カナダにおける Bitcoin ATMの利用調査

明治大学総合数理学部先端メディアサイエンス学科
4-4-76 井垣 秀星

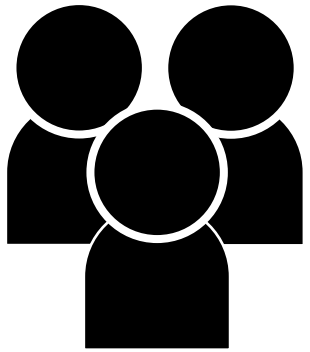
本研究の概要

目的1
Bitcoin ATMと利用者の利用調査

本研究

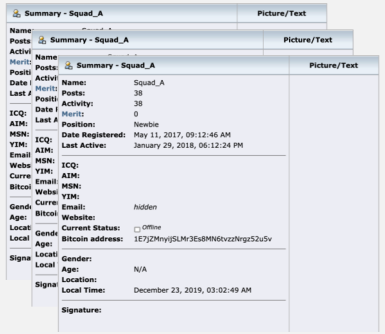
Bitcoin ATM

Bitcoin ATM利用者

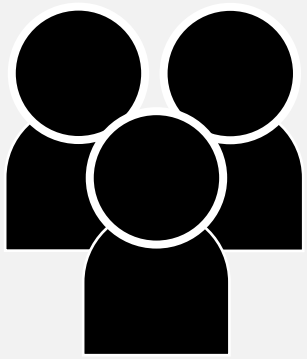


先行研究

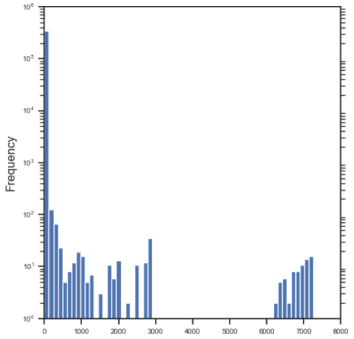
Bitcoin Talk



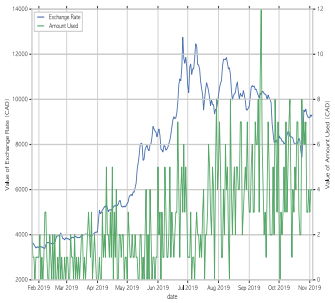
Bitcoin Talk利用者



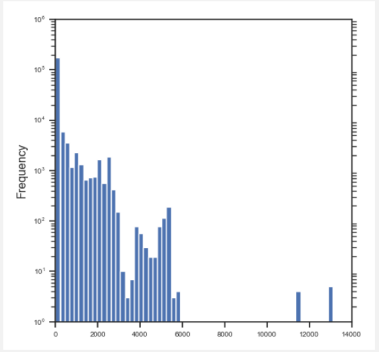
目的2
Bitcoin Addressの使い方を比較



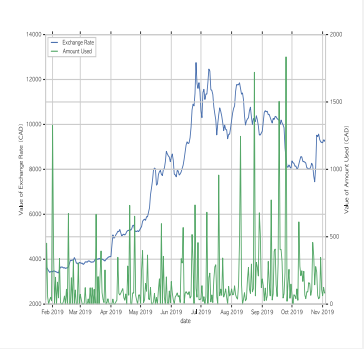
Address利用期間



取引回数

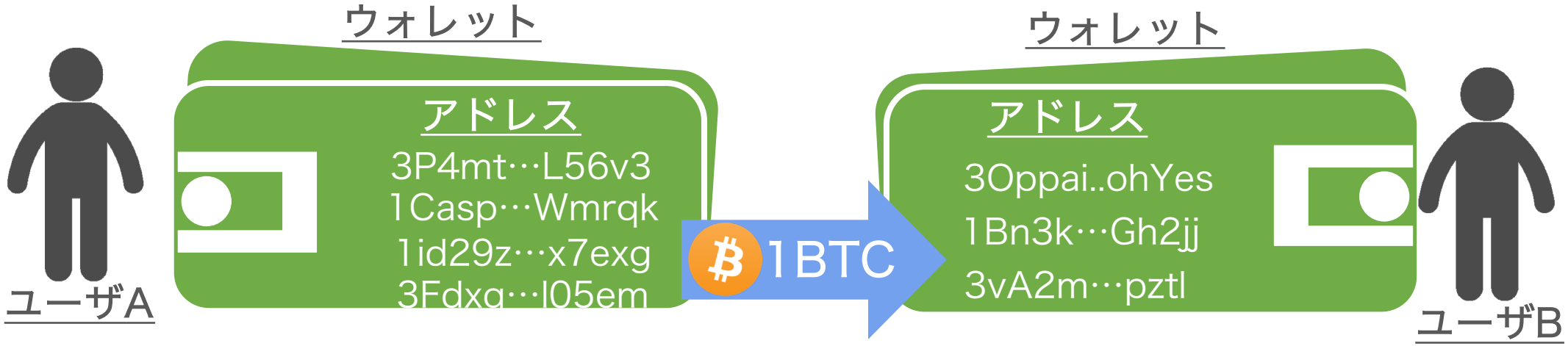


Address利用期間

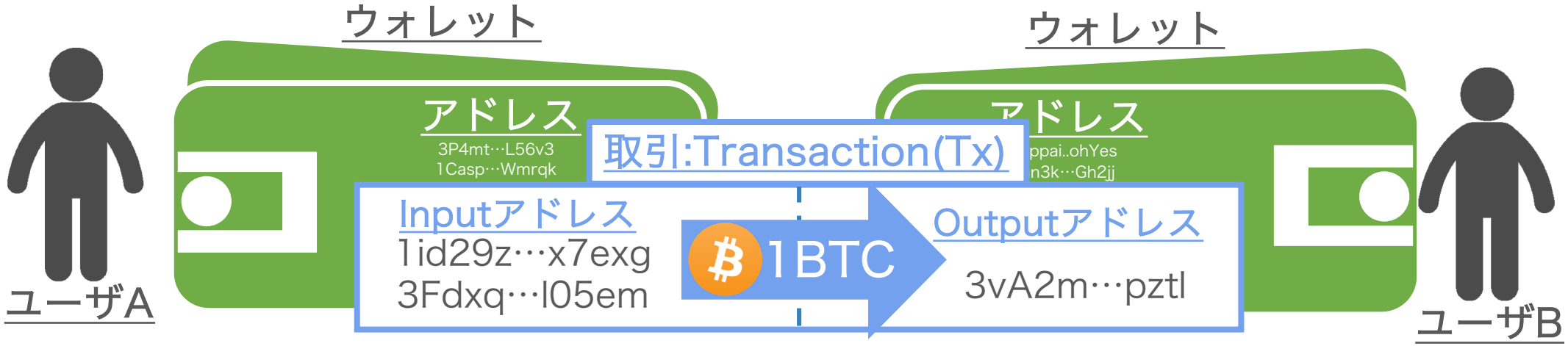


取引回数

