Blockchain’s today and tomorrow are scholars of yesterday.

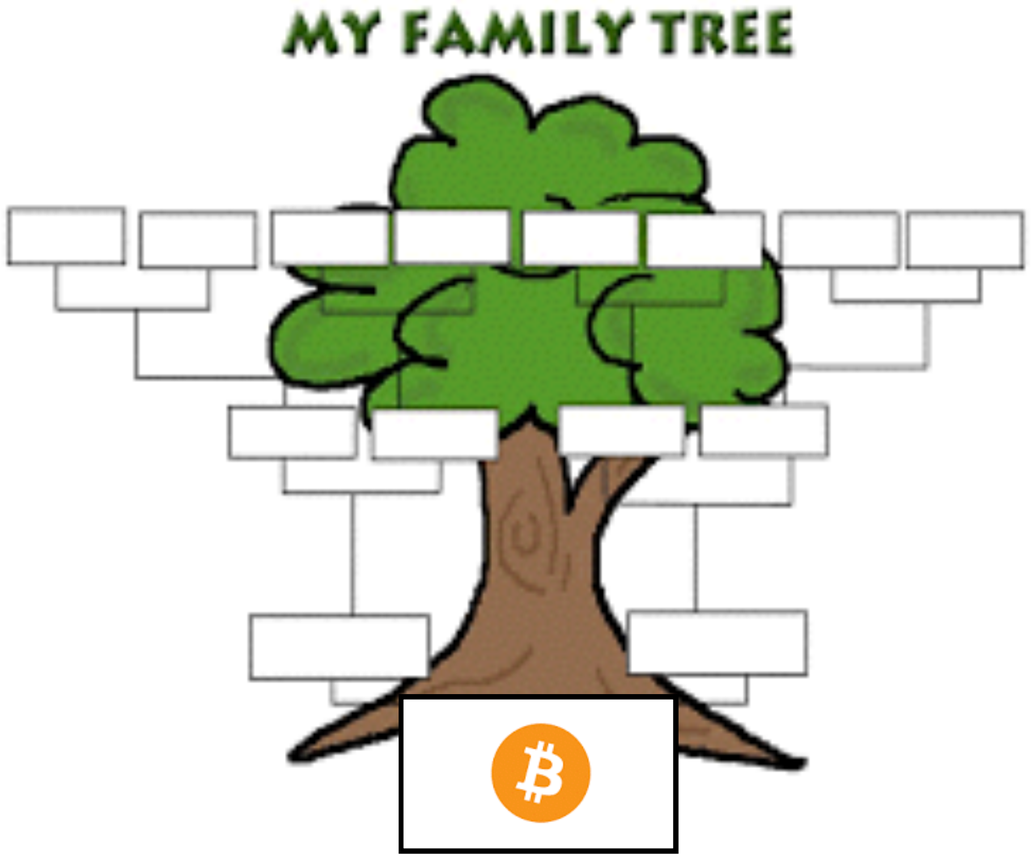
ブロックチェーンにまつわる温故知新

Shin’ichiro Matsuo, Ph.D.

