

Future of Blockchain: Prospective on Bitcoin

Shin'ichiro Matsuo
Georgetown University

Blockcahin@UBC Conference



GEORGETOWN UNIVERSITY



About Me



@Shanematsuo

- Research Professor at Georgetown University
 - Director of Blockchain Technology and Ecosystem Design (B-TED) research center
- Director's Liaison for Financial Cryptography at MIT Media Lab
- Co-Founder of Bsafe.network (Blockchain Research)
- 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.

How Mature?



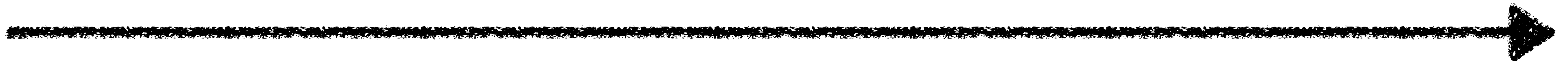
Refinement by iteration

Experimental

Technically
Confirmed

Commercialization

New Applications/
Ecosystem



Several huge incidents



Mt. Gox



The DAO Attack



Coincheck



Monacoin

Regulation is the matter, again

History

BitLicense (2015)

Current

Scam, scam and scam

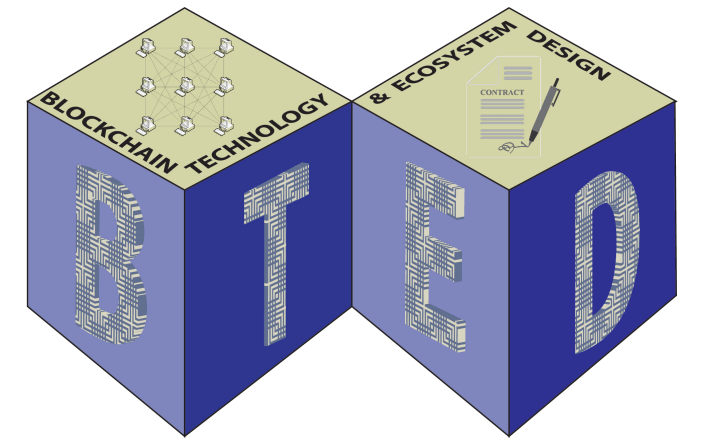
“Cryptocurrency” to “Cryptoasset”

Now is the time to revisit what original Bitcoin claims.

What is “the Cryptocurrency Exchange?”

No uniformed 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.

Satoshi's boundary

Payment system

Settlement system

More applications






Without Trusted Party
(nearly equal to
“decentralization”)

With Trusted Party

Gaps between Satoshi's paper and real

- There is no exchange to Fiat Currency in the ecosystem
 - Everything is closed inside Bitcoin ecosystem
- All participant has 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		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 constitution
 - Branching 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

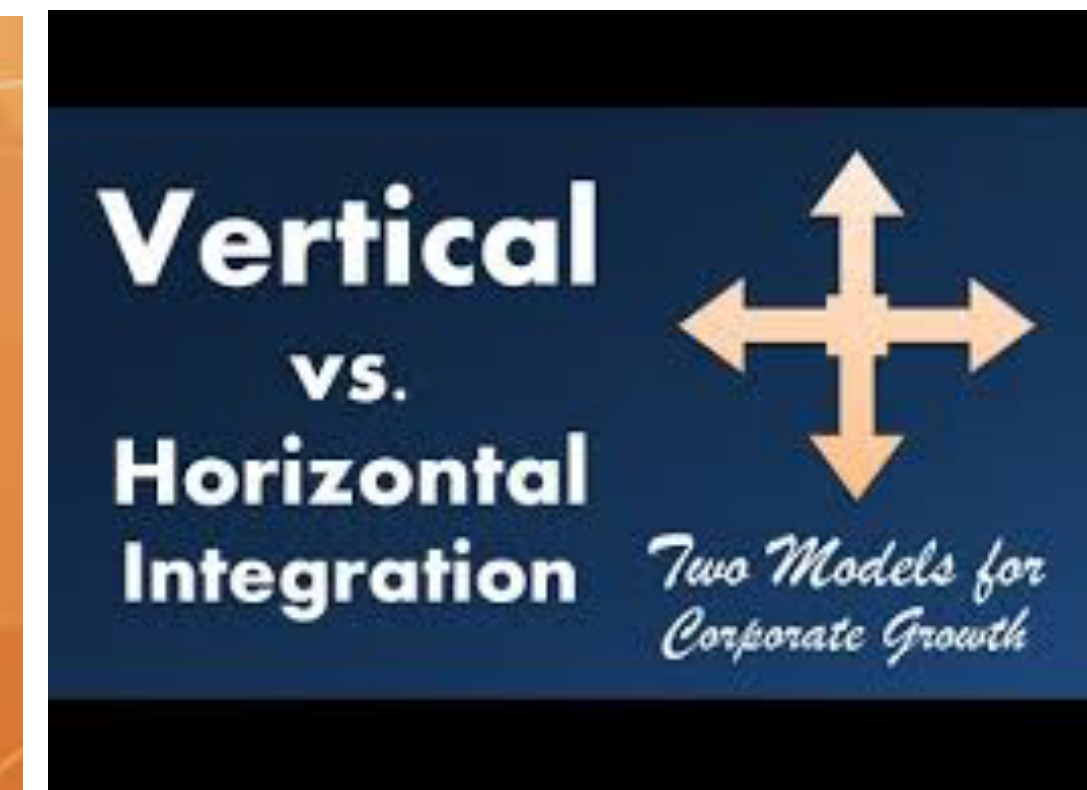
- In Japan, users of telephone paid “registration fee” as a initial cost for facilities of telephone network.
 - 80K JPY in 1976
 - The registration was transferable: traded like “a right.”
 - Currently, the registration fee (as a right) is not needed: The market value of “the right” become almost zero.
 - 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 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

