Make Blockchain Mature: academic and multi-stakeholder process

May 15, 2019, Consensus 2019

Shin'ichiro Matsuo, Georgetown University
Blockchain and Technology Ecosystem Design (B-TED) Research Center

GEORGETOWN UNIVERSITY

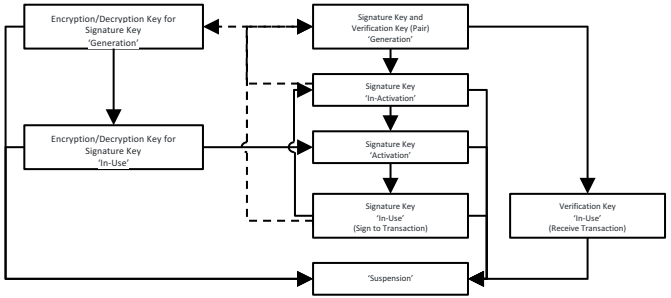
Example of immaturity: Too many mega-incidents

Date	Victim	Value of coin loss
Feb 2014	Mt.GOX (Japan)	$450 Million
Aug 2016	Bitfinex (HongKong)	$77 Million
Apr 2017	Youbit (Korea)	$35 Million
Jan 2018	CoinCheck (Japan)	$535 Million
Feb 2018	BitGrail (Italy)	$170 Million
Jun 2018	Coinrail (Korea)	$40 Million
Sep 2018	Zaif (Japan)	$59 Million
May 2019	Binance (China)	$40 Million

Prompt reaction in Japan: Cryptoassets Governance Task Force (CGTF)

CGTF CRYPTOASSETS GOVERNANCE TASK FORCE

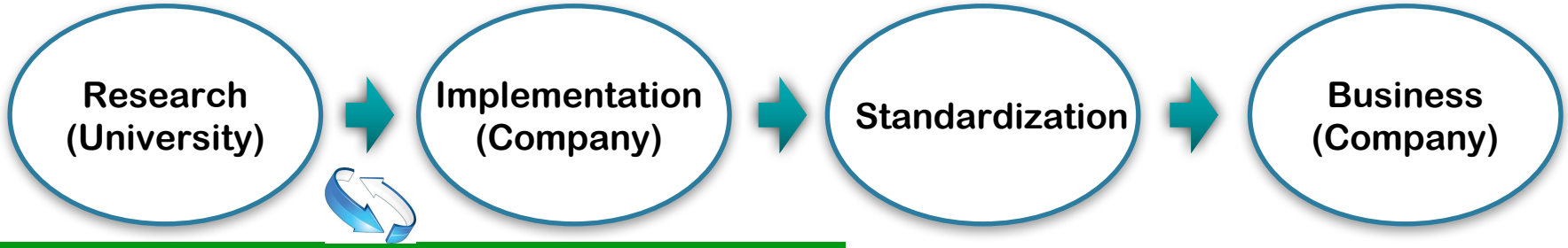
- Initiated right after the Coincheck Incident
- Multi-stakeholder discussion: Engineer, exchanges, business, and academia
- Conducts study on the risk analysis, security consideration and best practices for cryptocurrency exchange (digital asset custodians)
- Cryptographic Key lifecycle management
- Input to ISO TR23576 and IETF I-D



GEORGETOWN UNIVERSITY

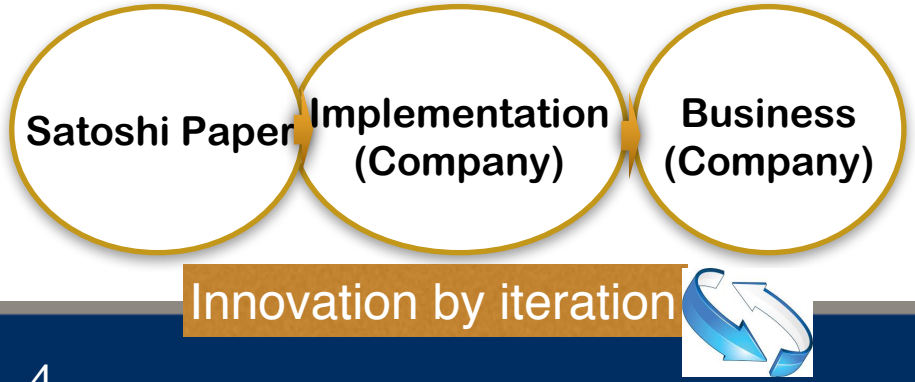
Maturing process: from academia to engineering

