SEER

SEER WHITE PAPER

A Next-generation Blockchain-based Decentralized Prediction Market

SEER

目 录

Abstract

SEER is a next-generation blockchain-based decentralized prediction market built on the Graphene toolkit. It allows users to express their judgments about future events by means of the market mechanism and makes effective predictions by gathering intelligence and ideas. Equipped with multiple-hosts decentralized Oracles, SEER offers users credible decentralized prediction market service. Also, SEER Committee and a mechanism of arbitration have been set up to maintain high efficiency, impartiality and self-government. In the early stage, SEER's project team mainly focuses on building a bottom blockchain layer and compiling smart contract s on a basic prediction market feature. Apart from this, SEER pursues extensive collaboration with data providers, aiming to connect blockchain and the real world, and narrow the gap between the upstream industries and users. In the middle of the SEER project and its development route, customized development projects will be launched, such as sports betting, finance market prediction, assets price prediction and event prediction.

Chapter 1 Design Philosophy

1.1 Background

During the initial release, SEER will create a basic prediction market that attracts users around the world to frequent small-amount predictions and provides academic support for prediction as a sociological proposition. After the basic prediction market has been completed, customized industry-specific decentralized applications for predictions will be developed and released on the basis of SEER's demand analysis on diverse industries, such as finance, insurance, social politics and sports betting.

1.2 Development direction

During the early stage, SEER will provide users with basic prediction market applications, development interfaces and data integration interfaces, invite developers, data service providers and entities of relevant industry chains to participate in developing SEER-based applications.

1.3 Innovative highlights

With the powerful Graphene toolkit-based blockchain platform, SEER is able to provide an underlying blockchain system in high-speed operation, and a reliable decentralized Oracle framework for prediction market.

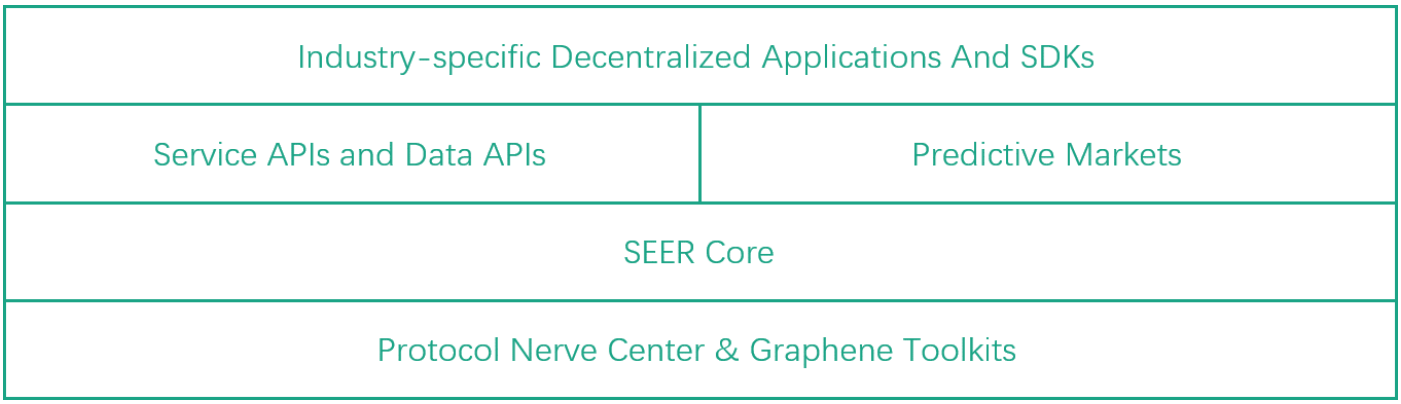
Protocol nerve center

Although the Turing complete virtual machine, to a certain degree, facilitates blockchain extension, after the DAO event, Ethereum has been directly divided into ETH and ETC through the hard fork

to solve relevant problems. The protocol nerve center has been introduced by SEER, which is a decentralized logic neural network formed by developers, the Committee, witnesses, all token holders and logic states; the operation of all application logics and blockchain protocols are under control of a protocol center. Hence, App and protocol updates require no hard fork, but depend on the self-adaption of the protocol nerve center.

