Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2024.049996

ARTICLE

A Framework Based on the DAO and NFT in Blockchain for Electronic Document Sharing

Lin Chen[1], Jiaming Zhu[1], Yuting Xu[1], Huanqin Zheng[1] and Shen Su[1,2,*]

[1]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, 510006, China

[2]Engineering Research Center of lntegration and Application of Digital Learning Technology, Ministry of Education, Beijing, 100816, China

*Corresponding Author: Shen Su. Email: sushen@gzhu.edu.cn

Received: 24 January 2024 Accepted: 07 April 2024 Published: 08 July 2024

ABSTRACT

In the information age, electronic documents (e-documents) have become a popular alternative to paper documents due to their lower costs, higher dissemination rates, and ease of knowledge sharing. However, digital copyright infringements occur frequently due to the ease of copying, which not only infringes on the rights of creators but also weakens their creative enthusiasm. Therefore, it is crucial to establish an e-document sharing system that enforces copyright protection. However, the existing centralized system has outstanding vulnerabilities, and the plagiarism detection algorithm used cannot fully detect the context, semantics, style, and other factors of the text. Digital watermark technology is only used as a means of infringement tracing. This paper proposes a decentralized framework for e-document sharing based on decentralized autonomous organization (DAO) and non-fungible token (NFT) in blockchain. The use of blockchain as a distributed credit base resolves the vulnerabilities inherent in traditional centralized systems. The e-document evaluation and plagiarism detection mechanisms based on the DAO model effectively address challenges in comprehensive text information checks, thereby promoting the enhancement of e-document quality. The mechanism for protecting and circulating e-document copyrights using NFT technology ensures effective safeguarding of users' e-document copyrights and facilitates e-document sharing. Moreover, recognizing the security issues within the DAO governance mechanism, we introduce an innovative optimization solution. Through experimentation, we validate the enhanced security of the optimized governance mechanism, reducing manipulation risks by up to 51%. Additionally, by utilizing evolutionary game analysis to deduce the equilibrium strategies of the framework, we discovered that adjusting the reward and penalty parameters of the incentive mechanism motivates creators to generate superior quality and unique e-documents, while evaluators are more likely to engage in assessments.

KEYWORDS

Electronic document sharing; blockchain; DAO; NFT; evolutionary game

1 Introduction

The Internet has become the primary means for people to work, entertain, and share knowledge in the information age. As a result, an increasing number of digital works are being circulated, stored, and

utilized online. However, e-documents, which are one of the most commonly used data carriers on the Internet, are vulnerable to copyright infringement due to their easily replicable nature and the limited effectiveness of current protection measures. Infringements not only violate the rights of creators but also diminish their creative initiative. Therefore, creators and readers may be less likely to share their e-documents on the network. This goes against the original intention of using e-documents as a means to share knowledge and hinders the integration and development of knowledge.

Existing research has proposed solutions for constructing e-document sharing systems that have been successfully commercialized. These systems mainly rely on centralized storage to share creators' e-documents with readers. Duplicate e-documents are identified using plagiarism detection algorithms or manual means, and digital watermarking is the primary method for e-document copyright protection. They prioritize the commercial value of e-documents over copyright protection, resulting in limited measures and various shortcomings. In particular, centralized storage poses significant security risks due to the high degree of data centralization, and the plagiarism detection algorithms used are unable to comprehensively check contextual and stylistic aspects of e-documents. Professional reviewers can conduct comprehensive contextual and stylistic checks. However, the high degree of centralization poses a risk of malicious activities, wherein professionals might provide biased assessments for personal gain. Additionally, there is no e-document evaluation mechanism to prevent the uploading of inferior e-documents. Digital watermarking technology can only provide evidence for infringement traceability, which does not prevent e-document plagiarism. Furthermore, these systems lack effective incentive mechanisms, which results in users having little motivation to share resources.

In this paper, we propose an e-document sharing framework based on decentralized autonomous organization (DAO) and non-fungible token (NFT) in blockchain. Considering the interests of authors, readers, and the reputation of the system, the framework rejects poor-quality and plagiarized e-documents and penalizes the authors of such e-documents, while rewarding authors who upload high-quality and original e-documents. On the one hand, the framework incorporates a DAO-based evaluation mechanism to assess the quality of e-documents and prevent the inclusion of inferior content. In addition, using DAO, the framework establishes a plagiarism detection mechanism that comprehensively checks uploaded e-documents for elements such as textual context and style. Furthermore, recognizing problems in the governance mechanism of existing DAOs, such as low voting participation and susceptibility to manipulation, this paper introduces innovative optimizations to address these concerns. On the other hand, considering the system efficiency, a hybrid storage approach is adopted, where the source files of e-documents are stored in decentralized off-chain storage servers, while metadata, including encrypted storage addresses, keyword groups, content summaries, digital watermarks, and creator signatures, are stored on-chain. The cryptographic algorithms, tamper resistance, decentralization, timestamping, blockchain storage, and consensus mechanisms inherent in the blockchain ensure the authenticity and effectiveness of NFT. And NFT itself has a strong circulation that encourages the circulation and sharing of e-documents. Once an e-document has undergone evaluation and plagiarism checks, the system uses NFT technology to mint a unique NFT, which serves as the sole credential for its on-chain transactions and circulation. Finally, our experiments validate the security of the optimized governance mechanism in DAO. Evolutionary game theory [1] is used to derive the equilibrium strategies of the framework, which indicate that by adjusting reward and penalty parameters, authors are incentivized to produce higher quality and original e-documents, while reviewers are more inclined to participate in reviews. This work contributes to the exploration of shared, managed, and operational models for e-documents, providing a new solution to promote e-document digitization and cross-platform sharing. The main contributions of this paper are as follows:

- **DAO-based e-document evaluation and plagiarism detection:** In response to the difficulty of distinguishing e-documents, we addressed this problem by combining the characteristics of document resources with existing e-document plagiarism detection technologies. The result is the design of an e-document evaluation and plagiarism detection mechanism based on the DAO. First, our framework performs a preliminary comprehensive evaluation of e-documents through evaluation and plagiarism detection algorithms, automatically identifying and intercepting duplicates and poor-quality e-documents. Then, within the DAO, a decentralized governance approach is used to perform a comprehensive evaluation of the electronically evaluated e-documents to ensure the final quality of the e-documents. This ensures the quality and originality of e-documents uploaded to the system, providing users with a higher quality e-document sharing environment.
- **NFT-based e-document copyright protection and circulation:** Due to the limitations of existing e-document copyright protection methods, we adopt a hybrid on-chain and off-chain approach. It establishes a bidirectional link between on-chain NFTs and off-chain source e-documents. This method provides more secure e-document copyright protection and leverages the strong tradability of NFTs to encourage e-document sharing.
- **Evolutionary game-based optimization for framework governance:** The framework involve game relationships between voting and decision making, risk and reward, and other factors. These relationships can change as participants, goals, and external environments change. Understanding and managing these relationships is crucial for the stable development of the framework. An evolutionary game model was constructed to analyze the equilibrium in which the decisions of creators and voters are all optimal. The implications of these findings are significant for framework governance.

2 Related Work

In recent years, e-document sharing systems have been extensively studied on prominent platforms such as IEEE Xplore [2], JSTOR [3], and CNKI [4], which are widely recognized for their specialized content and wide distribution. Among them, IEEE Xplore and JSTOR do not have a plagiarism detection mechanism and therefore do not provide verification services for the originality of e-documents. However, they do use a peer review mechanism to assess the quality of e-documents. CNKI, on the other hand, uses plagiarism detection algorithms to check electronically authored documents, but does not evaluate the quality of the e-documents. These platforms typically employ measures such as digital watermarking [5] or application restrictions to limit user access to e-documents, thereby mitigating copyright concerns to some extent.

However, these e-document sharing systems suffer from two shortcomings. First, they are characterized by centralization, which leads to security issues such as data vulnerability and the inability to establish ownership. Second, they lack effective incentive mechanisms to encourage user participation in system development.

Several innovations have been proposed to address these challenges. Ismail et al. [6] implemented a P2P application that allows researchers from different communities to share reference materials, but it lacks permission control. Han et al. [7] proposed a Decentralized Document Management System (DDMS) that assigns access rights to multiple users to improve document security. Verma et al. [8] proposed the use of blockchain technology and attribute encryption to jointly guarantee the transmission of secure and valid digital certificates, and the use of Interplanetary File System (IPFS) to store encrypted data to ensure privacy and resistance to external interference. Vimal et al. [9] proposed a

more mature blockchain-based e-document sharing system. This system adopts a hybrid on-chain and off-chain storage model, first storing source e-documents in the IPFS, then recording the off-chain storage paths of e-documents in the blockchain, coupled with providing certain rewards to users. However, this system still has some limitations. They use a file deduplication algorithm based on file hashes, which means that even minor changes to an e-document, such as changing a punctuation mark, will result in significantly different file hashes, leading to poor accuracy.

