**香 港 中 文 大 学（深 圳）**

**THE CHINESE UNIVERSITY OF HONG KONG, SHENZHEN**

**Undergraduate Research Awards**

**APPLICATION FORM**

|  |  |  |
| --- | --- | --- |
| Name  (In English): Shulin Ke | 姓名  ﹝中文﹞: 柯舒麟 | 性别  Gender: 男 |
| 学号  Student I.D. No: 119020022 | 学院  School: SME | 主修/课程  Major /Programme: Financial Engineering |
| 电子邮箱  E-mail: 119020022@link.cuhk.edu.cn  联络电话  Phone Number: 13338466985 | 修业年  Year of Attendance: 2  累计平均成绩  Cumulative GPA: 3.49 | 预期毕业年份/学期  Expected Year / Term of Graduation: 2023 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 研究项目 | | | | | |
| RESEARCH PROJECT PROPOSAL | | | | | |
| 题目 | | Incentive Mechanism Design On Blockchain Storage | | | |
| Title of Proposal | |  | | | |
| 描述 | | | | | |
| Brief description  *This part is suggested to be written in English, except for special requirements.*  I decide to publish this paper in the conference INFOCOM 2021 this year corporate with Dr. Yunshu Liu who is now studying in CUHK Shatian Campus. Yunshu Liu will be the first author of this paper while I will be the second author together with Zhixuan Fang, Man Hon Cheung, Prof. Wei Cai, and Prof. Jianwei Huang as the third, fourth, fifth, and sixth author. Here’s the abstract of the paper which illustrate the topic:  “The booming of blockchain systems leads to significant storage cost for miners, which is difficult to cover by users' transaction fees. Such a phenomenon may jeopardize the blockchain security in the long-run. In this paper, we propose an incentive mechanism to alleviate this insufficient-fee problem in delay-insensitive blockchain applications by adjusting the transaction time limit, which is an easily implementable modification to the blockchain protocol. Specifically, we model the interactions among the protocol designer, users, and miners as a three-stage decision process. In Stage I, the protocol designer optimizes the time limit to maximize the social welfare. In Stage II, each user adjusts his transaction generation probability and transaction fee to maximize his payoff. In Stage III, each miner selects a transaction to record to maximize his payoff. The model's Nash equilibrium show that our scheme can generate sufficient fees under delay-insensitive applications, via raising the fee threshold and increasing the market competition. The numerical results show that our scheme may increase the social welfare for delay-sensitive applications. We further implement a blockchain protocol and deploy 114 nodes. The experiments show when users greedily update their transaction fees based on their payoffs, the average fees converge to the analytical results.” | | | | | |
| Guidelines:   1. Brief introduction 2. Significance/motivation 3. Expected contribution/outcome 4. Research methodology 5. Research plan 6. **Brief introduction**   I decide to publish this paper in the conference INFOCOM 2021 this year corporate with Dr. Yunshu Liu who is now studying in CUHK Shatian Campus. Yunshu Liu will be the first author of this paper while I will be the second author together with Zhixuan Fang, Man Hon Cheung, Prof. Wei Cai, and Prof. Jianwei Huang as the third, fourth, fifth, and sixth author. In this paper, we propose an incentive mechanism to alleviate this insufficient-fee problem in delay-insensitive blockchain applications by adjusting the transaction time limit, which is an easily implementable modification to the blockchain protocol.   1. **Motivation**   With the booming of cryptocurrencies, its underlying blockchain protocol imposes significant and fast growing storage costs on the operation nodes (often referred as miners). For example, for the second largest cryptocurrency Ethereum, its data size grows by nearly 11 folds from 385 gigabytes to 4 terabytes. This means, it costs miner $200 per month to store the entire Ethereum blockchain on its solid state hardware.  Despite transactions take up the majority of blockchain data, their fees are often insufficient to cover their storage costs. In a blockchain system, users generate transactions. To motivate miners to record and store their transactions, users need to propose transaction fees as the long-term compensation for miners’ storage costs. Although the transaction fees are the key to compensate for the blockchain storage costs, there are a lot of insufficient-fee transactions, where their fees are not enough for their storage costs, recorded in the blockchain. For example, almost all early-stage transactions are zero-fee in Bitcoin.  With insufficient transaction fees and huge storage costs, miners will have less incentives to stay in the system, jeop ardizing the system security. For example, the number of full-node miners storing the entire Ethereum blockchain has declined 66% since 2018. With fewer miners, it will increase the likelihood of a single point of failure in blockchain, and will lower the difficulty for malicious miners to conduct majority attacks. To maintain a healthy decen- tralized ecosystem, it is critically important to design a proper mechanism to motivate the users contribute enough transaction fees for miners’ storage costs.  A key reason for the transaction fee to be sufficient is that it is often determined by the user to shorten his transaction wait- ing time, instead of compensating the storage cost (e.g. Bitcoin and Ethereum wallets ). The transaction waiting time is difference between the time that the transaction is recorded in blockchain and its generation time. Some of the blockchain applications are delay-insensitive (e.g. crowdfunding and day- ahead-energy trading), where users are more tolerant to waiting time. These users’ transactions are the major reason for insufficient-fee issue, since users have little incentive to pay high fees to shorten the waiting time.  To the best of our knowledge, there are no previous studies on the incentive mechanism design to remedy this insufficient- fee problem from the waiting time perspective. We will take the first step in this paper to design such a mechanism to control waiting time and encourage users pay sufficient fees for delay-insensitive applications.   