

ブロックチェーンのイノベーションに対する価値と グローバルな視点で推進のための注力すべきこと



December 16, 2022

Shin'ichiro Matsuo, Georgetown University

GEORGETOWN UNIVERSITY
CyberSMART

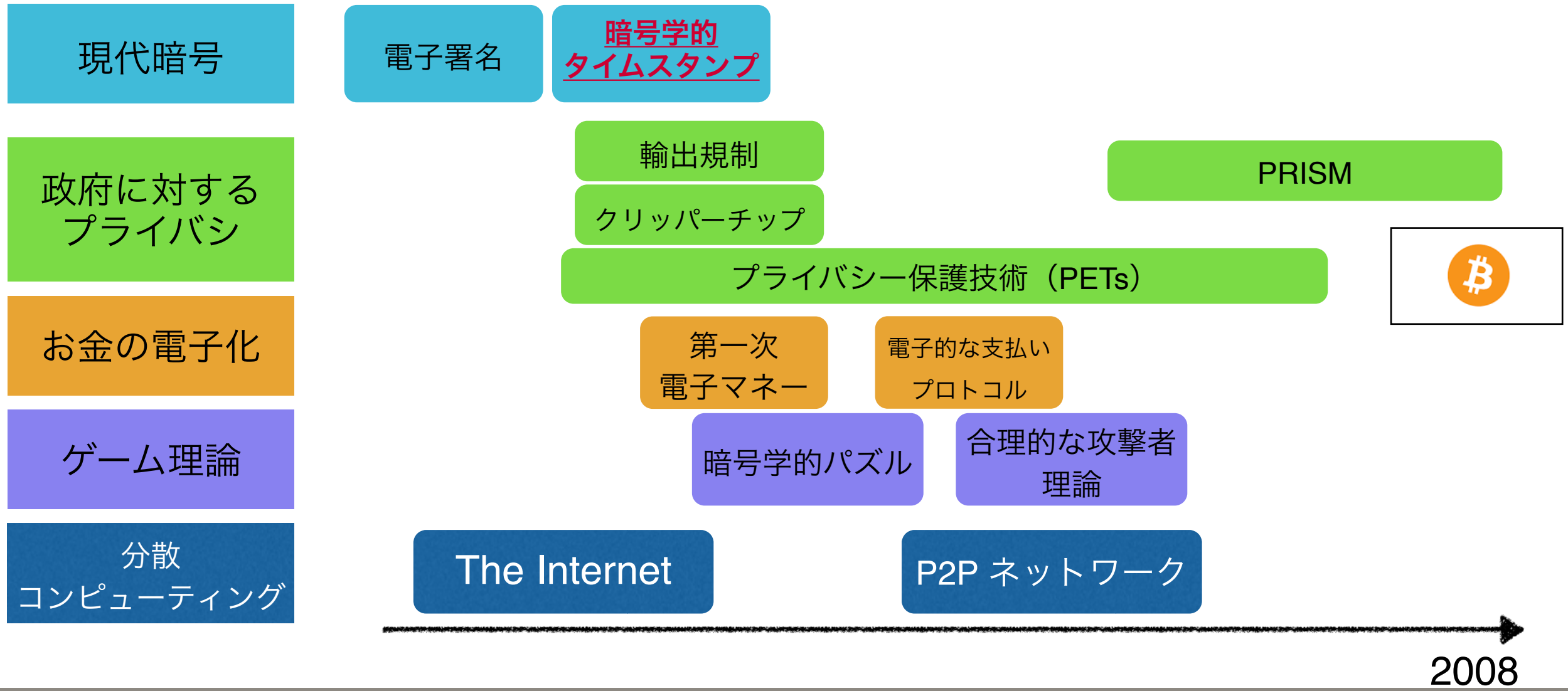
Satoshi NakamotoのWhite Paper (未査読) に書かれているBitcoinの説明

同意している二者が信頼できる第三者を必要とせず、直接取引が可能な、トラストの代わりに暗号的証明に依拠する電子支払いシステム

分散されたピア・ツー・ピアのタイムスタンプサーバーを使って、トランザクションの時間的順序の計算機的証明を生成することによる、二重支払い問題を解決するシステム

Satoshi論文の中には、Currency（通貨）という言葉や、Decentralized（非中央集権）という言葉が一回も出てこないことに注意

Bitcoinの発明に至る技術史



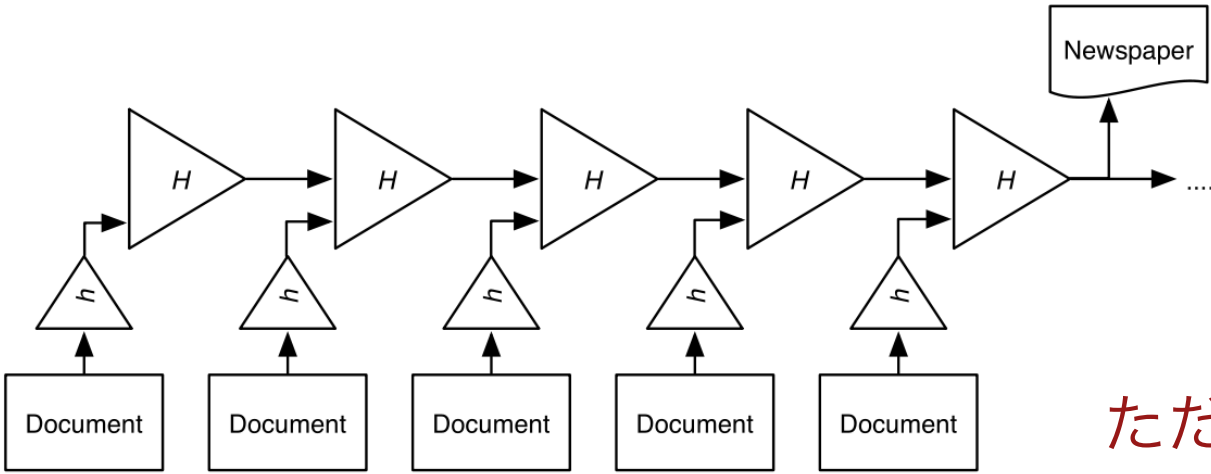
暗号的タイムスタンプ - ブロックチェーンの基本的データ構造 - (1990)

