

Communication required in the era of decentralized finance
– Lessons from the process of BGIN –



September 15, 2021

Shin'ichiro Matsuo, Georgetown University

GEORGETOWN UNIVERSITY

CyberSMART

About me: Shin'ichiro Matsuo



@shanematsuo

- Research area: Cryptography, Cryptographic protocols, privacy, and information security
 - ex.: E-cash, e-voting, cryptographic time-stamp, RFID authentication, and blockchain
- Georgetown University, Research Professor of Computer Science
 - Co-director of CyberSMART Research Center
- NTT Research Inc. Head of Blockchain Research
- Blockchain Governance Initiative Network (BGIN) acting co-chair
- Leader of six standardization project at ISO/IEC(TC307, JTC1 SC27), former Japanese Head of Delegate (SC27/WG2)
- OCED Blockchain Expert Policy Advisory Board (BEPAB) member
- ISO TC68 X.9 (US national body) member for CBDC standards
- Program chair of Scaling Bitcoin 2018 Tokyo, IEEE ICBC 2022, program committee member of cryptography, blockchain conferences (Financial Cryptography etc.)
- Trusted Web Council member (Japanese cabinet office)
- Former member of CRYPTREC

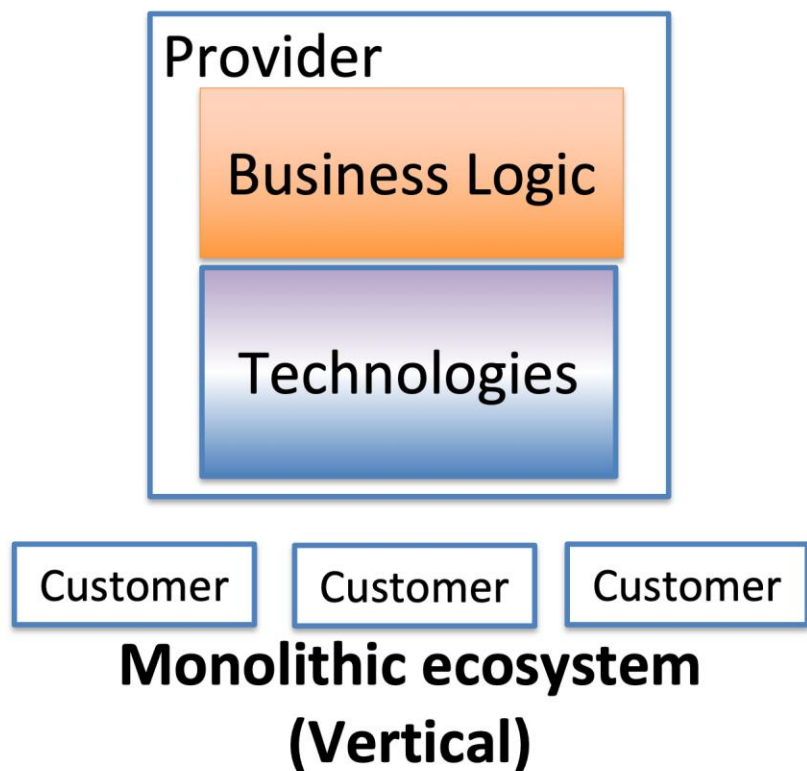
**I don't have any cryptoassets for academic neutrality.
I have no interest in exchange rate between cryptoassets and fiat currency.**

Take Away

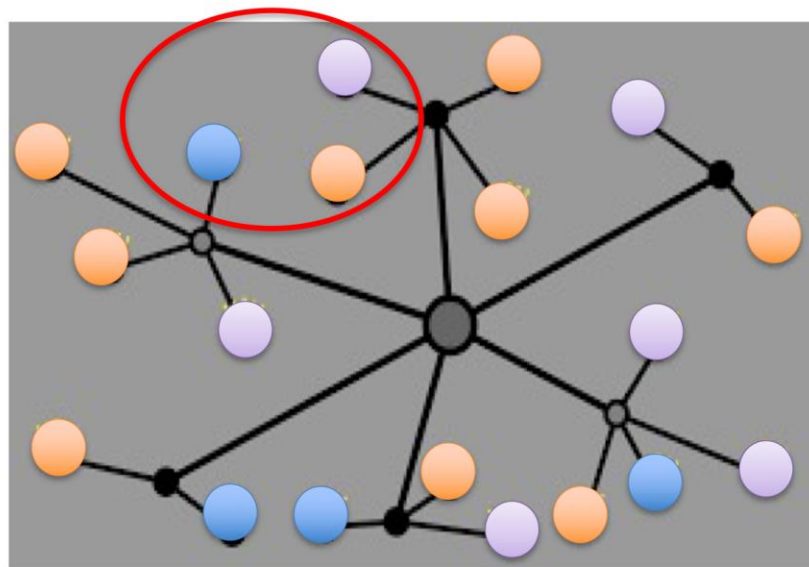
- Why the ordinary way of regulation does not work to achieve both promotion of innovation and create a trusted financial system
 - Understandings of stakeholders and ecosystem of digital - decentralized financial system
 - Understandings of structure of problems on technology, business, operation and regulation
- A style of governance to build trustable innovation in the era of decentralized finance
 - Importance of multi-stakeholder process
 - BGIN's activities
 - A proposal of healthy communication on technology, business, operation and regulation

Note: To avoid confusion, blockchain means “permission-less blockchain” in this talk

Decentralization + Layering = Unbundling and Permissionless

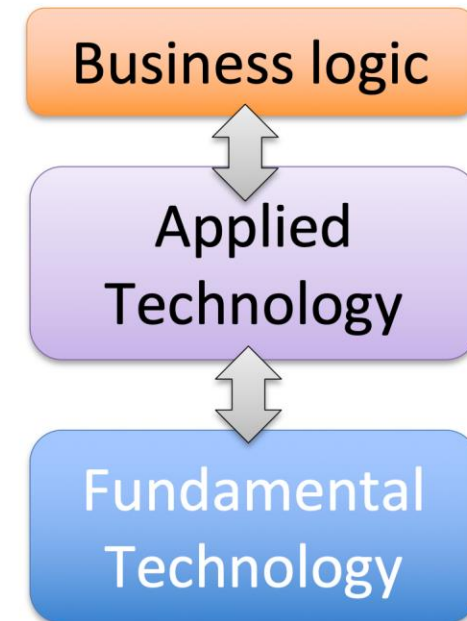


**Organizations own everything
provide service**



**Decentralized and permissionless System
(Unbundled)**

**Anyone can be a service provider and a part of
ecosystem without permission**



Regulatory goals and example of problems in digital - decentralized financial system

Regulatory Goals(*)

Financial Stability

Consumer/Investor
Protection

Preventing financial
crime

Examples of problems

Emergency and bankruptcy of financial services caused by governance which regulators don't aware (e.g. lending which does not cover risks, and program trading)

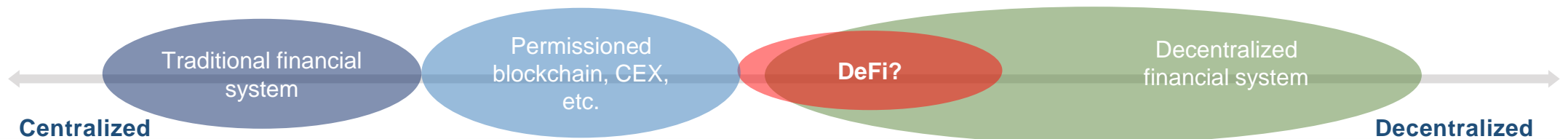
Cyber attack, lost of customers' asset by internal fraud Scam

Money Laundering
Terrorist financing

(*)Not only goals of regulators, but also goals of society

Decentralized Finance and so-called “DeFi”

