Impermanent Loss and Gain of Automated Market Maker Smart Contracts

Hyoung Joong Kim, *Member, IEEE*, Soohyuk Choi, Yong Tae Yoon, Shiyong Yoo, *Member, IEEE*

***Abstract*—Smart contract is an important building block of blockchain. Automated market makers are working without an order book, and they determine the price of assets automatically. It is reported that he automated market makers have the impermanent loss, which causes financial damage to liquidity providers. Impermanent loss makes the liquidity providers hesitant to deposit assets in the liquidity pool. Therefore, their participation incentive from liquidity provision should be anticipated by automatic market makers inherently. However, the existence of impermanent gain has never been reported. Impermanent gain is important to attract liquidity providers without giving compensation incentives. This study shows that for some automated market makers, impermanent gain coexists with impermanent loss. Examples showing the coexistence and conditions are provided.**

***Index Terms*—Blockchain, cryptocurrency, decentralized finance, impermanent gain, impermanent loss, market maker, smart contract.**

I. Introduction

SMART contracts on blockchain [1] are an important building block for many applications, including smart grid [2], energy trading [22], vehicular device [3], cryptocurrency [4], voting [5], education system [6], identity authentication [7], and decentralized finance (DeFi). Smart contracts are automatically and autonomously executed in real-time without human intervention. Therefore, smart contracts can exclude human errors and cronyism. These unmanned systems are considered fair and cost-effective. However, smart contracts become harmful if their vulnerabilities are not thoroughly remedied. One famous vulnerability that is frequently occurring as security hole is the reentrancy attack. DeFi based on smart contracts has grown explosively from 2020, securing credibility and liquidity. These DeFi services include lending, asset management, and decentralized exchange.

An automated market maker (AMM) smart contract is a crucial part of the DeFi ecosystem, in particular, for the decentralized exchange systems. DeFi ecosystems do their functionalities by the decentralized participants without centralized control tower. Meanwhile, AMMs rely on mathematical formulas to facilitate trading and automatically set the price of an asset or multiple assets. AMMs of the decentralized exchanges recently have replaced the traditional order book so that all trades are conducted through swaps on their liquidity pools. AMMs allow the users to buy and sell in real-time without matching orders. The buy-and-sell orders listed in the order book are arranged by price. Moreover, the price of the assets at an exchange is set by the matching order algorithms, such as price-time priority algorithm or price pro-rata algorithm. It is determined by double auction. Sellers and buyers can offer market, limit, or conditional orders on the centralized exchanges. Meanwhile, the AMMs have provided the decentralized exchanges mathematical price valuation models. As those formulas are adopted, market makers are price setters, whereas traders are price takers. That is to say, sellers and buyers have no choice but to accept the price determined by the market maker. As long as the formulas cause impermanent loss, the winners are the arbitrageurs, and the losers are the liquidity providers.

Wang [8] suggested the following requirements to be a good AMM algorithm. Constant function market maker (CFMM) needs to be convex curves or convex hyperplanes to conform to the principle of supply and demand. Another requirement is the robustness against malicious attacks, such as front-running (slippage) attacks [9][21]. Front-running is an action plan where an attacker benefits from prior access to privileged market information about upcoming transactions and trades [9]. Wang [8] also suggested the computational efficiency of the asset amount determination.

Meanwhile, Hanson [10, 11] has proposed market-scoring rule for the market prediction. Recently, Hanson's [10, 11] market-scoring rule, the logarithmic market scoring rule (LMSR), showed the potential of the AMM tool. LMSR is one of the CFMM and AMMs. Note that the LMSR is quite popular because of the following three reasons [12]: (1) it was the first AMM for prediction markets and decentralized exchanges; (2) it has a simple analytical form that is rather complicated than constant function market makers; and (3) it has bounded loss.

Othman *et al*. [13] have proposed liquidity-sensitive LMSR (LS-LMSR) by introducing a parameter and adaptive to the market situation; they aim to make the scoring liquidity sensitive. The LMSR and LS-LMSR algorithms set the price of a

This research was supported by a grant of the Korea Health Technology R&D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (grant number: HI19C0785)

H. J. Kim is with the School of Cybersecurity, and the Cryptocurrency Research Center, Korea University, Seoul, 02841, Korea (e-mail: khj-@korea.ac.kr).

