東京都立 国分寺高等学校
2020年 11月 18日(水)

ネットワーク研究の最前線

首藤 一幸
東京工業大学　情報理工学院　准教授

bit.ly/kbj1118

Tokyo Tech

首藤 一幸 (46)

しゅどう　かずゆき

1973 生まれ

1989 神奈川県立 横須賀高等学校

1992 早稲田大学

学部 4年, 修士課程 2年, 博士課程 3年

2001 産業技術総合研究所

研究員

国の研究所

2006 ウタゴエ(株)

取締役 最高技術責任者 (CTO)

スタートアップ

（ベンチャー企業）

2008/12 東京工業大学

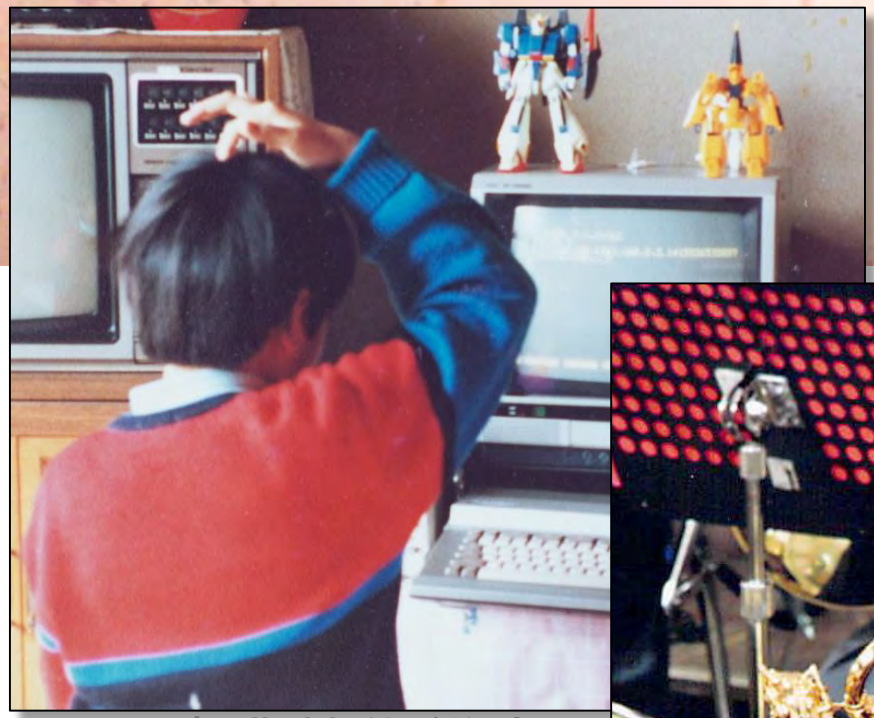
准教授

大学

ネットワーク / 分散システム（大学～）

サックス / 吹奏楽（高校）

コンピュータ（小5～）



小６ (1985)

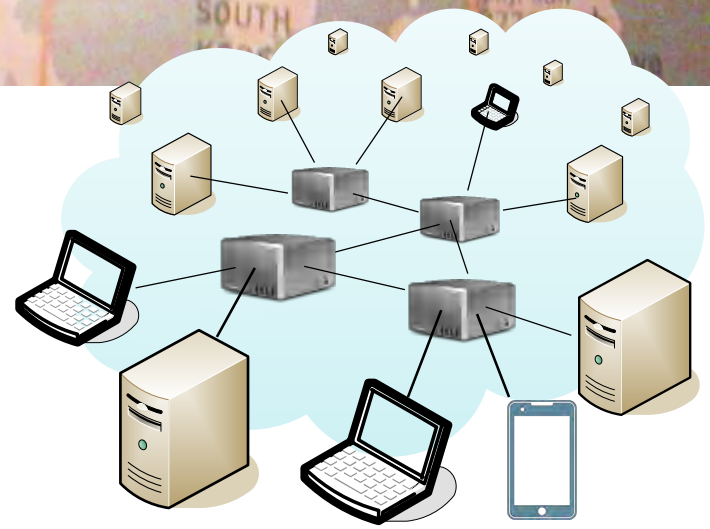
高３ (1991)

大学院 博士課程 修了 (2001)

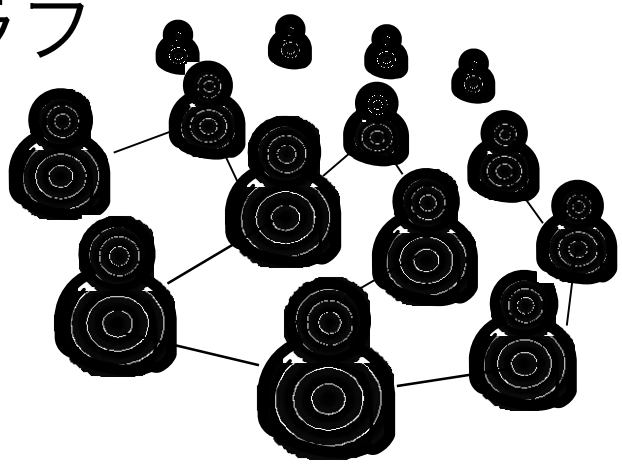
2006 ウタゴエ(株)
取締役 最高技術責任

2008/12 東京工業大学
准教授

２種類の「ネットワーク」研究



- **コンピュータ ネットワーク**
  - ≒ インターネット
  - いろいろな層 / レイヤがある
    物理 ～ アプリ



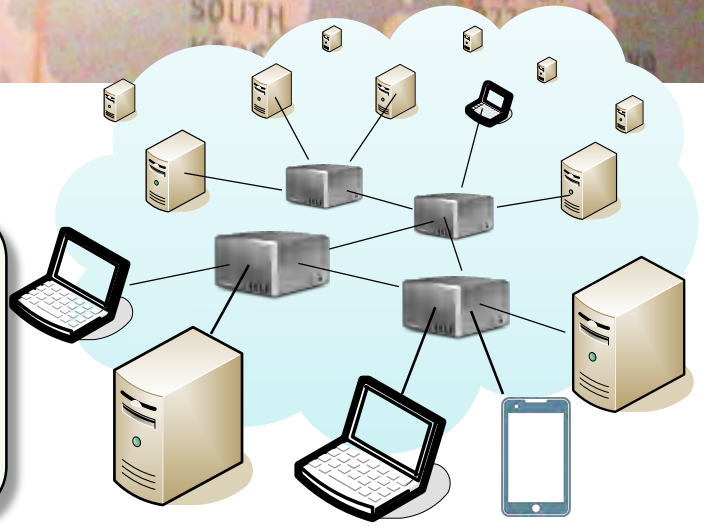
- **ソーシャル ネットワーク** / グラフ
  - 人間関係のネットワーク
  - SNS が流行って、
    研究しやすくなった。

