BSafe.network

Building Neutral Bitcoin/Blockchain Research Network by Academia

Shin’ichiro Matsuo

Workshop on Privacy, Security, Trust & Blockchain Technologies

Traditional sense of maturity and innovation

Refinement by iteration

Experimental | **Technically Confirmed** | **Commercialization** | **New Applications/ Ecosystem**

Maturing stability

Examples of technology issue: Is blockchain really secure?

Who does verify/certify/prove the security of Blockchain?

Variety of expertise can do.

Formal security definitions and fine-grained technical requirements?

We do not have them for entire blockchain technology.

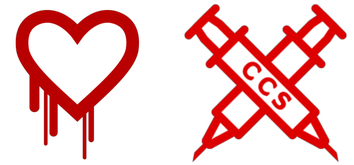
Trust-less by Cryptography

Not rely only on cryptography. By other background, e.g. security economics, as well.

The case of SSL/TLS: without precision engineering

Many attacks/vulnerabilities are found from 2011.

Heartbleed, Poodle, FREAK, DROWN, CCS Injection



Problems

No security proof

No procedure for verification of technology.

No experts on the verification of cryptographic protocols

Insufficient quality assurance of program code

The case of “the DAO”

Had a chance to lose 50M Dollars by this attack.

Caused by vulnerability of the code

The way of workaround is still not decided.

Problems

Vulnerability handling

Procedure for work around

Over-investment to uncertified technology and codes

Issues in the current blockchain

Cryptography and Cryptographic Operation

Secure System Design and Operation

Trade-off between Performance/Scalability and “De-centralization”

Finality and Immutability

+ Need healthy community and ecosystem by designing better incentive/economic model

Security economics/ game theory/ incentives

The Security of Bitcoin/ Cryptocurrency/Public Blockchain relies not only on technology but also on incentive design.

Some flaws in the current design of Bitcoin ecosystem are the cause of debates and chaos.

Games in blockchain ecosystem

NSFNet for “the Internet”

ARPANET

CSNet

Research Networks (NSFNET)
Non-Profit

Externalizing Costs
Commercial ISPs
Making $$$

1969

1981

1985

CIX Association
1991

April 30th 1995

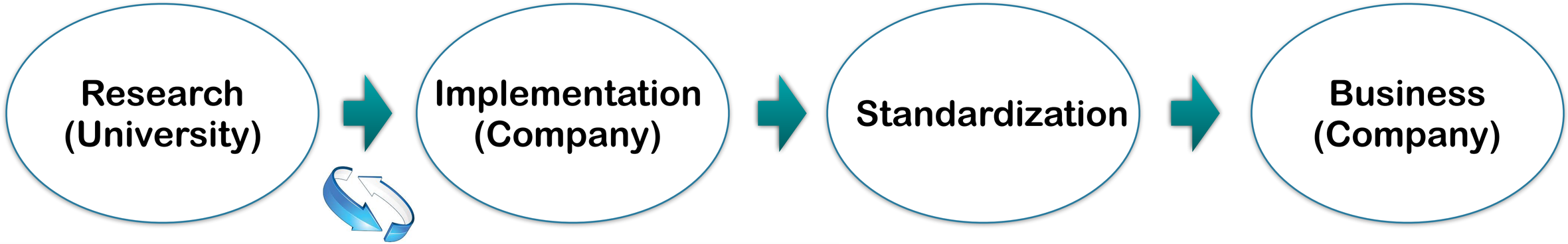
1977 — 1995

Berkeley Software Distribution (BSD)