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

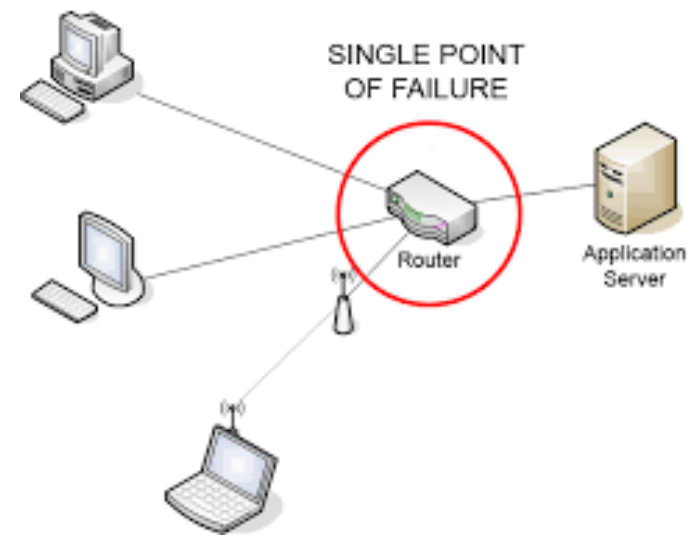


ただし、信頼できるサービス提供事業者が必要

ブロックチェーンの本当の貢献

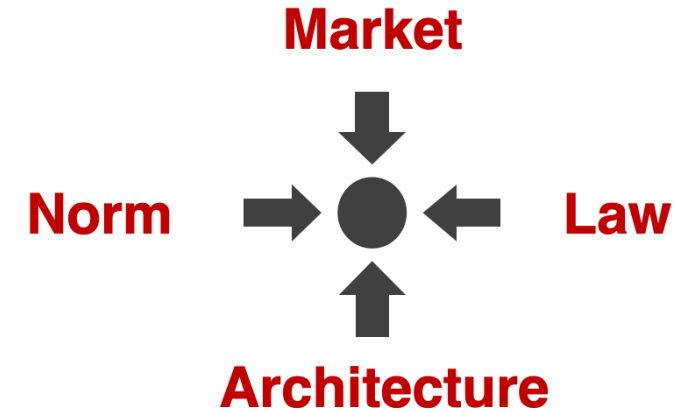
持続的な単一障害点（Single Point of Failure: SPOF）の除去

- 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、さまざまな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



デジタル化の意味：なぜ我々はソフトウェアを書くのか

- ソフトウェアがデジタル「社会」のルールを規定する時代になった。そのルール作りのためにソフトウェアを書く。
 - Lawrence Lessig “Code”
 - デジタル市場のルールと市場は、プラットフォームのソフトウェアが規定
- なぜ日本はデジタル不戦敗したのか
 - ルール作りとソフトウェアの関係を理解していなかった
 - そもそも、日本人はルール作りよりルールに従う傾向



<i>High</i> <i>Business Criticality</i> <i>Low</i>	Rule Makers ■ Dictate industry ■ Larger market share ■ Higher margins	Rule Breakers ■ Born on the Web ■ Out of market ■ Radical innovation
	Rule Takers ■ Have rules dictated ■ Laggard ■ Lower market share	Rule Shakers ■ 2nd/3rd tier ■ Space invaders ■ Innovators
	<i>Low</i>	<i>High</i>
	<i>Practice Innovation</i>	

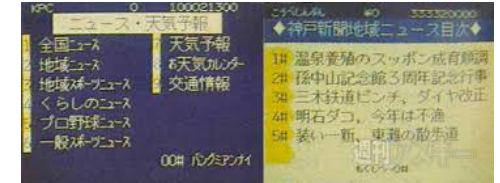
インターネットの開発・普及が変えたイノベーションのあり方

パーミッションレスイノベーション

- 通信チャネルと多方向の通信の権利をアンバンドル (新たなルール作りがやりやすいアーキテクチャ)
 - 非中央のアーキテクチャ: Routing, BGP
 - テクノロジーのレイヤ化
- TCP/IP, i.e. “stupid network”
- アンバンドル化が、新しいサービス、ビジネス、経済の発生を草の根から促進
- ただし、Step-by-stepであり、インターネットらしい多方向のサービス（例：SNS）の登場は、インターネット商用化の約8年後



Minitel (France)

