# Ethical Concerns in Blockchain Security Research

Shivali Halabe, Jack Nash
*Cornell University*

## Abstract

As a novel field, blockchain security offers many opportunities for researchers to discover and report vulnerabilities which put user information and money at risk. However, several researchers in this area employ methods that may be unethical: deanonymizing wallet addresses of non-consenting users, optimizing lucrative attack strategies in unregulated areas without proposing mitigation, and conducting unauthorized or unlawful attacks. In this paper, we evaluate the aforementioned research techniques in terms of their alignment with fundamental ethical principles and suggest avenues for blockchain security researchers to limit harm.

## 1 Introduction

In the last decade, as the popularity of cryptocurrency, decentralized finance, and general blockchain technology has grown, blockchain security has become an important field in the broader scope of security and privacy research. How anonymous are these services, and how can users maintain privacy in the face of adversarial actions? How secure are these networks, and what vulnerabilities could attackers potentially exploit? What laws and regulations govern these systems, and how can we ensure that users are protected?

The importance of such concerns explains the recent increase in quantity and quality of blockchain security research. But, while security researchers generally keep the public's welfare and interest in mind, forms of investigating these technologies often have unintended consequences which harm users and aid malicious actors. In seeking to discover and highlight vulnerabilities that exist within blockchains, researchers have displayed a lack of respect for user information or exchange policies, exposed new and improved forms of attack for adversaries, failed to provide adequate protections against uncovered weaknesses, and avoided taking accountability for potential negative effects of their research.

With the goal of elevating blockchain security research to a point where it provides the expertise and insight to answer vital questions about new technology without causing harm, we review nine papers through an ethical lens. We consider the techniques employed in these papers and how they either promote or safeguard against more adversarial activity. We make recommendations on how papers that fall short of ethical guidelines can improve in regards to user safety and general societal benefit. The intent of this paper is to help clarify how blockchain security research can be conducted and published in an ethically defensible manner in order to truly reap the benefits of cutting-edge investigations.

## 2 Related Works

Research ethics are of great importance in computer science fields, given the ability to perform large scale experiments digitally. In 2012, the Menlo Report [7] was published by the Department of Homeland Security with the goal of establishing standardized ethical principles for computer science researchers. It describes four assessment principles:

1. Respect for persons - voluntary, informed, and consenting participation
2. Beneficence - no harm done
3. Justice - fair and equal treatment
4. Respect for law and public interest - transparency and legal due diligence

There also exist ethics frameworks such as [3] that are more targeted towards security research. Schrittwieser et al. proposed four lines that a researcher should not cross: do not harm humans actively, do not watch bad things happen, do not perform illegal activities to harm illegal activities, and do not conduct undercover research. We found the Menlo Report to support a more nuanced and generally applied view of ethics in research and thus made extensive use of it in our review.

Additionally, we highlighted some security research ethics reviews that are influential in the structure and methodology of this paper. In [2], Chiauzzi et al. performed a case study on ethical and terms of use violations in the online patient community. In [3], Dittrich evaluated ethics in social honeypots and leans heavily on the guidelines of the Menlo Report. More specific to blockchains, Tang et al. theoretically examined the ethical issues likely to surface during research on blockchains [15]. Finally, Hyrynsalmi et al. conducted a review of papers about blockchain ethics [6]. They found that attention to ethics historically has been low but is now rising, although proposed ethics models like [15] have not yet been put into use. We aimed to add to the growing pool of literature on blockchain ethics and to identify papers that have room for improvement, as well as papers that exemplify thoughtful research and can serve as models for the future.

## 3 Methodology

We selected papers that utilized questionable methods by reviewing research on blockchain security from recent IEEE Security and Privacy Symposiums. We also examined other works by the same authors, as there are few researchers currently at the forefront of blockchain security. We then sought out research which conducted similar experiments to and addressed all the ethical concerns presented in the initial papers.

To evaluate nine total research papers in a standardized and fair manner, we divided the papers into three categories: Deanonymization, Optimized Attack Strategies, and Real-Time and Simulated Attacks. Based on the research techniques used, stakeholders involved, and potential for harm within a category, we associated each set of three papers with a fundamental ethical principle of security research as described in the Menlo Report [7]. In the context of a category's respective principle, we identified one paper which had clear ethical issues, one paper which had less potential for harm but still possessed significant areas of improvement in ethics, and one paper which clearly abode by ethical guidelines.