Source of technology related immaturity

Unproven technology

Security
Scalability
Trust model

Community Risk and Quality assurance

Need healthy community and ecosystem

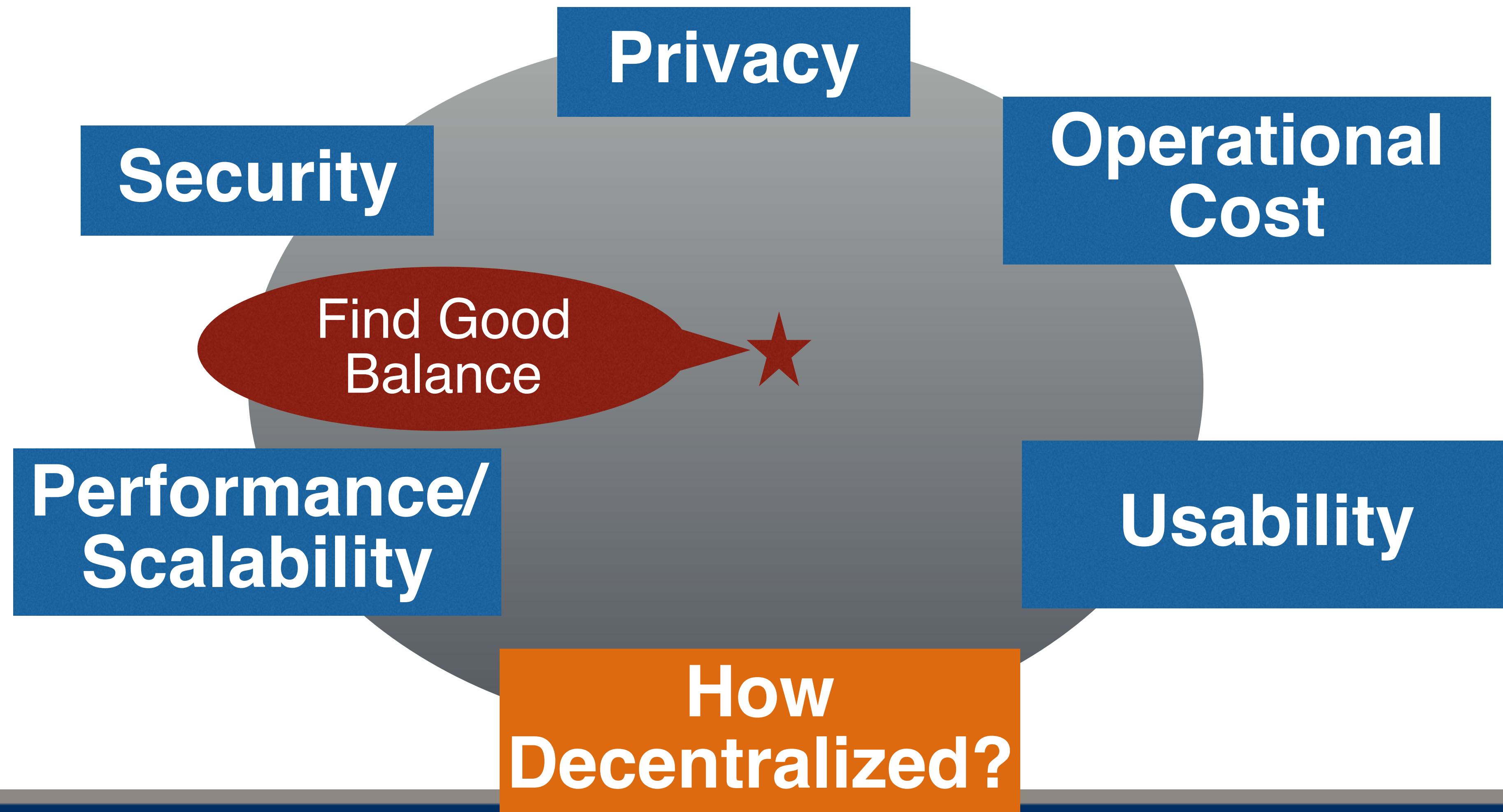
Lack of evaluation criteria toward technological due-diligence

Standardization

Gap between

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

Trade-offs in 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**

Game theory/ incentives / regulation

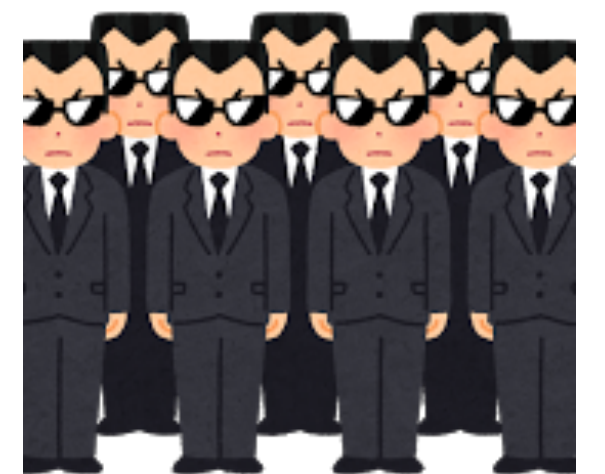
**The Security of Bitcoin/
Cryptocurrency/Public Blockchain
relies not only on technology but
also on incentive design.**



Games in
blockchain
ecosystem

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

Regulation: Recent hot topic



Scaling!

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

Trade-offs among scalability and security

Recent Selfish mining warns us again

Two Directions toward scaling

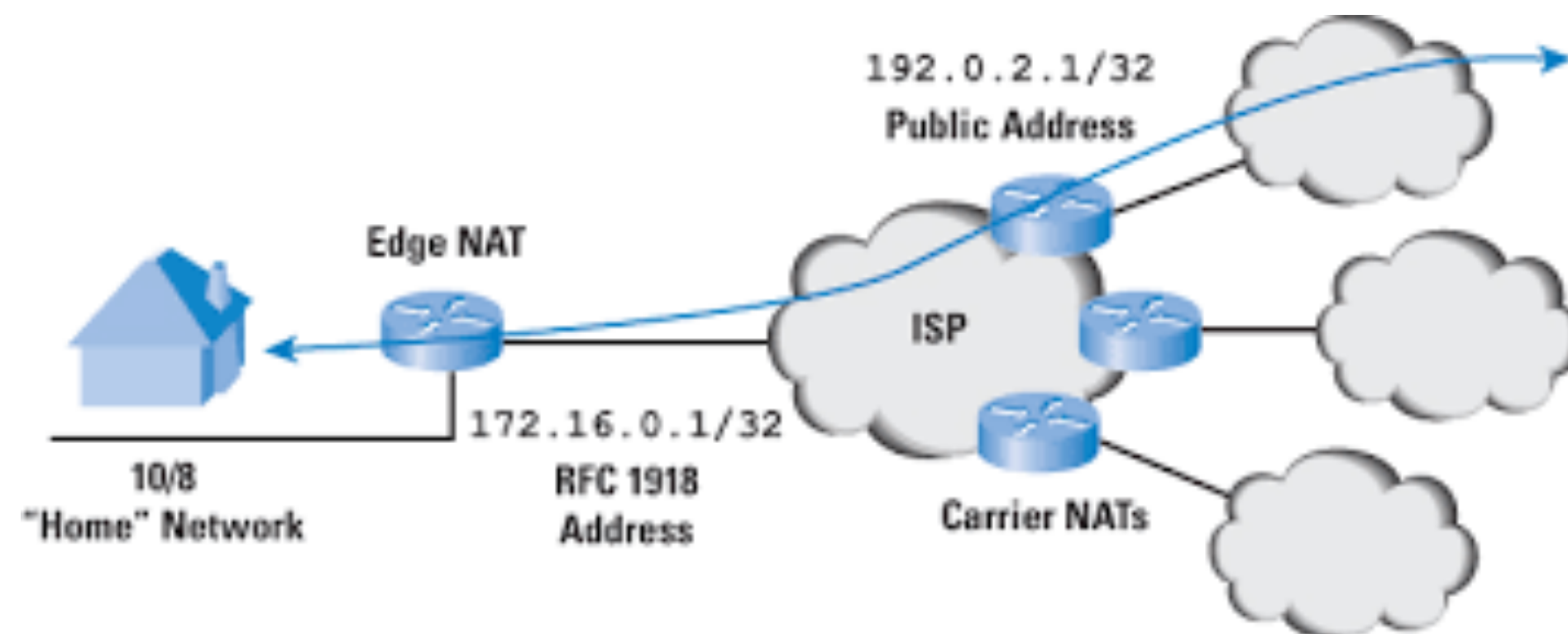
Off-chain vs On-chain

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 boarder

Simplicity

Reconsider Blockchain as a “Slow-network”

The Internet is called as “Stupid-network”.

