Meet Autonomous System Research

2019

Contents

1 Abstract

Blockchain industry is in rapid development, with constantly condensation of new consensuses. New technologies emerge, from the underlying level such as consensus mechanism, cryptography and smart contract etc. to the application level like traceability, credibility, games, etc. In the meanwhile, new idea of governance, business models and designs of token continuously appear. Integrating innovations in technology and model promotes the development of the industry and academia. It is believed that blockchain is developed to a certain extent by consensus of community, which tend to be a recognition of the technology, idea or organization structure. The development of blockchain is stimulated by innovation, which is usually able to create the largest scale of consensus as fast as possible. Furthermore, consensus formed across the innovation will leverage the power of capital to promote the further development of the whole blockchain. Despite that innovation also plays an important role in traditional industries, for most times it must be passed on to customers through products and user experience; there is a long process of transformation from innovation to the generation of profits that can maintain the enterprises survival and development, which makes many startups cautious in innovation. In contrast, in blockchain industry, the consensus of community, condensed by innovation, has endowed the team with strong power to generate considerable revenue to support continous innovation. By far, there is nearly no such an area that could turn intellectual ideas into revenue in such rapid pace.

Autonomous System Research (ASResearch) is committed to making solid academic research and promoting to the development of blockchain through innovation. As an emerging area, blockchain involves various fields and disciplines such as distributed systems, programming languages, virtual machines, cryptography and economics. With the introduction of cryptography and game theory, the consensus of blockchain system has withstood the test of time for over a decade, though some relevant mechanisms are not perfect yet. However, this interdisciplinarity makes innovation a difficult task in blockchain industry. Therefore, we believe that innovation through solid academic research is a significant and indispensable way for the development of blockchain. Relatively, putting innovations without strict validation into practice may cause huge losses to the project proponent and the community. Therefore, we believe that innovation with formalized curiosity is a significant and indispensable way for the development of blockchain industry.

ASResearch consists of a number of doctors and masters who has engaged in blockchain studies with solid research capabilities and knowledge in multiple related areas for a long time. Meanwhile, ASResearch actively cooperates with universities and research institutes for exploration of basic theories and deep understanding of all aspects of blockchain system. We believe that the deep understanding of blockchain is the basis of sustainable innovation, which is not only the foundation of ASResearch but also the significance of ASResearch for the blockchain.

2 Completed works

2.1 Underlying Technology of Blockchain

2.1.1 Blockchain Runtime Environment

Blockchain Runtime Environment (BRE) was proposed to solve the problem of upgrades of blockchain system. Currently, most of blockchain projects have to conduct soft fork or hard fork in the process of system upgrading, where the hard fork requires shutdown to maintain the whole blockchain system, which not only causes the losses of blockchain projects, but also hinders the wide use of blockchain in real production systems environment. It is hard to imagine that the system need to be temporarily shut down for upgrading if it was already fully deployed in a financial or industrial system.

The solution from BRE is to deploy the protocol code of the blockchain system on the blockchain in a certain data format. The client will continuously obtain the latest blockchain protocol code on the blockchain and update the local blockchain protocol code, and execute the latest code, so as to achieve the automatic upgrading of the blockchain system. More specifically, BRE adopt LLVM JIT to execute C++ code on the chain. On the basis of the automatic upgrade, BRE further solves the problem of concurrent execution of different versions of the code on the chain, and further improves the execution performance on the premise of ensuring correctness.

Meanwhile, the design of BRE effectively decentralizes the rights of “nodes” or “miners” in the blockchain system. In networks such as Bitcoin’s PoW consensus, miners are not only given “administrative” rights to mine blocks, but also often controls the upgrade direction of the system. When the community reach a consensus on a certain technical iteration, the consensus cannot be implemented effectively due to the willingness or efficiency of the miners, which results in obvious imbalance of rights in the governance of blockchain system and inhibits the long-term effective development of community ecology. The design of BRE provides an effective tool for the community to upgrade the system rapidly on the premise of reaching an effective consensus, and balances the power of users, developers and miners effectively in the ecosystem at the system level.

In addition to providing the ability to upgrade blockchain, BRE also provides the ability to distribute and update software through the blockchain system. That is, developers can develop softwares, relevant or irrelevant to the blockchain, then distribute and update it through BRE, which provides a wide imagination space for the use of blockchain system.

