Decentralized Funding of Public Goods in Blockchain System: Leveraging Expert Advice

Jichen Li, Yukun Cheng*, Wenhan Huang, Mengqian Zhang,
Jiarui Fan, Xiaotie Deng*, *Fellow, IEEE,* Jan Xie and Jie Zhang

***Abstract*—Public goods projects, including open-source technology, client development, and blockchain knowledge education, play a crucial role in the thriving blockchain ecosystem. Consequently, the decision-making process for funding public goods is a significant concern within blockchain ecosystem studies. This work develops a human oracle protocol approach that involves experts, funders, and public goods projects to address the problem of investing in public goods on the blockchain. In our human oracle approach, funders contribute their investments, which are stored in a funding pool. Experts provide investment advice based on their experience with public goods projects. The decisions made by the human oracle regarding the amount of support from the funding pool are based on the reputation of the experts. The reputation of each expert is updated according to the project's implementation performance compared to their advice. In other words, better investment performance leads to a higher reputation. Besides being applied to static model, our human oracle can also be extended to accommodate dynamic setting, in which the experts might leave or join the decision- making process. Therefore, we introduce a regret bound to measure the effectiveness of our human oracle. Theoretically, we prove an upper regret bound for both static and dynamic models and demonstrate its tightness with an asymptotically equal lower bound. Empirically, we provide evidence that our oracle's investment decisions closely align with optimal investments in hindsight. This highlights the efficiency and effectiveness of our human oracle approach in guiding funding decisions for public goods projects in the blockchain ecosystem.**

***Index Terms*—Class, IEEEtran, LaTeX, paper, style, template, typesetting.**

I. Introduction

With the exponential growth of the blockchain ecosystem in recent years, participants now have a greater demand for not only efficient transaction capabilities but also a wide range of functionalities from blockchain systems. In order to attract more individuals to join the blockchain ecosystem, sponsors with capital on the blockchain aspire to incentivize and support the development of public goods projects. These projects encompass various aspects such as client development, open-source technology, knowledge databases, and more, all aimed at fostering the flourishing of the blockchain ecosystem. One notable platform dedicated to fundraising for blockchain public goods is Gitcoin Grants [1]. Supported by the Ethereum Foundation and other blockchain systems, Gitcoin Grants provides a dedicated space for raising funds specifically for public goods in the blockchain realm. At present, there is a remarkable lineup of nearly 3000 public goods projects awaiting funding from this platform.

The Gitcoin Grants platform presently employs the Quadratic Funding (QF) protocol [2] for matching project funding. This protocol collects funds into an investment pool and distributes them based on the number of donors and the amount donated to each project. While the QF protocol is efficient in allocating investments, it does have several drawbacks.

Firstly, the QF protocol can be influenced by the biases of the crowd, resulting in a skewed estimation of project utility by donors. The QF protocol relies on the donors' predictions of the utility that they will receive from the project. However, those predictions may not be accurate in practice. Even worse, the whole community may have a prejudice toward projects, leading to an unsuitable investment allocation [3]. Secondly, the QF protocol lacks the ability to utilize hindsight, such as feedback on previous project utilities, to inform investment decisions for subsequent projects. This limitation prevents the correction of investment mistakes made in previous projects. Furthermore, the QF protocol is highly susceptible to Sybil attacks [4]. These attacks exploit the ease and low cost of creating new identities, allowing for the forging of fictitious identities to manipulate the allocation of funds. In 2021, the Gitcoin platform reported that they detected more than 1,377 times of attacks within a 3 months grants [5]. Although the platform subsequently utilizes identity authentication technology to prevent sybil attacks as much as possible, this phenomenon cannot be completely eliminated.

These deficiencies highlight the practical challenges faced by the QF protocol in terms of accurate utility predictions, the absence of feedback on project implementation, and vulnerability to Sybil Attacks. Addressing these issues is crucial for improving the effectiveness and integrity of project funding allocation on the Gitcoin Grants platform.

To tackle the aforementioned challenges, we integrate the "prediction with experts' advice" framework [6]–[8] into our human oracle for funding public goods projects in the blockchain system. The design of this framework revolves

*Corresponding authors.

J. Li and X. Deng are with the Center on Frontiers of Computing Studies, Computer Science Department, Peking University, Beijing, China. Email: {limo923, xiaotie}@pku.edu.cn

Y. Cheng is with the School of Business, Jiangnan Univeristy, Wuxi, China. Email: ykcheng@amss.ac.cn

W. Huang and M. Zhang are with School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. Email: {rowdark, mengqian}@sjtu.edu.cn

J. Fan is with Tsinghua University, Beijing, China. Email: fanjr20@mails.tsinghua.edu.cn

J. Xie is with Cryptape, Beijing, China. Email: jan@cryptape.com

J. Zhang is with School of Business, the Univeristy of Bath, Bath, Engliand. Email: jz2558@bath.ac.

around several key concepts: maintaining a group of experts from the community, making investment decisions based on the advice of highly reputable experts, and adjusting expert reputations based on project performance in hindsight.

Incorporating expert opinions into the investment process for public goods projects offers several advantages. Firstly, experts possess extensive investment experience, which can lead to more accurate predictions regarding project performance. Secondly, by updating expert reputations based on project performance, the protocol can select appropriate experts with higher reputations, resulting in more precise project investments. Finally, in our protocol, funders' donations are stored in the funding pool, eliminating any incentives for them to engage in Sybil attacks.

However, experts, who are not involved in the Quadratic Funding (QF) mechanism, may attempt to profit from Sybil attacks. Therefore, our human oracle implements identity verification for each expert during the registration phase, effectively countering Sybil attacks by experts. Importantly, funders or donors are not required to provide any identification to the protocol, fostering a high willingness to donate. This approach strikes a balance between ensuring the integrity of the system and maintaining the privacy and convenience of funders and donors.

When applying the existing expert advice framework to public goods investment, we encounter the following problems that need to be addressed.

1) Evaluation of Expert Advice: The existing prediction protocols with expert advice typically calculate the loss of each expert by comparing the actual performance of a project with their prediction for that project. However, in the case of public goods investment, the feedback received only pertains to the performance of projects under one expert's investment advice. As a result, this feedback cannot be directly utilized to evaluate the advice provided by other experts.
2) Evaluation of Expert Advice: The existing prediction protocols with expert advice typically calculate the loss of each expert by comparing the actual performance of a project with their prediction for that project. However, in the case of public goods investment, the feedback received only pertains to the performance of projects under one expert's investment advice. As a result, this feedback cannot be directly utilized to evaluate the advice provided by other experts.

The main contribution of this work is to design an investment protocol for a human oracle, consisting of three types of participants: funders, projects, and experts, for the public goods projects investment problem in blockchain system. Funders continuously contribute their investments to a funding pool. Each project proposes a request for investment for its development. Experts submit their investment advice for those projects. With continuous investment flow, we assume that the pool usually has sufficient funds for a project.

To settle the first problem, we require the investment protocol to gather the advice from experts twice for each project. At first, the experts shall submit their investment advice separately. After receiving all advice, the protocol goes to select one expert based on the reputations of experts. Once one expert's advice is adopted, all experts are required to submit their predictions for the performance of project under the selected advice. Then our protocol computes the loss of each expert by comparing the actual project's performance and her prediction for performance under this selected investment advice. To sum up, the first advice of all experts is used to select an appropriate expert, and the second one is used to compute the loss of each expert.

We first study the static setting, in which no experts are offline and all experts remain in the expert set. To settle the above second problem, we extend our protocol to a more general dynamic setting, where some experts may leave and some new ones may join in the expert set. For both of two settings, we provide the lower bounds of the worst cases on the ranking regret and show that the upper bounds of our protocol asymptotically matches these lower bounds.

The rest of this paper is organized as follows. Section II introduces the background and the related work on the public goods investment problem. In Section III, we propose the structure and components of our investment protocol. In Section IV, we theoretically analyze the lower bounds of the worst cases on the ranking regret and prove that the upper bounds of our protocol matches these lower bounds within a constant factor. Last section conducts a series of experiments to demonstrate the effectiveness of our protocol.

II. Background and Related Work

A. Quadratic Funding

The quadratic funding (QF) protocol, proposed by Buterin et al. [2], presents a mechanism for funding public goods within a blockchain system. This protocol assumes that funders have quasi-linear utility functions and aim to achieve socially optimal outcomes when there is complete information. However, directly applying the QF protocol to settings with non-quasi-linear utility functions may not be appropriate. Pasquini et al. [3] highlighted this limitation when considering a funding pool with limited funds, such as Gitcoin Grants [1]. They pointed out that the social efficiency of the QF protocol relies on the ratio between the actual subsidy and the ideal subsidy. Furthermore, when dealing with incomplete information, the efficiency property of the QF protocol is only satisfied under highly restricted conditions [9]. Although some work has attempted to study the Quadratic Mechanism with imperfect information, they have only discussed it in simple voting settings [10]. Therefore, extending the application of quadratic funding beyond complete information remains a crucial problem that needs to be addressed.

