



Academic Research on (public) blockchain

Direction and update of BSafe.network

Shin'ichiro Matsuo

The 2nd Workshop Basing Blockchain

About Me : Shin'ichiro Matsuo



@Shanematsuo

- **Project Professor at Keio University**
- **Research Fellow at the University of Tokyo**
- **Director's Liaison for Financial Cryptography at MIT Media Lab**
- **Research Professor at Georgetown University**
 - **Director of Blockchain Technology and Ecosystem Design (B-TED) research center**
- **Co-Founder of Bsafe.network**
- **Program committee and editor: Scaling Bitcoin, IEEE, ACM conferences, Ledger Journal and more...**
 - **Program co-chair of Scaling Bitcoin 2018**
- **Standardization at ISO TC307 (Blockchain and DLT)**
- **Ph.D. from Tokyo Institute of Technology**

About Me



@Shanematsuo

**I have no Bitcoin and any
cryptocurrencies**

**I have no position on “the exchange
rate to FIAT currency.”**

Understanding The Public Blockchain and research directions

Several huge incidents



Mt. Gox



The DAO Attack



Coincheck



Monacoin

What is “the Cryptocurrency Exchange?”

No uniform definitions and models

Revisit what Satoshi proposed

An electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other **without the need for a trusted third party.**

In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.

Mind the gap between Payment and Settlement!

Satoshi's border

Payment system

Settlement system

More applications



Cryptocurrency
Exchange



Without Trusted Party
(nearly equal to
“decentralization”)
Prevent double spending




With trusted party

Other functionalities of
currency

Gaps between Satoshi's paper and real

- There is no exchange to fiat currency in the ecosystem.
 - Everything is closed inside Bitcoin ecosystem
- All participants have equal computational power
- Lack of consideration of Governance

Functions of currency, what Satoshi proposed and the reality

	What Satoshi Says	Reality of use
Medium of Exchange		
Measure of Value		
Standard of deferred payment		Some of... 
Store of Value		
Invest? Gambling by FX		Mainly 

Governance and regulation issues

- **Bitcoin = New economical nation**
 - Mathematics of Bitcoin = (economical) Constitution of the nation
 - Current chaos of governance: Lack of procedure of amendment of the constitution
 - Fork of Bitcoin: independence with new constitution
- **How do we think the new economical nation?**
 - Decentralized Virtual Currency (for greater innovation) vs. stable virtual currency

Possibility of another ATARI shock

- Video Game Crash of 1983
- Too many “Junk Games” discounted the value of game platform.
 - Lack of control of quality
- Nintendo started control of quality of each game.
- In the case of current many Virtual Currency and ICO projects?
- How can we control the quality in the era of decentralization?



What the exchange rate to fiat says:

Similarity to Japanese telephone registration fee

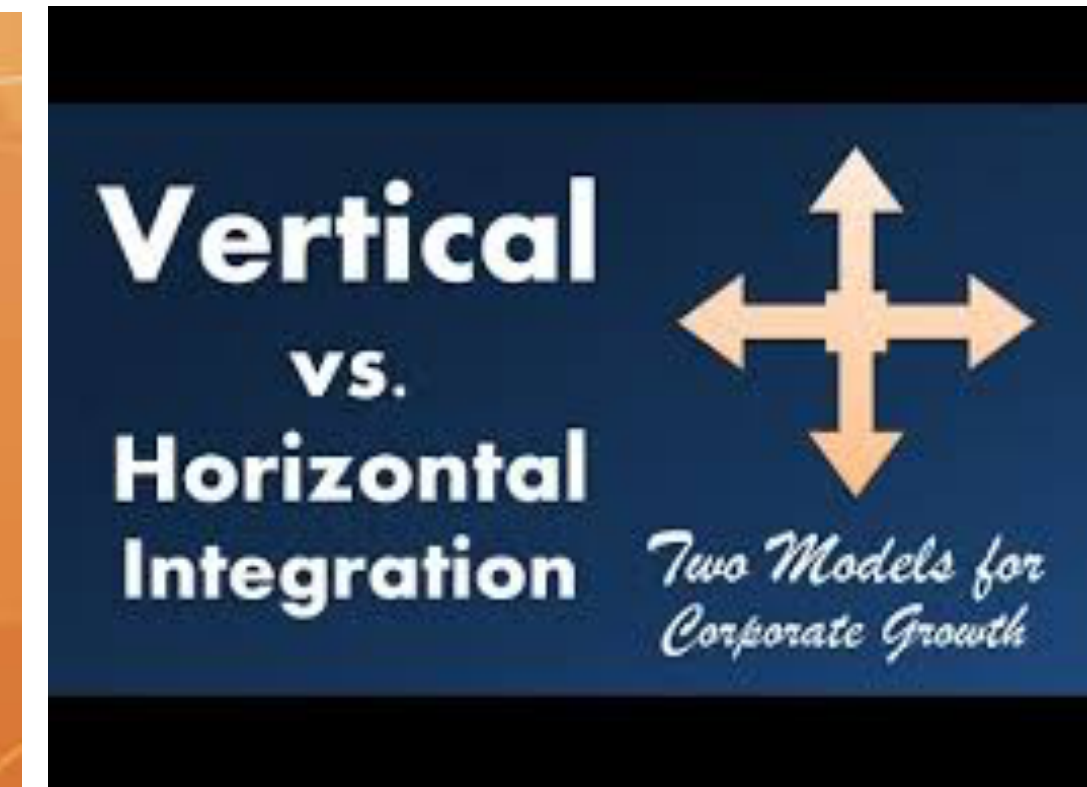
- In Japan, users of telephone paid “registration fee” as a initial cost for facilities of telephone network.
 - 80K JPY in 1976
 - The registration was transferable: traded like “a right.”
 - Currently, the registration fee (as the right) is not needed: The market value of “the right” becomes almost zero.
 - The cost for each communication became near zero: source of tons of merits of internet ecosystem
- Similarity to the exchange rate of Bitcoin to fiat currency
 - Mining cost as an initial cost of initiating decentralized blockchain network
 - Bitcoin as a medium of exchange something: Do we need to pay expensive cost to obtain it?

