Quantitative modelling of risks in Decentralized Finance

Emmanuel Gobet

SORBONNE UNIVERSITÉ

LPSM LABORATOIRE DE PROBABILITÉS STATISTIQUE & MODÉLISATION

Kaiko

September 2nd, 2025

Several co-authors: Ankush Agarwal, Michael Allouche, Mnacho Echenim, Louis Latournerie, Anne-Claire Maurice, Anastasia Melachrinos, Benoit Nieto, Ju-Yi Yen, Ruixun Zhang, . . .

International Conference on Stochastics and Computational Finance 2025 - Lisbon

Papers on my webpage and on https://hal.science/

Supported by the ANR "BlockFi" 2024-2028

anr agence nationale de la recherche

Acknowledgement of the support of Kaiko for data and expertise

The context of crypto-assets and digital assets

For more details on blockchain infrastructure/actors/markets, see our tutorial at SIAM FME Philadelphia, June 2023, [GM23]

Bitcoin's Goal

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

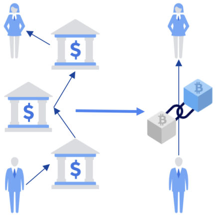
2009

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Source: Nakamoto, S. (2008). Bitcoin whitepaper. URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019).

What is bitcoin about ?

Bitcoin is a peer-to-peer form of digital cash, enabling one individual to **transfer value** to another digitally **without the need for specific third-party intermediaries** to approve or deny the transaction.



A Revolution for trust, privacy, and security.

About Blockchain and its Evolution

Bitcoin

Bitcoin allows transfers between users. It is like having a software that can do only one thing: **transactions**

Would be possible to have more features ? To allow more actions than simple transactions ?

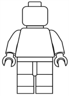
Ethereum

The Ethereum blockchain was born a few years after bitcoin, in **2014**.

The native crypto of that chain is called ether **(ETH)**.

Ethereum also allows direct **transactions** between users, but there is a major change: **Ethereum allows computer programs to run directly on the blockchain !**

What is a smart contract?



Hey, I'm a smart contract.

I promise you the following

1. **Immutable.** I will never modify or change your code.
2. **Authenticated calls.** I will always run the function you tell me too (assuming the code allows me!).
3. **Atomic.** I will never let code execution "stop half way" it is ALL or NOTHING with me.
4. **No privacy.** I like to gossip and I can't keep secrets - Everything you tell me will be public knowledge.

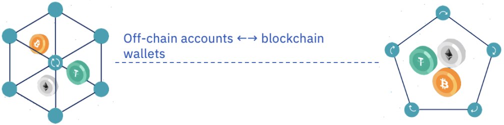
Other examples of Blockchain: Binance Smart Chain, Polygon, Avalanche, Tezos . . .

On-chain operations, in real time, at https://txstreet.com

Differences between CEX and DEX

✓ CEX=Centralized Exchanges (off-chain): Binance, Coinbase $\cdots$

✓ DEX=Decentralized Exchanges (on-chain): smart contracts $\cdots$



Centralized Exchanges (CEXs)

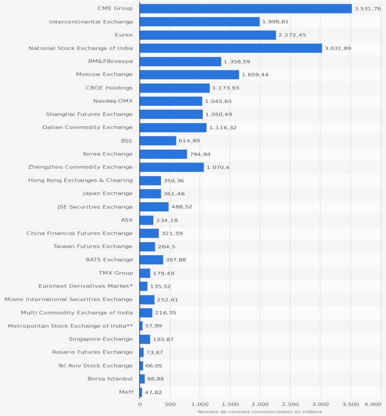
- Centrally managed (off-chain)
- Exchange controls your assets
- Listing fees and due diligence for new trading pairs
- Regulatory jurisdictions and KYC
- Barriers to market making
- Uses an order book
- You cannot trade if the exchange is down

Decentralized Exchanges (DEXs)

- Decentralized protocol (on-chain)
- You control your assets
- Anyone can list a pair by creating a new liquidity pool
- No regulation or KYC
- Anyone can be a market maker
- Automated Market Maker
- Data recorded directly on the blockchain

Traditional Finance: a few big centralized exchanges

Main exchanges for derivatives in the work in 2015, in terms of number of contracts (in millions) - SOURCE: Futures Industry Association

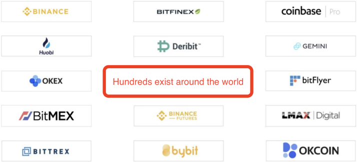


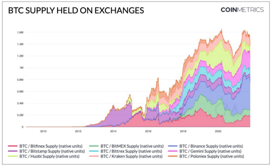
▷ One asset ≈ one exchange ≈ one price at a given time

The market organisation is concentrated around few places.

Crypto Finance: fragmented market

✓ Centralized Exchanges (off-chain)





✓ Decentralized Exchanges (on-chain):

# Trades	Exchange	# Pools	%	# Mints	# Burns
960924	curv	344	0,16%	566152	421482
1398792	blc2	1275	0,59%	93864	44279
471382	crv2	18	0,01%	18261	11276
114814668	usp2	195403	90,03%	3924111	1740615
11976425	sush	3684	1,70%	531695	308206
32452350	usp3	13037	6,01%	1108823	1242071
2787827	blcr	3291	1,52%	305293	200417

Number of trades and liquidity pools, by decentralized exchange, on Ethereum

✓ About 1700 cryptocurrencies traded on a daily basis

See AMM in the last part of the talk.

It's a bit like the Wild West!!

lack of standardization, only a part is regulated, a lot of freedom (the spirit of libertiarism) in the design of new activitiess/services owing to the blockchain, many innovations, new space for quantitative modelling ...

It's a bit like the Wild West!!

lack of standardization, only a part is regulated, a lot of freedom (the spirit of libertiarism) in the design of new activitiess/services owing to the blockchain, many innovations, new space for quantitative modelling ...

However...

On the other hand, regulators/banks are currently taking measures regarding the trading and investment of digital assets:

- ✓ 2025, August 7 about pension funds: "Trump on Thursday signed an executive order that allows 401(k) accounts to invest in alternative assets"
- ✓ 2025, July 18: The GENIUS Act (Guiding and Establishing National Innovation for U.S. Stablecoins Act) was signed into law by President Trump
- ✓ 2025 June: Recommendations about risk management of digital assets issued by ESMA, EIOPA, EBA in Europe
- ✓ 2023 November about CBDC and DeFi AMM: Project Mariana between BIS, Banque de France, Monetary Authority of Singapore, Swiss National Bank
- ✓ Since 2023, Canton Network (BNP Paribas, Goldman Sachs, UBS, Deutsche Börse, Moody's, Cboe, ...): public-permissioned blockchain
- ✓ Bank projects: Forge (Société Générale), JPMorgan (Onyx), Citigroup (Citi Token Services), Bank of America, Börse Stuttgart Digital, etc

Aim of this talk

Overview of quantitative issues met in this emerging field

Guided tour in selected topics:

- ✓ Market data and statistical modelling
- ✓ Lending-borrowing protocols
- ✓ Automated Market Maker

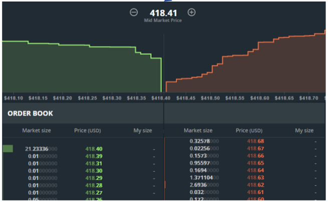
Please feel free to contact me if you look for a PostDoc position in that context, with expertise in statistics, risk modeling, computer science...

What is the price of an asset or the rate between tokens X/Y?