We analyzed each paper, discussing how research with clear ethical issues could harm users, further empower attackers, or promote illegal activity; how research in an ethical gray area could become more robust to ethical misuse; and how research that followed fundamental ethical principles provided concrete examples of how to carry out specific experiments while maintaining respect for moral guidelines.

## 4 Results

### 4.1 Deanonymization

A major distinction of cryptocurrencies is their relative anonymity, with some coins specifically marketing themselves towards privacy-conscious users. Naturally, there is a subfield of research on blockchains that investigates the level of privacy of these cryptocurrencies and deanonymization. Research in this area can violate the Menlo Report's [7] first pillar: respect for persons. The report calls for voluntary participation with informed consent and consideration for the impact of the work on people who are not targets of the research. Both are issues in deanonymization, as explored in the following three papers.

#### 4.1.1 Blockchain Is Watching You: Profiling and Deanonymizing Ethereum Users

In [5], the authors investigated privacy of transactions using Ethereum. They determined three user "quasi-identifiers": time-of-day activity, transaction fee, and transaction graph analysis using [12]. On a dataset which they built and released, they analyzed these attributes to group and deanonymize Ethereum users.

This paper's ethical shortcomings stem from its data collection and usage practices. The authors collected addresses by scraping Twitter, the Humanity DAO public registry, and transactions with an Ethereum mixer known as Tornado Cash. Although some argue that users with publicly available addresses have inherently consented to their participation, such a reach does not align with the Menlo Report. The authors' statement that the addresses were "presumably related to regular users" implied that not much thought was given to who was included in the dataset. Furthermore, there is a larger problem in that non-consenting users who used Tornado Cash, signaling they wanted anonymity, were deanonymized regardless of their decision to use a mixer.

Overall, the authors did not respect the privacy of the users they deanonymized. Their words and actions signify a careless approach towards curating their data. Because their analysis was formed around transaction fees and time-of-day activity, it is unclear why the researchers could not have instead analyzed themselves and other consenting participants or given a post-facto notification of their involvement, as done in [1, 9]. Even if the authors felt there was no other way to fairly evaluate their metrics, the paper could have benefited from a discussion explaining what alternatives were considered but ultimately deemed infeasible.

#### 4.1.2 Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network

Moreno-Sanchez et al. [9] examined the transaction network Ripple, which works by exchanging IOUs as payments. As with cryptocurrencies like Bitcoin, Ripple transactions are pseudo-anonymous and visible on a public ledger; but Ripple offers a unique security mechanism known as a hot-cold wallet. If the secret key for a wallet is compromised, the attacker can use it to issue many, often unlimited, IOUs. Hot-cold wallets allow a user to have a "hot", or online, wallet which can be used for daily transactions. Periodically, it receives credit from a "cold", or offline, wallet. If the secret key for a hot wallet is compromised, the potential loss is bounded by this credit-extending scheme.

The authors scraped a variety of public sources to create and release a dataset of 174,738 hot-cold wallets. Using their dataset, they proposed mechanisms to cluster and link Ripple wallets. Regarding respect for law and public interest– the fourth pillar of the Menlo Report, which we examine in our third set of papers– the authors did well. In collecting their dataset, they followed the outlined protocols for the appropriate APIs and emphasized this adherence in their paper. However, their respect for persons was less clear. Since the users in the dataset gave no consent to be a part of the experiment, the authors actively circumvented a security mechanism elected by Ripple users. Instead of merely connecting a set of transactions to a user through their deanonymization experiment, the authors linked a user's hot and cold wallets and consequently posed a security risk for the owner. By releasing this curated dataset with their analysis already performed, they exposed unaware users to potential attacks.

Additionally, when describing their conversations with the gateways, the authors wrote that the "responses do not include any wallet missed by our heuristics." While they wanted to highlight the effectiveness of their techniques, this statement alludes to the fact that the wallets in this dataset which used the named gateways were all confirmed to be correctly linked. As a result of the researchers' desire to demonstrate the quality of their work, information was disseminated about the dataset's unwitting users.

On the other hand, the authors contacted gateways to confirm that they correctly linked wallets and to alert them to the discovered bug. In section 6.3, they included a brief but commendable discussion of ethical principles they considered. Moreno-Sanchez et al. were more thoughtful about their ethical considerations than [5], but they could have done more to abide by the principles outlined in the Menlo Report.

