資料２

分散型金融の時代に求められる規制のためのコミュニケーション
- BGINのプロセスに学ぶ -

September 15, 2021
Shin’ichiro Matsuo, Georgetown University

GEORGETOWN UNIVERSITY
CyberSMART

自己紹介: 松尾真一郎

@shanematsuo

- 主な研究領域：暗号、暗号プロトコル、プライバシ、情報セキュリティ
  - 例：電子現金、電子投票、暗号学的タイムスタンプ、RFID認証、ブロックチェーン
- ジョージタウン大学 Department of Computer Science 研究教授
  - CyberSMART研究センターダイレクター
- NTT Research Inc. （米国）　Head of Blockchain Research
- Blockchain Governance Initiative Network（BGIN）暫定共同議長
- ISO/IECにおける技術標準の6つのプロジェクトのリーダー（TC307, JTC1 SC27）、元日本HoD（SC27/WG2）
- OCED Blockchain Expert Policy Advisory Board (BEPAB)メンバー
- ISO TC68 X.9 (米国国内委員会）メンバー （CBDC標準化）
- Scaling Bitcoin 2018 Tokyo, IEEE ICBC 2022プログラム委員長（その他、ブロックチェーン、暗号技術の国際会議のプログラム委員メンバー（Financial Cryptography等）
- 内閣官房Trusted Web推進協議会構成員
- 過去に暗号技術検討会構成員等

学術的中立性のためビットコインや暗号資産は持っていません。
暗号資産と既存通貨との交換レートについては関心はありません。

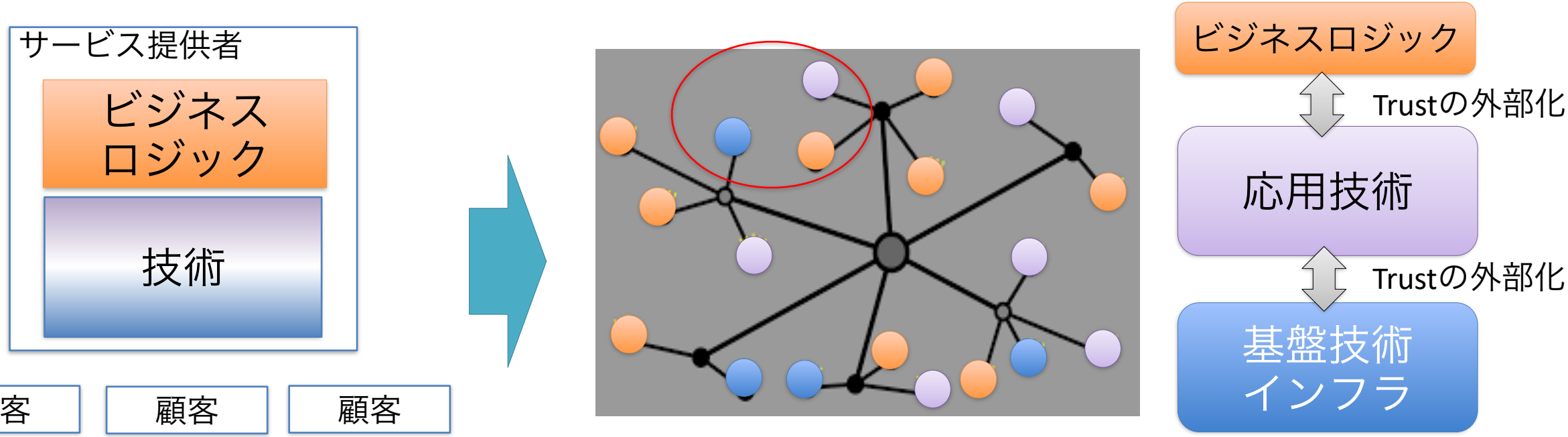
この発表におけるTake Away

- 分散型技術を利用したイノベーションを促進しつつ、信頼あるシステムを構築したいのに、なぜこれまでのやり方はworkしないのか
  - デジタル・分散型金融におけるステークホルダーとエコシステムの理解
  - 技術、ビジネス、運用、規制上の問題の構造の理解
- 分散型金融の時代に信頼あるイノベーションを促進するために必要なスタイル
  - マルチステークホルダープロセスの重要性
  - BGINでの取り組み
  - 技術、ビジネス、運用、規制を考える上でのコミュニケーションの提案

但し書き：議論を混乱させないため、本発表ではブロックチェーンとはパーミッションレスブロックチェーンのことを指します

イノベーションの源泉としての分散型技術

Trust（の一部）の外部化とアンバンドリング



統一されたシステム
(垂直統合)

一組織がサービス提供のための
全てを所有しコントロールする

分散化されたパーミッションレスなシステム
(アンバンドルされた水平分業)

誰もが誰かの許可を得ることなく、
サービス提供者とエコシステムの一部になれる

Trust（の一部）の外部化が、イノベーションの源泉であり、一方で課題を引き起こすポイントになる

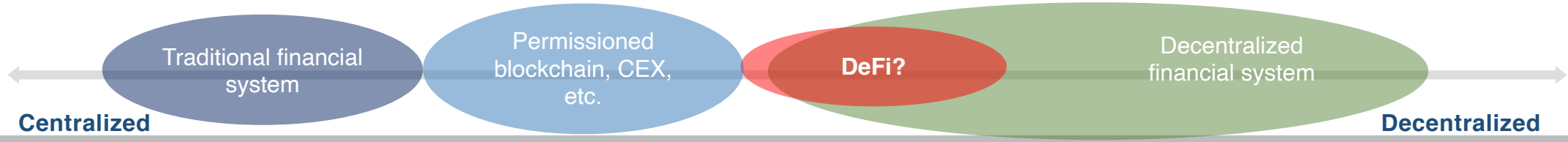
金融当局の規制目標とデジタル・分散型金融における問題の例

金融当局の規制目標(*)	問題の例
金融安定	金融当局が把握できないガバナンスによる金融サービスの危機・破綻（リスクがカバーできていないレンディングやプログラム取引など）
消費者・投資家保護	サイバー攻撃、内部不正等による顧客資産の流出 詐欺的事件
金融犯罪防止	マネーロンダリング テロリストファイナンシング

