How Global Scale Academic Research Network helps Crypto-Economics Research

Eric Burger, Feng Chen, Joaquin Garcia-Alfaro,
Shin’ichiro Matsuo, Shigeya Suzuki and Pindar Wong

Crypto Economics Security Conference

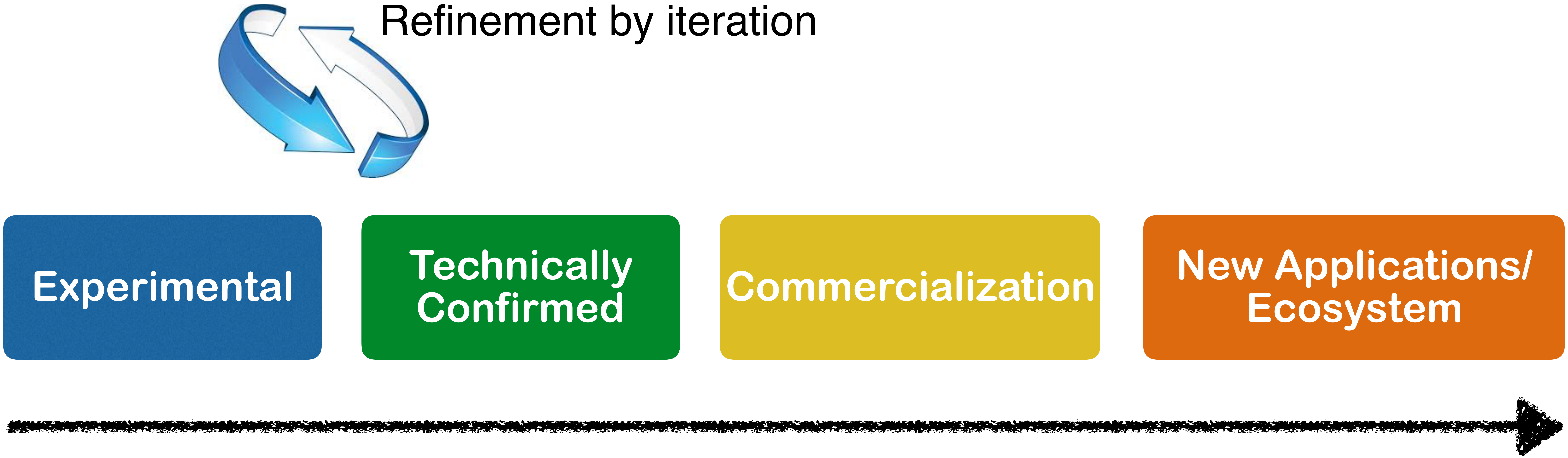
GEORGETOWN UNIVERSITY

BSafe network

Outline of this talk

1. Overview of the international research test network : BSafe.network
2. Ongoing monitoring on cryptocurrency behavior

Traditional way to development of technology



Refinement by iteration

Experimental

Technically Confirmed

Commercialization

New Applications/ Ecosystem

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/game theory, as well.

The case of SSL/TLS

Many attacks/vulnerabilities are found during this 5 years.

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 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

