 \cdot 10^{-3}$	195.2647
100000	$4{,}150 \cdot 10^{-5}$	$5{,}011 \cdot 10^{-3}$	120.7390

LINK ↔ ETH

size [$]	fractional cost ours	fractional cost UNI	ratio cost UNI/ours
10	$0{,}000$	$5{,}707 \cdot 10^{-5}$	∞
100	$4{,}470 \cdot 10^{-6}$	$2{,}032 \cdot 10^{-5}$	4.5450
1000	$1{,}659 \cdot 10^{-5}$	$1{,}664 \cdot 10^{-5}$	1.0031
10000	$1{,}637 \cdot 10^{-5}$	$5{,}114 \cdot 10^{-3}$	312.3494
100000	$1{,}834 \cdot 10^{-5}$	$5{,}024 \cdot 10^{-3}$	273.9272

Conclusion



Thank You!

Questions & Comments?

Lioba Heimbach, Roger Wattenhofer

ETH Zurich – Distributed Computing – www.disco.ethz.ch

Setting slippage

unattackable transaction

Setting slippage

unattackable transaction

$$s \cdot \delta_{v_y} \geq 2b$$

Setting slippage

unattackable transaction

$$\boxed{s \cdot \delta_{v_y}} \geq 2b$$

victim's maximum loss

Setting slippage

unattackable transaction

$$s \cdot \delta_{v_y} \geq \boxed{2b}$$

attacker's minimum costs

Setting slippage

unattackable transaction

$$s \cdot \delta_{v_y} \geq 2b$$

$$\Rightarrow$$

$$s_a = \frac{2b}{\delta_{v_y}}$$

$s < s_a$ ensures that transaction is not attackable

Setting slippage

expected transaction re-sending cost

$$\sum_{i=0}^{\infty} p\left(s, \delta_{v_x}\right)^i \left((l+m)b + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

Setting slippage

expected transaction re-sending cost

$$\sum_{i=0}^{\infty} p(s, \delta_{v_x})^i \left((l + m)b + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

transaction failure likelihood

Setting slippage

expected transaction re-sending cost

$$\sum_{i=0}^{\infty} p(s, \delta_{v_x})^i \left(\boxed{(l+m)b} + E(s|\tilde{s} > s)\delta_{v_y} \right)$$

Ethereum transaction
fee for re-sending

Setting slippage

expected transaction re-sending cost

$$\sum_{i=0}^{\infty} p(s, \delta_{v_x})^i \left((l+m)b + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

expected price change

Setting slippage

expected transaction re-sending cost

$$\sum_{i=0}^{\infty} p\left(s, \delta_{v_x}\right)^i \left((l+m)b + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

$$= \frac{p\left(s, \delta_{v_x}\right)}{1 - p\left(s, \delta_{v_x}\right)} \left((l+m)b + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

Setting slippage

expected transaction re-sending cost

$$\sum_{i=0}^{\infty} p(s, \delta_{v_x})^i \left((l+m)b + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

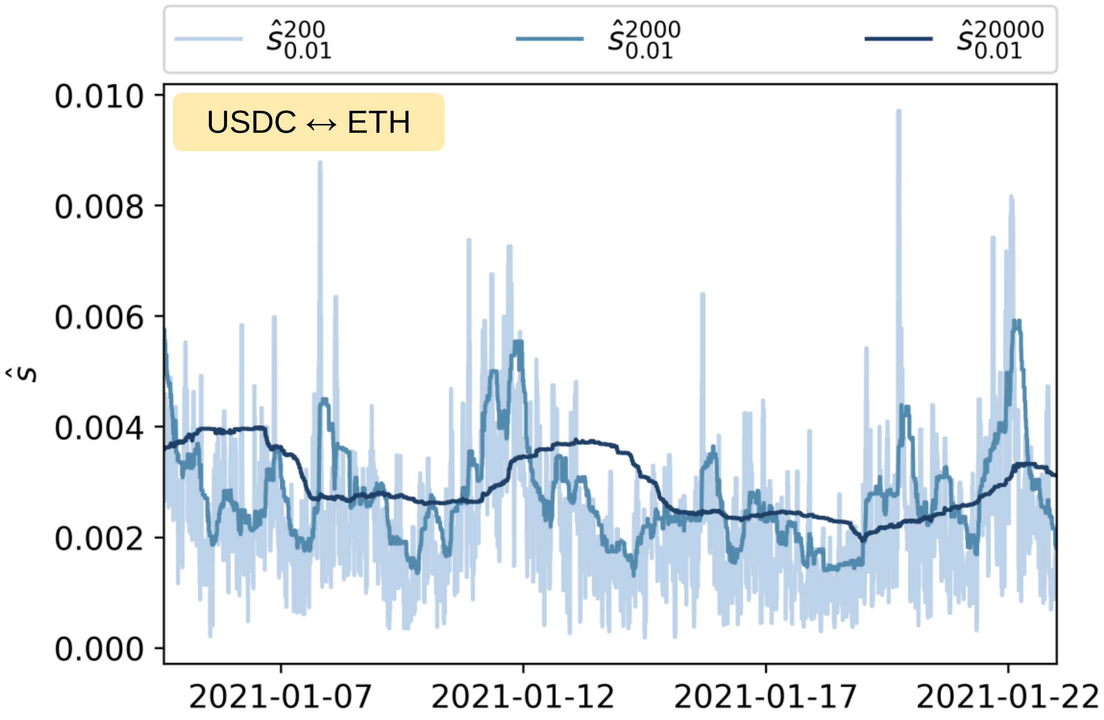
$$= \frac{p(s, \delta_{v_x})}{1 - p(s, \delta_{v_x})}\left((l+m)b + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