Competition among Blockchain technologies/services

Common to Internet-like innovation

Fail Fast

Horizontal and Vertical



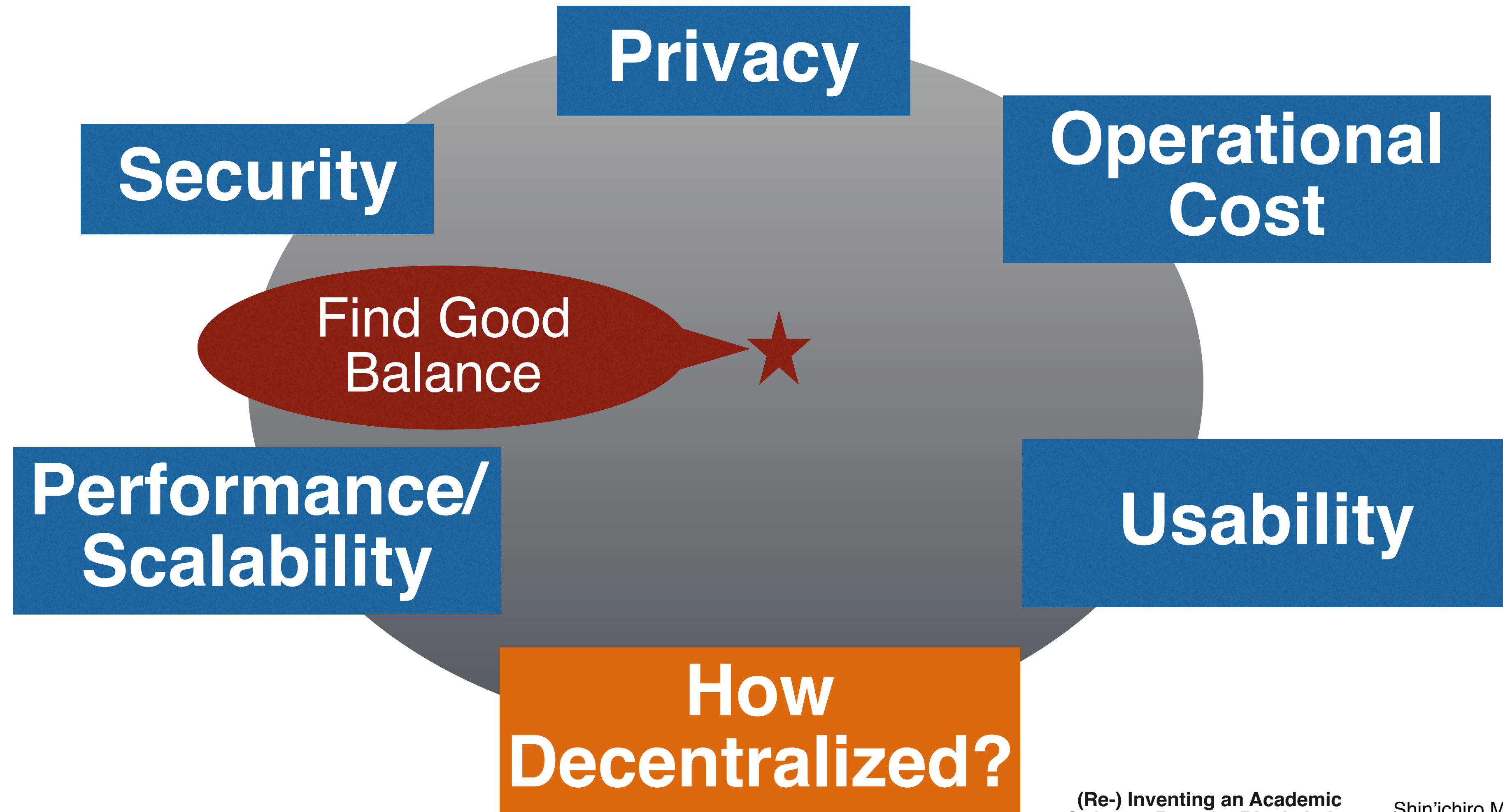
Difference to Internet-like innovation

Experiment using consumers money/asset

Lack of Due-diligence: Need to have good way to realize it

Ecosystem for innovation: competition among blockchain projects

Trade-offs Bitcoin and Blockchain Technology



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**

Source of technology related immaturity

Unproven technology

Security
Scalability
Trust model

Community Risk and Quality assurance

Need healthy community and ecosystem

Lack of evaluation criteria toward technological due-diligence

Standardization

Gap between

- What original Satoshi paper proposes and
- Expectation to Blockchain technology and its application

Game theory/ incentives / regulation

**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

Regulation: Recent hot topic



Two Research Areas

- Scaling and Privacy Enhancement
- Broaden Satoshi's boundary

Scaling!

7 tx/sec (textbook Bitcoin) vs 10,000 tx/sec (VISA)