両分野に取り組む研究者はほぼいない。というくらい別分野。

２種類の「ネットワーク」研究

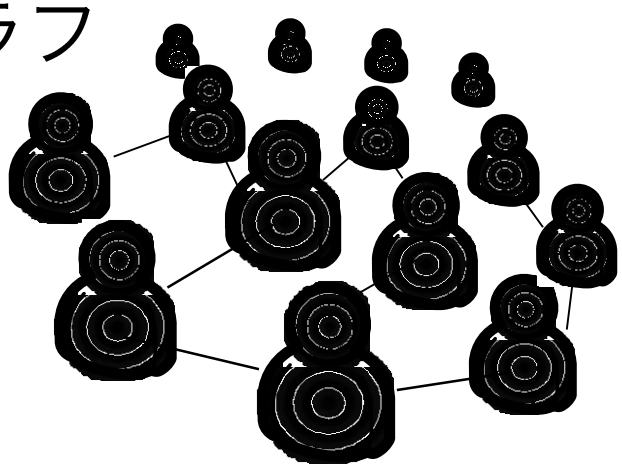
- **コンピュータ ネットワーク**

暗号通貨・ブロックチェーンの
性能向上



- **ソーシャル ネットワーク** / グラフ

ランダムウォークによる
特徴量推定



両分野に取り組む研究者はほぼいない。というくらい別分野。

本日の内容

- コンピュータ ネットワークの研究 p.6 ～ 17
  - 暗号通貨・ブロックチェーンの性能向上 12 ページ
- ソーシャル ネットワークの研究 p.18 ～ 24
  - ランダムウォークによる特徴量推定 7 ページ
- 人生の選択にあたって p.25 ～ 29
  - 後悔最小化の法則, … 5 ページ

コンピュータ ネットワーク

暗号通貨・ブロックチェーンの
性能向上

暗号通貨　または仮想通貨, 暗号資産

cryptocurrency　　crypto asset

- デジタルなお金は、いろいろある。
  - Suica, PASMO, PayPay, ○○ポイント, …

3,000 種類以上ある

- 暗号通貨：Bitcoin (BTC), Ethereum (ETC), Ripple (XRP), …
  - Bitcoin に端を発する、非集中的 (後述) なもの
  - 時価総額 30兆円　「通貨」になりたいが現状「資産」

暗号通貨の起源

- 2008年の論文

  ネットで見つかる。
  和訳もある：
  https://coincheck.blog/292
  読むのもいいのでは？

Bitcoin: A Peer-to-Peer Electronic Cash System

ビットコイン: peer-to-peer 電子現金 システム

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

- 2009年 1月のメール

Bitcoin v0.1 released

Satoshi Nakamoto satoshi at vistomail.com

Thu Jan 8 14:27:40 EST 2009

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Satoshi Nakamoto
が誰なのかは、
今日に至るまで不明

Bitcoin の非集中 分散システム

- インターネット上に約 1万ノード (サーバ)
  - インターネット側からは通信できないノードを含めると、数万

GLOBAL BITCOIN NODES DISTRIBUTION

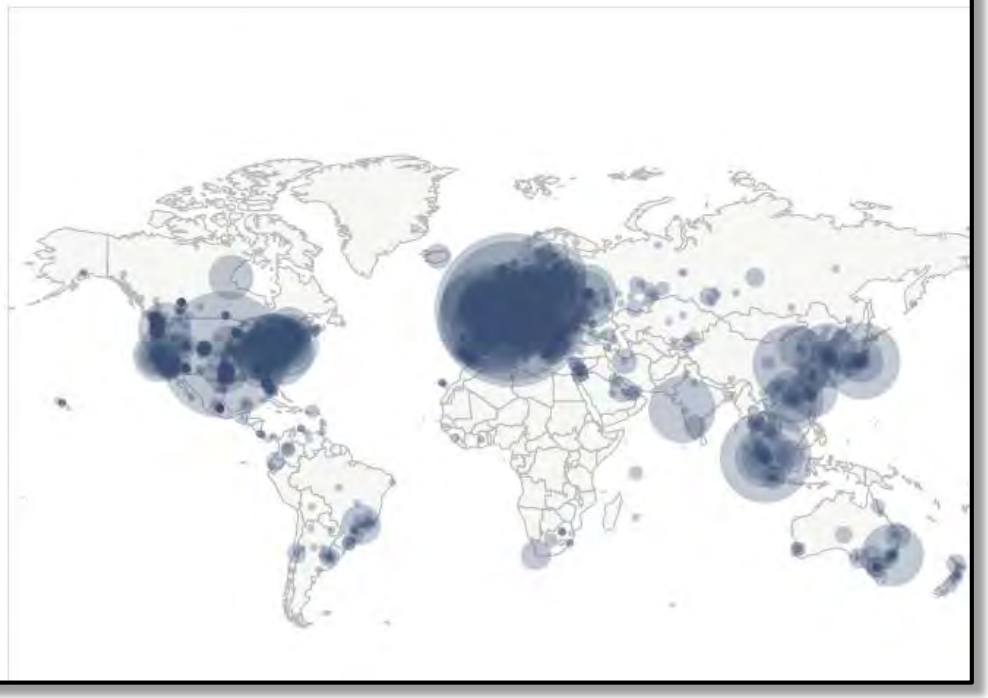
Reachable nodes as of Sat Nov 14 2020 20:22:40 GMT+0900 (日本標準時).

10907 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	2679 (24.56%)
2	United States	1868 (17.13%)
3	Germany	1725 (15.82%)
4	France	558 (5.12%)
5	Netherlands	447 (4.10%)
6	Canada	316 (2.90%)
7	United Kingdom	315 (2.89%)
8	Singapore	300 (2.75%)
9	Russian Federation	218 (2.00%)
10	Japan	218 (2.00%)



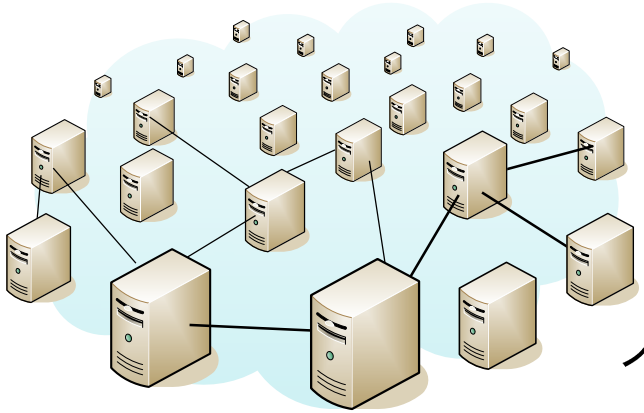
http://bitnodes.earn.com/ より

- 非集中 → 一部壊れても全体は動作し続ける

トラストレス / trustless

- 非集中 / decentralized

- 誰かを信用する必要がない → 「**trustless**」
  トラストレス
  - 政府, 銀行, 企業, … 等を信用する必要がない。
  - 実際は、ノードのうち例えば 2/3 は悪意のないノード (運用者) である必要がある。