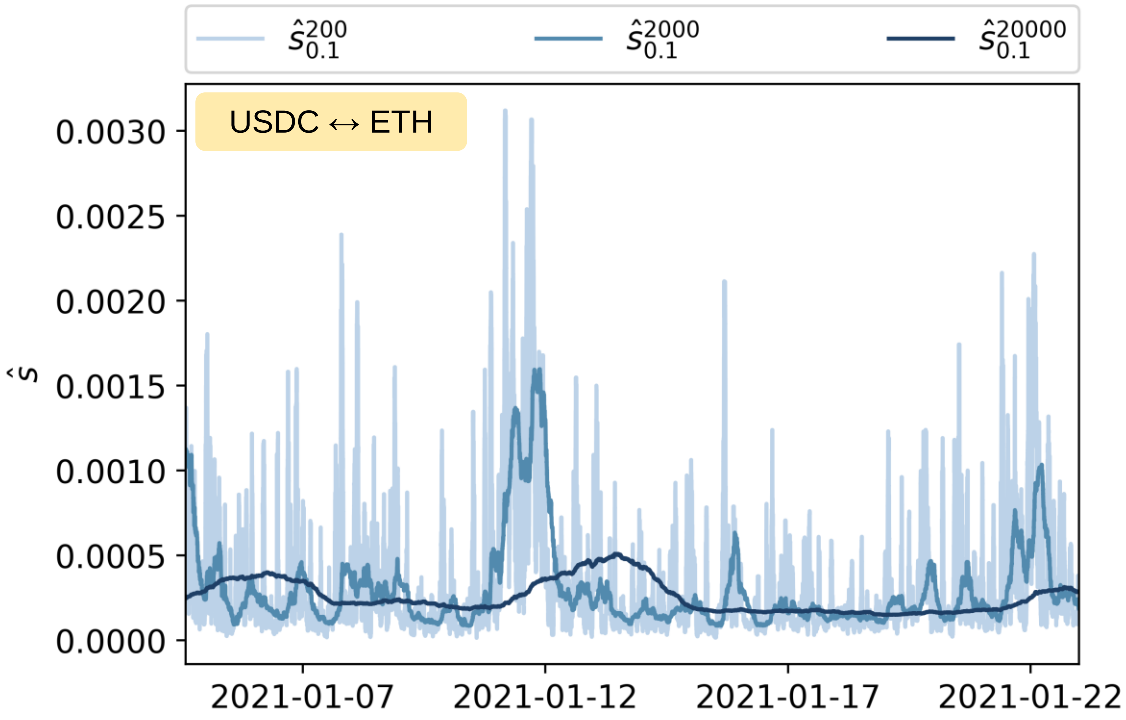
$$s_r = \frac{p(s, \delta_{v_x})}{1 - p(s, \delta_{v_x})}\left(\frac{(l+m)b}{\delta_{v_y}} + E(s|\tilde{s} > s)\delta_{v_y}\right)$$

$s_r < s_a$ expected transaction re-sending cost does not exceed sandwich attack cost

