0°DAO

Social Networks Reputation Systems And The Blockchain Revolution

Zero⁰DAO Light Whitepaper

1 Background

Incentive dilemma of Social Network Motivation

incentivizing good behavior makes good behavior disappear

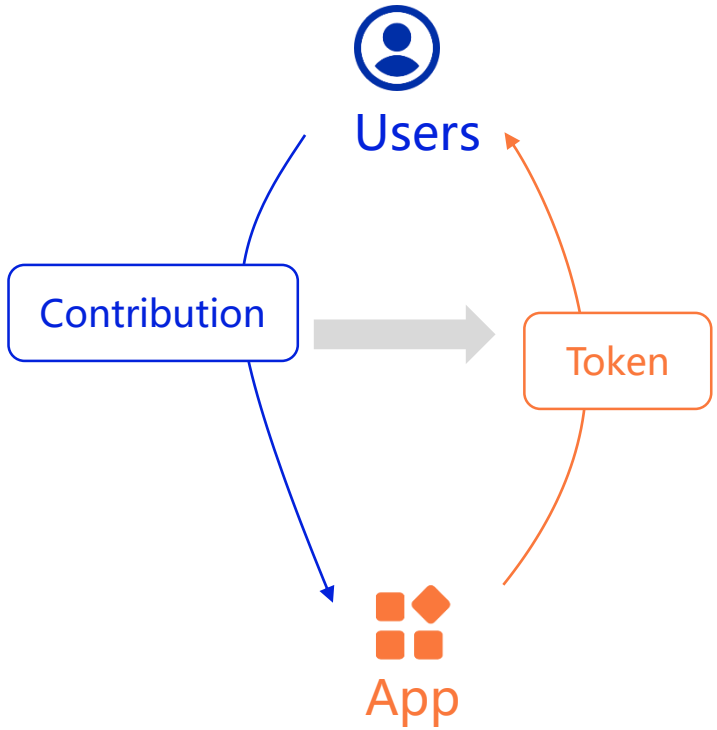
Ideal

Users = Shareholder

Contribution = Earnings

Data = Value

Actions



Results

Helping Others

I hope more people know me

Self-realization

Social Motivation

I am valuable

Sharing Spirit

The joy of creation

Annihilation

Material Motivation

Pay me!

Zero⁰DAO Social Finance

Amplify social motives

All for one, one for all

Amplify social motives

We still quantify user contributions and settle them into Tokens, which we call social currency. It is frozen and at some point assigned to users trusted by the owner, it is also social currency and goes on to be shared.

I am for me, I am for everyone

Retention of material motives

Users still retain a small percentage of Tokens This percentage is adjusted by the community to suit the needs of different operational phases

Sybil's home turf

The heroes stop here

Quadratic Voting as an example

Scholars have identified a model called Quadratic Voting that ensures consistency between individual interests and social welfare maximization and solves the free-rider problem.

However, it has an Achilles heel and cannot defend against cheating problems, namely Sybil Attacks. Not coincidentally, the blockchain is the Sybil's home turf.

Zero⁰DAO Reputation System

Reputation systems are one of the most effective solutions to Sybil attacks, but they can themselves run into Sybil attack problems. Current reputation system solutions are in the following categories.

	Decentration	Security	Sybil resistance	Experience	Quantifiable
Fully certified	×	×	√	×	×
Partial Certification	○	○	○	○	×
Evaluation-based	√	○	○	×	√
Transaction-based	○	○	○	○	√
Activity -based	○	○	√	○	○
Oracle	○	×	×	√	√
Zero⁰DAO	√	√	√	√	√

Quantifiability is a very important point who ensures the usability of the reputation system, for example, in movie voting applications where the need for security level is low, a lower reputation threshold can be used, while financial applications requiring higher security set a higher reputation threshold.

Solutions

Social Finance

1. The app quantifies user contributions and sends them to social currency of A

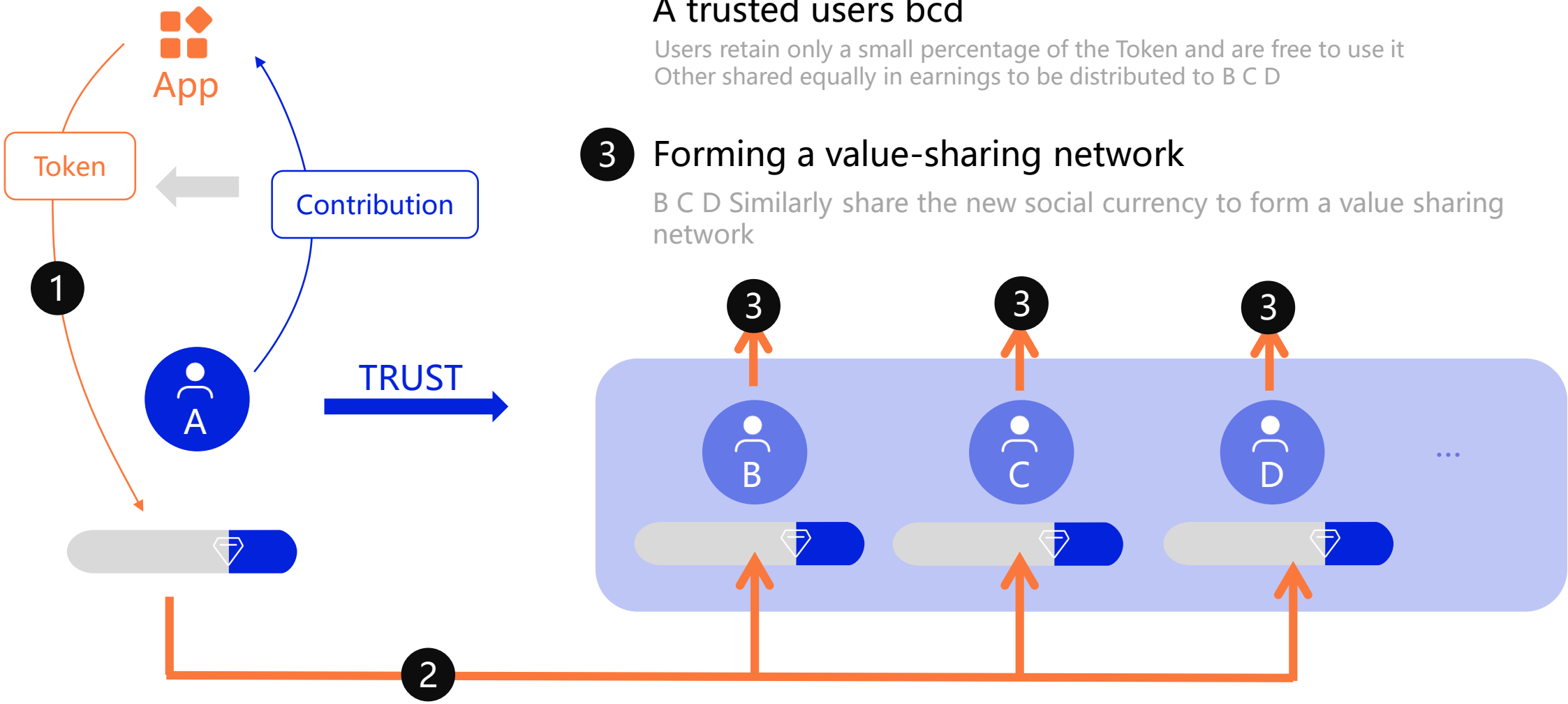
   This part of the Token is frozen and cannot be used by the owner

2. The system periodically assigns as social currency to A trusted users bcd

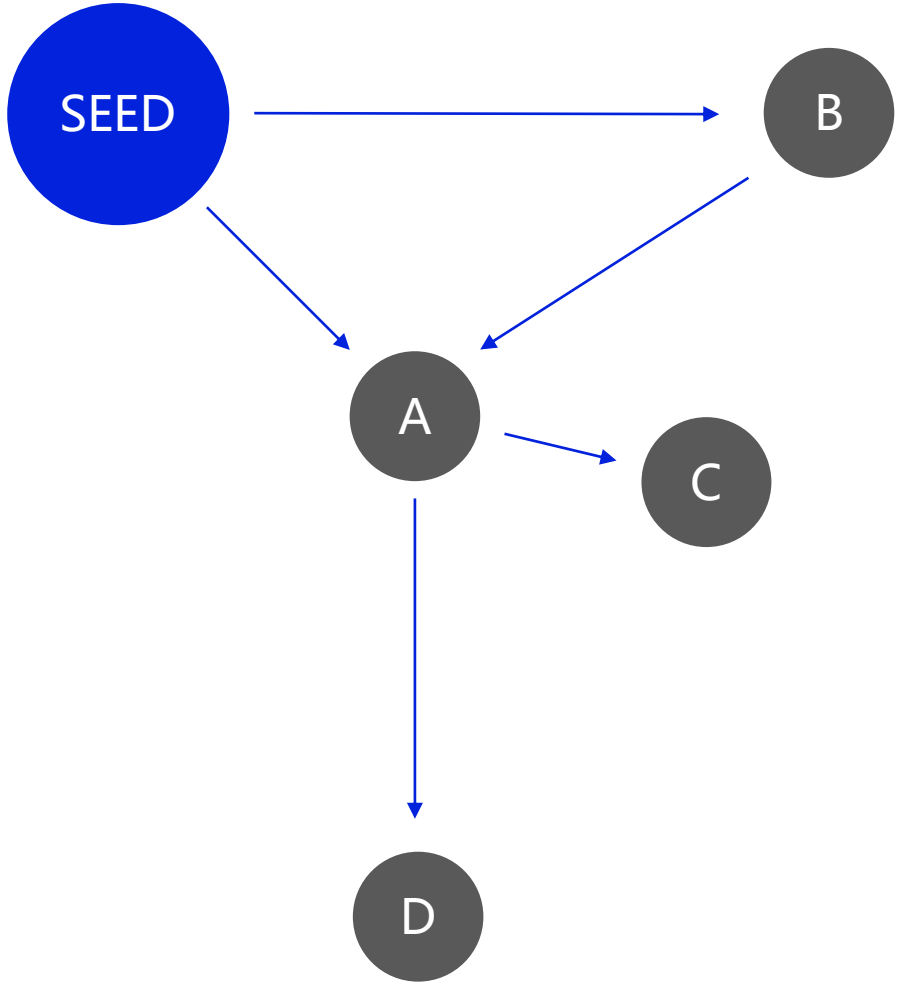
   Users retain only a small percentage of the Token and are free to use it
   Other shared equally in earnings to be distributed to B C D