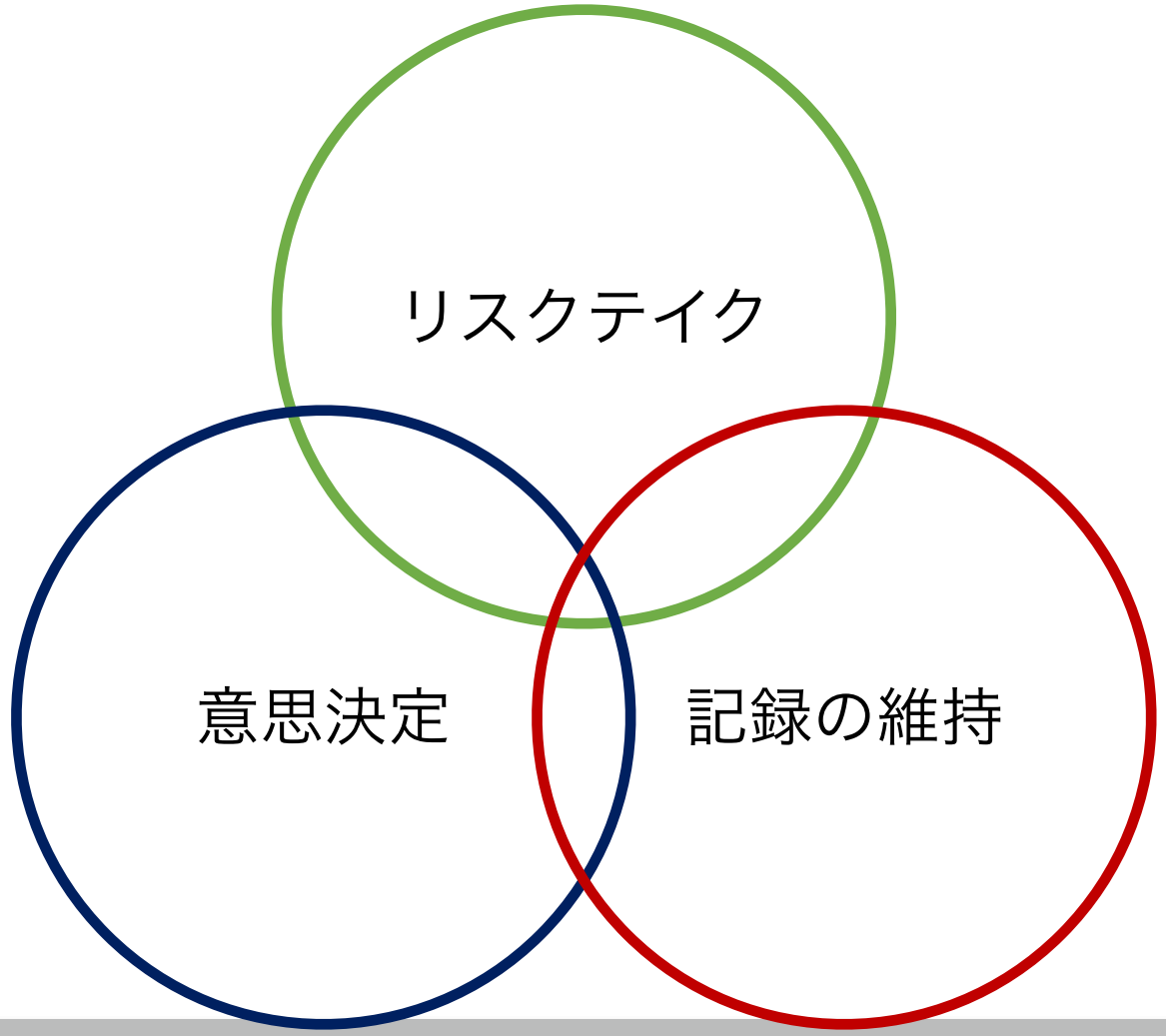
(*)規制当局だけの目標ではなく、本来社会全体の目標である

「分散型金融」のスコープ

- **Decentralized financial technology 分散型金融技術**
  - 金融サービスの提供にあたり、1つ、あるいは複数の中間者あるいは集中的プロセスの必要性を軽減、あるいは取り除く可能性をもった技術（FSBレポート "Decentralised financial technologies"より松尾訳)
  - 規制当局の観点では、KYCがないことは分散型金融を性格づけるわけではない
- **Decentralized financial system 分散型金融システム**
  - 伝統的な中央管理者がいる金融システムとは対照的に、分散型金融技術がもたらす新しい金融システム全般
- **(So-called) DeFi いわゆるDeFi (マーケティングワード)**
  - 分散型金融システムを構成し得る特定のアプリケーション
    - Uniswap, Compound, Maker 等
    - 分散の度合いはアプリケーションによって異なる
    - 完全な分散型ユースケース（例：Bitcoin）に比べると、分散の度合いは低いことが多い



分散型金融にまつわる「分散」の意味



- **意思決定の分散化**
  - bottom-up approach
  - On-chain Governance (Governance Tokens)
- **リスクテイクの分散化**
  - Peer-to-Pool (Protocol)
  - Peer: People or Bot
- **記録の維持の分散化**
  - DLT
  - IPFS

どこは分散化していてもよく、どこは分散化が相応しくないかなど、個別のビジネス・プロジェクトの分散化の度合いとリスクの性質は詳細に評価される必要がある。

分散型金融は本当に分散化されているのか？

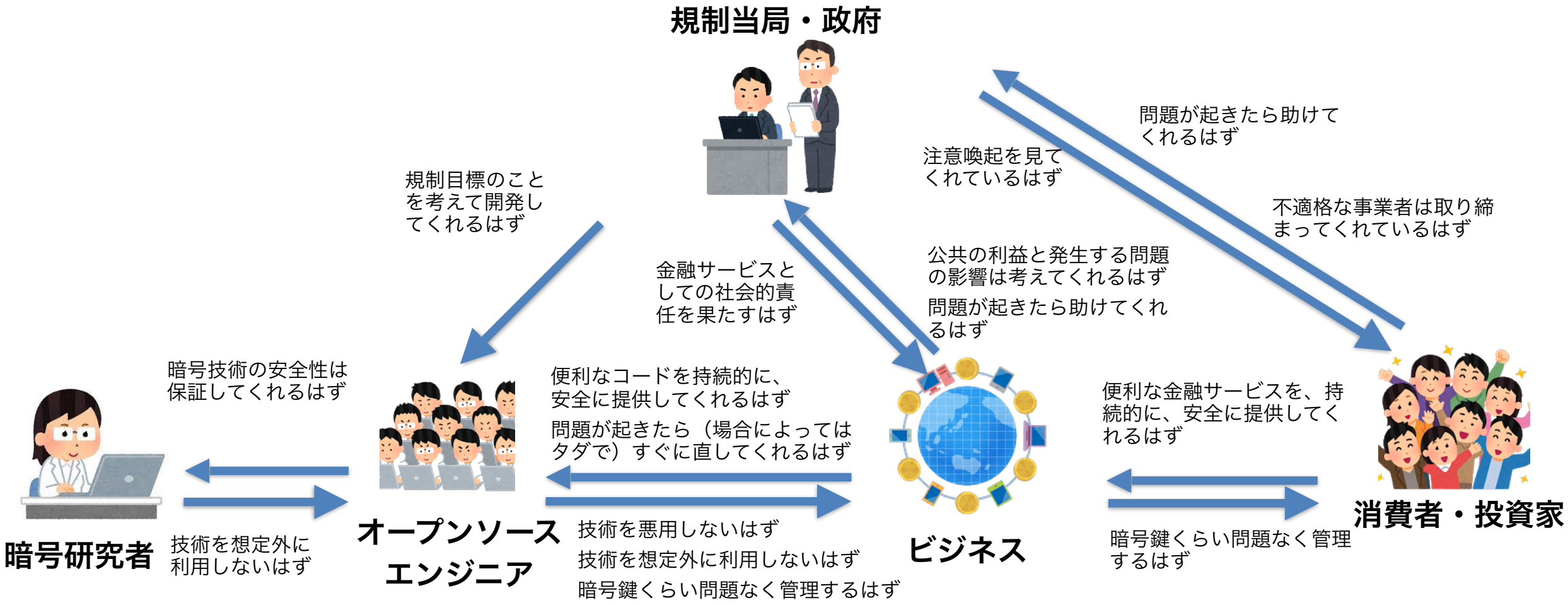
Gary Gensler 米・SEC委員長の発言（2021年8月19日 The Wall Street Journal）

“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.”