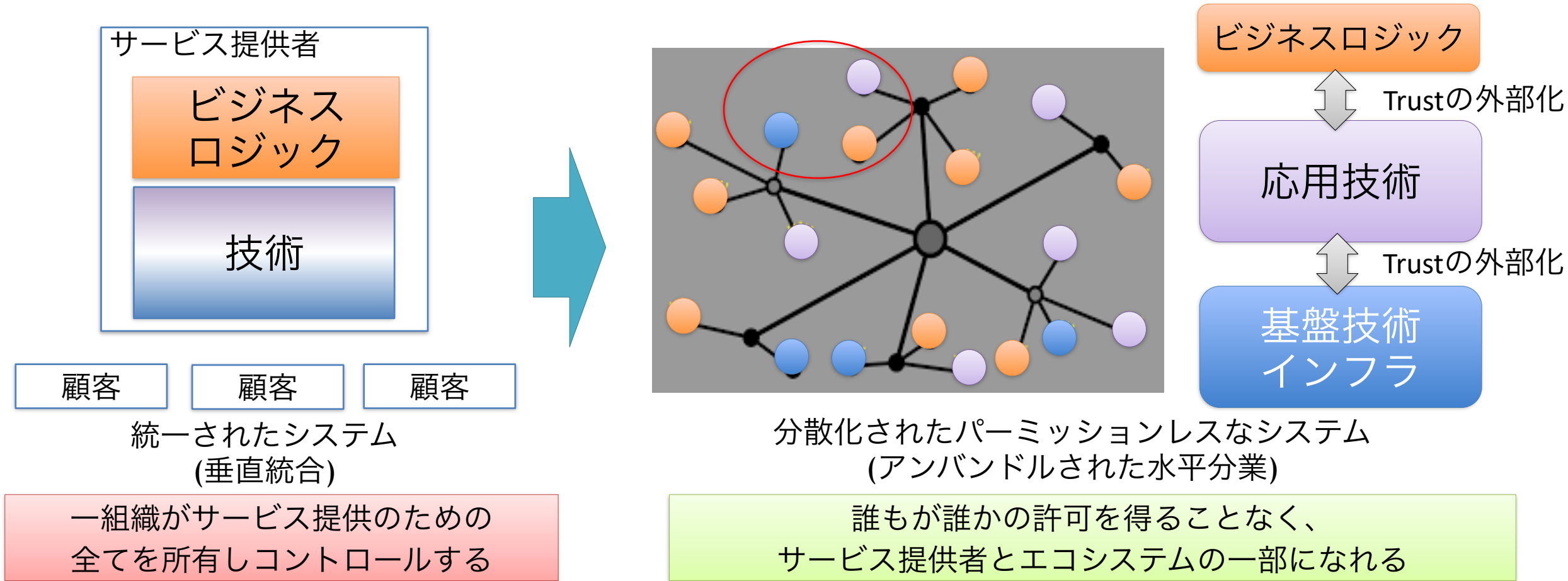


CAPTAIN (Japan)



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



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

ブロックチェーンが「台帳」に加える産業的メリット

- 長期保証が可能な持続的な台帳は、人間社会のあらゆる経済活動の根幹
 - マイニング等の報酬メカニズムが機能する限りにおいて一企業が管理するより持続的（一企業が単独で赤字でも長期（永久）保証をするサービスができるか？）
- 台帳から単一障害点を取り除ける
 - サーバの障害だけではなく、ビジネス上の理由による事業の停止・撤退などがあってもシームレスに台帳を継続可能
- プログラム可能性と複数の帳簿の柔軟な連携
 - 単なる資金移動だけでなく、より複雑なビジネスプロセスやシステム連携を容易が容易になる
- 簿記と会計に関する不確実性の軽減
 - 現在の簿記と会計システムにおける不確実性（粉飾やバブルの元）を、プログラム可能な帳簿により軽減
- オンボーディングが容易なオープンイノベーションの土台
 - 規制に準拠した台帳システム（会計監査、税制）の外部化によるスタートアップの初期コストの大幅低減
 - グローバルな共通台帳による、協業、オープンイノベーションの促進

ブロックチェーンの課題と日本における推進のために必要な技術投資の骨格

ブロックチェーンの課題

- セキュリティ・トラスト
 - 鍵管理
 - 危殆化対策
 - ブロックチェーンのトリレンマ、スケーラビリティとセキュリティ
 - スマートコントラクトセキュリティ
 - オラクル問題（よく指摘されているNFTの問題もここに帰着する）
 - ブリッジ問題
 - 安全性証明がない
 - インシデントハンドリング・レスポンス
- 運用上の課題
 - 永続性（暗号の危殆化、経済的インセンティブ）
 - 電力消費問題（本来の思想やセキュリティとのトレードオフ）
- 規制上の課題
 - 証券該当性
 - ガバナンス問題

セキュリティとスケーラビリティを
両立させる理論と技術

システムセキュリティの技術と運用

社会工学・経済学とコンピューター
サイエンスとの協業

規制対応のための技術
(Regtech/Suptech)

