web: *https://remyjkim.github.io* jkkim123@seas.upenn.edu Updated :November 2022

# Foundations for Decentralized Economics: AMM and Staking

Remy Kim

*Keywords: Automated Market Makers, Optimization, Asset Pricing, Portfolio Theory, Game Theory, Stochastic Modeling, Differential Privacy, Zero-Knowledge Proofs*

Smart contracts and their Turing-complete execution layers opened up a new frontier of financial assets (also referred to as "digital primitives"). Although seemingly very simple in their workings, these digital financial assets call for a transformative shift in economic concepts that sustained the traditional finance (TradFi). My research centers around unveiling the potential (and the following risks) of the two most representative digital primitives, automated market maker (AMM) and staking, using mathematical guarantees along with empirical on-chain data and proposing better constructions that improves on the existing inventions.

Automated Market Maker (AMM), first proposed and widely implemented by Uniswap, was the breakthrough that provided Decentralized Finance (DeFi) the momentum it needed, now that smart contracts offered the most basic function of an economy: barter between goods(=tokens). Various forms of automated market making have been launched as protocols since, which is thoroughly investigated in [XPCF21] in light of several criteria such as fee mechanism, divergence loss (usually called the "impermanent loss") and protocol security. However, these automated market making mechanisms introduce a new actor previously not seen in traditional market making: the liquidity providers. Adequate mechanism designs that incentivize liquidity providers while harming its original purpose of trading are necessary; which at times call for accurate asset pricing incorporated in the AMM and certain stress/risk assessments as well. Moreover they have to be computationally efficient to be able to execute using distributed forms of computation.

Staking of tokens adds another layer of complexity in the system. Staking, which was originally proposed as a means of preserving a chain's security and reducing energy consumption, has now evolved into an entirely new primitive for digital assets: for proving certain share of ownership or locking the digital asset so as to contain any sell pressures. Staking derivatives are widely falsely understood as only a means for yield-farming or accruing interest. Staking, however, can also be viewed as international interest markets; thus, staking levels of certain chains need to be widely monitored and must be incorporated into a wider framework of decentralized financial economics.

Consequently, the main thrust of my research is around these four pillars of questions:

1. **Can we construct "efficient" AMM liquidity pools that considers the diverse properties of the underlying tokens, and provide more rigorous analyses of their behavior?**

   Replicating certain payoffs (such as those that replicate a call option or treasury bonds) as an automated market maker requires certain assumptions as shown in [Eva21] and [AEC21b]. Drawing several parallels with traditional financial products such as ETFs([LM18]) or bonds([Hul12]), stricter assumptions or relaxation may arise for certain automated marking making. Especially application of automated market making of bonds are a special interest: AMMs that can deal with diverse maturity and duration would require a precise asset pricing model incorporated in the design.
   Liquidity fracture across decentralized exchanges (DEXes) is a capacity-restrictive factor of a liquidity pool. Simulating multiple DEXes liquidity scenarios and quantifying the opportunity cost of not having a one unified liquidity, as well as constructing a game-theoretic cooperation method between methods, would greatly resolve this capital inefficiency problem.
   Most current literature largely assume an existence of a larger, external market price and focus on the roles of arbitrageurs for rebalancing the pool. However, with the recent collapse of major centralized exchanges, the possibility that on-chain automated market makers themselves could be the most liquid market and the most efficient one. If that is the case, considering into the factors of leveraging and transaction costs would become a necessity.

2. **Can we construct novel incentive mechanisms other than simple trading fee mechanism for liquidity providers so as to secure adequate amount of liquidity? What are the "cost of liquidity" from the protocol's tokenomics perspective (the liquidity pool equivalent of "cost of capital" for corporate finance)?**

   Liquidity pools can be viewed as a public goods for the underlying tokens, thus it is critical to secure a sufficient amount of liquidity for a more efficient price discovery. Viewing liquidity pools as some sort of mutual funds that fixes the asset allocation to a certain proportion, liquidity pools not only need to be capital efficient, but also be self-improving or reflective of external data. Dynamic weightings or stochastic feedback controls are only beginning to be considered as a means towards efficient rebalancing of the assets but needs to be more deeply investigated.
   Moreover, as more complicated automated market makers are used, certain stress tests or risk assessment methods should be implemented to measure systemic risk of a pool or even across DEXes (some starting points could be looking at how exchange-traded funds' risks are evaluated and managed [HK$^{+}$09], [LM18]), [HNH15].