In the realm of existing plagiarism detection algorithms, Devlin et al. [10] introduced a pre-trained deep learning model known as Bidirectional Encoder Representations from Transformers (BERT) for natural language processing tasks, including text classification and named entity recognition. In the context of plagiarism detection, BERT can be used to assess the semantic similarity of texts. Moreover, Nunes et al. [11] proposed an unbiased estimator, DotHash, for the intersection size of two sets. The method utilizes the tendency of sets of random high-dimensional vectors to be orthogonal to create fixed-size representations for sets. A simple dot product of these sketches serves as an unbiased estimator of the size of the intersection of sets. Tan et al. [12] introduced Data Aware Sensitive Hashing (DASH), a data-dependent hashing scheme for approximate nearest neighbor search in high-dimensional space. DASH is based on the search framework of QALSH and takes the residual distance prior into account to evaluate a common distribution family for achieving probability guarantee. However, these algorithms do not comprehensively account for contextual and stylistic elements, limiting their effectiveness in the area of e-document copyright protection.

In addition, the rapid development of blockchain technology in recent years has given rise to DAO and NFT. DAO is an innovative organizational structure that encodes standard management and operational regulations on the blockchain through smart contracts. Members participate in the governance of the organization through voting, and the results are recorded on the blockchain. Decisions can be automatically executed by smart contracts without centralized control or third-party intervention. This allows for autonomous operation and provides a significant guarantee for the security of internal governance within an organization due to its decentralized nature [13]. NFTs are based on Ethereum's Ethereum Request for Comments 721 (ERC-721) and ERC-1155 token standards. NFT casting is done through smart contracts combined with metadata. Contract calls are also used for NFT circulation and destruction. All NFT-tagged assets can be freely traded based on user-defined values such as age, rarity, and liquidity, providing a new application paradigm for digital copyright protection [14,15].

3 Architecture

3.1 Architecture Design

As shown in Fig. 1, the system adopts the common front-end and back-end separation architecture, and divides the system into the presentation layer, middleware layer, contract layer, and storage layer.

- **Presentation layer:** The front-end architecture is implemented using Vue.js and ElementUI to achieve data visualization, providing users with an entry point to participate in the system. The results of the system operation are displayed directly to the users as feedback.
- **Middleware layer:** This layer consists of four main components. The first part is a Natural Language Processing (NLP)-based text quality analysis module, which provides an initial assessment of the quality of e-documents. The second part is a text plagiarism detection module based on mature algorithms, which performs an initial check for e-document duplication. The third part is a digital watermarking module based on encryption techniques that generates

digital watermarks for qualified e-documents. The final component is a connection to a trusted third-party identity authentication system that verifies the digital identity of users and creates a unique account address in the system, where a user's digital identity corresponds to an account address.

- **Contract layer:** The smart contracts of the system are developed using the Solidity language. Several business contracts have been designed to meet the functional requirements of the system. The general functionalities include data encryption and decryption, system token coinage and reputation, token transfer, and access control. The business functionalities mainly consist of two modules: the DAO module and the NFT module. The DAO module supports the system's DAO-based evaluation and plagiarism detection mechanisms through internal mechanisms such as voting, incentives, and arbitration. The NFT module provides a secure circulation mechanism and copyright protection for e-documents through activities such as mining, burning, and transferring NFTs.
- **Storage layer:** Due to the high cost of storing large files on the blockchain and the potential congestion caused by excessive data storage, the system uses two storage engines for data storage [16]. These include a distributed storage system built by multiple independent servers, and a blockchain system built on Ethereum [17]. The Ethereum blockchain is used to store structured data such as users' digital identities, e-document metadata, and operation logs. On the other hand, the off-chain distributed storage system is used to store the source files of e-documents uploaded by users.

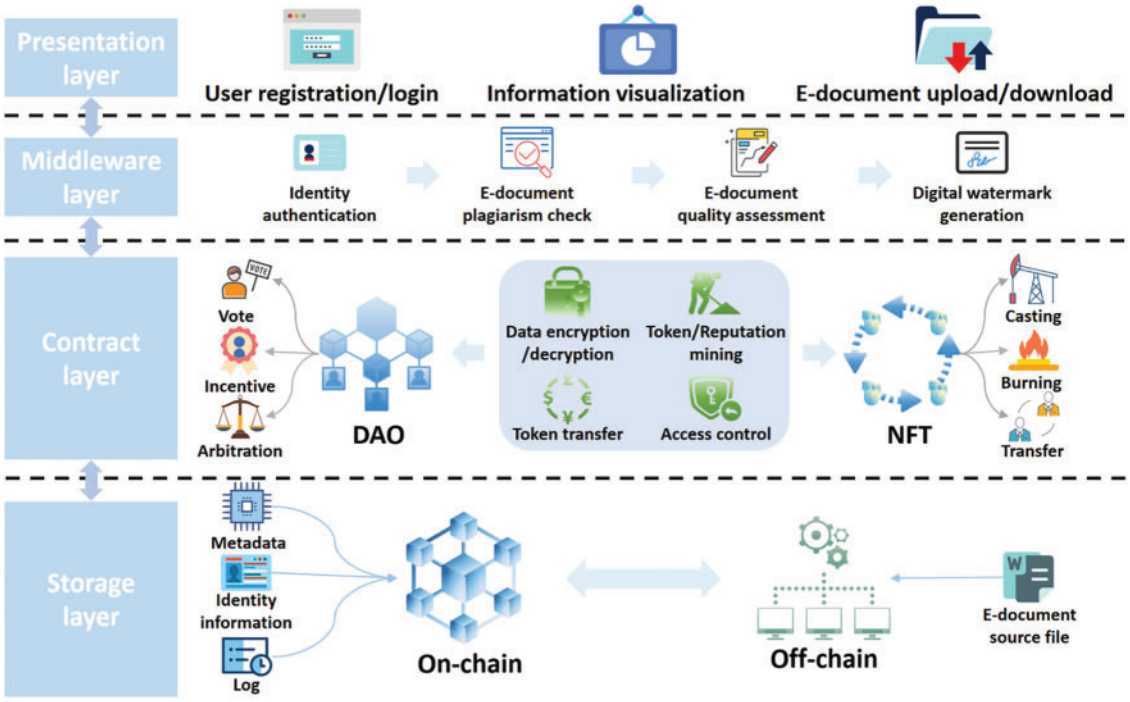

Figure 1: E-document sharing system architecture

3.2 Module Design

3.2.1 DAO-Based E-Document Evaluation and Plagiarism Detection

Recognizing the potential threat of malicious users seeking substantial on-chain asset rewards by generating numerous poor-quality and duplicate works to execute Distributed Denial of Service (DDoS) attacks, leading to severely degraded user experience and potential damage to the system's reputation, user retention, and eventual bankruptcy, we have developed an e-document evaluation and plagiarism detection mechanism based on the DAO. This mechanism evaluates and checks the works submitted by authors, rejecting substandard and plagiarized submissions while encouraging the upload of high-quality and original works. Fig. 2 illustrates the process flow of the DAO-based e-document evaluation and plagiarism detection mechanism.