NSFNET T3 Network 1992

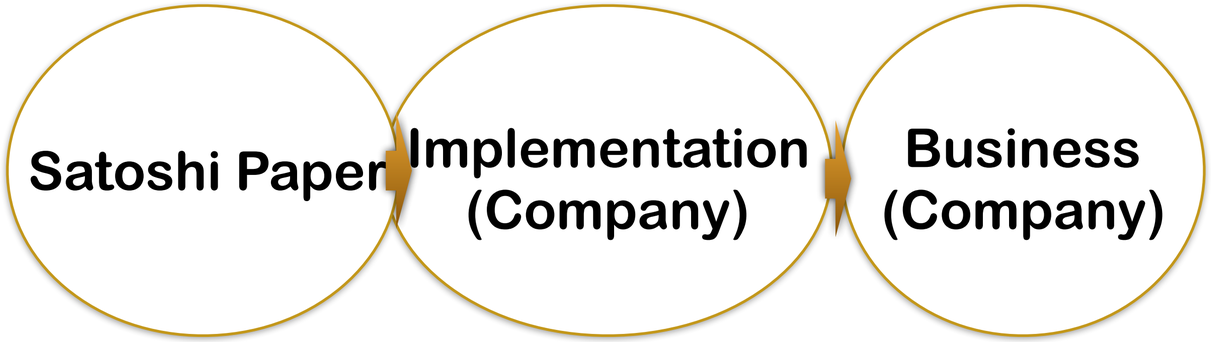
Academic Research is still needed

The Case of Internet Technology

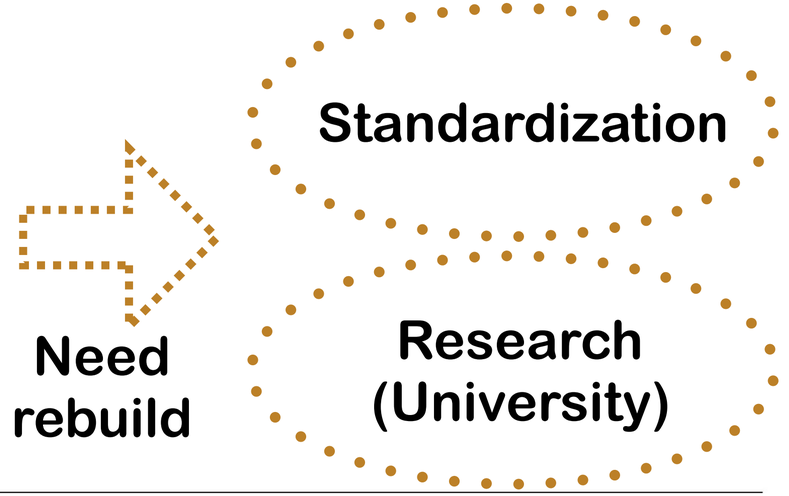


"BSD" and open-source facilitated innovation

The Case of Bitcoin and Blockchain

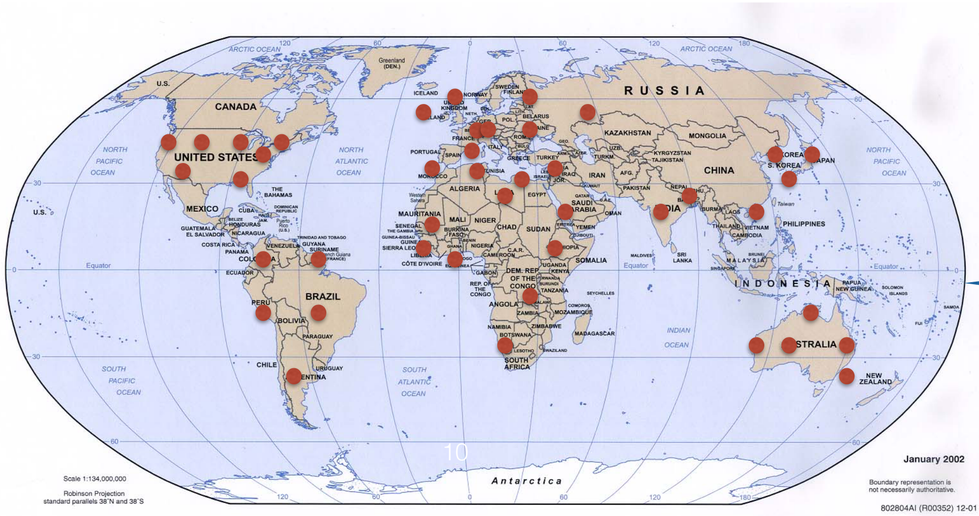


Innovation by iteration



BSafe.network: Plays the Same Role as NSFNet and BSD

- A neutral, stable and sustainable research test network for Blockchain technology by international universities.
- Founded by me and Pindar Wong in March 2016. Each university becomes a blockchain node.
- Research on Blockchain and its applications
  - Not limited to Security. All aspects will be researched.



- Neutral platform
- de-anchored trust of Blockchain network
- More nodes (with Neutrality)
- Testbed for academic research

Why is university the good place?