3. **Using differential privacy and/or zero-knowledge proofs, can we find trading curves that ensure certain level of privacy for traders using a liquidity pool?**

   That all transactions are transparent on the blockchain also implies minimum privacy of financial interactions. However, this is not optimal in all cases. Especially with block validators maximizing Miner-Extractable Value using a mempool data (that keeps all the buffer of transactions waiting to be processed) over repeating, discrete periods of 10 19 seconds, frontrunning and backrunning attacks are easily conducted. [CK22] and [CAE21] provides some hints as to how to decide on the design parameters of a Constant Function Market Maker to minimize such costs: obscuring certain trade information by adding random components or batching transactions.
   Setting up adversarial settings where the adversary is only equipped with certain modes of queries and information and analyzing their advantages provide a great base for formulating the tradeoff between the performance (i.e. latency, price accuracy) and the privacy. Furthermore, how utilizing zero-knowledge proofs changes how the adversarial game is playes also needs further investigation.

4. **Can we improve the vanilla staking model that minimizes the trade-off between security-enhancing aspect of staking and its liquidity level? What economic role does staking play in relation to other digital assets and can we model them?**

   Staking has become an integral part of blockchain now and forms the basis of on-chain "interest markets." Macroeconomic theory on inflation and interest rates have some room for application here; carry trade portfolios are also possible. Simulating these conditions with continuous time models would give us some measure of dynamic equilibrium over changes in interest rates. To extend the parallel with currency a bit farther, we can view staking as an optimal control problem, whereby the consensus layer provides a feedback loop that reflects the staking ratio of a chain as well as the implied interest rates in the market. This is in comparison with what the central banks does to the economy using its set of monetary policies. What role liquid staking derivatives [SJ22] would play as an intermediary product is also a topic of interest.

**Going Forward:** I am extremely excited to pursue research in decentralized finance, asset allocation/pricing, differential privacy and smart contracts. It just thrills me wondering about the groundwork that my colleagues and I will be laying around decentralized finance. A new form of economy calls for new laws and new perspectives. Much more work needs to be done to apply the connection we have discovered to construct more diverse toolkits of digital primitives. In the past five years, we as a community has built a trustless financial infrastructure out of thin air, that is now capable of handling trillion dollars worth of transactions. I hope that the field's progress on rigorously analyzing the implications of these primitives and creating new ones empowers every individual's financial autonomy in the foreseeable future.

# Appendix 1. Building blocks of Decentralized Finance (WIP)

1. What is a CFMM, AMM? How are they different from market makers in NYSE?
2. Price stability and arbitrage?
3. What is Staking?
4. How are tokens traded across chains?
5. What is differential privacy?
6. What is zero knowledge proof?

# Appendix 2. Notes on current literature for each topic

1. **Can we construct "efficient" AMM liquidity pools that considers the diverse properties of the underlying tokens, and provide more rigorous analyses of their behavior?**

   [Eva21] shows that setting the weight of a G3M equal to the elasticity of a given payoff function ensures that the LP shares replicate the payoff. Here, replication is also studied under more general assumptions by utilizing uses for the underlying asset price.

   [AC20] introduces the concept of trading set that holds all information about the trading function corresponding to a CFMM model. The paper also utilizes path deficiency to show that CFMMs reflect external market prices in a computational efficient way and that assets held in the CFMM have lower bounds.

   [ACE22] analyzes the role of curvature across various asset pairs and its effect on LP returns and liquidity. The paper also applies this in the context of price stability, incentivized liquidity provision models and the greeks of such LP positions.

   [AEC21b] provides a way that, given a desired payoff function V (that is concave, nonnegative, non-decreasing, 1-homogeneous), we can recover a CFMM trading function $\psi_V$ that produces such desired payoffs. The paper notes $\psi_V$ is a Fenchel conjugate of -V and utilizes two charateristics of such trading function—perspective transform and quadratic payoffs—to illustrate several applications, including geometric mean market maker, Black-Scholes covered call price and perpetual American put option price. Future research is still left open for payoffs with less strict assumptions and how to approximate them as well as for whether fees can mitigate arbitrage losses, allowing replication without additional capital.

   [AAE+21] generalizes the pairwise asset trade problem into a multi-asset trade one by solving instead a convex relaxation of the original non-convex problem; and provides a linear and a markowitz trading variant of the problem. The novelty lies is the generality of this problem setting and its easiness of evaluation using modern convex optimization tools such as CVXPY.

   [AEC21c] provides a much bolder proof than [AEC21b] that any monotonic payoff (such as those of cash-or-nothing, logarithmic, capped-power-payoffs or constant proportion portfolios) can be replicated using only LP shares in CFMMs. Here, the authors also provide formulas for arbitrageurs' earnings.