#### 4.1.3 Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis

In [1], Biryukov and Tikhomirov observed that, despite Bitcoin's perceived anonymity, it does not have many privacy guarantees. They proposed a new deanonymization technique involving transaction propagation analysis, using Bitcoin as a case study in addition to three privacy-centric coins: Monero, Dash, and Zcash. To demonstrate the effectiveness of the attack, they performed experiments where they deanonymized themselves and estimated their potential loss.

The authors sidestepped issues around respect for persons by using themselves as subjects where possible. For their experiments, they logged their traffic and ran a clustering algorithm to attempt to re-identify themselves. They performed five experiments with Bitcoin (four on the testnet and one on the mainnet) and one each with Zcash, Dash, and Monero. Across the board, they demonstrated respect for persons by minimizing their impact and interaction with unwitting users. In their section on ethical considerations, the authors assured that logs generated during this experiment were deleted afterwards and that they limited the number of connection slots utilized when they could not use their own machines. Altogether, Biryukov and Tikhomirov's paper excelled at conducting effective blockchain research without sacrificing ethics.

#### 4.1.4 Summary

In deanonymization research, user data privacy is of utmost importance. Beres et al. used involuntary participants and acted with little regard for the safety of their data in [5], whereas some participants were contacted and made aware of the experiment after the fact in [9]. Although the latter improved upon the level of involvement of unaware users, Biryukov and Tikhomirov [1] showcased more ethically sound research practices by performing experiments on themselves. Moreover, they included an ethics section of the paper. Similar methods should be adopted across this subfield.

### 4.2 Optimized Attack Strategies

This category encompasses research which involves optimizing existing attacks against the blockchain to yield greater profit for the attacker. Research in this area is crucial for predicting methods of future attacks and implementing appropriate safeguards; but, if presented poorly and without protective countermeasures, such work can be easily exploited by malicious actors. Thus, papers that optimize attack strategies may not adhere to the Menlo Report's principle of beneficence, which calls for the maximization of probable benefits and minimization of probable harm.

#### 4.2.1 Attacking the DeFi Ecosystem With Flash Loans for Fun and Profit

A novel piece of blockchain technology is a flash loan: a loan valid within a single atomic blockchain transaction that must be repaid by the end of the borrowing transaction, allowing for no debt default risk or collateral. However, weaknesses in current flash loan implementations leave room for malicious actors to conduct profitable attacks. Two such attacks are optimized by Qin et al. in [11], yielding over double the original profit. However, the authors offered no countermeasures to defend against harmful use of their strategies.

The bulk of the paper discussed a post-mortem of a pump attack and arbitrage (PAA) and an oracle manipulation attack, followed by an optimization of attack parameters to maximize attacker revenue and a quantification of opportunity loss. In the post-mortem, the authors explained the mechanics of a PAA attack and detailed arbitrage opportunities stemming from the attack's structure. Next, the authors optimized the attacks by creating and solving a system of linear equations and constraints. For the PAA attack, the optimization focused on the amount of collateral required for the attack; for the oracle manipulation, the optimization primarily concerned preserving costs in gas fees and maximizing profit with reduced consumption. The authors experimentally evaluated their strategies on a locally deployed blockchain to show a dramatic increase in profits.

Despite their work in improving upon malicious actors' efforts in undermining blockchain technology, the authors did not propose any countermeasures. Furthermore, they named several decentralized exchanges which would likely be impacted by their optimized attacks– yet they did not make any note of having reported their findings to the exchanges prepublication. While their experiments were instrumental in identifying important breaches in blockchain security, the authors did not take action to ensure that this research could not be utilized by adversaries to more profitably attack users and exchanges. The Menlo principle of beneficence requests the minimization of probable harm by security researchers, and Qin et al. did not meet this requirement, given their failure to take responsibility for the consequences and possible uses of their flash loan attack optimizations.

### 4.2.2 Optimal Selfish Mining Strategies in Bitcoin

Sapirshtein, Sompolinsky, and Zohar [14] investigated a selfish Bitcoin mining attack originally proposed by Eyal and Sirer [4]. In Eyal and Sirer's strategy, a miner withholds certain blocks, inflating their payoff share above what it should be: proportional to its computational power. By exploiting conflict-resolution in the protocol, the malicious miner steals blocks from honest participants. The authors optimized this attack and built a theoretical framework by finding a profit threshold. They also analyzed communication delays and showed that they can cause the profit threshold to disappear.

