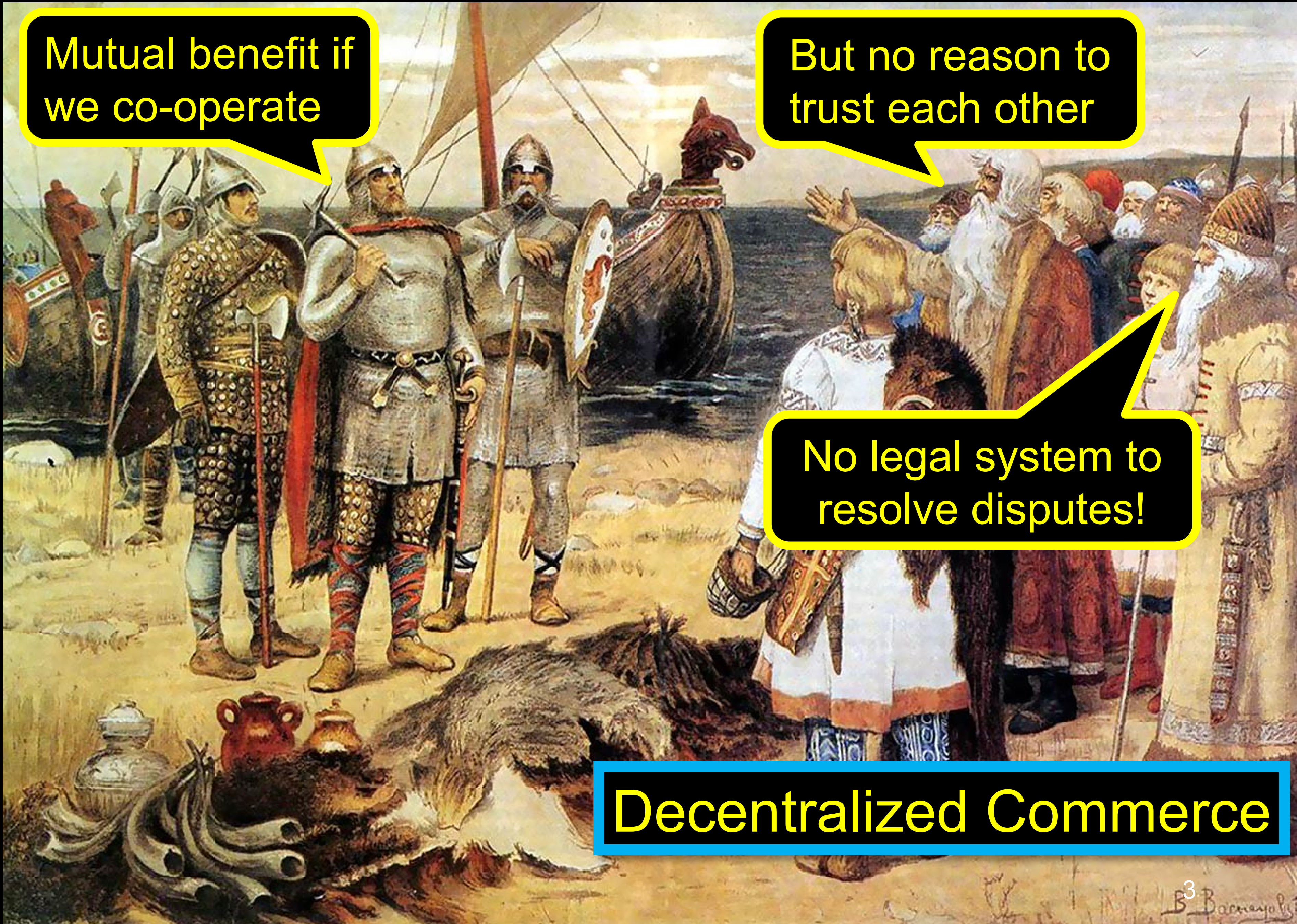
D’INFORMATIQUE DE SORBONNE UNIVERSITÉ

Further Decentralizing Decentralized Finance
June 2024

Maurice Herlihy
Brown University

Joint work with Sergio Rajsbaum & Sam Devorsetz

The Grand Challenge


Mutual benefit if we co-operate
But no reason to trust each other
No legal system to resolve disputes!
Decentralized Commerce

Road Map

Background: Contracts, AMMs, etc.

What if: decentralized arbitrage?

What if: defensive rebalancing?

Road Map

Background: Contracts, AMMs, etc.

What if: decentralized arbitrage?

What if: defensive rebalancing?

Distributed Ledger (blockchain)

Cash				
Date	Description	Increase	Decrease	Balance
Jan. 1, 20X3	Balance forward			$ 50,000
Jan. 2, [illegible]	[illegible]	[illegible]		60,000
Jan. 3, 20X3	Cash sale	5,000		65,000
Jan. 5, 20X3	Paid rent		[illegible]	58,000
Jan. 7, 20X3	Paid salary		3,000	55,000
Jan. 8, 20X3	Cash sale	[illegible]		59,000
Jan. 8, 20X3	Paid bills		[illegible]	57,000
Jan. 10, 20X3	Paid tax		[illegible]	56,000
Jan. 12, 20X3	Collected receivable	7,000		63,000

Append-only list of events

Not just financial

Everyone agrees on content

Tamper-proof!

Specific technology unimportant

Smart Contracts

Not smart

Not a contract

I/O State machine

Trusted

Trading Electronic Assets

Our Electronic Assets

"gold"

stablecoin?

numéraire

"silver"

