ビットコイン取引履歴を利用したダークウェブ市場の解明

代表研究者　　土　屋　陽　一　　明治大学　商学部　准教授

1 はじめに

セキュリティとプライバシーを確保する技術は、オンライン活動を促進する鍵となります．しかし、これらの技術は、社会に貢献する先駆的な商品やサービスを提供する一方で、違法行為を行うためのツールを提供することにもなりかねません．特に、2 つのオンライン匿名化技術がダークウェブ市場の創設につながっています．1 つ目の技術は、ブロックチェーンに基づく完全に分散化されたデジタル通貨である Bitcoin です (Nakamoto, 2008)．ブロックチェーンと呼ばれる公開型の分散型台帳を用いてすべての取引履歴を管理することで、二重支出を防ぎ、中央管理を避けることができます．すべての取引記録は公開されていますが、ビットコインのアドレスと取引が社会における実際のアイデンティティと一致しない限り、ビットコインの支払いは匿名となります．2 つ目の技術は Tor ネットワークで、ユーザーのメッセージは、ユーザーとユーザーが訪問するウェブサイトの間のバッファとして機能する一連のリレーを経由します(Dingledine et al., 2004)．

このように、ウェブサイトは最後のリレーまでしか接続を追跡できないため、ウェブサイトの訪問者の場所を特定することは困難です．ダークウェブ上のサイトの管理者は、ウェブサイトのサーバーの場所を隠すことで、法執行機関を回避することができます．最初に成功したダークウェブ市場である Silk Road は、2011 年 2 月に開設されました．その後、数多くのダークウェブ・市場が開設されています．これらの新しいオンライン市場は、eBay や Amazon などの合法的なオンラインマーケットと多くの点で共通していますが、匿名性とセキュリティに重点を置き、身元確認のリスクを制限しています (Christin, 2013)．米連邦捜査局 (FBI) はさまざまなダークウェブ市場を閉鎖しましたが、ダークウェブ上の不正取引はすぐに再開されるため、警察の介入による影響は限定的です (Soska and Christin, 2015;Aldridge and De'cary-He'tu, 2016; Van Wegberg and Verburgh, 2018)．

多くの研究が、スクレイピングフレームワークを使用してデータを収集し、ダークウェブ市場の活動を測定しています．このアプローチ は、次のような種類の測定誤差をもたらす (Soska and Christin, 2015)．第一に、スクレイピングは常に利用できるわけではないので、スクレイピング手法はすべての情報を抽出できない可能性がある．第二に、より深刻なのは、買い手のフィードバックがベンダーとその商品の品質を示すために使用されるため、スクレイピングは実際の取引価格と数量を捕捉できない．そのため、実現した価格や数量は、掲載されているものとは異なる可能性があります．さらに、フィードバックはタイムリーではない可能性があり、スクレイピングでは特定のダークウェブ市場の全期間をカバーすることはできません．したがって、時間経過に伴う市場の発展は不正確な可能性があります．

本研究は，2011 年から 2017 年の間に運営されていた最大かつ最も活発なマーケットプレイスである Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, Abraxas, AlphaBay に焦点を当て，ビットコイン取引によるダークウェブ・マーケットプレイスを調査した数少ない研究の 1 つである．ビットコイン取引の記録は、各取引の販売量と日付に関する正確な情報を提供するため、既存研究による手法における測定誤差は回避されます．したがって、本研究で用いるアプローチは、市場の規模、発展、および時間経過による変動に関してより精確な証拠を提供し、先行研究のギャップを埋めます．特に、我々の手法は、これまで調査されていなかった市場での活動の証拠を提供します．Silk Road が保有するビットコインの残高は、ビットコインの取引記録を用いて調査されています (Meiklejohn et al., 2013)．これに対し、これまで調査されていなかったビットコイン取引管理の特徴に着目し、それを上記 7 市場に適用したものである．そのため、マーケットプレイスの活動状況だけでなく、成長や閉鎖の理由をより明確に把握することができます．

公益財団法人電気通信普及財団
研究調査助成報告書　第36号　2021年度

2 先行研究

先行研究では、スクレイピングの手法を用いて、出品数、業者数、商品カテゴリ、販売量などの市場特性を推定しています．これらの研究では、スクレイピング手法によりベンダーからのフィードバック情報を収集しているため、ベンダーの視点から見たダークウェブ市場のいくつかの側面が明らかになっています．

最も包括的な研究では、2013 年から 2015 年にかけて、35 の市場を合計 1905 回スクレイピングし、78,509 件のアイテムリストを収集しています（Soska and Christin, 2015）．市場全体の規模は、ピーク時には 65 万米ドルに達し、その後は 1 日 30 万～50 万米ドル程度で安定しており、この期間の全体の年間収益は 1 億 1,000 万～1 億 8,200 万米ドルであったことが示唆されています．業者の数は、Silk Road が開設されてから大幅に増加しており、閉鎖時には、Silk Road には合計 1400 の業者が存在していました．これは、業者だけでなく、ダークウェブ市場の競争が激化していることを示唆しています．業者ごとの売上高を見ると、1000 ドル未満の業者が全体の約 70%、1000～1 万ドルの業者が約 18%、10 万ドル以上の業者は約 2%にとどまった.100 万ドル以上の売上を上げたベンダーは 35 社しかなく、上位 1%の成功したベンダーが全売上の 51.5%を占めていました．Silk Road から AlphaBay までのデータを使用すると、これらの市場でのコモディティ化は進んだものの、これまで想定されていたより限定的なものでした（Van Wegberg et al.2018）．Silk Road については、1239 人の異なる販売者が出品した 24,385 種類のユニークな薬物が収集され、分析された（Christin, 2013）．算出された総販売量は月に 122 万米ドルで、2012 年半ばまでの年間販売量は約 1,500 万米ドルに相当していました．シルクロードの業者の多くは、市場参入から 3 カ月以内に姿を消し、サンプル期間全体で活動を続けたのはわずか 9%であったことがわかりました． さらに、シルクロードを利用する業者と買い手の数は大幅に増加し（Aldridge and De'cary-He'tu, 2014）、収益は 2012 年半ばの合計 1,440 万米ドルから、市場が閉鎖される直前の 2013 年 9 月には合計 8,970 万米ドルにまで増加したことが判明しました．年間の販売量は、2013 年には 1 億米ドル以上に増加したことが示されています（Soska and Christin, 2015）．