S. Choi is with the SymVerse, Seoul, 02841, Korea (e-mail: contact@symverse.com).

Y. T. Kim is with the Department of Electrical and Computer Engineering, Seoul National University, Seoul, 08826, Korea (e-mail: ytyoon@snu.ac.kr).

S. Yoo is with the Business School, Chung-Ang University, Seoul, 06974, Korea (e-mail: sy61@cau.ac.kr).

cryptocurrency pair by keeping the constant cost value unchanged. A logarithmic function expresses the cost. A bonding curve is a mathematical curve that defines a relationship between price and supply of assets. Bonding curve (between two assets as a pair, such as ETH and USDC, where the ETH is a cryptocurrency with price volatility, and the USDC is a stablecoin) or bonding hyperplane (for more than two assets) can be used for setting the price.

CFMM [14] sets the price by maintaining the cost value unchanged (i.e., equal to a constant). Other types of algorithms, such as constant product market maker (CPMM) algorithm [15], constant sum market maker (CSMM) algorithm, and constant mean market maker (CMMM) algorithm [16], also set the price in such a way that the cost value remains unchanged over the bonding curves or bonding hyperplanes. Meanwhile, a hybrid approach called StableSwap [17] combines the CPMM and CSMM algorithms to take the advantages of both methods. Constant circle market maker (CCMM) and constant ellipse market maker (CEMM) also do similar thing.

Liquidity providers supply asset pairs to the liquidity pool, and they may lose money and suffer from an impermanent loss (a.k.a. divergent loss). Impermanent loss is the temporary loss of asset values occasionally experienced by liquidity providers because of volatility in a trading pair. Liquidity provider's asset value can be increased or decreased after trading. The composition ratio of assets is changed, and, as a result, the asset price and value are changed after asset trading. Impermanent loss occurs when the deposited asset value is decreased; it is still a loss, whether large or small. This loss is impermanent because it can only be temporary. If the impermanent loss is large, liquidity providers are strongly hesitant to supply liquidity to the liquidity pool. Moreover, the loss disappears when the composition ratio of the assets returns to the original ratio deposited by the liquidity provider. Impermanent loss is a hot topic and has been studied [8, 9, 13, 15, 16, 17, 18, 19].

The contributions of this paper can be summarized as follows. To the best of our knowledge, this study is the first to show that impermanent gain and impermanent loss coexist for some AMMs. Previous study has already shown that CPMM has the property of impermanent loss [16]. Meanwhile, this present study shows that the CPMM does not have impermanent gain property at all. Moreover, CSMM does not have the property of impermanent loss because the price is invariant. However, this study shows that the relative price in the CSMM is not invariant, and the CSMM has both the property of impermanent gain and impermanent loss. For the LS-LMSR and CCMM and AMMs, this study also shows that both impermanent gain and impermanent loss coexist.

This paper is organized as follows. Section 2 introduces the mathematical background of various AMM asset cost functions and asset value functions to define the value difference functions, which indicates impermanent loss and impermanent gain. Section 3 derives the condition to obtain an impermanent gain and shows that impermanent gain can coexist with impermanent loss. Section 4 concludes the paper with some suggestions.

II. Mathematical Background

Consider a pair of two assets where $\boldsymbol{q}_t(x_t, y_t)$ denotes the asset pair with the number of assets x and y at time t. The AMM uses a cost function $C(\boldsymbol{q}_t)$ to set the price of cryptocurrency pairs at a trading. Suppose a liquidity provider has deposited an asset pair (x_0, y_0), where the asset y is a stablecoin. Note that y is considered a unit of account because it is a stablecoin; it is also divisible, fungible, and countable. Its price is unity.

