International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Front-running attack in decentralized finance in the metaverse: A systematic review

Tamimul Alam *, Md. Asraf Ali and Md. Hasibur Rahman

Computer Science and Engineering, American International University-Bangladesh, Bangladesh.

International Journal of Science and Research Archive, 2024, 11(01), 2315–2324

Publication history: Received on 12 January 2024; revised on 18 February 2024; accepted on 21 February 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.1.0332

Abstract

The Metaverse is a developing mirror of the real world that promises to revolutionize socializing, business, and digital asset connections. Such technology will change the physical world and its environment. Decentralized Finance (DeFi) will completely transform the global financial system. Recent years have seen DeFi transform the financial industry. Since DeFi expanded, banking, insurance, and investing have changed significantly. The decentralized finance sector is growing rapidly, showing that digital currencies and platforms could replace the old financial system. It eliminates expensive intermediaries, lowers transaction costs, and increases financial services access for all, regardless of location or income. Decentralization could provide a risk-free and efficient solution for Metaverse's financial ecosystem, but it has drawbacks. Before implementing financial decentralization, security risks were the main concern. The review paper discusses DeFi's main role in the Metaverse financial ecosystem and security concerns. Front-running attacks are one of the biggest security risks in DeFi, which could cost investors a lot of funds as well as damage the ecosystem.

Keywords: Metaverse; DeFi; Blockchain technology; Front-Running; Security

1. Introduction

DeFi is a fast-emerging section of the cryptocurrency business that aims to give customers more accessible, transparent, and secure financial services than traditional banking [1]. Meanwhile, the Metaverse is a new concept that aspires to build a fully immersive virtual environment that anybody may visit at any time [2]. DeFi has great potential to provide risk-free and efficient Metaverse financial services as these two areas converge. The "metaverse," a virtual universe with a coherent moral code and a different economic system linked to the real world, was created from the prefix "meta" (transcendence) and suffix "verse" (universe). Neil Stephenson, who created the concept in his 1992 science fiction novel Snow Crash [3], says users can game, socialize, buy virtual goods, and participate in virtual markets. Users can access the metaverse by creating virtual reality avatars. Since its beginnings, the metaverse has been called second life, Three dimensional (3D) virtual worlds, and life-logging. A fully immersive, highly spatiotemporal, and self-sustaining virtual shared place combines the physical, natural, and digital worlds [7].

The metaverse determines content ownership and asset rights using digital twins, Virtual Reality (VR), Augmented Reality (AR), 5th generation (5G), wear-able sensors, Blockchain Intelligence (BCI), Artificial Intelligence (AI), and blockchain/Non-Fungible To-ken (NFT) [8].