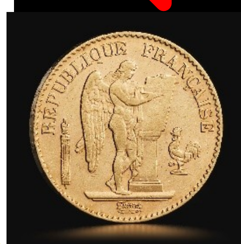
volatile

speculative

Automated Market Maker

I own “liquidity pools” of gold & silver

Automated Market Makers



Alice

Exchange rate is function of my pool sizes

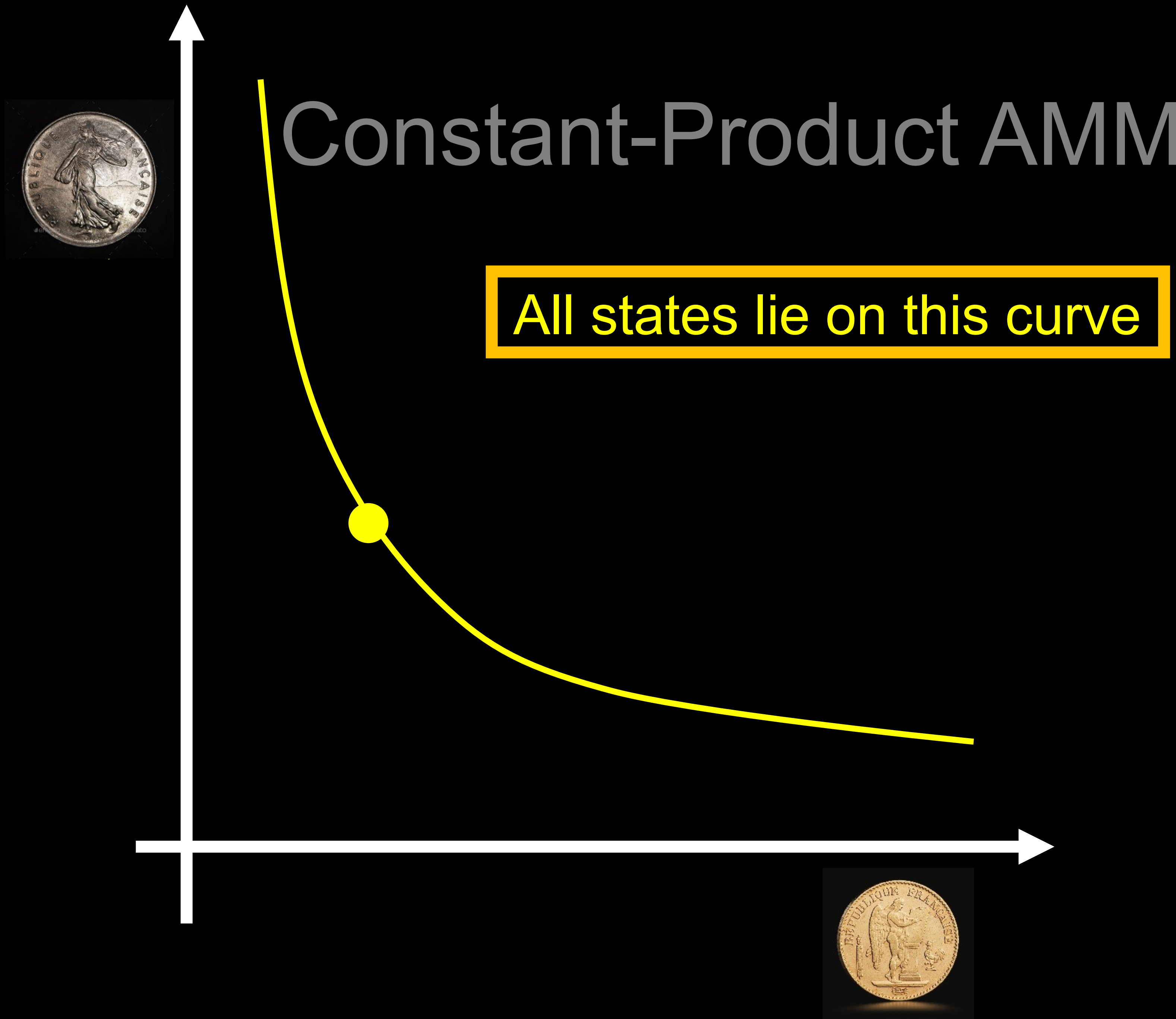
Will trade silver for gold

Multi-Billion Dollar Business

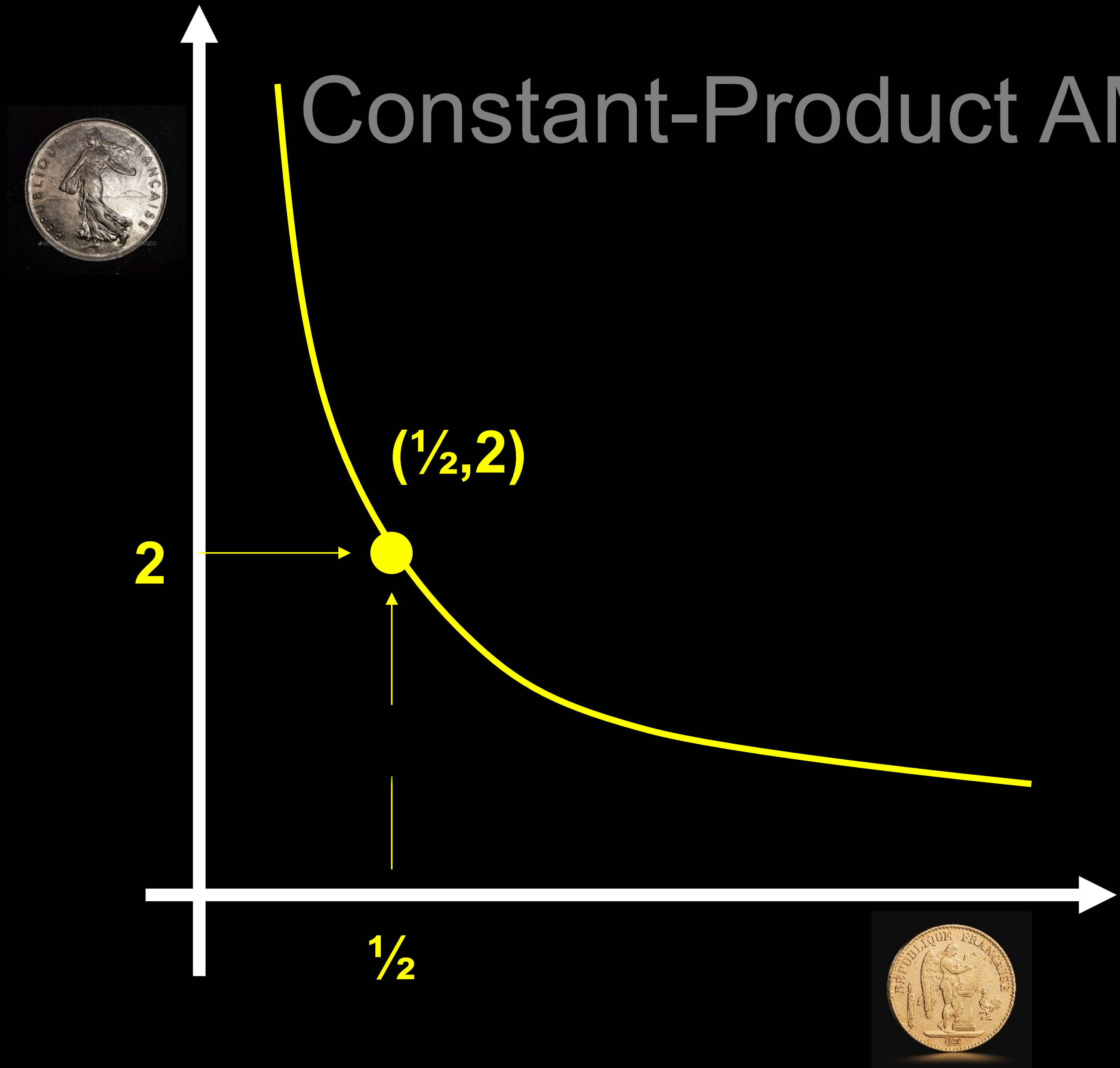
UNISWAP

SushiSwap

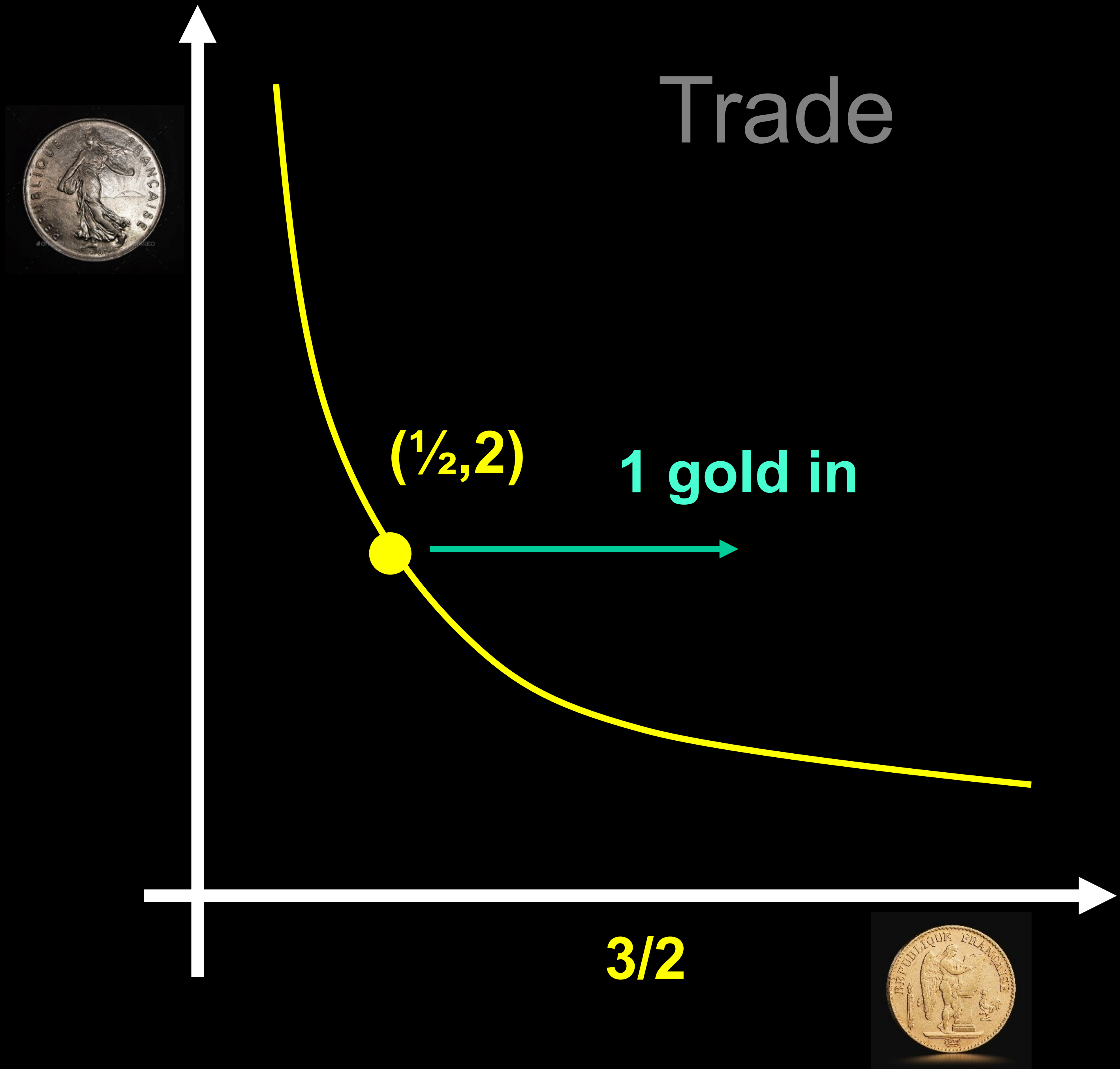
Constant-Product AMM



Constant-Product AMM



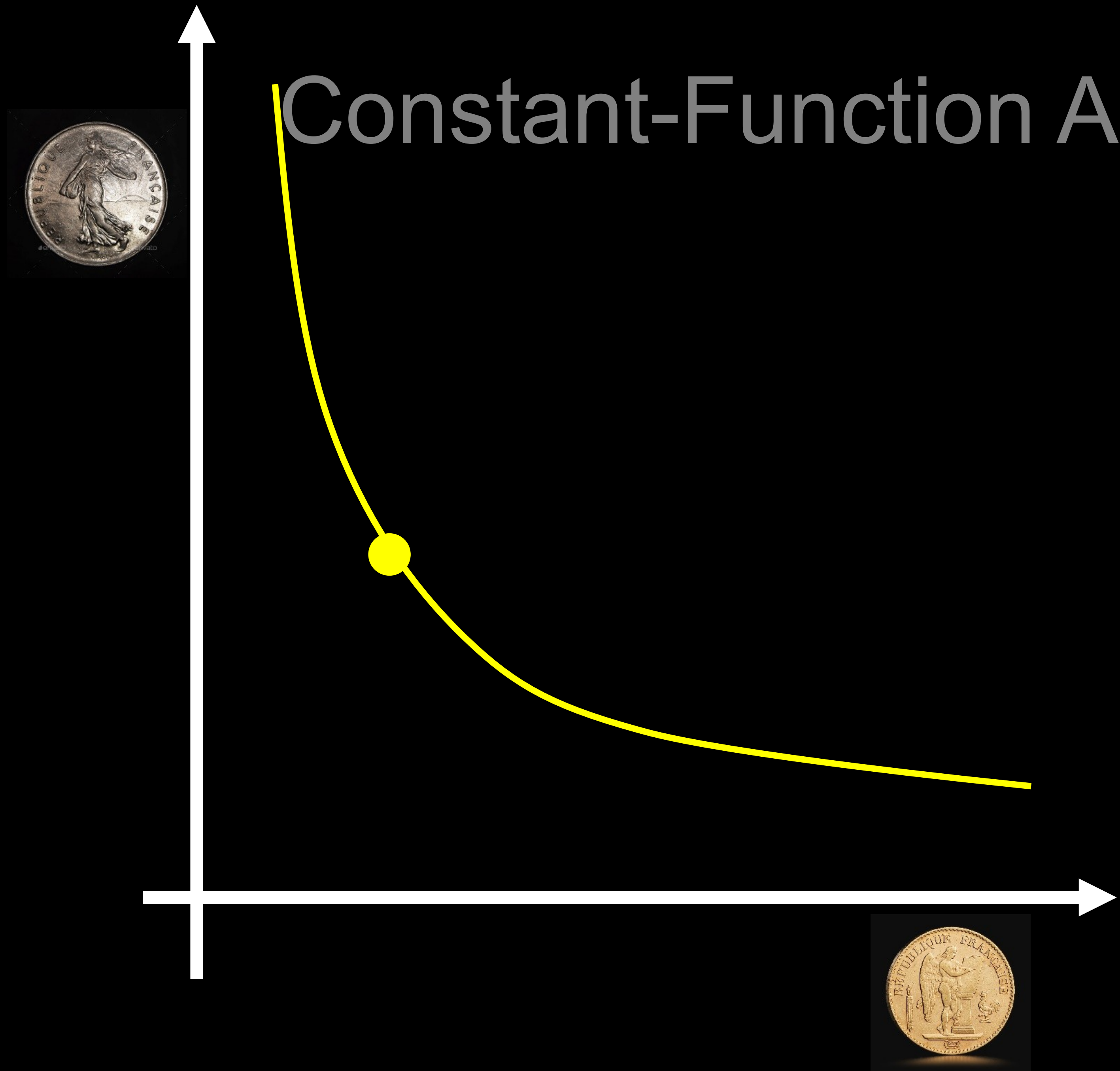
Trade



Trade

We ignore fees

Constant-Function AMM



Constant-Function AMMs

“trading function”

Well-behaved …

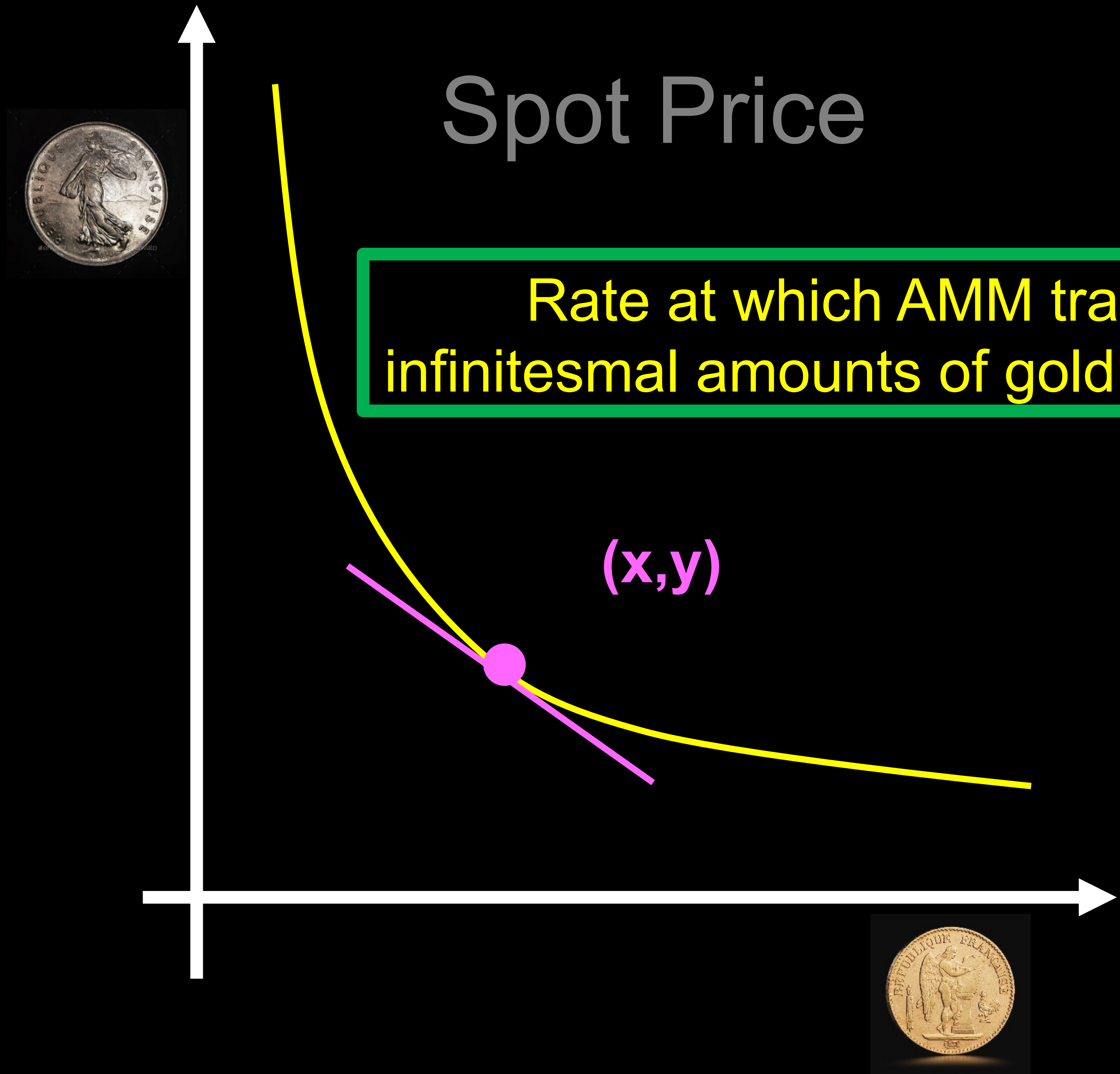
“capitalization”

AMM’s wealth

Unchanged by trades

Changed by investment

Spot Price


Rate at which AMM trades infinitesmal amounts of gold for silver
(x,y)

Classical AMM Theory

CEX

Requires a *central reference market*

Publishes prices for all assets

Parties can trade @ prices

Little or no slippage

(*E.g.*, Coinbase, NYSE)

Classical Arbitrage

2 silver = 1 gold

1 silver = 1 gold

CEX

AMM

Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX

AMM

Classical Arbitrage

2 silver = 1 gold

1 silver = 1 gold

CEX

AMM

ARB

Classical Arbitrage

2 silver = 1 gold

CEX

1 silver = 1 gold

AMM

Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX

AMM

Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX

Classical Arbitrage

2 silver = 1 gold

1 silver = 1 gold

CEX

Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX

Classical Arbitrage

2 silver = 1 gold

2 silver = 1 gold

CEX

AMM

Classical Arbitrage

I changed my spot price!

CE

My spot price did not change!

AR

I made a risk-free profit at the AMM's expense!

age

But I am paying for arbitrage!

I maximize my profit when I make AMM & CEX prices equal

CEX

AMM

Eventual market efficiency

Road Map

Background: Contracts, AMMs, etc.

What if: decentralized arbitrage?

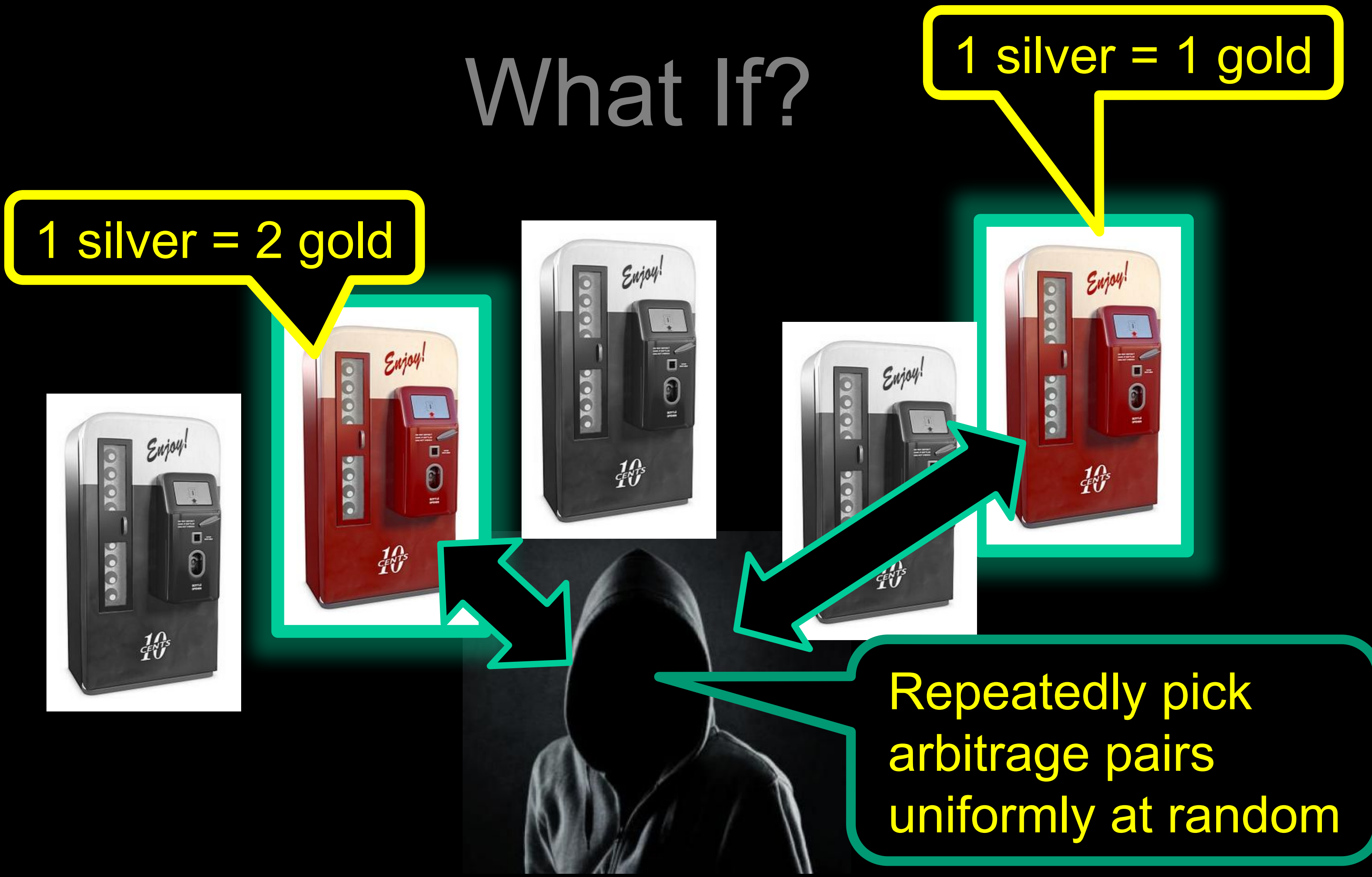
What if: defensive rebalancing?

What If?

What If?


…
1 silver = 2 gold
…
…
1 silver = 1 gold
Like "*population protocols*" in distributed computing
No global price information
Info spreads only by local pair-wise interactions

What If?


1 silver = 1 gold
1 silver = 2 gold
Repeatedly pick arbitrage pairs uniformly at random

Why?

"long tail" tokens not traded on CEX

CEX may not be accessible, timely, etc.

Fraud!!! MtGox, FTX, Celsius, Voyager, QuadrigaCX, LIBOR, etc.

Mathematical model of independent scientific interest?

Convergence, but to What?

Converges toward …

$$(S_i(0), G_i(0)) \rightsquigarrow \left(\frac{C_i}{\sum_j C_j} \sum_j S_j(0), \frac{C_i}{\sum_j C_j} \frac{(\sum_j C_j)^2}{\sum_j S_j(0)} \right)$$

i^{th} AMM's initial silver and gold pools

Convergence, but to What?

Converges toward …

$$(S_i(0), G_i(0)) \rightsquigarrow \left(\frac{C_i}{\sum_j C_j} \sum_j S_j(0), \frac{C_i}{\sum_j C_j} \frac{(\sum_j C_j)^2}{\sum_j S_j(0)} \right)$$

*i*th AMM's initial silver and gold pools

All the silver

All the remaining gold

Convergence, but to What?

Converges toward …

$$(S_i(0), G_i(0)) \rightsquigarrow \left(\frac{C_i}{\sum_j C_j} \sum_j S_j(0), \frac{C_i}{\sum_j C_j} \frac{(\sum_j C_j)^2}{\sum_j S_j(0)} \right)$$

i^{th} AMM's initial silver and gold pools

Divided in proportion to capitalizations

Time to Convergence?

Time until expected prices agree within

$$\Theta\left(n^2 \log n \log\left(\frac{1}{\epsilon}\right)\right)$$

Number of AMMs

Desired precision

(Proofs via potentials and spectral methods)

Price-Fixing?

$$\widehat{P} = \frac{\left(\sum_i S_i(0)\right)^2}{\left(\sum_i C_i\right)^2}$$

Final price if arb profits in gold

Final price if arb profits in silver

$$\widehat{P}^* = \frac{\left(\sum_i C_i\right)^2}{\left(\sum_i G_i(0)\right)^2}$$

All points between if arb profits mixed

How much Gold does AMM_i lose to Arbitrage?

$$C_i \left(\frac{C_i}{S_i(0)} - \frac{\sum_j C_j}{\sum_j S_j(0)} \right)$$

Weighted by capitalization

Road Map

Background: Contracts, AMMs, etc.

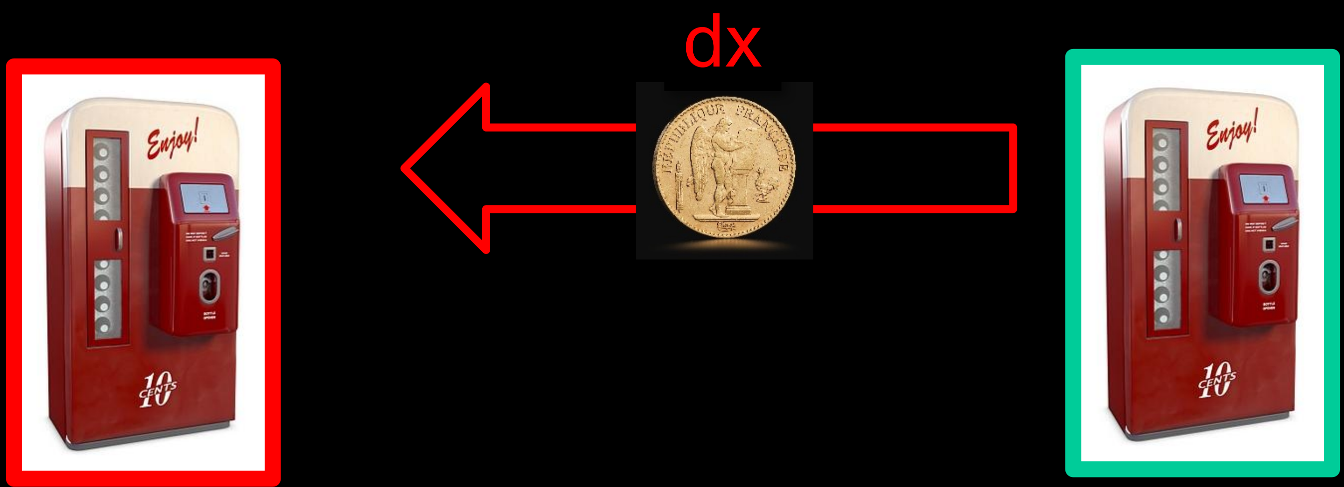
What if: decentralized arbitrage?

What if: defensive rebalancing?

