明治大学総合数理学部

2019 年度

卒　業　研　究

カナダにおける Bitcoin ATM の利用者調査

学位請求者　先端メディアサイエンス学科

井垣秀星

目次

第 1 章　はじめに 2
1.1　概要 . . . 2
1.2　背景 . . . 2

第 2 章　データの説明 4
2.1　Bitcoin Talk . . . 4
2.2　Bitcoin ATM . . . 4
2.3　Bitcoin ATM 利用者 . . . 4
2.4　Bitcoin 価格 . . . 4

第 3 章　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実験 7
3.1　概要 . . . 7
3.2　方法 . . . 8
3.3　結果 . . . 9
3.4　考察 . . . 10

第 4 章　カナダにおける Bitcoin ATM の利用者調査実験 12
4.1　調査目的 . . . 12
4.2　データの収集 . . . 12
4.3　データの分析 . . . 12
4.4　実験結果 . . . 14
4.5　考察 . . . 19

第 5 章　おわりに 24

参考文献 26

第 1 章

はじめに

1.1 概要

近年, 暗号通貨の利用者が増加している. 中でも 2009 年 から運用が開始された Bitcoin[1] の Blockchain Explorer サービス*のウォレットを保持しているユーザ数は, 2018 年の 31, 253, 090 から 2019 年は 44, 005, 417 と 1 年間で 1, 000 万以上増加している. その理由として, 銀行などの第三者機関を介さずに取引できることや, 資産価値, 匿名性が高いという特徴が挙げられる.

匿名性評価, 属性推定についてのいくつかの先行研究が行われている. 永田は送信先集合による匿名性の評価実験により最大で 80.5% のアドレスが識別されることを示した [4]. Dupont らはタイムゾーン属性を 72% で推定できることを示した [5]. しかしながら全てのユーザが所属するタイムゾーンの昼の時間帯に活動するわけではなく, 平均推定精度は 72% にとどまっていた. さらに, 取引が 0 の時間帯を特徴量としていたので, 1 回でも取引をすると誤りを引き起こしていた. そこで, 本研究では一つ目の研究として取引時間分析の相関係数に基づくノイズに対する頑強性の高い推定方法を提案する.

さらに, 自分の研究を含め研究にて取り扱った Bitcoin Talk の登録ユーザは Bitcoin に技術関心のある技術力の高いユーザであることから一般の Bitcoin 利用者と比較して偏っていることが懸念される. そこで本研究では, オンラインではなく, 実機にて預貯金操作をする必要があり, 利用場所が限定される特徴から Bitcoin ATM 利用者に着目する. Bitcoin ATM 設置台数が 600 台を超えたカナダの Bitcoin ATM 利用者 Address を用い, Bitcoin Talk 利用者データとの統計的違いを示す. 二つ目の研究として Bitcoin ATM, 利用者の利用特徴の調査, また属性ごとに Bitcoin Address の利用方法が異なることを明らかにすることを目的とする.

1.2 背景

1.2.1 Bitcoin

Bitcoin は Nakamoto 氏の論文を基に特定の中央管理者を持たず, 2009 年より運用が開始された暗号資産である. 取引の検証や承認, 新たなビットコインの発行は全ユーザの合意によって行われる. ビットコインの取引に関する情報はブロックに格納される. ブロックは約 10 分に 1 個生成され, 各ブロックが 1 つ前のブロックと繋がってブロックチェーンを構成し, ノード間で分散管理されている. ブロックや取引に関する情報は Blockchain のクライアント, もしくは Blockchain Explorer サービスで確認できる.

*https://www.blockchain.com/explorer

1.2.2 Bitcoin Talk

Bitcoin Talk は Bitcoin 開発者のコミュニティサイトである. Bitcoin に関する質問から議論まで, 様々なスレッドが立てられて話し合いが行われており, サイトに登録することで参加することが可能になる. サイトに登録すると個人のプロフィールページが割り当てられ, 登録者は Bitcoin Address や居住地などを登録・公開することができる.

1.2.3 Bitcoin ATM

Bitcoin ATM は現金を利用して Bitcoin, Ethereum などの暗号通貨を購入できるサービスで, 図 2.1 の様な機械を利用する. 通常の ATM とは異なり, 銀行口座, 本人確認の必要はなく, 現金を保持している人は誰でも利用できる. 購入の手順は現金を投入, Bitcoin を受信する Bitcoin Address を提示, 提示した Bitcoin Address に対して Bitcoin ATM Address から現金が送られて完了する. Bitcoin ATM を提供している企業の合計数は 53 企業, その中には General Bytes, Bitcoin Depot, Delloite といった企業が存在する. 初めて設置されたのは, 2013 年 10 月 29 日, 都市はカナダのバンクバーである. ATM は 2019 年 11 月時点で週に 9.3 台のペースで設置されており, 設置台数は累計で 6,000 台を超えた. 設置箇所はアメリカに 3,924 台, 次いでカナダが 653 台, イギリスに 272 台, オーストリアには 189 台あることが確認されている [7].

第 2 章

データの説明

2.1 Bitcoin Talk

Bitcoin Talk のサイトの登録者が登録している Bitcoin Address をスクレイピングにより取得した. 取引は Blockchain Explorer サービス [2] から取得した. Bitcoin Address の属性名は Bitcoin Talk として扱う.

2.2 Bitcoin ATM

カナダに設置されている Bicoin ATM3 台を直接利用して Bitcoin Address を取得した. Bitcoin ATM の Bitcoin Address は複数回利用した結果, 変更されていないことも確認した. 取得した Bitcoin Address と Bitcoin ATM の企業は表 2.1 の通りで, それぞれの名称を ATM1, ATM2, ATM3 と呼ぶ. これら 3 つの Bitcoin ATM Address から発生した取引を Blockchain Explorer サービス [2] から取得した. 取引は Bitcoin ATM への入金目的の取引, Bitcoin ATM 利用者の取引, Bitcoin ATM を標的とした Dusting Attack の 3 種類に分類できる. この 3 つは取引中の Input Bitcoin Address, Output Bitcoin Address の数や Bitcoin Address によって区分される. 3 種類の取引から Bitcoin ATM 利用者の取引のみを抽出した. Bitcoin ATM 利用者の取引の形を表 2.2 に示す. 区分したそれぞれの取引数を表 2.3 に示す. また, ATM2 では約 1 年間, ATM3 では約半年間にわたって Bitcoin Address が利用されていない期間が確認された. そのため, 取引のなかった前後の期間ごとにデータを分割して別々に分析を行った. 分割した期間に対してはそれぞれ期間の番号を割り当てた. 分割した期間と期間の番号を表 2.4 に示す.

2.3 Bitcoin ATM 利用者

Bitcoin ATM から表 2.2 で定める Bitcoin Address を Bitcoin ATM 利用者 Address と定める. さらに Bitcoin ATM Address ごとに取引を全て取得し Bitcoin ATM 利用者取引として扱う. Bitcoin ATM 利用者 Address の属性名はそれぞれ ATM1, ATM2, ATM3 とする.