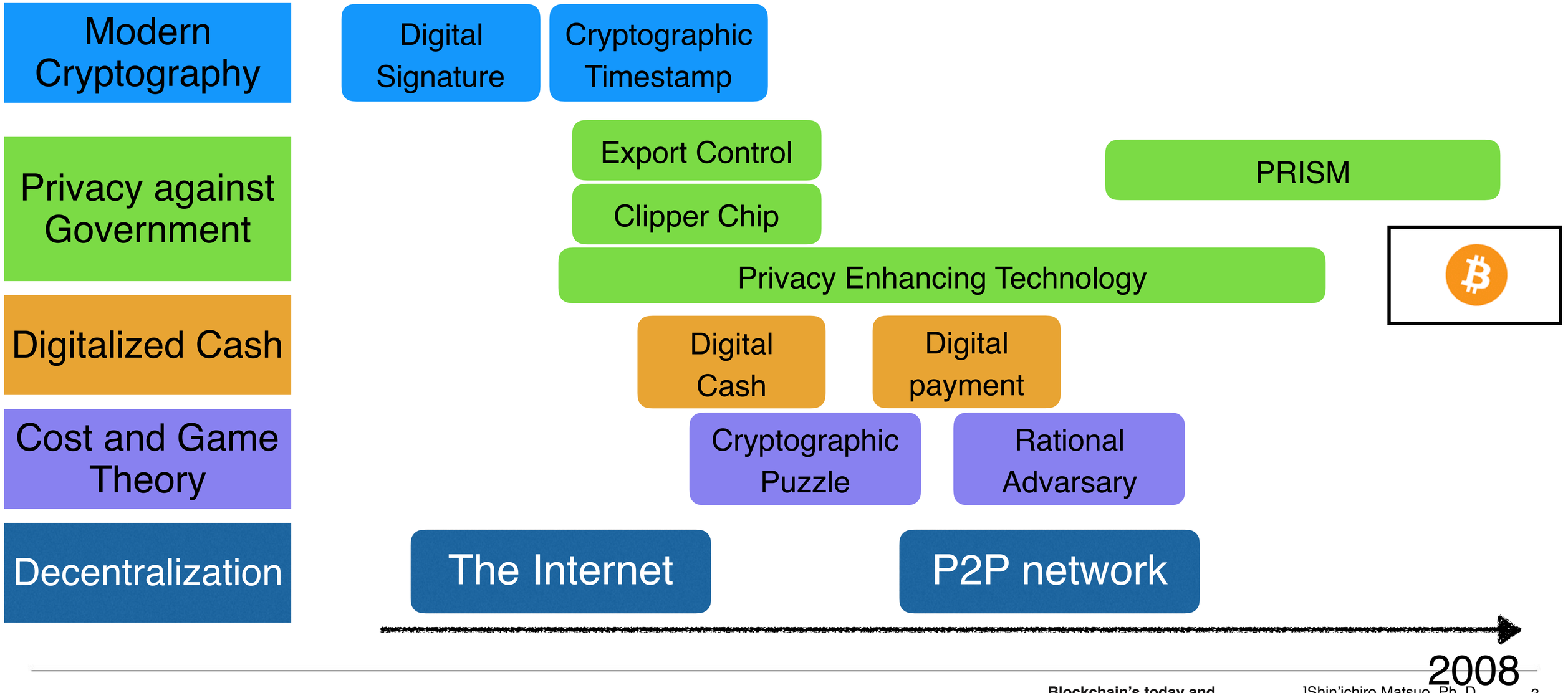
The New Context Conference 2017 Tokyo

How Did Bitcoin/Blockchain Born?

Entirely new invention?



Chronology Before Bitcoin



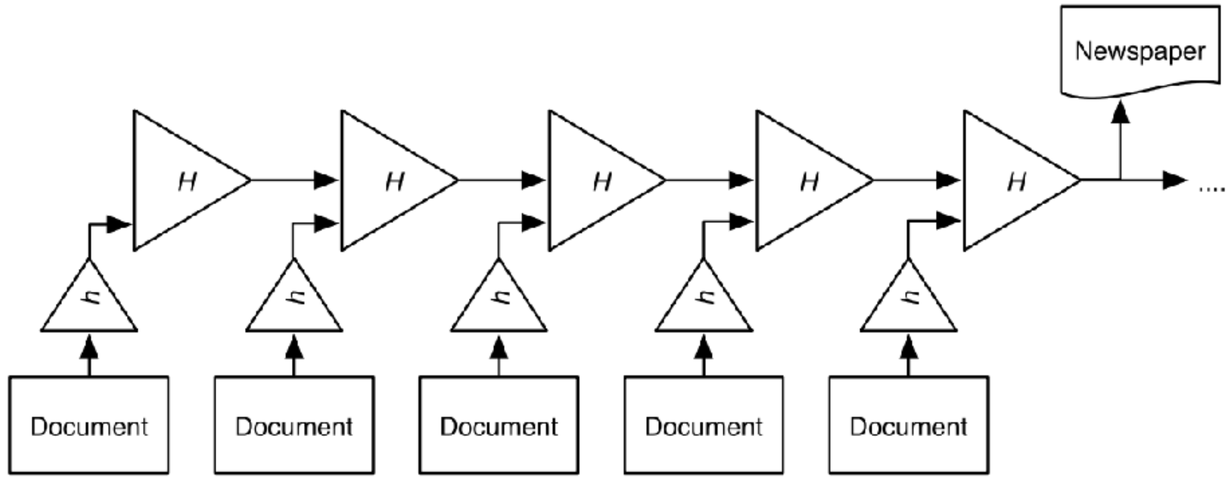
Where the Data Structure of Blockchain Came From… (1990)

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

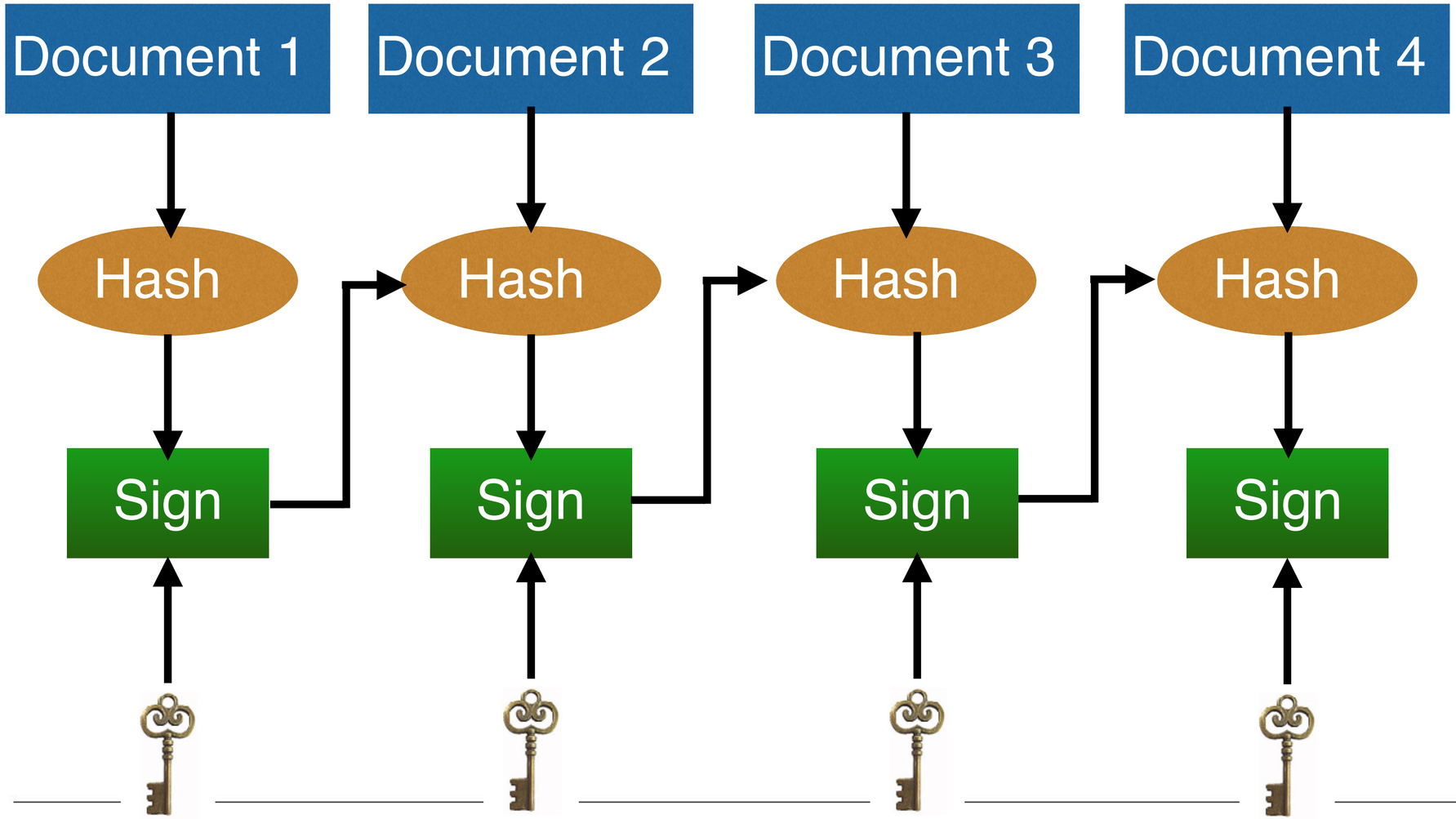
Bellcore
445 South Street
Morristown, N.J. 07960-1910



