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)

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Increase</th>
<th>Decrease</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan. 1, 20X3</td>
<td>Balance forward</td>
<td>$</td>
<td></td>
<td>$50,000</td>
</tr>
<tr>
<td>Jan. 2, 20X3</td>
<td>Sold inventory</td>
<td>-</td>
<td>5,000</td>
<td>60,000</td>
</tr>
<tr>
<td>Jan. 3, 20X3</td>
<td>Cash sale</td>
<td>5,000</td>
<td></td>
<td>65,000</td>
</tr>
<tr>
<td>Jan. 5, 20X3</td>
<td>Paid rent</td>
<td></td>
<td></td>
<td>58,000</td>
</tr>
<tr>
<td>Jan. 6, 20X3</td>
<td>Paid salary</td>
<td></td>
<td>3,000</td>
<td>55,000</td>
</tr>
<tr>
<td>Jan. 8, 20X3</td>
<td>Paid bills</td>
<td>2,000</td>
<td></td>
<td>57,000</td>
</tr>
<tr>
<td>Jan. 10, 20X3</td>
<td>Paid tax</td>
<td>1,000</td>
<td></td>
<td>56,000</td>
</tr>
<tr>
<td>Jan. 22, 20X3</td>
<td>Collected receivable</td>
<td></td>
<td>7,000</td>
<td>63,000</td>
</tr>
</tbody>
</table>

- 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

<table>
<thead>
<tr>
<th>Currency</th>
<th>Code</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>EURO</td>
<td>EUR</td>
<td>0.6644</td>
</tr>
<tr>
<td>JAPAN</td>
<td>JPY</td>
<td>109.00</td>
</tr>
<tr>
<td>SINGAPORE</td>
<td>SGD</td>
<td>1.3712</td>
</tr>
<tr>
<td>HONG KONG</td>
<td>HKD</td>
<td>7.0043</td>
</tr>
<tr>
<td>NEW ZEALAND</td>
<td>NZD</td>
<td>1.646</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.2536</td>
</tr>
</tbody>
</table>
Our Electronic Assets

“gold”
stablecoin?
numéraire

“silver”
volatile
speculative
Automated Market Maker

I own “liquidity pools” of gold & silver
Automated Market Makers

Exchange rate is function of my pool sizes

Alice

Will trade silver for gold
Multi-Billion Dollar Business

UNISWAP

SushiSwap
Constant-Product AMM

All states lie on this curve
Constant-Product AMM

\[ \sqrt{xy} = 1 \]
Trade

\((\frac{1}{2}, 2)\) 1 gold in

\(\sqrt{xy} = 1\)
Trade

We ignore fees

\[
\sqrt{x} = 1
\]

(\frac{1}{2}, 2)

1 gold in

4/3 silver out

(\frac{3}{2}, \frac{2}{3})
Constant-Function AMMs

\[ f(x, y) = c \]

“trading function”

Well-behaved ...

“capitalization”

AMM’s wealth

Unchanged by trades

Changed by investment
Spot Price

Rate at which AMM trades infinitesimal amounts of gold for silver

\( f(x, y) = c \)
Classical AMM Theory

Requires a *central reference market*

Publishes prices for all assets

Parties can trade @ prices

Little or no slippage

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

CEX
Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX  AMM
Classical Arbitrage

1 silver = 1 gold
2 silver = 1 gold

CEX

AMM
Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX

ARB

AMM
Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX

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

1 silver = 1 gold

2 silver = 1 gold

CEX
Classical Arbitrage

1 silver = 1 gold

2 silver = 1 gold

CEX
Classical Arbitrage

2 silver = 1 gold

CEX

AMM
Classical Arbitrage

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

My spot price did not change!

I changed my spot price!

AMM
I maximize my profit when I make AMM & CEX prices equal. But I am paying for arbitrage! Eventual market efficiency.
Road Map

Background: Contracts, AMMs, etc.

What if: decentralized arbitrage?

What if: defensive rebalancing?
What If?
What If?

1 silver = 1 gold

1 silver = 2 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?

\[ (S_i(0), G_i(0)) \sim \left( \frac{C_i}{\sum_j C_j} \sum_j S_j(0), \frac{C_i}{\sum_j C_j} \frac{(\sum_j C_j)^2}{\sum_j S_j(0)} \right) \]

\( i^{th} \) AMM’s initial silver and gold pools
Convergence, but to What?