B. Prediction with Experts Advice

The prediction with expert advice problem is a well-known learning problem that was first introduced as a framework for online learning in 1994 [6]. In this problem, a *learner* is faced with an online optimization task, where they must make a decision at each round regarding which of the n experts' advice to follow. Simultaneously, the learner has access to the gains obtained in all previous rounds, except

for the current round t, and chooses one expert based on the historical performances. At each round t, an *adversary* sets the gains for all experts. If the adversary has access to the learner's choices from all previous rounds and sets the gains accordingly in round t, we refer to it as a "fully adversary". This decision-making process is repeated for a total of T rounds, and the learner's objective is to optimize her cumulative gain throughout the process.

To analyze the performance of a decision algorithm in this online optimization problem, the classical regret is introduced:

$$R(T) = \sum_{t=1}^{T} \boldsymbol{w_t} \boldsymbol{l}_t - \min_{j \in [n]} \sum_{t=1}^{T} l_{t,j}, \tag{1}$$

where $\boldsymbol{w_t}$ is the vector of experts' chosen probability and $\boldsymbol{l}_t$ is the vector of losses in round t.

The most famous classical algorithm in the prediction with expert advice framework is Hedge Algorithm [11]. The Hedge algorithm sets the weights of all experts as one initially. Then in each round t, the learner makes a decision based on experts' weights. After the decision, the learner will receive an optimal decision g_t and update each expert's weight according to the distance between her advice and g_t. This design enables that the master algorithm makes not many more mistakes than the best expert, even without any prior knowledge about their expertise level. The classical regret of Hedge algorithm is $O(\sqrt{T \ln n})$ and further works [12], [13] improve the efficiency of the algorithm in applications.

However, although the Hedge algorithm is effective, it does not work when the expert set changes in the process, that is, the sleeping experts setting [11], [14]. As the computational hardness of the sleeping experts setting is well-proved by [15]–[17], several previous works research on the sleeping experts setting under some restrictions. For example, [18] discussed the case that the expert set only grows up, while in [19], the experts set only shrinks. However, there is no study on the situation of the substitution of experts. In the substitution setting, the number of available experts is constant, while some of them may be substituted by new comers. Formally, for the set of experts $E = \{e_1, \cdots, e_N\}$, at each round $t \in \{1, 2, ..., T\}$, the adversary chooses a set of experts E_t to be available such that $|E_t| = n$. In other words, the adversary sets some experts to sleep forever. Meanwhile, it brings an equal number of new experts. As [15], [17], [20], we adopt the ranking regret as our notion of regret. Let us denote π and Π as an ordering over the set of all experts E and the set of all permutations, respectively. The first available expert of permutation π in round t is $\sigma^{\pi}(t)$. The cumulative loss of π with respect to experts E_t is the sum of the loss of $\sigma^{\pi}(t)$ at each round. Then the ranking regret is defined as:

$$R_{\Pi}(T) = \sum_{t=1}^{T} \boldsymbol{w_t} \boldsymbol{l_t} - \min_{\pi \in \Pi} \sum_{i=1}^{T} l_{t,\sigma^{\pi}(t)}, \tag{2}$$

where $\boldsymbol{w_t}$ is the vector of weights for available experts and $\boldsymbol{l}_t$ is the vector of experts' losses in round t.

C. Human Oracle

The human oracle is a mechanism that incorporates data obtained from human responses to specific problems into the blockchain system. Individuals with blockchain accounts can input blockchain data by answering formal or informal inquiries and signing transactions. Human oracles are commonly utilized for voting and assessing answers to problems. Chainlink [21] employs a K-out-of-M multi-signature approach to achieve consensus among M different oracles, some of which can be humans. If the same answer is reported by at least K oracles, it is deemed acceptable. Chainlink oracles are primarily utilized by DeFi projects and applications to provide market prices. Gnosis and Augur [22] employ human oracles for voting, allowing individuals with blockchain accounts to dispute reported results by staking their tokens if they disagree with the current answer.

Human oracles can also provide answers for problems with arbitrary formats. Reality.eth is an on-chain smart contract oracle system that relies on crowd-sourcing, where individuals can post and answer questions. Participants can answer with a bond or correct an incorrect answer by providing a bond at least twice the value of the previous answer's bond. If their answer becomes the final answer, they can retrieve their bonds; otherwise, their bonds are awarded to those who supply the correct answer.

However, human oracles are highly based on 'the wisdom of crowds'. The outcome of a human oracle is a 'belief' of current crowds in blockchain systems so that attackers can manipulate it. Human oracles usually introduce verification periods [23] or forks [22] to protect the benefits of honest agents. The fork is to divide people into several groups, each of which has a similar opinion and belongs to a corresponding universe [22]. The verification periods employ several people [23] or experts [24] to redress the prejudice of the crowds.

D. Project Evaluation

Directly evaluating a project can be challenging and nuanced due to the inherent differences in project nature and the subjective and incomplete nature of people's information. However, using indicators to assess projects across various domains can offer a viable alternative to address these existing challenges. The indicator approach, as exemplified by Takim [25] in the assessment of construction projects and generalized by Koelmans [26] in measuring project success, has been chosen. In our discussion, we have compiled relevant indicators for public goods and reorganized them to provide a more comprehensive means of project evaluation.

We are interested in the post-project indicators. Post-project indicators are crucial to measuring the success of a project and evaluating its value. At this level, many useful indicators stem directly from the design and implementation of the project, assessing success on the basis of process and execution. Koelmans [26] mentioned fundamental indicators such as progress schedule and cost, in terms of time and finance respectively. As Sohn and Joo [27] found out, process factors can also involve adjustment of strategy, periodic conquest of technological gap, and improvement of a manufacturing environment, etc.

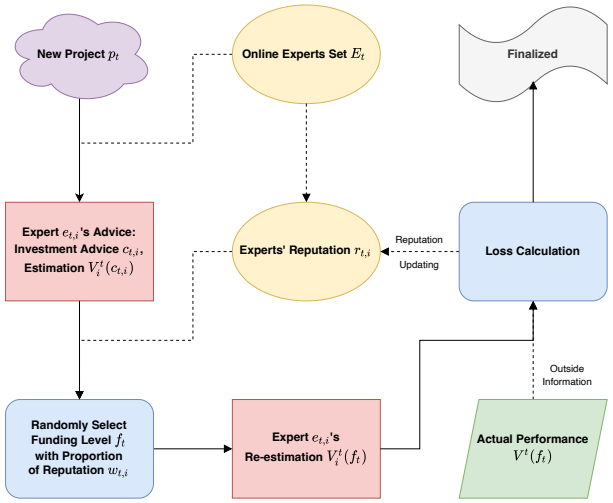

Fig. 1. Investment Protocol Flowchart.

These indicators are not only the manifestations of project performance but also partially deterministic of the future success of the project.

III. Model

In this paper, we study the problem of public goods investment in a blockchain society, wherein a series of potential public goods projects $P = \{p_1, ..., p_T\}$ are proposed continuously in rounds T. In this context, the society can be considered as a community or group of participants, aiming to fund these public goods. Let $V^t(f_t)$ represent the utility of the public good project p_t, which is a value function associated with the funding level f_t. Similar to the Quadratic Funding protocol [9] and other established economic models [28], [29], we assume that V^t is concave, smooth, and increasing.

Our objective is to develop a funding investment protocol within the blockchain system that incorporates expert advice. When a public good p_t is proposed, our investment protocol should determine the appropriate funding level f_t. The goal of the protocol is to maximize the overall net social welfare of all projects, which can be expressed as follows:

$$SW = \sum_{t=1}^{T} (V^t(f_t) - f_t). \tag{3}$$

A. Protocol Outline

Our investment protocol operates through multiple rounds, indicated by $t \in \{1, 2, ..., T\}$. Each round commences when a new project p_t is proposed. In each round t, a group of n experts, denoted as $E_t = \{e_{t,1}, \cdots, e_{t,n}\}$, provides investment advice for the project and operates as follows. We need to mention that the identity of experts may vary from one round to another.

At the beginning of round t, each expert $e_{t,i}$ possesses a reputation value of $r_{t,i}$, which is carried over from the previous round. The oracle maintains the list of expert reputations $R_t = \{r_{t,1}, \cdots, r_{t,n}\}$, satisfying $r_{t,i} \in \mathbb{R}^+$. When round t begins, every expert i initially recommends an investment level $c_{t,i}$ and provides an estimation $V_i^t(c_{t,i})$ for the project p_t's social welfare under the recommended investment level. Subsequently, the investment protocol randomly selects an expert with a selection probability proportional to their reputation value, which can be expressed as:

$$w_{t,i} = \frac{r_{t,i}}{\sum_{k=1}^{n} r_{t,k}}. \tag{4}$$

Here the selection probability $w_{t,i}$ can also be interpreted as the weight assigned to expert $e_{t,i}$. The vector of weight in round t is denoted as $\boldsymbol{w}_t = (w_{t,1}, \cdots, w_{t,n})$. Once an expert $e_{t,i}$ is selected, their investment advice is implemented, and project p_t is funded at the designated funding level $f_t = c_{t,i}$. After receiving information about the funding level f_t, all experts must submit their estimations $\widehat{V}_i^t(f_t)$. Concurrently, project p_t begins to be implemented, and the oracle receives an evaluation of the project's social welfare, $V^t(f_t)$, after a fixed period of time. It is important to note that $\widehat{V}_i^t(f_t)$ represents the subjective estimation from expert i, while $V^t(f_t)$ signifies the objective performance measured from various dimensions (further details on project evaluation will be discussed in Section III-F).

