# Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem

Ye Wang
wangye@ethz.ch
ETH Zurich
Zurich, Switzerland

Patrick Zuest
patrick.zuest@inf.ethz.ch
ETH Zurich
Zurich, Switzerland

Yaxing Yao
yaxingyao@umbc.edu
University of Maryland, Baltimore County
Baltimore, United States

Zhicong Lu
zhiconlu@cityu.edu.hk
City University of Hong Kong
Hong Kong, China

Roger Wattenhofer
wattenhofer@ethz.ch
ETH Zurich
Zurich, Switzerland

## ABSTRACT

Decentralized finance (DeFi) enables crypto-asset holders to conduct complex financial transactions, while maintaining control over their assets in the blockchain ecosystem. However, the transparency of blockchain networks and the open mechanism of DeFi applications also cause new security issues. In this paper, we focus on sandwich attacks, where attackers take advantage of the transaction confirmation delay and cause financial losses for victims. We evaluate the impact and investigate users' perceptions of sandwich attacks through a mix-method study. We find that due to users' lack of technical background and insufficient notifications from the markets, many users were not aware of the existence and the impact of sandwich attacks. They also had a limited understanding of how to resolve the security issue. Interestingly, users showed high tolerance for the impact of sandwich attacks on individuals and the ecosystem, despite potential financial losses. We discuss general implications for users, DeFi applications, and the community.

**ACM Reference Format:**
Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. 2022. Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3491102.3517585

## 1 INTRODUCTION

Recently, blockchain-based decentralized finance (DeFi) markets have emerged in the blockchain ecosystem. They are attracting a surge of interest with a total gross value locked (GVL) of up to 133 billion USD by August 2021 [12]. In traditional centralized cryptocurrency trading markets (e.g., Binance, OKEx), trades are controlled by a centralized operator, and traders have to transfer their assets to this central authority [33]. Unlike centralized markets, DeFi markets inherit the characteristics of blockchains, i.e., the decentralized and permissionless nature [61]. DeFi markets are smart contracts deployed on blockchains [52] which support a wide variety of financial services [41, 46], such as borrowing and lending [40], asset exchanges [19], leverage trading [6], as well as novel applications such as flash loans [48]. However, since there is no regulation in DeFi markets and all user information, transaction information, and market information is public to anybody, DeFi-related security issues have emerged [27, 28, 48, 68].

One of the most common security issues is known as a sandwich attack [68]. Sandwich attacks have received attention from academia [20, 21, 28, 47, 65, 67], as well as the blockchain community [10, 45] within a short time after first being reported by Zhou et al. [68] in 2020. Sandwich attacks happen in automated market maker (AMM) decentralized exchanges (DEXes) [60], where the exchange rate of each transaction is determined by the trading volume and the reserved liquidity in the market. Here is how sandwich attacks work: An attacker observes a non-executed transaction (victim transaction) in the blockchain P2P network. The attacker then quickly buys the asset for a low price. The attacker makes sure that its transaction is scheduled shortly before the victim transaction ("front-run"). The attacker then sells the asset shortly after the victim transaction ("back-run") to make a profit.

Sandwich attacks have an impact on the price of an asset. After a buy transaction (front-run transaction) is completed, the reserves of two tokens in the liquidity pool change. Consequently, the price of the asset will be higher than if no attack had taken place (cf. Figure 2). This results in a worse exchange rate and financial losses to the victim. Potential profits can also incentivize miners to mount forking attacks and thus bringing concrete, measurable consensus-layer security challenges to the blockchain system [27].

Although sandwich attacks have received widespread attention, the magnitude of their impact is unclear. Furthermore, we want to know how users perceive sandwich attacks. In this paper, we aim to fill these two knowledge gaps through a mixed-method study. We first quantify the impact of sandwich attacks, both on the entire market and on individual traders, providing a ground truth of the severity of the security issue. Then, we examine the knowledge gap between user perception and the real impact of sandwich

*CHI '22, April 29-May 5, 2022, New Orleans, LA, USA*
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9157-3/22/04…$15.00
https://doi.org/10.1145/3491102.3517585

attacks by interviewing both DeFi insider users ($n = 5$) and non-professional DeFi users ($n = 10$).

This paper makes three contributions.

- First, we provide a ground truth of the impact of sandwich attacks, one of the common security issues in the blockchain ecosystem. We analyze transaction data of Uniswap V2 [18] and Sushiswap [16] quantitatively. We find that, in April 2021, the monthly number of sandwich attacks has reached 84,000 (on average one attack every 30 seconds). Over a period of one year, the financial losses of victims exceeded 90,000 ETH (300 Million USD) out of 6 million ETH trading volume. The impact has more than doubled since the end of 2020 [28, 47]. The probability that a potential victim will be attacked has increased fourfold, i.e., from 10% to 40%. These quantitative results indicate that users are not effectively defending themselves against sandwich attacks as of April 2021, indicating a potential gap between users' perceptions of sandwich attacks and their real-world impact.
- Second, our work elucidates the gap between users' perceptions of sandwich attacks and its real world impact, illustrating the security challenges of emerging DeFi markets in the blockchain ecosystems. Our qualitative study shows that both insider and non-professional users were unaware of the severity of the attacks, likely because online resources (e.g., technical blogs, public speeches) generally ignore the real impact of sandwich attacks on traders. In addition, our interviewees have differing opinions on the impact of sandwich attacks: While sandwich attacks can lead to financial losses for non-informed traders, they can also be beneficial to traders and the blockchain ecosystem as a whole.
- Third, we explore implications of the security challenges in the DeFi ecosystem for blockchain systems, DeFi applications, and DeFi users. We summarize the security challenges in DeFi systems in three categories: information asymmetries between different users, misleading protocol design of DeFi applications, and collaborations between different stakeholders. We suggest that the platform operators and other community members with advanced knowledge could improve the awareness of users by educating them with fundamental knowledge. Moreover, DeFi applications may integrate mitigation strategies for users in their financial services. We further discuss the philosophical question of if sandwich attacks are malicious or just side effects of transparent monetary transactions.

## 2 BACKGROUND OF SANDWICH ATTACKS

In this section, we first introduce AMM DEXes [60], where sandwich attacks take place. Then, we review the mechanism of sandwich attacks.

### 2.1 AMM DEXes

DEXes support trading between different cryptocurrencies. The prevalent DEXes are built as so-called automated market makers (AMM). They aggregate liquidity (i.e. cryptocurrencies) contributed by liquidity providers in token pools. Traders exchange assets with liquidity and pay commission fees to the liquidity pool. Any single buy or sell order can be executed independently of other trades on AMM DEXes. For example, when traders want to exchange cryptocurrency $A$ for $B$, they can call a smart contract function that transfers $A$ from the traders' account to the liquidity pool and sends $B$ from the liquidity pool to the traders' account. The exchange process does not involve the participation of any other traders. The exchange rate between $A$ and $B$ is determined by transparently predefined functions encoded in the DEX smart contract.

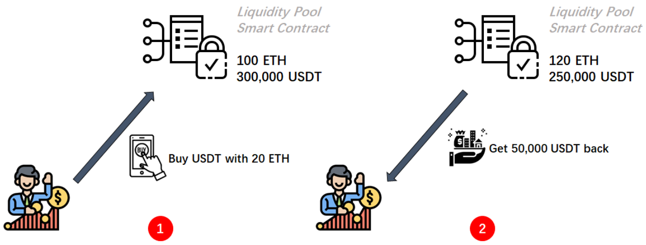


**Figure 1: An example of an asset exchange on AMM DEXes with constant product function and no commission fee. The trader sends 20 ETH to the liquidity pool and gets 50,000 USDT back. The product of the amount of ETH and USDT in the liquidity pool is constant, i.e., 30,000,000.**

Constant product functions are one of the most widely used pricing mechanism. Assume a trader wants to exchange $\delta_a$ of $A$ for $B$ token and the liquidity of $A$ and $B$ are $a$ and $b$. The following equation always holds during the transaction: $a \cdot b = (a + \delta_a \cdot r_1) \cdot (b - \frac{\delta_b}{r_2})$, where $r_1$ and $r_2$ denote the commission fee in asset $A$ and $B$ respectively (cf. Figure 1). In Uniswap [18] and Sushiswap [16], $r_1 = 0.997$ and $r_2 = 1$, which indicates that the commission fee is equal to $3‰ \cdot \delta_a$. The remaining liquidity in the pool is equal to $(a + \delta_a, b - \frac{r_1 \cdot r_2 \cdot b \cdot \delta_a}{a + r_1 \cdot \delta_a})$.

Because market operations in AMM DEXes are invoked by transactions on blockchains, users are required to pay a transaction fee to the miners. Specifically, in Ethereum every transaction costs a predetermined amount of "gas". A transaction issuer specifies how much they are willing to pay per unit of gas (i.e., the gas price). The transaction fee paid to miners corresponds to the product of the total gas consumption and the gas price.

### 2.2 Attack Mechanism

The exchange rate of each transaction on AMMs is determined by predefined algorithms and market liquidity reserves [19]. A buy order will increase the price of an asset, while a sell order decreases the asset price. Therefore, sandwich attackers can utilize such price changes to take a profit from a victim transaction. Attackers can continuously monitor the network to find a victim transaction $T_V$ which entails price differences. When a sandwich attacker observes $T_V$, it can buy the asset for a low price before the victim transaction is executed (a front-running transaction $T_{A1}$), and sell the asset after the victim transaction increases the price (a back-running transaction $T_{A2}$). Using this approach, attackers can generate a profit. In particular, the exchange rate of the victim transaction is worse than it would have been without a front-running transaction. This

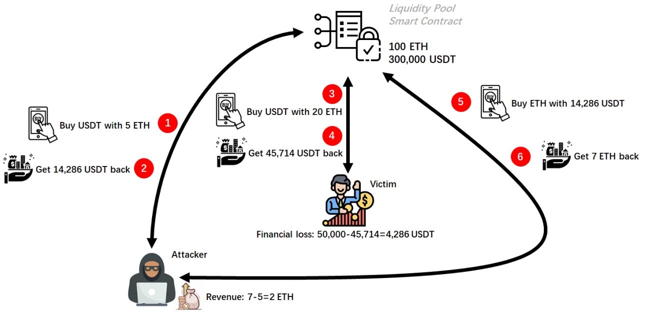


**Figure 2: An example of sandwich attacks on AMM DEXes with constant product function and no commission fee. The attacker front-runs the victim transaction with a buy order of USDT and back-runs the victim transaction with a sell order. The reserves in the liquidity pool change after each transaction. The original state is 100 ETH/300,000 USDT. Then it becomes 105 ETH/285,714 USDT after the first transaction from the attacker. After the victim transaction, the reserves in the liquidity pool change to 125 ETH/240,000 USDT. Finally, the reserves change to 118 ETH/254,286 USDT after the second transaction from the attacker.**

results in a financial loss for the victim and hence negatively influences their security.

