BLOCKCHAIN SECURITY: CATEGORIZATION AND QUANTIFICATION OF MINER EXTRACTABLE VALUE

by

HAOXIN_YU

Signature Work Product, in partial fulfillment of the Duke Kunshan University Undergraduate Degree Program

April 14, 2022

Signature Work Program

Duke Kunshan University

APPROVALS

_____

Mentor: Luyao Zhang, Assistant Professor of Economics, Social Science Division

Senior Research Scientist, Data Science Research Center

_____

Marcia B. France, Dean of Undergraduate Studies

ABSTRACT

Financial services have benefited from Blockchains and Decentralized Finance (DeFi). However, opportunistic traders use the so-called Miner Extractable Value (MEV) to extract monetary value from the mesh of DeFi smart contracts, raising quantifiable, proof-of-work-based security issues, which pose threats to the Ethereum blockchain. Quantitative insights on MEV were often lacking in a related study, making it difficult to quantify the practical dangers. Furthermore, earlier studies only focused on limited DEXes. Our study looks at how the arbitrage trading category has manifested in real-world applications. We also estimate the MEV that occurred because of arbitrage trading from the searcher and miner perspectives. We extended our discovered application scenario to a greater range of decentralized exchanges than in the previous study, including Uniswap v2, Uniswap v3, Curve, Balancer, Bancor, and 0x. There are 125 different users (account) addresses and 1969 smart contracts executing 25834 arbitrages between blocks 12965000 and 13000000, resulting in a profit of 1.132M USD. Furthermore, a high percentage of successful arbitrage transactions are found at the end of the blocks. Arbitrages relevant to Uniswap V2 accounted for the majority of all arbitrage transactions, with a large portion involving two or three markets.

ACKNOWLEDGEMENTS

I especially thank professor Luyao Zhang for her mentorship, whose expertise was invaluable in guiding and suggesting creating and polishing the SW products. Additionally, I would like to thank professor Fan Zhang for his suggestions on my previous results, methods, and expertise in MEV and order fairness. Moreover, I would like to thank my fellow scholar Ziliang Tian for sharing useful literature sources, insightful discussion, and feedback. I am also grateful for the technical support received from Xin Ma, a member of Duke Kunshan University's IT Office, and Zesen Zhuang, a Junior Student at Duke Kunshan University. It is also worth mentioning that the early research that led to my final SW research direction was supported by the Undergraduate Research Fund at the Center for the Study of Contemporary China (CSCC), Duke Kunshan University.

TABLE OF CONTENTS

ABSTRACT (ENGLISH) III

ABSTRACT (CHINESE) III

ACKNOWLEDGEMENTS IV

TABLE OF CONTENTS V

LIST OF TABLES VI

TABLE OF FIGURES VI

INTRODUCTION 1

MATERIAL AND METHODS 4

1. Data Descriptor *4*
2. Methodology: *5*

RESULTS 8

1. Data Dictionary Tables: *8*
2. Data Statistics (Table: Mean, Count, Std., ...) *13*
3. Data Analysis Results *16*

DISCUSSION 18

CONCLUSIONS 21

REFERENCES 22

APPENDICES 25

LIST OF TABLES

Table 1 Token Prices Information Data 8
Table 2 Ethereum Blocks Information Data 9
Table 3 MEV Arbitrage Transaction Information Data 10
Table 4 Transaction Miner Payments Information Data 11
Table 5 Token Swap Information Data 12
Table 6 Arbitrage Trading Information Statistics 13
Table 7 Transaction Miner Payments Information Statistics 14
Table 8 Token Prices Information Data Statistics 15
Table 9 Token Swap Information Data Statistics 15
Table 10 Markets and Platforms 16

TABLE OF FIGURES

Figure 1 Data Acquisition and Processing 5
Figure 2 Arbitrage Transaction Position 17
Figure 3 Arbitrages trading Total Amount 17
Figure 4 Arbitrages trading Amount by Protocols 18
Figure 5 Gross profits and MEV value 18

INTRODUCTION

According to the background of blockchain trilemma, termed by Vitalik Buterin, it addresses the challenges developers face in creating a scalable, decentralized, and secure blockchain without compromising on any facet. As the properties and the underlying formal foundations of blockchain technologies are still under debate, in practical terms, new blockchains with security and privacy claims seem to be coming out increasingly rapidly (Halpin and Piekarska 2017). Since the consensus algorithm plays a crucial role in maintaining the efficiency of blockchain and is highly connected with the performance of a blockchain application, we mainly focused on consensus security, specifically on the security issues related to the proof of work algorithm. One reason is that Proof of Work (PoW) powered blockchains currently account for more than 90% of the total market capitalization of the existing digital currencies, and another reason is that there exists an increasing trend in examining the risks and attacks relevant to the proof-of-work based blockchains (Gervais et al. 2016). Among those risks, as Miner Extractable Value (MEV) was first introduced, it was said to have posed concrete, measurable, consensus-layer security risks and generated a realistic threat to the Ethereum blockchain (Daian et al. 2020). Therefore, my research question is about how to measure blockchain security, specifically focusing on the categorization and quantification of MEV risk.

In the financial system, we now use Decentralized Finance (DeFi) to describe an organization consisting of protocols and financial products (Babel et al., 2021). Smart contracts, processing on blockchains, characterize these products. Generally, a blockchain is a chain of blocks with sustained growth in which the transaction records are recognized and connected (Treleaven, Gendal Brown, and Yang 2017). As for the principles, the typical consensus algorithms of blockchain incorporate proof of stake (PoS) and proof of work (PoW). Even more to the point, the proof of work algorithm has posed thorny problems such as high electricity consumption resulting from mining activities, out of scalability caused by fixed block size, and MEV risk (Harvey, Ramachandran, and Santoro 2020). The smart contract can be considered a significant development (Deloitte 2019). The concept of a smart contract was first proposed as a transaction agreement that enforces the terms of a contract, which is computerized (Szabo 1996).

Furthermore, it intimately bounds up with DeFi. DeFi can utilize smart contracts to produce protocols more transparently, and thus much more value has been trapped in smart contracts (Schär 2021). For example, the Ethereum DeFi space will possess about 80 billion US dollars as locked capital in smart contracts by August 2021 (DeFiPulse 2021). Moreover, DeFi techniques or protocols have been widely used among various user types, allowing users to complete asset transactions, lending, borrowing, and exchanging on the blockchain (Zheng et al. 2020).