3. Forming a value-sharing network

   B C D Similarly share the new social currency to form a value sharing network



Reputation System ■ TIR Algorithm



The TIR algorithm, formerly known as Google's text retrieval algorithm for search engines, is used to replace the vulnerable PageRank algorithm, which is computationally simple and requires no iterations compared to its TrustRank counterpart.

The TIR algorithm relies on two assumptions

- High-influence users are less likely to trust fake users
- The longer the trust, the more credible it is

TIR algorithm features

Finality

Algorithms with deterministic structured data and deterministic computational results

Efficient

Low validation costs to ensure it can run at the blockchain

Dynamicity

Can reflect user activity

Security

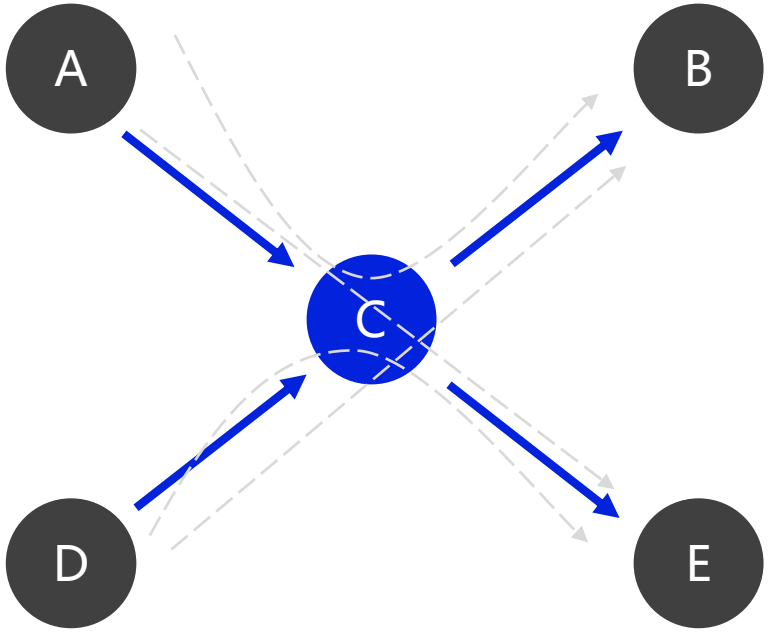
Resistant to Sybil attacks

Quantifiable

Quantitative expression of the user's reputation value

Reputation System

Sybil resistance



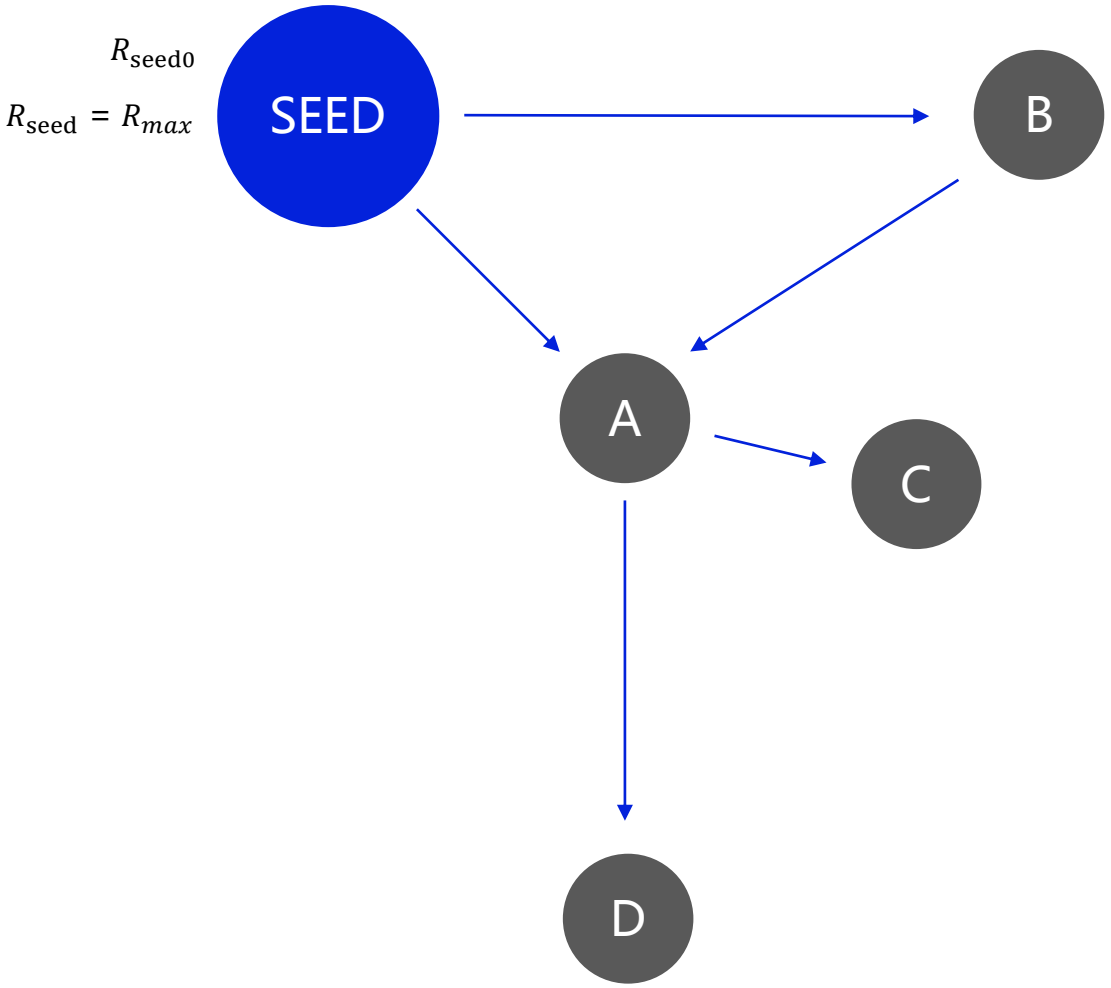
Seed selection

Based on the longest shortest path

Select the longest shortest path through the most number of nodes as seed users
The larger the network, the higher the account cost, the more difficult it is to cheat

User	Number of longest shortest paths through the nodes
A	2
B	2
Seed C	4
D	2
E	2

Reputation System ■ TIR Algorithm



■ Calculation steps

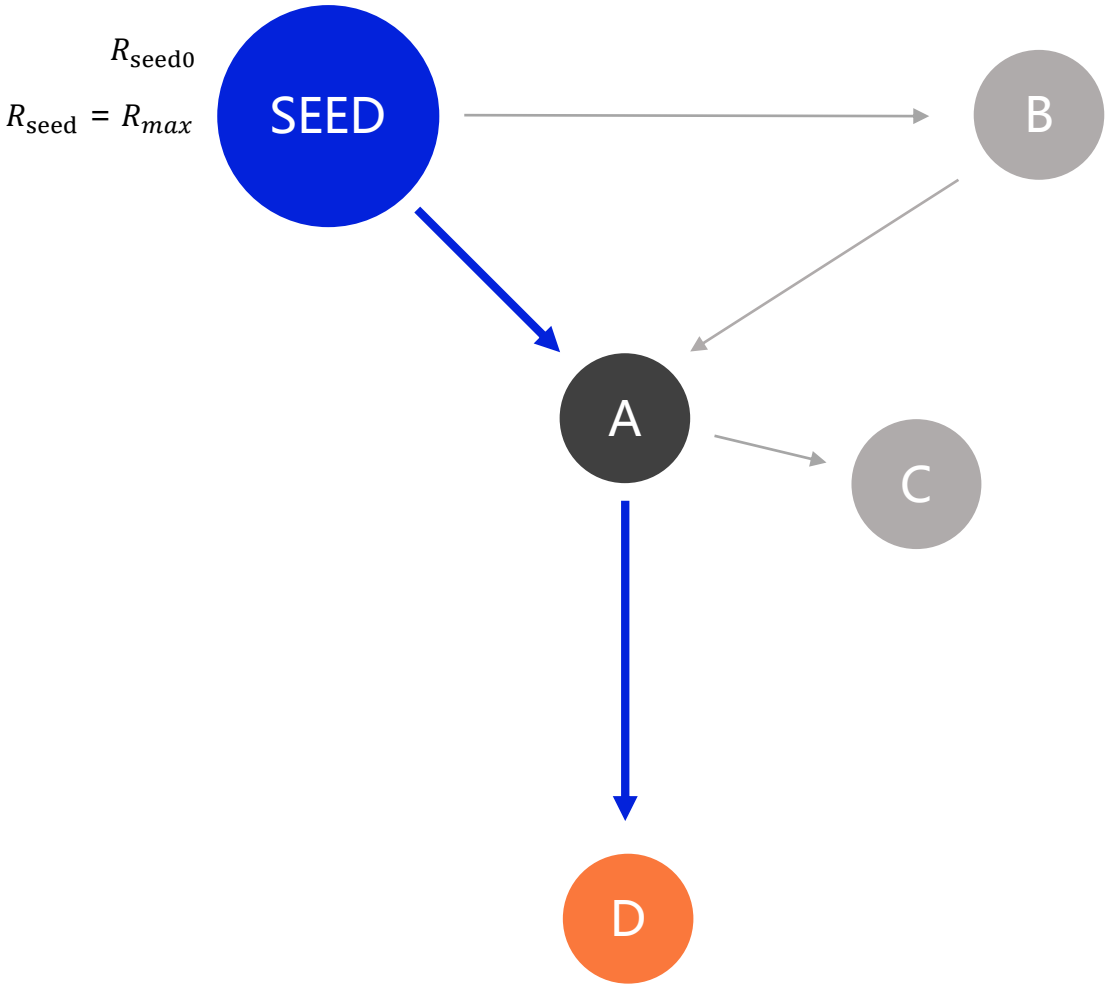
❶ Determine the seed user and set its score to a constant R_{max}