We illustrate an example of sandwich attacks in Figure 2. The victim transaction aims to buy USDT with 20 ETH in the market. If there was no attacker, the trader would get 500,000 USDT back, as shown in Figure 1. However, a sandwich attacker may submit a front-running transaction and a back-running transaction to get 2 ETH as revenue from the victim transaction, while the victim gets a worse price for its exchange.

The price increase is limited by the chosen slippage rate of $T_V$, which is the maximum difference between the ideal price observed on the market and the real price of the exchange order. If the market price increases too much before the victim transaction is executed, its slippage detection will be triggered, and the transaction will fail. On the other hand, in most scenarios, the larger the market price move generated by the victim transaction, the more revenue sandwich attackers can get.

Therefore, most sandwich attacks will push an asset's price close to the worst acceptable price of a victim transaction, which is determined by the slippage rate. We refer the interested reader to the supplementary materials of this paper for comprehensive analytical computations of the attacking input and financial loss of sandwich attacks.

Most AMM DEXes require a commission fee. Moreover, executing transactions on the blockchain consumes gas and traders have to pay gas fees to miners. The cost of sandwich attacks may thus exceed the revenue of an attack, resulting in a negative net profit of a sandwich trade.

# 3 RELATED WORK

In this section, we first provide background knowledge of security issues in decentralized finance markets and the mechanism of sandwich attacks.

## 3.1 Security Challenge in Decentralized Finance

In 2009, Bitcoin [42] became the first worldwide permissionless transaction system. Traders can send and receive money online without relying on custodial third parties. Moreover, Bitcoin also popularized the primitive of smart contracts [57]: some lines of code that execute when pre-set conditions are met. Ethereum [62] is one of the most used blockchain platforms with smart contract implementations [25]. These contracts enabled the development of complex financial services and the creation of hundreds of thousands of cryptocurrencies. [26].

Earlier financial services for cryptocurrencies are mostly centralized. These applications are developed outside of the blockchain system, and the trading mechanism and system architecture are not open to the public. DeFi applications on the other hand are deployed on the blockchain and the respective code is often open-sourced. Therefore, there are three key challenges to security in the DeFi market compared to the CeFi market.

The first security challenge relates to blockchain system security. Since DeFi applications are smart contracts on the blockchain system, their execution is affected by blockchain vulnerabilities. For instance, Eclipse attacks [31, 34] to the blockchain system could separate the network, which results in churning logic among different market orders. Feather forking [66] and block reorganization [35, 67] may cause consensus vulnerabilities and thus lead to double-spending issues [22] in DeFi markets.

The second challenge is related to specific smart contract implementations. Since DeFi developers typically release the source code of their applications publicly, design flaws and code mistakes can be easily found and exploited by attackers. Take reentrancy attacks [43, 56], delegatecall injection attacks [53], and attacks with mishandled exceptions in codes [44, 49] as examples. There were nearly a dozen attacks [1–5, 7, 8, 11, 13–15] exploiting smart contract implementations and DeFi users lost over 80M USD.

The third security challenge, and also the most common one, stems from the protocol of DeFi applications. Since DeFi applications are deployed on a permissionless blockchain platform, all market states can be observed publicly in real-time. Meanwhile, traders' transactions are broadcast to the blockchain P2P network and stored in a mempool. The transactions in this mempool can be accessed by anyone before miners include them in a block. Therefore, attackers can forecast the future market states based on non-executed transactions in the network and use this knowledge to manipulate market operations. For instance, attackers may observe a victim transaction from the mempool and front-run [27] or back-run them [69] to take profit. Moreover, DeFi applications are isolated from outside of the blockchain platform, while external information cannot be utilized by these applications in real-time. Therefore, DeFi applications rely on each other and share information to determine market operations. For example, some lending borrowing applications use the real-time exchange rate in DEXes to determine the collateral rate [63]. Some attackers target dependencies between platforms by manipulating the state of one application and profiting from another one [67].

Since security challenges related to DeFi protocols involve interactions between traders and DeFi applications, it is hard to detect them effectively before launching applications. Furthermore, such security issues are associated with DeFi markets and continuously impact DeFi users in the long term. Therefore, it is important to understand how users become aware, perceive, and prevent security issues in DeFi markets. In this paper, we take sandwich attacks as an example and conduct both quantitative and qualitative studies to explore security issues for users in DeFi markets and the blockchain ecosystem.

## 3.2 Sandwich Attacks

Since the first paper on sandwich attacks came out, there have been several studies considering the emerging security issues in DeFi markets. Zhou et al. [68] introduced the mechanism of sandwich attacks, evaluated attack implementations on the Ethereum network, and further suggested a better attack implementation [67]. Qin et al. [47] quantified the emergence of sandwich attacks in DeFi markets considering 144 cryptocurrencies. Ferreira et al. [28] further analyzed the attacking strategies among different attackers. Yüksel [65] considered a mitigation strategy of sandwich attacks based on DEXes mechanism design. Angeris et al. [20] analyzed the strategy of miners when collaborating with sandwich attackers from the game-theoretical perspective. Bartoletti et al. [21] introduced a better implementation for sandwich attackers when there exists an external market providing stable exchange prices. However, no previous studies has fully considered the real impact of sandwich attacks on the DeFi markets and individual users. They also have not provided any information about user awareness of sandwich attacks in DeFi markets. Given that the sandwich attack is an unavoidable security issue in the blockchain ecosystem, understanding user perception of and attitude towards sandwich attacks may help us improve the security of online markets based on blockchain technology.

## 3.3 Security Awareness of Blockchain Users

The HCI community has noticed the blockchain security issues and several user studies [17, 30, 38, 58, 59] have been conducted to understand user motivation, behavior, security perception, and security-related practices. Trust [37, 51], usability issues [29, 59], and complicated key management [17, 58] have been reported as the main challenges for using cryptocurrencies. However, these studies have not considered security issues in DeFi markets, which contain most user activities on blockchains and interactions between users. Moreover, their definition of security focusses on asset management and not on financial operations. The process of trading cryptocurrencies on the market may be riskier for users than keeping assets in wallets. Given that DeFi transactions are an emerging use case of cryptocurrencies on blockchain systems, our work explores more prevalent security issues in the blockchain ecosystem.

# 4 MEASURING THE IMPACT OF SANDWICH ATTACKS

To better understand the real-world impact of sandwich attacks on DeFi users, we conduct a quantitative study to find sandwich attacks that happened on the predominant DEXes, i.e., Uniswap and Sushiswap, and show how DeFi users are impacted. Compared to previous studies on sandwich attacks in the security community, which focus on attackers' strategies, we analyze sandwich attacks from the perspective of DeFi users. We aim to explore the following questions: How many sandwich attacks have been conducted on these DEXes? How much money did users lose because of sandwich attacks? Which kind of transactions are most likely to be attacked? What is the probability that a trader will be sandwich attacked?

## 4.1 Identifying Sandwich Attacks

We run our own Ethereum node to get access to the block history. A modified geth client is used to export all transaction receipts where a swap event was triggered by a smart contract of Uniswap or Sushiswap. Our analysis starts at block number 10000835 (May 4, 2020), where Uniswap version 2 has been deployed and ends at block number 12344944 (April 30, 2021). The detailed method for identifying sandwich attacks is provided in the supplementary file.

## 4.2 Measuring the Impact of Sandwich Attacks on DeFi Markets

In the given period, we analyzed $2,344,109$ blocks using the heuristics above. In total, we discovered $480,276$ sandwich attacks. We found $964$ different proxy contracts that conducted at least one attack transaction. The most active proxy contract (0x0000..0084) processed $51,475$ of the attack transactions we discovered ($5.36\%$). Overall, we observe sandwich attacks in $5,728$ pools. The most popular pair was ETH-YELD which was attacked almost $3,500$ times. More then a quarter of liquidity pools ( $1,450$ out of $5,728$) have only been attacked once and around 55% of the involved pools were attacked 10 times or less. The share of pools that were attacked 100 times or more represent 18.5% of all attacked pools.

To make statements about the financial loss of the victims of sandwich attacks, we focus on transactions where at least one of the two involved tokens is ETH (which is the case for $96.28\%$ of attacks). This allows us to sum up the accumulated loss of victims in ETH, which is approximately equal to attack revenue. The accumulated loss and the number of sandwich attacks over time can be seen in Figure 3. Both he number of attacks and the accumulated loss have increased steeply since May 2020.