Need to consider the trade-offs among scalability and security

Recent selfish minings on Monacoin and Bitcoin gold warns us again

Two Directions toward scaling

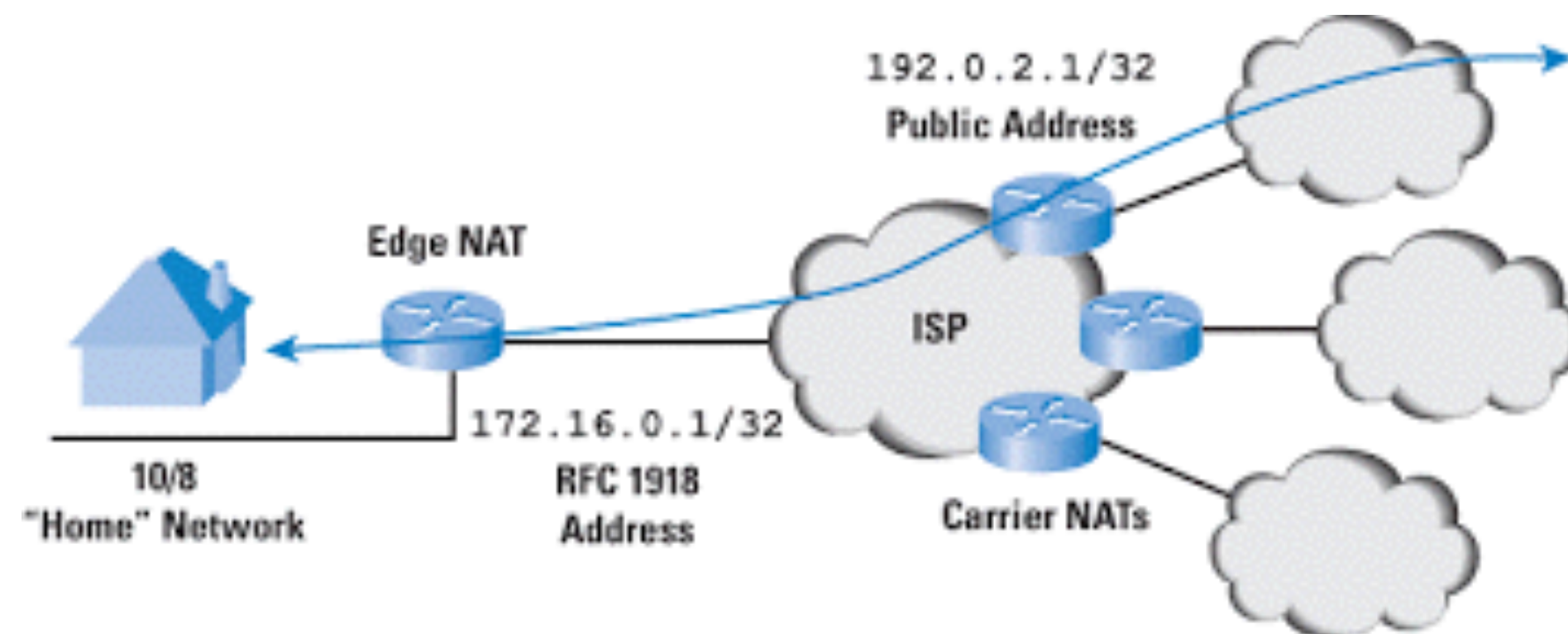
Off-chain vs On-chain

Lightning
Network

Scalable, Instant Bitcoin/Blockchain Transactions



Like IPv4+NAT and IPv6



Both directions are important.

Layer 2 Technology of Blockchain

Layer 2

Lightning
Network

Scalable, Instant Bitcoin/Blockchain Transactions



TumbleBit

Layer 1



Enhance
Scalability, privacy...

Beyond the payment

Enrichment of scripting

Carefully broaden the Satoshi's border

Simplicity

Simplicity: A New Language for Blockchains

Russell O'Connor
roconnor@blockstream.com

2017-12-13

Abstract

Simplicity is a typed, combinator-based, functional language without loops and recursion, designed to be used for crypto-currencies and blockchain applications. It aims to improve upon existing crypto-currency languages, such as Bitcoin Script and Ethereum's EVM, while avoiding some of the problems they face. Simplicity comes with formal denotational semantics defined in Coq, a popular, general purpose software proof assistant. Simplicity also includes operational semantics that are defined with an abstract machine that we call the Bit Machine. The Bit Ma-

Reconsider Blockchain as a “Slow-network”

The Internet was called as “Stupid-network”.

End to End Principle

Let the ends do it

Let the user decide

Too redundant but produced tons of innovations

Blockchain is a “slow network”

10 minutes block interval : for security and caused by BGP and the Internet limitation

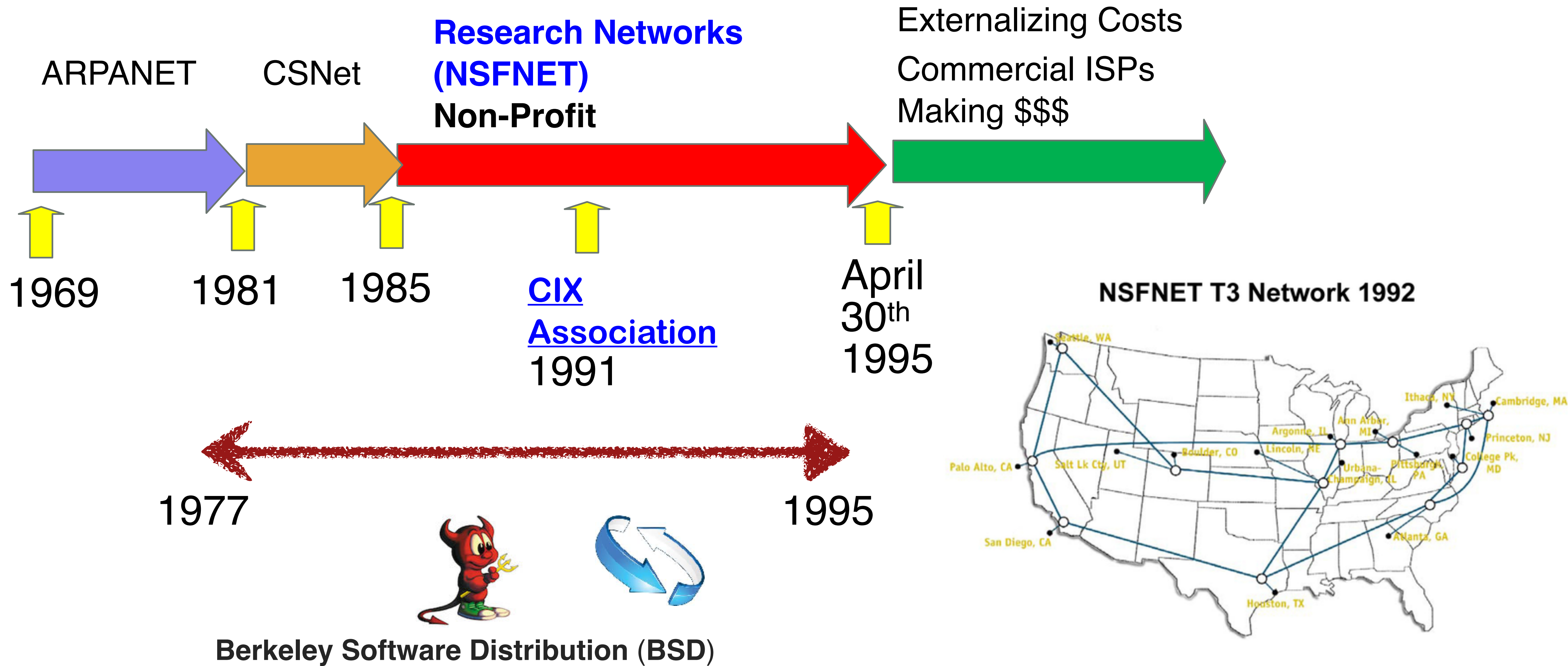
Let collaboration of over 51% nodes do it

Too redundant but **eliminate tampering** and is **expected to produce tons of innovations**

Update of BSafe.network

Technology development, quality control and governance in the decentralization era

NSFNet for the Internet



History of Berkeley Software Distribution (BSD) UNIX

AT&T
Unix

Came to
Berkeley

Beginning of
BSD Unix

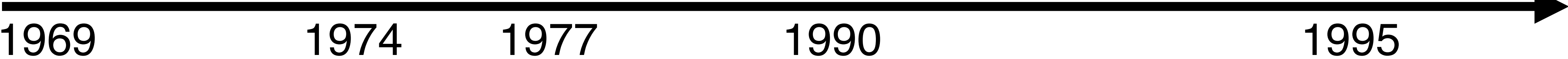


Ultrix (DEC)