Seed users are considered as trusted users and pass reputation values to other users through trust relationships.

The reputation of a user is the sum of the reputation values passed to it by all seed users.

Reputation System

TIR Algorithm

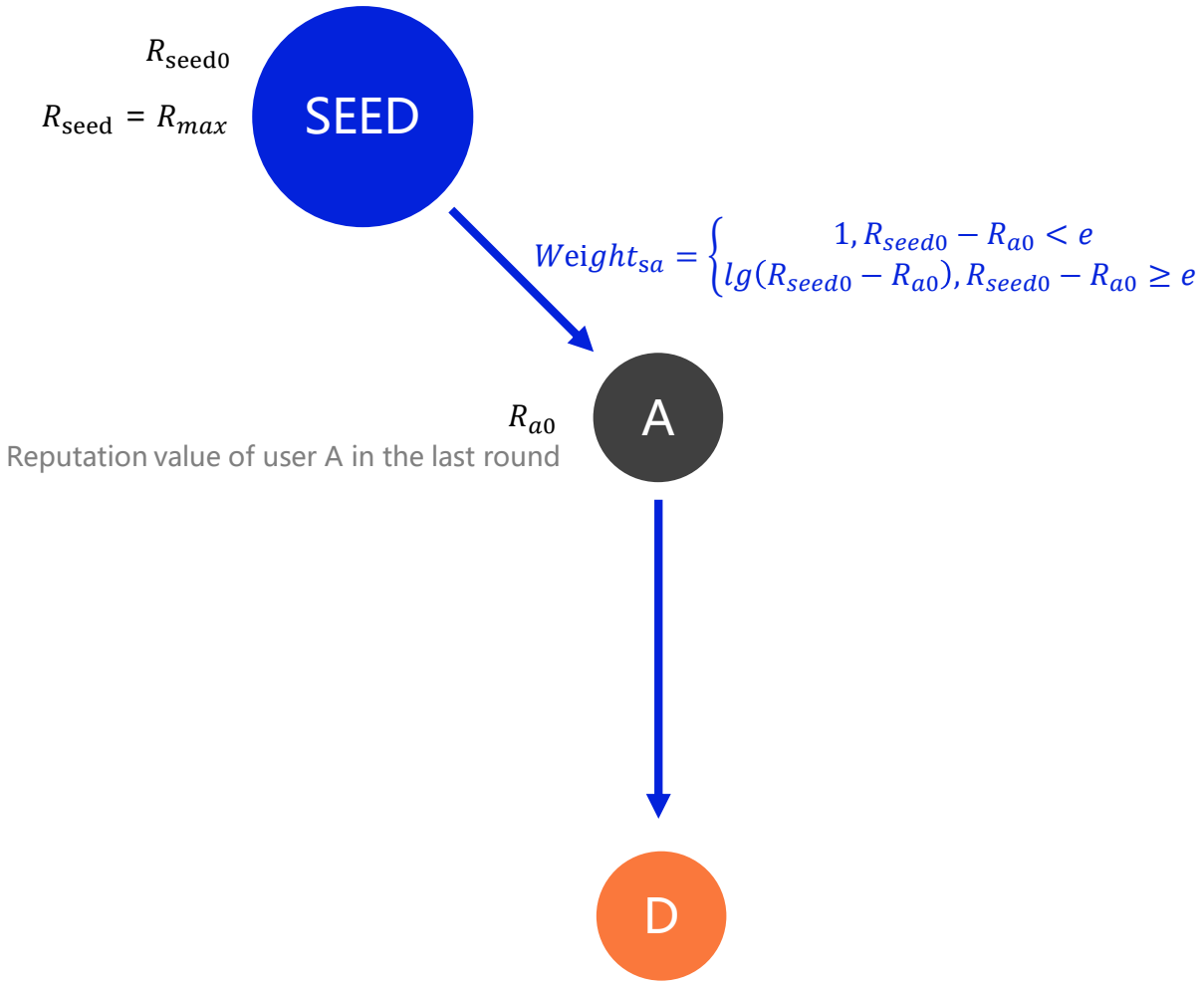


Calculation steps

❷ Calculate the weighted shortest path between the target node and the seed user

Taking user D as an example, the shortest path in the graph is Seed -> A -> D , and calculate the path length based on the reputation of users in the previous round

Reputation System ■ TIR Algorithm



■ Calculation steps

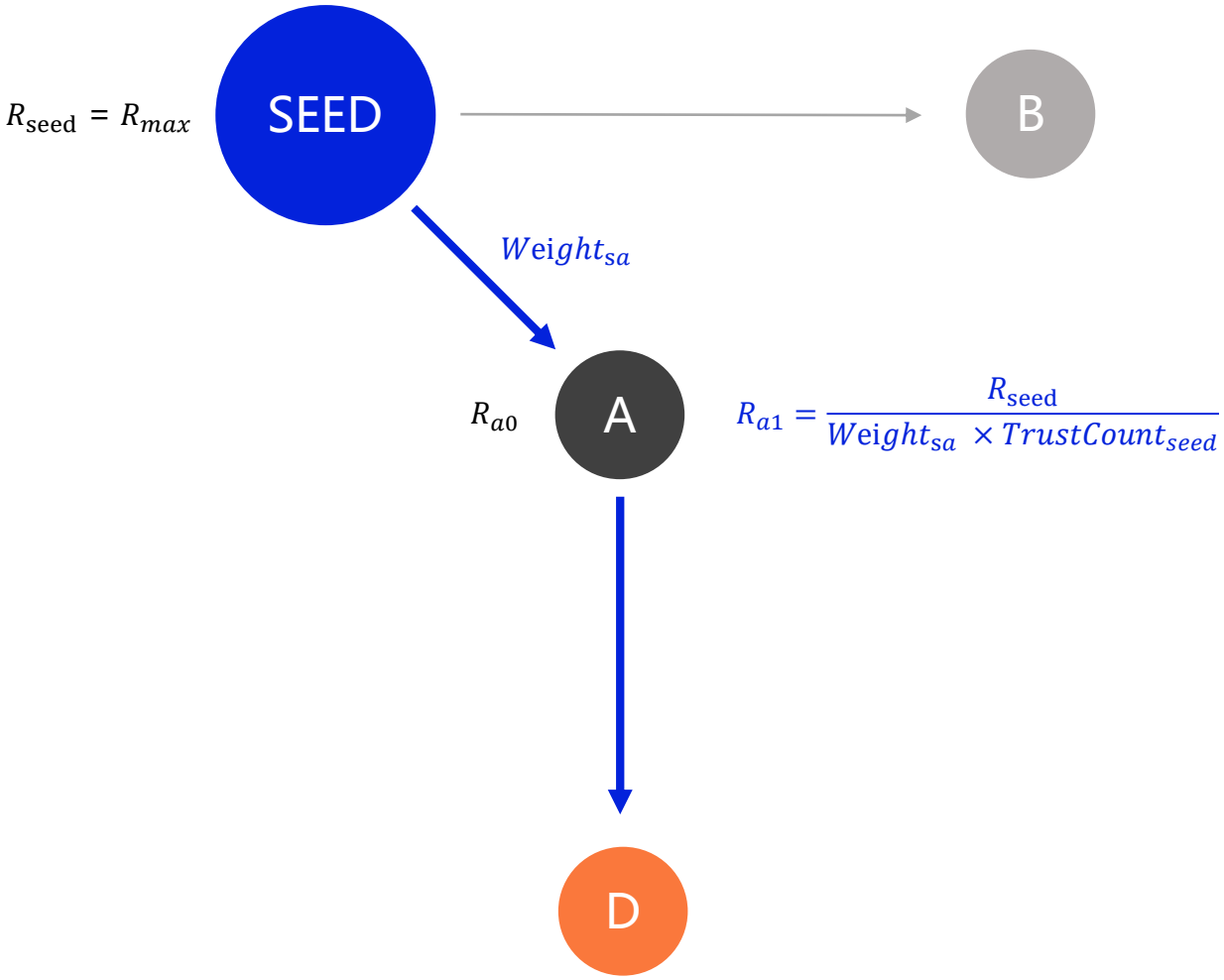
❸ Path weight calculation

The path length is a confidence level, which stems from our assumptions.