Unfortunately, the authors provided no protections against the attack they optimized. Instead, they demonstrated that the countermeasures originally proposed by [4] were not as effective as believed, and attackers with less than a quarter of the resources used to mine could still profit from selfish mining. Given that they offered no defense mechanisms and also demonstrated how current ones could be undermined, Sapirshtein et al. did not meet the Menlo Report's bar for beneficence.

### 4.2.3 Quantifying Blockchain Extractable Value: How Dark Is the Forest?

In [10], the authors provided an algorithm capable of replacing unconfirmed blockchain transactions without understanding the logic of the victim transactions– a strategy which could have yielded over 35.37M USD over two years on historic data. We argue that, because the paper details multiple countermeasures to mitigate the effects of the optimized algorithm, it does not violate the beneficence principle of the Menlo Report.

The paper began with Qin et al. evaluating the profitability of sandwich attacks, liquidations, and decentralized exchange arbitrages for 32 months prior to the start of their research. Next, the authors proposed a novel generalized trading replay algorithm for adversaries to replace their own address for sender's addresses in victim transactions, facilitating even more lucrative front-running attacks. The authors described two naive protections against their algorithm and noted their loopholes; then, they detailed a more advanced mode of protection using a BEV relayer. They subsequently dedicated a section of the paper to discussing the drawbacks and poor-functioning miner incentives of BEV, as well as possible mitigants for these issues.

Like the other evaluated papers which optimize attack strategies to maximize profit, this paper provided an algorithm for undermining blockchain security that could cause tangible harm to users and systems. The difference is that, in this paper, the authors took measures to prevent this harm from occurring. They discussed three separate countermeasures in detail, going so far as to explore protection mechanisms for the pitfalls of one of their countermeasures itself. In fact, over a third of the paper is dedicated to alleviating potential negative effects of the research. This paper made an effort to maximize probable benefits and minimize probable harm, embodying the core tenets of beneficence.

### 4.2.4 Summary

Researchers in this area present extremely lucrative attack strategies in detail that allows them to be replicated, sometimes even naming potential victim exchanges. Less ethical papers simultaneously exemplify limitations of countermeasures thought to be valid against these attacks or fail to provide countermeasures that can prevent against misuse of their work. Authors optimizing blockchain attack strategies must propose protection mechanisms– measures which are advanced enough to derail malicious actors– before paper publication. All such papers should dedicate a substantial section to mitigating harm caused by the optimized attack. While countermeasures are difficult to discover, it is the moral responsibility of the researchers to maximize probable benefits (as per the Menlo Report) by bringing in other academics and continuing to seek a solution in the name of user safety.

## 4.3 Real-Time and Simulated Attacks

A significant portion of blockchain security research is dedicated to conducting or simulating real attacks against blockchains nodes, decentralized finance exchanges, or other victims. This research plays a vital role in finding weak spots in existing protocols and technologies, but it is necessary that the researchers' attacks abide by the law and do not harm users or systems. We examined selected papers in context of the Menlo Report's principle of respect for law and public interest: engaging in legal due diligence, being transparent about methods and results, and maintaining accountability.

#### 4.3.1 High-Frequency Trading on Decentralized On-Chain Exchanges

Front-running is the act of placing a transaction with knowledge of a future transaction. It is common on blockchains due to their publicly accessible data, and many exchanges still seek effective protection. In [16], the authors analyzed and empirically evaluated sandwich attacks, an augmented variant of front-running, on the decentralized exchange Uniswap; but they failed to notify Uniswap of their actions and to obtain permission for attacking the network beforehand.

The authors began by quantifying the possible daily revenue from conducting sandwich attacks on the exchange in both single- and multiple-adversary situations. As the first to formalize sandwich attacks, the authors devised and implemented an attack against their own transactions on the network by simultaneously front-running and back-running. They took advantage of the Uniswap default slippage protection strategy to maximize profits. While Zhou et al. proposed no countermeasures or potential solutions to the attack, they disclosed their results to Uniswap before publication so that the exchange could tighten slippage protections.