   [AECB22] converts a non-convex optimization problem of finding the optimal route to trade (given sets of amm pools) into a convex dual problem over multiple time periods. This convex optimization also works when there is a fixed transaction cost, whereby the optimzation problem becomes a mixed-inteeger convex program (MICP).
   Other papers also worth noting are (WIP):

[ACEL22]
[MMRZ22]
[JDE+22]
[CAEK21]

2. **Can we construct novel incentive mechanisms other than simple trading fee mechanism for liquidity providers so as to secure adequate amount of liquidity? What are the "cost of liquidity" from the protocol's tokenomics perspective (the liquidity pool equivalent of "cost of capital" for corporate finance)?**
   [EAC21] elucidates the trade-off between size of the fee and the cost of arbitrage (as well as the extent of rebalancing) using dynamic programming of cost optimization (a control-inspired approach). Especially in geometric mean market makers under geometric brownian motions, costs are minimized as fees approach zero.

   [O2] breaks down the return for LP into three components: inventory holding return($\frac{V_{T,FIXED}}{V_0}-1$), adverse selection cost(($\frac{V_T}{V_0}-1$) $-$ ($\frac{V_{T,FIXED}}{V_0}-1$)) and fee yield($\frac{F_T}{V_0}$) where $V_{T,FIXED} = x_0 + y_0 P_T$ is what the staked assets would be worth in USD if the LP had held them passively outside of the AMM.
   Other papers also worth noting are (WIP):
   [AI21]
   [Aoy20]
   [CJ21]
   [CKA+22]
   [DECA22]
   [HSW22]
   [QZG+21]
   [GPH+20]
   [CP12]
   [WM22]

3. **Using differential privacy and/or zero-knowledge proofs, can we find trading curves that ensure certain level of privacy for traders of a liquidity pool?**
   [AEC21a] shows that current CFMMs are incapable of providing privacy of trade given a reasonable assumption of adversary; even with nonzero fees, general homogeneity and unknown marginal price and non-strict concavity respectively, the proof still holds along with uniqueness to the reconstructed value arising in the process of the adversary's attack (but does not yet generalize this proof to more strictly convex CFMMs). However, the authors still suspect there are privacy-guaranteeing CFMMs to be discovered and leaves it as open conjecture.

   [CAE21] shows that, given an adversary that can query transactions (by a set of agents transacting with the pool that is $\mu$-stable and $\kappa$-liquid) $\Delta_1, \Delta_2..\Delta_n$ as a block (but not their original order), the precision of the adversary cannot exceed $\Omega(\kappa)$. Using Uniform Random Execution(URE) to permute the execution order, the paper proves a lower bound in the trade-off between pricing accuracy and privacy of users' trading sizes.
   Other papers also worth noting are (WIP):
   [KDC22]
   [KCCM20]
   [KC20]
   [WCW+22]

4. **Can we improve the vanilla staking model that minimizes the trade-off between security-enhancing aspect of staking and its liquidity level? What economic role does staking play in relation to other digital assets and can we model them?**

[CHT22]
[BSU20]
Other papers also worth noting are (WIP):
[CK22]

# References

[AAE+21] Guillermo Angeris, Akshay Agrawal, Alex Evans, Tarun Chitra, and Stephen Boyd. Constant function market makers: Multi-asset trades via convex optimization. *arXiv preprint arXiv:2107.12484*, 2021.

[AC20] Guillermo Angeris and Tarun Chitra. Improved price oracles: Constant function market makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 80–91, 2020.

[ACE22] Guillermo Angeris, Tarun Chitra, and Alex Evans. When does the tail wag the dog? curvature and market making. 2022.

[ACEL22] Guillermo Angeris, Tarun Chitra, Alex Evans, and Matthew Lorig. A primer on perpetuals. *arXiv preprint arXiv:2209.03307*, 2022.

[AEC21a] Guillermo Angeris, Alex Evans, and Tarun Chitra. A note on privacy in constant function market makers. *arXiv preprint arXiv:2103.01193*, 2021.

[AEC21b] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating market makers. *arXiv preprint arXiv:2103.14769*, 2021.

[AEC21c] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating monotonic payoffs without oracles. *arXiv preprint arXiv:2111.13740*, 2021.

[AECB22] Guillermo Angeris, Alex Evans, Tarun Chitra, and Stephen Boyd. Optimal routing for constant function market makers. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, pages 115–128, 2022.

[AI21] Jun Aoyagi and Yuki Ito. Coexisting exchange platforms: Limit order books and automated market makers. 2021.

[Aoy20] Jun Aoyagi. Liquidity provision by automated market makers. *Available at SSRN 3674178*, 2020.

[BSU20] Pierpaolo Benigno, Linda M Schilling, and Harald Uhlig. Cryptocurrencies, currency competition, and the impossible trinity 2020 bank of canada annual economic conference. 2020.