ブロックチェーンエコシステムに必要な人材

	従来型(非ブロックチェーン)システム	コンソーシアム型ブロックチェーン利用システム	パブリック型ブロックチェーン利用システム
テクノロジー	- 機能要件整理(業務フロー等) - 非機能要件整理(セキュリティ, 可用性等) - UI/UX検討 - 基盤/ミドル/APフレームワーク選定 - 基盤/ミドル/AP設計・構築・実装 - APデバッグ - 運用監視、障害検知方式 - 障害解析/リカバリ/修正	+ - ブロックチェーン基礎知識/基盤ごとの特性把握/基盤選定 - 秘密鍵のセキュリティ ※過去に暗号資産の流出事件が多発 - 秘密鍵管理のUX検討 ※秘密鍵のライフサイクル(発行・更新・破棄)をいかに簡単にするか - スマートコントラクトAPの設計・実装 - スマートコントラクトAPのデバッグ ※スマートコントラクトのバグを空いた事件が多発 ※障害発生時にリカバリはできない	+ Layer-2技術の理解・動向把握 (相互運用性、トラスト基盤(DID)等) ※個々のノードの運用監視はできない ※障害発生時にリカバリはできない
メソドロジー	- 非機能要求の基準(非機能要求グレード) - セキュリティ基準(FISC, PCIDSS等) - 開発方法論(ウォーターフォール, Agile) - アーキテクチャのベストプラクティス (オンプレ/クラウド, モノリス/マイクロサービス等) - デザインパターン/APフレームワーク - セキュアコーディング手法 - テスト手法/解析ツール - 運用フロー/運用製品・ツール	+ - ブロックチェーン利用システムにおける非機能要求の基準 - インシデント発生時の対応方針/BCPの策定 - ブロックチェーン利用システムにおけるセキュリティ基準 - ブロックチェーン利用システムのアーキテクチャ - スマートコントラクトAPのセキュアコーディング手法 - スマートコントラクトAPのテスト手法/解析ツール ※これらの基準/手法は現存しないか、現存していたとしても枯れていない認識	+ - 法規制/標準規格の理解・動向把握 - DAOのガバナンス
リレーション インタラクション	- 製品ベンダとのリレーション構築 - OSSコミュニティ/コンソーシアムへの参画・コミット活動	+ - ブロックチェーン基盤ベンダとのリレーション構築 - ブロックチェーン関連コミュニティ/コンソーシアムへの参画・コミット活動	※不特定多数のノードで実行されるため、サービス提供者と実行者の間でインタラクションはない

第1回デジタル資産ラウンドテーブル平栗勇人 様 (NTTデータ) 資料「分散台帳技術を用いたシステム開発・運用に必要なスキルマップ」より

アメリカのデジタル資産に関する大統領令とフォローアップ

- 2022年3月に署名された、デジタル資産の責任ある開発に関する大統領令に対する対応が2022年9月16日に公開された
 - 投資家保護
 - 安全で安価な金融サービスへのアクセス
 - 金融安定
 - 責任のあるイノベーションの追求
 - グローバルな金融のリーダーシップ
 - 金融犯罪の防止
 - CBDCの開発
- 赤字の項目で、NSF, NIST等を通じた大規模な研究開発を宣言



アメリカのデジタル資産に関する大統領令とフォローアップ

- 米国は、この分野がデジタル社会におけるグローバルなルールメイキングの鍵になる認識の表れ。
- 安全で安価な金融サービスへのアクセスでの要求の例

The National Science Foundation (NSF) will back research in technical and socio-technical disciplines and behavioral economics to ensure that digital asset ecosystems are designed to be usable, inclusive, equitable, and accessible by all.

NSFは、デジタル資産エコシステムが、全ての人にとって使い勝手がよく、包摂的で、公平で、アクセス可能であるようにするために、**技術、社会工学、行動経済学の研究**を支援する。



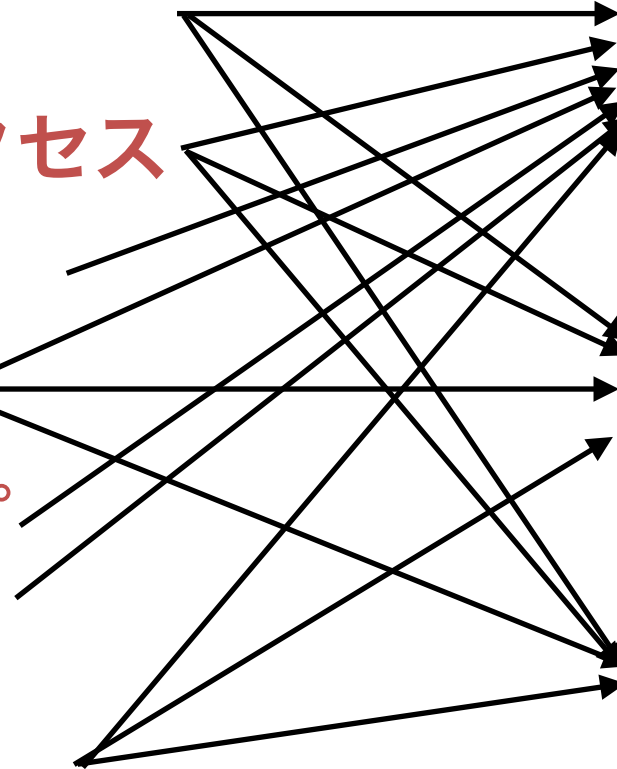
大統領令とフォローアップ文書が求めている次のステップ

- 投資家保護
- 安全で安価な金融サービスへのアクセス
- 金融安定
- 責任のあるイノベーションの追求
- グローバルな金融のリーダーシップ
- 金融犯罪の防止
- CBDCの開発