Technology Issues of Current Blockchain

Cryptography and Cryptographic Operation

Secure System Design and Operation

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

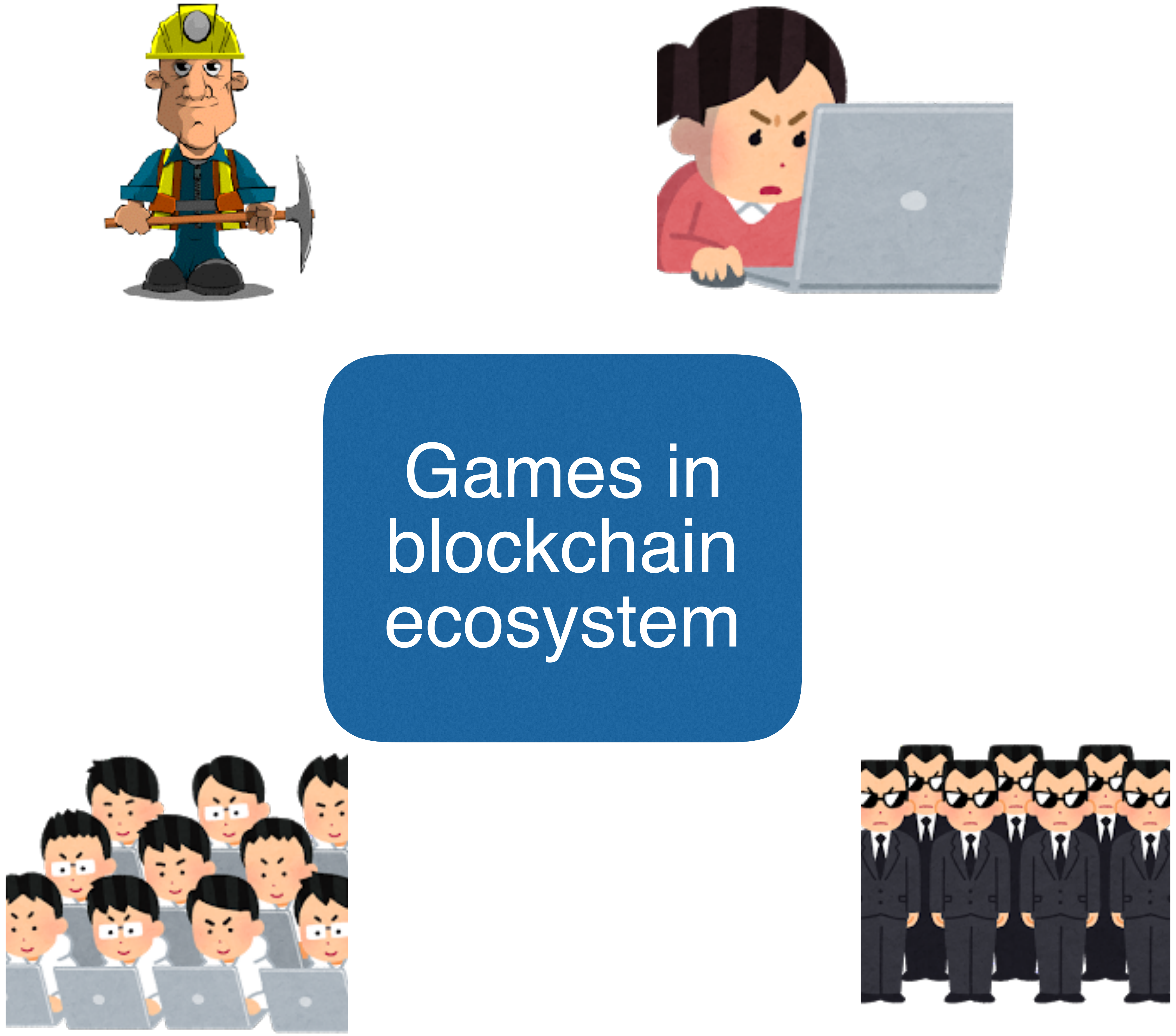
Finality and Immutability

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

Security economics/ game theory/ incentives

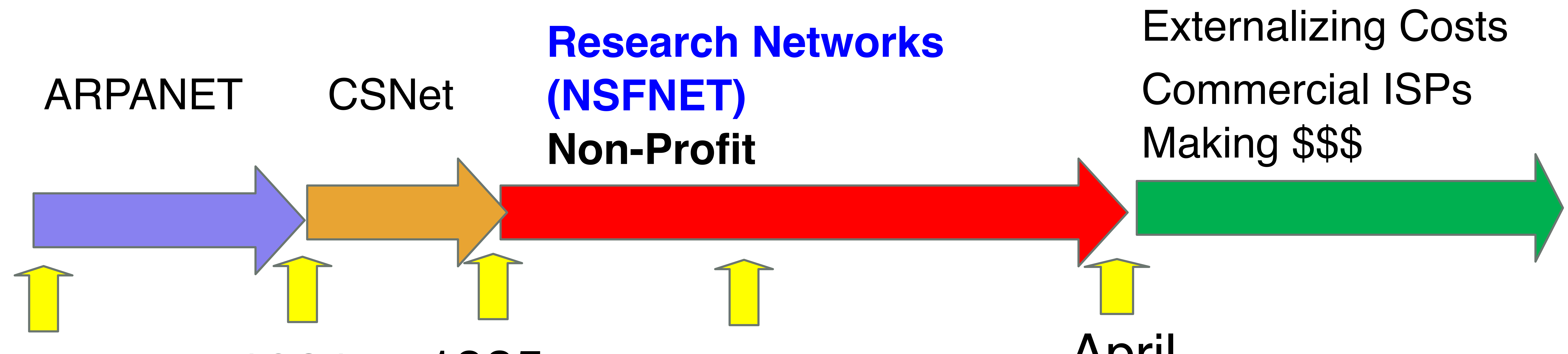
The Security of Bitcoin/ Cryptocurrency/Public Blockchain relies not only on technology but also on incentive design.