But needs centralized server(s)

Hysteresis Signature was Invented in Japan (2002)

Waseda Univ., Yokohama National Univ., Tokyo Denki Univ. and Hitachi Ltd.



Needs centralized server(s)

Privacy against Government

Export control of cryptography (-2000)

Clipper Chip by NSA (1993-1996): A encryption/ decryption chip
- US Government can decrypt.

PRISM: Surveillance by NSA

Financial Cryptography Conference

Usually is held in Caribbean Islands

1st conference (1997) was held in Anguilla.

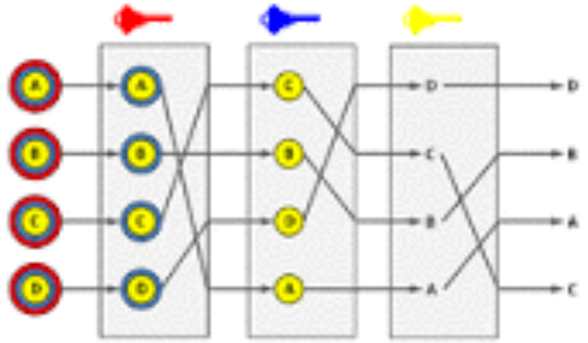
Free from export control of cryptography

Tax Haven

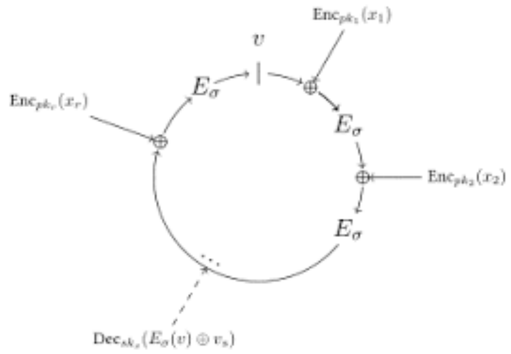
Initiated by Cypherpunk

Privacy Enhancing Technologies

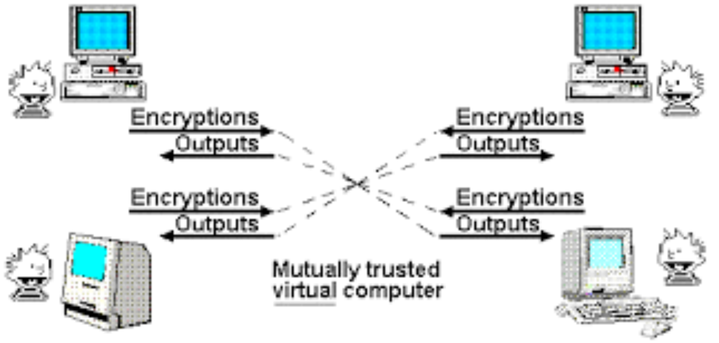
Blind Signature



Mix-Net/Tor



Group Signature/Ring Signature



Multi Party Computation

History of Research on Digitalized Cash (90s)

