

# AI Ethics on Blockchain: Topic Analysis on Twitter Data for Blockchain Security\*

Yihang Fu<sup>1</sup>, Zesen Zhuang<sup>1</sup>, and Luyao Zhang<sup>\*1</sup>

Duke Kunshan University, Suzhou, Jiangsu, 215316, China

\*corresponding author: lz183@duke.edu

Data Science Research Center & Social Science Division

Duke Kunshan University

**Abstract.** Blockchain has empowered computer systems to be more secure using a distributed network. However, the current blockchain design suffers from fairness issues in transaction ordering. Miners are able to re-order transactions to generate profits, the so-called miner extractable value (MEV). Existing research recognizes MEV as a severe security issue and proposes potential solutions, including prominent Flashbots. However, previous studies have mostly analyzed blockchain data, which might not capture the impacts of MEV in a much broader AI society. Thus, in this research, we applied natural language processing (NLP) methods to comprehensively analyze topics in tweets on MEV. We collected more than 20000 tweets with #MEV and #Flashbots hashtags and analyzed their topics. Our results show that the tweets discussed profound topics of ethical concern, including security, equity, emotional sentiments, and the desire for solutions to MEV. We also identify the co-movements of MEV activities on blockchain and social media platforms. Our study contributes to the literature at the interface of blockchain security, MEV solutions, and AI ethics.

**Keywords:** AI Ethics, Blockchain Security, Natural Language Processing (NLP), Twitter, Flashbots, MEV

---

\* The corresponding author Luyao Zhang is supported by National Science Foundation China on the project entitled “Trust Mechanism Design on Blockchain: An Interdisciplinary Approach of Game Theory, Reinforcement Learning, and Human-AI Interactions.” (Grant No. 12201266). Yihang Fu is supported by the Summer Research Scholar (SRS) program 2022 under Prof. Luyao Zhang’s project titled “Trust Mechanism Design: Blockchain for Social Good” at Duke Kunshan University. Zesen Zhuang is supported by the Social Science Divisional Chair’s Discretionary Fund for undergraduate research in Prof. Luyao Zhang’s related interdisciplinary research courses as a Teaching and Research Assistant at Duke Kunshan University. Both Zesen Zhuang and Luyao Zhang are also with SciEcon CIC, an NPO aimed at cultivating interdisciplinary research with both profound insights and practical impacts. We thank the anonymous referees at the Computing Conference for their professional and thoughtful comments.

## 1 Introduction

Blockchain has enabled computer systems to be more secure using a distributed network. [26, 27, 29, 3] However, the current blockchain design suffers from fairness issues in transaction ordering. [9] Miner extractable value (MEV), first coined by Daian et al. in 2020 [6], refers to the value that miners can extract by reordering the transactions on the blockchain. For example, on the Proof-of-Work (PoW) Ethereum [18], miners can order, include, and exclude transactions in mem-pool, a pool where transactions are stored or sorted temporarily before adding to the new blocks. Researchers [21] found that from 2015 to 2020, the 199724 frontrunners had cumulative profits of more than 18.4 billion USD. Since the transition of Ethereum from PoW to Proof-of-Stake (PoS), miners no longer have a role in the blockchain protocol. Instead, validators take charge of validating transactions on the blockchain. However, the method of extracting value by manipulating the transaction order still exists. Therefore, people now use MEV as an abbreviation for the maximum extractable value in PoS Ethereum, the so-called Ethereum 2.0. Existing research recognizes MEV as a severe security issue and proposes potential solutions [8, 25] including the prominent Flashbots [22]. However, previous studies have mostly analyzed blockchain data, which might not capture the impacts of MEV in a much broader AI society. Therefore, we extend the study of MEV from blockchain data to a broader community on social media platforms. Specifically, our study targets two research questions (RQs):

1. **RQ1:** What are the main keywords and topics being discussed in tweets with #MEV and #flashbots hashtags, and what are the connections between those keywords?
2. **RQ2:** What are the connections between the MEV activities on blockchain and discussions on social media platforms?

In this study, we applied natural language processing (NLP) methods to analyze topics in tweets on MEV comprehensively. We queried more than 20000 tweets with #MEV and #Flashbots hashtags from 2019 to October 2022. We also included corresponding Google Trend data in the same period for reference and comparison. To explore the connections between the MEV activities on blockchain and discussions on social media platforms, we collected the gross profit data of MEV from Flashbots. Our results show that the tweets discussed profound topics of ethical concern, including security, equity, emotional sentiments, and the desire for solutions to MEV. According to the keyword statistics, the discussion about MEV is highly concentrated on the Ethereum blockchain. The result also indicates that the MEV problem is one of the most urgent problems on the Ethereum blockchain, and practical solutions are highly demanded. In addition to Flashbots, the topics mention several alternative solutions to MEV, but Flashbots appears to be the most promising one. Some potential nontraditional solutions are also mentioned, such as machine learning. Moreover, other nontechnical keywords indicate that people generally express negative emotions toward MEV, e.g., a feeling of unfairness. We also identify the

co-movements of MEV activities on blockchain and social media platforms. Our study contributes to the literature at the interface of blockchain security, MEV solutions, and AI ethics. In Section 2, we discuss the related literature and background. Section 3 introduces the data and methodology. Section 4 presents the results of the two research questions respectively. Section 5 discusses and concludes. We provide a glossary Table 7 in the Appendix.

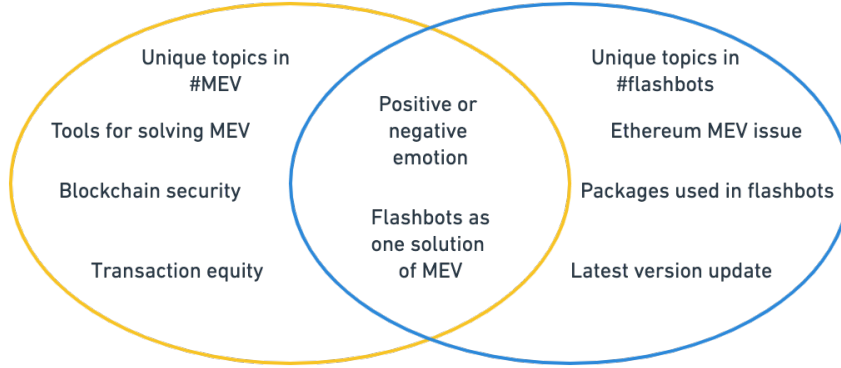


Fig. 1: Common topics between MEV and flashbots, and unique topics in the two hashtags

## 2 Related Literature and Background

Our research contributes to three lines of literature: blockchain security, MEV solutions, and AI ethics.