DeFiという言葉は少し誤ったものである。なぜならば、オープンソースのソフトウエアのようなソフトウエアを書くだけでなく、ガバナンスに関する権利や手数料などを得るコアグループがいるからだ。この中には、後援者やスポンサーのための、幾らかのインセンティブ構造も存在する。

現実には 分散的技術の作り手 分散的技術に乗っかって マネタイズするグループ の2重構造になっている点を指摘

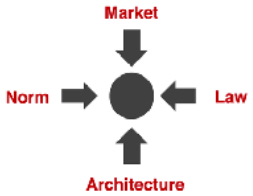
分散型金融におけるステークホルダーとTrustに対する（過剰な）期待



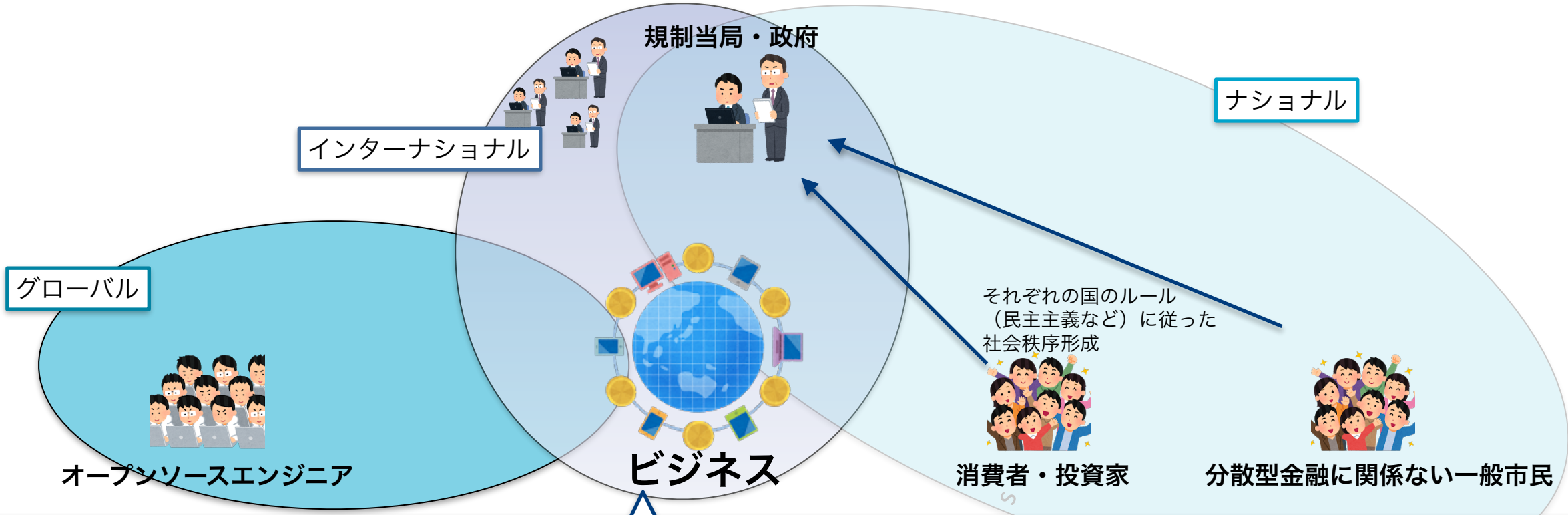
責任の依存関係（誰が誰の肩の上に乗っているか）の全容が解明されていない
何事にも万能薬はないが、ある仕組みがうまく行く前提条件や環境が維持できているとは限らない

Global - International - National

- グローバル：地球に1つ共通の営みで、国家の都合とは独立に存在する　例）インターネット、ビットコイン、ブロックチェーン
- インターナショナル：各国家の事情に基づき、国家間の事情を調和させるための営み
- ナショナル：国別の事情により、それぞれのガバナンス（日本では民主主義）によって形作られる営み



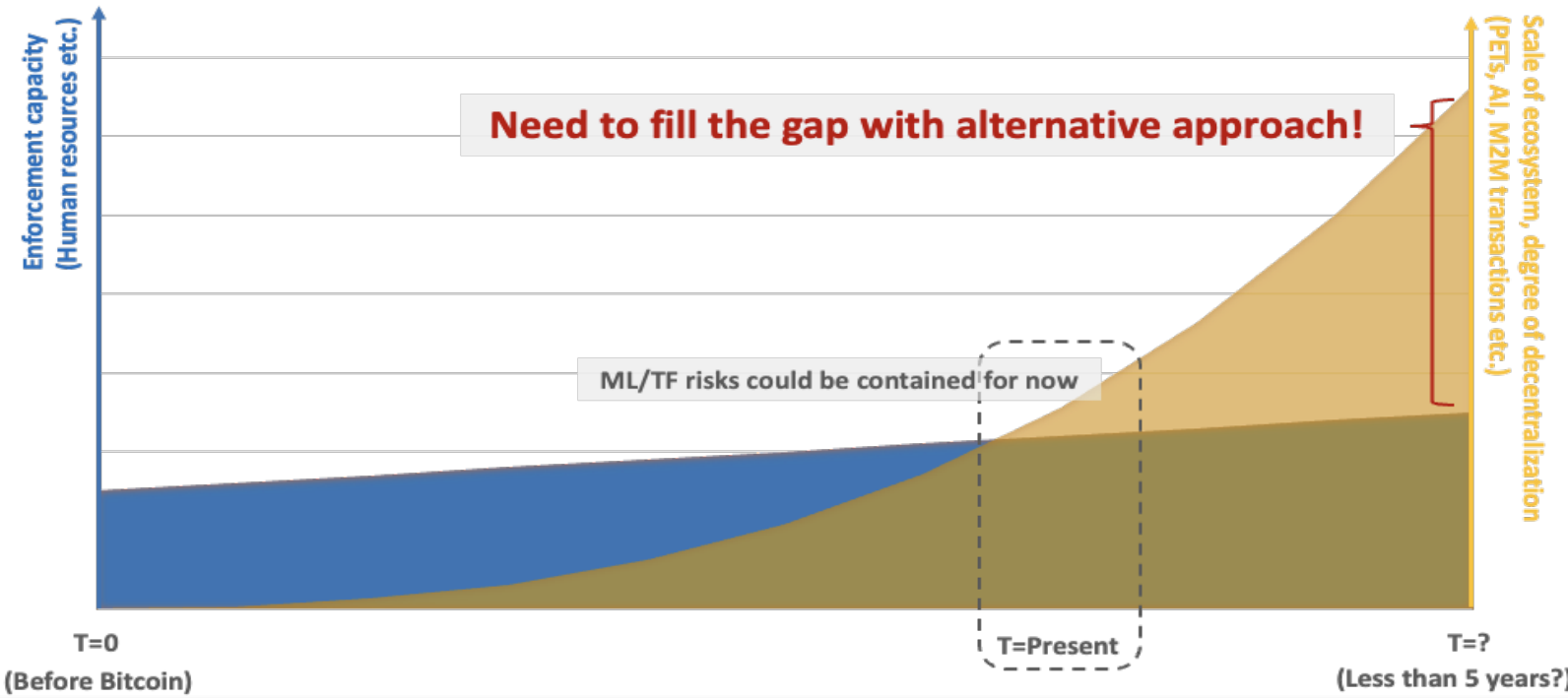
グローバルな技術を使いながらもArchitectureの作り手（エンジニア、分散型金融ビジネス）が秩序の作り手の一部になり同時に社会のガバナンスに対する責任も発生する