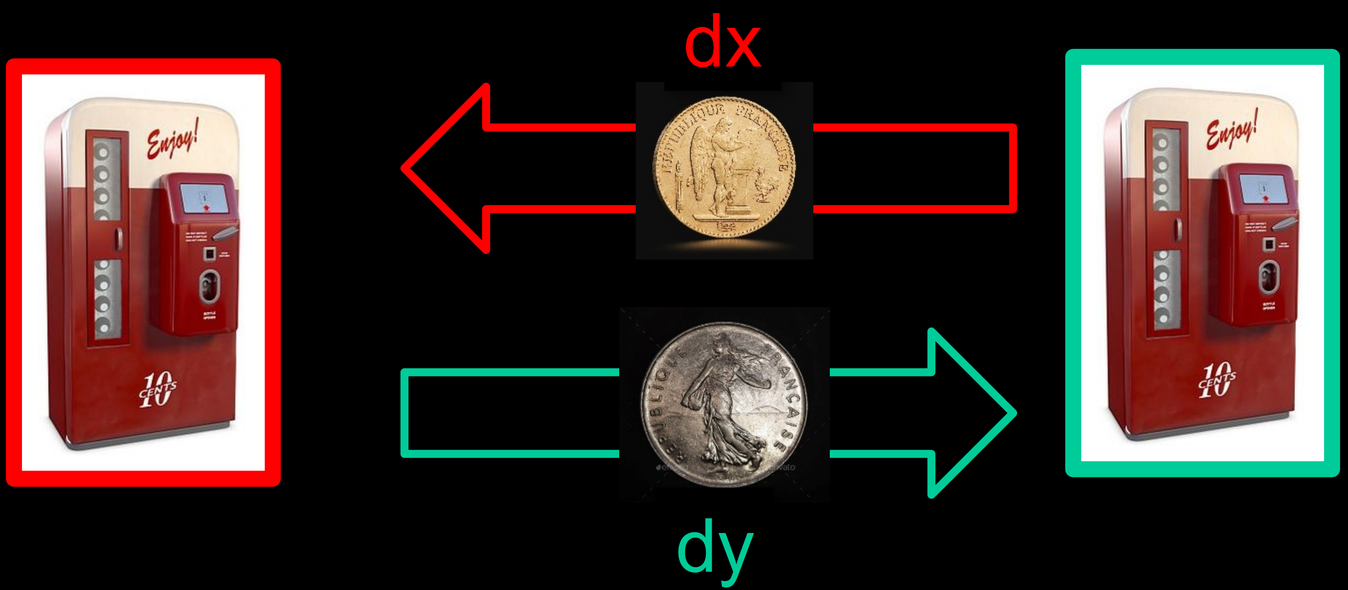
Let’s rebalance ourselves & keep the arbitrage profits!

Zut, alors!

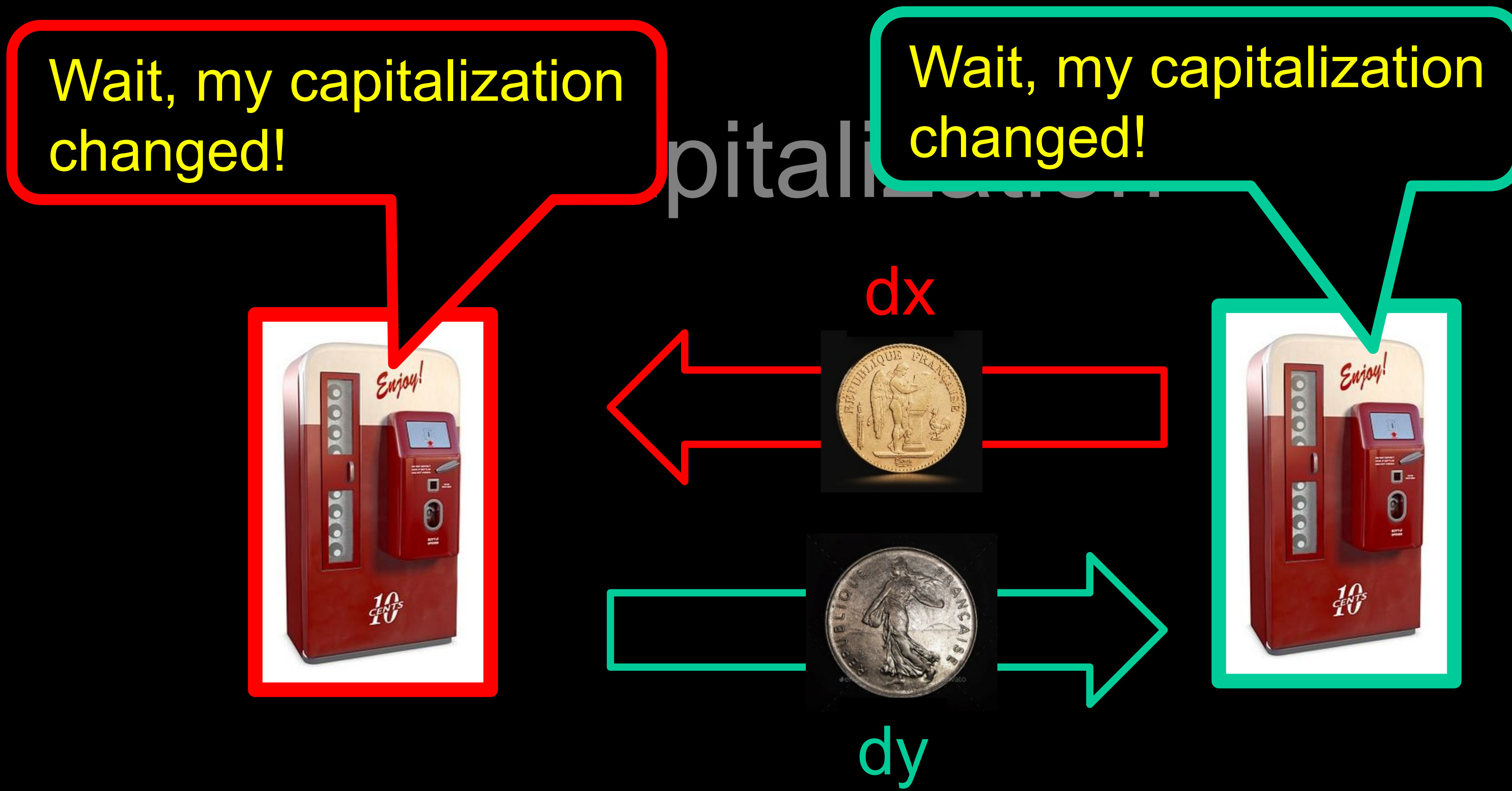
Rebalancing

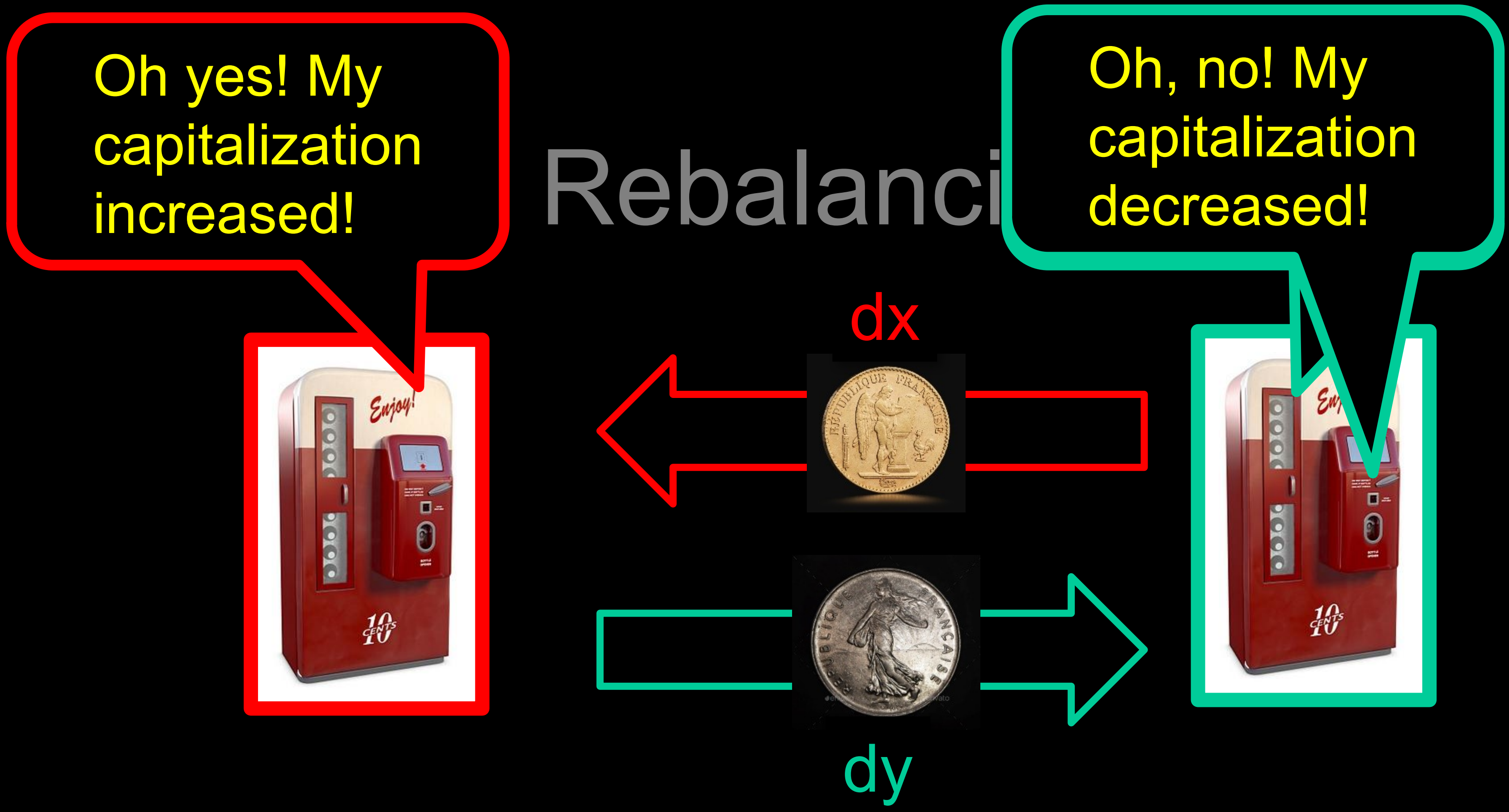


Rebalancing



Spot Prices

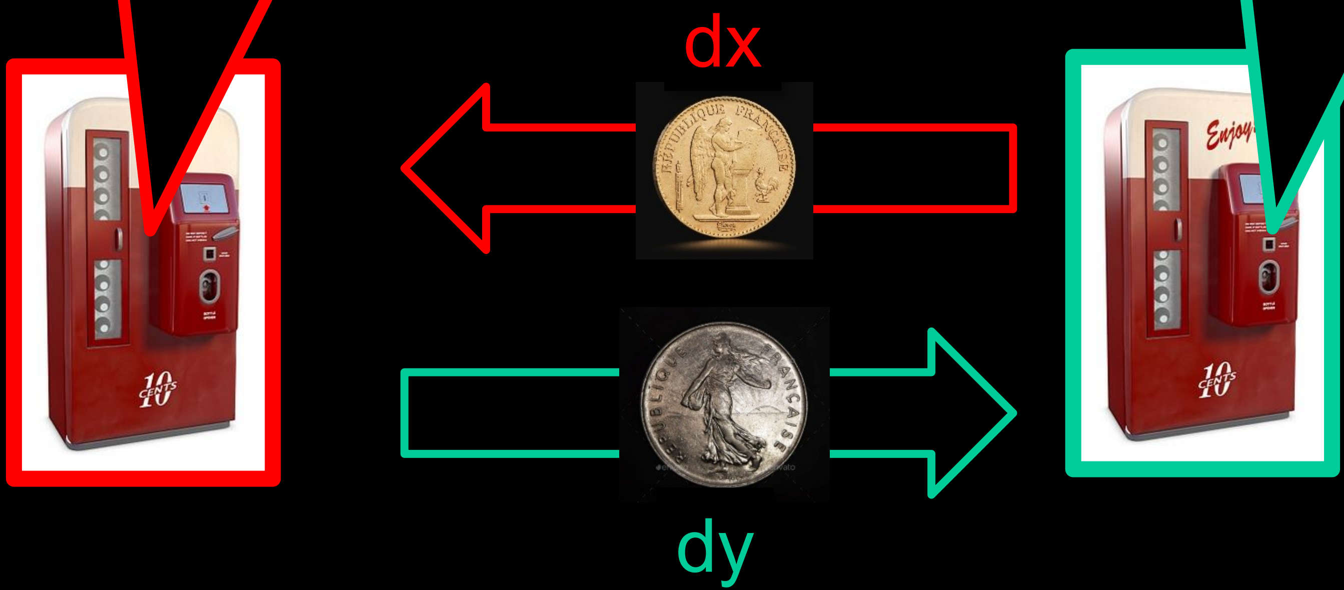

Wait, my capitalization changed!
Wait, my capitalization changed!
dx
dy


Oh yes! My capitalization increased!
Rebalanci
Oh, no! My capitalization decreased!
dx
dy

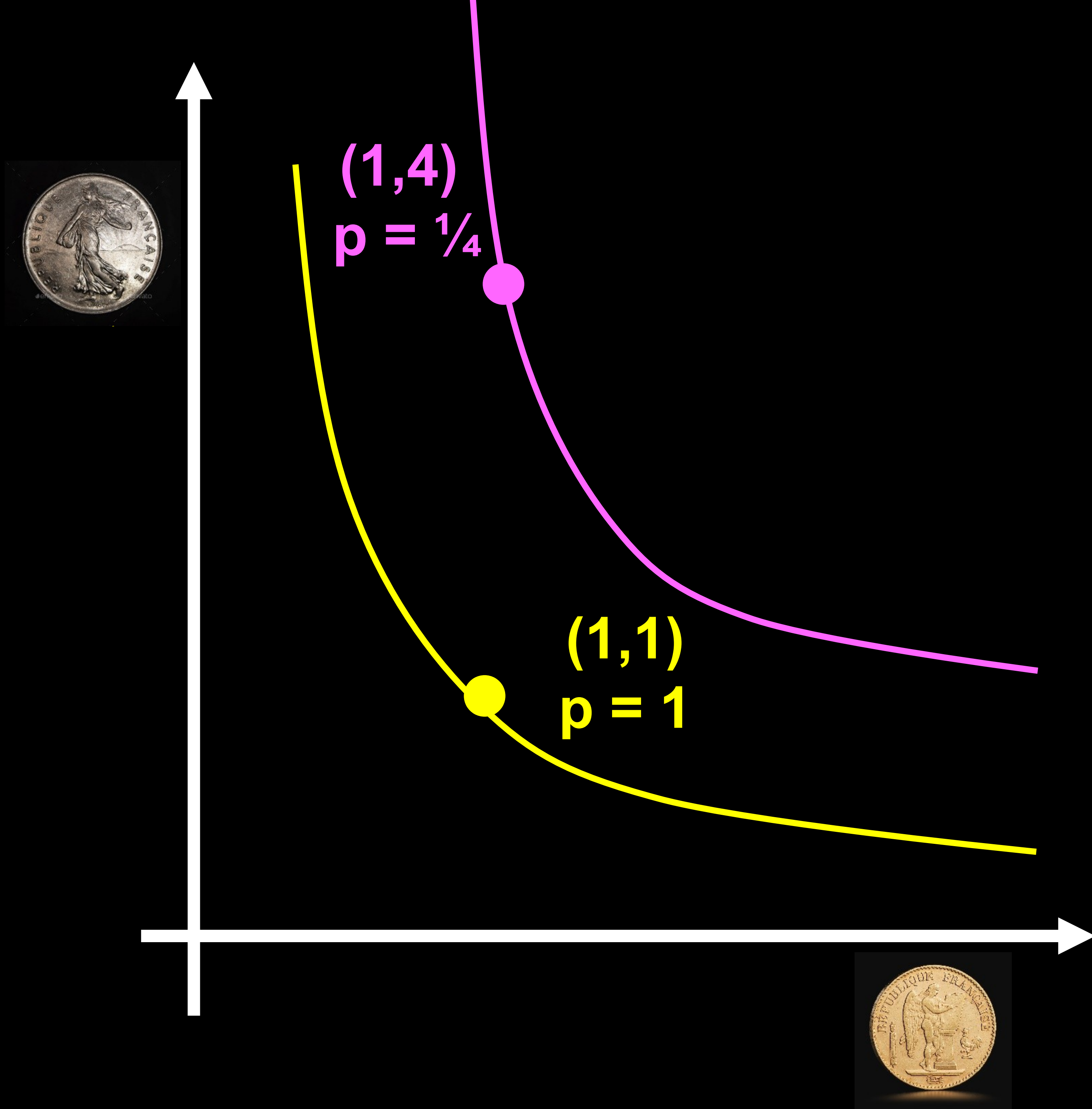
Prices equal & capitalization increased!