▷ Limit Order Book in Traditional Finance

Mid Price

Makers
Provide liquidity by placing sell orders

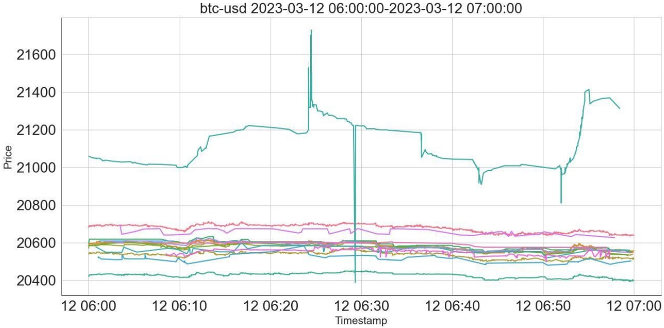


Takers
Take liquidity by placing buy orders

A trade occurs if the buy / sell orders match up

▷ Look at the exchange trading the asset and collect the price !!

▷ What is the "market consensus" price for a digital asset in a fragmented market?



Example of time-series for a given pair on different CEXs.
For AMM on DEX, see later.

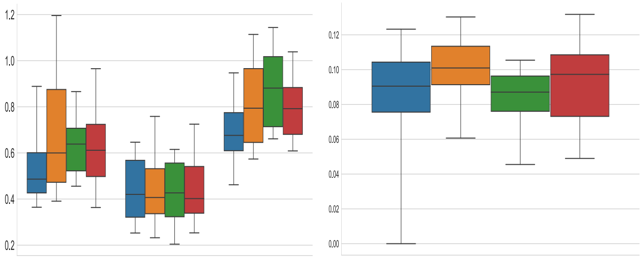
Understanding data characteristics

Using Kaiko's Instrument Explorer `https://instruments.kaiko.com/#/instruments` and Trades product `https://docs.kaiko.com/#historical-trades`.

- ✓ 67 pairs during 4 different days, including both stressed (2022-05-05, 2022-06-12) and calm (2022-06-28, 2022-12-09) periods in the market.
- ✓ 268 use cases (one pair for one period) for a total of 80,448,919 trades.

	Number of trades		Returns		
Period	Mean	Std.	Mean	Std.	Ann. Vol.
2022-05-05	96	156	$-0.44 \cdot 10^{-4}$	$8 \cdot 10^{-4}$	55%
2022-06-12	188	311	$-0.19 \cdot 10^{-4}$	$15 \cdot 10^{-4}$	104%
2022-06-28	94	149	$-0.24 \cdot 10^{-4}$	$8 \cdot 10^{-4}$	56%
2022-12-09	42	74	$-0.04 \cdot 10^{-4}$	$5 \cdot 10^{-4}$	36%

Table: Data statistics (number of trades, returns) per minute by discarding 5% of the lowest and the highest returns. The annualized volatility associated with the standard deviation of the returns is added.



(a) (b)

Figure: (a): Box plot of the estimated tail-index on the volumes (left), on the price returns (middle) and on the product of the two (right) for all considered pairs on 2022-05-05 (blue), 2022-06-12 (orange), 2022-06-28 (green) and 2022-12-09 (red).
(b): Box plot of the estimated upper tail dependence for all considered pairs and periods.

In summary, both V and P are heavy tailed with dependence in the tail

The problem of aggregating fragmented prices to get ONE price

Many sources of anomaly: Market corruption, Fat finger, Novice investor, Premium (Korean), DEX trade, Underlying fees, Arbitrage...

▷ Features:

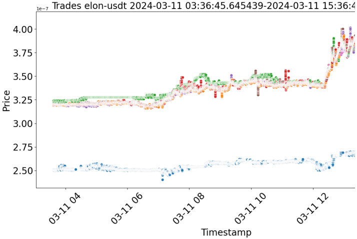
- ✓ Crypto market is very volatile and its liquidity keeps increasing
- ✓ Price returns and volumes are known to be heavy-tailed
- ✓ Distributions vary a lot from one exchange to another
- ✓ All exchanges matter

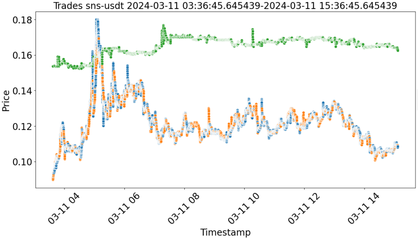
▷ Constraints:

- ✓ need for real time aggregation, impossible to update the price in the past (price/rate can be used for settlement)
- ✓ Reference rates are published every 5 seconds for derivative pricing
- ✓ Need to robust statistics
- ✓ The aggregated time series should be without outlier (to compute historical volatility...)

The zoology of anomalies

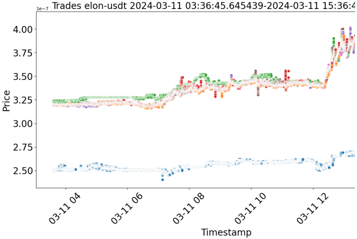
▷ **Exchange offset**: Multiple regimes with large volume

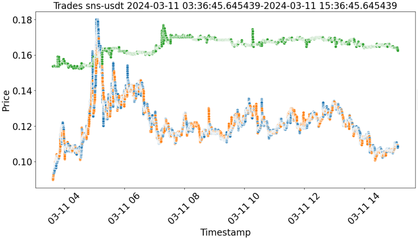




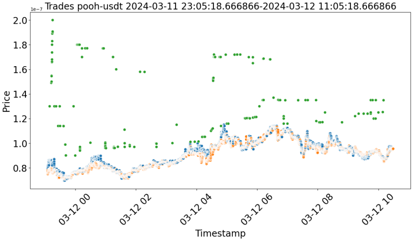
The zoology of anomalies

▷ **Exchange offset**: Multiple regimes with large volume

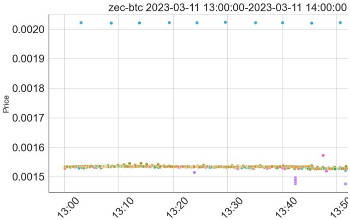


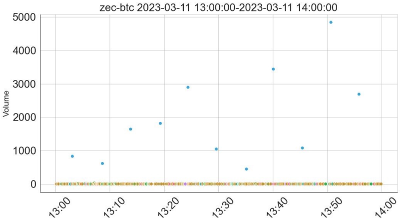


▷ **Large volatility**: Prices are very volatile in one exchange

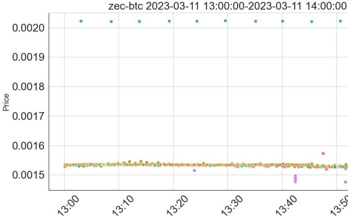


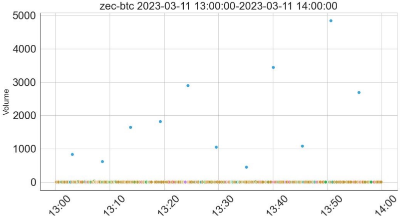
▷ **A few big trades**: The BLUE exchange represents 3% of the trades and 99% of the volume



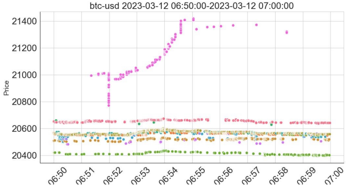


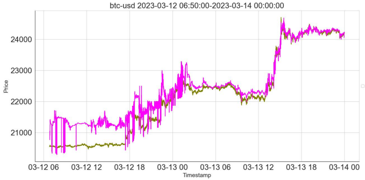
▷ **A few big trades**: The BLUE exchange represents 3% of the trades and 99% of the volume