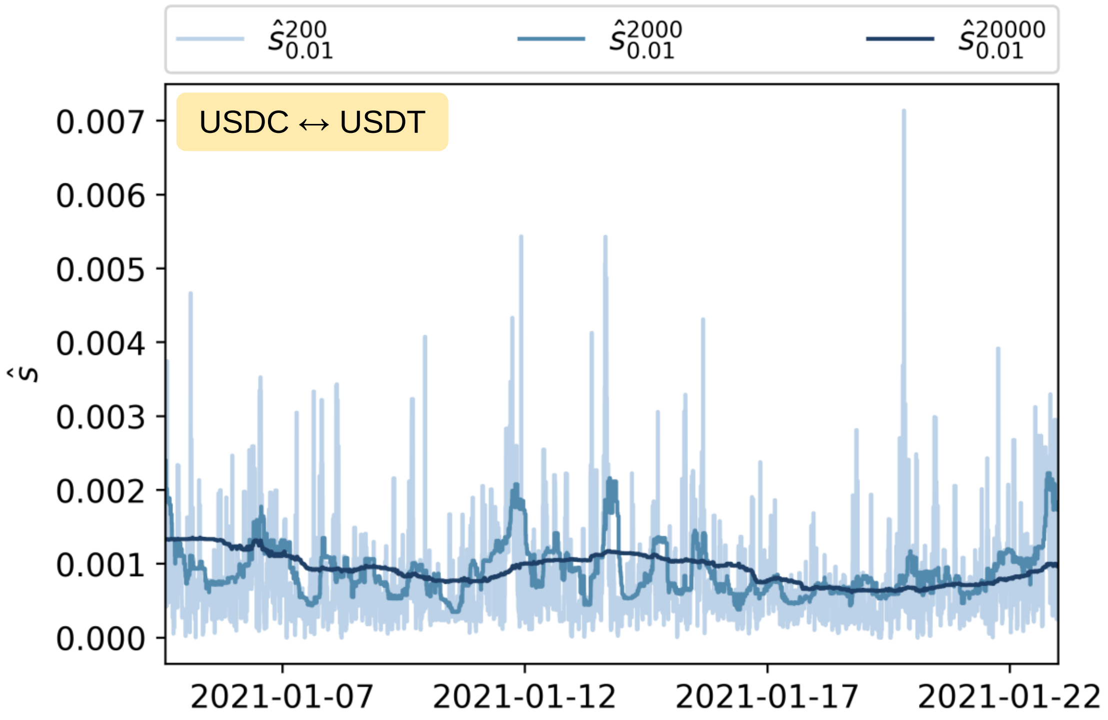
Computing lower bound for slippage tolerance (s_r)

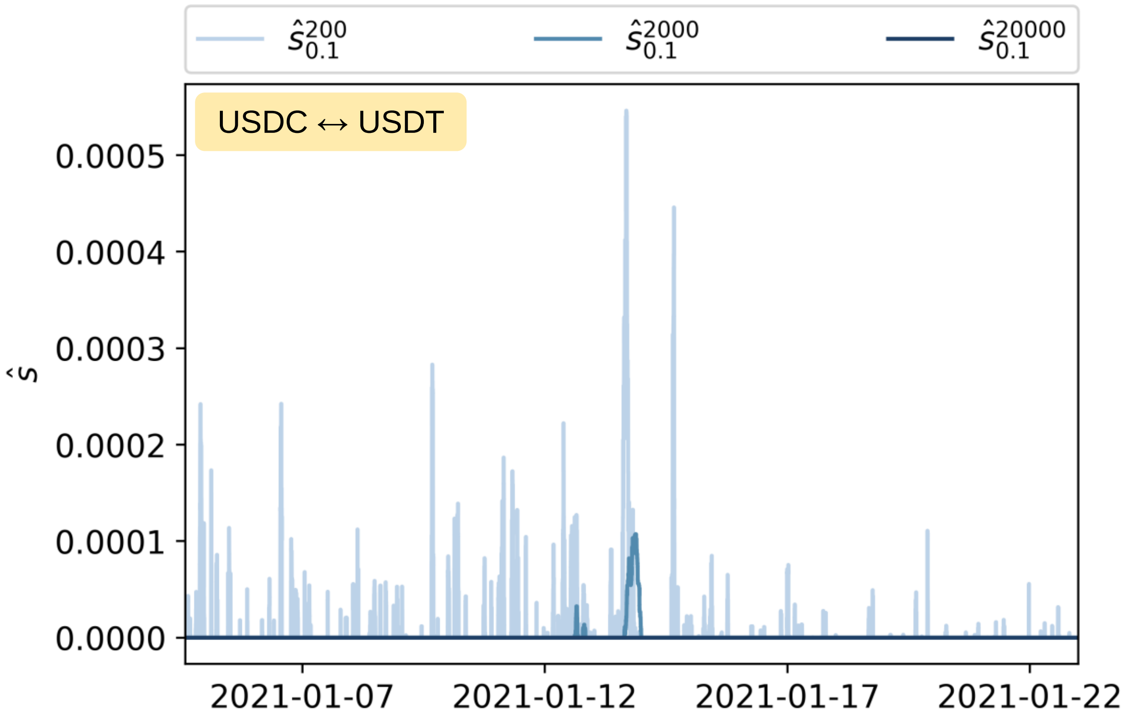
Computing lower bound for slippage tolerance (s_r)