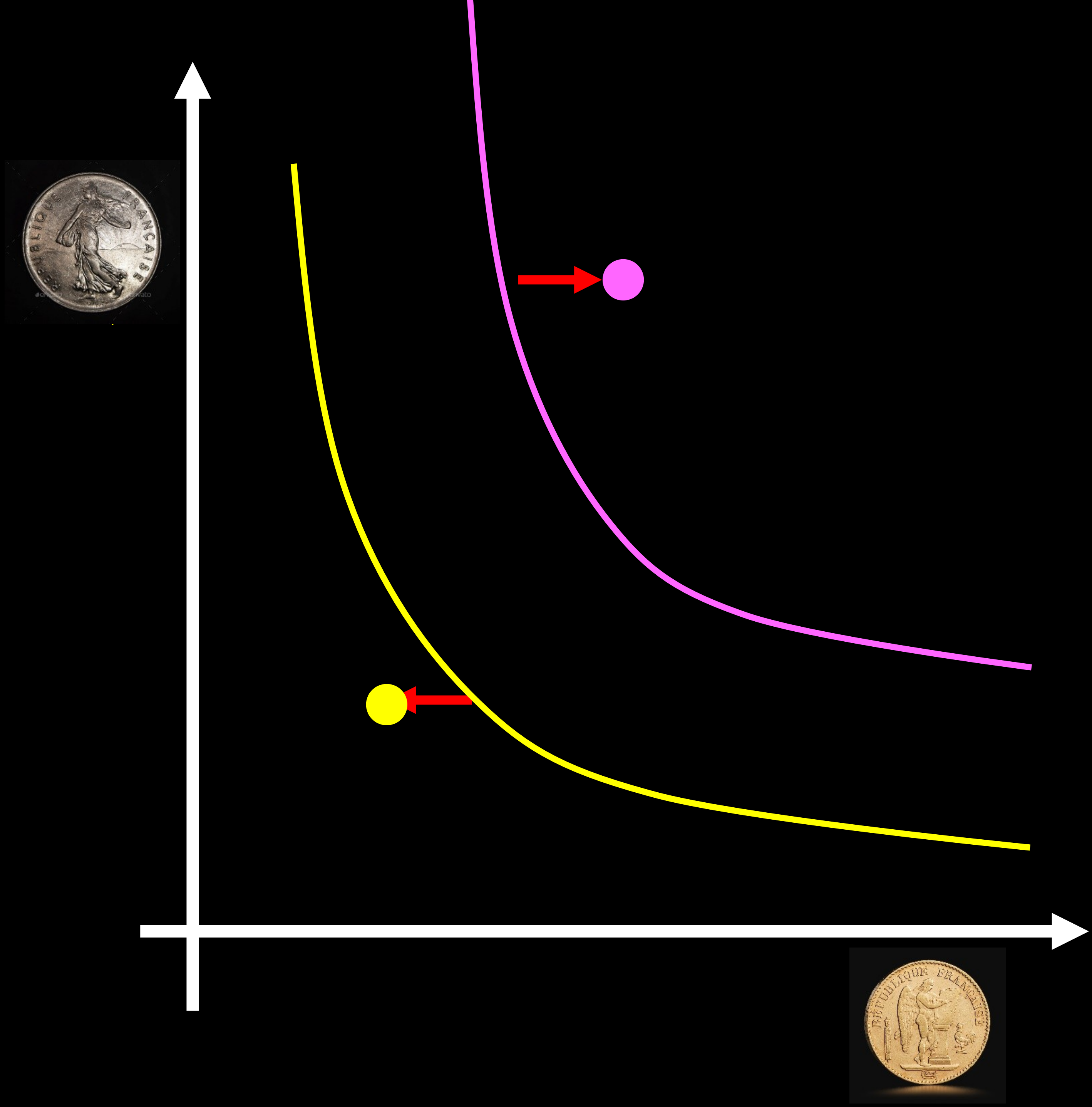
Win Rebal

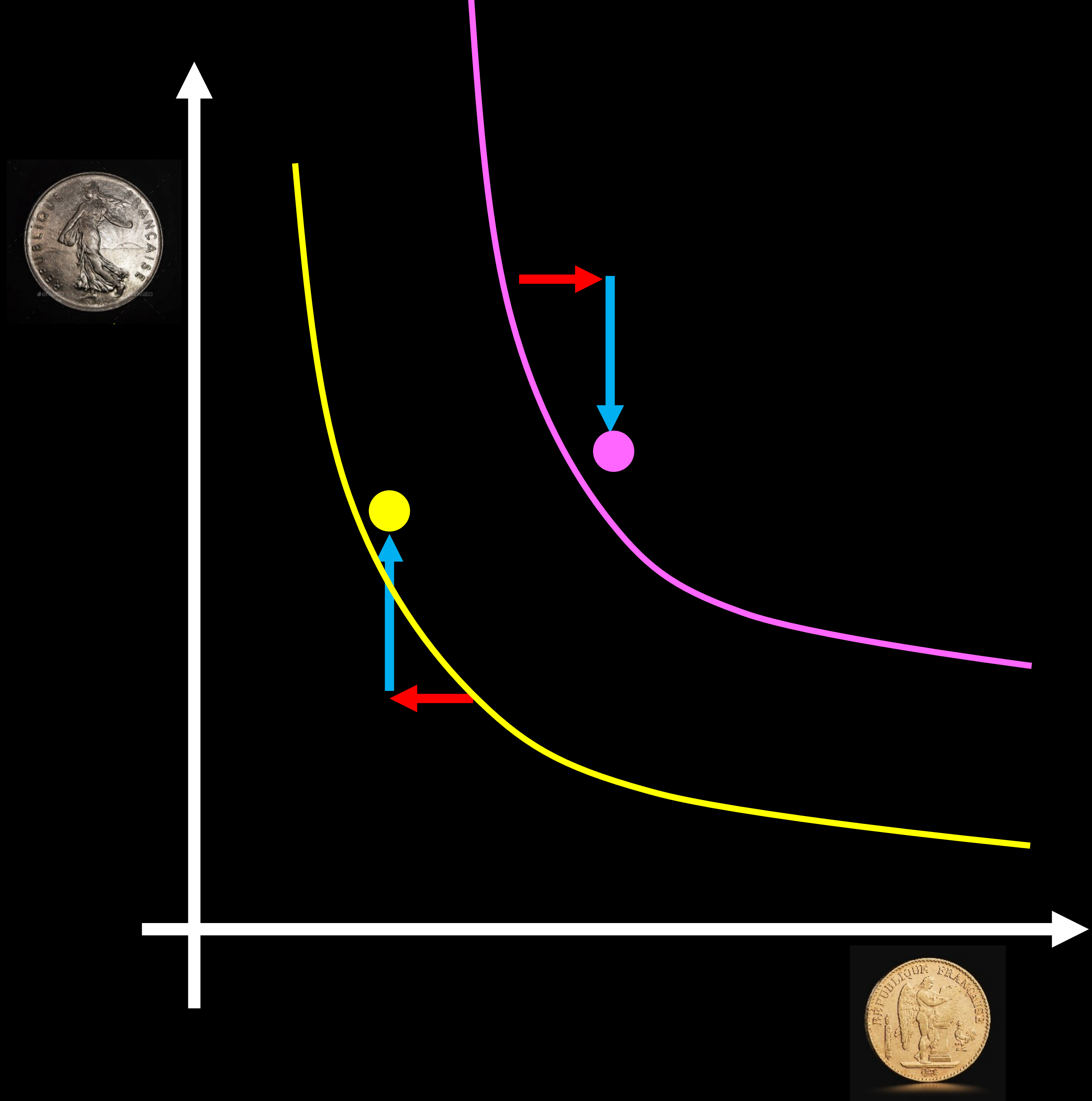
Prices equal & capitalization increased!

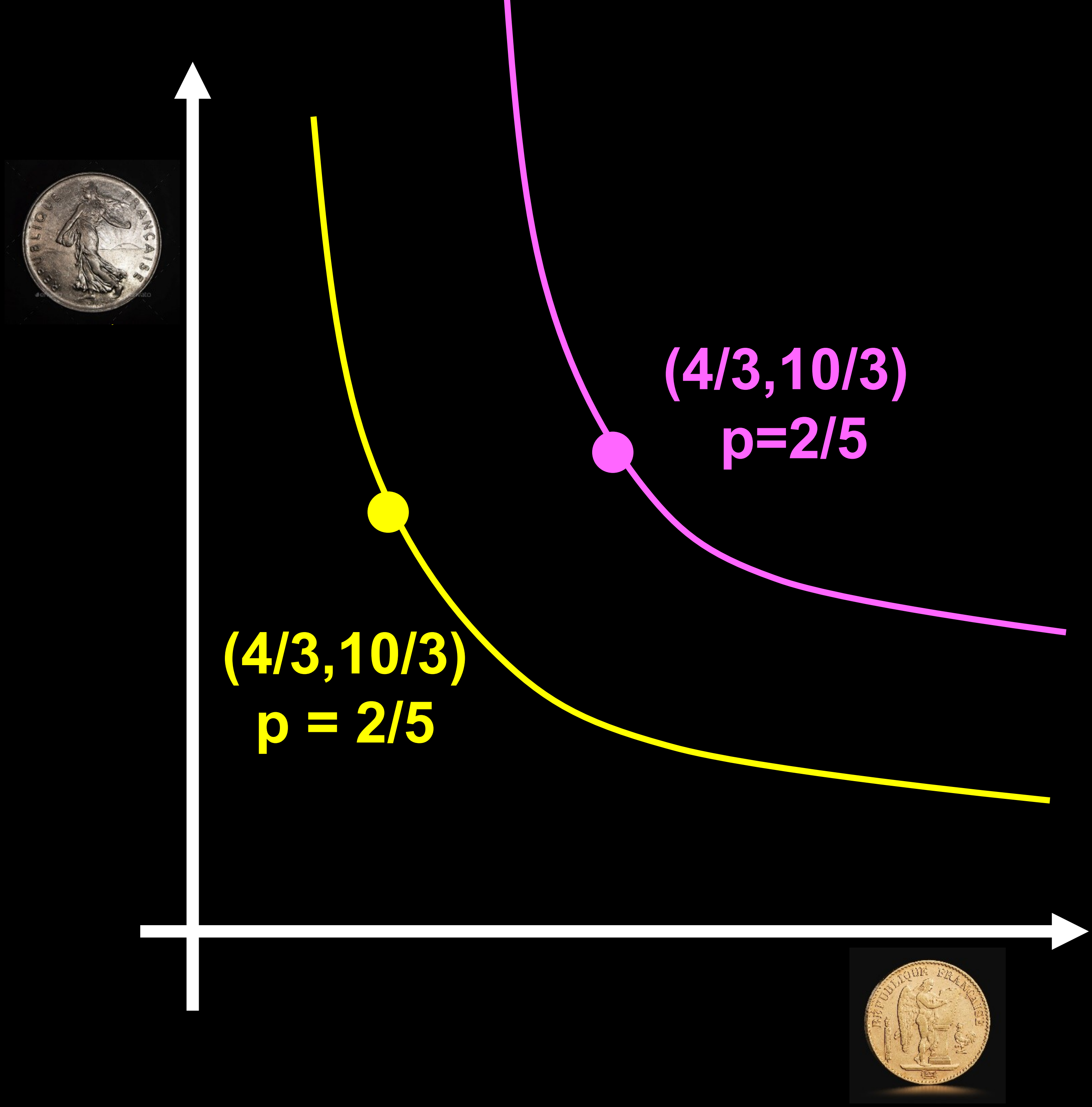


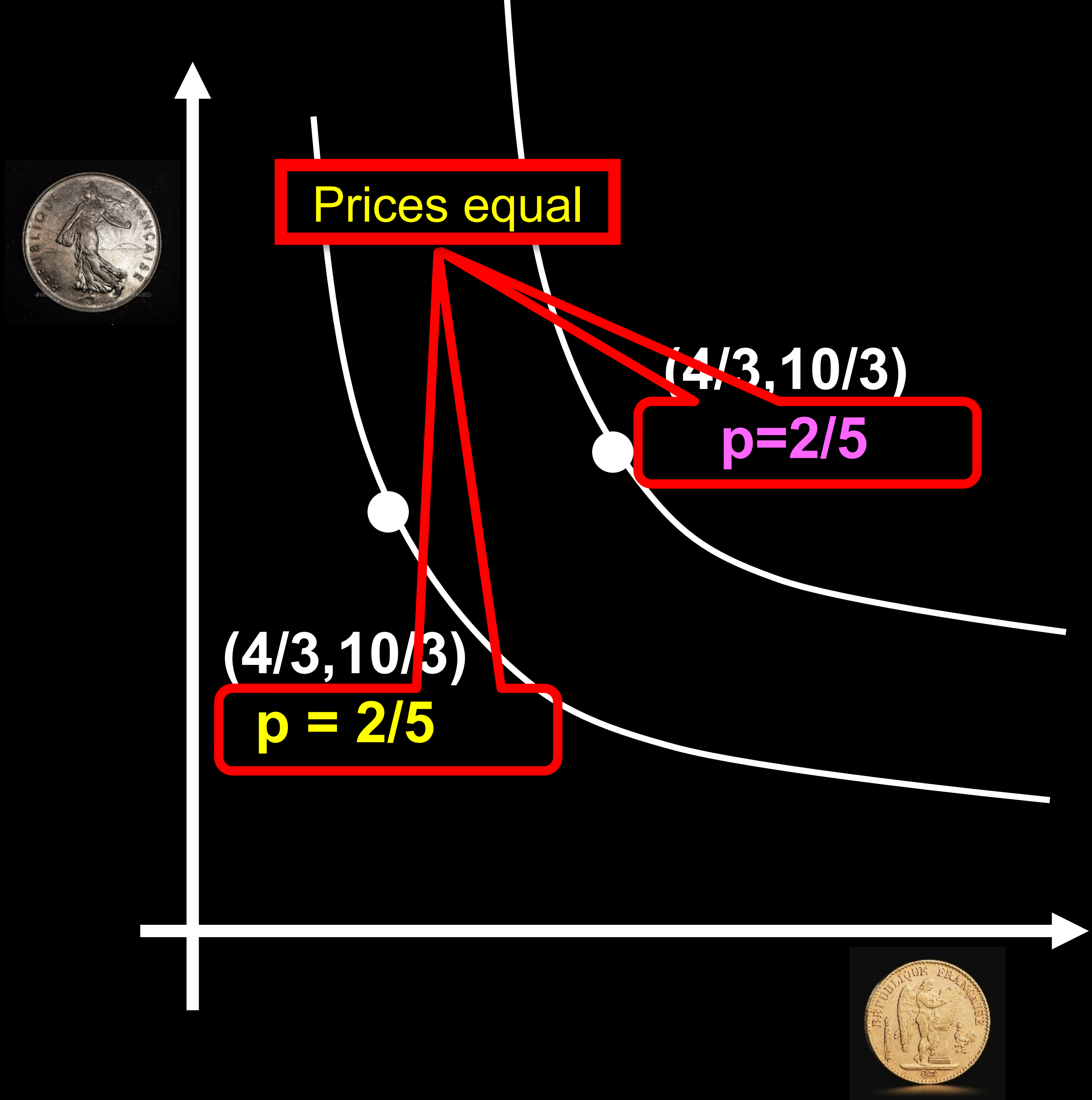
Is this outcome too good to be true?