- **Decentralized financial technology**
 - Technologies that have the potential to **reduce or eliminate the need for one or more intermediaries or centralised processes** in the provision of financial services (FSB "Decentralised financial technologies")
 - From regulatory perspective, KYC-free does not characterize decentralized financial technology
- **Decentralized financial system**
 - The new financial system (as opposed to the conventional centralized financial system) that decentralized financial technology could bring
- **(So-called) DeFi**
 - Specific applications that are (can be) part of the decentralized financial system
 - Uniswap, Compound, Maker etc.
 - The type and degree of decentralization varies depending on the application
 - **Law degree of decentralization** compared to near fully decentralized use cases (e.g., Bitcoin)



Three Types of Decentralization



- ❑ **Decentralization of decision-making**

- ❑ bottom-up approach
- ❑ On-chain Governance (Governance Tokens)

- ❑ **Decentralization of risk-taking**

- ❑ Peer-to-Pool (Protocol)
- ❑ Peer: People or Bot

- ❑ **Decentralization of record keeping**

- ❑ DLT
- ❑ IPFS



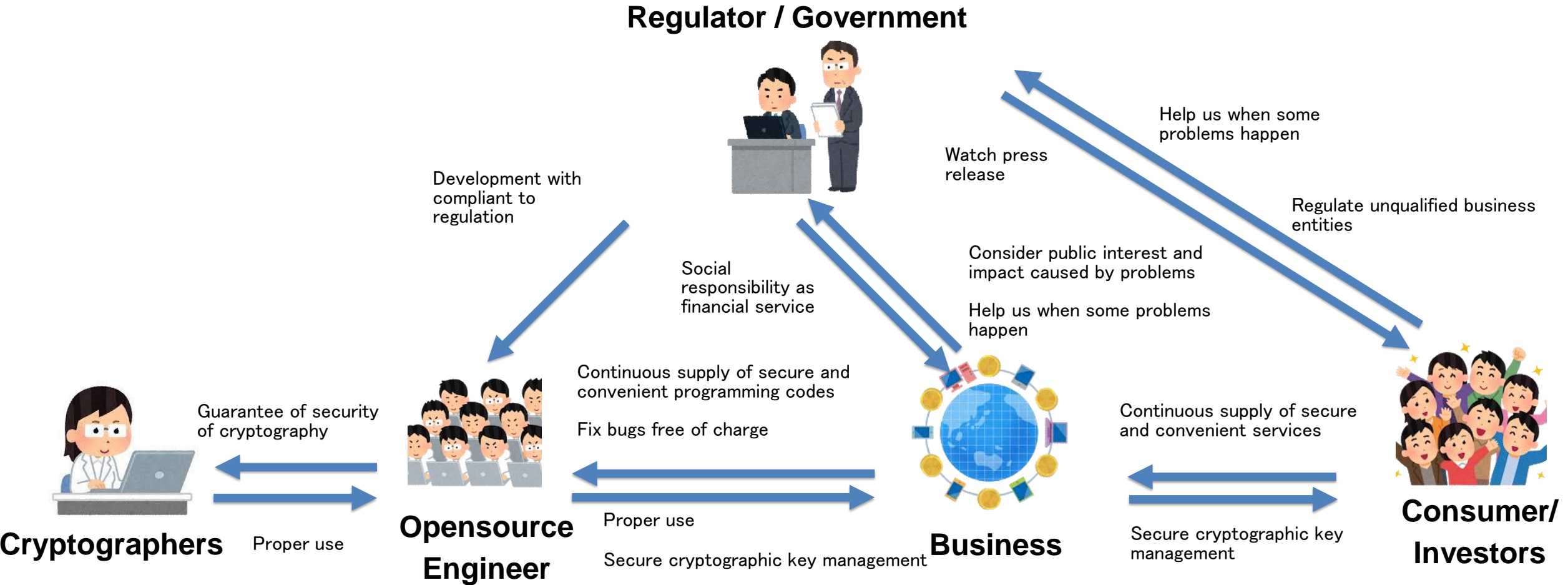
The degree of decentralization and risk characteristics of each project must be closely examined.
Where should (or shouldn't) it be decentralized?

Is DeFi truly decentralized?

Gary Gensler, Chairman of SEC (US) (8/9/2021 The Wall Street Journal)

“DeFi is a bit of a misnomer, because there’s still a core group of folks that are not only writing the software, like the open-source software, but they often have governance and fees. There’s some incentive structure for those promoters and sponsors in the middle of this.”

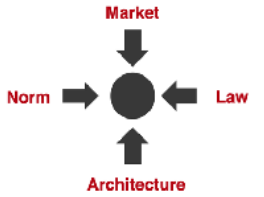
Stakeholders of decentralized financial systems and excessive expectations on trust



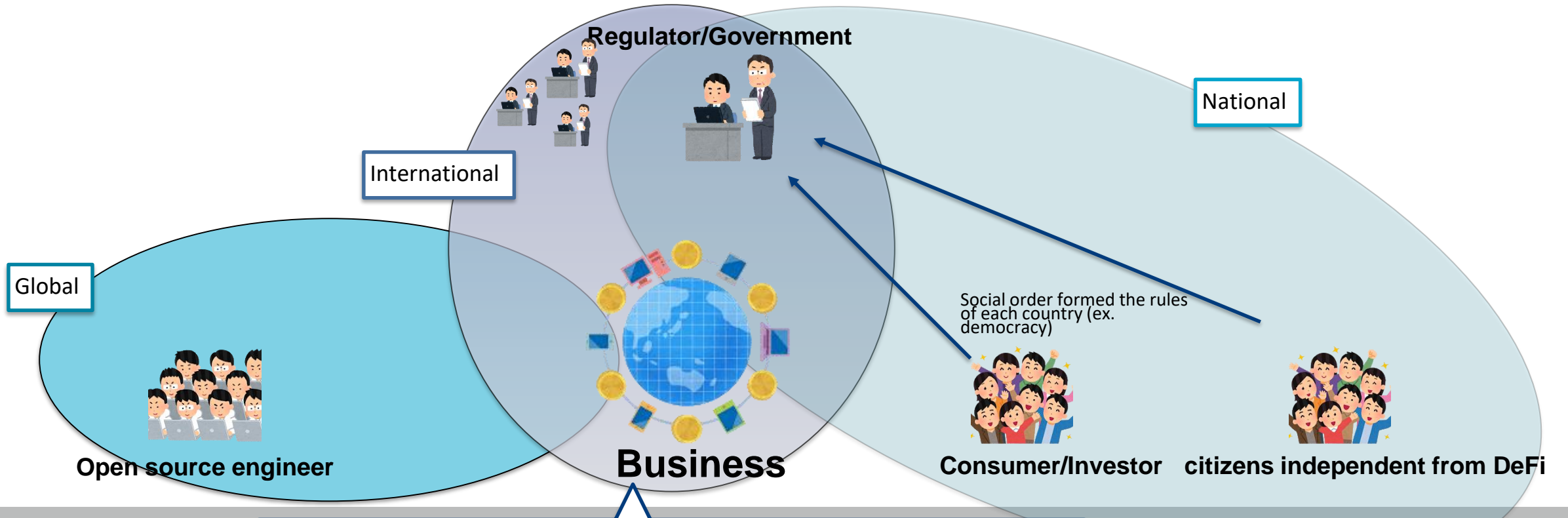
Dependencies of responsibilities are unclear.
There is no silver bullet. It is unclear if the business maintain conditions and environment to operate it without problems.

