国際的学術研究ネットワークBSafe.network
ステータスアップデート

松尾真一郎

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？

インターネット技術の熟成におけるNSFNetの役割

ARPANET

CSNet

Research Networks (NSFNet)
Non-Profit

Externalizing Costs
Commercial ISPs
Making $$$

1969

1981

1985

[CIX Association](#) 1991

April 30th 1995

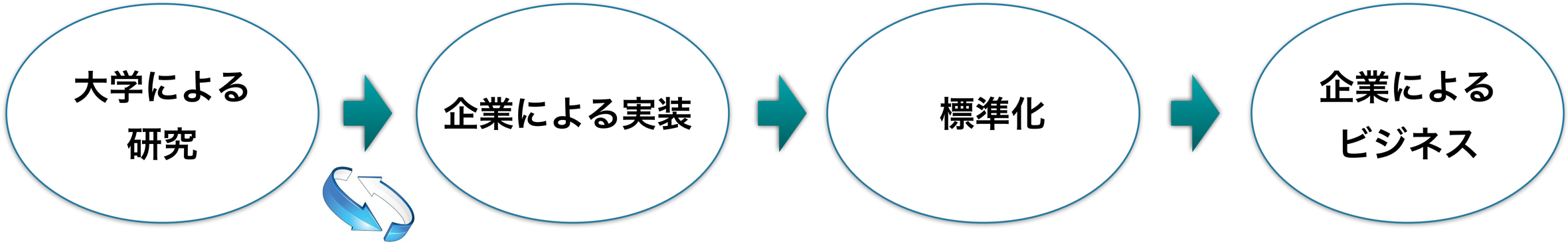
1977 — 1995

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