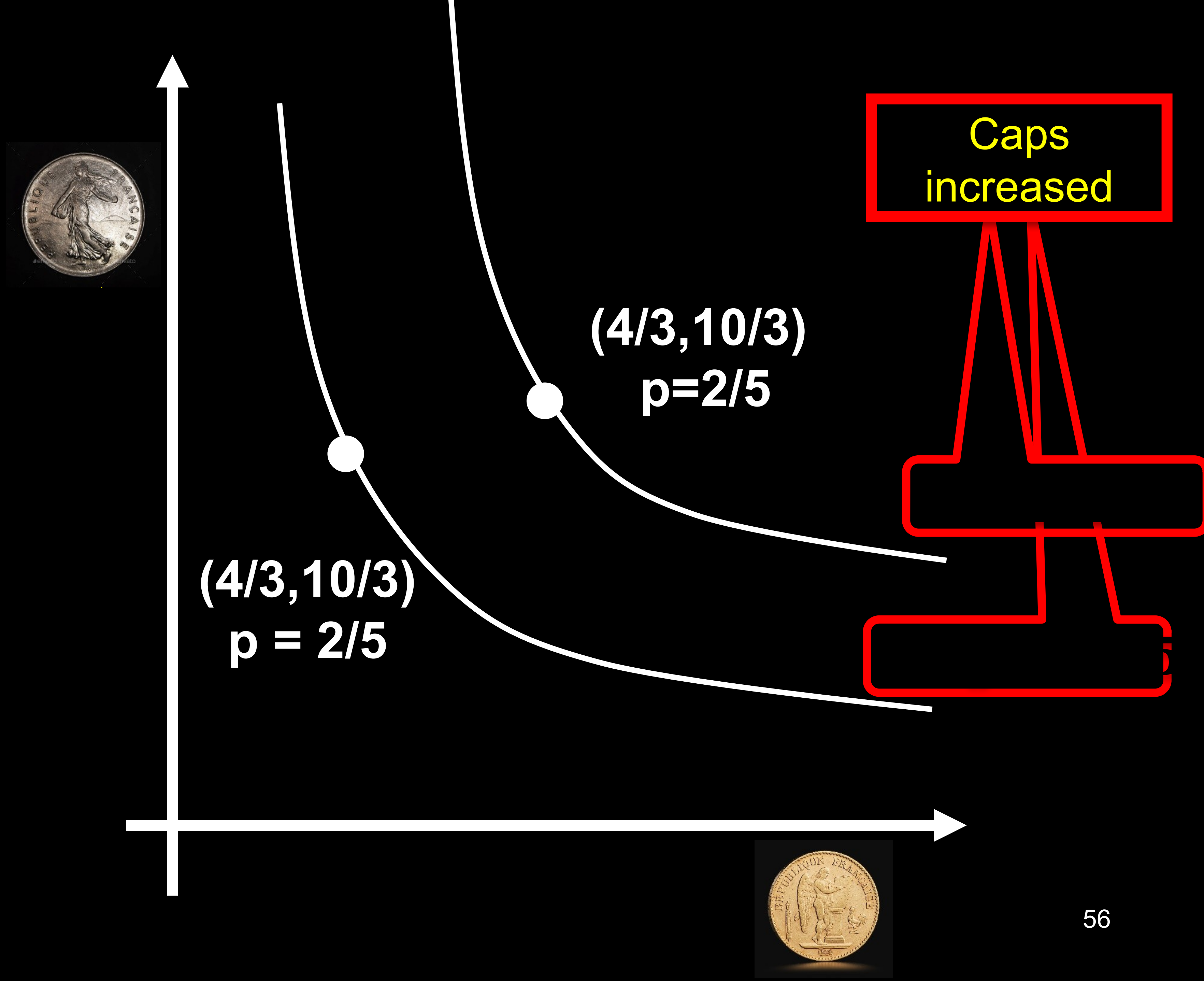

(1,4)
p = ¼
(1,1)
p = 1



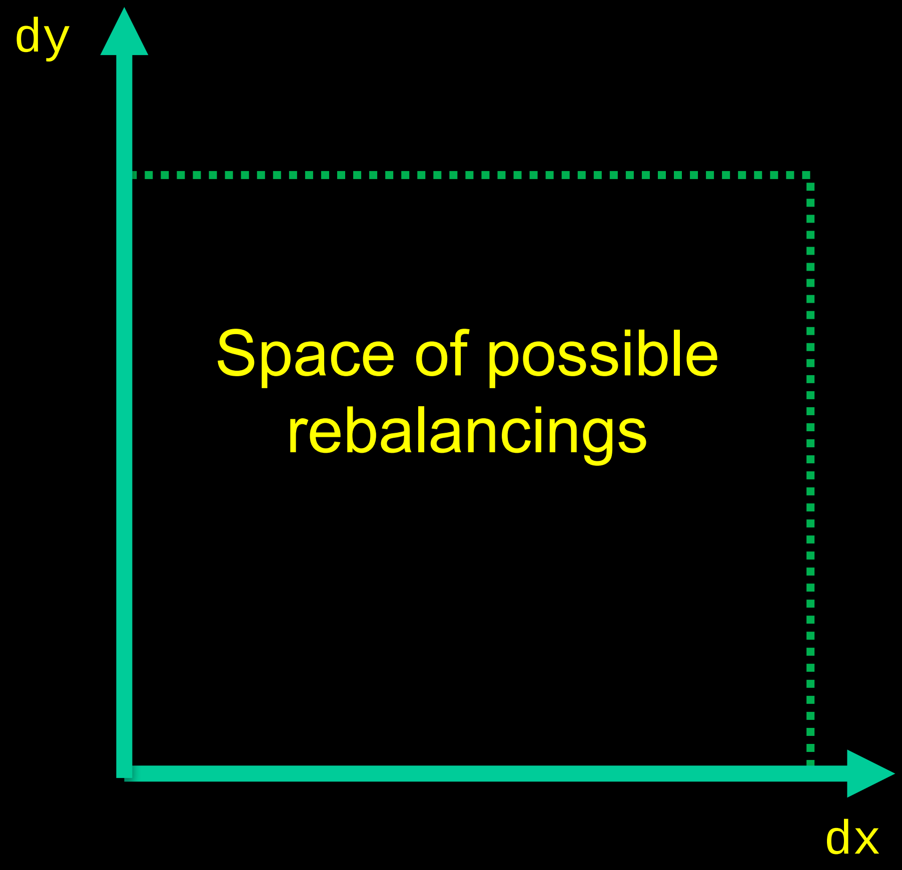



(4/3,10/3)
p=2/5
(4/3,10/3)
p = 2/5

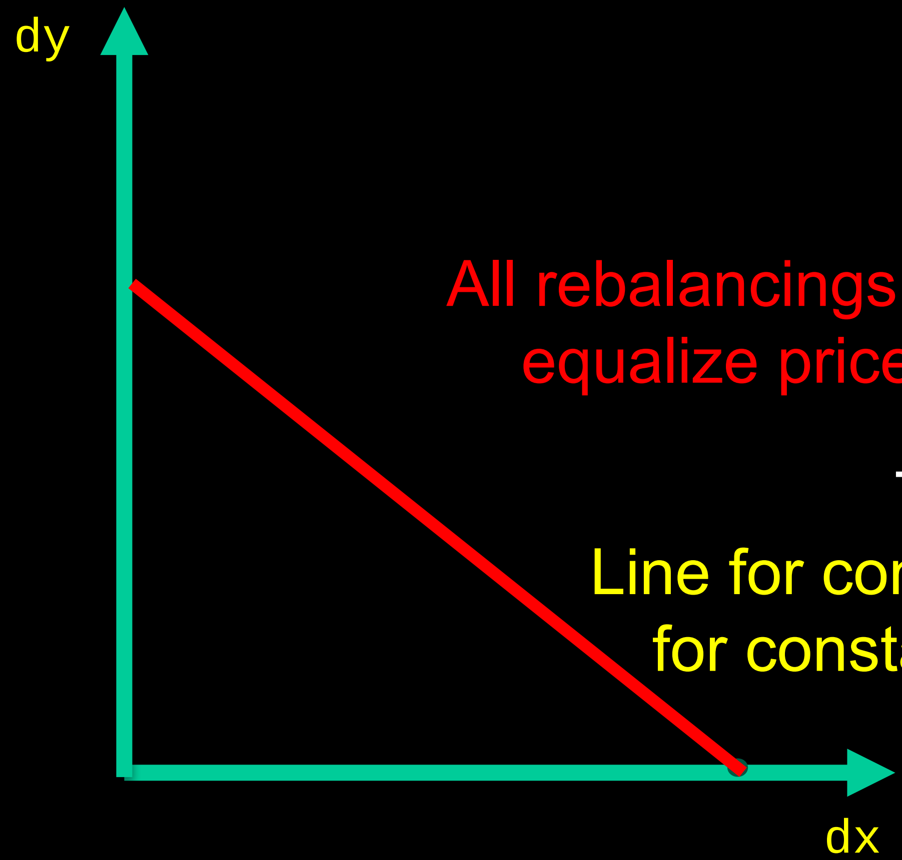

Prices equal
(4/3,10/3)
p=2/5
(4/3,10/3)
p = 2/5


Caps increased
(4/3,10/3)
p=2/5
(4/3,10/3)
p = 2/5

Theorem

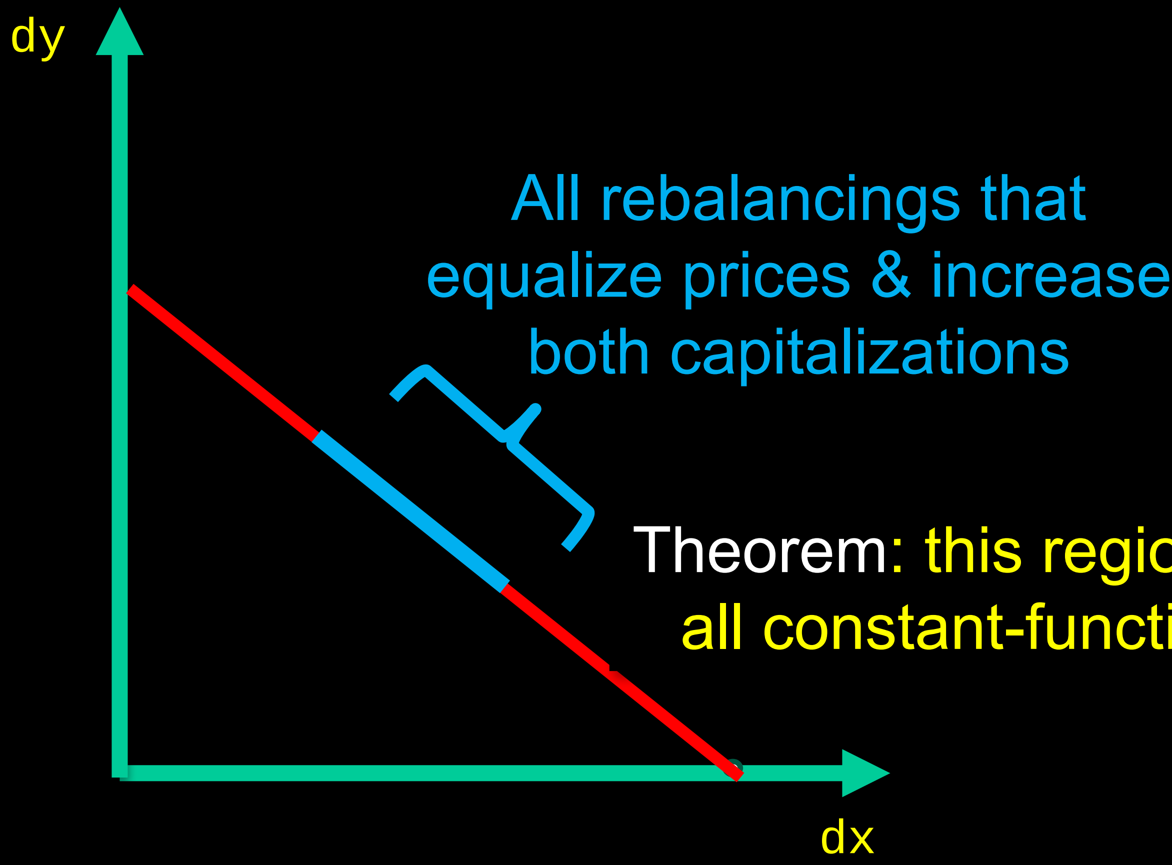


Theorem



Theorem:
Line for constant-product, curve for constant-function AMMs

Theorem



Theorem: this region exists for all constant-function AMMs

Convergence and Prices

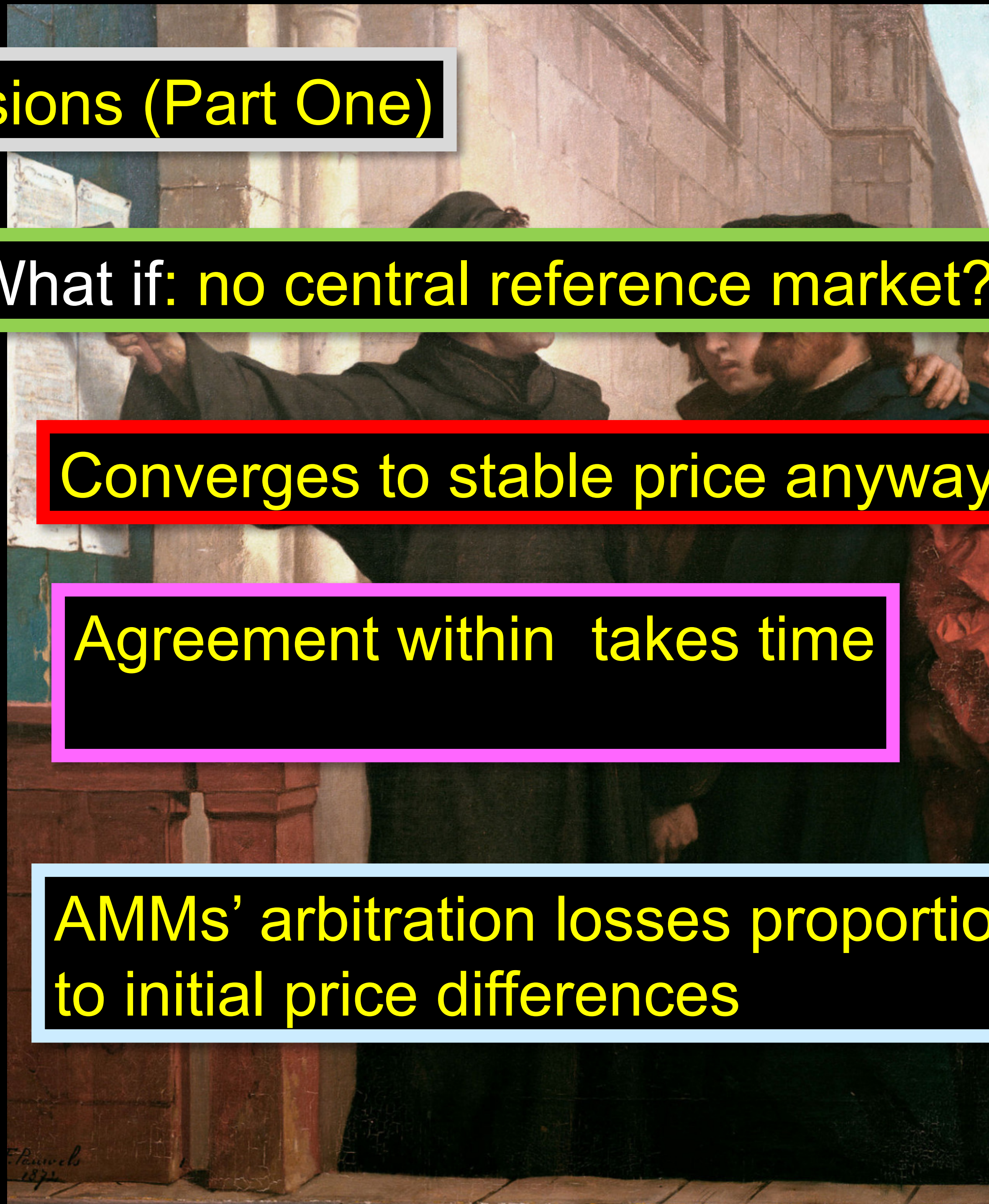
Convergence time to stable price:

Between $(n \log n)$ & $O(n^2 \log n)$

Formulas for stable states & prices:

Similar, not exactly the same

Conclusions (Part One)



What if: no central reference market?

Converges to stable price anyway

Agreement within takes time

AMMs' arbitration losses proportional to initial price differences

Conclusions (bis)

What if: AMM rebalance themselves?

Can avoid arbitrage losses

Possible to equalize prices &
increase both capitalizations!

Convergence, stable prices, etc.
similar to decentralized arbitrage


Ask me anything


REPUBLIQUE FRANÇOISE
24
LIVRES.
A
L'AN II.

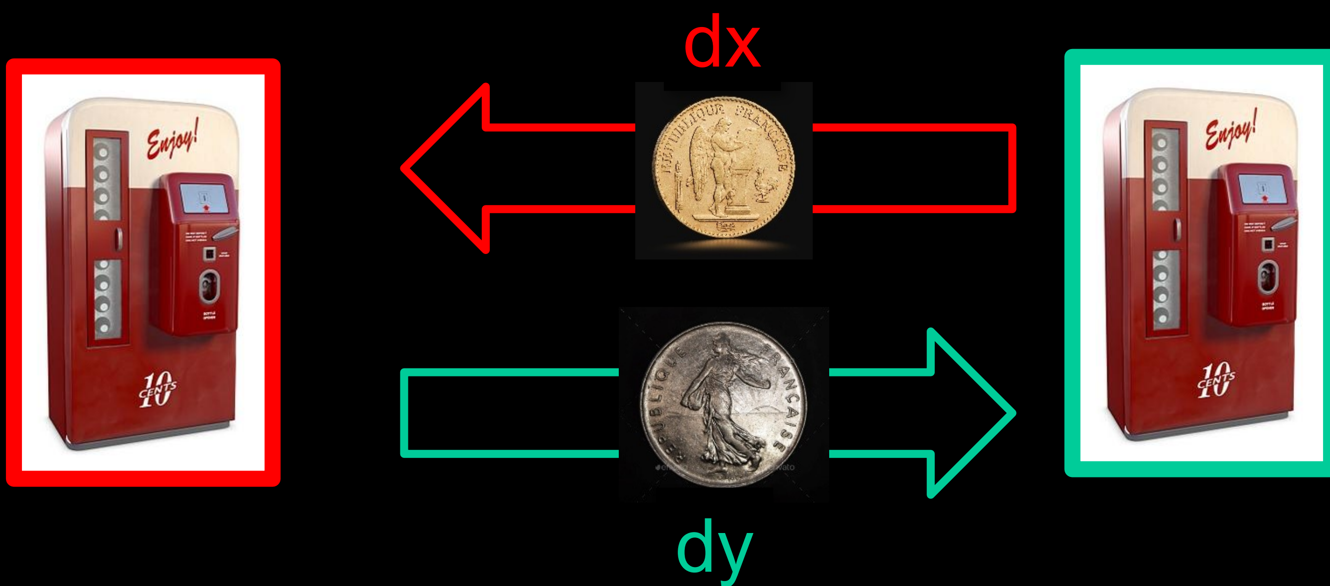

REPUBLIQUE FRANÇAISE


RÉPUBLIQUE FRANÇAISE

Let’s rebalance ourselves & keep the arbitrage profits!

Zut, alors!