End to End Principle

Let the ends do it

Let the user decide

Too redundant but produces innovation

Blockchain is a “slow network”

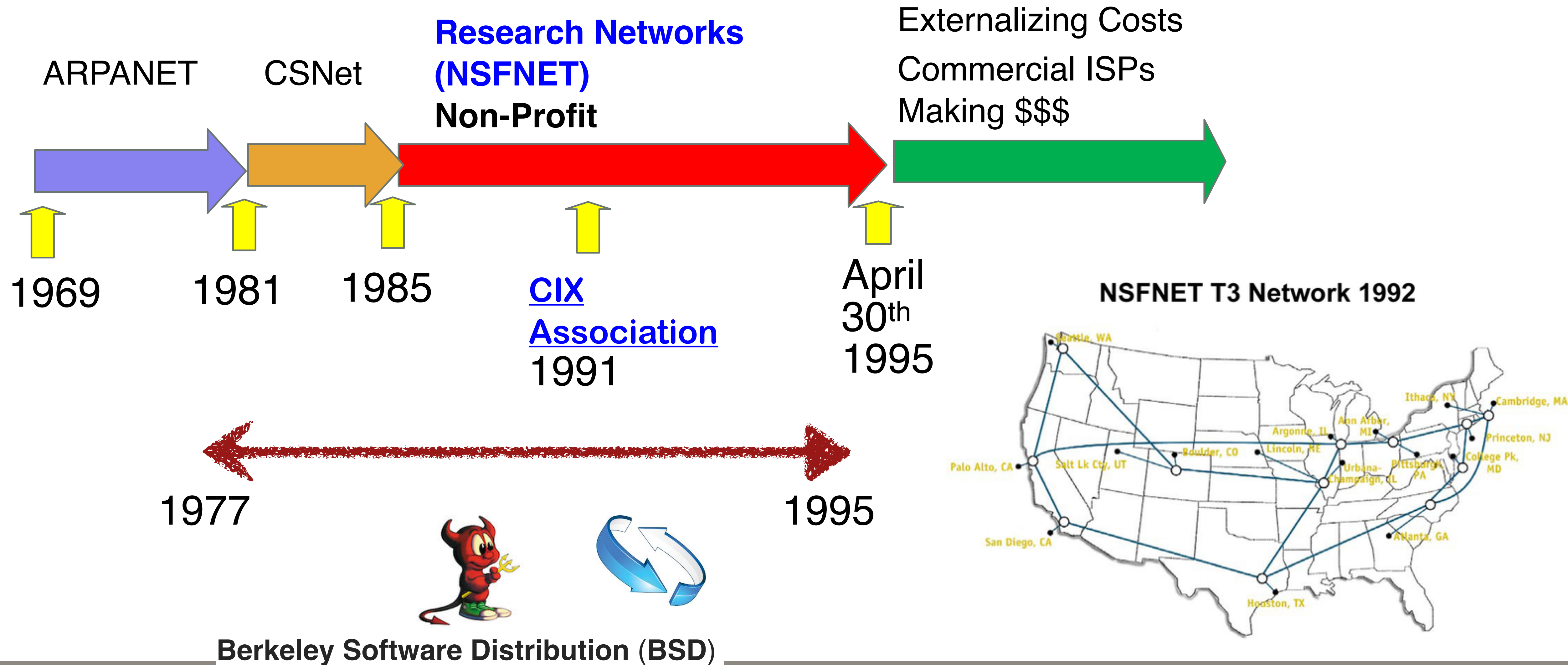
10 minutes block interval : for security and from DNS and the Internet limitation

Let collaboration of over 51% nodes do it

Too redundant but eliminate tampering and produces innovation

THE WAY FORWARD

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

1969

1974

1977

1990

1995

Outcomes from Berkeley Software Distribution (BSD)

