複数の仮想通貨ネットワーク情報を用いたシステムおよび運用におけるリスクの調査

リスク工学グループ演習 8 班
西 貴弘　南 翔　向 渓子　渡辺 春菜
アドバイザー教員　面 和成

1. はじめに

Bitcoin をはじめとする仮想通貨は世界で大きな話題となっており，仮想通貨チャートを配信しているコインマーケットキャンプ[1]によると，2018 年 10 月 8 日現在，2042 種類の通貨が存在する．仮想通貨全体の時価総額は約 25 兆円となっており，非常に大きな市場となっている．

仮想通貨とは，紙幣のような実態がなく，多くが発行者のいない通貨であり，P2P ネットワーク上で分散型台帳技術を用いた取引が保証されている．仮想通貨の特徴として，匿名性が高く，またオンラインで手続きが完了するため利便性が高いことなどが挙げられる．一方で，その利便性ゆえにハッカー等による攻撃の対象となり，仮想通貨の不正流出やユーザー情報の漏洩などに繋がっている．2018 年 1 月には仮想通貨取引所大手の Coincheck から NEM が流出し，被害額は約 580 億円にのぼる [2]．9 月にはテックビューロから Bitcoin 等の仮想通貨約 67 億円分が流出した [3]．また，韓国警察庁が公表した，過去 3 年間で韓国国内で発生したハッキング事件に関するレポートによると，取引所のハッキングは 7 件，個人の仮想通貨ウォレットのハッキングは 158 件であり，取引所だけではなく個人のウォレットも攻撃の対象となっていることが分かる [4]．

よって，仮想通貨のシステムや運用において問題がある場合、重大な流出リスクに繋がる危険性がある。

2. 研究目的

仮想通貨を送金するには秘密鍵が必要である．秘密鍵を盗まれると勝手に他人に自分の仮想通貨が送金されてしまう．ネットに繋がっているホットウォレットは常にハッキング攻撃を受ける可能性があるため，仮想通貨の流出リスクを抑制するためには秘密鍵をオフラインに保管する等の対策が必要となる．しかし秘密鍵をオフラインに保管していても，送金する際にネットワークに接続されるため，完全に流出リスクを防ぐことはできない．そこで流出時のリスクを抑えるためには複数のウォレットと秘密鍵のセットを用意して金額的なリスクを分散させることが効果的である．しかし複数の端末を持つことは費用の増大につながるため，複数の通貨を 1 つの端末で扱うノードも存在すると考えられる．すなわち複数の仮想通貨ネットワークに 1 端末で参加しているノードは流出リスクが大きい可能性がある．仮想通貨ネットワーク上に重複するノードの持つ端末の所有者によって以下の場合に分けられる．

- サーバ型ウォレット：
  通常は複数の端末に分けて管理するはずであるため，重複ノードが取引所である場合，適切な運営を行っていないと考えられる．取引所で扱う仮想通貨の額は多く，そのウォレットを分散させずに保管している場合，1 つのサーバが乗っ取られると，莫大な金額の仮想通貨が流出するリスクが存在する．
- クライアント型ウォレット：
  個人の仮想通貨ウォレットを端末に保管していると考えられる．個人の所有する金額は取引所に比べれば少ないが，複数の仮想通貨ウォレットを 1 端末に保管している場合，それぞれウォレットを分けている場合に比べてリスクが増大する．

よって仮想通貨ネットワーク上のシステムおよび運用リスクを明らかにするために複数の仮想通貨ネットワーク上のノードの重複を調査することが重要である。本研究では，仮想通貨ネットワークに出現する情報をもとに重複するノードを抽出し，その重複するノードが意味するリスクについて考察した．リスクの考察においては，地理情報とドメイン名を用いた．

3. 分析手法

本研究の分析は Bitcoin，Ethereum，Dash，NEM の 4 つの仮想通貨それぞれのネットワークにおいて，2018 年 4 月 1 日から 9 月 30 日までの期間内に出現した IPv4 アドレス及びドメインを調査対象とした．上記期間に出現した各仮想通貨のノード数を表 1 に示す．尚，ドメインは IPv4 アドレスに名前解決可能であったもののみを調査対象とした．IPv6 アドレ