SunOS

4.4 BSD Lite
Release 2



Outcomes from Berkeley Software Distribution (BSD)

Academic research and efforts matured codebase of Unix

Many Descendants

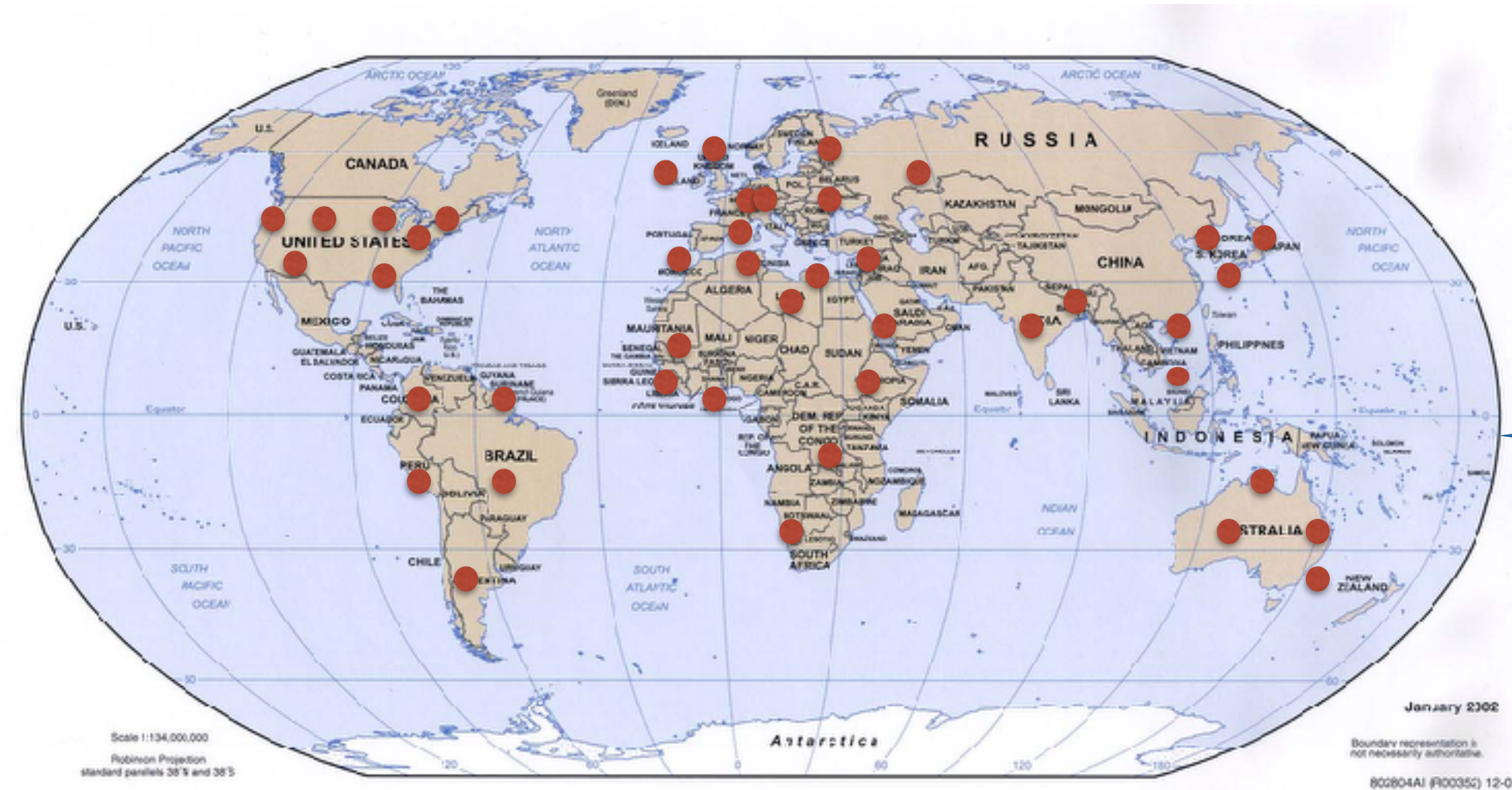


Firm foundation of Internet ecosystem

Collection of knowledge, tons of experts and engineers are helping development of Linux