Rebalancing



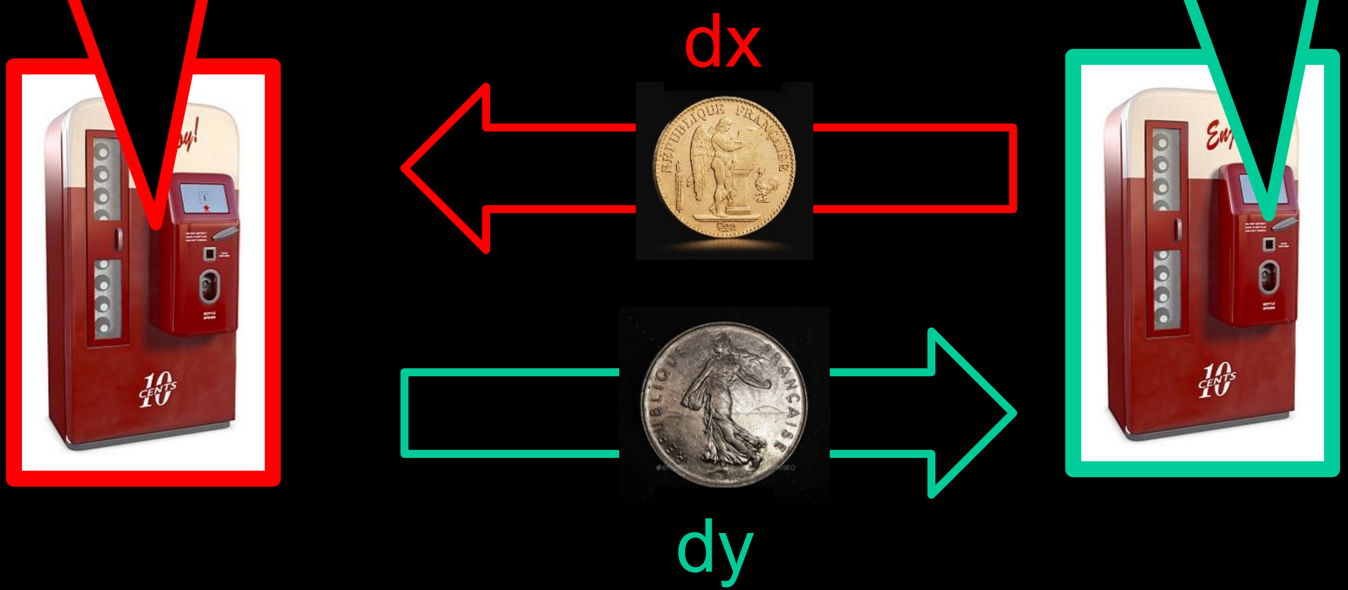
Spot Prices

Our prices agree!
Our prices agree!
dx
dy
Enjoy!
10 CENTS
Enjoy!
10 CENTS

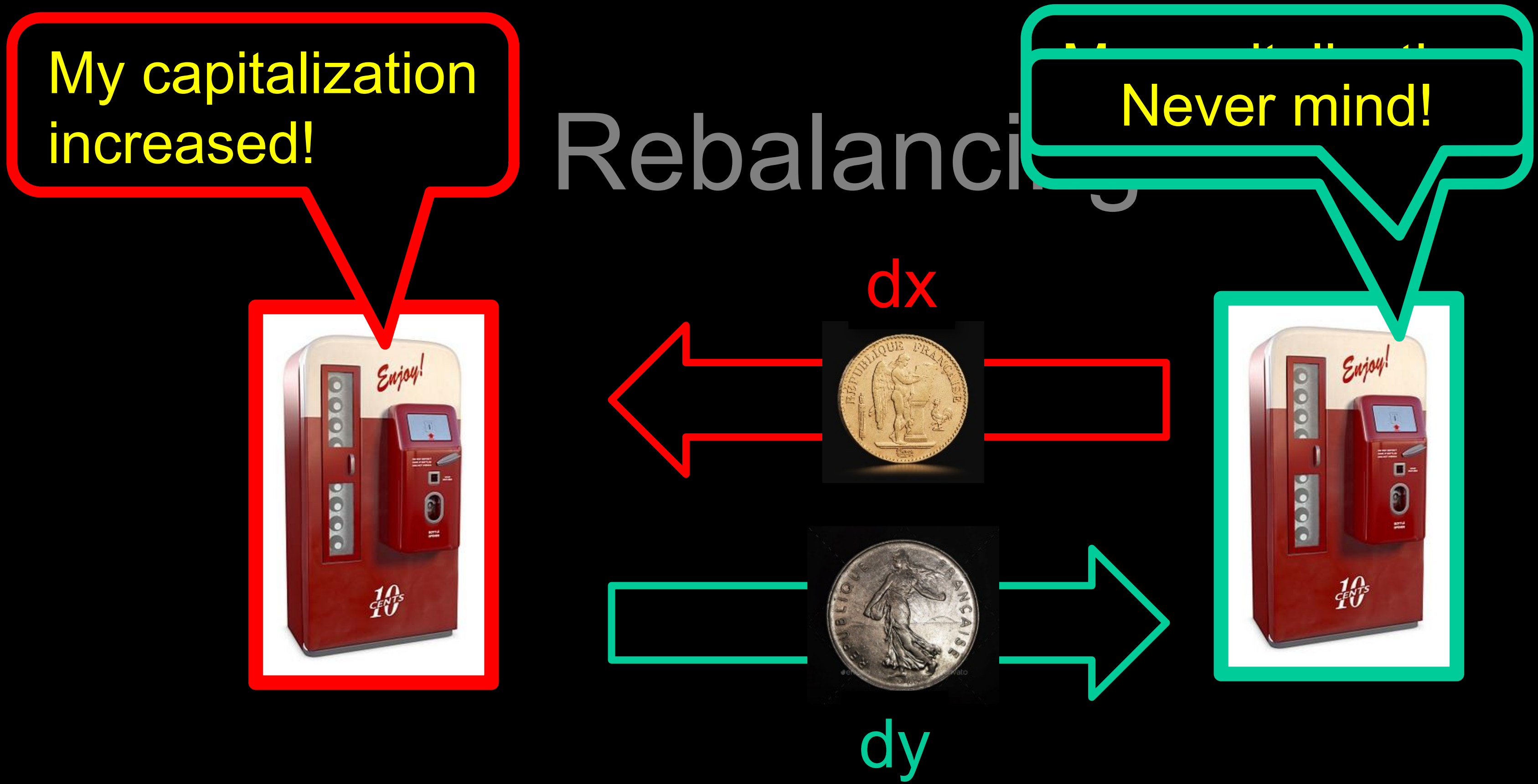
Capitalizat

Wait, my capitalization changed!

Wait, my capitalization changed!



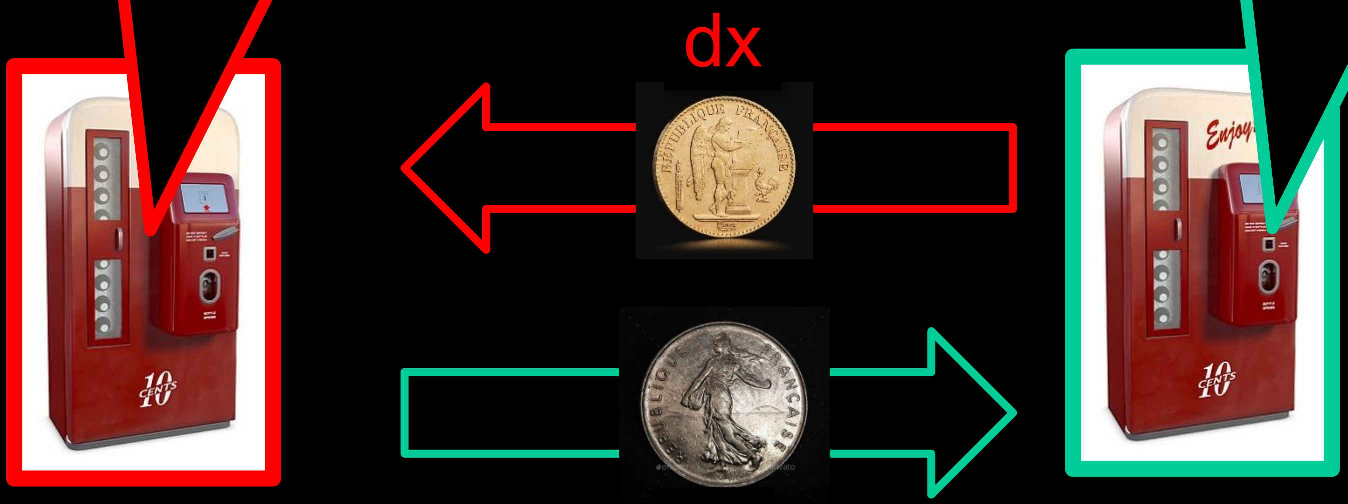
Rebalanci



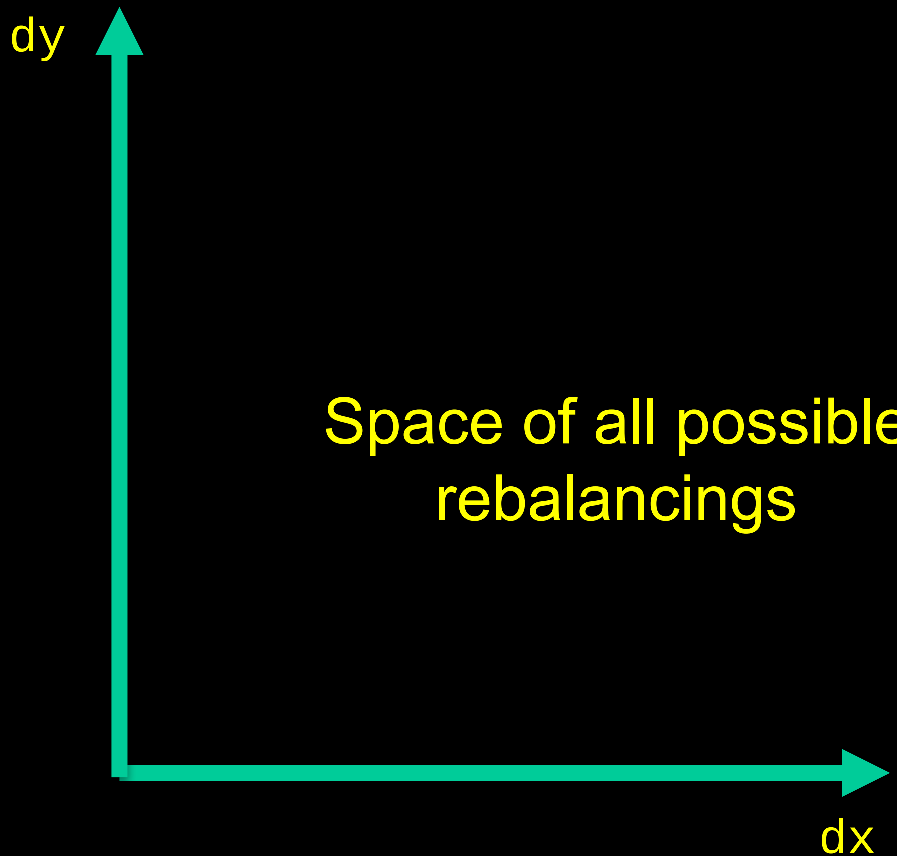
Prices equal & capitalization increased!

Win Rebal

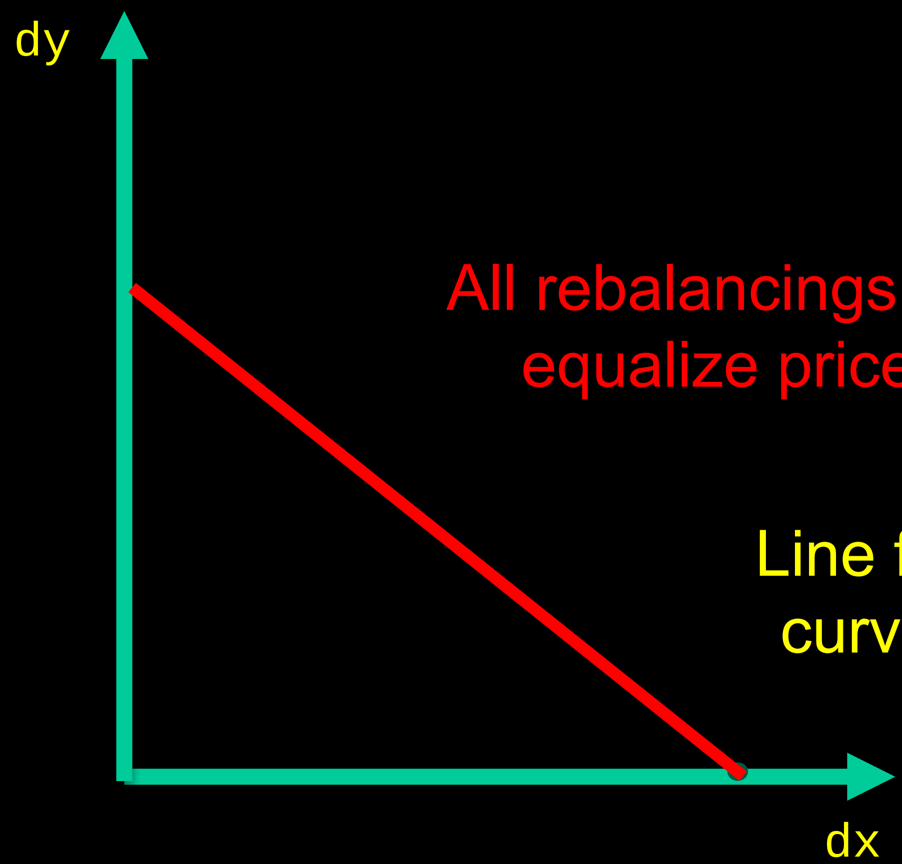
Prices equal & capitalization increased!



