# ダークネット観測情報を用いた 仮想通貨市場におけるリスクの考察 ～仮想通貨市場におけるオルタナティブ・データの活用～

# Evaluation of Risk in Crypto Currency With Darknet Observation Information

中川　慧 [1,2*]　今村　光良 [1,3]　面 和成 [4]
Kei Nakagawa[1,2] Mitusyoshi Imamura[1,3] Kazumasa Omote[4]

[1] 野村アセットマネジメント株式会社
[1] Nomura Asset Management Ltd.
[2] 筑波大学 大学院 ビジネス科学研究科
[2] University of Tsukuba Graduate School of Business Sciences
[3] 筑波大学 大学院 システム情報工学研究科
[3] University of Tsukuba Graduate School of Systems and Information Engineering
[4] 筑波大学 システム情報系
[4] University of Tsukuba Faculty of Engineering, Information and Systems

**Abstract:** Bitcoin is a crypto currency that is a peer-to-peer(P2P) network systems based on distributed ledger technology and is being used as an alternative payment system. Reliability and safety are very important aspects of payment system. However, in recent years, with an increase in value, crypto currency becomes a target of a malicious users and the attacks that strike the vulnerability of the system are regarded as a problem. Such a problem significantly reduces reliability and safety as a payment system for crypto currency. Therefore, it is necessary to pay attention to cyber security risks inherent in the system, as well as price fluctuations usually focused on financial asset prices. In this research, we propose to use information observed in darknet as alternative data. It is useful in evaluating the risk in the crypto currency market. The darknet is a name of an IP address space unallocated by terminals or the like among spaces that can be assigned IP addresses. The darknet is mainly used for observing signs of security incidents. This is useful for investors to grasp potential risks of crypto currency markets and is important for service providers to explain security risks and measures. In addition, the darknet observation information has a prospect of utilizing not only the crypto currency but also the monitoring of the security risk of companys.

## 1　はじめに

近年、世界規模で急速に利用者数が拡大し、注目を集めているのが Bitcoin を代表とする仮想通貨である。仮想通貨とは、ウェブ上に投稿された論文 [20] を基に、有志により開発がすすめられている P2P 型の分散台帳 (ブロックチェーン) を用いたシステムを指す。台帳に記録される数値が金融資産として取引され、取引手数料が安価であり、決済代替手段としての活用がすすめられたことから「通貨」と呼ばれている。

仮想通貨はその市場規模が大きくなるにつれて、投資対象として投資家からの関心が高まり、学術方面では、金融資産としての分析が活発に行われるようになった。例えば、伝統的な資産である株や債券などに対して用いられる、時系列解析に基づく分析がある。時系列解析のモデルには、条件付き平均モデル、条件付き分散モデルがある。条件付き平均モデルの代表例としては、AR モデル、MA モデル、ARMA モデルがあり、

*連絡先： 野村アセットマネジメント株式会社
〒 103-0027 東京都中央区日本橋 1 丁目 12-1
E-mail: kei.nak.0315@gmail.com

これらは株価の水準あるいは収益率のモデリングおよび予測に用いられる。AR モデルは過去の株価の線形結合で将来の株価を予測するモデルであり、MA モデルは過去の株価の攪乱項の線形結合で将来の株価を予測するモデルである。ARMA モデルは AR と MA の両者を組み合わせたモデルである。一方で、条件付き分散モデルには、ARCH モデルや、ARCH をさらに一般化した GARCH モデルが提案されている [12]。

Bitcoin については、条件付き分散モデルを用いて、ボラティリティの分析や、ヘッジ手段としての有効性など分析した先行研究がある [7, 8, 16]。

時系列解析以外には、Bitcoin に関連するニュースの発信および拡散に用いられるソーシャルメディアを代表とした web 上から得られるデータをクロスセクショナルな特徴量として、Bitcoin 価格との関係性について調査した先行研究 [11, 19] もある。