### 2.1 Blockchain Security: MEV issues

Ethereum blockchain facilitates transactions with the use of smart contracts. In Ethereum, nodes collect transaction information from networks, and miners record the transactions into blocks. Before being added to the blocks, transactions are temporarily stored and sorted in the mem-pool. Miners select transactions in the mem-pool and execute Proof of Work. Whoever (miners) wins the race of PoW can add the block to the network. [18] The order of transactions is predetermined. The execution depends on the initial transaction sets in front of the block or in the same block. However, when Daian et al. [7] introduced frontrunning in cryptocurrency decentralized exchange (DEX), miners could change the order of the transactions. In general, MEV is an activity in which attackers (or profit seekers) discover certain instabilities and look for extractable values

[1]. MEV has different strategies to obtain profits. One of the most common strategies is called a sandwich attack. For example, if A is prompting a transaction to purchase a token, the attackers who discovered A’s attempt could buy this token ahead of A at a high price and then sell this token after A. The attackers manage to extract a profit from the series of transactions. Another commonly used strategy is called the arbitrage attack. . In arbitrage, the same good is purchased and sold simultaneously in different markets, and profits are made from the difference in the price of the same good in different markets. In Ethereum, if two or more DEXs offer the same token in different prizes simultaneously, one can buy the cheaper token and sell it at a higher price. Our research contributes to the literature by analyzing concerns about blockchain security discussed on social media platforms.

## 2.2 MEV solutions: Flashbots and alternatives

Methods to mitigate MEV problems are divided into two main categories: democratization and minimization. MEV minimization sets up roles to make MEV impossible or increases the risk to be larger than the MEV benefits. For example, Ethereum 2.0 upgrades from proof-of-work (PoW) to proof-of-stake (PoS) and introduces slashing [15] to punish misbehavior regarding MEV. Third-party researchers propose minimization solutions such as fair sequencing services [8] and Conveyor [12]. Alternatively, MEV democratization tries not to eliminate but to democratize MEV behavior so that everyone has access to information that is available to miners. The most popular approaches, such as Flashbots [22] direct transactions to private relays to reduce the mem-pool bidding war [23].<sup>1</sup> Flashbots aim to mitigate the negative externalities of the current MEV by establishing a fair, transparent, and permissionless ecosystem. Two initiatives mainly support it, *MEV-geth* and *MEV-inspect* [7]. Specifically, Flashbots provide a new auction ecosystem with three primary roles: searchers, relays, and miners. Searchers seek MEV opportunities. Once they find potential transactions promoted by peers, they create a bundle that contains a set of transactions. The bundle includes the fee paid to the miners and the searchers themselves. Searchers then send the bundles to the relays instead of the mem pool. Relays collect the bundles and send them to the miners. Since the bundles are sent to the Flashbots, the miners are exclusively Flashbots miners. Miners then collect bundles and select the most profitable ones, and only one transaction can be accounted for in each block. Miners can determine which transaction to mine based on MEV-geth, a forked version of the Go-Ethereum client [22]. Our research contributes to the literature by evaluating MEV solution discussions on social media platforms and their connections to MEV activities on the blockchain.

## 2.3 AI Ethics

Researchers have expressed concern about the ethical aspects of security issues related to blockchain technologies. Bertino et al. [4] noted that if data were gath-

<sup>1</sup> There are also similar solutions like Eden Network [14] and CoW Protocol [16], etc.

ered and used, based on some ethical principles of data transparency, it would provide a novel way for policy-makers to assess the mechanism of blockchain transactions. Another group of researchers proposed a list of ethical concerns about blockchain technology categorized into four areas: technology stack, cryptocurrencies, smart contracts, and decentralization. One of the major concerns in the cryptocurrency area is whether the coin mining mechanism is ethically sustainable and fair [19]. Regarding this question, Ben and his colleagues assessed Flashbots. They argued that in the new auction mechanism of Flashbots (as introduced previously), only some users can receive fair profits, and miners benefit more than searchers [22]. However, although the researchers provided comprehensive insights into the ethical discussion, the existing research needs to better evaluate the ethical issue of blockchain based on the real-life reactions of blockchain users. In this article, we measure and evaluate people’s reactions and feedback toward blockchain security issues on social media platforms.

### 3 Data and Methodology

The data and code in this project are open-sourced and can be accessed at <https://github.com/SciEcon/blockchain-ethics>

In-index	Date	Tweets
0	2021-12-31 15:53:38+00:00	@willwarren No worries @foldfinance solves thi...
1	2021-12-31 05:56:23+00:00	Vshadow textbackslashn#Imgoodgirl\n...
2	2021-12-31 05:49:28+00:00	This is what a sandwich attack looks like. The...
3	2021-12-29 21:11:16+00:00	#Memoria...líderes de jxc apoyaron públicament...
4	2021-12-29 17:34:14+00:00	even if you don’t have that much money to clai...

Table 1: Sample Tweets Data

#### 3.1 Data

We collected three datasets. The first includes tweets and Google Trends data. For Tweets, we used **snsrape**<sup>2</sup> to query primary data for our research. **snsrape** is a Python library to scrape posts on a variety of social networks with specific topics or hashtags. We queried two datasets, one with the hashtag #mev and the other with the hashtag #flashbots. We queried Twitter data from 2019-01-01 to

<sup>2</sup> <https://github.com/JustAnotherArchivist/snsrape>

2022-10-01. In total, we found in total 20574 tweets with hashtag #mev and 852 tweets with hashtag #flashbots. The queried data includes two columns which are date and content. Table 1 shows examples of downloaded data. Next, we use Python library `pytrend`<sup>3</sup> to query Google Trend data for two topics, “MEV” and “flashbots”. `pretend` provides API to automatically download reports from Google Trend<sup>4</sup>. Then, we merge the Google Trend data with the tweets by date as in Table 2. In addition, we also queried Ethereum MEV records from the flashbots’ MEV-Explore dashboard<sup>5</sup> to compare on-chain and social media activities.

	date	google trend	tweet_volume	tweet_len
<b>0</b>	2021-04-11	23	3	20.666667
<b>1</b>	2021-04-18	23	2	37.500000
<b>2</b>	2021-04-25	0	1	42.000000
<b>3</b>	2021-05-02	0	1	34.000000
<b>4</b>	2021-05-09	24	1	19.000000

Table 2: Sample Merged Data: column **date** shows the date in YYYY-MM-DD format; column **google trend** shows the Google Trend index; column **tweet.\_volume** is the count of tweets with a specific topic (“MEV” for example); column **tweet\_len** is the sum of the length of the tweets in one day.