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 experiments

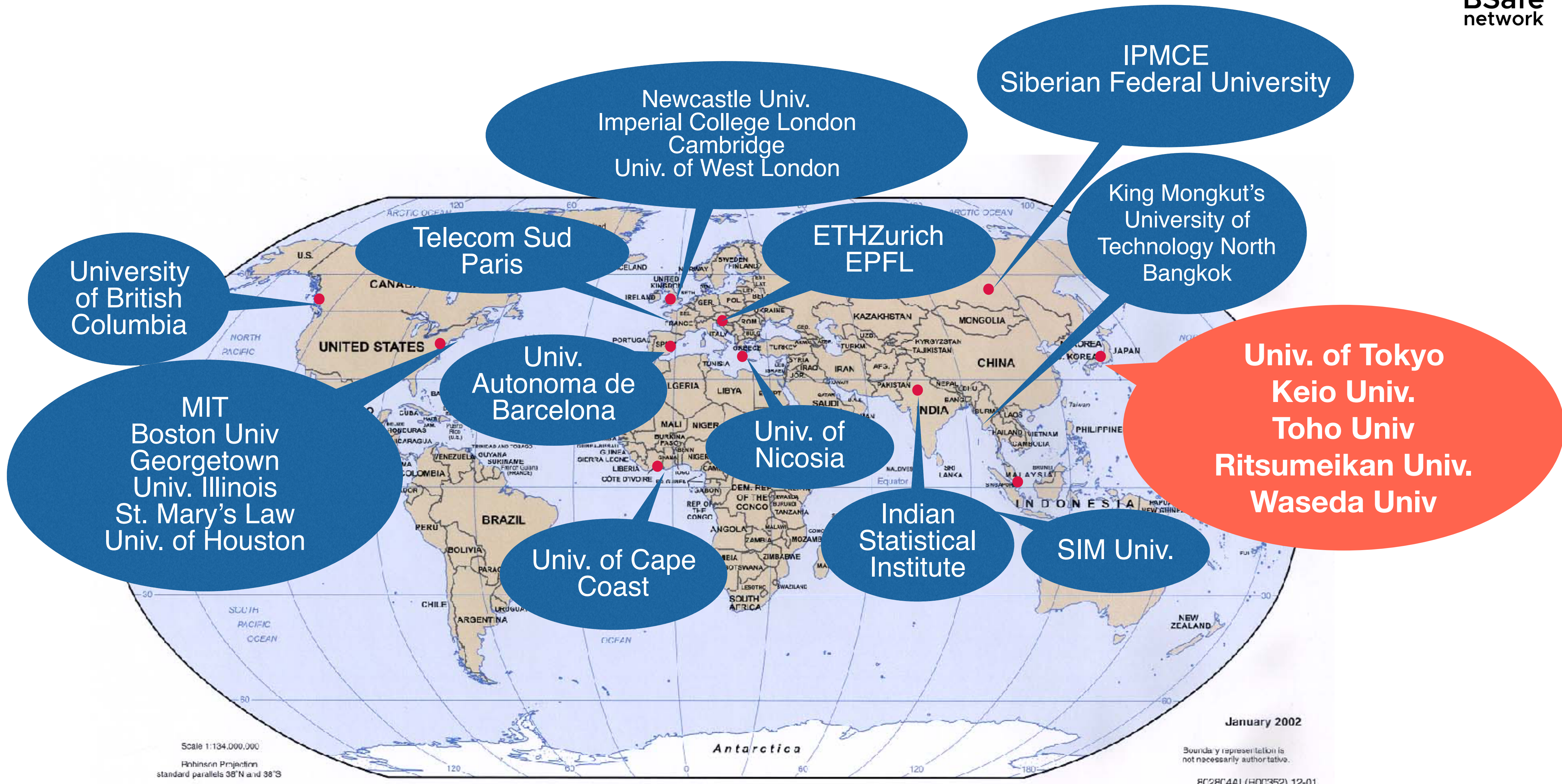
The place of neutrality

The place of diversity

The place of international collaboration

The number of university: > 15K, scalable!

28 International Universities Already Join and We Add More...

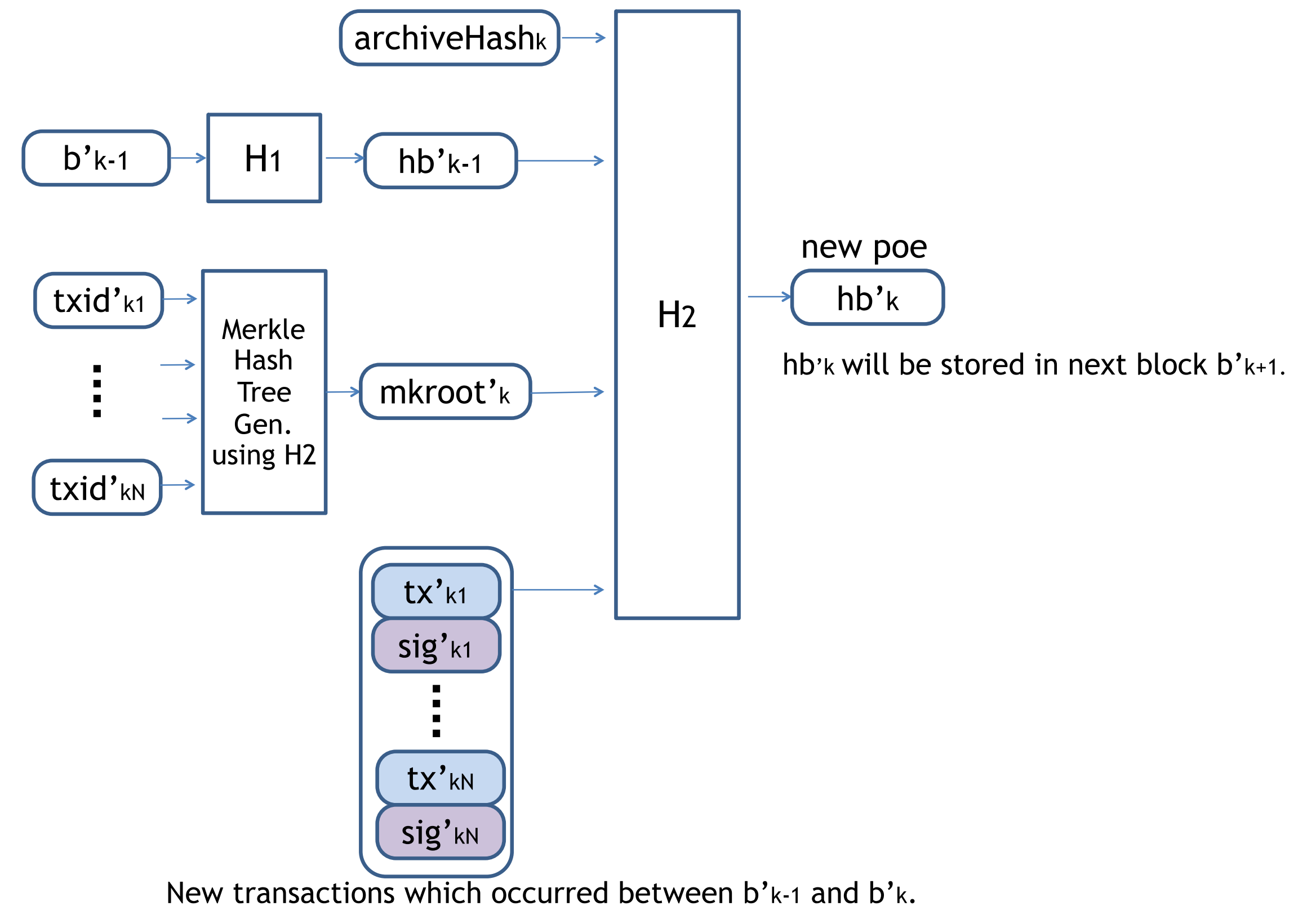


Example of experiment: Long Term Blockchain

Extension of validity of the chain upon compromise of underlying cryptographic algorithms

Application of Long Term Signature (ETSI Standard)

Experiment by 2 Japanese, 2 European, 2 US and 1 Canada nodes.