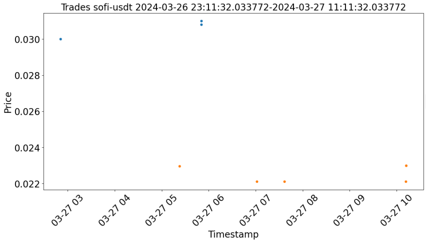


▷ **Outlier or Leader?**

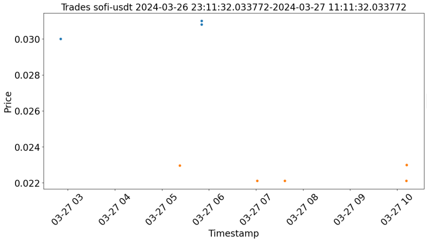




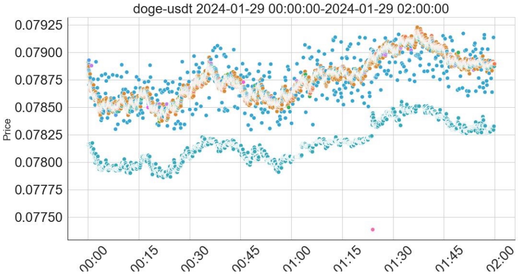
▷ **Liquidity issue**: Low liquidity + multiple regimes + liquidity holes



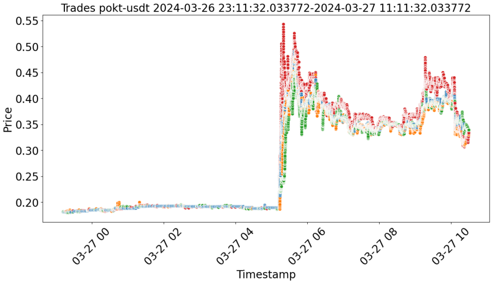
▷ **Liquidity issue**: Low liquidity + multiple regimes + liquidity holes



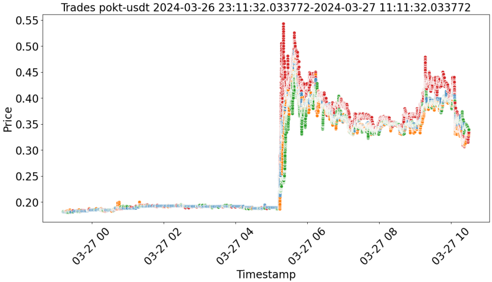
▷ Exchange offset + Point anomalies + Noisy exchange



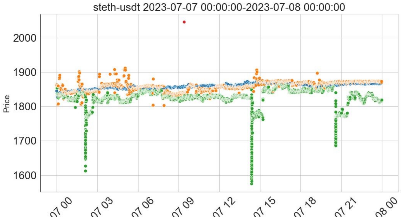
▷ **Market Movement**: Quick market evolution (opportunity, crash, news)



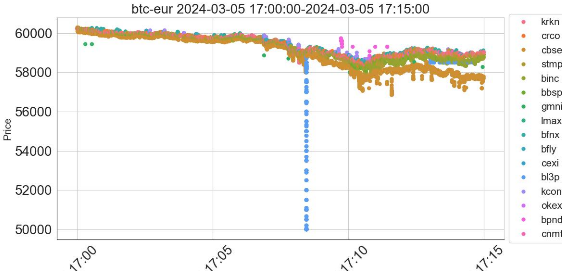
▷ **Market Movement**: Quick market evolution (opportunity, crash, news)



▷ **Large Liquiditation**: Order book cleaning



▷ Flash crash



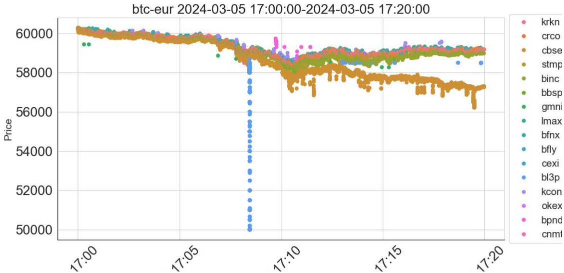
✓ Coinbase (major exchange) starts to deviate

✓ Similar volume and number of trades

✓ All liquidity on Coinbase

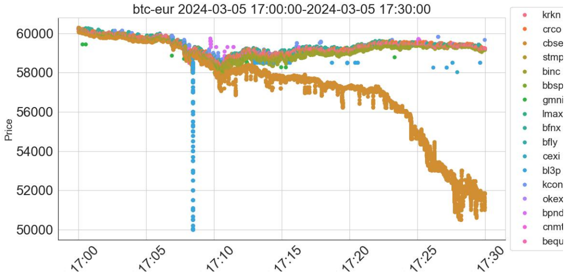
✓ Coinbase catches up – it was a flash crash due to algo trading

▷ Flash crash



- ✓ Coinbase (major exchange) starts to deviate
- ✓ Similar volume and number of trades
- ✓ All liquidity on Coinbase
- ✓ Coinbase catches up – it was a flash crash due to algo trading

▷ Flash crash



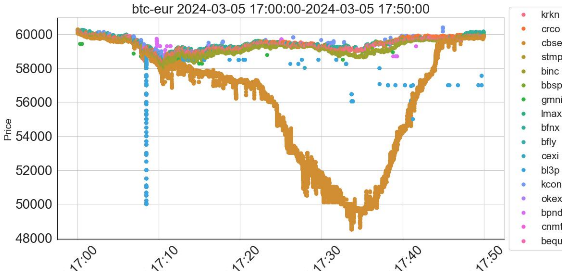
✓ Coinbase (major exchange) starts to deviate

✓ Similar volume and number of trades

✓ All liquidity on Coinbase

✓ Coinbase catches up – it was a flash crash due to algo trading

▷ Flash crash



- ✓ Coinbase (major exchange) starts to deviate
- ✓ Similar volume and number of trades
- ✓ All liquidity on Coinbase
- ✓ Coinbase catches up – it was a flash crash due to algo trading

Statistics/ML issues (many are open. . .)

- ✓ How to flag anomalies in real time, *i.e.* fast computation time?
- ✓ How to aggregate the price at one date? See Robust Weighted Median later
- ✓ How to be reactive to market movement, *i.e.* avoid false positive?
- ✓ How to detect which exchange is leading or lagging?
- ✓ How to model the vector of time-series for a given asset? (accounting for exchange fees, arbitrage,. . .)
- ✓ How to detect that an exchange becomes an outlier among other exchanges?
- ✓ How to price non traded pairs?
- ✓ How to aggregate CEX order books?
- ✓ . . .

Price agreggation: existing methods

✓ Volume-Weighted Average Price (VWAP):

$$\widehat{\mathtt{VWAP}}_n := \frac{\sum_{i=1}^n V_i P_i}{\sum_{i=1}^n V_i}.$$

Used by [Nas22] to obtain the Nasdaq Crypto Index (NCI) and by FTSE Russell [FTS22] to compute Digital Asset Reference Prices.

