Xu, X. Y., Tian, M.H., & Li, Z.H. (2022). Improving spam filtering in enterprise email systems with blockchain-based token incentive mechanism. In Li, E.Y. *et al.* (Eds.) *Proceedings of The International Conference on Electronic Business, Volume 22* (pp. 247-256). ICEB'22, Bangkok, Thailand, October 13-17, 2022

Improving spam filtering in enterprise email systems with blockchain-based token incentive mechanism

Xiaoying Xu [1]
Minghao Tian [2]
Zhihong Li [3,*]

*Corresponding author
[1] Associate professor, South China University of Technology, China, bmxyxu@scut.edu.cn
[2] Postgraduate, South China University of Technology, China, tianwei1182000@live.com
[3] Professor, South China University of Technology, China, bmzhhli@scut.edu.cn

ABSTRACT

Spam has caused serious problems for email systems. To address this issue, numerous spam filter algorithms have been developed, all of which require extensive training on labeled spam datasets to obtain the desired filter performance. However, users' privacy concerns and apathy make it difficult to acquire personalized spam data in real-world applications. When it comes to enterprise email systems, the problem worsens because enterprises are extremely sensitive to the possible disclosure of confidential information during the reporting of spam to the cloud. Targeting these obstacles, this study proposes a blockchain-based token incentive mechanism, with the aim of encouraging users to report spam while protecting business secrets and ensuring the transparency of reward rules. The proposed mechanism also enables a decentralized ecosystem for token circulation, fully utilizing the advantages of blockchain technologies. We developed a prototype of the proposed system, on which we conducted a user experiment to verify our design. Results indicate that the proposed incentive mechanism is effective and can raise the probability of spam reporting by more than 1.4 times.

Keywords: Spam Filtering; Blockchain; Token Incentives; User experiment.

INTRODUCTION

Spam is a serious concern for email systems. According to the Spam and Phishing Analysis Report published by Kaspersky, 45.47% of global email traffic in the third quarter of 2021 was spam. Situation becomes even worse in the email systems of large organizations and enterprises, due to the public nature of their email addresses (Lee & Chang, 2021; Wood & Krasowski, 2020). According to the Coremail Enterprise Email Security Report, the number of spam emails identified in enterprises reached 760 million in the fourth quarter of 2021, and the total number of phishing emails increased by 95.43% year-on-year. Obviously, anti-spam is of great practical significance, and many email service providers are developing automatic spam filtering algorithms.

Spam filtering algorithm can identify and filter spams on basis of training on a large scale of labeled spam datasets but collecting training data is difficult. Many filtering algorithms are reported to reach high accuracy on the open spam dataset for testing purposes (Shrivas et al., 2021). When it comes to real applications, however, most spam data is gathered through the traditional method of manually annotating. Furthermore, the strict privacy protection requirements prevent email service providers from accessing their clients' email content. In this situation, it can be difficult to ensure the quality of the spam database because of difficulties such as a lack of regular updates, a huge gap between the data and the real spams received by the user, etc. Even if the filtering algorithm is highly accurate in testing tasks, filtering services often struggle to discover new types of spam in a timely manner, resulting in a significant drop in spam filtering accuracy in real applications.

Another method for gathering training data is to ask users to report spams they have received, but the privacy concerns and apathy of users make this method impractical. Especially in enterprise email applications, some enterprise email systems even do not provide users with the feature of reporting spams to the cloud due to the concerns about the leakage of business secrets. Furthermore, email receivers are not active in reporting spam because there are no obvious incentives to do so. Therefore, a well-design mechanism for encouraging users to report spams under the premise of data security is essential, especially in the enterprise scenarios.

The wide applications of blockchain in a variety of industries inspires us to come up with a novel solution to the aforementioned issues by developing an anti-spam ecosystem with user participation. The successful adoption of blockchain-based token incentive mechanisms in decentralized autonomous organizations (DAOs) like Steemit and other blockchain-empowered communities have demonstrated their enormous potentials. As a typical example, the tokens (Steem) issued by Steemit have a total market value of more than 88 million dollars (September 2022). Most of these tokens are used to reward their users for posting or discovering high-quality content, hence boosting user engagement. Moreover, the decentralized nature of blockchain facilitates the resolution of the trust problem, thereby ensuring the security of users' digital assets on the blockchain platform.

Therefore, this paper proposes a blockchain-based token incentive mechanism to improve spam filtering in real-world applications, specifically enterprise email systems. Utilizing the most recent advancements in blockchain technology, the proposed design aims to collect more personalized labeled spam data while protecting privacy and business secrets. Users participating in the proposed mechanism, in particular, can earn token rewards for reporting spam. Tokens can be used to obtain benefits from enterprises. The enterprises then utilize the tokens they have collected to waive service fees from email service providers. The service providers pay for the fee waiver and receive updated and personalized labeled spam data in return, hence improving filtering performance. We also created a system prototype and conducted a user experiment to assess the effectiveness of our design. The results suggested that the proposed mechanism increased the likelihood of users' reporting spam by 1.4 times when compared to non-token incentives.

Following are the originality and contributions of our work: (1) We propose a novel solution to the problem of email spam using a blockchain-based incentive mechanism that focuses more on training data than on the filtering algorithm. (2) We contribute to the existing literature on blockchain applications by utilizing the decentralization property of blockchain to the scenario of enterprise email systems. (3) We construct a prototype of the proposed enterprise email system and conduct a user experiment to evaluate the efficacy of our design, with methodological implications for future empirical studies of blockchain.