Then, the asset value of the liquidity provider at time 0 is given as follows [16]:

$$V\big(\boldsymbol{q}_0(x_0, y_0)\big) = \frac{y_0}{x_0} \cdot x_0 + y_0 = 2y_0. \tag{1}$$

Composition ratio of the two assets is changed from (x_0, y_0) to (x_n, y_n) by trading two assets. One can add δx to the pool to make $x_n = x_{n-1} + \delta x$; thus, $y_n = y_{n-1} - \delta y$. Similarly, one can add δy to the liquidity pool to make $y_n = y_{n-1} + \delta y$; hence, $x_n = x_{n-1} - \delta x$. The asset value of the pair (x_n, y_n) at time t is computed as follows:

$$V\big(\boldsymbol{q}_n(x_n, y_n)\big) = \frac{y_n}{x_n} \cdot x_n + y_n = 2y_n. \tag{2}$$

However, the value of the original pair composition (x_0, y_0) assessed by the relative price y_n/x_n at time n is computed as

$$V\big(\boldsymbol{q}_n(x_0, y_0)\big) = \frac{y_n}{x_n} \cdot x_0 + y_0. \tag{3}$$

In addition, impermanent loss is computed from the difference D of the two asset values $V\big(\boldsymbol{q}_n(x_n, y_n)\big)$ and $V\big(\boldsymbol{q}_n(x_0, y_0)\big)$, such that

$$D(x_n) = V\big(\boldsymbol{q}_n(x_n, y_n)\big) - V\big(\boldsymbol{q}_n(x_0, y_0)\big). \tag{4}$$

If the value of D is negative, there exists an impermanent loss. Many research works [8, 9, 18, 20] have tackled the impermanent loss. Scholars have tried eliminating or mitigating the impermanent loss. If the value of $D(x_n)$ is positive, an impermanent gain exists. This paper introduces the concept of impermanent gain for the first time.

A. Constant Product Market Maker

CPMM starts from the cost function from the product of x_0 and y_0, such as

$$C\big(\boldsymbol{q}_0(x_0, y_0)\big) = x_0 \cdot y_0 = k. \tag{5}$$

At time n, the number of y_n given x_n is computed from the following equation

$$C\big(\boldsymbol{q}_n(x_n, y_n)\big) = x_n \cdot y_n = k. \tag{6}$$

Note that the CPMM cost function is a hyperbola. Uniswap, a decentralized exchange, uses this formula for a pricing purpose.

One can add δx to the pool to make $x_n = x_{n-1} + \delta x$; then,

$y_n = y_{n-1} - \delta y$. The cost function in Equation (6) is used to determine δy by using $y_n = k/x_n = k/(x_{n-1} + \delta x)$ and obtaining δy by subtraction such that $\delta y = y_n - y_{n-1}$.

Hence, y_n is computed from Equation (6) as follows:

$$y_n = \frac{k}{x_n}. \tag{7}$$

For the CPMM, the relative price of asset x with respect to y at time n is computed from Equations (2) and (7):

$$p_n = \frac{y_n}{x_n} = \frac{k}{x_n^2}. \tag{8}$$

Thus, the asset value of the pair (x_n, y_n) at time t is computed from Equations (2) and (7) as follows:

$$V\big(\boldsymbol{q}_n(x_n, y_n)\big) = 2 \cdot \frac{k}{x_n}. \tag{8}$$

Hence, $D(x_n)$ of the CPMM is computed from Equations (2), (3), and (9):

$$D(x_n) = 2 \cdot \frac{k}{x_n} - \Big(\frac{k}{x_n^2} \cdot x_0 + y_0\Big). \tag{10}$$

B. Liquidity-Sensitive Logarithmic Market Scoring Rule

Similarly, for the LMSR and LS-LMSR, the cost function is given as follows:

$$C\big(\boldsymbol{q}(x_n, y_n)\big) = b \cdot \ln\big(e^{x_n/b} + e^{y_n/b}\big) = k. \tag{11}$$

Hence, y_n is computed from Equation (11):

$$y_n = b \cdot \ln\big(e^{k/b} - e^{x_n/b}\big). \tag{12}$$

Thus, the asset value of the pair (x_n, y_n) at time t is computed from Equations (2) and (12) as follows:

$$V\big(\boldsymbol{q}_n(x_n, y_n)\big) = 2 \cdot b \cdot \ln\big(e^{k/b} - e^{x_n/b}\big). \tag{13}$$

For the LS-LMSR, the relative price of the asset x with respect to y is at time n is computed as:

$$p_n = \frac{y_n}{x_n} = b \cdot \ln\left(e^{\frac{k}{b}} - e^{\frac{x_n}{b}}\right)/x_n. \tag{14}$$