Global - International - National

- Global: Common activities on the earth, independent from nations e.g. the Internet, Bitcoin, Blockchain
- International: Activities to harmonize relationship among nations
- National: Activities which resulted from governance style (Democracy in Japan) of each nation

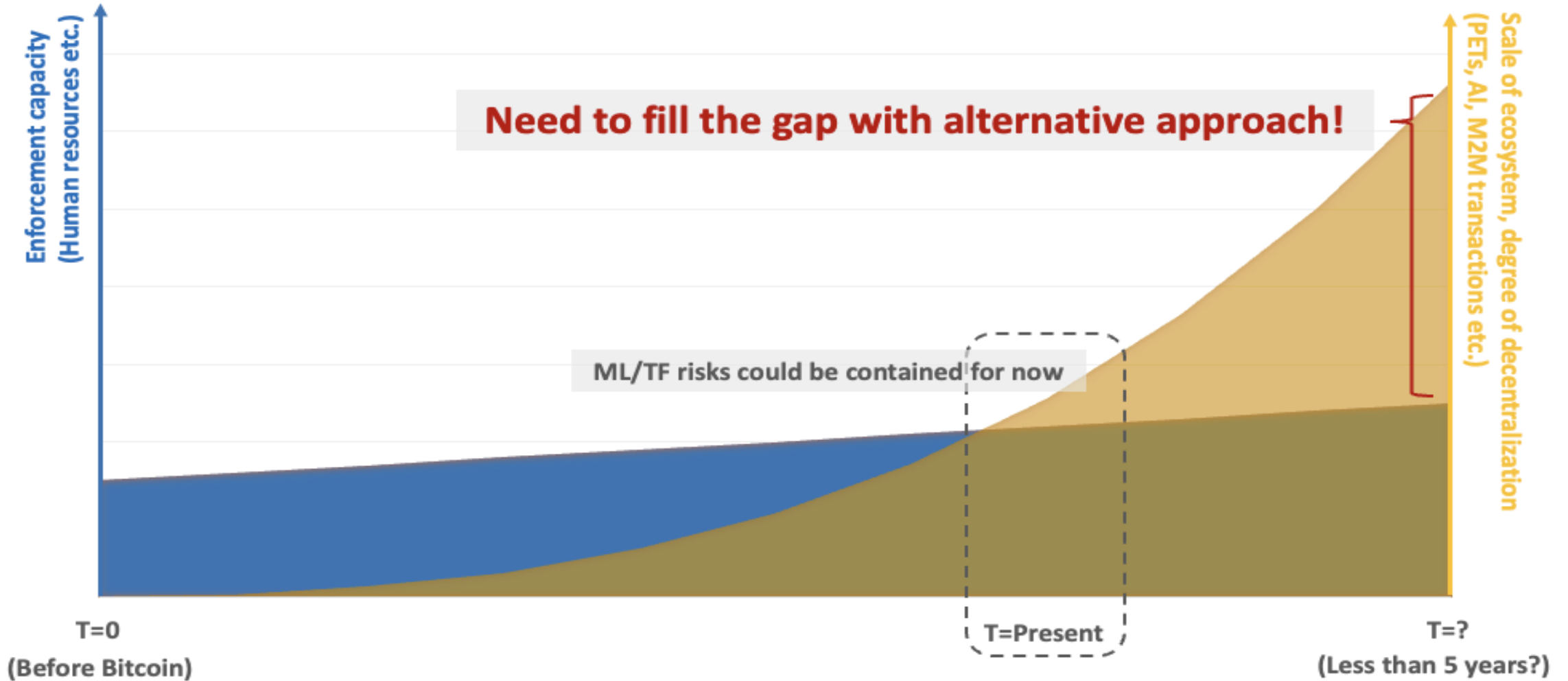


Creator of architecture (engineers and business) becomes creators of social order using global technologies. At the same time, they owe responsibility for social governance.



Understandings on global technology
 Harmonization with nation's rule (e.g. not overwrite decision by democracy)
 Harmonization with international order

Linear vs Exponential

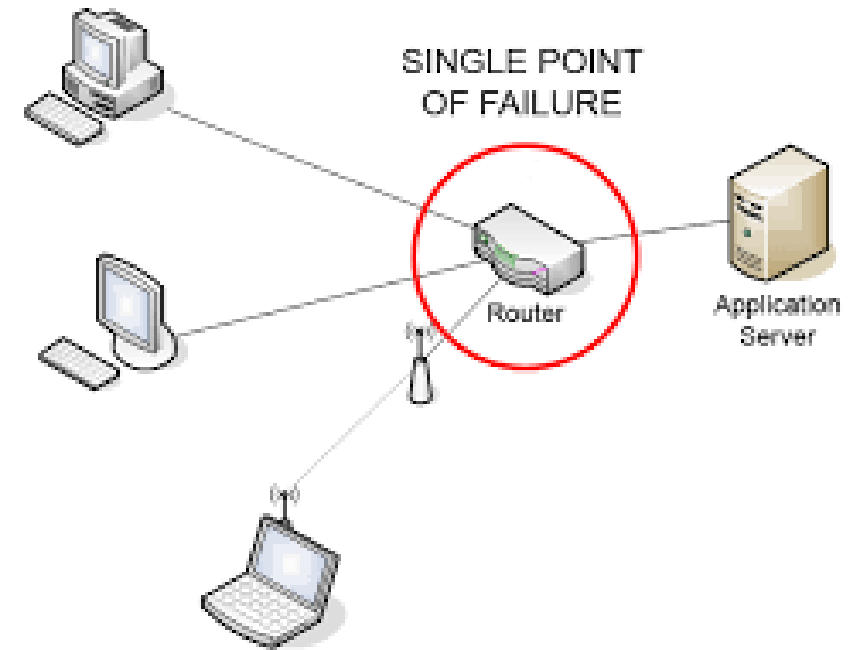


- In more forward-looking manner, FATF's approach could not be future-proofing considering that the decentralized financial transactions could expand exponentially (e.g. M2M transactions) while FATF's current approach may grow just linearly due to its physical limitations (i.e. human resource capacity)

Why “without trusted party” matters

Elimination of Single Point of Failure (SPOF)

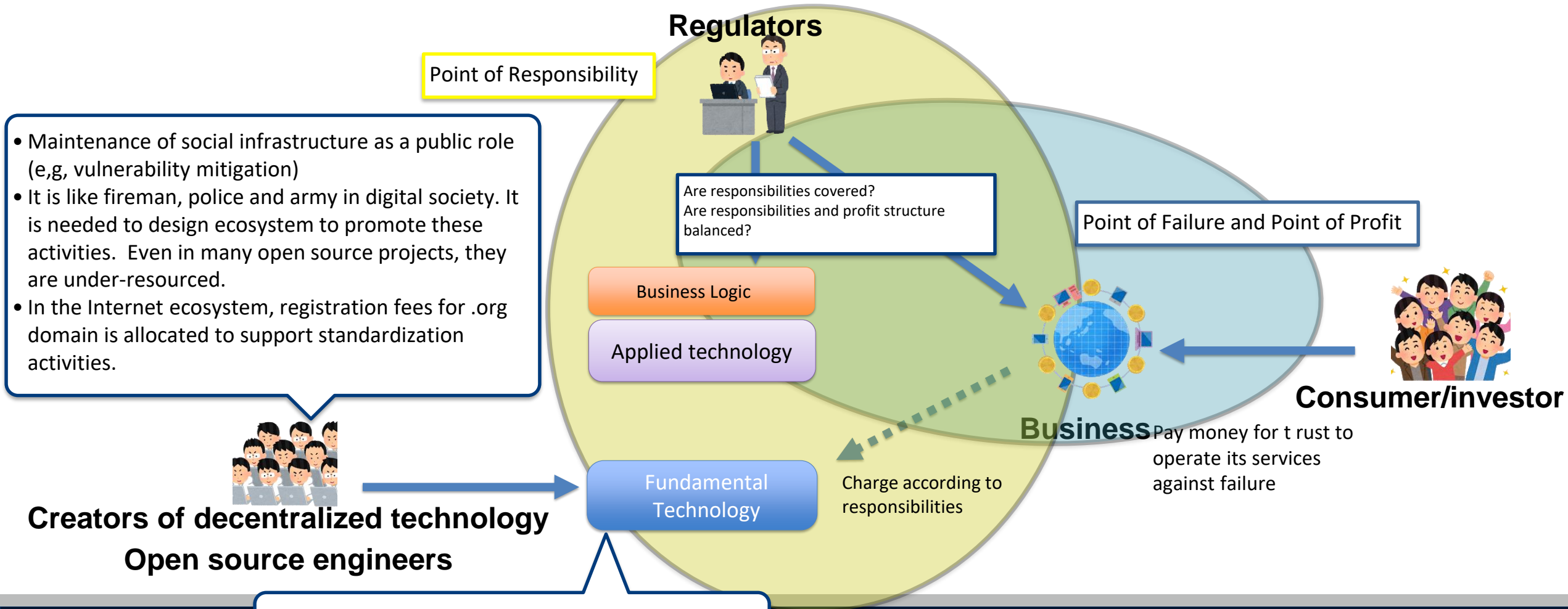
- Problems of SPOF
 - Resiliency against fault and cyber attacks
 - Business continuity
 - e.g. Cryptographic time-stamping service vs. Bitcoin
- Blockchain’s contribution
 - Continuous updates of ledger: with proper incentive mechanism design (e.g. mining reward). It tolerate a certain amount of malicious users.
 - We can externalize a part of trust of financial services with SPOF-less ledger. It can reduce costs for innovations.



