Privacy, DEXs, and DeFi, oh my!

zkSessions: DeFi + Privacy

Guillermo Angeris

~~February 15~~ February 22, 2021

Outline

A (very) quick intro to CFMMs and AMMs

Can we make it private?

Some solutions

Conclusion

Trading with Uniswap and friends

- CFMM is a contract with *reserves* of coin A and B
  (We will call them R_α and R_β)
- And some *trading function*, or 'invariant,' $\varphi(R_\alpha, R_\beta)$

Trading with Uniswap and friends

- CFMM is a contract with *reserves* of coin A and B
  (We will call them R_α and R_β)

- And some *trading function*, or ‘invariant,’ $\varphi(R_\alpha, R_\beta)$

- Traders are allowed to remove (or add) coin A (or B) so long as

$$\varphi(R_\alpha, R_\beta) = k$$

Uniswap

- For example, Uniswap (or 'constant product markets') have

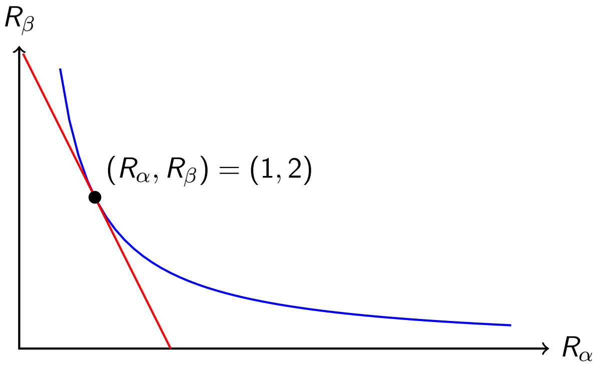
$$\varphi(R_\alpha, R_\beta) = R_\alpha R_\beta = k.$$

- Which means the price of A in terms of B is

$$p(R_\alpha, R_\beta) = \frac{R_\beta}{R_\alpha}.$$

Uniswap (continued)

- The price of a CFMM is equal to the *slope* of the trading function



Many other DEXs are CFMMs

- mStable (or constant sum markets)

$$\varphi(R_\alpha, R_\beta) = R_\alpha + R_\beta$$

Many other DEXs are CFMMs

- mStable (or constant sum markets)

$$\varphi(R_\alpha, R_\beta) = R_\alpha + R_\beta$$

- Balancer (or G3Ms, or constant mean markets):

$$\varphi(R_\alpha, R_\beta) = R_\alpha^w R_\beta^{1-w}$$

where $0 < w < 1$

Many other DEXs are CFMMs

- mStable (or constant sum markets)

$$\varphi(R_\alpha, R_\beta) = R_\alpha + R_\beta$$

- Balancer (or G3Ms, or constant mean markets):

$$\varphi(R_\alpha, R_\beta) = R_\alpha^w R_\beta^{1-w}$$

  where $0 < w < 1$

- Curve:

$$\varphi(R_\alpha, R_\beta) = (R_\alpha + R_\beta) - C(R_\alpha R_\beta)^{-1}$$

  with $C > 0$

Many others... (continued)

- The specifics don't matter!
- We will only note that (most) AMMs can be written this way

Many others... (continued)

- The specifics don't matter!
- We will only note that (most) AMMs can be written this way
- Now we can go to the more important question

Outline

A (very) quick intro to CFMMs and AMMs

Can we make it private?

Some solutions

Conclusion

The bad news

The bad news

- No.

The bad news

- No.
- More specifically:

The bad news

- No.
- More specifically:
  - Not really without major changes

The bad news

- No.
- More specifically:
  - Not really without major changes
  - Under even relatively weak adversaries

The bad news

- No.
- More specifically:
  - Not really without major changes
  - Under even relatively weak adversaries
- (Sorry!)

Our adversary (Eve)

- Can't access any external balances (including CFMM reserves)
- Can read public data
  - Marginal price of CFMM
  - Check if a trade is feasible
- Can interact with CFMM contract
- Knows the CFMM trading function
- Wants to know Alice's trade

Result

- Eve knows *when* Alice trades $\Longrightarrow$ game over

Result

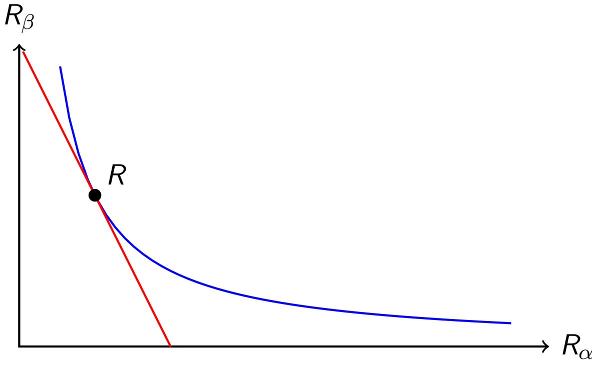
- Eve knows *when* Alice trades $\Longrightarrow$ game over
- Why?
- Eve knows price before Alice's trade and after Alice's trade
- (And any nonzero trade)
- Gives simple system of equations!

Result (continued)

- This happens even when the marginal price is not revealed!