ピア / peer
ノード / node

非集中 分散システム (peer-to-peer)

ブロックチェーン

- 暗号通貨 Bitcoin が提供した価値
  - 非集中 (→ トラストレス) に
  - 二重使用を防止
    - 整合性 を保つ
    - 改ざん困難性
- … これは、通貨に限らず他に応用できるのでは？

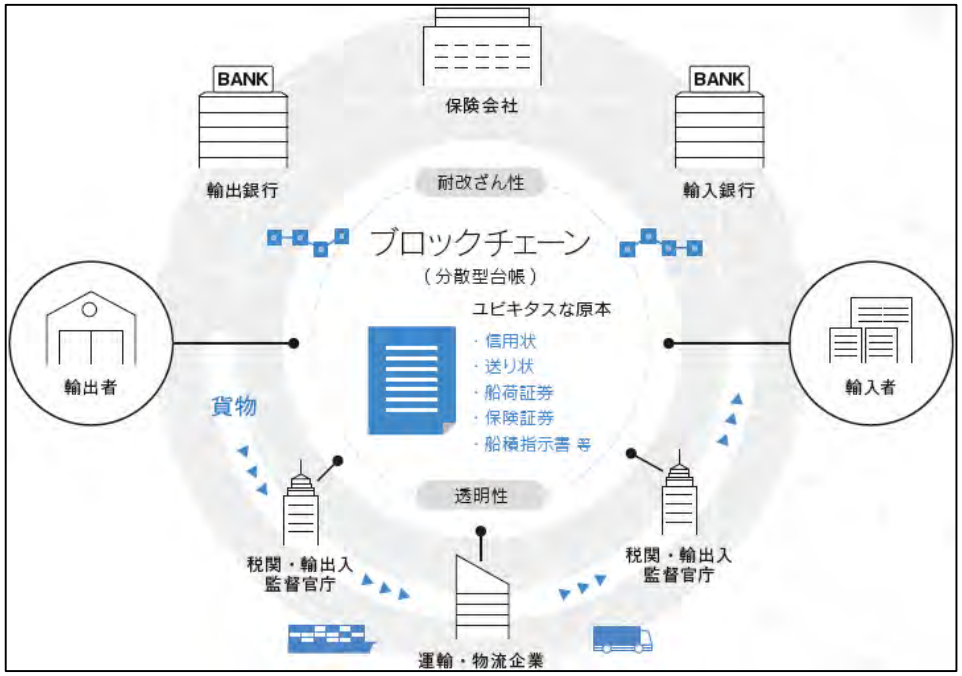
ブロックチェーン または
Distributed Ledger Technology (**DLT**) / 分散台帳技術

「ブロックチェーン」は特定のデータ構造を指す語なので、
それを嫌って、DLT と呼ぶ人も多い。

ブロックチェーンの応用例：追跡 / trace

- IBM Food Trust
  - **食品**の来歴を追跡可能に
- TradeWaltz (NTT データ他)
  - **貨物**を追跡可能に

吉濱佐知子氏 (IBM Research - Tokyo) の資料

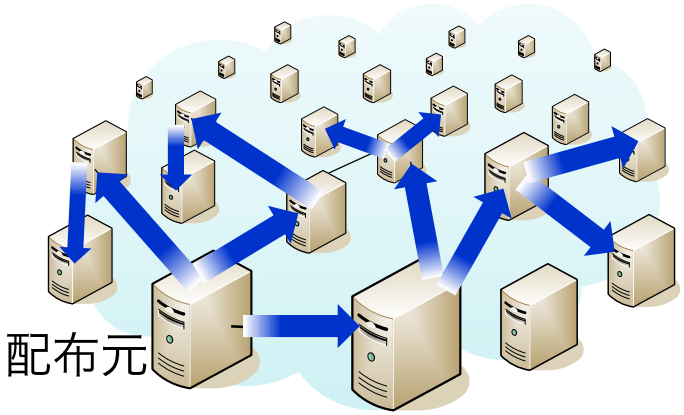


トレードワルツ社 資料

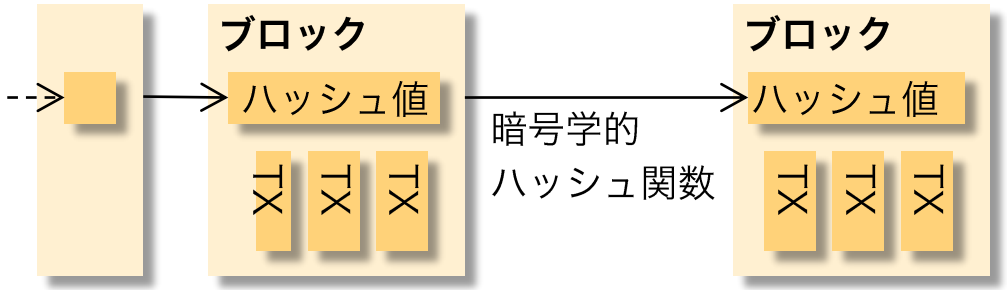
- デジタル化の恩恵 +
  ブロックチェーンの恩恵：改ざん困難・トラストレス …

性能の向上　安全性は保つ

- 性能：トランザクション (取引, TX) / 秒 = TPS
  - TX の例：Aさんから Bさんに 1 BTC 送金
  - 既存　VISA (クレジットカード) 1,700 TPS, PayPal 平均 320 TPS
  - 暗号通貨　Bitcoin 7 → 27 TPS, Ethereum 15 TPS 前後　**圧倒的に不足**
- 性能向上には、ノード (サーバ) 間での
  データ伝搬の高速化が欠かせない。　理屈は省略