Although they only attacked their own transactions, the authors conducted an attack on Uniswap without receiving prior permission from the exchange. Failing to obtain consent from Uniswap beforehand displays a lack of transparency that should be present in blockchain security research. Zhou et al. informed Uniswap after successful attacks were conducted, so that the exchange could implement improved protection mechanisms, but they ignore the fact that similar problems could exist on several Automated Market Maker decentralized exchanges which closely follow Uniswap's model; and, as no countermeasures were proposed in the paper, the authors provided these other exchanges with few suggestions on how to shield themselves against sandwich attacks. Due to this lack of accountability, the paper is in clear violation of the Menlo Report's principle of respect for law and public interest.

#### 4.3.2 Burning Zerocoins for Fun and for Profit

Ruffing et al. [13] examined an attack on Zerocoin that allows a malicious user to destroy the money of legitimate users, thereby exposing an important missing property in Zerocoin's security model and its formal analysis. Their attack involved eavesdropping the serial number and using it to mint their own coin. This prevented the serial number from being used to mint any more coins, "burning" the legitimate user's coin. Even worse, the attacker could take the stolen coin and transfer it to themselves, destroying a legitimate coin and profiting in the process.

To their credit, the authors included and analyzed a solution to the attack. They offered a fix to the security model and existing scheme. In terms of disclosure, they contacted the Zerocoin maintainers, who then hired Ruffing to implement a safeguard. The authors only later realized that older, not newly minted coins relied on Zerocoin and were still vulnerable. For SmartCash, PIVX, and Hexxcoin, the maintainers chose to disable Zerocoin functionality.

The authors did well in developing and, to some extent, deploying a fix for the discovered bug, but they could have done more to maximize public interest. They failed to promptly recognize the breadth of the vulnerability, leading to a necessary disablement of Zerocoin functionality. It is difficult to decide when disclosure in a paper is sufficient for publication; but, in this case, the opportunity to protect public interest was concrete and achievable. The authors had already implemented protections for newly minted Zerocoins and could have plausibly completed a robust protection mechanism for older coins as well.

#### 4.3.3 Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network

In [8], Marcus et al. conducted eclipse attacks on Ethereum nodes to exploit the peer-to-peer network used for neighbor discovery. They launched these attacks against self-hosted victim nodes using two hosts and pinpointed specific protocols that led to vulnerabilities in the Ethereum network. Finally, the authors presented countermeasures to protect Ethereum from eclipse attacks, many of which were incorporated into the new Ethereum geth client. Because of the simulation of attacks on researcher-owned nodes, identification of weakness areas and protection mechanisms, and implementation of countermeasures prior to publication, this research abides by the Menlo principle of respect for law and public interest.

The paper began by explaining why Ethereum nodes are especially vulnerable to eclipse attacks, due to Ethereum's use of the Kademlia peer-to-peer protocol. The authors provided a deep exposition on this topic by reverse-engineering the code of the Ethereum geth client. Next, the authors conducted two off-path eclipse attacks using connection monopolization and carefully crafted node identifiers, as well as another attack using time manipulation. They warned against other effects of leaving these weaknesses unaddressed, including attacks on consensus, blockchain layer-two protocols, and smart contracts. Lastly, Marcus et al. provided countermeasures that can be used to prevent these attacks, most notably recommending that Ethereum use a combination of IP address and ECDSA public key as node identifiers in lieu of only public keys. The authors even showed how to harden Ethereum via design decisions that stray from the Kademlia protocol. Several of their countermeasures were adopted in geth v1.8.

Similar to the methods of the above two researchers, Marcus et al. empirically tested attacks on a blockchain, but they went above and beyond to serve public interest. Not only did they provide an in-depth explanation of the causes and effects of the vulnerabilities in question and conduct their attacks on self-hosted nodes, but they also provided several countermeasures to alleviate the risks they exposed. They made long-term improvement suggestions to the Ethereum clients in question and ensured that the fixes were deployed prior to the paper's publication to avoid any exploitation of their work. The authors showed utmost respect for law and public interest by ensuring a lack of harm in their attacks, maintaining transparency in their research and results, and holding themselves responsible for mitigating negative effects of their research.

### 4.3.4 Summary

When researchers simulate or outright attack victims to discover areas of improvement in blockchain security, they often employ unethical methods that show disrespect for the the law and public interest: targeting live exchanges without express permission and failing to suggest protection mechanisms that would mitigate negative effects if their attacks were to be replicated on other victims. Researchers can align better with the principles of the Menlo Report if they conduct simulated attacks on self-hosted victims or obtain consent from exchanges before using them for real-time attacks. They are morally obligated develop and report on countermeasures in order to alleviate any ensuing harm.