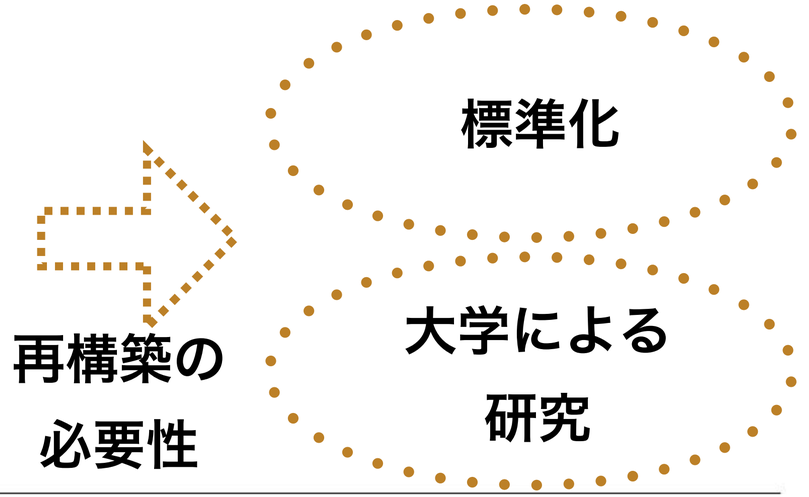
インターネットの時の技術の熟成ステップ



BSDとオープンソースによる技術開発

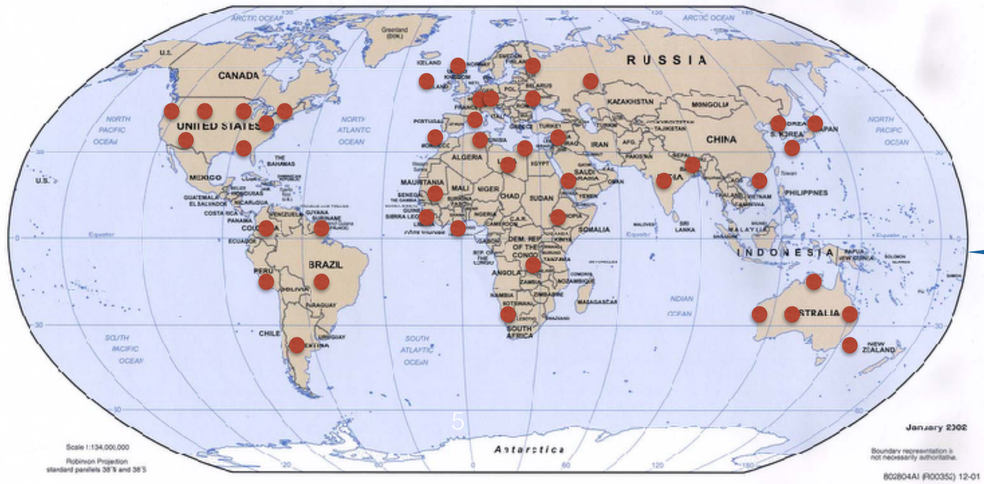
Bitcoinとブロックチェーンの場合

繰り返しによる改善



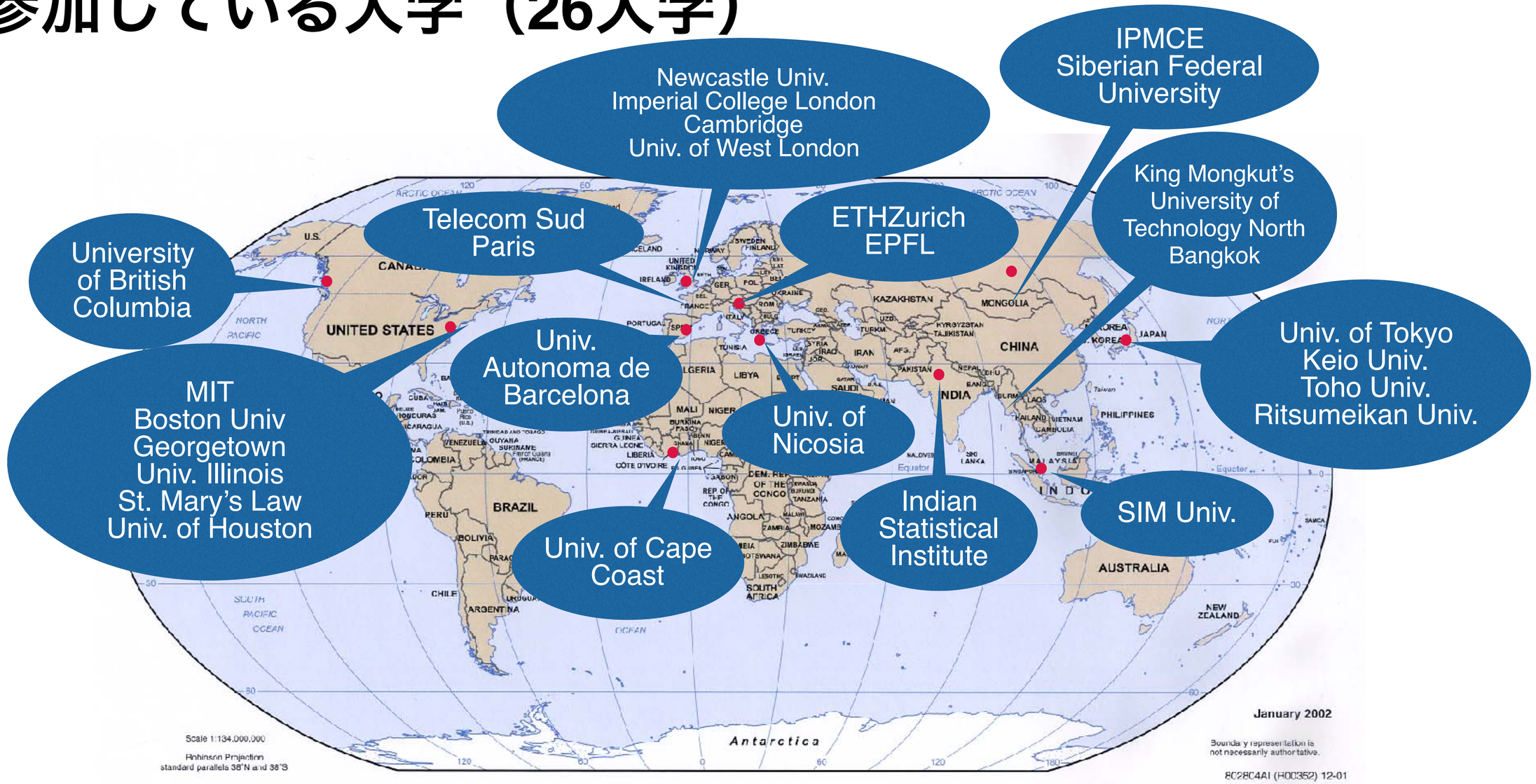
BSafe.networkプロジェクト

- 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
- 2016年5月にPindar Wongとともに構築開始
- 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