Academic research and efforts matured codebase of Unix

Many Descendants

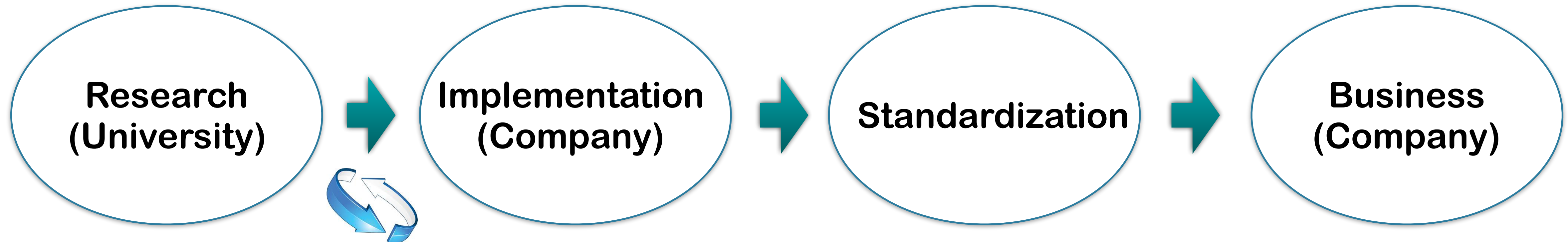


Firm foundation of Internet ecosystem

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

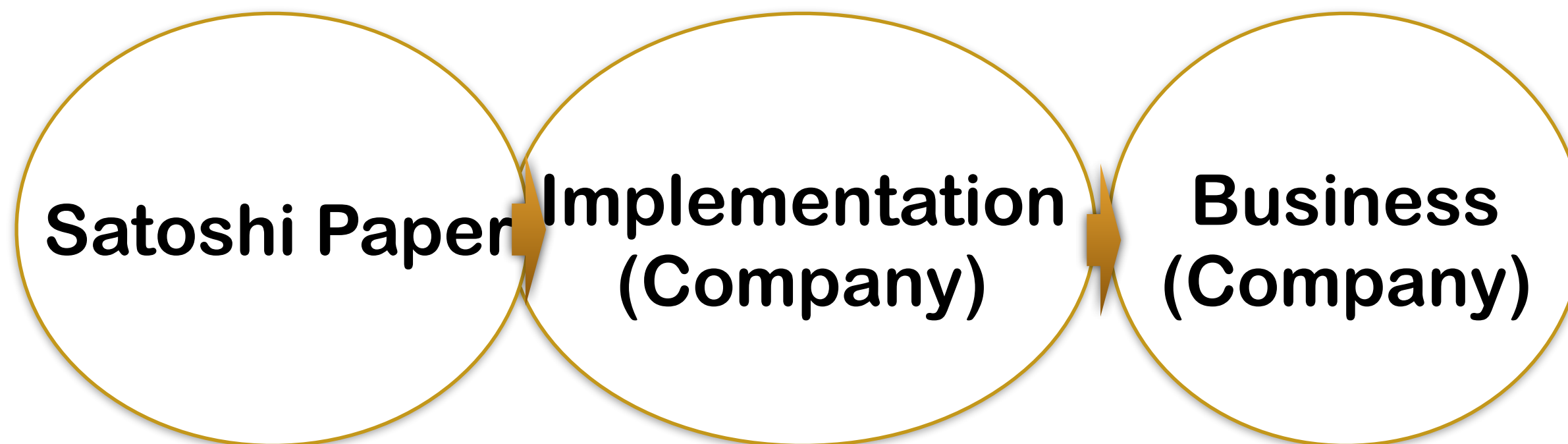
Academic Research is still needed

The Case of Internet Technology

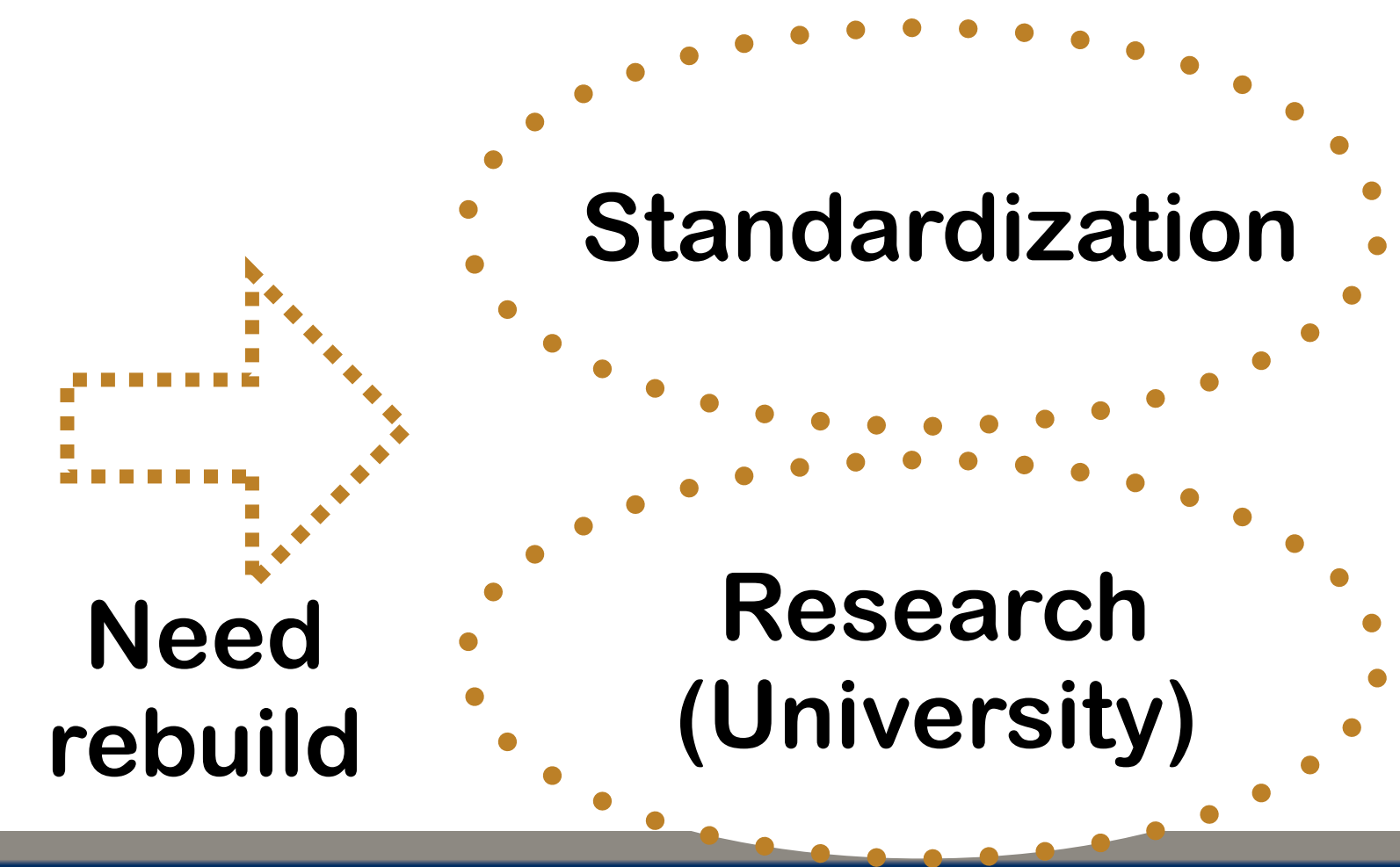


