International Journal of Industrial Engineering, 31(6), 1426-1437, 2024

# IMPERMANENT LOSS MITIGATION FOR DECENTRALIZED EXCHANGES THROUGH OPTIMIZATION

**Gyu M. Lee[1] and Hyoung Joong Kim[2, 3, *]**

[1]Department of Industrial Engineering
Pusan National University
Busan, Korea

[2]Department of Digital Finance Management
Hoseo University
Cheonan, Korea
[*]Corresponding author's e-mail: khj-@korea.ac.kr

[3]Next-generation Communication Convergence and Open Sharing System (NCCOSS)
Kookmin University
Seoul, Korea

This paper presents a novel combinatorial optimization problem to address impermanent loss in decentralized exchange (DEX) smart contract protocols. Despite a decade of attempts, eliminating impermanent loss has remained a persistent challenge in decentralized finance. We introduce a new pricing methodology based on the actual asset values within liquidity pools and define the concept of value gain. Our key theoretical contribution is the mathematical proof of a sufficient condition for impermanent gain, which we term "origin crossing." We demonstrate that impermanent gain occurs whenever a transaction crosses the origin. Building on this finding, we propose a new Maximal Extractable Value (MEV) extraction mechanism utilizing transaction batching and reordering optimization. This approach is proposed for a future smart contract protocol that, when deployed as open-source blockchain infrastructure, offers multiple benefits to the DeFi ecosystem: reduced gas costs, mitigation of impermanent loss, and minimized slippage through optimization modeling. This research advances both the theoretical understanding of impermanent loss and provides practical solutions for DEX implementation.

**Keywords:** Decentralized Exchanges, Impermanent Loss, Mathematical Pricing, Permutation of transactions

(*Received on November 6, 2024; Accepted on December 6, 2024*)

## 1. INTRODUCTION

In recent years, cryptocurrency has emerged as a revolutionary force in the financial world, challenging traditional economic systems and sparking widespread interest and debate. Originating with the advent of Bitcoin in 2009, cryptocurrencies are digital or virtual currencies that use cryptography for security, making them difficult to counterfeit. Unlike conventional currencies issued by central banks, cryptocurrencies operate on decentralized networks based on blockchain technology, which ensures transparency, security, and immutability of transactions while preventing double-spending.

One of the primary motivations for using cryptocurrencies is to protect against inflation and the depreciation of fiat currencies. Unlike traditional money (fiat), most cryptocurrencies have a limited supply, often capped by mathematical algorithms. This scarcity makes it impossible for any government or central bank to arbitrarily increase the supply, thus safeguarding against inflation. As central banks print more money during economic crises, the value of fiat currency can decrease. Cryptocurrencies, with their fixed supply, offer an alternative store of value that isn't subject to such manipulation.

Cryptocurrencies operate on decentralized networks (blockchains) without central authority. This decentralization provides several benefits: 1) *Financial Sovereignty* because users have direct control over their funds without relying on banks or intermediaries; 2) *Reduced Transaction Fees* since cryptocurrency transactions often have lower fees compared to traditional banking systems; 3) *Global Accessibility* because anyone with an internet connection can participate in the cryptocurrency ecosystem, regardless of their locations or nationalities. Cryptocurrencies enable seamless cross-border transactions. Traditional international money transfers by SWIFT systems can be slow, expensive, and subject to currency

conversion fees. With cryptocurrencies, individuals can send funds globally without intermediaries, making remittances more efficient.

Cryptocurrencies provide access to financial services for the unbanked and underbanked populations. Many people worldwide lack access to traditional banking infrastructure, but they can participate in the crypto economy using a smartphone and an internet connection.

The potential for high returns motivates many investors to participate in the cryptocurrency market. While it's a volatile space, some individuals see it as an opportunity to diversify their investment portfolios. Speculators also engage in cryptocurrency trading, aiming to profit from price fluctuations. However, this speculative aspect can be risky. Beyond investment, the underlying blockchain technology has various applications. Smart contracts, decentralized finance (DeFi), non-fungible tokens (NFTs), and other innovations are driving interest in cryptocurrencies. People are motivated by the potential impact of blockchain technology on various industries, including finance, supply chain, healthcare, and more.

The concept of cryptocurrency is deeply rooted in the principles of cryptography and computer science. The groundwork was laid by the development of digital currencies and the rise of cryptographic techniques in the late 20th century. David Chaum (1983) introduced the idea of digital cash through his paper "Blind Signatures for Untraceable Payments," proposing a form of encrypted currency. Wei Dai (1998) proposed "b-money," an anonymous, distributed electronic cash system. Around the same time, Nick Szabo developed the concept of "bit gold," which included the core elements of modern cryptocurrencies, like proof of work. The pseudonymous Satoshi Nakamoto (2008) published the Bitcoin whitepaper, "Bitcoin: A Peer-to-Peer Electronic Cash System," detailing a decentralized digital currency system. Bitcoin was officially launched in 2009 as open-source software, marking the beginning of the cryptocurrency era.

Since then, thousands of cryptocurrencies have been developed, each with unique features and applications. From the rise of Ethereum, which introduced smart contracts, to the development of decentralized finance (DeFi) platforms, the cryptocurrency landscape continues to evolve rapidly, promising to reshape the future of finance.

Centralized cryptocurrency exchanges (CEXs) have played a critical role in the growth and adoption of digital assets by providing a user-friendly platform for buying, selling, and trading cryptocurrencies. However, despite their popularity and utility, these exchanges face several significant problems and challenges that can undermine their functionality, security, and overall trustworthiness. CEXs operate under a centralized model, where a single entity controls the exchange platform. This centralization contradicts the core principles of cryptocurrencies, which emphasize decentralization and user autonomy. CEXs are prime targets for hackers due to the large amounts of digital assets they hold.

