BSafe.network

The Research Network for Blockchain Technology

White Paper

January 1, 2017

1. Summary

The BSafe.network is a neutral and open research network for Bitcoin, blockchain and distributed ledger technologies established by academic researchers. This network's short-term aim is to identify and engage academic interest in the emerging Bitcoin and blockchain technology space. By bringing academic rigor and excellence, it enables telemetry and a scientific approach to long-term innovation and engenders societal trust in these new digital public platform technologies. The project aims to mimic the same degree of impact that BSD (Berkeley Software Distribution) and the NSFNET (The National Science Foundation Network) had on the evolution of the Internet. The former provided robust, liberally licensed software that put into practice the many theoretical advances made by academia. The latter scaled expertise, experience and resources.

Each individual, or a group of researcher(s), conducts academic research over the BSafe.network on their protocol of interest (initially the Bitcoin, Ethereum and Hyperledger Protocols). By operating research nodes on these protocols the BSafe.network establishes additional neutral, stable and sustainable blockchain nodes that contribute to the better understanding of the properties of public blockchain networks such as Bitcoin and Ethereum. It also becomes a common academic platform on which to conduct coordinated international joint research projects. The BSafe.network provides a neutral platform that produces fair and reliable competitions of blockchain-related technology and applications using a technological layered approach the same as with Internet technology.

Research results on the BSafe.network can be deployed as software code, academic papers, technical papers, experimental analysis of results and guidelines. These results help to drive more applied innovation and real-world safe use of blockchain technology with the contribution by academia.

2. Background

After the invention of Bitcoin[1], the Bitcoin protocol, many crypto-currencies, blockchain and distributed ledger technology and applications were developed. "Bitcoin" and "blockchain" are recognized as the foundation of future transactions and a new digital ecosystems. Hence, a large number of startup companies and experimental projects have emerged in this space.

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"

Bitcoin and blockchain technology are thought to have the similar potential transformative impact to society as the Internet. However, development of commercial applications appears faster than the development of the Internet during the equivalent period of development.

If one compares the history of blockchain technology to the development of the Internet, technology is developed and deployed through the following 5 steps; (1) academic research by universities, (2) development and deployment by companies, (3) standardization, (4) commercialization and monetization by companies (5) new requirements for research.

These are natural, iterative steps to deploy stable and mature technology to the public. This is the reason why the Internet became a foundation of our business and life, though current blockchains are not mature enough and comparable to the Internet's development in its early stage in 1990's. For example, NSFNET (The National Science Foundation Network) and BSD (Berkeley Software Distribution) served important roles to make the Internet technology mature enough for commercialization. However, in the case of the Bitcoin Protocol, much investment was injected into the business community and startup companies, hence, these companies started their business with unmeasured technology. In the past development process, there are no standardization activities and too weak a link between Bitcoin developers and academic universities which can provide deep insight and careful verification of the technology.

Bitcoin and blockchain currently collect much media attention under the keyword of "Fintech". This indicates that many persons are only vaguely aware of the meaning and impact of these technologies. However, to make these technologies stable and sustainable, we need careful study by scientist, economist, sociologist etc. Thus, we should connect academia to the protocol development community. That is, we need to actively include the blockchain ecosystem with academia. This does not mean that the current technology is unsound. It means the ecosystem with academia and standardization is a stronger foundation of future innovation by Bitcoin and blockchain.

As a result, at this time we need to connect academia to blockchain technology to make these technology more reliable and sustainable toward long-term innovation.

3. Goal of BSafe.network

3.1. Goal

The goal of the BSafe.network is to construct a neutral, stable and sustainable research network for blockchain technology. This network is used for academic

research, not only technology research but also interdisciplinary social and economic research. BSafe.network aims to become an academic foundation of Bitcoin and blockchain and an academic safety net for these technologies like the NSFNET for the Internet technology and aims to provide the same degree of impact as BSD (Berkeley Software Distribution).

To realize a sustainable and decentralized blockchain network, large numbers of stable and neutral nodes are needed. The BSafe.network aims to help build this network by using the neutral role of a academia like university. BSafe.network aims to have a criticial mass of nodes as a proportion of the current number of Bitcoin nodes.

BSafe.network aims to connect academia and real-life development, and to be a testbed and trust anchor for any research and real-life technology and application. For example, Bitcoin and other blockchain technology such as Ethereum can be linked to BSafe.network. The research results can be used for the future development of reliable technology, applications, technology and operational guidelines to which society can refer for the safe use of Bitcoin and blockchain technology.

3.2. Benefits

Benefits from BSafe.network are as follows.

- We can have a reliable and neutral blockchain network for academic research with large number of nodes.
- Researchers conduct any blockchain related research
  - Blockchain technology
  - Application
  - Economic aspects
  - Social and Political aspects
- Researchers conduct international joint research over the BSafe.network
- We can easily provide the research results to public
  - Technology
  - Codes
  - Experimental results
  - Technical and operational guideline

3.3. Who can join

Universities and individual researchers can join the BSafe.network. Each participant must eventually operate a node of the BSafe.network in their protocol of research interest. Because neutrality is critical value of the BSafe.network, private companies can join research over BSafe.network

through university. There are ideally minimum three nodes per a country to realize uniform distribution of the nodes.

4. Technical overview

On the BSafe.network, each academic organization sets up a blockchain node. All nodes communicate with other nodes in a Peer-to-Peer (P2P) network manner. Each node is a fully operational blockchain node, and participants may add non-full node (like SPV-node) for their research purposes.