The place for experimentation

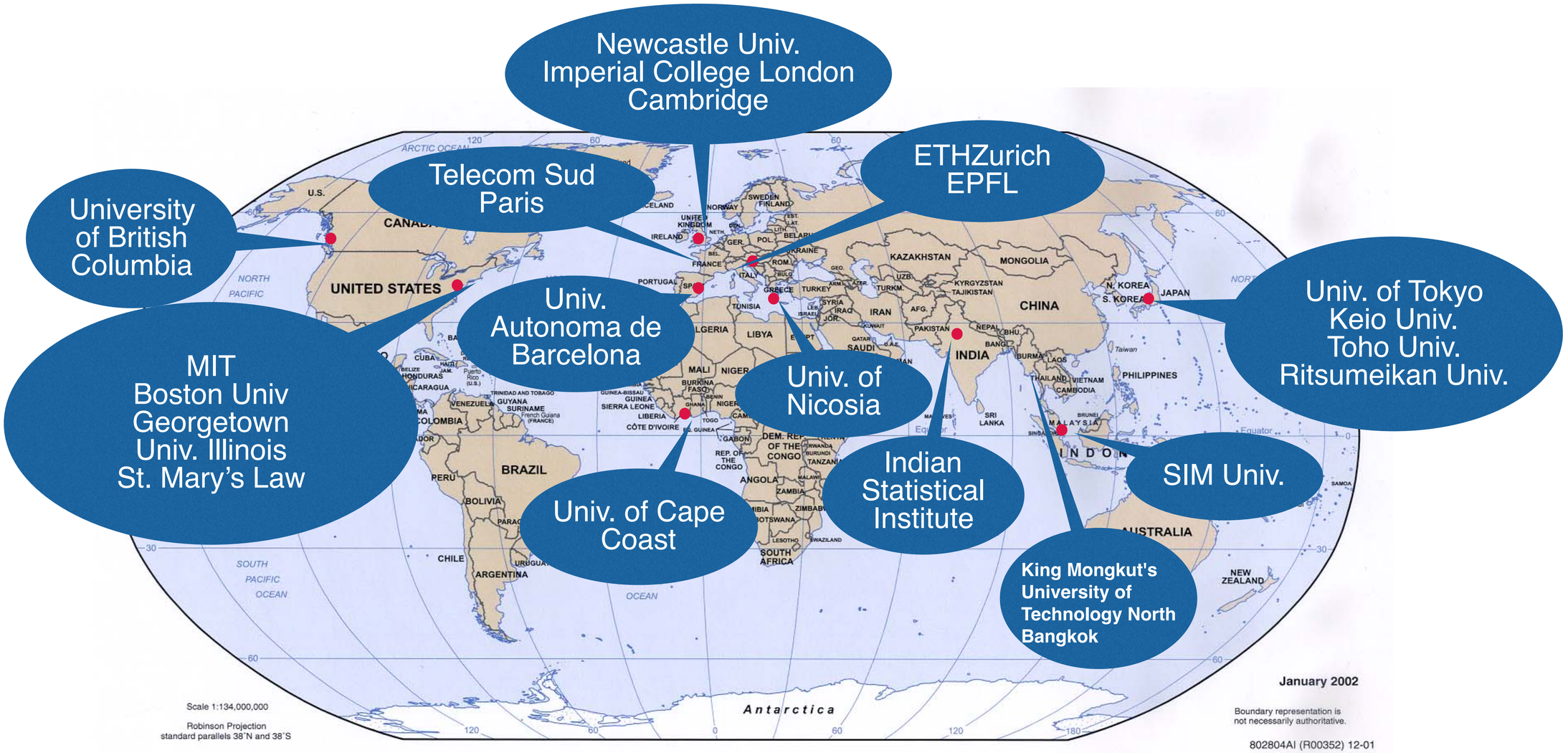
The place of neutrality

The place of diversity

The place of international collaboration

The number of university: > 15K, scalable!

