ブロックチェーン技術の成熟に向けた国際的学術研究ネットワークBSafe.Network の取り組み

松尾真一郎

「ブロックチェーンの未来」ワークショップ

一般的なイノベーションと技術の成熟の進み方

繰り返しによる改善

研究・実験

技術の検証

商用化

新しいアプリケーションとエコシステム

安定性・成熟度

ブロックチェーン技術の成熟度の現在地は？

SSL/TLSにおける事例

2011年以降、数多くのプロトコル仕様や実装の問題が発覚

Heartbleed, Poodle, FREAK, DROWN, CCS Injection

問題の原因

SSL/TLSには安全性の十分な証明や検証結果がない

SSL/TLSを策定した当時、Netscape社、IETFで安全性検証を行う公式プロセスがなかった。

SSL/TLSを策定した当時、安全性検証を行う十分な数のエキスパートがいなかった。

プログラムコードの品質保証が必ずしも十分ではなかった

the DAO事件

50Mドルが流出してしまう可能性があった事件

コードの脆弱性により発生

このようなコードの脆弱性による問題が発生した時に、公式にどう対処すr
べきかについて、標準的な解決策は決まっていない

The DAO事件の教訓

コードの検証の必要性

脆弱性ハンドリングと対象プロセスの必要性

検証が不十分技術に対する過剰投資と、攻撃者のインセンティブ

現在のブロックチェーンに関する代表的な課題

暗号技術の運用

システムデザインと
セキュアな運用

非中央集権と
スケーラビリティの
トレードオフ

ブロックチェーン的
ファイナリティ

+ より良い、インセンティブと経済モデルをデザインすることによる、健全なコミュニティとエコシステムの必要性

インターネット技術の熟成におけるNSFネットの役割

ARPANET

CSNet

Research Networks (NSFNET)
Non-Profit

Externalizing Costs
Commercial ISPs
Making $$$

1969

1981

1985

CIX Association
1991

April 30th 1995

1977

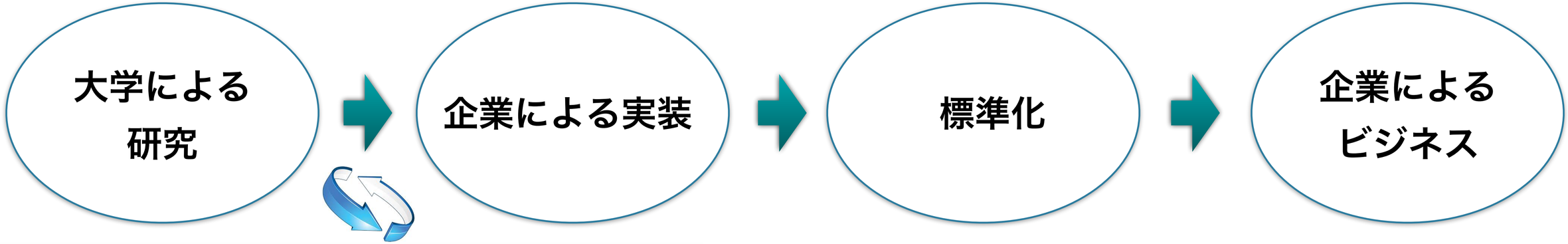
1995

Berkeley Software Distribution (BSD)