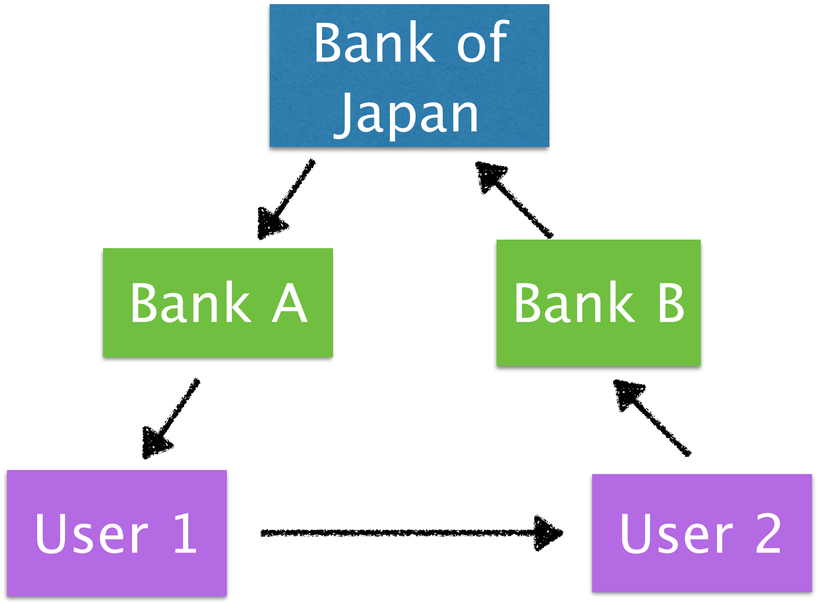
David Chaum

Stephan Brands

Visa Cash

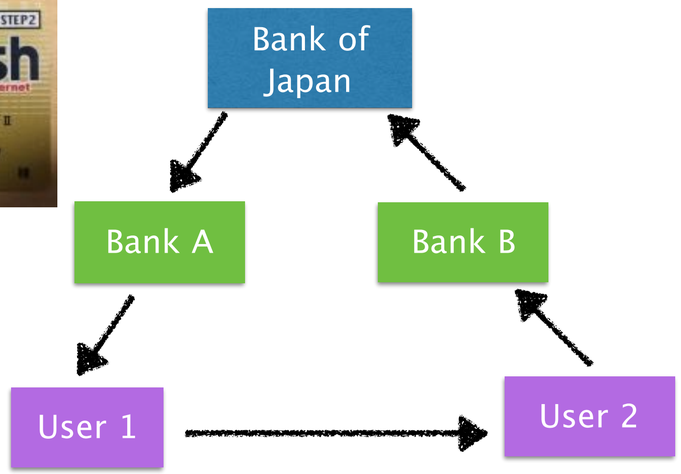
MONDEX

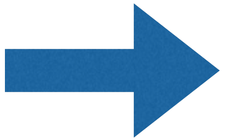
Internet Cash by Bank of Japan and NTT (1997-2000)

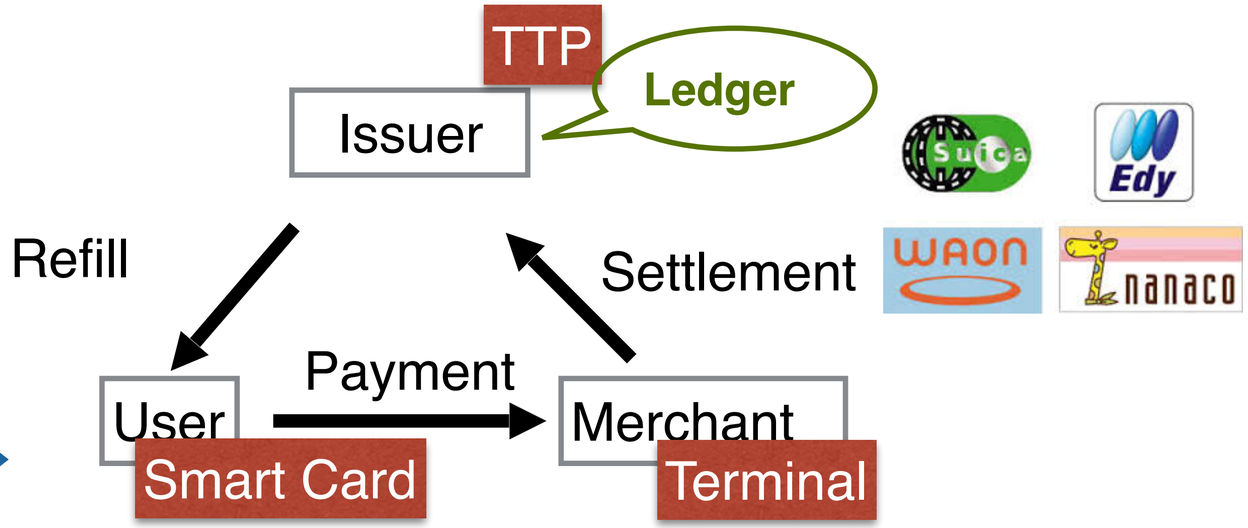


- Implement “Cash” issued by the “Bank of Japan”
- Transferable thorough e-mail attachment
- Multi-currency

Ideal Digitalized Cash vs. Practical Digital Payment







Anonymous
Offline payment
Transferable
Open-loop
Heavy cryptography

Transaction Identified
Online payment
Non-Transferable
Closed-loop
Lighter Processing