"BSD" and open-source facilitated innovation

The Case of Bitcoin and Blockchain

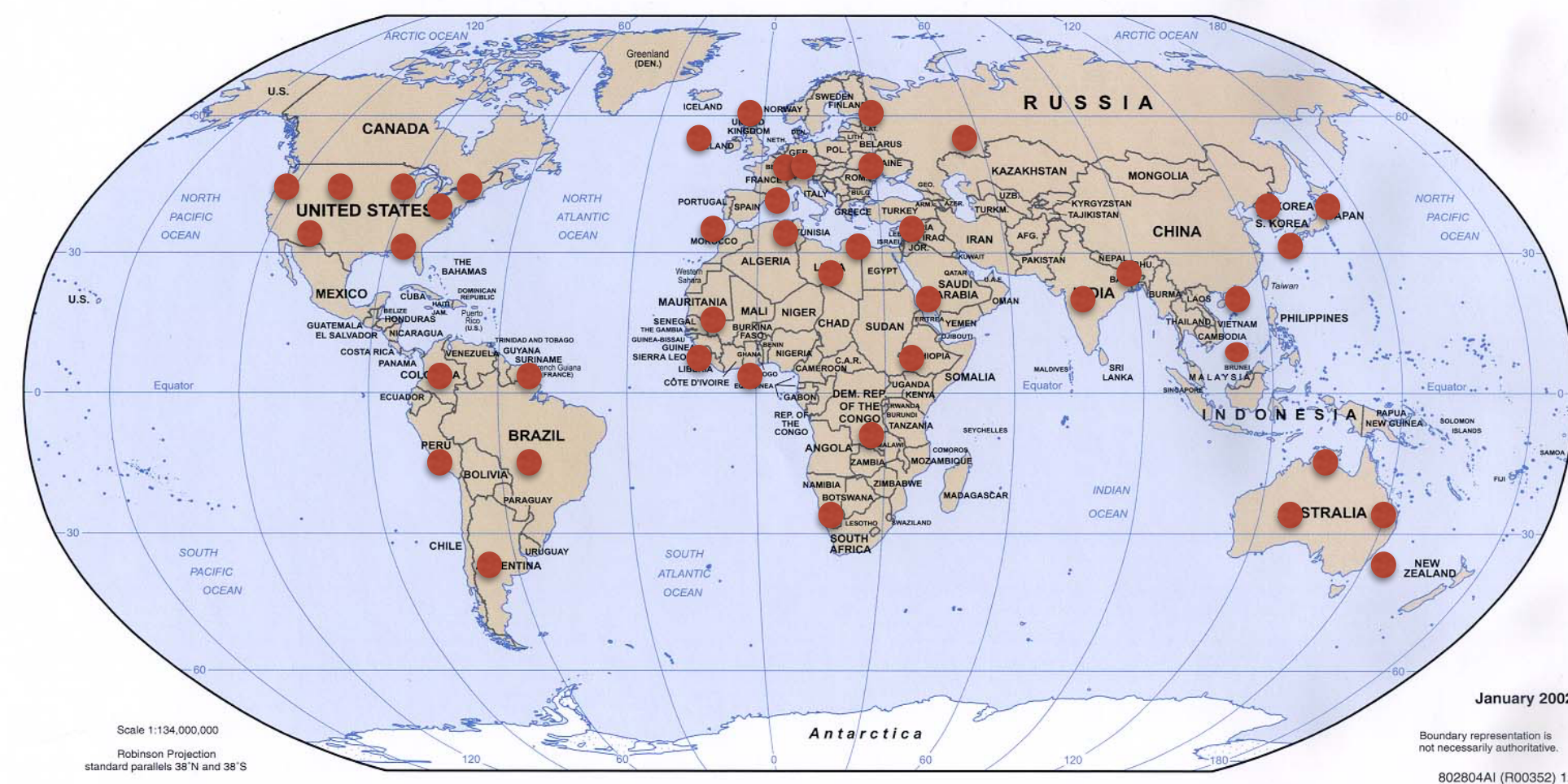


Innovation by iteration



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 experiments

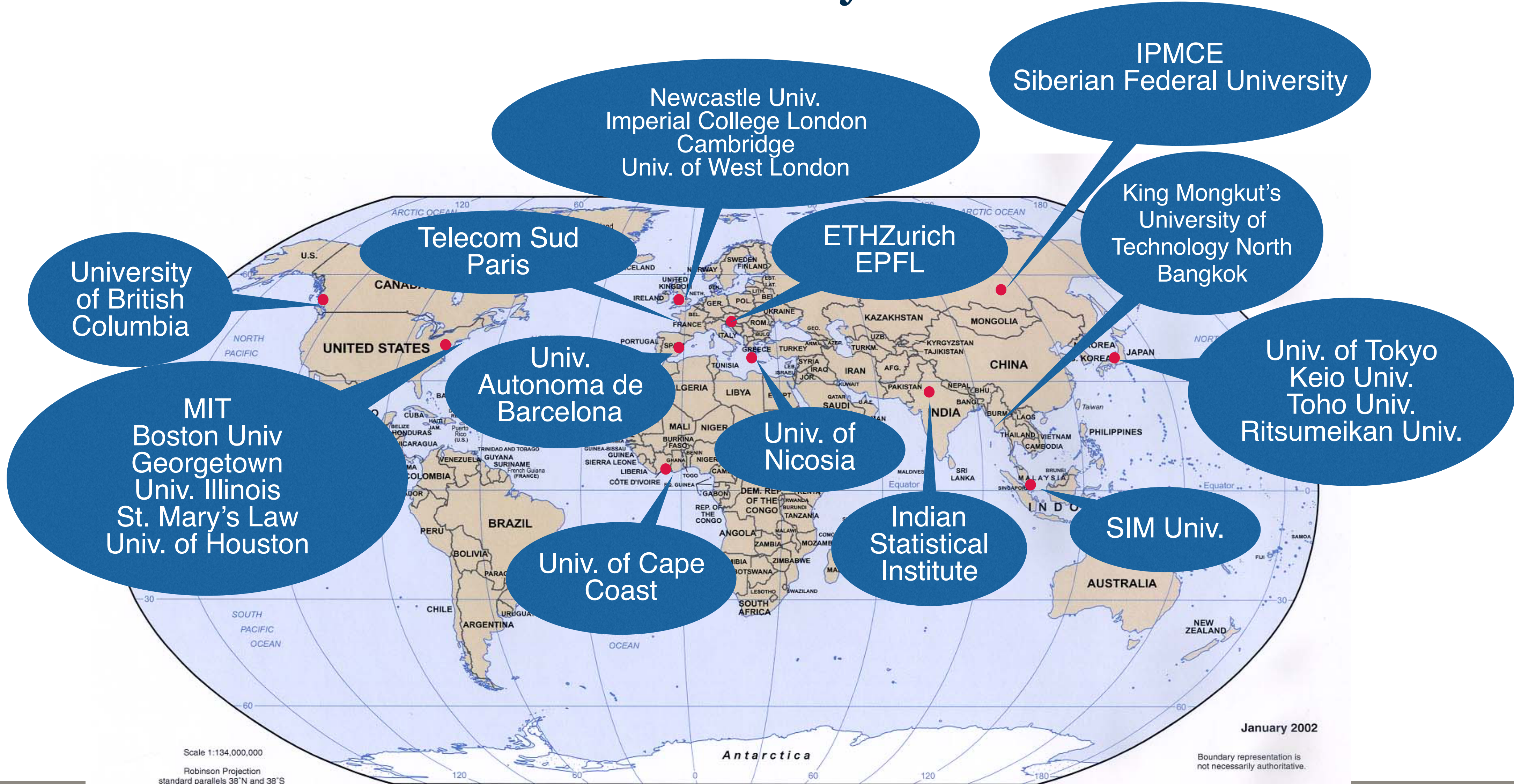
The place of neutrality

The place of diversity

The place of international collaboration

The number of university: > 15K, scalable!