RELATED WORK

Spam Filtering

Prior research on spam filtering has concentrated extensively on algorithm design. Naive Bayes, Decision Tree, and SVM are the most commonly used mail filtering algorithms (Mujtaba et al., 2018). On this basis, many researches introduce neural networks for mail recognition, such as MLP (Apoorva & Sangeetha, 2021), LSTM(Saumya & Singh, 2022), ensemble learning(Zhao et al., 2020), etc., and built recognition models that integrated multiple algorithms. Shrivas et al. (2021) assessed the models integrating various algorithms, compared and summarized four models made up of naive Bayes, decision tree, K-NN, SVM, MLP and RF, and found that the model composed of MLP, Naive Bayes and RF had the best performance. However, these solutions have not adopted the personalized filtering strategy.

The personalized filtering strategy builds on the conventional mail filtering algorithm and considers heterogeneous user patterns. Since the classification of spam varies depending on the user's interests, hobbies, and usage patterns, i.e., an email may not be considered spam by one user while being considered spam by another, the personalized filtering strategy further enhances the filtering accuracy. For example, Liu et al. (2017) proposed the CPSFS filtering model that divides spam into "totally spam" - considered spam by all users, and "half spam" - considered spam by certain users, and filters spams on both the server-side and the client-side. Their experiment revealed that CPSFS was more precise than ordinary Bayesian filtering. Similarly, Chen & Xu (2018) developed a client-side mail re-filtering mechanism. In their solution, a dynamic filter was built with several time windows and self-learning methods to achieve effective filtering. In spite of its better performance, a fundamental shortcoming of the personalized filtering strategy is that it relies heavily on the availability of users' spam data.

Whatever algorithm is employed, sufficient labeled spam data is required for training the filtering algorithm. An algorithm, particularly one for personalized filtering, can only accomplish its desired filtering performance when users report receiving spam. Our effort focuses on resolving the issue of how to get spam data from users, which has received very little attention up to this point.

Applications of Blockchain

Blockchain has been adopted in many fields and has demonstrated its utility. A survey indicated that blockchain technology may strengthen information systems in terms of interoperability, efficiency, and elimination of third-party intermediary costs. (Berdik et al., 2021). When it comes to specific cases, blockchain helps ensure data security and reshapes trust transfer in supply chain management (Moosavi et al., 2021) and other applications like federal learning(Toyoda et al., 2020). In conclusion, the application of blockchain is both technological transformation and mechanism remodeling to the traditional information system.

However, there are relatively few studies in the application of blockchain in mail systems, and discussions in this field are just focused on data security. For example, when applied in email system, blockchain can enable users to send and receive emails without a trusted third party (TTL). Specifically, the mail sender in blockchain-based email system sends one key to the receiver and uploads another key to the blockchain, and receiver can only decrypt the mail when having the two keys (Hinarejos et al., 2019; Hinarejos & Ferrer-Gomila, 2020). Although blockchain has been shown to improve data security of email systems, there are many potentials of blockchain in reshaping the incentive mechanism of spam reporting in email systems, which still remain unexplored.

Blockchain-Based Token Incentives

Blockchain-based token incentives refer to the method of smartly issuing blockchain-based tokens as rewards. Many studies have summarized its distinct application value. The decentralized structure of blockchain tokens promotes user-to-user transactions by resolving the trust and privacy challenges that plague traditional centralized systems. Additionally, it facilitates the establishment of a token economy with substantial monetary value that can provide users with substantial economic returns (Thelwall, 2018), which is beneficial for online platforms to attract early users and to solve the "chicken or egg" conundrum

(Drasch et al., 2020). The following three application aspects of blockchain-based token incentives have been intensively investigated:

(1) The blockchain's decentralized structure and the automatically executed smart contract enable convenient, low-cost and secure transactions between users, meeting the needs of many fields. ImaniMehr and DehghanTakhtFooladi (2019) created a token incentive mechanism for P2P streaming media transmission so that users can gain the most benefit from donating their own network resources, hence improving the overall performance of streaming media transmission. In order to overcome the current challenges with distributed renewable energy trading and generation, Wang et al. (2019) developed a token-based incentive mechanism for distributed renewable energy, and set up a decentralized power trading system. The network resources and electricity contributed by users may be easily quantified and confirmed with very low cost.

(2) The transparency of token incentive rules and the non-tampering of blockchain data can aid in eliminating the concerns of unfairness. Gong & Fan (2019) applied token incentive mechanism to information sharing behavior in the scenario of online marketing. They linked the tokens to the uses' reputation in an equitable manner to ensure the reputation's veracity and to boost the marketers' willingness and quality of information sharing. Weng et al. (2019) introduced token incentives in federated learning to provide participants with a fair guarantee to prevent participants from misleading training, inference attacks, and other improper behaviors. Experiments with simulations indicate that token incentives are more likely to induce participants to comply with rules and behave appropriately. Dang et al. (2022) developed a dynamic incentive mechanism for supervising employees in the service industry. The usage of tokens and smart contracts overcomes the fairness problem regarding whether to reward or punish employees. The experimental results indicate that this mechanism can help employees better moderate their behavior when interacting with clients.

(3) Blockchain-based token incentives are used address data security concerns. In the medical field, for example, electronic medical records can be stored on blockchain to ensure data security. On the assumption of ensuring the authenticity and privacy of experimental data and medical records, the use of a blockchain-based token reward mechanism can improve people's enthusiasm for participating in clinical trials (Jung et al., 2021).