* Corresponding author: Tamimul Alam

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

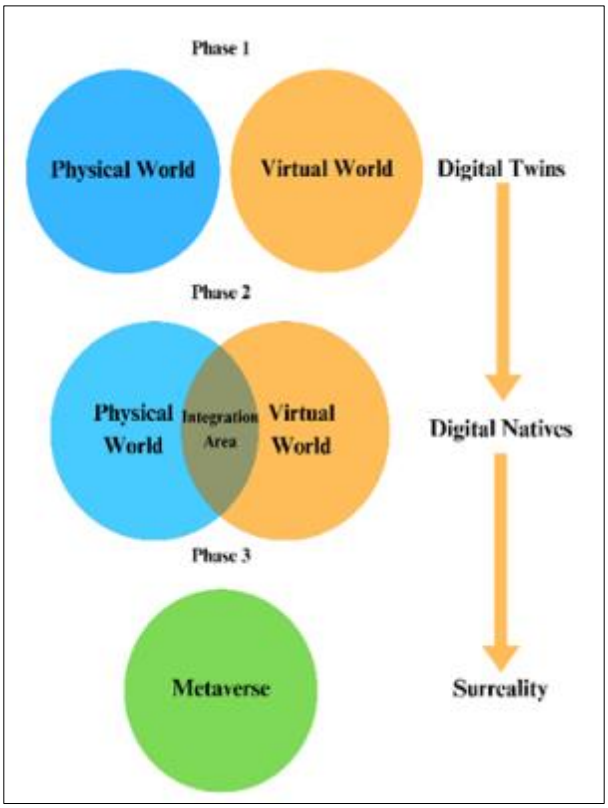

Figure 1 The metaverse's development was divided into three distinct stages

Smart gadgets and sophisticated enabling technologies will make the metaverse a reality and acquire worldwide interest. Facebook became "Meta" to build the future metaverse [9]. Other tech heavyweights join Metaverse. DeFi offers financial services and merchandise to anyone having Ethereum and an internet connection [10]. DeFi is unique in its ability to provide open, always-accessible markets without central authorities blocking payments or access. DeFi is a suitable solution since code manages sluggish, error-prone functions and improves security [11]. DeFi is a new and emerging Bitcoin industry that provides financial services to the Internet [12]. Decentralized blockchain technology Ethereum lets customers access financial products and services without banks. Oracles retrieve data for Compound, MakerDao, Uniswap, and Aave DeFi protocols. Oracles supply DeFi apps with Bitcoin exchange rate data in certain instances [13].

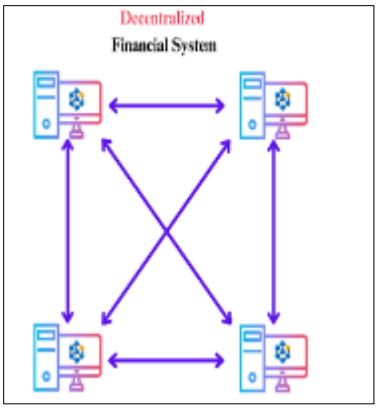

Figure 2 Decentralized financial (DeFi) system

DeFi markets are open and accessible, a plus. Without gatekeepers, anyone can trade at any time and payments cannot be stopped. DeFi services are faster and more reliable than traditional financial services because they are automated and powered by code that anyone can inspect and evaluate [14]. DeFi is vital to metaverse ecology [15]. DeFi refers to bank less blockchain-based financial apps. Borrowing, trading, and earning interest are more transparent and

controlled with DeFi [16]. Digital transactions in the Metaverse are secure and transparent with DeFi. Metaverse users can benefit from DeFi's secure, decentralized banking. DeFi promises transparent banking but is risky [17]. Like any financial system, DeFi protocols have risks. Front-running can extract gains and cut cash by examining smart contract instructions and functions theory that has never been used [18]. The goal is to fix DeFi's front-running issue and security risks.

The article discusses Decentralized Finance (DeFi) and its role in the blockchain ecosystem. It covers the benefits of blockchain in enabling decentralized financial services, compares DeFi and CeFi financial services, analyzes DeFi's front-running attack, dis-cusses its effects and risks, and provides solutions to prevent attacks. The article also explores DeFi's future and solutions, focusing on the Metaverse and innovation-security balance. The study concludes that research and innovation are crucial for a strong DeFi ecosystem, and the article structure provides a comprehensive examination of DeFi's issues, potential solutions, and financial direction.

2. Dentralized Finance

Financial systems that do not rely on CeFi intermediaries, such as banks or brokerage firms, are known as DeFi. Instead, it employs blockchain technology to establish a peer-to-peer (P2P) network in which users may connect directly with one another [19]. The blockchain is a distributed ledger frame-work that protects and records transactions transparently. DeFi applications, which are built on top of blockchains, use smart contracts to automate financial transactions [20]. Some of the key benefits of DeFi include:

- Transparency and openness: DeFi apps are open and transparent, which means that anybody can examine the code and follow the transactions. This decreases the possibility of fraud and mis-use.
- Immutability: A transaction cannot be modified after it has been recorded on a blockchain. This provides users with a high level of security.
- Efficient: DeFi apps do not require middlemen, so they can be more efficient than traditional financial systems.
- Accessibility: Anyone with an internet connection, regardless of location or financial situation, can utilize DeFi apps [21].

Within the realm of DeFi, a diverse array of financial services is available, each underpinned by block-chain technology and characterized by their decentralized nature:

- Lending and borrowing: Traditional financial institutions charge higher interest rates than DeFi platforms for cryptocurrency lending and borrowing. User digital assets can be collateral for loans or lent for interest.
- Staking: Users can stake their digital currencies to receive incentives. This is analogous to putting money in a savings account.
- Yield farming: By supplying liquidity to DeFi marketplaces, users may earn money. This is a more complicated procedure than staking, but the returns can be greater.
- Decentralized exchanges (DEXs): DEXs enable peer-to-peer cryptocurrency trading, eliminating the need for centralized exchanges. These fac-tors may reduce costs, increase confidentiality, and boost marketability.
- Insurance: DeFi reinsurance systems provide individuals with the means to protect their financial assets from potential risks like hacking incidents and other losses [22].