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



Scale 1:134,000,000
Robinson Projection
standard parallels 38°N and 38°S

January 2002
Boundary representation is
not necessarily authoritative.
802804AI (R00352) 12-01

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)**

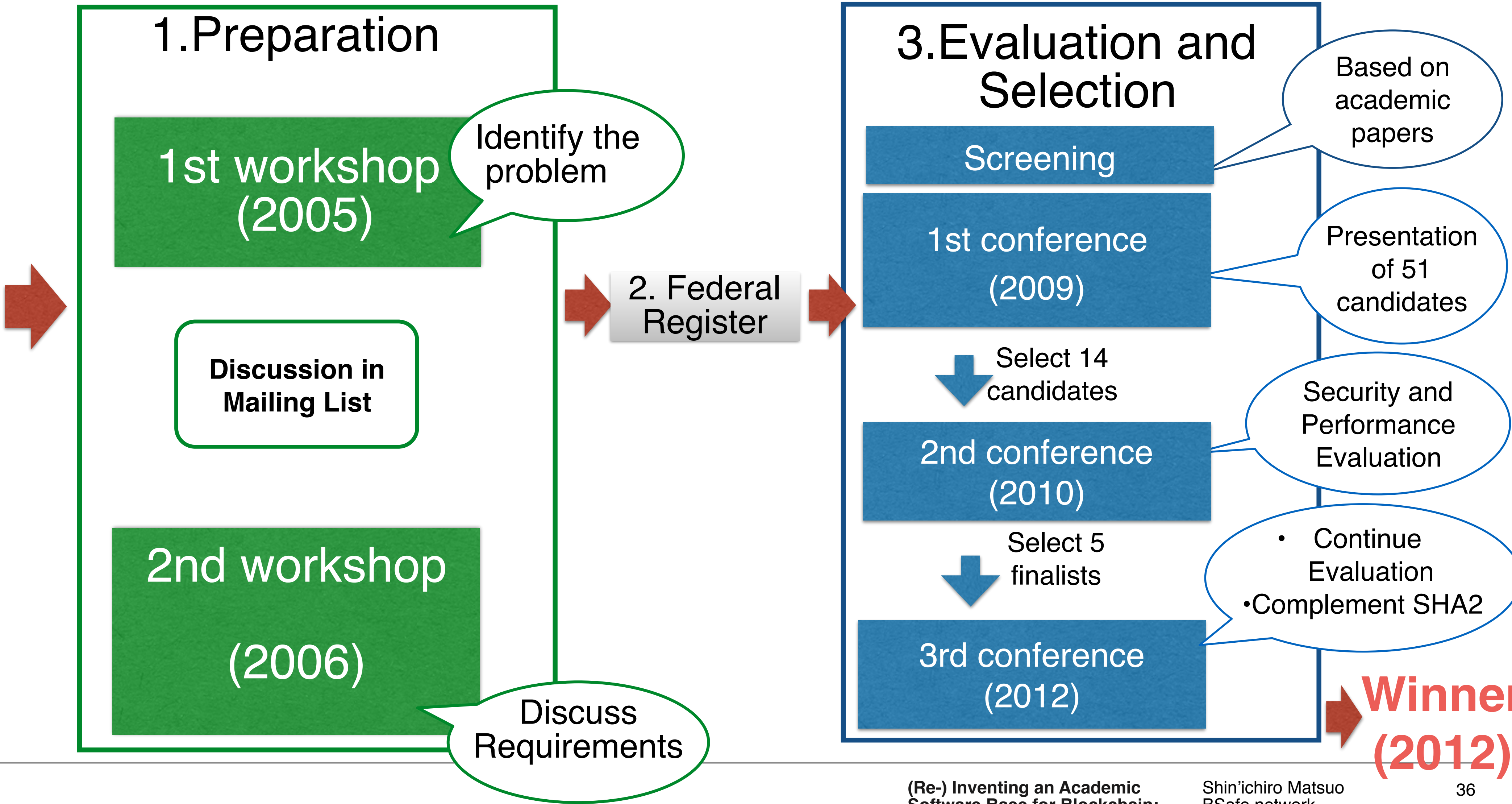
- Alternative to SHA2
- Open competition from international researchers
- Same as the AES competition
- Succeeded in making technology consensus by its careful process

NIST's and cryptographer's Intention for SHA-3 Competition

- The competition promotes the research on Hash function.
- Same as AES competition: We had much research results and knowledge from the competition.
- We didn't have sufficient knowledge on secure Hash function.
- Even if SHA-1 was compromised, NIST had SHA-2 as a alternative.
- However, SHA-2 has similar structure as SHA-1 (MD construction)
- We needed to consider another option.
- To have well studied technology and implementation
 - Not only security evaluation, but also implementation evaluation

Steps of SHA-3 Competition

Compromise of Standard Hash (2004)



Philosophy in SHA-3 Competition

- Open and public discussions
- Setting technical requirements
- Security and performance evaluation
- Using mailing list and wiki
- Cooperation with academic community
- Refer peer reviewed papers
- NIST SHA3 conferences were co-located with top conferences
- Requirements and evaluation criteria are consistently given by NIST.

Best Practice from SHA-3 Competition

1. Open discussion and public verifiability are key to fairness
2. Followings should be defined for good consensus.
 - Firm requirements
 - Evaluation criteria
 - Evaluation platform
 - Target applications and platform
3. Cooperation with academic community is important for trust and consent.
4. Aiming design diversity is good for long-term stability.

Layer 2 Competition for Blockchain

Two categories of competitions

Layer 2 Protocol Proposal

New protocol and implementation of Layer 2 technology to enhance scalability, privacy and security, and their trade-offs

Layer 2 Measurement method and tool

Measurement mechanisms

Standard dataset for evaluation

Goal of Layer 2 Competition

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++



Sponsors

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
- Program Co-chairs:
Shin'ichiro Matsuo (Georgetown University),
Tadge Dryja (MIT DCI)
Program committee members: TBA



Call for
Papers

Bitcoin Edge Dev++

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



Bitcoin Edge

NONPROFIT INITIATIVE

In recent months, through our communication with past **Scaling Bitcoin** sponsors and event participants about what problems they are experiencing that Scaling Bitcoin should focus on, we have received one message repeatedly - "Lack of talent". Organizations that want to participate in and integrate with the Bitcoin ecosystem face great difficulty recruiting developers with relevant expertise.

We are launching a new initiative called "Bitcoin Edge" to address this talent deficit. This initiative will run for the first time in Silicon Valley as the Tutorial Track called "Dev++" alongside the upcoming Scaling Bitcoin 2017 Scaling the Edge

Bitcoin Edge Dev++ Tutorial is meant to focus on scaling the development capacity of the ecosystem via education of developers in the field of cryptocurrency and helping the industry streamline the process of developer training. The primary focus of this tutorial will be a basic first-principles introduction to cryptocurrency as well as cryptocurrency-specific engineering methodologies, security practices, and standard operating procedures.