Recently, relay services have emerged in the blockchain ecosystem, especially in Ethereum. Relay services, such as Flashbots [9], are independent of the blockchain P2P network and offer an alternative option for users to communicate to miners. A centralized relay server forwards transactions directly to miners, without broadcasting them on the P2P network. Miners connected to the relay server then prioritize the highest bidding relay transaction at the top of a block. If a victim transaction is submitted to miners through relay services, attackers cannot observe the victim transaction in a mempool and attack it. However, these relay services also allow users to submit a bundle of transactions, even from other

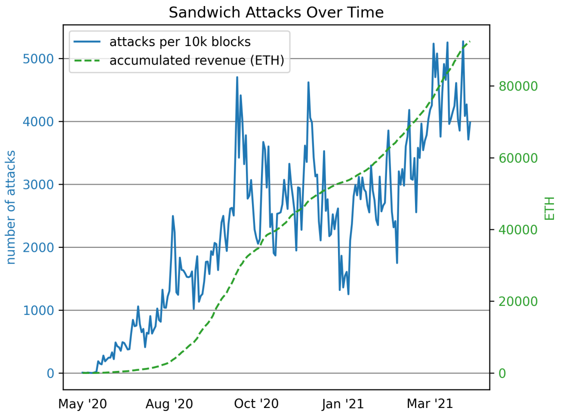


**Figure 3: The number of sandwich attacks we observed and the profit attackers accumulate (the financial loss of victims) over time.**

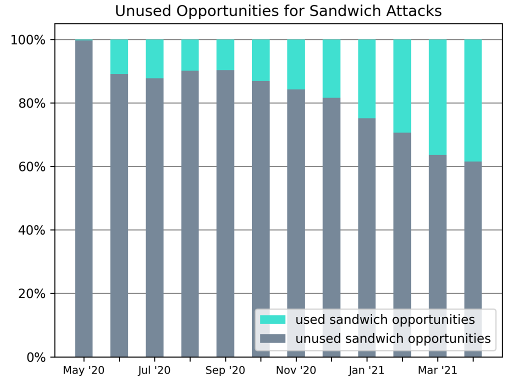


**Figure 4: Ratio of profitable sandwich opportunities that were used by attackers, considering only transactions with ETH as the input token.**

traders. Therefore, sandwich attackers are able to include their attacking transactions with the victim transactions together in a bundle and submit it to miners through relay services. Furthermore, relay services ensure that if the sandwich attackers cannot benefit from the attacking victim transactions due to the market change, miners will not execute the bundle in the next block [9]. Flashbots was launched at the beginning of January 2021 and by mid-April 2021, more than 80% of the Ethereum hashrate was using Flashbots [10]. The surge of financial loss at the beginning of 2021 could be connected to attackers collaborating with miners through relay services.

Following the mechanism of relay services, miners can ensure the success of the sandwich attack issued by attackers, while attackers share their profits with miners. Such cooperation between miners and attackers makes the interests of users suffer more seriously. Table 1 shows the observed changes ever since the emergence of the relay services. From January 2021 to the end of our measurement period, more than one third of sandwich attacks pay a gas price that is less or equal to 1 Gwei. Transactions through relay services are usually sent with a gas fee lower than 1 GWei. This observation indicates that miners started actively collaborating with sandwich attackers to extract additional value. In this symbiosis, miners do not charge gas fees from attackers, while attackers share their profits from sandwich attacks with miners. Meanwhile, more sandwich attacks result in a profitable outcome, which indicates the efficiency of the collaboration between attackers and miners.

| Property | Nov | Dec | Jan | Feb | Mar | Apr |
|---|---|---|---|---|---|---|
| Total Attacks | 52K | 60K | 48K | 51K | 76K | 84K |
| Gas Price $\leq$ 1 Gwei | 0% | 0% | 5% | 5% | 6% | 36% |
| Average Distance | 39.6 | 37.9 | 33.7 | 33.5 | 31.8 | 13.9 |
| Profitable Attacks | 78% | 76% | 67% | 80% | 84% | 92% |

**Table 1: Implications of active reordering by miners**

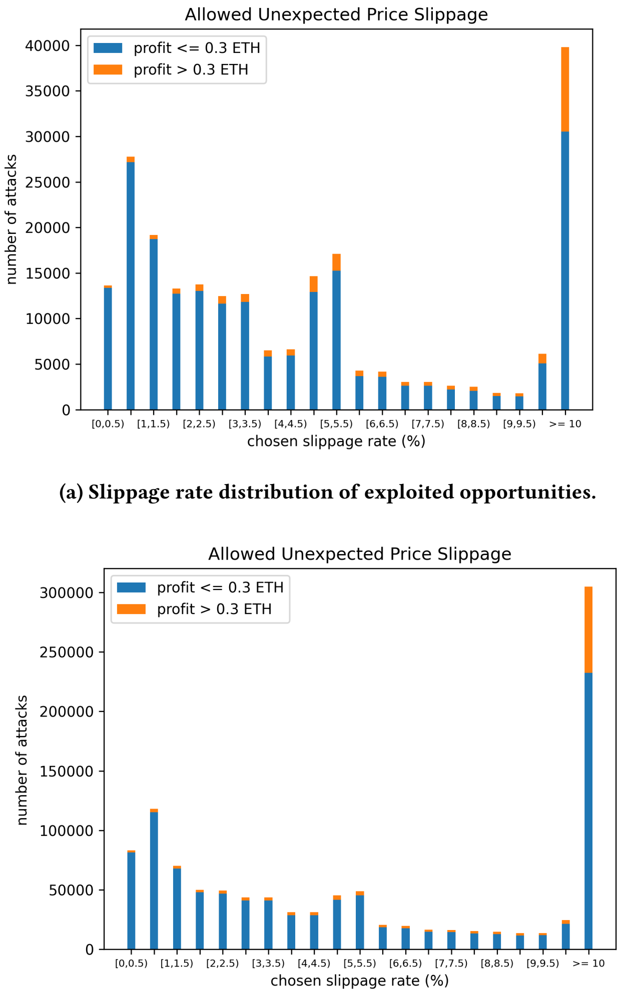
Moreover, our analysis showed that attackers always achieve the maximum possible profit, i.e. they choose an ideal input amount for the buy transaction and push the price to its limit. The minimum output and the actual output of the victim transaction differed by less than 1% on average. These facts suggest that sandwich attacks increasingly influence the average DeFi users on DeFi markets. In the rest of this section, we focus on individual victim transactions and explore which transactions are vulnerable to sandwich attacks.

### 4.3 Analyzing the Impact of Sandwich Attacks on Individual Traders

Whether a transaction can provide positive revenue to sandwich attackers depends on the slippage tolerance and the input amount of the victim transaction, as well as the sizes of the respective liquidity pools. The details for this calculation were included in the supplementary material.

To determine the risk to be attacked, we investigated all transactions that occurred in the given time frame. For transactions that were not attacked, We checked whether it would have been profitable to do so. There were $17,644,672$ transactions in the given time frame. Most bots, however, only execute attacks where ETH serves as input token, so we focus our analysis on the $9,003,759$ transactions where this was the case. In total, we found $3,612,343$ transactions with ETH as the input token that could have been profitably attacked. Figure 4 shows how the share of unused sandwich opportunities declined over time. For instance, when users submit a profitable victim transaction, the probability of being sandwich attacked has increased from $10\%$ to $40\%$ within half a year. This increasing trend of the utilization of sandwich opportunities suggests that sandwich attacks have widely impacted DeFi users.

As we introduced in Section 2, users set a slippage rate for their transactions to ensure that their transactions can be executed when the market price volatility is high. Attackers utilize the slippage rate setting and push the price of the victim transactions to its limit. Therefore, we examine the distribution of slippage rates of



**(a) Slippage rate distribution of exploited opportunities.**

**(b) Slippage rate distribution of unused opportunities.**

**Figure 5: Distribution of the chosen slippage rates for all profitable attacks where the victim was sent to a router contract.**

used and unused sandwich opportunities to understand how this setting influences the attack results. Note that the slippage rate also influences the the potential profit that can be generated from an affected transactions. If the slippage rate is 10%, the victim will suffer a financial loss of 10% compared to a scenario without sandwich attacks.

Figure 5 shows how the selected slippage rates are distributed. We find that the slippage rates of used and unused transactions are similar. However, the official Uniswap V2 interface suggests slippage rates between 0.1% and 1%. Such a high share of transactions with the slippage tolerance set to more than 10% reveals the knowledge gap of sandwich attacks in the DeFi community, as these transactions have a high risk of being attacked,.

## 5 INTERVIEW STUDY METHOD

Our measurement results suggest that there might be a gap between users' awareness of sandwich attack and the real-world situation. Therefore, we conducted an interview study to better understand users' perceptions and attitudes towards sandwich attacks.

### 5.1 Participant Recruitment

For our study purpose, we target two groups of DeFi users. The first group consists of DeFi insider users, i.e., those who work in the blockchain industry. These users include researchers, professional DeFi investors, and developers of DeFi applications. The second group consists of non-professional DeFi users, i.e., those who are not related to the blockchain industry.

We published our recruitment materials on Twitter and Discord. Additionally, we also utilized personal contacts of the research team to connect with the DeFi community and recruit participants. To qualify for the study, participants 1) needed to be aware of sandwich attacks and 2) could describe the mechanism of sandwich attacks.

However, during the recruitment, we observed that very few non-professional users had heard of sandwich attacks, making our recruiting effort difficult. As such, we decide to expand our recruitment strategy and also look for non-professional users without prior knowledge of sandwich attack. This is because even these DeFi users did not have prior knowledge of sandwich attack, they may still be impacted by these attacks. So, it is important to understand their general attitudes and perceptions of sandwich attack should they have the chance to learn about it. To help prepare these participants for the study session, we conducted an education session with non-professional DeFi users before interviewing them. Details of the education session can be found in Section 5.2.

From June to December 2021, we conducted interviews with five DeFi insider users (P1-P5), five non-professional DeFi users with background knowledge (B1-B5), and five non-professional DeFi users without background knowledge who participated in the education session (A1-A5). We conducted the interviews in English or Mandarin via Zoom. Each interview took 30-45 minutes and each participant received an equivalent of $15 USD honorarium for their time. Table 2 summarizes participants' demographics.

### 5.2 Education Session

As briefly mentioned, we conducted an brief education session on Clubhouse for non-professional DeFi users without background knowledge of sandwich attacks in June 2021. During the education session, we introduced four topics around sandwich attacks: the attack mechanism, the tools to determine whether a transaction has been attacked or not, the quantitative impact of sandwich attacks for traders, and the mitigation strategy to prevent attacks. This allowed non-professional users to understand the basic idea of sandwich attacks. We deliberately framed our education materials to be as neutral as possible.

### 5.3 Limitation

We note the following limitations in our qualitative study. First, we only included a relatively small sample of participants (n=15),

| ID | Occupation | DeFi experience | ID | Occupation | DeFi experience | ID | Occupation | DeFi experience |
|---|---|---|---|---|---|---|---|---|
| A1 | Programmer | < 0.5 year | B1 | Student | 2 years | P1 | Investor | 1.5 years |
| A2 | Housewife | 0.5 year | B2 | Artist | 3 years | P2 | Researcher | 2 years |
| A3 | Analyst | 1 year | B3 | Student | 1 year | P3 | Investor | 1 year |
| A4 | Student | < 0.5 year | B4 | Officer | 2 years | P4 | Developer | 1.5 years |
| A5 | Self-employed | 1 year | B5 | Editor | 0.5 year | P5 | Developer | 1 year |

**Table 2: Summary demographics of the interviewees.**

which may not comprehensively represent the general DeFi community. However, our study goal is not to thoroughly examine the security issue in the DeFi market. Instead, we aim to understand the gap between DeFi users' perception and the prevalence of security. Given the exploratory nature of our study, we believe that our study still provides unique insights that have not been investigated in the literature.