1. **Expected contribution**   To properly increase the transaction fee by controlling the transaction waiting time, we model the interactions among the protocol designer, users, and miners as a three-stage decision process.   * In Stage I (the transaction time limit optimization stage), the blockchain protocol designer determines the transaction waiting time limit to maximize the social welfare and alleviate insufficient-fee issue. * In Stage II (the transaction generation stage), each user chooses the transaction generation probability and fee to maximize his payoff, considering the other users’ strategies of others. * In Stage III (the mining stage), miners with heterogeneous storage costs maximize their own payoffs by selecting the proper transactions to include from the transaction pool.   Despite the complexity of the three-party interactions, we are able to derive the Nash equilibrium of Stages II and III. As a result, we can exploit the monotonic structure of the social welfare maximization problem in Stage I and numerically and effectively compute its optimal solution. The main contributions of this paper are as follows.   * + *Three-stage decision model:* We propose a model for blockchain protocol designer to characterize how transaction waiting time limit impacts the users and miners’ decisions, which applies to many current systems such as Bitcoin, Ethereum, and Litecoin.   + *Time limit optimization:* The protocol designer chooses the optimal time limit for social welfare optimization and encourage users to pay sufficient fee storage costs. We solve the integer programming by exploiting the monotonic structure of the social welfare. The Nash equilibrium of the model reveals that our scheme can alleviate the insufficient-fee issue for delay-insensitive applications due to the higher threshold fee and more intensive competition.   + *Numerical study and real-world blockchain experiments:* Numerical results demonstrate that the time limit optimization may also alleviate the insufficient-fee issue for delay-sensitive applications and increase their social welfare. Meanwhile, we implement a Bitcoin-based blockchain protocol and deploy 114 nodes using Docker. The experiments show that when each user greedily updates his transaction fee based on his payoff, the average fees converge to the expected fee at equilibrium.  1. **Research Methodology & Research plan**   We implement a blockchain protocol as well as experiment study in which deploy 114 nodes on the cloud. To be more specifically, we will implement a system of a complete Bitcoin-based blockchain protocol and deployed 114 nodes with Dockers. We will show that when each user greedily updates his transaction fee based on his payoff, the average fees converge to the expected fee at equilibrium. The experiments will show when users greedily update their transaction fees based on their payoffs, the average fees converge to the analytical results. We will model the interactions among the protocol designer, users, and miners as a three-stage decision process. In Stage I, the protocol designer optimizes the time limit to maximize the social welfare. In Stage II, each user adjusts his transaction generation probability and transaction fee to maximize his payoff. In Stage III, each miner selects a transaction to record to maximize his payoff. The numerical results will show that our scheme may increase the social welfare for delay-sensitive applications.  Journal publication in INFOCOM 2021 | | | | | |
| 项目开始日期  Project Start Date  yyyy/mm/dd | 2020.09 | | 项目结束日期  Project End Date  yyyy/mm/dd | 2020.12 | |
| 预期成果 | | | | |
| Expected Output (e.g. conference presentations, journal papers, etc.) | | | | |
| To properly increase the transaction fee by controlling the transaction waiting time, we model the interactions among the protocol designer, users, and miners as a three-stage decision process.   * In Stage I (the transaction time limit optimization stage), the blockchain protocol designer determines the transaction waiting time limit to maximize the social welfare and alleviate insufficient-fee issue. * In Stage II (the transaction generation stage), each user chooses the transaction generation probability and fee to maximize his payoff, considering the other users’ strategies of others. * In Stage III (the mining stage), miners with heterogeneous storage costs maximize their own payoffs by selecting the proper transactions to include from the transaction pool.   Despite the complexity of the three-party interactions, we are able to derive the Nash equilibrium of Stages II and III. As a result, we can exploit the monotonic structure of the social welfare maximization problem in Stage I and numerically and effectively compute its optimal solution. The main contributions of this paper are as follows.   * + *Three-stage decision model:* We propose a model for blockchain protocol designer to characterize how trans- action waiting time limit impacts the users and miners decisions, which applies to many current systems such as Bitcoin, Ethereum, and Litecoin.   + *Time limit optimization:* The protocol designer chooses the optimal time limit for social welfare optimization and encourage users to pay sufficient fee storage costs. We solve the integer programming by exploiting the monotonic structure of the social welfare. The Nash equilibrium of the model reveals that our scheme can alleviate the insufficient-fee issue for delay-insensitive applications due to the higher threshold fee and more intensive competition.   + *Numerical study and real-world blockchain experiments:* Numerical results demonstrate that the time limit optimization may also alleviate the insufficient-fee issue for delay-sensitive applications and increase their social welfare. Meanwhile, we implement a Bitcoin-based blockchain protocol and deploy 114 nodes using Docker. The experiments show that when each user greedily updates his transaction fee based on his payoff, the average fees converge to the expected fee at equilibrium.   Also, there will possibly be a publication of this paper on INFOCOM2021 this year. | | | | |

