

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

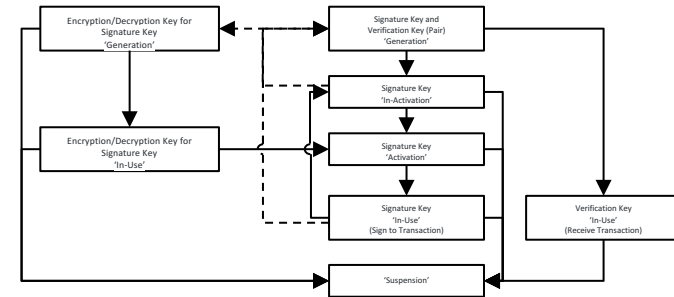
Date	Victim	Value of coin loss
Feb 2014	Mt.GOX (Japan)	\$450 Million
Aug 2016	Bitfinex (HongKong)	\$77 Million
Apr 2017	Youbit (Korea)	\$35 Million
Jan 2018	CoinCheck (Japan)	\$535 Million
Feb 2018	BitGrail (Italy)	\$170 Million
Jun 2018	Coinrail (Korea)	\$40 Million
Sep 2018	Zaif (Japan)	\$59 Million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



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

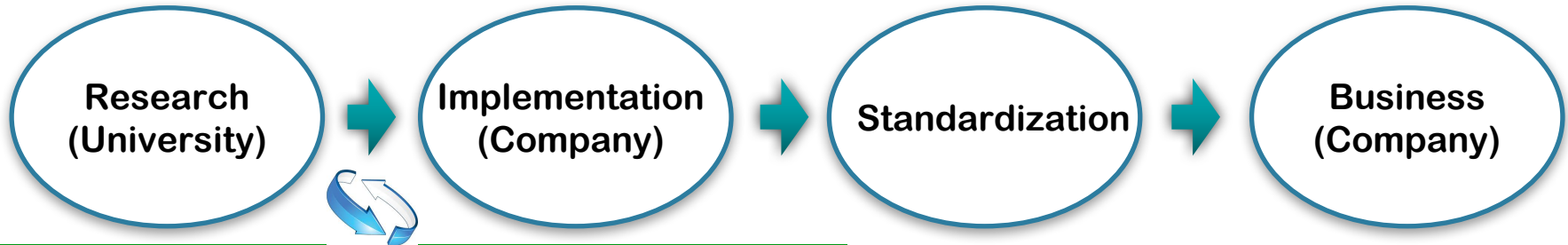


- Initiated right after the Coincheck Incident
- Multi-stakeholder discussion: Engineer, exchanges, business, and academia
- Conducts study on the risk analysis, security consideration and best practices for cryptocurrency exchange (digital asset custodians)
- Cryptographic Key lifecycle management
-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



Maturing process: from academia to engineering

The Case of Internet Technology

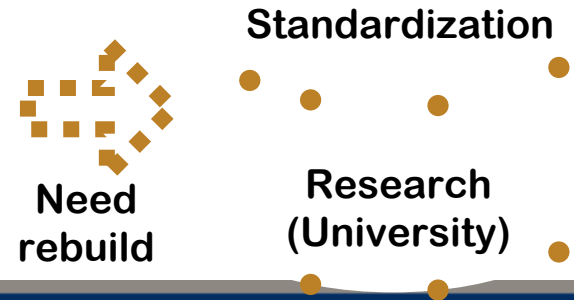


“BSD” and open-source facilitated innovation

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

© ISO ##### - All rights reserved

ISO/NP TR 23245
ISO TC 307/WG 2
Secretariat: XXXX

Blockchain and DLT - Technical Report on security vulnerabilities

WD stage

Warning for WDs and CDs

ISO #####-#####(X)

By Tampering an adversary could delay the propagation of transactions and blocks to specific nodes thus affecting the consensus.

4.4.5 Runtime environment vulnerabilities

(1) Infiltrating viruses and worms could lead to various negative consequences to the user data as well as data on the ledger and should be mitigated.