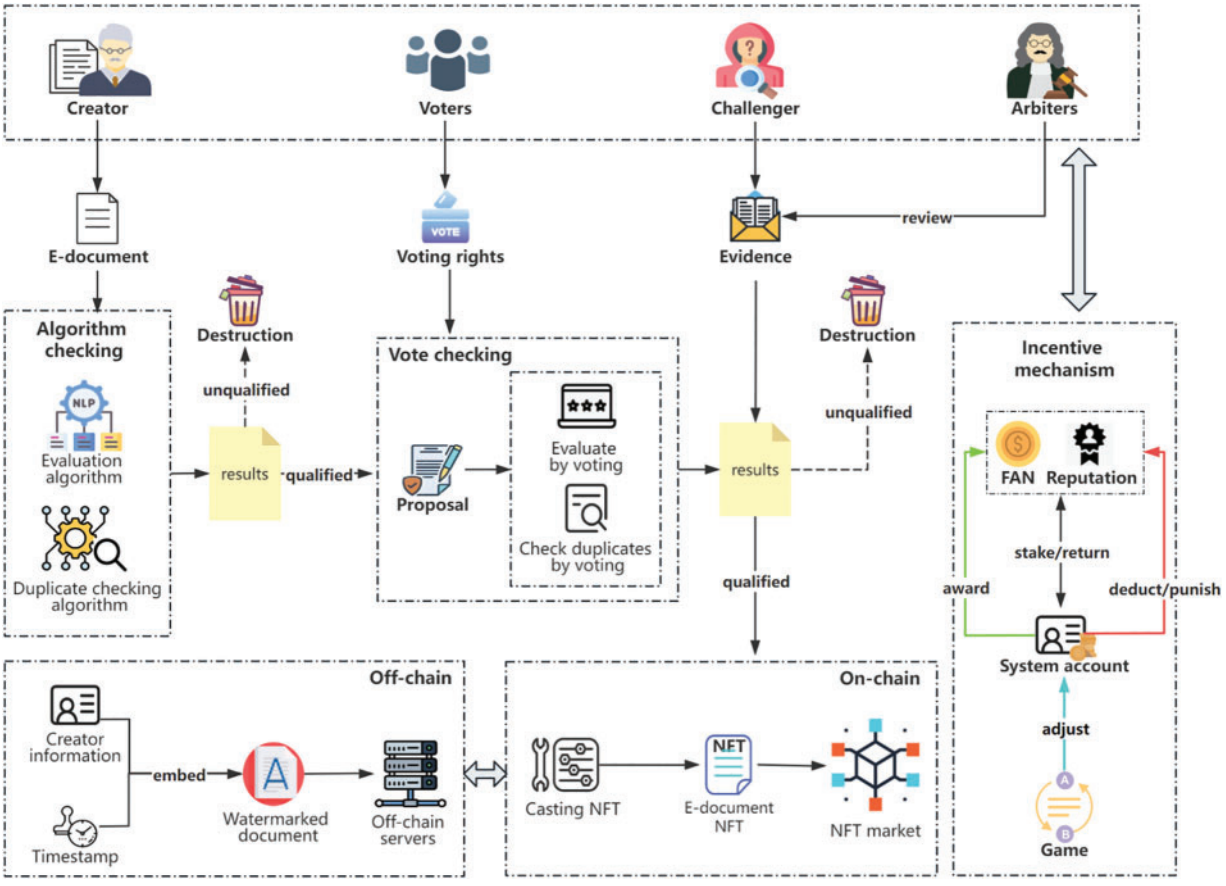

Figure 2: E-document sharing process based on DAO and NFT

When authors create e-documents and want to upload them to the system to earn revenue while ensuring the copyright protection of their e-documents, the process is as follows.

The author first pledges a certain amount of tokens (FAN tokens) to the system. FAN tokens are homogeneous tokens minted according to the ERC-20 standard, obtainable through fiat currency exchange, NFT issuance or trading, and participation in system governance.

Upon receipt of the e-document, the system automatically executes a NLP-based evaluation algorithm to obtain a preliminary assessment of the quality of the e-document [18,19]. This NLP-based text quality assessment technology evaluates the quality of the text by analyzing various textual features such as vocabulary, sentence structure, coherence, and discourse structure. After the algorithmic assessment, the system's plagiarism detection algorithm performs an initial check of the e-document [20–23]. If the algorithm determines that the e-document is of poor quality or has a high duplication rate, the system immediately deletes the e-document, confiscates the author's promised FAN tokens, and deducts their reputation. This approach minimizes attention consumption within the DAO and protects the rights of bona fide authors.

If the e-document passes the system's algorithmic evaluation and plagiarism check, the system triggers a DAO proposal for evaluation and plagiarism detection, attaching the main content of the e-document. Members of the DAO (system users) vote on the proposal regarding the evaluation and plagiarism check of the e-document. If the voting results indicate poor quality and a high rate of plagiarism, the system confiscates the author's pledged FAN tokens and deducts their reputation. Conversely, if the voting results unanimously approve the e-document, the system returns the author's pledged FAN tokens and provides appropriate rewards based on the voting results. Finally, the metadata of the e-document is extracted on-chain, forged into a unique NFT, and a digital watermark is generated off-chain and stored on distributed servers.

In addition, this paper presents optimizations to the DAO model in the following four aspects:

Reputation Mechanism

In existing DAOs, governance tokens often serve a dual function, performing both governance and monetary functions. This means that governance tokens may not only appear in internal trading markets, but may also be active in lending markets. Attackers can exploit this by borrowing from lending markets or renting delegations from potential vote-buying markets, thereby gaining a significant amount of voting power in a short period of time and launching governance attacks on the DAO.

To mitigate such problems, it is essential to consider decoupling tokens from governance, thus weakening the role of tokens in governance. To address this, we have designed a reputation mechanism that positions reputation as the primary means of DAO governance. User-acquired reputation is non-transferable, and to manifest reputation as a reflection of users' direct contributions to the system's copyright protection mechanisms, we further designed a reputation decay mechanism. After users earn reputation, it decays with the system's governance frequency (voting times), which encourages users to contribute more original works to the system and thus earn more reputation. This also motivates users to actively use their reputation by participating in the voting governance of the system. The decay is outlined below:

$$R(j) = R(j-1)e^{-\beta j} \tag{1}$$

where $j > 0$ and $\beta > 0$. $R(j)$ is the reputation value after the user has acquired reputation R after the j-th instance of the system initiating a vote. β is the decay rate. If $\beta = (1/30)ln2$, it means that the user's reputation is halved after 30 rounds of voting. It will be adjusted based on the level of user participation in system governance and its impact. j indicates the round of voting initiated in the system after the user received reputation.

Incentive Mechanism

To enhance the decentralized governance capability of the system and encourage user participation in system governance and content creation, a set of incentive mechanisms must be designed. Existing research on incentive mechanisms can be broadly divided into two categories: AI algorithm-based incentive models [24,25] and traditional incentive models. The former allows for more intelligent design and optimization of incentive mechanisms, but also introduces a certain degree of complexity. In comparison, we focus more on the latter with lower complexity. Our designed incentive mechanism mainly applies rewards or penalties to both creation and governance.

Creation incentive: When a user successfully uploads his or her creative work to the system and converts it into an NFT, the system rewards the user with reputation and FAN tokens. Considering the key role of reputation in system governance, and in order to prevent the formation of reputation whales and to protect the governance rights of the majority of system users, the reputation rewards gradually decrease as the number of works uploaded by the user increases. However, the higher the comprehensive evaluation of the work, the higher the reputation reward. The reputation rewards for creation are as follows:

$$R(i,x,y) = \begin{cases} 0, & if\ x = 0\ or\ y = 0 \\ e^{-\alpha(i-1)} ln(x+y), & if\ x > 0\ and\ y > 0 \end{cases} \tag{2}$$

where $i > 0$, and $R(i,x,y)$ represents the reputation reward for the author after successfully uploading the work for the i-th time and receiving a quality score x and a duplication rate score y. α is the decay rate. If $\alpha = (1/29)ln2$, it means that when the number of uploads reaches 30, the reputation reward provided by the system will be halved. i represents the number of successful uploads by the creator. The reputation reward for the first successful upload is $ln(x+y)$. This means that the creator reward depends entirely on the final score of the work. If $x = 0$ or $y = 0$, it means that the e-document is of poor quality or plagiarized, and the creator will not receive any reputation reward.

In addition, the FAN token reward during creation will also depend on the final score of the work. The higher the score, the more FAN token rewards the system will provide, and vice versa.

However, if the creator violates the concept of copyright protection by being determined by the system algorithm or group voting to be suspected of copying, plagiarism, or poor quality, not only will they not receive any rewards, but the system will also decide whether to impose penalties on the creator based on the participation of the voters. If a decision is made to impose penalties, reputation will be deducted as follows:

$$R(t) = \begin{cases} 0, & if\ t = 0 \\ e^{\gamma(t-1)}, & if\ t > 0 \end{cases} \tag{3}$$

whereas $R(t)$ represents the reputation penalty given to the creator after violating the copyright protection mechanism of the system for the t-th time. γ represents the growth rate. If $\gamma = 1$, it means that the penalty given by the system increases by e times each time. t indicates the number of times the creator has violated the system's copyright protection mechanism. If $t = 1$, $R(1) = 1$, the system gives them the smallest reputation penalty, which is because we consider that the creator may not have intended to violate the copyright protection mechanism, but rather made an unintentional mistake. In other words, our system has a tolerance of 1 time for violating the copyright protection mechanism.

If the creator's existing reputation is not sufficient to cover the reputation penalty imposed by the system, the system will deduct the creator's entire reputation.

Additionally, the pledged FAN tokens will be deducted by the system. In addition, the required pledge of FAN tokens for uploading works will increase significantly with each occurrence of misconduct. The goal is to encourage creators to maintain a positive creative attitude, otherwise they will incur high costs. The specific ratio is as follows:

$$F(t) = x^{t+1} \tag{4}$$

where $x > 1$ and $t \geq 0$. $F(t)$ represents the number of FAN tokens required for a creator to re-upload works after the t-th violation of the system's copyright protection mechanism. t indicates the number of times the creator has violated the copyright protection mechanism of the system. If $x = 2$, when $t = 0$, $F(t) = 2$, indicating that if the creator has not violated the system's copyright protection mechanism, the required pledge for each upload is the basic amount of 2 FAN tokens.