Table 1: Application value of Blockchain-based Token Incentives

Application value of Blockchain-based Token Incentives	Literatures	Application Scenarios
Decentralized trading	ImaniMehr & DehghanTakhtFooladi, 2019	Peer-to-peer video streaming networks
	Wang et al., 2019	Market of distributed renewable energy
Addressing trust issues	Gong & Fan, 2019	Market information sharing
	Weng et al., 2019	Federal learning
	Dang et al., 2022	Supervision of employee behavior
Data security	Jung et al., 2021	Medical trial recruitment

In conclusion, these studies demonstrate the rationales and advancements of employing token incentives instead of traditional virtual credit incentives. However, no direct discussion on the use of token incentives in email filed has been found. These previous studies are of great reference value for us regarding the design of token incentive mechanisms for spam filtering in enterprise email systems.

TOKEN INCENTIVE MECHANISM DESIGN

Challenges of Incentive Mechanism among Different Participants

There are three roles in an enterprise mail system: user, enterprise, and mail service provider. A user is the employee who uses the enterprise email systems to handle their work. An enterprise is the organization that purchases the mail service. A mail service provider is the company that develops mail systems and offers related services. Each of the three participants has its own needs. To better show the motivation behind our blockchain approach, we will analyze the trust issues between the email service providers and their enterprise customers, followed by a discussion of the limitations of traditional monetary end-user rewards.

Service providers seek to collect more spam data by offering incentives to improve spam filtering capabilities and market competitiveness. In practice, however, service providers cannot completely trust their enterprise customers since it is difficult to assure the openness and transparency of incentive issuance regulations. In particular, when the incentive service is run locally on the enterprise side, there is no guarantee that the enterprise will not use illegal ways to modify the codes or databases to defraud rewards. From the perspective of a service provider, it is eager to take control of the incentive-related codes and databases, and it desires that the incentive service execute locally on the service provider side.

Similarly, the enterprises do not fully trust the email service providers. An enterprise, like the service provider, cannot guarantee that the provider will not change the rules and database at the backend, reducing the issuance of incentives deserved by the enterprise and its users. Moreover, many large organizations require running their mail systems locally to ensure data

security and privacy. It may be unacceptable for them to allow the email service provider to gain control of the incentive service, which may reveal some operational information of its employees. Obviously, there is a significant conflict regarding the control of the incentive sub-system between the service provides and their enterprise customers.

When it comes to the end-user side, i.e., the employees in the enterprises, in most of the traditional designs, reporting of spam is just a voluntary activity of users in order to receive more accurate filtering services. This is far from satisfactory, even with monetary incentives. Economically speaking, service providers should consider the actual cost and benefit of offering incentives. The monetary rewards obtained by every user for reporting spam would be tiny, resulting in very little incentive effect, but the total cost of the service providers can be substantial. How to lower the cost and increase the effectiveness of rewards is a crucial design challenge for incentive mechanisms.

To summarize, targeting the trust issues, a decentralized structure is required to meet the needs of the three roles in the system. This is one of our main motivations to embrace blockchain in our design. The decentralized nature of blockchain allows the operation ledger to be distributed and stored among enterprises and service providers, hence resolving the trust issue between them. The on-chain smart contract enables automatic incentive issuance execution thus ensuring the openness and transparency of incentive issuance rules. Moreover, the tradable and multi-dimensional-value natures of blockchain tokens allow us to design the incentive mechanism in an ecological manner, which can be expected to improve the efficiency.

Users' Spam Reporting and Token Incentives

The tokens circulating in the system are referred to as reporting tokens. Reporting token incentives mean that users who report valid spam are rewarded in the form of tokens. Users can obtain tokens only by reporting spam. The service provider collects the spam reported by users and awards them with tokens. The enterprise acts as the mail auditor to prevent the leak of confidential information, and it also provides the token redeeming service for its employees. Figure 1 depicts the overall reporting token incentive process.

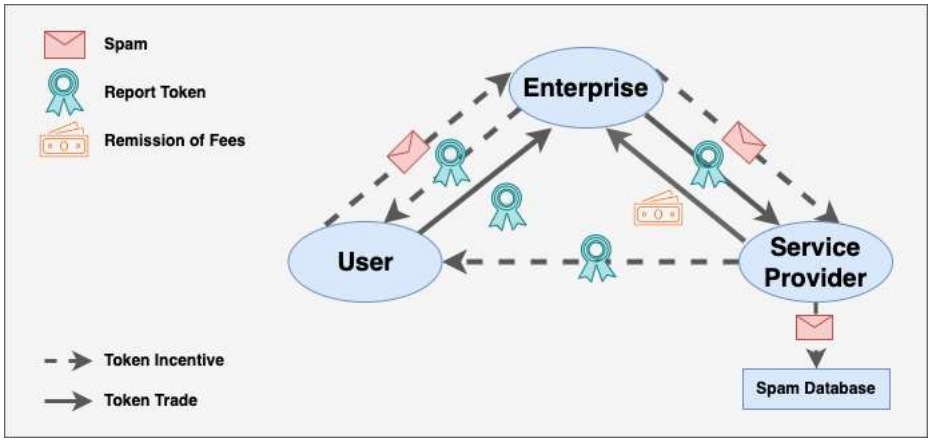

Figure 1: Process of the reporting token incentives

After receiving a spam email, a user of the enterprise notifies the enterprise via the system. After receiving the report, the enterprise examines the content of the email, confirms that it does not include any confidential information, and uploads the email to the service provider's spam database. After receiving the reported spam mail, the service provider verifies it and adds it to the enterprise's personalized filtering database or general spam database, enables the mail filtering model to do incremental training, and issues reporting tokens to the users who reported this spam.

