

## ビットコインのトランザクションデータベースの可視化と

## その為替相場分析への応用

## Visualization of Bitcoin transaction database and its application to the exchange market analysis

張 丘平  
Qiuping ZHANG前川 廣太郎  
Koutarou MAEKAWA延原 肇  
Hajime NOBUHARA

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

Department of Intelligent Interaction Technologies, Graduate School of System and Information Engineering, University of Tsukuba

Bitcoin is a peer-to-peer digital currency that has gained increasing attention among global investors since trading began around 2009, due in part to its ease of use in cross-border transactions. In this paper, based on the simple assumption that the value of Bitcoin is determined by its popularity, we propose a visualization of the transaction history of Bitcoin, which at some extent reflects the long-term price movement in the exchange market and therefore, could possibly predict the future price movement of Bitcoin. To realize the visualization, we firstly perform a statistical analysis of blockchain, the public ledger of Bitcoin transactions, and then construct our original time series database of balance of all Bitcoin addresses. Finally in the evaluation experiment, we visualize all transactions during 2011 by the proposed method and compare the result to the market price chart of the same period to confirm the effectiveness of proposed method.

## 1. はじめに

ビットコインは暗号技術を利用したオープンソースプロトコルに基づくピアツーピア分散型電子決済システム及びこのシステムにおける電子通貨である[Nakamura 2008]. 頭文字の大小による意味の違いがあり, 大文字表記 (Bitcoin) はプロトコルと決済システムを, 小文字 (bitcoin) は通貨自体を意味する. ビットコイン通貨はビットコインシステムの運営に演算能力を提供したピアツーピアネットワークのノードへの報酬という形で自動的に生成され, 市場に供給される. すなわち, 中央機関により発行される法定通貨や前払いの支払い手段である電子マネーとは異なるものである.

ビットコインシステムは既存の金融機関や決済代行業者に比べ低いコストで国際送金や決済が可能であるため, IT 起業家達に破壊的イノベーションと評価され, 2013 年以降, アメリカではビットコイン関連のベンチャー創業が活発になっている. また, 使用範囲の拡大に伴い, ビットコイン通貨は価値が増加すると予想され, 投資家達にも注目されている[Grinberg 2013].

本研究は, 投資家にとって有益な情報として, ビットコイン為替相場の長期的傾向を反映できる指標作成を目的とする. ビットコイン通貨の価値の源泉はビットコインシステムであるという単純な仮定に基づき, ビットコインシステムの実際の使用状況を直観的に把握できる可視化の実現を目指す.

## 2. 提案手法

まず, ビットコイン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法定通貨を用いてビットコイン通貨を売買することを為替あるいは取引という. また, ビットコインシステムにおいて, ユーザ間でビットコイン通貨を転送することをトランザクションという.

連絡先: 張 丘平, 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 計算知能・マルチメディア研究室, 〒305-8573 茨城県つくば市 天王台 1-1-1 3E 棟 307 号室, (080)3715-2683, zqp@iit.tsukuba.ac.jp

## 2.1 ビットコインの社会的価値についての考察

ビットコインシステムを利用した法定通貨建ての支払や送金は, 処理時間が短い点で, ビットコイン通貨の相場及びその変動にもたらす影響がほとんどないと考えられる. また, 一定時点におけるビットコイン通貨総量はプロトコルで決められているので, 流通するビットコイン通貨の相場が高ければ高いほど, ビットコインシステムを経由する支払や送金の額度が高くなり, ビットコインシステムにおける経済活動の規模及び影響が大きいと言える. 上の2点から, ビットコインシステムは常に社会的な利用価値があり, その価値とビットコイン通貨の相場とは相互作用があると考えられる.

## 2.2 為替相場の長期的傾向を反映する指標

2.1 の考察から, ビットコイン通貨の社会的価値の源泉はビットコインシステムであるという仮説を立て, ビットコイン通貨の為替相場の長期的傾向を反映する最もシンプルな指標はビットコインシステムのアクティブユーザの規模であると考えられる. 本研究では, この関係性を明らかにする作業を行うが, ビットコインシステムは高度な匿名性を持っているため, アクティブユーザ数の把握は容易ではない. そこで, アクティブユーザ数に強い相関を持つと考えられる以下の2つの統計量に着目する.

## (1) アクティブアドレス数

アクティブアドレスとは1日中少なくとも1件のトランザクションが発生するアドレス. これはビットコインシステムに対する分析を通じて取得しやすい.

## (2) 残高の低いアドレス数

一定時点において, ビットコイン通貨総量はプロトコルによって決められているので, 低い残高を持つアドレスは, 必ず高い残高を持つアドレスがビットコイン通貨を転送した後に生じるものである. 経験的にこういう転送トランザクションの多くは, 新規ユーザがビットコイン通貨の入手に伴って発生したものと考えられ, 新規ユーザの増加が低い残高を持つアドレスの増加の主な原因だと考える.