2.4 Bitcoin 価格

Bitcoin の価格は常に変化しており, 同じ 1BTC でも 1 週間で日本円にして 50 万円の変動も過去に存在した. このような状況で Bitcoin 量同士を比較することに意味はないため, カナダドルに変換して購入量を比較する.

図 2.1　Bitcoin ATM の機械

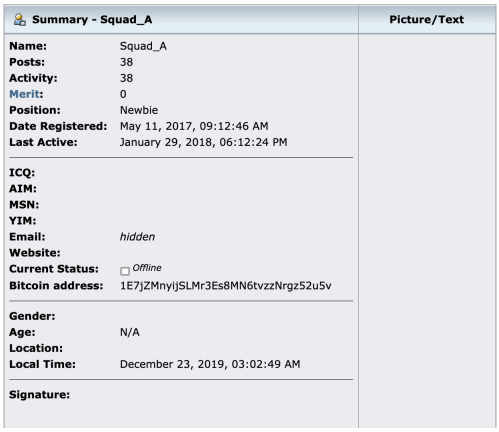

図 2.2　Bitcoin Talk のプロフィールページ

表 2.1　Bitcoin ATM データ概要

Bitcoin ATM 企業	ATM 名	Address
General Bytes	ATM1	35pJQef1CGscLec9jyddMu2DLU5Swq12wK
	ATM2	39XfbZ24X4MFYkLaeSeqGCn1M9YTz68kes
Delloite	ATM3	3ABE4BZkwv2ubYYGhUtNxL57gMwenUEuNW

表 2.2　Bitcoin ATM 利用者 Transaction の定義

Input	Output
Bitcoin ATM Address	Bitcoin ATM Address Bitcoin ATM 利用者 Address

表 2.3　Bitcoin ATM Transaction 数

ATM 名	期間番号	Bitcoin ATM Tx 数	Bitcoin ATM 利用者のみを含む Tx 数
ATM1	1	785	733
ATM2	1	1376	226
ATM2	2	212	99
ATM3	1	92	86
ATM3	2	37843	37150

表 2.4　属性別 Address の利用期間

属性名	期間番号	開始日	終了日	日数 [day]
Bitcoin Talk	1	2010-08-03	2019-10-28	3372
ATM1	1	2019-01-24	2019-11-03	284
ATM2	1	2016-12-14	2017-12-18	370
	2	2018-11-19	2019-10-31	347
ATM3	1	2019-01-09	2019-01-17	9
	2	2019-08-06	2019-11-04	91

第 3 章

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実験

3.1 概要

本実験では, アドレスデータセットと取引データセットを使用し, 提案手法である平均取引時間分布を Bitcoin ユーザの 25% から作成, 残りの Bitcoin ユーザの取引時間分布との相関係数を用い Bitcoin ユーザのタイムゾーン推定の精度を明らかにする. 本手順のシステム構成図を図 4.1 に示す.

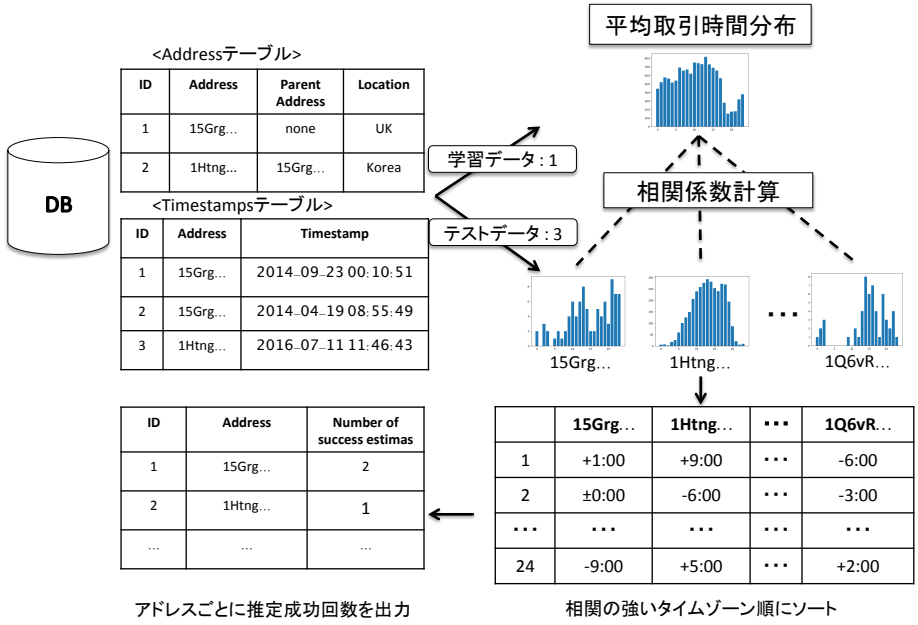

図 3.1 システム構成図

3.2 方法

3.2.1 アドレスデータセットの取得

Bitcoin のオンラインフォーラムである Bitcointalk[3] のプロフィールページにて公開されている address と Location データをスクレイピングにて取得し, address テーブルに表 3.1 に格納する. トランザクション内の同一 Input に格納されているアドレスは同一ユーザのものであると仮定し, 同一ユーザのアドレスを補完する. Bitcoin の取引所 BLOCKCHAIN[**?**] の取引データから, 同一 Input の収集元アドレスを Parent address と呼び, address テーブルに追加する. これらをアドレスデータセットとする.

3.2.2 取引データセットの取得

BLOCKCHAIN 取引データから取得する. アドレスデータセットの address が Input に入っている transaction 時刻の値を取得し, 表 3.2 の Timestamps テーブルに格納する.

3.2.3 タイムゾーンデータセットの取得

全タイムゾーンのデータを timeanddate[**?**] から取得し, time zone テーブルに格納する.

3.2.4 平均取引時間分布データの作成

平均取引時間分布データは, アドレスデータセットの 25% を一様分布でランダム抽出しこれらを学習用データとする. この学習用データを含む Address の取引データを取引データセットから抽出する. 出力された各 Address の取引データの Timestamp を UTC にし, 全ての Timestamp データをまとめ一つの平均取引時間分布データ f_* とする.

3.2.5 各アドレスの取引時間分布と相関の出力

3.2.4 節にて作成した学習用データ以外の 75% のデータをテスト用データとして使用する. テスト用データの未知の Address を i, 取引時間分布 f_i とする. 平均取引時間分布 24 個分ずらし 24 個の平均取引時間分布との相関係数 $c(fi, f_*), c(fi, f_* + 1), \ldots, c(fi, f_* + 24)$ を求め, 最大化するタイムゾー i_* をユーザ i のタイムゾーンと推定する. すなわち,

$$\begin{aligned} \mathrm{j}_* &= argmaxc(f_i, f_* + j) \\ j &\in \{0, \cdots, 24\} \end{aligned}$$

とする. i の正しいタイムゾーン i_* と推定 j_* との差が閾値 θ[時] 以内を推定成功とする. これをユーザごとに求める.

3.2.6 推定成功率の出力

本実験では, 3.2.4, 3.2.5 節の手順を 1000 回実施し, 推定成功回数の平均を求める.