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

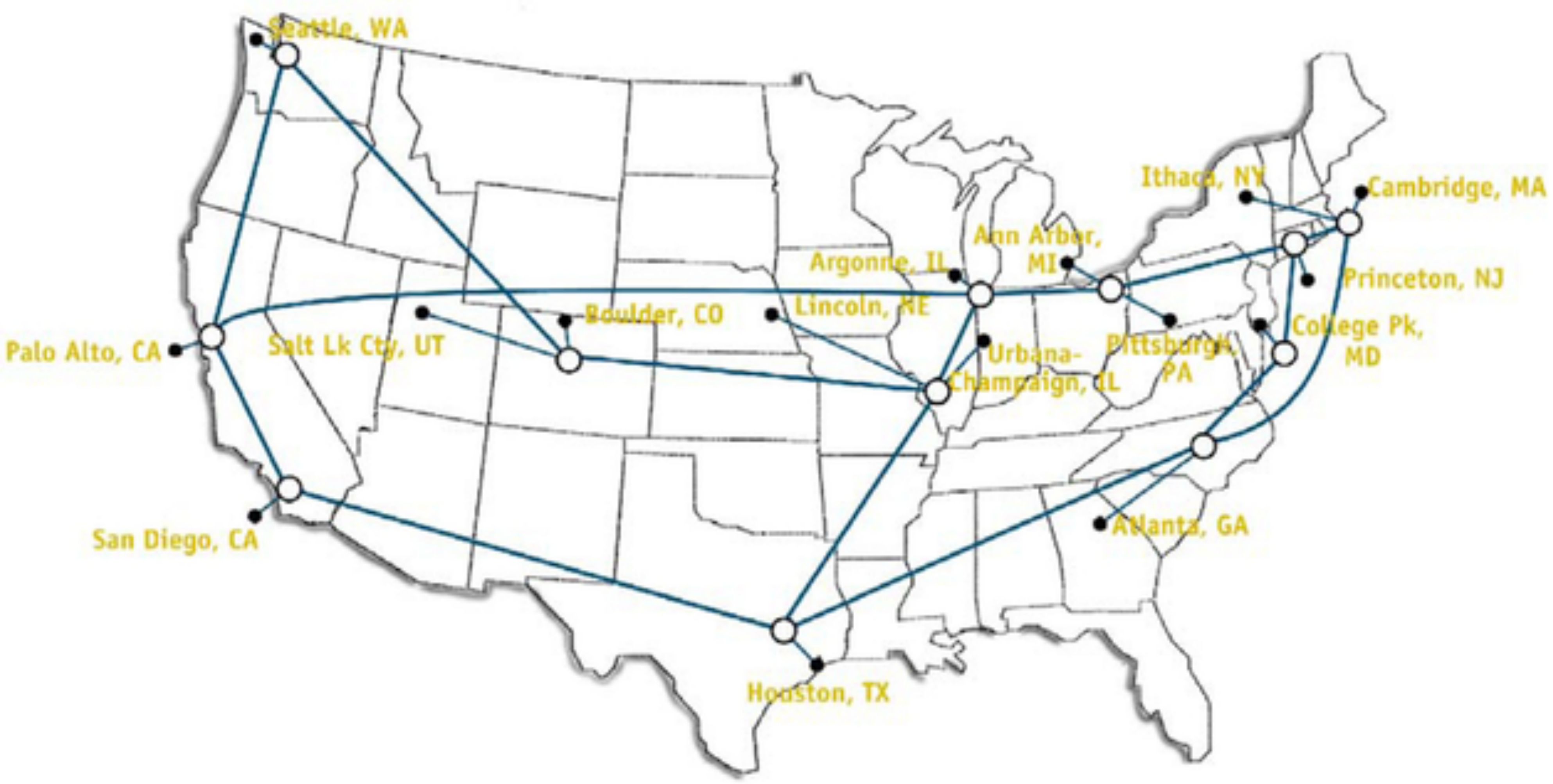
April 30th 1995

1977

1995

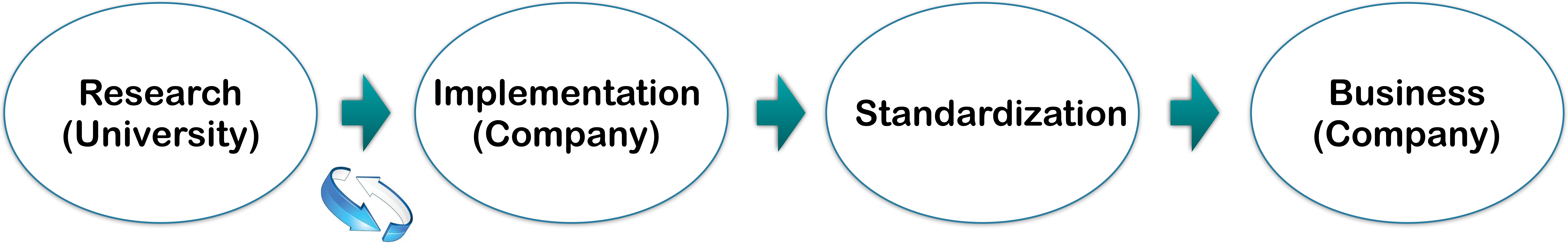
Berkeley Software Distribution (BSD)