NSFNET T3 Network 1992

アカデミアによる研究を交えた熟成ステップの再構成

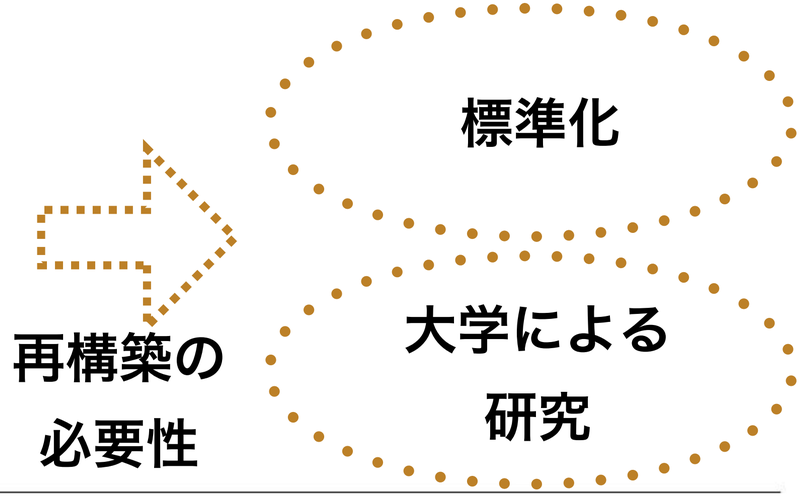
インターネットの時の技術の熟成ステップ



BSDとオープンソースによる技術開発

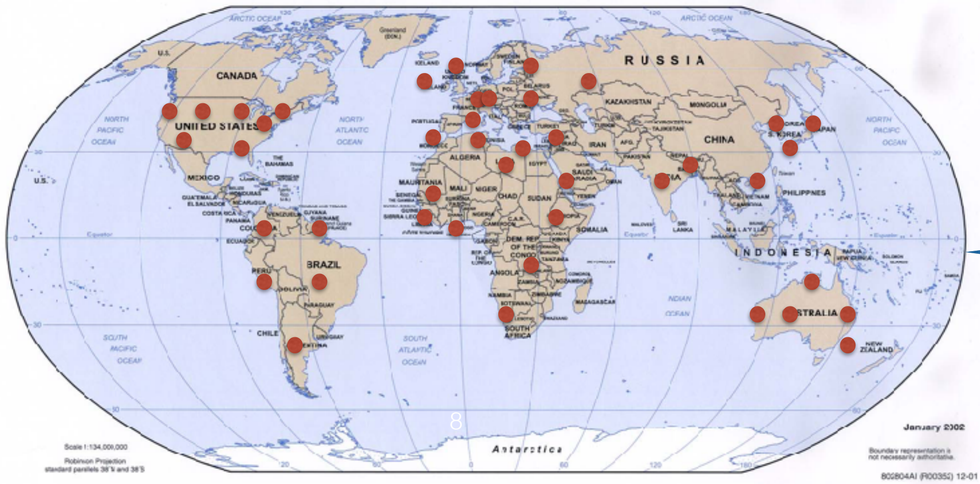
Bitcoinとブロックチェーンの場合

繰り返しによる改善



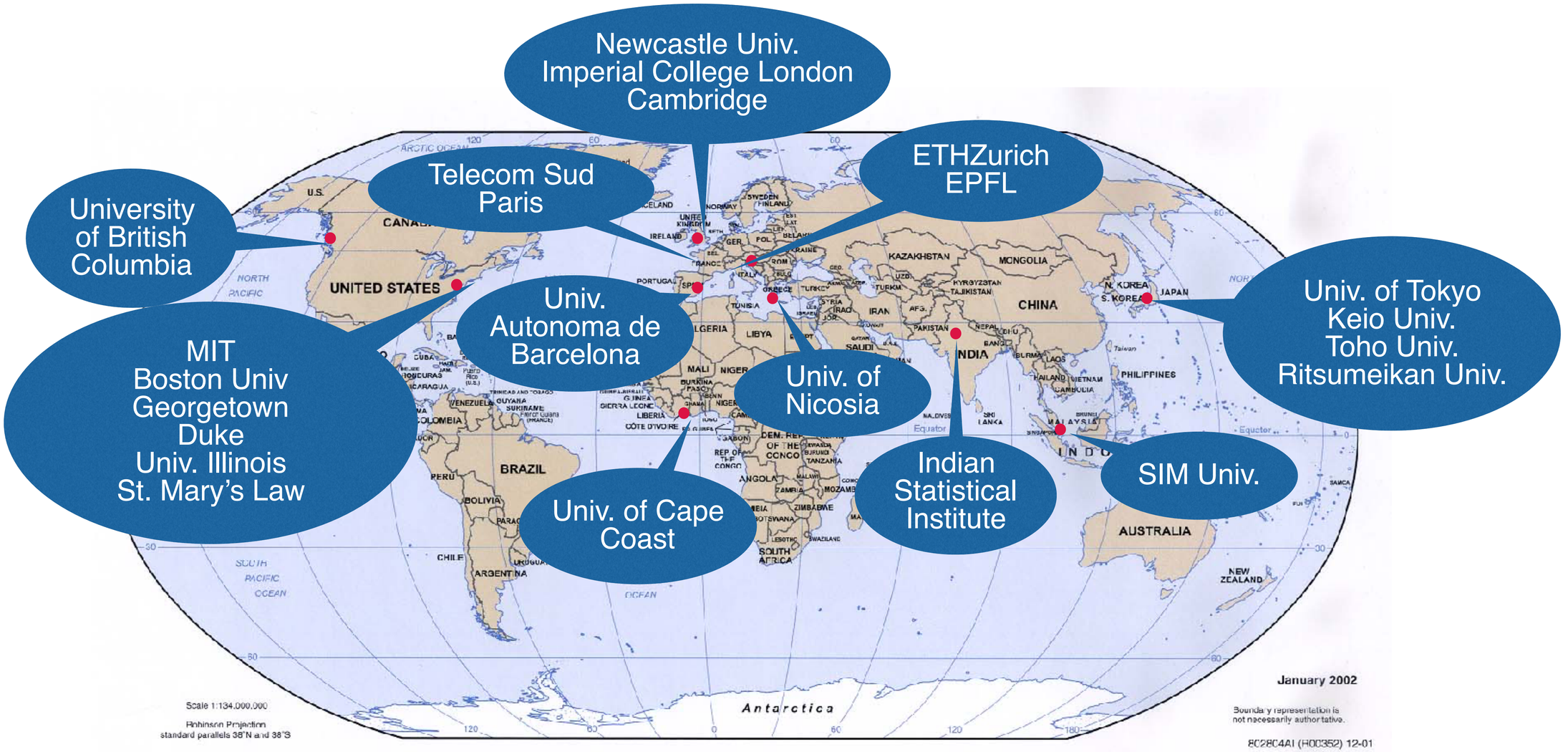
BSafe.networkプロジェクト

- NSFNetとBSDがインターネットに果たしたのと同じ役割をブロックチェーンに対して担う
- 中立的な立場で、安定かつ持続的なブロックチェーンの研究用テストネットワークを、世界中の大学で構築
- 各大学が実際のブロックチェーンノードを持ち、ブロックチェーンの諸技術のコードを実行し、研究開発と実験を行う。
- ブロックチェーンにまつわる広範囲な研究領域を対象とする
  - 暗号やセキュリティ技術に限らず、経済学、法規制の検討にも資する研究を対象
  - ネットワーク遅延などの実際の運用環境を考慮した研究
  - 単純なシミュレーションではできない、人間の行動を含めた研究



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

現在参加している大学（22大学）



中立性とダイバーシティの確保ため、より多くの地域と大学の参画のために活動中

大学が研究開発環境としてふさわしい理由

中立性を保った活動

学術的ダイバーシティ（情報科学、暗号、セキュリティ、経済学、法律、...）を持った活動

実験、検証の場