### 3.2 Methodology

Our NLP methods include keyword analysis and Latent Dirichlet Allocation (LDA), similar to the quantitative methods in [20].

**Keywords Analysis Methods** Analyzing the trend of discussion on a topic on social media and its high relevance is helpful to understand the history and development of the topic and future trends. In this study, we trace and then quantify the activity of the hashtags #mev and #flashbots on Twitter and compare them with their Google Trends profiles. We first conduct the Spearman correlation test between tweet volume and Google Trends data and then plot the time series for each hashtag to reveal the correlation between their activity on Twitter and Google. Next, we count and sort the keywords’ appearance (irrelevant words such as emojis and common words are excluded) in tweets and draw a word cloud that shows the most relevant topics discussed on social media to the two hashtags #mev and #flashbots. After that, we use Python library `NetworkX`<sup>6</sup> to draw a network on keywords. The edge in the network indicates

<sup>3</sup> <https://github.com/GeneralMills/pytrends>

<sup>4</sup> <https://trends.google.com/trends>

<sup>5</sup> Flashbots MEV-Explore public dashboard <https://explore.flashbots.net/> consists of various historical statistics of MEV activities on the Ethereum blockchain.

<sup>6</sup> <https://networkx.org/>

that two keywords occur in the same topic, and the thickness of the edge is proportional to the frequency of co-occurrence.

**Latent Dirichlet Allocation for Topic Analysis** We utilize Latent Dirichlet Allocation (LDA) [5] to reveal the topic tendency of the collected tweets on #mev and #flashbots. LDA is a statistical model that groups data and explains why some groups of data are similar. The LDA model is widely used in natural language processing. Our research utilizes an LDA model implemented in the Python library `gensim` [17]. The LDA in `gensim` implementation has three hyperparameters: (1) integer  $K$ , the number of topics; (2) rational number  $\alpha$  between 0 and 1 controls the per-document topic distribution, a higher  $\alpha$  results in more topics in a document; (3) rational number  $\beta$  between 0 and 1 controls the per-topic word distribution, a higher  $\beta$  results in more keywords in a topic. For results, the LDA model produces the probability of the corpus as shown in equation (1).

$$p(\mathcal{D}|\alpha, \beta) = \prod_{d=1}^K \int p(\theta_d|\alpha) \left( \prod_{n=1}^{N_d} \sum_{z_{d_n}} p(z_{d_n}|\theta_d) p(w_{d_n}|z_{d_n}, \beta) \right) d\theta_d \quad (1)$$

In equation (1),  $\theta$  is the joint distribution of a topic mixture,  $z$  is the number of topics, and  $N$  is the number of words in a set. The model is trained with various  $\alpha$ ,  $\beta$ , and  $K$ . We use a coherence score for parameter optimization. A high coherence score in a topic indicates a higher semantic similarity among keywords in which. We manually tried out  $K \in \{1, 5, 10, 15, 20, 25, 30\}$  then adopt SALDA [13] algorithm for  $\alpha$  and  $\beta$  to optimize hyperparameters. Ultimately, we achieved  $K = 20$ ,  $\alpha = 0.31$  and  $\beta = 0.61$  with a coherence score of 0.4296 for hashtag #flashbots and  $K = 5$ ,  $\alpha = 0.25$  and  $\beta = 0.91$  with a coherence score of 0.4687 for hashtag #mev.

## 4 Results

### 4.1 Answers to RQ1

This section answers the RQ1 based on the four analyses below:

1. We calculate and ranked the frequent keywords among the tweets under the hashtag of #MEV and #Flashbots.
2. We use the LDA analysis to analyze people's reactions and emotions behind the potential MEV security issue.
3. We establish Network Analysis (NA) to seek the intrinsic relationship between keywords under each Twitter hashtag.
4. We compare the Google Trend data with real-world events.

Keywords	Frequency
#flashbots	513
#Flashbots	340
MEV	219
#MEV	152
ETH	85
mist	84
Flashbots	76
opensea	72
#Ethereum	67
Support	65
artist	65
grow	65
Shill	65
Shizzlebotz	65
#nftshill	65
#PolygonNFT	65
#openseaNFT	65
#mev	49
thegostep	49
transactions	47
gas	46
miners	41
MIST	41
#DeFi	40
Ethereum	39
team	39
bertcmiller	31
transaction	31
#FlashBots	29
#mistX	28
NFT	26
front	25
#riverfrontrocks	25
#ethereum	24
EST	24

Table 3: Wordcount for #flashbots

Keywords	Frequency
#MEV	19928
#arbitrage	7511
Ecocent	5966
MEV	5957
WETH	5339
video	4398
simply	4357
explained	4352
System	4351
#HotWater	4349
info	3930
USDT	3318
USDC	3290
ROI	2908
ESP	2749
view	2578
WBNB	2382
triangular	2102
sandwich	2078
spatial	1570
profit	1267
DAI	1225
days	1175
contract	1075
eye	1016
#SandwichAttacker	1009
SAP	910
EigenPhi	877
#mev	816
pass	809
WBTC	768
BUSD	754

Table 4: Wordcount for #MEV



**Keywords** We rank the frequency of keywords for both hashtags as in Table 3 and Table 4. By calculating the word count of the keywords in each topic, we found similarities between these two hashtags. First, both have hashtags with relative semantic meanings. For example, like *Ethereum*, *miner*, and *crypto*, the terminologies in blockchain, are the most salient keywords, appearing more than 300 times, except for #MEV and #Flashbots. Also, we observed that #MEV or #Flashbots would be mentioned in the other hashtag simultaneously. This reflects the coherent relationship between these two hashtags. As we can see through the table 4 and 3, Flashbots was mentioned under the topic of MEV nearly 400 times, and MEV was mentioned nearly 400 times as well under the topic of Flashbots. After investigating the word frequency, we also explored the keyword connections by building up the word bigrams. As we can see in figure 2, with the selection of the semantic meaning, the top frequent bigrams for the #flashbots are "mev" & "flashbots", "crucible" & "copper", and "flashbots" & "mist". The top frequent bigrams for the #MEV are "extractable" & "value", "mev" & "flashbots", "macri" & "macri", "miner" & "extractable", "front" & "running", "defi" & "mev" and "cpb" & "mev".

