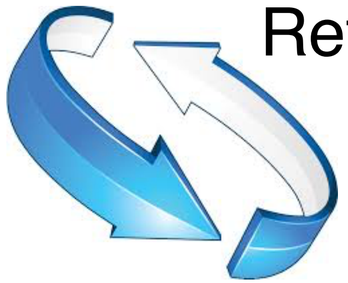
# How academia can help maturing blochchain technology and Ecosystem

Shin'ichiro Matsuo and Paul Brigner
B-TED Research Center, Georgetown University

XC2: Blockchain for Supply Chain and Logistics Forum


GEORGETOWN UNIVERSITY

# How Mature?



Refinement by iteration

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

# Several huge incidents


Mt. Got


The DAO Attack
(50M)

Coincheck

Selfish Mining


Monacoin

# 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.**

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

**Regulation: Recent hot topic**

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**




BSafe network

GEORGETOWN UNIVERSITY

# History of Berkeley Software Distribution (BSD) UNIX

AT&T Unix

Came to Berkeley

Beginning of BSD Unix

Ultrix (DEC)

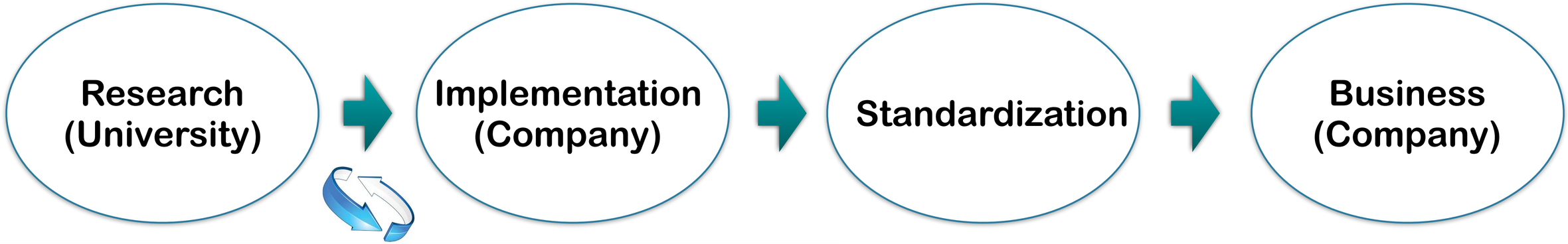

SunOS

4.4 BSD Lite Release 2

1969 1974 1977 1990 1995

# Academic Research is still needed

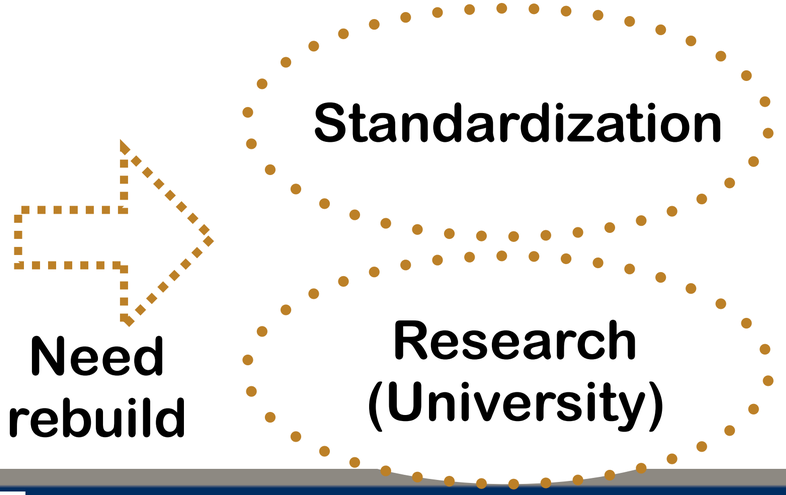
**The Case of Internet Technology**




"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