A low-reputation user trusts a high-reputation user, which is considered trustworthy. If a high-reputation user trusts a low-reputation user, the path length is the natural logarithm of the reputation value difference. In this case, the larger the reputation difference is, the longer the path is.

This is a common way in social computing; for example, just because Kobe trusts his elementary school classmates does not mean that his elementary school classmates have very high influence (reputation).

Reputation System ■ TIR Algorithm

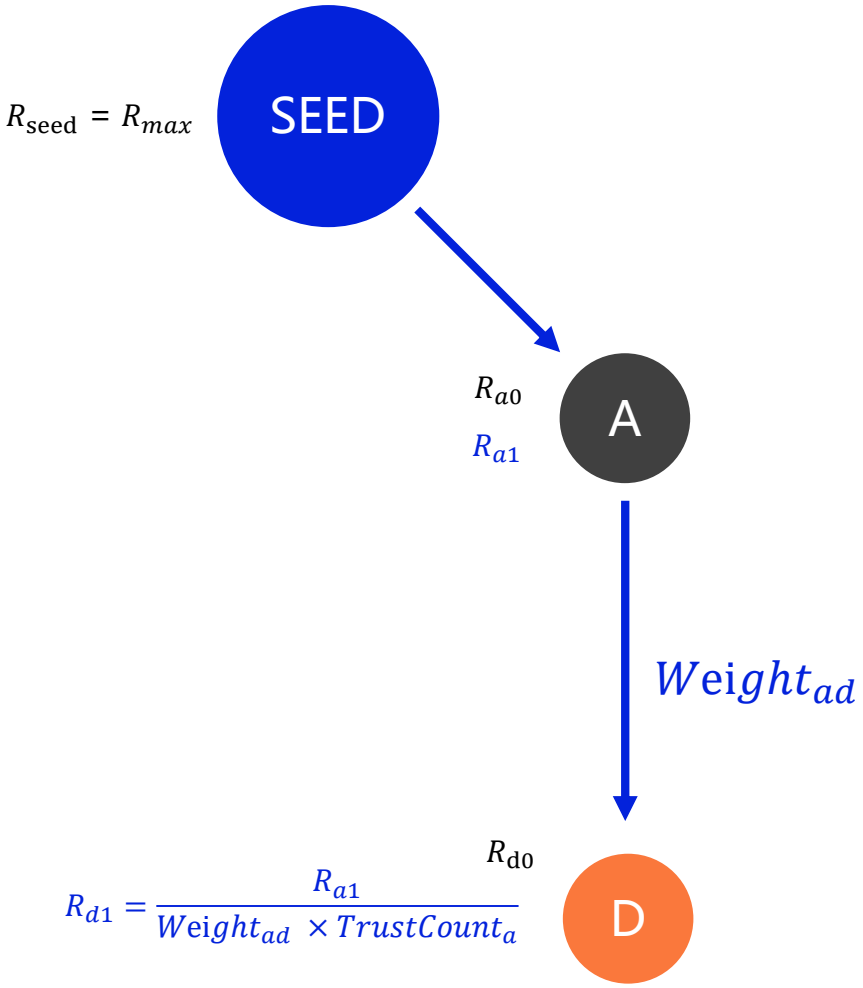


■ Calculation steps

❹ Calculating intermediate node transfer score

- Evenly divided according to the number of source node trusts
- Inversely proportional to the path weight

Reputation System ■ TIR Algorithm

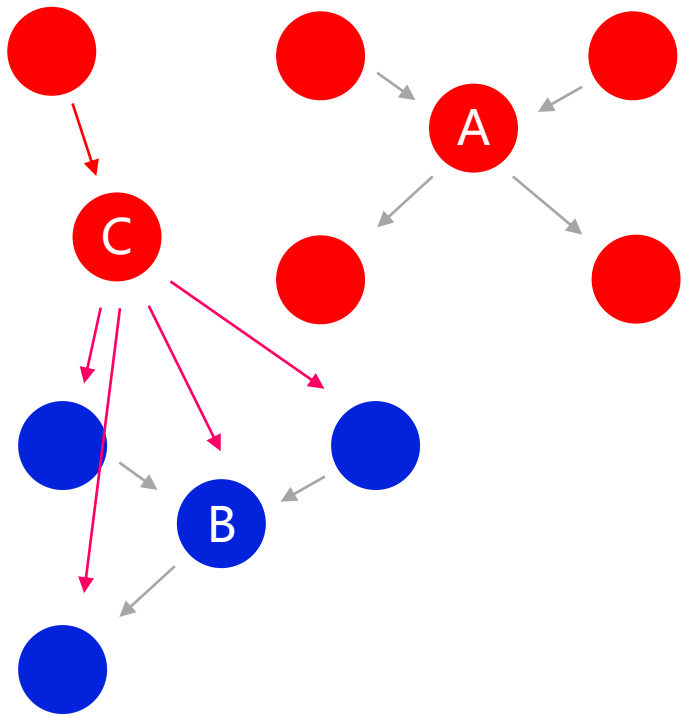


■ Calculation steps

❺ Calculate the path from A to D in the same way and calculate the reputation R_{d1}

Reputation System

Sybil resistance



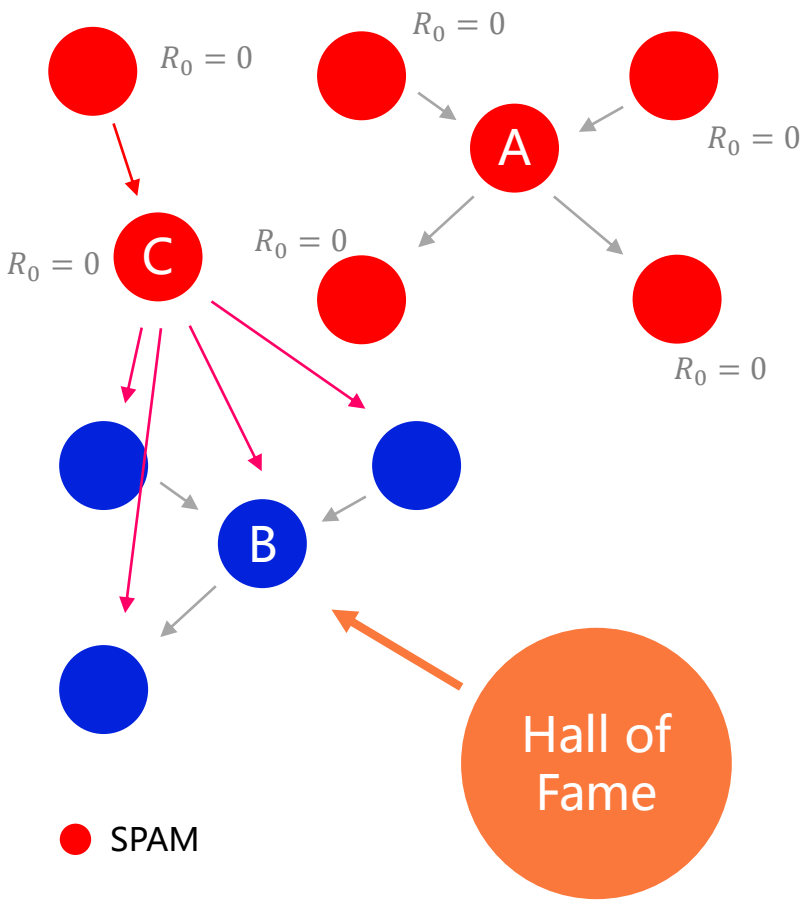
Sybil Attack

So far, the algorithm is still not able to blocking sybil attacks.

The algorithm will pick to cheat nodes when the attacker constructs a graph that is more favorable to him (e.g. more fake nodes and `trust`). Although we can raise the cost of an attack by setting higher account retention balances, raising fees, or raising gas, and expecting the network to be large enough so that the attacker does not have enough wealth or benefit to attack the network. But this also raises the cost of use for honest users, which is not elegant, and does not guarantee mathematical security.