ノード (サーバ) のネットワーク

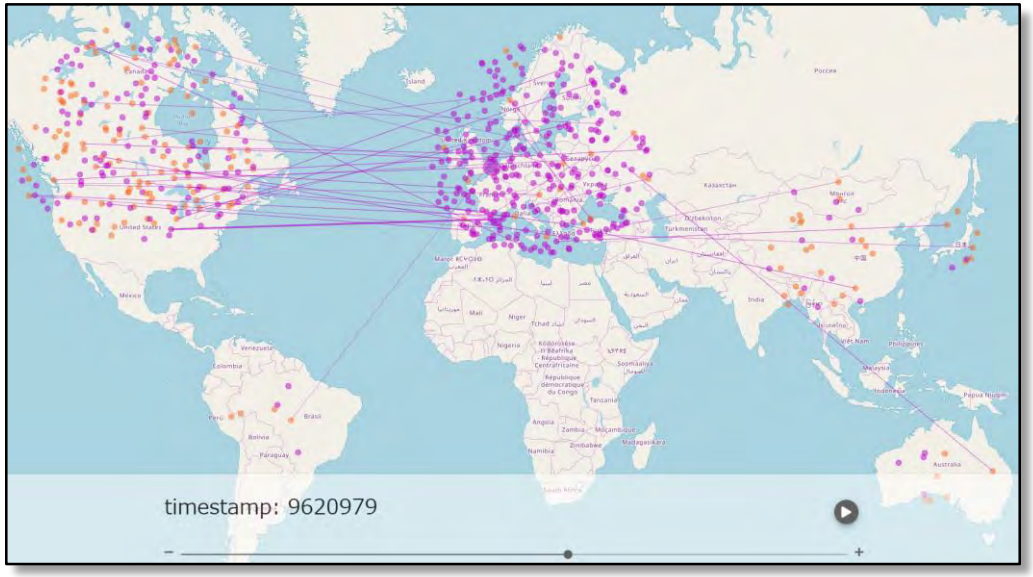


ブロックチェーンが用いるデータ構造

ノード間で、ブロックを伝搬させ、行き渡らせる

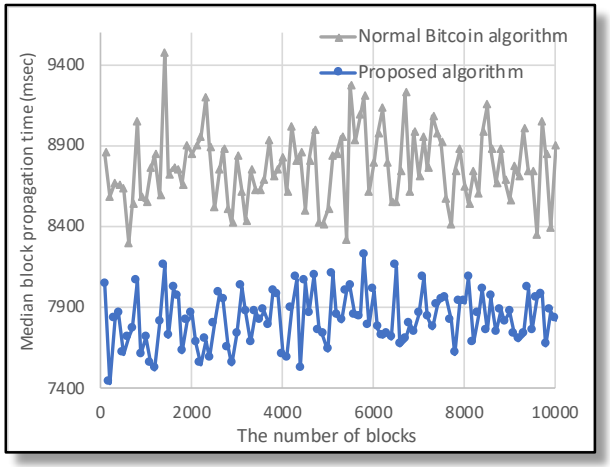
データ伝搬の高速化

- シミュレータの開発
- 手法の提案や評価

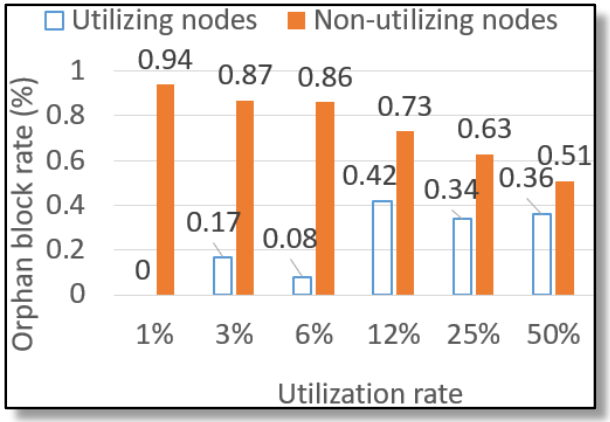


ブロックチェーン ネットワーク **シミュレータ**

SimBlock

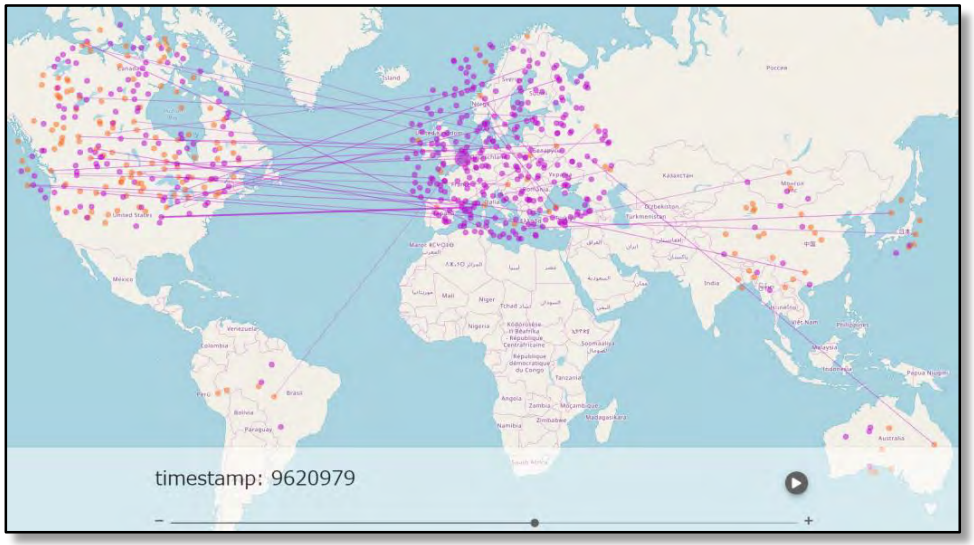


隣接ノード選択



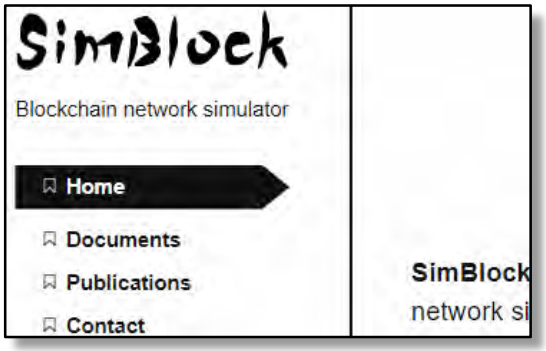
リレーネットワーク 効果推定

ブロックチェーン「ネットワーク」シミュレータ SimBlock



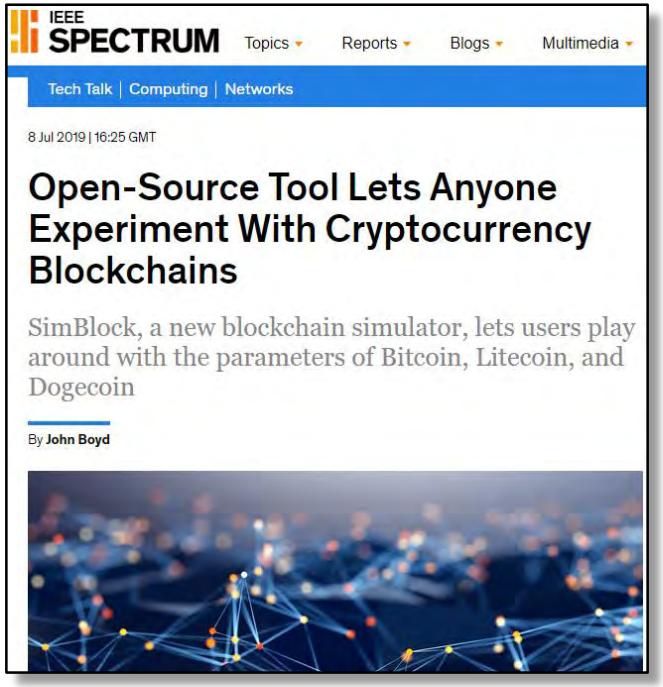
ビジュアライザ　縮小 Bitcoin ネットワーク, 600 ノード

ウェブサイト



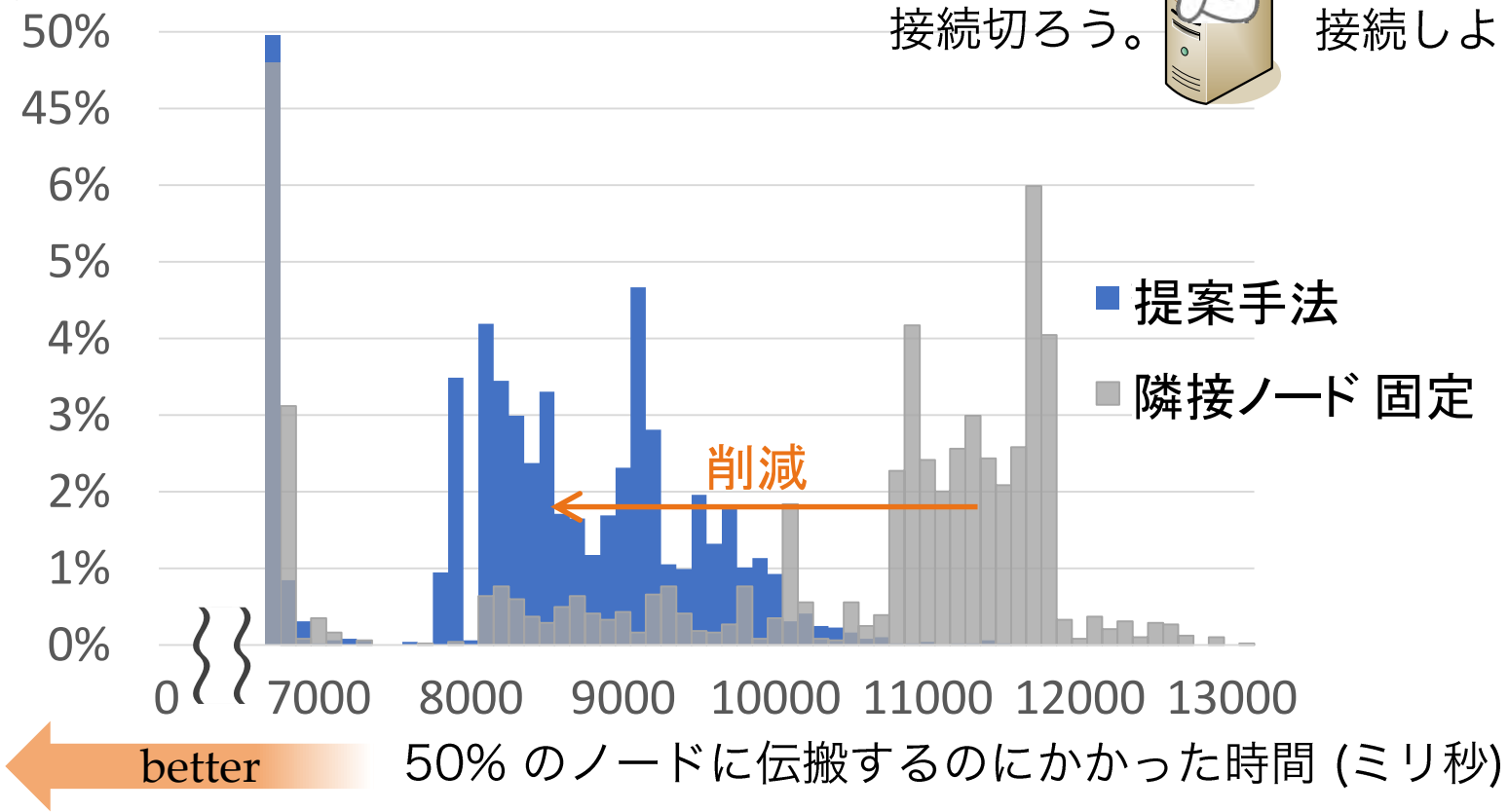
IEEE ICBC 2019 デモ, ソウル, 2019年 5月

IEEE Spectrum 記事