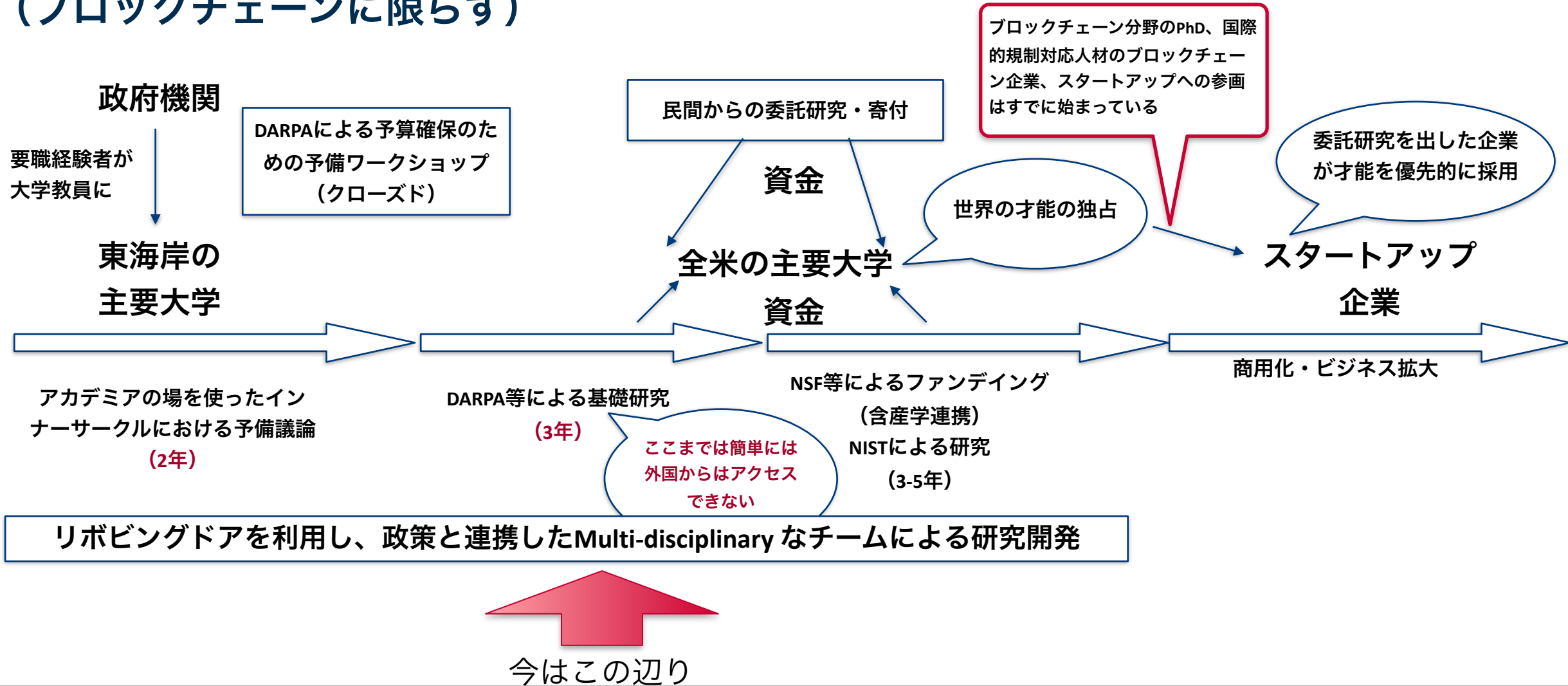
教育
人材育成
標準化

工学的・
社会工学・
経済学的研究

理論的研究



一般論としての米国の研究開発のエコシステムとパイプライン (ブロックチェーンに限らず)



日本政府として注力すべきこと（提言）

• 研究開発のメインストリームへの投資

- ブロックチェーンの革新的技術である暗号技術、分散コンピューティング技術、ゲーム理論などの先端研究への投資が必要
- 米国大統領令は、これらの分野が今後のグローバル社会における主要なルールメイキングの原動力であるということの表れ
- インターネットの歴史（NSFNet, BSD）に学び、テストベッドの構築を通じて技術と人材の集積地とするための活動
- 貢献の舞台である標準化へのフォーカス（ISO TC307, BGINなど）

• グローバルな視点での人材への支援

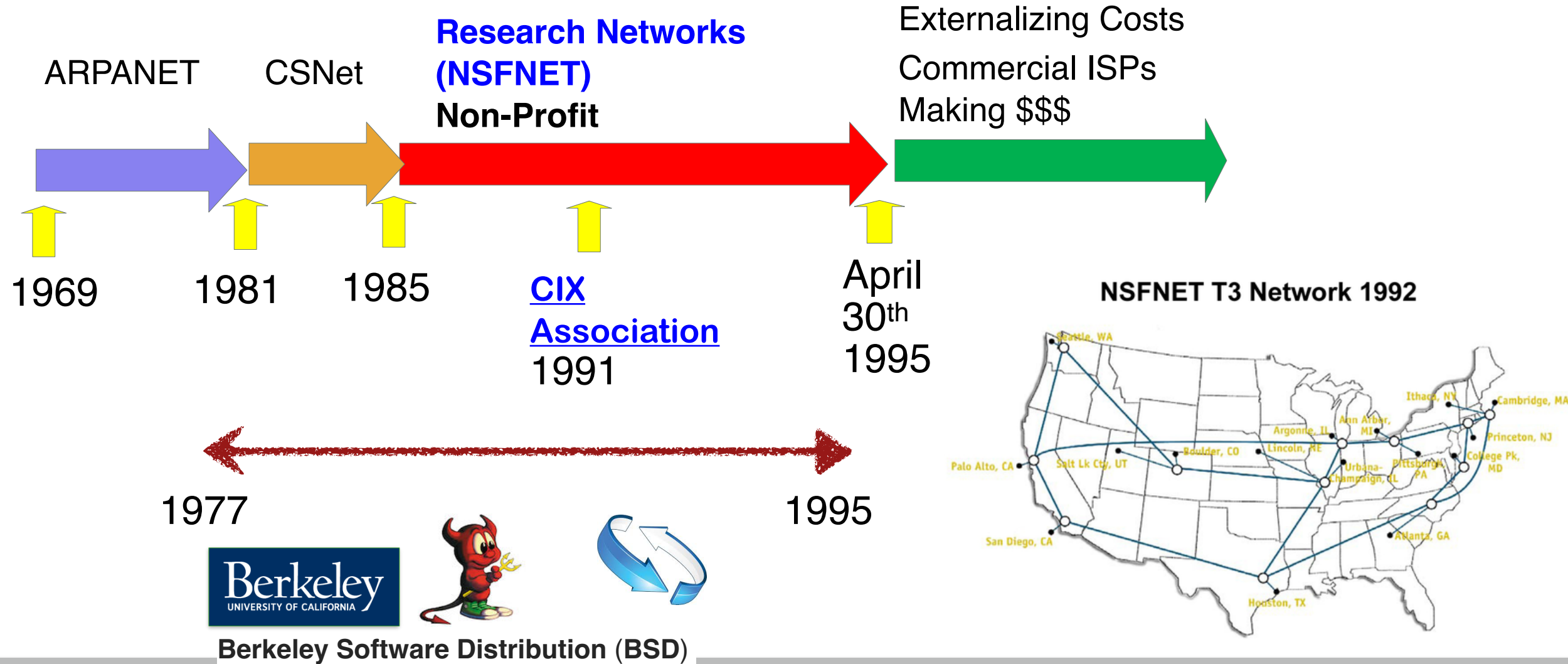
- ブロックチェーン技術はグローバルな技術であり、同時に国レベルでの調整（インターナショナル）を理解した人材こそが重要。事業家だけではなく、理論、技術、運用において世界をリードする人材が、グローバルに活躍するサポートが必要。
- 文部科学省の戦略的国際共同研究プログラム（SICORP）、「世界のトップ研究者ネットワーク参画のための国際研究協力プログラム」
- 未踏の優秀な若手の国際的派遣