スについても上記期間内において Bitcoin 及び Ethereum ネットワーク上に出現したが，IPv6 アドレスは今回の調査対象外とした． また，Bitcoin ノードの中には，996 件の.onion ドメイン(Tor を用いたノード)が確認された．これは匿名性を高めるために使用されるドメインであり，全て名前解決不可能であったため，調査対象外とした．

Bitcoin ネットワーク上の IP アドレス及びドメインは， https://bitnodes.earn.com/にて提供される API により取得した．Dash，Ethereum，NEM のネットワーク上の IP アドレス及びドメインは，それぞれ https://www.dashninja.pl/,https://www.ether-nodes.org/network/1，https://www.nodeexplorer.com/より 5 分毎に出現する IP アドレス・ドメインについて取得した．

以上より取得したデータを用いて，次の手順により分析を行った．

1. 重複分析のデータ前処理を行うために，それぞれの仮想通貨ネットワークの IP アドレス及びドメインを，IPv4 アドレスとそれ以外に分割した．尚，正引き(ドメインから IPv4 アドレスへの変換)が可能なドメインは，Python の socket ライブラリ及び WHOIS 検索(https://who.is/)を使用して正引きを行い，IPv4 アドレスとした．
2. 4 つの仮想通貨ネットワーク間の IPv4 アドレス同士を比較し，各仮想通貨ネットワーク間の重複 IPv4 アドレスを抽出した．
3. 各仮想通貨ネットワーク間の重複 IPv4 アドレスに対して，GeoIP2 データベースを用いて地理情報を導出し，各国の出現回数の計数及び世界地図上へのマッピングを行った．
4. Python の socket ライブラリを使用して各仮想通貨ネットワーク間の重複 IPv4 アドレスに対して逆引き(IPv4 アドレスからドメインへの変換)処理を行い，逆引き可能だった重複 IPv4 アドレスと逆引き不能だった重複 IPv4 アドレスに分割した．
5. 地理情報を用いて，各仮想通貨ネットワーク間の重複 IPv4 アドレスについて，逆引き不可能なものの国別集計を算出した．
6. 各仮想通貨ネットワーク間の重複 IPv4 アドレスについて，逆引き可能なもののドメインの内容を分析した．

表 1　各仮想通貨の出現ノード数の合計
(取得期間：2018/4/1～2018/9/30)

通貨	ノード数
Bitcoin 系列（Btc）	189661
Etherium 系列（Eth）	757223
Dash	30466
Nem	3854

4.　分析結果と考察

4.1　重複ノード数と地理情報分析の結果

3 章に示す通りに分析を行ったところ，各仮想通貨ネットワーク間に重複するノードが存在することが明らかとなった．各仮想通貨ネットワーク間の重複ノード数を図 1 に示す．2 種類の仮想通貨におけるノード重複はすべての組み合わせで存在した．Btc-Eth の組み合わせでの重複ノード数は他の組み合わせと比較して顕著に多い 3524 となった．これは Btc と Eth のネットワークに参加しているノード数が多く，調査対象の母数が多いためであると考えられる．3 種類の仮想通貨におけるノード重複は Eth-Dash-Nem 以外の組み合わせで存在した．特に Btc-Eth-Nem の組み合わせでは 8 つもの重複ノードが確認された．また，4 種類全ての仮想通貨ネットワークに重複するノードは存在しなかった．

共通の IP アドレスで複数の仮想通貨ネットワークを利用していることが明らかとなった．このことから，複数の通貨を保有するウォレットである可能性のあるノードが多く存在し，1 通貨のみの場合と比べてリスクが高いウォレットが存在していると考えられる．