Second, for the non-professional DeFi users who do not have prior knowledge with sandwich attack (n=5), our education session might bias their perceptions. However, we believe that the biases are limited because the education session, to some degree, simulates how users would go about learning sandwich attack and its impact in the real-world. This approach is similar to the one in Yao et al.'s prior work [64]. Moreover, only one third of our participants went through the educational session. Thus, we believe that our results are still valid.

## 5.4 Interview Protocol

**Sandwich Attack Perception**. We began our interviews with questions about interviewees' demographics. We then asked about their knowledge in using blockchain and DeFi to ensure that they had sufficient background for our study, e.g., "When did you start trading on DeFi markets? Which DEXes do you usually use?" We then asked them to explain sandwich attacks in their own words and to visualize their understanding of sandwich attacks on a piece of paper or a white board. Once we confirmed that the interviewees had a good understanding of sandwich trades, we asked them how they became aware of this attack pattern, e.g., "How did you become aware of sandwich attacks?" We followed up with additional questions about their knowledge and understanding of sandwich attacks, e.g., "What are your estimates for the number of attacks, the loss of traders, and the probability of being sandwich attacked?"

**User Attitude on Sandwich Attacks.** The second part of the interview is about user attitude towards sandwich attacks. We asked them how they perceived the impact of sandwich attacks on different stakeholders, e.g., "What do you think is the impact of sandwich attacks on DeFi traders and liquidity providers?"

**Mitigation of Sandwich Attacks.** In the last part of the interview, we focused on understanding interviewees' needs and expectations regarding the prevention of sandwich attacks. To better gauge interviewees' needs, we designed a web-based application as a technology probe, which is presented to the interviewees during the interview. We published our tool on https://www.defi-sandwi.ch/ (cf. Figure 6). It automatically checks whether a trade on Uniswap V2 can potentially be sandwich attacked. If this is the case, a suitable mitigation strategy is suggested. During the interview, we asked interviewees whether they knew any mitigation strategies, e.g., "How do you prevent your own transactions from being attacked?", "Are there any other strategies you are aware of to prevent sandwich attacks, but you have not tried yourself? Why don't you try them?" Then, we presented the mitigation tool that we developed and asked interviewees about their opinions, e.g., "Do you have any idea how the tool could be improved?" After collecting user feedback for the tool interface, we asked interviewees what they expected from a sandwich attack mitigation tool, including the information that they needed and the functionality they looked for to prevent such attacks.

## 5.5 Data Analysis

We audio-recorded all interviews after getting interviewees' permission. The recordings were then transcribed and translated to English by the researchers who conducted the interviews. We then followed a common approach, i.e., thematic analysis [23], to analyze our interview data. Two researchers coded all interview transcriptions individually. Once finished, the two researchers compared, discussed, and converged the codes. Only when researchers agreed on the code, the result was added into a code book shared among the research team. Codes were designed based on our research questions. Then, we further classified codes as themes, including but not limited to: personal experience; overall estimation; personal mitigation experience; mitigation perception.

Then, the research team discussed codes. During the discussion period, we analyzed the raw data again to ensure the correctness of our final qualitative findings.

# 6 KNOWLEDGE OF SANDWICH ATTACKS

We summarize users' knowledge of sandwich attacks from two perspectives, i.e., their awareness of whether they were attacked personally and their awareness of the global impact of sandwich attacks on DeFi traders.

## 6.1 Knowledge of Personal Experiences

Since all the trading history is public on the blockchain, users can determine whether they have been sandwich attacked by checking the transactions before and after their trades. There are two methods for the detection: manually browsing transactions on blockchain information explorers (such as https://etherscan.io/), and automatic detection with third-party tools (such as https://sandwiched.wtf/). However, we found that most users were not aware of whether their transactions have been sandwich attacked or not. This is for two reasons. The first reason is that some users did not care about small financial losses. Even if a transaction is sandwich attacked, the asset price still satisfies the slippage tolerance set by traders. Because the price is not worse than their expectation, they did not see a need to check whether they were attacked: *"Because my trading volume is small. I did not care whether I was attacked or not. So I have never checked on the blockchain." (B2)*

The second reason is that the current tools for detecting sandwich attacks may not go along with user's knowledge or trading habits. For example, some interviewees feel that there is an excessive amount of information on blockchain explorers. It is difficult for them to determine whether their transactions have been sandwich attacked:*"The website (Etherscan) looks nice. But it is too complicated for me. ...Yes, I learned how to use that, but it is still quite difficult for me to find other transactions attacking me." (A2)* Although third-party tools allow users to detect sandwich attacks on their transactions automatically, some of our interviewees perceive that these tools may not significantly help them. Even though they detect sandwich attacks and provide users with new information, they are independent of the DEXes and cryptocurrency wallets that traders use daily. The tools do not automatically inform traders after an attack, which makes them less useful. *"I was not attacked myself. But I found out that one of my friends has been attacked seriously by checking his account on sandwiched.wtf. I showed the results to him. Now he noticed how much money he lost because of these attacks. ...We might just look at it occasionally. We can't check it after every transaction." (A4)*

Moreover, we find that some users cannot correctly determine whether they have been attacked or not. For instance, the method that B4 described, to determine whether he has been attacked, is not correct: *"I can look at Etherscan and see the trades immediately before and after my trade. Then I know whether I have been attacked." (B4)* However, as we have shown in Table 1, the average distance between the front-run and back-run transaction is larger than 10, which indicates that B4 might underestimate the impact of sandwich attacks.

## 6.2 Knowledge of the Overall Impact

As we had shared information about the impact of sandwich attacks in the education session, we only asked B1-B5 and P1-P5 to estimate the daily number of sandwich attacks, the financial losses incurred by traders, and the probability that their transactions are being attacked. Compared with the results of our analysis in Section 4, we find that users have limited knowledge of the overall impact of sandwich attacks. For example, P2 and P4 believe that more than $80\%$ of the victim transactions will be attacked, which is not true at the end of April 2021. On the other hand, P3, B2 and B5 estimated that sandwich attacks did not happen very often. Our interviewees' estimate for the number of attacks ranges from 500 to $50,000$ per day, and their estimate for the financial losses varies from 50 ETH to $10,000$ ETH per day. Most of their estimates are far from the real data.

P2 believes that the competition in conducting sandwich attacks is fierce. He also knows that attackers cooperate with miners to improve the success rate further and reduce the attack costs. Therefore, he concludes that sandwich attacks have become a serious threat in the market that cannot be ignored. *"In fact, I have no idea of the number of sandwich attacks that happen every day. I thought it might be serious. So I gave a high number." (P2)*

P3, on the other hand, believes that DEXes still represent a very low percentage of the market. The mainstream trading markets are still CEXes. Therefore, he predicts that sandwich attacks only affect the markets in a very limited way. *"I use CEXes more these days, whereas Uniswap was the past. I don't think it has a huge influence." (P3)*

These findings suggest that user perception of sandwich attacks is more about the concept but not the real impact of such threats to financial security. We summarize the user knowledge of sandwich attacks from three perspectives:

- Although there are many tools for DeFi traders to explore market information, non-professional users still have challenges to know the comprehensive information of their transactions, such as the position of a transaction in a block, or information about other transactions that may influence theirs. Therefore, they may not be aware of the impact a sandwich attack has on them.
- When the financial loss from a sandwich attack is not significant, traders do not care whether they are being attacked.
- DeFi users do not have a clear idea how serious the impact of the attacks is on the entire ecosystem.

# 7 ATTITUDES TOWARDS SANDWICH ATTACKS

Sandwich attacks have inevitably become part of the DeFi ecosystem, as the average number of attacks increases every day. Even though people call sandwich trades "attacks", attackers do not hack or destroy the blockchain systems. They use strategies respecting the rules of the market. On the other hand, sandwich attackers generate a profit by inflicting losses on traders. Their behavior may even result in systemic consensus-layer vulnerabilities [27]. Given the two-sided nature of sandwich attacks, we explore users' attitude towards these attacks in this section from the perspective of individual traders and the blockchain ecosystem, respectively.

## 7.1 Perspective of Individual Traders

As we introduced in Section 2, when attackers observe a pending transaction in the network, they can front-run it such that the victim receives the least amount of an asset possible. The revenue of attackers can be up to 80% of the victim's trading volume. Our interviewees have two different views on this mechanism. Some of them think attackers cause avoidable financial loss to the victim and therefore have a negative impact on them. Others believe that sandwich attackers still follow the trading rules of the DeFi market and should not be blamed.