C. Constant Sum Market Maker

For the CSMM, the cost function is given as follows:

$$C\big(\boldsymbol{q}(x_n, y_n)\big) = x_n + y_n = k. \tag{15}$$

Hence, y_n is computed from Equation (15) as follows:

$$y_n = k - x_n. \tag{16}$$

Thus, the asset value of the pair (x_n, y_n) at time t is computed from Equations (2) and (16) as follows:

$$V\big(\boldsymbol{q}_n(x_n, y_n)\big) = 2 \cdot (k - x_n). \tag{17}$$

D. Constant Circle Market Maker

CCMM has been proposed by Wang [8]. For the CCMM, the relative price and the change in the asset values are computed with the given cost function as follows:

$$C\big(\boldsymbol{q}(x_n, y_n)\big) = (x_n - a)^2 + (y_n - b)^2 = k. \tag{18}$$

Hence, y_n is computed from Equation (18) as follows:

$$y_n = \sqrt{k - (x_n - a)^2} + b. \tag{19}$$

Thus, the asset value of the pair (x_n, y_n) at time t is computed from Equations (2) and (19):

$$V\big(\boldsymbol{q}_n(x_n, y_n)\big) = 2 \cdot \big(\sqrt{k - (x_n - a)^2} + b\big). \tag{20}$$

III. Impermanent Loss and Impermanent Gain

The asset value difference is a good barometer to show whether there is impermanent loss. The difference value $D(x_n)$ is calculated from Equations (2) and (3) as follows:

$$D(x_n) = 2y_n - \Big(\frac{y_n}{x_n} x_0 + y_0\Big). \tag{21}$$

Equation (21) is simplified:

$$D(x_n) = \Big(2 - \frac{x_0}{x_n}\Big) y_n - y_0. \tag{22}$$

If $D(x_n)$ is zero, then impermanent loss does not exist. A negative $D(x_n)$ denotes impermanent loss, whereas a positive $D(x_n)$ denotes impermanent gain. The sign of the difference $D(x_n)$ is determined by Equation (22).

Theorem 1: If $x_n = x_0$, then $D(x_n)$ is zero, no matter what AMM is used.

Proof: If $x_n = x_0$, then $y_n = y_0$. Thus, from Equation (22), when $x_n = x_0$ and $y_n = y_0$, then $D(x_n)$ is zero regardless of the type of AMM. ■

A. Constant Product Market Maker

For the CPMM, the CPMM AMM has the property of impermanent loss because showing that the sign of $D(x_n)$ is nonnegative is easy. For the CPMM, $D(x_n)$ is computed from Equations (7) and (22) as follows:

$$D(x_n) = \left(2 - \frac{x_0}{x_n}\right)\left(\frac{k}{x_n}\right) - \left(\frac{k}{x_0}\right). \quad (23)$$

Note that $D(x_n)$ in Equation (23) is rewritten as

$$D = \frac{1}{x_n^2}\left[-\left(\frac{k}{x_0}\right)x_n^2 + 2kx_n - kx_0\right]. \quad (24)$$

Equation (24) contains a quadratic function of x_n inside the square brackets. Note that the determinant Δ of the quadratic function is zero. It implies that $D(x_n)$ is convex upward; hence, its maximum value is zero. Thus, we can easily show that $D(x_n)$ is always negative except for $x_n = x_0$ no matter what the values of x_n, x_0, and k are. For $x_n = x_0$, $D(x_n)$ is zero. It implies that CPMM AMM never has the property of impermanent gain. The CPMM liquidity providers always have high chance of losing money. Thus, liquidity providers do not want to provide their assets to the liquidity pool if they are not given enough incentives to offset the losses.

B. Constant Sum Market Maker

The number of assets for the CSMM AMMs is determined by Equation (15). The price of x_n is determined as

$$p_n = \frac{y_n}{x_n} = \frac{k - x_n}{x_n}. \quad (25)$$

Here, note that the relative price of x_n is varying because the relative price is a function of x_n, as shown in Equation (25). The range of the relative price p_n is $(0, \infty)$ because the domain of x_n is $(0, k)$. Thus, the price of x_n is varying, and not a constant, which contradicts existing research works [16].