- 中立的なプラットフォーム
- 独立した信頼点
- 中立性を有する多数のノード
- 学術研究のテストベッド

現在参加している大学（26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

最新の活動

ブロックチェーンネットワークのモニタリング

レイヤー2技術のオープンコンペティション

ブロックチェーンネットワークのモニタリング

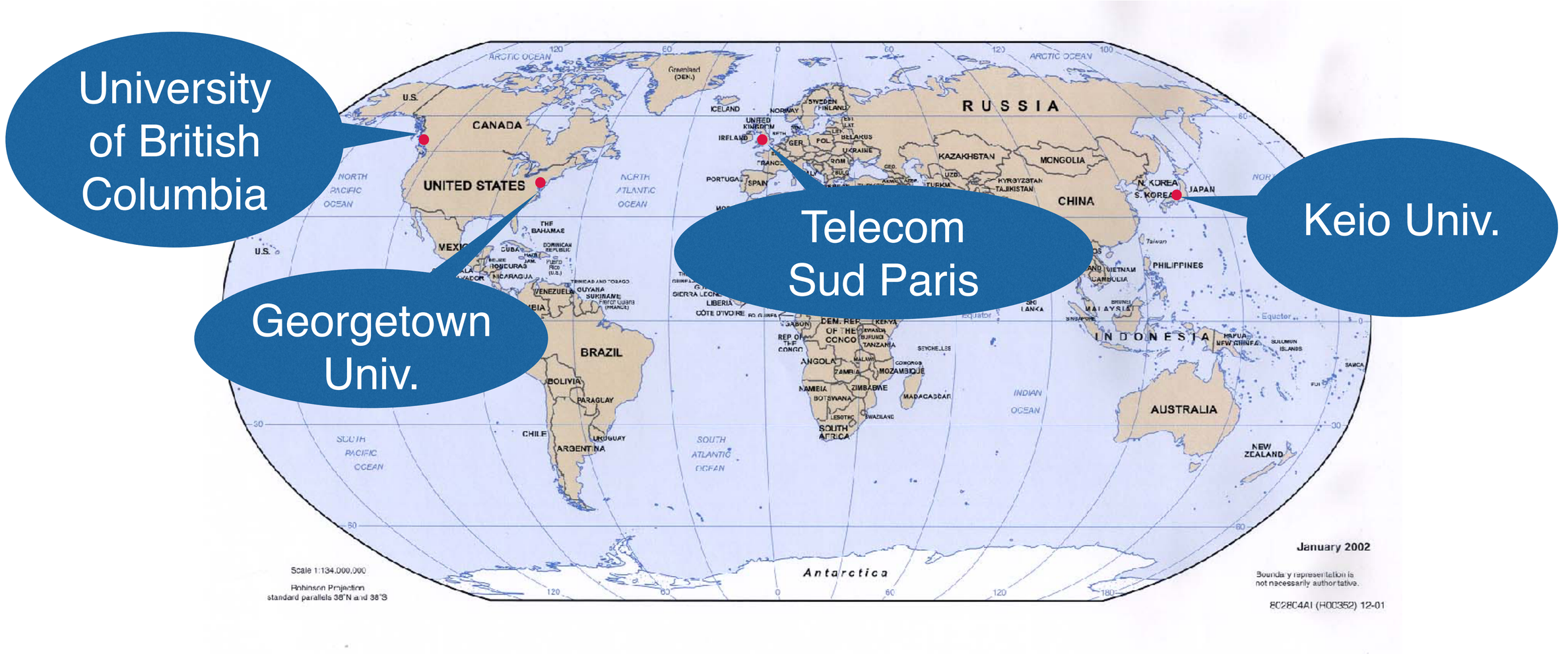
健全なエコシステムに向けたゲームとインセンティブ設計

<u>目的</u>

1. ブロックチェーンアプリにおけるゲーム理論的研究のためのデータセットの収集
2. データセットに基づいた行動の分析
3. より良いインセンティブ機構やゲーム理論的アプローチの設計
4. データセットを一般に共有するための基盤づくり

データモニタリングノード

現在4大学でモニタリングを行なっており、大学を増やす予定



モニタリング対象

- 暗号通貨: Bitcoin, Bitcoin Cash, Segwit2X, Zcash, Bitcoin Gold, …
- 各大学で各暗号通貨のノードを、研究目的で設置
- 2017年7月25日（8/1ハードフォークの1週間前）に開始
- 11月のフォーク（延期）、Bitcoin gold、….

収集データ
ブロックチェーン関連データ

1. Depth of Market

(a) Number of nodes

(b) Liquidity

(c) Number of trade

(d) Agility

2. Financial stability

(a) Robustness of the blockchain network

3. Kinds of transaction