Governance incentives: When users participate in system governance with their FAN tokens and reputation, they receive rewards in both FAN tokens and reputation. The specific reward mechanisms depend on the role the user plays in system governance.

As a challenger, you can pledge the same amount of FAN tokens as the creator, question the creator's work, and challenge the creator. If the challenge is successful, the challenger receives all of the FAN tokens pledged by the creator and gains the reputation deducted from the creator.

Users must first pledge tokens before becoming voters. Throughout the voting process, the system incentivizes voters based on their level of active participation. Incentives are closely tied to the circulation value of the resource created by the creator's behavior. Actively participating voters will be rewarded with FAN tokens, while passively participating voters may face reputation penalties and have their pledged tokens deducted.

As for whistleblowers, you can file a report by providing evidence of violations in the system to the arbitration committee. If the arbitration committee gives a positive result, you will receive the same FAN token rewards and reputation rewards from the system as your creative works.

Arbiters will receive FAN token rewards after each participation in the review process. This incentive encourages more users to participate in community management, contribute, and strive to become arbiters.

Voting Mechanism

In DAO governance, the voting mechanism is not only the most important, but also the primary means of governance. Aragon [26] uses two voting methods, 1T1V (one token, one vote) and 1P1V (one person, one vote). In the 1T1V system, the influence of the whales is considerable, meaning that the outcome of the vote can be easily manipulated by large token holders and does not reflect the true thoughts of the majority of the community [27]. On the other hand, the 1P1V system, while inherently fair, tends to overlook the influence of more knowledgeable and experienced individuals, resulting in a voting outcome that may not be consistent with rationality and somewhat reducing the incentive for voter participation. Colony [28] introduces reputation as the sole representation of voting power, but it still leaves room for significant influence by reputation whales. In addition, it overlooks the fact that in the early stages of the system, ordinary users may lack reputation and thus cannot exercise their voting rights in system governance.

In this paper, we have optimized the representation and weighting of voting rights. Both reputation and tokens are used to represent voting rights. This implies that users with reputation or FAN tokens can participate and influence the voting process for governance decisions. We have also refined the

weighting of FAN tokens and reputation in the voting process, ensuring a more nuanced and balanced approach to incorporating these factors.

$$W(r,n) = \begin{cases} 0, & \text{if } r = 0 \text{ and } n = 0 \\ \sqrt{r + \dfrac{n}{r+n}}, & \text{if } r \neq 0 \text{ or } n \neq 0 \end{cases} \tag{5}$$

whereas the voting power value W is computed comprehensively based on both the voter's reputation value r and the number of FAN tokens held n.

Since reputation is derived from a user's contribution value to the system, it is accorded greater respect and positive encouragement. Consequently, the voter's reputation value r has a higher weight in the calculation of voting rights. To ensure that the interests of the majority are prioritized in the voting process, we have deliberately reduced the influence of whales in the voting process. This adjustment is intended to create a more balanced and equitable voting environment where the influence of large token or reputation holders is reduced for the benefit of the broader community.

To address concerns about reputation whales, we have implemented the square root voting mechanism [29]. This means that the voting power W of a reputation whale is approximately the square root multiple of its reputation value, specifically about $\sqrt{r}$. In other words, if a reputation whale wishes to have a voting power of r, the reputation cost incurred would be approximately r^2. This results in a significant and expensive cost for reputation whales, ensuring that the majority of participants have more influence in the voting process.

To illustrate this mechanism, consider a scenario with a whale and $m\,(m > 1)$ regular voters. Suppose the whale has a reputation of $m \times r$, and each regular voter has a reputation of r. Even though their total reputation is the same, their voting power is significantly different. The whale's voting power is approximately $\sqrt{mr}$, while the regular voters' voting power is $m\sqrt{r}$. Therefore, even with the same total reputation, the majority of regular voters have more influence in the voting process.

For FAN token whales, we believe that compared to reputation, there are more diverse and straightforward ways to acquire FAN tokens, such as fiat currency exchange, trading, or content creation, as well as system incentives. Users find it easier to accumulate FAN tokens and become FAN token whales. Therefore, we limit the weight of FAN tokens in the voting process. In other words, in the absence of reputation, no matter how many FAN tokens a whale owns, its voting power will not exceed 1. During the voting process, participants who own FAN tokens but lack reputation have equal voting power, thus eliminating inequalities. This addresses the shortcomings of the 1T1V mechanism, significantly reduces the coupling between wealth and voting rights, and also grants basic voting rights to regular users in the early stages through FAN tokens.

Arbitration Mechanism

Potential disputes may arise in the governance of the system through voting, and there may also be instances of violations of the rules, such as bribery. To address these issues, we have established an arbitration committee.

In principle, all DAO members can become members of the arbitration committee by using their reputation and FAN tokens. Taking into account the members' professional skills, contributions, and potential for misconduct, the system will randomly select five members from the top 5% of reputation and FAN token holders among those who have staked. If there are less than five members, additional members will be selected sequentially until there are five. In addition, these five members have no visual

or participation rights in subsequent governance votes, including evaluation votes and plagiarism checks.

On the one hand, creators can challenge the voting results for their own work by staking more FAN tokens and requesting arbitration from the arbitration committee. Similarly, other DAO members can act as challengers by staking an equal amount of FAN tokens and providing evidence of plagiarism or poor quality of a work to request arbitration. During the voting process, since the arbitration committee is unaware of the voting results, they can make more professional and impartial judgments based on the evidence provided by the challengers or directly evaluate the e-documents uploaded by the authors.

On the other hand, all users can report rule violations within the system by staking FAN tokens and providing evidence to the arbitration committee. The highest and lowest scores of the committee members are excluded, and the remaining three scores are weighted, averaged, and rounded to determine the arbitration result. If the result is against the wishes of the appellant (creator, challenger, or whistleblower), the system will confiscate the staked FAN tokens and impose a reputation penalty. If the outcome is in the appellant's favor, they will receive governance rewards based on their identity type.

To further reduce the potential for misconduct within the arbitration committee, we are implementing a rotating committee mechanism. The selected arbitration committee will be responsible for arbitrating disputes and rule violations for the next five full governance votes (including evaluation votes and plagiarism checks). At the end of their term, the system will re-elect the arbitration committee members.

3.2.2 NFT-Based E-Document Copyright Protection and Circulation

Due to the immutable and unique nature of NFTs on the blockchain, they serve as effective tools for securing the exchange of e-documents. In addition, NFTs in the on-chain market benefit from their minimal storage requirements, trustworthiness, and immutable transaction records, making them more suitable for trading with enhanced liquidity and security. As a result, we have established a deep link between off-chain e-documents and on-chain NFTs. This approach not only protects the copyright of e-documents, but also leverages the high liquidity of NFTs to facilitate the process of sharing e-documents. The complete process is illustrated in Fig. 3.

When creators upload e-documents to the system, the system first adds creator information and timestamps as a watermark to the e-document using digital watermarking technology. This watermarked e-document is stored on distributed, off-chain servers. The system then encrypts the storage address of the e-document using asymmetric encryption algorithms. In addition, the system uses NLP technology to extract keyword phrases from the e-document, and finally, the system compiles the ciphertext of the e-document's storage address, keyword phrases, content summary, digital watermark, and creator's digital signature as metadata. This metadata is then recorded on the blockchain, and a unique NFT is created for the e-document. NFT holders have the right to rent, sell, download, and destroy the e-document associated with the NFT they own.

- **E-document rental:** When an NFT owner and a renter agree to a read rights rental transaction, the system obtains authorization from the NFT owner. It uses a private key to decrypt the storage address of the e-document resource and automatically retrieves the e-document based on its storage address. The system extracts keyword phrases and digital watermark information from the e-document for verification, thereby confirming the authenticity of the e-document. Using the original private key, the system generates a short-term private key for the tenant with a validity period equal to the rental period. The renter can use this short-term private key

to unlock the e-document and obtain reading rights, while the e-document owner receives the rental fee (in FAN tokens) from the renter as a copyright fee.