High-profile security breaches have resulted in substantial financial losses for both exchanges and their users. For example, the infamous Mt. Gox hack in 2014 led to the loss of 850,000 Bitcoins, and more recent breaches continue to highlight vulnerabilities in exchange security protocols. Users of CEXs do not have full control over their assets since the exchanges act as custodians. This means that users must trust the exchange to securely manage their funds. In the event of a security breach, mismanagement, or insolvency, users risk losing their assets, as seen in the cases of Mt. Gox and QuadrigaCX. Centralized exchanges operate in a complex and often unclear regulatory environment. They must comply with various laws and regulations, which can vary significantly between jurisdictions. This regulatory uncertainty can lead to operational challenges, fines, and even shutdowns. For instance, exchanges may face regulatory pressures related to anti-money laundering (AML) and know-your-customer (KYC) requirements, leading to increased compliance costs and potential legal risks. CEXs can be susceptible to market manipulation practices such as wash trading, spoofing, and front-running. These activities can distort market prices and trading volumes, undermining the integrity of the market and eroding investor confidence. Technical issues, system failures, and downtime are significant concerns for CEXs. These operational risks can result in service disruptions, which may lead to financial losses for traders who are unable to execute trades during critical market movements. For example, major exchanges have experienced outages during periods of high market volatility, frustrating users and impacting their trading activities. The operations of CEXs are often opaque, with limited visibility into their internal processes, order books, and financial health. This lack of transparency can create distrust among users, who may be concerned about the potential for insider trading, preferential treatment, or hidden fees. The insolvency of the CEX FTX in 2022 caused uncertainty and highlighted the need for better transparency practices. CEXs may face geographic and legal restrictions that limit their ability to serve users in certain regions. Regulatory constraints can force exchanges to restrict access to users from specific countries, reducing the availability of services and limiting the growth of the global cryptocurrency market. Many CEXs charge high fees for transactions, deposits, withdrawals, and other services. These fees can be a barrier for small-scale traders and investors, reducing the accessibility and attractiveness of the platform. CEXs also have the authority to freeze accounts, restrict withdrawals, and delist cryptocurrencies. This centralized control can lead to censorship, limiting users' ability to freely access and transact with their digital assets. Such actions may occur due to regulatory pressure, legal disputes, or internal policies. CEXs offer higher liquidity compared to decentralized exchanges. However, this liquidity relies on the exchange's ability to attract traders and maintain order books. If an exchange faces liquidity issues or sudden outflows, it can disrupt trading and impact market stability.

Decentralized exchanges (DEXs) have emerged as a transformative force in the cryptocurrency ecosystem, addressing many of the issues associated with CEXs. Operating on blockchain technology and smart contracts, DEXs facilitate peer-to-peer trading of digital assets without the need for intermediaries.

One of the primary advantages of DEXs is their improved security. Since users retain control of their private keys and funds, the risk of large-scale hacking incidents is significantly reduced. By eliminating the centralized custodial model, DEXs mitigate the risk of major security breaches that have plagued CEXs. DEXs often offer greater privacy compared to CEXs. They typically do not require extensive know-your-customer (KYC) procedures, allowing users to trade without disclosing personal information. This anonymity appeals to users who prioritize privacy and wish to avoid surveillance and data breaches associated with centralized platforms. By enabling users to maintain control of their funds throughout the trading process, DEXs minimize custodial risk.

There is no need to deposit funds into a centralized wallet controlled by the exchange, thereby reducing the risk of loss due to exchange insolvency, mismanagement, or fraud. DEXs are inherently more resistant to censorship and regulatory intervention. Since they operate on decentralized networks without a single point of control, it is difficult for authorities to impose restrictions or shut down the platform. This resilience is crucial in jurisdictions with stringent regulatory environments and enhances the global accessibility of cryptocurrency trading. The operations of DEXs are typically transparent and verifiable on the blockchain. All transactions are publicly recorded, ensuring transparency and accountability. Users can independently verify the integrity of the order book, trade history, and smart contract operations, fostering a higher level of trust in the platform. DEXs often have lower fees compared to CEXs. Since there are no intermediaries involved in the trading process, transaction costs are minimized.

Additionally, DEXs do not charge listing fees, making it more cost-effective for new and emerging cryptocurrencies to be traded. DEXs provide global access to financial services without geographical restrictions. Users from any part of the world can trade on a DEX as long as they have an internet connection and a compatible cryptocurrency wallet. This inclusivity is crucial for promoting financial inclusion and democratizing access to digital assets. DEXs embody the core ethos of decentralization, empowering users by removing the need for trust in a central authority. This shift from centralized control to decentralized governance aligns with the foundational principles of blockchain technology and promotes a more equitable financial ecosystem. The open-source nature of many DEX platforms fosters innovation and flexibility. Developers can build and integrate new features, improve existing protocols, and create new decentralized financial (DeFi) applications on top of DEX infrastructures. This continuous innovation drives the evolution of the cryptocurrency market and expands the range of available financial services. The decentralized architecture of DEXs eliminates single points of failure, enhancing the overall robustness and reliability of the platform. This resilience is crucial for maintaining uninterrupted service, especially in the face of technical issues, regulatory pressures, or malicious attacks.

DEXs present a way to set prices mathematically unlike the order book-based trading system, which has been a widely-known method to determine prices in the stock markets for over 400 years. Impermanent loss (IL) is a phenomenon that affects liquidity providers (LPs) in DEXs, particularly those using automated market maker (AMM) models like Uniswap, SushiSwap, and Balancer. It occurs when the value of assets deposited into a liquidity pool changes compared to when they were deposited. This change can lead to a situation where the liquidity provider's assets are worth less than they would have been if they had simply held the assets outside the pool. Impermanent loss is one of the most significant research topics in DeFi (Loesch *et al.*, 2021; Aigner and Dhaliwal, 2021; Boueri1, 2021; Tiruviluamala *et al.*, 2022; Hafner and Dietl, 2024; Tangri *et al.*, 2023)

Consider a liquidity pool (LP) containing equal values of Ethereum (ETH) and a stablecoin (USDT). If the price of ETH increases significantly, arbitrage traders buy ETH from the pool (because it is cheaper there) and sell it on the open market (where it is more expensive), causing the ETH in the pool to decrease and USDT to increase. The liquidity provider's share of the pool now consists of less ETH and more USDT. When the liquidity provider withdraws their assets, they receive less ETH and more USDT than they initially deposited. If the value of ETH has increased significantly, the total value of their assets may be lower than if they had simply held onto their original ETH and USDT outside of the pool.