Silk Road 2.0、Agora、Evolution、Nucleus、Abraxas に焦点を当てた研究はわずかしかない．Silk Road 2.0 の 2014 年 2 月 28 日から 2014 年 11 月までの総販売量は、約 6,600 万米ドルと推定されています（Demant et al., 2018）．Agora については、2014 年 11 月 28 日から 2015 年 4 月 24 日までのデータが収集され（Demant et al., 2018）、総販売量は約 6100 万米ドルと推定されました．Agora のベンダー数は、2014 年秋に 1000 以上のピークに達するまで急激に増加し、その後、2015 年 1 月には 1000 以下に減少した（Soska and Christin, 2015）．Evolution については、2014 年 1 月から 2015 年 3 月までの調査で、商品数は 48,026 件、ベンダー数は 2702 件であった（Rhumorbarbe et al., 2016）． ベンダーの数は 2014 年 7 月には 1500 人程度だったが、その後急減した.その後、Agora とは対照的に増加し、2015 年 1 月には 2000 を超えている（Soska and Christin, 2015）．

AlphaBay については，2015 年 3 月 18 日から 2017 年 5 月 24 日までのデータを 27 回スクレイプで収集し（Christin, 2017），2015 年末にかけて AlphaBay が主導的な位置を占めていることがわかった．その収益はサンプル期間の終わりに向かって着実に増加し、ピーク時には Silk Road の約 2 倍に達していました．推定総収益は約 2 億 2,290 万米ドルで，取引の総価値は約 220 万円であった．さらに、2015 年 5 月から 2017 年 2 月までの AlphaBay での活動が推定された（United States District Court, 2017）．AlphaBay に関連するビットコインアドレスで行われた取引は 400 万件以上であった．そのため，AlphaBay には約 4 億 5000 万米ドルが入金されていました．一方，法的機関は，2016 年 4 月にミキサーサービスが導入され，ビットコインのウォレットアドレスが 34 万以上あったことを明らかにした． Tzanetakis（2018）は，2015 年 9 月から 2016 年 8 月までの薬物取引に着目してデータ収集を行った．薬物部門の総売上高は、サンプル期間中に 9,398 万米ドルと試算された．月間売上高は、2015 年 9 月の 0.14 百万米ドルから 2016 年 8 月の 16.05 百万米ドルのピークまで着実に増加した．

2017 年 1 月から 2018 年 3 月の間にダークウェブにおける暗号通貨の用途を調査した最近の研究があります（Lee et al.、2019 年）．彼らは、収集した暗号通貨アドレスの 99.8%をビットコインが占め、そのうち 80%が違法な目的で使用されていることを発見しました．また、市場規模は約 1 億 8000 万米ドルと推定している．Foley et al.（2019）は、2009 年 1 月 3 日から 2017 年 4 月末までのビットコイン取引を調査し、ネットワーククラスタ分析と検出制御推定と呼ばれる回帰アプローチによって違法行為を推定しました．それによると、年間約 760 億米ドル相当のビットコインがダークウェブの市場で使用されており、ビットコイン

取引全体の 46%を占めていました.

3 測定方法

3-1 ビットコイン取引

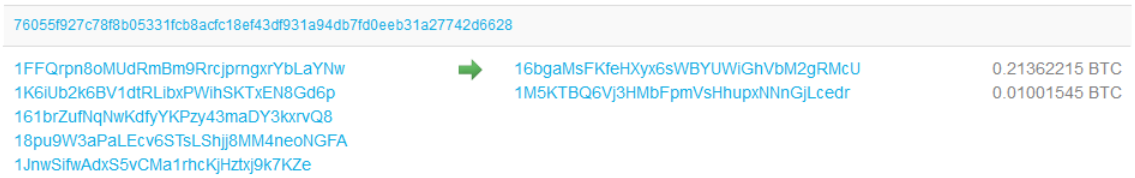
測定方法を紹介する前に、AlphaBay アドレスを使ってビットコイン取引を記録する方法を紹介します. ビットコインのユーザは, 任意の数のビットコインアドレスを含むことができるウォレットを持っています. 各アドレス *adr* は, 変換関数を介して, 一意の公開鍵/秘密鍵ペアにマッピングされる. 送信者のアドレス$\boldsymbol{a_s}$と受信者のアドレス$\boldsymbol{a_r}$との間の取引は, 次のような形式で行われる.

$\tau_h(\boldsymbol{a_s} \to \boldsymbol{a_r}) = \{S,\ \boldsymbol{B}, \boldsymbol{a_r}, sig_{sk(\boldsymbol{a_s})}(S,\ \boldsymbol{B}, \boldsymbol{a_r})\}$. ここで、$sig_{sk(\boldsymbol{a_s})}$は$\boldsymbol{a_s}$の公開鍵に対応する秘密鍵$sk(\boldsymbol{a_s})$を用いた署名、$\boldsymbol{B}$は$\boldsymbol{a_r}$に送金されたビットコイン(BTC)の量、$h$はビットコインネットワーク上で取引の有効性が確認された時間（ブロックの高さで表示)、Sは$\boldsymbol{a_s}$が B の BTC を取得した直近の取引の参照である. なお、ビットコイン保有者や取引のプライバシーを守るため、ウォレットの情報は公開していません.