4.5 Examples of existing risks

(1) Modification of data in ledger

The main functionality of blockchain technology and DLT is guaranteeing data consistency across all involved nodes and consequently guaranteeing that such data are protected from unauthorized modification. If unauthorized modification happens, it would lead to loss of integrity and consistency of ledger data across involved nodes, and therefore, cryptocurrency, as an example, such situation of a account/wallet.

(2) Disclosure of private information and confidentiality of ledger data built in their previous implementation could lead to management mechanism and management of may leak. The functionality of confidentiality of

(3) Denial of service

There is limitation in size of data which is attacker may intentionally produce huge amount

(4) Forking in blockchain.

In some cases, due to the change of codes include hard fork of chains. Side fork as well as code. The risk of attacks through unmanaged ledger as well as data loss.

(5) Compromise of Cryptography

Fig. 5-1 Basic model of a digital asset custodian

Functional components	Explanation
Customer Interface	Provides external and input functions such as login process, account management (deposit/withdraw instruction etc.) and trade instruction for the customers(users). Web application, API, etc.
Customer Authentication Function	Performs user authentication process for login to the digital asset custodian and exchange.
Customer Credential	Manages required IDs for login and verification information related

Current landscape of academia and standardization bodies

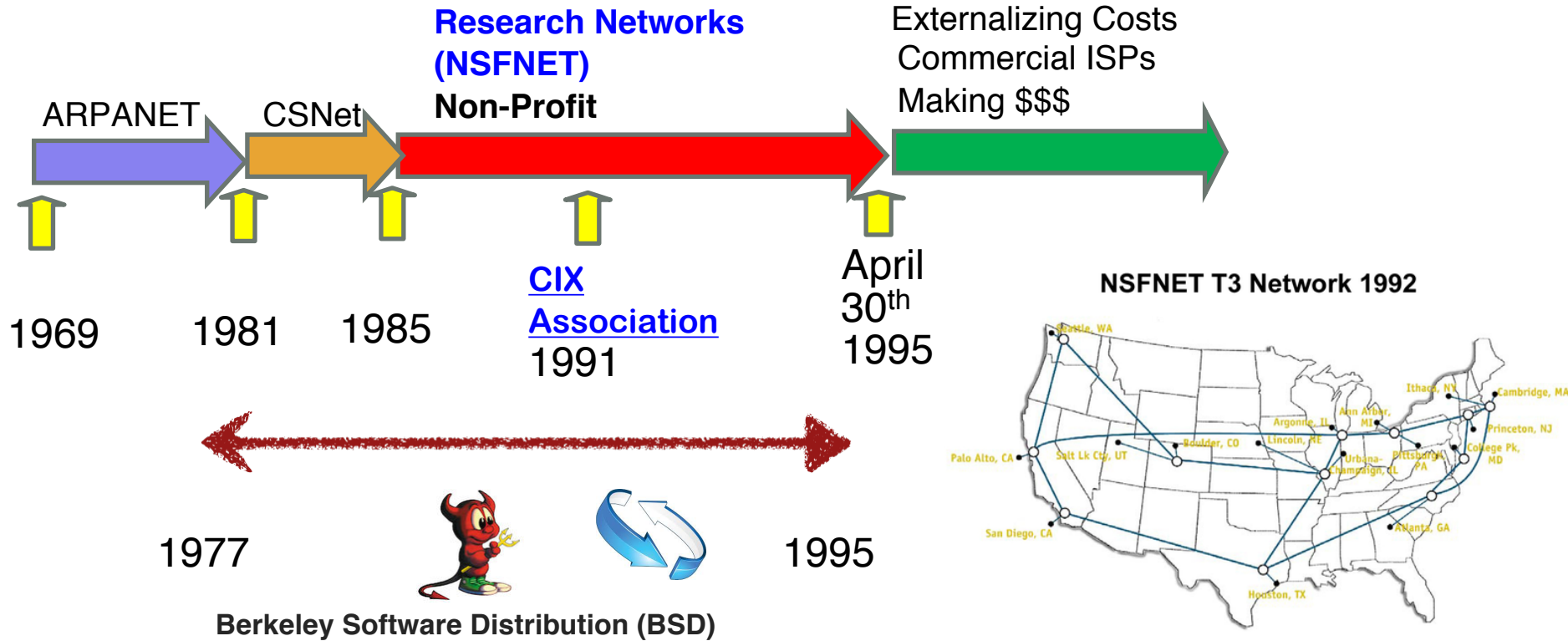
Academic conferences /
Journal (peer-reviewed)