For the CSMM, from Equations (15) and (22), $D(x_n)$ is computed as follows:

$$D = \left(2 - \frac{x_0}{x_n}\right)(k - x_n) - (k - x_0). \quad (26)$$

Note that $D(x_n)$ in Equation (26) is rewritten as

$$D = \frac{1}{x_n}[-2x_n^2 + (k + 2x_0)x_n - kx_0]. \quad (27)$$

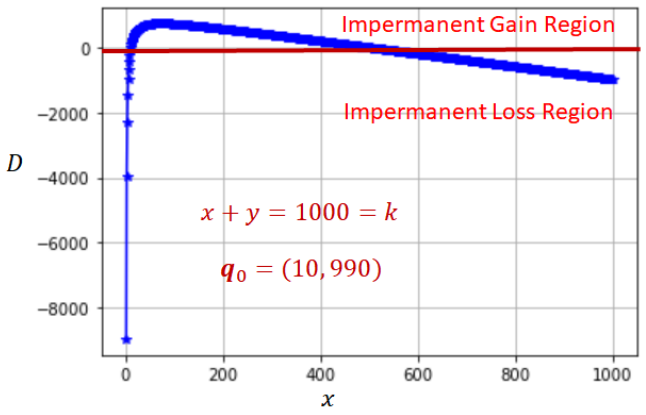

Figure 1. Loss and gain regions of a CSMM AMM

Equation (27) contains a quadratic function of x_n inside the square brackets. Note that the determinant Δ of the quadratic function is given as $\Delta = (k - 2x_0)^2$. The determinant shows us two important facts. The first fact is that both impermanent loss and impermanent gain coexist for $x_0 \neq k/2$. The second fact is that only impermanent loss exists for $x_0 = k/2$. Thus, we can easily show that $D(x_n)$ can be either positive or negative or zero, depending on the values of x_n, x_0, and k. When Equation (27) has two roots $x_n = k/2$ and $x_n = x_0$, both impermanent loss and impermanent gain coexist.

Theorem 2: If $x_0 \neq k/2$, then CSMM AMM has the property of impermanent gain for $x_0 < x_n < k/2$ or $k/2 < x_n < x_0$.

Proof: See the paragraph above the Theorem 2. ■

Observation 1: If $x_0 = y_0 = k/2$, CSMM AMM for Equation (15) has an impermanent loss property only for all x_n and y_n, which are both positive.

Figure 1 shows that impermanent gain occurs for a set of two x_0 values. In this case, the asset cost function is $x + y = 1000$, and the initial asset pair is given as $\boldsymbol{q}_0 = (10, 990)$, for example. The difference $D(x_n)$ is given as follows:

$$D = \frac{1}{x_n}[-2x_n^2 + 1020x_n - 10000]. \quad (28)$$

Thus, for $x_n = 10$ or $x_n = 500$, $D(x_n)$ is zero, which states that this CSMM AMM system has no loss or gain at these points. For $10 < x_n < 500$, the CSMM AMM has impermanent gain. Note that impermanent gain is innate in this case for the given initial asset pair. In Figure 1, at $x_n = 10$, zero crossing happens. Naturally, x_n is equal to x_0. However, at $x_n = 500$, another zero crossing happens. Thus, the left-hand side region from $x_n = 10$ is the impermanent loss region. Similarly, the right-hand side region from $x_n = 500$ is the impermanent loss region. The middle region between $x_n = 10$ and $x_n = 500$ is the impermanent gain region.

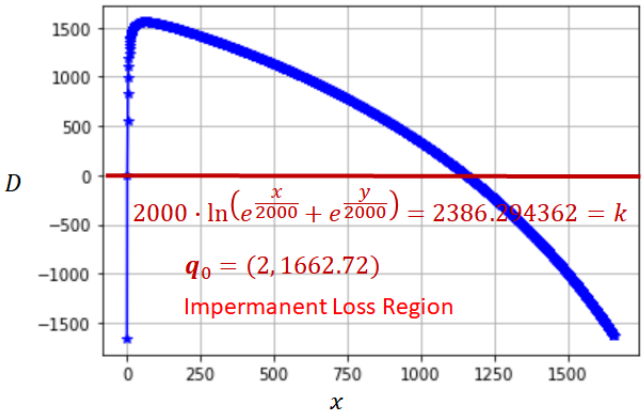

Figure 2. Loss and gain regions of an LS-LMSR AMM

In this example, impermanent loss region and impermanent

gain region coexist for all initial asset pairs $\boldsymbol{q}_0 = (x_0, y_0)$ except the value $x_0 = 500$. The CSMM AMM with the initial asset pair, for example, $\boldsymbol{q}_0 = (500, 500)$ and the asset cost function $x + y = 1000$, there is no impermanent gain region only in this condition. The existence of the impermanent gain region depends on the type of AMM, asset cost function with different constant k, and initial asset pair with different values of x_0.