Example of experiment: Monitoring in forking

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**

Monitoring nodes

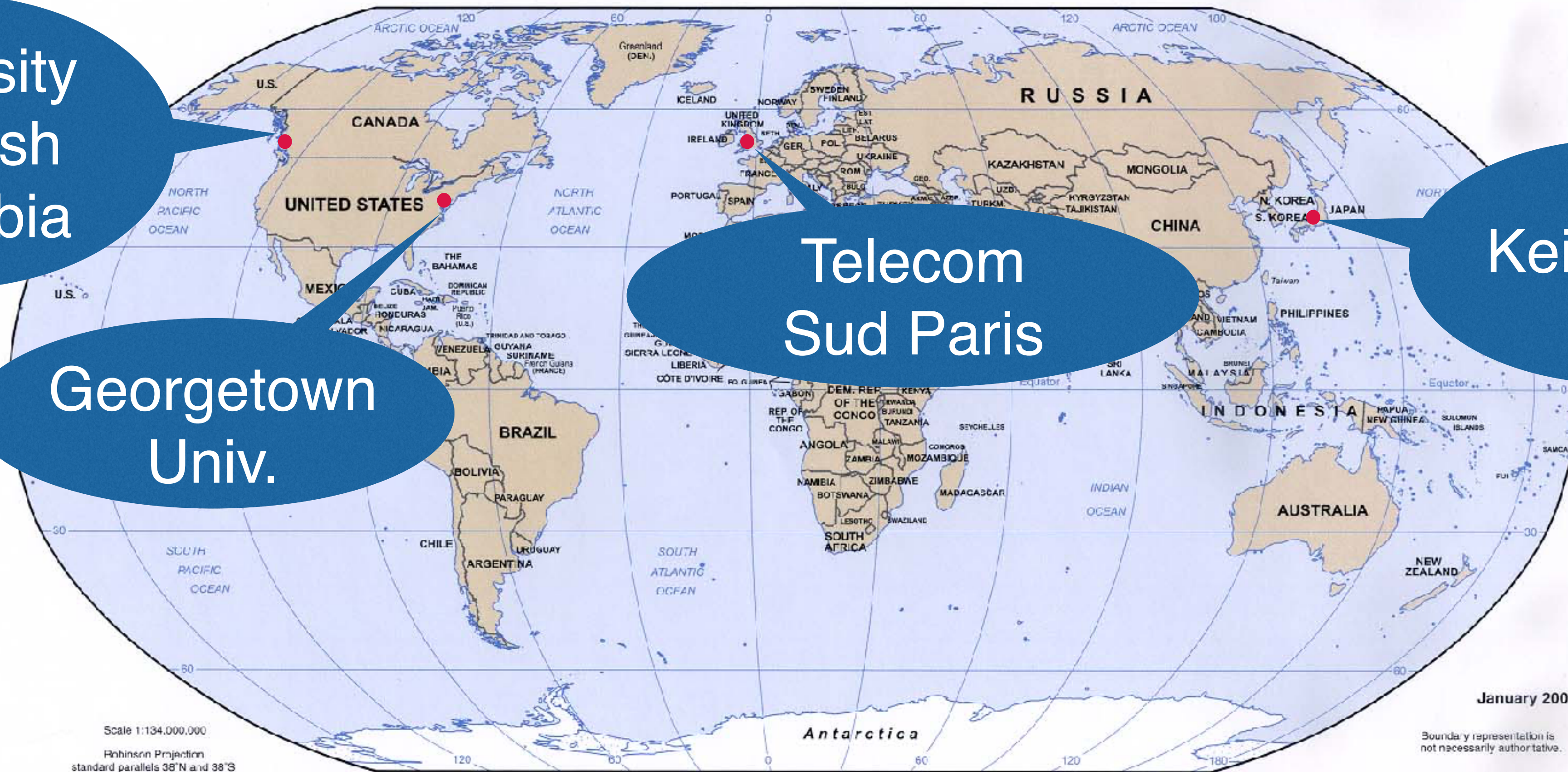
4 Universities conduct this monitoring now. More universities are desirable

University
of British
Columbia

Georgetown
Univ.

Telecom
Sud Paris

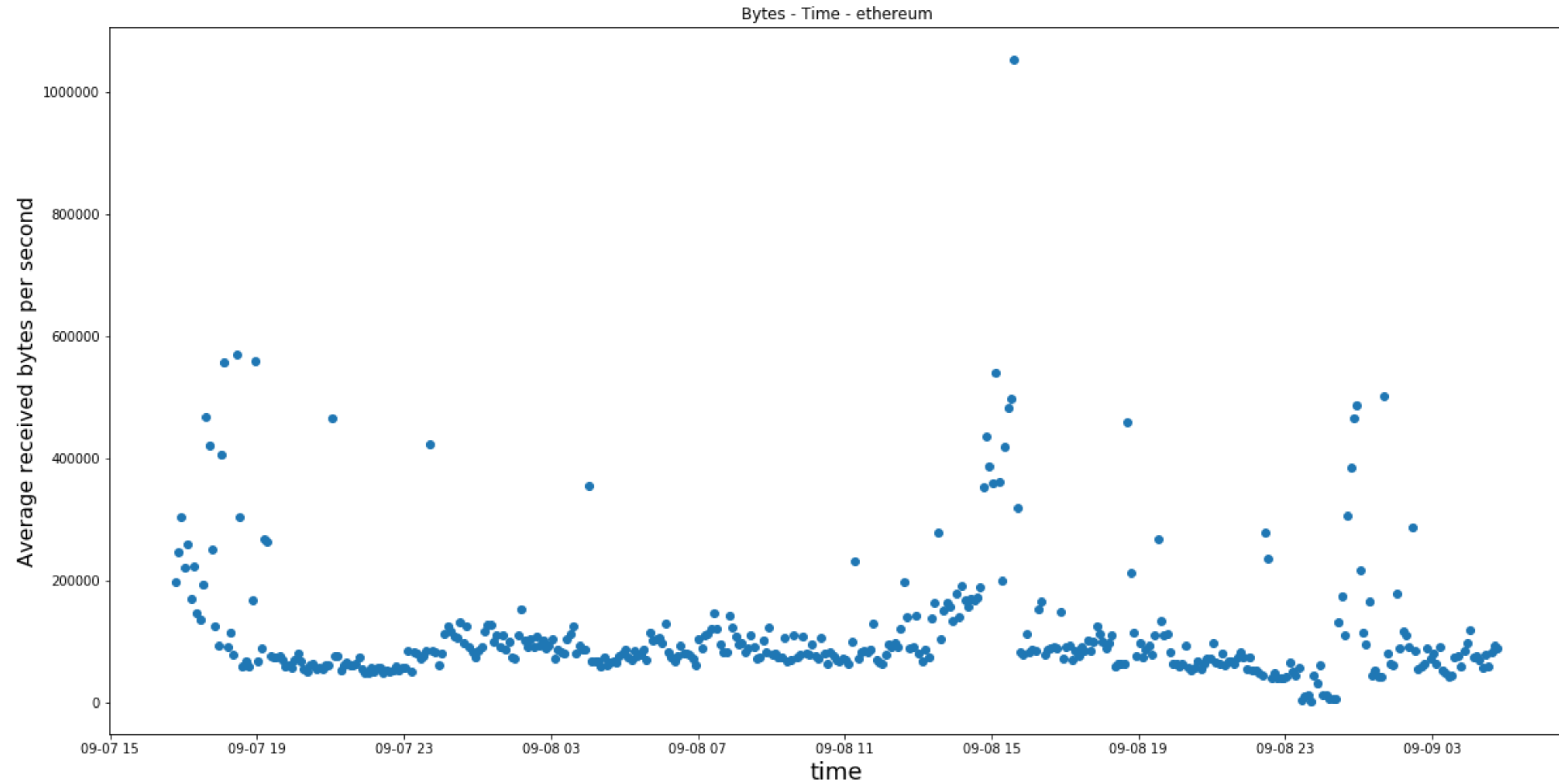
Keio Univ.