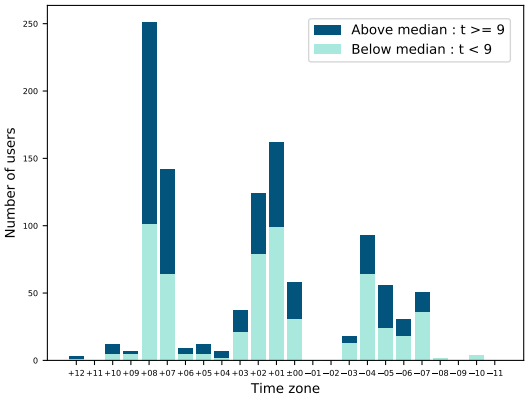

図 3.2　タイムゾーンごとのユーザ数

表 3.1　Address テーブルの例

Address	Parent Address	Location
1CasperDEhyGD81WNPo9qkaFnWxUSWmrqk	none	Hong Kong
1FdxQxtzkRRcCApy7AFGroUgjesyLKRENK	1CasperDEhyGD81WNPo9qkaFnWxUSWmrqk	Hong Kong

表 3.2　Timestamps テーブルの例

Address	Timestamp
1CasperDEhyGD81WNPo9qkaFnWxUSWmrqk	2012-02-18 00:57:33
1CasperDEhyGD81WNPo9qkaFnWxUSWmrqk	2012-02-18 04:24:46
1FdxQxtzkRRcCApy7AFGroUgjesyLKRENK	2012-06-23 23:45:23

表 3.3　データセット概要

期間	2009-1-3 2018-9-23 (9.5 年)
アドレス数	1,233
ユーザ数	1,086
タイムスタンプ数	327,310

3.3　結果

3.3.1　データの観察

取得したデータセットの概要を表 3.3, タイムゾーンごとのユーザ数を図 3.2 に示す. ここで, 全ユーザの取引回数の中央値である 9 回を基準にし, 取引回数に応じてユーザを 2 色に分けた.

3.3.2　推定成功回数

ユーザごとの取引回数に対し, j_* と i_* との差分を d_i と定める. 結果を図 3.3 に示す.

3.3.3　結果と推定成功率の評価

取得したデータセットの概要を表 3.3, タイムゾーンごとのユーザ数の分布を図 3.2 に示す. ここで, 全ユーザの取引回数の中央値である 9 回を基準にし, 取引回数に応じてユーザを 2 色に分けている. 推定成功回数閾値 θ 回以上の推定成功回数のユーザ数の割合を推定成功率

$$s_\theta = \frac{|\{i \in \mathbb{U} \mid t_i \geq m, |\ j_* - i_*\ | \leq \theta\}|}{|\{i \in \mathbb{U} \mid t_i \geq m\}|}$$

と定める. ここで,　取引回数が閾値 m 回以上のユーザのみを評価対象とする. 推定成功率 $m = 1$ 回の条件における推定成功率 s_1 は 9% であった. しかし, Dupont らと同じ条件である $m = 6$ 回以上の取引回数, かつ $\theta = 11$ 回の推定成功の条件においては 77% となった. 結果を図 3.4 に示す.

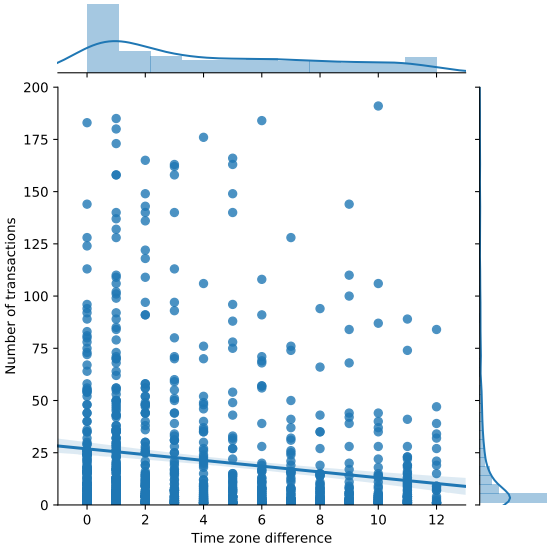

図 3.3　推定成功回数の取引回数についての散布図

3.4　考察

本実験では, 推定成功率は 77% で Dupont らの手法よりも推定成功率が高い. このことから, 多くの取引を行う場合は複数のアドレスを並行して使用し, またその場合は同一ユーザのものとされないために同一 Input に入るような使用はしないようにする必要があると考える.

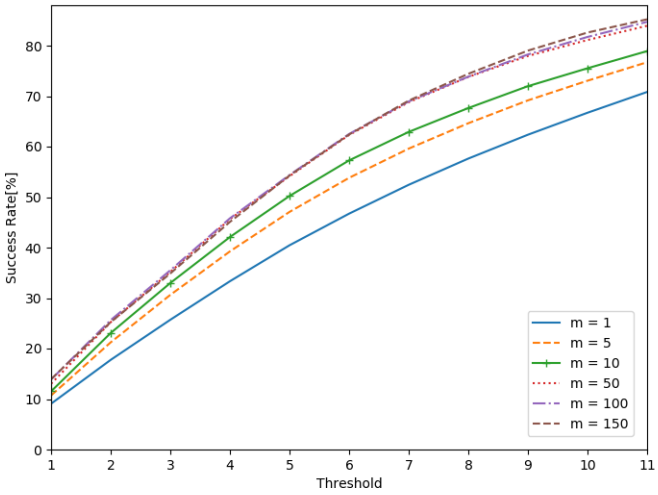

図 3.4　推定成功率

第 4 章

カナダにおける Bitcoin ATM の利用者調査実験

4.1 調査目的

本調査の目的は次の 3 つである.

(1) Bitcoin ATM の利用の特徴を調査する.

(2) Bitcoin ATM 利用者の特徴を明らかにする.

(3) Bitcoin ATM 利用者と Bitcoin Talk 利用者の取引の統計的な違いを明らかにする.

本調査の概要を図 4.1 に示す.

4.2 データの収集

(1)Bitcoin Talk のプロフィールページから Bitcoin Address の項目のみを抽出する.

(2)Bitcoin Talk 利用者 Address の取引を Blockchain Explorer から取得する.

(3) カナダに設置されている Bitcoin ATM に少額の預金を行い, 当著者の Bitcoin Address に送信している Bitcoin Address を Bitcoin ATM Address として Blockchain Explorer から取得する.

(4)Bitcoin ATM Address の全取引を Blockchain Explorer から取得する. 取得した取引の中から Bitcoin ATM 利用者取引として表 2.2 の定義に沿った取引のみを抽出し Bitcoin ATM 取引とする. 取得した Bitcoin 量は Bitcoin 価格のサイト [10] から取得した Bitcoin のカナダドル価格一覧を利用してカナダドルに変換した.

(5)Bitcoin ATM 取引から Bitcoin ATM Address 以外の Bitcoin Address を抽出して Bitcoin ATM 利用者 Address として扱う. Bitcoin ATM 利用者として収集した Bitcoin Address 数を表 4.2 に示す.

(6)Bitcoin ATM 利用者 Address 取引を Blockchain Explorer から取得する.