Since the service provider would be sensitive to the actual cost of issuing token incentives, it is better to make the cost predictable and controllable. Therefore, we refer to the token issuance rules used in the online community Minds (minds.com) and adopt the model of fixed total amount and contribution weighting. Contribution weighting means that the tokens are awarded to a user based on the weight of his or her contribution. The weight is calculated as the ratio between the number of spams a user report in each period, and the total number of spams reported in the whole system in that period. Fixed amount means that service providers provide a fixed number of tokens to award users in a certain period. As a result, in a system with *j* users, the *k*th user *(k<j)* receives *E* tokens in a period, as shown in Equation 1, where *N* is the total number of tokens awarded by the service provider in a period, n_k and n_i are the number of spams reported by the *k*th and *i* th users, respectively, in this period.

$$E = N \times \frac{n_k}{\sum_{i=1}^{j} n_i} \quad (1)$$

With the help of the decentralized ledger of blockchain, we believe both the users and the enterprises are not able to obtain token incentives through any malicious behavior, and that all the token rewards will be distributed fairly and objectively to the contributors. One reason is because all the incentive-related processes are transparent to all the participants in the email system. Any malicious behavior can be easily traced by other participants via the blockchain ledger. A further reason is that the block

data is immutable for every single participant, making any malicious backend operations impossible, and therefore, eliminating the trust concerns among different participants. The final reason is that, following consensus among the participants, all incentive rules are codified on smart contracts that automatically distribute token rewards. The immutability and self-execution of smart contracts ensure the objectivity and fairness of token reward distribution.

To sum up, in the whole incentive mechanism, users contribute by reporting spam and receive the reporting tokens as the work certificate. Enterprises and users benefit from a more effective and individualized spam filtering service, and obtain better mail filtering performance through the continuous training of personalized filtering algorithms. Mail service providers pay the token to obtain timely and accurate spam data, achieve better mail filtering performance through the continuous training of personalized filtering algorithms, and improves the competitiveness of their products. In fact, the value of the designed incentive mechanism can be enlarged through token trading and circulating in a token-ecosystem, which will be introduced in the following.

Token Trading and Circulating

After receiving the token rewards, users can redeem them from the enterprise according to the reward-to-redemption ratio that all the participants have agreed on. Redeeming options can be advanced mail services like huge attachment cloud storage and e-mail content refinement, as well as other benefit like the eligibility for internal purchasing funds. Furthermore, by creating a ranking list of users receiving tokens and awarding medals, enterprises may also transform the token into a comprehensive incentive that integrates economy, psychology, reputation, which may enhance the incentive effect.

Enterprises obtain tokens from users and use these tokens to trade for fee waivers from the service provider. Depending on the demands in the ecosystem, the service provider may issue new tokens when existing ones are insufficient. To prevent the service provider from issuing tokens arbitrarily, the minimum exchange ratio between token and usage fee waiver can be specified, which provide the value basis for the tokens.

The service provider might revise the number of tokens issued in each period to control the cost of rewards. The enterprise can decide whether to invest additional expenses to encourage users to report spams according to a tradeoff between the inventive cost and the fee waivers. Since the value of tokens is fundamentally assured throughout the token circulation loop, enterprises and service providers may regulate their expenses flexibly, and users can receive their appropriate benefits. As a whole, the entire mechanism can function effectively.

USER EXPERIMENT

Many researchers have used the evolutionary game method to measure the effectiveness of the incentive mechanism. However, in our context, it is difficult to use rational person hypothesis and to quantify earnings of users. Noticing that user experiment is also a practical and common method for analyzing the incentive impact in information systems since the usage scenario can be easily modified and controlled (Jung et al., 2021), we decide to employ the user experiment method to evaluate the effect of the designed blockchain token incentive mechanism.

Experiment Design

The experiment referred to the possible incentive input in the real word and set three groups. Although the value of a reporting token is designed to consistently change in the incentive mechanism, we set the value of a token at 1 RMB in the experiment by altering the reward-to-token ratio to control the rewards subjects received. As a result, not only can we set groups with and without incentives to compare the incentive effect, but also set groups with certain incentive quantity to compare the incentive effect of different incentive inputs. And considering the actual incentives that enterprises and service providers may input, we set the non-incentive group, the 1 token/spam group and the 5 token/spam group in the experiment. The process of user experiment is as follows:

(1) Click on the link. The entire user experiment was conducted with PCs, including assessing the subjects' system usage behaviors and their answering of questionnaires. The experimental subjects would receive the link before the experiment and started the experiment after clicking on it. After clicking the link, participants would be randomly redirected to different versions of systems with varied parameter settings corresponding to different experimental groups. The redirections were accomplished automatically in the backend with no user intervention required.

(2) Go through the experiment instructions. The page jumped to the experiment instructions after clicking the link. By reading the description, the subjects had a basic comprehension of the aims, processes, estimated duration of the experiment, as well as the basic concepts of blockchain and tokens. The subjects entered the prototype email system after confirming that they had finished reading the instructions.