9

# Why is university the good place?

**The place for experimentation**

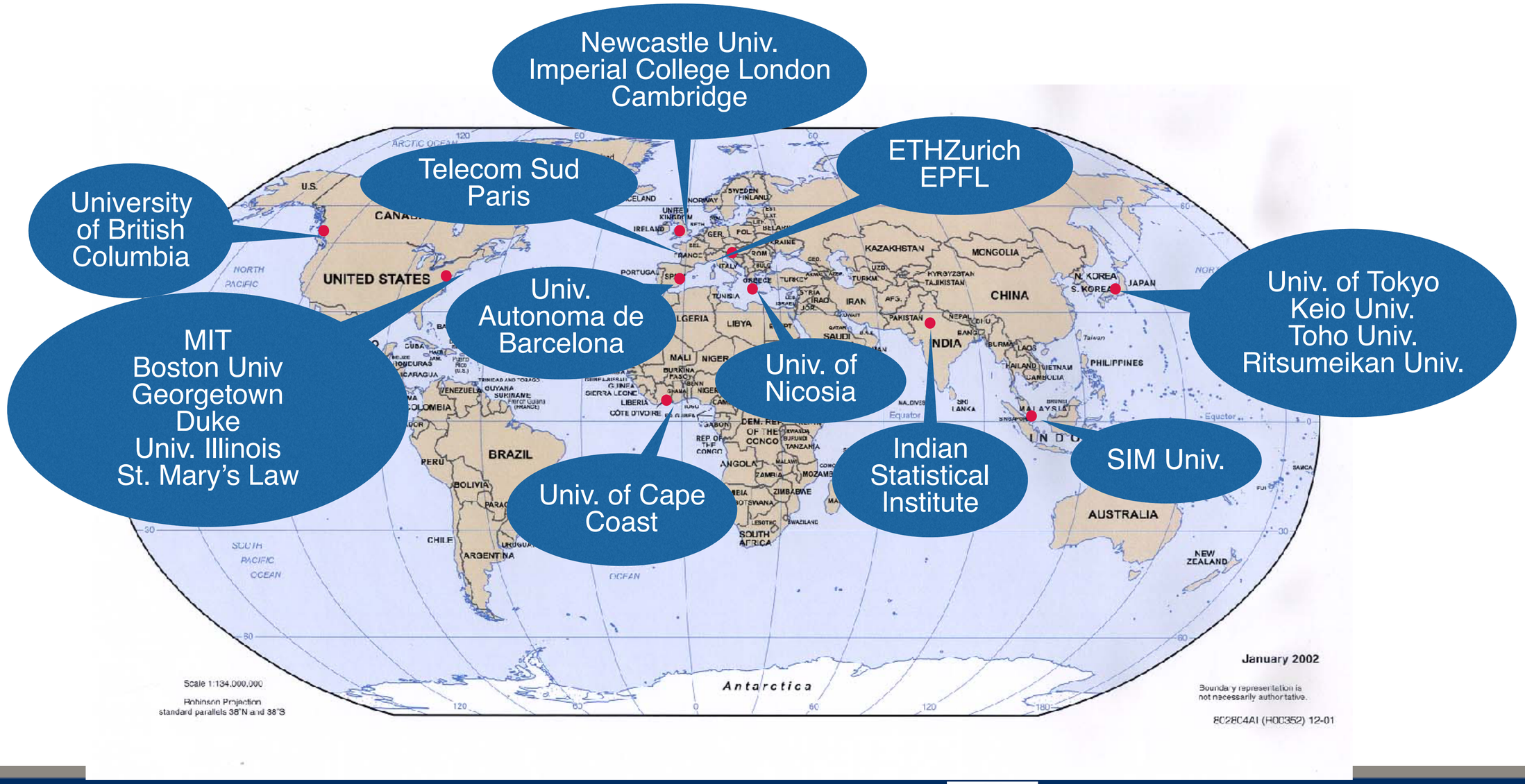
**The place of neutrality**

**The place of diversity**

**The place of international collaboration**

**The number of university: > 15K, scalable!**

# 27 International Universities Already Join and We Add More…






BSafe network

GEORGETOWN UNIVERSITY

# Example of Research Project: Sensor Network and Blockchain

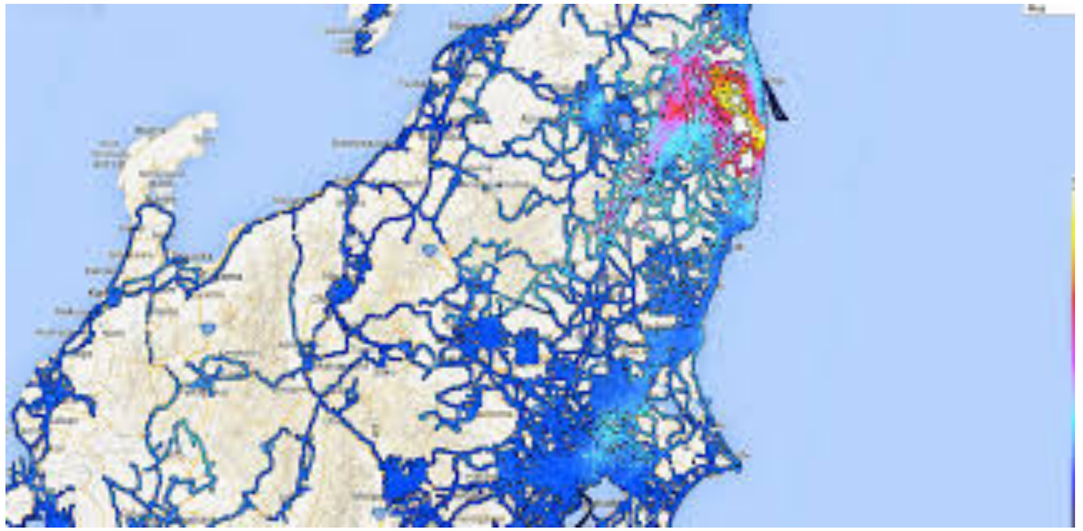
**Collaboration with Safecast: citizen science project**