C. B. *Liquidity-Sensitive Logarithmic Market Scoring Rule*

For the LS-LMSR, the value of $D(x_n)$ is a high-order function of x_n. Therefore, the closed-form solution cannot be easily derived, and we cannot show analytically whether this AMM has the property of impermanent loss or impermanent gain. Figure 2 shows an example of a situation similar to Figure 1.

The asset cost function, in this case, is given as Equation (13), where $b = 1000$. For $\boldsymbol{q} = (1000, 1000)$, the value of k is 2386.294632. If the initial asset pair is $\boldsymbol{q}_0 = (2, 1662.72)$, we can obtain Figure 2 that contains both impermanent loss and impermanent gain regions. Two zero crossings exist: one occurs at $x_n = 2$, and the other one is somewhere between $x_n = 1154$ and $x_n = 1156$. In this example, impermanent loss region and impermanent gain region coexist for all initial asset pair $\boldsymbol{q}_0 = (x_0, y_0)$ for the values $x_0 < 271$.

Observation 2: If $x_0 = y_0$, LS-LMSR AMM for Equation (11) has an impermanent loss property only for all x_n and y_n, which are both positive.

D. *Constant Circle Market Maker*

For the CCMM AMMs, the value of $D(x_n)$ is also a high-order function of x_n. Therefore, the closed-form solution cannot be easily derived, and we cannot show analytically whether this AMM has the property of impermanent loss or impermanent gain. Figure 3 shows an example of the situation similar to Figures 1 and 2.

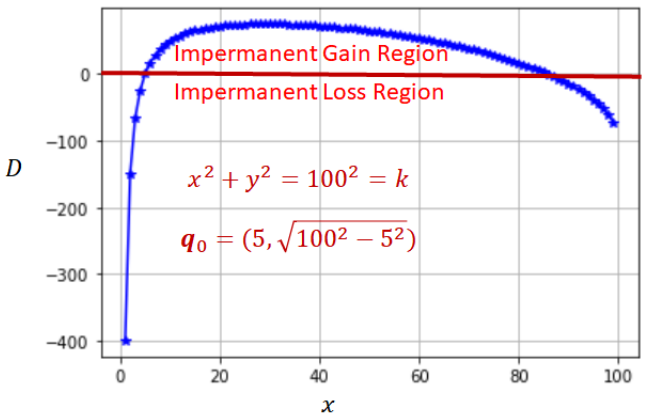

Figure 3. Loss and gain regions of a CCMM AMM

The asset cost function, in this case, is given as Equation (18), where $a = 0$, $b = 0$, and $k = 100^2$. For $\boldsymbol{q} = (100/\sqrt{2}, 100/\sqrt{2})$, the value of k is 100^2. If the initial asset pair is $\boldsymbol{q}_0 = (5, 99.8749)$, we can obtain Figure 3 containing both impermanent loss and impermanent gain regions. Similarly, there are two zero crossings: one occurs at $x_n = 5$, and the other one is somewhere between $x_n = 85$ and $x_n = 87$. In this example, impermanent loss region and impermanent gain region coexist for all initial asset pair $\boldsymbol{q}_0 = (x_0, y_0)$ except the value $x_0 = 100/\sqrt{2}$.

Appendix A shows the condition when the $D(x_n)$ has the property of impermanent loss only for the asset cost function $x^2 + y^2 = k$. Based on this simple case, we can derive the condition having both impermanent loss and impermanent gain property.

Observation 3: If $x_0 = \frac{k}{\sqrt{2}} + a$, and $y_0 = \frac{k}{\sqrt{2}} + b$, then CCMM AMM for Equation (18) has impermanent loss property only for all x_n and y_n, which are both positive.