*7.1.1 Malicious Behavior in DeFi Markets.* Some interviewees agree that sandwich attacks negatively impact traders. A5 believes that the slippage rate set by victims exists to enable trading in volatile market conditions and should not be exploited for attacks. Without any interference, the victims would get a better price. From this point of view, A5 agrees that sandwich attacks hurt traders in DeFi markets. *"They (attackers) earn a lot of money from us. If there are no sandwich attacks front-running these transactions, we won't* *lose money. ...These attackers turn uncertainty into certainty. My potential loss becomes a real loss." (A5)* Some other interviewees identified sandwich attacks as malicious towards traders. For instance, B5 compared sandwich attacks to other front-running behavior in traditional markets, which are always considered unethical or even illegal [32]. *"They are using information which has not been public to the market. They are front-running us. I cannot agree that front-running is a standard manipulation in markets. It is illegal!" (B5)*

*7.1.2 Serious Impact of DEXes Settings.* Moreover, A1 claims that the slippage rate is sometimes not set by users themselves, but is forced by the DEXes. For each trade, the DEX interface sets a lower bound for a slippage rate based on the current market price fluctuations. If a trader submits a trade with a slippage below that lower bound, the interface will reject the trader's request. Although the original intention of this setting was to increase the success rate of users' trades in dynamic markets, in A1's view, the combination of such a system setting and sandwich attackers causes serious financial losses for users. *"Sometimes they refuse my transaction if I set a low slippage rate. If I want to sell my tokens at that time, I have to set a high slippage rate, even 10%. It is not my fault, right? The markets and attackers stole my money together." (A1)*

*7.1.3 Behavior That Complies with Trading Rules.* In contrast, some of our interviewees do not believe that sandwich attacks have affected traders. Or in other words, they consider sandwich attackers to be normal traders. For instance, although B1 agrees that sandwich attacks are security issues in the DeFi ecosystems, she thinks that attackers just utilize the same authority issued to all DeFi participants: *"Sandwich attacks generate MEV*[1]*, which may cause instability at the system level. But these attackers, I do not consider them as attackers. They only use the common functions that are provided by the platform. Every entity follows the same rules defined by the code, so everyone is equal in the market. I don't think their actions are immoral to victim traders." (B1)* Similarly, P5 also does not think that anything is ethically wrong with sandwich attacks. P5 creates sandwich attacks on his own and believes that the DeFi platforms and the traders incentivize this trading behavior by making public offers at an acceptable price. *"Users supply a value that expresses the lowest price they're willing to accept. They broadcast this publicly. Sandwichers take the user's best public offer. There's nothing immoral about it." (P5)*

*7.1.4 Improvements on Traders' Security Perception.* Additionally, some interviewees believe that losing money is a valuable lesson in DeFi markets and blockchain ecosystems. P3 indicates that traders are motivated to learn more techniques to protect themselves after learning about an ecosystem's risks. Other than in traditional markets where the financial security of users is increased by the market makers or operators, in DeFi markets, traders mostly have to rely on themselves. Therefore, P3 thinks, it is important to improve traders' resistance to risk in such temporarily immature markets. Sandwich attack can be a wake-up call for users to take care of not only the safety of their assets but also the interactions with others in the market. *"Only when you lose money, will you learn what happens in the market. You will learn how to avoid losses. You have to learn in DeFi. Being attacked can motivate users to learn more and protect themselves the next time." (P3)*

Traders' attitude towards sandwich attacks from the perspective of individual traders can be summarized as follows:

- Some DeFi traders believe that sandwich attacks are unethical and harmful to individual traders because of the financial losses they incur, while others consider it common market arbitrage behavior.
- In addition to attackers, DEXes may also contribute to the increasing trend of sandwich attacks.
- Sandwich attacks can prompt users to understand DeFi markets better and the respective lessons could benefit them when trading in the future.

## 7.2 Perspective of the Blockchain Ecosystem

Previous studies [27, 47, 68] suggest that sandwich attacks have a negative impact on DeFi systems in two ways. First, sandwich attacks may introduce additional on-chain transactions. These transactions can take block space away from regular trades which leads to higher gas prices in the DeFi ecosystem [27, 68]. Secondly, the profit of sandwich attacks increase the miner extractable value (MEV) in blockchain systems [27] which can introduce systemic consensus-layer vulnerabilities, i.e., fee-based forking attacks and time-bandit attacks [27]. However, we find that traders have differing feelings about the impact on the blockchain system and DeFi platforms. On the one hand, they believe that the volume of sandwich attacks is so small that their impact on the system is minimal. On the other hand, they recognize that sandwich attacks increase the activity in DeFi markets and provide opportunities for more third-party services, improving the entire DeFi ecosystem.

*7.2.1 Influence on Gas Prices.* First, we find that compared to the potential impact of sandwich attacks on the system, traders care more about the real changes in the markets. A5, for instance, expressed that he only cares about the gas price he needs to pay. He does not care whether sandwich attacks take place or not. If the impact of sandwich attacks on the entire market is negligible, he will not change to other markets or platforms. *"If the gas price does not increase, I don't think we should care too much about the impact of sandwich attacks on Ethereum. If it only makes the gas price increases 1 GWei, then it can be ignored. I am not going to change to another DEX or platform because of this tiny change. The liquidity and the price are the most important things to me." (A5)*

Traders choose cryptocurrency markets based on the profits they can earn. Although sandwich attacks may cause a worse price and increase the gas fee, traders do not change their trading activities if other markets, such as CEXes, cannot provide better services than DEXes. Moreover, the market price is determined by the liquidity in the market. Sandwich attacks do not decrease the revenue of liquidity providers. Actually, the opposite is the case: As the number of sandwich attacks grows, liquidity provider earn more exchange fees. Therefore, the existence of sandwich attacks may not eliminate the users' preferences on DeFi markets. Meanwhile, sandwich attacks generally exist in any blockchain-based DeFi market. Currently, there is no published blockchain system

[1] Miner Extractable Value (MEV) is often used by miners to generate additional revenue on a block by re-ordering transactions in each block, in ways that are beneficial to them [27].

solution to eliminate sandwich attacks. Therefore, traders may not change the blockchain platform because of sandwich attacks.

*7.2.2 Contributions to the Community Development.* Another reason why traders do not believe that sandwich attacks have a negative impact on the platform is the emergence of more third-party services as a result. For instance, almost all interviewees complimented the tool that we built to prevent sandwich attacks. They assume that these community engagements can contribute to the development of DeFi markets. P2 thought that sharing such tools with the community can greatly help traders to make safe transactions. Additionally, other researchers can utilize it to improve the security level of DeFi markets. Therefore, sandwich attacks also motivate collaborative development among the DeFi community. *"I think that tool you guys made is particularly good. We can protect ourselves from sandwich attacks with these tools, like yours, or other third-party services like Flashbots. DeFi is still new. There are definitely a lot of imperfections. We cannot only rely on Ethereum or Uniswap themselves. So from this perspective, sandwich attacks motivate more people to develop the DeFi market and make it much better." (P2)*

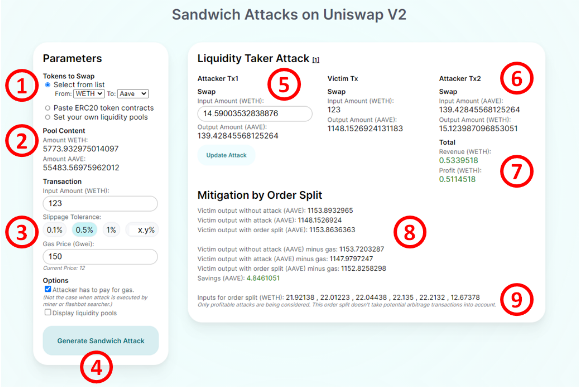
It is a challenge for individual traders to be familiar with all DeFi attacks and know defending strategies against them. Therefore, more and more developers may join the market to provide additional services to traders with a more secure trading environment. In particular, we observe that with the increasing trend of sandwich attacks, we and some other developers, such as sandwiched.wtf, have provided tools for traders to notice what happened in the market and to protect themselves. Because DeFi is decentralized, where no centralized operator takes responsibility for traders, markets only improve when safety hazards are exposed and addressed by the community.

Traders' attitudes towards sandwich attacks from the perspective of the blockchain ecosystem can be summarized as follows:

- Since the impact of sandwich attacks on the system is not tangible, traders do not perceive the negative impact of sandwich attacks on the blockchain ecosystem.
- Sandwich attacks have contributed to the security development of the community. Traders perceive that active community participation can increase the market's growth potential.

# 8 MITIGATION OF SANDWICH ATTACKS

Although sandwich attackers can utilize the transparency and the transaction ordering mechanism to take profit from other traders, there are still many mitigation strategies for traders to protect themselves from being attacked. In this section, we explore the mitigation of sandwich attacks. We first introduce two mechanisms for preventing sandwich attacks and a mitigation tool developed by the researchers. Then, we report the user perception of different strategies to mitigate sandwich attacks. Finally, we summarize the design implication on mitigation tools for sandwich attacks, e.g., which information users want to receive and what functionality they want the tool to provide.



Sandwich Attacks on Uniswap V2

Parameters

Tokens to Swap
● Select from list
From: WETH To: Aave
○ Paste ERC20 token contracts
○ Set your own liquidity pools

Pool Content
Amount WETH:
5773.932975014097
Amount AAVE:
55483.56975962012

Transaction
Input Amount (WETH):
123
Slippage Tolerance:
0.1% 0.5% 1% x.y%
Gas Price (Gwei):
150
*Current Price: 12*

Options
☑ Attacker has to pay for gas.
*(Not the case when attack is executed by miner or flashbot searcher.)*
□ Display liquidity pools

Liquidity Taker Attack [1]

Attacker Tx1
Swap
Input Amount (WETH):
14.5900353283887 6
Output Amount (AAVE):
139.42845568125264

Victim Tx
Swap
Input Amount (WETH):
123
Output Amount (AAVE):
1148.1526924131183

Attacker Tx2
Swap
Input Amount (AAVE):
139.42845568125264
Output Amount (WETH):
15.123987096853051

Total
Revenue (WETH):
0.5339518
Profit (WETH):
0.5114518

Mitigation by Order Split

Victim output without attack (AAVE): 1153.8932965
Victim output with attack (AAVE): 1148.1526924
Victim output with order split (AAVE): 1153.8636363

Victim output without attack (AAVE) minus gas: 1153.7203287
Victim output with attack (AAVE) minus gas: 1147.9797247
Victim output with order split (AAVE) minus gas: 1152.8258298
Savings (AAVE): 4.8461051

Inputs for order split (WETH): 21.92138 , 22.01223 , 22.04438 , 22.135 , 22.2132 , 12.67378
*Only profitable attacks are being considered. This order split doesn't take potential arbitrage transactions into account.*

**Figure 6: Screenshot of the Mitigation Tool. (1) Users can choose the liquidity pool that they would like to trade with or input the details of the liquidity manually. (2) The reserves of cryptocurrencies in the liquidity pool. (3) Settings of the transaction, including the input amount, slippage tolerance, and gas price. (4) Generate potential sandwich attacks. (5) The information of the front-run. Users can adjust the input amount of the front-run transaction. (6) The information of the corresponding back-run transaction. (7) The revenue and profit for sandwich attackers generated by attacking the victim transaction. (8) The changes to the output amount of the victim achieved by implementing the mitigation strategy. (9) The detailed mitigation strategy of order splitting.**

## 8.1 Mitigation Tools and Strategies

Based on the mechanism, we classify the mitigation strategies into two categories: making the transactions not profitable for sandwich attackers, and making the transactions not observable to attackers.