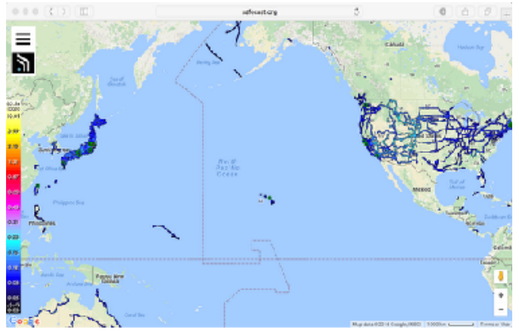
SAFECAST

**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**

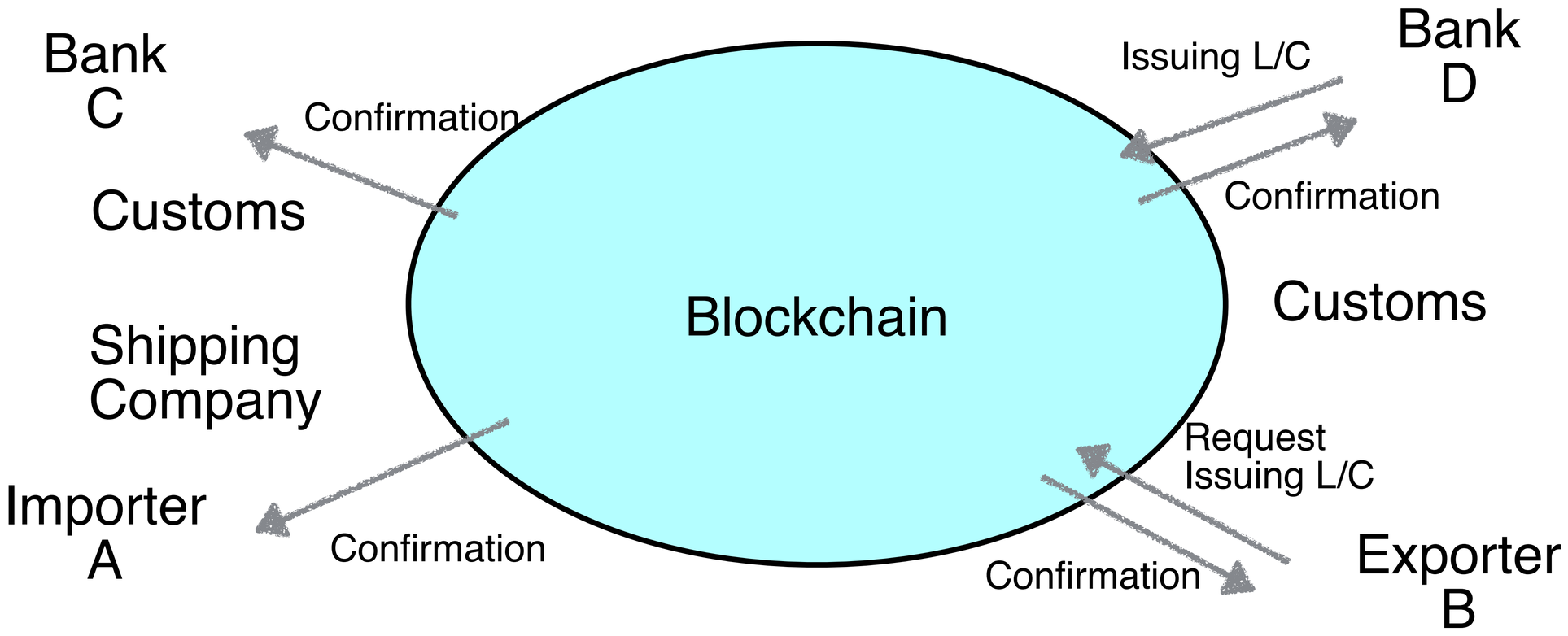
# Designing Domain Specific Language

**To limit possible execution states, which include “insecure” state, create new domain specific language**

Has enough capability to write business logic

Suitable for formal verification

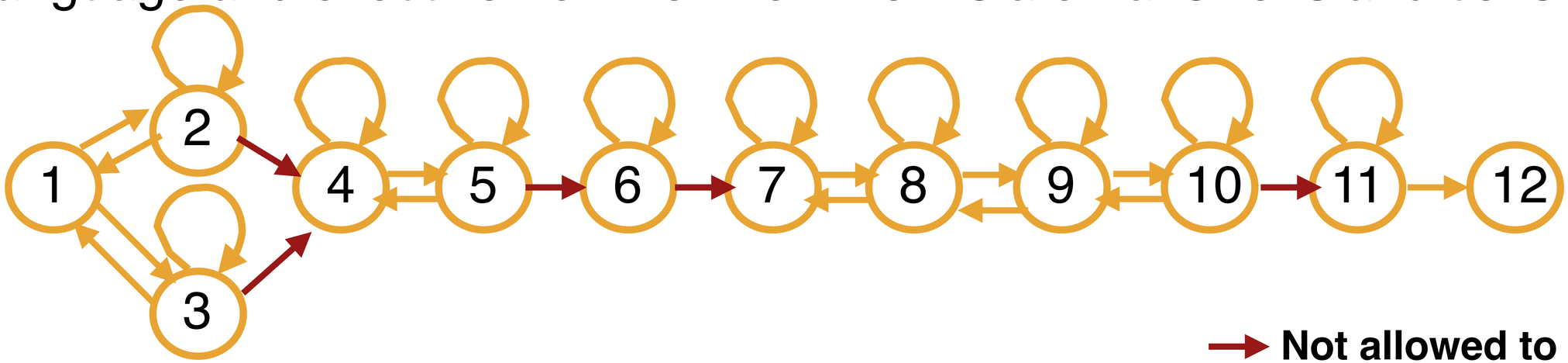
# Letter of Credit (L/C) and Trade Finance over Blockchain