Based on the evaluation $V^t(f_t)$, the protocol calculates the loss for each expert i, and utilizes it to update their reputation. At the conclusion of round t, project p_t is invested at funding level f_t, and all n experts have their reputations updated. A high-level overview of the investment protocol's functioning is illustrated in Figure 1 and the primary notations utilized in this article are presented in Table I.

B. Protocol Initialization

Our oracle differs from Gitcoin Grants in that it allows all funders to continuously contribute to the funding pool. In the event that there are existing public goods projects awaiting funding in the oracle, these projects will be randomly arranged, and all funders will collectively agree on the resulting project list denoted as P. [1] The investment protocol then proceeds to invest in each project sequentially, following the order specified in P. As soon as the investment protocol is initiated, any new public goods projects will be automatically incorporated into this list. In addition, at the start of the first round, the initial reputation of each expert is initialized by

$$r_{1,1} = r_{1,2} = . \cdots = r_{1,n} = 1.$$

C. Project Prediction

According to the investment protocol framework, when project p_t is decided for funding under level f_t, all experts, except for the one whose advice is adopted, are required to submit their estimations denoted as $\widehat{V}_i^t(f_t)$. Similar to the assumption made for V^p, we also force that all value functions $\widehat{V}_i^p$ should be concave and increasing. Additionally, we have the condition $V^t(0) = 0$, since a project cannot be implemented without any investment. Therefore, the value of $\widehat{V}_i^t(f_t)$ is bounded by the following lemma.

[1] For infrastructure projects or projects of utmost importance, we recommend funders to consider ad-hoc investments instead of utilizing our protocol.

TABLE I
MAIN NOTATIONS

T	The number of the total rounds;
m	The number of the substitute rounds in the total T rounds;
N	The total number of experts in the system;
n	The number of involved experts in each round;
$P = \{p_1, p_2, \cdots, p_T\}$	The set of project ; $\|P\| = T$ and p_t is the project in round t;
$E_t = \{e_{t,1}, \cdots, e_{t,n}\}$	The set of involved experts in the round t; $\|E_t\| = n$;
$R_t = \{r_{t,1}, \cdots, r_{t,n}\}$	The set of expert reputations in the round t; $\|R_t\| = n$ and $r_{t,i}$ is the reputation of expert $e_{t,i}$ in the round t;
$C_t = \{c_{t,1}, \cdots, c_{t,n}\}$	The set of experts' advice for project p_t in the round t; $\|C_t\| = n$ and $c_{t,i}$ is the advise of expert $e_{t,i}$ in the round t;
$\boldsymbol{w}_t = (w_{t,1}, \cdots, w_{t,n})$	The weight vector of experts in round t, where $w_{t,i}$ is proportional to the reputation of expert $e_{t,i}$;
$\boldsymbol{l}_t = (l_{t,1}, \cdots, l_{t,n})$	The loss vector of experts in round t, where $l_{t,i}$ is the loss of expert $e_{t,i}$;
$F = \{f_1, \cdots, f_T\}$	The set of investment decision in the protocol;
$L_t = \{l_{t,1}, \cdots, l_{t,n})\}$	The set of experts' losses in round t, $\|L_t\| = n$ and $l_{t,i}$ is the loss of expert $e_{t,i}$ in round t.

Lemma 1. *If expert $e_{t,i}$ is hnoest, her prediction $\widehat{V}_i^t(f_t)$ must satisfy the following conditions:*
(1) If $f_t \leq c_{t,i}$, then

$$\frac{f_t}{c_{t,i}}\widehat{V}_i^t(c_{t,i}) \leq \widehat{V}_i^t(f_t) \leq \widehat{V}_i^t(c_{t,i}) - c_{t,i} + f_t.$$

(2) If $f_t > c_{t,i}$, then

$$\widehat{V}_i^t(c_{t,i}) < \widehat{V}_i^t(f_t) < \min\{\frac{f_t}{c_{t,i}}\widehat{V}_i^t(c_{t,i}), \widehat{V}_i^t(c_{t,i}) - c_{t,i} + f_t\}.$$

Proof. Given that expert $e_{t,i}$ is assumed to be honest, her advice regarding $c_{t,i}$ should aim to maximize the net social welfare based on her prediction function $\widehat{V}_i^t$. Therefore,

$$\widehat{V}_i^t(f_t) - f_t \leq \widehat{V}_i^t(c_{t,i}) - c_{t,i}. \tag{5}$$

Under the assumption that V_i^t is concave and $f_t \leq c_{t,i}$, it is straightforward to conclude that

$$\frac{\widehat{V}_i^t(f_t)}{f_t} \geq \frac{\widehat{V}_i^t(c_{t,i}) - \widehat{V}_i^t(0)}{c_{t,i} - 0}. \tag{6}$$

By combining the inequalities (5) and (6), we obtain

$$\frac{f_t}{c_{t,i}}\widehat{V}_i^t(c_{t,i}) \leq \widehat{V}_i^t(f_t) \leq \widehat{V}_i^t(c_{t,i}) - c_{t,i} + f_t.$$

On the other hand, when $f_t > c_{t,i}$, there should be

$$\widehat{V}_i^t(f_t) > \widehat{V}_i^t(c_{t,i}), \tag{7}$$

Algorithm 1 Investment Protocol for Static Setting

Input: A list of project $P = \{p_1, \cdots, p_T\}$.
Output: A list of investment value $F = \{f_1, \cdots, f_T\}$.

for $i = 1, \cdots, n$ **do**
  $r_{1,i} = 1$ ▷ Initialize the reputation
for $t = 1, 2, \cdots, T$ **do**
  Each expert i submits its $c_{t,i}$ and $V_i^t(c_{t,i})$
  for $i = 1, \cdots, n$ **do**
    $w_{t,i} = \frac{r_{t,i}}{\sum_{k=1}^{n} r_{t,k}}$
  Select an expert $e_{t,i}$ with the probability of $w_{t,i}$
  Fund the project p_t with the value $f_t = c_{t,i}$
  Each expert $e_{t,i}$ re-submits its estimation $\widehat{V}_i^t(f_t)$
  Observe the actual performance $V^t(f_t)$
  for $i = 1, \cdots, n$ **do**
    $l_{t,i} = |V^t(f_t) - \widehat{V}_i^t(f_t)|$
    $r_{t+1,i} = r_{t,i}e^{-\eta l_{t,i}}$

under the assumption that $\widehat{V}_i^t$ is increasing. Also, the concavity of $\widehat{V}_i^t$ guarantees

$$\frac{\widehat{V}_i^t(f_t) - \widehat{V}_i^t(0)}{f_t - 0} < \frac{\widehat{V}_i^t(c_{t,i})}{c_{t,i}}. \tag{8}$$

By combining in-equations (5), (7) and (8), we obtain

$$\widehat{V}_i^t(c_{t,i}) < \widehat{V}_i^t(f_t) < \min\left\{\frac{f_t}{c_{t,i}}\widehat{V}_i^t(c_{t,i}), \widehat{V}_i^t(c_{t,i}) - c_{t,i} + f_t\right\}.$$

This lemma holds. □

Lemma 1 demonstrates that the estimate $\widehat{V}_i^t(f_t)$ of an honest expert cannot assume arbitrary value; rather, it is bounded within a reasonable interval. This finding proves instrumental in assessing the efficiency of our investment protocol.