Within the transaction process, DeFi traders can utilize the unalterable smart contracts that encode rules through which, for example, the automated market maker (AMM) operates (Uniswap 2020). The transactions in a certain block are executed in the order in which the miners of respective blocks contain them. In addition, the miners have the power to manage the sequence that which a transaction is executed (Werner et al. 2021). With this powerful control from the miners, a concept called Miner-extractable value (MEV) is drawing increasing attention. MEV was originally defined as a value that miners can generate directly from smart contracts as cryptocurrency profits and transaction fees (Daian et al. 2019). It is utilized to measure the degree to which miners can extract the value from the DeFi application users through sequencing of transactions or game strategies. However, MEV can be regarded as a potential risk to blockchain economies. For example, Daian et al. (2020) proved that a source of MEV, called ordering optimization (OO) fees, poses a realistic threat to Ethereum and causes systemic consensus-layer vulnerabilities.

Moreover, Angeris et al. (2021) argued that the MEV is particular to blockchains, which cannot be eliminated purely by cryptographic means. Not just miners, blockchain users, or traders, also tend to maximize obtained financial revenue through ongoing market participation (Qin, Zhou, and Gervais 2021). For example, non-mining traders can also extract value by adjusting, such as transaction fees, to make extra profits.

Miners have the most authority over transaction inclusion and ordering on Ethereum today before advancing to proof-of-stake consensus because they are the block makers. As Daian et al. (2020) introduced, MEV was originally defined as the value that may be extracted directly from smart contracts as bitcoin profits by miners, as discussed by and his colleagues in their article "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in

Decentralized Exchanges." MEV, on the other hand, occurs on all smart contract blockchains where a party is responsible for transaction ordering, such as validators in ETH2.0 and rollup providers in Optimistic Rollups. Therefore, the research and development organization Flashbots renamed MEV as a maximal extractable value, broadening the scope to cover other blockchain architectures while still being 'backward compatible' with its initial name. As previously stated, non-mining DeFi dealers and bot operators have been the primary drivers of MEV extraction on Ethereum thus far.

Through previous research on MEV, Daian et al. (2020) proposed the concept of MEV, and the categories of MEV were identified. They regarded different forms of MEV as novel risks on DeFi, and classified MEV into three categories, including Successful MEV extraction, Reversed MEV extraction, and Checked MEV extraction. However, their research in this section merely rested on the theoretical level. After Daian and his colleagues empirically proposed the statement that MEV was a potential threat to the Ethereum blockchain, related work was generally missing quantitative insights on the past MEV extraction to assess the practical risks (Qin, Zhou, and Gervais 2021).

Qin, Zhou, and Gervais (2021) published the paper "Quantifying Blockchain Extractable Value: How dark is the forest?", in which they extended the concept of MEV to BEV (blockchain extractable value), which represents that opportunistic traders extract monetary value from the mesh of decentralized finance (DeFi) smart contracts. Their work aimed to quantify the BEV risk by deriving the USD value extracted from sandwich attacks, liquidations, and arbitrages. In addition, they also formulated an original algorithm that can replay transactions, to mimic an aggrieved transaction and calculate its potential extractable value. However, they mainly focused on limited DEXes such as Uniswap, sushiswap, and linch.

In the proposed research, we will explore how the arbitrage trading category was manifested in practical applications, specifically in virtue of the transaction data recorded on Etherscan. The arbitrage revenue strategy was the most commonly seen strategy of MEV extraction, and it took the largest proportion of extracted MEV value previously. Additionally, there was almost no research on arbitrage in the Decentralized Exchanges (Boonpeam, Werapun, and Karode 2021). Considering these reasons and inspired by the previous work, we aim to quantify the MEV that

happened through arbitrage trading from both the searcher's and the miner's views. Compared to the previous study, we extended our application scenario to a larger number of decentralized exchanges, including Uniswap v2, Uniswap v3, Curve, Balancer, Bancor, 0x.

MATERIAL AND METHODS

1. Data Descriptor

(1) Introduction

As for the MEV Layer 2 data used in our proposed research, there is no readily available dataset. However, we could find all the required data on the Etherscan Platform. In order to query the data, we used the mev-inspect-py, an open-source tool designed for identifying MEV transactions, inspecting corresponding victim blocks, and querying relevant data (Flashbots 2022).

The previous researchers mainly focused on examining MEV extraction that happened on the blocks created relatively early. Additionally, as part of their research on quantifying MEV, most of them inspected specific Decentralized Exchanges (DEXes), such as Uniswap V1/2/3, Sushiswap, Swerve, linch, etc.

Hence, the data source we will be employing for our research concentrates on the higher-numbered blocks and other types of DEXes, including Curve, Balancer, 0x, etc. The queried data can be summarized into 11 Metatables introduced in the following sections. We will mainly pick 5 of them and make adjustments correspondingly to finalize the data tables we will use for analysis.

(2) Data Acquisition and Data Cleaning

The data acquisition and data preprocessing process are shown below:

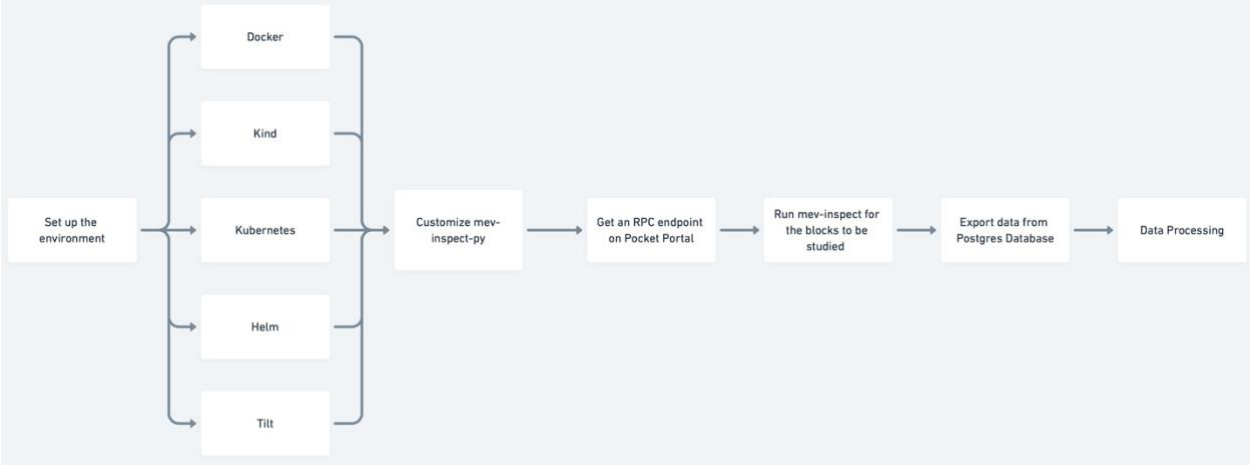


Figure 1 Data Acquisition and Processing

We have two data sources which are Google BigQuery and Etherscan. Moreover, we mainly used mev-inspect-py and Kaggle for data querying.