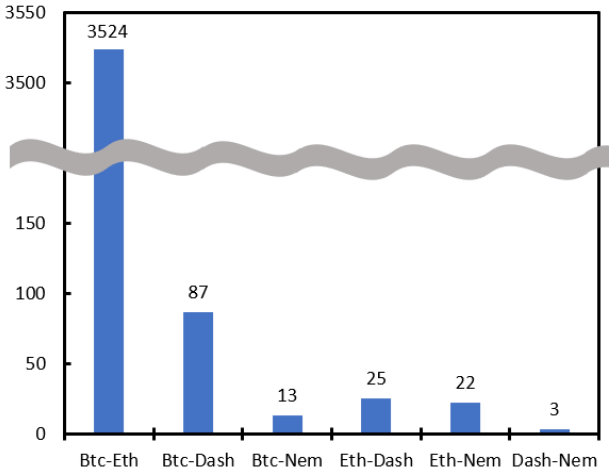

図 1　2 種類の通貨で重複したノード数

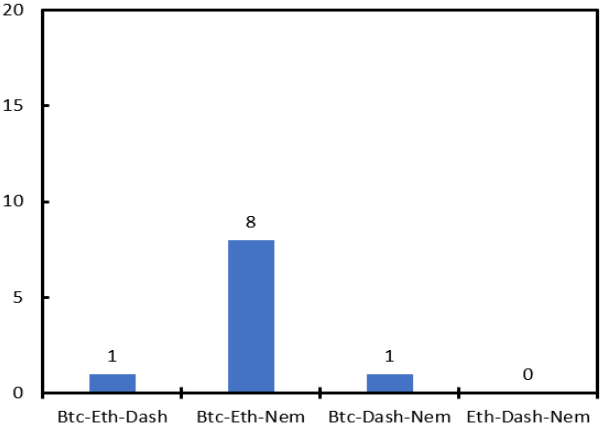

図 2　3 種類の通貨で重複したノード数

重複したノードから 3 章の手順に沿って地理情報を取得し国別に集計した結果を図 3 に示す．また各通貨の重複ノードの国別集計結果上位 5 か国を表 2 に示す．重複ノードは米国、欧州、東アジアの線先進国に多く分布した．Bitcoin と Ethereum の重複ノードは他の組み合わせと比較すると，先進国だけでなく発展途上国にもノードがみらた．発展途上国に重複ノードがあるケースとして，個人の保有の他にマイニング工場が置かれている可能性が考えられる．

表 2　各通貨の重複における国別集計結果（上位 5 か国）

btc-eth		**btc-dash**	
United States	602	Germany	32
Germany	581	Romania	25
China	442	Finland	20
Russia	241	Australia	4
others	1658	others	6
計	3524	計	87
btc-nem		**eth-dash**	
Germany	9	Netherlands	4
United States	1	United States	3
Singapore	1	Germany	3
Russia	1	Canada	2
France	1	others	13
計	13	計	25
eth-nem		**dash-nem**	
Spain	9	United States	1
Germany	7	Malaysia	1
Ukraine	1	Germany	1
Finland	1		
others	5		
計	22	計	3
btc-eth-nem		**btc-eth-dash**	
Germany	6	France	1
Russia	1		
France	1		
計	8	計	1
btc-dash-nem			
Germany	1		
計	1		

4.2　重複結果に基づく考察

重複したノード数が最も多かった Bitcoin_Ethream を対象とし，3 章の手順に沿って逆引きを行い，ドメイン取得を試みた．その結果，3524 の重複ノードのうち 2242 のドメインが取得でき，残りの 1282 のドメインは取得不可能であった．このドメイン取得不可能なノードには個人情報を隠したいと考えているクライアント型ウォレットが含まれているとともに，悪用する目的で個人情報を隠そうとするノードも含まれると考えられる．そこでドメイン取得不可であったノードについて地理情報を取得した．さらにドメインが取得できたものについてはその内容を分析した．

Bitcoin と Ethream の重複を国別に集計し，全重複ノードの国別割合と逆引きができないノードの国別割合をそれぞれ図 7，図 8 に示す．これらを比べると，中国ではその割合が増加した．この理由として，中国では Bitcoin の取引が原則禁止されているため，個人を特定しにくいように，ドメインに変換できないような形で利用していると考えられる．

次に，トップレベルドメイン(TLD)について数の多かったものの上位 15 種を図 9 に示す．トップレベルドメインで最も多かったものは，汎用トップレベルドメイン(gTLD)で誰でも利用可能な.com であった．同様に.net が三番目に多い結果となった．またドイツの国別トップレベルドメイン(ccTLD)である.de が全体の 2 番目に多い結果となった．この理由については後述される．さらに 4 番目はロシアの ccTLD である.ru となった．