Banks, brokerages, and other institutions dominated CeFi, the traditional financial system. CeFi provides lending, borrowing, trading, and investing. Distribution vs. centralization distinguishes DeFi from CeFi. Therefore, unlike CeFi apps, DeFi apps are not centralized [23].

Table 1 Compares and Contrasts the most important aspects of DeFi and CeFi

Feature	**DeFi**	**CeFi**
Centralization	Decentralized	Centralized
Transparency	Open and transparent	Closed and obtrusive
Security	Immutable and secure	More susceptible to hacking and fraud
Efficiency	More efficient	Less efficient
Accessibility	More accessible	Less accessible

DeFi is young but growing. DeFi faces many challenges, including security and scalability. DeFi could revolutionize banking by making it simpler and more transparent [22].

2.1. Cryptocurrency Exchanges

Cryptocurrency exchanges trade $10 billion daily. This novel idea allows Blockchain technology to decentralize the financial system. This new financial concept is Decentralized Finance. A popular alternative to centralized asset-to-asset trades in DeFi technology is DEX [24]. DeFi technology exchanges NFTs using Blockchain ledgers. While DeFi is safe, assaults occur [25]. Decentralized banking technologies will be unstable and distrusted after a “front-running attack”.

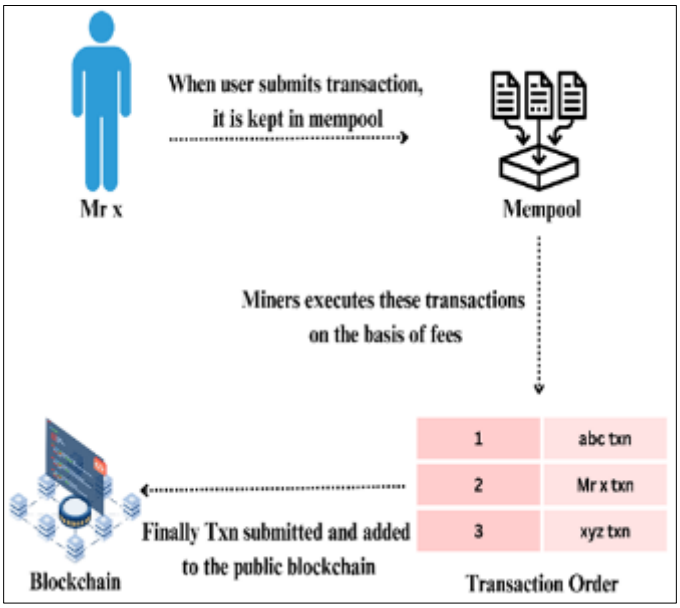

Figure 3 An example of how data is added to the blockchain for trans-actions

2.2. Smart Contracts

Simple computer programs called "smart con-tracts" run automatically, often by a system that lets users verify their operation. Smart contracts are of-ten executed on public blockchain networks [43, 44]. Ethereum is the largest Turing-complete smart con-tract system that can encode any smart contract functionality [44]. Ethereum smart contracts can perform shareholder voting [45], stakeholder-owned investment funds and vehicles [46, 47], fair ex-change protocols for goods [48], complex key management solutions [49], video games [50], virtual casinos, and more. On Ethereum, token-based virtual currency contracts are most popular among daily users. These tokens can replace rare items like video game collectibles [50] or company stock [51]. This sparked the "ICO boom," a $12 billion USD token-based capital investment craze. DEXes, a common smart contract, lets users trade such tokens without keeping them.

3. Front-Running Attack

Front-running attacks exploit blockchain construction principles. Malicious actors monitor mempool transactions awaiting confirmation. They use the time gap to maximize profits by sending transactions quickly [29]. This deception exploits the miner or bot's preference for the higher gas fee by executing the attacker's transaction before the original user's [30]. Example: a quiz game where players compete for a $50 prize by answering correctly quickly. Here, both players bet $25. Because they know the winning response, the attacker strategically submits the correct response first, winning unfairly. This example emphasizes the need to fix front-running vulnerabilities to improve blockchain reliability and fairness.