(4) Environment Set Up

To use the inspecting tool developed by a research organization Flashbots (Obadia 2021), we need to first set up the required environments[1].

2. Methodology:

1) Arbitrage Trading Categorization:

We use the following conditions to detect corresponding extracted arbitrage trading on Ethereum Blockchain. Generally, we took the heuristics introduced by Qin, Zhou, and Gervais (2021) in their paper "Quantifying Blockchain Extractable Value: How dark is the forest?" as references. In addition, we made certain adjustments corresponding to the architecture of the MEV inspecting tool (mev-inspect-py) developed by Flashbots. With these conditions and the tool mev-inspect-py, we can detect and extract only arbitrage trading

[1] Detailed instruction of setting up the environment: https://www.notion.so/Data-Descriptor-68535c3913634eee8a59c927d5762444#20ded40d23874c7b995e5acd299253e1

through a bulk of transactions, specifically those relevant to six decentralized exchanges, including Uniswap v2, Uniswap v3, Curve, Balancer, Bancor, 0x.

Conditions:

(1) Within an arbitrage, all token swap actions should occur in one transaction, implicitly assuming that the arbitrageur uses atomic arbitrage to minimize risk.

(2) There must be more than one token swap action within one arbitrage trading.

(3) An arbitrage's n swap activities s_1,... s_n must form a loop. Any swap action's input asset must be the same as the prior action's output asset, i.e. IN(s_i) = OUT(s_{i1}). The input asset for the first swap must be the same as the output asset for the last swap activity, i.e., IN(s_0) = OUT (s_n).

(4) The output amount of the previous action must be larger than or equal to the input amount of the corresponding swap action, i.e., in(s_i) $\leqslant$ out(s_{i-1}).

Arbitrage tradings mainly represent the process that which the traders initiatively buy and sell the assets in different trading markets to generate profits with the price differences in different markets (Qin, Zhou, and Gervais 2021). To define and inspect arbitrage trading with the historical transaction data, we regard it as an Ethereum transaction executing swaps where the starting balance is inferior to the ending balance. If the two balances are in different assets, we convert both in absolute ETH terms using Uniswap market prices.

As for our methodologies, there are some premises and illustrations that are applied:

(1) With the methods that we utilized, we can only detect historical Arbitrage MEV extraction on Ethereum Blockchain. Therefore, the MEV that we finally quantified only reflects the extracted MEV but not the potential MEV opportunities that may appear in the Mempool, i.e., in the pending transactions. Additionally, other arbitrage MEV opportunities might exist in the historical transactions, but no one found them or utilized them. As for these potential MEV extraction opportunities, we did not include them in our data analysis.

(2) According to the previous research on MEV quantification, they mainly used USD as the profit unit. Furthermore, most of them normalized the token prices from ETH to USD with the minute ETH price. However, in the proposed research, we utilized a more reasonable algorithm introduced by Flashbots (2021), which used per block's ETH price by averaging over the ETH-DAI, ETH-USDT, and ETH-USDC prices provided by Uniswap V2's oracle.

2) MEV transaction Inspection (tool: mev-inspect-py):

During the previous research, they did not include the data of pending transactions in the mempool but instead collected the data of transactions that were already completed. FFlashbots is a research and development organization focused on reducing the negative externalities of existing Miner (Maximal) Extractable Value extraction approaches and avoiding the existential threats MEV poses to state-rich blockchains like Ethereum (Flashbots 2021). They developed a tool, "mev-inspect-py," used to detect MEV transactions from the collected transaction data. For example, we can use it to find miner payments (gas + coinbase), token transfers and profit, swaps, and arbitrages.

Like using Python on Anaconda, we can run this tool locally on Kubernetes. After setting up the environment with Docker and Kind, we can select a block to be inspected and connected to the Postgres database to see the data inspection found in that block.

To examine each MEV transaction in this block, we can find, for example, certain arbitrage by querying the arbitrage table. Additionally, the user address that is about to extract MEV can be identified, and the profit amount of tokens can be calculated by getting the start amount and the end amount. The value of this amount of token at the time is regarded as the reward for executing the smart contract. During the process, we can learn the swaps involved in arbitrage and identify the trades performed on which DeFi applications.

To quantify the total MEV, we should also examine the miner payment, in other words, how much was paid to the miners for victim transactions using the same transaction hash. Within this process, we can get the gas price (The gas price is the value that is paid directly as gas), the coinbase transfer (The amount of ETH that is paid directly as a transfer to the miner's address),

and the total gas price (the gas price including the original gas price and the coinbase transfer gas price).