22 International Universities Already Join and We Add More…



Main activities

International joint research over actual research network

Experiments of theoretical research results

Evaluation of the technology

Rubber stamp before testnet

The place of competition: be a basis for future innovation

Example of Research project: Security Economics in Blockchain

Finding better setting of Game and Incentives toward healthy ecosystem

<u>Topics</u>
Gathering much data as possible around August 1st and after

Analyzing human activities

Designing games toward healthier game setting

Example of Research project: Sensor network and Blockchain

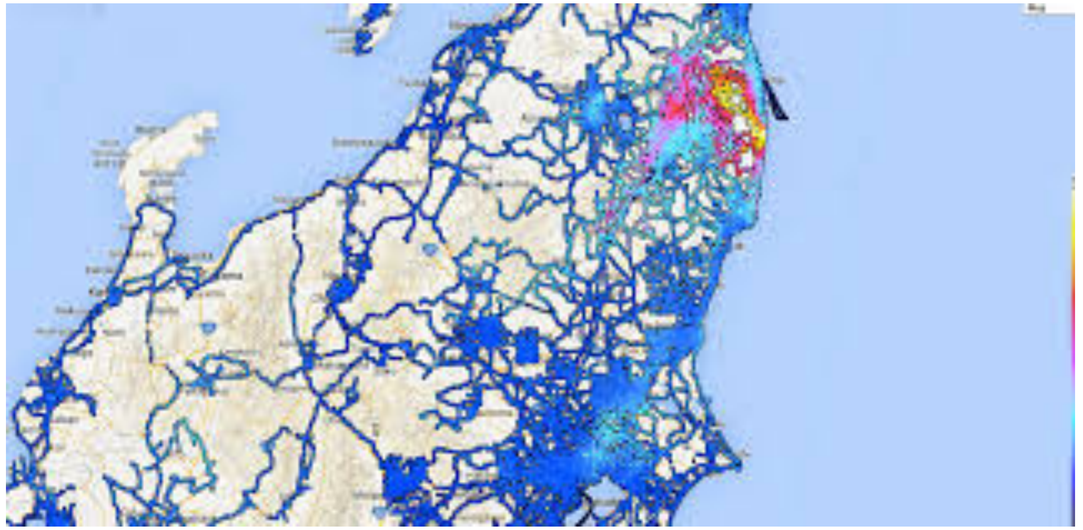
Collaboration with Safecast: citizen science project

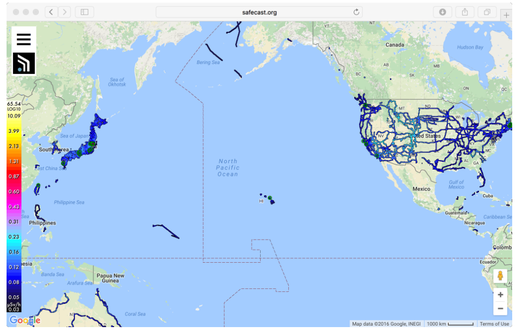
SAFECAST

Radiation data from global scale sensor network

Give provenance to the radiation data with its time and location

Share the data over blockchain to facilitate making new ecosystem





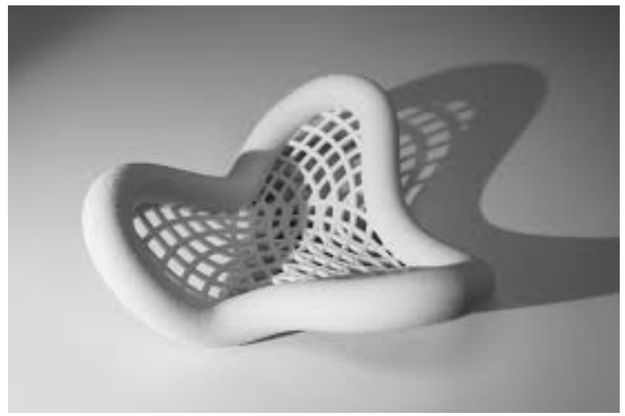
Example of Research project: Facilitate digital fabrication

Manage code and products for digital fabrication

Attach a RFID tag to products

Facilitate to both trace and trading of products using bitcoin and blockchain

Provenance, trading and payment



Education over BSafe.network

Two goals

1. “sand-box” for future top-level core developers and researchers
through research projects over BSafe.network

2. Education for undergrads to expand potential engineers of blockchain technology

Blockchain Education Network (BEN)
Grassroots Blockchain Education.
For students, by students.