Financial Cryptography
IEEE S&B CBT IEEE S&P
ACMCCS
EUROCRYPTO ACMBCC
Real World Cryptography
Stanford Blockchain Conference
CryBlocks CRYPTO
Ledger Journal

Existing
Standardization Bodies

ISO TC307
ITU-T SG-DLT
ISOC
IETF IEEE

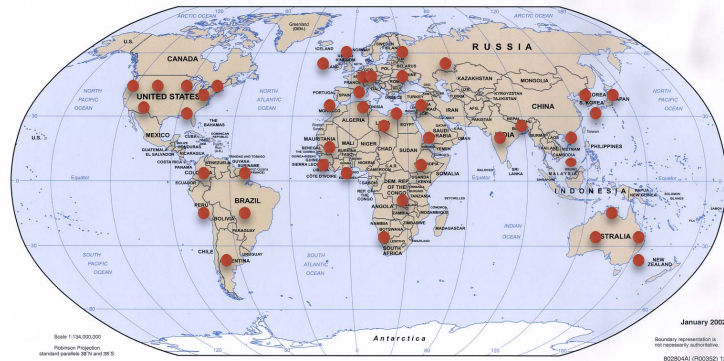
NSFNet and BSD for the Internet



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

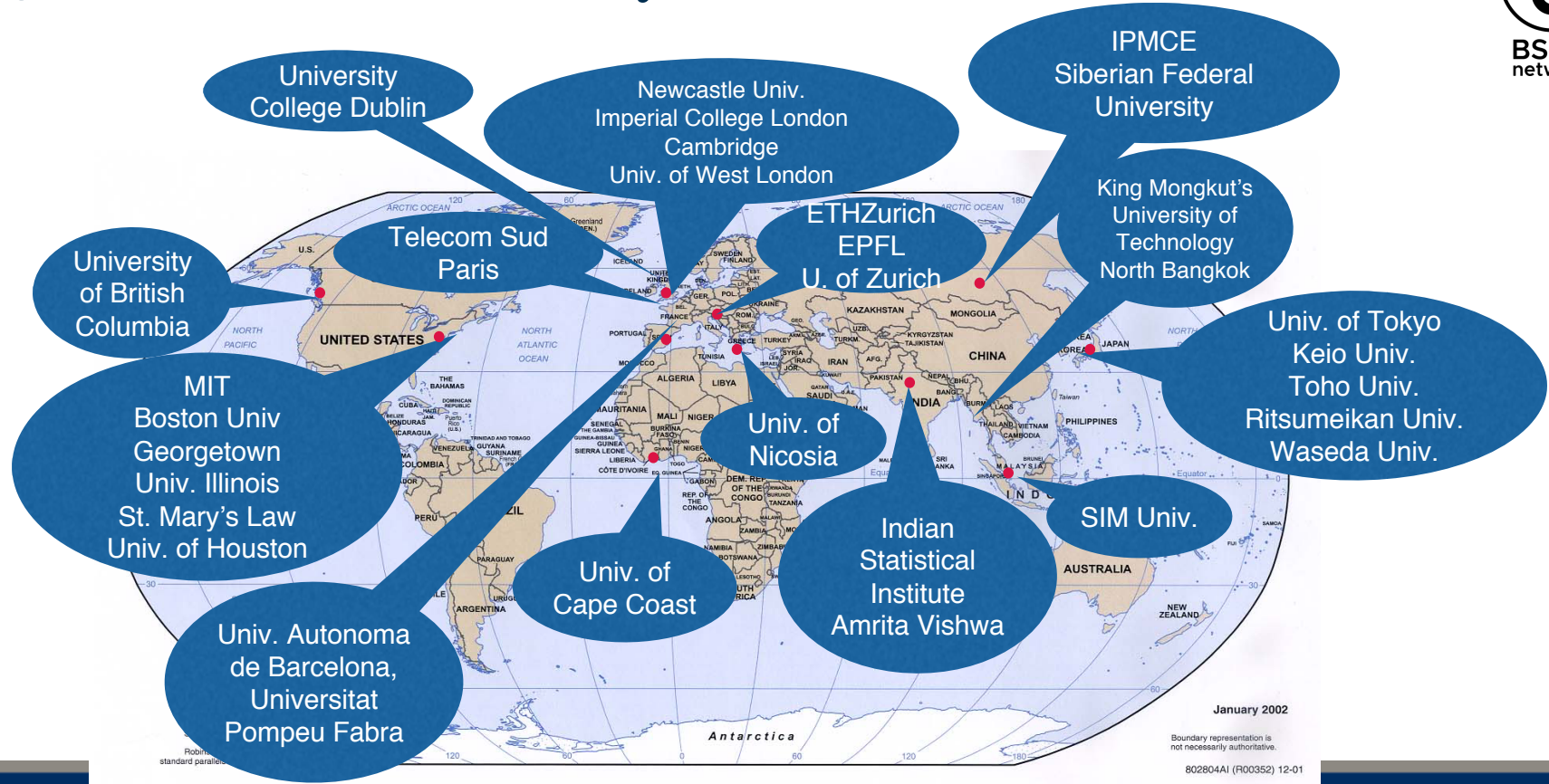
<http://bsafe.network>

- 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

31 Universities Already Join and We Add More...



January 2002

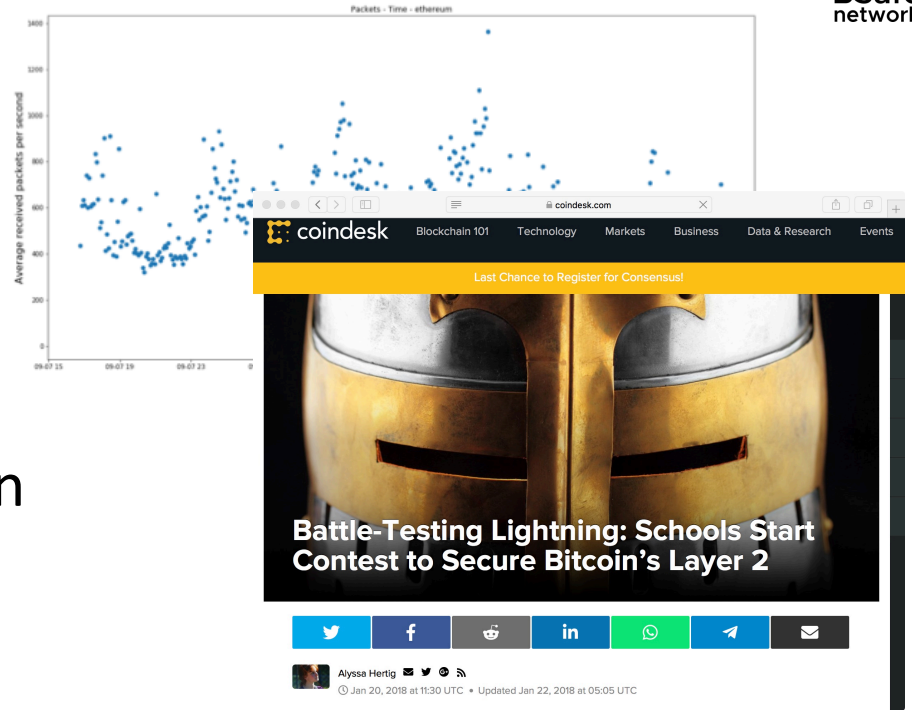
Boundary representation is not necessarily authoritative.