3) Data Analysis

With the collected data, we examined the following aspects of detected arbitrage trading and extracted MEV throughout the process:

(1) User Addresses & Smart Contracts

(2) Markets and Platforms

(3) Arbitrage Transaction Position

(4) Arbitrages Trading amount

(5) Gross profits and MEV value

The following are the mathematical formulas used for determining the traders' gross profit, direct payments to miners, and the overall extracted MEV value:

$$gross_{profit} = profit\_amount * USD\_price\ of\ the\ profit\ token\ /\ 10^{18}$$

$$miner_{payment} = [(gas\_used * gas\_price) + coinbase\_transfer] * USD\_price\ of\ the\ profit\ token\ /\ 10^{18}$$

$$MEV = gross\_profit - miner\_payment$$

RESULTS

1. Data Dictionary Tables:

Table 1 Token Prices Information Data

Column	Type	Description
timestamp	timestamp without the time zone	when the price happened

usd_price	numeric	the USD price of the gross profit
token_address	character varying(256)	the address of the token

Table 2 Ethereum Blocks Information Data

Column	Type	Description
block_number	numeric	block number
block_timestamp	timestamp without time zone	when the block was created
transaction_count	numeric	the transaction amount in the block

Table 3 MEV Arbitrage Transaction Information Data

Column	Type	Description
id	character varying(256)	unique id
created_at	timestamp without time zone	when the entry was added to the database
block_number	numeric	block number
transaction_hash	character varying(256)	transaction hash
account_address	character varying(256)	address that took the profit of the arb - can be a contract or an EOA
profit_token_address	character varying(256)	token that profit was taken in
profit_amount	numeric	gross profit - note: this does not account for miner payment
start_amount	numeric	starting amount of the profit token
end_amount	numeric	end amount of the profit token
protocols	character varying(256)	protocols associated with the arbitrage

Table 4 Transaction Miner Payments Information Data

Column	Type	Description
created_at	timestamp without time zone	when the entry was added to the database
block_number	numeric	block number
transaction_hash	character varying(66)	transaction hash
transaction_index	numeric	transaction index
miner_address	character varying(256)	address of the miner
coinbase_transfer	numeric	amount of ETH was paid as direct transfer to the miner
base_fee_per_gas	numeric	base fee for this block
gas_price	numeric	gas price (excludes coinbase transfer)
gas_price_with_coinbase_transfer	numeric	gas price (includes coinbase transfer)
gas_used	numeric	total gas used by the transaction

Column	Type	Description
transaction_to_address	character varying(256)	to address of the transaction
transaction_from_address	character varying(256)	from address of the transaction

Table 5 Token Swap Information Data

Column	Type	Description
created_at	timestamp without time zone	when the entry was added to the database
block_number	numeric	block number
transaction_hash	character varying(66)	transaction hash
trace_address	integer[]	trace address
abi_name	character varying(1024)	name of the ABI used to decode the swap
contract_address	character varying(256)	contract address
from_address	character varying(256)	address where tokens are coming from
to_address	character varying(256)	address where swapped tokens are going to

token_in_address	character varying(256)	address of the token going in
token_in_amount	numeric	amount of the token going in
token_out_address	character varying(256)	address of the token going out
token_out_amount	numeric	amount of the token going out
protocol	character varying(256)	protocol
error	character varying(256)	error
transaction_position	numeric	the position of a transaction

2. Data Statistics (Table: Mean, Count, Std., ...)

Table 6 Arbitrage Trading Information Statistics

	block_number	**start_amount**	**end_amount**	**profit_amount**
count	25834	25834	25834	25834
mean	12982650	4.964018e+23	4.96823e+23	421200800000000000000
std	9907.532	3.863547e+25	3.864236e+25	6.767717e+22

min	12965000	10030	25088	-1.20682e+23
25%	12974250	438294600000000000	456633100000000000	10286810000000000
50%	12982870	1025106000000000000	1048627000000000000	16443660000000000
75%	12990910	2861126000000000000	2908707000000000000	33618330000000000
max	13000000	5.421753e+27	5.421753e+27	1.087602e+25

Table 7 Transaction Miner Payments Information Statistics

	block_number	**transaction_index**	**base_fee_per_gas**	**gas_price**	**gas_price_with_coinbase_transfer**	**gas_used**
count	25834	25834	25834	25834	25834	25834
mean	12982650	47.071534	42937410000	92253130000	197617000000	208061.4
std	9907.532	88.246778	17115390000	220376100000	2357582000000	72416.68
min	12965000	0	1124968000	1423420000	1423420000	110215
25%	12974250	1	32277610000	37572260000	43203700000	151142
50%	12982870	3	39601960000	49128130000	58586100000	196168
75%	12990910	51	49441930000	71000000000	96841710000	240699

max	13000000	970	706750800000	6661693000000	282893600000000	1367098

Table 8 Token Prices Information Data Statistics

	usd_price
count	14967.000000
mean	3192.155274
std	10005.873811
min	0.013479
25%	0.879017
50%	13.649759
75%	384.211108
max	82070.757519

Table 9 Token Swap Information Data Statistics

	block_number	**token_in_amount**	**token_out_amount**	**transaction_position**
count	8.390150e+05	8.390150e+05	8.390150e+05	839015.000000

mean	1.298230e+07	4.924633e+28	3.135236e+28	129.985713
std	1.000367e+04	1.038915e+31	5.724562e+30	111.025829
min	1.296500e+07	1.000000e+00	0.000000e+00	0
25%	1.297367e+07	3.045215e+16	5.515213e+16	35.000000
50%	1.298221e+07	7.424881e+17	1.592861e+18	111.000000
75%	1.299076e+07	1.200000e+20	3.792379e+20	202.000000
max	1.300000e+07	4.964267e+33	4.120927e+33	1361.000000

3. Data Analysis Results

Table 10 Markets and Platforms

/ Platforms Markets /	1	2	>= 3	Total
2	207 (0.8%)	10591 (41%)	None	10799 (41.8%)
3	6975 (27%)	5683 (22%)	413 (1.6%)	13072 (50.6%)
>= 4	1033 (4%)	775 (3%)	155 (0.6%)	1963 (7.6%)

Total	8215 (31.8%)	17049 (66%)	568 (2.2%)	25834 (100%)