図 1 は、各ビットコインの取引がどのように記録されるかを示したものである. 左側に 5 つのビットコインアドレス$\boldsymbol{a_s}$があり、これが入力となる. 右側には出力として 2 つのビットコインアドレス$\boldsymbol{a_r}$があります. 左側の入力のアドレス$\boldsymbol{a_s}$から右側の出力のアドレス$\boldsymbol{a_r}$への取引が行われていることがわかります. 前者の出力のアドレスには 0.21BTC が、後者のアドレスには 0.01BTC が入りました. 入力を設定するためには, ユーザはアドレスの秘密秘密鍵$sk(\boldsymbol{a_s})$を知る必要があり, 複数のアドレスを持っているユーザはその秘密秘密鍵を管理している. したがって、1 つの取引で入力として記録されたアドレスは、同じユーザーが所有していることになります（Reed & Harrigan, 2013). これは、ダークウェブ市場での取引を識別するために使用された最初のヒューリスティックであり、これまでの研究でも使用されています（Androulaki et al., 2013)

ヒューリスティック 1.　2 つ以上のアドレスが同じトランザクションに入力されている場合、それらは同じユーザーによって所有されています. つまり、任意のトランザクションτ_hについて、すべての$adr \in \boldsymbol{a_s}$は同じユーザーによって所有される.

図 1. ビットコイン取引



3-2 ダークウェブ市場の取引測定

違法な商品やサービスを購入するために、ユーザーは自分のビットコインをサイトのビットコインアドレスに送金します. ユーザーから送金されたビットコインは、取引が完了するまでエスクローに保管されます. 取引が完了し、市場が手数料を取った後、市場はビットコインをベンダーに送ります.

ビットコイン取引によってダークウェブ市場の取引を特定するためには、これらの市場が所有するビットコインアドレスが必要です. ダークウェブ・市場が所有するビットコインアドレスの一部は、コミュニティの自主的な取り組みや法的機関が採用した措置により公開されています. 各市場が所有する既知のアドレスのセットをadr_{market}とします. なお、管理者はエスクローのためにビットコインアドレスの情報をユーザーや業者に送っています. そのため、彼らのビットコインアドレスは公開されている可能性が高い. これらの既知のアドレスは出発点であり、次のステップは、これらの市場が所有する他の未知のアドレスがあるかどうかを確認し、必要に応じてそのような未知のアドレスを見つけることである.

そのために、各市場が所有する既知のアドレス間の内部取引を調べる. 具体的には、adr^i_{market}、

$adr^{j}_{market} \in adr_{market}(i \neq j)$ のような任意のアドレスが与えられた場合、取引

$\tau_h(\boldsymbol{a_s} \rightarrow \boldsymbol{a_r}) = \{S,\ \boldsymbol{B}, \boldsymbol{a_r}, sig_{sk(a_s)}(S,\ \boldsymbol{B}, \boldsymbol{a_r})\}$で$adr^{i}_{market} \in \boldsymbol{a_s}$から$adr^{j}_{market} \in \boldsymbol{a_r}$に送金されたビットコイン

$B^j \in \boldsymbol{B}$を特定します．各市場のアドレス間のビットコイン取引を調査すると、図 1 にもあるように、0.01BTC を相互に送受信するという単純なパターンが得られる．つまり，例えば，AlphaBay が所有する Bitcoin アドレスを入力とし，同じく AlphaBay が所有する他の Bitcoin アドレスとの取引を出力として，0.01BTC の取引に関連した取引を探すのである．

AlphaBay については、0.01BTC の取引が内部取引全体の 98.1%を占め、0.1BTC 以上の取引が 1.2%を占めていることがわかります．その他の市場でも、各ダークウェブ市場が所有するアドレス間の内部取引は同様の分布を示しています．表 2 は、Evolution を除くすべての市場で、0.01BTC の取引が内部取引全体の 85%以上を占めていることを示しています．驚くべきことに、0.1BTC 以上のビットコイン取引は、Evolution を除くすべての市場の内部取引のうちせいぜい 10%程度です．ここで、ダークウェブ・市場の取引を識別するために使用される第 2 のヒューリスティックは、以下のように定式化されます．

ヒューリスティック 2.　あるアドレスが、ダークウェブ市場の既知のアドレスを出力(インプット)として 0.01BTC を受け取る(送る)取引の入力(アウトプット)となっている場合、入力(アウトプット)のアドレスはダークウェブ市場が所有している．つまり、$adr^{i} \in \boldsymbol{a_s}(\boldsymbol{a_r})$が任意の$adr^{j}_{market} \in adr_{market}$と$adr^{j}_{market} \in \boldsymbol{a_r}(\boldsymbol{a_s})$に対して、取引$\tau_h(\boldsymbol{a_s} \rightarrow \boldsymbol{a_r}) = \{S,\ \boldsymbol{B}, \boldsymbol{a_r}, sig_{sk(a_s)}(S,\ \boldsymbol{B}, \boldsymbol{a_r})\}$ $(B^j(\in \boldsymbol{B}) = 0.01$を満たし）に現れた場合、$adr^{i}$はダークウェブ市場が所有している．

7 つのダークウェブ市場で 0.01BTC の内部取引のパターンが観察されたことから、これらのダークウェブ市場では、ビットコインの管理に同じソフトウェアを使用していることが示唆されます．0.01BTC を送信する目的は、ユーザーの取引を匿名化して安全に行うためだと考えられます．この目的のために、当時から bitwasp が利用されていました．さらに、bitwasp は「シルクロードのような」ソフトウェアと呼ばれており、ダークウェブの市場を立ち上げるための主要なツールは他に導入されていない．これは、Silk Road の後に立ち上げられた 6 つの市場が、Silk Road の遺産を継承していることを示唆しているが、それらの市場が bitwasp を使用していたことを特定するのは難しい 6 つの市場が Silk road 的であるという根拠は、0.01BTC の内部取引という機能が、必要ではないがすべての市場に共通していたからである．7 つの市場のビットコインアドレスは、WalletExplorer から取得しています．WalletExplorer は有用なソースを提供しており、最近では学術研究でも使用されています（Toyoda et al.2018; Foley et al.2019; Lian et al.2019）．

次のステップは、このような市場が所有する未知のアドレスが他にもあるかどうかを確認し、必要に応じてこれらの未知のアドレスを見つけることです．自身のアドレス間での 0.01BTC の取引はほぼ閉じられています．つまり、それぞれの市場が所有しているこれらのアドレスが、所有していないアドレスと 0.01BTC の取引をすることはほとんどありません．Silk Road が所有する既知のアドレスは 350,036 件です．Silk Road が所有するこれらの既知のアドレスから非所有のアドレスへ（から）0.01BTC が送信（受信）された取引の平均数は 0.037 です．したがって、公的な取り組みによって明らかになったこのようなアドレスは、7 つの市場が所有するすべてのアドレスとして特定されます．これらのアドレスをもとに、そのアドレスを出力先とする市場外のアドレスとの取引を追跡し、その市場での購入を特定することができます．市場での購入を特定するためのヒューリスティックを以下のように定義する．