(a) Purely Financial

(b) Colored coin

(c) Pattern among kinds of coin

4. Blockchain protocol data

(a) Successful transactions

(b) Error transactions and protocol messages

収集データ
ネットワーク関連データ

1. Port scan for several IP address
2. Address scan for the same port
3. DNS related attack
4. Signaling

Layer 2 技術のオープンコンペティション

ある目的を達成する技術の開発と選択

共通の技術目標の設定

共通の評価クライテリアの設定

公平かつオープンで、公開検証された結果の提供

技術に関する新しい知見の獲得

信頼できる実装の提供につながる

Layer 2 技術

基盤となるブロックチェーン（Bitcoin, Ethereum）をそのまま利用しながら、ブロックチェーンを利用する側の別レイヤ（レイヤー2）で、機能拡張や性能向上を行う技術

（例）
Paymentのスケーラビリティ向上：Lightning Network

プライバシの向上：TumbleBit

オープン技術コンペティションの例： SHA-3

1. **標準ハッシュ関数の危殆化 (2004)**
   - MD5, RIPEMD, SHA0 and SHA1
   - SHA2はまだ安全
2. **新しいハッシュ関数の公募と評価 (2005-2012)**
   - SHA2が将来危殆化した時のための代替
   - 国際的な公募（AESのコンペティションと同じ）
   - 厳正なプロセスによって技術的な合意を得る良い成功例