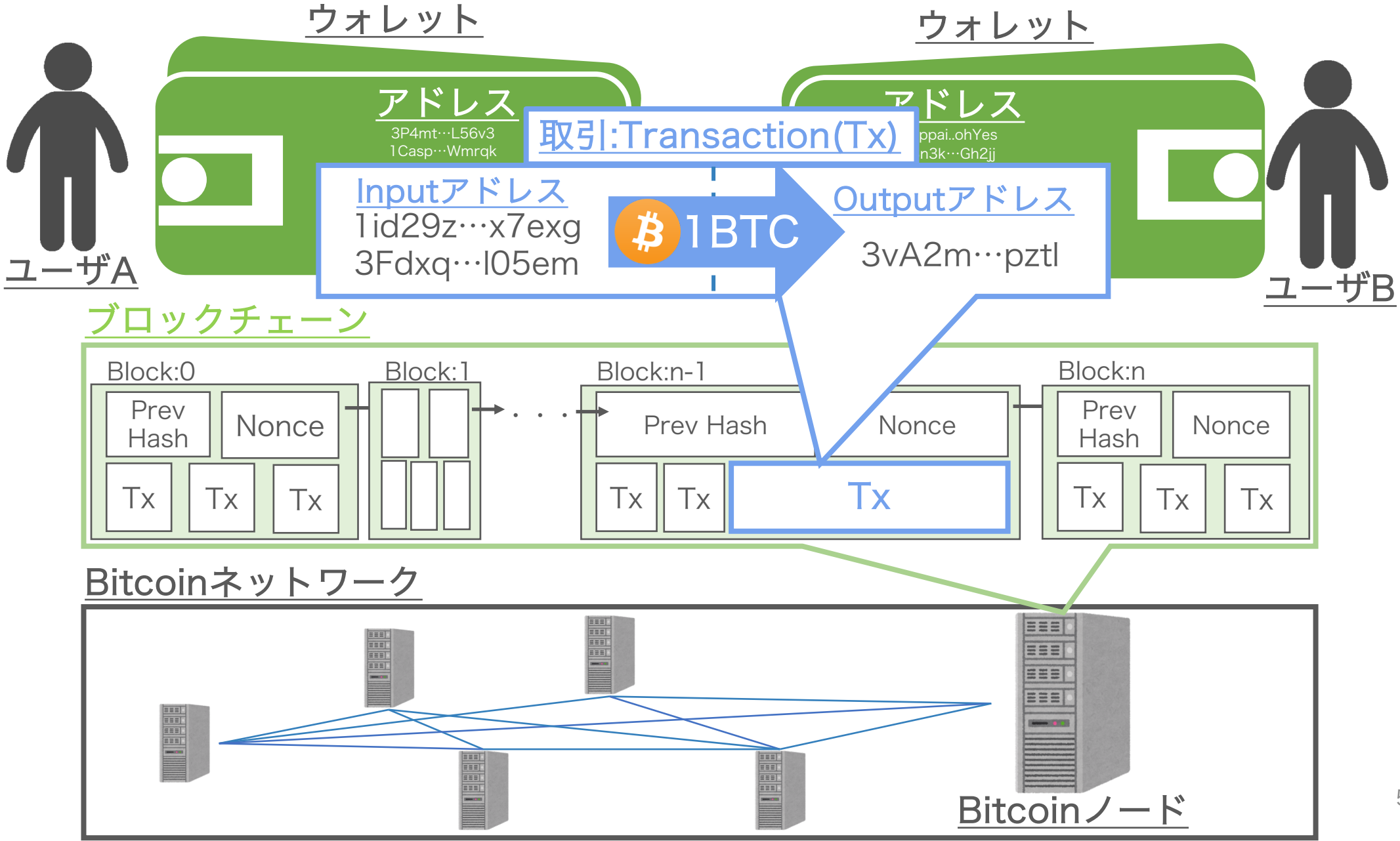
背景:Bitcoinの仕組み



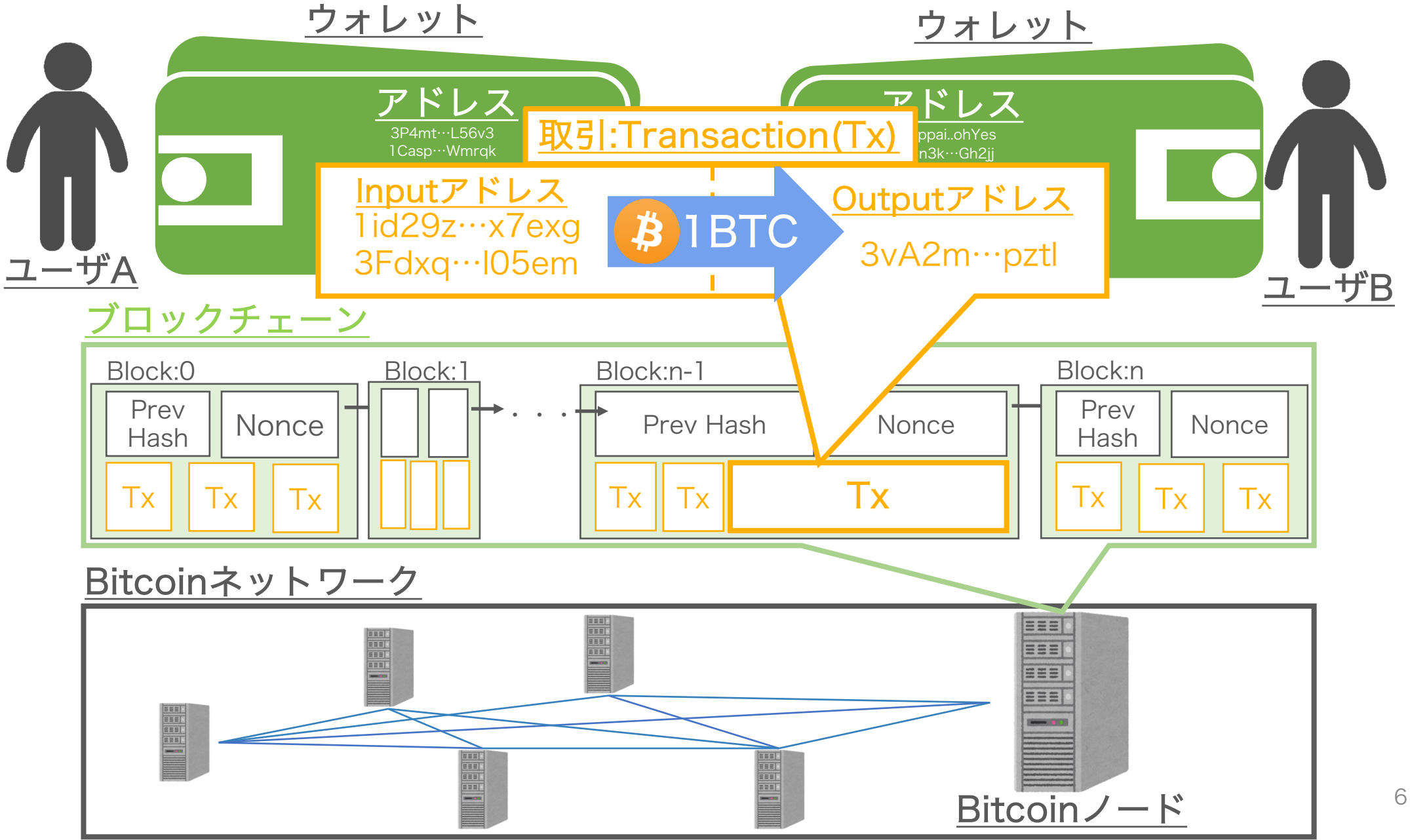
背景:Bitcoinの仕組み



背景:Bitcoinの仕組み



背景:Bitcoinの仕組み



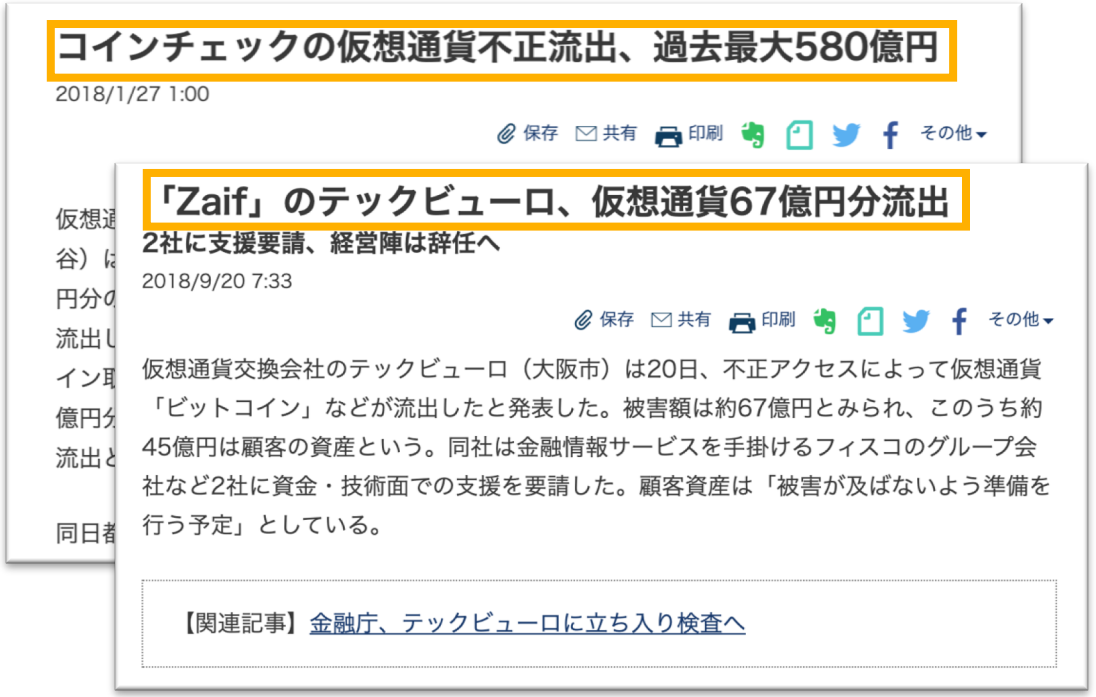
背景:暗号通貨の匿名性

暗号通貨の匿名性

ニュース

- コインチェック NEM 約580億円分不正流出(2018年1月)
- Zaif Bitcoin, Monacoin, Bitcoin chache 合計約67億円分不正流出(2018年9月)

=> 犯人が現実世界のどこの誰かわからない



コインチェックの仮想通貨不正流出、過去最大580億円

2018/1/27 1:00

保存 共有 印刷 その他

「Zaif」のテックビューロ、仮想通貨67億円分流出

2社に支援要請、経営陣は辞任へ

2018/9/20 7:33

保存 共有 印刷 その他

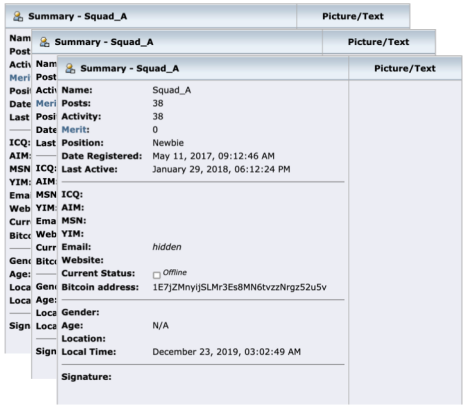
仮想通貨交換会社のテックビューロ（大阪市）は20日、不正アクセスによって仮想通貨「ビットコイン」などが流出したと発表した。被害額は約67億円とみられ、このうち約45億円は顧客の資産という。同社は金融情報サービスを手掛けるフィスコのグループ会社など2社に資金・技術面での支援を要請した。顧客資産は「被害が及ばないよう準備を行う予定」としている。

【関連記事】金融庁、テックビューロに立ち入り検査へ

先行研究

- 同一ユーザが管理するアドレスを識別(Meiklejohn, IMC'13, 2013)
- アドレス管理者のタイムゾーンを特定(Dupont, CodaSPY'15, 2015)
- Bitcoinアドレスの送金先集合に基づく匿名性の評価(永田, CSEC-80, 2018)
- 平均取引時間分布の相関を用いたBitcoinユーザのタイムゾーン属性の推定(井垣, 情報処理学会第81回大会, 2019)

背景:先行研究

	データ取得ソース	データセット	目的
先行研究	**Bitcoin Talk** 	• Input Address • Output Address • トランザクション	同一ユーザのアドレス? -> 匿名性の評価実験
		• Input Address • Output Address • ユーザのロケーション • トランザクション	ユーザのタイムゾーン属性はどこ? -> タイムゾーン推定実験
本研究	**Bitcoin ATM** 	• Input Address • Output Address • トランザクション	匿名性の評価実験 タイムゾーン推定実験 -> Bitcoin ATMの特徴は? -> Bitcoin Talkと同じ結果?