# State Transitions of common process of L/C

Four variables for state representation: Contract, L/C, Payment, Shipment

Create language and execution environment from state transitions and constraints




→ **Not allowed to reverse**

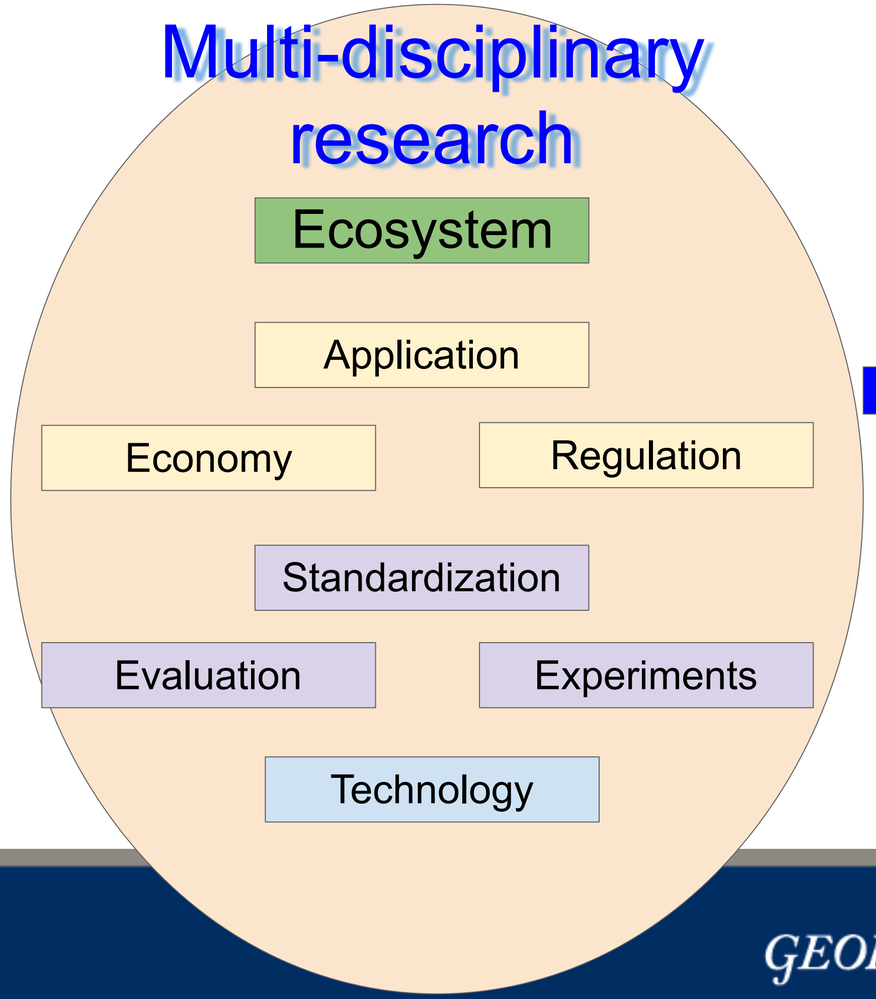
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L/C | Init | Init | Init | Init | Issue Req | Issue Req | Issued | Issued | Issued | Confirmed | Confirmed | Confirmed |
| Cash | Init | Init | Init | Init | Init | Cash Lock | Cash Lock | Cash Lock | Cash Lock | Cash Lock | Settled | Settled |
| Goods | Init | Init | Init | Init | Init | Init | Init | Shipped | Received | Received | Received | Received |
| Contract | Init | A signed | B signed | Both | Both | Both | Both | Both | Both | Both | Both | Fin |