その他、Bitcoin を伝統的資産と組み合わせた場合における分散効果について調査した先行研究 [4] などもあり、その関心の高さが伺える。

一方で、Bitcoin に対する関心は、投資対象である金融資産としてだけはなく、基盤技術であるブロックチェーンを用いた「システム」としての側面に注目が集まっている。そのため、Bitcoin のシステムとしての研究開発調査が拡大しており、学術方面においては、システムにおける動作プロトコルのメカニズムに焦点が当てられ、体系的な研究報告 [3] がある。近年は、その資産価格の上昇から、悪意あるユーザーの標的となり、攻撃の懸念や、マネーロンダリングの手段とされるなどの問題が指摘されている。そのため、特定ユーザーを識別する研究 [17] など、セキュリティ方面での学術的な取り組みが活発である。最近の観点としては、特に、先行研究 [13] で報告されている通り、ブロックチェーン上に記録されている情報を分析する場合に得られる情報は限定的であり、P2P ネットワークの通信情報を分析することの重要性が認識されている。

そこで本研究では、セキュリティ方面で、活用が検討されているネットワークの通信パケットを、仮想通貨市場におけるリスクを評価する上で、有効と考えられるオルタナティブ・データ[1]として、活用することを提案する。すなわち仮想通貨を金融資産ではなく、システムとして捉え、セキュリティの観点から有効な情報を用いて価格分析を行う。

以降、第 2 章では、関連研究として、本研究で利用するダークネット観測情報および分析手法である GARCHSK について紹介する。第 3 章では、ダークネット到達パケットを用いた Bitcoin 価格の実証分析を示し、第 4 章で結論を述べる。

[1]オルタナティブ・データとは価格や出来高などの従来金融資産の分析に用いていた公開情報以外のデータ群をいう。

# 2 関連研究

仮想通貨におけるオルタナティブ・データの活用としては、先行研究 [1] の、その日に確認できるユニークなアドレス数を用いた研究がある。当該研究は、ネットワークの価値がネットワークの規模より推定される利用者のネットワーク効果に着目している。一方で、ビットコインのネットワーク分析に用いるデータとして、ダークネットを用いることを提案した研究がある [24]。この研究では、従来のビットコインのネットワーク分析で活用される正常なネットワークにて観測される情報ではなく、イレギュラーなネットワークにて観測される情報を用いて、ビットコイン・ネットワークの分析を試みた研究である。そこで本研究では、このダークネット観測情報と、ビットコインの価格やリターンのモーメントとの関係を分析する。以下に、本研究で用いるダークネットを用いた先行研究および、分析手法である GARCHSK モデルについて紹介する。

## 2.1 ダークネットを用いた先行研究

一般的にダークネットという単語には、下記 2 つの意味合いで用いられることがある。

- Tor[6] などの匿名通信プロトコルや BitTorrent[5] や Napster[1]といった、違法行為に関与した技術やサービスを含む違法な薬物や個人情報などを取り引きするために用いるサーバーやプログラムによって形成されるネットワークの総称。
- IP アドレスの割り当てが可能な空間のうち、端末等が未割り当ての IP アドレス空間の呼称であり、スキャニング活動、分散型サービス拒否攻撃 (DDoS 攻撃)、マルウェア識別などのさまざまなサイバー脅威情報を生成するために活用されているものを指す [25]。

Bitcoin などの仮想通貨については、違法取引の決済手段として利用されることもあるため、主に前者の闇市場関連の意味として扱う先行研究 [10] 等もあるが、本研究で扱うのは後者である。

ダークネットに関する研究を調査した先行研究では、ダークネットの研究対象から、1. ダークネットの展開とセットアップ (展開)、2. 展開されたセンサーによるダークネットデータの測定と分析 (パケット分析)、3. パケットの可視化と表現のためのツールとテクニック (可視化) の 3 つのカテゴリに分類している。