Challenges in developing sustainable ecosystem with decentralized technologies

Point of Failure - Point of Responsibility - Point of Profit

It is important to maintain balance of responsibility and profit structure with covering dependency of responsibility



- It is basically infrastructure, and it is difficult to gain huge monetize, like Internet Service Providers.
- Bitcoin is a rare case with mining reward (sustainability is not guaranteed.)

Centralized, Decentralized and Poly-centric Stewardship

Centralized Trust



- Becomes the SPOF
- Blocker against permissionless innovation

Decentralized Trust



- Who is responsible for what?
- Broken incentive mechanism
- Works just for payment

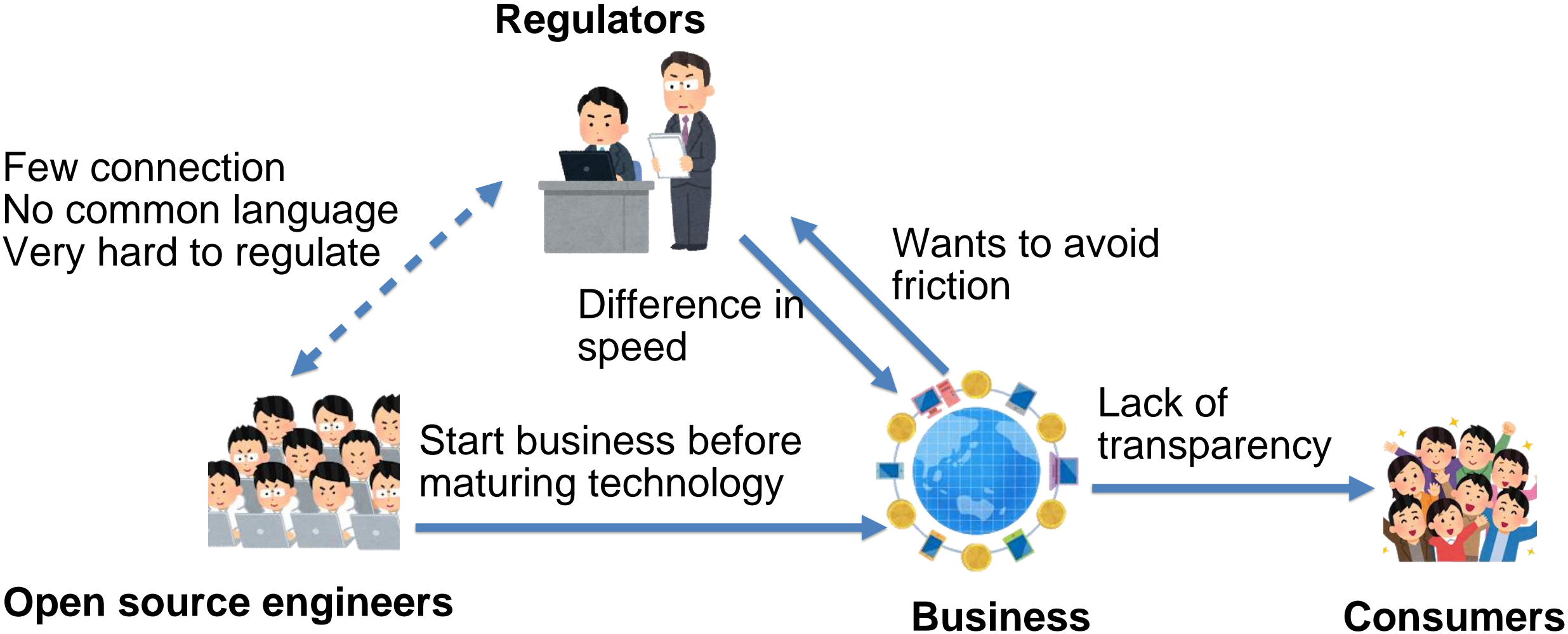


Poly-centric Stewardship



Permissionless Digital Trust Foundation

Stakeholders and the Current Situation



Multi-stakeholder discussion at 2019 G20

G20 HIGH-LEVEL SEMINAR ON FINANCIAL INNOVATION “OUR FUTURE IN THE DIGITAL AGE

Session 2: Multi-stakeholder Governance for a Decentralized Financial System

Jun Murai	Professor, Keio University
Klaas Knot	President, De Nederlandsche Bank, and Vice Chair, Financial Stability Board
Adam Back	Co-founder and CEO, Blockstream
Shin'ichiro Matsuo	Research Professor, Georgetown University
Brad Carr	Senior Director, Digital Finance, Institute of International Finance



2019 G20 Communique: Needs for multi-stakeholder dialogue on decentralized financial system

Technological innovations, including those underlying crypto-assets, can deliver significant benefits to the financial system and the broader economy. While crypto-assets do not pose a threat to global financial stability at this point, we remain vigilant to risks, including those related to consumer and investor protection, anti-money laundering (AML) and countering the financing of terrorism (CFT). We reaffirm our commitment to applying the recently amended FATF Standards to virtual assets and related providers for AML and CFT. We look forward to the adoption of the FATF Interpretive Note and Guidance by the FATF at its plenary later this month. We welcome IOSCO's work on crypto-asset trading platforms related to consumer and investor protection and market integrity. We welcome the FSB's directory of crypto-asset regulators, and its report on work underway, regulatory approaches and potential gaps relating to crypto-assets. We ask the FSB and standard setting bodies to monitor risks and consider work on additional multilateral responses as needed.

We also welcome the FSB report on decentralized financial technologies, and the possible implications for financial stability, regulation and governance, and how regulators can enhance the dialogue with a wider group of stakeholders.

We also continue to step up efforts to enhance cyber resilience, and welcome progress on the FSB's initiative to identify effective practices for response to and recovery from cyber incidents.

