Bitcoin の取引履歴の可視化とそのバブル状況分析への応用

張　丘平, 前川　廣太郎, 延原　肇

筑波大学大学院システム情報工学研究科知能機能システム専攻

{zqp, maekawa, nobuhara}@cmu.iit.tsukuba.ac.jp

概要　2008 年に提案された分散型電子決済システム Bitcoin は, 2013 年現在, その換金価格が上昇しており, 注目を集めている. Bitcoin の持つ, 独特の設計思想に関して, 政治, 経済, 金融, 法律などの方面から議論がなされており, 特に注目を集めているのが, 本質的な価値をもたない貨幣が引き起こしやすい投機的バブル問題である. 本研究は, 分散型電子貨幣 Bitcoin の公開型取引履歴 Blockchain に対する統計的解析を行い, 独自の解析データベースを構築することで, Bitcoin の支払先を代表する各アドレスの残高の歴史推移を視覚化する. また, 実世界の換金市場の価格変動と比較することで, Bitcoin の投機的バブル問題の原因が, Bitcoin のユーザーの急増であることを明らかにする.

キーワード　Bitcoin, peer-to-peer, 電子貨幣, 電子商取引, 情報可視化

1 はじめに

Bitcoin は 2008 年に提案された分散型電子決済システムである[1]．2013 年以降，Bitcoin は IT 起業家達に破壊的イノベーションと評価され，アメリカには Bitcoin 関連のベンチャー創業が活発になっている[2]. また，Bitcoin は仮想通貨としてその換金価格が大きく上昇しており，インターネットユーザー達に注目されている[3].

本研究では Bitcoin の公開型取引履歴 Blockchain を利用, 解析し Bitcoin で論争となっている投機的バブル問題の実態把握を目的とする．そのために，Blockchain に対する統計的解析と，独自のデータベース構築により，取引関連情報を視覚化するシステムを構築する.

2 提案手法

まず, Bitcoin に関する定義を説明する．ウェブサイトにおいて，日本円や米ドルなどの現実通貨を用いて Bitcoin を売買することを換金という．また，Bitcoin システムにおいて, ユーザーの間で Bitcoin を転送することを取引という.

Bitcoin 換金市場における投機的バブル問題の実態を把握するには, Bitcoin システムの取引状況を明らかにしなければならない. 本研究では, 取引によって各アドレスの残高の変化を可視化する手法を提案する.

Shamir らは, 2012 年 5 月 13 日までの取引履歴を分析し, 3,730,218 個のアドレスの残高を統計的に明らかにしている[4]. しかしこの研究ではある時点の最終残高を統計しただけであり, 取引状況の変化は把握しにくい. 本研究では, 残高の歴史推移に着目し, 現時点の統計だけではなく, その変化の様子を視覚化する.

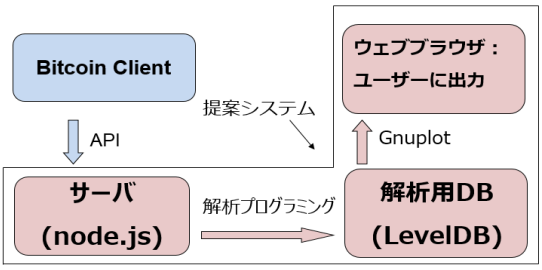

図1　システム構成

Blockchain には各アドレスの残高が記録されていないため, アドレスの残高推移の可視化するには, 独自の解析データベースが必要である. また, 幅広いユーザーが視覚化した結果を閲覧できるように, ウェブブラウザを利用した閲覧環境を構築する.

図 1 にシステムの構成を示す. システムは Node.js と LevelDB を用いて構築される. まずは Bitcoin クライアントの API を通じて, 取引情報を Blockchain からサーバに転送する. そして解析プログラミングを実行して残高の推移を記録するデータベースを作成する．最後に gnuplot を利用して可視化を実現する.

表1　Blockchain での取引情報の記録

取引	入力	出力	転送金額	発生時間
TX_1	A_0	A_1	V_{TX1}	T_{TX1}
TX_2	A_1	A_2	V_{TX2}	T_{TX1}

表1に Blockchain での取引情報の記録を示す．この例では，T_{TX1} に発生した取引 TX_1 には，アドレス A_0 から A_1 に金額 V_{TX1} を転送することを示している.

