取引件数の時間分布の相関を用いた Bitcoin 取引所のユーザのタイムゾーン推定

山崎孝順 †　草野 蘭之介 †　井垣秀星 †　松本寛輝 ‡　菊池浩明 †

明治大学総合数理学部 †　明治大学大学院 先端数理科学研究科 ‡

1　はじめに

暗号資産 Bitcoin は，匿名性とオープンソースによる透明性が高いことが特徴である．しかし，各ユーザのトランザクション情報は公開され，共有されているので，その情報から各ユーザの属性を推定することが出来るのではないかと考える．

2015 年に Dupont らは取引時刻に着目し，取引時間分布からアドレスを管理するユーザの居住地のタイムゾーンが特定できることを示した [1]．井垣らは Bitcoin のオンラインフォーラムである Bitcointalk のユーザに対して，77% のタイムゾーンを正しく推定した [2]．

本研究では，暗号資産のユーザは，本当にその国に居住しているのだろうか？という問題を考える．そこで，各国の暗号資産の取引所に着目する．アドレスに関する取引データを Bitcoin のブロックチェーンから取得し，世界 80 か所の取引所の取引時間分布とそれらに属するアドレスの取引時間分布の相関から，ユーザの所属国を推定する．

2　暗号資産のユーザの所属国推定実験

2.1　概要

本実験の目的は，取引所のユーザ集合の属性国を推定することである．図 1 に推定の原理を示す．取引所 E に属するユーザ 3 の取引時間分布 a_3 とインターネット利用時間分布 T_1, T_2, T_3 を比較して，最も相関の大きな時刻 T_1 を推定する．その取引所全ユーザ a_1, a_2, a_3 の推定時間分布を求める．

本実験で使用したデータは以下の 3 点である．(1) 各取引所の取引データ ([3]), (2) アドレス毎の取引データ ([3]), (3) インターネット利用時間帯データ（総務省).

2.2　実験方法

各取引所の取引データは Bitcoin のオンラインフォーラムである WalletExplorer.com のトップページの Exchanges 欄に掲載されている各取引所の取引データをスクレイピングにて取得した．各取引所に属するアドレス毎の取引データは，スクレイピングにて取得した．総務省ホームページの 2014 年から 2019 年の調査結果報告書より日本におけるインターネットの利用時間帯データを取得し，6 年間の平均をとったデータの UTC を 24 時間ずらしたデータを作成した．

各取引所の取引データとインターネット利用時間のデータを比較し，それぞれのデータのピークとの誤差を求める．各取引所に属するアドレス毎の取引データの推定分布を求める．

取引所が属する国の UTC を正解と定義する．正解と取引所の推定値の比較により，差が 2 以内のものを推定できたとする．取引所の推定値と取引所に属するアドレスの推定値の差が 2 時間以内の割合を求める．

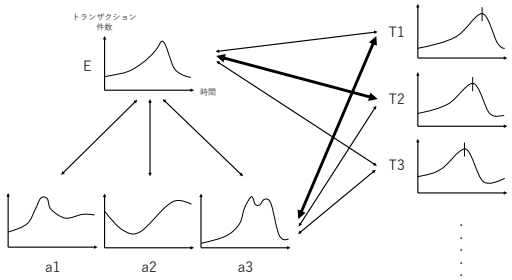

図 1　時刻推定の原理

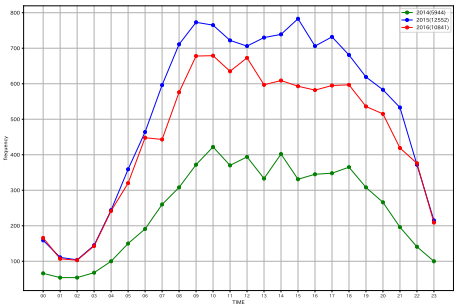

図 2　取引所データの年毎の取引数分布

2.3　実験結果

表 1 に主要な取引所の推定タイムゾーンとその取引所の取引数などの統計量を示す．

日本にある取引所 CoinCheck の取引データとの相関を表 2 に示す．インターネット利用時間は UTC+9 であるので，全年度，2016 年度，2017 年度の 3 つのデータはそれぞれ UTC+8 となる．

Time zone estimation of users of Bitcoin exchanges based on correlation of the distribution of transactions per hour

†Kojun Yamasaki, Rannosuke Kusano, Syusei 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.