Existing Bitcoin and many blockchain networks are realized by software with all related functionality tightly integrated together; including P2P network, consensus algorithm, forming blockchain, reward mechanism, and business logic. Considering the aims of BSafe.network, any researcher can conduct research on any related technology issues to blockchain. In the BSafe.network, these technical issues are considered with technology structures. By allocating these technology structures, research works can be done independent from other technology areas. This is same as the Internet technology and same idea which helped huge number of innovation of the Internet. A participant may develop any new technology and software code for each technology area. The supposed structure of technology area, but not limited to, is

(1) Network: Broadcasting transaction and blocks,
(2) Consensus: The agreement-reaching engine,
(3) Storage: Bootstrapping new nodes, storing archival data,
(4) Access control: Manage access rights of the storage data,
(5) Application: Transaction graph, scripting language semantics,
(6) View: Cached summary of the transaction log, and
(7) Side-plane: Off chain contracts.

The softwares operated at each node are shared by using common repository which can be accessed by all participants.

5. Steps of construction

BSafe.network is initiated and constructed through following four steps.

(1) Build a fundamental blockchain network

At the first step, BSafe.network delivers reference software as a fundamental blockchain network. In 2016, as a bootstrapping phase and proof of concept, BSafe.network conducts following research.

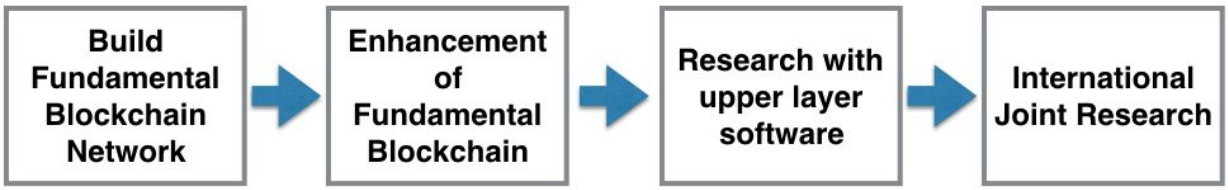

Fig. 1. Steps of construction

- Security evaluation of Bitcoin with Segregated Witness (SegWit)
- Add Ethereum and Hyperledger as targets of evaluation

(2) Enhancement of software of fundamental blockchain technology

In this step, enhancement of the fundamental software is conducted. This includes designing the specification of the layer (1) and technical structure of the upper layers. This step is needed to make layer-specific research. Software development guides and reference implementations are delivered to members.

(3) Research by using application software

In this step, members develop software for their research and do research by using the software. The software is registered into the BSafe.network repository and the status of research is managed (not controlled) by a committee of BSafe.network from operational and security reasons.

(4) Organizing international joint research

In this step, international joint research projects by using software developed by using BSafe.network are organized.

6. Organization

6.1. Organization overview

Bootstrapping

In 2016, BSafe.network is at the bootstrap phase. Small number of universities conduct proof of concept research. We aim to include 30 universities by the end of 2016.

After 2017

From 2017, BSafe.network aims to extend its scope and network wider by setting up a more formal organization. The organization and IP (Intellectual Property) policy will be discussed before proceeding to the next phase.

6.2. Membership

Membership of BSafe.network is managed by a secretariat. The participation by a academic researcher requires no fees. Each member should follow the bylaw and related operational rules.

6.3. Organization management

BSafe.network appoints Chair(s) to lead its activities. Secretariat(s) support the Chairs.

BSafe.network will have organization for planning, financial management, research management, deployment, liaison to related organization and public relation. The details are to be discussed.

6.4. Software management

Any participant may develop software for BSafe.network and using over it. All softwares related to BSafe.network are registered software repository inside the Safe.network. It may be published with approval by deployment committee. Fundamental software code for layer (1) is initially provided to all participants.

6.5. Research and discussion platform

BSafe.network sets online discussion platform for research and software development. This is basically accessible only by the participants.

6.6. Research management

Research activities on the BSafe.network are managed (not controlled) by the committee. That is, all research projects are registered and checked if software and protocol of the research project are correctly operated without software flaws and security incidents.

6.7. Research result deployment

Intellectual properties of research results, including software code, experimental data, academic papers, technical reports and patents belong to related researchers of each project. They can decide the intellectual policy of their results. Sponsor of BSafe.network may use the intellectual property. The research results may be published, when the related researchers and deployment committee agree, with referring BSafe.network.

7. How to join

To become a research node, the neutral academic researcher should read and agree the bylaw, then send the application form to the secretariat.

Contact information:
Web site: http://BSafe.network
E-mail: info@bsafe.network

8. List of current participants

North and South America

- Massachusetts Institute of Technology, Media Lab, USA
- Boston University, USA

Asia

- The University of Tokyo, Japan
- Keio University, Japan
- Toho University, Japan
- Ritsumeikan University, Japan
- SIM University, Singapore

Europe

- Newcastle University, UK
- ETH Zurich, Switzerland
- University of Nicosia, Cyprus
- Universitat Autonoma de Barcelona, Spain

9. Conclusion

BSafe.network is a neutral, stable and sustainable research network by universities. It can be used for academic research related to any layer in the blockchain technology stack and its applications. It is like “NSF-NET” of the Internet technology and it encourages technology enhancements, competitions and innovations with fine-grained layers of blockchain technology. It also becomes a platform of global scale joint research and experiments.