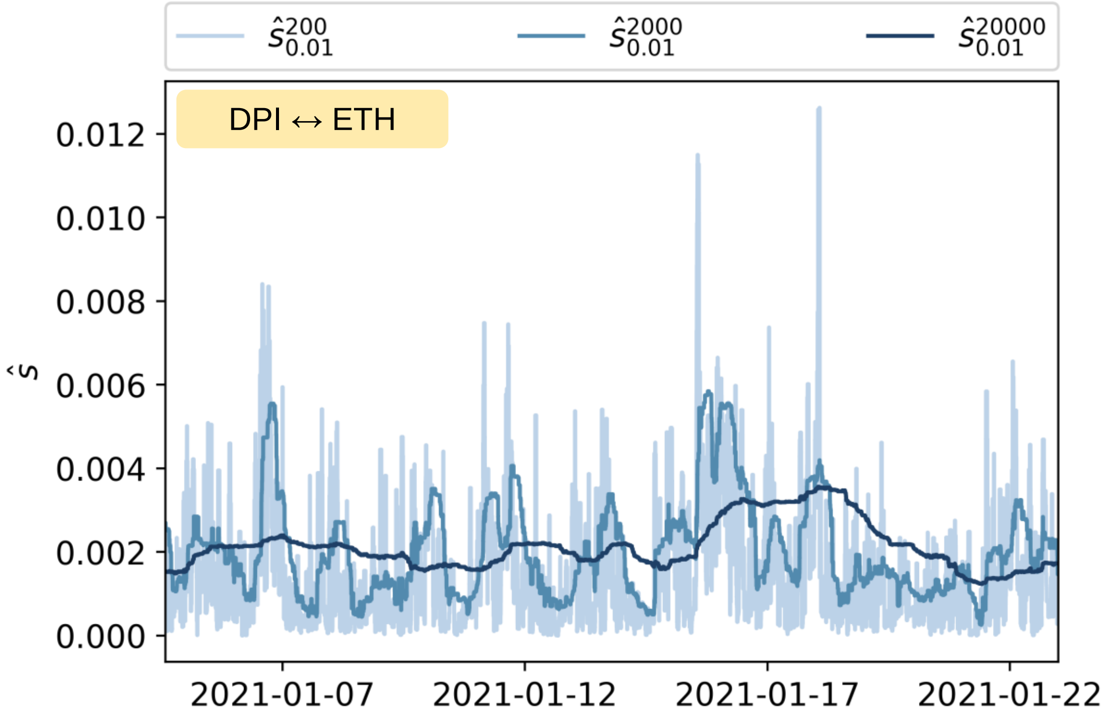


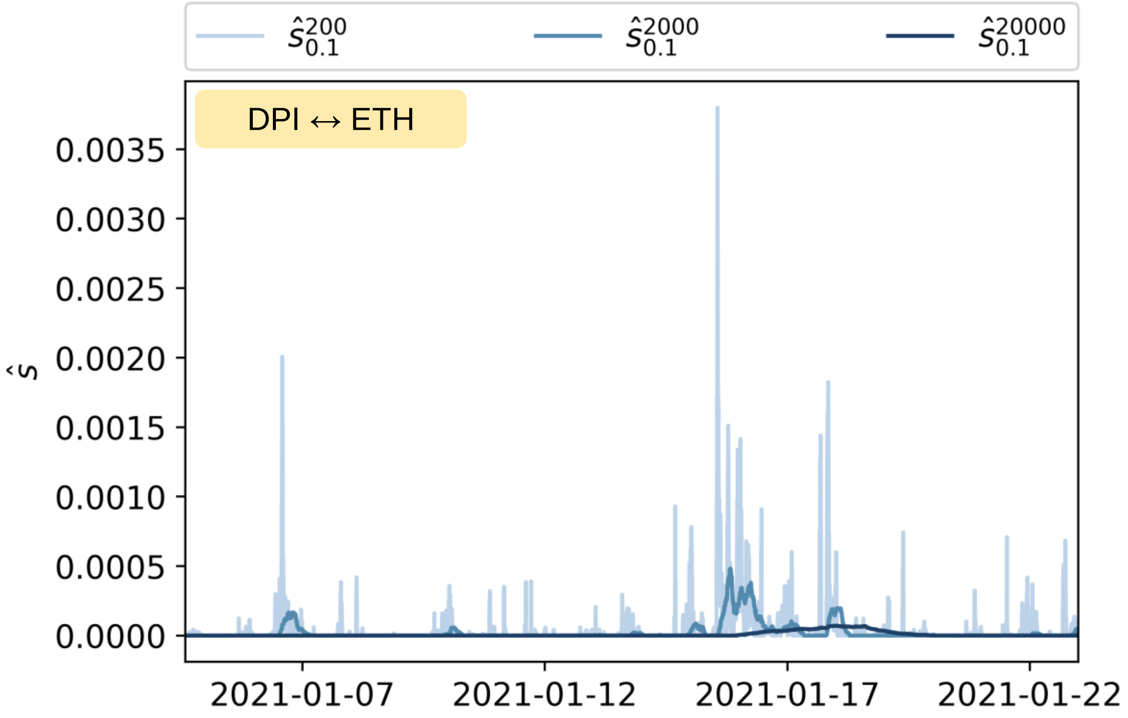
Computing lower bound for slippage tolerance (s_r)