D. Evaluation and Reputation update

In the evaluation phases of the protocol, it is essential to utilize a set of quantifiable indicators to measure the performance of public goods projects. This evaluation process allows for the updating of expert reputations. An expert's reputation is a reflection of the accuracy of their predictions regarding project investments. Consequently, experts with higher reputations are more likely to have their advice adopted by the protocol. Moreover, an expert's reputation should be updated based on their predictions concerning the performance of the current project, once the project has received funding. Specifically, following the funding of project p_t at level f_t, each expert must submit their prediction $\widehat{V}_i^t(f_t)$, and the actual performance $V^t(f_t)$ of project p_t can be observed after a specified time period has elapsed. As a result, the prediction loss of expert $e_{t,i}$ is defined as

$$l_{t,i} = |V^t(f_t) - \widehat{V}_i^t(f_t)|. \tag{9}$$

Let $\boldsymbol{l}_t = (l_{t,1}, \cdots, l_{t,n})$ represent the vector of losses in round t. Once all losses $\{l_{t,i}\}$ have been obtained, the protocol proceeds to update the reputation of expert $e_{t,i}$ at the end of round t by

$$r_{t+1,i} = r_{t,i}e^{-\eta l_{t,i}}, \tag{10}$$

Algorithm 2 Investment Protocol for Dynamic Setting

Input: A list of project $P = \{p_1, \cdots, p_T\}$.
Output: A list of investment value $F = \{f_1, \cdots, f_T\}$.

for $t = 1, 2, \cdots, T$ **do**
  if $t = 1$ **then**
    Select n experts uniformly to form E_1
    for $i = 1, \cdots, n$ **do**
      $r_{1,i} = 1$ ▷ Initialize the reputation
  else
    $E_t = E_{t-1}$
    $Die_t \leftarrow$ unavailable experts in E_t
    $d_t \leftarrow |Die_t|$
    Remove Die_t from E_t and uniformly select d_t experts from $N - \bigcup_{k=1}^{t-1} E_k$
    if $d_t == 0$ **then**
      $r_{t,i} = r_{t-1,i} \cdot e^{-\eta l_{t-1,i}}$
    else
      for all $e_{t,i} \in E_t - E_{t-1}$ **do**
        $r_{t,i} = (1-\alpha) \cdot \frac{1}{n} \cdot \sum_{k=1}^{n} r_{t-1,k} \cdot e^{-\eta l_{t-1,k}}$
      for all $e_{t,i} \in E_t \cap E_{t-1}$ **do**
        $r_{t,i} = (1-\alpha) \cdot \frac{1}{\eta} \cdot \sum_{k=1}^{n} r_{t-1,k} \cdot e^{-\eta l_{t-1,k}}$
        $+\alpha \cdot r_{t-1,i} \cdot e^{-\eta l_{t-1,i}}$
        $+\alpha \cdot \frac{1}{n-d_t} \cdot \sum_{k \in Die_t} r_{t-1,k} \cdot e^{-\eta l_{t-1,k}}$
  Each expert i submits its $c_{t,i}$ and $V_i^t(c_{t,i})$
  for $i = 1, \cdots, n$ **do**
    $w_{t,i} = \frac{r_{t,i}}{\sum_{k=1}^{n} r_{t,k}}$
  Select an expert $e_{t,i}$ with the probability of $w_{t,i}$
  Fund the project p_t with the value $f_t = c_{t,i}$
  Each expert i re-submits its estimation $\widehat{V}_i^t(f_t)$
  Observe the actual performance $V^t(f_t)$
  for $i = 1, \cdots, n$ **do**
    $l_{t,i} = |V^t(f_t) - \widehat{V}_i^t(f_t)|$

where $\eta > 0$ is a predetermined parameter.

E. Static Setting and Dynamic Setting

In each round t, a group of n experts $E_t = e_{t,1}, \cdots, e_{t,n}$ provide their advice. If $E_1 = \cdots = E_T$, indicating that the expert set remains the same throughout the entire process, this configuration is referred to as the *Static Setting*. The investment protocol for the static setting is outlined in Algorithm 1. However, due to various reasons, such as experts being offline or their reputations falling below a preset threshold θ, the expert set may change in the subsequent round. In the Investment Protocol, it is necessary to maintain a constant size of the expert set in each round. Therefore, when some experts expire, new experts need to be added to the expert set. This gives rise to a *Dynamic Setting*, as illustrated in Algorithm 2.

Suppose that there are N experts in the oracle, with n experts selected to provide recommendations in each round. Initially, the expert set E_1 is created by uniformly selecting each expert with a probability of $\frac{n}{N}$. In subsequent rounds $t\ (\geq 2)$, the expert set E_t may be updated by eliminating some experts and introducing new ones. Let Die_t denote the set of experts who are removed from E_{t-1}, specifically, $Die_t = E_{t-1} - E_t$. The size of Die_t is denoted by $|Die_t| = d_t$. To ensure that there are still n participating experts in round t, d_t experts are uniformly selected from the waiting expert set $N - \bigcup_{k=1}^{t-1} E_k$ and included in this round. Thus, we have

$$E_t = (E_t \cap E_{t-1}) \cup (E_t - E_{t-1}),$$

where each expert in $E_t \cap E_{t-1}$ is considered a senior expert, while all new experts are in $E_t - E_{t-1}$. Additionally, if $d_t > 0$, round t is referred to as a *substitute round*; otherwise, it is called a *normal round*. Suppose there are m substitute rounds out of the total T rounds.

In the dynamic setting, a crucial concern arises when establishing the reputation of new experts if $d_t > 0$. In order to address this matter, our investment protocol initializes the reputation of new expert $e_{t,i} \in E_t - E_{t-1}$ as

$$r_{t,i} = (1-\alpha)\frac{\sum_{k=1}^{n} r_{t-1,k} \cdot e^{-\eta l_{t-1,k}}}{n}, \tag{11}$$

where $\alpha \in [0, 1]$ represents a predetermined parameter. The initial reputation of a new expert, as shown in (11), is derived from a discounted average of the reputations of all participating experts in round $t-1$. For senior experts $e_{t,i} \in E_t \cap E_{t-1}$, their reputation is set to

$$\begin{aligned} r_{t,i} = (1-\alpha)\frac{\sum_{k=1}^{n} r_{t-1,k} \cdot e^{-\eta l_{t-1,k}}}{n} \\ + \alpha r_{t-1,i} \cdot e^{-\eta l_{t-1,i}} + \alpha \frac{\sum_{k \in Die_t} r_{t-1,k} \cdot e^{-\eta l_{t-1,k}}}{n - d_t}. \end{aligned} \tag{12}$$

Referring to equation (12), it is evident that the reputation $r_{t,i}$ of senior expert $e_{t,i}$ is a combination of their previous round's reputation, a partial of the total reputations, and a share of expired experts' reputations from round $t-1$. This is accomplished through a technique where each senior expert continues to use their index from the previous round, while the new expert inherits the index of one removed expert.

F. Implementation Instance

In the concluding section, we delve into the practical implementation of the protocol by presenting several instances of its application. It is important to emphasize that the implementation of our investment protocol requires an existing blockchain platform that has already established infrastructure projects. The effectiveness of our investment protocol relies on the guidance provided by experts who possess exceptional reputations. Consequently, the protocol encounters a significant challenge known as the cold-start problem. To address this issue, the initial rounds of the protocol are recommended to be executed concurrently with other investment protocols. During these rounds, experts are solely required to make predictions, following which the protocol updates their reputations by evaluating the accuracy of their predictions against the actual project outcomes. As a result of overcoming the cold-start phase, the protocol's performance gains enhanced reliability.

Secondly, if there is an abundance of projects requiring investment within a limited timeframe, we can introduce the "run in batch" approach, where experts provide advice for multiple projects in a single round. Subsequently, the

protocol will update the expert's reputation by considering the cumulative predicted loss. Implementing this method enhances the efficiency of the process while maintaining the regret bound of our protocol unaffected.

Thirdly, given the decentralized nature of blockchain, our focus lies primarily on the implementation details of how experts submit their opinions within the system. At the start of each new round t, in addition to the investment project p_j, the experts are assigned a deadline to submit their investment advice within. This so-called *time point*, can be determined by the block height in the blockchain. To ensure impartial decision-making, we mandate that experts initially provide the digest of their advice, specifically denoted as $h(c_{t,i})$ and $h(\widehat{V}_i^t(c_{t,i}))$, where $h(\cdot)$ is a hash function. [2] Subsequently, the selected expert $e_{t,i}$ discloses her advice $c_{t,i}$ as the final decision f_t. Following this, the remaining experts in the same round t are required to submit the hash value of their estimation for the social welfare of project p_t at the funding level f_t, denoted as $h(\widehat{V}_i^t(f_t))$. This submission must also be finalized within the specified timeframe. After that, all experts disclose their estimations $\widehat{V}_i^t(c_{t,i})$ and $\widehat{V}_i^t(f_t)$, allowing the smart contract to update their individual reputations. This hashing-first and subsequent revealing design also serves as a deterrent against strategic experts who may attempt to plagiarize others' ideas.

Finally, we are also concerned with the evaluation of projects during the implementation phase. Due to the inherent partiality and subjectivity of people's information about projects, direct evaluation can be challenging and nuanced. Thus, utilizing indicators to assess projects can serve as a viable alternative approach. We compiled a set of indicators pertaining to public goods and reorganized them to offer a more comprehensive approach to project evaluation, which is presented in Table II.

TABLE II
POST-PROJECT INDICATORS

Category and dimension	Indicator
Related to outcome and deliverables	Scope
	Quality
	Profitability
	Meets technical specification
Related to process and execution	Decision
	Cost
	Schedule
	Cost deviation
Objective measure	Construction time
	Speed
	Time Variation
	Unit Cost
	Net present value
	Accident rate
Subjective measure	Design team's satisfaction
	Functionality
	Community satisfaction
	Social obligation

[2]It is important to note that both $c_{t,i}$ and $\widehat{V}_i^t(c_{t,i})$ are continuous variables in our paper. In the discrete case, cryptographic techniques such as digital signature and commitment scheme can be employed to safeguard against potential pre-computed dictionary attacks.

