カナダにおける Bitcoin ATM の利用者調査

井垣秀星 †　　松本寛輝 ‡　　菊池浩明 †

明治大学総合数理学部 †　明治大学院総合先端数理科学研究科 ‡

1　はじめに

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 [2]. 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 [3]. 我々はタイムゾーン属性推定研究を平均取引時間分布を用いて行い, 77% の結果を示した [4]. これらすべての研究において Bitcoin Talk†サイトに登録している利用者の Bitcoin Address を全 Bitcoin Address の標本データとして利用している.

しかし, 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. 本研究では Bitcoin ATM 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.

2　データの分析

2.1　調査目的

本研究では以下の 2 つを目的とする.

(1) Bitcoin ATM の利用の特徴を調査する.

(2) 属性ごとの Bitcoin Address の使い方を明らかにする.

本調査の概要を図 1 に示す.

2.2　方法

2.2.1　Bitcoin Talk データの収集

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. 取引は Blockchain Explorer から取得する.

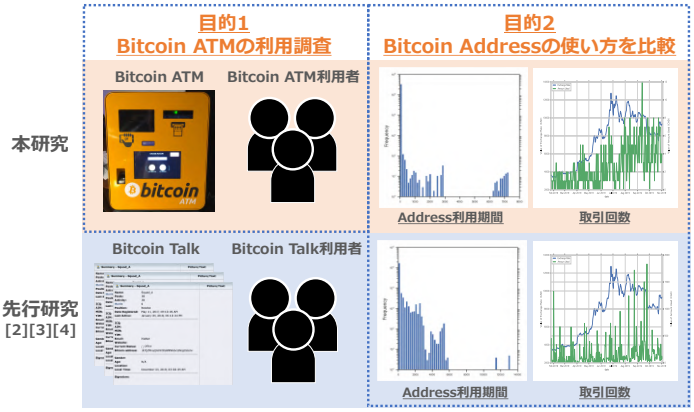

図 1　概要図

表 1　Bitcoin ATM 利用者取引の定義

Input	Output
同じ Bitcoin ATM Address が 1 つ以上	同じ Bitcoin ATM Address が 1 つ以上 Bitcoin ATM 利用者 Address が 1 つ

表 2　属性別 Bitcoin Address の利用期間と Address 数

属性名	期間番号	開始日	終了日	日数 [day]	アドレス数
Bitcoin Talk	1	2010-08-03	2019-10-28	3372	1897
ATM1	1	2019-01-24	2019-11-03	284	552
ATM2	1	2016-12-14	2017-12-18	370	218
	2	2018-11-19	2019-10-31	347	79
ATM3	1	2019-01-09	2019-01-17	9	81
	2	2019-08-06	2019-11-04	91	22605

2.2.2　Bitcoin ATM 利用者データの収集

カナダに設置されている Bitcoin ATM3 台を現地にて実際に預貯金をして利用した. Bitcoin Address に送信している取引から送信元の Bitcoin ATM Address を取得する. Bitcoin ATM Address の取引は Blockchain Explorer から取得する. 取得した取引には,

(1)Bitcoin ATM に入金目的の取引

(2)Bitcoin ATM 利用者 Address の取引

(3)Dusting Attack の標的となっている取引

合計 3 種類が存在した. 本研究では表 1 の定義に沿った取引のみ (2) を抽出し, Bitcoin ATM 利用者 Address の取引として扱う. 取引から Bitcoin ATM 以外の Bitcoin ATM 利用者 Address を抽出する. Bitcoin ATM Address は ATM2, ATM3 に関して利用されていない期間が存在した. そのため表 2 の期間ごとに分けて分析を行う.

2.3　実験結果

2.3.1　Bitcoin ATM 取引に関する調査

Bitcoin ATM の取引数と Bitcoin 全体の 1 日あたりの総取引数を図 2 に示す. ここで, Bitcoin ATM3 の 2019 年 8 月以降の総取引数の増減が Bitcoin 全体の取引数とほぼ同じ挙動をしていることに注意せよ.