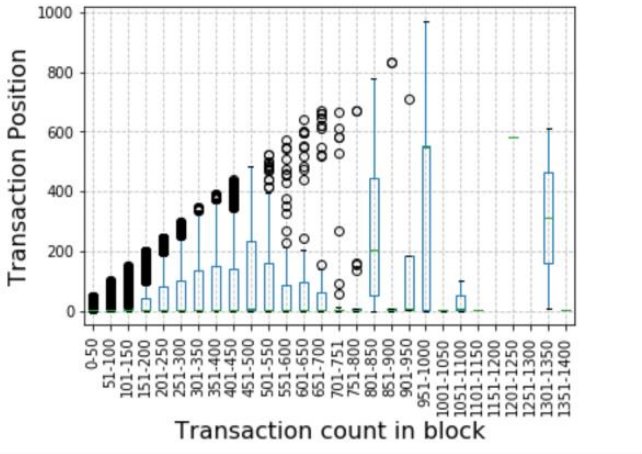


Figure 2 Arbitrage Transaction Position

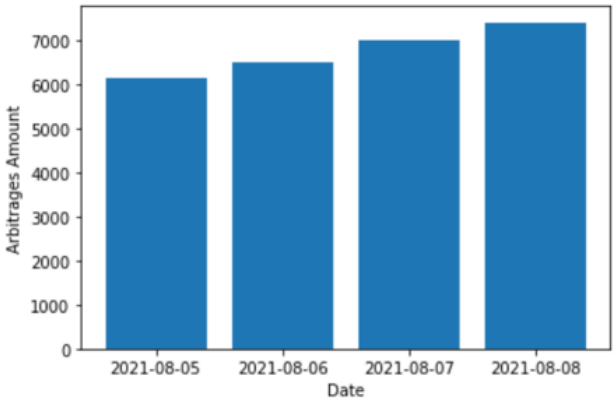


Figure 3 Arbitrages trading Total Amount

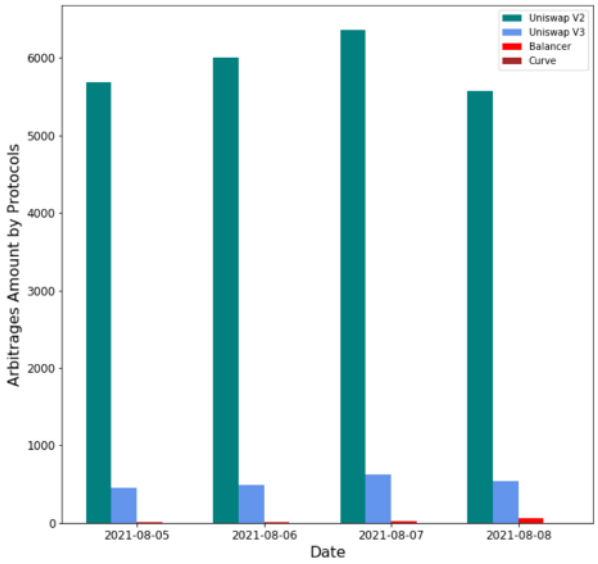


Figure 4 Arbitrages trading Amount by Protocols

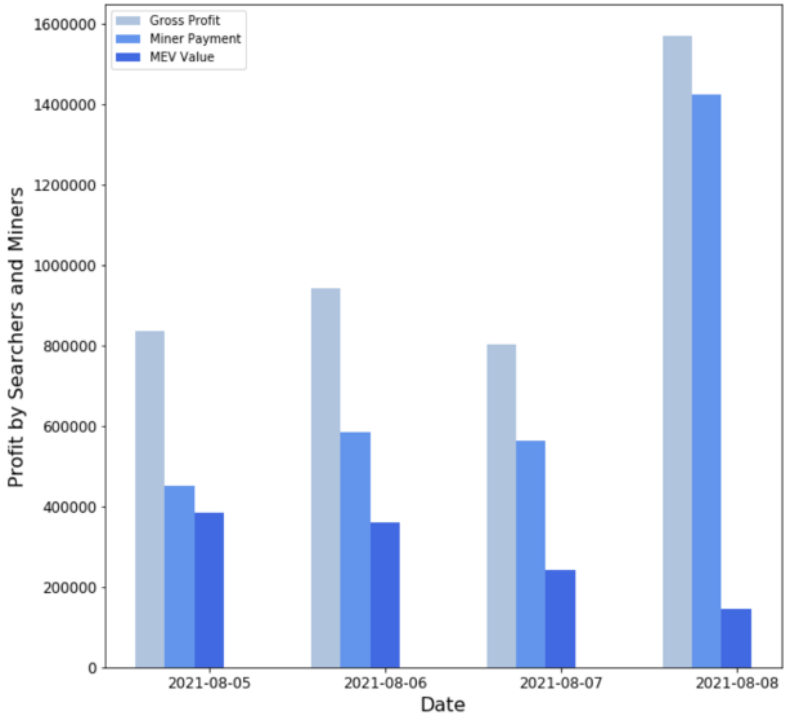


Figure 5 Gross profits and MEV value

DISCUSSION

1. Data Summary and Statistics

We summarized our required data into five data tables, including arbitrages, miner_payments, prices, blocks, swaps:

(1) The arbitrages table has a data amount of 25384, which records the arbitrages attack that happened on the Ethereum blockchain from block 12965000 to block 13000000.

(2) The miner_payments table has a data amount of 25384, which records the information of total gas fees and tokens that went directly to miners through the arbitrage MEV summarized in the arbitrages table.

(3) The prices table has a data amount of 14967, which summarizes the USD price information of the profit tokens on each specific day. Additionally, the blocks that we examined are all within the time range.

(4) The swaps table has the largest data amount of 839015 since it records every swap that happened in each detected arbitrage transaction (several swaps might happen within a single transaction).

We combine the data from these tables to calculate the overall extracted MEV and visualize by categories.

2. User Addresses, Smart Contracts

   From block 12965000 to 13000000 (5th of August, 2021 - 8th of August, 2021), we find 125 distinct users (account) addresses and 1969 smart contracts executing 25834 arbitrages trades on Uniswap V2, Uniswap V3, Balancer, Curve, resulting in a profit of 1.132M USD. Based on our findings, 7612 arbitrage transactions (29.5%) were communicated to miners on a private basis. Additionally, all inspected arbitrage transactions are executed using smart contracts.

3. Markets and Platforms

   To gain more insights on arbitrage, we looked into the markets and platforms involved in the transactions. Table 10 shows that most traders or searchers choose simple arbitrage

trading techniques involving two or three marketplaces (two-point arbitrage and triangular arbitrage). Only about 5% of traders used equal to or more than four markets to conduct their arbitrage. We also discovered that certain transactions combine two arbitrage opportunities into one. These behaviors may provide a bigger return because the gas price is lower. They are riskier, though, because the more markets they are involved in, the more competitors they will have to outrun. WETH, USDC, and USDT are all implicated in more than 90% of the arbitrages we found.