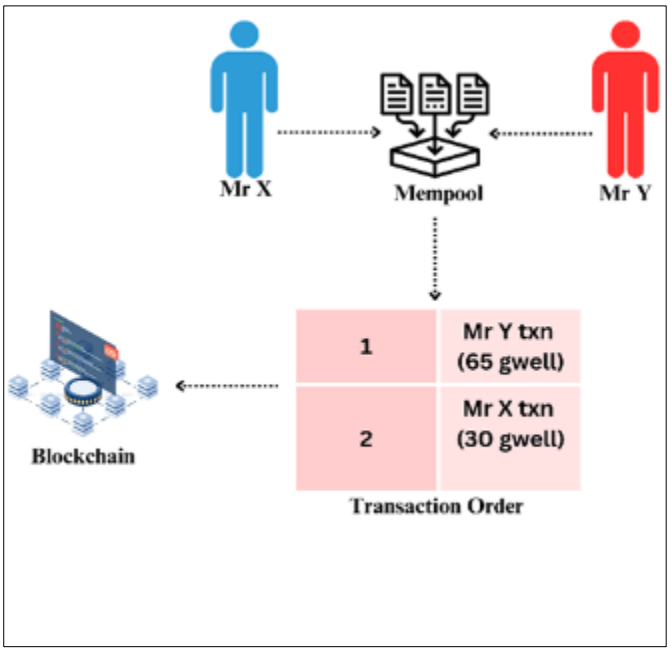

Figure 4 An example of front-running in a quiz game

Mr. X and Mr. Y participated in a game where Mr. X knew the answer and submitted the correct response with a fee of 30 gwei (gwei is a unit of ether (ETH) used on the Ethereum blockchain platform for transaction fees) [31]. Mr. Y, who didn't know the answer, watched the mempool and submitted the same response with higher gas fees (65 gwei) after seeing Mr. X's transaction. As Mr. Y's transaction had a higher fee, the miner prioritized it over Mr. X's, and Mr. Y won the game and received $50, while Mr. X lost, even though he/she had the correct answer. This is an example of a front-running attack [28]. This incident highlights the vulnerability of block-chain transactions to such attacks and the need for safeguards to ensure fairness and prevent manipulative operations like front-running. Maintaining the integrity of decentralized systems necessitates the implementation of strong security measures and the promotion of transparent protocols.

3.1. GAS

The computing effort required to complete a transaction on a blockchain network is measured in gas. Gas is used in Ethereum to pay for the processing of transactions and smart contracts. A gas limit and a gas price must be specified when a user transmits a transaction on the Ethereum network. The gas limit is the maximum quantity of gas a user is prepared to pay for the transaction, whereas the gas price is the amount of ether (the Ethereum net-work's coin) a user is willing to pay per unit of gas. A transaction's total cost is calculated by multiplying the gas limit by the gas price. The market demand for transaction processing determines the gas price. If the network is overburdened with unconfirmed transactions, users may have to pay a higher gas price to ensure that their transactions are processed fast. Users may be able to pay a lower gas price and yet have their transactions processed in a fair length of time if the network is less congested.

3.2. Mempool

Blockchain nodes store validated transactions in the mempool, or memory pool, until miners add them to the blockchain [32]. This interim repository helps the network efficiently manage transactions and ensure their orderly inclusion into the distributed ledger. Miners prioritize mempool transactions, which is crucial. High-fee transactions are prioritized and more likely to be included in the next block. Transactions with higher fees are processed faster [33]. A dynamic incentive system encourages users to attach competitive fees to their transactions, competing for faster processing times. As the blockchain ecosystem evolves, optimizing mempool management and fee structure improves transaction speed and network efficiency, ensuring a responsive and streamlined user experience [32].

3.3. Defi Security Issues

Smart contracts simplify financial transactions in DeFi, eliminating intermediaries and facilitating peer-to-peer exchanges. This decentralized strategy eliminates hurdles and limits in traditional financial systems to improve transparency, cost, and financial inclusion. The study by Zetzsche et al. [10] stated the potential impact of DeFi on the

rule of law, focusing on three key aspects: legal jurisdiction and applicable law, enforcement, and data protection and privacy. DeFi's decentralized nature raises concerns about data protection and privacy violations, potentially impacting institutions relying on it.

Consequently, DeFi represents a challenge to the traditional legal role of the state, both in terms of the intentions underlying the DeFi ideal and the realities of technological evolution. In a volatile financial market, DeFi protocols can mitigate risk and provide profits, as shown in the study by Metelski and Sobieraj [11]. Using scientific approaches, the article examines DeFi protocol performance indicators and valuations. It investigates the effects of total value locked, protocol revenue, total income, gross merchandise volume, and the inflation factor on the valuations of DeFi protocols representing decentralized exchanges, lending protocols, and asset management. Granger causality tests and panel regression models with fixed effects are employed. The findings reveal that DeFi protocol valuations are influenced by performance indicators, while the degree and direction of these interactions differ depending on the variable. The sole variable with predictive potential was determined to have a two-way causal association between DeFi protocol values and gross merchandise volume.