4.3 データの分析

4.3.1 Bitcoin ATM 利用の特徴

Bitcoin Explorer の wallet 利用者は増えていることを 1.1 節にて触れた. そのため, Bitcoin ATM 利用者も日々増加していることが想定される Bitcoin ATM 利用に関して明らかにすることを目的に利用回数と利用金額に関して統計情報を計算した. さらに Bitcoin 価格との関係を捉えるため Bitcoin 価格データと重ねて時系列

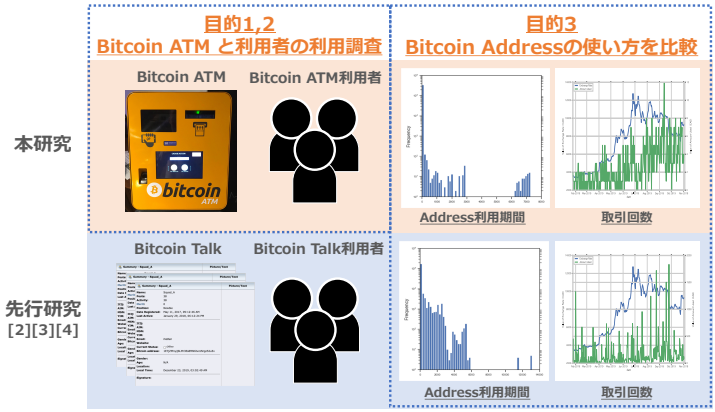

図 4.1　システム構成図

表 4.1　取得した Address 数

属性名	期間番号	合計
ATM1	1	552
ATM2	1	218
ATM2	2	79
ATM3	1	81
ATM3	2	22605
Bitcoin Talk	1	1897

表 4.2　Bitcoin ATM 利用者 Address 数

ATM 名	期間番号	Address 数 (ユニーク)		
		合計	2 回以上利用	1 回利用
ATM1	1	552	56	496
ATM2	1	218	3	215
	2	79	8	71
ATM3	1	81	4	77
	2	22605	3533	19072

データとして可視化を行なった.

4.3.2　Bitcoin ATM 利用者の特徴

Bitcoin ATM 利用者 Address の利用期間, 利用日の統計量を計算しそれぞれ可視化した. 取引の数, 取引中の Input Bitcoin Address 数, Output Bitcoin Address 数も同様に行った.

4.3.3　Bitcoin ATM 利用者と Bitcoin Talk 利用者の統計量の比較

Bitcoin Address の使い方の違いを明らかにするため Bitcoin Talk 利用者も Bitcoin ATM 利用者と同じ値の算出を行い, Bitcoin ATM 利用者の結果と比較を行った.

4.4 実験結果

4.4.1 Bitcoin ATM 間の比較

Bitcoin ATM 取引を利用して 1 日当たりの利用回数, 総利用金額を利用回数で割った利用平均金額を表 4.3, 表 4.4 に示す. さらに単位時間ごとの利用頻度のデータを加え, 時系列にて図 4.2, 図 4.3, 図 4.4, 図**??** 図 4.5, 図 4.6 で示す. Bitcoin ATM 利用者 Address は同じ Bitcoin Address の利用よりも 1 度しか利用されていない Bitcoin Address の方が多いことが表 4.2 からわかる. 取得した 3 つの Bitcoin ATM Address の内, 表 4.3 より Delloite の ATM3 は利用期間が 3 台の間でもっとも短いにも関わらず 1 日あたりの利用回数の中央値, 平均が他のものに比べて期間 1, 2 ともに飛び抜けて多い. General Bytes の ATM1, ATM2 では 1 日あたりの利用回数に関しては似通った値になっている. 1 日当たりの利用金額に関しては ATM2 のみ中央値, 平均において ATM1, ATM3 と比較して桁が一つ小さくなっていることが表 4.4 から分かる.

表 4.3　Bitcoin ATM 1 日あたりの利用回数に関する統計量

ATM 名	期間番号	1 日あたりの利用回数				
		mean	min	med	max	std
ATM1	1	2.58	0	2	10	2.22
ATM2	1	0.61	0	0	6	1.07
	2	0.29	0	0	4	0.62
ATM3	1	30.44	0	0	139	48.08
	2	412.36	137	415	601	82.50

表 4.4　Bitcoin ATM 利用金額に関する統計量

ATM 名	期間番号	1 日あたりの利用平均金額 [CAD]				
		mean	min	med	max	std
ATM1	1	165.03	0	71.18	1932.26	272.79
ATM2	1	8.12	0	0	151.92	18.04
	2	11.28	0	0	170.42	26.40
ATM3	1	162.55	0	0	440.82	197.34
	2	348.87	117.98	365.17	548.60	113.40

表 4.5　属性別 Transaction 数に関する統計量

属性名	期間番号	Address 別 Transaction 数				
		mean	min	med	max	std
Bitcoin Talk	1	101.53	1	22	6081	317.36
ATM1	1	14.93	1	2	498	48.89
ATM2	1	8.67	1	2	1028	71.43
	2	12.37	1	2	212	35.45
ATM3	1	37.20	2	2	960	116.08
	2	14.44	1	2	45092	327.96