Reputation System

Sybil resistance



Hall of Fame

- The community selects a small number of Hall of Fame users

  SPAM nodes have no reputation value, or very little reputation value they cannot influence the Hall of Fame selection

- Use distance from the Hall of Fame as a calculation factor

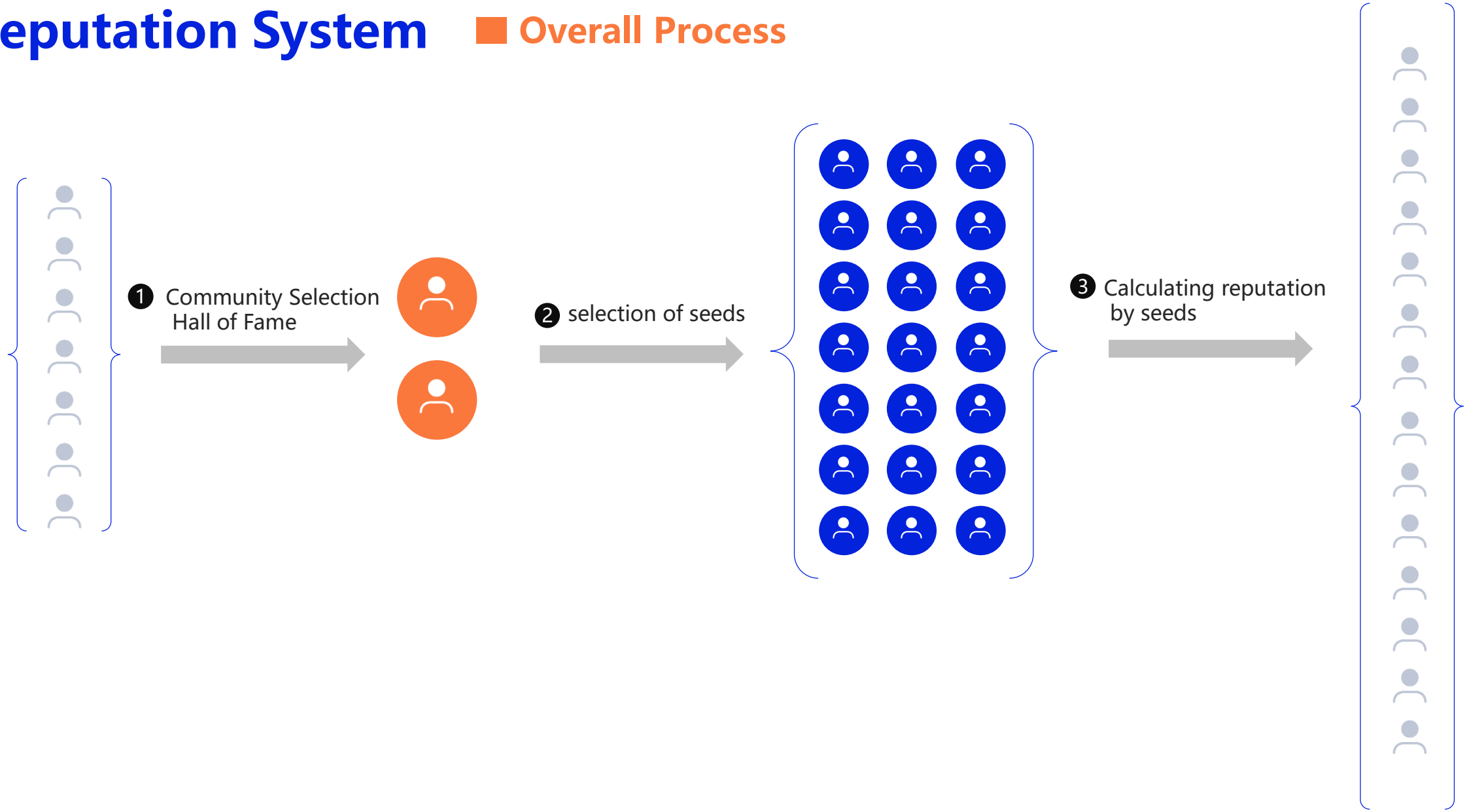
  The selection of seed nodes not only considers the longest shortest path, and also incorporates the distance to the Hall of Fame, thus ensuring the mathematical level of security of the network.

- Blocking SPAM nodes

  Only a very small number of Hall of Fame users under the supervision of the community need to be selected to derive a large number of seed nodes, ensuring a secure governance radius that allows fake nodes to be excluded from the seed users. Also ensures the coverage of the reputation system

Reputation System

Overall Process



3 Implementation

Layer1 Blockchain

Substrate

Zero⁰DAO is developed base-substrate
Enables us to share in the development of the substarate ecosystem
including smart contract support, cross-chain support, and more.

Full Capability blockchain

Zero⁰DAO supports smart contracts
so that Dapp and other chains can better leverage our social finance, social relationship and reputation systems.

Reflexivity Of the Algorithm

Algorithms change user behavior, algorithms are incomplete
Zero⁰DAO utilizes forkless upgrades of substrate to perform algorithm upgrades

Challenge Roles

Analyst

Allocate social currency

Update user reputation

Obtain commission

validator

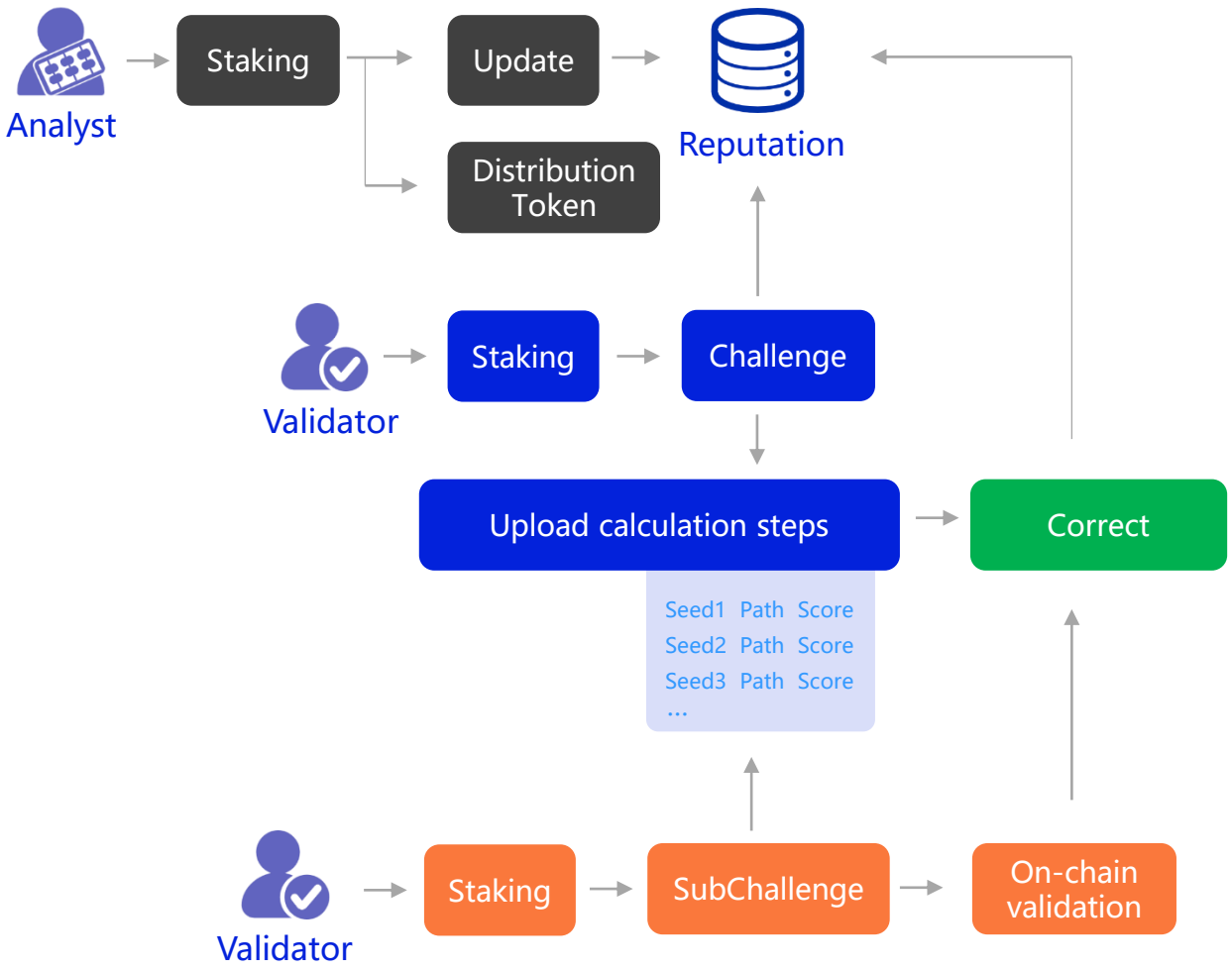
Challenge incorrect reputation values

Upload the path and reputation value of each seed to the target user

Clear data after the challenge is completed

Receive challenge revenue

Challenge Process



Challenge Period

Compared to Token transfers, reputation systems are not as time-sensitive, so we have a very secure window. During this period each user can challenge the current calculation. If there is no challenger after this period, the reputation value is considered credible. The accountant or the challenger receives the benefit after this period.

SubChallenge

In order to reduce the consumption of resources on the chain to a greater extent, the system does not validate the calculation results. The Validator only needs to upload data to the chain quickly.

Other challengers can validate the uploaded data and can initiate a second challenge to eliminate errors before the system validates the calculation.