ビットコイン・ネットワークとダークネットの関係について調査した先行研究 [24] は 3 つのカテゴリーのうち 2. のパケット分析に該当する。

[1]Peer-to-Peer によるファイル共有サービス

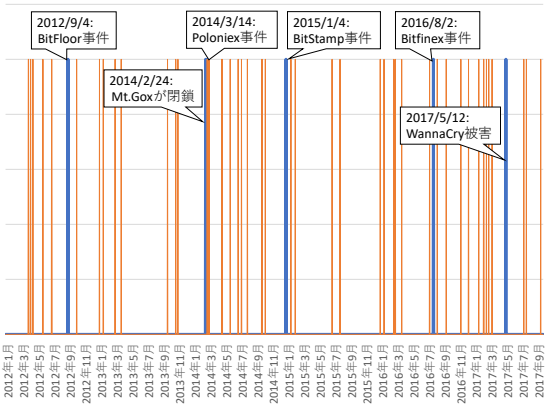


図 1: パケットの異常時とセキュリティ・インシデント

上述の研究では、まず、ダークネットを用いてビットコインネットワークを分析するにあたり、そもそもビットコイン・ネットワークで利用される通信がダークネットにて観測されるか確認している。本来ダークネットは端末等が未割り当ての IP アドレス空間であるため、通信が発生しないことが前提となる。しかしながら、通信が観測されないはずの空間に通信が観測されることを報告している。先行研究 [10] にて、世界中に観測点を持ち、大規模なプロジェクトに分類される国立研究開発法人情報通信研究機構 (NICT) の NICTER プロジェクト [15] にて観測しているダークネット上に観測される通信情報を用いて、2011 年 1 月 1 日から 2017 年 10 月 5 日の期間について分析した。具体的には、ビットコインなどの P2P 型のサービスがインターネットを介して端末間を接続する際に用いる、接続設定に着目した。そして、この接続設定に該当する通信に対する 1 日あたりの総パケット数の変化を確認している。また、図 1 の通り、観測値の異常値とセキュリティ・インシデントが関連する可能性について示唆した。

## 2.2 GARCHSK モデル

分散不均一性[2]を示す経済、金融時系列の条件付きボラティリティの時系列変化をモデリングするため、[9] は ARCH(AutoRegressive Conditional Heteroscedasticity) モデルを提案した。

[2] は ARCH モデルを一般化した GARCH(Generalized ARCH) モデルを提案した。(AR-)GARCH モデルは次式のように、資産リターン $r_t$ の条件付き分散 $h_t$ を過去の収益率のショック $\varepsilon_{t-1}$ の 2 乗に、過去の分散 $h_{t-1}$ の線形和で表現する。なお、定常性を満たすためには、$|\alpha| < 1, \beta_1 + \beta_2 < 1$ また分散の非負性から $0 < \beta_0, \beta_1, \beta_2$ の係数制約が必要である。

$$r_t = \alpha_0 + \alpha_1 r_t + \varepsilon_t \tag{1}$$
$$h_t = \beta_0 + \beta_1 \varepsilon_{t-1}^2 + \beta_2 h_{t-1} \tag{2}$$
$$\varepsilon_t | I_{t-1} \sim N(0, h_t) \tag{3}$$

[18] は条件付き分散をモデル化する GARCH モデルをさらに拡張して、条件付き歪度、条件付き尖度の変動も取り込んだ GARCHSK(GARCH Skewness-Kurtosis) モデルを提案した。また GARCHSK モデルによる実際の資産価格変動の実証分析を行い、株や為替のいくつかでは条件付き歪度、条件付き尖度の存在が確認された。このモデルの特徴は条件付き歪度、条件付き尖度の変動を GARCH モデルと同等のわかりやすい構造で明示的に捉えることができる。かつ、推定は容易である。GARCHSK モデルの具体的な定式化は次の通り。

$$r_t = \alpha_0 + \alpha_1 r_t + \varepsilon_t \tag{4}$$
$$h_t = \beta_0 + \beta_1 \varepsilon_{t-1}^2 + \beta_2 h_{t-1} \tag{5}$$
$$s_t = \gamma_0 + \gamma_1 \eta_{t-1}^3 + \gamma_2 s_{t-1} \tag{6}$$
$$k_t = \delta_0 + \delta_1 \eta_{t-1}^4 + \delta_2 k_{t-1} \tag{7}$$
$$\eta_t = h_t^{\frac{-1}{2}} \varepsilon_t \tag{8}$$
$$\eta_t | I_{t-1} \sim g(0, 1, s_t, k_t) \tag{9}$$