• 税金だけでない、米国並みの事業環境整備（スタートアップエコシステム全般）

- 米国では、大学、VC、スタートアップによる戦略的な投資と人材獲得戦略が活発に行われている（例：ブロックチェーン人材（Ph.D., 規制対応人材など）。米国から見る限り、ブロックチェーン分野で、日本のVC、スタートアップは、グローバルな人材確保を含む戦略的な運用が見られない。この点の改善が必要。日本にもブロックチェーン分野の技術分野で先端的な人材は少ないながらもいるが、プラットフォーマーや海外のプロジェクトに取られている。
- 異なるステークホルダーの間での知見の集約・移転の場への支援（草の根ベースで行われている、デジタル資産ラウンドテーブルなど）

參考資料

インターネット商用化前の道のり



Berkeley Software Distribution (BSD) UNIXの歴史

AT&T
Unix

Came to
Berkeley

Beginning of
BSD Unix



Ultrix (DEC)



SunOS

4.4 BSD Lite
Release 2

1969

1974

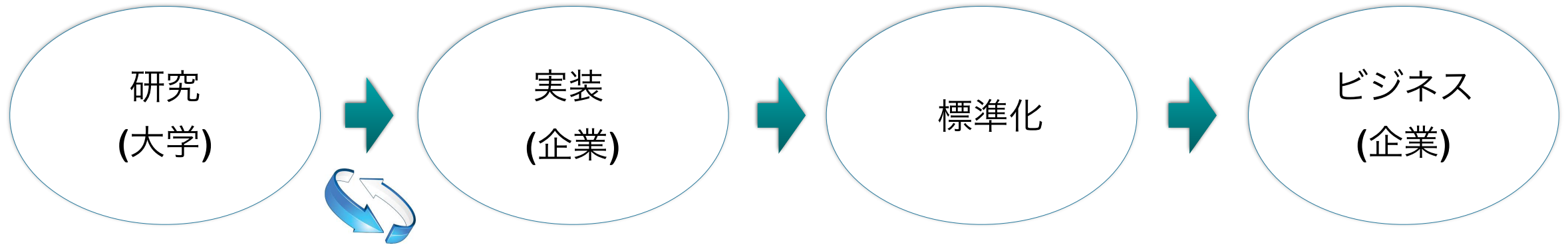
1977

1990

1995

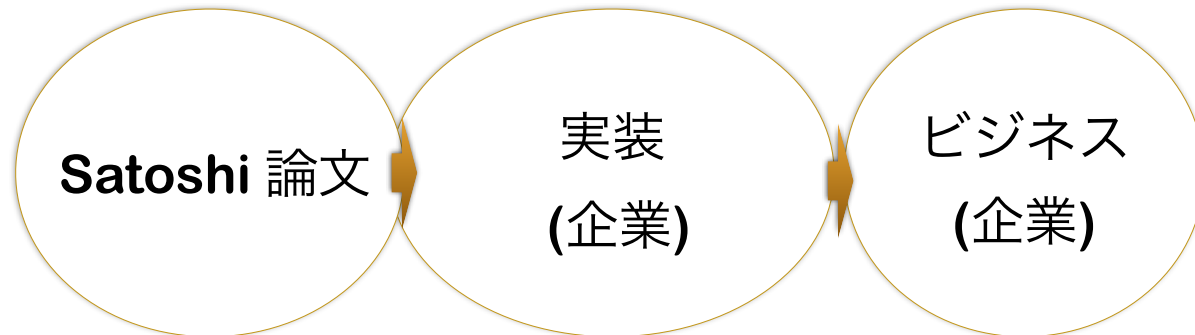
アカデミアの貢献の経緯の違い

インターネットの技術の開発

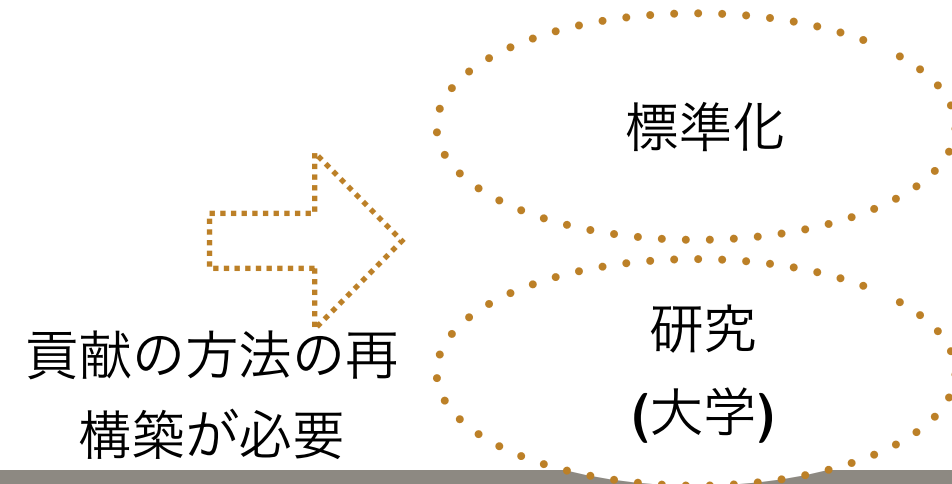


“BSD” とオープンソース開発が貢献

Bitcoinとblockchainの開発



スタートアップ的アジャイル開発が中心



Berkeley Software Distribution (BSD)から出てきたもの

学術からの貢献がUnixのコードを成熟させた

数多くの子孫



インターネットエコシステムの強固な基盤を作り上げた

ここで集積された知見や数多くのエキスパートやエンジニアが、のちのLinuxなどのOSの開発に役立った

記 号 処 理 31-3
(1 9 8 5. 3. 1 2)

続・電子メール呼びかけ報告記

徳田雄洋（山梨大学工学部）

徳田英幸（カーネギーメロン大学）

[https://ipsj.ixsq.nii.ac.jp/ej/index.php?
action=pages_view_main&active_action=repository_action_common_download&item_id=31355