FSB
FINANCIAL
STABILITY
BOARD

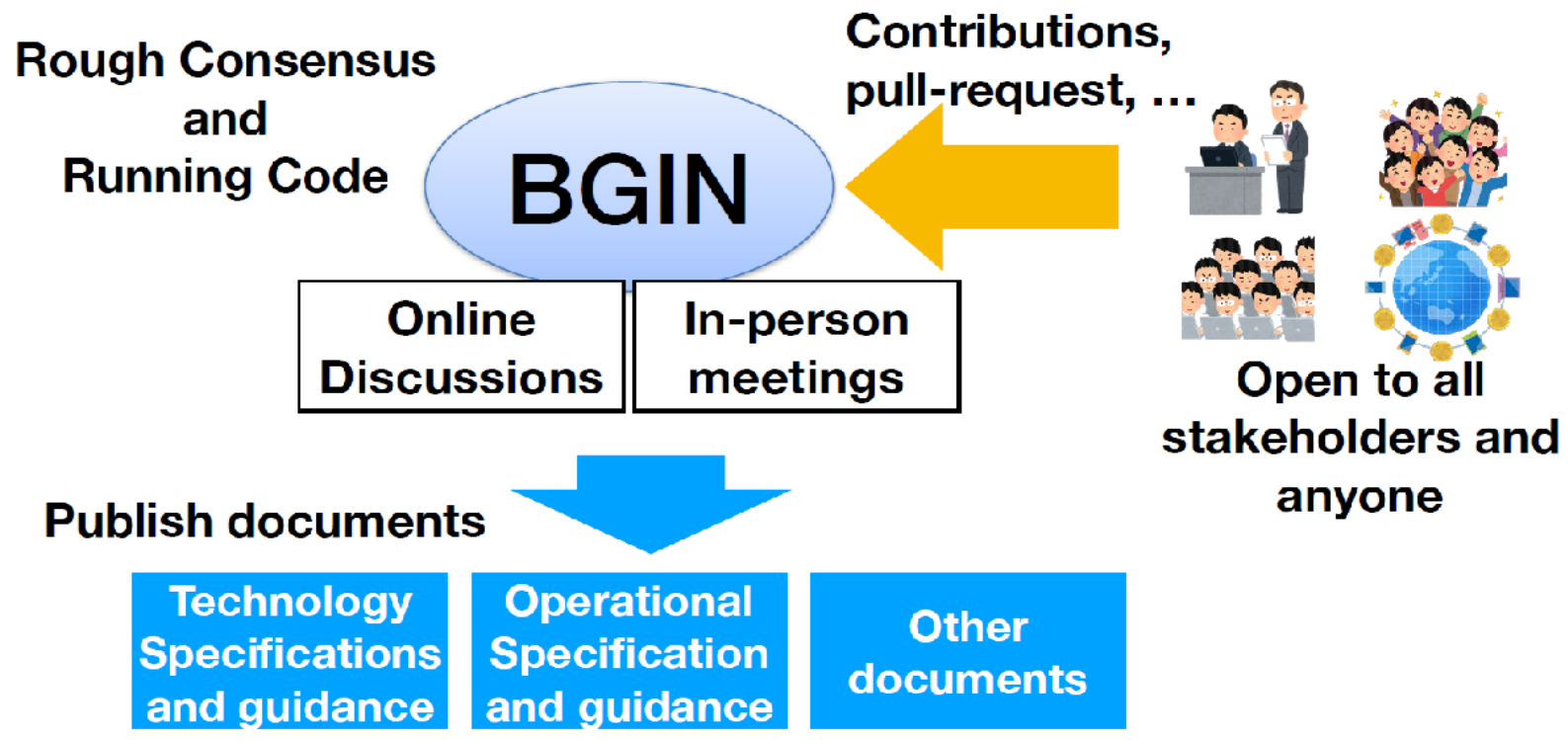
Decentralised financial technologies

Report on financial stability, regulatory and
governance implications

6 June 2019

Blockchain Governance Initiative Network (BGIN)

- An **open and neutral sphere** for all stakeholders to **deepen common understanding** and to **collaborate to address issues** they face in order to attain sustainable development of the blockchain community.



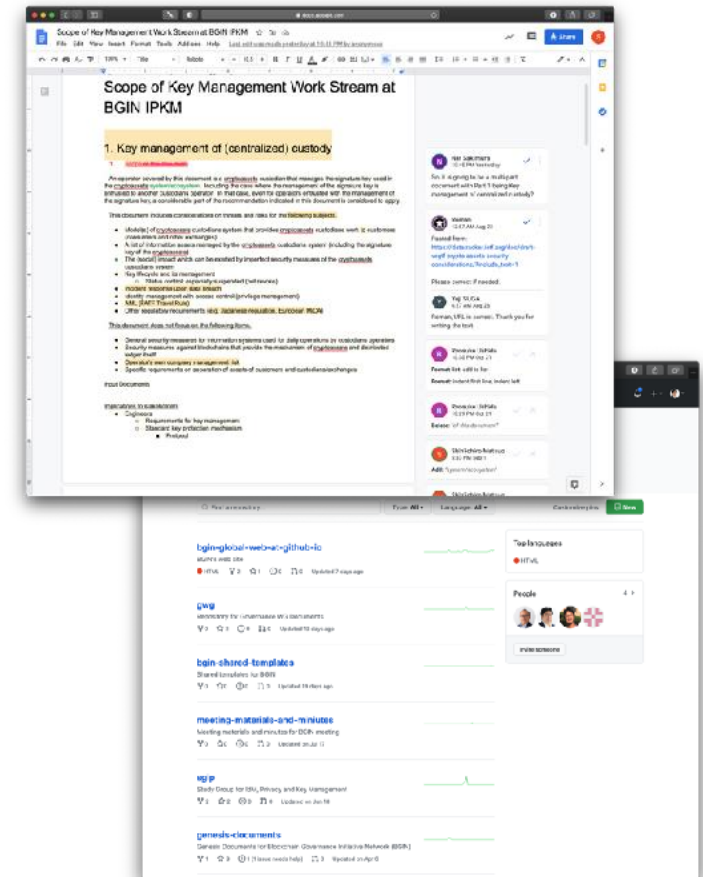
<https://bgin-global.org>

Tentative goals:

1. Creating an open, global and neutral platform for multi-stakeholder dialogue
2. Developing a common language and understandings among stakeholders with diverse perspectives
3. Building academic anchors through continuous provision of trustable documents and codes based on open source-style approach

Discussion style of BGIN

- General meetings (three times/yea), WG/SG/TF (bi-weekly calls)
 - Three general meetings until now (online)
 - Block #1 November, 2020 Mumbai, India
 - Block #2 March, 2021 Paris, France
 - Block #3 July 2021 Washington DC/New York, USA
 - Future meetingsL Block #4 November 2-4, 2021Africa, Block #5 Spring 2022, Tokyo Japan
- Use mailing lists and chat tool for open discussions
- Editing of documents is conducted using GitHub and GoogleDocs. Full open process and anyone can review and provide comments.
- Rough consensus



Current document development at BGIN

- Identity, Privacy and Key Management Working Group
 - Key Management of Centralized/Decentralized Custody
 - Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations
- Decentralized Treasury Working Group
- Internal Governance Working Group
 - Governance of BGIN
- Bylaw TF
 - Preliminary Bylaw

(Draft)

Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations

Introduction

With the advent of decentralized finance, which generally refers to "DeFi", regulatory authorities are paying increasing attention to the privacy, traceability, and identity aspects of DeFi systems to address regulatory challenges that the development of the decentralized financial technologies bring. While the rapid development of scaling and privacy enhancing technologies (PETs) by open-source blockchain communities could enhance scalability and privacy protection, lack of robust monitoring tools could adversely impact the ability of enforcement officers to trace financial transactions for financial crime prevention. As each stakeholder has different goals and objectives, there needs to be a venue for constructive dialogue to take place.

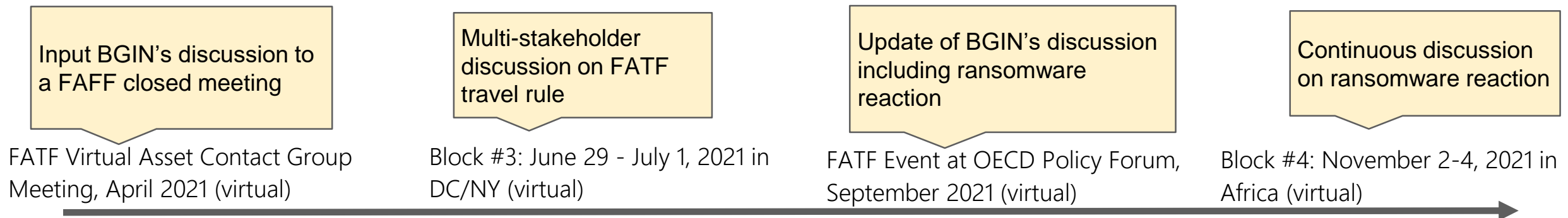
With this in mind, this document created under the current workstream, with contributions from diverse stakeholders including engineers, regulators, and financial institutions, aims to provide a source of reference especially for regulators and policy makers to have a collective understanding by, for example, analyzing recent development of major DeFi projects and technical advancements.