**LDA analysis** We used Genism, an open-source library for unsupervised topic modeling to implement text analysis. We selected 1, 3, 5, 10, 15, 20, 25 as the targeted number of topics to calculate the corresponding coherence score. We found that when  $k = 1$  (the number of topics), the coherence score of #flashbots (0.482) is the highest. When  $k = 3$ , the coherence score of #MEV, which equals 0.47 is the highest outcome in our model. This indicates that when the number of topics for #flashbots is 1, and the number of topics for #MEV is 3, the words in the corpus are relatively more semantically interpretable to humans. Figure 3 plots the different coherence scores under the different number of topics for two hashtags. Since the coherence score is also attributable to the two hyperparameters, we adopted Pathik’s SA-LDA algorithm to find a pair of approximately suitable  $\alpha$  and  $\beta$ . We found that when  $\alpha = 0.31$ ,  $\beta = 0.61$ , and the number of topics = 20, the coherence value of #flashbots equals 0.4296, which is the highest among all the outcomes of tested combinations. In the same way, when  $\alpha = 0.25$ ,  $\beta = 0.91$ , and the topic = 5, the approximate highest coherence value of #MEV equals to 0.4687. After excluding some words without semantic meaning, for example, emojis and persons’ names, we identify the sets of words categorized by different topics in Table 6. We summarize our main findings in Figure 1. Our results show that the tweets discussed profound topics of ethical concerns including security, equity, emotional sentiments, and craving for solutions of MEV. Table 5 illustrates the top 30 salient terms generated by the LDA model with the selected parameters of #MEV and #flashbots. Combined with LDA analysis, we find that the top 30 salient terms, including some frequently mentioned keywords such as *ethereum*, *smart contract*, and *solution*, etc., are not categorized by the topics. That is to say, the LDA model did not recognize some of their semantic meanings successfully.

Topic ID	bigram	count	Topic ID	bigram	count
0	('mev', '#flashbots')	16	0	('extractable', 'value')	22
1	('crucible', '#copper')	11	1	('mev', '#flashbots')	16
2	('flashbots', '\$mist')	9	2	('macri', 'macri')	15
3	('mist', '🐳')	9	3	('miner', 'extractable')	13
4	('flashbots', '#mev')	9	4	('front', 'running')	13
5	('flashbots', 'team')	8	5	('consentidxs', '#mev')	13
6	('mistx', '#flashbots')	7	6	('defi', '#mev')	12
7	('mist', 'mistx')	7	7	('cpb', '#mev')	11
8	('flashbots', 'poap')	6	8	('💖', '💖')	10
9	('samiches', '#flashbots')	6	9	('mev', 'solution')	9
10	('alchemist', '#alchemistcoin')	6	10	('smart', 'contract')	9
11	('flashbots', 'v02')	6	11	('flashbots', '#mev')	9
12	('gas', 'price')	6	12	('mev', '#ethereum')	8
13	('mist', '#crucible')	5	13	('prinsjesdag', '#mev')	8
14	('alchemist', 'radio')	5	14	('macri', '#macri')	8
15	('🐳', '\$mist')	5	15	('stay', 'tuned')	7
16	('mistx', '#crucible')	5	16	('mh', '#mev')	7
17	('copper', '#flashbots')	5	17	('mev', '#mehwishhayat')	7
18	('mist', '#flashbots')	5	18	('extractable', 'value')	7
19	('support', 'new')	4	19	('mev', '#defi')	7
20	('new', 'artist')	4	20	('sobre', '#mev')	7
21	('artist', 'help')	4	21	('look', 'like')	6
22	('help', 'u')	4	22	('solution', '#mev')	6
23	('u', 'grow')	4	23	('del', '#mev')	6
24	('grow', 'shill')	4	24	('crypto', '#defi')	6
25	('shill', 'shizzlebotz')	4	25	('level', '#domainname')	6
26	('shizzlebotz', '#nftshill')	4	26	('sandwich', 'attack')	5
27	('nftshill', '#polygonft')	4	27	('💖', '@mehwishhayat')	5
28	('polygonft', '#flashbots')	4	28	('@mehwishhayat', '💖')	5
29	('flashbots', '@opensea')	4	29	('💖', 'mh')	5
30	('@opensea', '#openseanft🔥')	4	30	('mehwishhayat', '💖')	5
31	('stay', 'tuned')	4	31	('💖', '#mehwishsource')	5
32	('flashbots', 'protect')	4	32	('mev', '\$eth')	5
33	('dark', 'forest')	4	33	('frontrunning', '#mev')	5
34	('copper', 'mistx')	4	34	('mev', '#crypto')	5
35	('copper', '#samiches')	4	35	('mist', '🐳')	5
36	('mist', '@_alchemistcoin')	4	36	('join', 'u')	5
37	('mist', '\$mistx')	4	37	('fair', 'sequencing')	5
38	('mistx', '#crucible')	4	38	('sequencing', 'service')	5
39	('flashbots', 'community')	4	39	('mev', 'front')	5
40	('per', 'block')	4	40	('\$7600', 'phenomenal')	5
41	('transparency', 'report')	4	41	('phenomenal', 'top')	5
42	('white', 'hat')	4	42	('top', 'level')	5
43	('miner', 'extractable')	3	43	('domainname', 'sale')	5
44	('extractable', 'value')	3	44	('sale', '#mev')	5
45	('bertcmiller', '#flashbots')	3	45	('mev', '#machinelearning')	5
46	('mist', '\$uni')	3	46	('machinelearning', '#datascience')	5
47	('@_alchemistcoin', '@thegostep')	3	47	('datascience', '#python')	5
48	('crucible', 'session')	3	48	('python', '#ai')	5
49	('utc', '/')	3	49	('ai', '#100daysofcode')	5

Fig. 2: Bigram of keywords: the bigram of keywords, which illustrates the most frequent keyword pairs that were mentioned in tweets under the hashtag of #MEV and #Flashbots.