&item_no=1&attribute_id=1&file_no=1&page_id=13&block_id=8](https://ipsj.ixsq.nii.ac.jp/ej/index.php?action=pages_view_main&active_action=repository_action_common_download&item_id=31355&item_no=1&attribute_id=1&file_no=1&page_id=13&block_id=8)



２．呼びかけ以前

（1977年9月－1983年12月）

呼びかけ人の一人である徳田英幸（現カーネギーメロン大学）は、USENETに依存するウォータールー大学の大学院に、1977年9月より在学中、機会あるごとに電子メール網への参加の重要性と日本が研究開発用の電子メール網から孤立していることを、日本からの来訪者に説明した。KDDの関係者も含め何人かの人々に、USENETの論理マップ等の資料を手渡ししたが、ほとんど効果はなかった。徳田英幸は1983年9月に、ARPAインターネットの参加地点であるカーネギーメロン大学へ就職した。

片山卓也(東工大)は、1983年4月より、JUNETとCSNET に依存するノースカロライナ大学に在外研究員として滞在し、電子メール網の重要性を痛感した。同大学のブルース・スミスと共に、日本と米国間の電子メール接続法を検討する。こ

3. 呼びかけ (1984年1月 - 7月)

1984年1月はじめ 何人かの日本からの来訪者との議論を通じ、筆者たちは電子メール網参加の呼びかけを行うことに決める。基本的には、企業内ネットの協力を仮定せずに、USENETタイプのリレーを国際間・国内間に持ちたいという提案の内容とする。呼びかけの方法は、直接郵送、bit誌への寄稿、情報処理学会誌への投稿とすることに決める。

この頃、村井純(東工大)は、日本UNIX
ユーザ会の中に、ネットワーク研究会を
発足させた。

以上の呼びかけを通じて、何度か議論
にのぼった話題を以下にまとめる。

1) USENET型メールリレーの法律的問題

新しく成立した電気通信事業法の下で
の、日本国内におけるUSENET型メールリ
レーの合法性の検討を行う。

2) 単一計算機上の電子コミュニティ

リモートログインとファイル転送のみ
からなる単一計算機上の中規模電子コミ
ュニティの実験を行う。すなわち、かつ
ての 米国のTHEORYNETの試みの日本版で
ある。関連して例えば、KERMITプロトコ
ルの国産パソコン用ソフトウェアの交換
を促進する。

4) 大規模プロポーザル

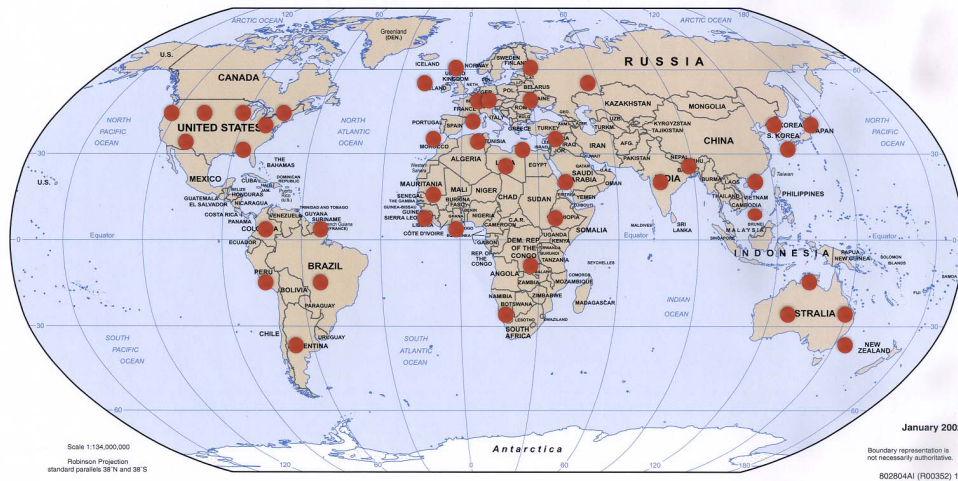
日本の中に、米国のARPAインターネットやCSNET、そして欧州のESPRIT IESに相当する計算機科学研究用のコンピュータ・ネットワークを建設する具体的プロポーザルを作成する。