# 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

## Next step

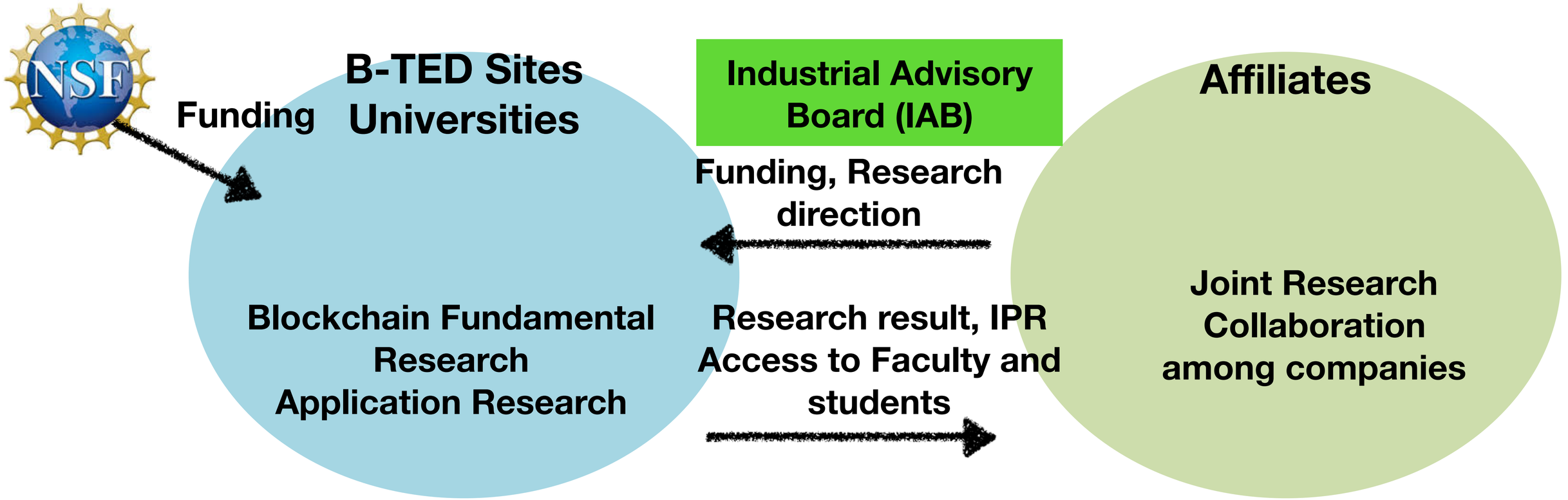



**Goal**

**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.

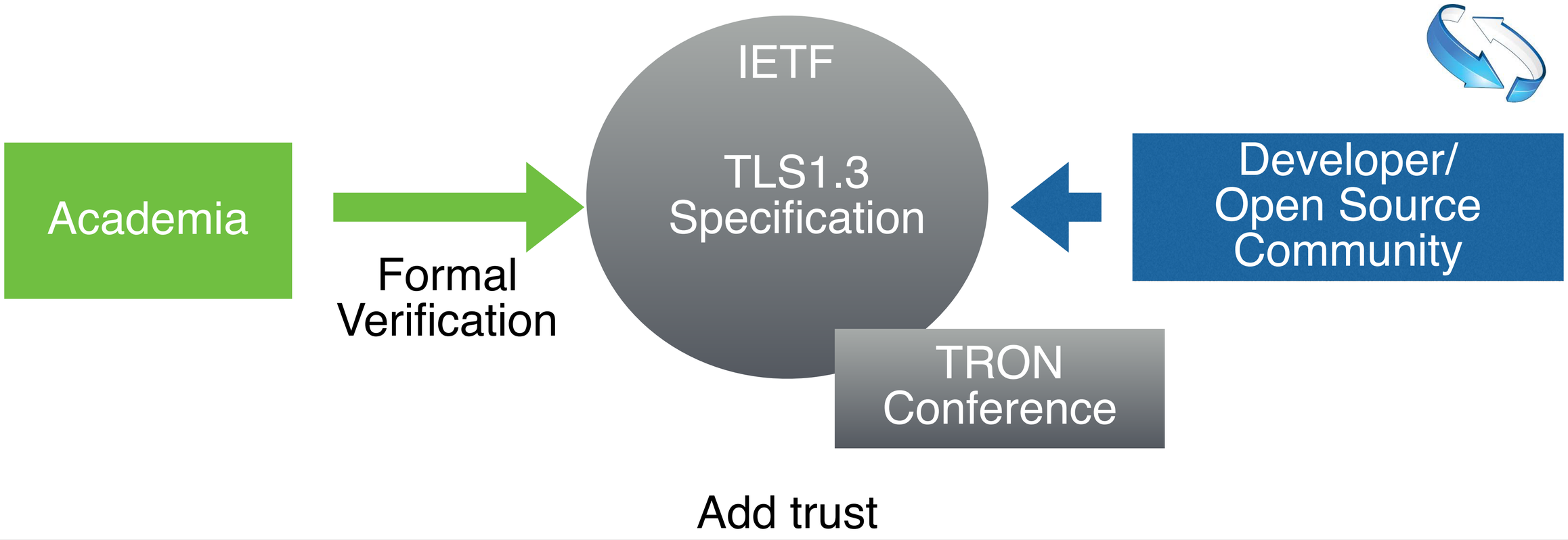
# Member Universities

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