Theorem



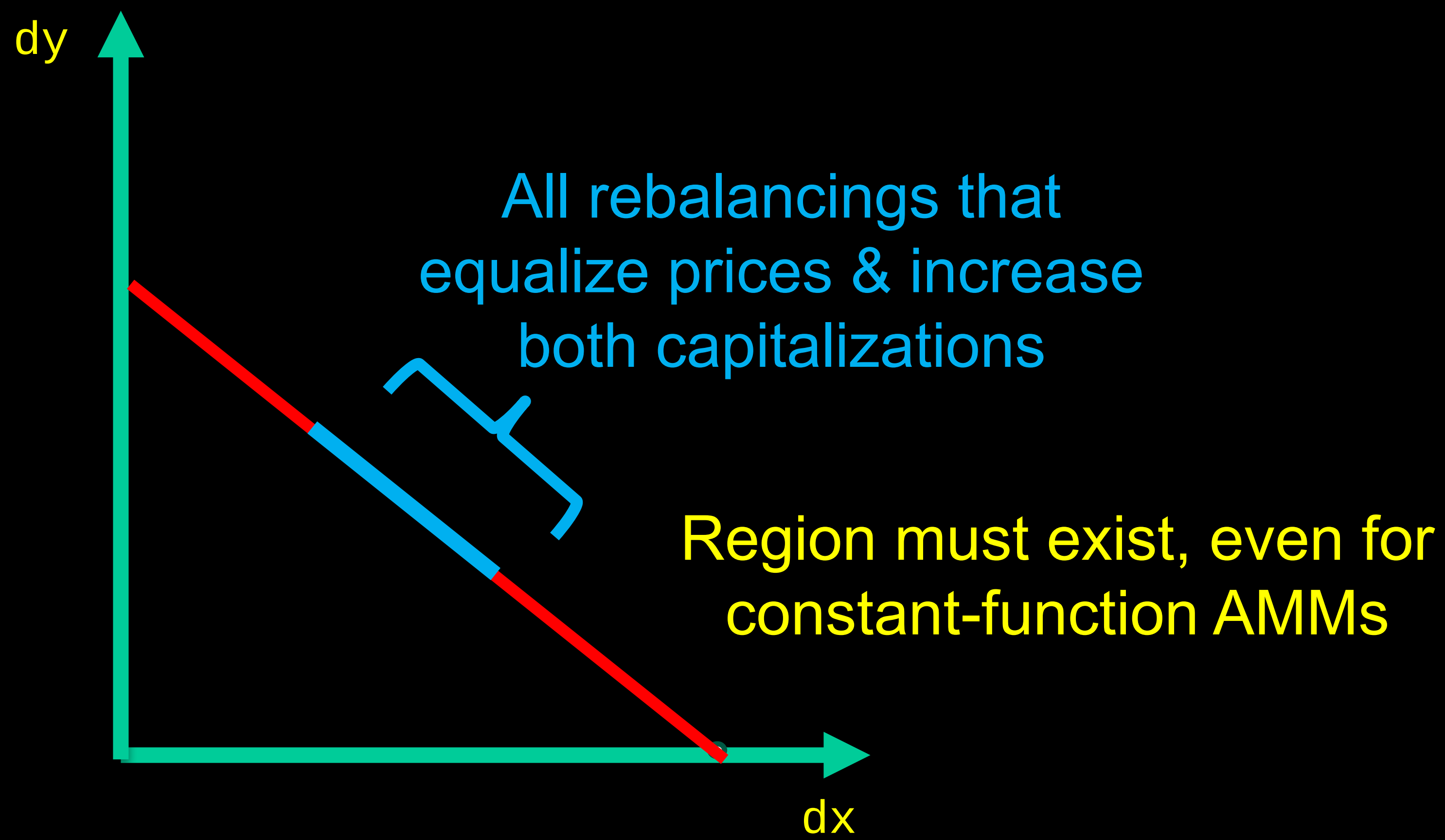
Theorem



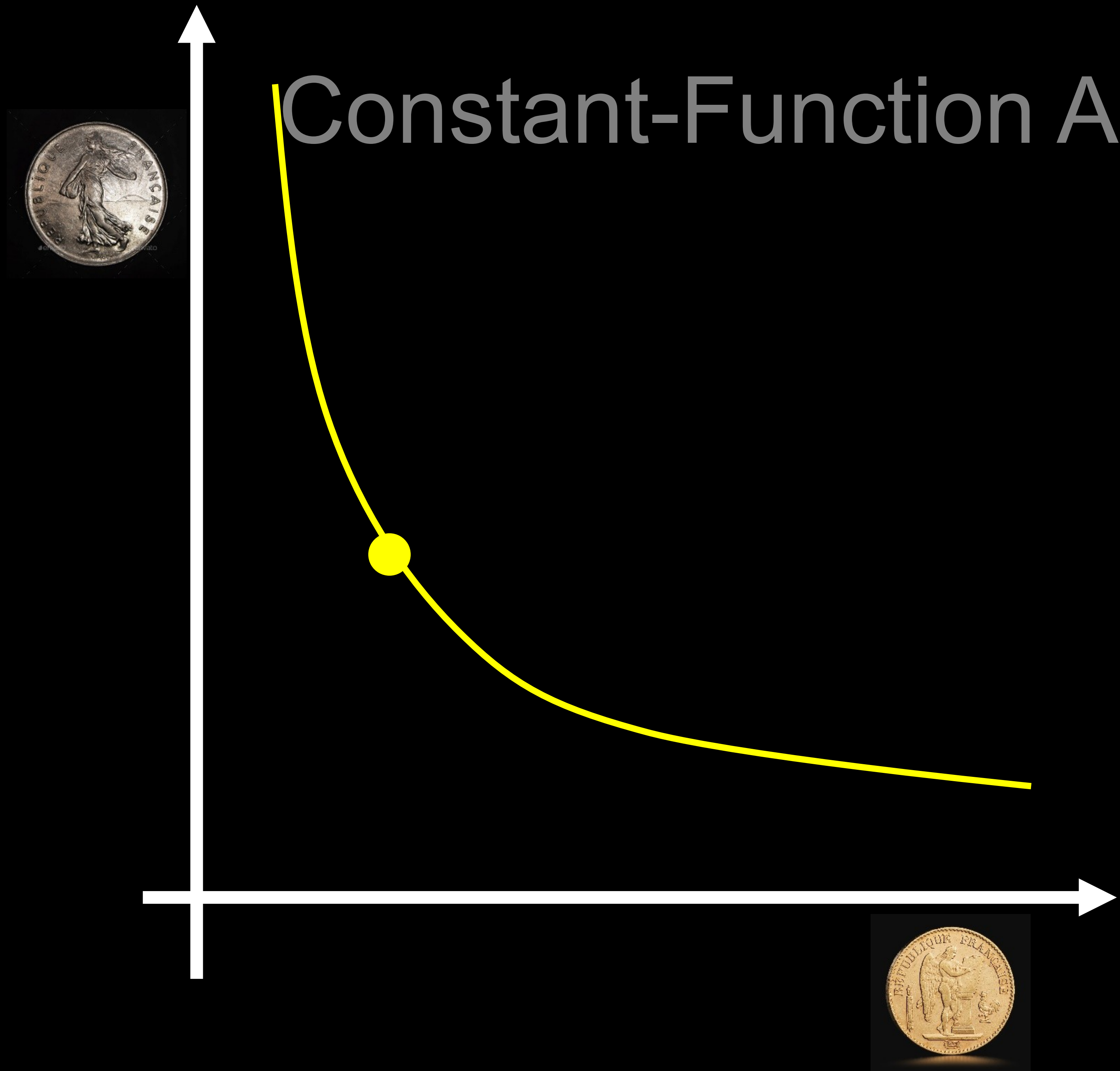
All rebalancings that equalize prices

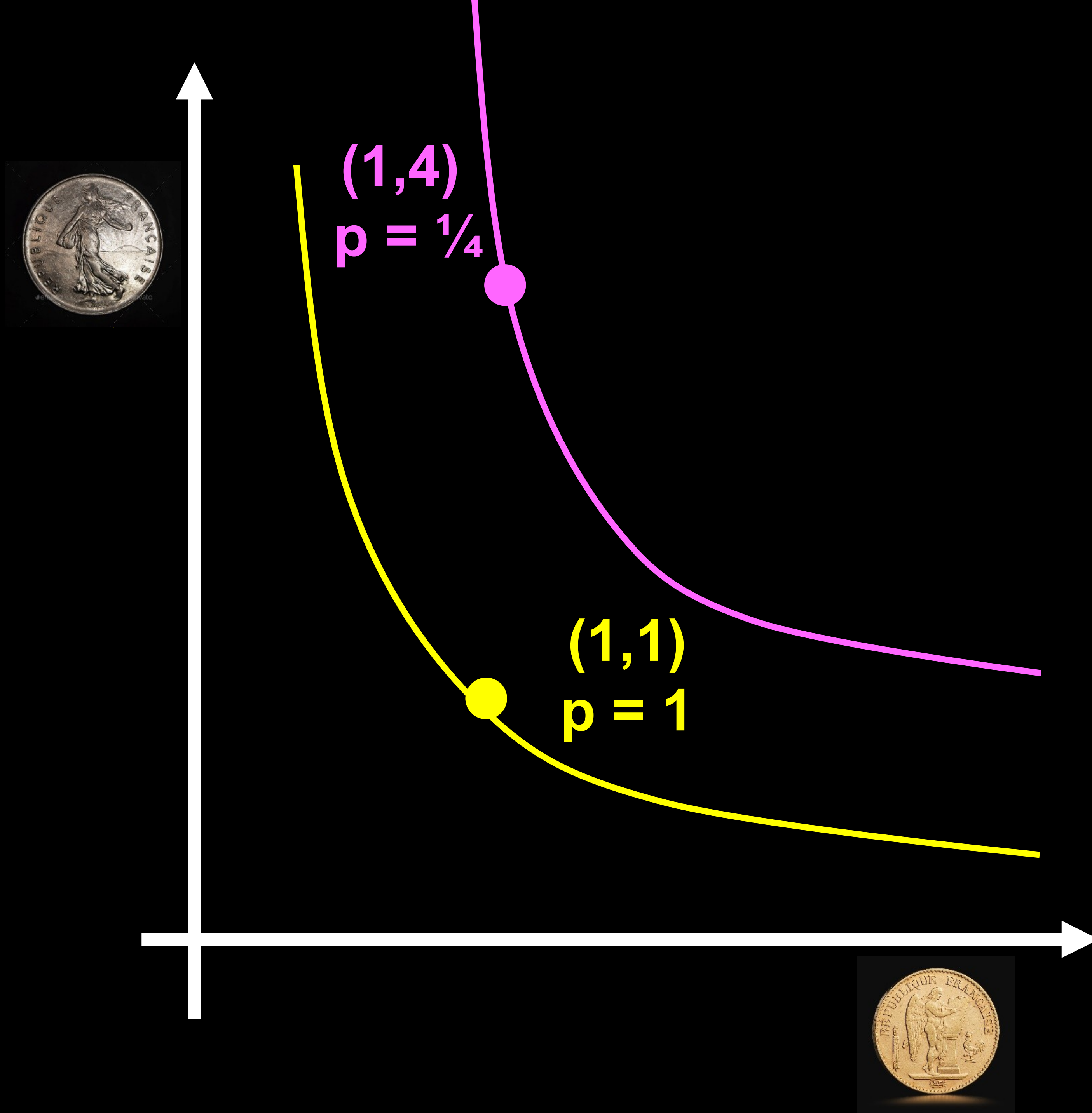
Line for constant-product, curve for general AMMs

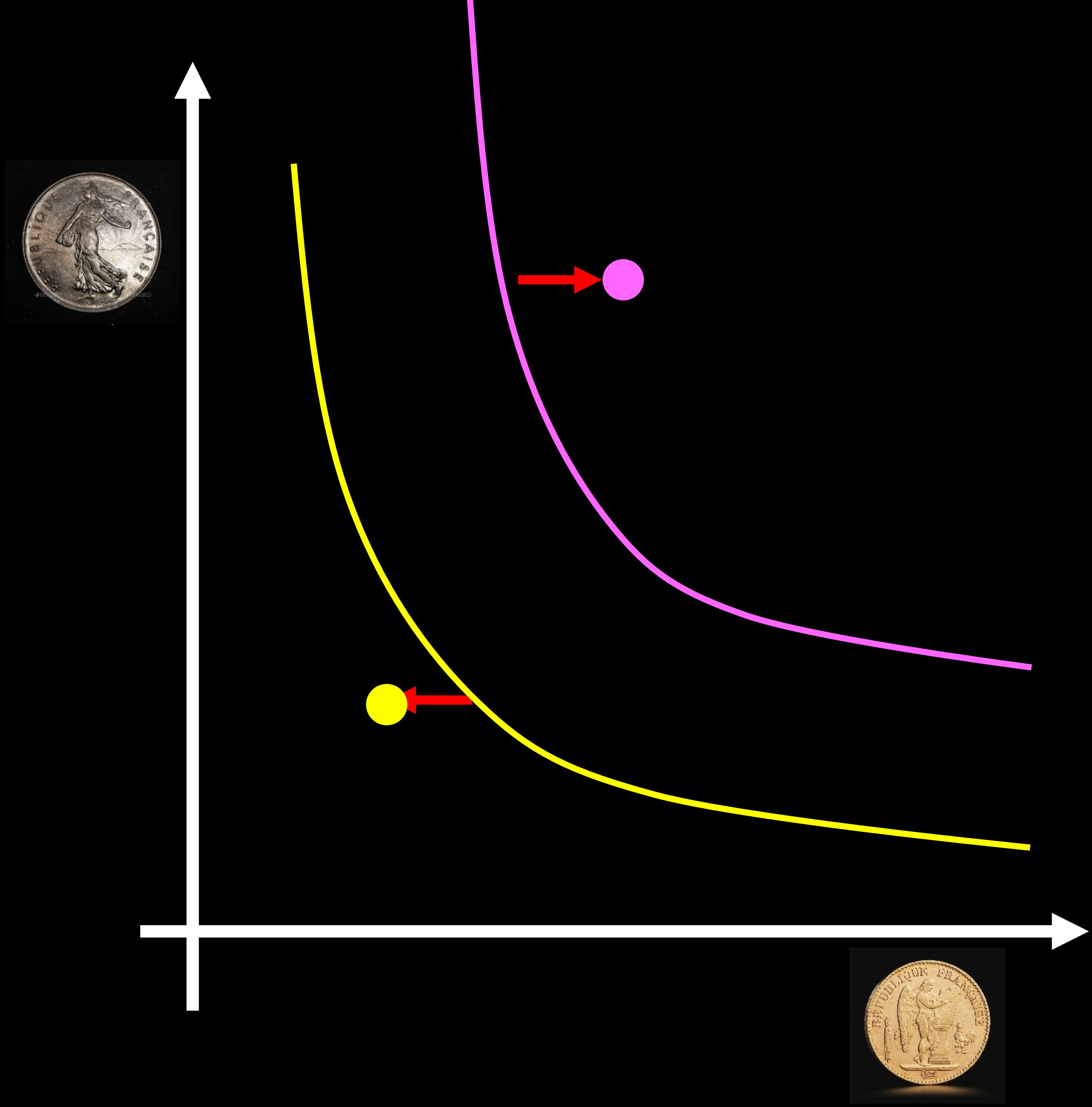
Theorem

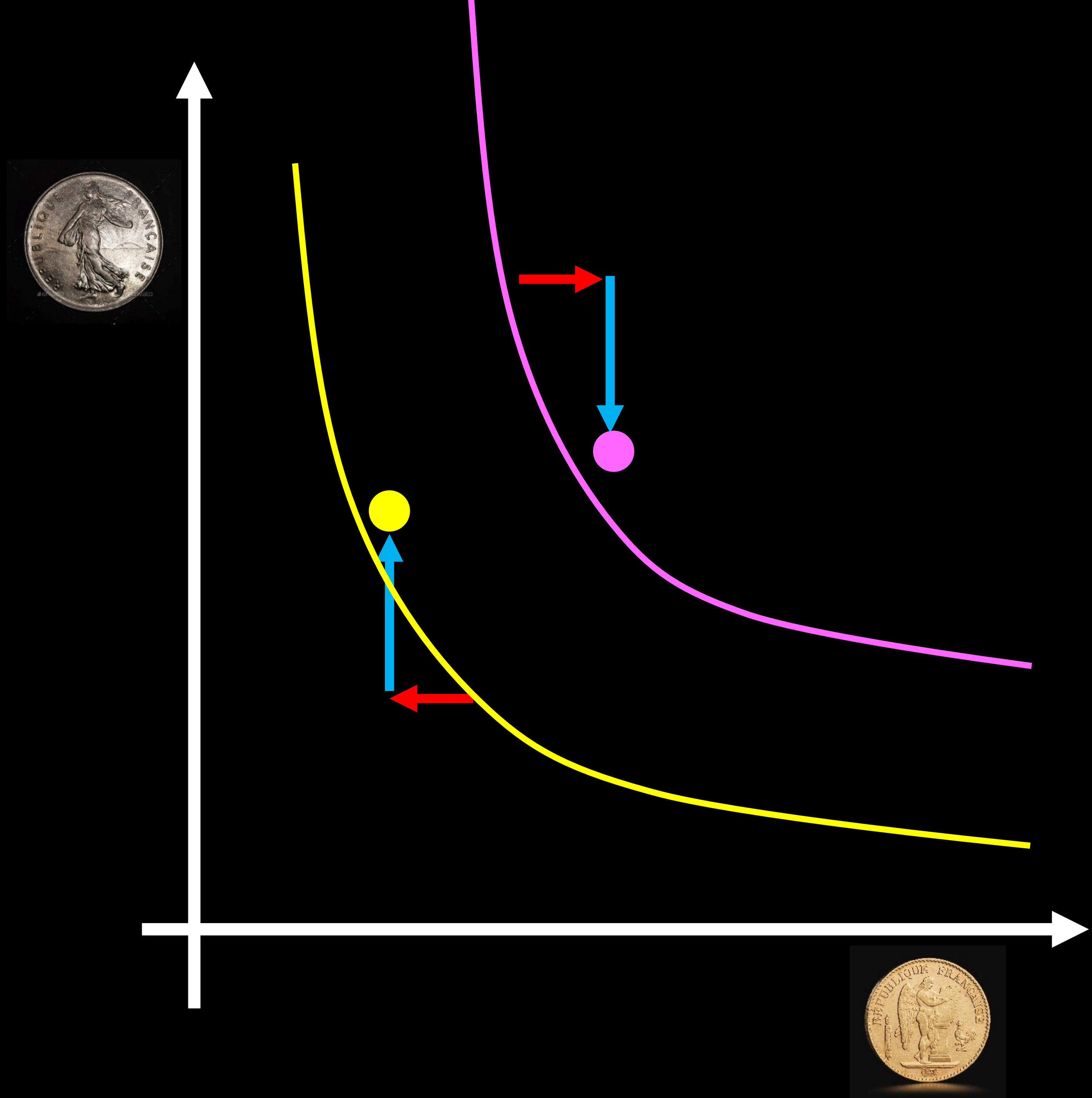

dy
dx
All rebalancings that
equalize prices & increase
both capitalizations
Region must exist, even for
constant-function AMMs