Impermanent loss is inevitable in DEXs due to several reasons: Firstly, cyptocurrencies are known for their price volatility. As prices fluctuate, the relative values of assets in a liquidity pool change, leading to impermanent loss. Given the nature of crypto markets, these price changes are a constant and unavoidable feature. Secondly, the design of AMM-based DEXs relies on arbitrage traders to maintain price consistency with external markets. This arbitrage activity is crucial for the functioning of the DEX but inherently leads to impermanent loss as it adjusts the asset balances in the pool. Thirdly, for DEXs to function efficiently and provide liquidity for traders, they need to adjust the asset ratios in response to market prices. This automatic adjustment process, while ensuring market efficiency, also means that liquidity providers experience impermanent loss whenever there is significant price movement.

It is known that there is no perfect way to hedge against impermanent loss without sacrificing the benefits of providing liquidity, such as earning trading fees and rewards. Liquidity providers must accept a certain level of risk as part of the trade-

off for the potential gains. While impermanent loss cannot be completely avoided, there are strategies to mitigate its impact. Providing liquidity to pools with a diverse range of assets or stablecoins can reduce the impact of price volatility. To compensate for potential impermanent loss, many DEXs offer incentives, such as liquidity mining rewards. Liquidity providers can actively manage their positions, monitoring market conditions and adjusting their liquidity allocations accordingly. In this study, we find a way to mitigate the recognition of potential impermanent loss by optimizing the sequences (reordering) and volumes (batching) of transactions in DEXs, considering the fact that a certain number of transactions are recorded and publicized in every block generation.

## 2. PRICING METHOD IN DECENTRALIZED EXCHANGE

Impermanent loss can be considered as a penalty imposed on liquidity providers of liquidity pools in all DEXs. It occurs in a situation where liquidity providers gain more benefit from not depositing assets than depositing them into the liquidity pool. However, most liquidity providers still provide liquidity despite the impermanent loss because they expect transaction fees to compensate for the loss and to obtain governance token rewards. In addition, it is known that most AMMs have failed to avoid impermanent loss. Kim et al. (2022) calculated the amount of the impermanent loss of four automated market makers under the assumption that the price of an asset in a liquidity pool is the ratio of the numbers of two assets and showed that impermanent gain is achievable in certain cases. However, this case is limited effectively to only the CPMM. As Kim et al. (2024) showed, the only case where the price is expressed as a ratio of the numbers of two assets is the CPMM of Uniswap v1. We want to show that CPMM impermanent loss can be mitigated by utilizing batching and reordering of multiple transactions. It is important to note that the impermanent loss is computed using the price after trading is completed, with the number of initial assets deposited into the liquidity pool and the number of assets after trading.

This study is important in academia and businesses because it suggests that the impermanent loss is mitigated by rearranging the transactions within blocks. First of all, a discussion about how the asset prices have been calculated in the CPMM model is given and we propose a new pricing method for the assets in liquidity pools of CPMM DEXs.

The current CPMM DEXs have been using a price that is roughly calculated before the asset trading. We will call this price as the reference price. The proposed price is what we call the actual price, which is calculated accurately after the actual trading... The second price is the actual price, which is accurately calculated after the actual trading. These two prices are different, and the amount of the difference is called slippage.

If the reference price is used to calculate the impermanent loss, the impermanent loss seems unavoidable. Kim et al. (2024) have studied the properties of the reference price in the various CFMMs. It has been known that impermanent loss always occurs except when the transactions lead to the initial state of the liquidity pool. This study shows that the impermanent loss is avoidable if the actual price is used and offers the necessary conditions for the impermanent gain. Thus, this study is important to note as a catalyst in studying impermanent loss.

This study is only concerned with a constant product market maker model. This model involves two assets in a liquidity pool. Let them be called the asset coin and stablecoin, respectively. Two variables *x* and *y* are the quantities of the asset coin and stablecoin, respectively. In the CPMM model, the cost function is given as $C(\boldsymbol{q}) = k$, where $k$ is a constant and $\boldsymbol{q}$ represents the state containing *x* and *y*.

Let the prices of the asset coin and stablecoin be $p_x$ and $p_y$, respectively. They are obtained by differentiating the cost function as follows:

$$p_x = \frac{dC(\mathbf{q})}{dx}$$
$$p_y = \frac{dC(\mathbf{q})}{dy}.$$

In AMM models of DEXs, let the prices of the asset coin and stablecoin be $P_x$ and $P_y$, respectively. As the stablecoin price is set at 1, so $P_y = 1$. It is because the stablecoin is used as a unit of account. The actual price, $P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$, is determined as the ratio of the difference between $x_{t-1}$ and $x_t$ (so called $\Delta x$)and the difference between $y_{t-1}$ and $y_t$ (so called $\Delta y$), as follows.

$$P_x(\mathbf{q_t} - \mathbf{q_{t-1}}) = -\frac{y_t - y_{t-1}}{x_t - x_{t-1}} = -\frac{\Delta y}{\Delta x}$$

For any transaction, $\Delta x$ is either positive or negative, while $\Delta y$ is negative or positive, respectively. In other words, $\Delta x$

and $\Delta y$ have opposite signs. Since the price must always be positive, it explains the above equation.

If the difference between $x_{t-1}$ and $x_t$ goes infinitesimal, we write the above equation as follows.

$$P_x(\mathbf{q_t}) = \lim_{x_t \to x_{t-1}} -\frac{y_t - y_{t-1}}{x_t - x_{t-1}} = -\frac{dy_t}{dx_t} = \frac{p_x}{p_y}.$$

The value of the assets in the liquidity pool is given as a product of the corresponding price and quantity as follows.

$$V_x = P_x \cdot x \text{ and } V_y = y\,,$$

where $V_x$ and $V_y$ are the values of the asset coin and stablecoin, respectively.