Disclaimer: The views expressed in the document are personal views of the participating members of the BGIN community and should not be seen as the official views or recommendations of the institutions with which they are affiliated.

Copyright statement: Text to be provided by Internal Governance WG.

Mutual conversation with FATF

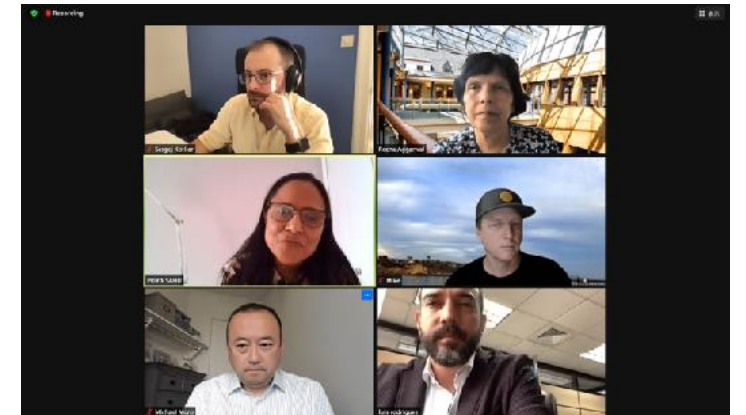
- BGIN was invited to closed meeting (VACG) and gave a presentation on FATF regulations (including travel rule), as a result of multi-stakeholder discussions at BGIN.
- At BGIN Block #3, FATF VACG Co-chair gave an invited talk and had an open discussions with all stakeholders including Bitcoin Core.
 - BGIN and FATF discussed potential collaborative works to develop a document on a framework to trace payment for ransomware attack.



Discussion on El Salvador's activity on Bitcoin

7/2/2021 (BGIN Block #3 Day3)

- A multi-stakeholder discussion by Engineer, academia (ex-regulator), business, financial institution (del Banco Centroamericano de Integración Económica para El Salvador)
 - Pros: Financial inclusion, importance of innovation; 70% is unbanked (decrease of remittance fee and finance for small business)
 - Cons: Concern about AML/CFT
- Merit to take risk by Government with thinking the case of the Internet
- Support by del Banco Centroamericano de Integración Económica para El Salvador to achieve AML and solve governance issues
- Discussion on issues when institutional investor participates cryptocurrency sector (e.g. custody, insurance, ETF), value of Bitcoin, price finding functionality etc.
- Need for participation of wider stakeholders for rule making



Discussions at BGIN Block #3

- Revision of FATF travel rule
 - Balance between AML/CFT and privacy
 - Ransomware reaction
- Institutionalization of Bitcoin in El Salvador
- Drafting of security document for Centralized / Decentralized custody
- Final drafting of regulatory concerns on DeFi
- Internal governance of BGIN
- Future work items
 - Governance of SSI/DID
 - Governance of decentralized exchange and custody
 - Governance of NFT

A proposal: Communication to consider technology, business, operation, and regulation for decentralized financial systems

- We don't know what we don't know - not to create the best financial system by your idea only
- The first step: creating common understandings
 - Definitions of terms
 - Regulatory goals (with detailed conditions)
 - Ways to achieve the regulatory goals
 - Potential and limitations of technologies
- Create culture and environment for healthy communications to propose new idea each other
 - Concern on technology, business and operation and improvement (from regulators and academia)
 - Proposal of new technologies to solve problems and make regulation efficient, like Linear vs. Exponential (from Engineers).
 - In US, it is seriously considered to involve experts who have healthy communications with regulators
- Add evaluation/verification process with global academia

Creating a format of mutual communications

- Needs for a format of documents to be verified by the third party including academia ex.)
 - General regulatory concern (by regulators)
 - Technical specification and design for third party review (when a business entity develop new technology and business)
 - How the business covers the regulatory concerns
 - Proposal to refine regulations and supporting tools
- Needs for a process to reach consensus on technical specifications and operations among stakeholders ex.)
 - Open verification by academia (including competition)
 - Self-evaluation and double check by authorities
 - Call for new evaluation criteria for new technologies and business

APPENDICES

BGIN Initial Contributors

● 23 experts with diverse backgrounds (**Engineers**, **Regulators**, **Internet Pioneers**, **Academia**, **Business**, **Standards**.)

Mai Santamaria
Head of Financial Advisory team (SFAD),
Department of Finance Ireland
Dublin, Ireland



Jumpei Miwa
Director, Fintech and Innovation Office,
Financial Services Agency, JAPAN



Yuta Takanashi
Deputy director, Office of International Affairs,
Financial Services Agency, JAPAN



Jeremy Rubin
San Francisco, US



Danny Ryan
Ethereum Foundation



Yuji Suga
Internet Initiative Japan Inc. / CGTF
Tokyo, Japan



David Ripley
COO, Kraken
San Francisco, US



Philip Martin
Chief Information Security Officer,
Coinbase Global Inc.



Flora Li
Director, Huobi Blockchain Academy
Beijing, China



Brad Carr
Managing Director, Digital Finance,
Institute of International Finance
Washington D.C., US



Julien Bringer
CEO, Kallistech
Paris, France




Nat Sakimura
Chairman, OpenID Foundation
Tokyo, Japan



Michèle Finck
Senior Research Fellow,
Max Planck Institute for Innovation and Competition
Munich, Bavaria, Germany



Nii Quaynor
Chairman, Ghana Dot Com Ltd
Accra, Ghana




Pindar Wong
Chairman, VeriFi Limited
Hong Kong, China




Shin'ichiro Matsuo
Research Professor,
Georgetown University
Washington D.C., US



Aaron Wright
Clinical Professor of Law,
Cardozo Law School
New York, US



Katharina Pistor
Professor, Columbia Law School
New York, US



Shigeya Suzuki
Project Professor,
Graduate School of Media and Governance,
Keio University
Fujisawa, Japan



Joaquin Garcia-Alfaro
Full Professor, Institut Mines-Télécom
/ Institut Polytechnique de Paris
Paris, France



Kazue Sako
Waseda University
Tokyo, Japan



Robert Wardrop
Director,
Cambridge Centre for Alternative Finance
Cambridge, UK



Byron Gibson
Program Manager,
Stanford Center for Blockchain Research
San Francisco, US



A document on regulatory concerns for decentralized financial systems

[5. Problem statement](#) [5](#)

[5.1 Regulatory and supervisory challenges](#) [9](#)

[5.2 Review of other existing literature on the subject \(Institutions/Researchers\)](#) [10](#)

[5.2.1 Takanashi et al. \(2020\)](#) [10](#)

[5.2.2 Ushida and James \(2021\)](#) [10](#)

[6. How decentralized finance \(DeFi\) ecosystem currently works](#) [11](#)

[6.1 Motivation/goals of DeFi community](#) [11](#)

[6.2 Definition of DeFi and ambiguously used terms](#) [11](#)

[6.3 Key technologies in place](#) [12](#)

[6.3.1 Emerging decentralized financial technologies](#) [12](#)

[6.3.2 Privacy Enhancing Technologies \(PETs\)](#) [13](#)

[6.4 Governance mechanism](#)

[6.4.1 Overview of the ecosystem](#)

[6.4.2 Case Study: Dash](#) [14](#)

[7. How DeFi ecosystem is likely to advance](#) [16](#)

[7.1 Advancement of DeFi ecosystem to date and future direction](#)

[7.2 Further decentralization](#)

[7.3 Recentralization](#)

[8. Regulatory implications](#) [16](#)

[8.1 Linear vs Exponential](#)

[8.2 Takeaways from multi-stakeholder roundtable](#)[16](#)

[7.1.1 CoDecFin](#)

[7.1.2 BGIN Block #2 meeting](#)

[8.3 Applicability and limitation of existing regulatory framework](#)

(Draft)

Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations

Introduction

With the advent of decentralized finance, which generally refers to "DeFi", regulatory authorities are paying increasing attention to the privacy, traceability, and identity aspects of DeFi systems to address regulatory challenges that the development of the decentralized financial technologies bring. While the rapid development of scaling and privacy enhancing technologies (PETs) by open-source blockchain communities could enhance scalability and privacy protection, lack of robust monitoring tools could adversely impact the ability of enforcement officers to trace financial transactions for financial crime prevention. As each stakeholder has different goals and objectives, there needs to be a venue for constructive dialogue to take place.