++ Obeys to the FOREX symmetry rule

– – Not robust to price and volume outliers

✓ Volume-Weighted Median price (VWM):

$$\widehat{\mathtt{VWM}}_n := \inf\left\{p : \frac{\sum_{i=1}^n V_i \mathbf{1}_{P_i \le p}}{\sum_{i=1}^n V_i} \ge \frac{1}{2}\right\}.$$

See Federal Reserve Bank of New York [Fed15] on interest rates. At work at the Chicago Mercantile Exchange [PK16] [CF 22b] [CF 22a] and Bloomberg [Gal18].

++ Robust to price outliers

– – Not robust to volume outliers

Theoretical guidance about statistical fluctuations

Cumulative distribution function (c.d.f.) of the weighted price as

$$F_{\mathtt{W}}(x) := \frac{\mathbb{E}\left[W \cdot \mathbf{1}_{P \le x}\right]}{\mathbb{E}\left[W\right]}, \qquad x \ge 0.$$

$$\mathtt{WAP} := \frac{\mathbb{E}\left[W \cdot P\right]}{\mathbb{E}\left[W\right]}.$$

$$\mathtt{WM} := \arg\inf_{p} \ \mathbb{E}_{\mathtt{W}}\left[|P - p|\right].$$

$$q_{\mathtt{W}}(\alpha) := \inf\left\{p : \frac{\mathbb{E}\left[W \mathbf{1}_{P \le p}\right]}{\mathbb{E}\left[W\right]} \ge \alpha\right\}.$$

Data-based definitions:

$$\widehat{\mathtt{WAP}}_n := \frac{\sum_{i=1}^n W_i P_i}{\sum_{i=1}^n W_i},$$

$$\widehat{q_{\mathtt{W},n}}(\alpha) := \inf\left\{p : \frac{\sum_{i=1}^n W_i \mathbf{1}_{P_i \le p}}{\sum_{i=1}^n W_i} \ge \alpha\right\},$$

$$\widehat{\mathtt{WM}}_n := \widehat{q_{\mathtt{W},n}}\left(\frac{1}{2}\right).$$

Assumptions

(H0): The c.d.f. $F_{\mathtt{W}}$ has a density $f_{\mathtt{W}}$:

$$F_{\mathtt{W}}(x) = \int_0^x f_{\mathtt{W}}(x')dx'.$$

$(\mathbf{H}_{\mathbf{X}}^{\kappa})$**:** X has a finite moment of order $\kappa > 2$: $\mathbb{E}\left[X^{\kappa}\right] < +\infty$.

$(\mathbf{H}_{\mathbf{X}}^{\Gamma})$**:** X has a sub-gamma distribution, i.e. $\mathbb{E}\left[e^{cX}\right] < +\infty$ for some $c > 0$.

$(\mathbf{H}_{\mathbf{X}}^{\mathbf{G}})$**:** X has a sub-Gaussian distribution, i.e. $\mathbb{E}\left[e^{cX^2}\right] < +\infty$ for some $c > 0$.

Asymptotic fluctuations on WM and WAP

Theorem

Under L_2 conditions on W and P,

$$\sqrt{n}\,(\widehat{q_{\mathtt{W},n}}(\alpha) - q_{\mathtt{W}}(\alpha)) \Rightarrow \mathcal{N}\,(0, \dots)\,,$$
$$\sqrt{n}\left(\widehat{\mathtt{WAP}}_n - \mathtt{WAP}\right) \Rightarrow \mathcal{N}\,(0, \dots)\,.$$

Mathematically interesting but non-relevant in practice (small n)

Non-asymptotic fluctuations on WM and WAP

$$\mathcal{Q}_n^{>}(\alpha, x) := \mathbb{P}\left(\widehat{q_{\mathtt{W},n}}(\alpha) - q_{\mathtt{W}}(\alpha) > \frac{x}{\sqrt{n}}\right), \qquad \mathcal{Q}_n^{\leq}(\alpha, x) := \mathbb{P}\left(\widehat{q_{\mathtt{W},n}}(\alpha) - q_{\mathtt{W}}(\alpha) \leq -\frac{x}{\sqrt{n}}\right),$$

$$\mathcal{W}_n^{\geq}(x) := \mathbb{P}\left(\widehat{\mathtt{WAP}}_n - \mathtt{WAP} \geq \frac{x}{\sqrt{n}}\right), \qquad \mathcal{W}_n^{\leq}(x) := \mathbb{P}\left(\widehat{\mathtt{WAP}}_n - \mathtt{WAP} \leq -\frac{x}{\sqrt{n}}\right).$$

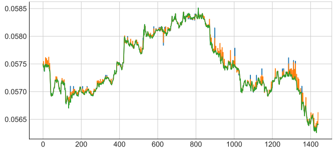
Simplified bounds (Theorems)

	$\max(\mathcal{Q}_n^{>}(\alpha, x), \mathcal{Q}_n^{\leq}(\alpha, x))$	$\max(\mathcal{W}_n^{\geq}(x), \mathcal{W}_n^{\leq}(x))$
Sub-Gaussian assumptions for $X = \ldots$	$\exp\left(-cx^2\right)$ $X = W$, no condition on W	$\exp\left(-\frac{cx^2}{1 + c\frac{x^2}{n}}\right)$ $X = W$ and $X = W \cdot P$
Sub-gamma assumptions for $X = \ldots$	$\exp\left(-\frac{cx^2}{1 + c\frac{x}{\sqrt{n}}}\right)$ $X = W$, no condition on W	$\exp\left(-\frac{cx^2}{\left(1 + c\frac{x}{\sqrt{n}}\right)^3}\right)$ $X = W$ and $X = W \cdot P$
Heavy-Tail assumptions for $X = \ldots$, for $\kappa > 2$	$\frac{c}{n^{\frac{\kappa}{2}-1} x^{\kappa}} + \exp\left(-cx^2\right)$ $X = W$, no condition on W	$\frac{c\left(1 + \frac{x}{\sqrt{n}}\right)^{\kappa}}{n^{\frac{\kappa}{2}-1} x^{\kappa}} + \exp\left(-\frac{cx^2}{1 + c\frac{x^2}{n}}\right)$ $X = W$ and $X = W \cdot P$

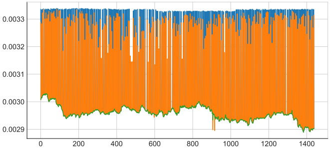
Define RWM by setting $W = \log(1 + V/q_{0.5}(V))$ which is sub-gamma distributed.

Proof: use the arsenal of concentration inequalities

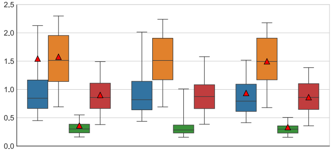
Experiments on real data



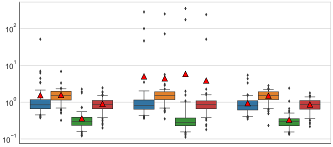
(a)



(b)



(c)



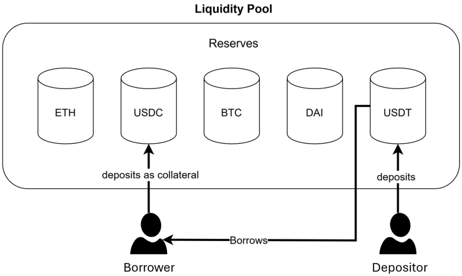
(d)

Figure: (a)-(b): Comparison between $\widehat{\mathtt{VWM}}_n$ (blue), $\widehat{\mathtt{VWAP}}_n$ (orange) and $\widehat{\mathtt{RWM}}_n$ (green) on real data aggregation per minute of the pair eth/btc (a) and zec/btc (b) on 2022-06-28.
(c): Box plot of the annualized RV (over all pairs) from $\widehat{\mathtt{VWM}}_n$ (left), $\widehat{\mathtt{VWAP}}_n$ (middle) and $\widehat{\mathtt{RWM}}_n$ (right) on 2022-06-28 (blue), on 2022-06-12 (orange), on 2022-09-12 (green) and on 2022-05-05 (red). The mean is emphasized by a red triangle and outliers are discarded.
(d)Box plot of the annualized RV taking into account outliers with the y-axis in log-scale.