IV. Theoretical Analysis

This section provides a comprehensive analysis of the effectiveness of the investment protocol in both static and dynamic settings. For the sake of notation simplicity in proofs, we assume that the estimated values provided by each expert fall within the range of $[0, H]$. Consequently, by dividing the constant H, we can scale the losses of experts to the interval $[0, 1]$. We demonstrate that our investment protocol has a tight lower bound on classical regret or ranking regret, with a constant factor, in both the static and dynamic settings.

A. Analysis for static setting

In the static scenario, experts are not removed from the expert set E_t during each round. We utilize the concept of minimax regret [8], which is defined as follows:

$$\inf_{W} sup_{\boldsymbol{l}_1,\ldots,\boldsymbol{l}_T} \left\{ \sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t - \min_{j\in[n]} \sum_{t=1}^{T} l_{t,j} \right\},$$

for evaluating the performance of the investment protocol. Here, W represents the set of all possible weight combinations for experts across T rounds. Subsequently, we demonstrate that our protocol's regret nearly matches the minimax lower bound in the static scenario.

Theorem 1. *Let L be a universal constant. In the static setting, when T tends to infinity, the investment protocol has a lower bound on its minimax regret:*

$$\lim_{T\to+\infty} \inf_{W} sup_{\boldsymbol{l}_1,\ldots,\boldsymbol{l}_T} \left\{ \sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t - \min_{j\in[n]} \sum_{t=1}^{T} l_{t,j} \right\} \geq \frac{1}{L}\left(\sqrt{T/2\ln n}\right). \tag{13}$$

Proof. As the infimum is taken over all forecasting weighting strategies W, we introducing i.i.d. symmetric Bernoulli random variables $l_{t,1}, ..., l_{t,n}$ (i.e., $\Pr[l_{t,i} = 0] = \Pr[l_{t,i} = 1] = \frac{1}{2}$) for all $t \in [T]$, we clearly has:

$$\inf_{W} sup_{\boldsymbol{l}_1,\ldots,\boldsymbol{l}_T} \left\{ \sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t - \min_{j\in[n]} \sum_{t=1}^{T} l_{t,j} \right\} \geq \inf_{W} E\left[\sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t - \min_{j\in[n]} \sum_{t=1}^{T} l_{t,j} \right].$$

Since all the variable $l_{t,i}$ is completely random, for all forecasting strategies one obviously has $E[\sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t] = T/2$. Thus,

$$\begin{aligned} \inf_{W} E\left[\sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t - \min_{j\in[n]} \sum_{t=1}^{T} l_{t,j} \right] &= E\left[\frac{T}{2} - \min_{j\in[n]} \sum_{t=1}^{T} l_{t,j} \right] \\ &= \frac{1}{2} E\left[\max_{j\in[n]} \sum_{t=1}^{T} (1 - 2l_{t,j}) \right] \\ &= \frac{1}{2} E\left[\max_{j\in[n]} \sum_{t=1}^{T} \delta_{t,j} \right], \end{aligned}$$

where $\{\delta_{t,j}\}$ are i.i.d. Rademacher random variables (i.e., $\Pr[\delta_{t,j}=1]=\Pr[\delta_{t,j}=-1]=\frac{1}{2}$). By Lemma 2 ([8] Lemma A.11 and A.12), as shown below, we can achieve

$$\lim_{T\to+\infty}\inf_{W} E\left[\sum_{t=1}^{T}\boldsymbol{w}_t\boldsymbol{l}_t-\min_{j\in[n]}\sum_{t=1}^{T}l_{t,j}\right] \geq \frac{1}{L}\left(\sqrt{T/2\ln n}\right).$$

Then, this result holds. □

Lemma 2 ([8])**.** *Let $Z_{t,i}$ for all $i\in[n]$ and $t\in T$ be the Rademacher random variables, and $G_1,\cdots,G_n$ are independent standard normal random variables. Then,*

$$\lim_{T\to\infty} E\left[\max_{i\in[n]}\sum_{t=1}^{T}Z_{t,i}\right]=\sqrt{T}\cdot E\left[\max_{i\in[n]}G_i\right]$$
$$\lim_{n\to\infty} E\left[\max_{i\in[n]}G_i\right]=\sqrt{2\ln n}.$$

In addition to the lower bound of minimax regret obtained in Theorem 1, we also investigate the upper bound of the classical regret, defined in (1), by using the method presented in the proof of Multiplicative Weights Update [30].

Theorem 2. *Consider the investment protocol runs for T rounds with n experts. Define $R(T)$ in (1) as the classical regret, then for a given constant $\eta\in(0,+\infty]$:*

$$R(T)\leq\frac{\ln n}{\eta}+\frac{\eta T}{2}. \tag{14}$$

Proof. We establish the upper bound of classical regret using the potential method, where the potential function is defined as $\Phi(t)=\frac{1}{\eta}\ln\sum_{i=1}^{n}r_{t,i}$. Therefore,

$$\begin{aligned}
\Phi(t+1)-\Phi(t)&=\frac{1}{\eta}\ln\sum_{i=1}^{n}r_{t+1,i}-\frac{1}{\eta}\ln\sum_{i=1}^{n}r_{t+1,i}\\
&=\frac{1}{\eta}\ln\frac{\sum_{i=1}^{n}r_{t+1,i}}{\sum_{i=1}^{n}r_{t,i}}=\frac{1}{\eta}\ln\frac{\sum_{i=1}^{n}r_{t,i}e^{-\eta l_{t,i}}}{\sum_{i=1}^{n}r_{t,i}}\\
&=\frac{1}{\eta}\ln\sum_{i=1}^{n}w_{t,i}e^{-\eta l_{t,i}} &(15)\\
&\leq\frac{1}{\eta}\ln\sum_{i=1}^{n}w_{t,i}\left(1-\eta l_{t,i}+\frac{(\eta l_{t,i})^2}{2}\right) &(16)\\
&=\frac{1}{\eta}\ln\left(1+\sum_{i=1}^{n}w_{t,i}\left(-\eta l_{t,i}+\frac{\eta^2 l_{t,i}^2}{2}\right)\right)\\
&\leq\frac{1}{\eta}\sum_{i=1}^{n}w_{t,i}\left(-\eta l_{t,i}+\frac{\eta^2 l_{t,i}^2}{2}\right) &(17)\\
&=-\sum_{i=1}^{n}w_{t,i}l_{t,i}+\frac{\eta\sum_{i=1}^{n}w_{t,i}l_{t,i}^2}{2}\\
&=-l_t+\frac{\eta\sum_{i=1}^{n}w_{t,i}l_{t,i}^2}{2}.
\end{aligned}$$

Here, $l_t=\sum_{i=1}^{n}w_{t,i}l_{t,i}$ represents the expected verification loss in round t; (16) is correct because $-\eta l_{t,i}\leq 0$ and $\mathrm{e}^x\leq 1+x+\frac{x^2}{2}$, for any $x\leq 0$; (17) holds because $\ln(1+x)\leq x$, given that $x\geq -1$.

Due to the fact that for all t rounds, $|l_{t,i}|\leq 1$ and $\sum_{i=1}^{n}w_{t,i}=1$, we have

$$\Phi(t+1)-\Phi(t)=-l_t+\frac{\eta\sum_{i=1}^{n}w_{t,i}l_{t,i}^2}{2}\leq -l_t+\frac{\eta}{2}. \tag{18}$$

Summing (18) from $t=1$ to T, we obtain

$$\Phi(T+1)-\Phi(1)=\Phi(T+1)-\frac{\ln n}{\eta}\leq-\sum_{t=1}^{T}l_t+\frac{\eta T}{2},$$

which can be rewritten as:

$$\sum_{t=1}^{T}l_t+\Phi(T+1)\leq\frac{\ln n}{\eta}+\frac{\eta T}{2}. \tag{19}$$

Finally, let i^* denote the index of the expert with the minimum accumulated loss. According to the definition of $\Phi(T)$, we have

$$\begin{aligned}
\Phi(T+1)&=\frac{1}{\eta}\ln\sum_{i=1}^{n}r_{T+1,i}\geq\frac{1}{\eta}\ln r_{T+1,i^*}\\
&=\frac{1}{\eta}\ln\mathrm{e}^{-\eta\sum_{t=1}^{T}l_{t,i^*}}=-\sum_{t=1}^{T}l_{t,i^*}=-\min_{i\in n}\sum_{t=1}^{T}l_{t,i}. &(20)
\end{aligned}$$

Combining (19) and (20), it is not hard to deduce that

$$R(T)=\sum_{t=1}^{T}l_t-\min_{i\in n}\sum_{t=1}^{T}l_{t,i}\leq\frac{\ln n}{\eta}+\frac{\eta T}{2}.$$

This result holds. □

Moreover, by setting the constant $\eta=\sqrt{\ln n/T}$, we can establish that the upper bound of the classical regret converges to $O(\sqrt{T\ln n})$.

Corollary 1. *The classical regret of the investment protocol in the static setting is upper bounded by $O(\sqrt{T\ln n})$.*

Remarks for choosing expert. The investment protocol can improve its robustness by utilizing a weighted average of expert advice to make investment decisions. It is important to highlight that even in the case of delayed feedback, the proof of Corollary 1 can be adapted following a similar approach as presented in [13].