Computing lower bound for slippage tolerance (s_r)



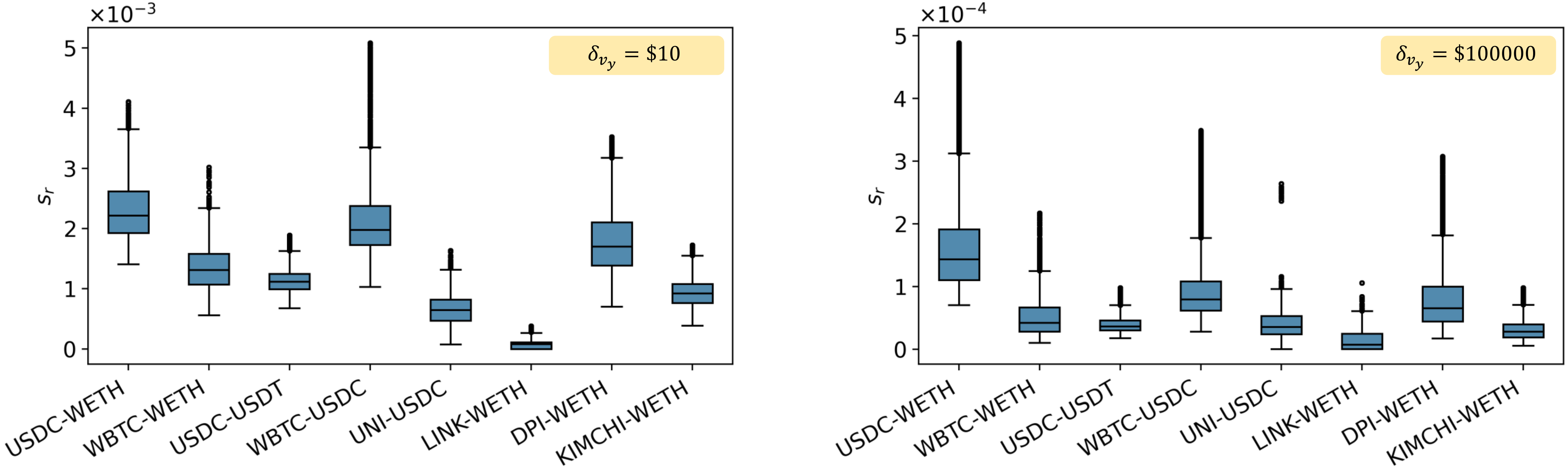


Computing lower bound for slippage tolerance (s_r)

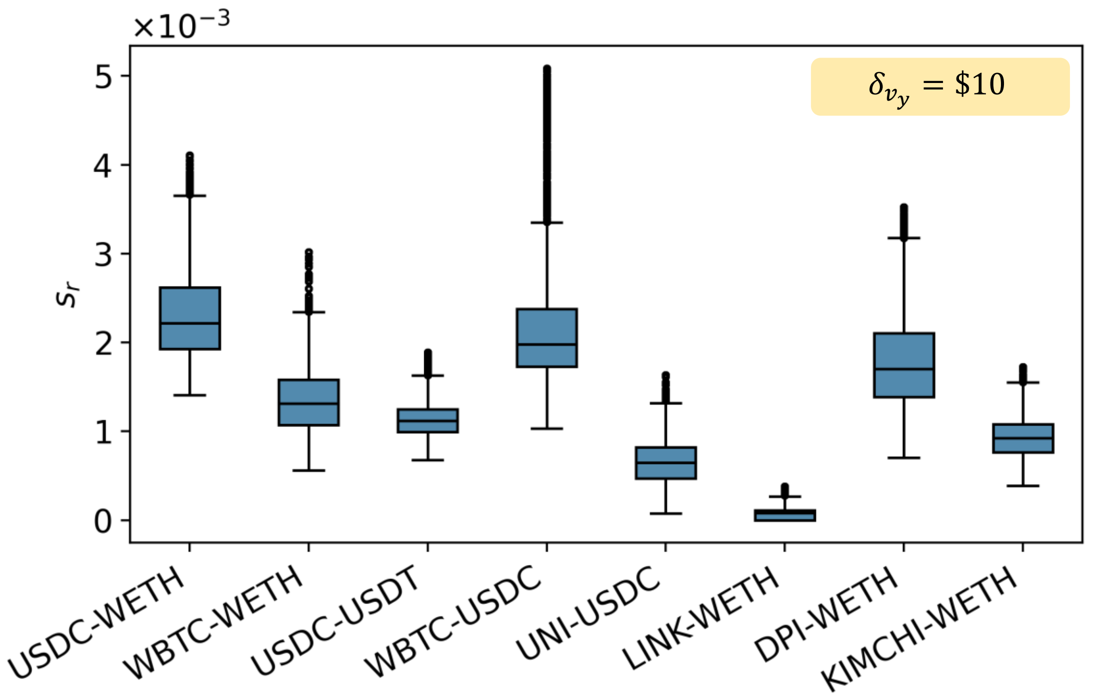
p=0.01	USDC⇌WETH		USDC⇌USDT		WBTC⇌WETH		DPI⇌WETH	
	μ	η	μ	η	μ	η	μ	η
window size								
200	$-2.37 \cdot 10^{-3}$	0.637	$-8.04 \cdot 10^{-4}$	0.512	$-1.03 \cdot 10^{-3}$	0.611	$-1.65 \cdot 10^{-3}$	0.656
2000	$-2.74 \cdot 10^{-3}$	0.093	$-8.95 \cdot 10^{-4}$	0.06	$-1.22 \cdot 10^{-3}$	0.106	$-2.03 \cdot 10^{-3}$	0.078
20000	$-2.93 \cdot 10^{-3}$	0.014	$-9.27 \cdot 10^{-4}$	0.014	$-1.37 \cdot 10^{-3}$	0.007	$-2.13 \cdot 10^{-3}$	0.045