Chapter 2 Technology Overview

2.1 Platform model



Industry-specific Decentralized Applications And SDKs

Service APIs and Data APIs Predictive Markets

SEER Core

Protocol Nerve Center & Graphene Toolkits

SEER is mainly composed of four layers:

The bottom layer consists of the protocol nerve center and Graphene toolkits that provide underlying blockchain service. Particularly, the blockchain of the protocol nerve center enables decentralized upgrade while the Graphene toolkits allow fast transaction confirmation at the average speed of 1.5s and efficient multi-transaction processing (3,300 transactions per second). It is a high- performance and low-lag underlying blockchain platform.

SEER Core, as implied by its name, is the core and secondary layer for communication with the Graphene toolkit to implement the underlying service logic.

The third is the service layer that encapsulates third-party developer interfaces, data integration interfaces and prediction market interfaces.

The top layer is composed of exclusive industry applications and SDKs. Different operational procedures and applications with customized interfaces will be developed according to the specific demands of target industries. Decentralized applications built on webpage, PC, iOS and Android will be available. Meanwhile, third-party developers can access the SDK and sample applications to develop their-own independent applications with customized interfaces.

2.2 Token—SEER COIN (SEER)

SEER coin is the basic system token that can be used to:

1. Proceed transactions and purchase gas for calling the smart contract;
2. Apply to be an Oracle with a certain amount of SEER coins as the deposit;
3. Serve as the token in the prediction market.

2.3 Functions of prediction market

The prediction market depends on the wisdom of the crowd to predict a future event. The prediction results produced by this operating mechanism have a greater accuracy than polls and other conventional statistical methods. In addition to the public wisdom-based probability prediction of future events, economists also view that the Marginal Trader Hypothesis (MTH) also has certain effects on the prediction market—and more particularly, there are always traders who buy underestimated assets and sell overestimated ones, making prices remain at a reasonable level. In terms of the prediction market, the market will continuously correct misconceptions and

improve the accuracy. Presently, the prediction market has already been applied to numerous aspects, such as prediction of election results, economic indicators, stock price movements and policy trends.

The IEM (Iowa Electronic Markets) put into operation since 1988 is a typical example. Established by the University of Iowa Tippie, the IEM has often been used to predict the results of political elections, especially the U.S. presidential elections and the U.S. Congress elections. The remarkable consistency between the final prediction results produced by the IEM and the actual results has demonstrated that the prediction market has a greater accuracy than polls and other sampling surveys.

SEER is mainly used to predict the results of sports events. By reference to the successful cases of the previous prediction markets and based on the blockchain technology, it employs the theories of prediction markets to predict future events and thereby provides prediction results for research and reference purpose. Since the blockchain technology is adopted, accordingly, the system operation will be decentralized. It is an autonomous prediction market of the sports industry. In the SEER Prediction Market, those having made accurate predictions respectively win a full-token prize.

Example: Assumed that there is a competition between player A and B and 30 participants intend to predict the result, among whom, one contributes a specific number of tokens via the SEER Prediction Market to set up a prediction market of the competition. All participants have to make payments with tokens before prediction. Assumed that there is a prediction about whether player A can defeat player B in the competition. If 20 participants make a prediction that player A will win the competition whereas the other 10 participants predict that player B will defeat player A, before

the competition starts, the prediction market will be locked on automatically and output a specific probability—the prediction result of the competition. In this case, if the given prediction result produced by the prediction market is 66%, it suggests that player A is likely to defeat player B in the competition, which can be applied to statistical analysis conducted by the public and statisticians. After the competition, the prediction market will be immediately closed and the SEER platform will automatically complete the allocation of awards according to the correct competition result provided by the Oracle.

2.4 Oracle framework

Oracle is a bridge of data flow between the real world and the SEER blockchain platform. A reliable Oracle mechanism plays an essential role in the judgment and execution of smart contracts based on the correct data acquired by the blockchain platform from the real world. In the above prediction market example, the accuracy of the competition result provided by the Oracle will significantly affect the follow-on allocation of rewards. Therefore, the reliable, trustworthy and neutral Oracle is one of the core functional parts of the system.