B. Analysis for dynamic setting

In the dynamic setting, the performance of a prediction protocol is evaluated using the ranking regret, as defined in (2). In this subsection, we initially examine the lower bound of the ranking regret under fully adversarial conditions. Subsequently, we establish that this lowerbound is asymptotically tight for our investment protocol, with a constant factor.

Theorem 3. *In the dynamic setting under fully adversarial conditions, the minimax ranking regret is lower bounded by $\Omega(\sqrt{(m+1)T\ln n})$, where m represents the number of substituted rounds in a total of T rounds and n denotes the number of involved experts in each round.*

Proof. We use π^* to denote the optimal permutation with the minimum ranking regret. For any permutation π, the first

expert participating in round t is denoted $\sigma^{\pi}(t)$, and their corresponding loss is $l_{t,\sigma^{\pi}(t)}$.

The m numbder of substituted rounds, is represented by $t_1, t_2, ..., t_m$, respectively. Define τ_i as the set of time-step indices for rounds occurring between t_{i-1} and t_i, i.e., $\tau_i = \{t|t_{i-1} < t \leq t_i\}$. Specifically, we define $t_0 = 0$ and $t_{m+1} = T$. Consequently, the T rounds can be divided into $m+1$ time periods denoted by $\{\tau_1, \cdots, \tau_{m+1}\}$.

We divide each time period τ_i into two equal parts, denoted by τ_i^1 and τ_i^2, respectively. Let $l_{\tau_i^1,j}$ and $l_{\tau_i^2,j}$ as the sequences of losses for expert e_j during the first and second half of the period τ_i. In the first part, the adversary subjects each expert to losses drawn independently and identically from a Bernoulli distribution with $p = \frac{1}{2}$. At the end of the first part τ_i^1, the adversary evaluates the accumulated losses of n experts during this time period and selects the expert with the lowest cumulative loss up to the point, denoted as e_{i^*}. Subsequently, in the second part of this time period, the loss for expert e_{i^*} is zero. For all other experts, the adversary imposes losses on them according to the loss sequence $l_{\tau_i^1,j}$. In particular, for $e_j \neq e_{i^*}$, the loss sequence $l_{\tau_i^2,j}$ in the second part of time period τ_i is obtained by element-wise subtraction of 1 from $l_{\tau_i^1,j}$, denoted as $l_{\tau_i^2,j} = 1 - l_{\tau_i^1,j}$. Once the time period τ_i is completed, the adversary replaces e_{i*} with a new expert.

Let us now analyze the ranking regret over T rounds under the given construction. According to the definition in Equation (2), the ranking regret over T rounds can be expressed as:

$$\begin{aligned} R_{\Pi}(T) &= \sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t - \min_{\pi \in \Pi} \sum_{i=1}^{T} l_{t,\sigma^{\pi}(t)} \\ &= \sum_{t=1}^{T} \boldsymbol{w}_t \boldsymbol{l}_t - \sum_{i=1}^{m+1} \sum_{t \in \tau_i} l_{t,\sigma^{\pi^*}(t)} \\ &= \sum_{i=1}^{m+1} \left(\sum_{t \in \tau_i} \boldsymbol{w}_t \boldsymbol{l}_t - \sum_{t \in \tau_i} l_{t,\sigma^{\pi^*}(t)} \right). \end{aligned}$$

Considering the construction, we observe that in each period τ_i, expert e_{i^*} experiences the lowest loss and is subsequently replaced in the following period τ_{i+1}. Therefore, it becomes evident that $\pi^* = (e_{1^*}, e_{2^*}, \cdots, e_{(m+1)^*}, \cdots)$. So, let us simplify the expression:

$$\begin{aligned} \sum_{i=1}^{m+1} \left(\sum_{t \in \tau_i} \boldsymbol{w}_t \boldsymbol{l}_t - \sum_{t \in \tau_i} l_{t,\sigma^{\pi^*}(t)} \right) &= \sum_{i=1}^{m+1} \left(\sum_{t \in \tau_i} \boldsymbol{w}_t \boldsymbol{l}_t - \sum_{t \in \tau_i} l_{t,i^*} \right) \\ &= \sum_{i=1}^{m+1} R(\tau_i), \end{aligned} \tag{21}$$

where i^* represents the index of the expert with the minimum cumulative loss. By combining the lower bound of minimax regret (13) for the static setting and equation (21), we obtain:

$$\begin{aligned} R_{\Pi}(T) = \sum_{i=1}^{m+1} R(\tau_i) &\geq \frac{1}{L} \sum_{i=1}^{m+1} \sqrt{(\tau_i)/2 \ln n} \\ &\geq \frac{1}{L} \sqrt{(m+1)(T/2) \ln n} \\ &= \Omega(\sqrt{(m+1)T \ln n}. \end{aligned} \tag{22}$$

The inequality (22) holds due to the fact that $\sum_{i=1}^{m+1} \tau_i = T$ and the application of the Cauchy-Schwarz inequality. □

In the following, we aim to demonstrate that the lower bound of $\Omega(\sqrt{(m+1)T \ln n})$ can be achieved by our investment protocol, thereby establishing its superior performance. Before presenting the proof, it is necessary to introduce the following preliminary result.

Theorem 4. *Consider a scenario where there are m substituted rounds within a total of T rounds. Let $R_{\Pi}(T)$ denote the ranking regret of the investment protocol in a dynamic setting. Then for $\eta \in (0, +\infty]$ and $\alpha \in [0, 1)$, we have*

$$R_{\Pi}(T) \quad \leq \frac{(m+1)}{\eta} \ln \frac{n}{(1-\alpha)} + \frac{\eta T}{2}. \tag{23}$$

Proof. Similar to the proof in Theorem 2, we employ the potential method to establish the upper bound (23). For this purpose, we introduce the potential function $\Phi(t) = \frac{1}{\eta} \ln \sum_{i=1}^{n} r_{t,i}$. Subsequently, we consider two cases depending on whether round $t+1$ is a substitution round or a regular round.

Case 1. If round $t+1$ is a regular round, then the reputation updating process follows the same protocol as in the static setting. Applying equation (15), we can express the change in potential function as

$$\Phi(t+1) - \Phi(t) = \frac{1}{\eta} \ln \sum_{i=1}^{n} w_{t,i} e^{-\eta l_{t,i}}.$$

Case 2. If round $t+1$ is a substituted round, then the reputation updating process becomes more complex. However, we can observe that

$$\begin{aligned} \sum_{e_{t+1,i} \in new_t} r_{t+1,i} &= d(1-\alpha) \frac{\sum_{k=1}^{n} r_{t,k} e^{-\eta l_{t,k}}}{n}; \\ \sum_{e_{t+1,i} \notin new_t} r_{t+1,i} &= (n-d)(1-\alpha) \frac{\sum_{k=1}^{n} r_{t,k} e^{-\eta l_{t,k}}}{n} \\ &\quad + \alpha \sum_{k=1}^{n} r_{t,k} e^{-\eta l_{t,k}}; \\ \sum_{i=1}^{n} r_{t+1,i} &= \sum_{e_{t+1,i} \in new_t} r_{t+1,i} + \sum_{e_{t+1,j} \notin new_t} r_{t,j+1} \\ &= \sum_{i=1}^{n} r_{t,i} e^{-\eta l_{t,i}}, \end{aligned}$$

where d represents the number of substituted experts.

Therefore, for the substituted round, we also have

$$\begin{aligned} \Phi(t+1) - \Phi(t) &= \frac{1}{\eta} \ln \sum_{i=1}^{n} r_{t,i} e^{-\eta l_{t,i}} - \frac{1}{\eta} \ln \sum_{i=1}^{n} r_{t+1,i} \\ &= \frac{1}{\eta} \ln \sum_{i=1}^{n} w_{t,i} e^{-\eta l_{t,i}}. \end{aligned}$$

Finally, it is necessary to scale $\Phi(T+1)$. It should be noted that if round $t+1$ is a substituted round, the following inequality holds for all i and j: $r_{t+1,i} \geq \frac{1-\alpha}{n} r_{t,j}$.