Top 30 Most Relevant Terms (Overall term frequency)	
#Flashbots	#MEV
mist	macri
mistx	mev
flashbots	extractable
crucible	ethereum
gt	value
gas	see
bundles	op
copper	chain
team	mist
poap	inflate
alchemist	si
eth	aiz
samiches	eth
mev	flashbots
going	video
pm	door
bertcmiller	mehwishhayat
good	chainlink
future	energy
week	mempool
thanks	front
see	capital
ethereum	love
thegostep	miner
crypto	us
leaksblockchain	worldpastsaday
new	look
block	people
via	makes
miners	fair

Table 5: Top 30 most salient terms of two hashtags

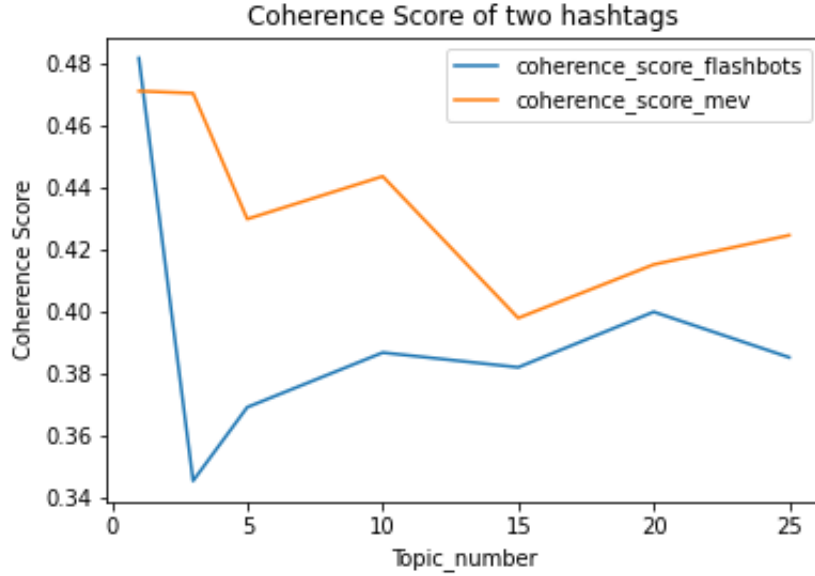


Fig. 3: Coherence Score for #MEV

**Keywords Network** We used NetworkX on Python to visualize the outcome found in Figure 4 and 5. Each node represents a commonly used keyword extracted from tweets of #MEV and #flashbots, and each edge represents a connection between two keywords. The number of edges of each node represents the number of respective networks with other keywords. We can identify the most commonly mentioned keywords and their relative co-occurring keywords by this analysis. We can see in the solution that the most frequent keywords that appeared together with #flashbots are **ethereum**, **smartcontract**, **solution**, etc. The most frequent keywords connected with #MEV are **flashbots**, **sandwich**, **miner**, etc.

**Google Trend and Twitter Data** We also researched Google Trends data of two keywords (namely, #MEV and #flashbots) to compare their Twitter volume and offline activities. We used the Google Trends API Pytrend to query the Google Trends data. Google Trends reveals the popularity of top search queries in Google Search across various regions and languages. In general, the Google Trends of #MEV and #flashbots show moderate consistency with the respective Twitter volumes. We ran the Spearman correlation test between Twitter volume and Google Trends, and the results showed that #MEV had more moderate consistency (with coefficient= 0.45) than #flashbots (with coefficient = 0.202).

Furthermore, we observed that each peak of flashbots google trends have a certain time interval, with the peaks of Flashbots twitter volume. Figure 6 illus-

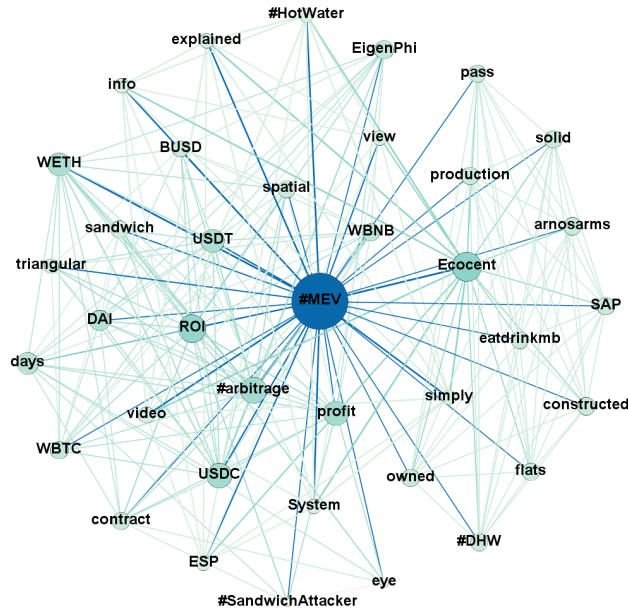


Fig. 4: Network of keywords for #MEV

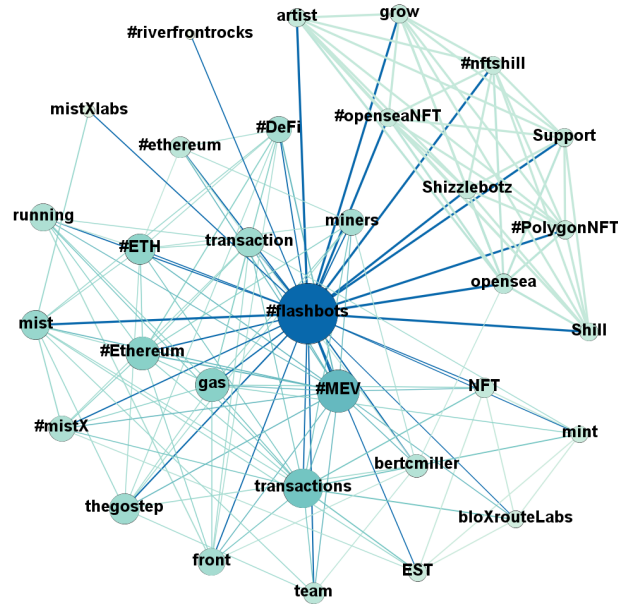


Fig. 5: Network of keywords for #flashbots

trates the staggering peaks of Google Trend and Twitter volume for #Flashbots. Also, we found that every peak of Google Trend or Twitter volume of #Flashbots could match up with a big offline event of Flashbots corporation. For example, on January 2021, Flashbots Auction Alpha (v0.1) was made available for miners and searchers to adopt. The same year, in May, August, and September, Flashbots Auction Alpha updated and published its latest versions corresponding to the peaks shown in Figure 7. This will be further discussed in the discussion part. However, the situation of #MEV was slightly different. Although the Spearman correlation test indicates a higher correlation between Google trends and Twitter volume, those two lines do not show much consistency in peaks.