(3) Independent user exploration. The experimental subjects could freely explore the prototype system, interact with it, and accomplish operations such as viewing mails, sending mails, reporting mails, and so on. In its initial state, the email system had several mails in its bin and inbox, including two wrongly filtered mails: one was spam but recognized as non-spam, another one was non-spam but recognized as spam. By reporting wrongly filtered emails, the user could get reporting tokens. In addition, a specific email reading task was assigned based on the actual content of the email to guarantee that the subjects

used the system correctly. The subjects entered the scene of receiving a new email after confirming the completion of email reading and investigating the system functionalities.

(4) Receive new emails. The subjects received new emails, read them, and then acted on them. Three new messages were received by them: two of which were unfiltered spam and one of which was not. The user experiment terminated when the subjects affirmed that they had read the emails and completed the action. And then the browser would navigate to the questionnaire link.

(5) Complete the questionnaire. The questionnaire comprised three questions and used a five-level scale to assess the strength of incentives users perceived in order to investigate their subjective perceptions of incentive effect.

Table 2 The Questionnaire of Perceived Incentive Strength

Variables	Number	Questions
Perceived Incentive Strength	PIS1	The system can issue many rewards
	PIS2	I get a lot of rewards for reporting spam
	PIS3	If I actively report spam, I can quickly redeem the prize I want

Prototype System Construction

We constructed the mail prototype used in the experiment by creating the front end of the mail system using Vue3 and the Element Plus component library. Because the focus of this study is the token incentive mechanism, rather than the technical implementation of the email system, it does not go into technical specifics. Some of the prototype's key processes and pages are depicted below. Since the experiment was conducted in China, the original language of the system interfaces was Chinese. The text in the flowing figures was translated from Chinese using Google Translate.

When users enter the prototype, the interface will display an experiment instruction dialog, followed by a token description dialog (Figure 2) if the user is assigned to rewarded groups (group 1 and group 2).

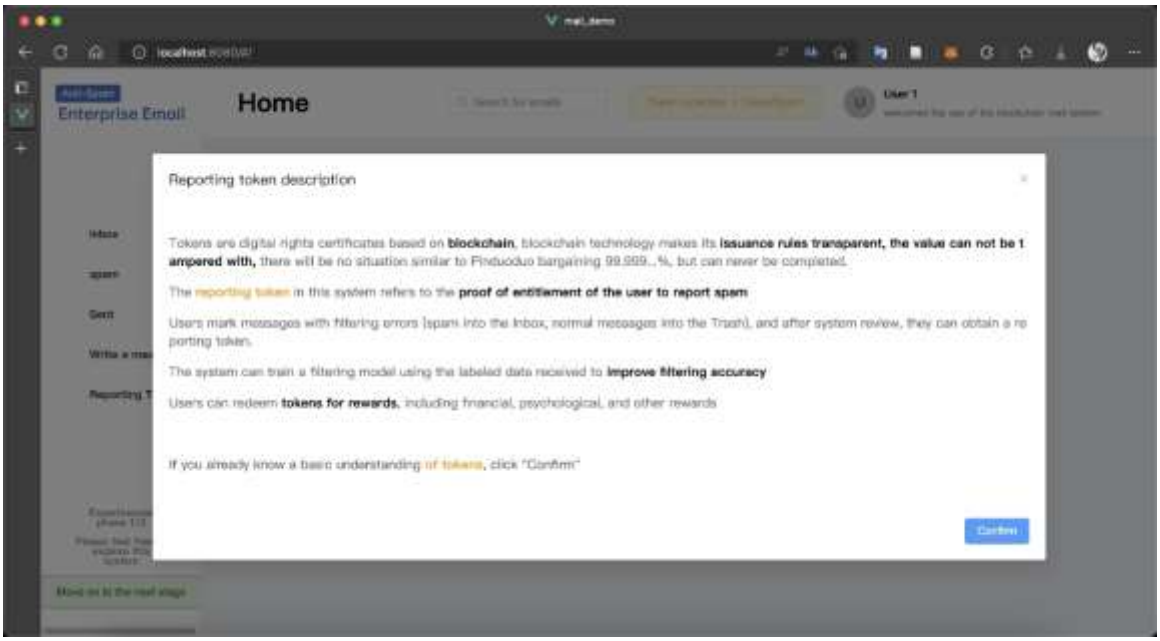

Figure 2: Token description in prototype

The main page of the prototype system contains the navigation bar on the left, the information bar on the top and the email content on the right. Users can go to the inbox, spam, sent, compose, and reporting token interfaces through the navigation bar. The information bar shows the brief information of the user and his or her token rewards. The interface of inbox is shown in Figure 3. Other pages expect for the token page are all basic functions of traditional email systems.