NSFNET T3 Network 1992



Academic Research is still needed

The Case of Internet Technology



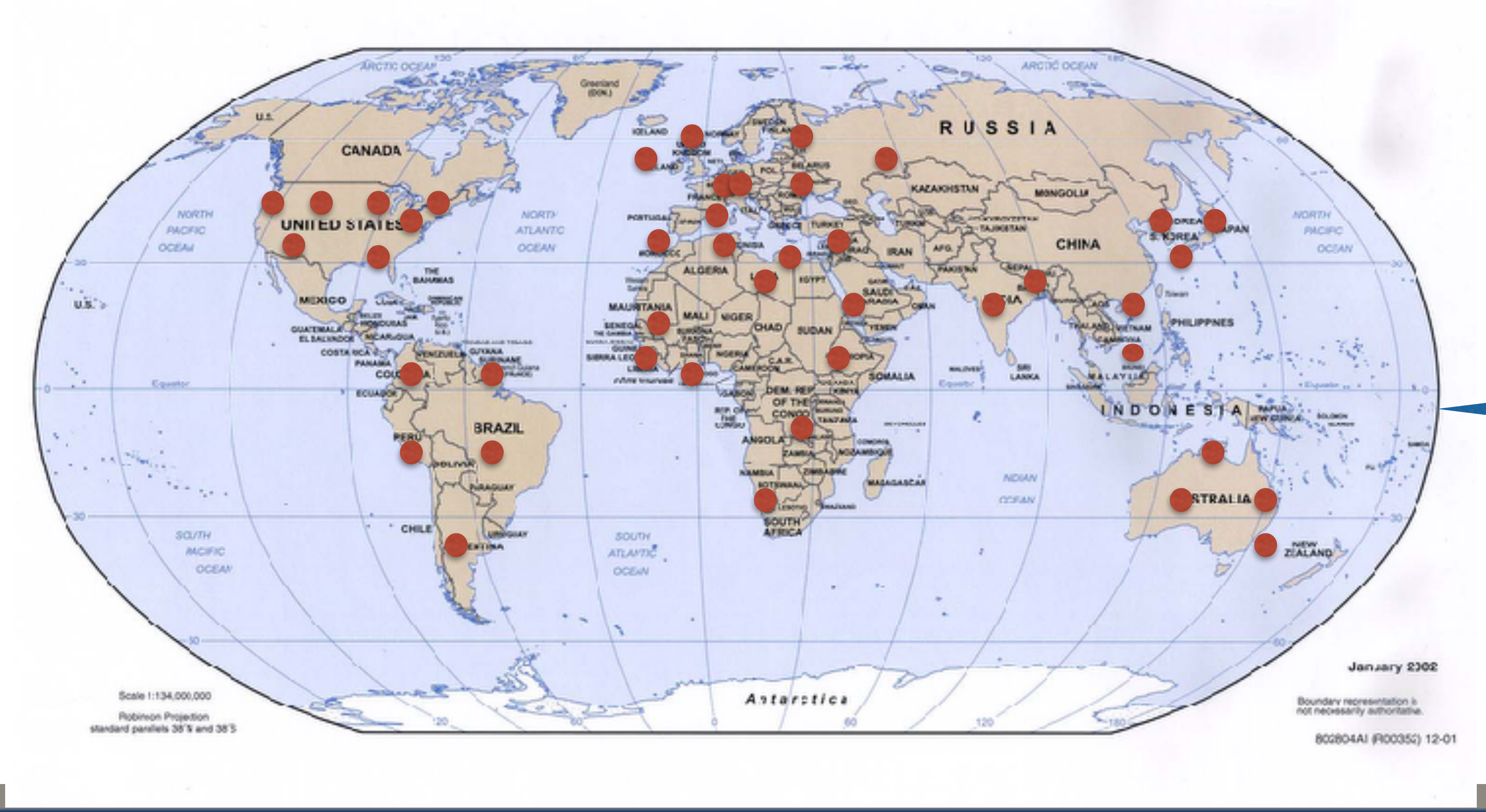
“BSD” and open-source facilitated innovation

The Case of Bitcoin and Blockchain

Satoshi Paper
Implementation (Company)
Business (Company)
Innovation by iteration
Need rebuild
Standardization
Research (University)