グローバルな技術への理解
各国のルールに従った秩序との調和（例えば民主主義の結果の意思決定を上書きはできない）
インターナショナルな秩序との調和

Linear vs Exponential

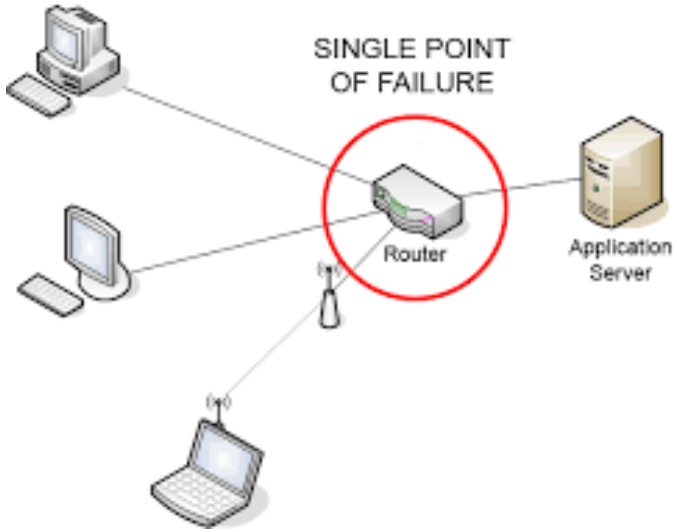
- P2P, M2Mの金融トランザクションは、指数関数的に増加する可能性があるのに対して、規制当局や問題に対処する「人」の数は指数関数的に増えない（予算とリソースは指数関数的に増えない）ため、FATFトラベルルールのような従来型規制アプローチは対応できなくなる。
- そのため、新しい金融秩序の作り手であるビジネス組織とエンジニアから、このギャップを埋める技術の提案が出ることが必要である。



ブロックチェーンの本当の貢献

持続的な単一障害点（Single Point of Failure: SPOF）の除去

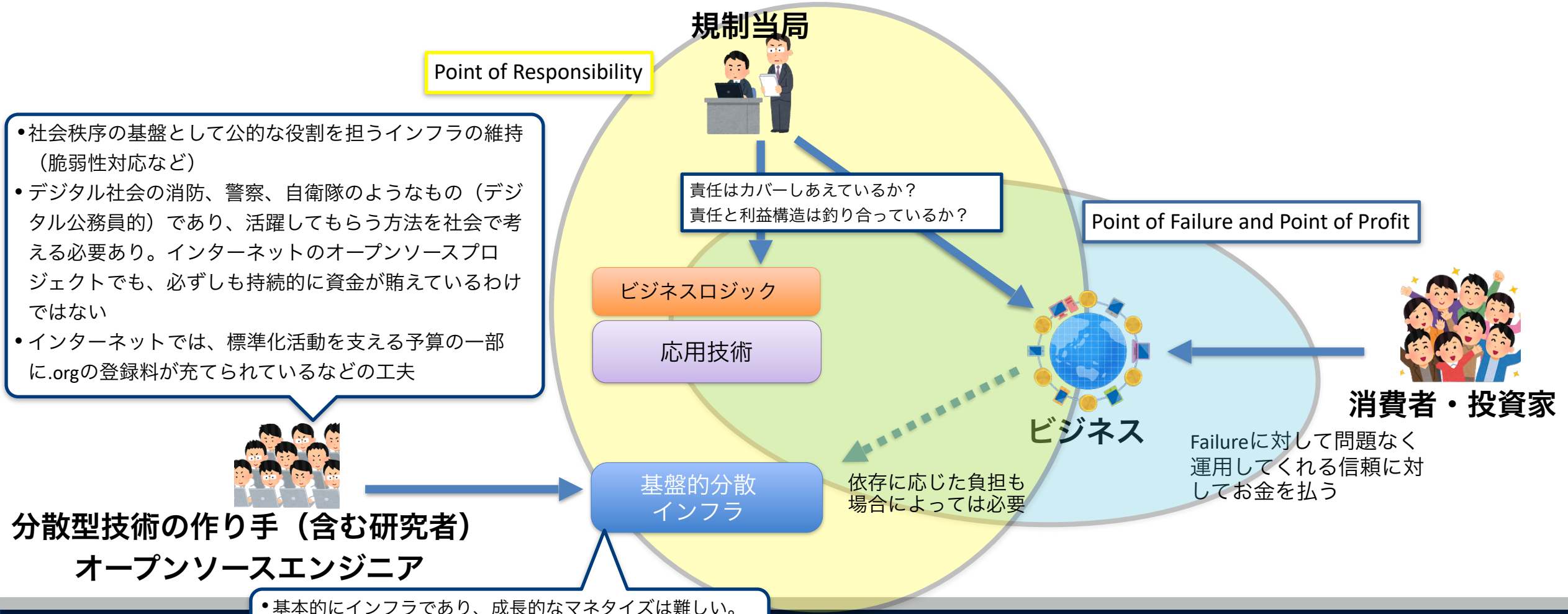
- SPOFの弊害
  - 故障やサイバー攻撃への耐性
  - ビジネス上の継続性
    - 例）暗号学的タイムスタンプによるタイムスタンプサービス vs. ビットコインの発明
- ブロックチェーンの貢献
  - 適切なインセンティブ設計（例：マイニング報酬）があれば、一定数の悪意を持った参加者 or ノードの故障があっても、持続的に台帳を更新できる
  - SPOFがない持続的な台帳があることで、金融サービスの信頼の一部を外部化することが可能になり、イノベーションへのコストを軽減することができる



分散型の技術を取り込んだ持続的なエコシステムを構築するときの課題

Point of Failure - Point of Responsibility - Point of Profit

必要な責任の依存関係をカバーしつつ、責任と利益構造が持続的に釣り合う状態を保ち続けることが重要



- 社会秩序の基盤として公的な役割を担うインフラの維持（脆弱性対応など）
- デジタル社会の消防、警察、自衛隊のようなもの（デジタル公務員的）であり、活躍してもらう方法を社会で考える必要あり。インターネットのオープンソースプロジェクトでも、必ずしも持続的に資金が賄えているわけではない
- インターネットでは、標準化活動を支える予算の一部に.orgの登録料が充てられているなどの工夫