4. Front-Running Attack in Defi

People front-run deals to profit unfairly from pending transactions. Yazici examined blockchain DEX arbitrage bot profits [32]. Revenue-generating bot transactions are examined. For early block position and execution, priority gas auction bots bid up transaction prices. We formalize and analyze PGAs, a novel continuous-time, partial-information game-theoretic model. The team builds frontrun.me for PGA real-time statistics. Priority fees and mining yield Miner/Maximal Extractable Value (MEV), which measures consensus-layer security flaws, is another systemic threat, the paper says. Pre-empting trades to profit at others' expense is harmful and possibly illegal [34]. Front-running DeFi blends public trade data and miners' transaction order skills. Pro-posed cryptography stops permissionless blockchain aggressive front-running. DeFi users must be fair, safe, and secure.

4.1. Liquidity Concentration

Concentration of AMM liquidity matters. Liquidity providers (LPs) must provide liquidity at all prices in traditional AMMs. Innovative protocols like Uniswap V3 help LPs allocate liquidity within price ranges. The new ecosystem capital efficiency mechanism reduces LP temporary losses [35]. Use Uniswap V3 to strategically position liquidity in price ranges where LPs are confident or expect more trading. LPs can optimize exposure and reduce liquidity provision price swing losses with this innovation. In-creased provider control over liquidity deployment, participation, and AMM model stabilization reduces liquidity concentration in Uniswap V3 [36]. AMM improvement indicates decentralized financial system growth. By targeting specific market sectors, Uniswap V3, and other protocols improve liquidity provisioning economics and DeFi ecosystem resilience [37].

4.2. Uniswap Version 3

Ethereum Virtual Machine noncustodial automat-ed market builder Uniswap v3. Uniswap v3 raises liquidity provider capital, Oracle pricing, and fees. DeFi liquidity comes from permissionless blockchain smart contracts [36]. CFMMs like Uniswap v1 and v2 sell only part of the pool's assets, making them capital-inefficient. Previous measures like Curve and Yield Space fragmented liquidity. Mohan claims Governance-controlled and independent Uniswap v3 contracts [37]. Bitcoin price discovery, arbitrage, DEX token exchange Examining AMMs. Neoclassical economics views companies as black boxes that use technology to produce outputs. AMM automatically selects inputs and outputs to maximize profits. Forex and finance literature says AMMs allow two- and three-point arbitrage.

5. Efficient Techniques for Front-running Attack in Defi

A suitable plan for addressing the enduring front-running vulnerabilities seen in DeFi transactions with-in the vast Metaverse landscape is presented by the convergence of technological advancements and regulatory frameworks. A multifaceted strategy is essential to successfully reduce the risks brought on by front-running attacks. Modern cryptographic protocols, smart contract optimization, and decentralized order execution mechanisms are among the most effective methods currently in use. These technological solutions improve information asymmetry, transaction integrity, and transaction privacy. In addition to these technological safeguards, regulatory actions that promote accountability, uphold transparency, and promote platform-to-platform collaboration can add another layer of protection. Combining these tactics can help the Metaverse eco-system create a decentralized financial system that is more dependable and secure, ultimately opening the door for widespread adoption and innovation. A combination of technological and regulatory measures can be implemented to address front-running vulnerabilities in DeFi

transactions within the Metaverse. Some of the most efficient techniques that are being used to mitigate font running attacks are:

- Transaction Ordering Dependence (TOD) solutions: TOD is the practice of miners taking ad-vantage of the order of transactions within a block. Mitigations include "Commit-Reveal" methods, in which users submit a hashed version of their transaction (the "commit") and then expose it. This limits miners' ability to front-run transactions [38].
- DEX Utilizing AMMs: AMMs such as Uniswap have transformed the old order book paradigm, which is prone to front-running, into a liquidity pool model. However, this does not completely solve the problem because there is still potential for arbitrage, which can result in front-running [39].
- Sandwich Attack Prevention: Sandwich attacks are a type of front-running in which a malicious ac-tor places a transaction both before (front-running) and after (back-running) a victim's transaction. Slip-page tolerance settings in DEXs can be used to pre-vent this, although it does not eliminate the problem [40].
- MEV Solutions: Flashbots is research and development organization dedicated to mitigating the negative externalities associated with MEV. They offer "Flashbots bundles," which are collections of transactions that users can submit directly to miners instead of the public mempool, decreasing the possibility of front-running [41].
- Layer-2 Solutions: Layer-2 solutions, such as rollups, can assist in preventing front-running by boosting transaction throughput and making the transaction ordering process opaque, lowering the profitability of front-running [30].
- Consensus mechanisms and network upgrades: Some initiatives are investigating novel consensus processes and network improvements to reduce the profitability of front-running. The Ethereum 2.0 up-grade, for example, will have shard chains and proof-of-stake, which may minimize some front-running difficulties [42].