802804AI (R00352) 12-01

Past/ongoing research over BSafe.network

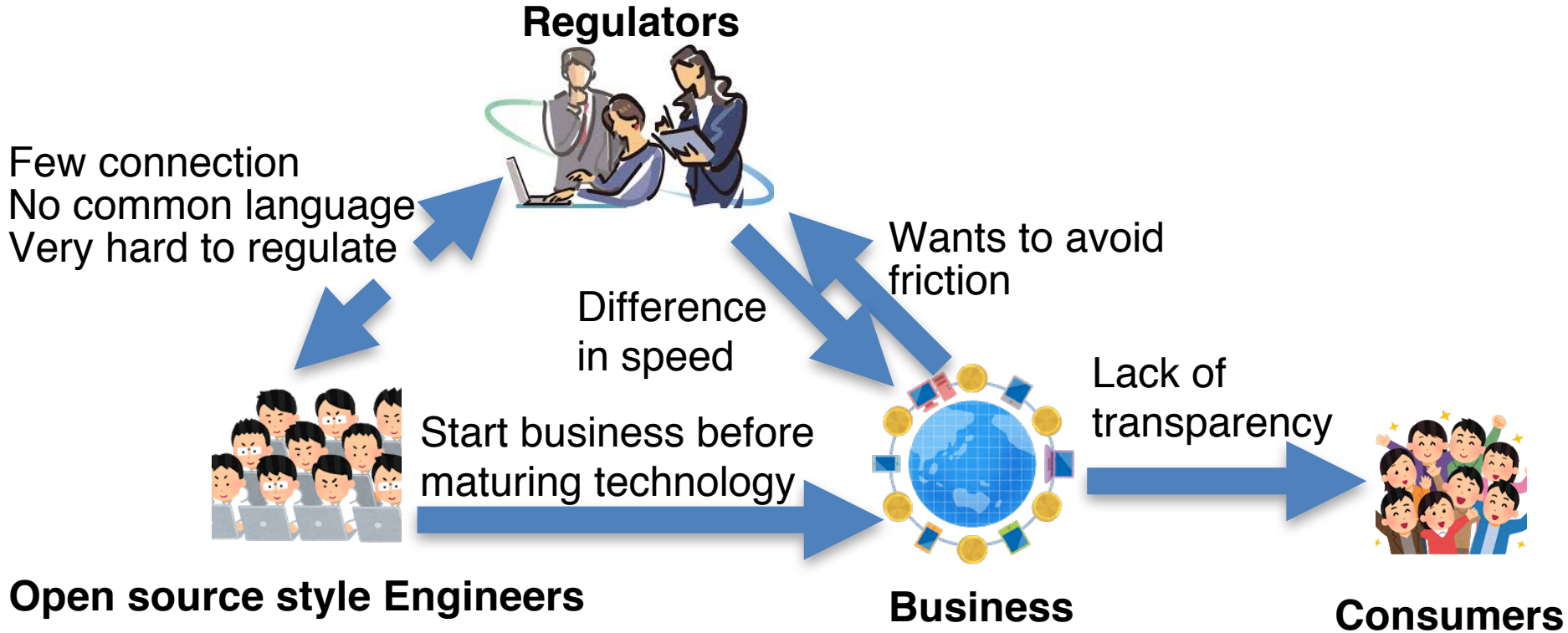


- Test of segwit
- Monitoring of Bitcoin forks
- Long-term blockchain
- Layer 2 technology competition
- Discussion Forum



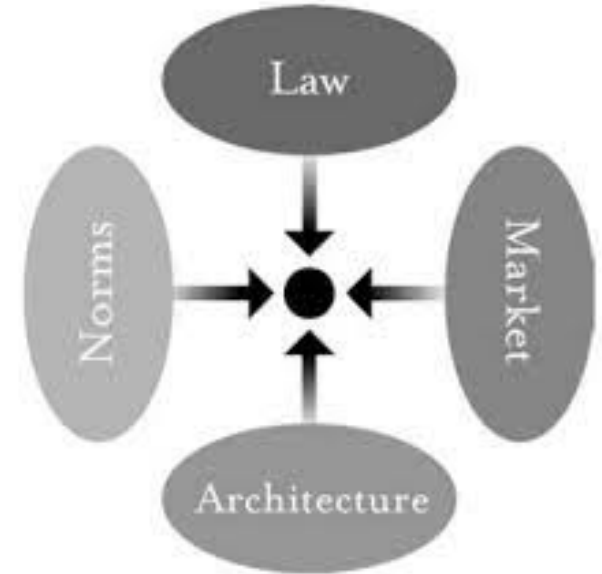
<https://www.coindesk.com/battle-testing-lightning-26-schools-start-contest-secure-bitcoins-layer-2>

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