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

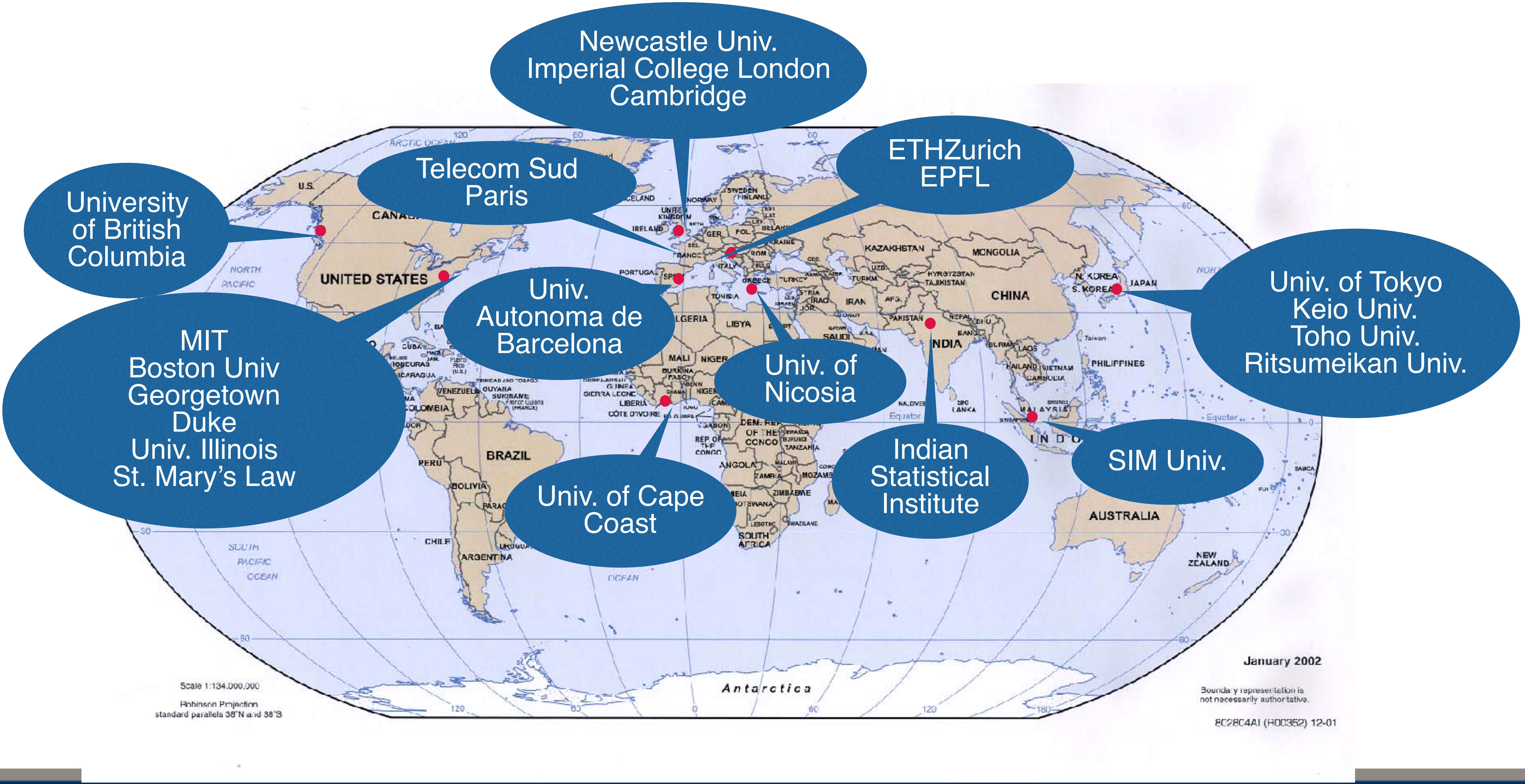
The place of neutrality

The place of diversity

The place of international collaboration

The number of university: > 15K, scalable!

23 International Universities Have Already Join and We Add More…



University of British Columbia

Telecom Sud Paris

Newcastle Univ.
Imperial College London
Cambridge

ETHZurich
EPFL

Univ. of Tokyo
Keio Univ.
Toho Univ.
Ritsumeikan Univ.

MIT
Boston Univ
Georgetown
Duke
Univ. Illinois
St. Mary's Law

Univ. Autonoma de Barcelona

Univ. of Nicosia

Univ. of Cape Coast

Indian Statistical Institute

SIM Univ.

Research project: Security Economics in Blockchain

Finding better setting of Game and Incentives toward healthy ecosystem

Goals

1. **Gather datasets which can be utilized for security-economics analysis on cryptocurrency**

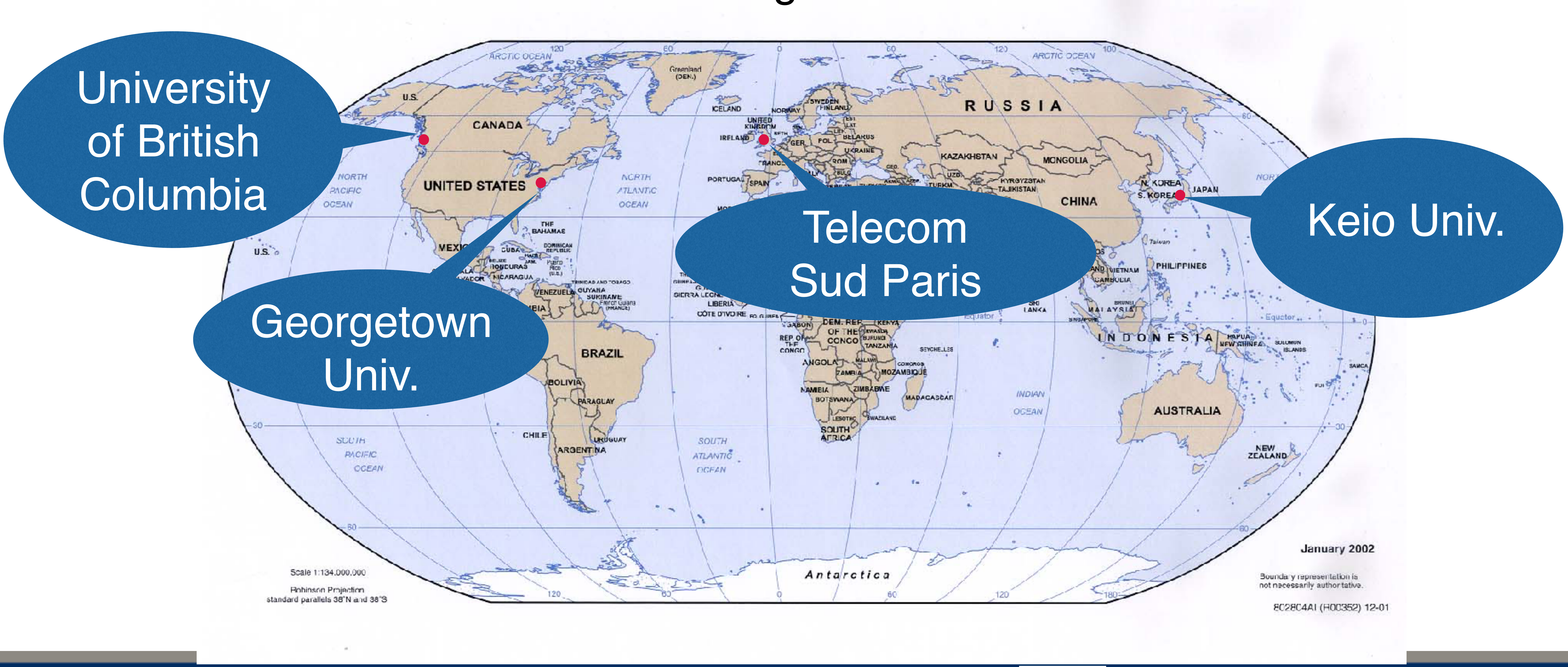
2. **Analysis on behaviors based on these datasets**