## 2.3 従来の全トランザクション履歴の定量分析に関する研究と問題点

Shamir らは、ビットコインシステムの使用状況を把握するために、2009年1月3日から2012年5月13日までのトランザクション履歴を分析し、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[Shamir 2012]。しかしこの研究では2012年5月13日その時点の残高を統計しただけであり、アクティブアドレス数の変化の解明や相場傾向分析への応用は行っていない。本研究は相場傾向の分析のため、アクティブアドレス数及び残高の低いアドレス数の変化を同一のグラフで直観的に把握できる可視化方法を説明する。

## 2.4 アドレスの残高推移の可視化

まずはブロックチェーンと呼ばれるビットコインシステムの公開型トランザクション履歴に対する統計的解析を行う。それに、ビットコイン通貨の支払先を代表する各ビットコインアドレスの残高を時系列解析により明らかにする。さらに、独自の解析データベースを構築することで、ビットコインシステムの使用状況関連情報を可視化するシステムを実現する。

図1に解析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。まずはビットコインクライアントのAPIを通じて、トランザクション情報をブロックチェーン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。

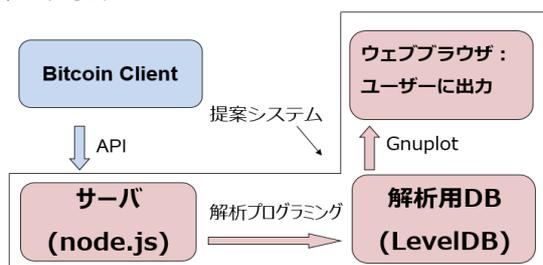


図1 システムの構成

表1にBlockchainでの取引情報の記録を示す。この例では、TX<sub>1</sub>に発生した取引TX<sub>1</sub>には、アドレスA<sub>0</sub>からA<sub>1</sub>に金額V<sub>TX1</sub>を転送することを示している。

取引	入力	出力	転送金額	発生時間
TX <sub>1</sub>	A <sub>0</sub>	A <sub>1</sub>	V <sub>TX1</sub>	T <sub>TX1</sub>
TX <sub>2</sub>	A <sub>1</sub>	A <sub>2</sub>	V <sub>TX2</sub>	T <sub>TX2</sub>

表1 ブロックチェーンでのトランザクション記録

この取引TX<sub>1</sub>にてアドレスA<sub>1</sub>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<sub>1</sub>と取引発生時間T<sub>TX1</sub>とのハッシュ、Hash(A<sub>1</sub>+T<sub>TX1</sub>)で、値はV<sub>TX1</sub>である。

またある取引TX<sub>2</sub>にてアドレスA<sub>1</sub>は再び使用されるなら、解析データベースにHash(A<sub>1</sub>+T<sub>TX2</sub>)をキーとして検索する。記録が存在する場合更新し、存在しない場合新しい記録を書き込む。A<sub>1</sub>がトランザクションの入出力によって値はV<sub>TX1</sub>±V<sub>TX2</sub>である。

キー	値
Hash(A <sub>1</sub> +T <sub>TX1</sub> )	V <sub>TX1</sub>
Hash(A <sub>1</sub> +T <sub>TX2</sub> )	V <sub>TX1</sub> ±V <sub>TX2</sub>
...	...
Hash(A <sub>1</sub> +T <sub>TXn</sub> )	V <sub>TX1</sub> ±V <sub>TX2</sub> ±...±V <sub>TXn</sub>

表2 提案データベースでのトランザクション関連情報の記録

このようにして、取引情報の解析データベースを作成する。表2にA<sub>1</sub>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。

## 3. 各種指標の可視化および関係性解析

提案手法を用いて2010年7月から2012年9月までのトランザクション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。1つの点は1個のアクティブアドレスに対応しており、縦軸はそのアクティブ時間、横軸はトランザクション実行後の残高を示している。

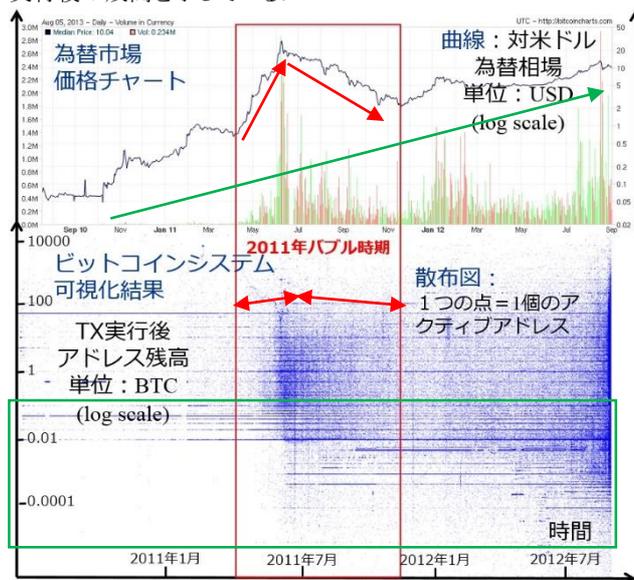


図2 提案システムによる可視化の結果

赤い矢印が示しているように、2011年に為替相場の傾向が上昇または下降であることはトランザクション実行後残高のアドレス分布の疎密変化に対応していることが定性的に明らかになった。また、青いコラムの部分から、残高の低いアドレス数の増加は相場の長期的上昇トレンドに対応していることが明らかになった。これは、以下の2つのことを示唆している。

- 相場の上昇または下降トレンドはアクティブユーザー数の増減に対応している。
- 相場の長期的上昇トレンドは新規ユーザーの増加に対応している。

## 4. まとめ

本研究はビットコイン為替相場の長期的傾向を反映できるビットコインシステムに対する可視化分析手法を提案した。為替相場チャートと比較することで、過去のデータに対する有効性を示した。今後の展望としては、市場の変動予測を目標とする。

### 参考文献

- [Nakamura 2008] Satoshi: Bitcoin: A peer-to-peer electronic cash system, 2008.
- [Grinberg 2013] Reuben: Bitcoin: An Innovative Alternative Digital Currency, Hastings Science & Technology Law Journal, 2013.
- [Shamir 2012] Adi: Quantitative Analysis of the Full Bitcoin Transaction Graph, The Weizmann Institute of Science, 2012.