取引履歴の解析に基づくBitcoinのサービス識別手法

慶應義塾大学 理工学部 情報工学科 豊田健太郎 / toyoda@ics.keio.ac.jp

研究目的

仮想通貨による犯罪フォレンジクスのために，与えられたBitcoinアドレスが含まれる取引履歴を**解析・処理**し，**教師あり学習によりそのBitcoinアドレスがどのような犯罪・サービスに使用されているかを識別する**手法を開発しています


取引所


マイニングプール


マーケットプレイス


ギャンブル

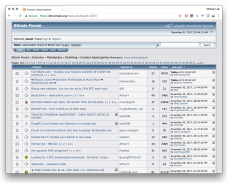

フォセット


ロンダリング


投資詐欺

提案手法 [1]

[1] K. Toyoda et al., "Multi-class Bitcoin-enabled Service Identification Based on Transaction History Summarization," in Proc of. *IEEE International Conference on Blockchain* 2018.



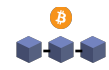
168SKtdY1V... : マイニングプール

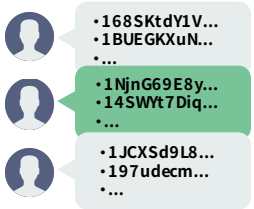
1NjnG69E8y... : 取引所

1JCXSd9L8... : ギャンブリング

1. Webからのデータ収集

様々な目的に使用されているBitcoinアドレスを収集


Bitcoin Blockchain



2. アドレス・クラスタリング

同一ユーザが保持する複数のBitcoinアドレスを推定

3. 取引履歴の抽出

ユーザ毎にBitcoin取引履歴の抽出

4. 取引履歴の特徴抽出

ユーザ毎に取引の特徴抽出
(取引頻度，送受の割合，送受額の大きさ…)

5. 機械学習

取引の特徴の違いを教師あり学習により学習し，
Bitcoinアドレス毎にサービスを識別

特性評価

データセット：Webから収集し，マニュアルでラベル付加した計26,313件のBitcoinアドレス

識別器： Random Forests (#Trees = 100)

評価項目： 10-fold 交差検証で求めた正答率 (サービス毎にBitcoinアドレスを正しく識別した割合)

	取引所	フォセット	ギャンブル	投資詐欺	マーケットプレイス	ロンダリング	マイニングプール
取引所	**0.41**	0.04	0.14	0.12	0.17	0.05	0.06
フォセット	0.04	**0.80**	0.04	0.09	0	0	0.03
ギャンブル	0.10	0.06	**0.54**	0.15	0.11	0	0.05
投資詐欺	0.04	0.12	0.09	**0.72**	0.01	0	0.02
マーケットプレイス	0.05	0	0.08	0	**0.85**	0.02	0
ロンダリング	0.02	0	0	0	0.04	**0.94**	0.01
マイニングプール	0.12	0.09	0.06	0.03	0	0.01	**0.70**

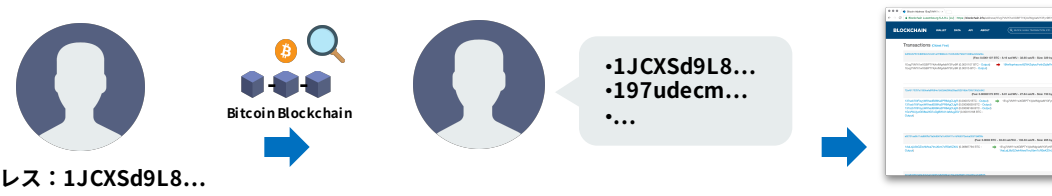
Bitcoinの取引履歴の時系列解析：Pirate@40の高利息投資プログラムの例

慶應義塾大学 理工学部 情報工学科 豊田健太郎 / toyoda@ics.keio.ac.jp

研究背景

- Bitcoinはアドレス間で送金を行う**仮想通貨**として急速に普及しています
- Bitcoinアドレスの作成は個人情報を必要としないため，**違法商品の取引決済**，**投資詐欺 (高利息投資プログラム)**などに悪用されるケースが報告されています
- そこでフォレンジクスの観点から，分析対象のBitcoinアドレスが含まれる取引履歴を**時系列解析**し，**取引の傾向の変化度を算出**する手法が求められています

提案手法： Bitcoinの取引履歴の時系列解析手法 [2]



アドレス：1JCXSd9L8...

1. 分析対象アドレスの決定

2. アドレス・クラスタリング
分析対象アドレスのユーザが保持する複数のBitcoinアドレスを推定

3. 取引履歴の抽出
推定したBitcoinアドレスが含まれる取引履歴を抽出

4. 取引履歴の特徴量を時系列で抽出
取引の特徴抽出 (取引頻度，送受の割合,…) をウィンドウ毎に算出

5. 取引の異常度を算出
複数の特徴から変化度 (異常度)を算出

特性評価

Pirate@40の高利息投資プログラムとは：

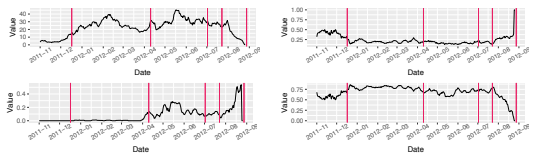
- ハンドルネーム (Pirate@40) による投資詐欺
- 週利7%の高利息投資プログラム
- 2011年11月にFirst Pirate Saving & Trustとして登場
- 2012年8月に利息の配当を停止
- 2013年，米国SECが告発


THE WALL STREET JOURNAL.
Trendon Shavers Sentenced in First Bitcoin Securities-Fraud Case
Judge says Texas man carried out 'classic Ponzi scheme'

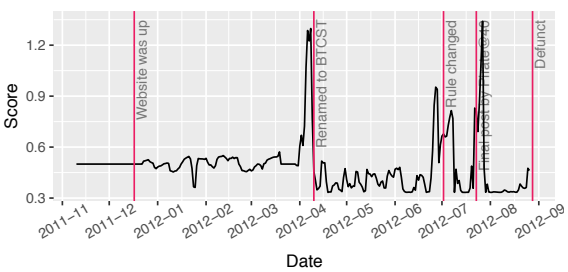
Source: The Wall Street Journal,

異常検知により検知すべき主なイベント：

1. 2011年12月17日 ホームページを公開
2. 2012年 4月10日 BTCST (Bitcoin Saving & Trust)と名称変更
3. 2012年 7月2日 週利を7%から5%に引き下げ
4. 2012年 7月23日 Pirate@40から最後の投稿
5. 2012年 8月26日 配当を停止



Pirate@40の取引履歴から算出した4つの特徴量の時系列変化



4つの特徴量から手法[1]で算出した異常度の変化と5つのイベント

[1] R. Jiang et al., "Anomaly Localization for Network Data Streams with Graph Joint Sparse PCA," in ACM KDD 2011.
[2] K. Toyoda et al., "Time Series Analysis for Bitcoin Transactions: The Case of Pirate@40's HYIP Scheme," in IEEE ICDMW 2018.