BSafe.network Layer 2 Technology Competition
Call for proposal and rules of competition

December 8, 2017
BSafe.network

1. Background of BSafe.network affiliated competition series and reasons for holding layer 2 competition

Nowadays, many cryptocurrency projects and blockchain based projects are becoming reality, and there are a large number of technologies and implementations. The development of theory and technology to make blockchains mature enough for actual applications is important if we are to provide a foundation for building upon, much like what happened with the Internet itself. Scaling Bitcoin and other academic conferences are the places to find the future progress of blockchain technology. In addition to such conferences, we need a place to provide scientific evidence to evaluate and compare blockchain technologies. This evidence is not limited to performance, but also security, privacy, game theory, economics, and regulation. BSafe.network is the neutral academic research test network by international universities with 24 universities currently participating. BSafe.network plans to hold a series of open technology competitions on many aspects of blockchain technologies. The aims of the open competition are:

- facilitating development and progress of theory,
- conducting technology verification over BSafe.network,
- providing review by university researchers/professors,
- providing the source of scientific/academic results, and
- publishing technically reviewed software.

Currently, "layer 2 technology for blockchain" is a category of technology to enhance blockchain based transactions by connecting the decentralized nature of blockchain and actual applications by segregating a huge number of transactions. There are also other

types of layer 2 technology to enhance privacy. Lightning network and TumbleBit are examples of Layer 2 technologies. Because layer 2 protocols provide different trust models than blockchains, there may be trade-offs among performance, security, privacy and so on. This competition aims to have deep and scientific knowledge of designing and evaluating layer 2 technology to facilitate further research and development of layer 2 technology.

2. Goals
The goals of this competition are
- Collecting attack models on layer 2 networks,
- building measurement of security and performance of layer 2 technology. and
- better understanding the trade-offs of using layer 2 technology.

This competition does not aim to select some technologies as standards or candidates of standards. It aims to provide public academia backed data and research results. Outcomes to the public are as follows.
- Program codes: cc-by license
    - Layer 2 technology software codes
    - Evaluation software codes/platform
- Evaluation data for each proposal
- Common evaluation dataset

As byproducts of this competition, we can provide public security testing theory and tools for Layer 2 technologies.

3. Categories of the competition
We conduct two categories of competitions as follows.
1) **Proposing layer 2 protocol and code**
   We call for layer 2 technology to enhance all or some of scalability, privacy and security, and their trade-offs.
2) **Proposing attacking/measurement tool for Layer 2 technology**
   We call for technology evaluation methodology and software for layer 2 technology. They include common datasets for evaluation. Please refer to section 4 for evaluation criteria to be considered.

4. Evaluation method
In this competition, we evaluate each proposal in two ways; theoretical evaluation and experimental evaluation. Theoretical evaluation is reviewing submitted technical documents by university researchers through a scientific review process. Experimental

evaluation is performing experiments for each submission using BSafe.network isolated research test network by installing submitted software and running each blockchain network for three months, with evaluation datasets. Experiments include not only performance evaluation but also security evaluation and attacks performed by university researchers.

5.Technical requirements and evaluation criteria
5.1. Technical requirements
The proposed layer two technologies in this competition should fulfill following technical requirements.

1) Reference application
   Payment
2) Correctness
   Double spending is not possible or theoretically difficult
3) Security
   The entire system composed of layer 1 and layer 2 has resistance against fault, denial of service of nodes and network connections, and attack to nodes and network.
4) Privacy
   The entire system composed of layer 1 and layer 2 assure unlinkability or fungibility of payment transaction
5) Fundamental layer 1 technology
   Bitcoin with segregated witness

5.2. Evaluation criteria
Supposed evaluation criteria are as follows.

1. Performance
   a. Number of transactions/sec
   b. Network latency
2. Security/Trust
   a. Resistance to fault/crash/attack to nodes
   b. Degree of decentralization
   c. Resistance to DoS attack to make layer 2 transactions fail
   d. Scenario and data set to evaluate
   e. Availability of layer 2 nodes
3. Privacy/Fungibility
   a. Correlation among transactions
   b. Unlinkability among transactions
   c. Unlinkability to identity

6. Schedule

Call for submission start: December 8, 2017

Submission of expression of interest: 23:59 UTC April 6

Full submission deadline: A several weeks after April 6

Evaluation and experimentation start: May, 2018

Disclosure of a list of proposals: May, 2018

Evaluation and experimentation end: July, 2018

Announcement of a winner and excellent proposals: August, 2018

Technical presentation and awarding ceremony: September, 2018

7. Submission procedure

Anyone can submit a proposal to this competition, but need to meet the following procedure and submission requirements.

Each submitter must submit the following.

1. Cover sheet
    a. Category of submission (Layer 2 technology or evaluation)
    b. Name of submitter(s) with the corresponding submitter
    c. Email address
    d. Name of technology
2. Technical documents
    a. Design rationale
    b. Algorithm specification and supporting documents
    c. Self-evaluation documents in security and efficiency
    d. Intellectual property disclosure
3. Software code
    a. Any programming language is acceptable
    b. Installation documentation is needed.
    c. Providing installation package is recommended.

All submitters need to carefully submit the program code to avoid security vulnerabilities and bugs. Before running software over BSafe.network, we will conduct the security analysis and source code check. If we found any major problem in the code, the proposal is not considered for the competition. If the evaluating committee judges that the technical documents do not contain enough information and data for theoretical evaluation, the proposal is not considered for the competition. Note that no code changes are allowed after submission.

8. B-Prize

We are planning to award a winner and excellent proposals "B-Prize" with certain amount of money. Details will be announced when it is decided.

9. Note on business neutrality

The layer 2 technology competition focuses on providing technical knowledge to help further research and development. The result does not endorse anything about other aspects including soundness of business, exchange rates of cryptocurrencies and tokens. To preserve business neutrality, we do not evaluate any proposal with existing/upcoming plans of ICO or selling tokens.

10. Evaluation committee (alphabetical order)

Chen Feng, University of British Columbia
Joaquin Garcia-Alfaro, Telecom Sud Paris
Ethan Heilman, Boston University
Jordi Herrera Joancomartí, Universitat Autònoma de Barcelona
Jameson Lopp, BitGo
Jeremy Rubin, Bitcoin Core Contributor
Rusty Russell, Blockstream
Shigeya Suzuki, Keio University

Other committee members will be added after confirmation.

11. Contact and submission

E-mail: layer2.competition@bsafe.network
Website: http://bsafe.network

Revision history

- December 8, 2017: Initial version
- January 31, 2018: Add note on business neutrality
- March 20, 2018: Add evaluating committee member
- March 29, 2018: Add process of expression of proposal

About BSafe.network

BSafe.network is an international and neutral research test network for blockchain technology. It plays a similar role as what NSFNET and BSD did for the development of the internet technology, for blockchain technology. The network consists of international universities to preserve neutrality, and as of December 8, 24 universities from North America, Europe, Asia and Africa are a part of BSafe.network.