2.4.1 Applying to be an Oracle

One applies to be an Oracle and inputs correct results for prediction markets will be rewarded—which is the economic incentive of prediction markets. Yet, to ensure the authenticity of the input data, Oracle applicants must pay a specific number of tokens as the registration fee and the corresponding Oracles are required to authorize the system to lock a given number of tokens as deposit, which must exceed the total number of tokens paid by all participants in a specific

prediction of a prediction market. If an Oracle has maliciously input false results for times, it will be determined to be a malicious user by the Committee and as a result, the system will confiscate the locked-up deposit from such Oracle and block the corresponding account, leading to loss of its potential future incomes. This ensures that Oracles will provide authentic and reliable data as possible.

2.4.2 Decentralized Smart Oracle

To further ensure the input data authenticity, a multiple hosts-based decentralized Oracle function has been introduced, with which, if a prediction market builder sets a specific threshold value, only when there are 10 Oracles apply for the prediction and at least seven of these Oracles output the same result in the prediction market will such result be adopted. At the same time, the prediction market builder may complete weight setting of an Oracle separately. For example, if an Oracle enjoys a comparatively high reputation, it can have a greater weight. The multiple-hosts model, to a greater extent, ensures the reliability of prediction results and improves the robustness of the overall system. Meanwhile, it prevents the system from failing to output prediction results when a single-point service is unavailable due to system faults. As to the prediction markets having a limited number of participants or the timeliness demanding ones, to output prediction results as early as possible, the prediction market builder may also use a common single-host model.

2.4.3 Approaches to challenging Oracle prediction results

Despite the low probability, it remains possible that an Oracle will manipulate results. To eliminate such manipulation, participants are allowed to challenge the results produced by an Oracle in

order to supervise its operation. If any participants firmly believe that one or more Oracles have maliciously provided false results, they can apply for an Oracle challenge with the Committee within seven days. The applying participant is required to contribute/lock the number of tokens equal to 1/10 of the total tokens paid by the participants in a specific prediction market to margin the challenge and provide the Committee with the corresponding evidence and certifications for investigation. During the investigation (14 days), the Committee will look into and verify the grounds and evidence submitted by both parties and put the application to a vote. If the majority of the Committee presumes that the involved Oracle(s) has/have maliciously provided false results, which has adversely affected the correct result of the prediction, the given result of such prediction will be deemed as null and void and the tokens paid by all participants will be returned accordingly. No matter such malicious behavior has affected the result or not, the corresponding deposit contributed by the Oracle(s) determined to have provided false results in a prediction will be distributed to the applicant as a reward. If an Oracle repeats its malicious behaviors, the system will block its account and confiscate its deposit in full amount. If the Committee determines that the applicant initiates the challenge maliciously, the system will confiscate the applicant's deposit and grant the Oracle being challenged an amount equal to the said deposit.

2.4.4 Oracle reputation and credit system

The user information of each Oracle contains the user's credit standing, reputation and all historical data and violation data. The credit standing of an Oracle is calculated according to cases and severity of violations recorded by the Committee and the number of predictions that the Oracle has participated in. The reputation of an Oracle is the result based on the votes received from

users according to the weight of token holdings. When a prediction market builder sets up predictions, the Oracles having a reputation or credit standing lower than a specific value can be excluded and refused to participate in the prediction at the prediction market builder's will.

2.5 Anchor token in prediction markets

It has come to our notice that the prediction market participants may have a demand for a relatively stable token to participate in predictions. With the Graphene toolkits, it is easy to develop such system-level anchor currency as BITCNY or BITBTC. Yet, it requires substantial demands, a large-scale trading capacity, adequate channels and fiat gateways (arbitrageurs) to maintain the system-level anchor currency. As a prediction market, its trading capacity, without doubt, is inferior to that of a decentralized exchange like BitShares. It is impossible to maintain the stability of the system-level anchor in lack of trading capacity, channels and arbitrageurs. The Steem Backed Dollars (SBD) of the Graphene toolkit-based Steemit is a fine example. Although the SBD merely aimed to use the Steem token to provide security for its value, because of the above-mentioned factors and its issuing mechanism, the SBD fails to fulfill its preset long-term anchoring objective, i.e., to anchor the value of 1 SBD in 1 US dollar.

To prevent the system-level risk and provide a relatively permanent anchor token, SEER drops the system-level anchor token. Instead, it offers prediction market builders anchor token options for specific prediction markets, leaving the decision to the prediction market builders on whether they should commission the function or not. The detailed procedure is as follows:

(1) A prediction market builder commissions the function and pays anchor deposit according to the forced stop-loss ratio jointly determined by witnesses and the Committee.