More information

<https://tokyo2018.scalingbitcoin.org>

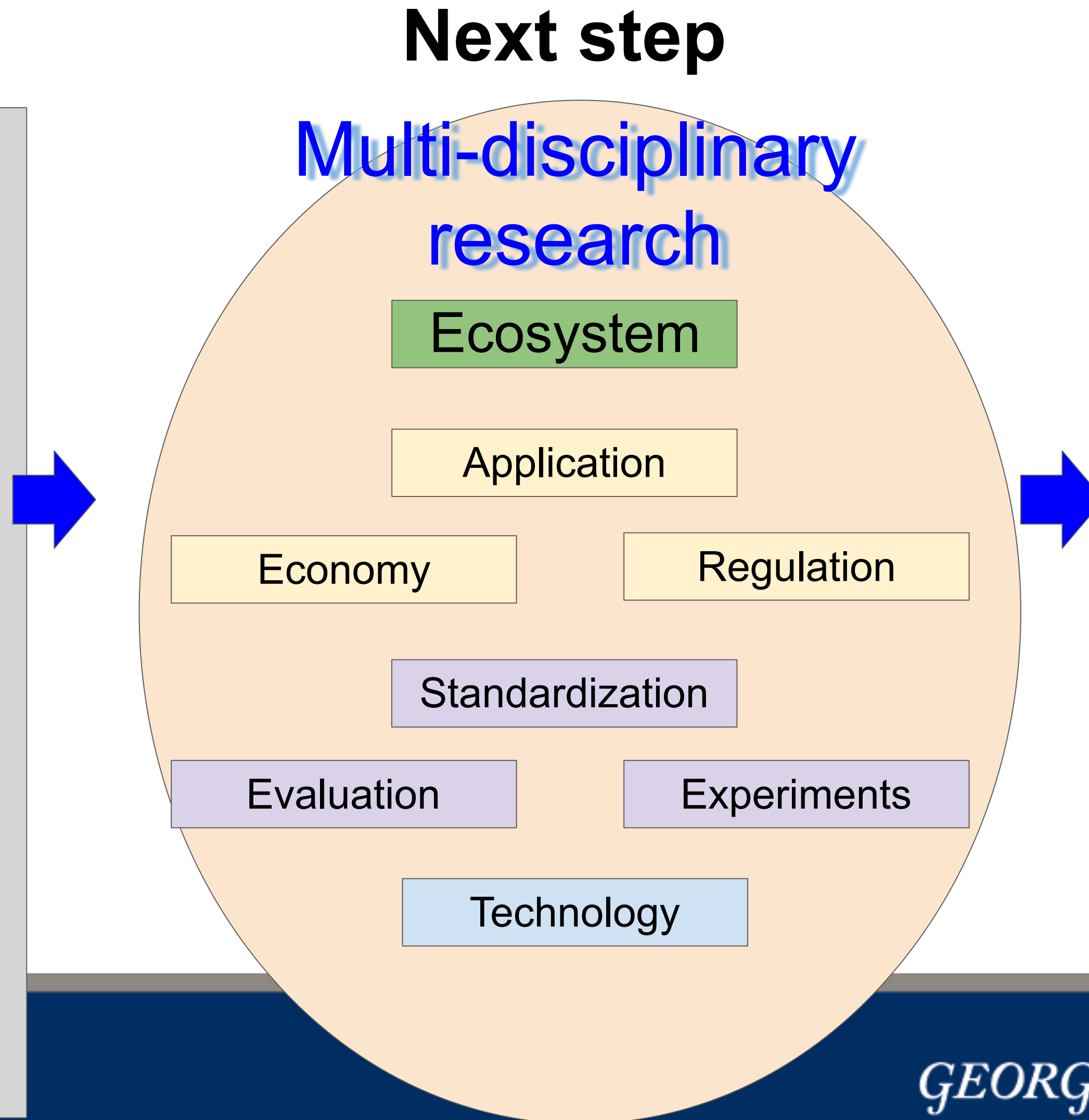


The next step of Blockchain R&D

From tons of experiments to new ecosystem design

- 2017

- Tons of experiments to seek use cases
 - Few use cases with utilizing merit of public blockchain
 - Limitation of technology
- Gap between expectation and real
- Regulation Issues
 - ICO
 - Much scams
- Governance of public blockchain
 - Bitcoin scalability
 - Many forks and chaos
- Many less-focused consortiums

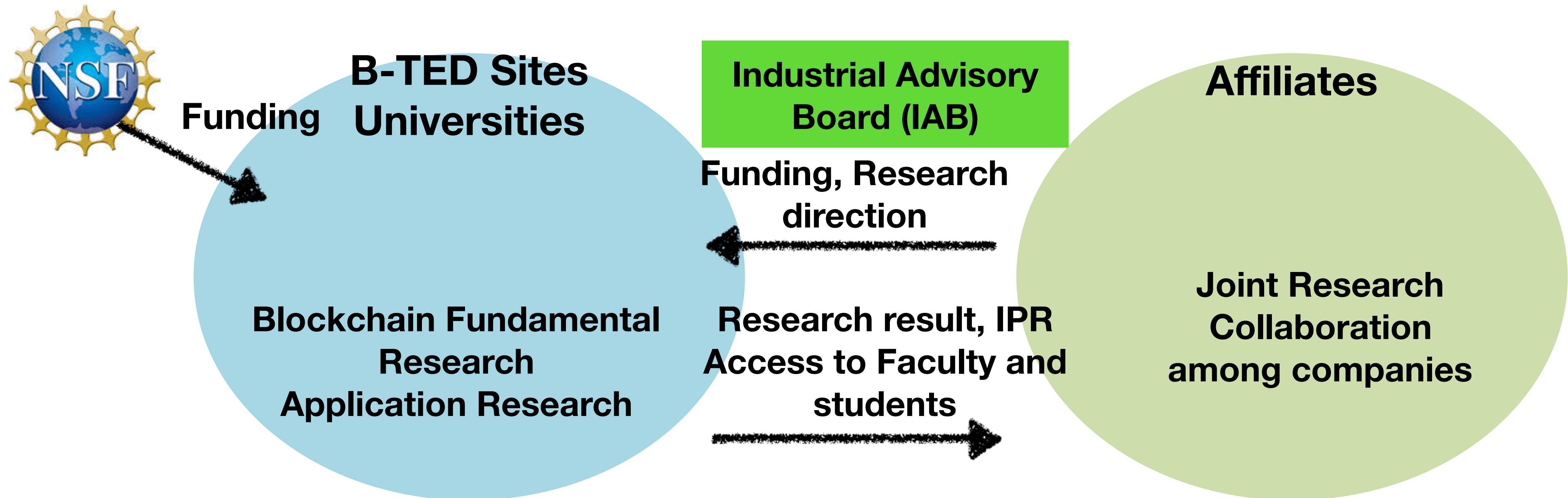


Goal

Becoming the Internet like innovative platform and ecosystem

- Permissionless
- Cross-border
- Web of business and applications
- Vertical over new horizontal

Blockchain Technology and Ecosystem Design (B-TED) Research Center



Goals of B-TED

- Be a trusted Industrial - academic research platform and anchor
 - NSFNet and BSD for Blockchain
 - Provide independent, academic and neutral evaluation criteria for Blockchain technology
- Provide research results and IPR to Affiliates
 - Multi-disciplinary research, International connection
 - Technology and ecosystem design: tech, economics, legal and connection to industry, government and regulators
 - Applications and its deployment
- Contribution to Standardization
 - IETF, ISO, IEEE, etc.