背景:Bitcoin ATM

特徴

- 登録作業は不必要
- 現金を利用して暗号通貨を購入
- 購入にはBitcoin Addrressが必要
- 実機の利用が必須のためタイムゾーンが限定

補足

- 2019年11月時点 設置台数は6,000台以上
- カナダには600台以上設置

BitcoinAddress
提示箇所

現金投入口

研究:データセット

Addressテーブル

Address	属性
1CasperDEhy…	Bitcoin Talk
1MiningaRyy…	ATM1
3ecP15Hj8ex…	ATM1
1oPPa3ckb9…	ATM2
1m8x9guqP…	ATM3
1FdxQxtzkRR…	Bitcoin Talk
3sLo47kLpee…	ATM2
1FdxQxtzkRR…	ATM1
…	…

Transactionテーブル

Address	TxHash	InOut	Timestamp
1CasperDEhy…	0a8996…	0	2012-02-18 00:57:33
1CasperDEhy…	e5f374…	1	2012-02-18 04:24:46
1MiningaRyy…	036a3…	0	2012-06-23 23:45:23
1MiningaRyy…	81aaa…	1	2013-07-11 13:05:51
1FdxQxtzkRR…	f4004…	1	2013-08-09 21:43:21
1oPPa3ckb9…	a634a…	0	2012-04-27 20:32:26
1oPPa3ckb9…	15abb…	1	2012-07-23 01:42:27
1m8x9guqP…	13054…	0	2014-09-11 08:22:51
…	…	…	…

属性の説明

- 本実験では合計で3台のBitcoin ATMを利用した. それぞれの属性名をATM1, ATM2, ATM3とした.
- 機種はATM1, ATM2が同じ, ATM3のみ異なる.