Local First
Janitors, not Managers
Swarm Do-Acracy

Activities in 2016 and 2017

2016

Bootstrapping phase

The first “SEED Node(*)” at Keio University, Japan

Add universities from Asia, Europe and United States

First project: Attacking Bitcoin+Segregated Witness

2017

More universities

External funding

Firm organization

More research projects

Collaboration with Developer community

Collaboration among Bitcoin developers and academia through BSafe.network

Bitcoin developer community

Bitcoin software

BIP
(Bitcoin Improvement Proposal)

Experiments
Competition

Research Results

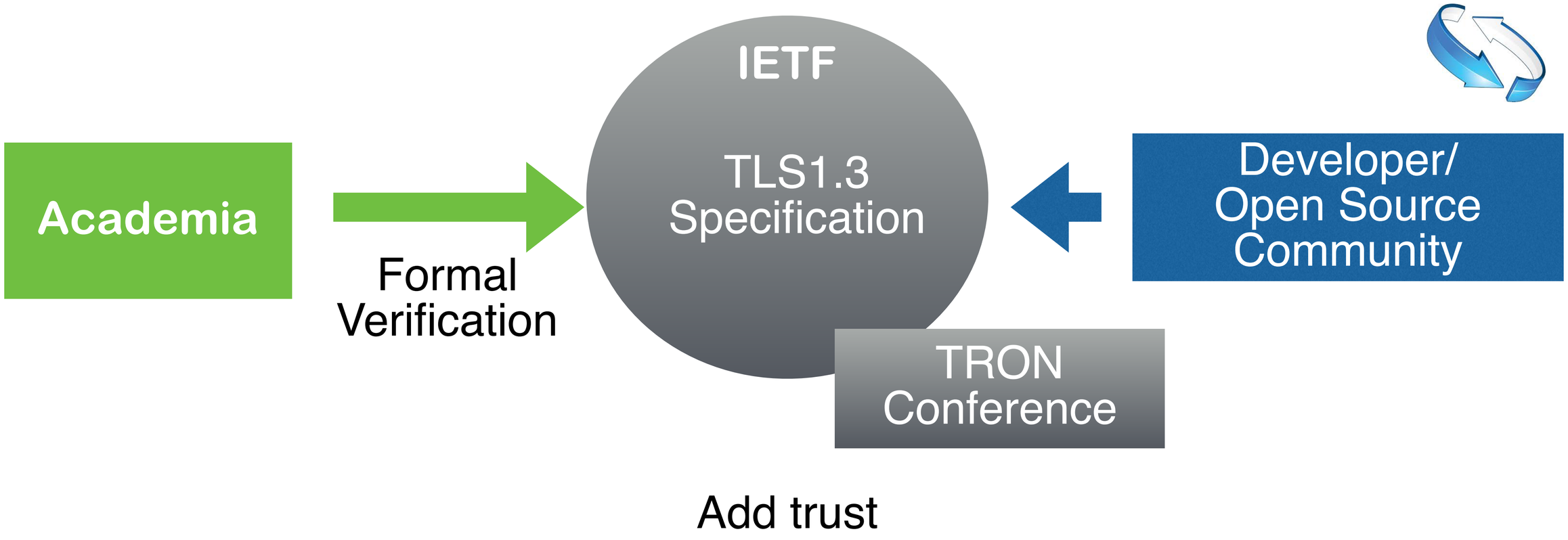
BSafe.network

Academia

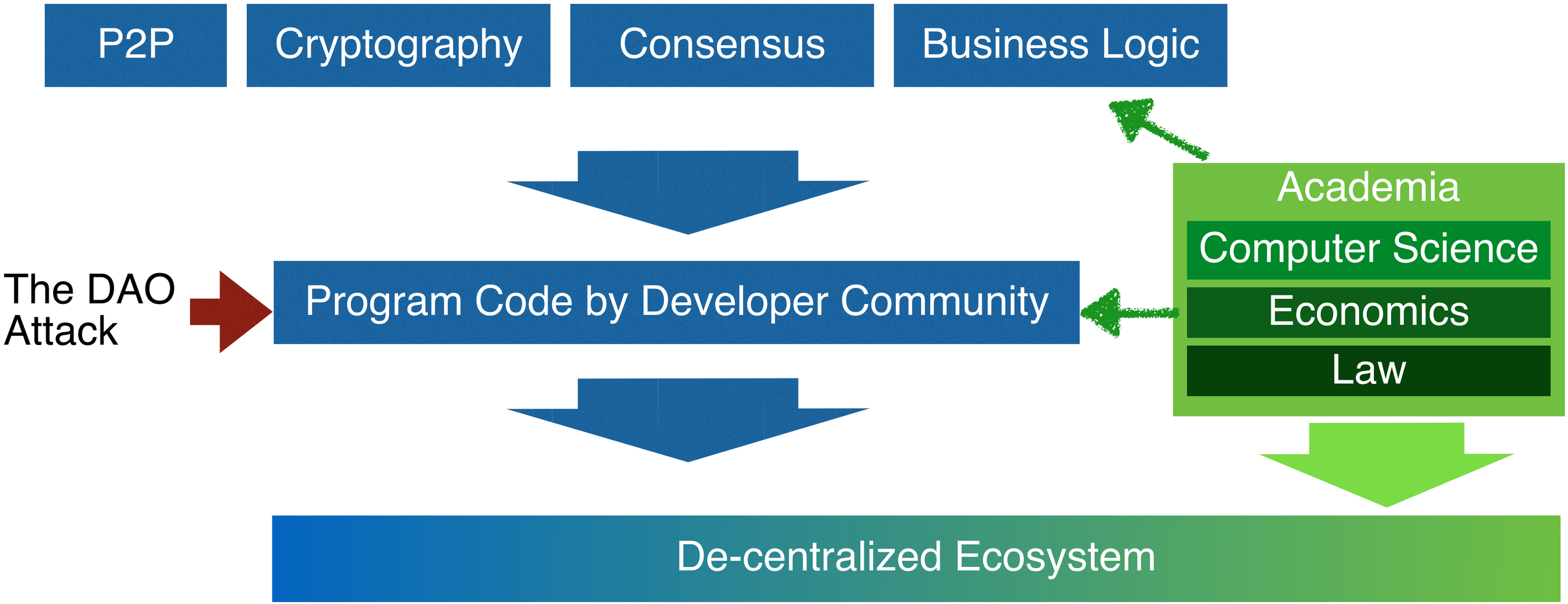
Research

BRR
(Bitcoin Research Request)

Practice from the development of TLS1.3