The terminology impermanent loss was made on the premise that there is no way how the value of the liquidity provider's assets makes a profit. However, it misleads to a belief that permanent or impermanent gain can never exist. Thus, this study defines liquidity provider's value gain, G, as follows:

$$G_t = P_x \cdot (x_t - x_0) + (y_t - y_0),$$

where $x_0$ and $y_0$ refer to the quantities of the asset coin and the stablecoin at the time the liquidity provider first entrusted the asset pair, respectively. If $G_t > 0$, then the liquidity provider benefits from the impermanent gain. Otherwise, one suffers from impermanent loss.

Denote $P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$ and $P_x(\mathbf{q_t})$ as the actual price and the reference price, respectively. It is trivial that these two prices are not equal, as shown above. Note that the actual price is a first-order Markov process, and the reference price is a zero-order Markov process. The previously-known curve of impermanent loss can be expressed using the reference price as follows:

$$G_t(\mathbf{q_t}) = P_x(\mathbf{q_t}) \cdot (x_t - x_0) + (y_t - y_0).$$

In this case, it can be shown that

$$G_t(\mathbf{q_t}) \leq 0.$$

In order words, impermanent loss occurs at all times whenever the reference price is used in calculating the impermanent loss or gain.

In contrast, the actual price can be used in calculating the value gain as follows:

$$G_t(\mathbf{q_t} - \mathbf{q_{t-1}}) = P_x(\mathbf{q_t} - \mathbf{q_{t-1}}) \cdot (x_t - x_0) + (y_t - y_0).$$

In the following, we show this value gain $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$ can be positive if certain conditions are satisifed in the well-known CPMM model. It is an important discovery to shed light on the future of DEXs.

## 3. IMPERMANENT GAIN IN CONSTANT PRODUCT MARKET MAKER MODEL

We start to describe the CPMM model, which is used in Uniswap (Aoyagi and Ito, 2021) and show how to calculate value gain $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$, using an example for easy understanding. Then, the necessary condition for impermanent value gain is given in this section. In the meantime, the condition for impermanent loss is also presented.

As mentioned in Section 1, the CPMM cost function is given as a product of $x_t$ and $y_t$, which are the quantities of the asset coin and stablecoin at time t, respectively.

$$C(\mathbf{q_t}) = x_t \cdot y_t = k.$$

The price of each asset is obtained by differentiating the cost function with respect to the corresponding asset. Thus,

$$p_x(\mathbf{q_t}) = \frac{dC(\mathbf{q_t})}{dx_t} = y_t, \qquad p_y(\mathbf{q_t}) = \frac{dC(\mathbf{q_t})}{dy_t} = x_t.$$

If we calculate reference price $P_x(\mathbf{q_t})$, it is obtained as follows:

$$P_x(\mathbf{q_t}) = \frac{p_x(\mathbf{q_t})}{p_y(\mathbf{q_t})} = \frac{y_t}{x_t} = \frac{k}{x_t^2}.$$

As explained above, it can be proved that value gain $G_t(\mathbf{q_t})$ is always negative or zero when the above reference price is used in the calculation. It means that impermanent loss always takes place.

Now, we want to show that impermanent gain is possible using an example. In this example, we use the actual price $P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$ to calculate the value of assets in the liquidity pool and value gain $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$. Let $x_0 = y_0 = 10$. In CPMM, product constant $k = 100$, which must be maintained at all times. If $x_{t-1} = 5, y_{t-1} = 20$. Assume that a transaction has been made at time t by adding 15 asset coins more into the liquidity pool (i.e., $x_t = 20$). Because $k = 100$, it must be that $y_t = 5$. This transaction was putting 15 asset coins into and taking out 15 stablecoins from the liquidity pool. The actual price of the asset coin is calculated as follows:

$$P_x(\mathbf{q_t} - \mathbf{q_{t-1}}) = -\frac{5-20}{20-5} = 1.$$

Using this actual price, we obtain the following value gain.

$$G_t(\mathbf{q_t} - \mathbf{q_{t-1}}) = 1 \cdot (20-10) + (5-10) = 5.$$

Note that the value gain is positive at 5. In this example, it is observed that a profit is made without loss.

The second example is given in the following. Assume $x_0 = y_0 = 10$. Let $x_{t-1} = 20$ and $y_{t-1} = 5$. Consider a transaction making $x_t = 5$ and $y_t = 20$. Then, the actual price is obtained as follows:

$$P_x(\mathbf{q_t} - \mathbf{q_{t-1}}) = -\frac{20-5}{5-20} = 1.$$

Using this actual price, we obtain the following value gain. +

$$G_t(\mathbf{q_t} - \mathbf{q_{t-1}}) = 1 \cdot (5-10) + (20-10) = 5.$$

It is still positive at 5. It is observed that a profit is made similarly to the first example.

This discovery is important and meaningful to show that the impermanent gain is achieveable when we use the actual price. As seen from examples, CPMM enforces the relative prices of the asset coin with respect to stablecoin during the transaction, which is 1, i.e., the actual price of the asset coin, because 15 asset coins and 15 stablecoin were swapped in the liquidity pool. Therefore, it is more realistic to use the actual price instead of the reference price in DEXs,

Denote $(x_0, y_0)$ as the origin in our study. At this origin, it is conjectured that the sufficient condition for the impermanent gain exists. We denote it as the *origin crossing*, which occurs when a transaction is made in such a way that the quantity of the assets coin crosses the origin. That is, "$x_{t-1} < x_0 < x_t$" or "$x_t < x_0 < x_{t-1}$".

**Theorem 1.** In the CPMM model of $x_t \cdot y_t = k$ for a positive constant $k$, If any transaction makes $x_{t-1} < x_0 < x_t$or $x_t < x_0 < x_{t-1}$, then value gain $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$ is always positive.