ヒューリスティック 3. ダークウェブ市場が所有していないアドレスを入力とする取引が，ダークウェブ市場が所有するアドレスを出力とする場合，そのような取引は，それらの市場での購入として識別される．

つまり、$\tau_h(a_s \to a_r) = \{S,\ B, a_r, sig_{sk(a_s)}(S,\ B, a_r)\}$が$adr^i \in a_s$、$adr^i \notin adr_{market}$となる場合、$\tau_h(a_s \to a_r)$はダークウェブ市場での購入と識別されます.

市場が所有する既知のアドレスの外にある 0.01BTC の取引は，誤認識のリスクがあるため，追跡されません．これらのダークウェブ・市場とは関係のない 0.01BTC の取引が行われることもあります．0.01BTC の合法的な取引が行われることもあります．6 つの市場での取引はヒューリスティック 3 を使用して識別し、米ドル換算のビットコイン価格を使用して米ドルでの販売量を推定します.各取引の販売量を計算するために、取引日のビットコイン価格の終値を使用します．ある日のすべての取引を集計し、その日のビットコイン価格を乗じることで、各市場における 1 日の販売量が算出されます．月間販売量は、月内の毎日の販売量を集計して算出します.

4 結果

4-1 月間取引

ダークウェブ市場の総販売量は､Silk Road では 2012 年 6 月から 2013 年 10 月の間に 1 億 9,270 万米ドル、AlphaBay では 2014 年 12 月から 2016 年 2 月の間に 1 億 6,600 万米ドルとなっています．これに対応して、Silk Road 2.0 では 1 億 1,290 万米ドル、Agora では 2 億 2,070 万米ドル、Evolution では 6,970 万米ドル、Nucleus では 8,830 万米ドル、Ablaxas では 3,560 万米ドルが全期間にわたって販売されています．また，観測期間中の平均月間販売額は，Silk Road が 1,070 万米ドル，Silk Road 2.0 が 870 万米ドル，Agora が 1,050 万米ドル，Evolution が 470 万米ドル，Nucleus が 490 万米ドル，Abraxas が 300 万米ドル，AlphaBay が 1,100 万米ドルとなっています．AlphaBay は，2017 年 6 月まで運用を継続しており，観測期間終了後もさらに大きな売上を上げているように見えた．したがって，AlphaBay は，閉鎖されるまで最も成功したダークウェブ市場であったと思われます．我々の結果は，これまでの研究とおおむね一致しており，また新たな知見も得られた．これらのダークウェブ市場を含めた我々の推定値は，2013 年に 1 億 6,100 万米ドル，2014 年に 2 億 2,700 万米ドル，2015 年に 3 億 6,600 万米ドルでした．また、これらの推定値は、2014 年と 2015 年に確認されたダークウェブ市場が、それぞれ 2 億 5400 万米ドルと 3 億 5700 万米ドル相当のビットコインを獲得したことを確認しています（CHAINALYSIS，2019）.

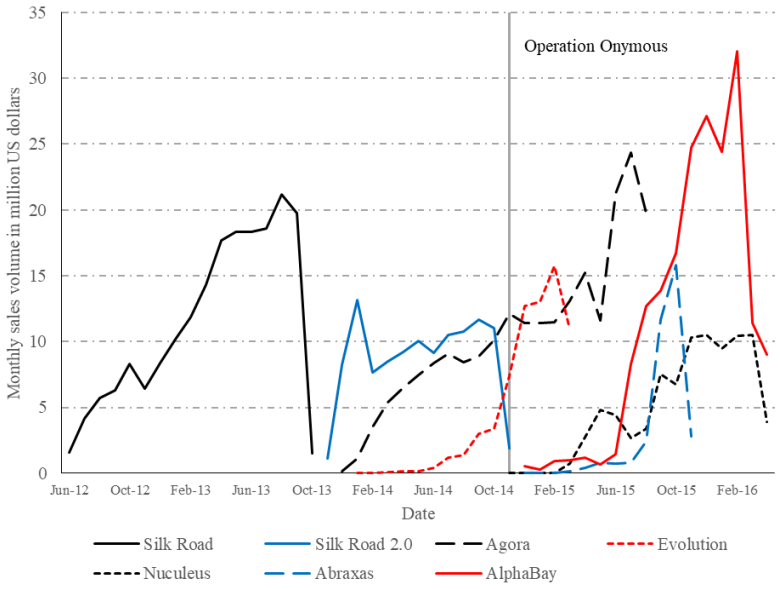
図 2 は、各市場の月ごとの販売量を時系列で示したものです．各市場の収益が時間の経過とともにどのように発展したか、また市場間で主導的な地位がいつどのように変化したかが明確に示されています．Silk Road は順調に成長し、Silk Road 2.0 は急速に成長し、Silk Road の閉鎖後の 2014 年 1 月に 1300 万米ドル以上のピークを迎えました．Agora は 2013 年 12 月に運営を開始し、2014 年 11 月には月次売上高が 1,200 万米ドルを超えるなど順調に成長し、2014 年 12 月には Evolution の月次売上高が Agora を上回りました．Evolution は 2014 年 1 月に運用を開始しましたが、その月次売上高は運用開始当初は少なかったです．2014 年後半から Evolution の存在感が急激に高まり、2014 年 12 月には月次販売量が Agora を上回り、2015 年 2 月までトップの座にありました.