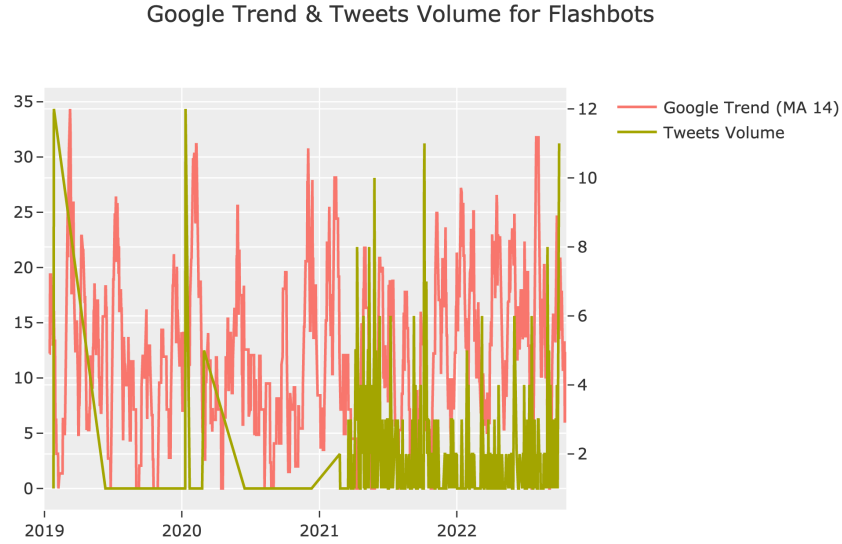


Fig. 6: Time series for Google trend and Twitter volume of #Flashbots

## 4.2 Answers to RQ2

To respond to this research question, we query the gross profit data of MEV from 2019 to 2022 using Flashbots API. Gross profit here refers to the amount that attackers acquire from MEV arbitrages. As presented in figure 8, we observe that there exist three spikes between late 2020 and July 2021. At the same time, we compare the gross profit data with Twitter volume data. Interestingly, we find that each spike in gross profit data corresponds to a spike in Twitter

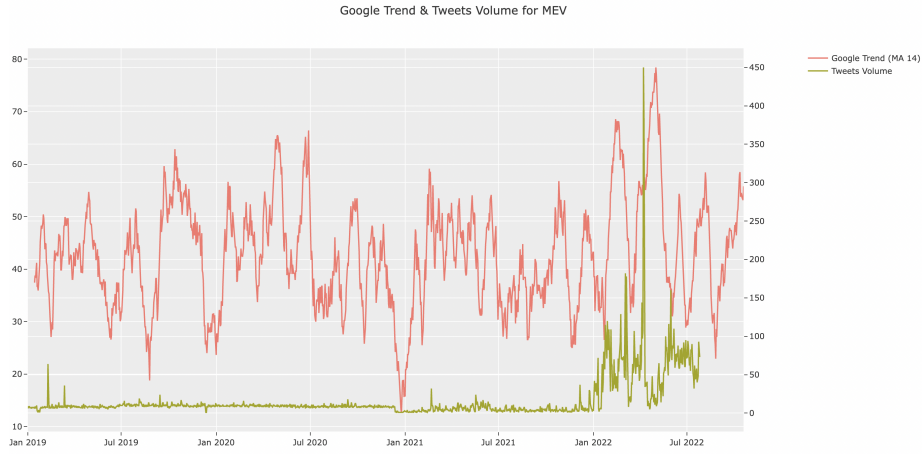


Fig. 7: Time series for Google trend and Twitter volume of #MEV

volume data. We find that After July 2021, the gross profit of MEV remained at a relatively stable and low value when the Twitter volume was at a high level. Thus the high Twitter volume could not be explained by the gross profit in MEV. Instead, We discovered some potential causes from offline events. In the third quarter of 2021, EIP-1559 [10], a proposal to reform the Ethereum fee market, and a new version of Zero-Knowledge Rollups, ZK-rollups [2], regarded as one of the complete solutions to prevent MEV problems, were released. We calculated the frequency of the keywords before and after July of 2021 separately, and we found the frequency of keywords "Solution", "Prevent" and "Attack" after 2021.7 was higher than the time before that time. Thus, the release of ZK-rollups and the new Ethereum transaction mechanism might be the driving force for the high social media appearance of MEV topics.

## 5 Conclusion and Discussion

In conclusion, we apply Natural Language Processing (NLP) methods to comprehensively analyze topics in tweets of MEV. Our results show that the tweets discussed profound topics of ethical concerns including security, equity, emotional sentiments, and the craving for solutions of MEV. We also identify the co-movements of MEV activities on blockchain and on social media platforms. Our study contributes to the literature at the interface of blockchain security, MEV solutions, and AI ethics.