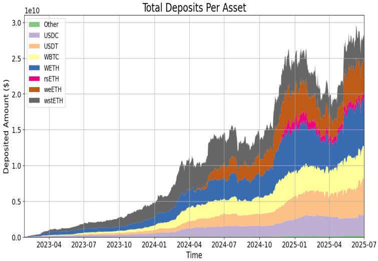
Lending-borrowing protocols

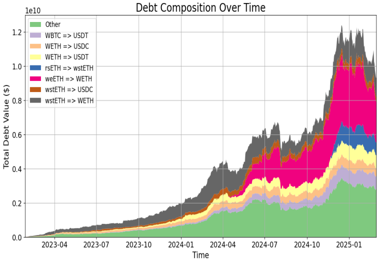
Work with Louis Latournerie (PhD student).

- ✓ Run in the blockchain, everything encoded in smart contract
- ✓ Principle:
  - ✓ lending tokens allow for earning returns
  - ✓ they can serve also as collaterals to borrow other tokens (and paying interest rates)
  - ✓ the interest rate depends on the utilization rate of the pool
  - ✓ if the collateral is not enough (Health Factor), the position may be automatically liquidated
- ✓ Examples: Aave, Compound, Morpho



Amount of assets in Aave



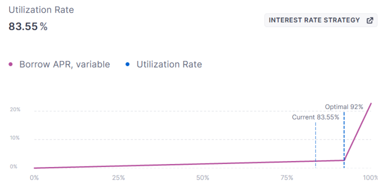


As of January 31 st, 2025:

- ✓ Total of 38 pools (7 pools in 2023, 50 pools as of today)
- ✓ About 40 digital assets (WETH, USDC, USDT, DAI, WBBTC, LINK, . . .)
- ✓ 25,000 depositors ($>$ \$100)
- ✓ 14,000 borrowers ($>$ \$100)
- ✓ Around \$30 billion deposited, \$12 billion borrowed

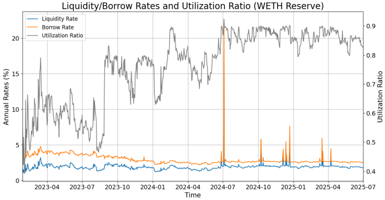
Interest rate

✓ It depends on the utilization rate of the asset in the Aave pool (multi-agent problems)



This feature contributes to the robustness of the protocol

✓ Borrowing rate > lending rate

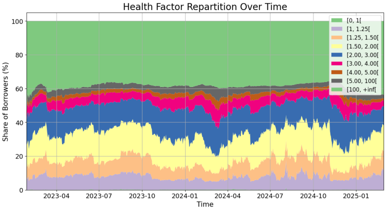


Liquidation

- ✓ For a given user, write $V_{i,t}$ for the amount in asset i: $V_{i,t} > 0$ if lending, $V_{i,t} < 0$ if borrowing
- ✓ At any time, a Health Factor is computed

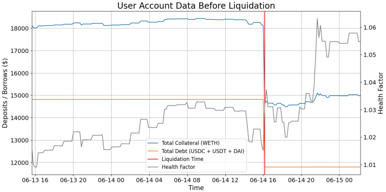
$$\mathrm{HF}_t = \frac{\sum_i V_{i,t}^{+} \mathrm{LT}_i}{\sum_i V_{i,t}^{-}}$$

where LT_i is the liquidation threshold (about 75%)

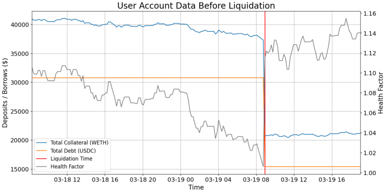


- ✓ If $\mathrm{HF}_t \leq 1$, then anyone can take the role of liquidator: repay the debt, take an equivalent amount of collateral, augmented by the liquidation bonus (which depends on the assets, typically around 5%).
- ✓ Like a knock-out option (very sudden)

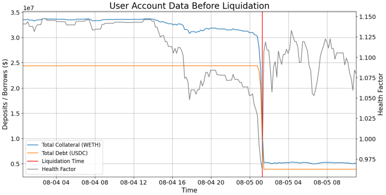
A few examples based on real data



June 14th 2024: HF≈ 1.02, the risk of liquidation is quite high!



March 18th 2024: HF moves from 1.10 (ok!) to 1, the risk of liquidation gets higher and higher!



August 5th 2024: HF moves suddenly from 1.10 (ok!) to 1, the liquidation yields a loss of about 500k$ (about 17% of the collateral)

Quantitative modeling issues to handle

✓ Compute the term structure of borrowing interest rate (including the liquidation risk), Latournerie PhD thesis

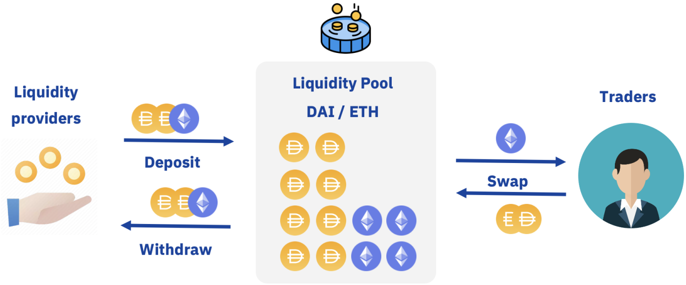
✓ Assess the systemic risk (bad debt can happen when jump/gap risk occurs)

✓ Design of safe and robust lending-borrowing protocol

Automated Market Maker (AMM)

Q: How to permit the automated execution of buy and sell orders in a blockchain (without Limit Order Book and a 3rd party)?

Pools based DEXs General Functioning



- ✓ The amount of tokens for each trade is decided by the **algorithm of the pool**
- ✓ Rules according to a **Constant Function Market Making**
- ✓ Exemples: Balancer, Curve, mStable, Sushiswap, Uniswap, etc
- ✓ Transactions are on-chain.

Uniswap v2 - Principles

✓ Based on the Constant Function Market Makers:

$$\mathcal{I}(x, y) = x \cdot y.$$

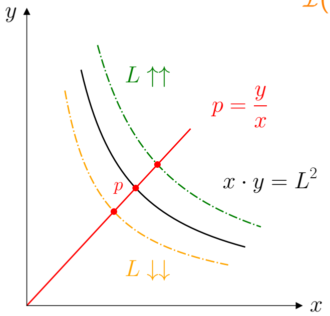


Figure: How prices and quantities can evolve in a Uniswap v2 protocol

✓ Price/tokens/liquidity relations:

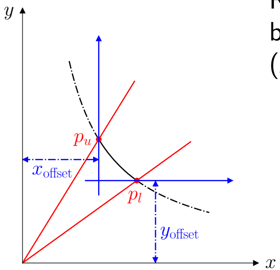
$$x = \frac{L}{\sqrt{p}} = \frac{L}{\pi} \quad \text{and} \quad y = L\sqrt{p} = L \cdot \pi.$$

where p is the pool price and π is the square root price

Uniswap v3 - Principles

Detailed analysis from the source code in [EGM25].