- **E-document sale:** When an NFT owner chooses to sell the ownership of an e-document in a one-time transaction, the system still requires authorization from the NFT owner. It then follows the same process as for e-document rental to verify the authenticity of the e-document. Then, during the transaction, the system encrypts the NFT's storage address with the buyer's public key using asymmetric encryption. It also generates a new digital watermark with the buyer's information and the time of the transaction, which is attached to the e-document. After the transaction is completed, the buyer becomes the owner of the e-document. They can choose to rent reading rights or resell ownership of the e-document. The seller receives FAN tokens paid by the buyer as copyright fees.
- **E-document download:** When a user downloads an e-document, the system first performs permission verification to determine whether the user is authorized to download the resource. Only after successful verification, the user can download the e-document from the off-chain server. This approach ensures maximum privacy and security for the e-documents while guaranteeing their integrity and authenticity.
- **E-document destruction:** If an NFT owner no longer wants a particular e-document to be available for reading, or wants to increase the value of other e-documents by preventing the continued circulation of a particular e-document, they can choose to destroy that e-document. On the blockchain, NFTs can be called directly for destruction. As for e-documents on off-chain servers, they are not deleted outright. Instead, a separate storage space is allocated for them and they are marked as "destroyed". This makes the e-document invisible to all users. Considering that speculators could buy NFTs at low prices, destroy them, and then upload them back into the system to earn high rewards, these "destroyed" e-documents serve as comparison data during the system's plagiarism checks, thus preventing arbitrage activities.

3.2.3 Smart Contract-Based E-Document Access Control

To ensure the confidentiality and integrity of e-document data within the system, this paper proposes an access control method after analyzing the usage scenarios of e-documents. To prevent off-chain attackers from disrupting the system's access control module through DDoS and similar attacks, we have implemented the access control method in the form of on-chain smart contracts, which ensures tamper-proof access control and reduces the risk of attacks. The specific functions are as follows:

(1) We have established different user roles and assigned different permissions to each role, creating a role-based multi-level access control model.

(2) A dynamic permission control module was implemented, allowing NFT owners to dynamically grant and revoke permissions to visitors. Only NFT owners are allowed to download the relevant e-documents from the off-chain servers.

(3) We have also implemented a contribution-based access control method. Users who reach a certain level of contribution can access some special functions within the system. For example, the system can periodically send NFTs to users who have made significant contributions.

In summary, by setting access control permissions, the system can effectively protect the ownership rights of NFT owners over e-documents while encouraging users to participate in community development.

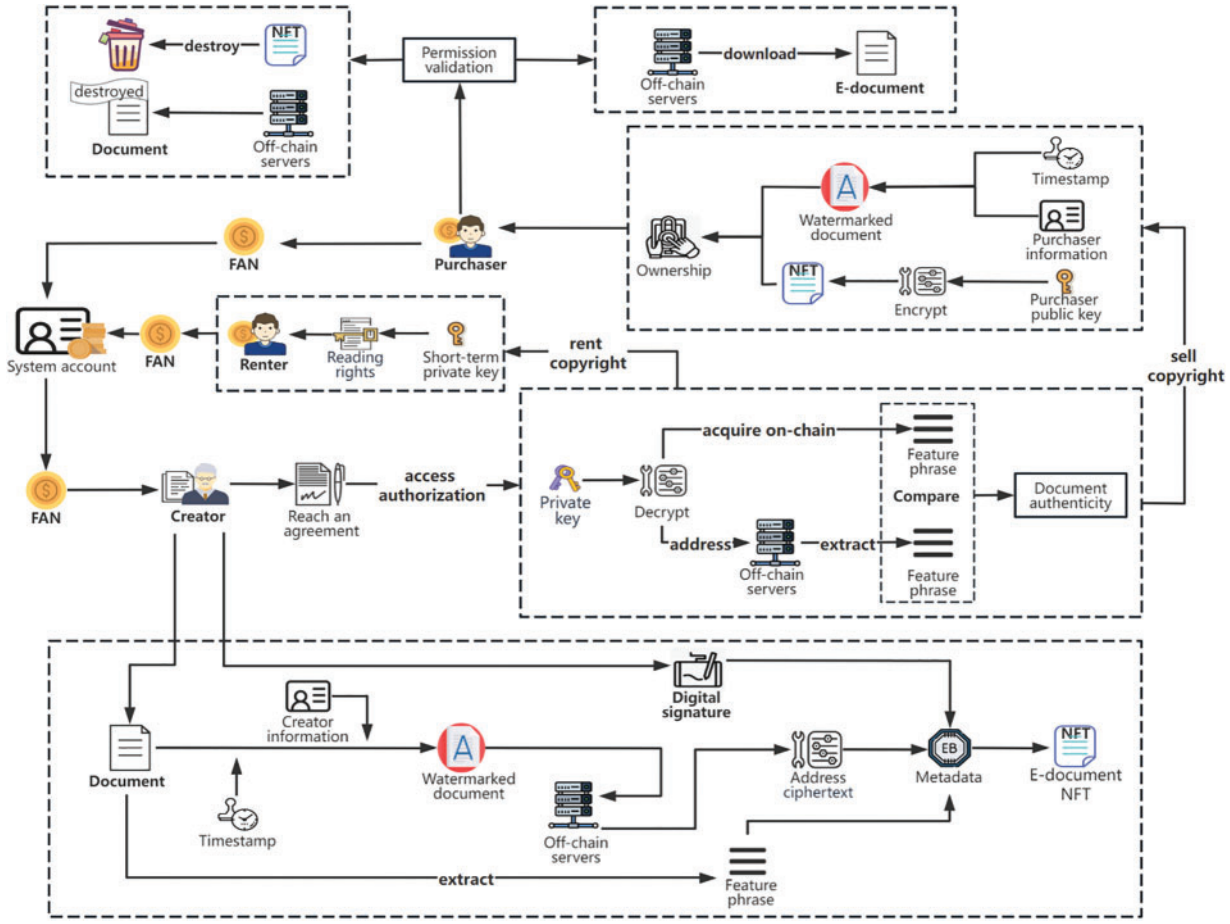

Figure 3: NFT-based e-document copyright protection and circulation process

3.2.4 E-Document Storage Combining On-Chain and Off-Chain

Blockchain is primarily used to process ledger transactions and small data due to limited block sizes, high transaction fees, and the long consensus time required to create each block. When dealing with large data, a common approach is a combination of on-chain and off-chain solutions. This involves storing the source files of large data off-chain and recording the file's storage address on the blockchain.

Inspired by the popular on-chain and off-chain hybrid solutions, we take an approach that combines off-chain storage with on-chain certification. On-chain storage is used for small data such as user identity information, transaction logs, and e-document metadata. Off-chain storage is used to store the source data of e-documents. To ensure data security, the off-chain storage solution used in this paper is a distributed storage system consisting of multiple off-chain servers.

4 Experimental Evaluation

This section focuses on the security performance of the voting mechanism and the derivation of the evolutionary game of the incentive model. Prior to this, we conduct a performance evaluation of the framework using empirical data. The framework consists of two parts: on-chain DAO and NFT, and

off-chain distributed file storage. Since DAO and NFT are deployed on Ethereum, their performance can be approximated to Ethereum's performance data. The performance of the distributed file storage system can be evaluated based on three metrics: IOPS (Input/Output Per Second), bandwidth, and latency. The detailed data is listed in Table 1.

Table 1: Empirical data to evaluate the framework performance

	On-chain			Off-chain		
Sections	DAO and NFT			Distributed file storage system		
Metrics	Throughput	Block creation time	Transaction latency	IOPS	Bandwidth	Delay
	15 TPS	about 12 s	about 15 s	about 187.5 MB/s	1.5 Gbps	about 34 ms

Based on the data presented, it appears that the combination of on-chain and off-chain components of the system is working adequately without any significant performance bottlenecks. Additionally, the system's availability is confirmed.

4.1 Security of the Governance Mechanism

In this section, we present the experimental setup and the performance of our voting mechanism. We will compare the effectiveness of our voting mechanism with current mainstream mechanisms, namely the 1T1V and 1P1V mechanisms of the Aragon platform, and the reputation voting mechanism of the Colony platform.

In the 1P1V mechanism, each participant has one vote, and all votes have the same weight, ensuring "absolute fairness". However, due to the anonymity of the blockchain, multiple on-chain voters may represent a single entity, and collusion among multiple participants is possible. Our work focuses on analyzing this scenario by setting up an experiment in which a potential adversary increases its control over on-chain voter identities after each round, in order to participate in the next round of voting.

In the 1T1V mechanism, each participant votes with the tokens they hold, where one token represents one vote. Participants with more tokens have more voting power, which can lead to unexpected results. Therefore, we set up an experiment where a potential attacker (token whale) increases its token holdings after each round in order to participate in the next round of voting.

In the reputation voting mechanism, each participant votes with the reputation they have, and there is a fixed conversion ratio between reputation and voting rights, such as 1 reputation equals 1 vote (1R1V). Similarly, participants with more reputation have more voting power, which can influence the voting outcome and lead to unexpected consequences. In our experiment, we set up a scenario where a potential attacker (reputation whale) increases its reputation after each round in order to participate in the next round of voting.