(2) When the prediction market is open, SEER retrieves external anchor token price information through the price feed service provided by the witnesses and sets the corresponding price as the benchmark (base price).

(3) When the prediction market is closed, likewise, SEER acquires the current price (spot price) of the anchor token through the price feed service provided by the witnesses. On that basis, the spot price-base price difference can be calculated. If the spot price is lower than base price but within the range of forced stop-loss ratio, the loss from price difference should be undertaken by the prediction market builder. In contrast, if it is the opposite case, the gain from price difference should be attributed to the prediction market builder. With this mechanism, regardless of the changes in the price of the target anchor currency during prediction market operation, as long as the price is within the range of the given stop-loss ratio, the exchange rate between the token used by prediction market participants and the target anchor currency will be anchored in that at the beginning of the prediction market operation.

Example: Assumed that a prediction market builder employs the SEER BTC to set up a prediction. SEER BTC is considered the token of the prediction with Bitcoin as the anchor currency.

If the SEER BTC-SEER ratio is 1:1000 at the beginning of the prediction market operation and it turns into 1:1050 in the end, each Bitcoin can be used to exchange more SEER tokens. Because the prediction market settlement will be proceeded according to the preset exchange rate of 1:1000, the additional 50 SEER tokens/Bitcoins is deemed as the prediction market builder's gain from the prediction. In contrast, the corresponding loss is also borne by the prediction market builder.

2.6 Academic research and data integration interfaces

To promote academic research on prediction markets, except for the general App development interfaces, SEER also provides a user-friendly historical data retrieving program, searching interfaces and data statistics interfaces for academic researchers. It is free to call full-node data integration interfaces. In the meanwhile, since not all researchers desire for full-node operation, SEER also offers light-node data integration interfaces—which are charged according to the number of interfaces—and the data call requests will be sent to the witnesses in transaction packets for full-node operation before returning the data. researchers have access to relevant data interfaces for research purpose at an extremely low cost.

2.7 Isolated decentralized application programs

To meet the demands of prediction market builders, SEER offers a series of SDKs and samples of decentralized applications so that market builders can develop their own decentralized applications. In SEER, users can build prediction markets and mark them with special labels before filtering the prediction markets in the blockchain with self-developed decentralized applications to display the prediction markets created by specific builders.

2.8 Encrypted private prediction markets

As far as we know, there are enormous demands for private prediction markets. Considering that off-chain solutions may require direct connection between prediction market builders and participants—which poses a risk of exposure of whereabouts to the market builders and

participants, we have introduced a new type of efficient and encrypted blockchain-based private prediction markets so that only designated participants and builders have access to all information about their private prediction markets. Meanwhile, each private prediction market only allows participation of designated users and relevant information of the blockchain will be completely encrypted. Diffie–Hellman key exchange (DH) and Rijndael key schedule (also known as the Advanced Encryption Standard (AES)) are applied to raise the processing efficiency and security level and enable the system to perform "traitor tracing". Details are given as follows:

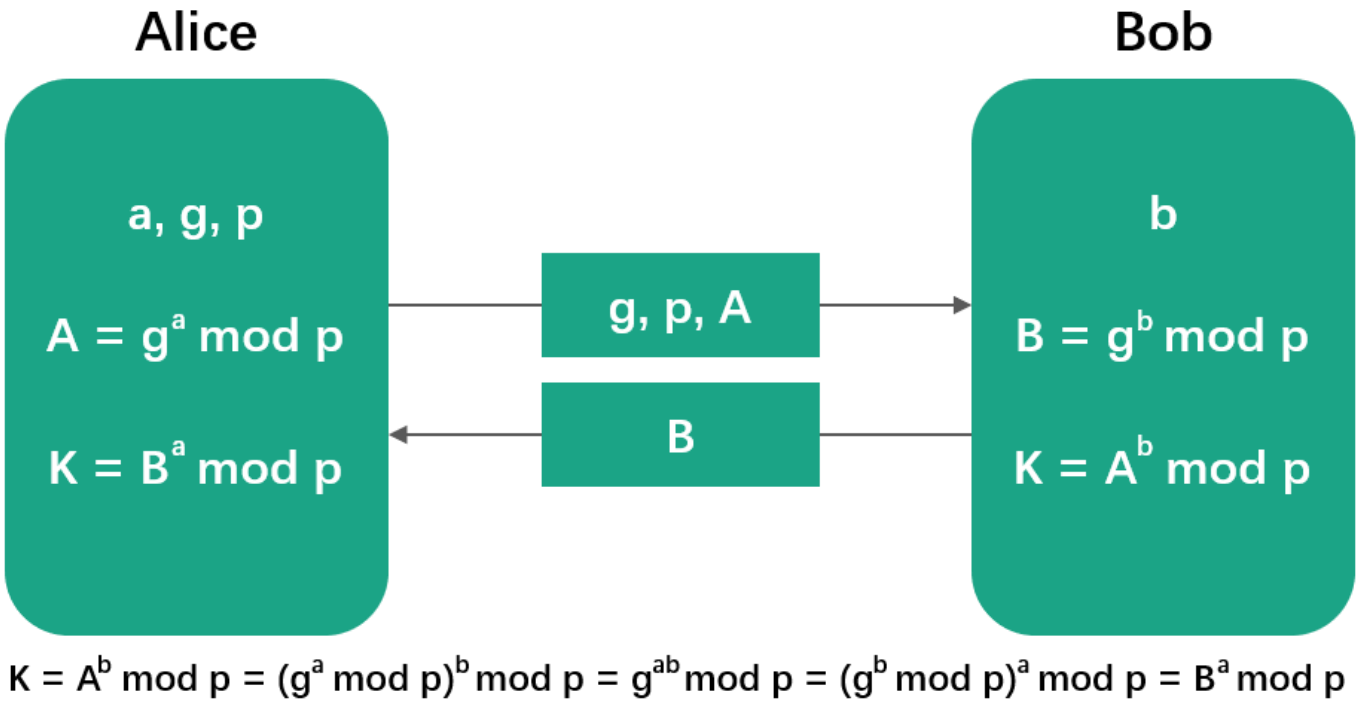
Firstly, transactions with special labels in the blockchain pass DH while market builders and participants exchange keys through a secure encrypted communication channel initially built on the SEER main chain. In this case, no information of locations will be revealed to either party. With SEER's efficient TPS (3,300 transactions per second and a block per 1.5 seconds), the encrypted communication channel is anticipated to generate and distribute keys within 5-10 seconds.

(DH-based key exchange process)

Secondly, one-to-one encryption is applied to all transmitted information with Rijndael symmetric encryption algorithm. Prediction market builders encrypt their prediction markets with keys and send them to market participants through encrypted channels so that the participants can use the keys to access relevant information by decrypting the blockchain-based prediction markets and perform relevant actions without building new communication channels to exchange keys with the market builders. Since the keys distributed to different market participants vary, if any participant's

key has been leaked, the market builder can identify the corresponding participant based on the key, revoke the keys (i.e., traitor tracing) and throw the participant to the blacklist.

Users without keys cannot view any information about the encrypted prediction markets of the blockchain.



Chapter 3 Administration

3.1 Committee

The Committee is the core of the SEER administrative framework. The Committee members are elected by SEER coin holders. The voting weight of every coin holder is determined by the proportion of its holdings to the total system capacity.

SEER has 11 Committee members in total and the authority and responsibilities of these Committee members are as follows:

(1) Adjusting transaction fee;

(2) Specifying blockchain parameter settings;

(3) Resolving disputes between prediction and crowdfunding markets;

(4) Processing applications for challenging Oracles;

(5) Reviewing proposals on developer remunerations, marketing campaigns and so on.

Clearly, the Committee is an important part of SEER. It is not only responsible for blockchain parameter management, but also in charge of the prediction and crowdfunding markets in case of any problems or disputes. What's more, the Committee, for the sake of accuracy, has the final say on the results produced by the decentralized Oracles.

Considering its special functions, to ensure every decision made by the Committee is the manifestation of most stakeholders' will, each decision has to pass the Committee upon approval of the majority of the Committee members. Since the Committee members are elected by the SEER token holders, SEER has managed to reach the optimum balance in terms of operating efficiency, democracy and fairness.

3.2 Witnesses

Similarly, witnesses are also elected by the SEER token holders according to the same voting weight calculation method as that of Committee member election. The election of witnesses has no effect on the Committee. One applying to be a witness is required to provide a specific number of tokens as collateral.