ここで、$g$ は平均 0、分散 1、歪度 $s_t$、尖度 $k_t$ を持つ確率密度関数である。なお、定常性を満たすためには、$|\alpha| < 1, \beta_1 + \beta_2 < 1, |\gamma_1 + \gamma_2| < 1, \delta_1 + \delta_2 < 1$ また分散と尖度の非負性から $0 < \beta_0, \beta_1, \beta_2, \delta_0, \delta_1, \delta_2$ の係数制約が必要である。

彼らは、Chebyshev-Hermite 多項式を用いた Gram-Charlier 展開によって GARCHSK モデルの確率密度関数 $g(0, 1, s_t, k_t)$ が従う次のような分布を導出した。

$$g(\eta_t | I_{t-1}) = \frac{\phi(\eta_t)\psi^2(\eta_t)}{\Gamma_t} \tag{10}$$
$$\phi(\eta_t) = \frac{1}{\sqrt{2\pi h_t}} exp(\eta_t^2 - h_t) \tag{11}$$
$$\psi(\eta_t) = 1 + \frac{s_t}{3!}(\eta_t^3 - 3\eta_t) + \frac{k_t - 3}{4!}(\eta_t^4 - 6\eta_t^2 + 3) \tag{12}$$
$$\Gamma_t = 1 + \frac{s_t^2}{3!} + \frac{(k_t - 3)^2}{4!} \tag{13}$$

$\eta_t = h_t^{\frac{-1}{2}} \varepsilon_t$ より $\varepsilon_t$ の確率密度関数は $f(\eta_t | I_{t-1}) = h_t^{\frac{1}{2}} g(\eta_t | I_{t-1})$ となる。したがって、定数項を除いた対数尤度関数 $l_t$ は次のようにかける。

$$l_t = -\frac{1}{2} ln h_t - \frac{1}{2}\eta_t^2 + ln(\psi^2(\eta_t)) - \Gamma_t \tag{14}$$

よって、GARCHSK モデルの各パラメータは最尤法により $l_t$ を最大化することで求めることができる。

[2] ある時期にはボラティリティが平均して小さく、別の時期にはボラティリティが平均して大きくなる傾向が観察される。このようなボラティリティが時期によって異なった水準を示すことを分散不均一性またはボラティリティ・クラスタリングと呼ぶ。分散不均一性は経済・金融時系列データに幅広く見られる現象である。

表 1: データ期間におけるビットコインの日次リターンの統計量

| 平均 | 標準偏差 | 歪度 | 尖度 |
|---|---|---|---|
| 0.43 | 4.58 | 0.43 | 15.65 |
| サンプル数 | 最大値 | 最小値 | Jarque-Bera (p-値) |
| 2,102 | 41.59 | -31.09 | 14,107 (0.000) |

## 3 実証分析

前述の通り、本来ダークネットは端末等が未割り当ての IP アドレス空間であるため、通信が発生しないことが前提となる。しかしながら、通信が観測されないはずの空間に特に異常な量の通信が観測された場合、その前後で価格やモーメントにどのような影響を及ぼしているのかを分析する。各次数のモーメントの変動をとらえるために GARCHSK モデルを使用する。分散、歪度、尖度など通常の各次数のモーメントは、ある期間において一定の値をとるが、GARCHSK モデルを用いることで、各時点ごとの分散、歪度、尖度の時系列変化を捉えることができる。

### 3.1 データ

本分析に用いるデータとしては、先行研究 [24] と同様に、国立研究開発法人情報通信研究機構 (NICT) の NICTER プロジェクト [15] にて観測しているダークネット上に観測される通信情報を用いて、2011 年 1 月 1 日から 2017 年 10 月 5 日の期間について分析した。Bitcoin の価格については、coindesk[3]にて公開されている Bitcoin Index の値を用いた。

はじめに分析対象のデータ期間全期間における統計量を確認する。表 1 は日次リターンの統計量を整理した表である。日次の標準偏差は 4.5% と非常にボラタイルで、正の歪度を持ち、尖度も 15 と非常に大きい。当然ながら Jarque-Bera 検定による正規性はなく、通常の金融資産と同じくファットテールな分布を持つ。