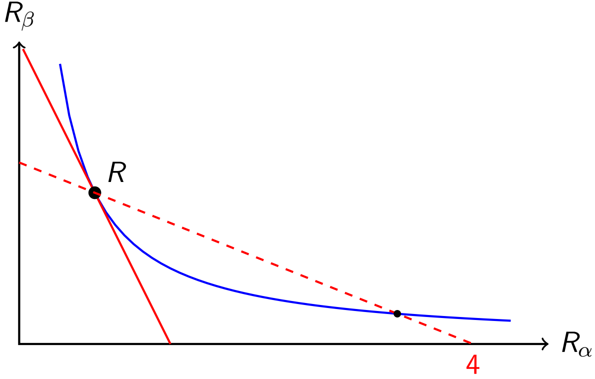
Result (continued)

- This happens even when the marginal price is not revealed!
- Eve can approximate it by querying a small trade ($\delta \to 0$):



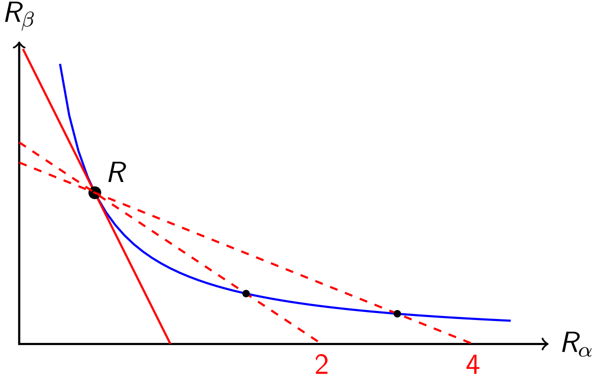
Result (continued)

- This happens even when the marginal price is not revealed!
- Eve can approximate it by querying a small trade ($\delta \to 0$):



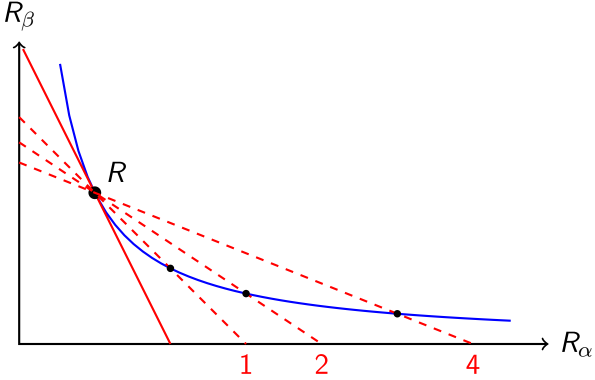
Result (continued)

- This happens even when the marginal price is not revealed!
- Eve can approximate it by querying a small trade ($\delta \to 0$):



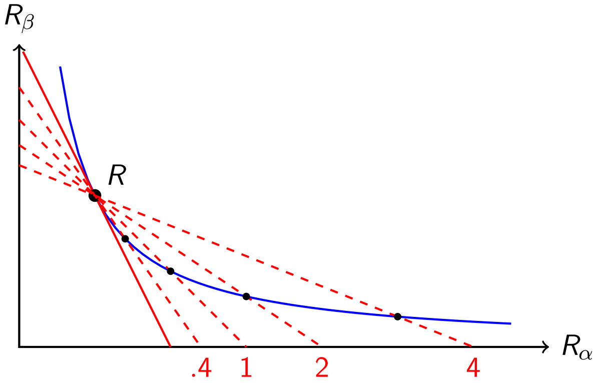
Result (continued)

- This happens even when the marginal price is not revealed!
- Eve can approximate it by querying a small trade ($\delta \to 0$):



Result (continued)

- This happens even when the marginal price is not revealed!
- Eve can approximate it by querying a small trade ($\delta \to 0$):



Outline

A (very) quick intro to CFMMs and AMMs

Can we make it private?

Some solutions

Conclusion

Proof caveats

Proof caveats

- No randomness in query

Proof caveats

- No randomness in query
- Known trade time (*i.e.*, Eve knows when Alice traded)

Adding noise

- To preserve privacy, we can add *randomness* to the price
- Prevents Eve from guessing exact marginal price
- $\implies$ (more work) that Eve cannot know true price change

Adding noise

- To preserve privacy, we can add *randomness* to the price
- Prevents Eve from guessing exact marginal price
- $\implies$ (more work) that Eve cannot know true price change
- Downside: requires that the noise is $\sim$ trade size!

  Could be very expensive for traders or LPs

Changing the order

- We can also batch DEX orders
- Prevents Eve from knowing which trade is Alice's

Changing the order

- We can also batch DEX orders
- Prevents Eve from knowing which trade is Alice's
- Downside: requires batch trade $\gg$ Alice's trade

  If not, Eve knows most of Alice's trade!
- Also can be very slow in practice

Outline

A (very) quick intro to CFMMs and AMMs

Can we make it private?

Some solutions

Conclusion

Privacy is hard

Privacy is hard

- Current implementations of CFMMs cannot be private :(
- Proof applies in many cases, where price impact is known

Privacy is hard

- Current implementations of CFMMs cannot be private :(
- Proof applies in many cases, where price impact is known
- But there are some (reasonable) solutions!

Privacy is hard

- Current implementations of CFMMs cannot be private :(
- Proof applies in many cases, where price impact is known
- But there are some (reasonable) solutions!
- Maybe there are even better mechanisms...?

Acknowledgements

- Tarun Chitra (Gauntlet)
- Alex Evans (Placeholder)
- zkSessions team!