With this in mind, this document created under the current workstream, with contributions from diverse stakeholders including engineers, regulators, and financial institutions, aims to provide a source of reference especially for regulators and policy makers to have a collective understanding by, for example, analyzing recent development of major DeFi projects and technical advancements.

Disclaimer: The views expressed in the document are personal views of the participating members of the BGIN community and should not be seen as the official views or recommendations of the institutions with which they are affiliated.

Copyright statement Text to be provided by Internal Governance WG.

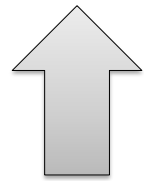
Internet Governance as an Ecosystem

International

vs.

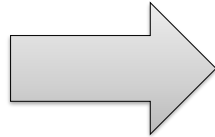
Global

**Multi-stakeholder
Conversation**



As one of
stakeholders

Governments



Non Profit



Non Profit



Manages
Domain names

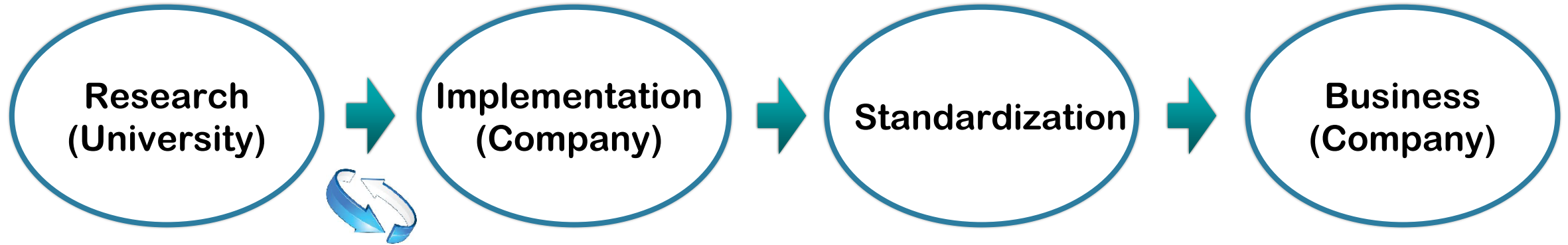


Technology
Standard

Participation as
individual

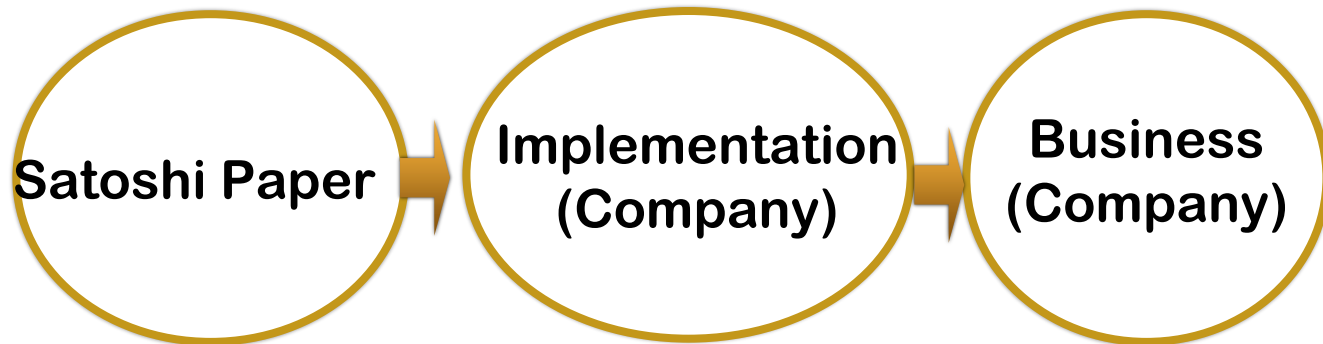
Academic Research is still needed

The Case of Internet Technology



“BSD” and open-source facilitated innovation

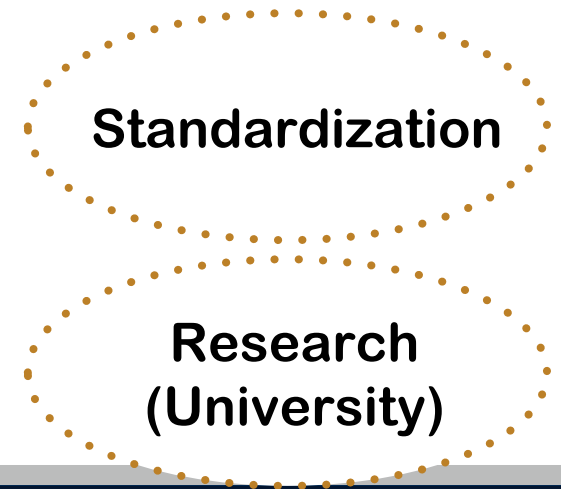
The Case of Bitcoin and Blockchain



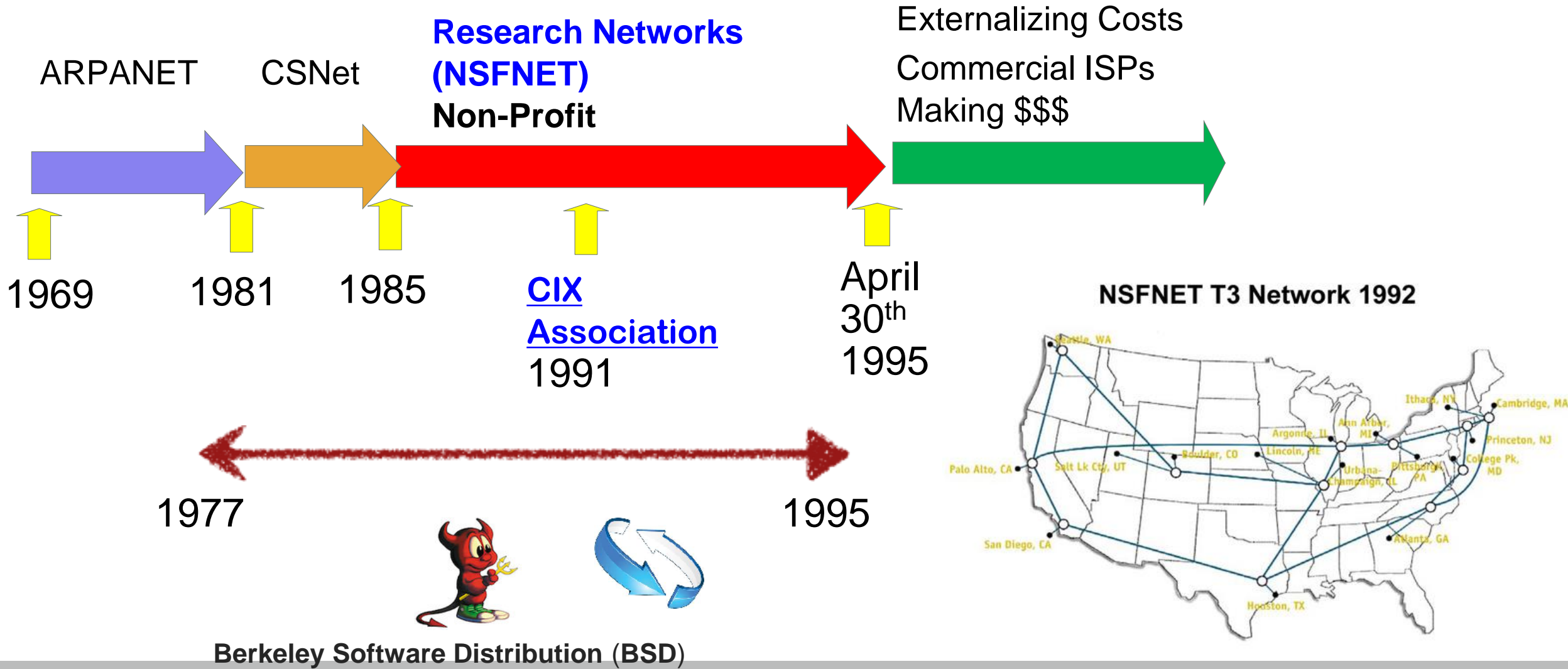
Innovation by iteration



Need
rebuild



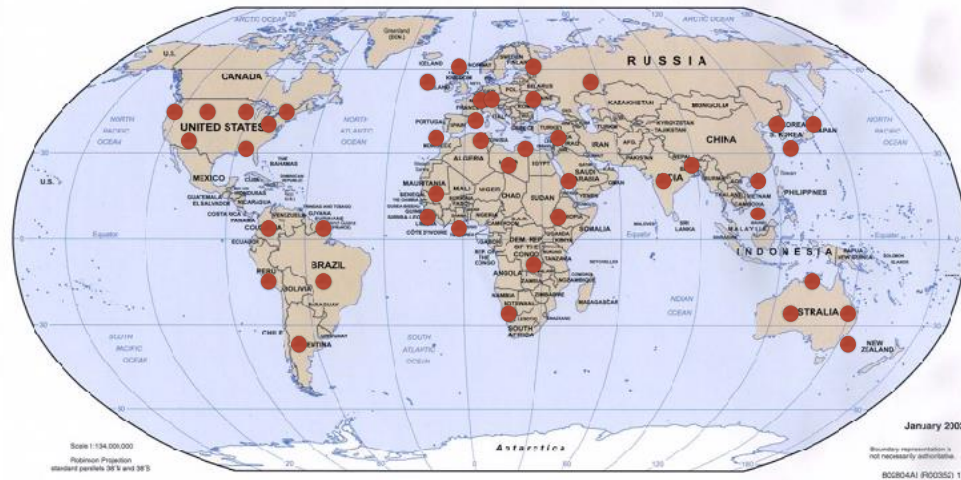
NSFNet for the Internet





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

- **A neutral, stable and sustainable** research test network for Blockchain technology by international universities.
- Provide a source of neutral knowledge by academia
- 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

G20 and International Standard Setting Bodies (SSBs)

G20 Financial Ministers and Central Bank Governors meeting

The Financial Stability Board

**Basel Committee on
Banking Supervision**