- 基本的にインフラであり、成長的なマネタイズは難しい。例）インターネットのISP
- ビットコインはマイニング報酬を利用した稀有な例（ただし永続するかは未知）

イノベーションの促進と信頼あるシステムの両立へ必要なこと

中央集権的な信頼

- SPOFになり得る
- パーミッションレス イノベーションの 阻害要因

非中央集権的な信頼

- 誰が何に責任を負っているのかが不明確になりがち
- インセンティブ設計が今のところ完全ではない
- 支払いではうまく機能するがより広い応用では未知数

複数の主体による相互協力 Poly-centric Stewardship

パーミッションレスな信頼基盤

GEORGETOWN UNIVERSITY | CyberSMART

ステークホルダー間のコミュニケーションの課題

規制当局

十分なコミュニケーション
チャネルがない
共通言語がない
技術自体への規制の可否

スピードの違い

なるべく規制による制約を避けたい

技術の成熟度への誤解

透明性の欠如

分散型技術の作り手（含む研究者）
オープンソースエンジニア

ビジネス

消費者・投資家

2019 G20 におけるマルチステークホルダー議論

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で合意された分散型金融における対話についてのコミュニケ

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

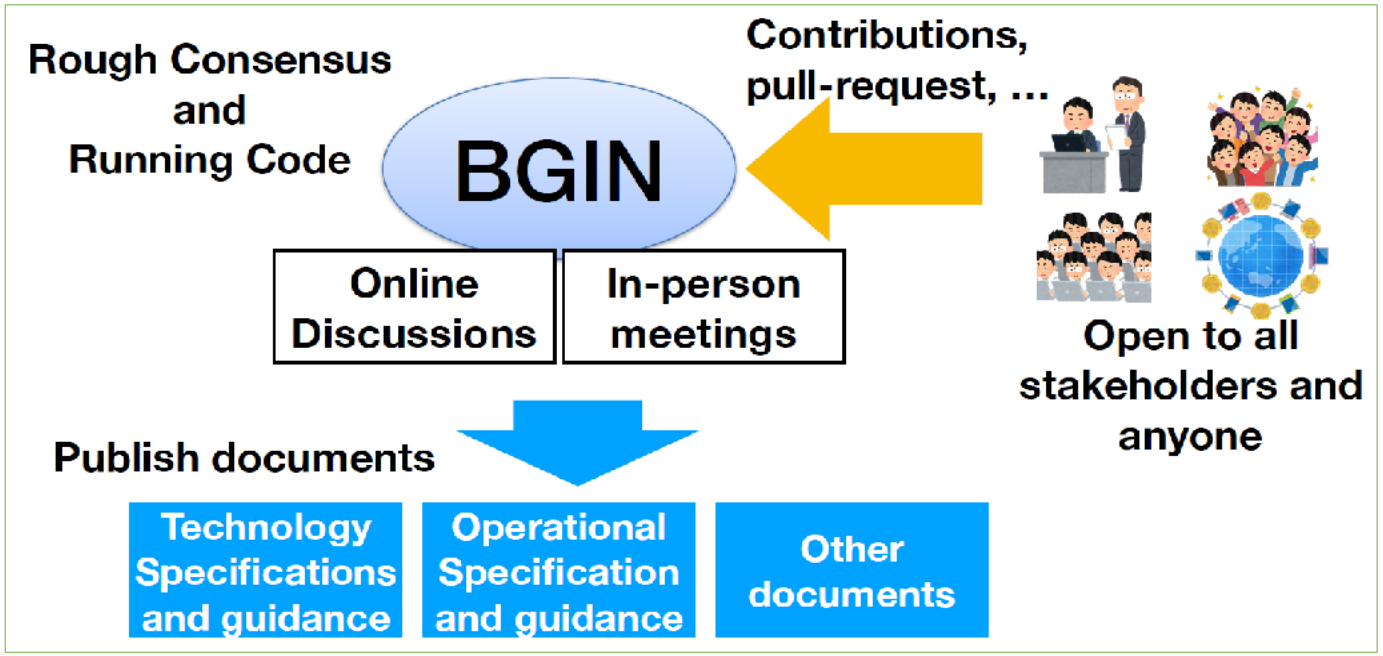
Decentralised financial technologies

Report on financial stability, regulatory and governance implications

6 June 2019

Blockchain Governance Initiative Network (BGIN)の概要

ブロックチェーンコミュニティの持続的な発展を達成するために、共通理解の醸成と
課題への対処のための協力を目的とした、全てのステークホルダーのための公開で中立な場



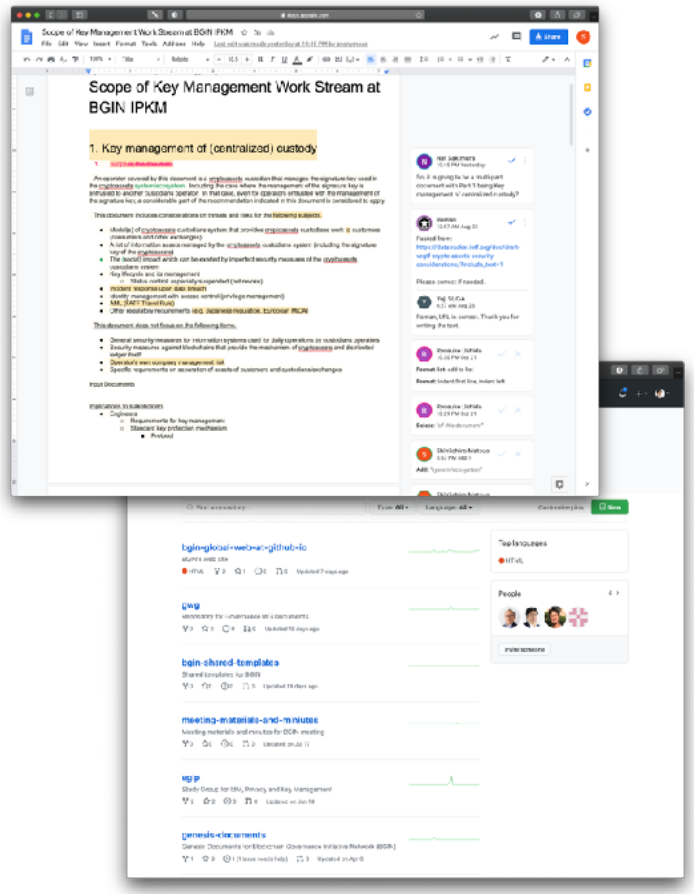
https://bgin-global.org

現時点での目的:

1. マルチステークホルダー間の対話のための公開、グローバル、そして中立なプラットフォームの構築
2. 多様な観点に基づいたステークホルダー間での共通言語と理解の達成
3. オープンソース的アプローチ基づく、信頼ある文書コードの継続的な提供を通じた学術的アンカーの構築