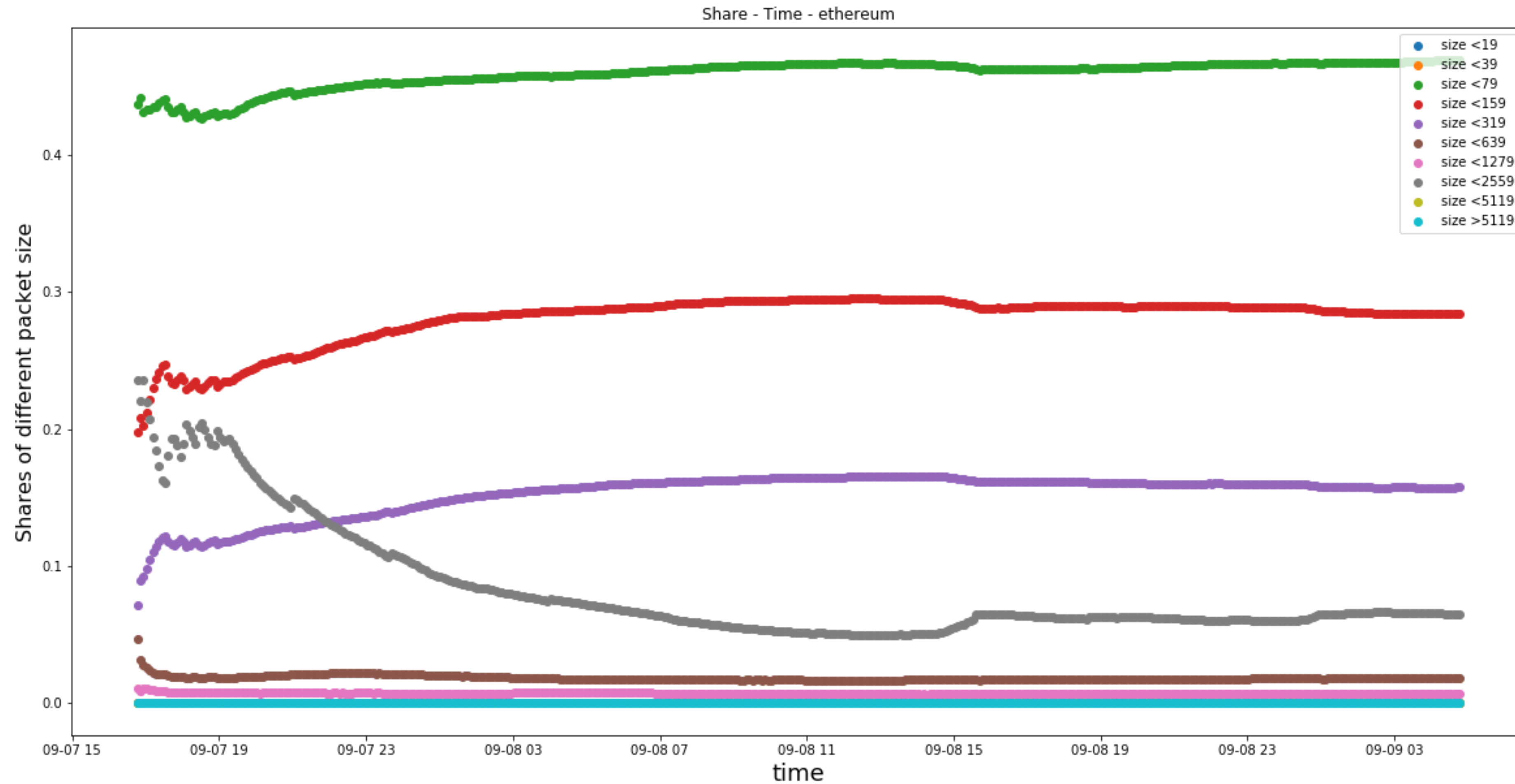
Target of Monitoring

- Cryptocurrency: Bitcoin, Bitcoin Cash, Segwit2X and Zcash.
- Each member university operate one node per above cryptocurrency
- Started July 25th (one week before August 1st Fork)

Average received bytes per second



Shares of different kinds of packet size



Open Competition of Technology

A good way to develop and select a appropriate technology which fits a certain goal.

Has a common goal

Has a common evaluation criteria

Fair, open and public verifiable result

Produces new knowledge on technology

Produces reliable codebase



An example of open competition of technology: SHA-3

1. Compromise of standard hash functions (2004)

- MD5, RIPEMD, SHA0 and SHA1
- SHA2 is still secure

2. Develop a new hash standard (2005-2012)

- Alternative to SHA2
- Open competition from international researchers
- Same as the AES competition
- Succeeded in making technology consensus by its careful process

Layer 2 Competition for Blockchain



Layer 2 Measurement method and tool

Measurement mechanisms
Standard dataset for evaluation

Provide neutral evaluation results from experiment and reviews by experts

- 1) Collecting attack models on layer 2 network,
- 2) Building measurement of security and performance of layer 2 technology
- 3) Finding better and best realization

Not selecting something, but provide academia backed data and research results to public

Outcome to public

Program codes: cc-by license
Evaluation software/platform
Layer 2 software
Evaluation data

Byproduct

Security testing theory and tools for Layer 2 technology

Scaling Bitcoin 2018 Tokyo

- A Series of workshops to enhance bitcoin technology
- The place where good new technological advances are presented
 - 2015 Montreal: Lightning
 - 2015 Hong Kong: Segregated Witness
 - 2016 Milan: TumbleBit, MimbleWimble
 - 2017 Stanford: FlyClient, etc
- Scalability, privacy, game-theory, ...
- Will be held **in Tokyo** October 6 and 7
- An associated event: Bitcoin Edge Dev++



<https://tokyo2018.scalingbitcoin.org>

Theme of this year: Kaizen 改善

- A Japanese word registered in Oxford dictionary. and US version of Wikipedia.
It represents Japanese culture on precision engineering.
- Let us “Kaizen” Bitcoin and Blockchain technology!