4. Arbitrage Transaction Position

   Figure 2 shows that a high percentage of profitable arbitrage transactions are surprisingly located at the end of the blocks when displaying the arbitrage transaction positions in blocks. We would anticipate the arbitrage transactions to be competitive and execute harmful front-running with increased gas prices. For example, out of 851 transactions in this block, one of the most profitable arbitrages deals we observed was at index 832.

5. Arbitrages Trading Amount

   In Figures 3 and 4, by visualizing arbitrage trading amounts in total and by protocols, we find that based on the data we have collected, we can see an increasing trend in total arbitrage amounts along with the time series, which is consistent with the previous research. Additionally, we found that the arbitrages relevant to Uniswap V2 took the largest proportion of all arbitrage transactions, and the amount is much higher than that related to other DEXes.

6. Gross Profits and MEV value

   In Figure 5, to gain more insights on the overall MEV value, we calculated the gross profits, which represent the revenue that traders expected to generate by synchronizing the prices of assets on several different markets, and the miner payment that miners received through paid gas and direct coinbase transfer from the traders. We can see a descending trend in the MEV profit and the time series, which is surprisingly contrary to the ascending trend in the total arbitrage amounts.

CONCLUSIONS

With the development of the sustainability concept, there are numerous studies on sustainability risks from institutions and enterprises, such as the research on ESG risks. Furthermore, risk management is a significant segment in sustaining growth rather than speculation for the blockchain economy. The proposed research provides references on DeFi risks and examination of MEV on the proof-of-work blockchain, taking Ethereum blockchain as a typical example.

The approach in the proposed research has an extension compared to the previous research. Based on the previous studies, we further investigate the actual application scenarios of defined categories of MEV. Additionally, we adopt a similar method of quantifying MEV on DeFi applications different from the previously examined Decentralized Exchanges (DEXes). With the algorithms we used, we can detect the arbitrage trading relevant to certain decentralized exchanges, including Uniswap v2, Uniswap v3, Curve, Balancer, Bancor, 0x. However, within the block range, we have examined, we only find those related to Uniswap v2, Uniswap v3, Curve, and Balancer. We may extend the range of blocks and certain periods when going through striking changes in future research.

Furthermore, our research mainly examines the transactions running on the Ethereum blockchain, utilizing the proposed methods to identify the arbitrage transactions that fit our purpose and correspond to the data. In future research, the researchers can further investigate the transactions based on other blockchains or explore how miners and traders extract value from the DeFi applications other than the ones we have studied. In addition, they could further examine the MEV extraction that happened with other types of trading strategies, such as sandwich attacks, liquidations, and NFT trades.

Although blockchain has brought users benefits such as data transparency and decentralized trading platforms, many people still do not adopt it due to unexpected risks, implying the significance of the lucid and quantified assessment of those risks. The proposed research could help illustrate the novel term MEV with real-world examples and application scenarios. Furthermore, it can support stakeholders and investors in choosing low-risk products and assist

developers in managing their products' risks. In addition, such findings could help assess the risks under different regulations from various regions to determine the enforceability of the transactions.

REFERENCES

Angelis, Stefano De. 2016. “FACULTY of INFORMATION ENGINEERING, COMPUTER SCIENCE and STATISTICS DEPARTMENT of COMPUTER, CONTROL and MANAGEMENT ENGINEERING Assessing Security and Performances of Consensus Algorithms for Permissioned Blockchains.” https://arxiv.org/pdf/1805.03490.pdf.

Angeris, Guillermo, Alex Evans, and Tarun Chitra. 2021. “A Note on Bundle Profit Maximization.” https://web.stanford.edu/~guillean/papers/flashbots-mev.pdf.

Aspris, Angelo, Sean Foley, Jiri Svec, and Leqi Wang. 2020. “Decentralized Exchanges: The ‘Wild West’ of Cryptocurrency Trading.” SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3717330.

Babel, Kushal, Philip Daian, Mahimna Kelkar, and Ari Juels. 2021. “Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts.” https://arxiv.org/pdf/2109.04347.pdf.

Boonpeam, Naratorn, Warodom Werapun, and Tanakorn Karode. 2021. “The Arbitrage System on Decentralized Exchanges.” https://www.computing.psu.ac.th/profile/backend/upload/992321922.79911.pdf.

Businesswire. 2020. “RepRisk Launches New Version of Its ESG Risk Platform.” Www.businesswire.com. March 17, 2020. https://www.businesswire.com/news/home/20200317005044/en/RepRisk-Launches-New-Version-of-its-ESG-Risk-Platform.

CFA Institute. 2020. “ESG Investing and Analysis.” CFA Institute. 2020. https://www.cfainstitute.org/en/research/esg-investing.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2019. “Flash Boys 2.0: Frontrunning, Transaction

Reordering, and Consensus Instability in Decentralized Exchanges." https://arxiv.org/pdf/1904.05234.pdf.

———. 2020. "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability." IEEE Xplore. May 1, 2020. https://doi.org/10.1109/SP40000.2020.00040.

DeFiPulse. 2019. "DeFi Pulse | the DeFi Leaderboard | Stats, Charts and Guides." Defipulse.com. 2019. https://defipulse.com/.

Deloitte. 2019. "Upgrading Blockchains." Deloitte Insights. 2019. https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html.

Dybvig, Philip H., and Stephen A. Ross. 1989. "Arbitrage." Finance, 57–71. https://doi.org/10.1007/978-1-349-20213-3_4.

Flashbots. 2022. "Mev-Inspect-Py." GitHub. March 1, 2022. https://github.com/flashbots/mev-inspect-py.

Forkast.news. 2021. "Could Ethereum's Upgrade Affect Miners' MEV Manipulations?" Forkast.news. 2021. https://forkast.news/how-will-ethereums-upgrade-affect-miners-mev/.

Gervais, Arthur, Ghassan Karame, Karl Wüst, Eth Zurich, Switzerland, Vasileios Glykantzis, Hubert Ritzdorf, Srdjaň Capkun, Eth Switzerland, and Zurich. 2016. "On the Security and Performance of Proof of Work Blockchains." https://eprint.iacr.org/2016/555.pdf.

Halpin, Harry, and Marta Piekarska. 2017. "Introduction to Security and Privacy on the Blockchain." 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), April. https://doi.org/10.1109/eurospw.2017.43.