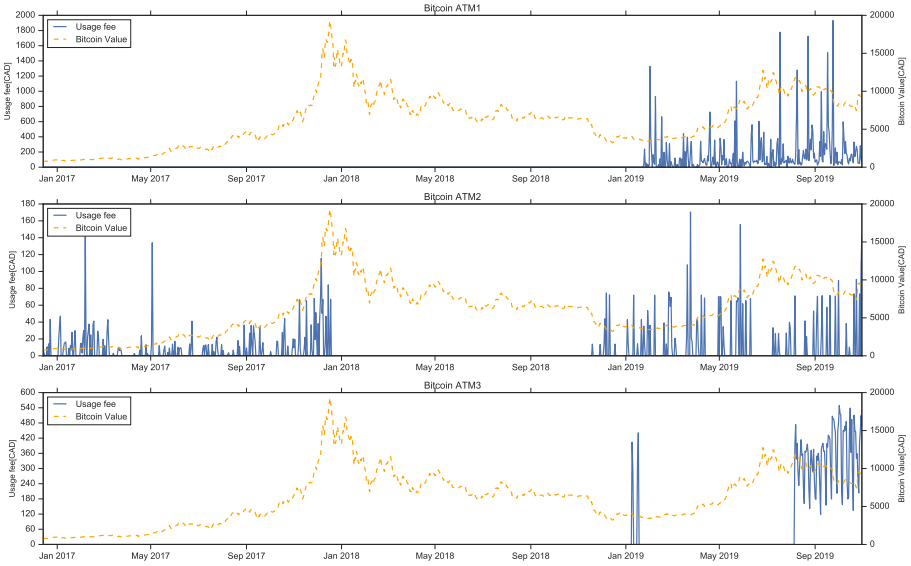

図 4.2　Bitcoin ATM 1 日あたりの平均利用金額と 1BTC あたりのカナダドル価格

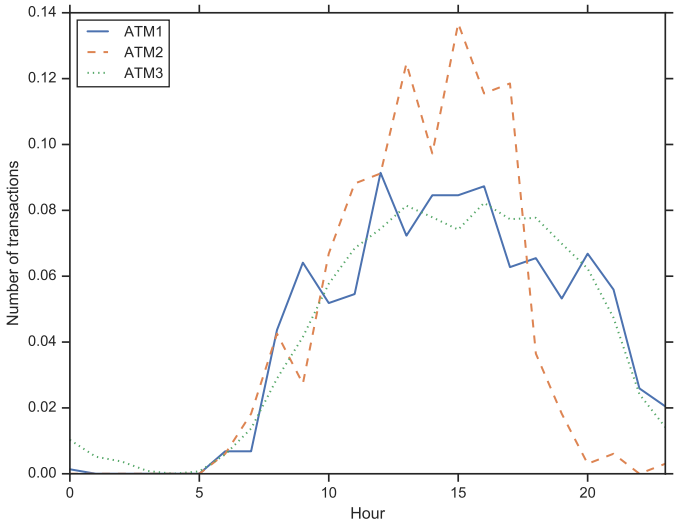

図 4.3　Bitcoin ATM 1 時間毎の利用頻度

4.4.2　Bitcoin 価格変動と Bitcoin ATM 取引回数

Bitcoin の価格の前日との差額と 1 日ごとの Bitcoin ATM 取引回数の相関係数の結果を Bitcoin ATM ごとに計算した結果を表 4.8, 散布図と線形回帰線を図 4.12 に示す. ATM3 台とも, Bitcoin 価格の変動と取引回数に相関関係がないことがわかる.

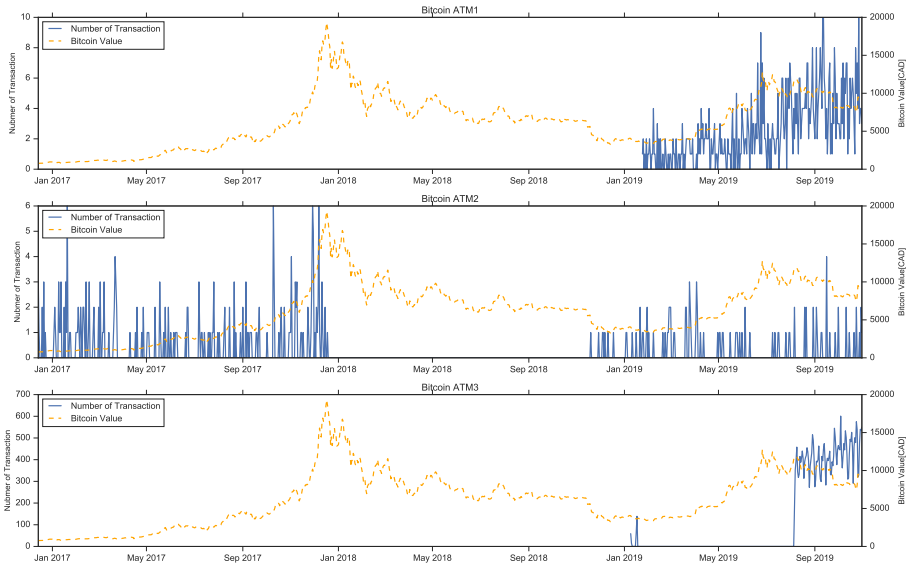

図 4.4　Bitcoin ATM 1 日あたりの利用回数と 1BTC あたりのカナダドル価格

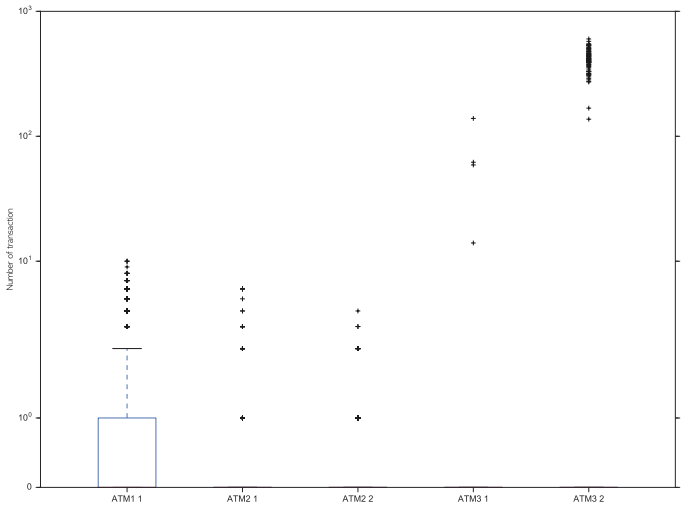

図 4.5　Bitcoin ATM 利用回数

4.4.3　属性間の取引数統計量の比較

Bitcoin Address ごとの取引数に関して表 4.5, 図 4.7 に示す. Bitcoin Talk 利用者 Address ごとの取引数は平均, 中央値において 3 台すべての ATM よりも桁が一つ大きいことがわかる.

4.4.4　属性間 Bitcoin Address 利用期間, 利用間隔に関する統計量の比較

Bitcoin Address ごとに確認できた一番はじめの取引と最後の取引の日数からその間の日数を抽出し表 4.6, 図 4.9 にまとめた. さらに, 全取引の間の時間を取引利用間隔として表 4.7, 図 4.11 に示す. これらから Bitcoin