データ伝搬の高速化：隣接ノード選択の提案

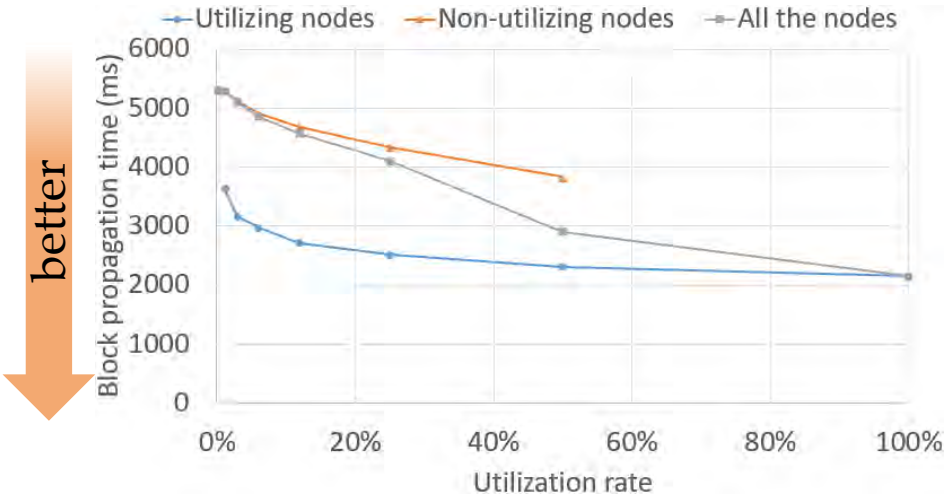
- 隣接ノード選択
  - 通信が速そうなノードを選んでつながる



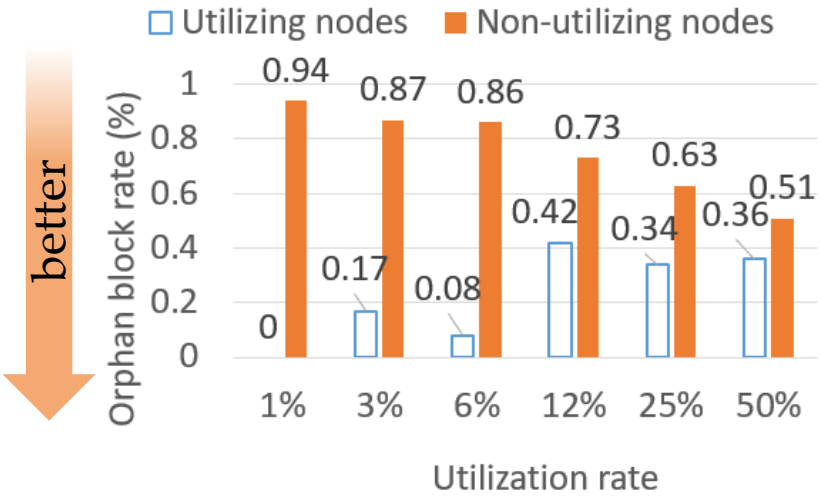
データ伝搬の高速化：リレーネットワークの効果推定

- リレーネットワーク
  - ブロックを高速に伝搬してくれるサービス

リレーネットワークの例: FALCON



50% のノードへの伝搬時間



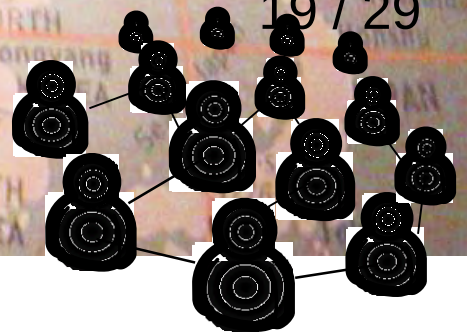
生成したブロックが孤立ブロックになる確率

低下 → マイニング報酬を逃しにくい

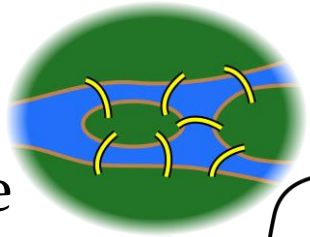
ソーシャル ネットワーク

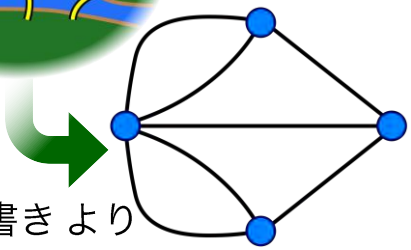
ランダムウォークによる
特徴量推定

ソーシャル ネットワーク



- 人のつながりのネットワーク
  - スモールワールド実験 (1967年〜) by スタンレー・ミルグラム
    - 知人の知人の…を辿って手紙が届くか？ in 米国
    - 平均 5.5人　人口 約 2億人もいたのに
  - SNS が流行って、研究しやすくなった