Harvey, Campbell R., Ashwin Ramachandran, and Joseph Santoro. 2020. "DeFi and the Future of Finance." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3711777.

Makarov, Igor, and Antoinette Schoar. 2019. "Trading and Arbitrage in Cryptocurrency Markets." Journal of Financial Economics 135 (2). https://doi.org/10.1016/j.jfineco.2019.07.001.

Mingxiao, Du, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. 2017. "A Review on Consensus Algorithm of Blockchain." https://blockhack.osive.com/_downloads/33a65d87de38eaf5b8d817681a3e4674/7.pdf.

Obadia, Alex. 2021. “Quantifying MEV: Introducing MEV-Explore V0.” Flashbots. February 24, 2021. https://medium.com/flashbots/quantifying-mev-introducing-mev-explore-v0-5ccbee0f6d02.

Qin, Kaihua, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. 2021. “An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities.” Proceedings of the 21st ACM Internet Measurement Conference, November, 336–50. https://doi.org/10.1145/3487552.3487811.

Qin, Kaihua, Liyi Zhou, and Arthur Gervais. 2021. “Quantifying Blockchain Extractable Value: How Dark Is the Forest?” https://arxiv.org/pdf/2101.05511.pdf.

Rahouti, Mohamed, Kaiqi Xiong, and Nasir Ghani. 2018. “Bitcoin Concepts, Threats, and Machine-Learning Security Solutions.” IEEE Access 6: 67189–205. https://doi.org/10.1109/access.2018.2874539.

RepRisk. 2021. “RepRisk Methodology Overview II. Research Approach and Scope.” https://www.reprisk.com/content/static/reprisk-methodology-overview.pdf.

Schär, Fabian. 2021. “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.” Papers.ssrn.com. Rochester, NY. April 1, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3843844.

Szabo, Nick. 1996. “Nick Szabo -- Smart Contracts: Building Blocks for Digital Markets.” Hum.uva.nl. 1996. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Treleaven, Philip, Richard Gendal Brown, and Danny Yang. 2017. “Blockchain Technology in Finance.” Computer 50 (9): 14–17. https://doi.org/10.1109/mc.2017.3571047.

Uniswap. 2020. “Home | Uniswap Protocol.” Uniswap Protocol. 2020. https://uniswap.org/.

Wang, Bin, Han Liu, Chao Liu, Zhiqiang Yang, Qian Ren, Huixuan Zheng, and Hong Lei. 2021. “BLOCKEYE: Hunting for DeFi Attacks on Blockchain.” IEEE Xplore. May 1, 2021. https://doi.org/10.1109/ICSE-Companion52605.2021.00025.

Werner, Sam, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William Knottenbelt. 2021. “SoK: Decentralized Finance (DeFi).” https://arxiv.org/pdf/2101.08778.pdf.

Xu, Jiahua, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. 2021. "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols." ArXiv:2103.12732 [Cs, Q-Fin], October. https://arxiv.org/abs/2103.12732.

Yu, Haoxin. 2021. "On the Mechanics of Sustainability: ESG Rating and Company Performance." Papers.ssrn.com. Rochester, NY. July 10, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899898.

Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. 2020. "An Overview on Smart Contracts: Challenges, Advances and Platforms." Future Generation Computer Systems 105 (April): 475–91. https://doi.org/10.1016/j.future.2019.12.019.

APPENDICES

APPENDIX A: SSRN Article

Intro: Previous periodical research progress and outcomes were conducted in a paper published on SSRN - a repository for preprints devoted to the rapid dissemination of scholarly research in the social sciences and humanities. The title of this paper is On the Mechanics of Sustainability: ESG Rating and Company Performance, and the paper was mainly about the illustration, examination, and simulation of ESG rating methodologies from two representative agencies - RepRisk and MSCI.

Sponsor: Center for the Study of Contemporary China (CSCC)

Yu, Haoxin. 2021. "On the Mechanics of Sustainability: ESG Rating and Company Performance." Papers.ssrn.com. Rochester, NY. July 10, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899898.

APPENDIX B: Medium Article

Intro: We composed an article about DeFi and Blockchain Risks - An introduction and examination of DeFi risks, published on Medium - a well-known social publishing platform where expert and undiscovered voices can share their writing on any topic. The article introduced eight risk categories on DeFi and blockchain and demonstrated case studies on each risk category. In addition, we briefly discuss existing solutions and the quantification of some of those risks. Since Miner Extractable Value (MEV) is considered one of the DeFi risks, we can get some inspiration by examining other DeFi risk categories and potential solutions.

Content:

Introduction

Nowadays, with increasing complaints about the inefficiency of the traditional financial system, decentralized finance (DeFi) and its base—blockchain—have taken on greater importance. These innovations can minimize many of the problems involved in the traditional financial system. For example, DeFi can help possess transactions with a high volume of assets by developing smart contracts in the form of dApps, which users can utilize for certain types of services regardless of the size of the transaction. In addition, DeFi can alleviate users' limited access to financial services because it allows large institutions and any other user access to financial products with beneficial terms and competitive pricing. Furthermore, DeFi improves transparency because one party can know its counterparty's capitalization. Both parties can read the smart contracts during a transaction process to determine whether the terms are agreeable. However, in traditional finance, some powerful counterparties may postpone or withhold their end of a financial agreement when encountering small players (Harvey, Ramachandran, and Santoro 2020).