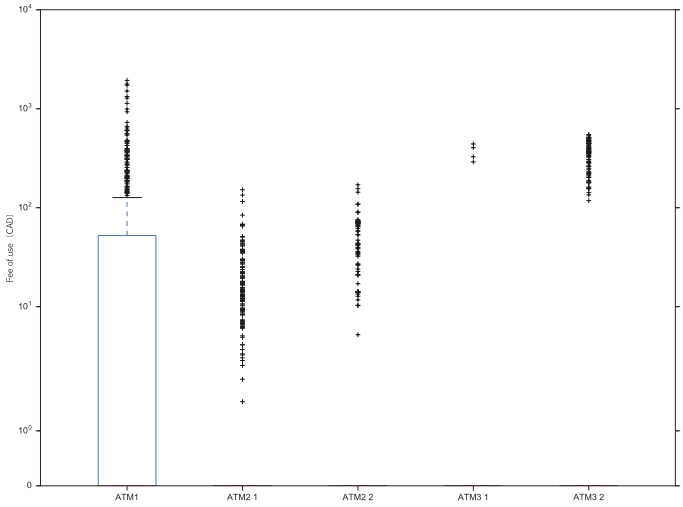

図 4.6　Bitcoin ATM 利用金額

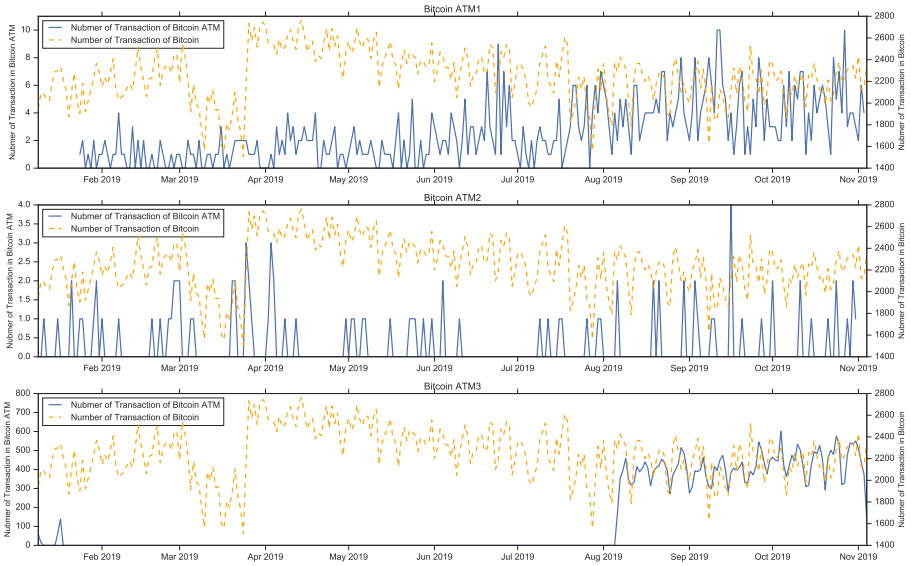

図 4.7　Bitcoin ATM 取引数と Bitcoin 総取引数

Talk 利用者 Address 利用期間は約半年以上利用されている Bitcoin Address が多い, しかし, Bitcoin ATM の利用期間は約 1 日以下のものが大半であることが表 4.6 からわかる. Bitcoin Address を利用している間隔に関しては Bitcoin Talk 利用者も Bitcoin ATM 利用者も遜色がないことが表 4.7 からわかる.

4.4.5　属性間の取引の Input Address, Output Address 数に関する統計量の比較

Bitcoin Address 取引ごとの Input Address 数に関する統計量を表 4.9, 図 4.13 に, Output 数に関しては表 4.10, 図 4.15 に示す. Input Address 数, Output Address 数両方の統計値に関して Bitcoin Talk 利用者と Bitcoin ATM 利用者の間に大きな差は見られない. Bitcoin Talk 利用者の Output Address 数平均に関しては桁が一つ大きくなっているが, 最大の Output Address 数も桁が一つ大きくなっており, さらに標準偏差の値も大きく, いく

表 4.6　属性別 Address 利用日数に関する統計量

属性名	期間番号	Address 別 利用日数 [day]				
		mean	min	med	max	std
Bitcoin Talk	1	398.74	0	183.16	2846.91	496.09
ATM1	1	41.92	0	0.14	1730.89	152.82
ATM2	1	69.63	0	1.16	1605.97	178.88
	2	57.95	0	0.12	1152.39	163.94
ATM3	1	107.07	0	0.93	1106.23	213.56
	2	26.95	0	0.12	2278.20	120.26

表 4.7　属性別 Address 利用間隔に関する統計量

属性名	期間番号	利用間隔 [hour]				
		mean	min	med	max	std
Bitcoin Talk	1	96.31	0	3.30	56864.19	809.95
ATM1	1	72.21	0	11.31	31578.79	553.97
ATM2	1	217.60	0	1.00	17346.31	1141.32
	2	122.21	0	14.99	10021.4	529.77
ATM3	1	71.03	0	11.12	6811.04	306.98
	2	48.12	0	4.32	31594.49	318.06

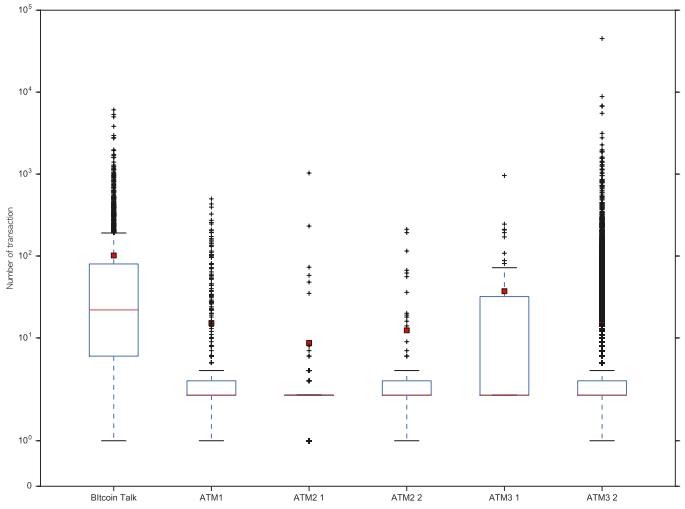

図 4.8　属性別 Transaction 数 ボックスプロット

表 4.8　Bitcoin ATM 取引回数と金額の相関係数

ATM1	ATM2	ATM3
0.019152	0.215929	0.191784

つかの大きい値に平均が釣られて大きくなっていることがわかる.

4.5　考察

Bitcoin ATM3 取引数が Bitcoin 全体の取引数と同じ挙動をしていることから, Bitcoin ATM 利用者の取引数が Bitcoin 全体の取引数を支配している可能性が考えられる. このようになる理由は, 一般的な支払いに

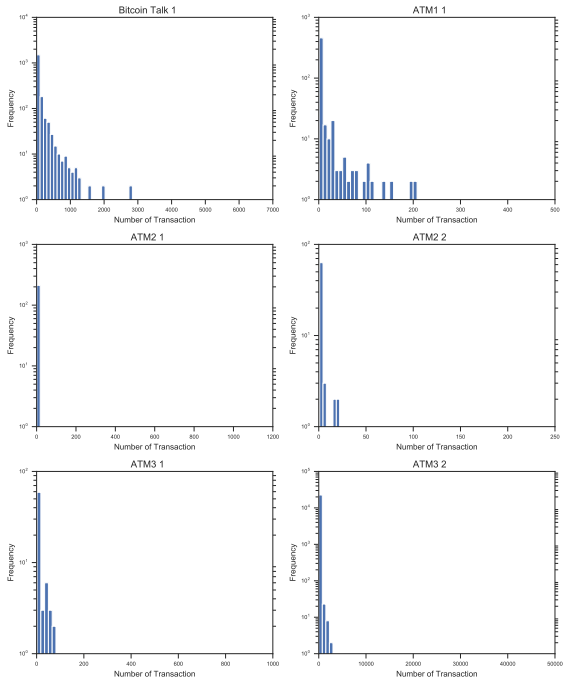

図 4.9　属性別 Transaction 数 ヒストグラム

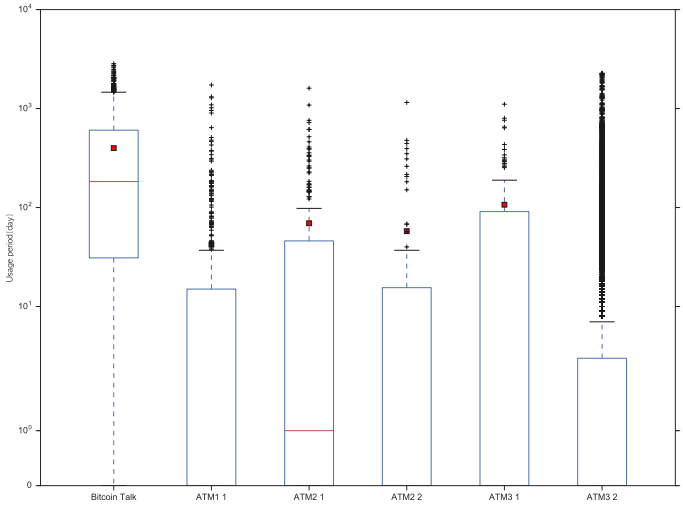

図 4.10　属性別 Address 利用期間 ボックスプロット

Bitcoin が浸透していないことが原因だと考えられる. このため, Bitcoin ATM や取引所と一般人所有の Bitcoin Address 間での受送金が取引の大半を占めるようになっているのではないかと考えられる.