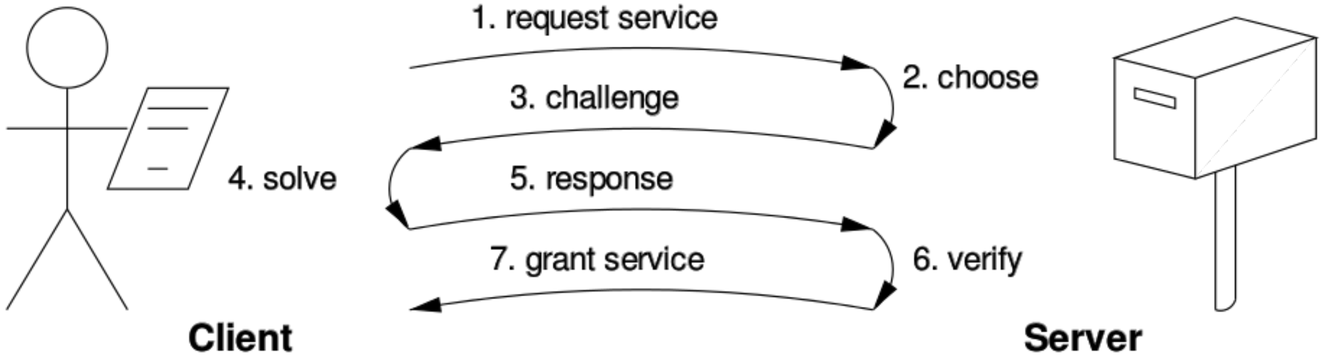
Add Cost to Attack: Cryptographic Puzzle

Originally, was proposed to prevent Denial of Services (DoS) and spam mails (1993).

This idea is utilized in Proof of Work of Bitcoin.

Game theoretical nature in Bitcoin:

- **Cost to attack vs. cost for future reward**



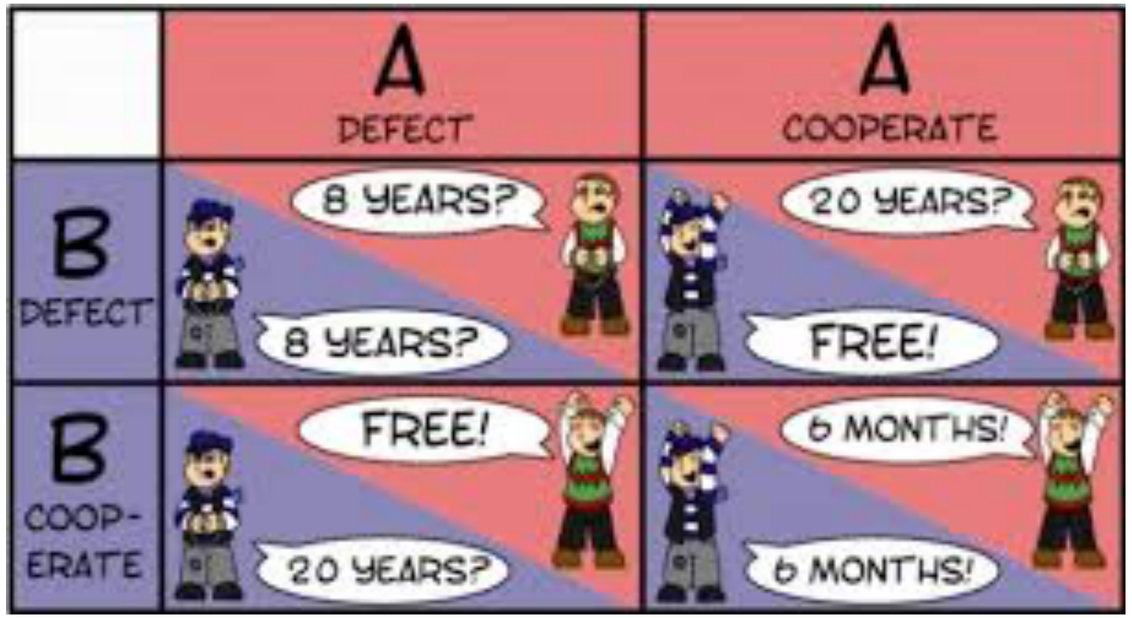
Cryptography and Game Theory (2002-)