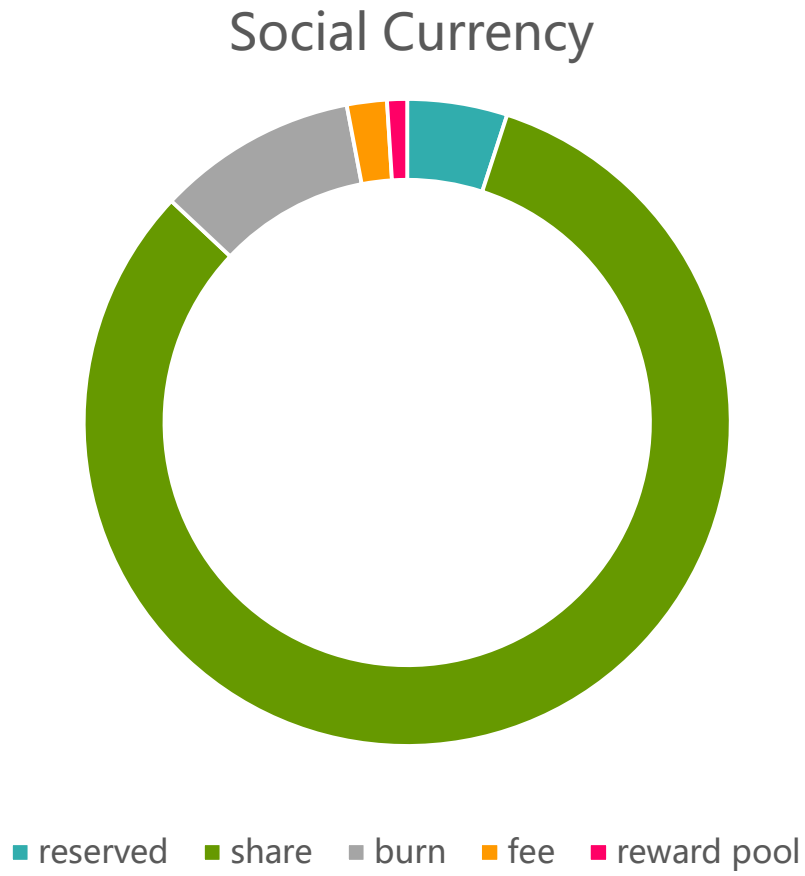
Proxy

After the challenge period has expired, there will be a claiming period in which the challenger or accountant must claim the proceeds and clear the challenge data.

If the challenge proceeds are not claimed after the claiming period, anyone else can claim them for them and receive a portion of the proceeds, while updating the reputation value and clearing the data.

Challenge

Earnings Distribution



The Analyst updates the user's reputation value while allocating the amount to be allocated to that user, being divided into 5 parts.

❶ Reserved

Unlock to the owner's free balance. The percentage can be adjusted by the community.

❷ Share

Transfer to the social currency of users trusted by the owner.

❸ Burn

Share to all users.

❹ Fee

Analyst's fee

❺ Reward pool

Used to solve the verifier's Dilemma.

4 Applications

Social Finance

- Blockchaining of traditional social networks
- Radical Social Networking
- Blockchain computing advertising

Reputation System

- On-chain Governance
- Unsecured Lending
- Super Bank

Zero-cost payment

- Charity
- Open Source Community
- New Crowdfunding
- Decentralized Storage
- Copyright Market

Social Finance ■ Blockchaining of traditional social networks

■ One Click Access

ZeroDAO does not care about how the application stores its data, it is the same whether he stores it decentrally or on his own servers. We only provide the underlying economic system and user relationships so that even pre-existing non-blockchain communities can easily access the network with a single Trust button.

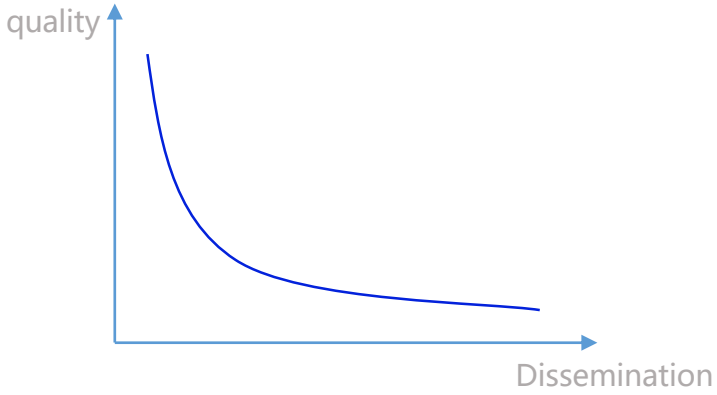
■ Activating Communities

The social motivation of ZeroDAO amplification effect is more likely to activate the traditional community vitality. How much revenue users get ultimately depends on how many quality users pay attention to it, which will not destroy the community atmosphere and will also motivate more quality users to create more quality content.

Social Finance ■ Radical Social Networking

Community evaporation

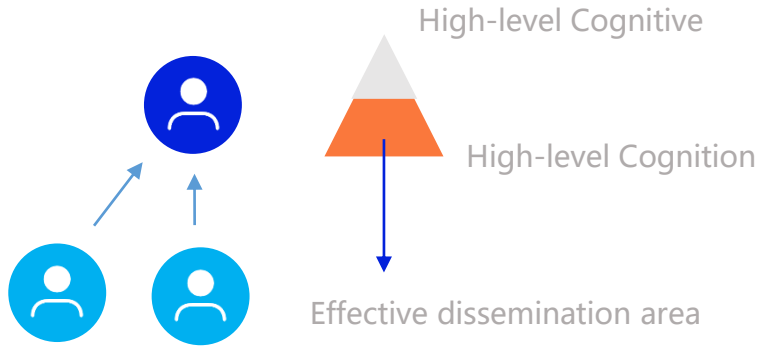
It refers to the development of social networks, with the growth of user volume, the quality of content then declined, and some people call it the expulsion of good money from bad money, which is almost the current community operation can not fundamentally solve the problem.



Quality-Dissemination disorder

Rumors, extreme and radical content are more likely to be widely distributed, while professional content goes unnoticed, as is often the case in large social networks and communities.

It in turn backfires on users who have no incentive to produce quality content, causing a vicious cycle.



Cognitive dissonance

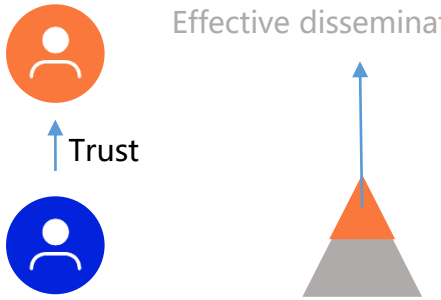
Essentially it lies in the cognitive disparity between the information source and the audience in social networks, i.e. users downgrade information to their fans

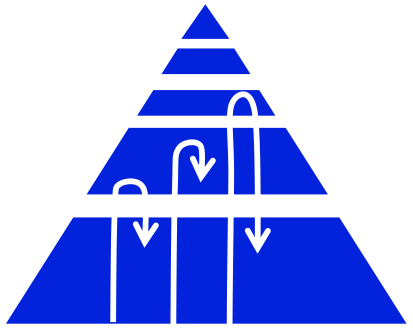
Most fans have less cognitive ability than a quality professional, resulting in the inability to identify quality content and spread it。

TIP: This is only from a professional point of view, not to divide people into high and low perceptions, for example, Bolt is high perception in sprinting, but not necessarily in cooking. A chef is more cognizant than Bolt in cooking, but probably can't outrun him.

Social Finance ■ Radical Social Networking

■ Upward dissemination





■ Upward dissemination

Content posted by users is no longer distributed to their own followers
Instead, they are distributed to their trusted users

■ Economic system design

ZeroDAO's social finance has fundamentally solved the problem of negative incentives, based on which the economic system of the dissemination process needs to be designed to ensure the good operation of the product. And the difference of economic system design will give birth to different social network models.

■ Gradually dissemination

Depending on the reputation value, the message is spread step by step, and the user can choose UP to spread the message to the next level, or do nothing

The higher the quality of the content, the more it spreads. Theoretically, if your message is of high enough quality, you can send it to any people.