Witnesses are mainly responsible for processing transactions, signing on transactions, packing them into blocks for the purpose of transmitting them to other witnesses for confirmation and providing price feed service. A certain number of tokens are granted to witnesses on a monthly basis as the reward for processing transactions. The witnesses around the world should be taken into account as a key factor for decentralization of the blockchain system. They are required to be responsible for voters and properly process transactions. Every block generated by a witness will be officially recognized and accepted only when it has been confirmed by most of other witnesses. The tokens granted to witnesses are used for routine expenses arising from running servers and maintenance and rewarding them for being witnesses.

3.3 Prediction market builders, Oracle and crowdfunding participants

SEER considers prediction market builders, Oracles and crowdfunding participants as individuals making contributions to the system. Oracles are providers of neutral and authentic real-world data while prediction market builders and crowdfunding participants facilitate the expansion of the system and present more sports events for other users. Hence, they also should be rewarded with tokens as witnesses are granted tokens by the system for processing transactions. The level of a

prediction market participant supporting a specific prediction market should be taken into consideration when calculating the tokens to be granted.

3.4 Account reinstatement

SEER is able to introduce the key recovery function that enables reinstatement of a partner's account via a designated key provided by an account so that users can reset their accounts by using the original keys under the assistance of their key recovery partners.

3.5 Account blocking

Because certain Oracles in prediction markets may deliberately keep submitting false results and there may exist other malicious users, SEER plans to adopt a complete account blocking, declaration and appealing mechanism. Through deliberation of the Committee, the accounts of malicious users will be blocked upon approval of the majority of the Committee members.

3.6 Cross-platform user login system

SEER will have the Web Authorization (OAuth) protocol-based cross-platform user login and binding functions. Presently, the WeChat/Weibo/Alipay Apps have been added to the development blueprint for cross-platform login verification. It is anticipated that this function will be first applied to the minimum valid version. The development team has successfully completed the interoperability between the OAuth protocol and the Graphene toolkits.

Chapter 4 Application Context

4.1 Sports betting

Sports betting is an enormous market and SEER has provided an authentic decentralized sports betting solution. In addition to the general functions of a single-host Oracle, an advanced decentralized Oracle based on the multiple-hosts model is also available, which can efficiently prevent the failure in timely producing results due to frauds or single-point fault of the traditional centralized service.

4.2 Assets price prediction

Assets price including that of real estate and bulk commodities is closely associated with our daily life. A user may build a prediction market via SEER and invite other users to participate in the prediction about a specific type of assets where other users can intuitively learn the estimated price of those assets. For instance, in a market on the "prediction about the average housing price in Shenzhen in 2018", users who intend to purchase houses in Shenzhen can adjust their plans according to the prediction results contributed by the market participants.

4.3 Financial market prediction

Presently, there are still drawbacks to financial market prediction that the tools are generally inaccurate, inefficient and expensive. To overcome these disadvantages, SEER offers a convenient, reliable and efficient prediction market tool. Getting rid of complicated settings, the tool enables

users to build prediction markets on SEER and invite other users to participate in predictions about "U.S. GDP growth in 2018" or other issues. From SEER, fund managers and professional investors can learn various opinions about the coming events at a low cost, but in a more accurate way.

4.4 Event prediction

In addition to what's mentioned above, SEER also allows predictions about political, social and other events, e.g., whether Trump has the chance to serve for another term of office, whether the box office of a film can reach RMB 1 billion, or when the next iPhone is coming.

Chapter 5 Development Route

5.1 Development blueprint

Launched in October 2016. At the same time, the SEER development project is underway and expects to release the first minimum valid version at the beginning of 2018, which is provided with prediction market building and other fundamental functions. The third-party developer interfaces are anticipated to be released in the second quarter of 2018. By then, other Apps and prediction market APIs will also be successively released.

5.2 Supporting third-party developers

We are fully aware that SEER can only sustain development by continuously providing accesses of a greater number of Apps and developing attractive gameplay. Hence, SEER will provide a series of development interfaces and data integration interfaces for third-party developers upon release for the convenience of secondary development by the platform carrier and data providers. In addition, SEER will retain a specific amount of community promotion fund for the purpose of publicity and development support. Specifically, the community promotion fund will be used for holding developer meetings, activities and development contests in order to cultivate more developers for SEER, offer diversified gameplay and constantly improve the SEER ecosystem.