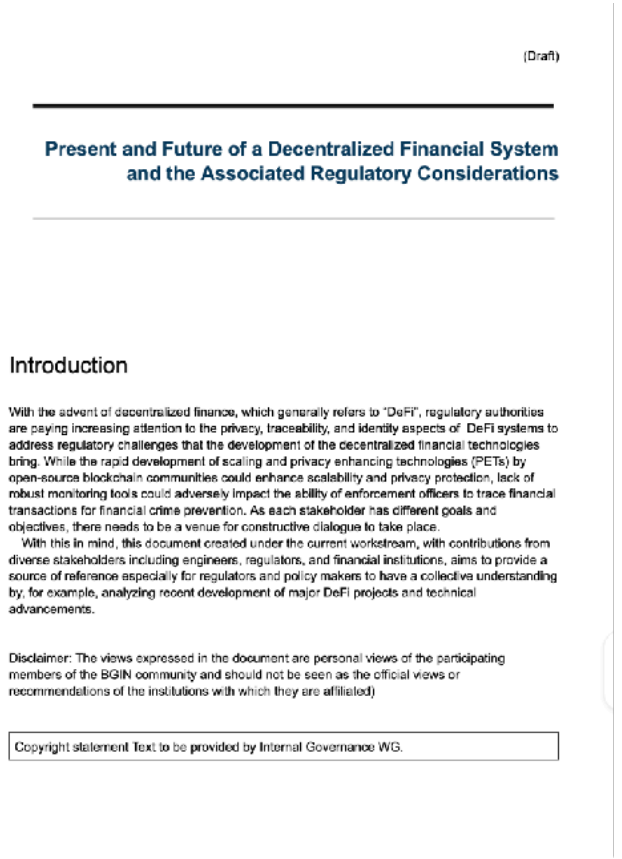
BGINにおける議論の進め方

- 議論は、総会（年3回）、部会（WG/SG/TF）単位で行われる隔週のミーティングで行われる（誰でも参加可能）
  - 総会は現在まで3回開催（全てオンライン）
    - Block #1 2020年11月 ムンバイ/インド
    - Block #2 2021年3月 パリ/フランス
    - Block #3 2021年7月 ワシントンDC,ニューヨーク/米国
    - 今後の予定 Block #4 2021年11月2-4日 アフリカ、Block #5 2022年春 東京/日本
- オンラインの議論プラットフォームとして、メーリングリスト、チャットツールを活用
- 文書の編集は、GitHubとGoogleDocsなどで行われる。編集途中の文書も公開で、誰でも参照やコメントが可能
- ラフコンセンサスによる、文書編集プロセスでの合意



BGINで現在検討中の課題と出版予定の文書

- 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
  - BGIN自体の内部ガバナンス
- 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.

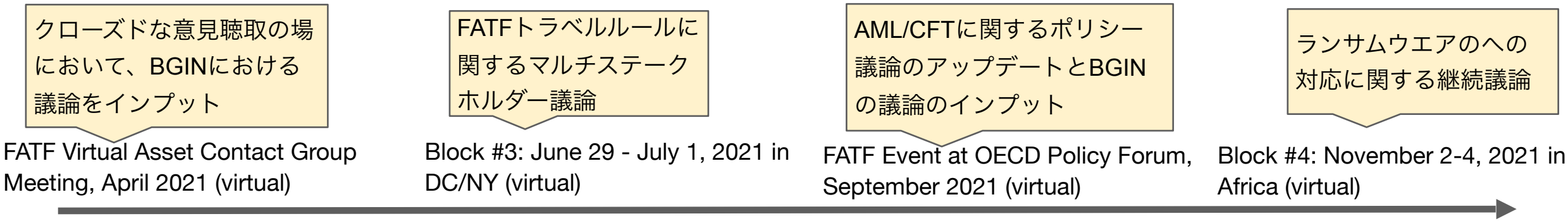
With this in mind, this document created under the current workstream, with contributions from diverse stakeholders including engineers, regulators, and financial institutions, aims to provide a source of reference especially for regulators and policy makers to have a collective understanding by, for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

FATFとの対話

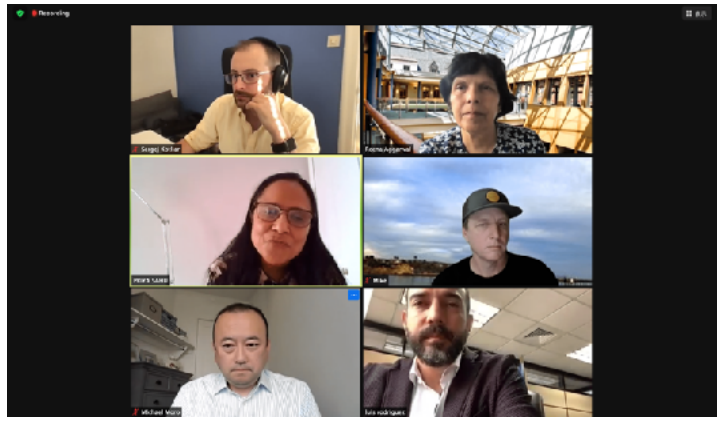
- FATFの暗号資産規制（含むトラベルルール）におけるクローズドな意見聴取の場（VACG）に招待され、BGINでのマルチステークホルダーによるオープンな議論をインプット
- BGIN第3回総会（Block #3）に、FATFからVACG Co-chairが特別講演、及びBitcoin Core等のエンジニアを含むマルチステークホルダーとQ&Aを含む議論を実施。
  - その結果として、FATFを含むマルチステークホルダーの協力の皮切りとして、暗号資産がランサムウエア攻撃の支払いに使われた時のトレースのフレームワークを共に検討することを議論



El Salvadorのビットコイン法定通貨化に関する議論

2021年7月2日（BGIN Block #3 Day3)

- エンジニア、アカデミア（当局経験者）、ビジネス、金融機関（エルサルバドル中米経済統合銀行）関係者によるマルチステークホルダー・ディスカッションを実施
  - ビットコイン法定通貨化の賛成派：金融包摂、イノベーションの重要性（エルサルバドルの人口の70%はUnbankedで、送金手数料の削減、小規模企業へのファイナンス等が喫緊の課題）を強調
  - 慎重派：AML/CFT等の懸念を指摘
- インターネットとの対比で、政府としてリスクをとって早期に新技術へ対応していくことの利点の指摘
- 中米経済統合銀行（開発銀行）としてAML等の規制対応やガバナンス上の課題を克服するために支援を行っていく旨を表明
- 暗号資産セクターへの機関投資家参入にあたっての課題（例：カストディや保険、ETF）やビットコインの本源的価値、取引所の価格発見機能などについて議論
- 当局サイドから、ルールメイキングには当局だけではなく技術者など幅広いステークホルダーが関与すべきとの意見



BGIN Block #3（第3回総会: 2021年7月）での議論

- FATFトラベルルールの改訂についての議論
  - AML/CFTとプライバシのバランス
  - ランサムウエア対策
- エルサルバドルのビットコイン法定通貨化に関する集中討議
- Centralized / Decentralized custodyのセキュリティに関するドキュメントのドラフティング
- DeFiの規制上の論点についてのドキュメントの最終ドラフティング
- BGINの内部ガバナンスに関する議論
- 将来の検討課題の議論
  - SSI/DIDのガバナンス
  - 分散型取引所・カストディのガバナンス
  - NFTのガバナンス

分散型金融の技術、ビジネス、運用、規制を考える上でのコミュニケーションの提案

- We don’t know what we don’t know - お互いに「ぼくのかんがえたさいきょうのきんゆうしすてむ」を作ることはやめる
- まずは共通理解の構築
  - 言葉の定義
  - 規制当局の目的（条件を含めて詳細化する）
  - 目的の達成手段
  - 技術がもたらす可能性、限界
- ステークホルダーが提案し合う形のコミュニケーションのための文化と環境を作る
  - 技術、ビジネス、運用上の懸念点の指摘と改善提案（from 規制当局、アカデミア）
  - Linear vs. Exponentialなどの問題を乗り越えるために、規制を効率化するための技術の提案（from エンジニア）
  - 米国では、規制当局と健全な対話ができる人が企業のチームにいるかどうかが重視されている
- 暗号技術の設計から実装までの安全性を確認する考え方に習い、グローバルなアカデミアを交えた評価・検証プロセスを入れる