The Case of Internet Technology

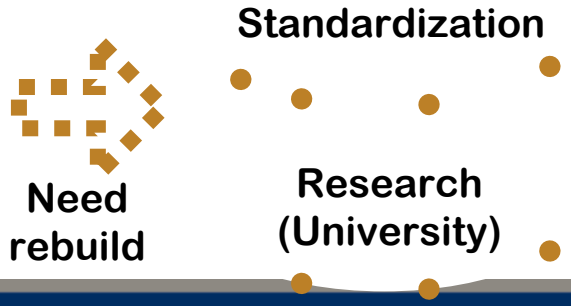


"BSD" and open-source facilitated innovation

The Case of Bitcoin and Blockchain



Innovation by iteration



Layers for security consideration

		Standards
Operation	Key Management, Audit, Backup	ISO/IEC 27000
Implementation	Program Code, Secure Hardware	ISO/IEC 15408
Application Logic	Scripting Language for Financial Transaction, Contract	Secure coding guides
Application Protocol	Privacy protection, Secure transaction	ISO/IEC 29128
Backbone Protocol	P2P, Consensus, Merkle Tree	ISO/IEC 29128
Cryptography	ECDSA, SHA-2, RIPEMD160	NIST,ISO

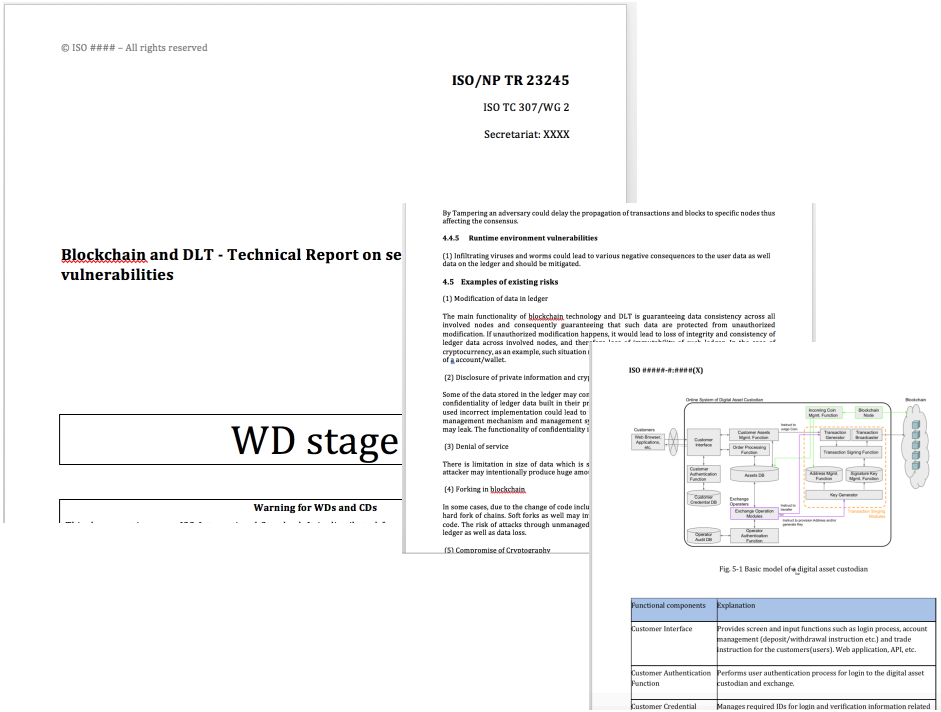
Two technical reports under edited in ISO TC307

- Security risks, threats and vulnerabilities (ISO TR23245)