ブロックチェーンLayer 2コンペティション

BSafe network

2つのカテゴリー

Layer 2 プロトコル提案

スケーラビリティ、セキュリティ、プライバシ、それらのトレードオフを向上するLayer2プロトコルとその実装

Layer 2 評価技術・ツールの提案

評価のためのメカニズム

評価のための標準データセット

Layer 2 コンペティションの想定成果

実験と専門家のレビューを経た中立な表結果の提供

1) Layer 2ネットワークにおけるアタックモデルの収集
2) Layer 2 技術のセキュリティの評価方法の確立
3) よりより実現方法の提案

何かを選出するのではなく、アカデミアによるデータと研究成果を一般に提供することを目的とする

公開の形で提供されるもの

プログラムコード cc-by license

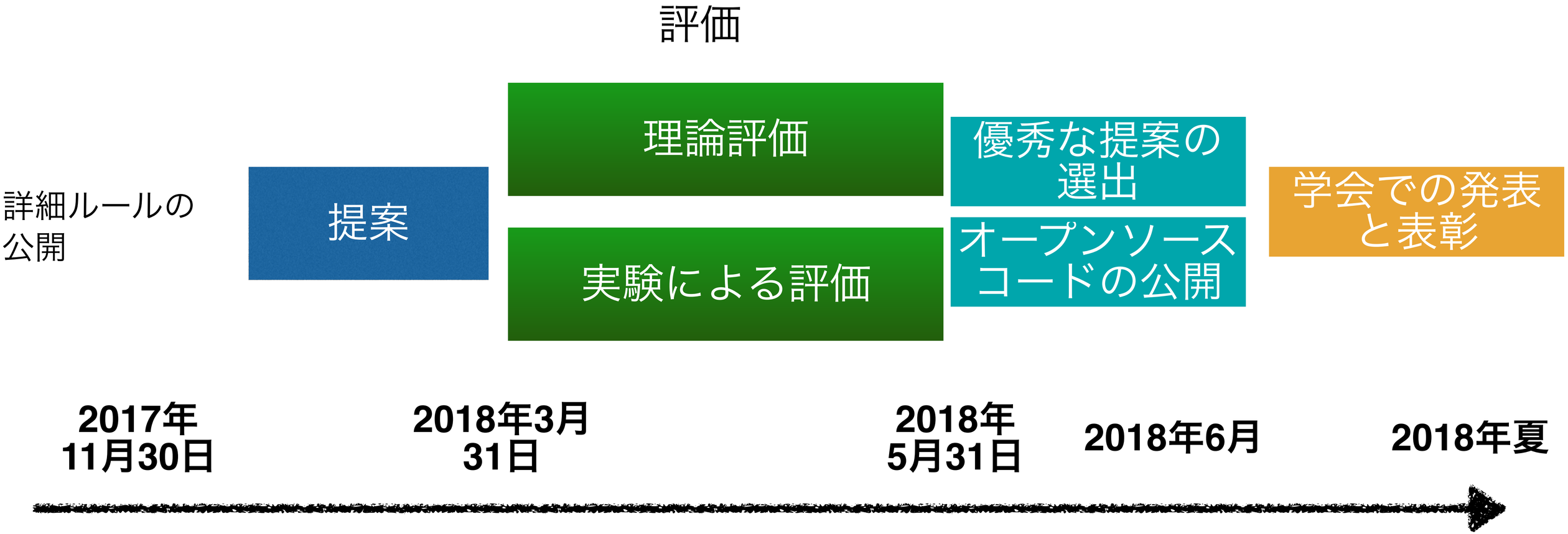
評価ソフトウエア、プラットフォーム
Layer 2 ソフトウエア

評価データ

副産物

セキュリティ評価理論と今後の研究のための基盤

スケジュール


評価
詳細ルールの
公開
提案
理論評価
実験による評価
優秀な提案の
選出
オープンソース
コードの公開
学会での発表
と表彰
2017年
11月30日
2018年3月
31日
2018年
5月31日
2018年6月
2018年夏

評価の方法（観点の例）

BSafe network

1.性能

単位時間あたりのトランザクション
地域的ダイバーシティ
ネットワーク遅延

2.セキュリティ/トラストモデル

ノードに対する故障/クラッシュ/攻撃への耐性
中央集権性
DoS攻撃
評価のためのデータセットと攻撃シナリオ
Layer 2 ノードのアベイラビリティ

3. Others are welcome!

参加募集と表彰

参加に必要な情報

技術設計方針、アルゴリズムとプロトコル、自己評価（セキュリティと性能）を記載した技術文書

BSafe.networkで実行可能なプログラムコード

詳細はBSafe.networkのWebページから
http://bsafe.network/technology-competiton/leyer2competition/index.html

B-Prize

優れた提案に対する表彰を予定
夏に行う予定のBSafe.network主催の学術会議で優秀提案の発表と表彰式