コミュニケーションのフォーマットの検討の必要性

- アカデミアを含むステークホルダーが第三者検証するに足りる文書（場合によっては論文）のフォーマットが必要。
  例）
  - 規制当局から、規制上の一般的な懸念を示した文書
  - 新しい技術とそれに基づくビジネスを開発する際に、技術の正当性、安全性を外部評価できるようにするための技術仕様、設計
  - 規制上の懸念点に対する対応
  - 必要に応じて、規制の修正提案とその修正を支えるツールや運用の提案
- 異なるステークホルダーの間で文書（技術仕様や運用）を合意するためのプロセスが必要。
  例）
  - アカデミアによる公開評価（場合によってはコンペティション）
  - 自己評価書の提出と、エキスパートによる追試
  - 評価基準が定まっていない場合には、評価基準や方法についても公募

参考資料

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 Fransisco, US

Danny Ryan
Ethereum Foundation

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

Julien Bringer
CEO, Kallistech
Paris, France

Nat Sakimura
Chairman, OpenID Foundation
Tokyo, Japan

Nii Quaynor
Chairman, Ghana Dot Com Ltd
Accra, Ghana

Pindar Wong
Chairman, VeriFi Limited
Hong Kong, China

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

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

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

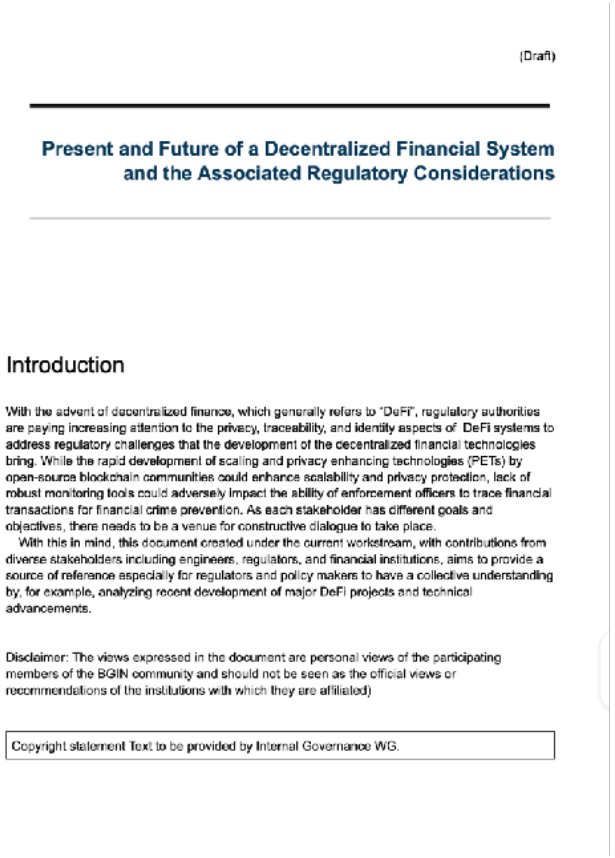
Joaquin Garcia-Alfaro
Full Professor, Institut Mines-Télécom / Institut Polytechnique de Paris
Paris, France

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

分散型金融に関する規制上の考慮点についてのドキュメント



(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)