Application Protocol **Backbone Protocol**

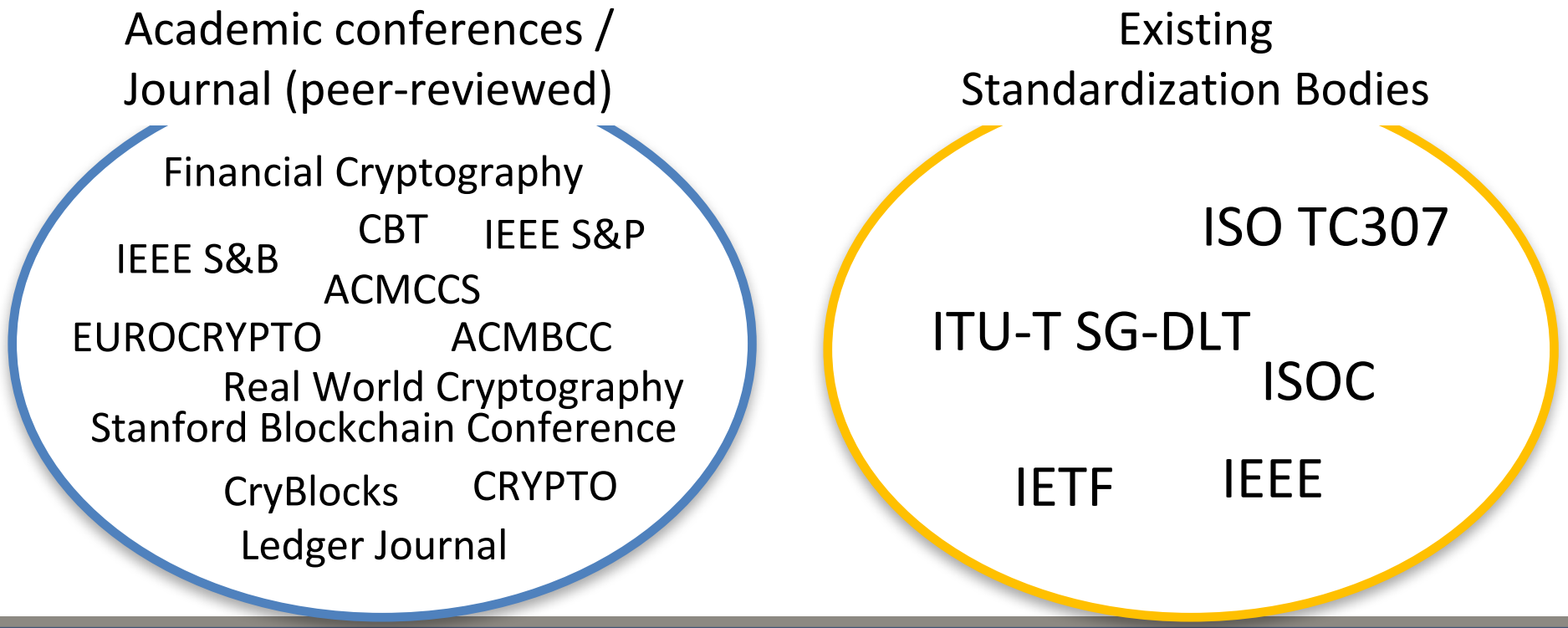
- Security of Digital Asset Custodians (ISO TR23576)