**Proof.** For easy understanding, we divide the proof into two cases.

i) $x_{t-1} < x_0 < x_t$

Since $x_{t-1} < x_0 < x_t, y_t < y_0 < y_{t-1}$from $x_t \cdot y_t = k$, which is illustrated in Figure 1. Coordinates of *P*, Q and *O* are $(x_{t-1}, y_{t-1})$, $(x_t, y_t)$, and $(x_0, y_0)$, respectively. In Figure 1, $P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$ is the negative (of the) slope $\overline{PQ}$ as follows.

$$P_x(\mathbf{q_t} - \mathbf{q_{t-1}}) = -\frac{y_t - y_{t-1}}{x_t - x_{t-1}}$$

Similarly, $P_x(\mathbf{q_t} - \mathbf{q_0})$ is the negative slope $\overline{OQ}$ as follows.

$$P_x(\mathbf{q_t} - \mathbf{q}_0) = -\frac{y_t - y_0}{x_t - x_0}$$

From Figure 1, $P_x(\mathbf{q_t} - \mathbf{q}_0) < P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$ and this can be rewritten as follows.

$$-\frac{y_t - y_0}{x_t - x_0} < -\frac{y_t - y_{t-1}}{x_t - x_{t-1}}$$

By multiplying a positive number $(x_t - x_0) > 0$ on both sides, value gain $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$ is obtained and proved to be positive as follows.

$$G_t(\mathbf{q_t} - \mathbf{q_{t-1}}) = -\frac{y_t - y_{t-1}}{x_t - x_{t-1}}(x_t - x_0) + (y_t - y_0) > 0.$$

ii) $x_t < x_0 < x_{t-1}$

Since $x_t < x_0 < x_{t-1}, y_{t-1} < y_0 < y_t$from $x_t \cdot y_t = k$, which is illustrated in Figure 2. Coordinates of P, Q and O are $(x_{t-1}, y_{t-1})$, $(x_t, y_t)$, and $(x_0, y_0)$, respectively. In Figure 2, $P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$ and $P_x(\mathbf{q_t} - \mathbf{q_0})$ are defined as the same equations in case i) for the negative (of the) slopes of $\overline{PQ}$ and $\overline{OQ}$, respectively.

From Figure 2, $P_x(\mathbf{q_t} - \mathbf{q_{t-1}}) < P_x(\mathbf{q_t} - \mathbf{q}_0)$ and this can be rewritten as follows.

$$-\frac{y_t - y_{t-1}}{x_t - x_{t-1}} < -\frac{y_t - y_0}{x_t - x_0}$$

By multiplying a negative number $(x_t - x_0) < 0$ on both sides, value gain $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$ is obtained and proved to be positive as follows.

$$G_t(\mathbf{q_t} - \mathbf{q_{t-1}}) = -\frac{y_t - y_{t-1}}{x_t - x_{t-1}}(x_t - x_0) + (y_t - y_0) > 0.$$

Both cases i) and ii) complete the proof. ■

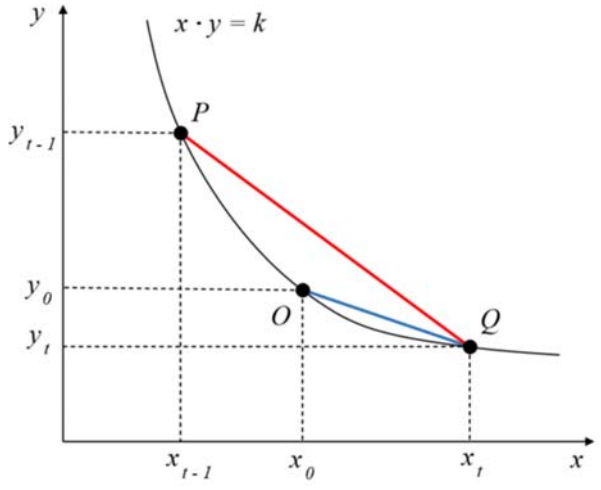


Figure 1. Origin Crossing in CPMM for $x_{t-1} < x_0 < x_t$

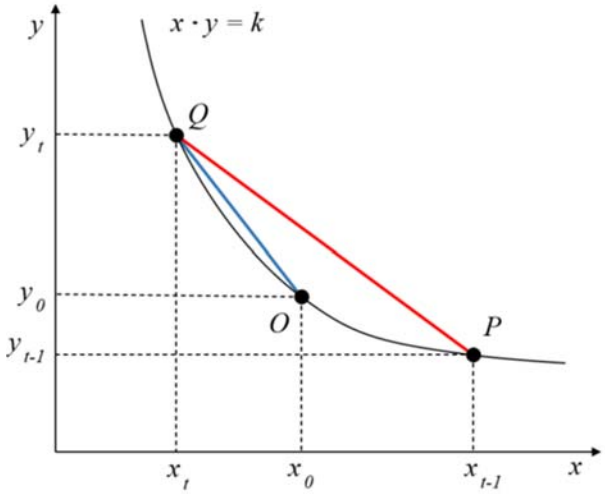


Figure 2. Origin Crossing in CPMM for $x_t < x_0 < x_{t-1}$

Theorem 1 defines the sufficient conditions of impermanent gain, which are "$x_{t-1} < x_0 < x_t$" or "$x_t < x_0 < x_{t-1}$".

Similarly, the sufficient conditions of impermanent loss are i) $x_{t-1} < x_t < x_0$, ii) $x_t < x_{t-1} < x_0$, iii) $x_0 < x_{t-1} < x_t$ or iv) $x_0 < x_t < x_{t-1}$ without the proof. Whenever one of these conditions is satisfied, the impermanent loss occurs.

This section explains that the impermanent gain is achievable when the origin crossing occurs by any transactions. Therefore, the next section considers how to make the origin cross occur to avoid impermanent loss and achieve impermanent loss.

## 4. A NEW COMBINATORIAL OPTIMIZATION PROBLEM FOR MAXIMUM EXTRACTABLE VALUE AND ORIGIN CROSSING

The blockchain produces blocks containing a series of transactions. Timestamping those transactions over geographically dispersed and internet-based networks or determining the sequence of those transactions is fundamentally impossible due to various reasons, including transmission delay. Therefore, decentralized blockchain networks allow miners to include, exclude or reorder the transactions in their mined blocks.