3. **Utilize these datasets to consider better incentive mechanisms and game theoretical analysis of crypto-economics**

4. **Build a foundation to share these datasets to public**

Monitoring nodes

4 Universities conduct this monitoring now. More universities are desirable



University of British Columbia

Georgetown Univ.

Telecom Sud Paris

Keio Univ.

Target of Monitoring

- Cryptocurrency: Bitcoin, Bitcoin Cash, Segwit2X and Zcash.
  - Will add Bitcoin Gold soon.
- Each member university operate one node per above cryptocurrency
- Started July 25th (one week before August 1st Fork)
- Next mile stone: November potential fork, and Bitcoin gold

Target data to be monitored (1/2)

Blockchain-related data

1. Depth of Market

(a) Number of nodes

(b) Liquidity

(c) Number of trade

(d) Agility

2. Financial stability

(a) Robustness of the blockchain network

3. Kinds of transaction

(a) Purely Financial

(b) Colored coin

(c) Pattern among kinds of coin

4. Blockchain protocol data

(a) Successful transactions

(b) Error transactions and protocol messages

Target data to be monitored (1/2)

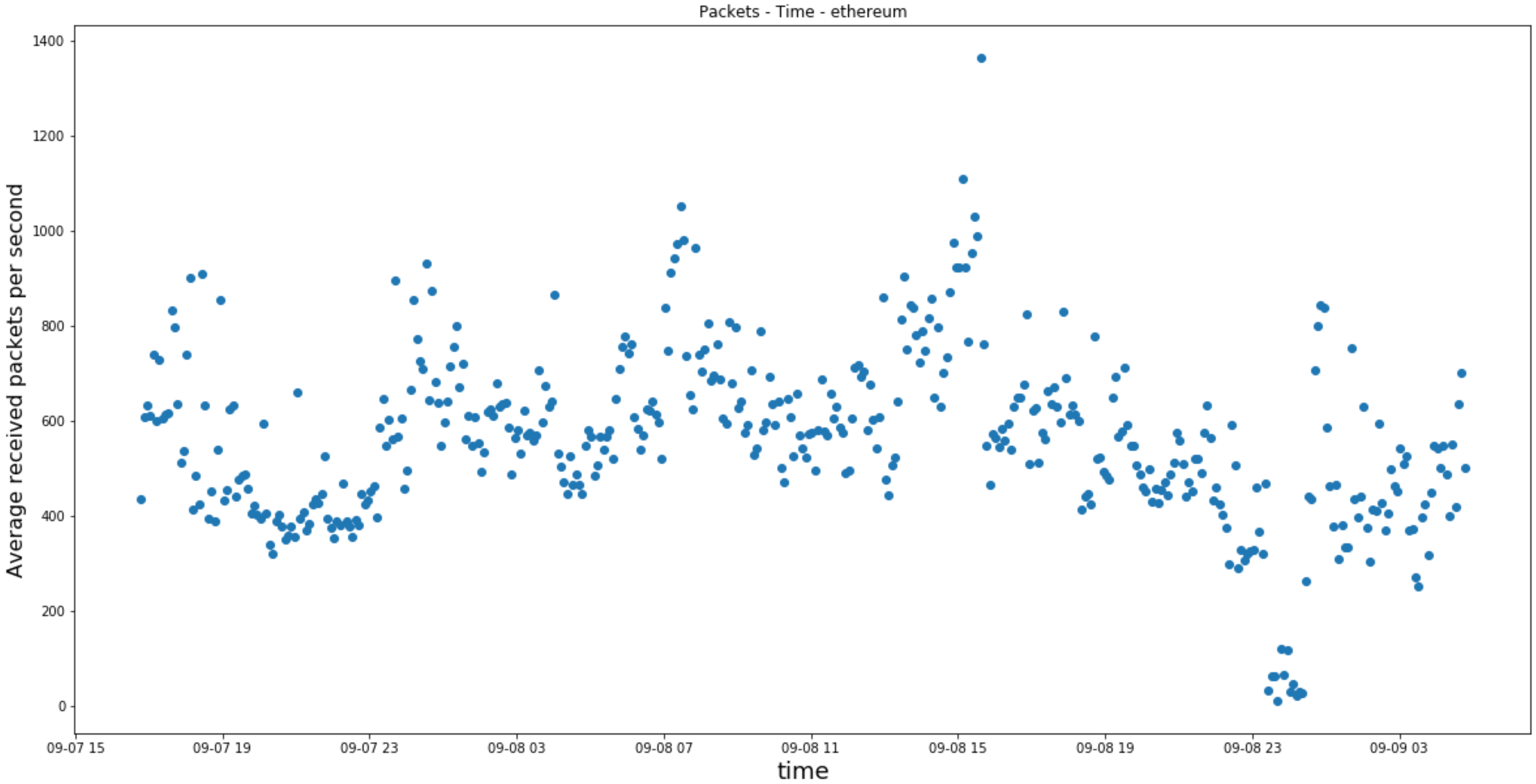
Network-related data

1. Port scan for several IP address
2. Address scan for the same port
3. DNS related attack
4. Signaling

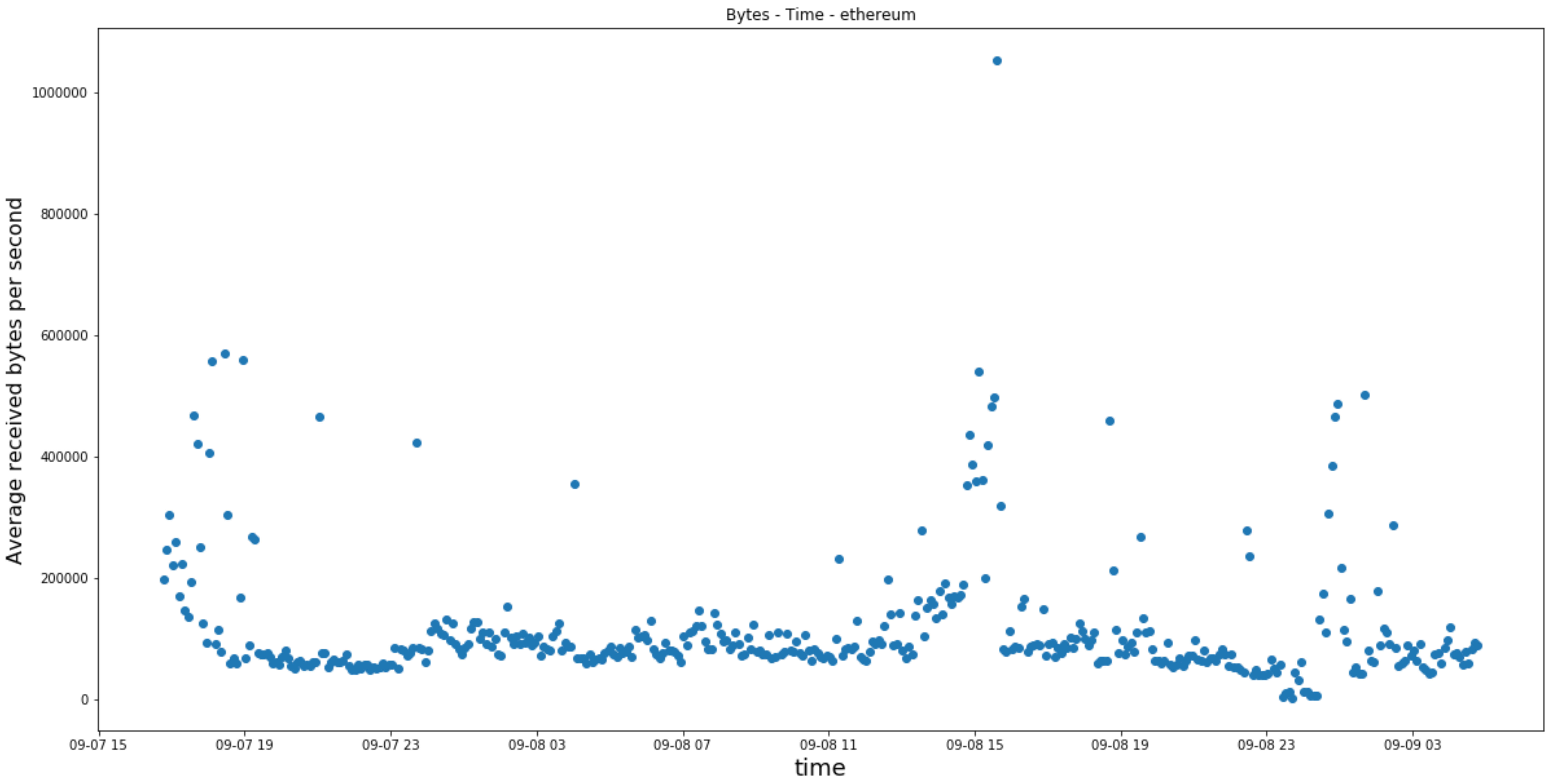
Current status

- As of august 24th, each node already has >2TB data.
- We are continuing monitoring and analyzing monitored data
  - No major evidence of cyber attack by now