Study on Bitcoin ATM users in Canada

†Shusei Igaki, Hiroki Kikuchi, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

‡Hiroki Matsumoto, Graduate School of Advanced Mathematical Sciences, Meiji University

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

†https://bitcointalk.org/

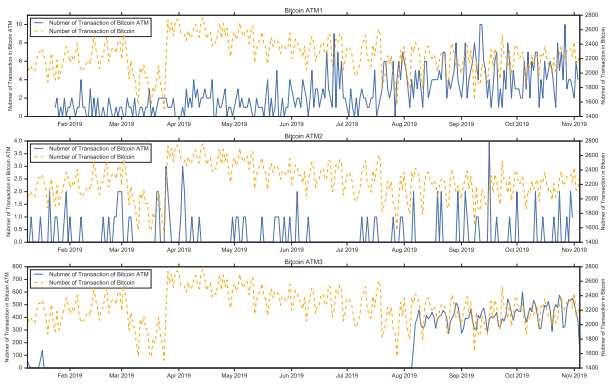

図 2　Bitcoin ATM 取引数と Bitcoin 総取引数

表 3　属性別 取引数の統計量

属性名	期間番号	Bitcoin Address 別 取引数				
		mean	min	median	max	stdev
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

表 4　属性別 Bitcoin Address 利用日数の統計量

属性名	期間番号	Bitcoin Address 別 利用日数 [day]				
		mean	min	median	max	stdev
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

2.3.2　取引数統計量

Bitcoin Address ごとの取引数に関する統計量を表 3 に示す. Bitcoin Talk 利用者ごとの取引数は平均, 中央値において, 3 台すべての ATM を大きく上回っている.

2.3.3　利用期間と頻度

Bitcoin Address ごとに識別した最初の取引と最後の取引の日数から Bitcoin Address の利用期間を定め, 表 4 にまとめた. さらに Bitcoin Address ごとの取引日の分布を図 3 に示す. Bitcoin Talk においては, 約半年以上の Bitcoin Address 利用期間が多いのに対して, Bitcoin ATM の利用期間は約 1 日以下で数回のみ取引しているのものが大半である.

2.4　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 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.

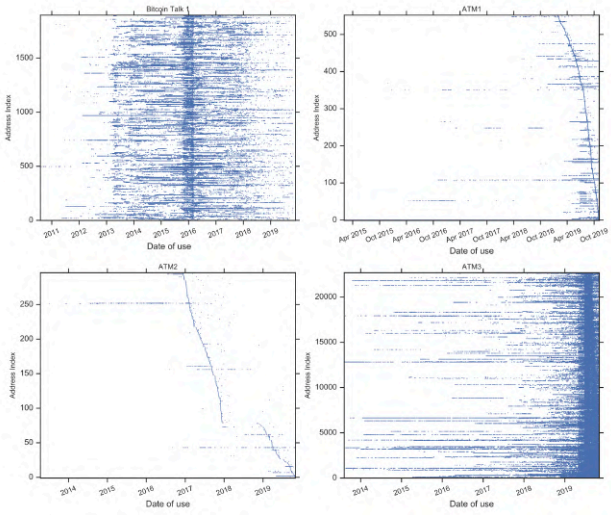

図 3　属性別 Bitcoin Address 取引日

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れる.

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 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.

3　おわりに

本稿では 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.

参考文献

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

[2] 永田倖大, 菊池浩明, “Bitcoin アドレスの送金先集合に基づく匿名性の評価”, 第 80 回コンピュータセキュリティ研究発表会 (CSEC-80), 2018 年.

[3] 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.

[4] 井垣秀星, 永田倖大, 菊池浩明, “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”, 情報処理学会第 81 回全国大会, pp.3_481-3_482, 2019.