IV. Concluding Remarks

This study reviews four constant function market makers: LS-LMSR, CPMM, CSMM, and CCMM. For the first time, this study showed the existence of impermanent gain mathematically and computationally thorough experiments. This paper showed that CPMM has impermanent loss property only. Meanwhile, LS-LMSR, CSMM, and CCMM can have both impermanent loss and impermanent gain altogether. For a specific condition, they have impermanent loss property only (see Observations in the previous section).

Even though an impermanent loss exists in CPMM AMM, this market maker attracted a large amount of total valued locked and leads the decentralized exchange markets. Liquidity providers want impermanent gain rather than impermanent loss. The existence of impermanent gain will be fully exploited in the future DeFi systems. However, impermanent gain also has the problem. Liquidity providers want to withdraw the assets from the liquidity pool when impermanent gain occurs. When liquidity providers encounter impermanent gain, the liquidity provider earns extra profits in addition to the deposited assets. Thus, the liquidity providers are motivated to leave the pool, taking advantage of the assets they deposited and the kind of windfall profit that comes from impermanent gain. Meanwhile, impermanent loss makes the liquidity providers passive in joining the pool as they lose by depositing the asset, whereas impermanent gain makes the liquidity providers take extra profit and leave the pool. However, liquidity providers may prefer impermanent loss to impermanent gain.

References

[1] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 49, no. 11, pp. 2266-2277, 2019.

[2] A. Kumari, R. Gupta, S. Tanwar, S. Tyagi and N. Kumar, "When blockchain meets smart grid: Secure energy trading in demand response management," *IEEE Network*, vol. 34, no. 5, pp. 299-305, 2020.

[3] L. R. Abbade, F. M. Ribeiro, M. H. da Silva, A. F. P. Morais, E. S. de Morais, E. M. Lopes, A. M. Alberti, and J. Rodrigues, "Blockchain applied to vehicular odometers," *IEEE Network*, vol. 34, no. 1, pp. 62-68, 2020.
[4] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 48, no. 9, pp. 1421-1428, 2018.
[5] K. Lee, J. I. James, T. G. Ejeta, and H. J. Kim, "Electronic voting service using blockchain," *Journal of Digital Forensics, Security and Law*, vol. 11, no. 2, pp. 123-135, 2016
[6] M Turkanović, M. Hölbl, K Košič, M Heričko, and A Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112-5127, 2018.
[7] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241-251, 2020
[8] Y. Wang, "Automated market makers for decentralized finance (DeFi)," Available at https://arxiv.org/pdf/2009.01676.pdf
[9] S. Eskandari, S. Moosavi, and J. Clark, "SoK: Transparent dishonesty: Front-running attacks on blockchain," *3rd Workshop on Trusted Smart Contracts*, 2019. Available at http://fc19.ifca.ai/wtsc/TransparentDishonesty.pdf
[10] R. Hanson, "Combinatorial information market design," *Information Systems Frontiers*, vol. 5, no. 1, pp. 107–119, 2003
[11] R. Hanson, "Logarithmic markets coring rules for modular combinatorial information aggregation," *The Journal of Prediction Markets*, vol. 1, no. 1, pp. 3–15, 2007
[12] A. Othman, Automated Market Making: Theory and Practice, PhD Dissertation, Carnegie Mellon University, 2012.
[13] A. Othman, D. M. Pennock, D. M. Reeves, and T. Sandholm, "A practical liquidity-sensitive automated market maker," *ACM Transactions on Economics and Computation*, vol. 1, no. 3, pp. 1–25, 2013.
[14] G. Angeris and T. Chitra, "Improved price oracles: Constant function market makers," *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pp. 81-90, 2020.
[15] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra, " An analysis of Uniswap markets, *Cryptoeconomic Systems Journal*, 2019, Available at SSRN: https://ssrn.com/abstract=3602203.
[16] B. Krishnamachari, Q. Feng, and E. Grippo, "Dynamic curves for decentralized autonomous cryptocurrency exchanges," 2021. Available at https://arxiv.org/pdf/2101.02778.pdf.
[17] M. Egorov, "StableSwap-efficient mechanism for stablecoin liquidity," 2019. Available at https://www.btcmoney.cc/uploads/home/20200901/88eaf78993e5ab93a5860afddc81fc74.pdf.
[18] G. Angeris, A. Evans, and T. Chitra, "When does the tail wag the dog? Curvature and market making," 2020. Available at https://arxiv.org/pdf/2012.08040.pdf
[19] F. Martinelli and N. Mushegian. "Balancer: A non-custodial portfolio manager, liquidity provider, and price sensor," 2019. Available at https://balancer.finance/whitepaper.
[20] B. Krishnamachari, Q. Feng, and E. Grippo, "Dynamic curves for decentralized autonomous cryptocurrency exchanges," 2021. Available at https://arxiv.org/pdf/2101.02778.pdf..
[21] A. Evans, "Liquidity provider returns in geometric mean transparent dishonesty: Front-running attacks on blockchain markets," 2020. Available at https://arxiv.org/pdf/2006.08806.pdf
[22] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Engineering*, vol. 14, no. 8, pp. 3690-3700, 2018.