Regarding the different peak times of Google trend and Twitter volume of #Flashbots, we identify connections between the peaks and the new version release in figure 9. We observed that the announcements of every latest version of Flashbots will be released through Twitter. Therefore, the peaks of the Google trend obviously tend to appear right after the peaks of Twitter volume. The

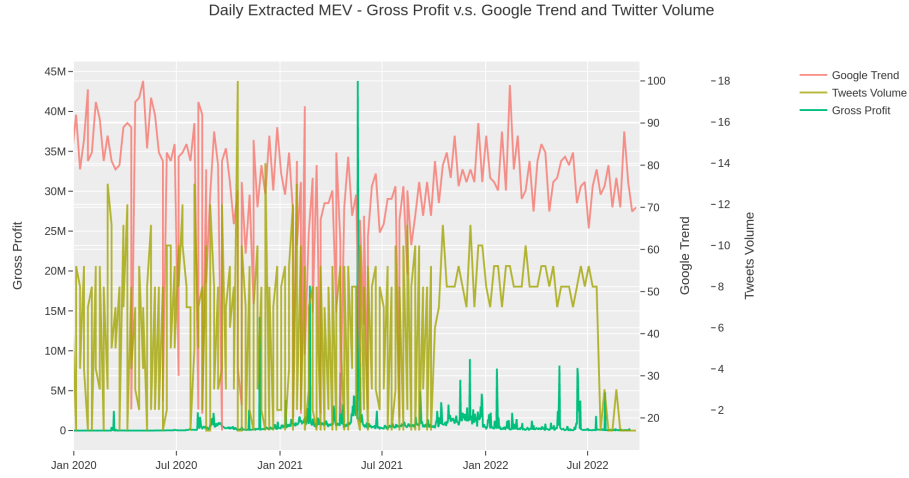


Fig. 8: MEV Gross profit, tweet volume, and Google trend

increases in Google and Twitter trends around the new Flashbots version releases are likely to be from the core teams of Flashbots. Future research could further explore how the discussions of #mev and #flashbots differ between users of different backgrounds and changes upon blockchain mechanism upgrades [28]. For example, how are the topics differ between the core developer team and a broader community of the general public? In the bigrams and the networks in Figure 2, for #MEV, the keywords that appear simultaneously with MEV (or mev), such as **ethereum**, **machinelearning**, and **solution**, indicate that MEV happened more often in Ethereum Blockchain; for #Flashbots, frequent keywords such as **frontrunning** and **sandwich** explain the core problems solved by Flashbots, namely, the sandwich attacks. Further research could study how the topics differ in alternative MEV solutions other than Flashbots.

Table 6 shows the successfully categorized topics by LDA. In #flashbots, the most frequently discussed topics are about some blockchain terminologies and DEXs platforms. Another salient topic under this hashtag expresses people’s emotional and ethical sentiments, such as fairness, trust, gratefulness, expectation, etc. In contrast, the topics under hashtag #MEV show people’s negative concerns about blockchain security issues such as inflation, unfairness, etc. However, existing research points out that the LDA model has a problem with processing sentiment analysis in short text [24]. Therefore, we will consider ameliorating the model in future studies.



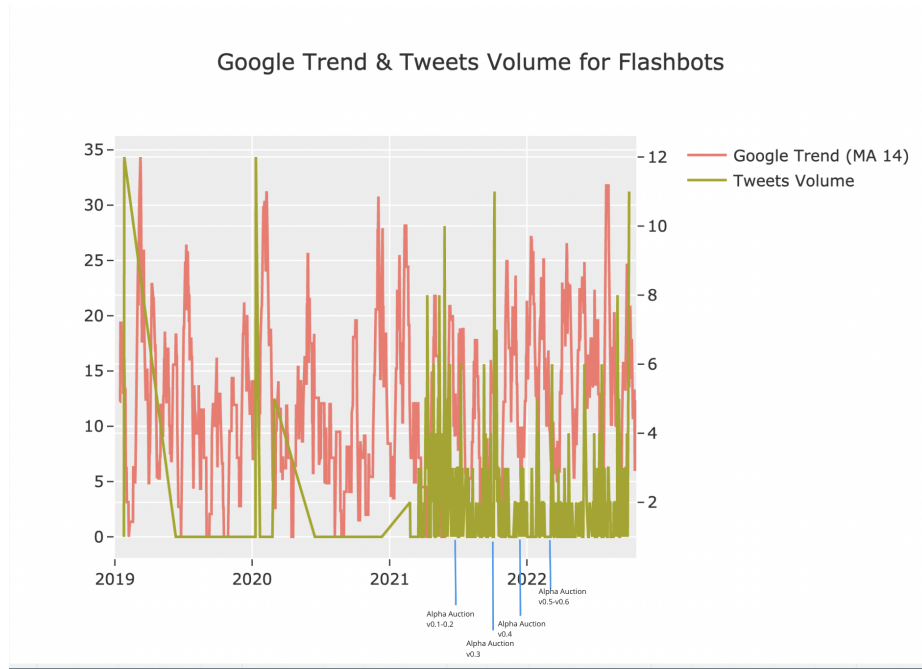


Fig. 9: #Flashbots time-series analysis with landmark events

#MEV	#Flashbots
1 Terminologies	Terminologies
2 Platforms, companies	Platforms, companies
3 Concerns, Worries	Mechanisms, auction, etc.
4 Fairness	Trust, grateful, etc.
5 Complaints	Future, wishes