次に、表 1 に示す通り日次リターンに対して AR(1) モデルを当てはめ、その残差についての自己相関を確認した。Ljung-Box 検定の結果、4 次までのすべての残差について自己相関があることがわかる。そのため、4 次の条件付きモーメントの自己相関をモデル化する GARCHSK モデルを当てはめる余地がある。具体的に

[3]https://www.coindesk.com/

表 2: AR(1) モデルの残差の Ljung-Box 統計量

| LB(20) $\varepsilon_t$ (p-値) | LB(20) $\varepsilon_t^2$ (p-値) | LB(20) $\varepsilon_t^3$ (p-値) | LB(20) $\varepsilon_t^4$ (p-値) |
|---|---|---|---|
| 58.94 (0.0000) | 881.43 (0.0000) | 81.32 (0.0000) | 77.47 (0.0000) |

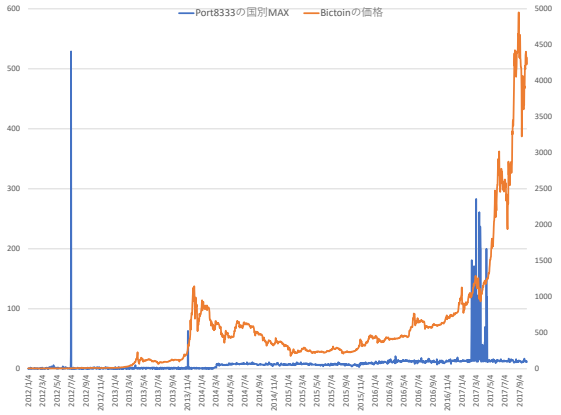


図 2: Price

日次リターンから推定した GARCHSK モデルのパラメータは表 3 の通りである。

次に、ダークネット観測情報から得られたパケットの「異常値」を定義する。図 2 はパケット観測値と Bitcoin の価格を合わせて表示した図である。明確にパケットの異常位置はわかるが、今回は 30 日間の標準化したパケット量が $+3\sigma$ を超えたら異常とした。また異常とされた日は 51 日存在した。

### 3.2 分析結果

以上の推定した条件付きモーメントおよび異常と定義したパケットを用いてそれらの関係を見ていく。図 3 から図 6 は、異常なパケットが発生した日とリターン、GARCHSK モデルで推定した条件付き分散、歪度、尖度を重ねて表示したグラフである。それぞれ分散は高いほうがリスクが大きいことを表し、歪度は低いほうが、尖度は高いほうが、極端な値をとるリスクが高いことを表している。グラフから条件付き分散、歪度、尖度がジャンプする前あるいは同時にパケットの異常値が検出されていることが確認できる。

さらに詳しくパケットの異常値が観測された前後の価格変動を包括的に確認する。表 4 は異常なパケットが観測される前 10 日の日次リターンのサマリーを示し、表 5 は観測後 10 日間示している。まず、パケットの観

表 3: GARCHSK モデルのパラメータ推定結果

| | $\alpha_1$ | $\beta_0$ | $\beta_1$ | $\beta_2$ | $\gamma_2$ | $\gamma_1$ | $\gamma_2$ | $\delta_0$ | $\delta_1$ | $\delta_2$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 係数 | 0.0988 | 0.0008 | 0.0783 | 0.4509 | -0.0900 | 0.0145 | -0.1700 | 1.2787 | -0.0000 | 0.6887 |
| 標準誤差 | 0.0142 | 0.0201 | 0.0159 | 0.0159 | 0.0159 | 0.0159 | 0.0142 | 0.0170 | 0.0160 | 0.0142 |
| t 値 | 6.9323 | 0.0377 | 4.9192 | 28.3306 | -5.6544 | 0.9082 | -11.9379 | 75.3242 | -0.0000 | 48.3634 |