2.1.2 Account Rank

Account Rank (AR) is proposed to measure the importance of the blockchain addresses (i.e. users, accounts). Currently, most blockchain projects simply take staking as measurement. Such designs have certain defects: they have no abilities to resist Sybil Attack effectively, or compromises the liquidity of tokens.

After many studies and discussions, by considering various factors comprehensively, we finally designed the most suitable criterion for measuring the on-chain importance of users-Account Rank[1]. The core design includes the following aspects:

1. Median Account Stake: We take the Median Account Stake of users in a period as one of the core variables of AR: the value of Median Account Stake x means the users hold x value of native token for at least half of the period, which can prevent the same asset from being utilized by multiple accounts.

2. In-and-Out Degree: The directed loop in the transaction graph of users within a period is firstly removed, then the amount of assets transferred in and out are recorded respectively. After that a specific function is used to calculate the In-and-Out Degree. This degree can measure the user's activity and has the ability to against cheating: it can be proved that removing directed loops guarantees the upper limit of the In-and-Out Degree that users can increase through frequent transfers.

3. Wilbur Function: Wilbur Function f is one of the original functions, it has the following features: (a) $f(x+y) > f(x) + f(y)$, strictly resisting Sybil Attack; (b) $\lim_{x,y\to\infty} f(x+y) = f(x)+f(y)$, preventing the domination from big accounts. The Wilbur function is used in all the above indicators for the final calculation of the AR.

The AR is a fundemental algorithm for developing various onchain applications and it provides a powerful guarantee for discovering the true value of the blockchain world. Developer Incentive Protocol, Governance Token Issuance Protocol and other applications have been derived from AR. It is foreseeable that AR will be more widely used in various scenarios with the increasing user's demands for value on the chain.

2.1.3 Developer Incentive Protocol

Developer Incentive Protocol (DIP) is aimed to provide constant incentives for developers of outstanding Decentralized Application (DApp) on the blockchain.

We believe that developers' interests are not fairly distributed whether in decentralized application platforms or traditional centralized application platforms: currently the main revenue source for developers is user purchase and advertisement placement. Ad-free applications often bring good user experience and the platforms often relies on high-quality DApps to attracts users to make profit, but in such way, the Developer's interest on the DApps cannot be guaranteed. On the other hand, the profits generated by the platform is not directly distributed to the related developers. Based on above considerations, we believe that the it is benefitical for the platform to provides certain incentives for developers to attract high-quality applications continuously.

In the ecosystem of blockchain, as new-block rewards represent the incremental value of the blockchain ecosystem, the distribution of new-block rewards determines

[1] `https://github.com/ASResearch/nr-report.git`

the incentive direction of the decentralized system. Given this, the main function of DIP is to distribute part of new-block rewards to the DApp developers fairly and justly, promoting the symbiotic and prosperous development of users, block chain platform and developers.

The design of DIP mainly consists of two parts: Ranking the DApps and distributing rewards to the developers. In a certain period, we give a ranking score to each DApp based on the total times of invocations from users and those users' ARs. At last, each developer's deserved reward is calculated through DApps' ranking scores.

The advantages of DIP design are:

1. The introduction of users' ARs naturally prevents Sybil Attack, i.e. manipulation by creating a large number of accounts to invoke a DApp cannot increase benefits;
2. The so-called Quadratic Voting model is adopted to calculate the ranking score, i.e. users can contribute more to the actual ranking scores through calling different DApps, which essentially increases the costs of bribing users;
3. The calculation of the final rewards guarantees that the duplication and split of DApps cannot bring more rewards to its developer.

The DIP is the first application of the AR, which has been providing sustainable rewards and positive incentives to a large amount of developers. Please see the Mauve Paper of Developer Incentive Protocol for more details[2].

2.1.4 Consensus Algorithm

Consensus algorithm is the core to ensure the stability and security of a blockchain system. We are committed to designing and implementing innovative and superior consensus algorithms based on in-depth understanding and investigation of the current advanced and widely used consensus algorithms.

The design of consensus algorithm is a significant project. Current works include the following aspects:

Consensus Survey [3]

Consensus has always been an important concept in distributed systems, and the initiation of blockchain has created a stronger demand for consensus algorithms. There have been more than 5,000 references to the Bitcoin white paper so far, most of them are consensus-level results, not including the Byzantine Fault-Tolerance Problem (BFT) proposed by Lamport, a Turing Award winner, before the birth of Bitcoin.