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

- $i^{th}$ AMM’s initial silver and gold pools
- All the silver
- All the remaining gold
Convergence, but to What?

Converges toward …

\[(S_i(0), G_i(0)) \sim \left( \frac{C_i}{\sum_j C_j} \sum_j S_j(0), \frac{C_i}{\sum_j C_j} \left( \sum_j C_j \right)^2 \left( \sum_j S_j(0) \right) \right) \]

\(i^{th}\) 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?

\[ \hat{P} = \frac{\left( \sum_i S_i(0) \right)^2}{\left( \sum_i C_i \right)^2} \]

Final price if arb profits in gold

\[ \hat{P}^* = \frac{\left( \sum_i C_i \right)^2}{\left( \sum_i G_i(0) \right)^2} \]

Final price if arb profits in silver

All points between if arb profits mixed
How much Gold does $AMM_i$ lose to Arbitrage?

\[ \frac{C_i}{S_i(0)} - \frac{\sum_j C_j}{\sum_j S_j(0)} \]

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

dx
Rebalancing

dx

dy
Our prices agree!

Spot Prices

Our prices agree!

(dx, dy)
Wait, my capitalization changed!

Capitalization

\[ \text{dx} \]

\[ \text{dy} \]

Wait, my capitalization changed!
Rebalancing

Never mind! Rebalancing is too expensive.

Oh, no! My capitalization decreased!

Oh yes! My capitalization increased!
Win-Win Rebalancing

Prices equal & capitalization increased!

Prices equal & capitalization increased!

Is this outcome too good to be true?
\[ \sqrt{xy} = 1.05 \]
\[ \sqrt{xy} = 2.1 \]

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

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

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

p = 2/5

√\( xy \) = 1.05

√\( xy \) = 2.1

Prices equal
(4/3, 10/3) 

$p = 2/5$

Caps increased
Theorem

Space of possible rebalancings
Theorem

All rebalancings that equalize prices

Theorem:
Line for constant-product, curve for constant-function AMMs
All rebalancings that equalize prices & increase both capitalizations

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
Let’s rebalance ourselves & keep the arbitrage profits!

Zut, alors!
Rebalancing

dx

dy
Spot Prices

Our prices agree!

dx

dy

Our prices agree!
Wait, my capitalization changed!

Wait, my capitalization changed!

dx

dy
My capitalization increased!

Never mind!
Prices equal & capitalization increased!

Prices equal & capitalization increased!
Theorem

Space of all possible rebalancings
Theorem

All rebalancings that equalize prices

Line for constant-product, curve for general AMMs
All rebalancings that equalize prices & increase both capitalizations

Region must exist, even for constant-function AMMs
Constant-Function AMM

\[ f(x, y) = c \]
\[(1, 4) \quad p = \frac{1}{4}\]

\[(1, 1) \quad p = 1\]
\sqrt{\frac{\Delta t}{\Delta x}} = \frac{1}{\sqrt{\frac{\Delta y}{\Delta x}}} = \frac{1}{2}
\[ \sqrt{xy} = 0.5 \]
\[ \sqrt{xy} = 2.1 \]

\((4/3, 10/3)\)

\(p = 2/5\)

\((4/3, 10/3)\)

\(p = 2/5\)
\[ \sqrt{xy} = 0.5 \]
\[ \sqrt{xy} = 2.1 \]

Point: \((4/3, 10/3)\)

\[ p = \frac{2}{5} \]
Prices equal

\( \sqrt{xy} = 1.05 \)

\( \sqrt{xy} = 2.1 \)

\((4/3, 10/3)\)

\( p = 2/5 \)
\[
\sqrt{xy} = 1.
\]
\[
\sqrt{xy} = 2.
\]

(4/3,10/3)

\[ p = 2/5 \]

Caps increased
\[(1,4)\]
\[p = \frac{1}{4}\]

\[(4/3, 10/3)\]
\[p = \frac{2}{5}\]

\[(4/3, 10/3)\]
\[p = \frac{2}{5}\]