Bitcoin 取引の可視化

永田倖大†
明治大学総合数理学部　先端メディアサイエンス学科‡

1　はじめに

Bitcoin は Nakamoto の論文[1]に基いたディジタル通貨である．第三者機関を介さずに取引できることや，ブロックチェーンなどの技術により，近年，注目度が増している．Bitcoin の取引データは公開されており，世界中の誰もが確認することが可能である．しかし，取引情報は独立して記録されているので，Bitcoin の取引がどのブロックをたどってきたのかというブロックチェイン間の繋がりを見ることは，難しい．繋がりを見ることが可能になれば，特定の Bitcoin がいつ使われてきたかを確認することができる．

そこで，本研究では Bitcoin の取引データを収集し，収集したデータを基に特定の Bitcoin が過去に使われてきた取引情報の可視化を行い，ブロック同士の繋がりを明らかにすることを目的とする。

2　実験

2.1　データ収集方法

世界中の Bitcoin 取引の情報や，ブロック情報などを記録しているサイト Bitcoin ブロックエクスプローラー[2]を用いて，取引データを収集する．データ収集は手作業で行い，自分でデータ量は決定する．

本実験では 8 行の取引を収集した．表 1 の取引データは 2016 年 1 月に，Bitcoin ブロックエクスプローラーサイトで公開されている実在する取引データを収集した．表 1 の取引データ以降にも取引は続いているが割愛している．

図 1 に Bitcoin ブロックエクスプローラーで公開されている取引例を示す．

図 1　取引データ[2]

ここで201417が取引が格納されているブロック，5c76eb4dfb0941856a22983ef05b2f5c669dadc98ea34ea11974cacba9dc7が取引ID，1MdYC22Gmjp2ejVPCxyYjFyWbQCYTGhGq8，1E86A5E6ANEVPuay2XLGVsXjaxT5MbRm，19PphSFxzmsSZ3JRacQArEgN1b67ar83がアドレスである．合計インプットは取引で使用されたビットコインの総額である．

1MdYC22Gmjp2ejVPCxyYjFyWbQCYTGhGq8から1E86A5E6ANEVPuay2XLGVsXjaxT5MbRmへ50.53036298BTC，19PphSFxzmsSZ3JRacQArEgN1b67ar83へ0.10481202BTCを送金している．

2.2　取引データ形式

取引データには，ID，親番号，深さ，ブロック番号，が含まれる．ID はユニークであり，ブロック番号は取引が含まれているブロックの番号で，深さは図 1 のツリーのどの深さにいるのか，親番号はノードの親の ID を表している．親番号が 0 の時は，親ノードは存在しない．表 1 にデータ例を示す．

表 1　取引データ例

ID	親番号	深さ	ブロック番号	送金額
1	0	1	200000	50.635175
2	1	2	201417	50.635175
3	2	3	201419	50.53036298
4	2	3	201742	0.10481202
5	3	4	201548	50.1615802
6	3	4	201420	0.36878278
7	4	4	207133	0.00009994
8	4	4	201755	1.4777

2.3　実験環境

実験環境を表 2 に示す．

表 2　実験環境

OS	OS X El Capitan 10.11.2
メモリ	8GB
言語	Processing 3.0.1

2.4　プログラム内容

収集したデータを可視化するプログラムBitcoinTxVisualizeを用いて，表 1 のcsvファイルを読み込み，可視化した結果を図 2 に示す．

†Visualization of Bitcoin transactions , Koudai nagata
Department of Frontier Media Science, Interdisciplinary Mathematical Science, Meiji University

Algorithm ： BitcoinTxVisualize	
	Csvファイル読み込み ノードに情報を格納 ノードの表示位置，枝の表示位置を決定 ノード，枝を描画

2.5　実行結果

図 2 に表 1 のデータを使ったプログラムの実行結果を示す．

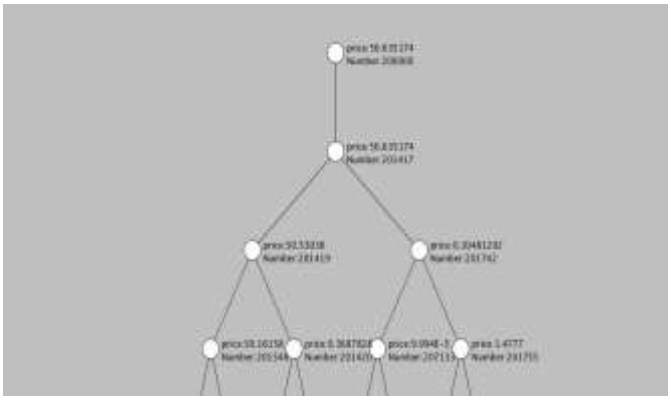

図 2　実行例

ノードの右に表示されている price は受け取った Bitcoin の総額である．Number はその Bitcoin を他のアドレスに向けて送金した取引が含まれているブロック番号であり，そしてノードから出ている枝の本数が、取引先件数である．線が出ていないノードは，それより先で取引が行われておらず，保有している状態になっている．

例えば図 2 の深さ 2 のノードは，50.635174BTC を受け取りその Bitcoin を 2 つのアドレスに向けて，50.53036,0.1481202 ずつ送金している．そしてこの取引が格納されているブロック番号が 201417 である．

図 2 では深さが 4 までしか表示されていないが割愛している．

2.6　改善点

図 3 の様に，深くなるにつれて，ノード 1 つを表示できるスペースが狭くなってしまう．右下のノードのブロック番号が重なってしまい見づらい．さらに，1 つのノードに対して多くの子ノードが繋がっている時もブロック番号が重なってしまう．

本実験では，データ収集は手動で行っているため大量のデータを集めるのは困難である．取引データは図 1 のページに 1 つずつしか公開されておらず，例えば 1000 件の取引データを収集するためには手動で約 1000 回クリックしなければならないからである．

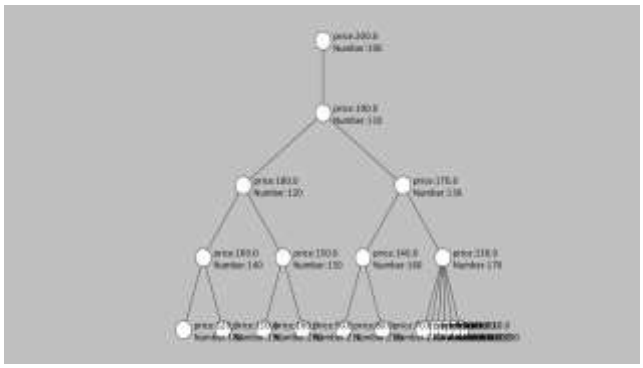

図 3　改善が必要な例

3　おわりに

Bitcoin の取引情報に基づいて， Bitcoin のブロックの繋がりを可視化する BitcoinTxVisualize を開発した．少ないデータ量では可視化した図は見やすく，繋がりを理解することは容易であるが，データ量が大きい時は，可視化した図はノードが重なってしまい図 3 の様に見づらくなってしまう．他にもデータ量が増えると price と Number の表示が重なってしまい確認しづらくなる．さらにデータ収集は手動で行っているため，多くのデータを集めるのは困難である．

なので，多くのデータにも対応し，よりブロックの繋がりが理解しやすいようにプログラムを改善し，データ収集を自動化することを今後の課題とする．

参考文献

[1] S.Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (https://bitcoin.org/bitcoin.pdf ,2015 年 4 月参照).

[2] Bitcoin Block Explorer - Blockchain.info(https://blockchain.info/en/ , 2015 年 4 月参照)