Bitcoin ATM 利用者の特徴として, 半数程度の Address が 2 回程度の取引しか発生させず, 1 日以内に他の Address に Bitcoin を送信している. これらのことから Bitcoin ATM 利用者は Address を使い捨てる特徴があることが言える. この特徴から匿名性を考慮した利用者が多いことが考えらえる.

それに対して Bitcoin Talk 利用者の Bitcoin Address は中央値が 22, 平均で 101 回ほどの取引であり, Bitcoin Address 利用期間の中央値は約半年, 平均が約 1 年である. このことから Bitcoin Talk 利用者は 1 つの Address

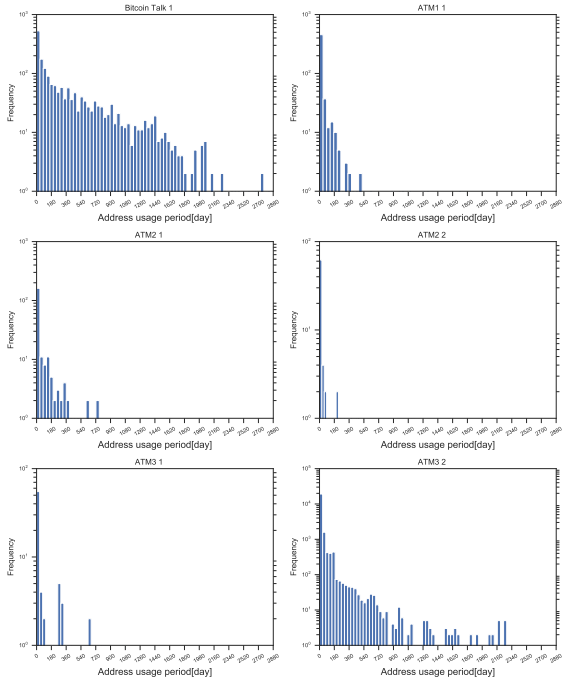

図 4.11　属性別 Address 利用期間 ヒストグラム

表 4.9　属性別 Transaction 内の Input 数に関する統計量

属性名	期間番号	Input 数				
		mean	min	med	max	std
Bitcoin Talk	1	16.74	0	1	4507	69.85
ATM1	1	44.85	1	1	888	114.80
ATM2	1	5.55	1	1	593	24.88
	2	42.36	1	1	1000	121.00
ATM3	1	13.25	1	1	639	49.29
	2	46.18	1	1	1098	127.01

を長く, 複数回にわたって利用しており, 匿名性を気にした使い方はされていない. 取引数と Bitcoin Address 利用期間の違いにより送金先合計数には明らかな違いが生じることから, Bitcoin ATM 利用者は Bitcoin Talk 利用者よりも匿名性の意識が高いことが考えられる.

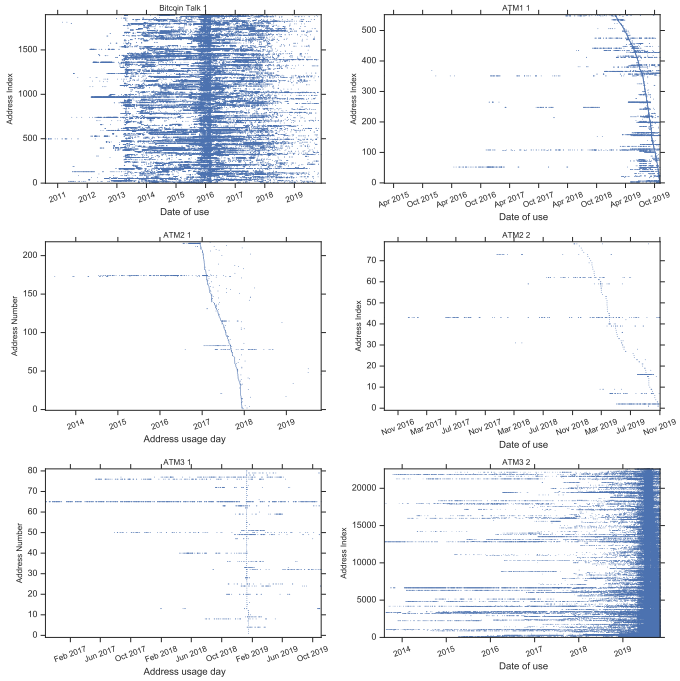

図 4.12　属性別 Address 利用間隔

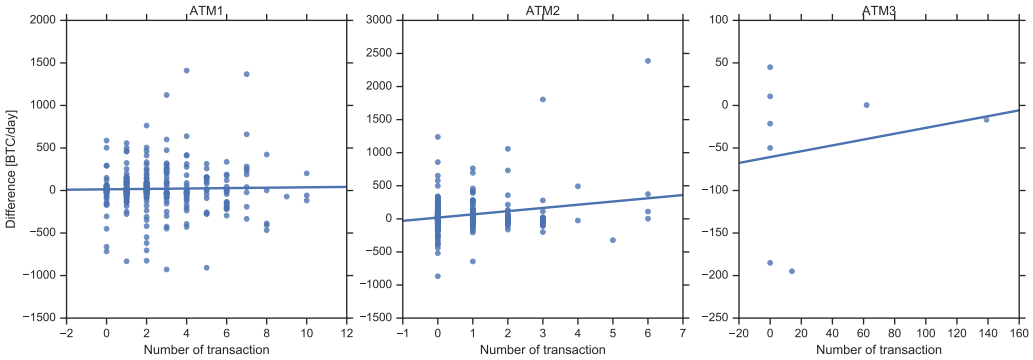

図 4.13　Bitcoin ATM の利用回数と Bitcoin 価格変動の関係

表 4.10　属性別 Transaction 内の Output 数に関する統計量

属性名	期間番号	Output 数				
		mean	min	med	max	std
Bitcoin Talk	1	149.60	0	2	13107	509.58
ATM1	1	7.56	1	2	2901	60.76
ATM2	1	3.05	1	2	200	7.24
	2	5.09	1	2	100	9.50
ATM3	1	13.67	1	2	2901	141.06
	2	6.94	1	2	7266	109.89