6. Conclusion

To conclude, the convergence of the Metaverse with DeFi could change the financial landscape. DeFi is crucial, using blockchain technology to create transparent, accessible, and automated financial services across borders. DeFi eliminates middlemen and uses smart contracts to simplify peer-to-peer transactions and increase transparency. Growth and adoption have shown it can revolutionize sectors. Security concerns dominate DeFi. The front-running attack, in which bad actors use transaction knowledge to gain an unfair advantage, is a major issue. This hack might cost investors a lot of money and damage the DeFi ecosystem. Novel cryptographic algorithms and transaction-ordering dependencies are being studied to reduce this risk. As the Metaverse and DeFi grow, these security issues must be addressed while maximizing their revolutionary potential. Meeting these two realms could restructure financial ecosystems, improve user experiences, and transform transactions and interactions. To fully reap the benefits, research, and innovation are need-ed to develop a solid and secure financial infrastructure in the Metaverse's virtual landscapes. To effectively counter the persistent issue of front-running in the DeFi space, we propose the implementation of the Optimizing AMMs algorithm. Conventional AMMs, due to their inherent price predictability, are susceptible to front-running attacks. However, by infusing an optimization layer into AMMs, the entire price-setting process gains a heightened level of un-predictability and intricacy, creating formidable barriers for attackers aiming to forecast and exploit transaction sequences. The innovative Optimizing AMM algorithm functions by dynamically adjusting pricing parameters based on an array of factors including historical trading trends, liquidity depth, and market volatility. This adaptive pricing mechanism introduces a layer of uncertainty, effectively diminishing the foreseeability of price fluctuations. Consequently, this approach serves as a deterrent, dissuading opportunistic individuals from identifying lucrative prospects. In addition, the method introduces stochastic transaction execution delays, further complicating the efforts of malicious actors to strategically time their transactions. By amalgamating these strategies, the DeFi ecosystem can foster a more secure and equitable trading environment. This discourages opportunists from finding lucrative opportunities. Additionally, stochastic transaction execution delays complicate malicious actors' transaction timing strategies. The DeFi ecosystem can im-prove trading security and fairness with these strategies.

Compliance with ethical standards

Acknowledgments

We would like to express our deepest gratitude to Prof. Dr. Md. Asraf Ali for his invaluable guidance, unwavering support, and insightful feedback throughout the entire duration of this research project. His expertise and mentorship have been instrumental in shaping the direction of our study and refining our approach. We are truly grateful for his

dedication to academic excellence and his commitment to fostering our intellectual growth. Thank you, Prof. Dr. Md. Asraf Ali, for your profound influence on this research endeavor.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] R. Sharma, What Is Decentralized Finance (DeFi) and How Does It Work?, Investopedia, Sep. 2022, [Online]. Available: https://www.investopedia.com/decentralized-finance-defi-5113835

[2] L.-H. Lee, All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda, arXiv.org, Oct. 06, 2021. https://arxiv.org/abs/2110.05352

[3] Wikipedia contributors, Snow Crash, Wikipedia, Sep. 2023, [Online]. Available: https://en.wikipedia.org/wiki/Snow_Crash

[4] J. Sanchez, Second life: An interactive qualitative analysis, in Society for Information Technology & Teacher Education International Conference, 2007, pp. 1240–1243.

[5] ACM PUB27 New York, NY, USA, 3D Virtual worlds and the metaverse: Current status and future possibilities: ACM Computing Surveys: Vol 45, No 3, ACM Computing Surveys. https://dl.acm.org/doi/10.1145/2480741.2480751

[6] A. Bruun and M. L. Stentoft, Lifelogging in the wild: Participant experiences of using lifelogging as a research tool, in IFIP Conference on Human-Computer Interaction, 2019, pp. 431–451, doi: 10.1007/978-3-030-29387-1_24.