Sealed-bid Auction

Vickrey Auction and (M+1) - price auction

Dynamic Programming and combinatorial auction

A class of Pareto Optimal



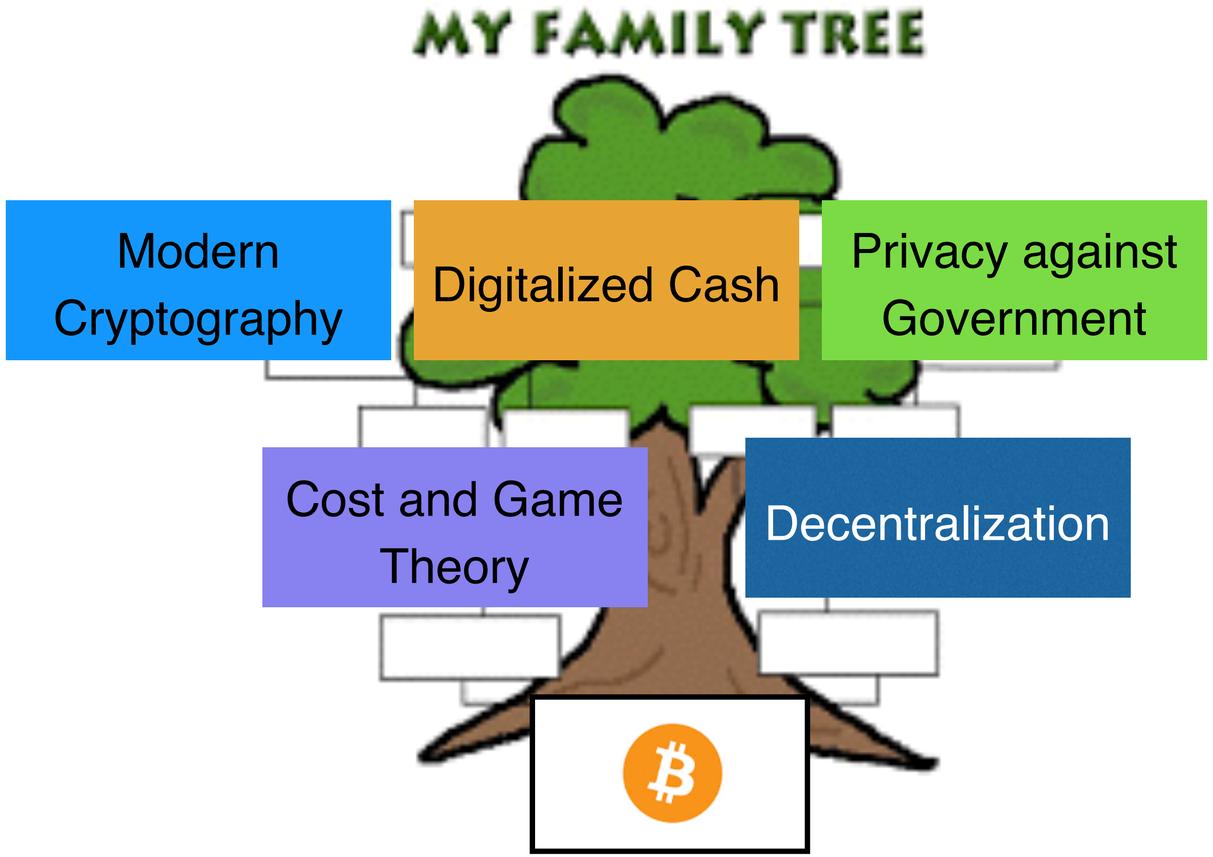
Decentralized Communication: The Internet and P2P

Resilient against fault and malicious activities

No one need to and can govern entire system.

Sharing small trust and responsibility to maintain the system

Bitcoin: Perfect Mix of Past Movements!



Mixing merits of past history of technology development.

Inheritance in Technology Development

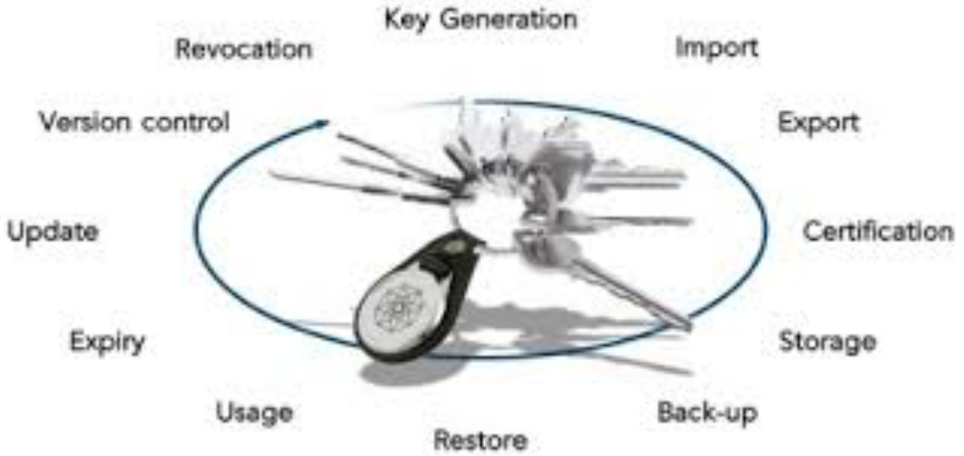
Merits of technologies

Defects of technologies

Operation of Cryptography

Key management:

Cryptography is a tool to transform the problems of confidentiality, authenticity and integrity to key management.



All nodes have responsibility:

Securely manage the key

Security against cyber attack

Secure design of a system based on cryptography

Compromise of Cryptography

Increase of computational power of adversary

Need to extend key length

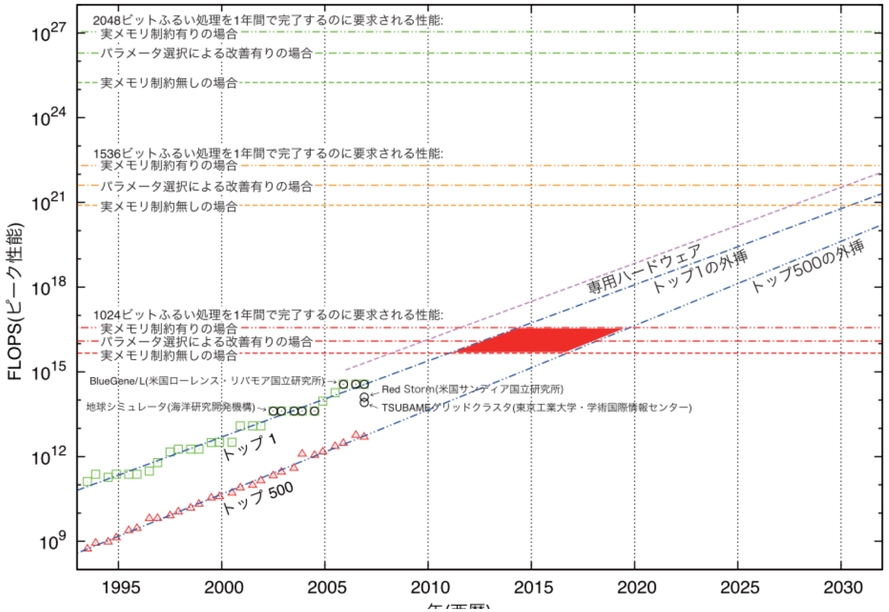
Finding vulnerability of cryptographic algorithm

Case of SHA1

Need transition of underlying cryptography

Long-term Signature (ETSI standard)

Application to Blockchain is to appear in ICCCN, next week.