Evolution の急成長は、Operation Onymous によって多くのダークウェブ市場が閉鎖されたことに起因している．Evolution の月間販売量は、2014 年 10 月の 340 万米ドルから 2014 年 11 月の 740 万米ドルへと 2 倍以上に増加しました．このような市場の参加者が他の市場に移動するだけであることが観察されるように（Van Wegberg & Verburgh，2018）、ユーザーは当時比較的小規模な市場であった Evolution に移動したようです．なお、ユーザーの移動は直接観察することができないため、月次の販売量から推測されている ．Agora の月間販売量は，2014 年 10 月から 11 月にかけて約 20%増加したが，すでに大規模な市場となっていたことや，参加者が逮捕されることを恐れたためか，その後数か月間停滞した．Evolution のピーク時の月間販売量は、2015 年 2 月に 1,500 万米ドルを超えていました．しかし､2015 年 3 月に Evolution の退場詐欺が発生した後、Evolution の参加者が Agora に移行したと思われることから、Agora は首位の座を奪還し、その月間販売量は再び増加に転じ、2015 年 7 月にはピークの 2,500 万米ドルを超えました.

Nucleus は 2013 年 11 月、Abraxas は 2013 年 12 月に運用を開始しました．Nucleus は Evolution の退出詐欺の後に急成長し，2015 年 3 月から 6 月までの総販売量は AlphaBay のそれを上回った．Abraxas の月次販売

量は 2015 年 9 月に急激に増加した．AlphaBay は 2014 年 12 月に運営を開始しました．Agora が自主的に撤退した後の 2015 年に，AlphaBay が最大かつ最も人気のある市場になったことは明らかである．AlphaBay の月間販売量は，6 月に Agora の月間販売量が急増した 1 か月後の 2015 年 7 月に急増した．これは主に Evolution からのユーザーの移行によるものである．AlphaBay は，Agora の閉鎖後に急成長し，Abraxas の閉鎖後にさらに成長したが，これもユーザーの移行を示している．また，Agora ユーザーが Abraxas に移行したことも考えられます．AlphaBay の月間販売量は 11 月に 2,000 万ドルを超え，2016 年 2 月には 3,000 万ドルを超えるピークを迎えているが，これは Agora の月間販売量が 2,000～2,500 万ドル程度，Abraxas の月間販売量が 1,000～1,500 万ドル程度であった活動の多くが AlphaBay に移行したことと整合的である（The Economist, 2017）．

図 2.　月間取引の推移



4-2 曜日・時間の分析

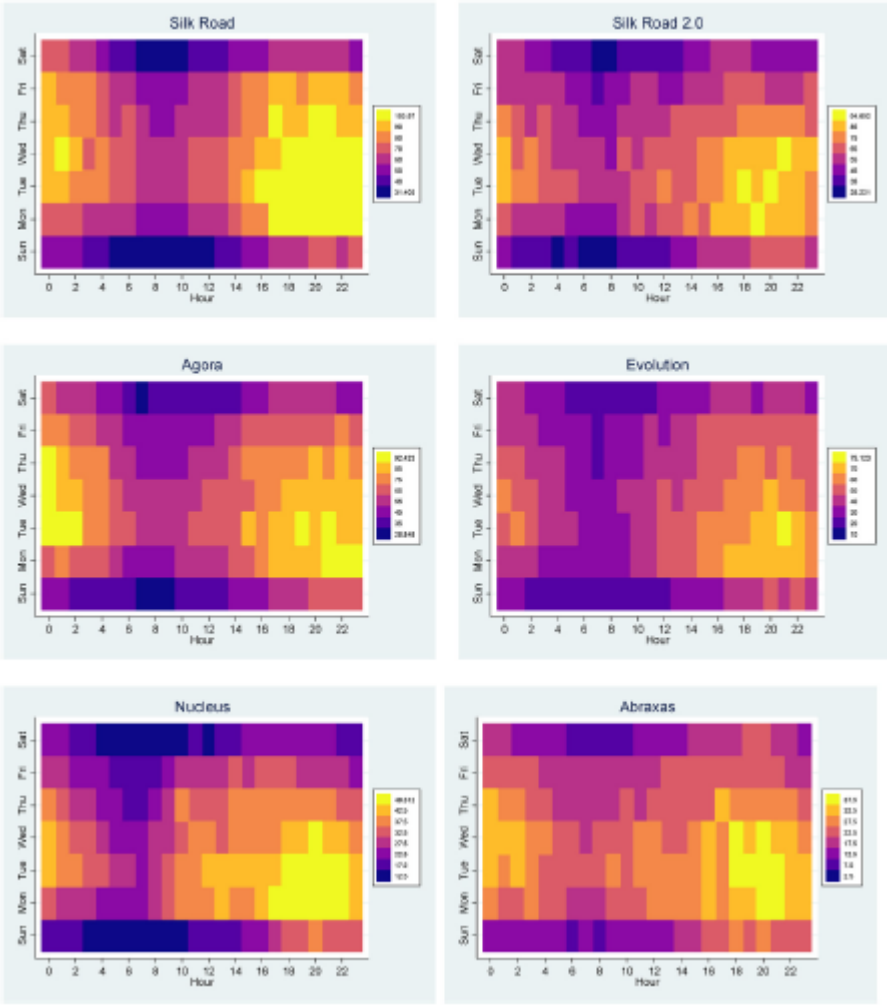
図 3 は、具体的な時間帯別、曜日別の取引パターンを調べたヒートマップです．図 3 を見ると、時間帯別では UTC 0 と 2 の間と UTC 18 と 22 の間におおよそ 2 つのピークがあることがわかります．先行研究によると、欧米諸国のダークウェブ市場では不正薬物の取引が多いとされています．このことから、この 2 つの取引量のピークは、アメリカやヨーロッパの国々での取引に起因するものと考えられます．1 日の取引パターンが米国と欧州で大きく異なることは考えられません．したがって、暗号市場での違法薬物取引が最も活発な国や地域では、夜間に取引が行われていることがわかります．イギリスや、ドイツ、オランダなどのヨーロッパ諸国では、取引のピークは夜から深夜にかけてです．米国およびカナダでは、UTC 0 から UTC 2 の間がピークとなり、それぞれ太平洋時間で午後 4 時から午後 6 時、東部時間で午後 7 時から午後 10 時に相当します．オーストラリアの場合、夜間は 2 番目に取引が活発な時間帯である UTC10 から UTC16 の間に相当し、オーストラリアのタイムゾーンでは午後 9 時から午前 3 時にあたります．オーストラリアでは、暗号市場における違法薬物市場がある程度大きくなっているにもかかわらず、ヨーロッパ諸国や米国では、そのシェアがはるかに大きいようです．