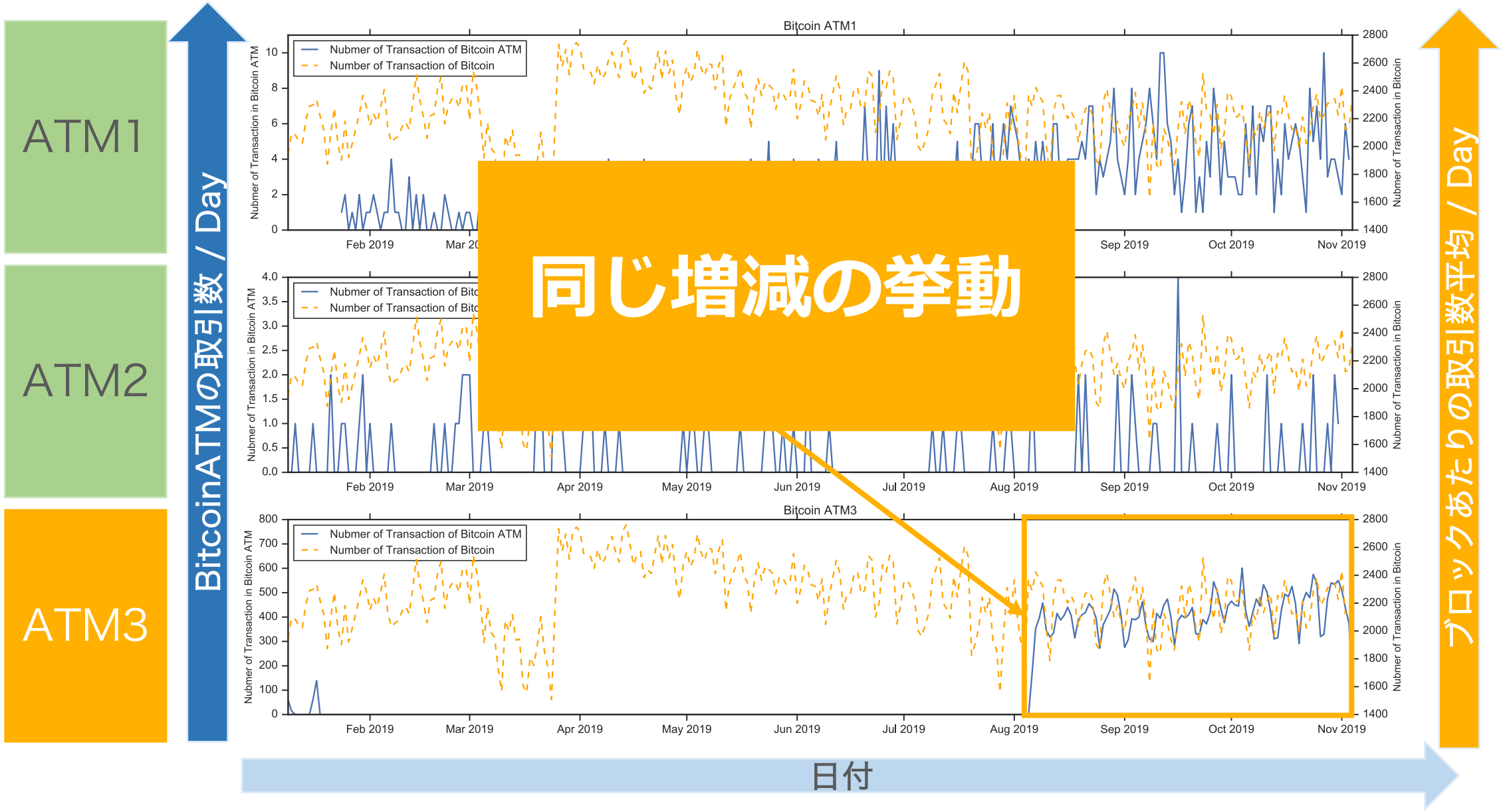
結果:Bitcoin ATM取引の特徴

ATM1

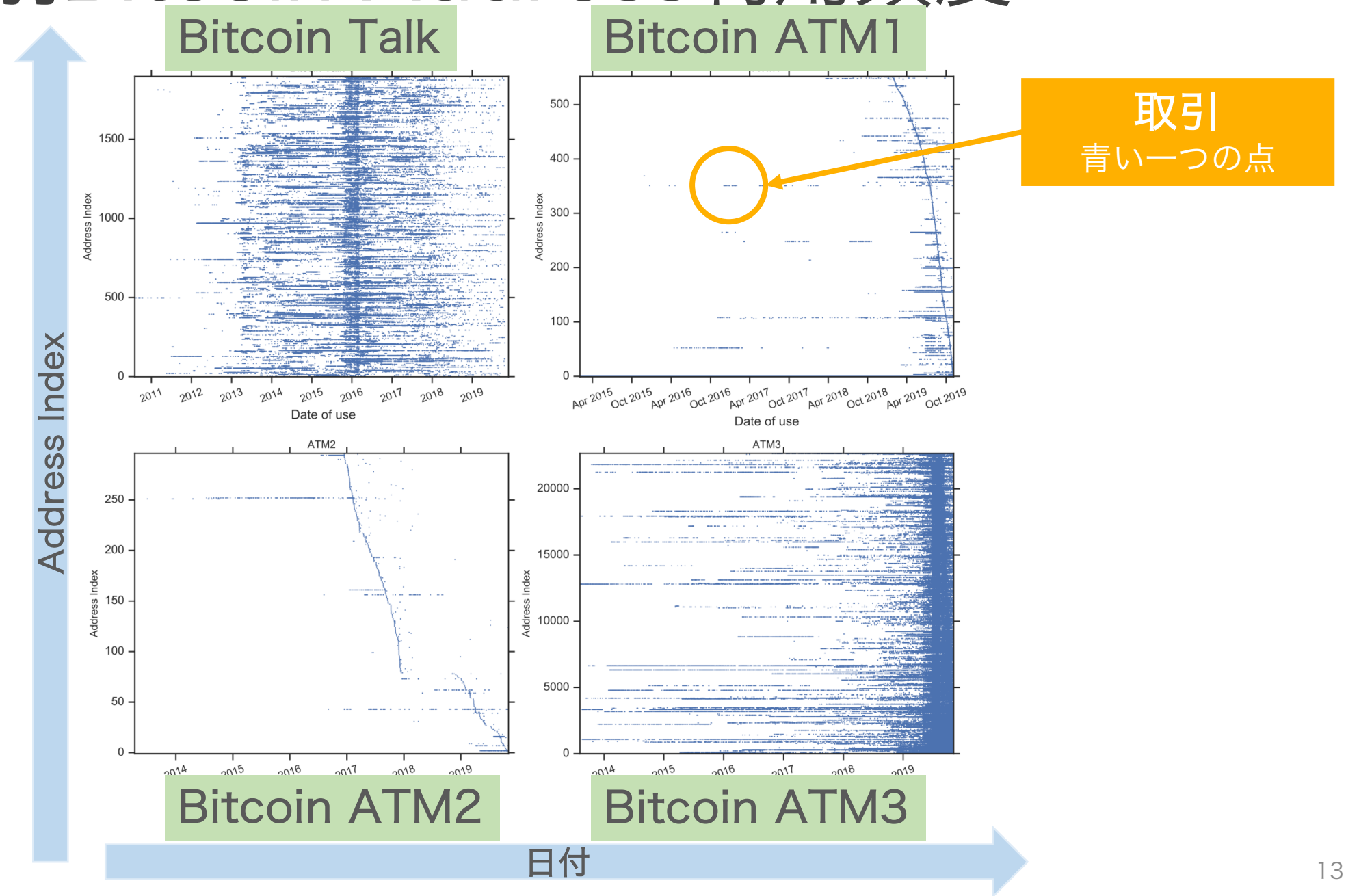
ATM2

ATM3

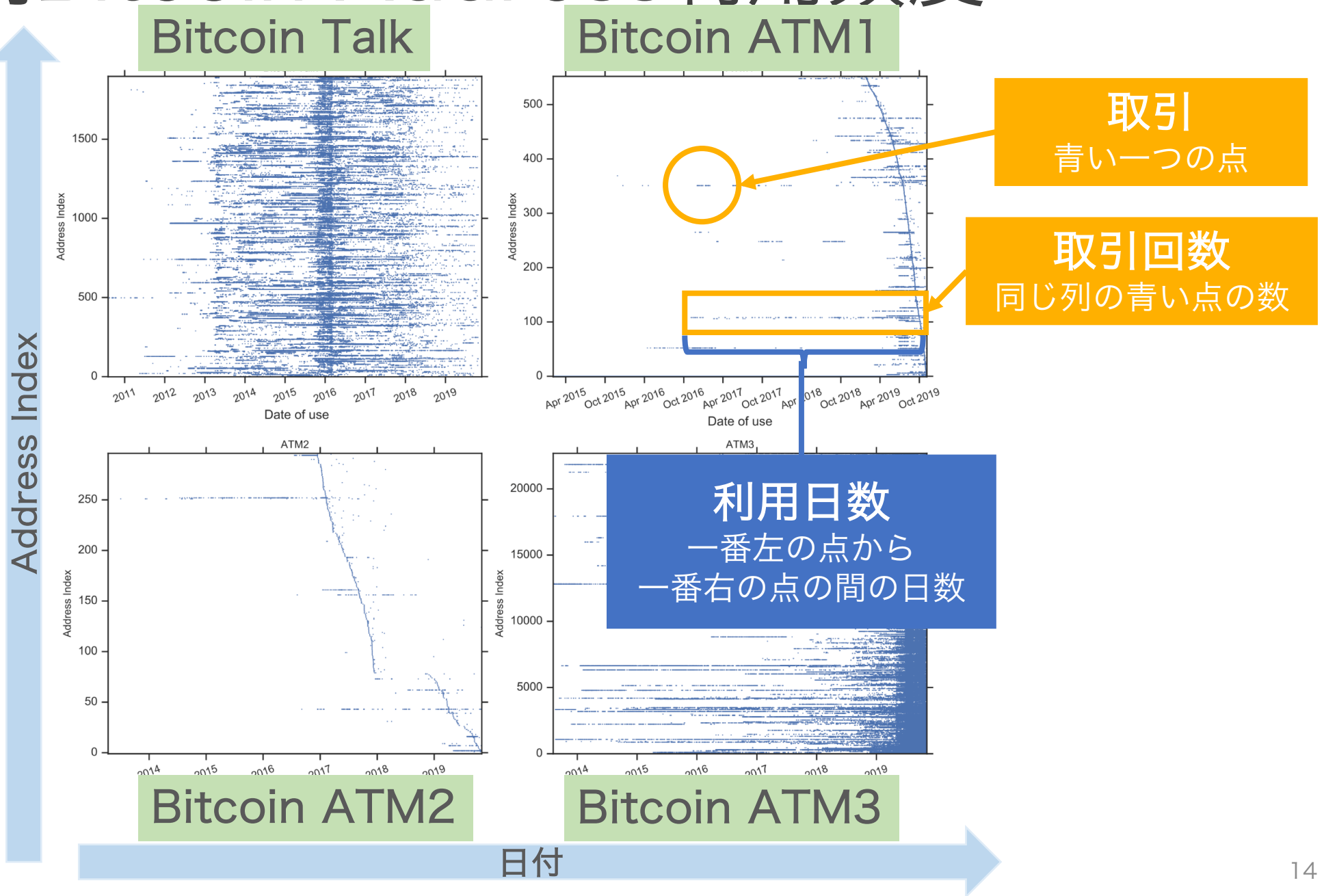
結果:Bitcoin ATM取引の特徴



結果:属性別Bitcoin Address利用頻度



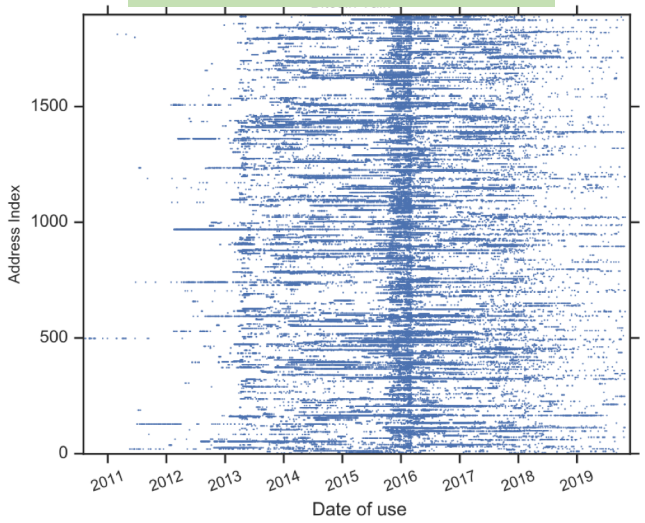
結果:属性別Bitcoin Address利用頻度



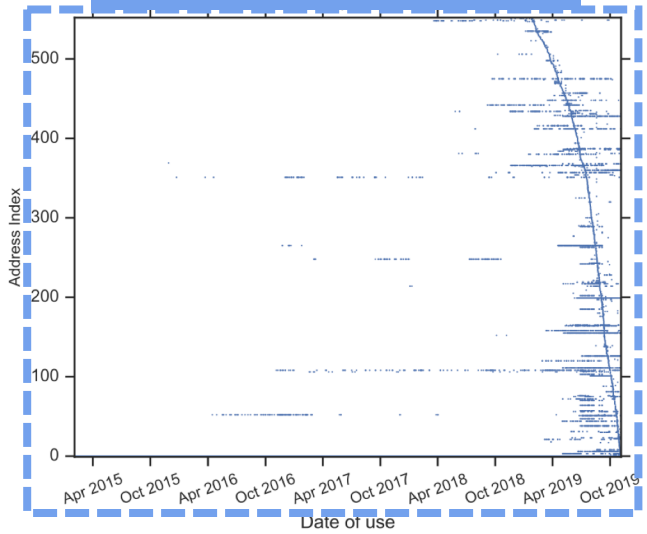