Recall that in the optimal permutation $\pi^* \in \Pi$ that minimizes the ranking regret, the first expert involved in round

t, denoted by $\sigma^{\pi^*}(t)$, has a loss of $l_{\sigma^{\pi^*}(t),t}$. Let $t_1, t_2, ..., t_m$ represent the m substituted rounds. Taking these into account, we have

$$\begin{aligned}\Phi(T+1) &= \frac{1}{\eta}\ln\sum_{i=1}^{n} r_{t+1,i} \\ &\geq \frac{1}{\eta}\ln\frac{(1-\alpha)}{n} r_{\sigma^{\pi^*}(t_m),t_m} e^{-\eta\sum_{t\geq t_m} l_{\sigma^{\pi^*}(t),t}} \\ &\geq \frac{1}{\eta}\ln\frac{(1-\alpha)^2}{n^2} r_{\sigma^{\pi^*}(t_{m-1}),t_{m-1}} e^{-\eta\sum_{t\geq t_{m-1}} l_{\sigma^{\pi^*}(t),t}} \\ &\cdots \\ &\geq \frac{1}{\eta}\ln\frac{(1-\alpha)^m}{n^m} e^{-\eta\sum_{t=1}^{T} l_{\sigma^{\pi^*}(t),t}} \\ &= -\sum_{t=1}^{T} l_{\sigma^{\pi^*}(t),t} - \frac{m}{\eta}\ln n + \frac{m}{\eta}\ln(1-\alpha). \quad (24)\end{aligned}$$

Therefore,

$$\begin{aligned}R_{\Pi}(T) &= \sum_{t=1}^{T} l_t - \sum_{t=1}^{T} l_{\sigma^{\pi^*}(t),t} \\ &\leq \frac{(m+1)}{\eta}\ln n + \frac{\eta T}{2} - \frac{m}{\eta}\ln(1-\alpha) \\ &\leq \frac{(m+1)}{\eta}\ln\frac{n}{(1-\alpha)} + \frac{\eta T}{2}.\end{aligned}$$

The proof is completed. □

By setting $\eta = \sqrt{2(m+1)\ln n/T}$ and $\alpha = 0$, we can establish the following upper bound of the investment protocol. Notably, this upper bound matches the lower bound stated in Theorem 3, albeit within a constant factor.

Corollary 2. *The ranking regret of then investment protocol is upper-bounded by* $O(\sqrt{(m+1)T\ln n})$.

V. Performance Evaluation

In the previous section, we have theoretically demonstrated the efficiency of our investment protocol. In this section, we further conduct simulations to evaluate the protocol's performance in a real-task scenario.

A. Environment Setup

In the simulation, we consider a community consisting of K individuals. We assume the utility functions of projects to be concave, smooth, increasing, and zero-intercept. To simulate the value functions for each individual k, we employ the following utility function: $V_k^p(x) = a_k x^{b_p}$, where a_k is drawn from an exponential distribution $Exp(\lambda)$, and b_p can take any value within the interval $(0, 1)$. Therefore, the social welfare function is denoted by $W^p(x) = A_p x^{b_p} - x$, where $A_p = \sum_{k=1}^{K} a_k$. However, due to potential inaccuracies in people's predictions, we introduce the utility prediction function $\widehat{V}_k^p = \hat{a_k} x^{b_p}$ for each individual k, wherein $\hat{a_k} \sim N(a_k + \beta, \sigma)$. Here, the parameter β represents the bias resulting from crowd prejudice.

In our investment algorithm, we incorporate N experts. For each expert $i \in [N]$, we assume its prediction of the social welfare function of project p is $\widehat{W}_i^p(x) = \widehat{A}_i x^{b_p} - x$, where $\widehat{A}_i$ follows a normal distribution $N(A_p, \kappa_i)$. The parameter κ_i is selected from the range $[\kappa_{min}, \kappa_{max}]$ and represents the prediction ability of expert i. In this section, we realize the following algorithm:

- Quadratic Funding Algorithm ([2])
- Static Expert Algorithm (Alg.1)
- Dynamic Expert Algorithm (Alg.2)

The environment parameters used in our simulation are shown in Table III.

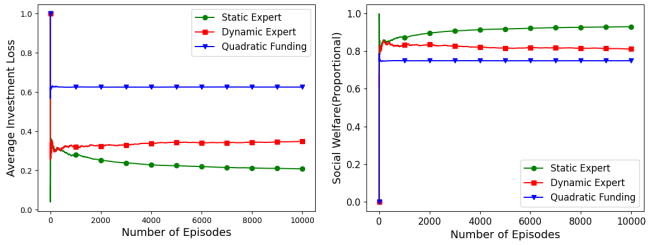

Fig. 2. The average investment loss and social welfare of the Quadratic Funding algorithm, the static algorithm, and the dynamic algorithm, proportional with the theoretical best.

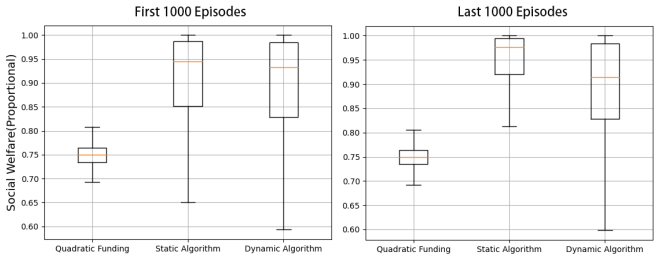

Fig. 3. The average social welfare of the Quadratic Funding algorithm, the static algorithm, and the dynamic algorithm in the first and last 1000 episodes.

TABLE III
Simulation Parameters

$K = 1000$	Number of people
$T = 10000$	Number of episodes
$\lambda = 2$, $b_p \in [0, 1]$	The parameter represents the average utility of individuals
$\beta = 1$, $\sigma = 1$	The parameter of the bias distribution
$\kappa_{min} = 500$, $\kappa_{max}^a = 1500$	The ranging about expert's ability

B. Performance Comparison

We first show the efficiency of our investment protocol in both static and dynamic settings. In the experiment, we suppose our investment protocol maintains $n = 20$ experts in all $T = 10000$ rounds. The learning rate of the static algorithm is $\eta = 0.05$. During the fact that the expert will be offline in the system, we substitute a random expert in every 500 rounds, and the hyperparameter of the dynamic algorithm is $\alpha = 0.2$

Fig. 2 illustrates the average investment loss and average social welfare of the Quadratic Funding, Static, and Dynamic

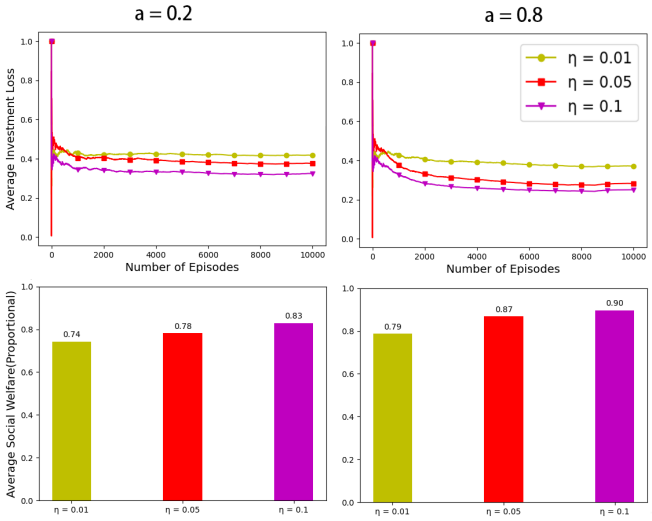

Fig. 4. The average investment loss and social welfare of the dynamic algorithm under different learning rates. The substituted rate of the algorithm is set to $\alpha = 0.2$ on the left and $\alpha = 0.8$ on the right.

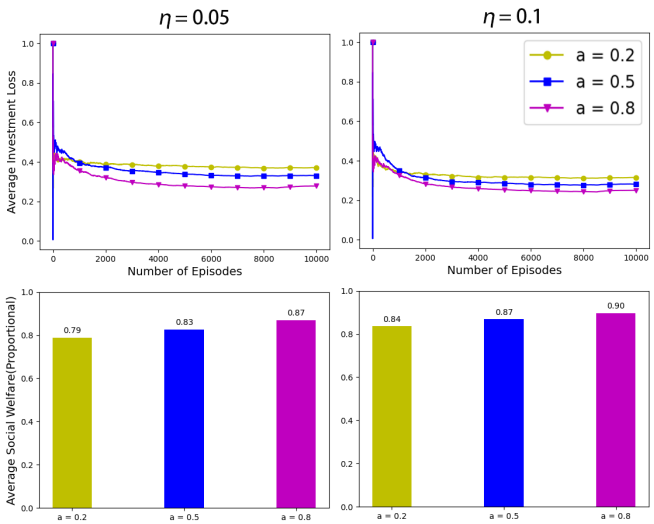

Fig. 5. The average investment loss and social welfare of the dynamic algorithm under different substituted rates. The learning rate of the algorithm is set to $\eta = 0.05$ on the left and $\eta = 0.1$ on the right.

algorithms in each round. To normalize the results, we divide them by the theoretical maximum outcome. It is evident that both the static and dynamic algorithms outperform the Quadratic Funding algorithm. Specifically, in the simulated environment, the Quadratic Funding algorithm incurs a loss of over 62% of the investment on projects, while the Static and Dynamic algorithms experience losses of only 24% and 33%, respectively. Moreover, in terms of social welfare, the Quadratic Funding algorithm achieves approximately 74% of the maximum social welfare compared to the theoretical maximum, while the static algorithm and the dynamic algorithm can reach 95% and 78%.

In Figure 3, we utilize box plots to present the distribution of social welfare in the first and last 1000 episodes for each algorithm. From the graph, it is evident that although the Quadratic Funding algorithm exhibits the highest stability in terms of social welfare, our algorithm consistently achieves higher social welfare values than the Quadratic Funding algorithm. This is true even during the initial 1000 rounds before our algorithm reaches total convergence. Moreover, despite operating in a dynamic environment with changing experts, our dynamic algorithm demonstrates a relatively strong convergence to a favorable decision-making level in the first 1000 rounds. The median social welfare closely resembles that of the static algorithm, while in the majority of cases, our algorithm surpasses the social welfare obtained by the Quadratic Funding algorithm. These findings indicate that even in the presence of environmental disturbances our algorithm still exhibits a superior performance.