次にセカンドレベルドメイン(SLD)と TLD を合わせたものについて多かったものの上位 15 種を図 10 に示す．最も多かったのは amazon のクラウドサーバサービスである amazonaws.com であった．

2 番目の your-server.de は YOURSERVER 社の VPS(virtual private server:仮想専用サーバ)であると考えられる．上位にはクラウドサービスや VPS が多く，これはクラウドサーバまたは VPS を利用して複数の仮想通貨ネットワークに参加しているノードが多く存在することを意味する．この理由の一つとしてクラウドサーバを使用して仮想通貨のマイニングに参加している可能性が考えられる．図においてドイツの ccTLD である.de が多い結果となったのはドイツのクラウドサーバやサービスを使用したネットワークへの参加が多いことに起因する．

8 番目に多かった in-addr.arpa は IP アドレスが DNS に登録されていない場合のドメインである．

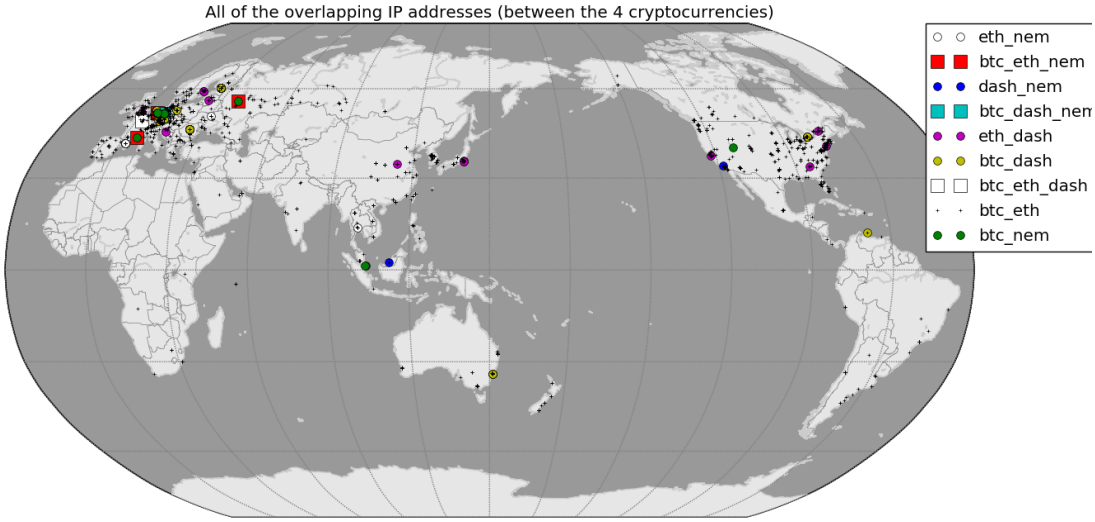

図 3　Bitcoin と Ethream の重複(国別集計：全重複ノード)

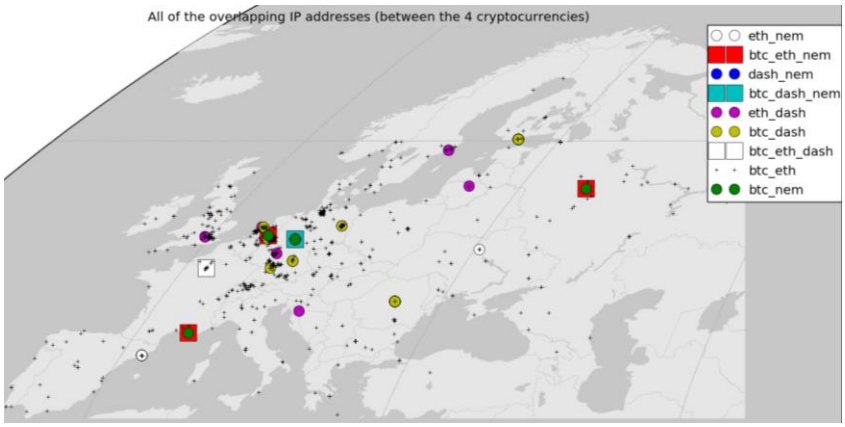

図 4　重複ノードの分布(拡大図：欧州)