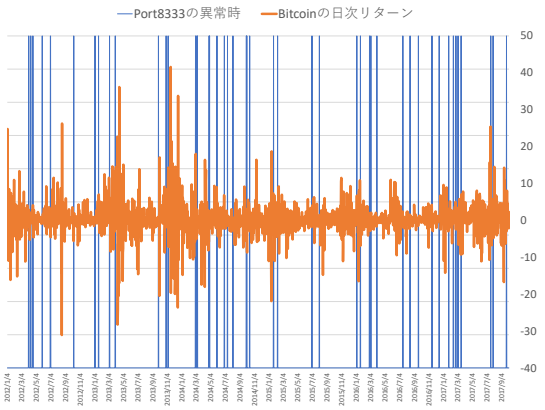


図 3: Return

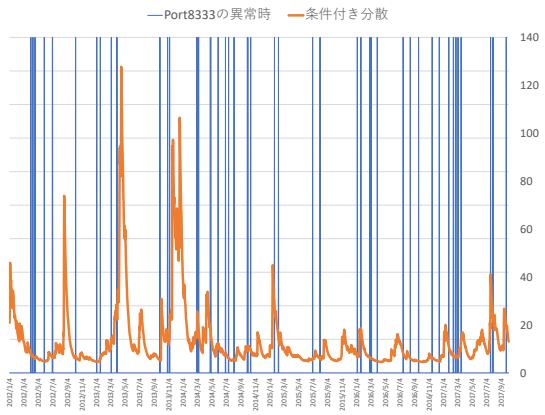


図 4: Vol

表 4: 過去 $+3\sigma$ を超える異常のパケットが観測された日までの前 10 日間のモーメント

| | 日次リターン | 条件付き分散 | 条件付き歪度 | 条件付き尖度 |
|---|---|---|---|---|
| 平均 | 0.92 | 10.80 | -0.06 | 4.07 |
| 標準偏差 | 5.22 | 5.05 | 0.28 | 0.47 |
| 歪度 | 0.81 | 1.07 | -0.68 | 5.40 |
| 尖度 | 8.03 | 3.80 | 24.27 | 37.77 |
| MIN | -10.97 | 4.72 | -2.49 | 3.89 |
| MAX | 24.78 | 28.44 | 1.77 | 8.17 |

表 5: 過去 $+3\sigma$ を超える異常のパケットが観測された日の後 10 日間のモーメント

| | 日次リターン | 条件付き分散 | 条件付き歪度 | 条件付き尖度 |
|---|---|---|---|---|
| 平均 | -0.34 | 21.10 | 0.13 | 4.44 |
| 標準偏差 | 3.74 | 25.53 | 0.97 | 2.56 |
| 歪度 | 0.79 | 2.01 | 6.44 | 8.71 |
| 尖度 | 11.27 | 6.10 | 60.99 | 90.01 |
| MIN | -16.17 | 4.57 | -4.00 | 3.89 |
| MAX | 7.43 | 127.73 | 10.04 | 33.57 |

測前後で日次リターンが反転してマイナスとなり、さらに、パケットが観測された後は条件付きボラティリティが倍程度大きくなっている。図 7 はパケットの異常値が観察された時点を 0 として、前後 20 日の累積リターンをプロットした図である。明らかに、異常値が観察された後では価格変動幅が大きくなっていることがわかる。

以上の分析から図 1 の通り、ハッキングをはじめとした何らかの Bitcoin のセキュリティ・インシデントが影響を与えている可能性を示唆する。

## 4 まとめ

本研究では、セキュリティ方面で、活用が検討されているネットワークの通信パケットを、仮想通貨市場におけるリスクを評価する上で、有効と考えられるオルタナティブ・データとして、活用した。仮想通貨を金融資産ではなく、システムとして捉え、セキュリティの観点から有効な情報を用いて価格分析を行った。

具体的には、ダークネット観測情報から得られたパケットデータの異常を検知することで、以下の事象を確認し、セキュリティ・インシデントに起因すると思われる価格変動リスクを回避できる可能性をしめした。