**International Association
of Insurance Supervisors**

**International Organization
of Securities Commissions**

Financial Action Task Force (AML/CFT)

All the SSBs work on blockchain and crypto assets related issues in some ways.

A Report by Financial Stability Board (FSB) : published on June 6 2019



FSB report on decentralised financial technologies considers:

- Financial stability, regulatory and governance implications of DLT and P2P;
- Sets out benefits and risks of increased use; and
- Underscores the importance of a multi-stakeholder dialogue.

A Report by Financial Stability Board (FSB) : published on June 6 2019

Decentralised financial technologies are likely to continue to evolve rapidly. Early liaison between regulators and a wider group of stakeholders might help ensure that **regulatory and other public policy objectives are considered in the initial design of technical protocols and applications**. This should help limit the emergence of unforeseen complications at a later stage.

Authorities may therefore wish to enhance their dialogue and cooperation with a wider group of stakeholders, including software developers, the engineering community, as well as businesses, academia, and other relevant stakeholders such as investors, consumers and users. This would help to assess the opportunities and risks of decentralised financial technologies. **It would also enable supervisors to continue to address emerging issues promptly and use supervisory resources effectively while at the same time remaining open to the benefits of financial innovation.**

Aspects of securing blockchain ecosystem

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

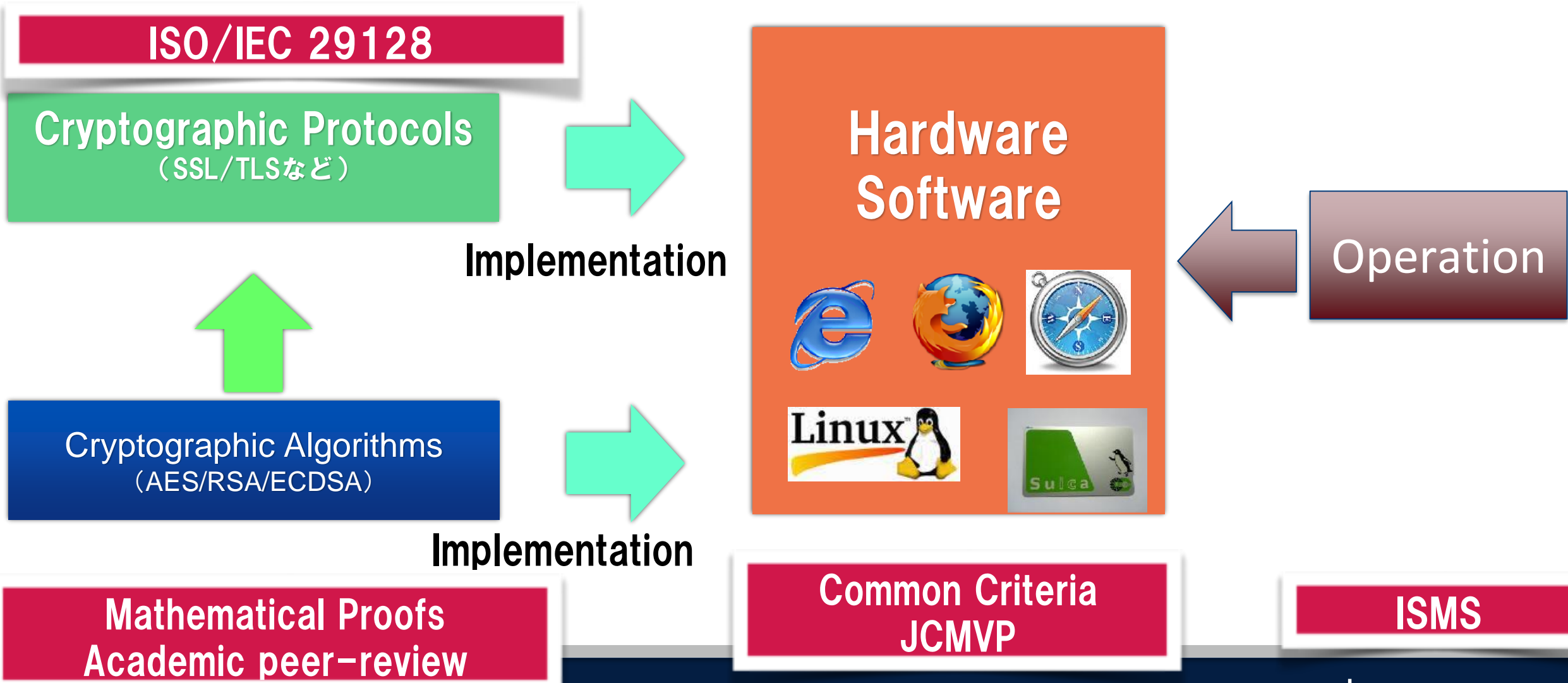
ISO/IEC 29128

Cryptography

ECDSA, SHA-2, RIPEMD160

NIST,ISO

Overview of verification and certification of cryptography and its implementation



Thank you!



GEORGETOWN UNIVERSITY
@yberSMART