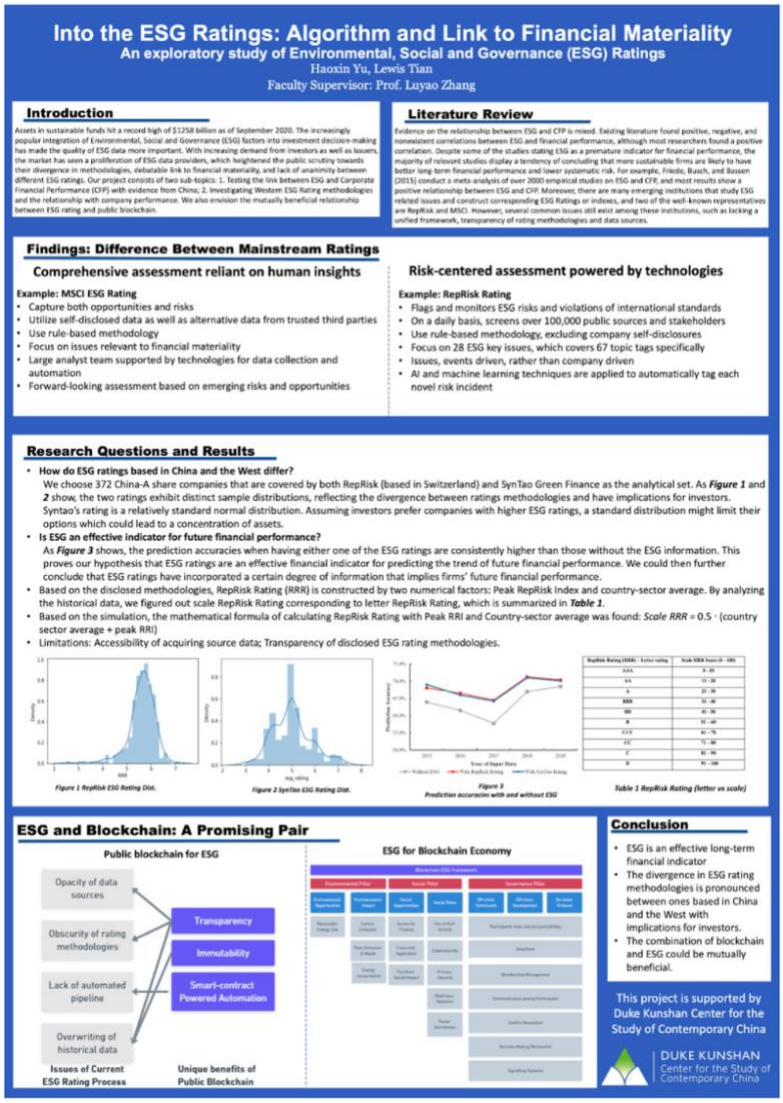
However, Harvey et al. (2020) mention that, as DeFi addresses these issues, it may introduce a novel set of risks. Considering these risks leads to a comparison with ESG — Environmental, Social Governance. ESG evaluates a firm's conscientiousness for environmental, social, and governance factors and is typically a score. Investors increasingly utilize these factors to identify material risks (CFA Institute 2020). Thus, several agencies have emerged to provide ESG Ratings for companies, and RepRisk is one of the representative agencies with the world's largest ESG database (Businesswire 2020). RepRisk (2021) emphasized that risk is a crucial indicator in

long-term value investment. It investigates ESG incidents and assesses corresponding risks to construct their ESG rating. The steps are taken in ESG prompt consideration to a similar rating instrument that might be designed for the risks involved in DeFi. The risks that DeFi introduces are also crucial and should be examined to maintain sustained growth instead of speculation. This article first introduces eight risk categories on DeFi and blockchain. Then, we demonstrate case studies on each risk category. Finally, we briefly discuss existing solutions and the quantification of some of those risks.

APPENDIX C: 2021 Fall Center for the Study of Contemporary China (CSCC) Undergraduate Poster Exhibition

Poster: Into the ESG Ratings - Algorithm and Link to Financial Materiality

Figure 6. CSCC Exhibition Poster



APPENDIX D: 2021 Fall Center for the Study of Contemporary China (CSCC) Undergraduate Research Exhibition Presentation

Time: Thursday, September 23 2021, 9:00 PM China Standard Time

Place: Online (Zoom)

Event Introduction:

CSCC undergraduate poster exhibition on China-related research will take place on 23rd September 2021 and we welcome anyone who has the interest to attend! Topics to be covered include but are not limited to the listed above.

This exhibition communicates and celebrates the participation of undergraduate students at DKU in scholarly inquiry, research, and creative endeavors. The aim is to give the students who have been involved in CSCC undergraduate research projects an opportunity to share their experience, receive valuable feedback on their work, and contribute to the scholarly conversation. Everyone is encouraged to attend and feel free to bring any insights and questions you have and discuss with all the researchers!

Presentation of each project generally takes 5 - 10 minutes (5-minute presentation, 3 minutes for questions, 2 minutes to transition to the next presenter).

Presentation Recording (with link):

https://duke.zoom.us/rec/play/sXyGHfAnx0RTYqxXeAujL7PQ5FxyQWx9kAoebrijApq1nvC5iJsi_khdScQPh1_GtC2PFysXeH2KcsVa.HozZimpkHRaTi87-?startTime=1632367080000&_x_zm_rtaid=kg7W3UqDTu6YPjsUOmqSrg.1638629240076.62ed168e8842ac8b1b12c4f7e222f0a2&_x_zm_rhtaid=886

APPENDIX E: 14th China UK Entrepreneurship Competition 2021 - Sustchaindex

Initial Proposal Submission Deadline: 30th Jan 2022

Semi-Final Time: Monday, Feb 28th 2022, 9:00 PM China Standard Time

Place: Online (Zoom)

Competition Introduction:

First launched in 2006, the Competition was one of the "Prime Minister's Initiative" projects in the UK, aiming to encourage new business ventures between China and the UK and is intended to simulate the real-world process entrepreneurs soliciting start-up funds from early-stage investors and venture capital firms.

Semi-Final Invitation Email Content:

Thank you for submitting your business plan to the Competition Panel. I am delighted to inform you that your team has successfully secured a place in the Semi-final of the 14th China UK Entrepreneurship Competition.

The Semi-final will be held ONLINE from 10am to 2pm on Monday, 28th February 2022. Your team, together with other 7 teams, will compete for 4 places in the Competition Final.

Please prepare a 10-minute presentation to demonstrate your business plan, which should cover the following points:

• Problems & solutions

• Description of product/service

• Analysis of target market & market size

• Analysis of competitors/competition

• Potential users/customers

• Team

• SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis

• Business model

• Financial projection (operation cost, profit and loss)

• Risk management

• Milestone

• Assessment and management of intellectual property (if applicable)

There will be a 10-minute Q&A session after your presentation, in which the judges will have questions regarding your business and presentation.

Semi-Final Presentation Slides:

Sustchain BUSINESS PLAN.pptx

We were finally ranked at 5 of 8, a little bit regretful that there were only 4 places for the Competition Final. However, the preparation process and the real-time presentation were absolutely precious experiences for us.