結果:属性別Bitcoin Address利用頻度

Address Index

Bitcoin Talk

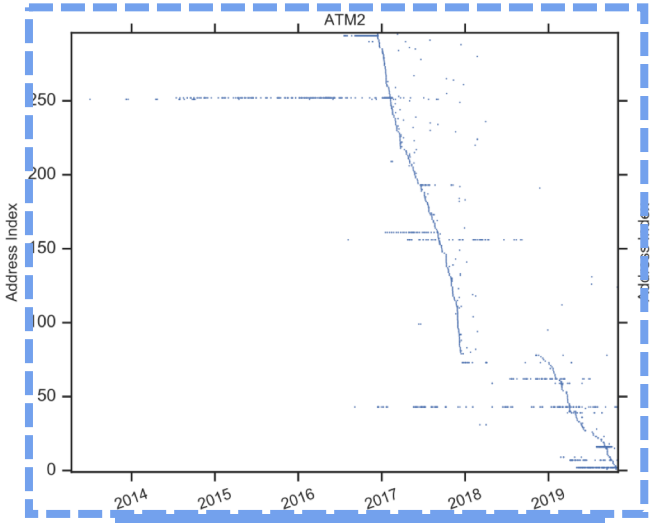


Bitcoin ATM1

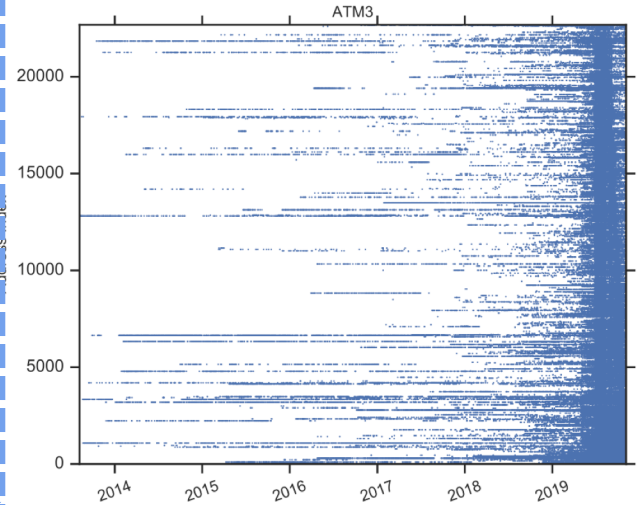


ATM1, ATM2

取引回数中央値：2回
利用日数中央値：0.14~1.16日
=> 短い期間, 数回のみ利用



Bitcoin ATM2



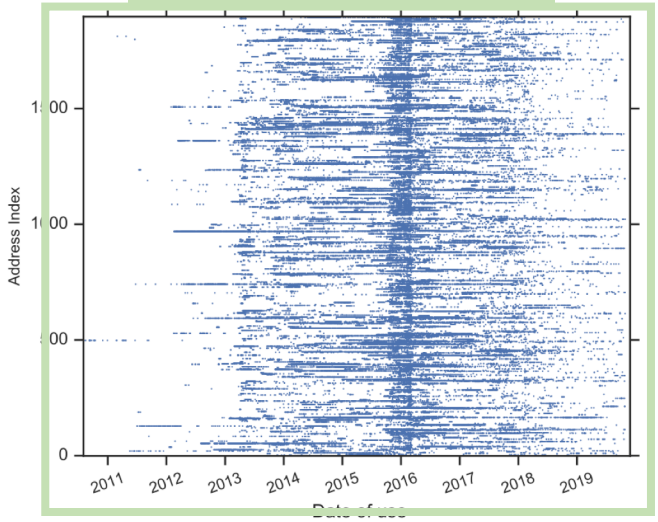
Bitcoin ATM3

日付

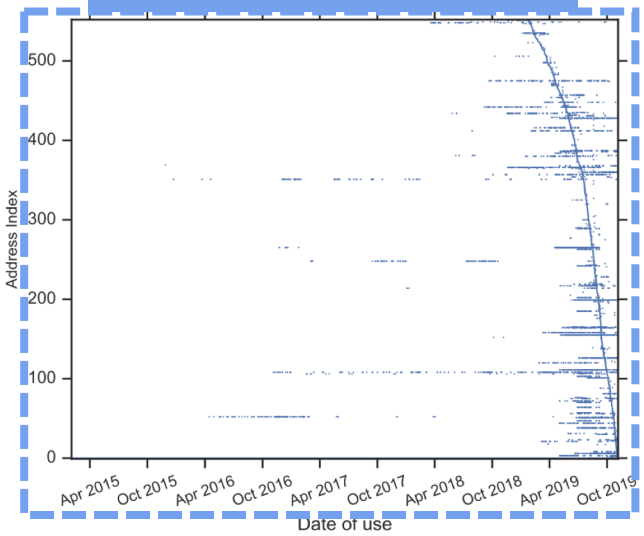
結果:属性別Bitcoin Address利用頻度