Difficulty of Long-term Assurance: Time-stamp Business

Cannot stop even if the business is not profitable

In the case of public blockchain?

Can we maintain enough number of blockchain nodes for a long term?

Understanding Redundancy of De-centralization

A mechanism for de-centralization is redundant.

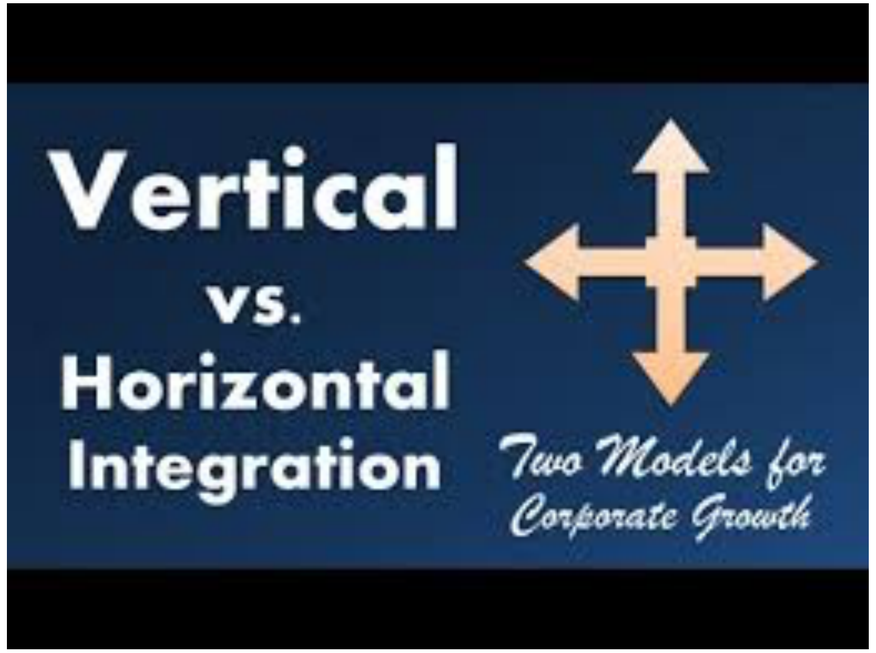
In the Internet, the same packet is resent when the original packet is lost.

In the Blockchain, all nodes should execute chatty protocol and store the same and huge data.

Horizontal ~~vs~~ and Vertical

- **Horizontal: extend the possibility of technology, combination and business**
  ex.) The Internet, Blockchain, Layering and standardization

- **Vertical: provides stable system and better UX**



An Article before the Internet

記 号 処 理 31－3
（１９８５. 3. １２）

続・電子メイル呼びかけ報告記

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）

An Article before the Internet (cont)

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イル網への参加の重要性と日本が研究開発用の電子メイ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、USENET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、電子メイ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、日本と米国の間の電子メイ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、筆者たちは電子メイ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。

An article before the Internet (cont)

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型メイ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型メイ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。