Maximum Extractable Value (MEV) in blockchain networks has emerged as a critical phenomenon that fundamentally shapes the dynamics of decentralized finance (DeFi) and market efficiency. This complex mechanism represents the maximum value that can be extracted from block production beyond standard block rewards and gas fees through strategic transaction ordering, inclusion, or exclusion. What began as "miner extractable value" has evolved into a comprehensive concept affecting the entire blockchain ecosystem, particularly within smart contract platforms like Ethereum, where sophisticated DeFi interactions occur. The significance of MEV extends far beyond simple value extraction, playing a pivotal role in blockchain economics and market efficiency. It has become deeply integrated into how blockchain markets function, influencing everything from basic token swaps to complex DeFi operations. The presence of MEV creates both opportunities and challenges that affect market dynamics, user experience, and protocol design across the DeFi landscape.

The exploitative potential of MEV manifests through various predatory practices that can harm users and threaten system stability. Sandwich attacks, where traders experience front-running and back-running around their transactions, result in adverse price execution and diminished user confidence. Time-bandit attacks involving block reorganization for MEV capture present significant threats to blockchain security by incentivizing chain reorganizations. These practices contribute to increased transaction costs and deteriorated trade execution, ultimately undermining user trust in DeFi protocols.

However, MEV is not inherently harmful and serves essential functions in maintaining market efficiency and price discovery. Arbitrage activities facilitated by MEV help maintain price consistency across different DEXs, contributing to market stability. Similarly, liquidation mechanisms in lending protocols benefit from MEV extraction, ensuring protocol solvency through swift action on undercollateralized positions. These activities, while profitable for extractors, provide crucial services to the DeFi ecosystem and help maintain its overall health. In DEX environments, MEV implementation takes various sophisticated forms. Transaction batching through batch auctions with uniform clearing prices effectively prevents front-running while maintaining market efficiency. Order flow optimization aggregates multiple trades, for optimizing gas usage and minimizing price impact. Fair ordering protocols implement time-weighted average price mechanisms and commit-reveal schemes, ensuring transparent and equitable trade execution.

This study suggests a constructive approach to extracting MEVs by reorganizing the transactions via reordering and batching to make the origin crossing occur for the purpose that the liquidity provider benefits the impermanent gain. Some optimization algorithms can be built in the smart contract of liquidity pool in DEXs to minimize the impermanent loss and maximize the impermanent gain. The suggested development of MEV requires carefully balancing beneficial market activities with user protection. As the DeFi ecosystem continues to evolve, more sophisticated ordering mechanisms, enhanced protection schemes, and novel economic models can be necessary to align stakeholder interests effectively. The success in managing MEV determines the long-term viability and efficiency of decentralized finance systems.

This study proposes a new combinatorial optimization problem to extract MEV and achieve impermanent gain for liquidity providers. The proposed problem combines transaction batching and transaction permutations. At this point, it is conjectured to be an NP-hard problem without proof.

The proposed combinatorial optimization problem is explained by example. To understand this problem, one must understand blockchain technology and DEX smart contracts. Although these are beyond the scope of this study, the following provides insight into how smart contract protocols must be improved at future DEXs.

Assume the roughly estimated sequence of transactions received at the node on a blockchain network. Note that the sequences at different nodes on the blockchain network may vary, depending on the topology and quality of internet transmissions. Therefore, ordering all transactions that occur worldwide based on a single authoritative timezone is almost impossible, and one can say the sequence of transactions may be different at different nodes in a blockchain network. However, any node (block producer) may have different sequences, but it can have its sequence of arriving transactions.

Without confusion, let a sequence of transactions at a certain node be given in Table 1. The first column shows the sequence number of transactions, and “0” represents the initial time of depositing a pair of the asset coins and stablecoins into the liquidity pool. The third and fourth columns show the quantities of the asset coins and stablecoins in the liquidity

pool, which were denoted as $x_0$ and $y_0$ in Section 3. The second and fifth columns represent $x_t - x_{t-1}$ and $y_t - y_{t-1}$, respectively. The sixth column shows the product constant k in the CPMM cost function at each transaction, being unchanged. The seventh column is $P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$. The eighth column indicates value gain $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$. Finally, the last column indicates whether the corresponding transaction causes impermanent loss (IL) or impermanent gain (IG).

Table 1. An example of a transaction list.

| Transaction No. | $\Delta x_t$ | $x_t$ | $y_t$ | $\Delta y_t$ | $k$ | $P_x(\mathbf{q_t} - \mathbf{q_{t-1}})$ | $G_t(\mathbf{q_t} - \mathbf{q_{t-1}})$ | IL or IG |
|---|---|---|---|---|---|---|---|---|
| 0 | | 10.00 | 1,000.00 | | 10,000 | 100.00 | | |
| 1 | −0.20 | 9.80 | 1,020.41 | 20.41 | 10,000 | 102.04 | 0.000 | |
| 2 | 0.10 | 9.90 | 1,010.10 | −10.31 | 10,000 | 103.07 | −0.206 | IL |
| 3 | −0.20 | 9.70 | 1,030.93 | 20.83 | 10,000 | 104.13 | −0.312 | IL |
| 4 | 0.10 | 9.80 | 1,020.41 | −10.52 | 10,000 | 105.20 | −0.631 | IL |
| 5 | 0.30 | 10.10 | 990.10 | −30.31 | 10,000 | 101.03 | 0.202 | IG |
| 6 | −0.20 | 9.90 | 1,010.10 | 20.00 | 10,000 | 100.01 | 0.100 | IG |
| 7 | −0.10 | 9.80 | 1,020.41 | 10.31 | 10,000 | 103.07 | −0.206 | IL |
| 8 | 0.10 | 9.90 | 1,010.10 | −10.31 | 10,000 | 103.07 | −0.206 | IL |
| 9 | −0.40 | 9.50 | 1,052.63 | 42.53 | 10,000 | 106.33 | −0.532 | IL |
| 10 | 0.20 | 9.70 | 1,030.93 | −21.70 | 10,000 | 108.52 | −1.628 | IL |
| 11 | 0.10 | 9.80 | 1,020.41 | −10.52 | 10,000 | 105.20 | −0.631 | IL |
| 12 | 0.20 | 10.00 | 1,000.00 | −20.41 | 10,000 | 102.04 | 0.000 | |
| 13 | −0.10 | 9.90 | 1,010.10 | 10.10 | 10,000 | 101.01 | 0.000 | |
| 14 | −0.30 | 9.60 | 1,041.67 | 31.57 | 10,000 | 105.22 | −0.421 | IL |
| 15 | −0.10 | 9.50 | 1,052.63 | 10.96 | 10,000 | 109.65 | −2.193 | IL |
| 16 | 0.10 | 9.60 | 1,041.67 | −10.96 | 10,000 | 109.65 | −2.193 | IL |
| 17 | 0.10 | 9.70 | 1,030.93 | −10.74 | 10,000 | 107.39 | −1.289 | IL |