The first approach to prevent sandwich attacks is to create transactions, such that they cannot be profitably attacked. For instance, traders may consciously set a low slippage rate or split their transactions with large input amounts into a series of smaller transactions. In the supplementary material, we show that there is an upper bound of the profit attackers can generate from a victim transaction. If the upper bound of the profit is negative, or smaller than the gas fees that attackers have to pay, the transaction will not be attacked.

The second approach to prevent sandwich attacks is to hide transactions until they are published in mined blocks. For instance, some relay services (cf. Section 4.2), such as Flashbots [9], provide private communication channels between traders and miners, which allow traders to submit transactions without publicly broadcasting them in the blockchain P2P network. In such scenarios, attackers cannot observe victim transactions before their execution and are thus unable to conduct attacks.

As we mentioned in Section 5.4, we built a mitigation tool to prevent sandwich attacks.[2] Our tool utilizes the first mitigation mechanism: It provides suggestions to traders on how to choose the volume and slippage rate of their transactions, such that attackers cannot generate any profit by attacking them. Users can choose the assets to be swapped from a predefined list or insert smart contract addresses of any ERC-20 tokens. If the respective trading pair exists on Uniswap, the contents of the liquidity pools are displayed. Users can also specify their own token pools; a functionality that allows for experimentation independent of the current Ethereum state. For their transaction, users need to specify the desired input amount, the slippage tolerance, and the gas price. The tool generates a potential sandwich attack and shows the losses of the trader. If a profitable sandwich attack is possible, we suggest users to split their transaction into several orders to prevent sandwich attacks (the algorithm is described in the supplementary material). We show the specific order splitting strategy and the respective savings on the website.

## 8.2 User Perception on Mitigation Strategies

*8.2.1 Setting Parameters of Transactions.* Although users may not know the optimal trading parameters to prevent sandwich attacks, some of them have already adopted the first mitigation strategy, i.e., setting a low slippage rate or a low trading volume. For instance, B5 stated that he fine-tuned slippage settings when trading on the public blockchain system. Similarly, after noticing the existence of sandwich attacks, A1 did not just follow the suggestions of the DEXes website to set the slippage rate of a transaction: *"Now I pay attention to the slippage rate. If the price fluctuates, I will wait until it becomes stable." (A1)*

Moreover, we find that many users did not have a solid rationale to set the trading parameters. For instance, P1 did not know whether his transaction might be attacked with the slippage rate he set: *"I did not compute whether my transaction will be sandwich attacked or not like the tool does. I just set a reasonably small slippage rate. Or, when I want to trade a lot in the market, I submit transactions slowly in different blocks." (P1)* However, according to the statistics shown in Figure 5, transactions with slippage rates lower than 0.5 can still be attacked. Therefore, setting transaction parameters according to personal judgment may not fully guarantee the security of a transaction.

*8.2.2 Submitting Transaction Through Private Channels.* Compared to the first mitigation strategy, we find fewer traders using the second mitigation strategy for their daily trades.

The first reason traders may not use these services is the incompatibility of DEXes and private channels. Compared to submitting transactions through the web interfaces of DEXes (cf. Figure 7), making transactions through private channels requires traders to have some advanced technical skills. These relay services do not provide an interface. Users have to call the smart contract functions directly on the blockchain without using third-party trading tools, which requires them to have a deeper knowledge of DEXes smart contracts. Not only average DeFi users but also some DeFi insider users mention that they lack such technical skills. *"I have not tried Flashobots. I cannot figure out how to use it. I do not make transactions in that way (calling smart contract functions). It seems like something for a professional blockchain developer who trades a lot everyday." (P3)*

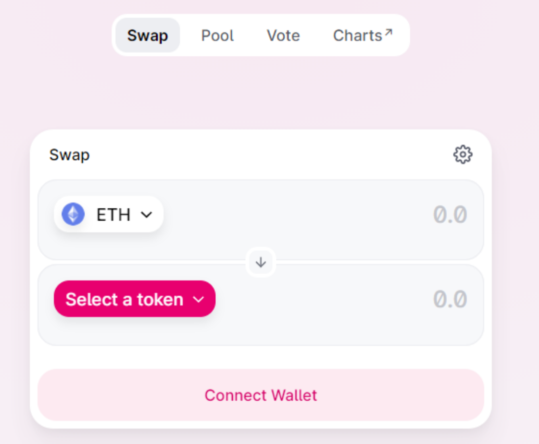


**Figure 7: The interface of Uniswap V3. Users only need to connect their cryptocurrency wallet to the application and can then easily conduct transactions on the website.**

The second reason traders prefer not to use the relay services is the dominance of a centralized party in the distributed blockchain system. For instance, Flashbots has collaborated with more than 80% of miners in Ethereum by April 2021 [10]. P4 expresses worries about the current scenario because P4 thinks that such relay services introduce too much centralization into DeFi markets. Since traders and miners can only exchange information through the relay, the relay service has absolute dominance in the DeFi market. They may reorder, manipulate, and cancel transactions to increase their own profit. Moreover, their operations are not transparent and not supervised by any other market participants. The public information cannot even prove whether they are operating selfishly or not. Based on such potential risks and security concerns, some interviewees have decided to abandon the use of third-party relay services. *"It totally changes the ecosystem. It is not decentralized anymore if we use Flashbots. They can manipulate my transaction if I send it to them but do not broadcast it in the network." (P4)*

We summarize the defense strategies of traders in three points:

- Traders are careful in setting trading parameters if they notice sandwich attacks.
- Technical difficulties may discourage traders from using relay services to prevent attackers front-running their transactions.
- It is more acceptable for traders to control their trading volume and slippage rate than to use centralized relay services in response to sandwich attacks because of security concerns.

[2] The tool is built with Javascript and HTML/CSS. The backend is implemented using Express.js and mainly serves as a gateway to the Ethereum network. The respective connection is established by using the web3.js and Infura APIs.

## 8.3 Design Implication for Mitigation Tools

Based on user feedback on the tool that we developed, we summarize four design implications for mitigation tools.

*8.3.1 Improving Awareness.* The first implication is that a tool needs to improve the awareness of sandwich attacks. Our interviewees expect DeFi applications, such as DEXes and cryptocurrency wallets, to inform them about the risk of sandwich attacks when making trades. For instance, A3 indicates that if the DEXes they use every day could inform them of such trading risks earlier, they would be able to realize the severity of the problem sooner and adjust their trading accordingly. *"I would like to be alerted directly on the Uniswap website when I am trading. If I know I might be attacked by a sandwicher, I can decide for myself if I want to lower the slippage." (A3)*

Similarly, P1 suggested that we should highlight the computation results, which is the thing he is most concerned about. *"You could display simple easy to understand effect and mitigation on top, nitty gritty below, and in big colorful text show me SAFE or VULNERABLE." (P1)*

*8.3.2 Detecting Real-Time Attacks.* The second implication is that it should defend against sandwich attacks in real-time. Because the attack transactions are not executed immediately in the blockchain, it is possible for victim traders to change their transactions when noticing that they are under attack. B3, for instance, told us that he had read some news that some DeFi traders created their own ERC-20 tokens and submitted fake transactions to attract sandwich attackers to attack them. However, their ERC-20 tokens have a special setting such that attackers cannot back-run to sell the token for profit. Therefore, these attackers lose money because they only bought the fake tokens in the front-run transaction. B3 expects similar tools could be implemented to protect traders in real-time.

P1 stated a similar idea that the mitigation tool could detect potential attacks in the blockchain network. Once the attacker's presence is detected, they can modify their transaction so that the attacker cannot profit from them, for example, by increasing the gas fee or canceling the transaction. *"It would be great to plug in mempool data and detect recent attacks or possible attacks live on Uniswap." (P1)*

*8.3.3 Automated Trading.* The third implication is to optimize the trading process of the mitigation tool. A2 tried to submit small trades to prevent sandwich attacks. However, she perceived such mitigation strategies are not user-friendly as she has to submit several transactions repeatedly on the DEXes. Therefore, A2 suggested to further develop our tool into a real product: *"I think it's a nice tool, but it should be a product. Turn it into a product that I can use to send my transactions to the chain!" (A2)* Although our tool provides a detailed mitigation strategy to users, they still have to conduct transactions themselves on the exchanges. P4 considered the tool useless until it turns into a browser extension or is included in official DEX interfaces.

On the other hand, using private channels for submitting transactions has certain technical requirements for users. If traders want to use a third-party relay service to send private transactions on DeFi markets, they must understand how to conduct transactions by calling smart contract functions. Therefore, traders expect that the threshold for using these defense strategies are lowered. For instance, A5 wants to submit Flashbots transactions directly in the interface of Uniswap. *"It would be nice if they could provide a selection of whether the transactions are submitted to the Ethereum mempool or to Flashbots." (A5)*

*8.3.4 Supporting Various DEXes.* The last implication is to support different DeFi markets. Some users worry that the mitigation tool may not help them to handle updated challenges. For example, the current version of our tool is only designed for DEXes using the constant product pricing mechanism, such as Uniswap V2 and Sushiswap, which hold a major share of the market. However, some tools may not provide a similar function for other emerging markets, such as Uniswap V3. Therefore, interviewees expected that the mitigation tools are adapted to the developments of DeFi markets. For instance, A4 told us that he also trades on other exchanges, such as Uniswap V3, Balancer, and 1inch. So he also wants to be able to guarantee the security of his transactions on other exchanges. *"Pretty cool, but will it support V3? It would also be good to see what attacks would look like on different DEXes, like Balancer, 1inch." (A4)*

# 9 DISCUSSION

Our research explored the impact of sandwich attacks in the DeFi markets as well as users' perception of the emerging security issue. In this section, we first discuss the roots of sandwich attacks and the rationale for this market behavior. Then, we provide a user-centric synthesis of security challenges in DeFi markets. Finally, we discuss how these challenges lead to general implications for different stakeholders in the blockchain ecosystem.

## 9.1 Unregulated Market Behavior in DeFi Markets

The main cause of sandwich attacks is that some transactions, which have not been executed in the market, were disclosed to other market participants, some of whom can utilize the leaked information to make profit for themselves. DeFi users have different levels of access to the information in the system because of their knowledge and technical capabilities. In this subsection, we discuss one philosophical question, i.e., are sandwich attacks malicious or just a limitation of transparent monetary transactions?