GEORGETOWN UNIVERSITY | CyberSMART

Internet Governance as an Ecosystem

International vs. Global

Multi-stakeholder Conversation

IGF Internet Governance Forum

Governments

As one of stakeholders

Non Profit

ICANN

Manages Domain names

Non Profit

Internet Society

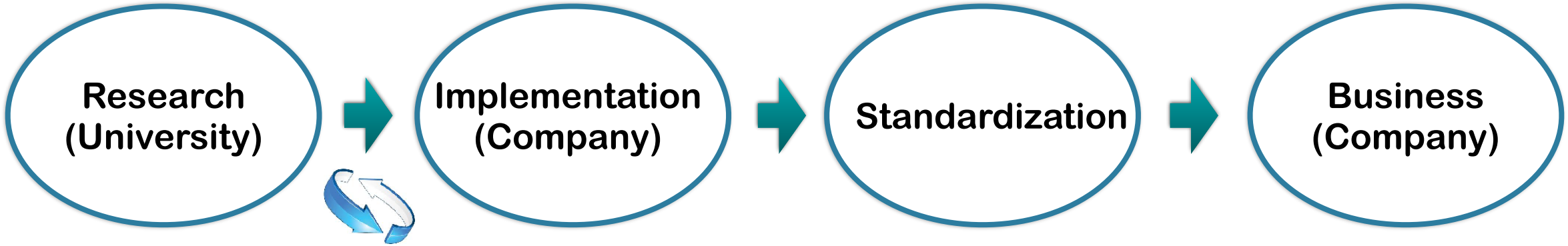
IETF®

Technology Standard

Participation as individual

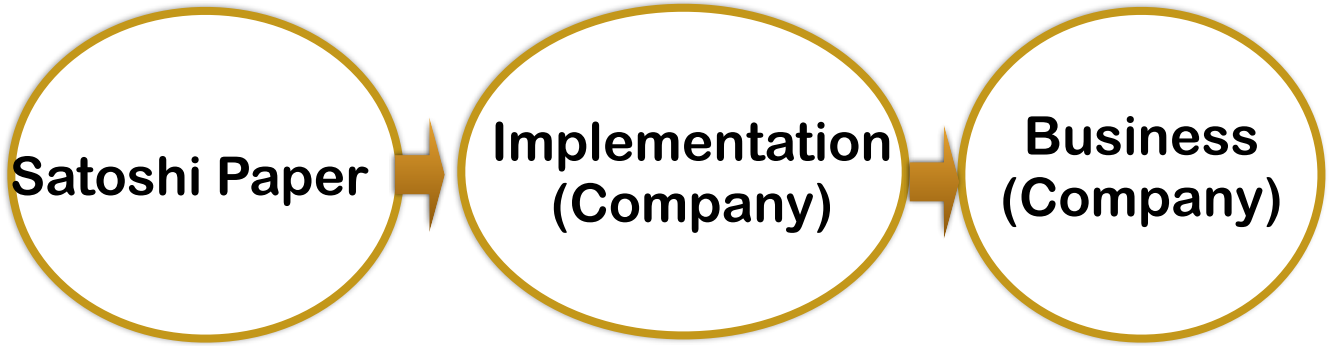
Academic Research is still needed

The Case of Internet Technology

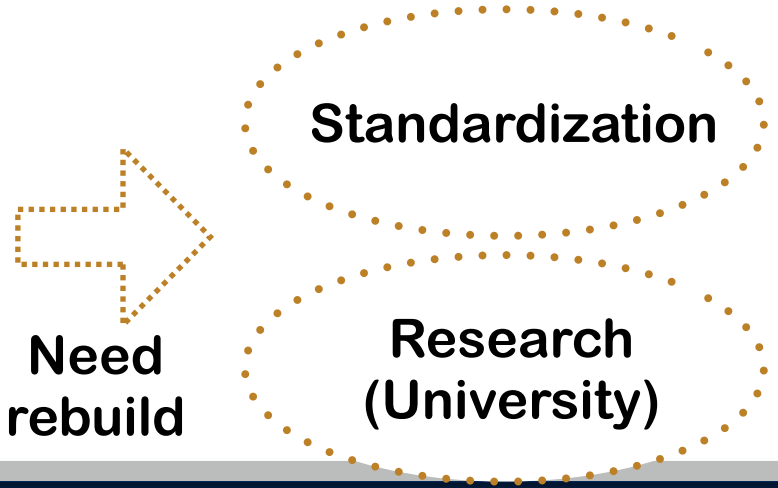


"BSD" and open-source facilitated innovation

The Case of Bitcoin and Blockchain



Innovation by iteration



NSFNet for the Internet

ARPANET

CSNet

Research Networks (NSFNET)
Non-Profit

Externalizing Costs
Commercial ISPs
Making $$$

1969

1981

1985

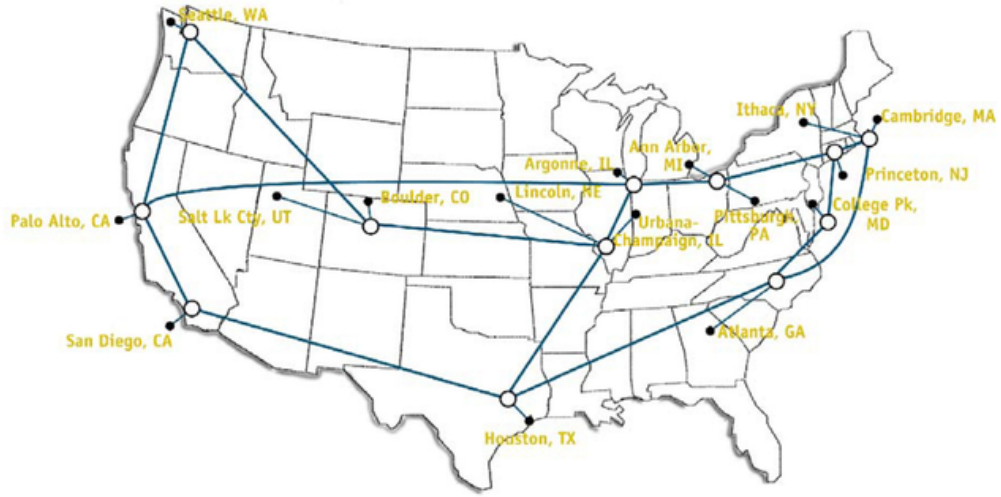
CIX Association
1991

April 30th 1995

1977 — 1995

Berkeley Software Distribution (BSD)

NSFNET T3 Network 1992

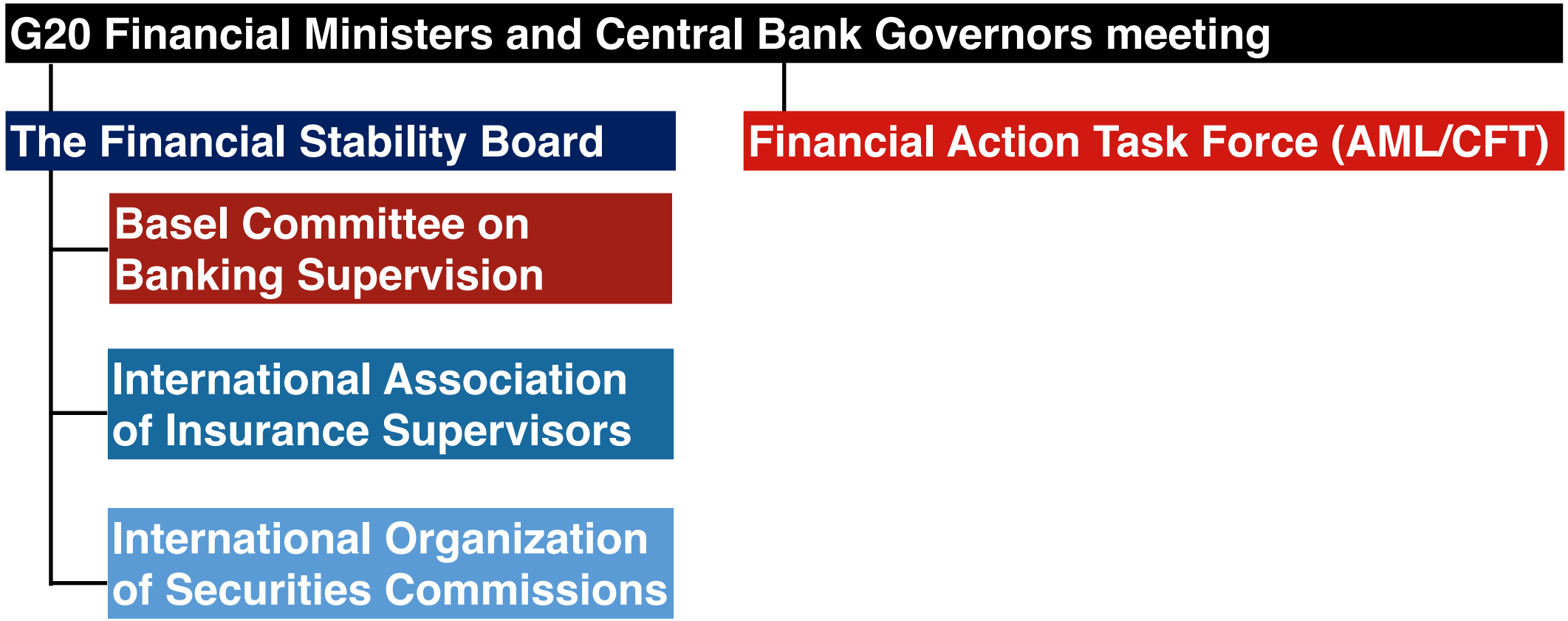


BSafe.network: Plays the same role as NSFNet and BSD

- 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)



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 FINANCIAL STABILITY BOARD

Decentralised financial technologies

Report on financial stability, regulatory and governance implications

6 June 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.**

ブロックチェーンに基づいたシステムの安全性の観点

運用	鍵管理、監査、バックアップ	ISO/IEC 27000
実装	プログラム、セキュアハードウエア	ISO/IEC 15408
ビジネスロジック	金融トランザクション, 契約	Secure coding guides
応用プロトコル	プライバシ保護, セキュアトランザクション	ISO/IEC 29128
基本プロトコル	P2P, コンセンサス, マークル木	ISO/IEC 29128
暗号アルゴリズム	ECDSA, SHA-2, RIPEMD160	NIST,ISO

暗号技術の設計から実装までの安全性確認の全体像

ISO/IEC 29128

暗号プロトコル

（SSL/TLSなど）

実装

暗号アルゴリズム

（AES/RSAなど）

実装

ソフトウエア

ハードウエア

運用

数学的な安全性証明
学会の査読によるチェック

Common Criteria
JCMVP

ISMS

Thank you!

GEORGETOWN UNIVERSITY
CyberSMART