Operation **Implementation**

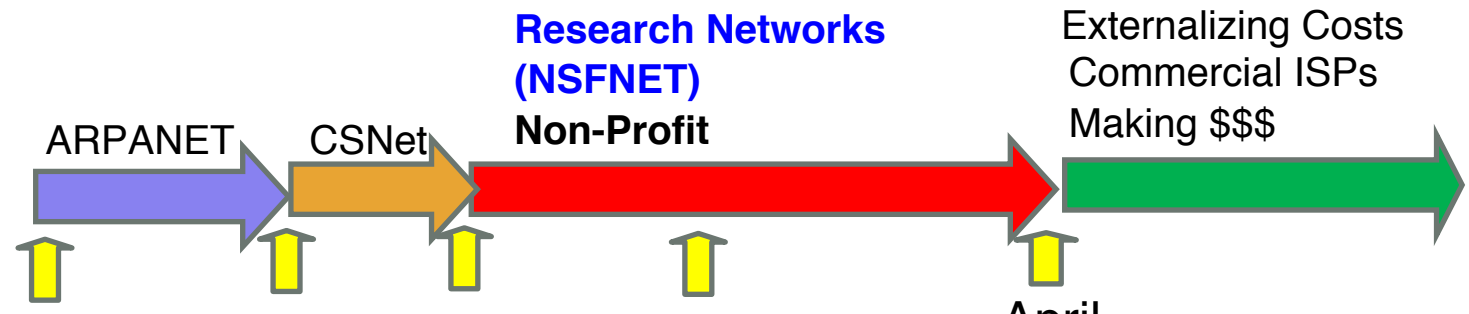


GEORGETOWN UNIVERSITY

Current landscape of academia and standardization bodies



NSFNet and BSD for the Internet



1977 1995

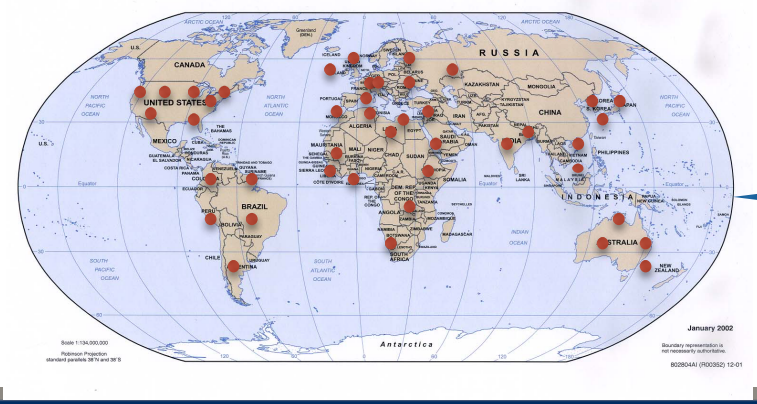
Berkeley Software Distribution (BSD)

NSFNET T3 Network 1992

BSafe.network: Plays the same role as NSFNet and BSD

http://bsafe.network

- **A neutral, stable and sustainable research test network for Blockchain technology by global 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.**