*Information Leakage in DeFi Markets.* We start by discussing the transmission of information in the public P2P network. In the most popular blockchain systems, such as Ethereum and Binance Smart Chain, there are two kinds of information transmitted through the P2P network: transactions and blocks. However, according to the definition of a blockchain, a distributed database maintained by nodes over a P2P network [42], only the block information is necessary to be transmitted through the P2P network for maintaining a valid blockchain system. In other words, blockchain systems do not necessarily ensure transparency of transaction information. In particular, some protocols have been proposed which ensure that trading information will not be available to other market participants before the execution of a transaction [36, 54]. From this perspective, we may infer that some developers of the DeFi community may not perceive sandwich attacks and other front-running operations as normal market behaviors which are acceptable in DeFi markets.

*Decentralized Autonomous Organizations.* Compared to traditional financial markets where centralized market operators and government regulators may set rules to identify malicious market operations, DeFi markets are developed on decentralized systems, where no such regulators exist. The threshold to determine a market operation as malicious might be higher in distributed systems managed by decentralized autonomous organizations. Only few market attacks have been resolved by the DeFi community [24, 55]. Therefore, we may infer that market participants have more freedom to access and exploit information in DeFi markets than traditional financial markets.

*Various Attitudes to Sandwich Attacks.* Based on our findings on users' attitudes towards sandwich attacks, it is hard to determine whether sandwich attacks should be considered malicious or normal market behaviors. Because users have different backgrounds, knowledge, experiences, and motivations, they thus have different perceptions of sandwich attacks. The blockchain systems provide fair markets for all DeFi users to either exploit profitable opportunities or protect themselves. Our quantitative findings show that the impact and the implementation of sandwich attacks have evolved with the development of DeFi markets, suggesting that the answer to the philosophical question also varies over time.

## 9.2 Security Challenges for DeFi Users

Our work illustrates the seriousness of security issues in DeFi markets and how they are disregarded by users. In particular, DeFi markets do not always work according to traders' expectation. For instance, while slippage rates were originally meant to allow for trades during volatile market conditions, they have enabled a surge of sandwich attacks. Moreover, sandwich attacks are not the only noteworthy security issue in decentralized finance. In this subsection, we explore three significant factors from users' perspective which may cause security challenges: information asymmetries, dependence on web applications, and collaboration between stakeholders.

### 9.2.1 *Information Asymmetries.*

One of the important characters of public permissionless blockchain systems is that all information is accessible to all users, including the system protocol, market mechanism, and trading information. Ideally, no market participants should benefit from information asymmetries because of the transparency of DeFi markets. However, our findings suggest that many users still have limited knowledge to acquire and utilize market information, which makes them susceptible to being attacked. We discuss two information asymmetries: on-chain information and off-chain information.

The first information asymmetry concerns pending transactions. Whoever has access to these transactions gains an informational advantage and is able to adjust their own behavior accordingly. Although the information about pending transactions is public in the P2P network, many users still struggle to learn about pending transactions in real-time, unless they run their own node or pay for a respective service. This might not be feasible for many DeFi users with a limited budget. From a user perspective, asymmetries of on-chain information might contribute to a growing sense of mistrust towards blockchain systems and the technology in general. Their trading security cannot be ensured because other users may utilize their informational advantage to generate a profit. Therefore, it is important to either prevent informational disadvantages or instead make the respective information easily available for everybody.

The second information asymmetry concerns the knowledge of security issues. Our findings demonstrate that users have a different degree of awareness of sandwich attacks, which may result in different strategies to prevent financial losses. DeFi markets involve a lot of applications and protocols. Therefore, it is hard for individuals to observe all potential security issues. This is especially severe, as there is no support by governmental regulations for users, as we know it from traditional finance. However, users in DeFi markets who benefit from security risks are typically not eager to share their strategies, as growing awareness or competition both lead to a decrease in profits. With the advent of DeFi and its ambition to also attract non-technical users, the information asymmetry has become even more fundamental. It forces users to educate themselves and to stay up to date about the current market situation.

### 9.2.2 *Dependence on DeFi Applications.*

With the development of the blockchain ecosystem, users do not have to broadcast transactions in the P2P network by themselves. On the contrary, many DeFi applications provide web services for users who do not have a sophisticated knowledge of blockchain technology to perform market operations. They have the aspiration of partially replacing traditional financial services. Our findings show that many users trade DEXes without properly understanding the way they operate. DEXes also provide little guidance on the price risks associated with using them. In the case of sandwich attacks, traders either trust the slippage rate recommended by the exchange or choose a fairly high rate to guarantee the successful execution of their transaction. They are usually not aware that the choice of a higher slippage tolerance can actually lead to a worse price and an unexpected financial loss.

While in traditional finance, legal entities ensure that users understand the implications of their actions - and that financial services hold what they promise -, this is not the case for decentralized services. Without a clear legal framework, it is an enormous challenge for DeFi application developers to walk the fine line between making an application user-friendly enough for the general public to use, and protecting their interests by informing them about the inner workings of a product. Moreover, some parts of DeFi applications are not built on blockchain system, such as their website. Users cannot fully understand and control what happens between submitting a trading request on the website and issuing a transaction in the P2P blockchain network. This can result in serious hacking events [39]. Therefore, when users fully depend on financial applications and utilize given protocols without properly understanding their inner workings, their trading in the market may be at potential risk.

*9.2.3 Collaboration Between Stakeholders.* Another security challenge for users is that some stakeholders have collaborations to exploit revenue from DeFi markets. For instance, miners can accept transactions from relay services, such as Flashbots, and prioritize these transactions in the mined block. Most of miners without collaboration with other parties order transactions according to their gas price [50]. However, the collaborations with centralized relay services change the execution order of transactions in blocks, which results in severe miner extractable value (MEV) [47]. Attackers paid almost no gas fees to miners, while these transactions have been executed at the top of the blocks. As the number of sandwich attacks executed in collaboration with miners is rapidly increasing, we can assume that the profit generated through DeFi attacks will always be shared with miners in the long run. In such a scenario, relay services could represent a central point in a supposedly decentralized network. This would even enable them to treat transactions differently depending on the address they were sent from or the smart contract they call. The continuous collaboration between different actors not only increases the complexity of the system but also decreases the cost of attacks. It hence becomes even more difficult for users to understand or effectively prevent attacks in DeFi markets

## 9.3 Implications

Our research has clear implications for the design of blockchain systems as a whole, the attack-relevant DeFi applications, as well as third-party service providers. We want to give an overview of the respective design considerations for these three levels of applications.

*9.3.1 Improving User Awareness by Educating Them.* During our workshop and our qualitative interviews, it has become obvious that many non-professional users only have limited knowledge about how blockchain systems operate. As we have covered in previous sections, this limited understanding makes sandwich attacks and other security issues in DeFi possible in the first place. Blockchain systems can take two approaches to protect users from such threats. First, the system can be engineered in a way such that the possibilities for exploits are minimal. This is, however, very difficult for dynamic, evolving systems like Ethereum, and makes it almost impossible to support such a wide variety of use cases. A better approach is to create a community where users are properly educated, security issues are discussed, and potential solutions can be independently implemented. In the instance of sandwich attacks, we observed that the Ethereum community did not only acknowledge the underlying issues but also supported research to find solutions. Additionally, the Ethereum platform is designed in a way which enables developers to easily create competing DeFi services and third party tools. This allows for a quick response to the security issue at hand and the development of valid mitigation strategies, at least for technical users. In the case of sandwich attacks, we saw several new DeFi services and third party tools emerge to help users protect themselves from attacks.

*9.3.2 Providing Direct Protection Against Security Challenges by DeFi Applications.* Compared to traditional finance, DeFi services are burdened with relatively little legal regulation. In order to build a successful business, they should, however, still strive to offer the best possible user experience. This also includes protecting users from potential security issues and informing them about the risks associated with using their service, even if they are not obligated to do so. In regards to sandwich attacks, a DEX called 1inch, for example, introduced private transactions to prevent customers from front-running attacks. Other than that, we have seen very limited reactions by DEX operators to protect users from the growing threat of sandwich attacks. We found this surprising, as additional mitigation mechanisms could directly benefit the users and are not too difficult to implement, as the emergence of third party tools illustrates. If DeFi services fail to take on this responsibility, it not only hurts the trust of their user base but might also strengthen their competition. Ever since sandwich attacks have become a topic of discussion in the Ethereum community, various new models for decentralized exchanges have emerged. Many of them try to mitigate the presented security issues by sharing profits generated through front-running with individual traders. If the impact of sandwich attacks continues to grow, they might become a viable alternative to the current leading exchanges.

*9.3.3 Encouraging Community to Develop Third-Party Tools.* Independent tools and services have always played an important role in blockchain systems. There were also several applications released to mitigate the impact of sandwich attacks. This includes our own tool which tells users whether their transaction is susceptible to an attack and suggests an ideal order split. Such tools can play an important role to increase the user awareness of a security issue and decrease its impact. In general, third party tools are most useful when they integrate seamlessly with other DeFi services. This is one way how our own web interface could be improved. Third party tools can bring great value to the community until the underlying issue is resolved either on the level of the DeFi service or of the blockchain system. They can even serve as an inspiration for future research or demonstrate how an issue could be resolved. We hope that with our own tool we were able to contribute to these developments.

*9.3.4 Trade-off Between Resisting And Being Attacked.* We have discussed three implications to eliminate the influence of security issues in DeFi markets. However, it is not clear whether investing resources to address security challenges, such as sandwich attacks, is sensible. In particular, as an individual user, it takes more effort to prevent attacks if the community is not able to provide enough help, such as providing trading tools without being attacked. Our qualitative findings show that some users did not invest their time to apply mitigation strategies to prevent sandwich attacks because they perceived that their financial loss might not be significant. Moreover, current mitigation strategies have some limitations. For instance, not all miners collaborate with centralized relay services, so if traders submit transactions through the private channel, their transactions might not be minded in the next block. This mitigation strategy is not suitable for traders who need immediate transaction execution. Therefore, from an individual perspective, it might not always be a sensible thing to prevent being attacked, while users should consider the trade-off between the potential loss and the resources investing.