In our voting mechanism, both tokens and reputation represent the right to vote. Each participant can vote with the tokens or reputation they have. Based on the same setup, we will analyze the impact of a potential attacker (reputation whale or token whale) on the voting results in our voting mechanism.

Since it is impossible to predict the voting choices of participants in an actual election, we assume that all voters cast random votes. To increase the representativeness of random experiments, we set the total amount of voting activity in our experiment in the millions. We have 100 random voters, including

1 potential attacker, participating in 100 rounds of voting activity. Each round consists of 100 voting cycles, with 100 voting events per cycle. This setup allows us to calculate the potential attacker's voting success rate in each voting cycle.

Furthermore, in all four mechanisms, after each round of voting, the representation used by the potential attacker for voting increases by the same proportion, as shown in Fig. 4.

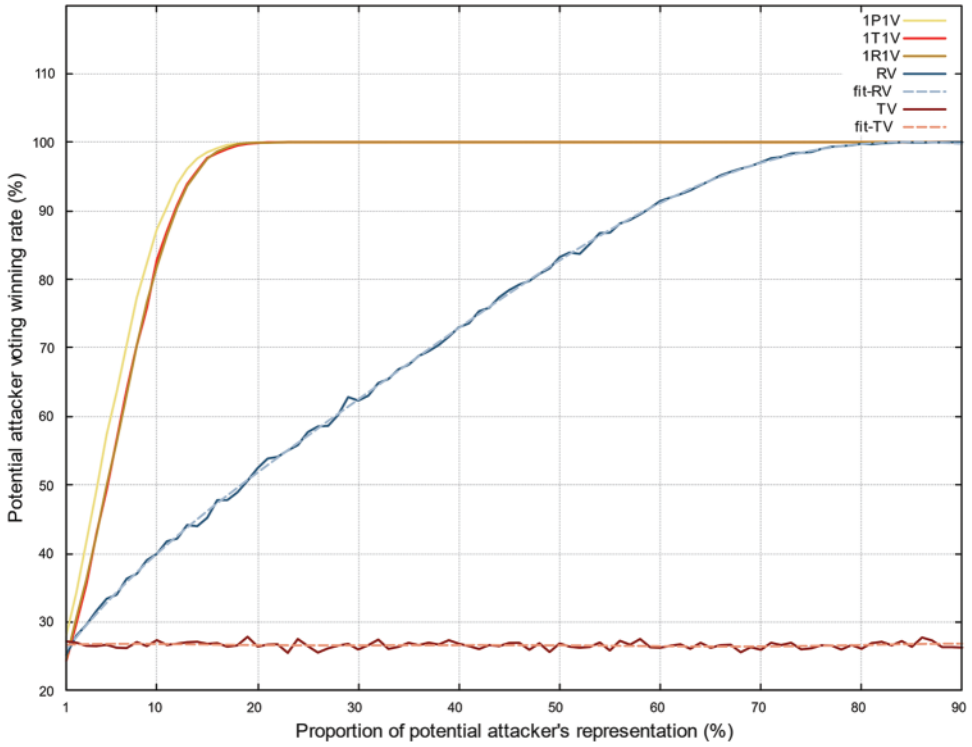

Figure 4: Influence of potential attackers in four voting mechanisms

From the figure, we can see that in the 1P1V, 1T1V, 1R1V, and our reputation voting (RV) scenarios, the potential attacker's voting influence is directly proportional to the representation they use for voting (on-chain identity, tokens, or reputation). In other words, the potential attacker's voting influence increases as they have more representation for voting, which is consistent with real-world scenarios. In addition, the growth rate of the potential attacker's voting influence is fast and nearly identical for the 1P1V, 1T1V, and 1R1V mechanisms. This indicates that without considering how the voting representation is acquired, whales have a similar influence in these mechanisms, reflecting that the essential nature of these voting mechanisms is similar. When the potential attacker's representation reach 23%, he or she will effectively determine all future voting results in these mechanisms.

In contrast, in our reputation voting scenario, the potential attacker's voting influence increases at a slower rate, and in our token voting (TV) scenario, an increase in their token holdings does not significantly affect the voting results, stabilizing around 27%. This shows that we have successfully decoupled tokens from governance.

Furthermore, we analyzed that in existing DAOs, whales typically hold voting rights in the range of 1% to 10%. Within this range, in our mechanism, reputation voting reduces the influence of whales by 39% compared to the other three mechanisms, while token voting reduces their influence by 51%.

This suggests that whales' influence is significantly reduced in our voting mechanism, thereby reducing the risk of them disrupting the system.

4.2 Evolutionary Game Modelling and Analysis

In the design of our DAO platform, there will be a game relationship between voting and creation, risk and reward, etc., which may vary with changes in participants, goals, and external conditions. Understanding and managing these relationships is crucial for the stable development of the DAO platform. In our work, we first construct an evolutionary game model [30–33]. We simulate the strategy evolution process using replicator dynamic equations, and then use the Jacobian matrix to compute and analyze the evolutionary equilibrium point of the game between creators and voters. This equilibrium point occurs when each participant chooses its optimal strategy and the strategies of the other participants are also in their optimal states, creating a balanced situation.

4.2.1 Evolutionary Game Model Construction

In our incentive mechanism, due to information asymmetry, in the game between creators and voters, creators have two possible strategies: one is to invest a lot of time and energy to actively create high-quality works, and the other is to create passively with poor-quality works. Meanwhile, voters also have two alternative strategies: one is to maintain a responsible attitude, carefully read and evaluate the creator's work, and make rational judgments, and the other is to vote casually without caring about the actual situation of the work. The following hypothetical relationship can be derived:

Assumption 1: In the creation process, creators randomly and independently choose between active and passive behavior. If creators choose to create actively, the cost is c_1, and they can benefit from it p_1, since their creation increases the resources of the platform, thereby increasing the circulation value of their works. If they choose to create passively, the cost is c_2, and the time and labor costs saved by passive creation will result in other direct economic benefits p_2. Therefore, we can assume that the probability of a creator choosing to create actively with high-quality works is x, while the probability of choosing to create passively with poor-quality works is $1 - x$.

Assumption 2: In the voting process, the behavior of voters is also random and independent. If voters choose to actively participate in platform governance, the cost is c_3. By actively participating in platform governance, they improve the system's decentralized governance capabilities, and the quality of the platform's circulating resources is higher, which brings many benefits to their own business activities p_3. If they choose to participate passively, their cost is c_4, and they may also receive other economic benefits p_4, but they will receive a reduction in platform influence n. Therefore, we can assume that the probability of a voter voting actively is y, while the probability of voting passively is $1 - y$.

Assumption 3: The platform's incentive mechanism consists of positive and negative incentives. If a creator creates passively, the platform does not receive any value from the resources, so the platform does not reward or punish voters. If a creator creates actively, the platform can gain value from the circulation of resources, so it rewards active voters with FAN tokens T. However, voters may need to expend more effort J to verify votes, and the platform also imposes a penalty of FAN tokens N on voters who perform poorly.

Assumption 4: If voters participate passively, the platform will not gain the potential value of works, so the platform will not provide incentives or penalties to creators. On the other hand, if voters actively participate, creators who actively create high-quality works will receive reputation rewards R

and token rewards S. Creators who passively produce poor-quality e-documents will be punished with a penalty F.

Based on the above assumptions, the utility matrix between creators and voters is constructed as shown in Table 2.

Table 2: Utility matrix for creators and voters

		Creators	
		Active creation	Passive creation
Voters	Active voting	$p_3 - c_3 + T - J, p_1 - c_1 + R + S$	$p_3 - c_3, p_2 - c_2 - F$
	Passive voting	$p_4 - c_4 - n - N, p_1 - c_1$	$p_4 - c_4 - n, p_2 - c_2$

4.2.2 Evolutionary Game Model Analysis

Based on the model we've constructed, we can further analyze the expected utility of participants as follows:

μ_x and μ_{1-x} represent the creators' expected utility for active creation and passive creation, respectively.

$\overline{\mu_x}$ represents the average expected utility of the creators.

μ_y and μ_{1-y} are the voters' expected utilities for active and passive voting, respectively.

$\overline{\mu_y}$ is the average expected utility of voters.