We do a survey on a series of famous professional papers helpful to the design of new consensus, which are divided into the following categories: 1. Thinking on

[2] https://github.com/ASResearch/dip-report.git

[3] https://github.com/ASResearch/consensus-survey.git

traditional Proof of Work(PoW); 2. Research on the Byzantine Fault-Tolerance Problem(BFT); 3. Research on random-variable-based Proof of Stake; 4. Discussion on non-chained data structure.

This extensive survey on consensus algorithms provides an important reference and guidance for designing new consensus.

Guideline for Designing Consensus Algorithm [4]

This guideline further analyzes the goals and concerns during the design of new consensus, based on the consensus survey.

This guideline independently proposes to separate the two processes: proposing block and reach consensus, and establishes the system model respectively to implement the mechanism independently. The advantages and disadvantages of PoW protocol, PoS protocol, chain-link protocol and voting protocol are analyzed.

Thus guideline is a necessary work to design new consensus algorithm, providing theoretical guidance.

TLA+Formal Verification [5]

The so-called formal verification refers to the specification of consensus algorithm through TLA+ language, which is very important in the project field, especially for distributed systems. Making corresponding abstract description before system development can help developers better understand the system and effectively find potential problems which is hard to be found in tests.

Formal verification is equivalent to drawing the blueprint for building consensus algorithms. Among currently open source blockchain projects, only few of them have specific formal specification for consensus algorithm, such as Ethereum[6]. We believe that TLA+ formal verification provides a real security guarantee for the consensus algorithm.

In terms of the current results, our consensus algorithm: 1. Supporting permissionless environment for mining new blocks; 2. The agreement process has strong originality, maximizing the system's security and resisting variants of potential attacks; 3. Ensuring continuous and stable high TPS and low validation time.

2.2 Tokenomics Design

We believe that the development and prosperous of blockchain ecosystem cannot be separated from the participation of token holders in the whole blockchain ecosystem. To some extent, there is a lack of rules and tools for interaction between token holders and the entire ecosystem. Therefore, we start from the voting scenario in on-chain governance to improve the interaction between token holders and the ecosystem. One

[4] https://github.com/ASResearch/pod_guideline.git

[5] https://github.com/ASResearch/consensus_spec.git

[6] https://github.com/ethereum/eth2.0-specs

of the cases is the design of ”Governance Token Issuance Protocol” which is applied for onchain governance and voting.

Governance token issuance protocol is the protocol that distribute voting rights in the form of ”governance token” based on the AR algorithm.

- Design Motivation: In a onchain governance and voting scenario, we need to design a protocol that meet the requirements of distribute voting rights reasonably, anti-manipulation and improve on-chain voting participation rate. Therefore we design the voting token issuance protocol that could incentivize voting behaviors, resist Sybil Attack and the voting rights is distributed with the coin-age-weighted trading activity taken into consideration.
- Issuance
  1. The issuing mechanism is similar to that of Bitcoin, which takes ’week’ as the issuing period and the the halving period is about four years.
  2. It can be obtained through “mining” behaviors, such as improving the AR of addresses by on-chain transfer, participating on-chain voting, pledging the native token of the ecosystem, etc.
- Voting process: three basic voting principles, two stage voting rules and voting supervision framework are designed to increase the costs of manipulation and the difficulty of collusion in the system.
- Iterative updating of the parameters: the parameters of the issuance protocol is governed by the entire community and can be dynamically self-adjustment The adjustment and upgrading of parameters follow the “bootstrap” and “holographic” principles in the governance process. That is, i) a complete parameter upgrading process and tools are provided for token holders on the basis of setting initial parameter placeholders and ii) it is decided by the community voting according to market feedback and ecological development in different periods.
- The main advantages of this design are:
  1. Establishing a reasonable dual-token economic system in the ecological, where the local currency stimulates storage and preservation from users, as a “good currency”; the voting token, as a “bad currency”, has clear usage and circulation scenes and destruction rules, stimulating the circulation and use, depositing incremental value of local currency, increasing user activity.
  2. The amount of governance token through weekly airdrops is positively correlated with users’ ARs and the amount of native token pledged. It can effectively prevent Sybil Attacks while preventing the voting rights from being completely controlled by large accounts. At the same time, it encourages users to improve address activity or conduct pledge of native token. The protocol was applied on a public chain since May 2019, within the initial four weeks after issuance, the protocol involved over 25% of users in voting and pledged more than 15% of the native token in circulation.