APPENDIX A

For the CCMM asset cost function $x_n^2 + y_n^2 = k$, $D(x_n)$ is given from Equation (21) as follows:

$$D(x_n) = 2y_n - \left(\frac{y_n}{x_n}x_0 + y_0\right).$$

The condition that $D(x_n)$ is to be zero is given as

$$2y_n x_n - y_n x_0 - y_0 x_n = 0,$$

$$2y_n x_n - y_n x_0 = y_0 x_n,$$

where

$$y_n = \sqrt{k - x_n^2} \geq 0,$$

and hence,

$$2\sqrt{k - x_n^2}x_n - \sqrt{k - x_n^2}x_0 = y_0 x_n$$

$$\left(2\sqrt{k - x_n^2}x_n - \sqrt{k - x_n^2}x_0\right)^2 = (y_0 x_n)^2$$

$$-4x_n^4 + 4x_0 x_n^3 + (4k - x_0^2)x_n^2 - 4kx_0 x_n + kx_0^2 = y_0^2 x_n^2.$$

The left-hand side of the equation is a fourth-order polynomial open downward, whereas the right-hand side is a quadratic polynomial open upward. Thus, the following three possibilities exist:

1. When both side polynomials do not meet, then the right-hand side polynomial has larger value for all x_n, and thus, $D(x_n)$ is negative. It means that the AMM has the property of impermanent loss only.
2. When both side polynomials meet at a single point, then the situation is similar to the case of 1 (i.e., impermanent loss only).
3. When both side polynomials meet at more than a single point, then $D(x_n)$ is either negative or positive, depending on the value of x_n. It means that the AMM has the property of impermanent loss and impermanent gain altogether.

Hyoung Joong Kim is a professor at the School of Cybersecurity, Korea University, Seoul, Korea. He is the head of the Cryptocurrency Research Center. He received his B.S. degree in electrical engineering and M.S. and Ph.D. degrees in control and instrumentation engineering, from the Seoul National University, Seoul, Korea. His research interests include information security, cryptocurrency, and data hiding.

Soohyuk Choi is the founder of Symverse blockchain and serves as the president of Korea Blockchain Startup Association and as an adjunct professor of the School of Cybersecurity, Korea University, Seoul, Korea. He received his B.A. and M.A. degrees in economics from Yonsei University in 1985 and the Ph.D. degree in economics from Northwestern University, Evanston, IL, in 1992. His research interests include game theory and cryptocurrency.

Yong Tae Yoon received the B.S., M.Eng., and Ph.D. degrees from M.I.T., Cambridge, MA, USA, in 1995, 1997, and 2001, respectively. He is currently a Professor at the Department of Electrical and Computer Engineering, Seoul National University, Seoul, South Korea. His research interests include power economics, smart grid/microgrid, and decentralized operation.

Shiyong Yoo received his B.S. and MA degrees on Agricultural Economics from Seoul National University, Seoul, Korea, in 1991 and 1993. He also received his Ph. D on Resource Economics and Finance from Cornell University, NY, USA, in 2003. He is currently a Professor of Finance at CAU Business School, and the Head of the Financial AI Research Center, Chung-Ang University, Seoul, Korea. His research interests include financial engineering and algorithm trading.