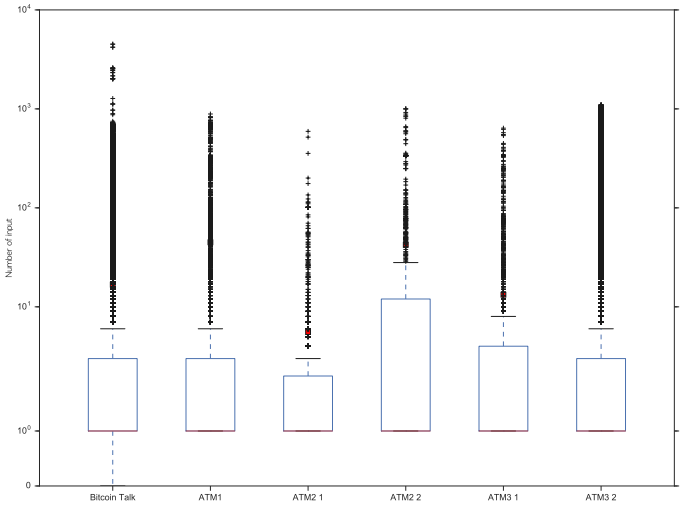

図 4.14　属性別 Transaction 内の Input 数 ボックスプロット

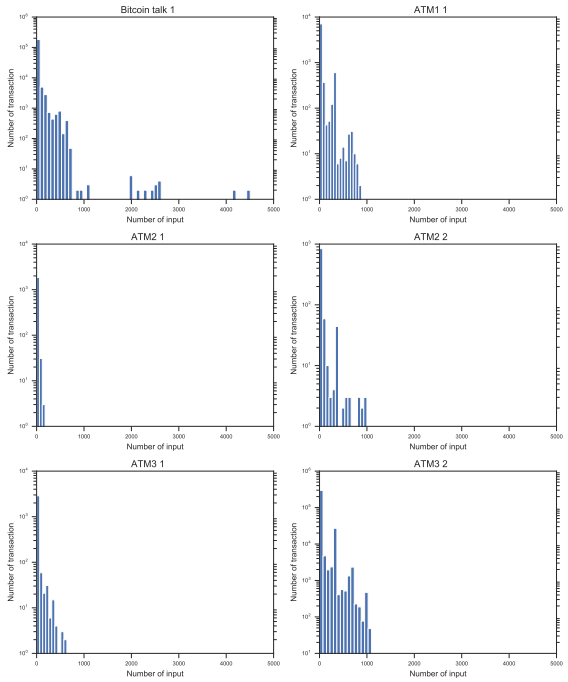

図 4.15　属性別 Transaction 内の Input 数 ヒストグラム

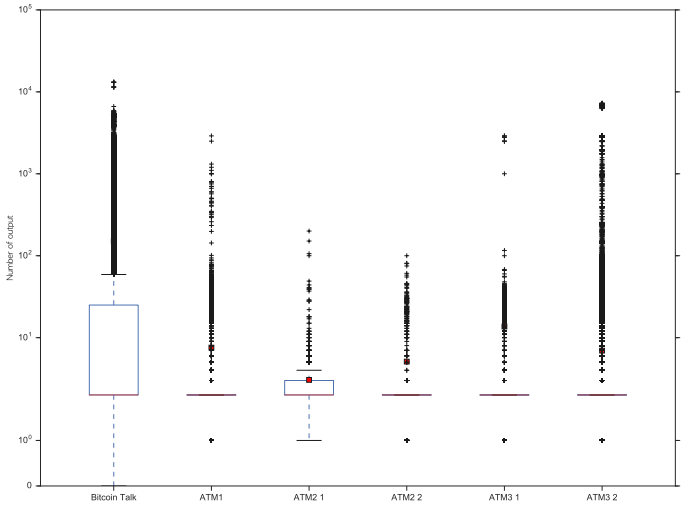

図 4.16　属性別 Transaction 内の Output 数 ボックスプロット

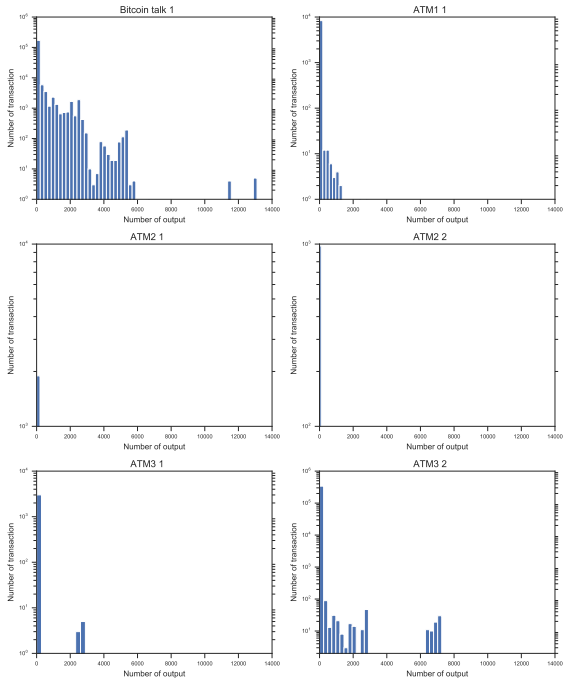

図 4.17　属性別 Transaction 内の Output 数 ヒストグラム

第 5 章

おわりに

本実験では Bitcoin アドレスの平均取引分布に基づくタイムゾーンの推定を行った. その結果, 相関を用いた推定成功率は Dupont らの手法を上回る結果であることを確認した. さらに, Bitcoin ATM 取引の特徴と Bitcoin ATM 利用者 Address と Bitcoin Talk 利用者 Address の特徴を比較して, 利用方法の違いを明らかにした.

今後の課題として, 実際に Bitcoin ATM 利用者に対して匿名性の評価実験, もしくは属性推定の実験を行い, Bitcoin Talk 利用者の結果との違いを明らかにすることを挙げる.

謝辞

本研究を行うにあたり，多くの方より御指導いただきました．特に，多大なる御指導を受け賜りました，明治大学総合数理学部先端メディアサイエンス学科，菊池浩明教授に深く感謝申し上げます．予備実験等に協力してくださった松本さん, 山崎さん, 草野さん, 皆様並びに菊池研究室の方々に深く感謝の意を表するとともに，謝辞とさせていただきます．

参考文献

[1] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Elecctronic Cash System”, 2008.

[2] Blockchain, (https://www.blockchain.com, 2019 年 11 月参照)

[3] Bitcointalk. (https://bitcointalk.org/, 2018 年 12 月参照)

[4] 永田倖大, 菊池浩明, ”Anonymity evaluation of Bitcoin addresses based on a set of output addresses”, 2018.

[5] J. Dupont, A. C. Squicciarini, ”Toward De-Anonymizing Bitcoin by Mapping Users Location”, In Proceedings of Conference on Data and Application Security and Privacy(CODASPY’15), pp.139-141, ACM, 2015.

[6] 井垣秀星, 永田倖大, 菊池浩明, ”Time zone estimation of Bitcoin user based on correlation of distribu- tions of transaction time”, 2019.

[7] COINTELEGRAPH, (https://jp.cointelegraph.com, 2019 年 12 月参照)

[8] coindesk,(https://www.coindesk.com/25-year-old-to-plead-guilty-to-running-unlicensed-crypto-exchange, 2019 年 12 月参照)

[9] www.coindeskjapan.com,(https://www.coindeskjapan.com/28190/, 2019 年 12 月参照)

[10] Bitcoin 価格, (https://min-api.cryptocompare.com, 2019 年 11 月参照)