現在、日本国内に満ちあふれている、VIDEOTEXを中心とした”ニューメディア”のかけ声の中で、オールドメディアが既に持っている可能性を、広範囲の人々に説明することは、法律制度、文化基盤の違いもあり、大変難しいことである。

1985年10月には韓国のソウルで太平洋沿岸国のコンピュータ・ネットワークと電子メール網に関する会議がアジアではじめて開催される。また日本と米国の経済学者とシミュレーション専門家の一部のグループがNSFにプロポーザルの提出準備中で、大規模なCSNETへの参加を計画していると伝えられる。

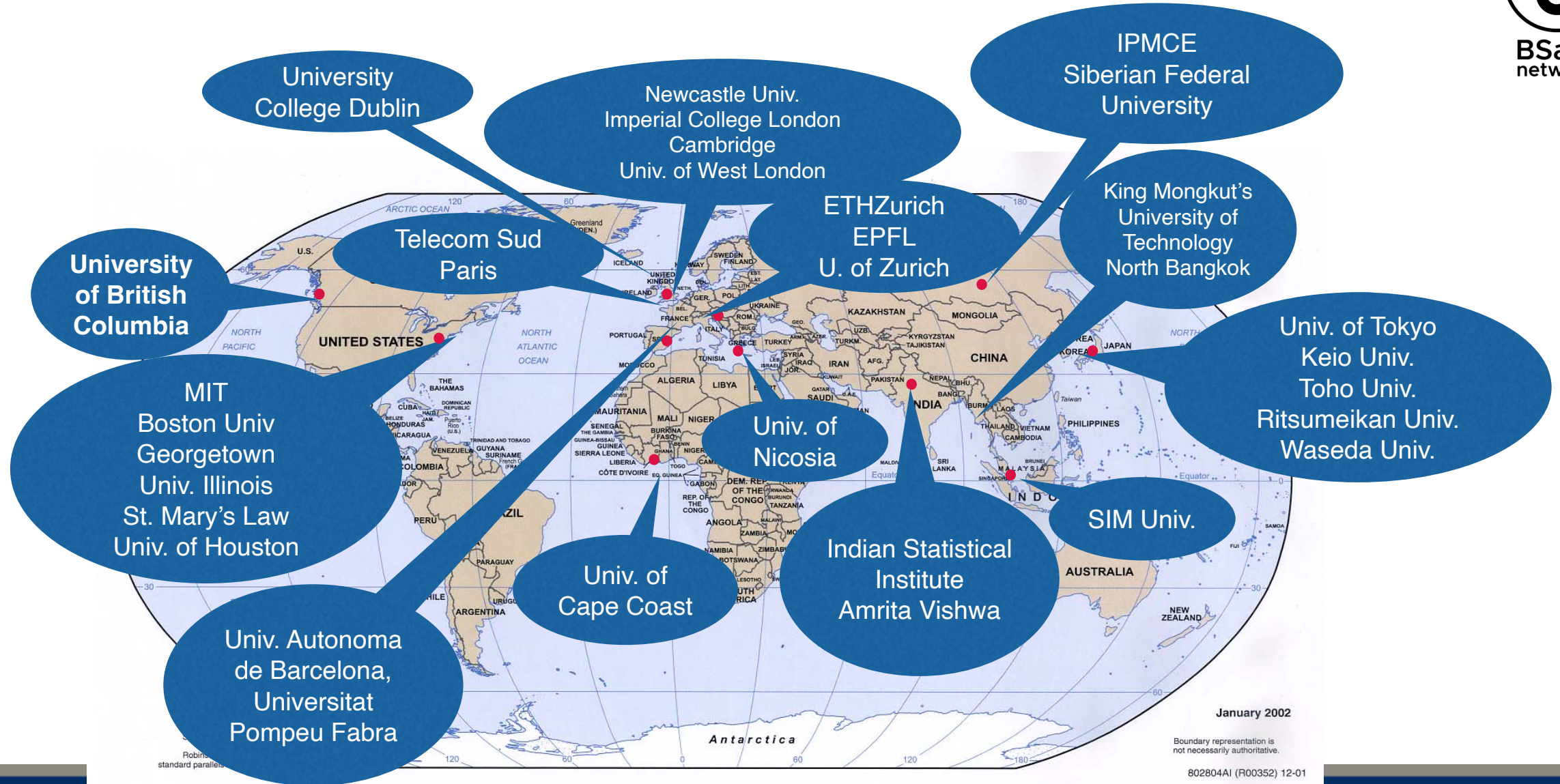
BSafe.network: ブロックチェーン技術開発によるNSFNet and BSD

- ・ グローバルな大学の連合による、ブロックチェーン技術の中立的、安定的、持続的な研究用テストネット
- ・ アカデミによる中立な知見の提供源
- ・ 2016年に設立。各大学が実験用ノードを運用



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

31 Universities Already Join and We Add More...



Thank you!



GEORGETOWN UNIVERSITY
CyberSMART