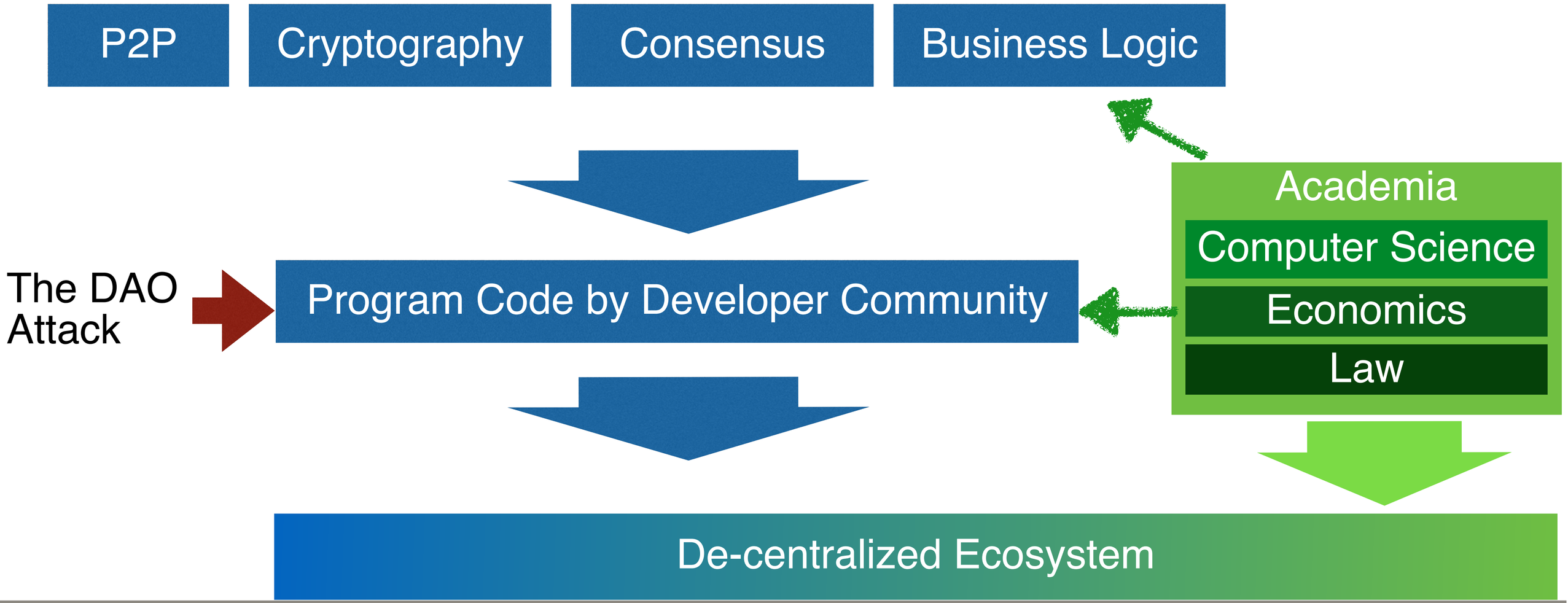
# Examples of research projects

- Foundation of Blockchain
  - Evaluation -> Common criteria for Due-diligence
  - Game Theory and security economics
  - Open Source Community organization
- Application 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



# Thank you!


GEORGETOWN UNIVERSITY