However, from the community perspective, we might not directly compare the cost of developing the community awareness, such as user education and application development. Compared to the self-protection of individual users, the effort of the community could benefit a larger number of users. Improving users' technical skills and knowledge may not only improve their abilities to prevent a certain security challenge but also consequently increase the whole community to respond more efficiently to other security challenges.

## 10 CONCLUSION

In this paper, we demonstrate a ground truth of the impact of sandwich attacks. The number and the probability of attacks have been growing massively until the end of April 2021. We also examine the perception of sandwich attacks among users and reveal the gap between user perception and the real-world impact. Our work provides a preliminary understanding of the security perception of DeFi users and insights for the development of the blockchain ecosystem.

## REFERENCES

[1] 2020. Akropolis Incident: Root Cause Analysis. https://blog.peckshield.com/2020/11/13/akropolis/.

[2] 2020. Origin Dollar Incident: Root Cause Analysis. https://blog.peckshield.com/2020/11/17/ousd/.

[3] 2020. Uniswap/Lendf.Me Hacks: Root Cause and Loss Analysis. https://blog.peckshield.com/2020/04/19/erc777/.

[4] 2021. 5/8/2021: Rari Capital Ethereum Pool — Post-Mortem. https://medium.com/rari-capital/5-8-2021-rari-ethereum-pool-post-mortem-60aab6a6f8f9.

[5] 2021. (5/8/21) Rari Capital Exploit Timeline & Analysis. https://nipunp.medium.com/5-8-21-rari-capital-exploit-timeline-analysis-8beda31cbc1a.

[6] 2021. Alpha Homora V2. Available at: https://alphafinancelab.gitbook.io/alpha-homora-v2/.

[7] 2021. Binance Smart Chain DeFi project BurgerSwap hacked for $7 million. https://cryptoslate.com/binance-smart-chain-defi-project-burgerswap-hacked-for-7-million/.

[8] 2021. Burgerswap attack analysis. https://hiram.wang/burgerswap-attack-analysis/.

[9] 2021. Flashbots. https://medium.com/@danrobinson/ethereum-is-a-dark-forest-ecc5f0505dfff [Accessed May 25, 2021].

[10] 2021. Flashbots Transparency Report — April 2021. https://medium.com/flashbots/flashbots-transparency-report-april-2021-9fef4d8dde07

[11] 2021. The Furucombo Incident Analysis: Cascading Trust. https://blog.peckshield.com/2021/02/27/Furucombo/.

[12] 2021. Gross Value Locked (USD). https://debank.com/ranking/locked_value.

[13] 2021. PeckShield Brief Analysis of BurgerSwap Lightning Loan Attack. https://blockcast.cc/news/peckshield-brief-analysis-of-burgerswap-lightning-loan-attack-the-logic-behind-the-defi-protocol-is-more-important-than-the-code/.

[14] 2021. Rekt - Force - REKT. https://www.rekt.news/force-rekt/.

[15] 2021. Rekt - Furucombo - REKT. https://www.rekt.news/furucombo-rekt/.

[16] 2021. SushiSwap. Available at: https://https://sushi.com/.

[17] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–19.

[18] Hayden Adams, Noah Zinsmeister, and Dan Robinson. 2020. Uniswap v2 Core. Available at: https://uniswap. org/whitepaper.pdf.

[19] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. 2021. Uniswap v3 Core Whitepaper.

[20] Guillermo Angeris, Alex Evans, and Tarun Chitra. 2021. A Note on Bundle Profit Maximization. (2021).

[21] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch-Lafuente. 2021. Maximizing Extractable Value from Automated Market Makers. *arXiv preprint arXiv:2106.01870* (2021).

[22] George Bissias and Brian Neil Levine. 2020. Bobtail: Improved Blockchain Security with Low-Variance Mining.. In *NDSS*.

[23] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development.* sage.

[24] Ryan Browne. 2021. Hacker behind $600 million crypto heist returns final slice of stolen funds. Available at: https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html.

[25] Vitalik Buterin et al. 2014. A next-generation smart contract and decentralized application platform. *white paper* 3, 37 (2014).

[26] Weili Chen, Tuo Zhang, Zhiguang Chen, Zibin Zheng, and Yutong Lu. 2020. Traveling the token world: A graph analysis of ethereum erc20 token ecosystem. In *Proceedings of The Web Conference 2020*. 1411–1421.

[27] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 910–927.

[28] Christof Ferreira Torres, Ramiro Camino, et al. 2021. Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain. In *USENIX Security Symposium, Virtual 11-13 August 2021*.

[29] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. Don't lose your coin! Investigating Security Practices of Cryptocurrency Users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. 1751–1763.

[30] Xianyi Gao, Gradeigh D Clark, and Janne Lindqvist. 2016. Of two minds, multiple addresses, and one ledger: characterizing opinions, knowledge, and perceptions of Bitcoin across users and non-users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 1656–1668.

[31] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 3–16.

[32] Larry Harris. 2003. *Trading and exchanges: Market microstructure for practitioners*. OUP USA.

[33] Campbell R Harvey, Ashwin Ramachandran, and Joey Santoro. 2021. *DeFi and the Future of Finance*. John Wiley & Sons.

[34] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. 2015. Eclipse attacks on bitcoin's peer-to-peer network. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*. 129–144.

[35] Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramer, Giulia Fanti, and Ari Juels. 2021. SquirRL: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning. In *NDSS*.

[36] Mahimna Kelkar, Fan Zhang, Steven Goldfeder, and Ari Juels. 2020. Order-fairness for byzantine consensus. In *Annual International Cryptology Conference*. Springer, 451–480.

[37] Irni Eliana Khairuddin and Corina Sas. 2019. An Exploration of Bitcoin mining practices: Miners' trust challenges and motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[38] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring motivations for bitcoin technology usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 2872–2878.

[39] Richard Lawler. 2021. Someone stole $120 million in crypto by hacking a DeFi website. Available at: https://www.theverge.com/2021/12/2/22814849/badgerdao-defi-120-million-hack-bitcoin-ethereum.

[40] Robert Leshner and Geoffrey Hayes. 2019. Compound Finance Whitepaper.

[41] Bowen Liu, Pawel Szalachowski, and Jianying Zhou. 2020. A first look into defi oracles. *arXiv preprint arXiv:2005.04377* (2020).

[42] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.

[43] Daniel Perez and Ben Livshits. 2021. Smart contract vulnerabilities: Vulnerable does not imply exploited. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*.

[44] Anton Permenev, Dimitar Dimitrov, Petar Tsankov, Dana Drachsler-Cohen, and Martin Vechev. 2020. Verx: Safety verification of smart contracts. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1661–1677.

[45] Chris Piatt, Jeffrey Quesnelle, and Caleb Sheridan. 2021. Eden Network. (2021).

[46] Kaihua Qin, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti, and Arthur Gervais. 2021. CeFi vs. DeFi–Comparing Centralized to Decentralized Finance. *arXiv preprint arXiv:2106.08157* (2021).

[47] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2021. Quantifying Blockchain Extractable Value: How dark is the forest? *arXiv preprint arXiv:2101.05511* (2021).

[48] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. In *International Conference on Financial Cryptography and Data Security*. Springer.

[49] Michael Rodler, Wenting Li, Ghassan O Karame, and Lucas Davi. 2021. EVMPatch: timely and automated patching of ethereum smart contracts. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*.

[50] Tim Roughgarden. 2021. Transaction Fee Mechanism Design. In *Proceedings of the 22nd ACM Conference on Economics and Computation*. 792.

[51] Corina Sas and Irni Eliana Khairuddin. 2017. Design for trust: An exploration of the challenges and opportunities of bitcoin users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6499–6510.

[52] Fabian Schär. 2021. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review* (2021).

[53] Clara Schneidewind, Ilya Grishchenko, Markus Scherer, and Matteo Maffei. 2020. ethor: Practical and provably sound static analysis of ethereum smart contracts. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 621–640.

[54] Yaakov Sokolik and Ori Rottenstreich. 2020. Age-aware Fairness in Blockchain Transaction Ordering. In *2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)*. IEEE, 1–9.

[55] Cryptopedia Staff. 2021. What Was The DAO? Available at: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao.

[56] Liya Su, Xinyue Shen, Xiangyu Du, Xiaojing Liao, XiaoFeng Wang, Luyi Xing, and Baoxu Liu. 2021. Evil Under the Sun: Understanding and Discovering Attacks on Ethereum Decentralized Applications. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*.

[57] Nick Szabo. 1996. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16)* 18, 2 (1996).

[58] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. Surviving the cryptojungle: Perception and management of risk among North American cryptocurrency (non) users. In *International Conference on Financial Cryptography and Data Security*. Springer, 595–614.

[59] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin Beznosov. 2021. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[60] Ye Wang, Yan Chen, Shuiguang Deng, and Roger Wattenhofer. 2021. Cyclic Arbitrage in Decentralized Exchange Markets. *Available at SSRN 3834535* (2021).

[61] Sam M Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J Knottenbelt. 2021. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778* (2021).

[62] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 2014 (2014), 1–32.

[63] Siwei Wu, Dabao Wang, Jianting He, Yajin Zhou, Lei Wu, Xingliang Yuan, Qinming He, and Kui Ren. 2021. DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications. *arXiv preprint arXiv:2104.15068* (2021).

[64] Yaxing Yao, Yun Huang, and Yang Wang. 2019. Unpacking People's Understandings of Bluetooth Beacon Systems-A Location-Based IoT Technology. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

[65] Akif Yüksel. 2021. Mitigating sandwich attacks in Kyber DMM. (2021).

[66] Ren Zhang and Bart Preneel. 2019. Lay down the common metrics: Evaluating proof-of-work consensus protocols' security. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 175–192.

[67] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. 2021. On the just-in-time discovery of profit-generating transactions in defi protocols. *arXiv preprint arXiv:2103.02228* (2021).

[68] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Arthur Gervais, et al. 2021. High-Frequency Trading on Decentralized On-Chain Exchanges. In *IEEE Symposium on Security and Privacy, 23-27 May 2021*.

[69] Liyi Zhou, Kaihua Qin, and Arthur Gervais. 2021. A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. *arXiv preprint arXiv:2106.07371* (2021).