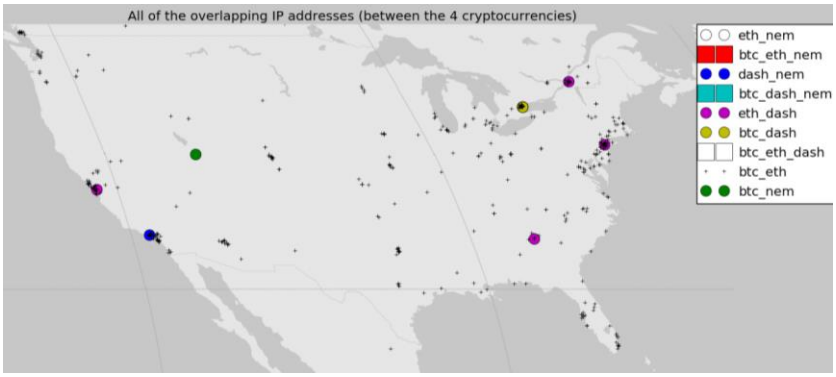

図 5　重複ノードの分布(拡大図：米国)

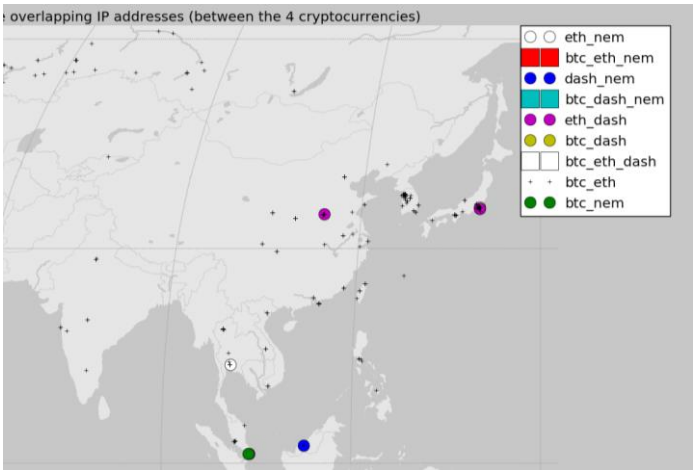

図 6　重複ノードの分布(拡大図：アジア)