- ✓ **Concentration of liquidity.** An LP provides an amount of liquidity L on a price range $[p_\ell, p_u)$: deposit of x_r and y_r
- ✓ **Swap trades.** Tokens are used by swap operations as long as the price is in the range $[p_\ell, p_u)$. When the price reaches p_ℓ (resp. p_u), all reserves of tokens Y (resp. X) will have been depleted.
- ✓ **Localized Constant Function Market Maker.** On the price range $[p_\ell, p_u)$, the constant product rule $x \cdot y = L^2$ applies with the main difference that x and y denote *virtual* token reserves instead of real reserves.



Representation of the *virtual* numbers (x, y) and the *offset* numbers $(x_{\text{offset}}, y_{\text{offset}})$ of tokens:

$$\begin{cases} x = x_r + x_{\text{offset}}, \\ y = y_r + y_{\text{offset}}. \end{cases}$$

$$\Longrightarrow \left(x_r + \frac{L}{\pi_u}\right) \cdot (y_r + L \cdot \pi_\ell) = L^2.$$

Example of Liquidity curve

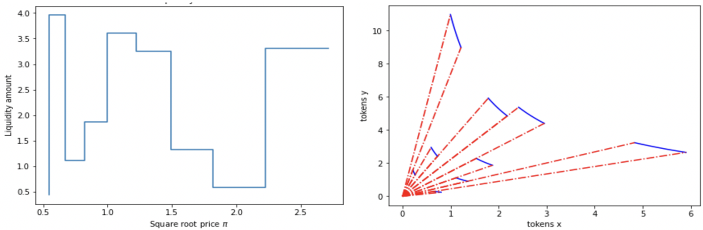


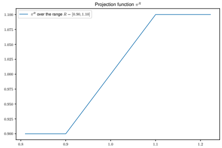
Figure: On the left: the liquidity curve.
On the right: the CPMM relation on each range.

- ✓ Not all tick ranges can actually be used to update liquidity: the ranges are a multiple of a fixed number δ_π of ticks, which is ruled at the setting of the pool, according to the swap fees ϕ.
- ✓ A range of δ_π ticks is called unitary range.
- ✓ One tick is 1 basis point.
- ✓ $\delta_\pi = 2, 10, 60, 200,$ according to swap fees $\phi = 0.01\%, 0.05\%, 0.3\%, 1\%$

Value of a LP position in a unitary range

For $R = [\pi_\ell, \pi_u)$, define the projected square root price function:

$$\pi \longrightarrow \pi^R = \begin{cases} \pi_u \text{ if } \pi_u < \pi_0, \\ \pi_\ell \text{ if } \pi_0 < \pi_\ell, \\ \pi \text{ otherwise.} \end{cases}$$

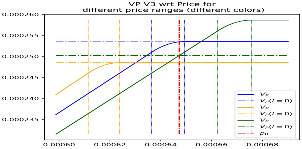


Theorem (V_P on a unitary range)

Adding a liquidity ΔL on the unitary range R at time 0 gives that the Y-value of the LP position equals to

$$V_P(t) = \Delta L \cdot g_R(p_t) \text{ with } g_R(p_t) := \left(\frac{1}{\pi_t^R} - \frac{1}{\pi_u}\right) \cdot p_t + (\pi_t^R - \pi_\ell),$$

given as a function of the square root price $\pi_t := \sqrt{p_t}$ at time t.



Value of the pool for 3 different price ranges (orange, blue, green). The dashed vertical lines in each color represent the considered unitary ranges in the variable price p. The dashed horizontal lines represent the initial value of the pool for the price p_0 depicted in red.

Value of a LP position with arbitrary liquidity curve

Theorem (V_P on multiples ranges)

Consider a liquidity provider adding a liquidity curve $(\Delta L_\pi)_\pi$ to the pool at time $t = 0$. Then, its Y-value net of swap fees at time t is

$$V_P(t) = p_t \cdot \int_{\pi_t}^{+\infty} \frac{\Delta L_\pi}{\pi^2} \mathrm{d}\pi + \int_0^{\pi_t} \Delta L_\pi \mathrm{d}\pi.$$

✓ Remarkably simple! Valid for any occurence of swap trades or other mint/burn events.

Corollary (Greeks of V_P)

The Delta and Gamma of the Y-value of the LP position is

$$\Delta_P(t) = \int_{\pi_t}^{+\infty} \frac{\Delta L_\pi}{\pi^2} \mathrm{d}\pi, \quad \Gamma_P^-(t) = -\frac{\Delta L_{\pi_t^-}}{2\pi_t^3}, \quad \Gamma_P^+(t) = -\frac{\Delta L_{\pi_t}}{2\pi_t^3}.$$

In particular, such a position is always concave in the spot rate.

✓ Any market move leads to (impermanent) loss for the LP

✓ The negative gamma is compensated by fees (see later)

Swap traders and fees bookkeeping

- ✓ Contrarily to Uniswap v2 pools, fees are not considered as additional tokens in the reserves of the Uniswap v3 pool
  open problem for approximation fees in Uniswap v2
- ✓ Uniswap v3 fees are concentrated specifically on each range
- ✓ If a_i^X is the number of tokens added by a swap trader to swap X for Y at t_i in R, then

$$\Delta\Phi_R^X = \sum_{\text{swap } X \text{ for } Y \text{ at } t_i \text{ in } R} \frac{a_i^X}{1-\phi} \cdot \frac{\phi}{L_i}$$

  Similarly for Y
- ✓ Getting a simple formula for the fees requires a model for the sequence of stochastic a_i^X and a_i^Y

Swap traders and fees bookkeeping

- ✓ Contrarily to Uniswap v2 pools, fees are not considered as additional tokens in the reserves of the Uniswap v3 pool
  open problem for approximation fees in Uniswap v2
- ✓ Uniswap v3 fees are concentrated specifically on each range
- ✓ If a_i^X is the number of tokens added by a swap trader to swap X for Y at t_i in R, then

$$\Delta\Phi_R^X = \sum_{\text{swap } X \text{ for } Y \text{ at } t_i \text{ in } R} \frac{a_i^X}{1-\phi} \cdot \frac{\phi}{L_i}$$

Similarly for Y

- ✓ Getting a simple formula for the fees requires a model for the sequence of stochastic a_i^X and a_i^Y

Analytical formula for fees

Theorem (Fees in X and Y accumulated over $[0, T]$)

Assume

- ✓ *Angeris [AKC⁺21] arbitrage model : the swap trades occur when the latent price process $(p_t)_t$ changes by ϕ%*

$$t_{i+1} := \inf\left\{t \geq t_i : p_t = p_{t_i}(1+\phi)^{\pm 1}\right\}$$

- ✓ *The latent price process follows an Itô dynamics of the form*

$$\frac{\mathrm{d}p_t}{p_t} = \mu_t \mathrm{d}t + \sigma_t \mathrm{d}W_t,$$

Then, the following convergences hold in probability (as $\phi \to 0$):

$$\mathrm{Fees}^X_{0\to T} \to \int_0^{+\infty} \Delta L_{b^{\frac{1}{2}}} \frac{A^b_T(p)}{4 \cdot b^{5/2}} \mathrm{d}b,$$

$$\mathrm{Fees}^Y_{0\to T} \to \int_0^{+\infty} \Delta L_{b^{\frac{1}{2}}} \frac{A^b_T(p)}{4 \cdot b^{3/2}} \mathrm{d}b,$$

where $A^b_T(p)$ is the local time of p at level b and time T.