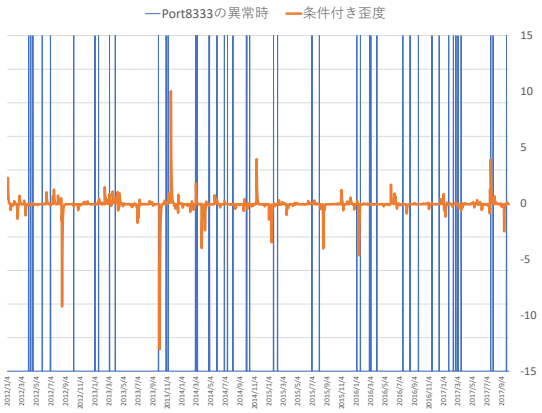


図 5: Skew

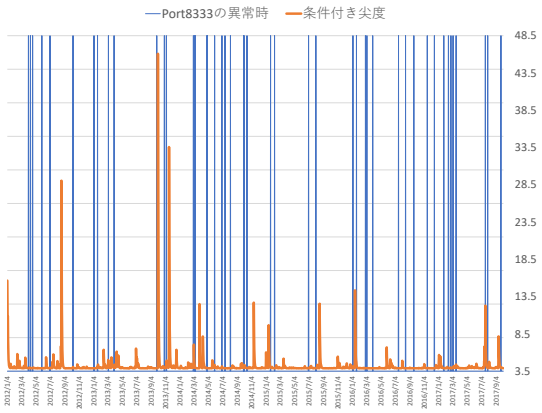


図 6: kurt

- パケットの異常観測の後、あるいは同時に条件付きモーメントがジャンプする。
- 異常観測後前後 10 日で日次リターンがマイナスになる。
- パケットが観測された後は条件付きボラティリティが倍程度大きくなる。

今後の展開としては、ダークネット観測情報を利用して、企業のセキュリティ・リスクもモニタリングすることが挙げられる。今回は Bitcoin を対象として分析のため、8333/tcp について確認したが、企業のセキュリティ・リスクとしは、well-known port と呼ばれる、一般的に特定サービス利用のためのポートを監視することで確認可能であると考える。セキュリティ・リスクが資産価格に与える影響については、主にイベント・スタディ法を用いた分析が主体であり、例えば、情報セキュリティ事故が企業価値 (株価) に与える負の影響をイベント・スタディの方法を用いて分析した研究 [26] や、脆弱性が発表されたときにソフトウェアベンダーの市場価値がどのように変化するかを検証した研究 [23] など

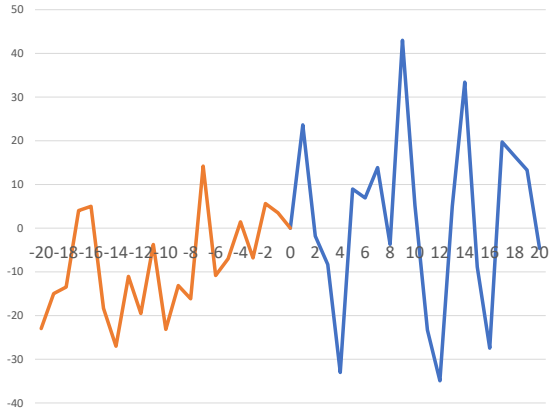

図 7: パケット異常値を基準とした累積リターン

がある。その他にも、脆弱性の発表が行われた際の株式市場の反応について纏めた研究 [22] や、ハッカーの攻撃を直接受けた企業および類似企業の株価がともに低下するといった研究報告 [14] もある。こうした情報セキュリティが株価に与える影響に関する体系的な調査をした研究 [21] では、企業の株価へのセキュリティ事象の影響の統計的有意性を報告している。

## 参考文献

[1] Ken Alabi. Digital blockchain networks appear to be following metcalfe ' s law. *Electronic Commerce Research and Applications*, Vol. 24, pp. 23–29, 2017.

[2] Tim Bollerslev. Generalized autoregressive conditional heteroskedasticity. *Journal of econometrics*, Vol. 31, No. 3, pp. 307–327, 1986.

[3] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pp. 104–121. IEEE, 2015.

[4] Marie Brière, Kim Oosterlinck, and Ariane Szafarz. Virtual currency, tangible return: Portfolio diversification with bitcoin. *Journal of Asset Management*, Vol. 16, No. 6, pp. 365–373, 2015.

[5] Bram Cohen. Incentives build robustness in bittorrent. In *Workshop on Economics of Peer-to-Peer systems*, Vol. 6, pp. 68–72, 2003.