    - Myspace 2003年〜, mixi 2004年〜, Facebook 2004年〜
  - 対象とする特徴量：人数 (ノード数), 友達の数 (次数), 影響力 (中心性), コミュニティ (クラスタ), 書き込みの伝搬, …
- 研究の道具：グラフ理論
  - グラフ：頂点 / node or vertex と 辺 / edge
  - 例：ケーニヒスベルクの橋 (1736年) by オイラー

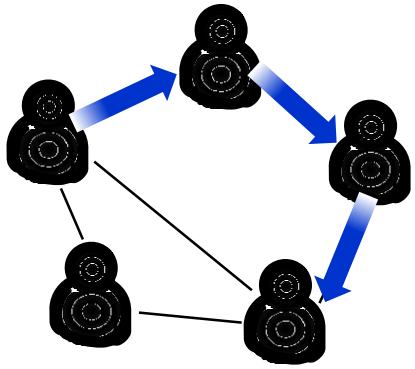




Wikipedia：一筆書き より

ランダムウォークによる特徴量の推定

- 全体は なかなか 調べられない…
  - 手に入らない, 大きすぎる (〜 10 の 9乗), …
- サンプリング、特にクロール、特に**ランダムウォーク**で調べる



① 隣接ノードリストを得る
② その中から次の対象ノードをランダムに選ぶ
③ 次の対象ノードに移る

クローリング

サンプリング結果の
ノード リスト
{1, 2, 4, 2, 7, …}

問い合わせ with
ノード ID

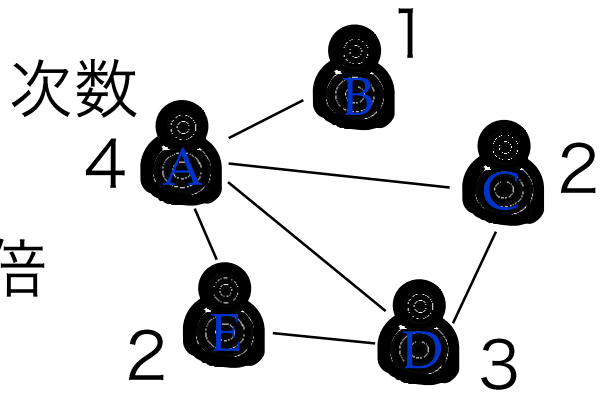
隣接ノード (友人)
リスト

ソーシャルネットワーキングサービス (SNS)