As a consequence, the value of the global LP-position is

$$J\big(t,(\Delta L_\pi)_\pi\big) = p_t \int_{\pi_t}^{\infty} \frac{\Delta L_\pi}{\pi^2}\mathrm{d}\pi + \int_0^{\pi_t} \Delta L_\pi \mathrm{d}\pi + p_t \int_0^{+\infty} \Delta L_{b^{\frac{1}{2}}} \frac{A_T^b(p)}{4\cdot b^{5/2}}\mathrm{d}b + \int_0^{+\infty} \Delta L_{b^{\frac{1}{2}}} \frac{A_T^b(p)}{4\cdot b^{3/2}}\mathrm{d}b.$$

Next questions

✓ When to exit? optimal stopping problem?

$$\sup_{t\in\mathcal{T}(\mathbb{R}^+)} \mathbb{E}\left[J\big(t,(\Delta L_\pi)_\pi\big)\right],$$

where the set $\mathcal{T}(\mathbb{R}^+)$ is the set of $\mathcal{F}$-stopping times taking finite non-negative values *with probability 1*.

✓ In which ranges to invest (add liquidity)?

Theorem

It is systematically better for the LP to burn each piece of liquidity ΔL_π at different times than to burn the entire liquidity curve $(\Delta L_\pi)_\pi$ at once.

As a consequence, the value of the global LP-position is

$$J\big(t,(\Delta L_\pi)_\pi\big) = p_t \int_{\pi_t}^{\infty} \frac{\Delta L_\pi}{\pi^2} \mathrm{d}\pi + \int_0^{\pi_t} \Delta L_\pi \mathrm{d}\pi + p_t \int_0^{+\infty} \Delta L_{b^{\frac{1}{2}}} \frac{A_T^b(p)}{4 \cdot b^{5/2}} \mathrm{d}b + \int_0^{+\infty} \Delta L_{b^{\frac{1}{2}}} \frac{A_T^b(p)}{4 \cdot b^{3/2}} \mathrm{d}b.$$

Next questions

- ✓ When to exit? optimal stopping problem?

$$\sup_{t \in \mathcal{T}(\mathbb{R}^+)} \mathbb{E}\left[J\big(t,(\Delta L_\pi)_\pi\big)\right],$$

where the set $\mathcal{T}(\mathbb{R}^+)$ is the set of $\mathcal{F}$-stopping times taking finite non-negative values *with probability 1*.

- ✓ In which ranges to invest (add liquidity)?

Theorem

It is systematically better for the LP to burn each piece of liquidity ΔL_π at different times than to burn the entire liquidity curve $(\Delta L_\pi)_\pi$ at once.

Now

- ✓ consider a single unitary range R and a unit liquidity, then the value of the LP position is

$$J_R(t) = g_R(p_t) + \frac{1}{4} p_t \int_0^t \sigma_s^2 p_s^{-1/2} \mathbf{1}_{p_s \in R} ds + \frac{1}{4} \int_0^t \sigma_s^2 p_s^{1/2} \mathbf{1}_{p_s \in R} ds$$

- ✓ assume that p is martingale.

Theorem

The value

$$U_t := \operatorname*{ess\,sup}_{s \in \mathcal{T}([t,+\infty))} \mathbb{E}\left[J_R^M(s) \mid \mathcal{F}_t\right]$$

is a super-martingale, which admits a right-continuous modification. If $t_0^\star = \inf\{t \geq 0 : U_t = J_R(t)\}$ is finite with probability one, it is the smallest optimal stopping time. If $\mathbb{P}(t_0^\star < \infty) < 1$, there is no optimal stopping time.

Theorem

$\sup_{t \in \mathcal{T}(\mathbb{R}^+)} \mathbb{E}[J_R(t)]$ *is invariant by time-change and thus, it can be computed in the case $\sigma = 1$ (Dambis-Dubins-Schwarz time-change).*

Theorem

In the case of martingale GBM case, there is no optimal stopping time and the sup is computed along sequences of stopping time increasing to $+\infty$: the LP has better to stay in the pool forever.

Proof.

- ✓ Consider ε-optimal stopping times
- ✓ Show that the sup can be computed by maximizing over exit times from intervals $[\varepsilon, \lambda]$ for $\varepsilon \downarrow 0$ and $\lambda > 0$
- ✓ Use explicit formulas (GBM) for occupation time measure stopped at exit times
- ✓ Optimize to get the result

$\square$

Theorem

In the case of martingale GBM case, there is no optimal stopping time and the sup is computed along sequences of stopping time increasing to $+\infty$: the LP has better to stay in the pool forever.

Proof.

- ✓ Consider ε-optimal stopping times
- ✓ Show that the sup can be computed by maximizing over exit times from intervals $[\varepsilon, \lambda]$ for $\varepsilon \downarrow 0$ and $\lambda > 0$
- ✓ Use explicit formulas (GBM) for occupation time measure stopped at exit times
- ✓ Optimize to get the result

$\square$

What is the return for the LP?

Consider the return with rate c, and stop at the exit time from $[0, \lambda]$:

$$V^{\lambda,c}(p_0) := \mathbb{E}\Big[\mathrm{e}^{-ct^\lambda} g_R(p_{t^\lambda}) + p_{t^\lambda} \frac{\sigma^2}{4} \int_0^{t^\lambda} \mathrm{e}^{-cs} p_s^{-1/2} \mathbf{1}_{p_s \in R} ds \\ + \frac{\sigma^2}{4} \int_0^{t^\lambda} \mathrm{e}^{-cs} p_s^{1/2} \mathbf{1}_{p_s \in R} ds \mid p_0\Big].$$

The best value for the LP is

$$\sup_{\lambda > 0} V^{\lambda,c}(p_0).$$

If c is too high, then one could expect that the above value equals to the initial investment $g_R(p_0)$, i.e. the LP can not beat such target return and he has better to exit immediately $(\lambda = p_0)$.

Equivalent interest rate of return

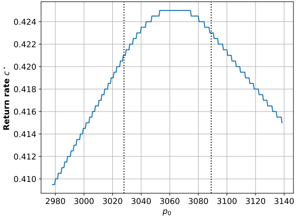
Equivalent interest rate of return $c^\star$ for the LP:

$$c^\star := \max\left\{c > 0 : \sup_{\lambda > 0} \frac{V^{\lambda,c}(p_0)}{g_R(p_0)} > 1\right\}.$$

✓ $c^\star$ depends on R, on p_0 and on the volatility σ

✓ By time-scale argument, we have $c^\star(R, p_0, \sigma) = \sigma^2 \cdot c^\star(R, p_0, 1)$.

Using PDE methods, one can compute $c^\star(R, p_0, 1)$ and get



✓ It is better the LP adds liquidity in the unitary range R such that $p_0 \in R$

✓ For 50% volatility, the expected return is $0.425 * 0.5^2 \approx 10.6\%$!!

Conclusion

What we have seen:

- ✓ Fragmented market: need for statistical modeling in large dimension, with robust techniques
- ✓ Lending-borrowing protocol: appealing but liquidation risk is here. What about systemic risk?
- ✓ Uniswap v3: asymptotic analysis can be applied to assess the returns for LP

and still a lot of research needs on these topics.