|  |
| --- |
| 个人陈述 |
| PERSONAL STATEMENT |
| As a student major in Financial Engineering, technologies related to blockchain are highly correlated with my major study in the undergraduate period. That is why I choose blockchain to be my research field. |

|  |  |  |
| --- | --- | --- |
| 获奖情况（由最近日期起） | | |
| SCHOLARSHIPS AND OTHER AWARDS RECEIVED WHILE AT UNIVERSITY (Start with most recent) | | |
| 奖励名称 | 奖励描述 | 获奖时间 |
| Name of Award | Brief description and value of the award | Period held: |
| 励耘奖学金 | 入学奖学金 | 2019.09 |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 导师评鉴 | | |
| SUPERVISOR(S)’ COMMENTS | | |
|  | | |
| 导师签名  SUPERVISOR’S SIGNATURE   * I hereby certify the authenticity and originality of the applicant’s proposal. | | |
| 导师姓名和学院  Name and School of Supervisor(s)  Wei Cai | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 2020.9.5 |
|  | Signature of Supervisor | Date |

|  |  |  |
| --- | --- | --- |
| 申请人签名  APPLICANT’S SIGNATURE | | |
| * I hereby agree to abide by URA’s policies and procedures governing the Undergraduate Research Awards. | | |
| 姓名  Name  Shulin Ke | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 2020.9.5 |
|  | Signature of Applicant | Date |

\*please submit the application form with all supporting documents to [*ura@cuhk.edu.cn*](mailto:ura@cuhk.edu.cn) before the application deadline.