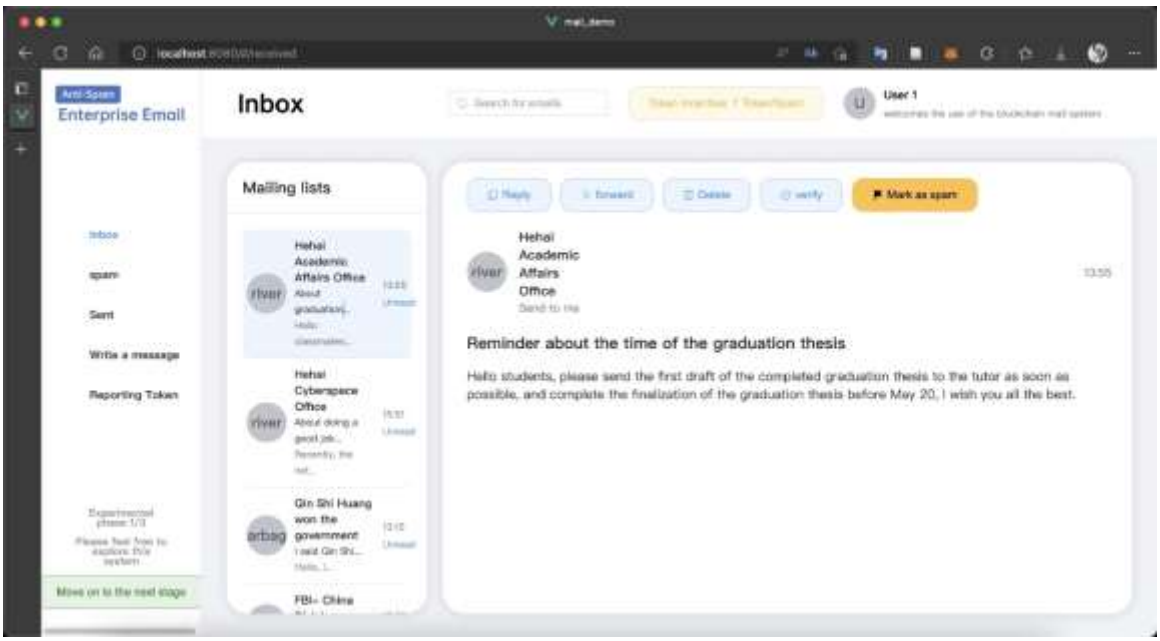

Figure 3: Inbox page in prototype

The token page for the rewarded groups is shown in Figure 4, which was not provided for the non-rewarded group. Users can use the rewarded tokens to redeem benefits in the token page, including premium service and some other specific products.

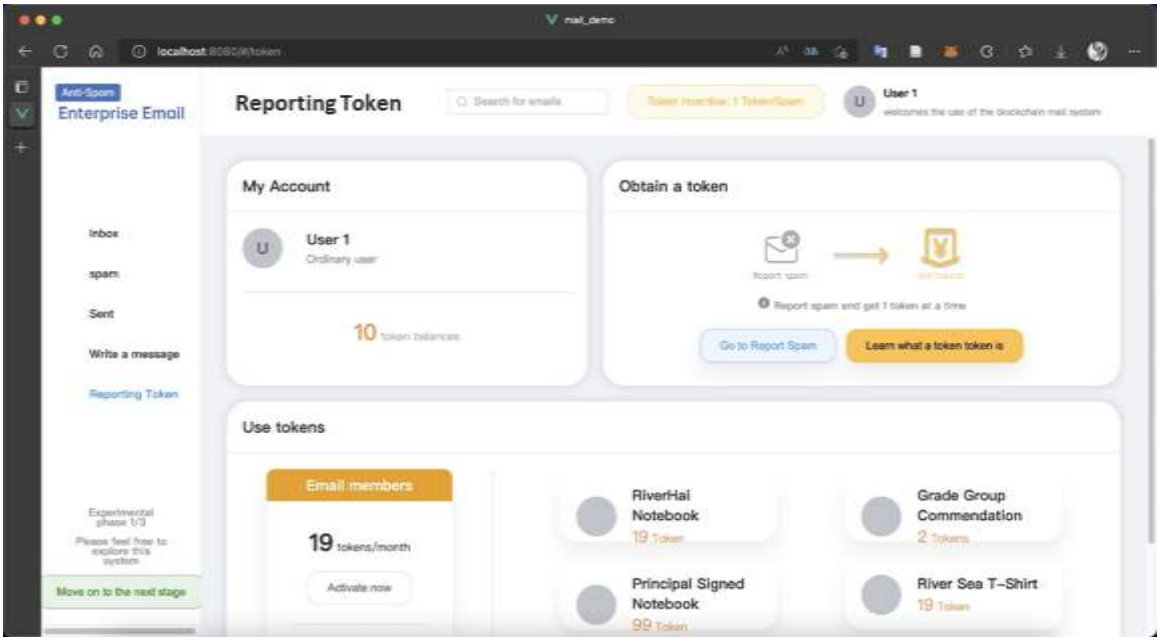

Figure 4: Token page in prototype

Implementation of Experiment

To make the experiment more rigorous, we conducted a pilot study by recruiting three experimental subjects, and then made focused adjustments on bugs and other problems discovered during the pre-experiment.

Table 3: Basic characteristics of the subject

Characteristics	Categories	Number of Participants	Proportion (%)
Sex	Male	32	64.0
	Female	18	36.0
Grade	Freshmen	6	12.0
	Sophomore	9	18.0
	Junior	16	32.0
	Senior	19	38.0

After the pilot study, 53 undergraduates participated in the formal experiment and completed the questionnaires. After removing three anomalous results, 50 valid records were obtained, with 17 in experimental group 1, 18 in experimental group 2, and 15 in experimental group 3. Table 3 shows the demographics of the experimental subjects. The distribution of participants among the three randomly assigned experimental groups was relatively balanced, and the findings of one-way ANOVA revealed no significant difference between gender and grade among the three groups.