The expected utility for creators and voters under different strategies can be summarized as follows, based on the definitions above:

$$\mu_x = y(p_1 - c_1 + R + S) + (1 - y)(p_1 - c_1) \tag{6}$$

$$\mu_{1-x} = y(p_2 - c_2 - f) + (1 - y)(p_2 - c_2) \tag{7}$$

$$\overline{\mu_x} = x\mu_x + (1 - x)\mu_{1-x} = x[y(R + S) + (p_1 - c_1) + yF - (p_2 - c_2)] - yF + (p_2 - c_2) \tag{8}$$

$$\mu_x = x(p_3 - c_3 + T - J) + (1 - x)(p_3 - c_3) \tag{9}$$

$$\mu_{1-y} = x(p_4 - c_4 - n - N) + (1 - x)(p_4 - c_4 - n) \tag{10}$$

$$\overline{\mu_y} = y\mu_y + (1 - y)\mu_{1-y} = y[x(T - J) + (p_3 - c_3) - (p_4 - c_4) + n + xN] - xN + (p_4 - c_4) - n \tag{11}$$

The replicator dynamic equations describe how strategies change over time in an evolutionary game model. In the game between creators and voters, their strategies evolve in response to changing environmental conditions. The replicator dynamic equations effectively model how participants choose their strategies based on performance. When the equation equals 0, the system has reached an equilibrium point.

$$F(x) = dx/dt = x(\mu_x - \overline{\mu_x}) = x(1 - x)(y(R + S + F) - (p_2 - c_2 - (p_1 - c_1))) \tag{12}$$

$$F(y) = dy/dt = y(\mu_y - \overline{\mu_y}) = y(1 - y)(x(T - J + N) - (p_4 - c_4 - (p_3 - c_3) - n)) \tag{13}$$

Setting both x and y results in a stable state for all of the system's strategic choices. In this case, the system has five equilibrium points: (0,0), (0,1), (1,0), (1,1), and (x^*, y^*), where $x^* = \frac{p_4 - c_4 - (p_3 - c_3) - n}{T - J + N}$ and $y^* = \frac{p_2 - c_2 - (p_1 - c_1)}{R + S + F}$.

The Jacobian matrix is a matrix consisting of the partial derivatives of the replicator dynamic equations with respect to the strategies. By calculating the Jacobian matrix, we can obtain the eigenvalues associated with equilibrium points, which allows us to determine the stability of those equilibrium points. Analyzing the stability of different equilibrium points is crucial for setting the parameters involved in the game between creators and voters in the system. To judge the local stability of equilibrium points in the replicator dynamic equations, it is crucial to satisfy the conditions of $trJ < 0$ and $detJ > 0$.

$$J = \begin{bmatrix} \frac{\partial F(x)}{\partial x} & \frac{\partial F(x)}{\partial y} \\ \frac{\partial F(y)}{\partial x} & \frac{\partial F(y)}{\partial y} \end{bmatrix} \tag{14}$$

$$J = \begin{bmatrix} (1-2x)(y(R+S+F) & x(1-x)(R+S+F) \\ -(p_2 - c_2 - (p_1 - c_1))) & \\ y(1-y)(T-J+N) & (1-2y)(x(T-J+N) - (p_4 - c_4 - (p_3 - c_3) - n)) \end{bmatrix} \tag{15}$$

Equilibrium point A: When $x = 0$, $y = 0$, then:

$$trJ = -(p_2 - c_2 - (p_1 - c_1)) - (p_4 - c_4 - (p_3 - c_3) - n) \tag{16}$$

$$detJ = (p_2 - c_2 - (p_1 - c_1))(p_4 - c_4 - (p_3 - c_3) - n) \tag{17}$$

Therefore, if $p_2 - c_2 - (p_1 - c_1) > 0$ and $p_4 - c_4 - (p_3 - c_3) - n > 0$, and the conditions $trJ < 0$ and $detJ > 0$ are satisfied, the system will have a unique equilibrium point at (0,0) (Table 3). That is, when the passive benefits received by creators and voters are greater than the positive benefits, they tend to choose low-cost passive creation and voting, respectively. The ultimate evolutionarily stable strategy is {passive creation, passive voting}.

Table 3: Analysis of the stability of equilibrium point A

$p_2 - c_2 - (p_1 - c_1)$	$p_4 - c_4 - (p_3 - c_3) - n$	trJ	$detJ$	Stable point
>0	>0	<0	>0	Yes
>0	<0	Uncertainty	<0	No
<0	>0	Uncertainty	<0	No
<0	<0	>0	>0	No

Equilibrium point B: When $x = 0$, $y = 1$, then:

$$trJ = (R + S + F - (p_2 - c_2 - (p_1 - c_1))) + (p_4 - c_4 - (p_3 - c_3) - n) \tag{18}$$

$$detJ = (R + S + F - (p_2 - c_2 - (p_1 - c_1)))(p_4 - c_4 - (p_3 - c_3) - n) \tag{19}$$

Thus, when $p_2 - c_2 - (p_1 - c_1) > R + S + F$ and $p_4 - c_4 - (p_3 - c_3) - n < 0$, the system has a unique evolutionary equilibrium point at (0,1) (Table 4). This means that if the difference in utility between passive and active creation for creators is greater than the rewards and penalties imposed by the system, and if the system heavily penalizes passive voting for voters, creators will tend to choose passive creation with higher utility, and voters will tend to choose active voting to avoid the penalty. The final evolutionarily stable strategy is {passive creation, active voting}.

Table 4: Analysis of the stability of equilibrium point B

$R+S+F-(p_2-c_2-(p_1-c_1))$	$p_4-c_4-(p_3-c_3)-n$	trJ	$detJ$	Stable point
>0	>0	>0	>0	No
>0	<0	Uncertainty	<0	No
<0	>0	Uncertainty	<0	No
<0	<0	<0	>0	Yes

Equilibrium point C: When $x = 1$, $y = 0$, then:

$$trJ = (p_2 - c_2 - (p_1 - c_1)) + (T - J + N - (p_4 - c_4 - (p_3 - c_3) - n)) \tag{20}$$

$$detJ = (p_2 - c_2 - (p_1 - c_1))(T - J + N - (p_4 - c_4 - (p_3 - c_3) - n)) \tag{21}$$

From the above, we can further analyze that when $p_2 - c_2 - (p_1 - c_1) < 0$, $p_4 - c_4 - (p_3 - c_3) - n > T - J + N$, the system has a unique evolutionary equilibrium point at (1,0) (Table 5). In other words, if the benefit of active creation to creators is greater than the benefit of passive creation, and at the same time the difference in benefit between passive and active voting to voters is greater than the rewards and penalties imposed by the system, creators will tend to choose active creation, and voters will tend to choose passive voting. The final evolutionarily stable strategy is {active creation, passive voting}.

Table 5: Analysis of stability in equilibrium points C

$p_2-c_2-(p_1-c_1)$	$T-J+N-(p_4-c_4-(p_3-c_3)-n)$	trJ	$detJ$	Stable point
>0	>0	>0	>0	No
>0	<0	Uncertainty	<0	No
<0	>0	Uncertainty	<0	No
<0	<0	<0	>0	Yes

Equilibrium point D: When $x = 1$, $y = 1$, then:

$$trJ = (p_2 - c_2 - (p_1 - c_1) - (R + S + F)) + ((p_4 - c_4 - (p_3 - c_3) - n) - (T - J + N)) \tag{22}$$

$$detJ = (p_2 - c_2 - (p_1 - c_1) - (R + S + F))((p_4 - c_4 - (p_3 - c_3) - n) - (T - J + N)) \tag{23}$$

Consequently, if $p_2 - c_2 - (p_1 - c_1) < R + S + F$ and $p_4 - c_4 - (p_3 - c_3) - n < T - J + N$, satisfying the conditions $trJ < 0$ and $detJ > 0$, the system has a unique evolutionary equilibrium point at (1,1) (Table 6). This can be understood by saying that if the system provides creators and voters with larger rewards and penalties, creators will tend to actively participate in the creation of high-quality

works, and voters will also tend to actively participate in the voting and evaluating of works. The final evolutionarily stable strategy is {active creation, active voting}.

Table 6: Analysis of stability in equilibrium points D

$p_2 - c_2 - (p_1 - c_1) - (R + S + F)$	$(p_4 - c_4 - (p_3 - c_3) - n) - (T - J + N)$	trJ	$detJ$	Stable point
>0	>0	>0	>0	No
>0	<0	Uncertainty	<0	No
<0	>0	Uncertainty	<0	No
<0	<0	<0	>0	Yes

Equilibrium point E: When $x = \dfrac{p_4 - c_4 - (p_3 - c_3) - n}{T - J + N}$, $y = \dfrac{p_2 - c_2 - (p_1 - c_1)}{R + S + F}$, then:

$$trJ = 0 \tag{24}$$

$$detJ = -(p_4 - c_4 - (p_3 - c_3) - n)\left(1 - \frac{p_4 - c_4 - (p_3 - c_3) - n}{T - J + N}\right) (p_2 - c_2 - (p_1 - c_1))\left(1 - \frac{p_2 - c_2 - (p_1 - c_1)}{R + S + F}\right) \tag{25}$$

In this case, the local equilibrium point is unstable because $trJ = 0$, which does not satisfy $trJ < 0$.