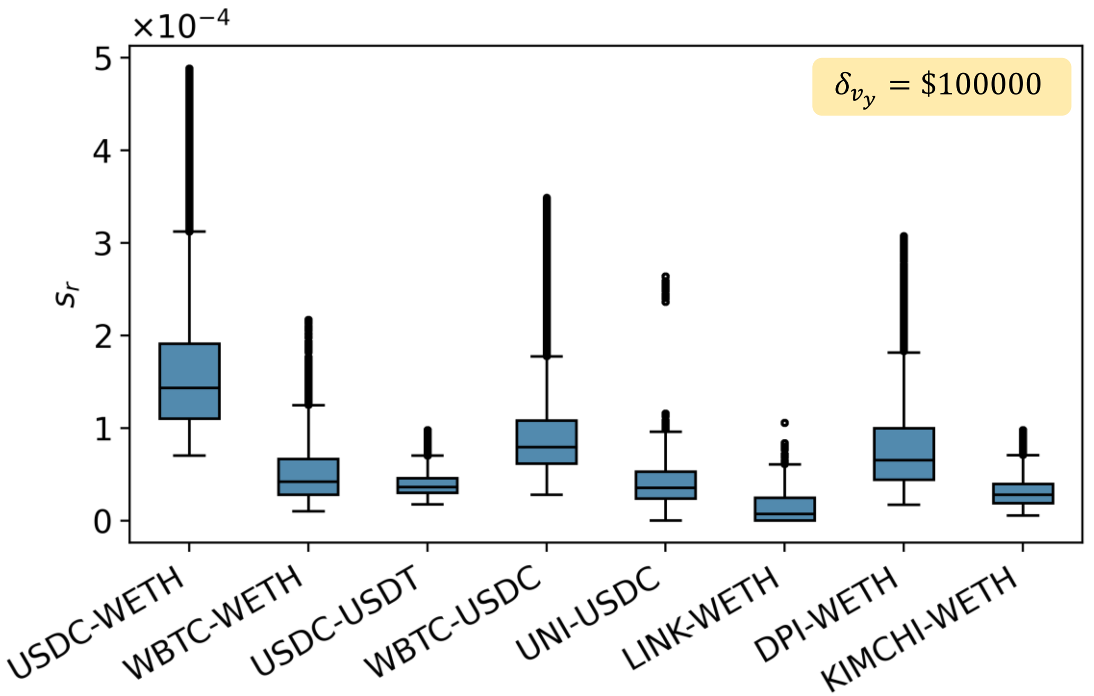
p=0.1	USDC⇌WETH		USDC⇌USDT		WBTC⇌WETH		DPI⇌WETH	
	μ	η	μ	η	μ	η	μ	η
window size								
200	$-3.49 \cdot 10^{-4}$	0.042	$-7.35 \cdot 10^{-6}$	0.335	$-1.85 \cdot 10^{-5}$	0.194	$-4.36 \cdot 10^{-5}$	0.213
2000	$-2.99 \cdot 10^{-4}$	0.001	$-1.24 \cdot 10^{-6}$	0.314	$-4.34 \cdot 10^{-6}$	0.148	$-2.18 \cdot 10^{-5}$	0.186
20000	$-2.56 \cdot 10^{-4}$	0.003	0.00	0.310	$-1.04 \cdot 10^{-6}$	0.114	$-7.81 \cdot 10^{-6}$	0.143