Results and Analysis

Table 4: Results of the Experiment

Group	Incentive Quantity（Tokens/Spam）	Average Score of the Perceived Incentive Strength	Average Number of Spams Reported	Average Probability of Reporting Spam（%）
1	5	3.78	2.54	63.5
2	1	4.06	2.69	67.3
3	0	/	1.12	25.0

The experiment results for the three experimental groups with varying reward levels are shown in Table 4. The results of the two rewarded groups were significantly different from those of the control group. Specifically, one-way ANOVA revealed significant differences between groups in the quantity of spams reported ($p = 0.016 < 0.05$). In terms of absolute numbers, rewarded users in the two groups reported 2.54 incorrectly filtered emails on average, but non-rewarded users reported only 1.12 emails. In terms of probability, the probabilities of reporting for the two groups of rewarded users are higher than 60%, but just 25% for the non-rewarded users. According to the results of the experiment, the incentive mechanism increased the likelihood of users' reporting spam by more than 1.4 times. The findings reveal that the proposed design has a substantial incentive effect.

Secondly, for the two rewarded groups, the results show that the average score of perceived incentive strength was significantly correlated with the average likelihood of marking spam emails, indicating that the greater the perceived value of incentives, the more likely users were to report spam. Such results are consistent with common sense.

However, it is interesting to find that within the two reward groups (group 1 and group 2), the token reward quantity does not affect the perceived incentive strength and the reporting behavior. The results of independent-sample t-test showed no significant difference in perceived incentive strength scores ($p = 0.15 > 0.05$) and number of spams reported ($p = 0.81 > 0.05$) between group 1 and group 2.

Discussion

In the application scenario of spam reporting, the token incentive mechanism has delivered exceptional results. The increased desire to report spam by the two groups receiving token incentives demonstrates the effectiveness of the token incentive mechanism from the users' perspective.

In terms of parameters, we compared the incentive effects of 1 token/spam and 5 tokens/spam According to the results, simply increasing the number of rewarded tokens did not make users perceive an increase in incentive strength, and the possible reasons are as follows:

(1) There is currently no incentive mechanism for reporting emails in the real world, and users feel uncertainty about how many rewards they should receive by reporting a spam mail. In other words, most users cannot create a unified cognition or standard for the quantity of incentives. For some users, 1 token/spam is already a lot, while for others, 5 tokens/spam is still rare. As a result, the perceived incentive strength varied between users in the same group, and eventually led to the insignificance of difference in perceived incentive strength scores and number of spams reported between groups.

(2) With the constraints of our experiment settings, participants could not fully reveal the value of a toke through redeeming, which brought some uncertainty towards the reward strength. This phenomenon suggests that, in order to maximize the incentive effect of blockchain tokens, it is crucial to build the ecosystem for token circulation.

During the experiment, we also learned that the difficulty of explaining tokens to users may reduce the effectiveness of token incentives. It was quite difficult to quickly convey the concept of a blockchain-based token to the majority of the experiment's participants, as they were unfamiliar with blockchain technology. Negative information regarding blockchain technology, such as mining and cryptocurrency price crashes, may damage users' faith in blockchain tokens, as individuals typically resort to the technology's reputation information when confronted with novel technologies or information systems (Li et al., 2008). Therefore, when promoting and deploying blockchain tokens in the real world, it is vital to explain the concept and technical principles of blockchain tokens to users in more detail.

CONCLUSION

This research aims at designing an incentive mechanism to encourage users to report spam emails. However, there exist trust problems among the three main roles in the enterprise email system. Enterprises are concerned about the possibilities of email

data leakage, and service providers are concerned about the misuse of incentive mechanism by users and enterprises. As a result, neither the enterprise nor the service provider can serve as the central node of the incentive system. A decentralized incentive mechanism is needed to address the trust problems between corporations and service providers. Therefore, we used blockchain-based tokens to build the incentive mechanism.

In the mechanism we designed, users can get tokens rewards by reporting spam, and then use tokens to redeem other benefits from the enterprise. The enterprise obtains tokens from users and uses them to pay the service provider's service fees. The service provider pays for the costs of fee waiver but gets timely, accurate and personalized labeled spam data, which helps improve filtering performance and enhance industry competitiveness. Furthermore, the mechanism of token issuance and circulation are designed to ensure the value of tokens and that enterprises and service providers can make flexible adjustment of the incentive cost.

The results of user experiment indicated that the incentive mechanism proposed in this paper can increase the probability of users reporting spam by more than 1.4 times. Further, the ecosystem for token circulation should be well-establish so that service providers may obtain spam data at a low cost. Moreover, it is necessary to explain more clearly to users about blockchain tokens and make them trust the new technologies.

The current study still has certain limitations. First, we only employ a user experiment approach for evaluation. The incentive mechanism can be further validated from the standpoint of speculative strategy in future study. Second, we were unable to fully simulate the environment for the ecosystem of token circulation due to the constraints of the experiment, which may be better implemented in future work. Third, the results may be biased as the experimental subjects are all undergraduate students. It is feasible to enhance the experiment by recruiting enterprise email users as the subjects. And fourth, although probable explanations for the experiment results have been provided, it would be better to interpret the results from a more theoretical perspective.

ACKNOWLEDGMENT

This work was supported by grants No. 72071083 and 72171089 from the National Natural Science Foundation of China, grant No. 2021A1515012003 from the Guangdong Natural Science Foundation of China, and grant No. 2021GZQN09 from the Project of Philosophy and Social Science Planning of Guangzhou in 2021.