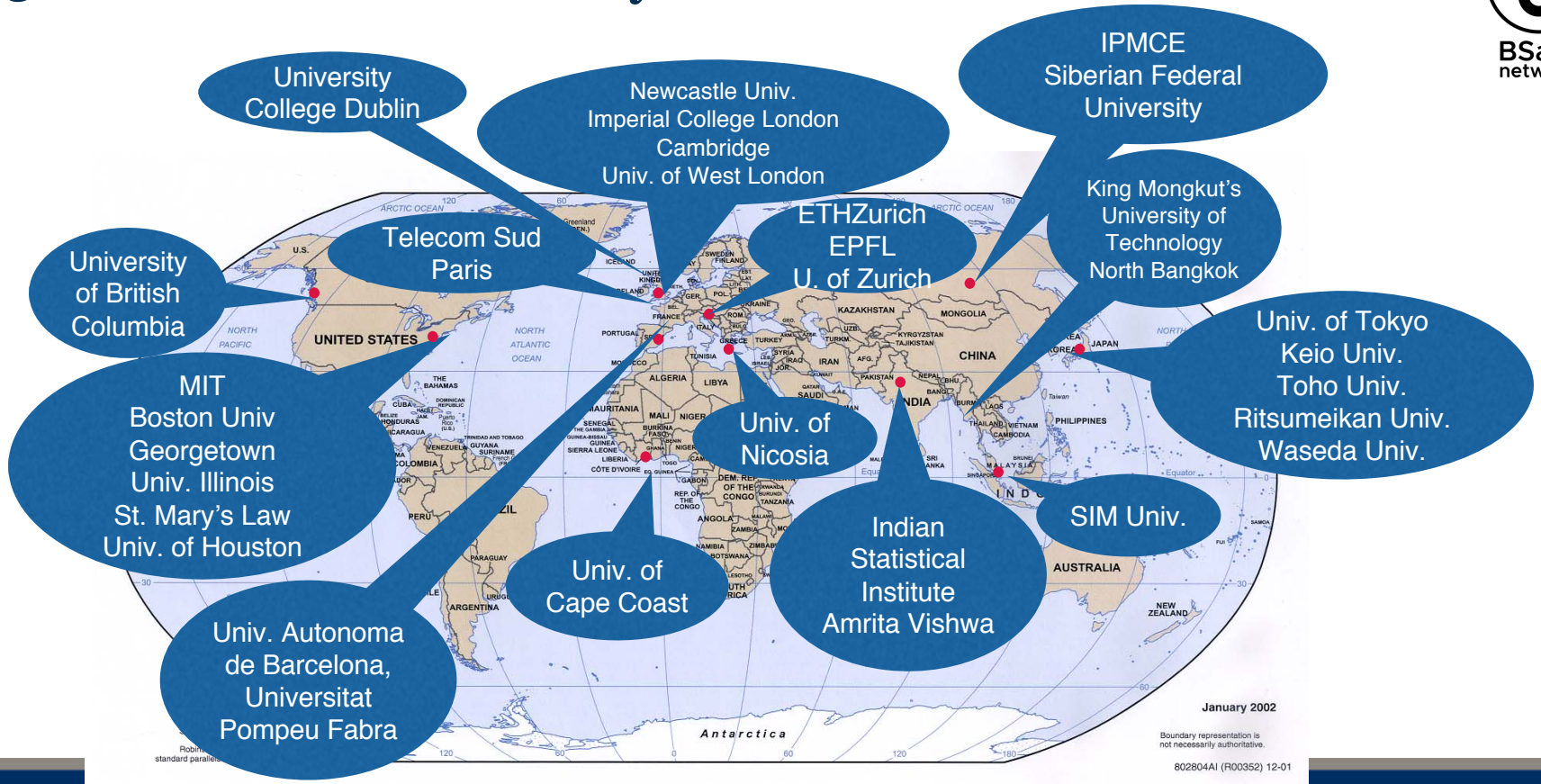


- Neutral platform
- de-anchored trust of Blockchain network
- More nodes (with Neutrality)
- Testbed for academic research