国際連携を容易に構築できる

大学の数（15,000以上で）：スケーラブル

研究開発活動を通した人材育成

主な活動

実稼働する研究ネットワーク利用した国際共同研究

理論的研究成果の、実環境における実験

技術評価

将来的には技術コンペティションなどの実施：イノベーションの基盤

活動状況

2016

ブートストラップ

最初のノードを慶應義塾大学に設置

アジア、ヨーロッパ、米国を中心にノードを拡大

最初の実験として、Bitcoin Core Developerから、Bitcoin+Segregated Witnessのコードの提供を受けて、検証などを行なった

2017

大学の追加

外部資金の検討

組織化

より多くの研究プロジェクト

開発者コミュニティとの連携

今後のアカデミアの役割

ブロックチェーン技術における中立なイノベーションプラットフォーム

技術、エコシステム、社会的および法的健全性の検証

未成熟なもの、不適格なものに対する警鐘

広範囲なバックグランドを持った専門家による連携

 情報科学、セキュリティ、暗号、経済学、法律

学術における連携をきっかけとした様々な国際連携

BSafe.networkを通じた開発者コミュニティとの連携

開発者コミュニティ

Bitcoin software

BIP
(Bitcoin Improvement Proposal)

実験、コンペ

研究成果

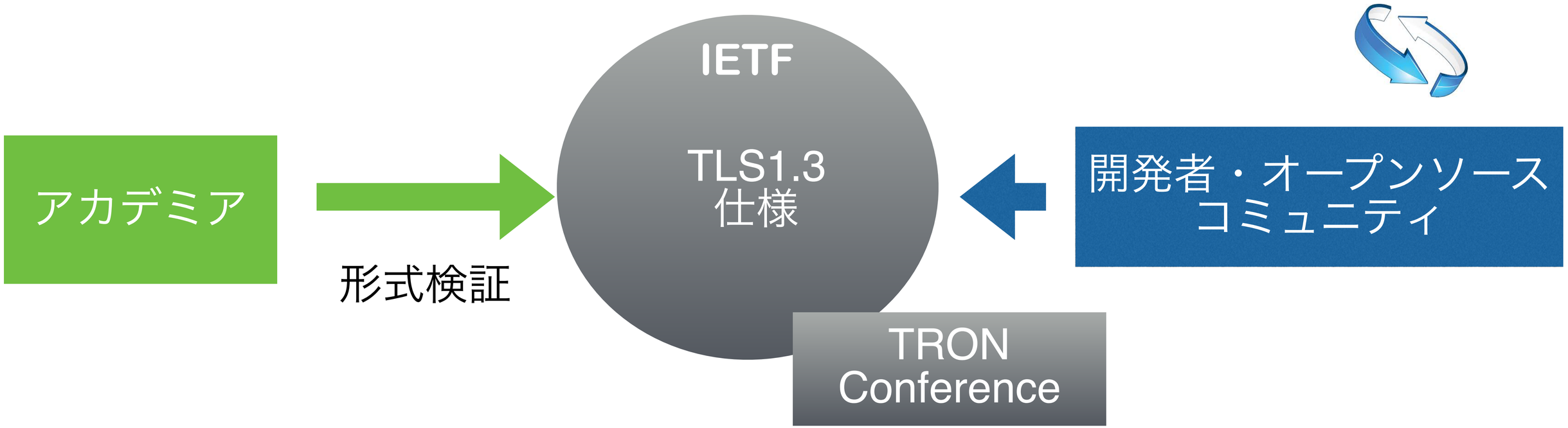
BSafe.network

アカデミア

研究の実施

BRR
(Bitcoin Research Request)

TLSの最新バージョン1.3の開発の教訓



信頼の付与

ダイバーシティによる非中央集権の確立