ランダムウォークによる特徴量の推定

- ランダムウォークで
  ノード訪れる回数は、均一ではない。
  - 次数に比例する

ノードA は
ノードB の４倍
訪問される



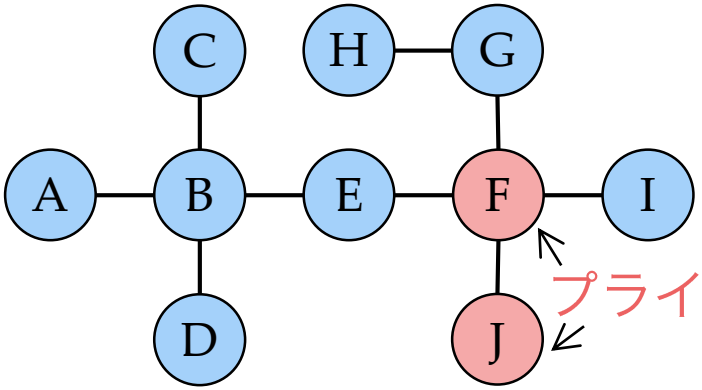
- 特徴量には、次数に応じた**補正**が必要

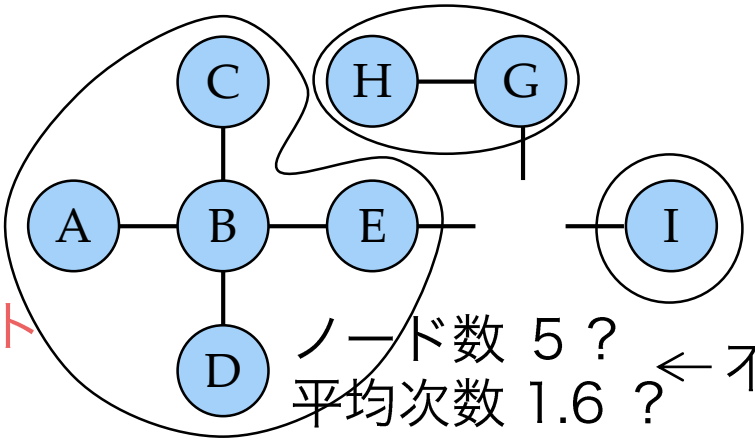
ランダムウォーク　　重み付け

ノード	A, B, A, D, E, A, C, …	
調べる属性	男, 女, 男, 男, 女, 男, 女, …	
次数	4, 1, 4, 3, 2, 2, 4, …	合計
補正	男 ¼ 人, …	男○人 女○人

ランダムウォークによる特徴量推定

- プライベートノード　例：Twitter の鍵アカウント
  - 隣接ノードリスト 非公開のノード





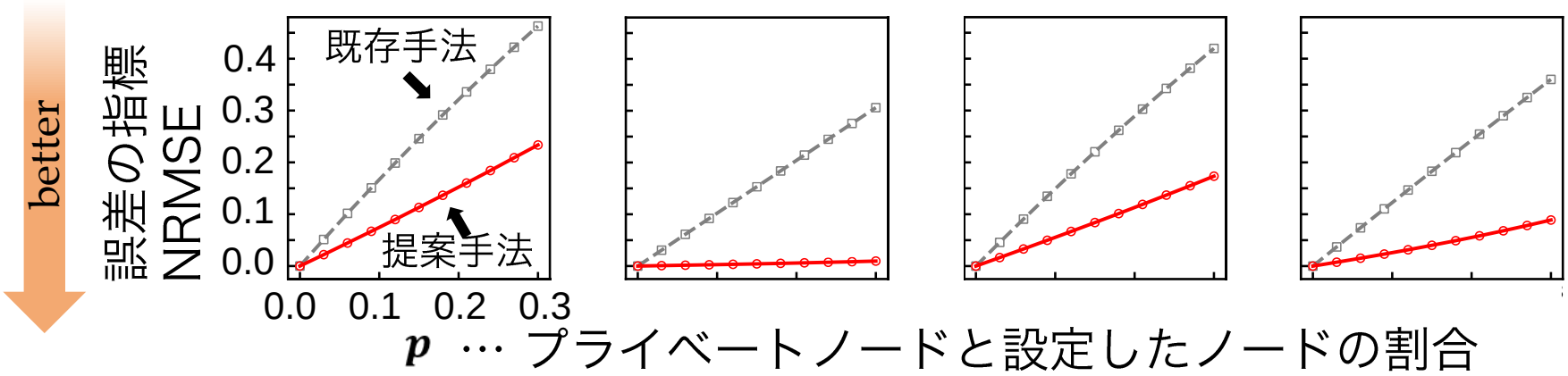
本来のネットワーク　　ランダムウォークできる範囲

- 従来：プライベートノードを無視
- 我々：プライベートノードを考慮

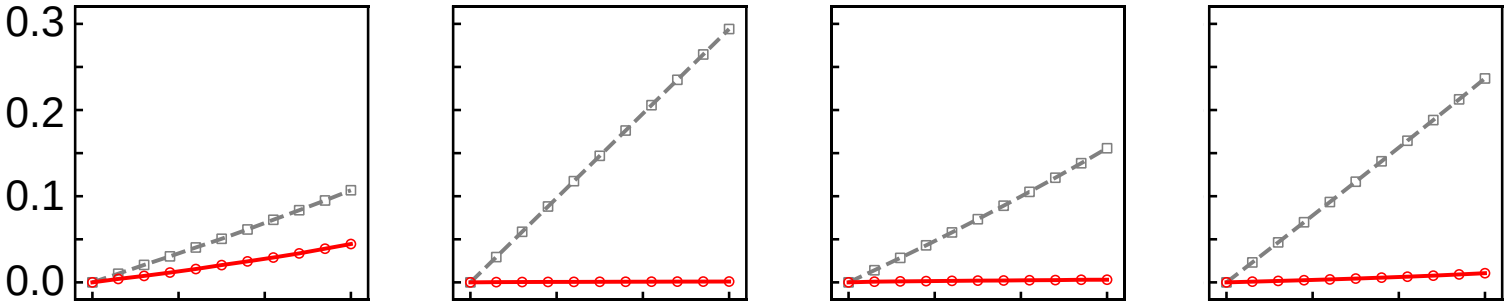
手法や証明は省略

実験結果 (1) 一部のノードを**人為的**にプライベートに

- 推定誤差が大きく減少
  - ノード数 の推定



  - 平均次数 の推定



様々なグラフ： YouTube Orkut Facebook LiveJournal

実験結果 (2) 現実のプライベートノード

- Facebook を対象とした推定
  - 2010年 10月にランダムウォークで集めた 1,016,275 ノード (ユーザ)