もしこの取引 TX_1 にてアドレス A_1 が初めて使用されるならば，解析データベースに新しい記録を書き込み，キーは A_1 と取引発生時間 T_{TX1} とのハッシュ，$Hash(A_1+T_{TX1})$ で，値は V_{TX1} である．

またある取引 TX2 にてアドレス A_1 は再び使用されるなら，解析データベースに $Hash(A_1+T_{TX2})$をキーとして検索する．記録があるなら更新し，ないなら新しい記録を書き込む． A_1 が入出力によって値は $V_{TX1}\pm V_{TX2}$ である．

このようにして，Blockchain の取引情報の解析データベースを作成する．表 2 に A_1 に対して処理済みの記録を示す．取引情報のサンプリング間隔を調整することで，記録の密度を調整することが可能であり，例えば，サンプリング間隔を 1 日と設定した場合に，当該日に発生した取引が積算・集約されて1つの値になる．

表2 提案データベースでの取引情報の記録

キー	値
$Hash(A_1+T_{TX1})$	V_{TX1}
$Hash(A_1+T_{TX2})$	$V_{TX1}\pm V_{TX2}$
…	…
$Hash(A_1+T_{TXn})$	$V_{TX1}\pm V_{TX2}\pm\ldots\pm V_{TXn}$

3 可視化実験

提案手法を用いて 2010 年 7 月から 2012 年 9 月までの取引履歴に対して解析データベースを作成する．解析したデータを元に gnuplot を利用して可視化を行う．図2に散布図の可視化結果を示す．一つの点は1件取引に対応しており，縦軸はその発生時間，横軸取引後の残高を示している．

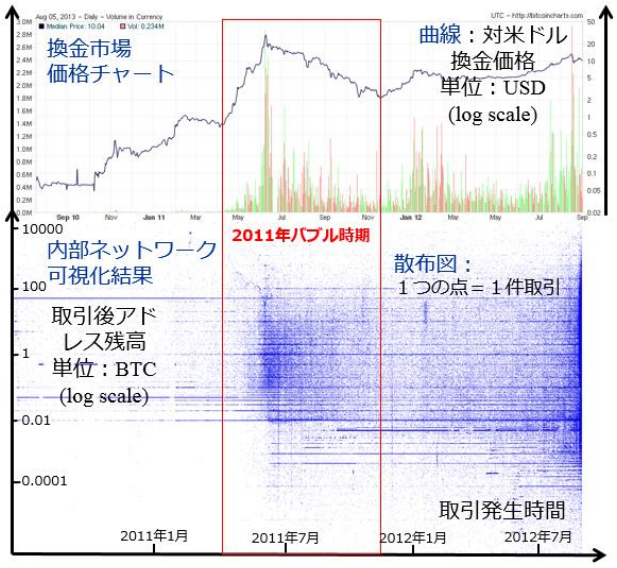

図2 可視化実験

換金市場[5]の価格チャート[6]と比較することで，2011 年のバブル時期に換金市場の価格変動に応じて内部ネットワーク取引後の残高のアドレス分布は分散化してゆく傾向を明らかになった．このような分散化は2つの意味を含んでいる．1つ目は取引件数の増加，2つ目これらの取引によってより低い残高を持つアドレスの増加である．また，一定時点において，Bitcoin システムの貨幣総量は既にプロトコルによって定めているので，より低い残高を持つアドレスの中の Bitcoin は換金によってより高い残高を持つアドレスから転送したものと推測され，この分散化の主な原因はユーザーの増加だと考える．

Bitcoin 換金市場のバブルの原因は2つあると考えられている．1つ目は本質的な価値をもたない仮想貨幣に対して行いやすい市場操作によって引き起こされたとする考え方である．2つ目は貨幣総量が一定であるシステムにユーザーが急に増加することによる市場結果であると考える，ことである．また，ユーザーの増加も市場操作に起因すると考えられる．散布図において，バブル前後の分散化状況を比較すると，バブルの一部の原因は市場操作である可能性は否定できないが，解析結果から，ユーザー数の増加が原因として大きな影響を与えていると考える．この解析結果は，Bitcoin 投資者がその発展実態と市場価値を把握する場合に，また，Bitcoin に関する諸論争を解決するに役に立つと考える．

4 まとめに

本研究は，Bitcoin の公開型取引履歴 Blockchain に対する統計的解析を行い，可視化を行った．換金市場の価格変動と比較することで，Bitcoin の取引ネットワーク内部の視点から，Bitcoin に関する論争の中心となる投機的バブル問題を考察し，その主な原因はユーザーの増加にあると結論づけた．しかし，Bitcoin システムは高度な匿名性を持っているため，実際のユーザー数の把握は難しくなっている．アドレスに基づくユーザーの解析ではなく，実際のユーザーのふるまいを解析してゆくことが今後の目標である．

参考文献

[1] "Bitcoin: A Peer-to-Peer Electronic Cash System", http://bitcoin.org/bitcoin.pdf
[2] "Bitcoin buzz grows among venture investors, despite risks", http://www.reuters.com/article/2013/10/01/us-markets-forex-bitcoin-idUSBRE9901HA20131001
[3] "Bitcoin | TechCrunch Japan", http://jp.techcrunch.com/tag/bitcoin/
[4] Dorit Ron, Adi Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph", The Weizmann Institute of Science, 2012
[5] "Mt.Gox - Bitcoin Exchange", https://www.mtgox.com/
[6] http://bitcoincharts.com/markets/mtgoxUSD.html