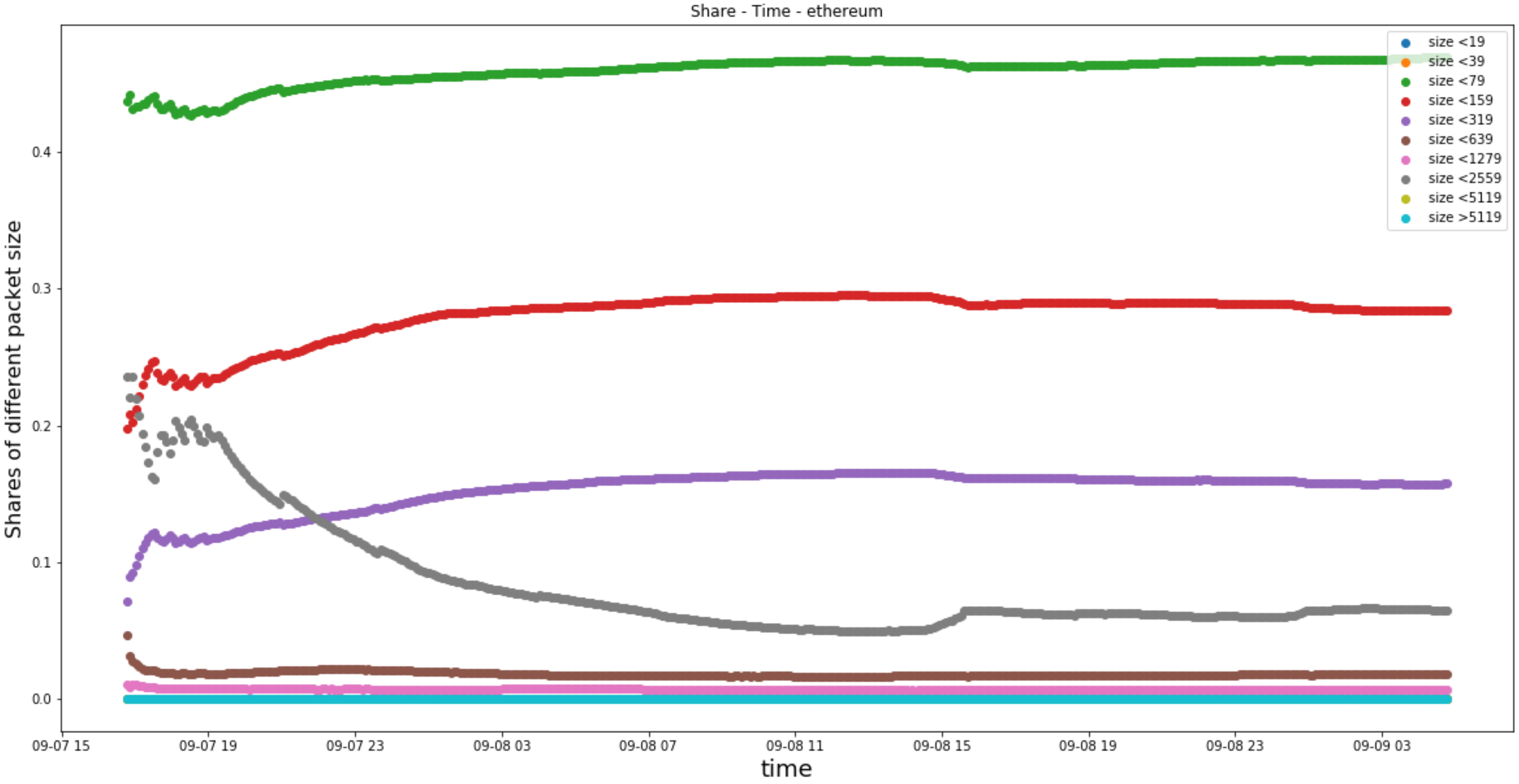
Average received packets per second



Average received bytes per second



Shares of different kinds of packet size



Future works

- Continue the analysis of block data
  - For the timing of: August 1st, Bitcoin 0.15.0, Bitcoin Gold (October 25), Segwit2x (November)
  - Game-theoretic analysis
    - Join of expert is welcome :-)
- Add more nodes
  - For accuracy of monitoring
  - Especially for cyber attacks
- Sharing datasets to public

Conclusion

Activities of BSafe.network

Ongoing Monitoring of Bitcoin and cryptocurrency

Fortunately, no evidence of cyberattack
Need more nodes, and continuous monitoring

Thank you!

1789

GEORGETOWN UNIVERSITY

BSafe
network