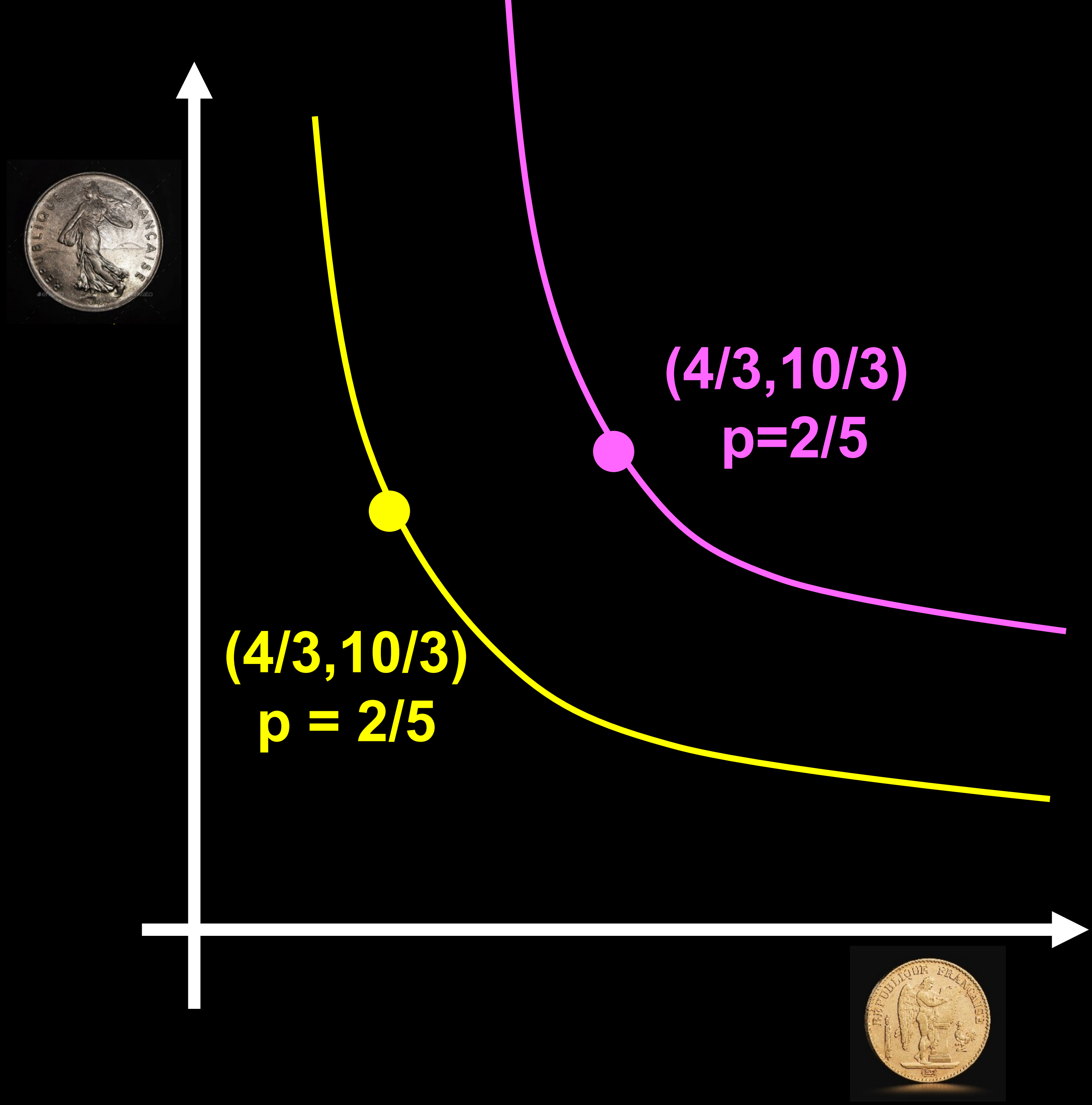
Constant-Function AMM

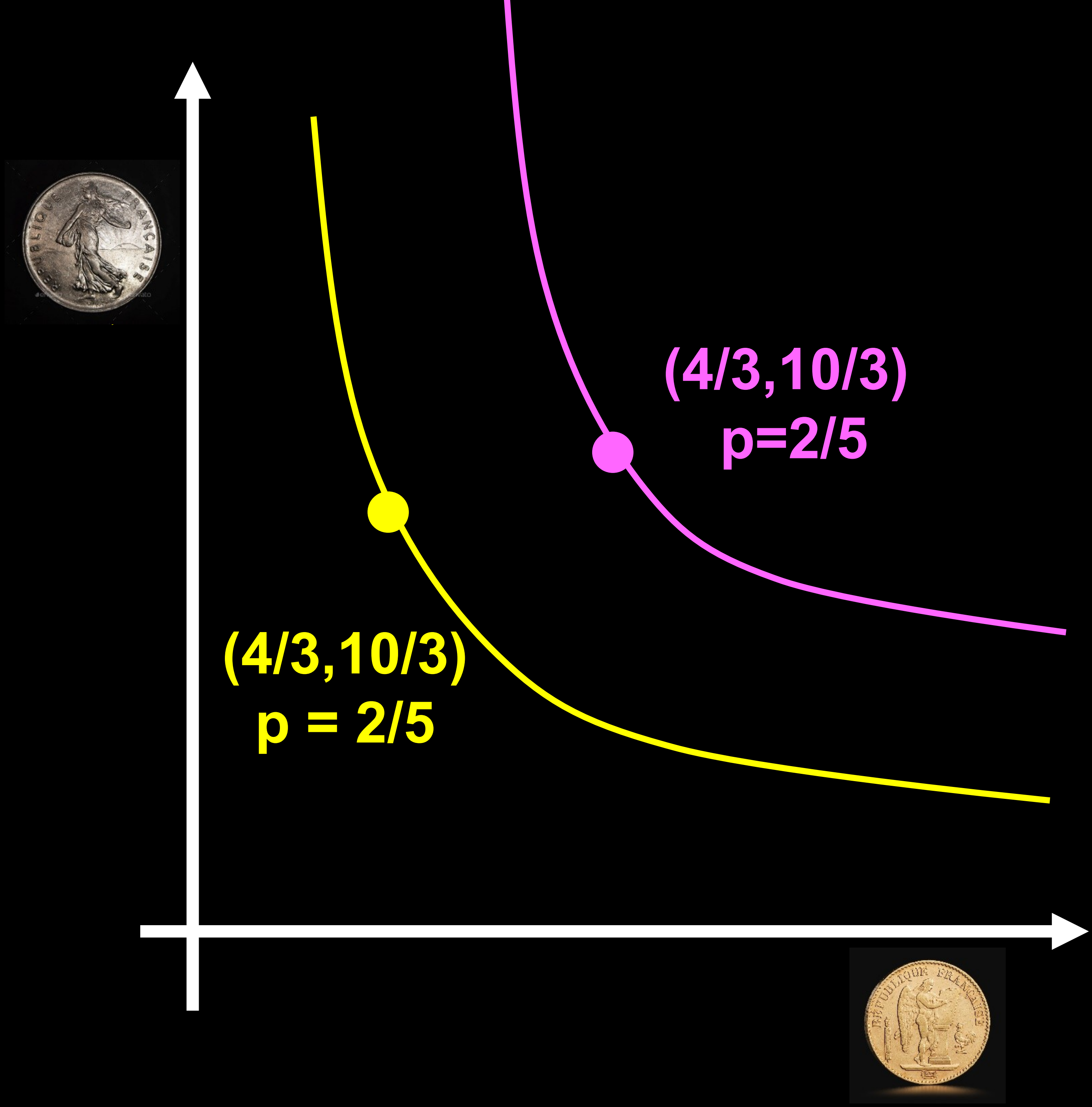


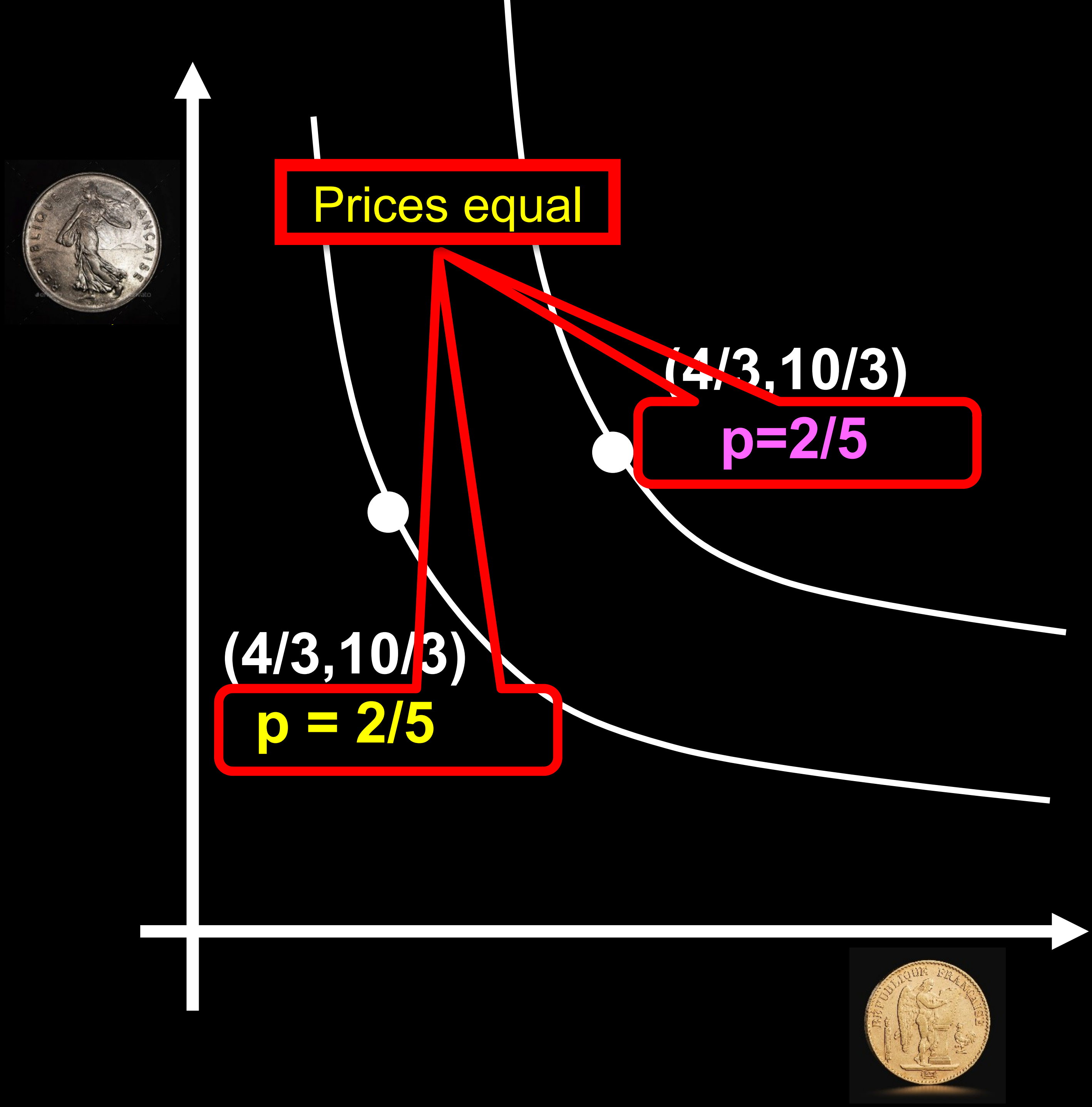

(1,4)
p = ¼
(1,1)
p = 1

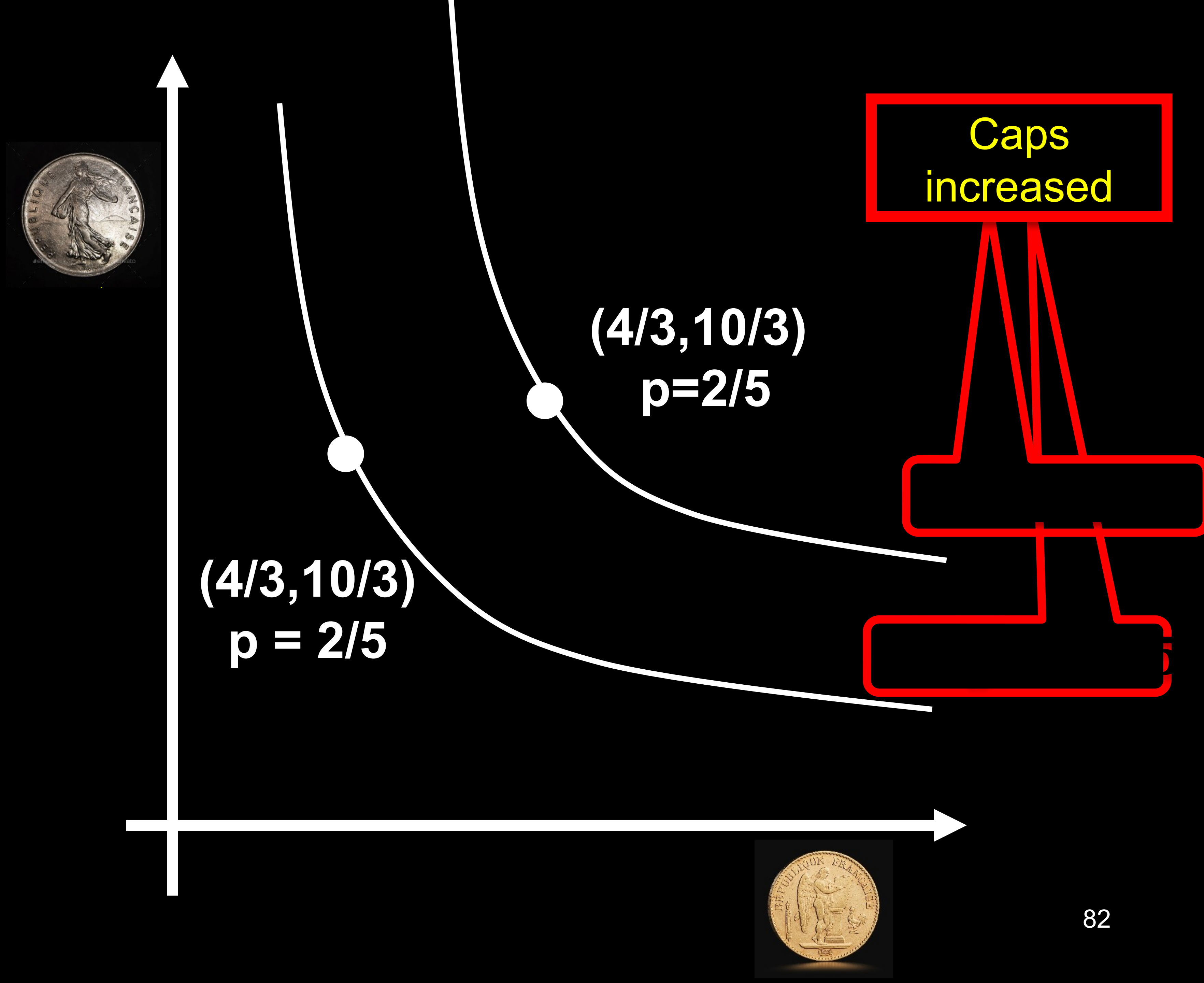


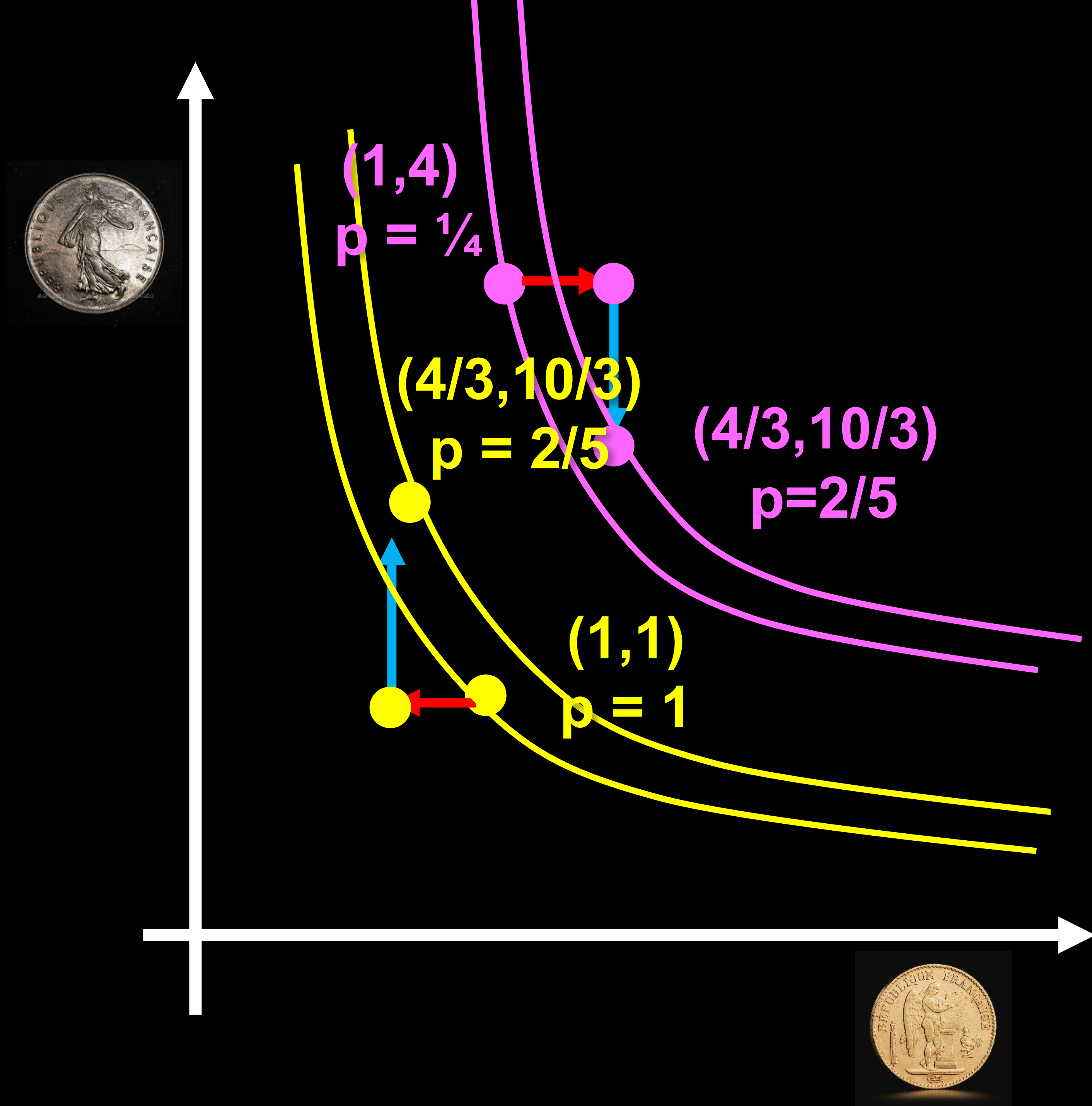



(4/3,10/3)
p=2/5
(4/3,10/3)
p = 2/5


(4/3,10/3)
p=2/5
(4/3,10/3)
p = 2/5


Prices equal
(4/3,10/3)
p=2/5
(4/3,10/3)
p = 2/5


Caps increased
(4/3,10/3)
p=2/5
(4/3,10/3)
p = 2/5


(1,4)
p = ¼
(4/3,10/3)
p = 2/5
(4/3,10/3)
p=2/5
(1,1)
p = 1