9

31 Universities Already Join and We Add More…

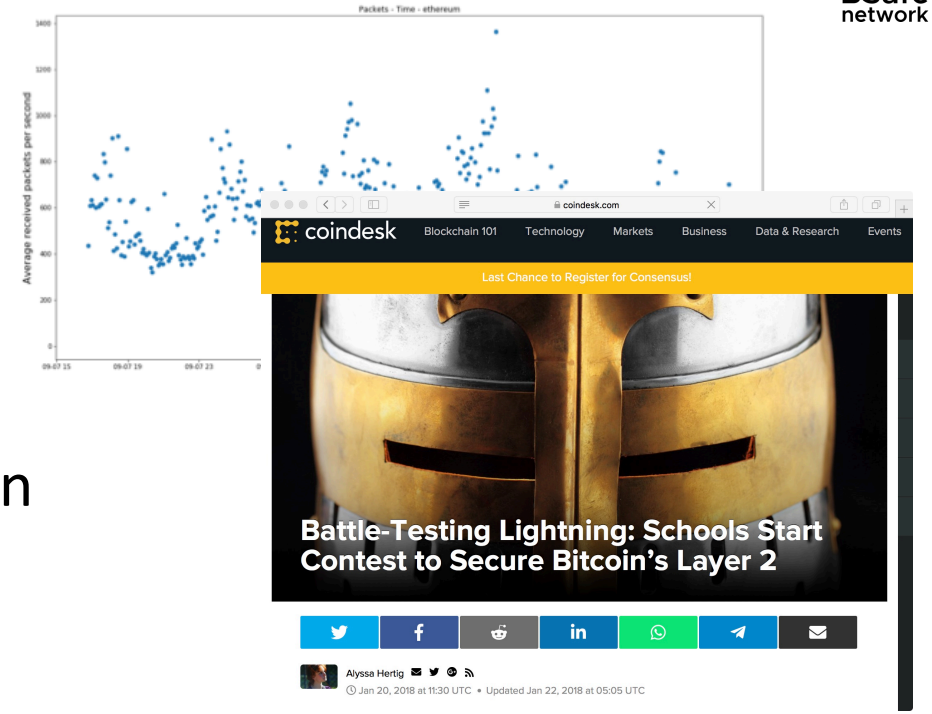
BSafe network



GEORGETOWN UNIVERSITY

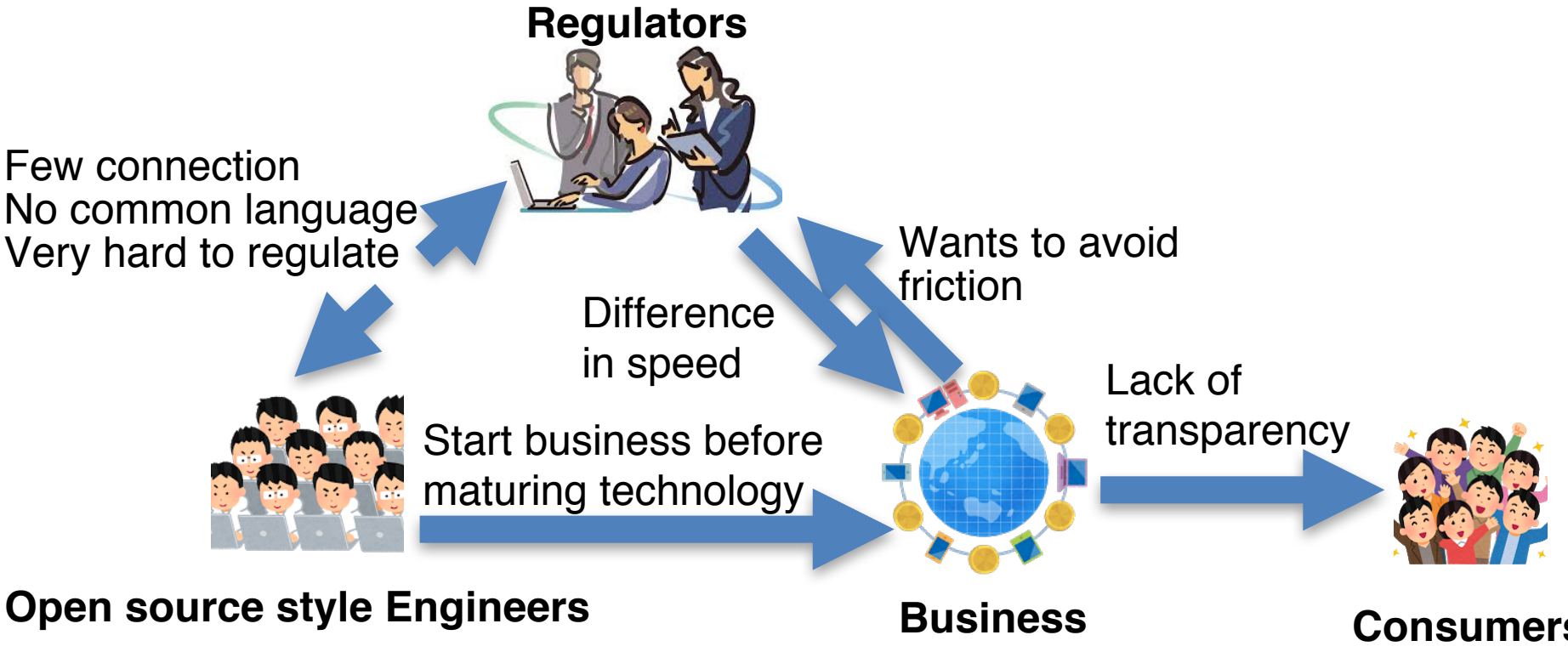
Past/ongoing research over BSafe.network

- Test of segwit
- Monitoring of Bitcoin forks
- Long-term blockchain
- Layer 2 technology competition
- Discussion Forum



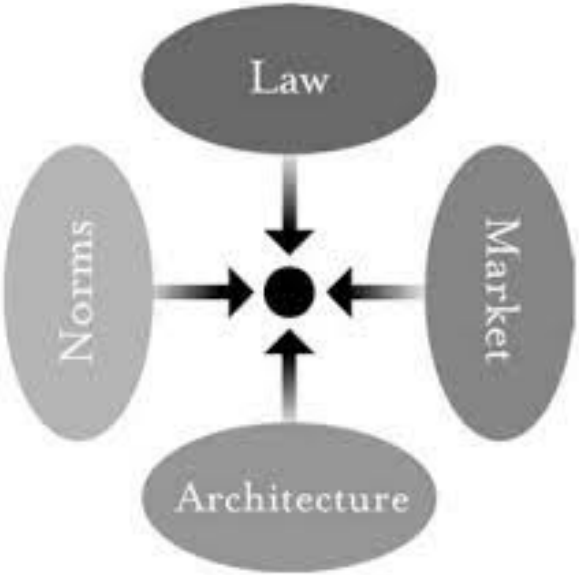
https://www.coindesk.com/battle-testing-lightning-26-schools-start-contest-secure-bitcoins-layer-2

Stakeholders and the Current Situation



Collaboration by Multi-stakeholders Implies Maturity

- Common understandings on regulatory goals
- Code as (a part of) law and order
  - Joint works become create orders for permissionless innovation
- Blockchain and DLT needs multi-disciplinary discussions
  - CS, Cryptography, Network, Economics, Law, etc.



Q & A

GEORGETOWN UNIVERSITY

Shin'ichiro Matsuo
BSafe.network