Lower bound for slippage tolerance (s_r)



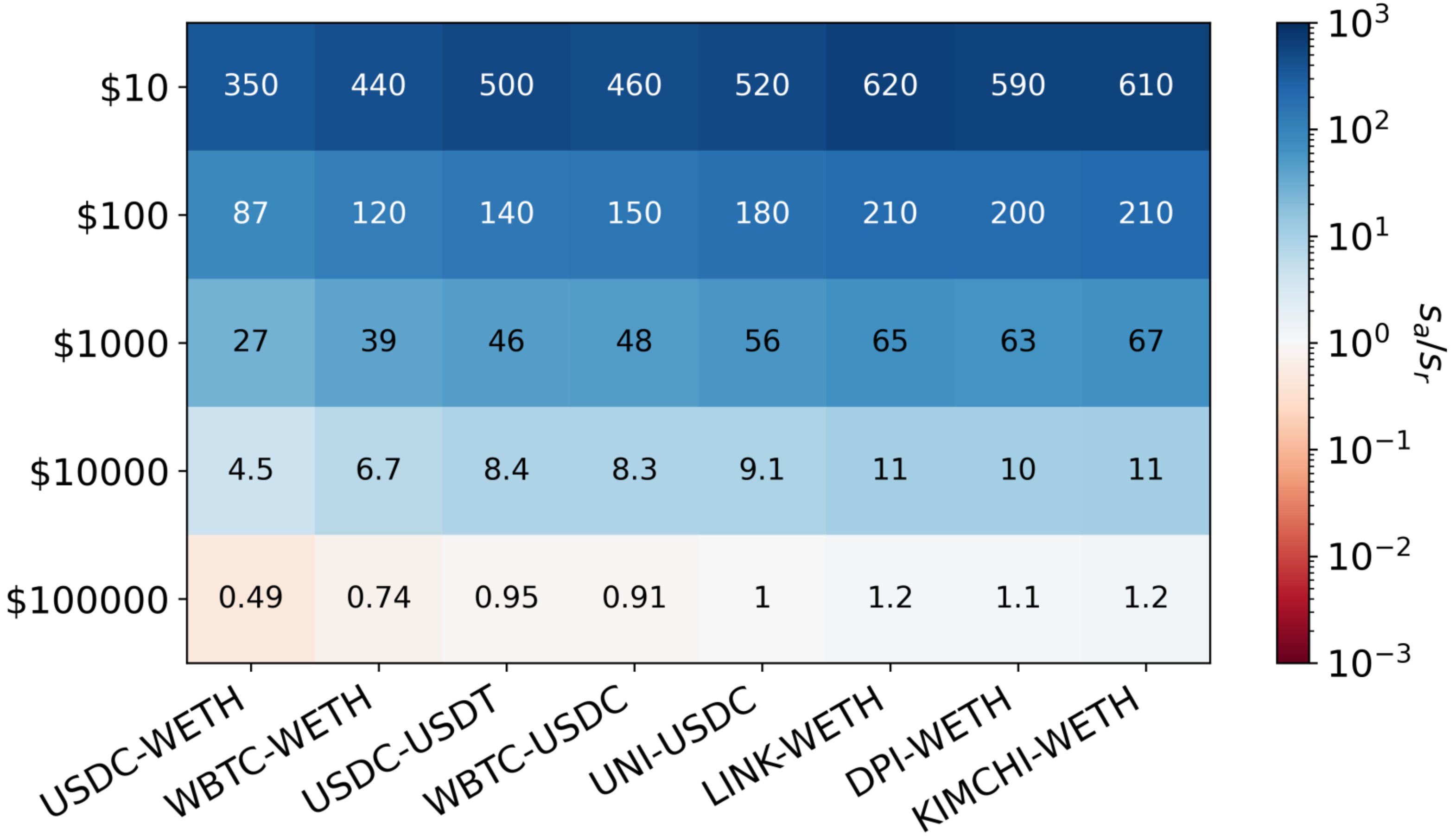
Lower bound for slippage tolerance (s_r)