表 1　タイムゾーン推定結果と取引数 (一部)

国	取引所名	UTC(正解)	UTC(推定値)	総取引数	総アドレス数
ドイツ	Coinomat	+2	+1	22510	5481
デンマーク	ExchangeMycoins	+1	+1	784	436
ポルトガル	Zyado	0	-1	1985	590
ブラジル	UseCryptos	-3	-1	11535	700
アメリカ	EmpoEx	-7	+1	2688	741
オランダ	CleverCoin	+1	+1	9647	2614
香港	AnxPro	+8	-7	326265	122166
シンガポール	CoinHako	+8	+10	136698	20588
ベトナム	BitcoinVietnam	+7	+6	6238	2276
トルコ	Exchanging.ir	+3	+2	35868	5
ケイマン諸島	BlockTrades	-5	-5	52426	27748

表 2　インターネット使用時間データと Coincheck の誤差表

比較対象	差	トランザクション件数
全年度	-1	987
2016	-1	477
2017	-1	320
2018	+4	100
2019	+6	90

表 3　推定値と正解との誤差

推定値と正解との差	取引所数
0	19
1	36
2	10
3	4
4 以上	11

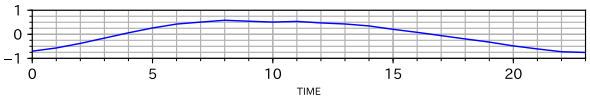

図 3　Coincheck の相関による時間分布

図 2 は，取引所 Exchanging.ir の年毎の取引数分布である．この取引所では 2015 年において取引件数が一番多く，約 1 万 3 千件行われていた．

図 3 は，取引所 Coincheck(全年度) とインターネット利用時間の相関係数の分布である．正解 T は UTC+9 であるが，推定 T^* は UTC+8 であった．

図 4 は，取引所 BX.in.th とそれに属する全アドレスの相対誤差分布を示す．誤差範囲は +12 から -11 である．取引回数が 15 回以上行われたアドレスが対象である．取引所 BX.in.th において，15 回以上取引が行われたアドレスは 6848 個存在した．

2.4　考察

取引所 BX.in.th は，推定値が正解と同じ値であった．図 4 より取引所 BX.in.th に属するアドレスは，取引所の推定値と同じ値をとるアドレスが多いことがわかる．同

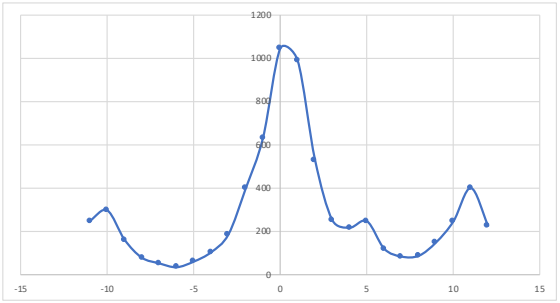

図 4　取引所 BX.in.th のアドレス分布

値 (差が 0) であるアドレスは 1044 個．差が 1 であるアドレスは 1619 個．差が 2 であるアドレスは 928 個．

3　おわりに

本研究では，推定値を求めるにあたってインターネット利用時間を使用し，取引所の利用者の所属国を推定した．推定値と正解の差が 2 の範囲内である取引所は，80 取引所中 65 取引所であった．このことから，取引所のユーザはその取引所が属する国に居住する可能性が高く，インターネット経由で Bitcoin 取引所を利用するユーザが多いと考えられる．

参考文献

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

[2] 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.

[3] WalletExplorer.com