■ Reputation as an influence

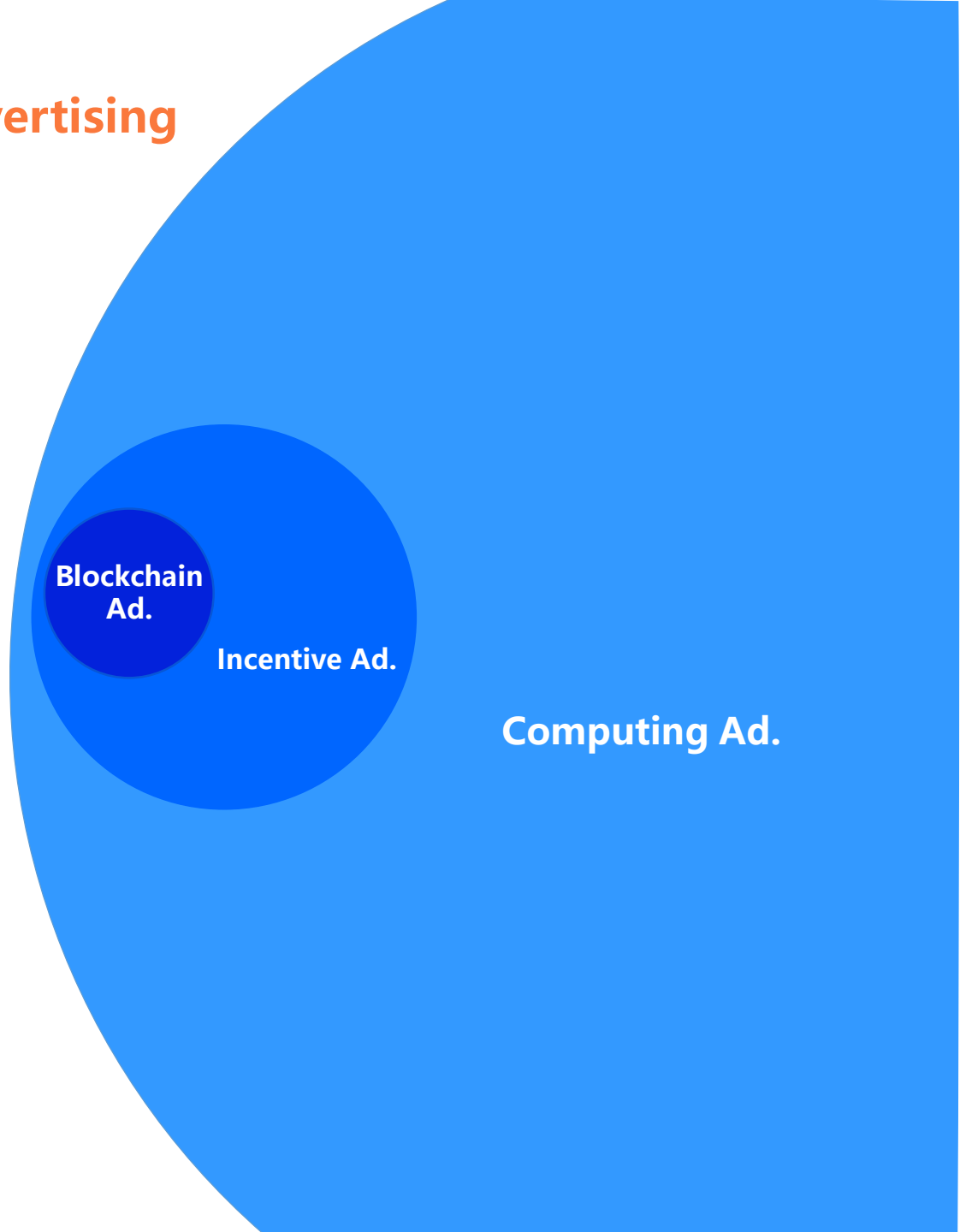
ZeroDAO's reputation system is somehow a reflection of the user's influence, which can indirectly react to the perceived ability and provide a basis for reverse propagation.

Social Finance ■ Blockchain computing advertising

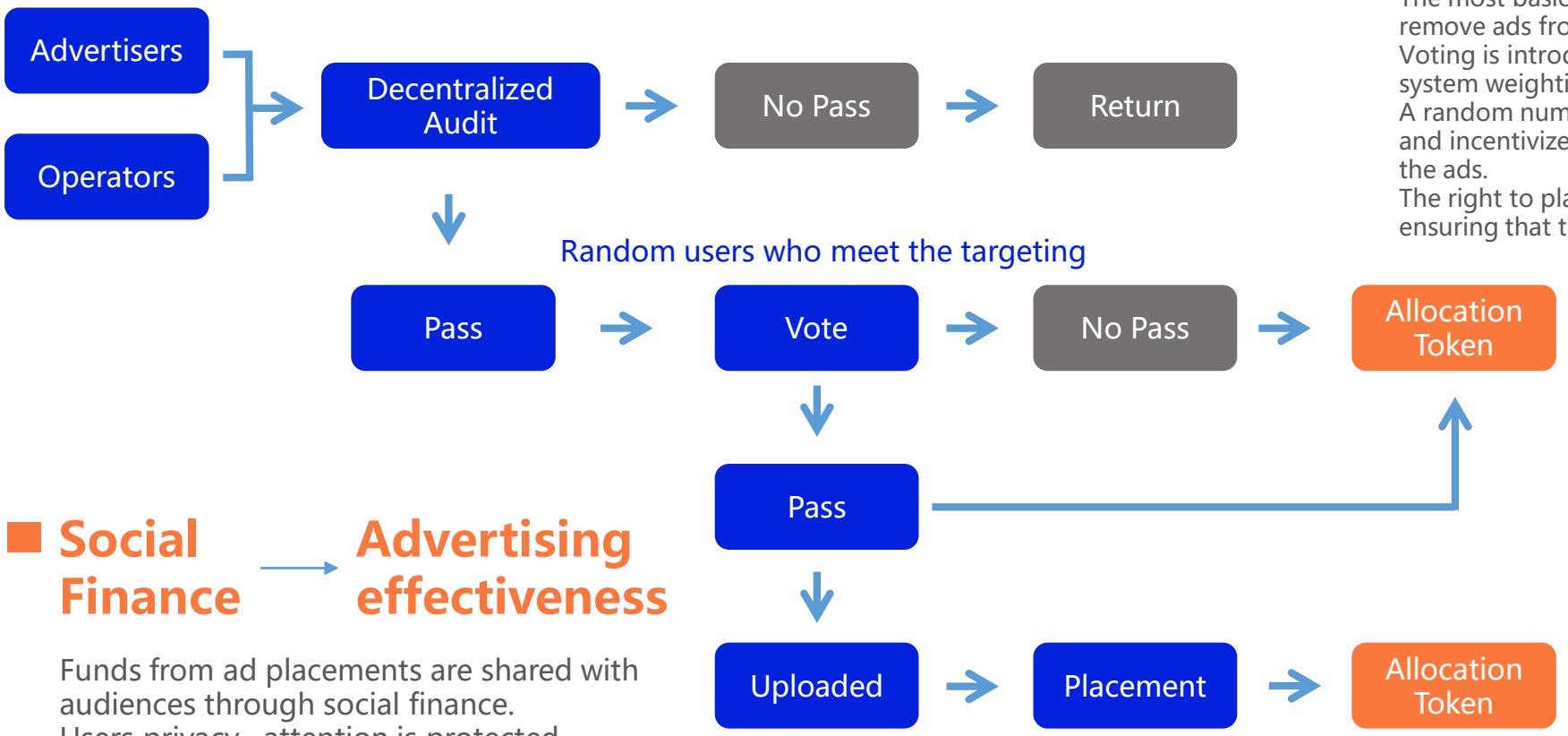
■ Traditional blockchain advertising evolves into incentive advertising

Traditional Blockchain Ads Settle Attention to Tokens. Evolves blockchain ads into incentive ads, extremely narrow scenario.

Attention → Token



Social Finance ■ Blockchain computing advertising



■ On-chain Governance → User Rights

The most basic right to calculate ads is the right to place and remove ads from the shelves.
Voting is introduced into ad management through reputation system weighting.
A random number of users are selected to vote on the ads and incentivize them to confirm the right to place and remove the ads.
The right to place and remove ads is given to users, thus ensuring that their rights are guaranteed.

■ Social Finance → Advertising effectiveness

Funds from ad placements are shared with audiences through social finance.
Users privacy , attention is protected.
At the same time does not turn advertising into Incentive advertising, to ensure the effectiveness of advertising.

On-chain Governance

Ideal country

To achieve an ideal-state style governance model, one only needs to set a very high participation threshold

Quadratic Voting

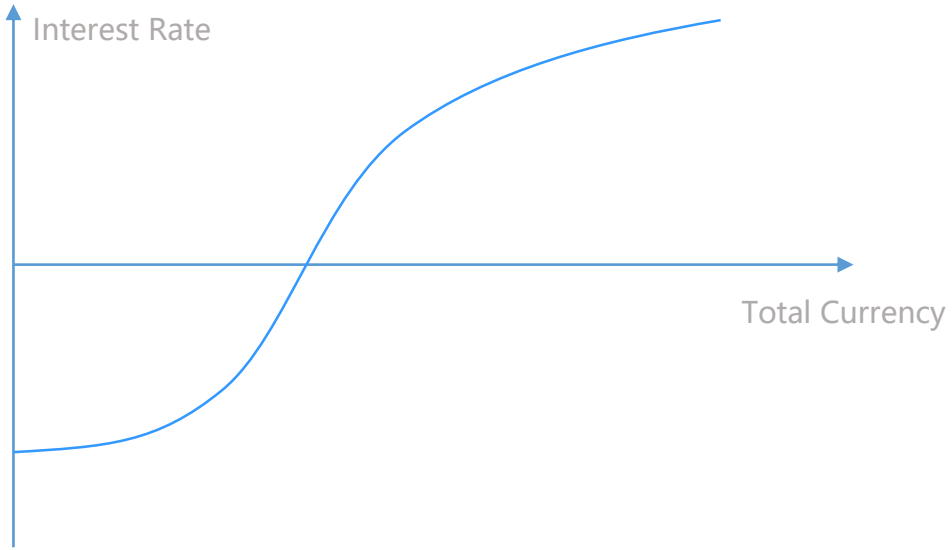
ZeroDAO's Sybil-attack resistant reputation system, capable of truly complete Quadratic Voting

……

A decentralized, quantifiable, Sybil-attack resistant reputation system will be the best place to experiment with on-chain governance, and you can use it to implement more ways to govern.

Super Bank

A more ideal banking model



Super bank is another banking model other than central bank-commercial bank, he operates on blockchain through smart contract, he has credit financial capability, directly facing users, sensing user behavior instantly and adjusting interest rate instantly. He has deterministic expectations, including a flexible total amount of issuance, deterministic interest rate changes, and therefore can effectively sense the economic crisis. Even in case of economic crisis, he possesses deterministic self-recovery ability.