Address Index

Bitcoin Talk

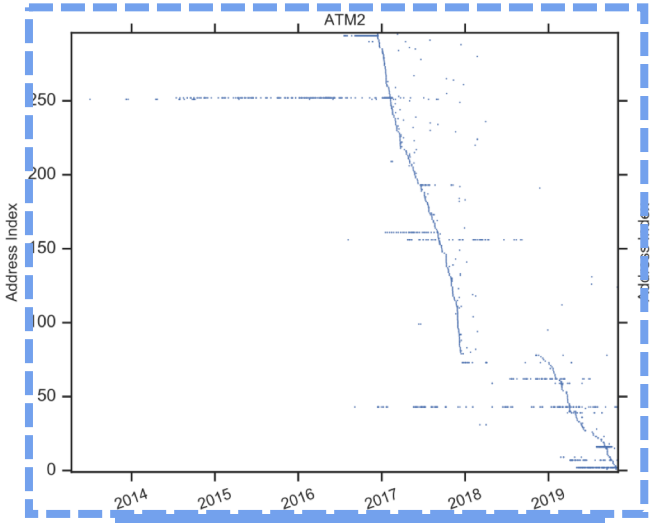


Bitcoin ATM1

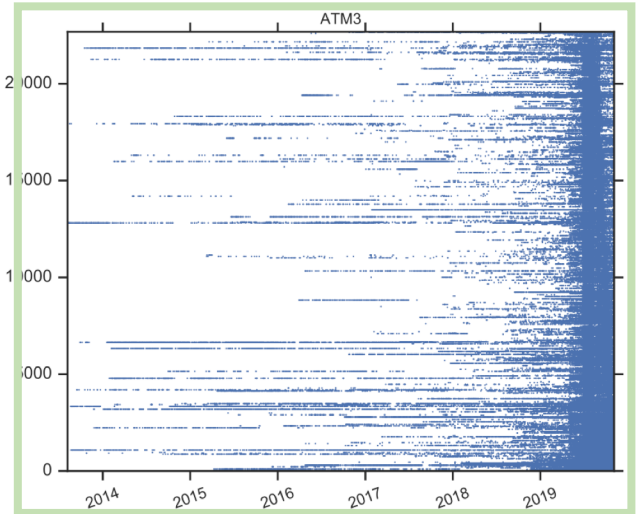


ATM1, ATM2

取引回数中央値：2回
利用日数中央値：0.14~1.16日
=> 短い期間, 数回のみ利用



Bitcoin ATM2



Bitcoin ATM3

Bitcoin Talk, ATM3

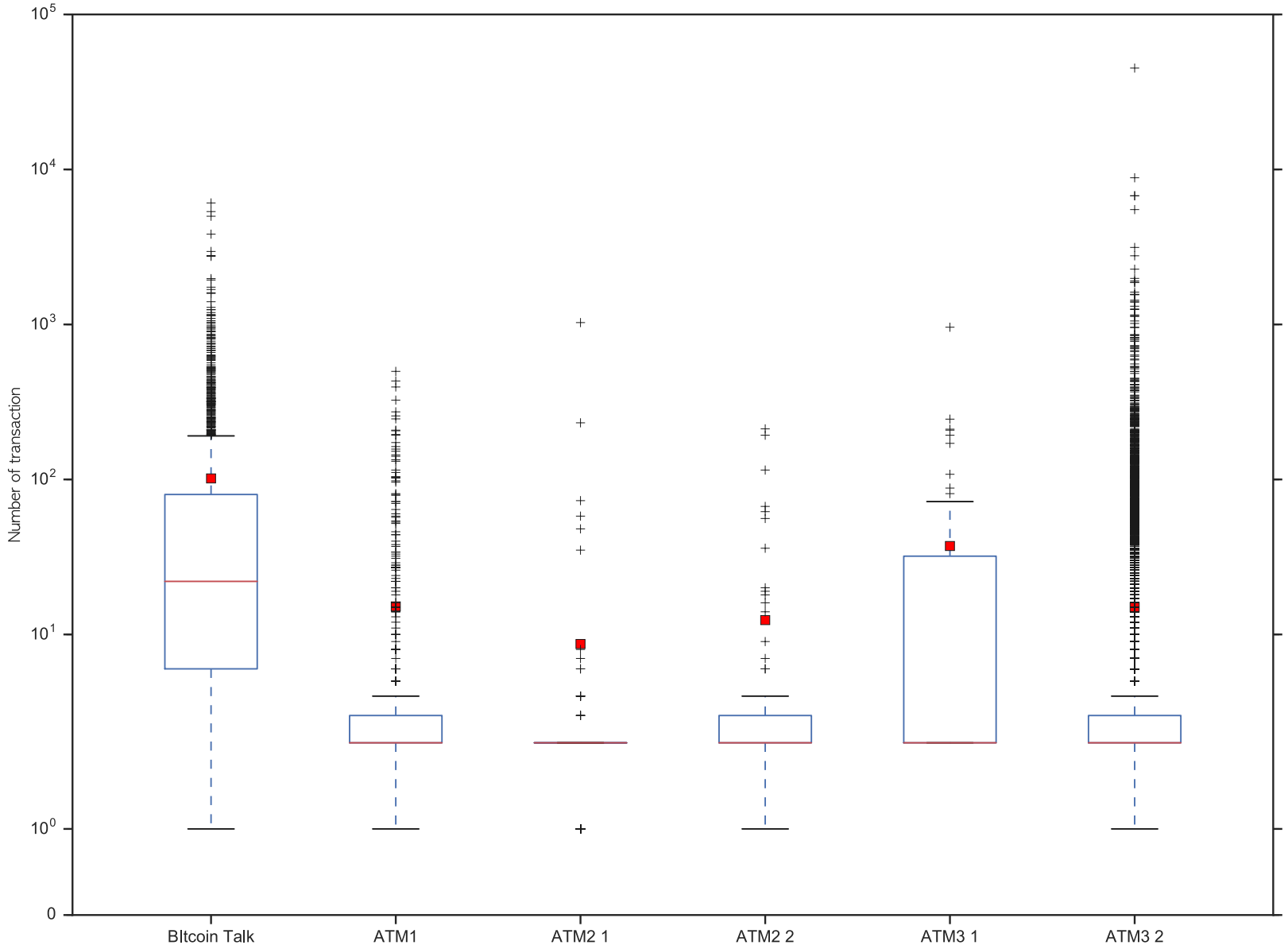
取引回数中央値：22回
利用日数中央値：183.16日
=>長い期間, 幾度も利用