[7] A survey on metaverse: fundamentals, security, and privacy, IEEE Journals & Magazine | IEEE Xplore, Jan. 1, 2023, https://ieeexplore.ieee.org/document/9880528.

[8] A. Bruun and M. L. Stentoft, Lifelogging in the wild: Participant experiences of using lifelogging as a research tool, in IFIP Conference on Human-Computer Interaction, 2019, pp. 431–451, doi: 10.1007/978-3-030-29387-1_24.

[9] EXPLAINED: Move Over Social Media? Why Facebook Wants To Be Known As A Metaverse Company, News18, Oct. 24, 2021,https://www.news18.com/news/explainers/explained-move-over-social-media-why-facebook-wants-to-be-known-as-a-metaverse-company-4359371.html.

[10] D. A. Zetzsche, D. W. Arner, and R. P. Buckley, Decentralized Finance, Journal of Financial Regulation, vol. 6, no. 2, pp. 172–203, 2020, https://doi.org/10.1093/jfr/fjaa010.

[11] D. Metelski and J. Sobieraj, Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations, International Journal of Financial Studies, vol. 10, no. 4, p. 108, 2022, https://doi.org/10.3390/ijfs10040108.

[12] J. P. Chousa, M. Á. López-Cabarcos, A. Šević, and I. González-López, A preliminary assessment of the performance of DeFi cryptocurrencies about other financial assets, volatility, and user-generated content, Technological Forecasting and Social Change, vol. 181, p. 121740, 2022, https://doi.org/10.1016/j.techfore.2022.121740.

[13] T. K. Sharma, Centralized Oracles Vs. Decentralized Oracles, Blockchain Council, 2021, https://www.blockchain-council.org/blockchain/centralized-oracles-vs-decentralized-oracles/.

[14] P. K. Ozili, Decentralized finance research and developments around the world, Journal of Banking and Financial Technology, vol. 6, no. 2, pp. 117–133, 2022, https://doi.org/10.1007/s42786-022-00044-x.

[15] R. Auer, The Technology of Decentralized Finance (DeFi), 2023, https://www.bis.org/publ/work1066.htm.

[16] S. M. Werner, SoK: Decentralized Finance (DeFi), arXiv.org, 2021, https://arxiv.org/abs/2101.08778.

[17] Money Market Fund Vulnerabilities: A Global Perspective - FEDERAL RESERVE BANK of NEW YORK, https://www.newyorkfed.org/research/staff_reports/sr1009.html.

[18] DeFi Security Lecture 8 — Front Running Attack - beaver-smartcontract-security - Medium, Medium, Apr. 19, 2022, https://medium.com/beaver-smartcontract-security/defi-security-lecture-8-front-running-attack-3247045dd9cd.

[19] E. Meyer, Decentralized Finance—A Systematic Literature Review and Research Directions, http://www.zbw.eu/econis-archiv/handle/11159/498725.

[20] F. Schär, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Review, vol. 103, no. 2, 2021, https://doi.org/10.20955/r.103.153-74.

[21] D. Metelski and J. Sobieraj, Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations, International Journal of Financial Studies, vol. 10, no. 4, p. 108, 2022, https://doi.org/10.3390/ijfs10040108.

[22] V. Gramlich, T. Guggenberger, M. Principato, B. Schellinger, and N. Urbach, A multivocal literature review of decentralized finance: Current knowledge and future research avenues, Electronic Markets, vol. 33, no. 1, 2023, https://doi.org/10.1007/s12525-023-00637-4.

[23] K. Qin, L. Zhou, Y. Afonin, L. Lazzaretti, and A. Gervais, CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance, ArXiv, 2021, /abs/2106.08157.

[24] P. Daian et al., Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges, ArXiv, 2019, /abs/1904.05234.

[25] W. Li, J. Bu, X. Li, and X. Chen, Security Analysis of DeFi: Vulnerabilities, Attacks and Advances, ArXiv, 2022, /abs/2205.09524.

[26] Front Running and Sandwich Attack Explained | by QuillAudits Team | Medium | Medium, Medium, Nov. 15, 2022, https://quillaudits.medium.com/front-running-and-sandwich-attack-explained-quillaudits-de1e8ff3356d.

[27] F. T. Christof, The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts, Ferreira Torres Christof, 2021, https://orbilu.uni.lu/handle/10993/46244.