Credit Finance

ZeroDAO provides a highly available reputation system that can be used to enable unsecured lending and thus credit finance, and blockchain finance will truly move into the realm of modern finance.

Total amount of flexible Currency

Aggregates are regulated through smart contract deterministic algorithms

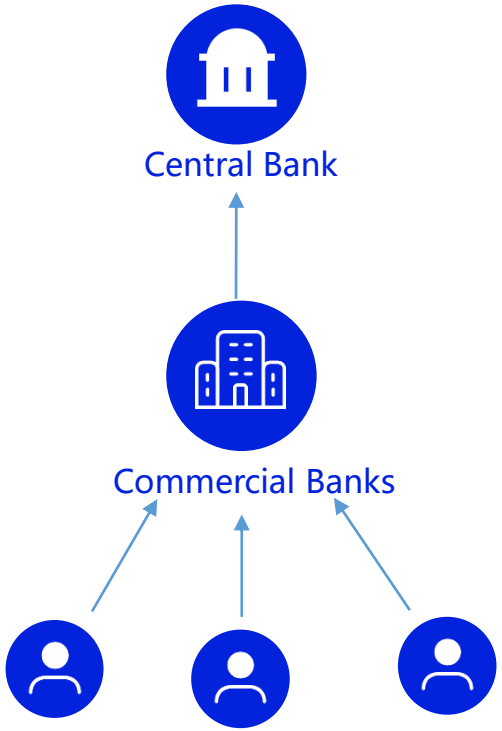
Aggregates are resiliently maintained within a range because of debt maturity and bad debt.

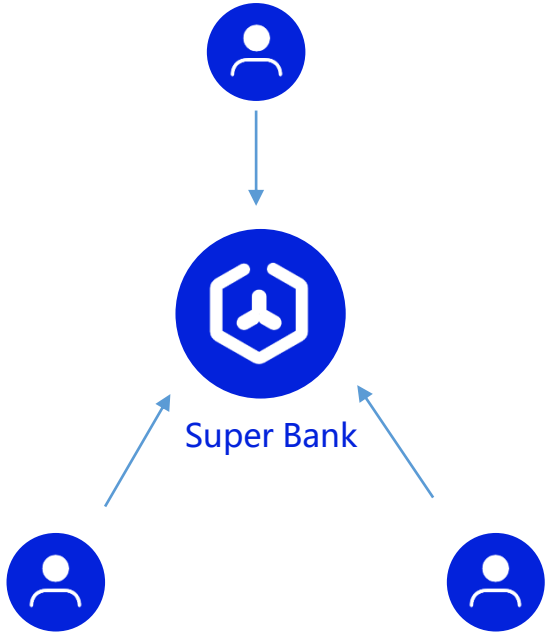
Instant Interest Rate

The interest rate is determined by the current aggregate and reputation system, which is instantly adjustable and flexible.
The interest charged at positive rates will be completely destroyed.
When the total amount is less than the threshold, negative interest rates can be achieved to encourage circulation.

Super Bank

A more ideal banking model





Instant Perception

Direct to the user.
Able to sense the market conditions behind each transaction.
Every transaction is dynamically adjusted.
There is no Minsky moment.

Deterministic expectations

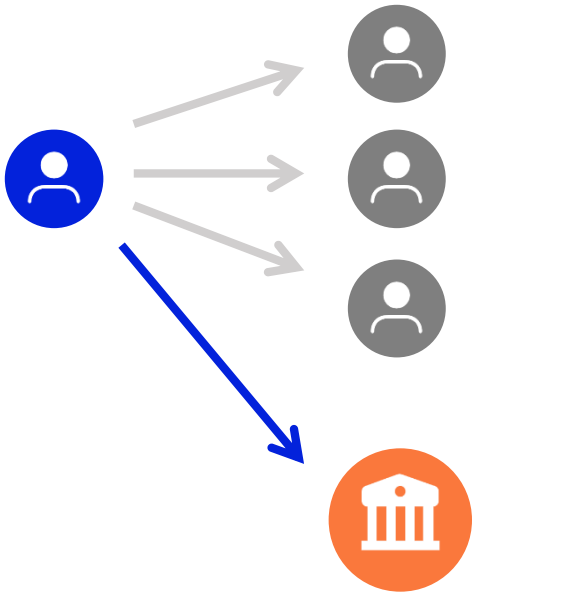
Controlled by smart contract algorithms.
Users have deterministic expectations of the future,thus reducing the reinforcement of risk by irrational behavior.

Independence

Decentralized nature gives it unparalleled independence.

Zero-cost Payment

The user didn't pay anything



Institutional Accounts

Institutional Accounts

- A special type of account that can be trusted like a normal account, except that it is only involved in distribution and not in the calculation of the reputation system.
- The allocated amount goes directly to the free account and is not reallocated.
- Reviewed by community vote.

Zero cost

- The funds obtained by the institution are derived from the social currency of user and cannot be used by owner without any loss to the user.
- Users have zero loss of payment in their mental accounts and are more willing to accept such a payment model, which is a new payment model that can be applied to a variety of scenarios.

Applications - New Payment Solutions

Charity | Open Source Community | New Crowdfunding | Decentralized Storage

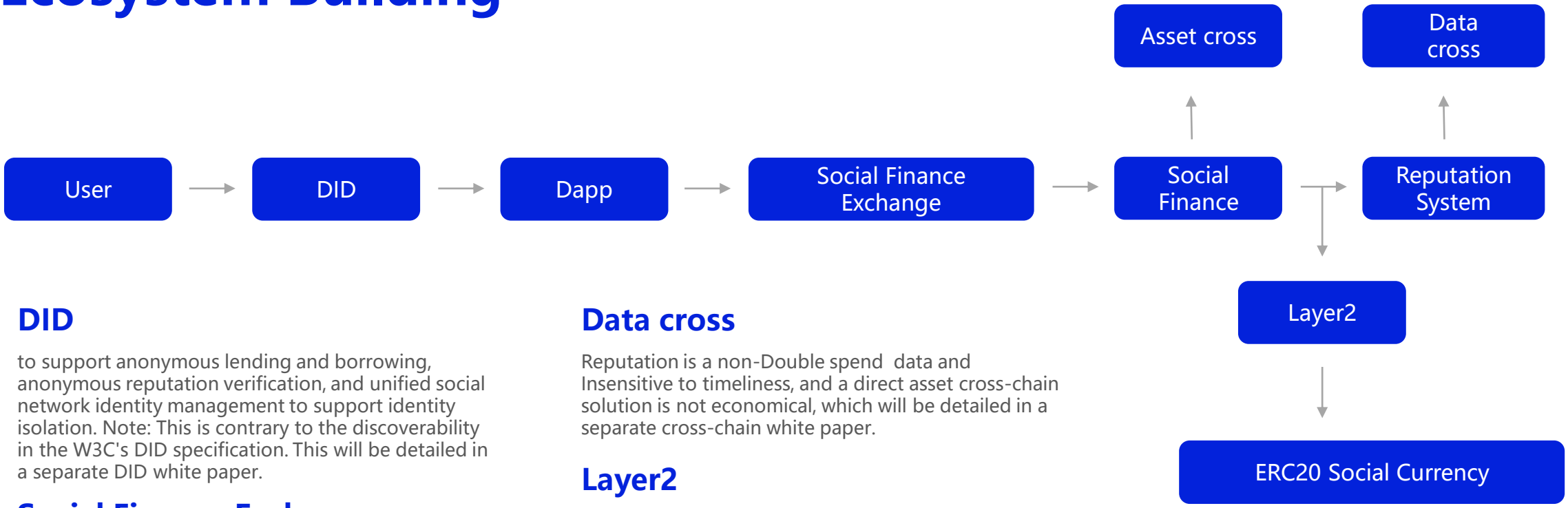
TIP: However, it is currently limited to payments to trusted institutions, and large-scale commercial use (e.g. in pay-per-month music applications, decentralized storage payments) needs to Solving collusion attack.

5 Future

Phased go-live

	Hall of Fame	Seed selection	Reputation System	Social Finance
Alpha	-	Operation team designation	Full	Full
Beta	Community Elections	Algorithm Selection	Full	Full
GA	Full	Full	Full	Full

Ecosystem Building



DID

to support anonymous lending and borrowing, anonymous reputation verification, and unified social network identity management to support identity isolation. Note: This is contrary to the discoverability in the W3C's DID specification. This will be detailed in a separate DID white paper.

Social Finance Exchange

The application can issue its own Token, which is exchanged for ZeroDAO's native currency and sent to the Social Currency of user directly through the social financial exchange when users withdraw.

Asset cross

Substrate already has a number of asset cross-chain solutions, so this is not the focus of ZeroDAO at this stage, and will leverage the ecosystem to enable asset cross-chain when the time is right.

Data cross

Reputation is a non-Double spend data and Insensitive to timeliness, and a direct asset cross-chain solution is not economical, which will be detailed in a separate cross-chain white paper.

Layer2

The resource consumption during the update period of reputation system is intensive, and the overall appearance is pulsating. The later ecology will adopt Layer2 solution to solve the temporal and spatial imbalance of resources, and at the same time can better support ERC20 social currency.

ERC20 Social Currency

Applications can also issue their own social tokens to synchronize system updates and distributions on Layer2.

Freedom Equality Customize