REFERENCES

Apoorva, K. A., & Sangeetha, S. (2021). Deep neural network and model-based clustering technique for forensic electronic mail author attribution. SN Applied Sciences, 3(3), 348. https://doi.org/10.1007/s42452-020-04127-6

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A Survey on Blockchain for Information Systems Management and Security. Information Processing & Management, 58(1), 102397. https://doi.org/10.1016/j.ipm.2020.102397

Chen S., & Xu D. (2018). A personalized mail re-filtering system based on the client. SCIENTIA SINICA Informationis, 48(12), 1681–1696. https://doi.org/10.1360/N112018-00138

Dang, S., Cao, S., Li, J., & Zhang, X. (2022). Dynamic incentive mechanism design for regulation-aware systems. International Journal of Intelligent Systems, 37(2), 1299–1321. https://doi.org/10.1002/int.22670

Drasch, B. J., Fridgen, G., Manner-Romberg, T., Nolting, F. M., & Radszuwill, S. (2020). The token's secret: The two-faced financial incentive of the token economy. Electronic Markets, 30(3), 557–567. https://doi.org/10.1007/s12525-020-00412-9

Gong, Y., & Fan, P. (2019). Research on the dynamic incentive mechanism of information sharing in social network services based on reputation mechanism. Cluster Computing, 22(S2), 5025–5031. https://doi.org/10.1007/s10586-018-2471-x

Hinarejos, M. F., & Ferrer-Gomila, J.-L. (2020). A Solution for Secure Multi-Party Certified Electronic Mail Using Blockchain. IEEE Access, 8, 102997–103006. https://doi.org/10.1109/ACCESS.2020.2998679

Hinarejos, M. F., Ferrer-Gomila, J.-L., & Huguet-Rotger, L. (2019). A Solution for Secure Certified Electronic Mail Using Blockchain as a Secure Message Board. IEEE Access, 7, 31330–31341. https://doi.org/10.1109/ACCESS.2019.2902174

ImaniMehr, Z., & DehghanTakhtFooladi, M. (2019). Token-based incentive mechanism for peer-to-peer video streaming networks. The Journal of Supercomputing, 75(10), 6612–6631. https://doi.org/10.1007/s11227-019-02863-0

Jung, S. Y., Kim, T., Hwang, H. J., & Hong, K. (2021). Mechanism Design of Health Care Blockchain System Token Economy: Development Study Based on Simulated Real-World Scenarios. Journal of Medical Internet Research, 23(9), e26802. https://doi.org/10.2196/26802

Lee, T., & Chang, H. (2021). A Study on the Effectiveness of Secure Responses to Malicious E-mail. Journal of Platform Technology, 9(2), 26–37.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. The Journal of Strategic Information Systems, 17(1), 39–71. https://doi.org/10.1016/j.jsis.2008.01.001

Liu, X., Zou, P., Zhang, W., Zhou, J., Dai, C., Wang, F., & Zhang, X. (2017). CPSFS: A Credible Personalized Spam Filtering Scheme by Crowdsourcing. Wireless Communications and Mobile Computing, 2017, 1–9. https://doi.org/10.1155/2017/1457870

Moosavi, J., Naeni, L. M., Fathollahi-Fard, A. M., & Fiore, U. (2021). Blockchain in supply chain management: A review, bibliometric, and network analysis. Environmental Science and Pollution Research, 1–15. https://doi.org/10.1007/s11356-021-13094-3

Mujtaba, G., Shuib, L., Raj, R. G., & Gunalan, R. (2018). DETECTION OF SUSPICIOUS TERRORIST EMAILS USING TEXT CLASSIFICATION: A REVIEW. Malaysian Journal of Computer Science, 31(4), 271–299. https://doi.org/10.22452/mjcs.vol31no4.3

Saumya, S., & Singh, J. P. (2022). Spam review detection using LSTM autoencoder: An unsupervised approach. Electronic Commerce Research, 22(1), 113–133. https://doi.org/10.1007/s10660-020-09413-4

Shrivas, A. K., Dewangan, A. K., Ghosh, S. M., & Singh, D. (2021). Development of Proposed Ensemble Model for Spam e-mail Classification. Information Technology and Control, 50(3), Article 3. https://doi.org/10.5755/j01.itc.50.3.27349

Thelwall, M. (2018). Can social news websites pay for content and curation? The SteemIt cryptocurrency model. Journal of Information Science, 44(6), 736–751. https://doi.org/10.1177/0165551517748290

Toyoda, K., Zhao, J., Zhang, A. N. S., & Mathiopoulos, P. T. (2020). Blockchain-Enabled Federated Learning With Mechanism Design. IEEE Access, 8, 219744–219756. https://doi.org/10.1109/ACCESS.2020.3043037

Wang, J., Zhong, H., Wu, C., Du, E., Xia, Q., & Kang, C. (2019). Incentivizing distributed energy resource aggregation in energy and capacity markets: An energy sharing scheme and mechanism design. Applied Energy, 252, 113471. https://doi.org/10.1016/j.apenergy.2019.113471

Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive. IEEE Transactions on Dependable and Secure Computing, 1–1. https://doi.org/10.1109/TDSC.2019.2952332

Wood, K. E., & Krasowski, M. D. (2020). Academic E-Mail Overload and the Burden of "Academic Spam." Academic Pathology, 7, 2374289519898858. https://doi.org/10.1177/2374289519898858

Zhao, C., Xin, Y., Li, X., Yang, Y., & Chen, Y. (2020). A Heterogeneous Ensemble Learning Framework for Spam Detection in Social Networks with Imbalanced Data. Applied Sciences, 10(3), 936. https://doi.org/10.3390/app10030936