But many quantitative issues also on:

- ✓ Implied volatility: lack of standardization of products, how to compare option prices on similar tokens?
- ✓ Derivatives: Futures, Perpetuals... need for arbitrage modeling.
- ✓ Interest rate modeling: no central bank, fragmented view point
- ✓ Stable coin

Thank you!

Conclusion

What we have seen:

- ✓ Fragmented market: need for statistical modeling in large dimension, with robust techniques
- ✓ Lending-borrowing protocol: appealing but liquidation risk is here. What about systemic risk?
- ✓ Uniswap v3: asymptotic analysis can be applied to assess the returns for LP

and still a lot of research needs on these topics.

But many quantitative issues also on:

- ✓ Implied volatility: lack of standardization of products, how to compare option prices on similar tokens?
- ✓ Derivatives: Futures, Perpetuals... need for arbitrage modeling.
- ✓ Interest rate modeling: no central bank, fragmented view point
- ✓ Stable coin

Thank you!

Conclusion

What we have seen:

- ✓ Fragmented market: need for statistical modeling in large dimension, with robust techniques
- ✓ Lending-borrowing protocol: appealing but liquidation risk is here. What about systemic risk?
- ✓ Uniswap v3: asymptotic analysis can be applied to assess the returns for LP

and still a lot of research needs on these topics.

But many quantitative issues also on:

- ✓ Implied volatility: lack of standardization of products, how to compare option prices on similar tokens?
- ✓ Derivatives: Futures, Perpetuals... need for arbitrage modeling.
- ✓ Interest rate modeling: no central bank, fragmented view point
- ✓ Stable coin

Thank you!

References I

Michaël Allouche, Mnacho Echenim, Emmanuel Gobet, and Anne-Claire Maurice.
Statistical error bounds for weighted mean and median, with application to robust aggregation of cryptocurrency data.
Mathematical Finance, 2025.

Ankush Agarwal and Emmanuel Gobet.
Optimal exit from Uniswap v3 and best expected return for a liquidity provider.
HAL https://hal.science/hal-05231633, 2025.

Guillermo Angeris, Hsien-Tang Kao, Rei Chiang, Charlie Noyes, and Tarun Chitra.
An analysis of Uniswap markets.
Cryptoeconomic Systems, 1(1), 2021.

Hayden Adams, Noah Zinsmeister, and Dan Robinson.
Uniswap v2 Core.
Technical report, Uniswap, 2020.
https://uniswap.org/whitepaper.pdf.

Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson.
Uniswap v3 core.
Uniswap, Tech. Rep., 2021.
https://uniswap.org/whitepaper-v3.pdf.

Maxime Bichuch and Zach Feinstein.
Implied volatility in decentralized finance from automated market makers, 2023.
Presentation at SIAM Conference on Financial Mathematics and Engineering, Philadelphia, 6-9 June 2023.

References II

Álvaro Cartea, Fayçal Drissi, and Marcello Monga.
Decentralised finance and automated market making: Execution and speculation.
Available at SSRN 4144743, 2022.

Álvaro Cartea, Fayçal Drissi, Leandro Sánchez-Betancourt, David Siska, and Lukasz Szpruch.
Automated market makers designs beyond constant functions.
Available at SSRN 4459177, 2023.

CF Benchmarks.
CME CF cryptocurrency real time indices, version 15.1, December 2022.
https://docs.cfbenchmarks.com/CME%20CF%20Real%20Time%20Indices%20Methodology.pdf.

CF Benchmarks.
CME CF cryptocurrency reference rates, version 15.1, December 2022.
https://docs.cfbenchmarks.com/CME%20CF%20Reference%20Rates%20Methodology.pdf.

Agostino Capponi, Garud Iyengar, and Jay Sethuraman.
Decentralized finance: Protocols, risks, and governance.
Foundations and Trends in Privacy and Security, 5(3):144–188, 2023.

Samuel Cohen, Marc Sabaté Vidales, David Siska, and Lukasz Szpruch.
Inefficiency of CFMs: hedging perspective and agent-based simulations.
In *International Conference on Financial Cryptography and Data Security*, pages 303–319. Springer, 2023.

References III

Agostino Capponi and Brian Zhu.
Optimal exiting for liquidity provision in constant function market makers, February 21 2025.
Available at SSRN: https://ssrn.com/abstract=5148585 or http://dx.doi.org/10.2139/ssrn.5148585.

Mnacho Echenim, Emmanuel Gobet, and Anne-Claire Maurice.
Unbiasing and robustifying implied volatility calibration in a cryptocurrency market with large bid-ask spreads and missing quotes.
Quantitative Finance, 23(9):1285–1304, 2023.

Mnacho Echenim, Emmanuel Gobet, and Anne-Claire Maurice.
Uniswap v3: impermanent loss modeling and swap fees asymptotic analysis.
SIFIN, in revision, 2025.
https://hal.science/hal-04214315/, version 3.

Federal Reserve Bank of New York.
Technical note concerning the methodology for calculating the effective federal funds rate, July 2015.
https://www.newyorkfed.org/medialibrary/media/markets/EFFR-technical-note-070815.pdf.

References IV

FTSE Digital Asset Research.
Guide to the calculation of the FTSE DAR Digital Asset Prices and FTSE DAR Reference Prices, November 2022.
https://research.ftserussell.com/products/downloads/Guide_to_the_Calculation_of_FTSE_DAR_Digital_Asset_Prices_and_Reference_Prices_Fixes.pdf.

Colin Gallagher.
CFIX methodology, Bloomberg cryptocurrency solutions, September 09 2018.
https://data.bloomberglp.com/professional/sites/10/CFIX-Methodology.pdf.

Emmanuel Gobet and Anastasia Melachrinos.
Decentralized Finance & Blockchain Technology.
In *SIAM Financial Mathematics and Engineering 2023*, Philadelphia, United States, June 2023.
https://hal.science/hal-04131680.

Sebastian Jaimungal, Yuri F. Saporito, Max O. Souza, and Yuri Thamsten.
Optimal trading in automatic market makers with deep learning.
arXiv preprint arXiv:2304.02180, 2023.

G. Lambert.
Uniswap v3 LP tokens as perpetual put and call options.
Medium, June 2021.
https://medium.com/@lambert-guillaume/uniswap-v3-lp-tokens-as-perpetual-put-and-call-options-5b66219db827.

References V

Jason Milionis, Ciamac C Moallemi, Tim Roughgarden, and Anthony Lee Zhang.
Automated market making and loss-versus-rebalancing.
arXiv preprint arXiv:2208.06046, 2022.

Nasdaq.
Nasdaq Crypto Index: index methodology, June 2022.
https://indexes.nasdaqomx.com/docs/methodology_NCI.pdf.

Andrew Paine and William J. Knottenbelt.
Analysis of the CME CF Bitcoin Reference Rate and Real Time Index, October 20 2016.
https://www.cmegroup.com/trading/files/bitcoin-white-paper.pdf.

Goran Peskir and Albert Shiryaev.
Optimal stopping and free-boundary problems.
Basel: Birkhäuser, 2006.

Sebastian Schmidl, Phillip Wenig, and Thorsten Papenbrock.
Anomaly detection in time series: a comprehensive evaluation.
Proceedings of the VLDB Endowment, 15(9):1779–1797, 2022.

Álvaro Cartea, Fayçal Drissi, and Marcello Monga.
Decentralised finance and automated market making: Predictable loss and optimal liquidity provision.
SIAM Journal on Financial Mathematics, 15(3):931–959, 2024.