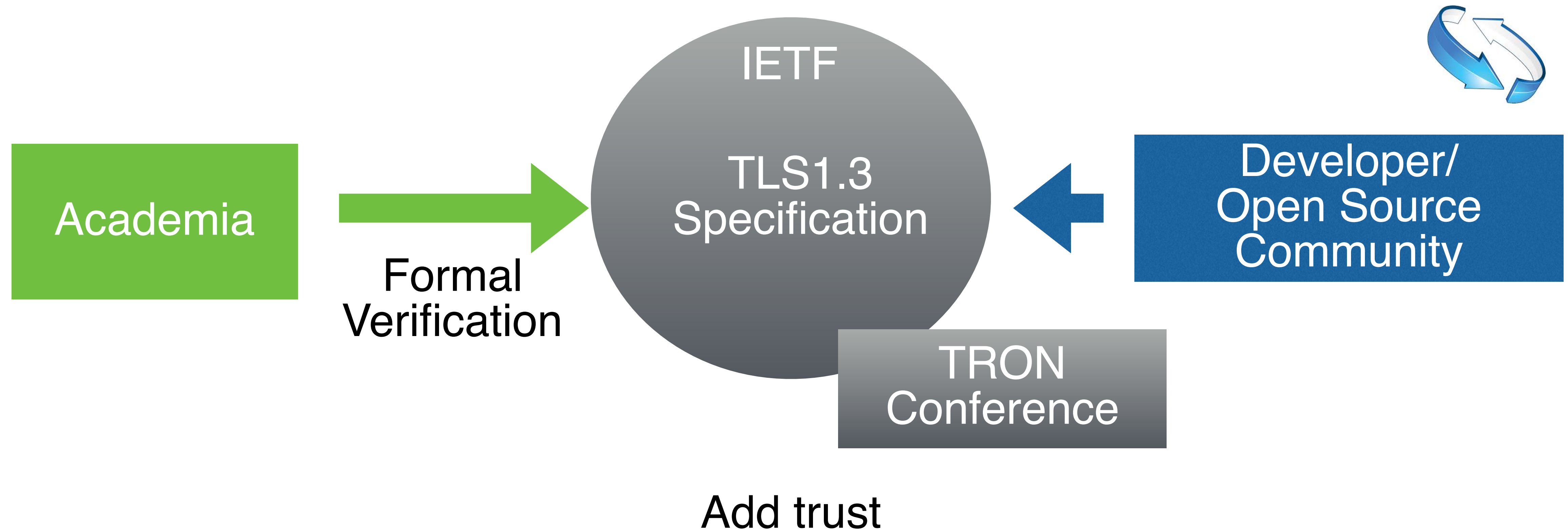
Member Universities

- Georgetown University (Leader)
- University of Houston
- University of Central Florida
- and more ...

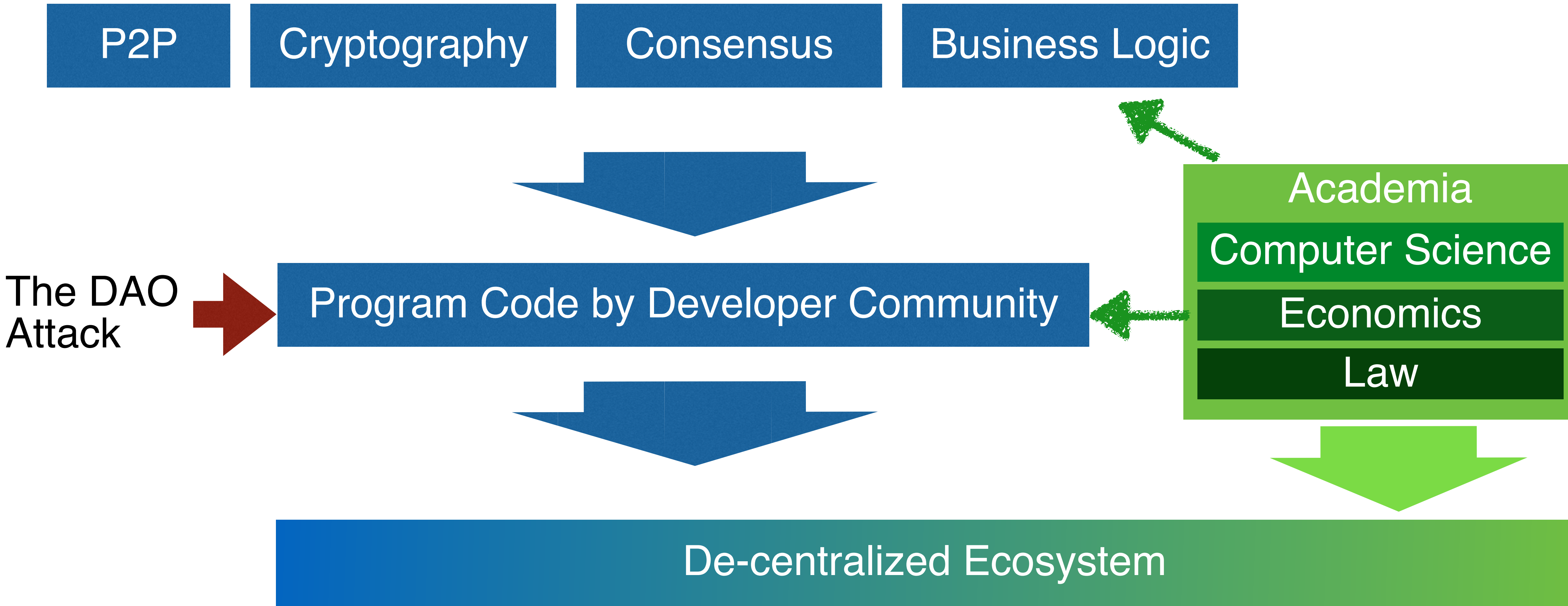
Examples of research projects

- Foundation of Blockchain
 - Evaluation -> Common criteria for Due-diligence
 - Game Theory and security economics
 - Open Source Community organization
- Applications of Blockchain
 - New forms of finance and economy
 - Blockchain x Security
 - Blockchain x Supply Chain and Logistics
 - Blockchain x IoT, Fog
 - Blockchain x Medical Record and Insurance

Practice from the Development of TLS1.3



Decentralization by Diversity



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

Thank you!



GEORGETOWN UNIVERSITY