手法	ノード数 (ユーザ数)	平均次数 (平均フレンド数)
既存	480,298,540	102.1
提案	656,874,081	137.0

プライベートユーザの割合 0.269

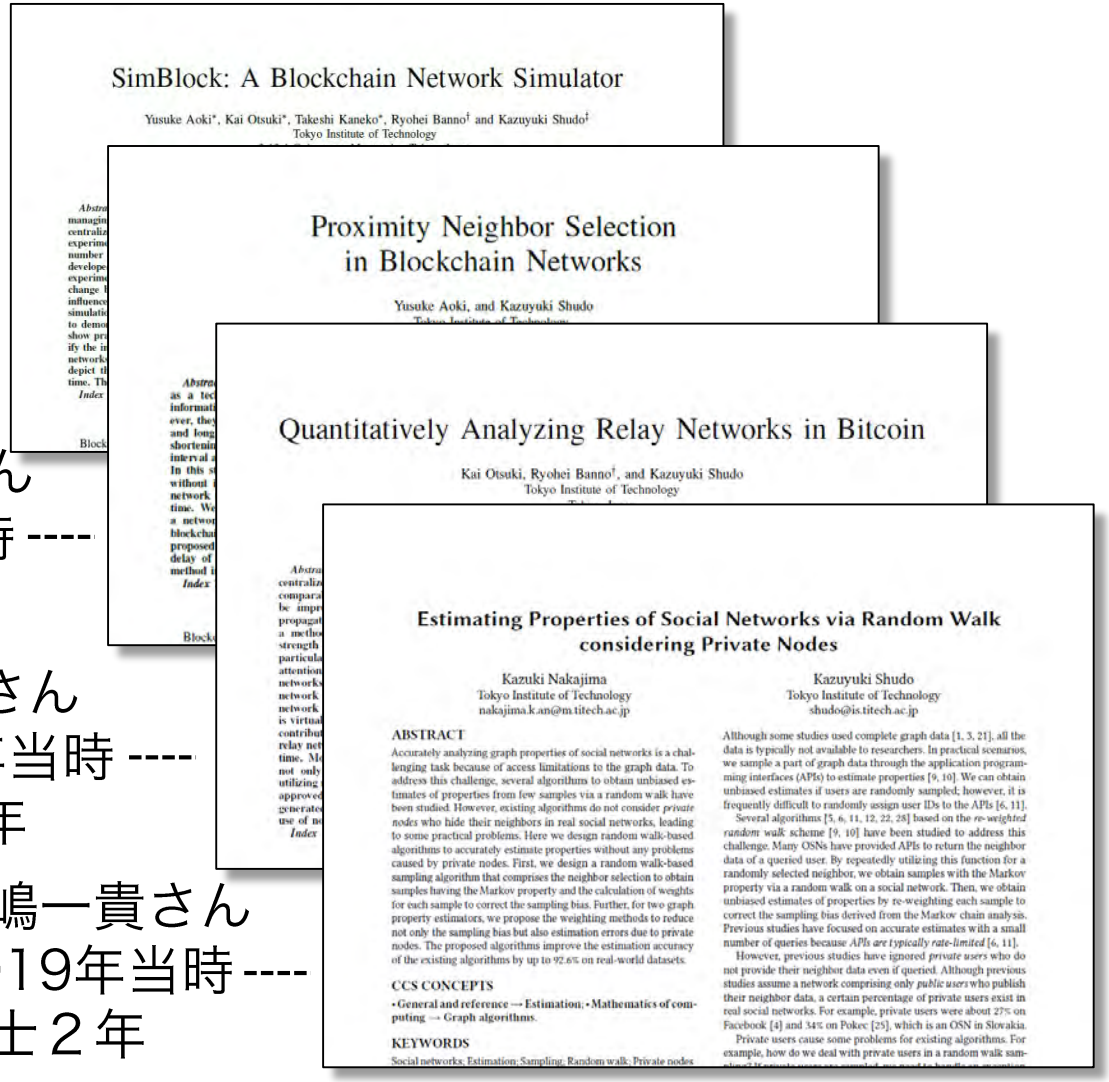
- より正確に推定できた のではないか
  - 2010年 7月時点ですでに、アクティブユーザ数は 500万を超えていた
  - 2010年 8月時点の調査で、プライベートユーザ数の割合は 0.266 だった。上記の結果はこの値とよく合っている

人生の選択にあたって

大学以降のシステム
親のため、は ほどほどに
後悔最小化の法則

論文

- 紹介した研究は大学院生が中心となって行った



青木優介さん
2018年当時 ----
修士２年

大月魁さん
2019年当時 ----
修士１年

中嶋一貴さん
2019年当時 ----
修士２年

- 論文誌や国際会議に投稿 → 審査 → 採択

大学以降のシステム 理系の事情

- 学部 ４年間
- 大学院 修士課程 (博士前期課程) ２年間
  - 高校生の私は、大学院の存在を知らなかった
  - 職業選択の幅が広がる。例：開発職だけでなく研究職も
    自分の学生には、進学を勧めてる。奨学金 とても借りやすい
  - 学費：国公立 学部と同じ (安い), 関東私大 学部より下がる 関西私大 学部と同じ (高い)
  - 東工大では８割くらい進学
    米国トップスクール (例：CMU) では、直接進学は、入学者の1〜2割
  - 国公立大：基本的に要受験 (院試)。一部、推薦的なものも
    私大：推薦も多い。私 (早稲田) の場合、成績上位 ½ は推薦ありだった
- 大学院 博士課程 ３年間
  - 東工大では学部の 1〜2割程度？
  - 職業選択の幅は広がらない。採用は、する側とされる側のマッチング

人生の選択にあたって (1)

- 親 (周囲) のため、は ほどほどに
  - **親は、自分が不安を感じたくない** → 子の安定を望む
  - 自分で決めないと、後悔の際、人のせいにしてしまう。
  - 親は先に死ぬ。最後まで面倒看てくれるわけでも、責任とってくれるわけでもない。

	自分が就きたい職業（夢！）		親として就いて欲しい職業（安定！）	
男の子	1	スポーツ選手	1	公務員
	2	警察官	2	医師
	3	運転士・運転手	3	会社員
		まったく違う ⟷		
女の子	1	ケーキ屋・パン屋	1	看護師
	2	芸能人・歌手・モデル	2	公務員
	3	看護師	3	薬剤師

人生の選択にあたって (2)

- 後悔最小化の法則
  - 選ばなかったら後悔してしまうだろう方を選ぶのがいい
  - 未来から現在を見返して、考える
  - やらなかったことへの後悔は、いくらでも想像が膨らむ。

2001 産業技術総合研究所 **国の研究所**

↓ この転職で、ものすごく悩んだ

2006 ウタゴエ(株) **スタートアップ**

↓ **(ベンチャー企業)**

2008/12 東京工業大学

- 人生の目標：死ぬ瞬間に「いい人生だった」と思うこと

・(技術的な) 名声や名誉
- 産総研
  △ 自由度が高いので、自分次第。
  ○ [redacted]。
- ウタゴエ
  △ [redacted]成功すれば○。

・世の中にインパクトを与えること
- 産総研
  ?? とにかく自分次第。
  × 直接の製品開発はしない。

・自分の発想で活動できる自由
- 産総研
  ○ お客相手の商売ではない。
  ○ 研究を提案できる。
  × [redacted]いろいろ制限される。[redacted]
- ウタゴエ
  △ ビジネス上の目的は、たいてい given。

・リタイアを選択できるくらいのお金
- 産総研
  × 無理。
- ウタゴエ
  ?? [redacted]成功すれば◎。

当時の分析メモ：
国の研究所と
ベンチャー企業の比較