3. Governance token used for voting will be refunded to users with a ratio larger than 1 (within certain limits), in order to encourage users to participate in the voting actively and simultaneously prevent the snowball effect.
4. The total number of governance token from weekly airdrops decays at a fixed rate. Based on this, we mathematically proved that the total amount of governance token will not exceed a certain upper limit, preventing the inflation. In addition, this design also contributes to the head effect, which means that users who join the ecosystem earlier can get more governance token.

Governance token issuance protocol plays a key role in promoting user participation and local currency value deposition, in the process of on-chain governance and community development.

2.3 Community Governance

We believe that blockchain projects, especially the public blockchain projects, are decentralized open source collaborative organization based on their own token and tokenomics. How to design the governance structure of decentralized collaboration organization and the governance rules of complex cooperative relations in collaboration is an important subject that every public blockchain project needs to solve.

We designed community governance structure and on-chain management tools for autonomous metanet according to the token raising and distribution structure to solve the problems that the centralized governance cannot cope with decentralized ecological development demands, the tragedy of the commons in traditional decentralized coordination, and the lack of effective iteration and upgrade tool, low incentives, low community participation in existing decentralized blockchain ecological. In the design of the governance system, we set up a complete governance structure with public onchain assets as the main governance object, onchain governance as the main governance method, working together with offchain organization structures and supervision mechanisms.

The design of the governance system mainly includes several aspects:

1. Basic rights claims, i.e. proposing three basic propositions, with onchain addresses as the basic unit: (a) Rights to own and operate onchain assets; (b) Right to propose proposals; (c) Rights to vote;

2. Offchain organization structure and supervision mechanism: three independently operating and mutually restricting organizations is founded: council, foundation and technical committee, which are responsible for expanding the scale advantage, efficiency advantage and productivity organization and guidance in ecology respectively;

3. Onchain cooperation and upgrading: the governance voting token and corresponding community cooperation platform, proposal process and voting rules, as well

as the upgrading process of corresponding rules and parameters are designed with the systematical feature of ”BRE”.

The advantages of this governance system are mainly reflected in:

1. System collaboration rules are holographic, and all roles in the system survive and develop under the uniform rules. At the same time, the rules for iteration are defined uniformly, providing a stable system foundation for the survival and development of multiple ecological roles, and promoting multiple benign games within the ecology effectively.

2. Collaborative processes are based on onchain tools and implemented in decentralized organizations, with assistance by the offchain community organizations and supervision mechanisms to enrich the dimensions and efficiency of decentralized cooperation.

3. With the cooperation rules of positive incentives, users in the community can obtain the original incentives distributed by the decentralized blockchain by improving the contribution degree to the economy and actively participating in the onchain governance, so as to benefit members of the community more justly and increase the participation of the community greatly.

3 Future Works

The future works of ASResearch will focus on research. On the whole, ASResearch believes that the blockchain system will be deployed and used on a large scale in terminal devices especially after the large scale adoption of 5G, significant development of artificial intelligence, chips and other related industries. ASResearch, therefore, will continue to explore the potential development in this direction, including but not limited to consensus algorithm for fast trade confirmations, efficient blockchain trading store system and secure smart contracts etc. Similarly, ASResearch will explore a more reasonable tokenomics design and the theory and practice of decentralized collaboration.

Currently ASResearch is forming a ResearchDAO on Ethereum to organize a group of academic professionals that is interested in research related to blockchain. The goal of ResearchDAO is to form a new type of academic organization that could engage top talents with an open, autonomous and self-evolving decentralized organization and let every individual researcher could work on their desired topic freely in a decentralized manner without relying on the administrative structure of any single academic organization. The ResearchDAO will support the collective academic intelligence in academic research and project incubation through its resources and network. All the fundings and benefits of the group will be managed by a multi-signed smart contract and distributed following the on-chain governance rules of the DAO.

ASResearch is willing to share our understanding with the whole industry and actively cooperate with the whole industry to explore new technologies and modes in practice and jointly promote the development of blockchain industry.