[6] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor the second-generation onion

router. Technical report, Naval Research Lab Washington DC, 2004.

[7] Anne Haubo Dyhrberg. Bitcoin, gold and the dollar–a garch volatility analysis. *Finance Research Letters*, Vol. 16, pp. 85–92, 2016.

[8] Anne Haubo Dyhrberg. Hedging capabilities of bitcoin. is it the virtual gold? *Finance Research Letters*, Vol. 16, pp. 139–144, 2016.

[9] Robert F Engle. Autoregressive conditional heteroscedasticity with estimates of the variance of united kingdom inflation. *Econometrica: Journal of the Econometric Society*, pp. 987–1007, 1982.

[10] Claude Fachkha and Mourad Debbabi. Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization. *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 2, pp. 1197–1227, 2016.

[11] David Garcia and Frank Schweitzer. Social signals and algorithmic trading of bitcoin. *Royal Society open science*, Vol. 2, No. 9, p. 150288, 2015.

[12] James Douglas Hamilton. *Time series analysis*, Vol. 2. Princeton university press Princeton, 1994.

[13] Jordi Herrera-Joancomartí. Research and challenges on bitcoin anonymity. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pp. 3–16. Springer, 2015.

[14] Oliver Hinz, Michael Nofer, Dirk Schiereck, and Julian Trillig. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, Vol. 52, No. 3, pp. 337–347, 2015.

[15] Daisuke Inoue, Masashi Eto, Katsunari Yoshioka, Shunsuke Baba, Kazuya Suzuki, Junji Nakazato, Kazuhiro Ohtaka, and Koji Nakao. nicter: An incident analysis system toward binding network monitoring with malware analysis. In *Information Security Threats Data Collection and Sharing, 2008. WISTDCS'08. WOMBAT Workshop on*, pp. 58–66. IEEE, 2008.

[16] Paraskevi Katsiampa. Volatility estimation for bitcoin: A comparison of garch models. *Economics Letters*, Vol. 158, pp. 3–6, 2017.

[17] Philip Koshy, Diana Koshy, and Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*, pp. 469–485. Springer, 2014.

[18] Ángel León, Gonzalo Rubio, and Gregorio Serna. Autoregresive conditional volatility, skewness and kurtosis. *The Quarterly Review of Economics and Finance*, Vol. 45, No. 4, pp. 599–618, 2005.

[19] Hsin-Ke Lu, Li-wei Yang, Peng-Chun Lin, Tzu-Han Yang, and Alexander N Chen. A study on adoption of bitcoin in taiwan: using big data analysis of social media. In *Proceedings of the 3rd International Conference on Communication and Information Processing*, pp. 32–38. ACM, 2017.

[20] Nakamoto Satoshi. Bitcoin:a peer-to-peer electronic cash system. *URL:http://www.bitcoin.org/bitcoin.pdf*, 2008.

[21] Georgios Spanos and Lefteris Angelis. The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, Vol. 58, pp. 216–229, 2016.

[22] Georgios Spanos, Lefteris Angelis, and Kyriaki Kosmidou. Is the market value of software vendors affected by software vulnerability announcements? In *Strategic Innovative Marketing*, pp. 465–469. Springer, 2017.

[23] Rahul Telang and Sunil Wattal. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, Vol. 33, No. 8, pp. 544–557, 2007.

[24] 今村光良, 面和成. ダークネット観測情報を用いたビットコインネットワークの分析. SCIS2018:2018年暗号と情報セキュリティシンポジウム.

[25] 小出駿, 鈴木将吾, 牧田大佑, 村上洸介, 笠間貴弘, 島村隼平, 衛藤将史, 井上大介, 吉岡克成, 松本勉ほか. 通信プロトコルのヘッダの特徴に基づく不正通信の検知・分類手法. コンピュータセキュリティシンポジウム 2014 論文集, Vol. 2014, No. 2, pp. 48–55, 2014.

[26] 廣松毅. 情報セキュリティ事故が企業価値に与える影響の分析-イベント・スタディ分析を用いたリス

ク評価の試み. 情報セキュリティ総合科学, Vol. 3,
pp. 91–106, 2011.