Definition of *kaizen* in English:

kaizen 



NOUN


[mass noun]


A Japanese business philosophy of continuous improvement of working practices, personal efficiency, etc.

[+ Example sentences](#)

Origin

Japanese, literally ‘improvement’.

Pronunciation 

kaizen /kai'zen/ 

Call for Proposals

- Two types of proposals
 - 20-30 minutes presentation
 - One hour long workshop
- Important dates
 - Submission deadline: 2018-06-30 23:59 UTC
 - Author notification: 2018-08-15 23:59 UTC



*Call for
Papers*

Program Committee

- Program Co-chairs: Shin'ichiro Matsuo, Elaine Ou

Engineering Perspective

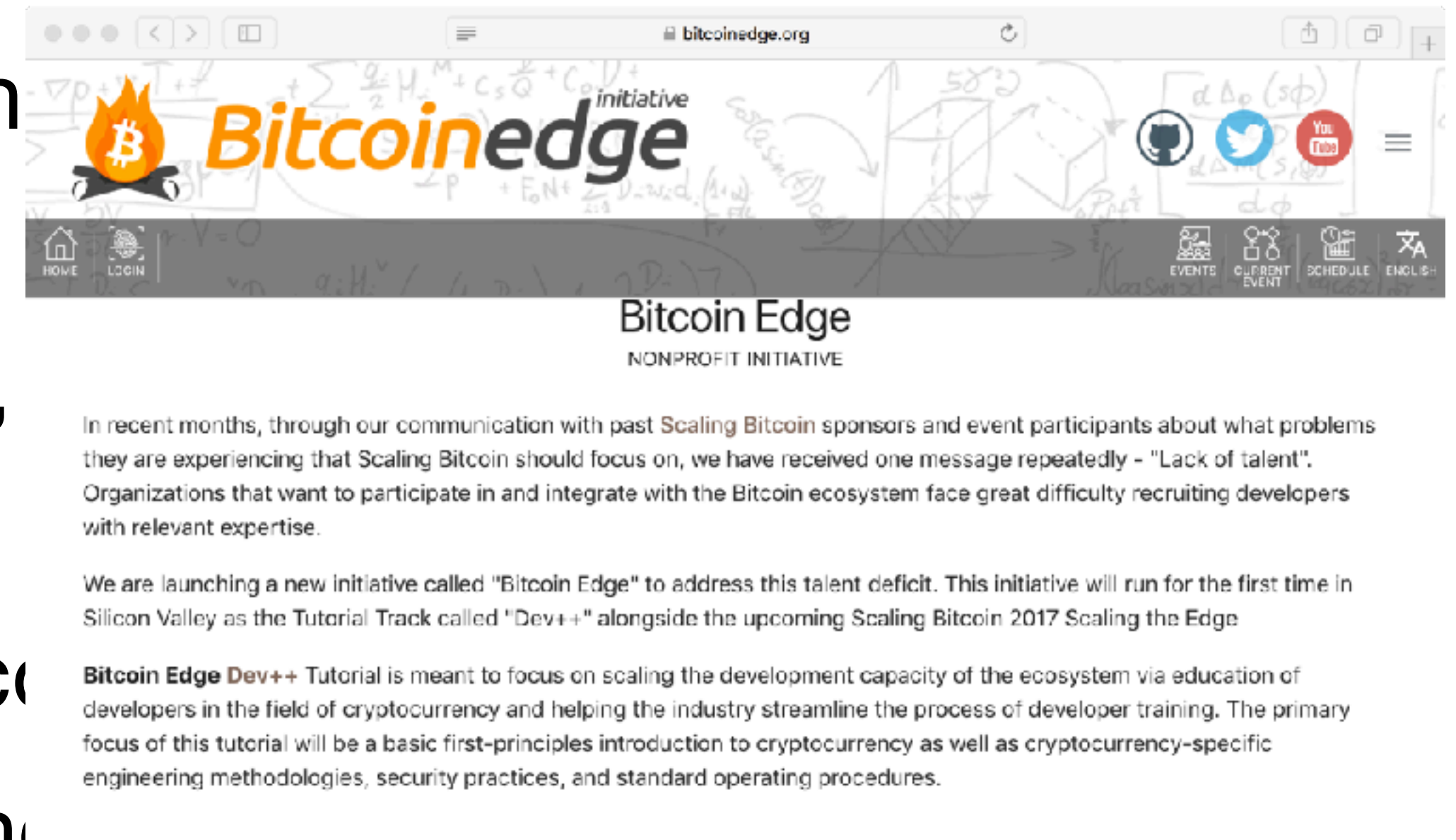
- Bryan Bishop, LedgerX, Bitcoin Core Contributor
- Ricardo Casatta
- Fabrice Drouin, Acinq
- Jameson Lopp, BitGo
- John Newbery, Chaincode
- Olaoluwa Osuntokun, Lightning Labs
- Rusty Russel, Blockstream
- Jonas Schnelli, Bitcoin Core Contributor
- David Vorick, Nebulous Labs
- Eric Voskuil, LibBitcoin

Academic Perspective

- Joseph Bonneau, New York University
- Benedikt Bunz, Stanford University
- Ittay Eyal, Technion Israel Institute of Technology
- Ethan Heilman, Boston University
- Brian Levine, University of Massachusetts at Amherst
- Kanta Matsuura, The University of Tokyo
- Ian Miers, Johns Hopkins University
- Andrew Miller, University of Illinois Urbana-Champaign
- Shigeya Suzuki, Keio University
- Aviv Zohar, The Hebrew University of Jerusalem

Bitcoin Edge Dev++

- Two days education program to broaden blockchain developers
- Good place to learn about blockchain, practice
- Bring your own laptop, write and run code
- Lecturers are Bitcoin core developers and
- Will be held on days before Scaling Bitcoin 2018
- <https://bitcoinedge.org>



Thank you!