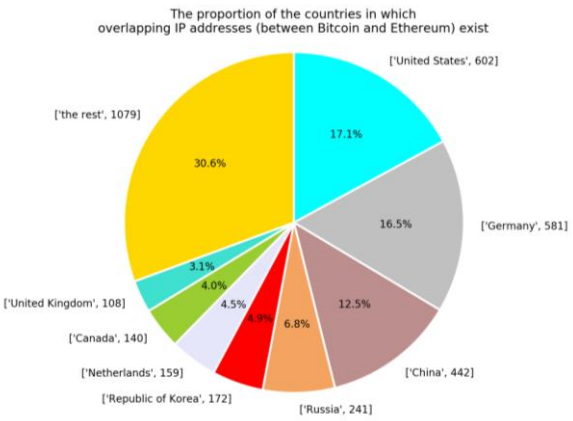

図 7　Bitcoin と Ethream の重複
（国別集計，全重複ノード）

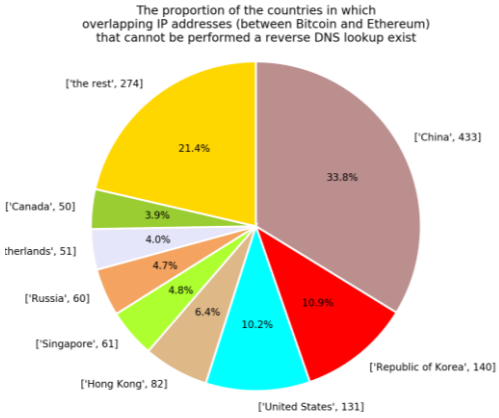

図 8　Bitcoin と Ethream の重複
（国別集計，逆引き不可ノード）

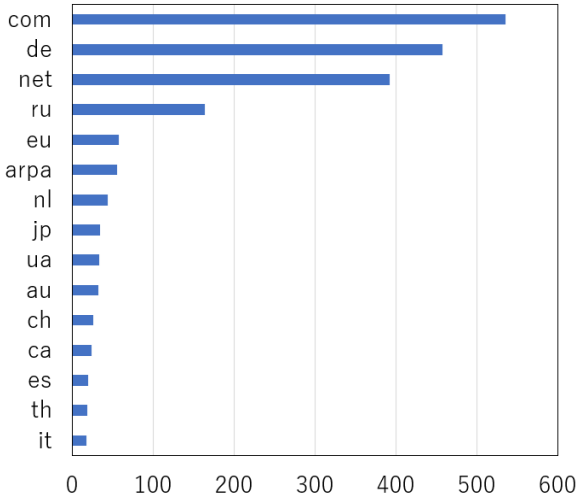

図 9　TLD 上位 15 種
（対象：Bitcoin_Ethream の重複ノードにおいて逆引き可能なもの）

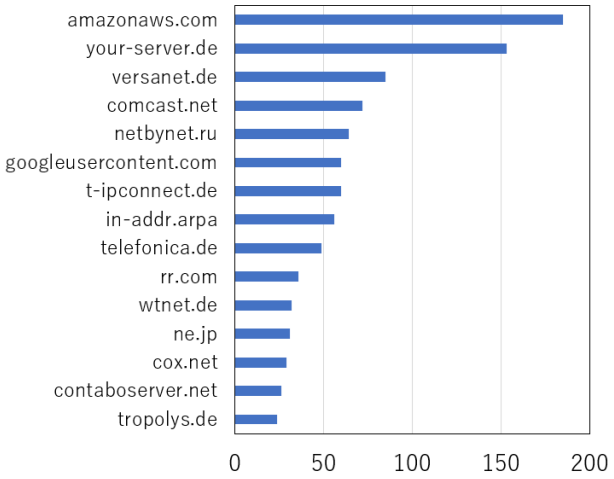

図 10　TLD+SLD 上位 15 種
（対象：Bitcoin_Ethream の重複ノードにおいて逆引き可能なもの）

5.　まとめ

Bitcoin，Ethereum，Dash，Nem の 4 種類の仮想通貨を対象として各仮想通貨ネットワークのノードの重複を調査した．2 種類の仮想通貨のノード重複は Bitcoin と Ethereum の組み合わせで 3524 となった．また，3 種類の仮想通貨のノード重複も確認された．これは複数の仮想通貨ネットワークに同一端末から参加していることを意味し，同一端末に複数の仮想通貨ウォレット及び秘密鍵を保管している場合，流出リスクが大幅に高くなる．また Bitcoin と Ethereum の重複ノードのうち，逆引きによって取得不可能なドメインが中国に多く分布しており，中国におけるクライアント型ウォレットの複数の仮想通貨ネットワークへの参加が多いという推測が得られた．さらにドメインが取得できたものにはクラウドサーバや VPS が多く見受けられ，これらはクラウドマイニング目的で参加していると考えられた．

6.　今後の課題

本研究では複数の仮想通貨ネットワークから得られる IP アドレスおよびドメインを対象として分析を行い，重複ノードの存在を明らかにするとともに，重複ノードの地理的分布を得た．しかしこれらから得られる情報では大きな流出リスクを伴なうノードを詳細に絞り込むまでには至っていない．仮想通貨ネットワークから得られる情報は IP アドレスやドメインのみでなく，使用アプリのバージョン情報などが取得できる．これらの追加情報を用いれば，各ノードの持つリスクについてより詳細に議論できると考えられる．

補注

本研究は筑波大学リスク工学専攻ケーススタディ研究と連携して行われた.

参考文献(以下，最終閲覧 2018 年 10 月 8 日)

1) コインマーケットキャンプ：
https://coinmarketcap.com/
2) 日本経済新聞：コインチェックの仮想通貨不正流出，過去最大 580 億円
https://www.nikkei.com/article/DGXMZO26231090X20C18A1MM8000/
3) 日本経済新聞：「Zaif」のテックビューロ，仮想通貨 67 億円分流出
https://www.nikkei.com/article/DGXMZO35555020Q8A920C1MM0000/
4) Bitcoin.com：NEWS
https://news.bitcoin.com/crypto-exchanges-wallets-hacked-korea/
5) https://kasobu.com/cryptocurrency-loss/
6) https://bitcoiner.link/595.html
7) https://salestechnologylab.com/