図 3 を見ると，月・火・水に取引が集中し，土・日には取引が少ないことがわかる．これは、Ladegaard（2019）が、Agora と Evolution での薬物取引が日曜日に著しく減少したという証拠を示したことと一致します．したがって、月曜から水曜の夜間は取引が多く、土日は一日中取引が少ないということになります．Ladegaard（2019）が示唆するように、ダークウェブ市場の買い手は週末までに受け取るために週の早い段階で薬物を購入し、ユーザーは週末や休日に薬物を購入する可能性が高い．実際、Thomas ら（2012）は、ヨーロッパの 19 都市を対象とした包括的な調査を通じて、金曜日と土曜日に違法薬物の使用が著しく増加することを明らかにしています．さらに、Otterstatter ら（2016）は、カナダのブリティッシュ・コロンビア州の

日次死亡率データを用いて、違法薬物の過剰摂取による 1 日の平均死亡率が土日で 0.8 を超えており、平均死亡率が最大でも 0.6 である平日よりも高いことを明らかにしました．これは、薬物使用者が休日にも薬物を使用していることを示しています．

研究結果は、ダークウェブユーザーが月曜から水曜の間に、休日に個人的に使用するためにダークウェブ市場で薬物を購入していることを示唆しており、また、ダークウェブ市場で購入した商品、特に薬物は個人的に使用するものであることを示唆しており、Aldridge and Décary-Hétu (2016)、Barratt ら (2016)、Demant ら (2018) と一致しています．さらに、ユーザーはオフィスや学校にいるときはダークウェブにアクセスできず、家に帰ってからそのようなサイトにアクセスするようです．この発見は、ダークウェブ市場で購入される薬物はほとんどが小売用であり、転売や卸売目的ではないことを示す多くの証拠と一致します．例えば、Dolliver (2015) は、2014 年 8 月から 9 月にかけて、Silk Road 2.0 は主に麻薬市場ではなかったことを示しています．このことから、ダークウェブ市場にアクセスする目的は違法薬物の購入ではないものの、ユーザーはそのようなサイトを利用しているところを見られないように慎重になっていると考えられます．

図 3.　平均取引量のヒートマップ



4-3 コインチェック事件の分析

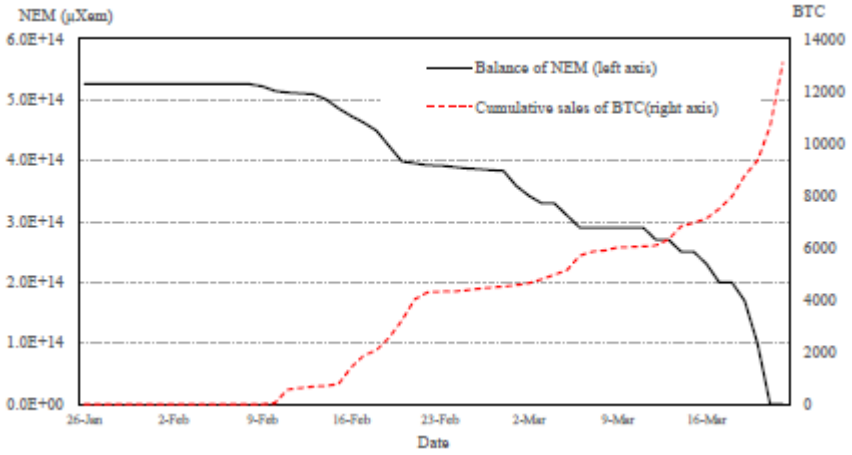
図 4 は、販売が低迷している時期と販売が増加している時期が交互にやってくるという明確なパターンを示しています．2 月 12 日以前は、盗まれた NEM はほとんど売れませんでした．盗まれた NEM は 2 月 13 日と 2 月 19 日に急速に販売され、その後 2 月 27 日まで販売は再び停滞しました．2 月末から 3 月 5 日までの期間は販売数が増加し、3 月 6 日から 3 月 10 日までは販売数が停滞しました．3 月 11 日からは、盗まれた NEM の販売量が増加しています．皮肉なことに、NEM.io 財団がモザイクタグシステムを無効化したと発表した 3

月 20 日には、盗まれた NEM の 10%以上が売却され、3 月 21 日にはさらに約 20%の盗まれた NEM が売却されたことから、追跡機能の無効化を発表した直後の 2 日間で、約 30%がマネーロンダリングされたことになります．その後、ハッカーは 3 月 22 日に盗まれた NEM が完売したことを発表しました．

観察された販売パターンは、購入者がダークウェブ市場への信頼を得た後に、慎重に、さらには積極的に盗まれた NEM を購入したというもので、ダークウェブ市場に関するこれまでの研究と概ね一致しています．これまでの研究では、ダークウェブ市場の利用者は詐欺に遭うことを懸念していることがわかっています．詐欺や不正行為は、ダークウェブ市場で広く利用されている可能性が高く、ハッキングの試みの餌食になります．サイト管理者は、フォーラムの投稿など複数のソースを使ってさまざまな種類のダークウェブ市場の窃盗や詐欺を探った後、ユーザーの資金を持ち逃げすることがあります．先行研究と同様に、盗まれた NEM の購入者は、当初、ハッカーからの申し出で詐欺に遭わないように慎重になっていました．しかし、さまざまなフォーラムや投稿を参考にしたり、少量の盗難 NEM を購入したりしているうちに、購入者はハッカーの申し出を信用するようになり、時間の経過とともに購入量が増えていきました．ダークウェブ市場の取引所が信頼を得たことで、より多くの買い手が現れ、その買い手が購入額を増やしていったと考えられます．市場運営の最後の 2 日間で、盗まれた NEM の約 3 分の 1 がマネーロンダリングされました．おそらく、NEM.io 財団が無効化されたトラッキングについて発表したことで、より多くの買い手が購入し、より大きな取引が行われたのだと思われます．