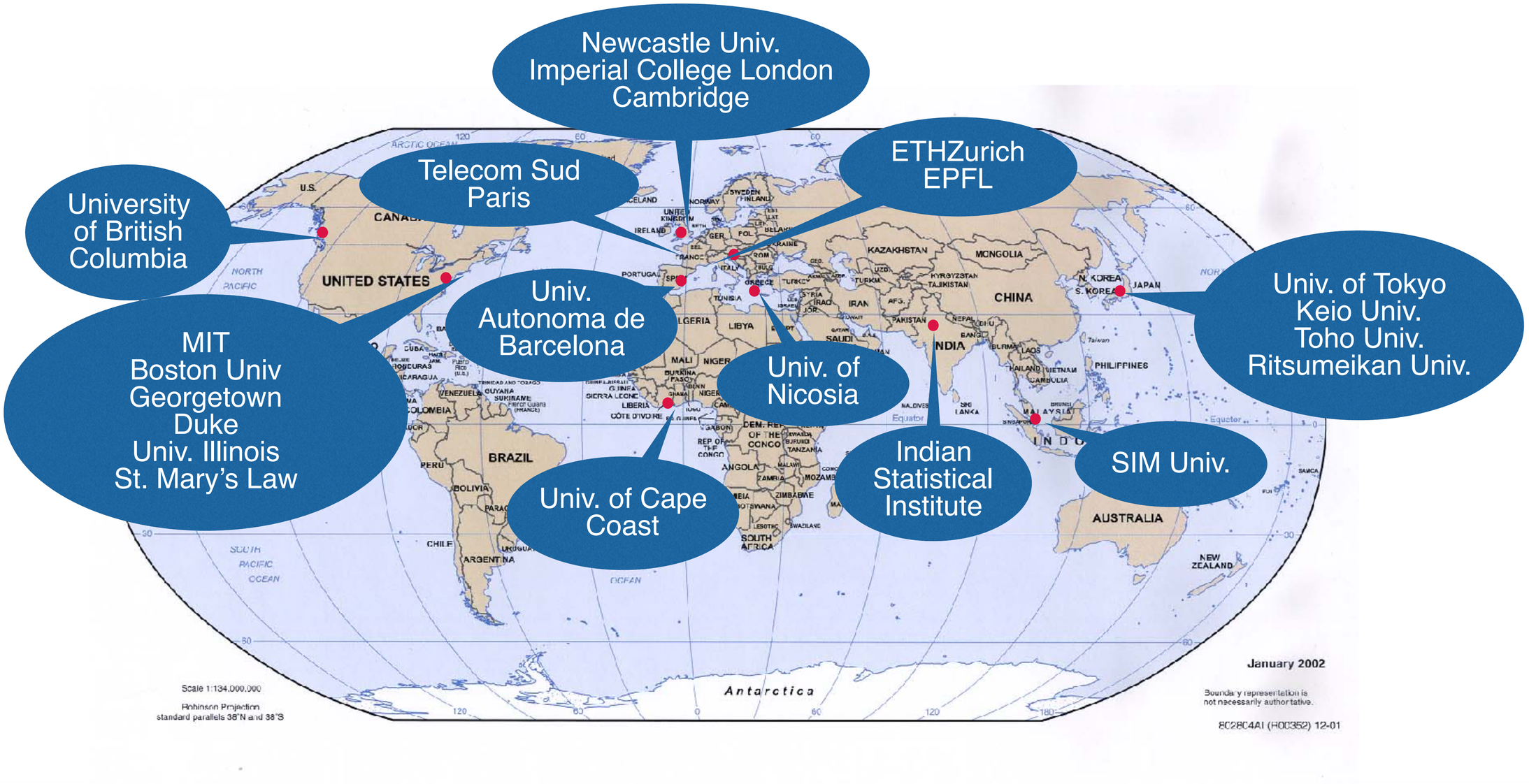
1985年10月には韓国のソウルで太平洋沿岸国のコンピュータ・ネットワークと電子メイル網に関する会議がアジアではじめて開催される。また日本と米国の経済学者とシミュレーション専門家の一部のグループがＮＳＦにプロポーザルの提出準備中で、大規模なCSNETへの参加を計画していると伝えられる。

BSafe.network: Plays the Same Role as NSFNet and BSD

- A neutral, stable and sustainable research test network for Blockchain technology by international universities.
- 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

22 International Universities Already Join and We Add More…



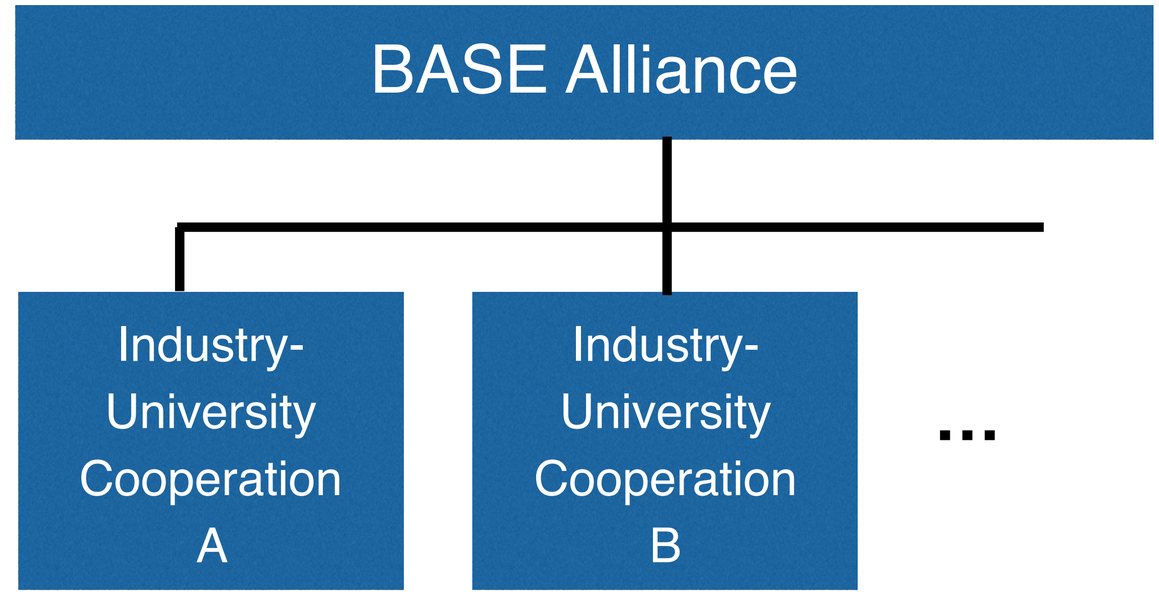
BASE (Blockchain Academic Synergized Environment) Alliance

Open and neutral alliance of Industry-University cooperation

Joint research, development, experiment

Initiated by the University of Tokyo and Keio University

Launch: July 24, 2017



Blockchain’s today and tomorrow are scholars of yesterday. Visiting yesterday is a source of promising tomorrow.