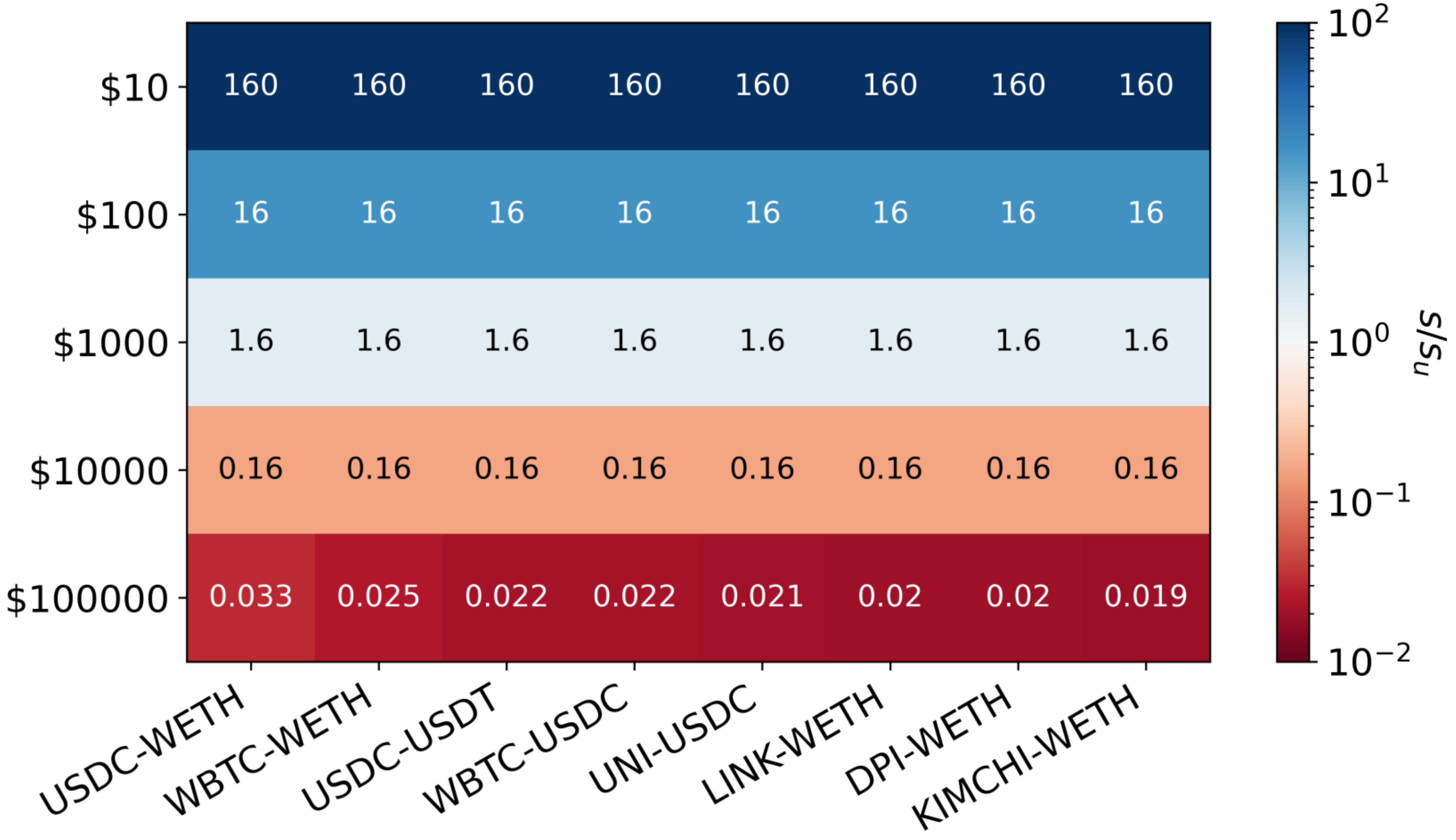


s_r smaller for low volume pools

Slippage tolerance comparison



Slippage tolerance comparison



Outlook: Uniswap V3

concentrated liquidity

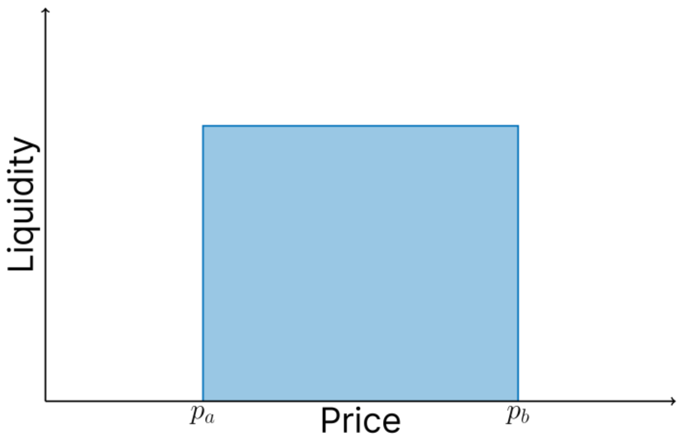
Outlook: Uniswap V3

concentrated liquidity

Outlook: Uniswap V3

concentrated liquidity

liquidity providers choose price range $[p_a, p_b]$ in which they would like to provide liquidity



Outlook: Uniswap V3

concentrated liquidity

liquidity providers choose price range $[p_a, p_b]$ in which they would like to provide liquidity