また、マネーロンダリングの大半はビットコインで行われたと推定される．盗まれた NEM がダークウェブ市場で交換された総額は、取引市場のレートで 226 億円（2 億 600 万ドル）と推定されます．これは、事件後に NEM の為替レートが大幅に下落したため、事件当時の市場レートによると盗難額の半分以下となります．また、ビットコインに交換された総額は、151 億ドル（1 億 3700 万ドル）と推定されます．これは、盗まれた NEM の 3 分の 2 がビットコインでマネーロンダリングされたことを意味し、3 分の 1 は Lightcoin などの暗号通貨でマネーロンダリングされたと推定されます．3 分の 2 という推定値は、違法な目的でのビットコインの使用に関する先行研究と一致しています．

図 4.　NEM 残高とビットコイン販売



5 おわりに

本研究では、ビットコイン取引を通じて、ダークウェブ市場取引を測定しました．その結果、利用者は、1 つの市場が閉鎖されても別の市場に移動すること、さらに、小売目的の麻薬取引が大部分を占めていること、が判明しました．また、国際的な司法機関による取り締まり活動は，これらの市場の利用者を混乱はさせているものの，短期的にも利用者の活動を抑止することはできなかったことが示されました．ダークウェブ市場の閉鎖を目的とした取り締まりは効果的ではなく、購入者や販売者を逮捕することが効果的であることを示唆しています．さらに、暗号通貨取引所がアカウント開設時に新規ユーザーの身元を確認する国際的な司法機関や政策的な協調・協同が強く求められることも示唆される．

【参考文献】

Aldridge, J., Askew, R., 2017. Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. Int. J. Drug Pol. 41, 101-109.

Aldridge, J., De'cary-He'tu, D., 2014. Not an 'Ebay for drugs': the cryptomarket 'silk road' as a paradigm shifting criminal innovation (May 13, 2014). Available at: SSRN. https://ssrn.com/abstract¼2436643. https://doi.org/10.2139/ssrn. 2436643 (accessed 26 April 2019) [Online].

Aldridge, J., De'cary-He'tu, D., 2016. Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets. Int. J. Drug Pol. 35, 7-15.

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security, pp. 34-51.

Barratt, M.J., 2012. Silk road: ebay for drugs. Addiction 107(3), 683-683.

Barratt, M.J., Ferris, J.A., Winstock, A.R., 2016. Safer scoring? Cryptomarkets, social supply and drug market violence. Int. J. Drug Pol. 35, 24-31.

Bashir, I., 2018. Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained. Packt Publishing Ltd.

Bhaskar, V., Linacre, R., Machin, S., 2019. The economic functioning of online drugs markets. J. Econ. Behav. Organ. 159, 426-441.

Brose'us, J., Morelato, M., Tahtouh, M., Roux, C., 2017. Forensic drug intelligence and the rise of cryptomarkets. Part i: studying the Australian virtual market. Forensic Sci. Int. 279, 288-301.

Brose'us, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., De'cary-He'tu, D., 2016. Studying illicit drug trafficking on darknet markets: structure and organisation from a Canadian perspective. Forensic Sci. Int. 264, 7-14.

Chainalysis, 2019. Decoding increasingly sophisticated hacks, darknet markets, and scams. Crypto Crime Report.

Christin, N., 2013. Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd International Conference on World Wide Web, pp.213-224.

Christin, N., 2017. An EU-Focused Analysis of Drug Supply on the AlphaBay Marketplace. EMCDDA Commissioned Paper. Disponible sur http://www.emcdda. europa. eu/document-library/eu-focused-analysisdrug-supply- alphabay-marketplace_en. (Accessed 26 April 2019) [Online].

Cunliffe, J., Martin, J., De'cary-He'tu, D., Aldridge, J., 2017. An island apart? Risks and prices in the Australian cryptomarket drug trade. Int. J. Drug Pol. 50, 64-73.

Dalins, J., Wilson, C., Carman, M., 2018. Criminal motivation on the dark web: a categorisation model for law enforcement. Digit. Invest. 24, 62-71.

De'cary-He'tu, D., Giommoni, L., 2017. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous. Crime Law Soc. Change 67(1), 55-75.

De'cary-He'tu, D., Paquet-Clouston, M., Aldridge, J., 2016. Going international? Risk taking by cryptomarket drug vendors. Int. J. Drug Pol. 35, 69-76.

Demant, J., Munksgaard, R., Houborg, E., 2018. Personal use, social supply or redistribution? Cryptomarket demand on silk road 2 and agora. Trends Organ. Crime 21(1), 42-61.

Dingledine, R., Mathewson, N., Syverson, P., 2004. Tor: The Second-Generation Onion Router. Naval Research Lab, Washington DC.

Dolliver, D.S., 2015. Evaluating drug trafficking on the tor network: silk road 2, the sequel. Int. J. Drug Pol. 26 (11), 1113-1123.