To understand Table 1, Transaction 1 is explained in detail. For Transaction 1, one buys the asset coin of amount 0.2 by paying the stablecoin of amount 20.41. That is, one takes out 0.2 asset coins from the liquidity pool and adds 20.41 stablecoins to the liquidity pool. After Transaction 1, there are 9.8 asset coins and 1021.41 stablecoins in the liquidity pool. If we multiply the quantities of the asset coins and stablecoins, we can obtain 10,000, which is a requirement in the CPMM model. The price of the asset coin in this transaction is $-\frac{20.41}{0.20} = 102.04$ (the seventh column), and the value gain is 0 because any transactions occurring at the origin lead to a value gain of 0. It can be easily shown from the equations in Section 3. Similarly, for Transaction 2, one sells the 0.1 asset coins and receives 10.31 stablecoins. The price of the asset coin in this transaction is 103.07 stablecoins, and the value gain is $-0.206$; that is, impermanent loss occurs in this transaction.

Transaction batching is defined as a manipulative aggregation of the same type of orders (buy or sell) in sequence for the purpose of avoiding impermanent loss. Transactions 10, 11 and 12 are all buy orders. If these three transactions are combined into a single batch order, it is called transaction batching and treated as a single order. In the current smart contract protocol in DEXs, all three transactions occur immediately and cannot be combined. The prices of the asset tokens are 108.52 stablecoins for 0.2 asset coins, 105.20 stablecoins for 0.1 asset coins and 105.20 stablecoins for 0.2 asset coins. If these three transactions are batched, the prices are averaged; i.e., $-\frac{(21.70+10.52+20.41)}{(0.20+0.10+0.20)} = 105.26$. Then, there exist discrepancies in what three buyers pay into the liquidity pool. Therefore, to implement the transaction batching in DEXs, a new smart contract protocol can be proposed but the detail is beyond the scope of this study. In addition, one of the benefits of transaction batching is the lower gas cost.

Transaction reordering is defined as a manipulative sequencing of transactions for the purposes of increasing the chance of transaction batching and avoiding impermanent loss. By reordering the transactions, transaction batching can be easier. Especially when buy and sell orders alternate, the transaction can be reordered for the transaction batching. Transaction reordering can be abused like MEV cases because they can manipulate the price of specific transactions, which are mentioned in this section. Therefore, transaction reordering must be done carefully and open for future smart contract protocols in DEXs.

Using transaction batching and reordering, the gas for the transaction can be saved and impermanent loss is avoided. Finally, impermanent gain can be achieved as well. Table 2 shows a transaction list after transaction batching and reordering.

It is not an optimized result, but it is presented as an example of improvement over the original transaction list. In Table 2, the shaded row contains the aggregated transaction results after transaction batching and reordering. 17 transactions in the original transaction list have been combined into 8 aggregated transactions. The transaction number and the amount of asset coin change are given for reference purposes from Table 1.

For example, Transactions 2 and 3 are reordered for transaction batching. Transactions 1 and 3 are combined into a single transaction in the DEX smart contract. As seen, there is no impermanent loss. Similarly, Transactions 2, 4 and 5 were aggregated into a single transaction, which leads to impermanent gain.

Note that no impermanent loss is observed. Table 2 is an improved transaction list containing less number of actual transactions and impermanent gain as a result of batching and reordering. There is an impermanent loss at the end of the list, but it is because of a finite number of transactions. If we have more incoming buy or sell orders, we can continue to produce impermanent gain, depending on the type of orders and the amount of asset coins in those orders.

However, a block must be produced in a reasonable amount of time. The number of transactions available for batching and reordering may be limited and impermanent loss can sometimes occur. But the number and amount of imperment loss can be surely optimized.

Table 2. An improved transaction list after transaction batching and reordering.

| Transaction No. | $\Delta x_t$ | $x_t$ | $y_t$ | $\Delta y_t$ | $k$ | $P_x(\mathbf{q}_t - \mathbf{q}_{t-1})$ | $G_t(\mathbf{q}_t - \mathbf{q}_{t-1})$ | IL or IG |
|---|---|---|---|---|---|---|---|---|
| 0 | | 10.00 | 1,000.00 | | 10,000 | 100.00 | | |
| 1 | −0.20 | | | | | | | |
| 3 | −0.20 | | | | | | | |
| | −0.40 | 9.60 | 1,041.67 | 41.67 | 10,000 | 104.17 | 0.000 | |
| 2 | 0.10 | | | | | | | |
| 4 | 0.10 | | | | | | | |
| 5 | 0.30 | | | | | | | |
| | 0.50 | 10.10 | 990.10 | -51.57 | 10,000 | 103.14 | 0.413 | IG |
| 6 | −0.20 | | | | | | | |
| 7 | −0.10 | | | | | | | |
| | −0.30 | 9.80 | 1,020.41 | 30.31 | 10,000 | 101.03 | 0.202 | IG |
| 8 | 0.10 | | | | | | | |
| 10 | 0.20 | | | | | | | |
| | 0.30 | 10.10 | 990.10 | -30.31 | 10,000 | 101.03 | 0.202 | IG |
| 9 | −0.40 | | | | | | | |
| | −0.40 | 9.70 | 1,030.93 | 40.83 | 10,000 | 102.07 | 0.306 | IG |
| 11 | 0.10 | | | | | | | |
| 12 | 0.20 | | | | | | | |
| | 0.30 | 10.00 | 1,000.00 | -30.93 | 10,000 | 103.09 | 0.000 | |
| 13 | −0.10 | | | | | | | |
| 14 | −0.30 | | | | | | | |
| 15 | −0.10 | | | | | | | |
| | −0.50 | 9.50 | 1,052.63 | 52.63 | 10,000 | 105.26 | 0.000 | |
| 16 | 0.10 | | | | | | | |
| 17 | 0.10 | | | | | | | |
| | 0.20 | 9.70 | 1,030.93 | -21.70 | 10,000 | 108.52 | −1.628 | IL |