日付

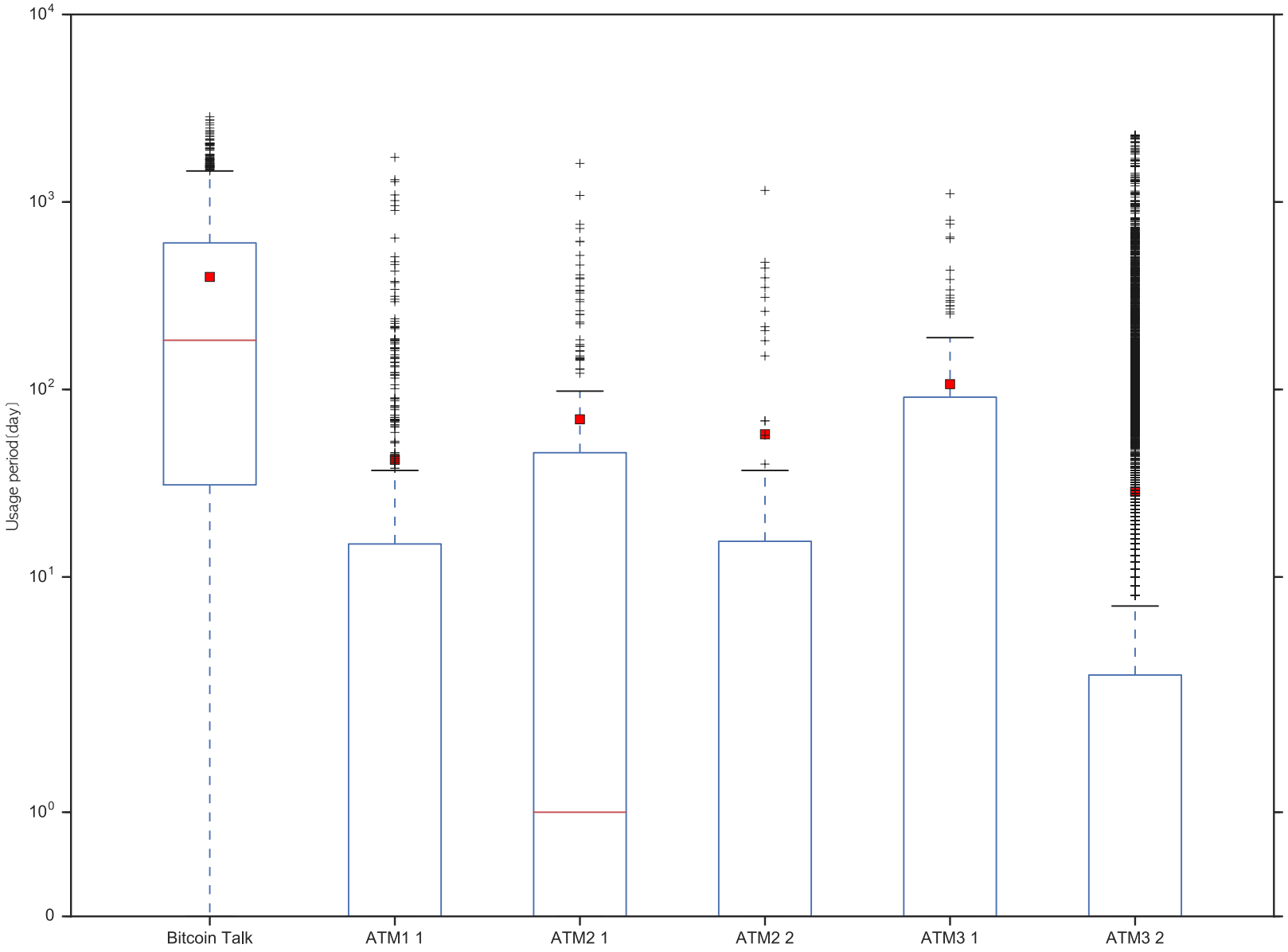
結論

結果	◘Bitcoin ATMの取引数とBitcoinシステムの取引数の増減が同じ挙動 ◘Bitcoin ATM利用者はBitcoin Talk利用者より取引数が少なく利用期間が短い
考察	• Bitcoinは一般的な支払いに利用されていない • 企業, 利用者間の取引が全体の取引量に大きく作用 • Bitcoin Talk利用者 = 長期間利用 • Bitcoin ATM利用者 = 使い捨てている => Bitcoin ATM利用者は匿名性を考慮 => Bitcoin ATM利用者とBitcoin Talk利用者は特徴が違うため匿名性も異なる

補足 属性別 取引数


10^5
10^4
10^3
10^2
10^1
10^0
0
Number of transaction
BItcoin Talk
ATM1
ATM2 1
ATM2 2
ATM3 1
ATM3 2

補足 属性別 Address利用期間



補足 Bitcoin ATM利用者定義

定義

Input Address	Output Address
一つ以上の同じBitcoin ATM Address	一つ以上の同じBitcoin ATM Address
	Bitcoin ATM 利用者 Address

具体例1

Input Address	Output Address
35pJQef1CGscLec9jyddMu2DLU5Swq12wK	35pJQef1CGscLec9jyddMu2DLU5Swq12wK
	1HeyUycFzdU1Tq3tm28xKbA3BJTyZhrg8e

具体例2

Input Address	Output Address
35pJQef1CGscLec9jyddMu2DLU5Swq12wK	35pJQef1CGscLec9jyddMu2DLU5Swq12wK
35pJQef1CGscLec9jyddMu2DLU5Swq12wK	35pJQef1CGscLec9jyddMu2DLU5Swq12wK
	1HeyUycFzdU1Tq3tm28xKbA3BJTyZhrg8e

補足 Bitcoin ATM

属性名	ATM1, ATM2	ATM3
画像		
企業	General Bytes	Delloite