European Monitoring Centre for Drugs and Drug Addiction, 2013. EU Drug Markets Report: A Strategic Analysis. Publications Office of the European Union.
Europol, 2014. Global action against dark markets on tor network. https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network (accessed 6 May 2019) [Online].
Europol, 2017a. Drugs and the darknet: perspectives for enforcement, research and policy. https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy (accessed 6 May 2019) [Online].
Europol, 2017b. Massive blow to criminal dark web activities after globally coordinated operation. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (accessed 6 May 2019) [Online].
Foley, S., Karlsen, J.R., Putnin¸ T.J., 2019. Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? Rev. Financ. Stud. 32 (5), 1798-1853.
Greenberg, A., 2013. Silk road competitor shuts down and another plans to go offline after claimed $6 million theft. https://www.forbes.com/sites/andygreenberg/2013/12/01/silk-road-competitor-shuts-down-and-another-plans-to-go-offline-after-6-million-theft/#1388af767e08 (1 December 2013)
(accessed 2 August 2020) [Online].
Hall, W., Weier, M., 2015. Assessing the public health impacts of legalizing recreational cannabis use in the USA. Clin. Pharmacol. Ther. 97 (6), 607-615.
Hiramoto, N., Tsuchiya, Y., 2020. Measuring dark web marketplaces via bitcoin transactions: from birth to independence. Forensic Sci. Int.: Digit. Invest. 35, 301086.
Interpol, 2015. Pharmaceutical crime on the darknet. A study of illicit online marketplace. https://www.gwern.net/docs/sr/2015-interpol-pharmaceuticals. pdf (accessed September 1 2020) [Online].
Jardine, E., Lindner, A.M., 2020. The dark web and cannabis use in the United States: evidence from a big data research design. Int. J. Drug Pol. 76, 102627.
Ladegaard, I., 2019. Crime displacement in digital drug markets. Int. J. Drug Pol. 63, 113-121.
Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., Son, S., Shin, S., 2019. Cybercriminal minds: an investigative study of cryptocurrency abuses in the dark web. In: Network and Distributed Systems Security (NDSS) Symposium 2019.
Liang, J., Li, L., Luan, S., Gan, L., Zeng, D., 2019. Bitcoin exchange addresses identification and its application in online drug trading regulation. In: Pacific Asia Conference on Information Systems (PACIS 2019).
Mardia, K., Kent, J., Bibby, J., 1979. Multivariate Analysis. Academic Press Inc, London.
Martin, J., 2014. Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs. Springer.
Masson, K., Bancroft, A., 2018. 'Nice people doing shady things': drugs and the morality of exchange in the darknet cryptomarkets. Int. J. Drug Pol. 58, 78-84.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., Mccoy, D., Voelker, G.M.,
Savage, S., 2013. A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference, pp. 127-140.
Moeller, K., Munksgaard, R., Demant, J., 2017. Flow my FE the vendor said: exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. Am. Behav. Sci. 61 (11), 1427-1450.
Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system. https://bitcoin. org/bitcoin.pdf (Accessed 20 March 2019) [Online].
Norbutas, L., 2018. Offline constraints in online drug marketplaces: an exploratory analysis of a cryptomarket trade network. Int. J. Drug Pol. 56, 92-100.

Otterstatter, M.C., Amlani, A., Guan, T.H., Richardson, L., Buxton, J.A., 2016. Illicit drug overdose deaths resulting from income assistance payments: analysis of the 'check effect' using daily mortality data. Int. J. Drug Pol. 33, 83-87.

Reid, F., Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. In: Security and Privacy in Social Networks. Springer, pp. 197-223.

Reuter, P., Kleiman, M.A., 1986. Risks and prices: an economic analysis of drug enforcement. Crime Justice 7, 289-340.

Rhumorbarbe, D., Staehli, L., Brose'us, J., Rossy, Q., Esseiva, P., 2016. Buying drugs on
a darknet market: a better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. Forensic Sci. Int. 267, 173-182.

Seber, G.A., 2009. Multivariate Observations. John Wiley & Sons.

Soska, K., Christin, N., 2015. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In: 24th USENIX Security Symposium (USENIX Security 15), pp. 33-48.

Steel, C.M.S., 2019. Stolen identity valuation and market evolution on the dark web. Int. J. Cyber Criminol. 13, 70-83.

Thomas, K.V., Bijlsma, L., Castiglioni, S., Covaci, A., Emke, E., Grabic, R., Hern'andez, F.,
Karolak, S., Kasprzyk-Hordern, B., Lindberg, R.H., Lopez De Alda, M., Meierjohann, A., Ort, C., Pico, Y., Quintana, J.B., Reid, M., Rieckermann, J., Terzic, S., Van Nuijs, A.L.N., De Voogt, P., 2012. Comparing illicit drug use in 19 European cities through sewage analysis. Sci. Total Environ. 432, 432-439.

Toyoda, K., Ohtsuki, T., Mathiopoulos, P.T., 2018. Multi-class bitcoin-enabled service identification based on transaction history summarization. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp.1153-1160.

The Economist, 2017. Two of the biggest dark-web markets have been shut down. https://www.economist.com/graphic-detail/2017/07/21/two-of-the-biggest-dark-web-darkets-have-been-shut-down (Accessed 15 January 2019) [Online].

Tzanetakis, M., 2018. Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. Int. J. Drug Pol. 56, 176-186.

Tzanetakis, M., Kamphausen, G., Werse, B., Von Laufenberg, R., 2016. The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. Int. J. Drug Pol. 35, 58-68.

United States District Court, 2017. United States of America vs. Alexandre Cazes- verified complaint for foreiture inrem. United States District Court, eastern District of California. https://www.justice.gov/opa/press-release/file/982821/ download (Accessed 24 January 2019) [Online].

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., Roxburgh, A., 2017. The recovery of online drug markets following law enforcement and other disruptions. Drug Alcohol Depend. 173, 159-162.

Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., Burns, L., 2016a. Who sells what? Country specific differences in substance availability on the agora cryptomarket. Int. J. Drug Pol. 35, 16-23.

Van Buskirk, J., Roxburgh, A., Bruno, R., Naicker, S., Lenton, S., Sutherland, R., Whittaker, E., Sindicich, N., Matthews, A., Butler, K., 2016b. Characterising dark net marketplace purchasers in a sample of regular psychostimulant users. Int. J. Drug Pol. 35, 32-37.

Van Hout, M.C., Bingham, T., 2013. 'Surfing the silk road': a study of users' experiences. Int. J. Drug Pol. 24 (6), 524-529.

Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C.H., Klievink, B., Christin, N., Van Eeten, M., 2018. Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets. In: 27th USENIX Security Symposium (USENIX Security 18), pp.1009-1026.

Van Wegberg, R., Verburgh, T., 2018. Lost in the dream? Measuring the effects of operation bayonet on vendors migrating to dream market. In: Proceedings of the Evolution of the Darknet Workshop, pp. 1-5.

Woolf, N.. Bitcoin 'exit scam': deep-web market operators disappear with $12m. https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars (18 March 2015). (accessed July 21.2020).

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Measuring dark web marketplaces via Bitcoin transactions: From birth to independence	Forensic Science International: Digital Investigation	2020 年 12 月
Dark web in the dark: Investigating when transactions take place on cryptomarkets	Forensic Science International: Digital Investigation	2021 年 3 月