C. Learning Rate Influence

In this section, we conduct a performance comparison of the dynamic algorithm under learning rate. To examine the impact of different parameter values on the algorithm's effectiveness, we test the algorithm while keeping either the α parameters fixed. The experiments are conducted in a controlled simulation environment under parameters shown in Table III, lasting for 10000 episodes. In every 500 episodes, a random expert is replaced by a new one. We test the learning rate η on $0.01, 0.5$ and 0.1.

The average loss and social welfare results are presented in Figure 4. Based on the figure, it can be concluded that although algorithms with lower learning rates initially exhibit better performance, algorithms with higher learning rates converge faster over episodes and outperform in terms of both average loss and social welfare metrics.

D. Substituted Rate Influence

Similar to the approach in the previous section, we conducted comparative experiments to assess the impact of the parameter α, referred to as the substituted rate, on algorithm performance. This parameter is a more sensitive hyperparameter, which determines the level of trust the algorithm places on newly introduced experts. We tested the results for $\alpha = 0.2, 0.5$, and 0.8.

Figure 5 presents the convergence of the dynamic algorithm on investment loss and the average value of social welfare for different α values. It can be observed that a higher substituted rate yields better results in the experiment. This is because, with higher alpha values, newly introduced experts gain reputation faster, leading to the selection of their valuable advice more quickly. However, at the same time, a higher substituted rate also results in increased fluctuations in the algorithm after expert changes.

E. Performance in Extreme Situation

In this section, we evaluated the performance of the dynamic algorithm in extreme scenarios. We designed a scenario where experts frequently change, with $m = 5$ or 10 random experts leaving every 250/500 rounds. Furthermore, our dynamic algorithm continued to maintain only 20 experts for decision-making in each round.

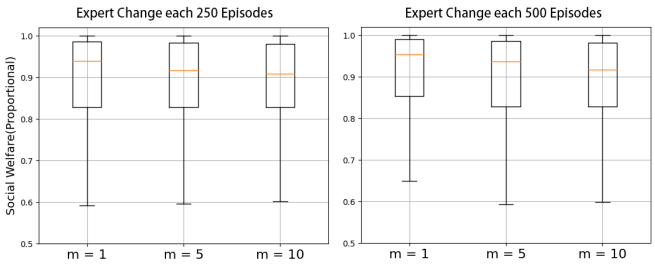

Fig. 6. The social welfare of the dynamic algorithm when $m = 1$, 5, 10 experts change in each 250 / 500 episodes

The results are depicted in Figure 6. Although the frequency of expert changes may lead to a slight decrease in social welfare, the median of overall social welfare still remains above 90% of the maximum social welfare. Moreover, the frequent expert changes do not significantly alter the lower quartile point, providing evidence of the stability of the dynamic algorithm.

VI. Conclusion

In this academic paper, we propose an investment protocol to address the funding problems of public good projects in blockchain systems. The protocol operates by maintaining a group of experts who provide advice and recommendations, and their reputation is continuously updated based on project feedback. This reputation-based system forms the basis for decision-making within the protocol. Moreover, our protocol is designed to be flexible and adaptable to dynamic environments. It can accommodate scenarios where experts can join or leave the decision-making process at any given time. To assess the effectiveness of our decision algorithm, we introduce a ranking regret bound as a benchmark. Theoretically, we establish an upper regret bound for both static and dynamic models. Additionally, we demonstrate the tightness of this upper bound by establishing an asymptotically equal lower bound. Furthermore, we conduct simulations to provide empirical evidence supporting our oracle's investment decisions, which closely align with optimal investments in hindsight. This empirical evidence underscores the efficiency and effectiveness of our human oracle approach in guiding funding decisions for public goods projects within the blockchain ecosystem.

References

[1] Gitcoin, "Grants: Discover and fund extraordinary public goods," 2021. [Online]. Available: https://explorer.gitcoin.co/
[2] V. Buterin, Z. Hitzig, and E. G. Weyl, "A flexible design for funding public goods," *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.
[3] R. Pasquini, "Quadratic funding under limited matching funds: Evidence from gitcoin," *Available at SSRN 3702318*, 2020.
[4] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.
[5] Disruptionjoe, "Gitcoin grants round 11 governance brief," 2021. [Online]. Available: https://gitcoin.co/blog/gitcoin-grants-round-11-governance-brief/
[6] N. Littlestone and M. K. Warmuth, "The weighted majority algorithm," *Information and computation*, vol. 108, no. 2, pp. 212–261, 1994.
[7] V. Vovk, "A game of prediction with expert advice," *Journal of Computer and System Sciences*, vol. 56, no. 2, pp. 153–173, 1998.
[8] N. Cesa-Bianchi and G. Lugosi, *Prediction, learning, and games*. Cambridge university press, 2006.
[9] L. V. Freitas, W. L. Maldonado *et al.*, "Quadratic funding with incomplete information," University of São Paulo (FEA-USP), Tech. Rep., 2021.
[10] A. Benhaim, B. Hemenway Falk, and G. Tsoukalas, "Balancing power in decentralized governance: Quadratic voting under imperfect information," *Available at SSRN*, 2023.
[11] Y. Freund and R. E. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting," *Journal of computer and system sciences*, vol. 55, no. 1, pp. 119–139, 1997.
[12] T. Erven, W. M. Koolen, S. Rooij, and P. Grünwald, "Adaptive hedge," *Advances in Neural Information Processing Systems*, vol. 24, pp. 1656–1664, 2011.
[13] A. Korotin, V. V'yugin, and E. Burnaev, "Adaptive hedging under delayed feedback," *Neurocomputing*, vol. 397, pp. 356–368, 2020.
[14] A. Blum, "Empirical support for winnow and weighted-majority algorithms: Results on a calendar scheduling domain," *Machine Learning*, vol. 26, no. 1, pp. 5–23, 1997.
[15] V. Kanade and T. Steinke, "Learning hurdles for sleeping experts," *ACM Transactions on Computation Theory (TOCT)*, vol. 6, no. 3, pp. 1–16, 2014.
[16] S. Kale, C. Lee, and D. Pál, "Hardness of online sleeping combinatorial optimization problems," *Advances in Neural Information Processing Systems*, vol. 29, pp. 2181–2189, 2016.
[17] R. Kleinberg, A. Niculescu-Mizil, and Y. Sharma, "Regret bounds for sleeping experts and bandits," *Machine learning*, vol. 80, no. 2, pp. 245–272, 2010.
[18] C. R. Shalizi, A. Z. Jacobs, K. L. Klinkner, and A. Clauset, "Adapting to non-stationarity with growing expert ensembles," *arXiv preprint arXiv:1103.0949*, 2011.
[19] H. Shayestehmanesh, S. Azami, and N. A. Mehta, "Dying experts: Efficient algorithms with optimal regret bounds," *Advances in Neural Information Processing Systems*, vol. 32, pp. 9983–9992, 2019.
[20] V. Kanade, H. B. McMahan, and B. Bryan, "Sleeping experts and bandits with stochastic action availability and adversarial rewards," in *Artificial Intelligence and Statistics*. PMLR, 2009, pp. 272–279.
[21] L. Breidenbach, C. Cachin, A. Coventry, A. Juels, and A. Miller, "Chainlink off-chain reporting protocol," *URl: https://blog. chain. link/off-chain-reporting-live-on-mainnet*, 2021.
[22] J. Peterson and J. Krug, "Augur: a decentralized, open-source platform for prediction markets," *arXiv preprint arXiv:1501.01042*, 2015.
[23] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, "Astraea: A decentralized blockchain oracle," in *2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2018, pp. 1145–1152.
[24] MakerDAO, "Introducing oracles v2 and defi feeds," 2019.
[25] R. Takim and A. Akintoye, "Performance indicators for successful construction project performance," in *18th Annual ARCOM Conference*, vol. 2, 2002, pp. 545–555.
[26] R. Koelmans, "Project success and performance evaluation," *Information and Management Journal*, vol. 41, pp. 229–236, 2004.
[27] S. Y. Sohn, Y. G. Joo, and H. K. Han, "Structural equation model for the evaluation of national funding on r&d project of smes in consideration with mbnqa criteria," *Evaluation and program planning*, vol. 30, no. 1, pp. 10–20, 2007.
[28] V. L. Smith, "Experiments with a decentralized mechanism for public good decisions," *The American Economic Review*, vol. 70, no. 4, pp. 584–599, 1980.
[29] P. G. Warr, "The private provision of a public good is independent of the distribution of income," *Economics letters*, vol. 13, no. 2-3, pp. 207–211, 1983.
[30] S. Arora, E. Hazan, and S. Kale, "The multiplicative weights update method: a meta-algorithm and applications," *Theory Comput.*, vol. 8, no. 1, pp. 121–164, 2012.