[CAE21] Tarun Chitra, Guillermo Angeris, and Alex Evans. Differential privacy in constant function market makers. *Cryptology ePrint Archive*, 2021.

[CAEK21] Tarun Chitra, Guillermo Angeris, Alex Evans, and Hsien-Tang Kao. A note on borrowing constant function market maker shares. 2021.

[CHT22] Lin William Cong, Zhiheng He, and Ke Tang. Staking, token pricing, and crypto carry. *Available at SSRN*, 2022.

[CJ21] Agostino Capponi and Ruizhe Jia. The adoption of blockchain-based decentralized exchanges. *arXiv preprint arXiv:2103.08842*, 2021.

[CK22] Tarun Chitra and Kshitij Kulkarni. Improving proof of stake economic security via mev redistribution. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*, pages 1–7, 2022.

[CKA$^+$22] Tarun Chitra, Kshitij Kulkarni, Guillermo Angeris, Alex Evans, and Victor Xu. Defi liquidity management via optimal control: Ohm as a case study. 2022.

[CP12] Yiling Chen and David M Pennock. A utility framework for bounded-loss market makers. *arXiv preprint arXiv:1206.5252*, 2012.

[DECA22] Theo Diamandis, Alex Evans, Tarun Chitra, and Guillermo Angeris. Dynamic pricing for non-fungible resources. *arXiv preprint arXiv:2208.07919*, 2022.

[EAC21] Alex Evans, Guillermo Angeris, and Tarun Chitra. Optimal fees for geometric mean market makers. In *International Conference on Financial Cryptography and Data Security*, pages 65–79. Springer, 2021.

[Eva21] Alex Evans. Liquidity provider returns in geometric mean markets. 2021.

[GPH$^+$20] Lewis Gudgeon, Daniel Perez, Dominik Harz, Benjamin Livshits, and Arthur Gervais. The decentralized financial crisis. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 1–15. IEEE, 2020.

[HK$^+$09] Craig S Hakkio, William R Keeton, et al. Financial stress: What is it, how can it be measured, and why does it matter. *Economic review*, 94(2):5–50, 2009.

[HNH15] Joanne M Hill, Dave Nadig, and Matt Hougan. *A comprehensive guide to exchange-traded funds (ETFs)*. CFA Institute Research Foundation, 2015.

[HSW22] Lioba Heimbach, Eric Schertenleib, and Roger Wattenhofer. Exploring price accuracy on uniswap v3 in times of distress. *arXiv preprint arXiv:2208.09642*, 2022.

[Hul12] John C Hull. Options, futures, and other derivatives. eight edition. *New Jersey: Prentice-Hall*, 2012.

[JDE$^+$22] Nicholas AG Johnson, Theo Diamandis, Alex Evans, Henry de Valence, and Guillermo Angeris. Concave pro-rata games. 2022.

[KC20] Hsien-Tang Kao and Tarun Chitra. Feedback control as a new primitive for defi. 2020.

[KCCM20] Hsien-Tang Kao, Tarun Chitra, Rei Chiang, and John Morrow. An analysis of the market risk to participants in the compound protocol. In *Third International Symposium on Foundations and Applications of Blockchains*, 2020.

[KDC22] Kshitij Kulkarni, Theo Diamandis, and Tarun Chitra. Towards a theory of maximal extractable value i: Constant function market makers. *arXiv preprint arXiv:2207.11835*, 2022.

[LM18] Martin Lettau and Ananth Madhavan. Exchange-traded funds 101 for economists. *Journal of Economic Perspectives*, 32(1):135–54, 2018.

[MMRZ22] Jason Milionis, Ciamac C Moallemi, Tim Roughgarden, and Anthony Lee Zhang. Automated market making and loss-versus-rebalancing. *arXiv preprint arXiv:2208.06046*, 2022.

[O2] Peter O'Neill. Can markets be fully automated? evidence from an "automated market maker". 2022.

[QZG$^+$21] Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. An empirical study of defi liquidations: Incentives, risks, and instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference*, pages 336–350, 2021.

[SJ22] Stefan Scharnowski and Hossein Jahanshahloo. Liquid staking: Basis determinants and price discovery. *Available at SSRN 4180341*, 2022.

[WCW+22] Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng, and Roger Wattenhofer. Cyclic arbitrage in decentralized exchanges. *Available at SSRN 3834535*, 2022.

[WM22] Mike Wu and Will McTighe. Constant power root market makers. *arXiv preprint arXiv:2205.07452*, 2022.

[XPCF21] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols. *arXiv preprint arXiv:2103.12732*, 2021.