Table 6: Semantic category of the most salient keywords

## References

1. *Sandwich attack* (2021). <https://www.mev.wiki/attack-examples/sandwich-attack> [Accessed: Whenever]
2. *MEV-resistant ZK-Rollups with Practical VDE (PVDE)* (2022). <https://ethresear.ch/t/mev-resistant-zk-rollups-with-practical-vde-pvde/12677> [Accessed: Whenever]
3. Ao, Z., Horvath, G., Zhang, L.: Are decentralized finance really decentralized? A social network analysis of the Aave protocol on the Ethereum blockchain. arXiv preprint arXiv:2206.08401 (2022). DOI 10.48550/arXiv.2206.08401. URL <https://arxiv.org/abs/2206.08401>
4. Bertino, E., Kundu, A., Sura, Z.: Data transparency with blockchain and ai ethics. *Journal of Data and Information Quality (JDIQ)* **11**(4), 1–8 (2019)
5. Blei, D.M., Ng, A.Y., Jordan, M.I.: Latent dirichlet allocation. *Journal of machine Learning research* **3**(Jan), 993–1022 (2003)
6. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. arXiv:1904.05234 [cs] (2019). URL <https://arxiv.org/abs/1904.05234>
7. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. arXiv:1904.05234 [cs] (2019). URL <https://arxiv.org/abs/1904.05234>
8. Juels, A.: *Fair Sequencing Services: Enabling a Provably Fair DeFi Ecosystem* (2020). <https://blog.chain.link/chainlink-fair-sequencing-services-enabling-a-provably-fair-defi-ecosystem/> [Accessed: Whenever]
9. Kelkar, M., Deb, S., Kannan, S.: Order-fair consensus in the permissionless setting. In: *Proceedings of the 9th ACM on ASIA Public-Key Cryptography Workshop*, pp. 3–14 (2022)
10. Liu, Y., Lu, Y., Nayak, K., Zhang, F., Zhang, L., Zhao, Y.: Empirical analysis of eip-1559: Transaction fees, waiting times, and consensus security. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS '22*, p. 2099–2113. Association for Computing Machinery, New York, NY, USA (2022). DOI 10.1145/3548606.3559341. URL <https://arxiv.org/abs/2305.02552>
11. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* p. 21260 (2008)
12. Network, A.: What’s Automata (IV): Conveyor (2021). URL <https://medium.com/atanetwork/whats-automata-iv-conveyor-93c9335e4f43>
13. Pathik, N., Shukla, P.: Simulated annealing based algorithm for tuning LDA hyper parameters. In: *Soft Computing: Theories and Applications*, pp. 515–521. Springer (2020)
14. Piatt, C., Quesnelle, J., Sheridan, C.: EDEN Network Whitepaper (2021). URL [https://edennetwork.io/EDEN\\_Network\\_\\_\\_Whitepaper\\_\\_\\_2021-07.pdf](https://edennetwork.io/EDEN_Network___Whitepaper___2021-07.pdf)
15. Piet, J., Fairoze, J., Weaver, N.: Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value (2022). DOI 10.48550/arXiv.2203.15930. URL <http://arxiv.org/abs/2203.15930>. ArXiv:2203.15930 [cs]
16. Protocol, C.: CoW Protocol Overview (n.d.). URL <https://docs.cow.fi/>
17. Řehůřek, R., Sojka, P.: Software Framework for Topic Modelling with Large Corpora. In: *Proceedings of the LREC 2010 Workshop on New Challenges for*

- NLP Frameworks, pp. 45–50. ELRA, Valletta, Malta (2010). <http://is.muni.cz/publication/884893/en>
18. Smith, C.: *Maximal extractable value (MeV)* (2022). <https://ethereum.org/en/developers/docs/mev/> [Accessed: Whenever]
  19. Tang, Y., Xiong, J., Becerril-Arreola, R., Iyer, L.: Ethics of blockchain: a framework of technology, applications, impacts, and research directions. *Information Technology & People* (2019)
  20. Tong, X., Li, Y., Li, J., Bei, R., Zhang, L.: What are People Talking about in #BackLivesMatter and #StopAsianHate? *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society* (2022). DOI 10.1145/3514094.3534202
  21. Torres, C.F., Camino, R., et al.: Frontrunner jones and the raiders of the dark forest: An empirical study of frontrunning on the ethereum blockchain. In: *30th USENIX Security Symposium (USENIX Security 21)*, pp. 1343–1359 (2021)
  22. Weintraub, B., Torres, C.F., Nita-Rotaru, C., State, R.: A flash (bot) in the pan: Measuring maximal extractable value in private pools. *arXiv preprint arXiv:2206.04185* (2022)
  23. Wiki, M.: Flashbots (n.d.). URL <https://www.mev.wiki/solutions/faas-or-meva/flashbots>
  24. Wu, D., Yang, R., Shen, C.: Sentiment word co-occurrence and knowledge pair feature extraction based lda short text clustering algorithm. *Journal of Intelligent Information Systems* **56**(1), 1–23 (2021)
  25. Yang, S., Zhang, F., Huang, K., Chen, X., Yang, Y., Zhu, F.: Sok: Mev countermeasures: Theory and practice. *arXiv:2212.05111 [cs]* (2022). URL <https://arxiv.org/abs/2212.05111>
  26. Zhang, L., Ma, X., Liu, Y.: Sok: Blockchain decentralization. *arXiv preprint arXiv:2205.04256* (2022). DOI 10.48550/arXiv.2205.04256. URL <https://arxiv.org/abs/2205.04256>
  27. Zhang, L., Tian, X.: On blockchain we cooperate: An evolutionary game perspective. *arXiv preprint arXiv:2212.05357* (2022). DOI 10.48550/arXiv.2212.05357. URL <https://arxiv.org/abs/2212.05357>
  28. Zhang, L., Zhang, F.: Understand waiting time in transaction fee mechanism: An interdisciplinary perspective. *arXiv preprint arXiv:2305.02552* (2023). DOI 10.48550/arXiv.2305.02552. URL <https://arxiv.org/abs/2305.02552>
  29. Zhang, Y., Chen, Z., Sun, Y., Liu, Y., Zhang, L.: Blockchain network analysis: A comparative study of decentralized banks. *arXiv preprint arXiv:2212.05632* (2022). DOI 10.48550/arXiv.2212.05632. URL <https://arxiv.org/abs/2212.05632>

## A Appendix

Keywords	Definition	Citation
Blockchain	Blockchain is a form of DLT (Distributed Ledger Technology) that stores data in a chain of blocks. Each block needs to be verified, validated, and then chained to another block	[11]
Ethereum	A blockchain platform	<a href="https://ethereum.org/en/developers/docs/intro-to-ethereum/">https://ethereum.org/en/developers/docs/intro-to-ethereum/</a>
DEXs	“Decentralized Exchanges where a smart contract or other forms of peer-to-peer network executes exchange functionality.”	[7]
Consensus Mechanism	“The entire stack of protocols, incentives, and ideas that allow a network of nodes to agree on the state of a blockchain.”	<a href="https://ethereum.org/en/developers/docs/consensus-mechanisms/">https://ethereum.org/en/developers/docs/consensus-mechanisms/</a>
PoW	Proof of Work is the mechanism that once allowed the decentralized Ethereum network to come to a consensus (i.e. all nodes agree) on things like account balances and the order of transactions.	[11]
PoW and Mining	Proof of Stake is the current consensus mechanism of Ethereum Blockchain. Ethereum uses proof-of-stake, where validators explicitly stake capital in the form of ETH into a smart contract on Ethereum.	<a href="https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/">https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/</a>
The Merge	The event that Ethereum decided to change the PoW mechanisms to PoS since the latter is more secure and less resource-intensive	<a href="https://ethereum.org/en/upgrades/merge/">https://ethereum.org/en/upgrades/merge/</a>

Table 7: The glossary table