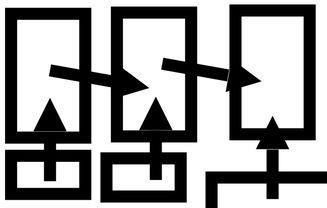


Decentralization by Diversity



Blockchain Research Network and Decentralized Academic Platform

Decentralized Academic Platform



Papers

Patents

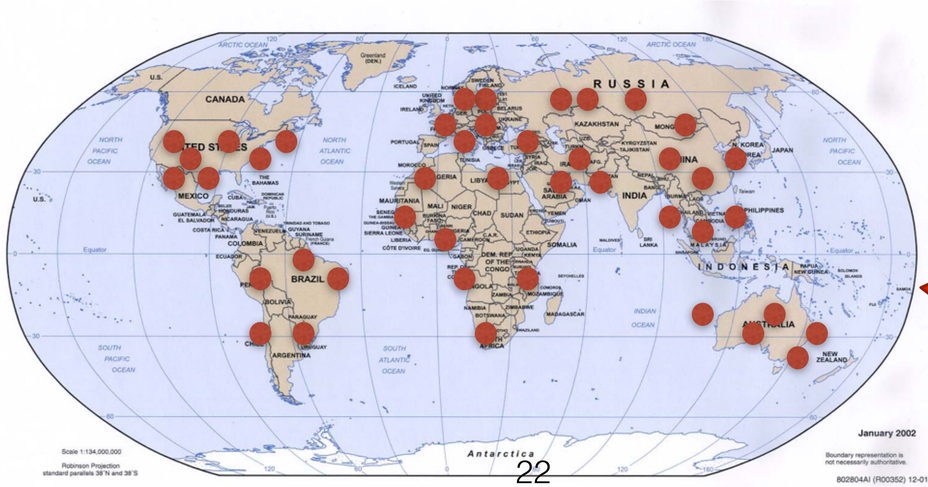
Research Funding
Reward to discussion

Discussions

- Decentralized Reviewing and open collaboration
- Prevent research misconduct
- Incentive to build the research network

Manage research fundings, papers, discussions, evaluations and patents over blockchain

University-level Blockchain Research Network



- Neutral Platform
- Trust Anchor of Bitcoin network
- Expand # of nodes from 6941 to # of univ. (with Neutrality)
- Testbed for academic research

Academia is the essential part of diversity, and it makes bitcoin/blockchain ecosystem healthy.