## 5. MANAGERIAL INSIGHT AND CONCLUSIONS

This study introduces a new combinatorial optimization problem that can be considered in the future DEX smart contract protocol. Continuous attempts to avoid impermanent loss have failed consistently over the decade. It is not easy to eliminate impermanent loss. The contribution of this study can be summarized as follows. This study proposes a new pricing method for DEX transactions, which is the actual price of the asset coins in the liquidity pool. Based on the actual price, the value gain has been defined. In addition, this study presents the fact that impermanent gain is achievable. From there, we derive the sufficient condition for impermanent loss and prove it mathematically. This sufficient condition is called origin crossing. Whenever a transaction crosses the origin, the impermanent gain occurs.

Therefore, a new way to extract MEV in DEX operations has been suggested. It utilizes transaction batching and reordering. We in this study, propose a new smart contract protocol that utilizes the optimization algorithms in transaction batching and reordering. If the protocol is open source as part of blockchain implementations, many benefits are available to the DeFi community. First of all, gas costs for transactions to be recorded in the block can be saved. Secondly, the notorious impermanent loss can be avoided and this kind of smart contract for DEX can attract more liquidity providers. It can result in the prosperous times of DEX smart contracts for transactions. In Section 1, we have introrudced several known issues that are involved only with CEXs. Thirdly, it can reduce the slippage, which is the price difference before and after the order, because we can consider the low slippage in the optimization model.

Regarding the optimization models and algorithms, various approaches can be considered in future research. The most straightforward approach is the metaheuristics, such as genetic algorithms, which have good fits to the permutation problems. Regarding transaction batching, some clustering algorithms can be utilized.

As mentioned earlier in the derivation of the actual prices, the first-order Markov process model can be used for the modeling and optimization. As proposed in this paper, the sufficient condition for impermanent gain is subject to the state of the liquidity pool before and after transactions. Therefore, this dynamic nature of the continuous DEX operations can be modeled as a stochastic process to optimize the reordering.

The current smart contract protocol produces immediate transactions whenever buy or sell orders arrive. Due to the nature of distributed network systems, it is inevitable to avoid unexpected delays or arbitrary sequencing of transactions. Instead of troubleshooting this phenomenon, we can utilize transaction batching and reordering to maximize MEV, which is the mitigation of impermanent loss. We propose a new design for DEX smart contracts. DEX smart contracts can maintain the age of individual buy or sell orders. Given the limit of the order ages, smart contracts can batch or reorder orders in such a way that the impermanent loss is avoided or slippage can be minimized and fairly distributed over the orders. Then, online algorithms are promising because they can handle online decision making under dynamically incoming orders.

Finally, the study of the optimization objective functions is undergoing as well. Many different objective functions have been identified and discussed. For example, in this study, we focused on minimizing the number of impermanent losses per transaction. Another objective function of our concern is the per-transaction impermanent gain. Minimum slippage can be another objective function. According to what we want to achieve in DEX operations through the optimization, different objective functions or a combination of them can be used. Therefore, multi-criteria decision making (MCDM) algorithms can be used for modeling the proposed optimization problem.

## ACKNOWLEDGMENT

This work is supported by the Academic Research Fund of Hoseo University (2024-0014-01), and the Next-generation Communication Convergence and Open Sharing System project supported by the Ministry of Education and National Research Foundation of Korea, and Composable Finance.

## REFERENCE

Aigner, A. A. and Dhaliwal, G. (2021). Uniswap: Impermanent loss and risk profile of a liquidity provider. *arXiv*, https://arxiv.org/abs/2106. 14404

Aoyagi, J. and Ito, Y. (2021). Coexisting exchange platforms: Limit order books and automated market makers. SSRN, https://papers.ssrn.com/ sol3/papers.cfm?abstract_id=3808755

Boueri, N. (2021). G3M impermanent loss dynamics. *arXiv*, https://arxiv.org/abs/2108.06593

Chaum, D. (1983). Blind Signatures for Untraceable Payments. Advances in Cryptology: Proceeding of Crypto 82., Springer, Boston, MA, USA

Dai, W. (1998). B-Money. http://www.weidai.com/bmoney.txt

Hafner, M. and Dietl, H. (2024). Impermanent loss conditions: an analysis of decentralized exchange platforms. *arXiv*, https://arxiv.org/abs/ 2401.07689

Kim, H.J., Lee, G. M., Lee, J., Kang, S., Chae, S. W. and Park, J.-S. (2024). A comparison of impermanent loss for various CFMMs. *Proceedings of the 2024 International Conference on Blockchain*, Copenhagen, Denmark, Aug. 2024.

Kim, H. J., Lee, J., Kang, S., Chae, S. W., Kim, Y.K., and Lee, G.M. (2024). Desirable price function and value ratio of constant function market makers. *Proceedings of the International Conference on Artificial Intelligence, Computer, Data Sciences and Applications*, Mahé, Seychelles, Feb. 2024.

Kim, H. J., Choi, S., Yoon, Y. T. and Yoo, S. (2022). Impermanent loss and gain of four automated market maker algorithms. *The Journal of Digital Assets*, 1(1): 1-12.

Loesch, S., Hindman, N., Richardson, M. B. and Welch, N. (2021). Impermanent loss in Uniswap v3. *arXiv*, https://arxiv.org/abs/2111.09192

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://ssrn.com/abstract=3440802

Tangri, R., Yatsyshin, P., Duijnstee, E. A. and Mandic, D. (2023). Generalizing impermanent loss on decentralized exchanges with constant function market makers. *arXiv*, https://arxiv.org/abs/2301.06831

Tiruviluamala, N., Port, A. and Lewis, E. (2022). A general framework for impermanent loss in automated market makers. *arXiv*, https:// arxiv.org/abs/2203.11352