According to the analysis above, the desired evolutionary equilibrium can be achieved by implementing higher rewards and penalties for creators and voters. This can be done by rewarding more reputation and FAN tokens or imposing higher penalties. In this way, creators will be incentivized to actively create high-quality works, while voters will be encouraged to actively participate in voting and evaluating e-documents.

5 Conclusion

The research demonstrates the potential of integrating blockchain, DAO, and NFT technologies to create a decentralized framework for e-document sharing. The proposed system addresses challenges in copyright protection and decentralization, presenting an alternative to centralized e-document sharing platforms. The implementation of DAO-based mechanisms for e-document quality assessment and plagiarism checks ensures the integrity and originality of the e-documents, promoting a culture of quality and innovation. Additionally, we propose a new voting mechanism for multiple user groups to address governance issues in existing DAOs. The experimental results confirm the security and efficiency of our voting mechanism, which significantly reduces the risks associated with manipulation and centralization. This study makes an important contribution by applying evolutionary game theory to analyze the incentives within the framework. The analysis reveals how the proposed system encourages participation and compliance through a balanced incentive structure that ensures the sustainability and efficiency of the ecosystem. Finally the adoption of NFT for e-document rights management showcases a novel approach to ensuring copyright protection while enhancing e-document liquidity.

Future research could investigate the scalability of this framework across various digital platforms, its applicability in other domains such as digital art or academic publishing, and the refinement of governance mechanisms within the DAO model to ensure greater security and participation equity. The work not only offers a new solution for e-document sharing but also lays the foundation for future developments in secure, decentralized content management systems.

Acknowledgement: The authors express gratitude to the editors and reviewers for their valuable suggestions on this paper, and to the foundation sponsors for their financial support of this study.

Funding Statement: This work is supported by the National Key Research and Development Program (2022YFB2702300), National Natural Science Foundation of China (Grant No. 62172115), Innovation Fund Program of the Engineering Research Center for Integration and Application of Digital Learning Technology of Ministry of Education under Grant Number No. 1331005, Guangdong Higher Education Innovation Group 2020KCXTD007, and Guangzhou Fundamental Research Plan of Municipal-School Jointly Funded Projects (No. 202102010445).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Lin Chen, Shen Su; data collection: Lin Chen, Yuting Xu, Jiaming Zhu; analysis and interpretation of results: Lin Chen, Yuting Xu; draft manuscript preparation: Lin Chen, Huanqin Zheng. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The voting scenario data used in this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Friedman D. Evolutionary games in economics. Econom: J Econm Soc. 1991;59(3):637–66. doi:10.2307/2938222.
2. IEEE Xplore. Available from: https://ieeexplore.ieee.org/. [Accessed 2023].
3. JSTOR Home. Available from: https://www.jstor.org/. [Accessed 2023].
4. CNKI. Available from: https://www.cnki.net/. [Accessed 2023].
5. Singh HK, Singh AK. Digital image watermarking using deep learning. Multimed Tools Appl. 2024;83(1):2979–94. doi:10.1007/s11042-023-15750-x.
6. Ismail A, Barbar A, Hajjar M, Quafafou M. A new document sharing system based on a semantic hierarchical peer-to-peer network. Int J Inf Educ Technol. 2017;7(5):400–5. doi:10.7763/IJET.2017.V9.960.
7. Han J, Kim H, Eom H, Son Y. A decentralized document management system using blockchain and secret sharing. In: Proceedings of the 36th Annual ACM Symposium on Applied Computing; 2021; Korea. p. 305–8.
8. Verma G, Kanrar S. Secure document sharing model based on blockchain technology and attribute-based encryption. Multimed Tools Appl. 2024;83(6):16377–94. doi:10.1007/s11042-023-16186-z.
9. Vimal S, Srivatsa SK. A new cluster P2P file sharing system based on IPFS and blockchain technology. J Ambient Intell Humaniz Comput. 2019;1–7. doi:10.1007/s12652-019-01453-5.
10. Devlin J, Chang MW, Lee K, Toutanova K. BERT: pre-training of deep bidirectional transformers for language understanding. arXiv preprint arXiv:1810.04805. 2018.

11. Nunes I, Heddes M, Vergés P, Abraham D, Veidenbaum A, Nicolau A, et al. DotHash: estimating set similarity metrics for link prediction and document deduplication. In: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining; 2023 Aug; Long Beach, CA, USA, p. 1758–69.
12. Tan Z, Wang H, Du M, Zhang J. DASH: data aware locality sensitive hashing. In: Web and big data. Cham: Springer Nature Switzerland; 2022. p. 85–100.
13. Wang S, Ding W, Li J, Yuan Y, Ouyang L, Wang FY. Decentralized autonomous organizations: concept, model, and applications. IEEE Trans Comput Soc Syst. 2019;6(5):870–8. doi:10.1109/TCSS.2019.2938190.
14. Wang Q, Li R, Wang Q, Chen S. Non-fungible token (NFT): overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447. 2021.
15. Gupta M. Reviewing the relationship between blockchain and NFT with world famous NFT market places. Scientif J Meta Blockchain Technol. 2023;1(1):1–8. doi:10.36676/sjmbt.v1i1.01.
16. Reijers W, Wuisman I, Mannan M, de Filippi P, Wray C, Rae-Looi V, et al. Now the code runs itself: on-chain and off-chain governance of blockchain technologies. Topoi. 2021;40:821–31. doi:10.2139/ssrn.3340056.
17. Buterin V. A next-generation smart contract and decentralized application platform. White Paper. 2014;3(37):1–36. doi:10.4236/jis.2016.75024.
18. McNamara DS, Graesser AC, McCarthy PM, Cai Z. Automated evaluation of text and discourse with Coh-Metrix. Cambridge: Cambridge University Press; 2014.
19. Biderman S, Schoelkopf H, Anthony QG, Bradley H, O'Brien K, Hallahan E, et al. Pythia: a suite for analyzing large language models across training and scaling. In: Proceedings of the 40th International Conference on Machine Learning; 2023 Jul; Honolulu, HI, USA, p. 2397–430.
20. Yulianti E, Pangestu N, Jiwanggi MA. Enhanced TextRank using weighted word embedding for text summarization. Int J Elect Comput Eng (IJECE). 2023;13(5):5472–82. doi:10.11591/ijece.v13i5.pp5472-5482.
21. Arabi H, Akbari M. Improving plagiarism detection in text document using hybrid weighted similarity. Expert Syst Appl. 2022;207:118034. doi:10.1016/j.eswa.2022.118034.
22. Veisi H, Golchinpour M, Salehi M, Gharavi E. Multi-level text document similarity estimation and its application for plagiarism detection. Iran J Comput Sci. 2022;5(2):143–55. doi:10.1007/s42044-022-00098-6.
23. Mansoor M, Al Tamimi M. Plagiarism detection system in scientific publication using LSTM networks. Intern J Tech Physic Prob Eng. 2022;4(4):17–24. doi:10.48175/568276.
24. Tutsoy O, Brown M. Reinforcement learning analysis for a minimum time balance problem. Trans Inst Meas Contr. 2016;38(10):1186–200. doi:10.1177/0142331215581638.
25. Tutsoy O, Brown M. An analysis of value function learning with piecewise linear control. J Exper Theor Artif Intell. 2016;28(3):529–45. doi:10.1080/0952813X.2015.1020517.
26. aragon.org. Available from: https://aragon.org/. [Accessed 2023].
27. Peña-Calvin A, Saldivar J, Arroyo J, Hassan S. A categorization of decentralized autonomous organizations: the case of the Aragon platform. IEEE Trans Comput Soc Syst. 2023, Early Access. doi:10.1109/TCSS.2023.3299254.
28. colony.io. Available from: https://colony.io/. [Accessed 2023].
29. Lalley SP, Weyl EG. Quadratic voting: how mechanism design can radicalize democracy. In: AEA Papers and Proceedings. American Economic Association; 2018. vol. 108, p. 33–7.
30. Yilin Z, Huimin M. Research on incentive mechanism of environmental sanitation self-regulatory organization based on evolutionary game theory. Oper Res Manag. 2021;30(4):115–21. doi:10.1371/journal.pone.0256046.
31. Fan W, Wang S, Gu X, Zhou Z, Zhao Y, Huo W. Evolutionary game analysis on industrial pollution control of local government in China. J Environ Manag. 2021;298:113499. doi:10.1016/j.jenvman.2021.113499.

32. Gao L, Yan A, Yin Q. An evolutionary game study of environmental regulation strategies for marine ecological governance in China. Front Mar Sci. 2022;9:1048034. doi:10.3389/fmars.2022.1048034.
33. Cao W, Yu J. Evolutionary game analysis of factors influencing green innovation in Enterprises under environmental governance constraints. Environ Res. 2024;248:118095. doi:10.3390/su14137807.