[28] T. K. Sharma, What Is Gwei? The Cryptocurrency Explained, Investopedia, 2022, https://www.investopedia.com/terms/g/gwei-ethereum.asp.

[29] T. Chen et al., An Adaptive Gas Cost Mechanism for Ethereum to Defend Against Under-Priced DoS Attacks, ArXiv, 2020, /abs/1712.06438.

[30] flashbots/mev-relay-js, GitHub, https://github.com/flashbots/mev-relay-js.

[31] H. Berg and T. A. Proebsting, HANSON'S AUTOMATED MARKET MAKER, The Journal of Prediction Markets, vol. 3, no. 1, pp. 45–59, 2012, https://doi.org/10.5750/jpm.v3i1.451.

[32] E. Yazici, Decoding Frontrunning: Understanding the Key Terms and Techniques, OMNIA, June 7, 2023, https://omniatech.io/pages/dec

[33] T. Chen et al., GasChecker: Scalable Analysis for Discovering Gas-Inefficient Smart Contracts, in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, pp. 1433-1448, July-Sept. 2021, doi: 10.1109/TETC.2020.2979019.

[34] C. Baum, SoK: Mitigation of Front-running in Decentralized Finance, 2021, https://eprint.iacr.org/2021/1628.

[35] D. Beaver and S. Haber, Cryptographic Protocols Provably Secure Against Dynamic Adversaries, in Springer eBooks, pp. 307–323, 2007, https://doi.org/10.1007/3-540-47555-9_26.

[36] npm: @uniswap/v3-core, Npm, https://www.npmjs.com/package/@uniswap/v3-core.

[37] V. Mohan, Automated market makers and decentralized exchanges: a DeFi primer, Financial Innovation, vol. 8, no. 1, 2022, https://doi.org/10.1186/s40854-021-00314-5.

[38] D. Bernhardt and B. Taub, Front-running dynamics, Journal of Economic Theory, vol. 138, no. 1, pp. 288–296, https://doi.org/10.1016/j.jet.2007.05.005.

[39] M. Bartoletti, J. Chiang, and A. L. Lafuente, A Theory of Automated Market Makers in DeFi, in Lecture Notes in Computer Science, pp. 168–187, 2021, https://doi.org/10.1007/978-3-030-78142-2_11.

[40] H. Adams, N. Zinsmeister, and D. Robinson, Uniswap v2 Core, 2020, https://uniswap.org/whitepaper.pdf.

[41] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, High-Frequency Trading on Decentralized On-Chain Exchanges, ArXiv, 2020, /abs/2009.14021.

[42] K. Wüst and A. Gervais, Ethereum Eclipse Attacks, ETH Zürich, https://doi.org/10.3929/ethz-a-010724205.

[43] N. Szabo, Formalizing and Securing Relationships on Public Networks, First Monday, vol. 2, no. 9, Sep. 1997, doi: 10.5210/fm.v2i9.548.

[44] Wood, G., et al. (2014) Ethereum A Secure Decentralized Generalised Transaction Ledger. Ethereum Project Yellow Paper, 151, 1-32.

[45] Patrick McCorry School of Computing Science, Newcastle University, Newcastle upon Tyne, UK, A Smart Contract for Boardroom Voting with Maximum Voter Privacy | Financial Cryptography and Data Security, Guide Proceedings. https://dl.acm.org/doi/abs/10.1007/978-3-319-70972-7_20

[46] Hard Fork Completed | Ethereum Foundation Blog, Ethereum Foundation Blog, Jul. 22, 2016. https://blog.ethereum.org/2016/07/22/hive-strived-clean-fork

[47] P. Daian.Analysis of the DAO exploit, Hacking Distributed, Jun. 18, 2016. https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/

[48] Fan Zhang Cornell University, Ithaca, NY, USA, Town Crier | Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM Conferences. https://dl.acm.org/doi/10.1145/2976749.2978326

[49] F. Zhang, Paralysis Proofs: Secure Access-Structure Updates for Cryptocurrencies and More, 2018. https://eprint.iacr.org/2018/096

[50] O. Kharif, CryptoKitties Mania Overwhelms Ethereum Network's Processing, Bloomberg.com, Dec. 05, 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-12-04/cryptokitties-quickly-becomes-most-widely-used-ethereum-app

[51] G. Fenu, L. Marchesi, M. Marchesi, and R. Tonelli, The ICO phenomenon and its relationships with ethereum smart contract environment. 2018. doi: 10.1109/iwbose.2018.8327568.