## 5 Conclusion

Overall, we found the Menlo Report to be a sufficient set of ethical guidelines for blockchain security research. While the guidelines are broad and overarching, examining research methods within their context exposes several underlying issues. We have discussed numerous ethical dilemmas that have arisen in blockchain security research papers: performing research on unaware and non-consenting users, providing attack strategies that can be copied and used for harm by adversaries without suggesting or implementing countermeasures, and attacking real services and publishing accounts of the employed methodology without express permission or in-place protection mechanisms. Our wish is that this review will lay the groundwork for establishing a set of ethical guidelines unique to blockchain security and create a higher moral standard which researchers can commit to meeting in their work. At the minimum, we hope that this will serve as a useful evaluation tool for blockchain security researchers aiming to ensure the ethical robustness of their empirical methods and techniques.

## References

[1] BIRYUKOV, A., AND TIKHOMIROV, S. Deanonymization and linkability of cryptocurrency transactions based on network analysis. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (2019), IEEE, pp. 172–184.

[2] CHIAUZZI, E., AND WICKS, P. Digital trespass: ethical and terms-of-use violations by researchers accessing data from an online patient community. *Journal of Medical Internet Research 21*, 2 (2019), e11985.

[3] DITTRICH, D. The ethics of social honeypots. *Research Ethics 11*, 4 (2015), 192–210.

[4] EYAL, I., AND SIRER, E. G. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (2014), Springer, pp. 436–454.

[5] FERENC BERES, ISTVAN A. SERES, ANDRAS A. BENCZUR, MIKERAH QUINTYNE-COLLINS. Blockchain is watching you: Profiling and deanonymizing ethereum users. *arXiv preprint arXiv:2005.14051* (2020).

[6] HYRYNSALMI, S., HYRYNSALMI, S. M., AND KIMPPA, K. K. Blockchain ethics: A systematic literature review of blockchain research. In *International Conference on Well-Being in the Information Society* (2020), Springer, pp. 145–155.

[7] KENNEALLY, E., AND DITTRICH, D. The menlo report: Ethical principles guiding information and communication technology research. *Available at SSRN 2445102* (2012).

[8] MARCUS, Y., HEILMAN, E., AND GOLDBERG, S. Low-resource eclipse attacks on ethereum's peer-to-peer network. *IACR Cryptol. ePrint Arch. 2018* (2018), 236.

[9] MORENO-SANCHEZ, P., ZAFAR, M. B., AND KATE, A. Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. *Proc. Priv. Enhancing Technol. 2016*, 4 (2016), 436–453.

[10] QIN, K., ZHOU, L., AND GERVAIS, A. Quantifying blockchain extractable value: How dark is the forest? *arXiv preprint arXiv:2101.05511* (2021).

[11] QIN, K., ZHOU, L., LIVSHITS, B., AND GERVAIS, A. Attacking the defi ecosystem with flash loans for fun and profit. In *International Conference on Financial Cryptography and Data Security* (2021), Springer, pp. 3–32.

[12] ROZEMBERCZKI, B., KISS, O., AND SARKAR, R. Karate club: an api oriented open-source python framework for unsupervised learning on graphs. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management* (2020), pp. 3125–3132.

[13] RUFFING, T., THYAGARAJAN, S. A., RONGE, V., AND SCHRODER, D. (short paper) burning zerocoins for fun and for profit-a cryptographic denial-of-spending attack on the zerocoin protocol. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (2018), IEEE, pp. 116–119.

[14] SAPIRSHTEIN, A., SOMPOLINSKY, Y., AND ZOHAR, A. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security* (2016), pp. 515–532.

[15] TANG, Y., XIONG, J., BECERRIL-ARREOLA, R., AND IYER, L. Blockchain ethics research: a conceptual model. In *Proceedings of the 2019 on Computers and People Research Conference* (2019), pp. 43–49.

[16] ZHOU, L., QIN, K., TORRES, C. F., LE, D. V., AND GERVAIS, A. High-frequency trading on decentralized on-chain exchanges. In *2021 IEEE Symposium on Security and Privacy (SP)* (2021), IEEE, pp. 428–445.