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

グループ演習8班
西 貴弘, 南 翔, 渡辺春菜, 向 渓子
アドバイザー教員　面 和成

筑波大学
University of Tsukuba

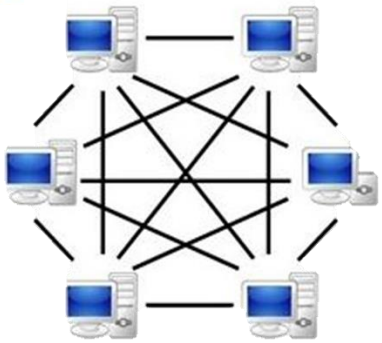
CONTENT

背景

仮想通貨

- 実体がない
- 発行者がいない
- 分散型台帳技術で取引を保証
- 匿名性
- 利便性

オンライン上で
手続きが完了



P2P-network

最近・・・

- Coincheck(取引所)からNEMの流出
- 個人のウォレットへのハッキング等が発生

ハッカー等による攻撃の対象となりやすく，
通貨の流出や情報漏洩が問題

背景

オフラインで保存していても，送金時の流出リスクは避けられない・・・

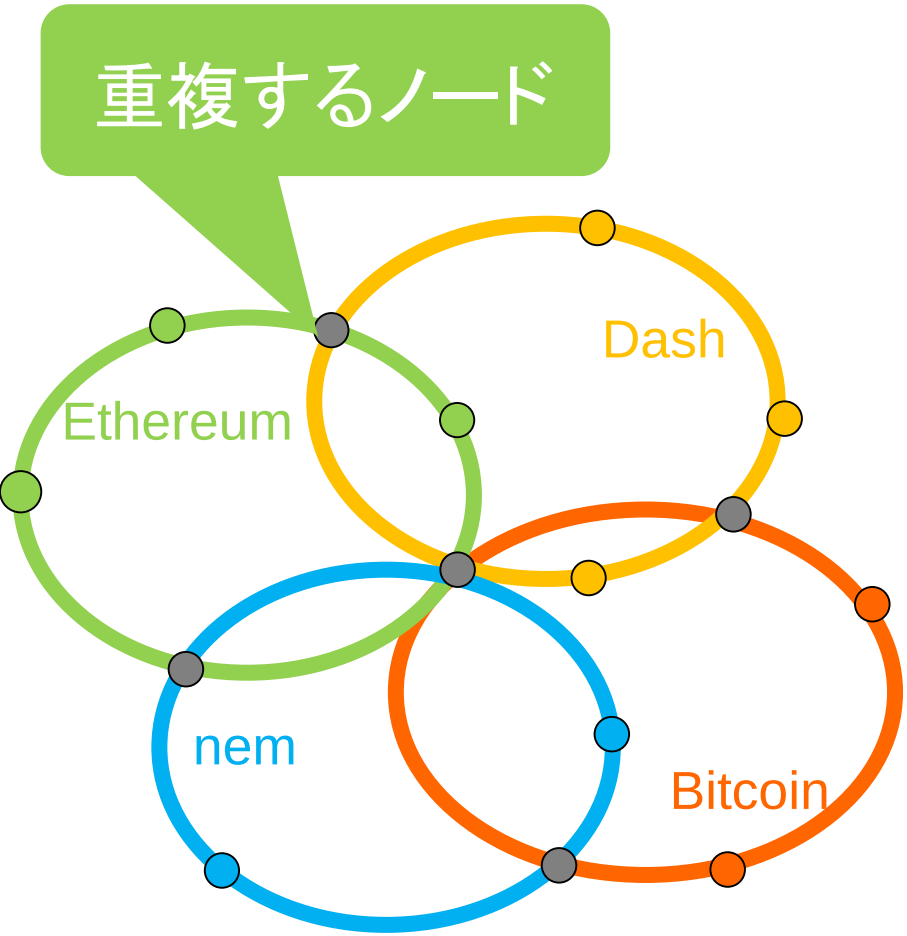
金銭リスクを分散させるべき
→ウォレット＆秘密鍵のセットを複数用意する

しかし，複数の端末を持つことは費用がかかる

複数の通貨を一つの端末で扱うノードが存在する可能性

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時リスクが大きい可能性がある

ノード重複が意味するもの



サーバー型ウォレット

例：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．
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

クライアント型ウォレット

例：個人の仮想通貨ウォレット
→　金額は少ないが，
ウォレットを分けている場合と比べ，流出時のリスクは増大

研究目的

複数の仮想通貨ネットワーク上のノードが重複
→流出時のリスクが高まる可能性

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必要

本研究

仮想通貨ネットワークに出現する情報から
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

分析手法:調査対象

bitcoin (ビットコイン)
ローンチ:2009年1月9日
通貨の単位:BTC
Proof of Work

Ethereum (イーサリアム)
ローンチ:2015年7月30日
通貨の単位:ETH
Proof of Stake

nem (ネム)
ローンチ:2015年3月31日
通貨の単位:XEM
Proof of Importance

DASH (ダッシュ)
ローンチ:2014年1月18日
通貨の単位:DASH
匿名性が高い・決済が速い

分析手法:調査対象

調査対象通貨	Bitcoin, Ethereum, Dash, NEM
対象期間	2018年4月1日～9月30日
情報	期間内に出現したIPv4アドレス及びドメイン

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
Ethereum 系列 (Eth)	757223
Dash	30466
Nem	3854

分析手法：分析の流れ

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する

各ネットワークの
IPアドレスの取得

IPアドレス
重複分析

重複IPアドレス
の特徴の調査

考察

①IPアドレス及びドメイン→IPv4アドレスとそれ以外に分割．
　正引き可能なドメイン→IPv4アドレスに変換

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
　各仮想通貨ネットワーク間の重複IPv4アドレスを抽出．

③ IPアドレスから地域情報を取得（GeoIPを使用）

分析手法：分析の流れ

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する

各ネットワークの
IPアドレスの取得

IPアドレス
重複分析

重複IPアドレス
の特徴の調査

考察

④ 重複IPv4アドレスに対して逆引き処理を行い，
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

⑤ 逆引き不能だった重複IPv4アドレスに対し，地域情報を取得．
逆引き可能だったIPv4に対しては，ドメイン情報を分析．

結果：重複ノード数

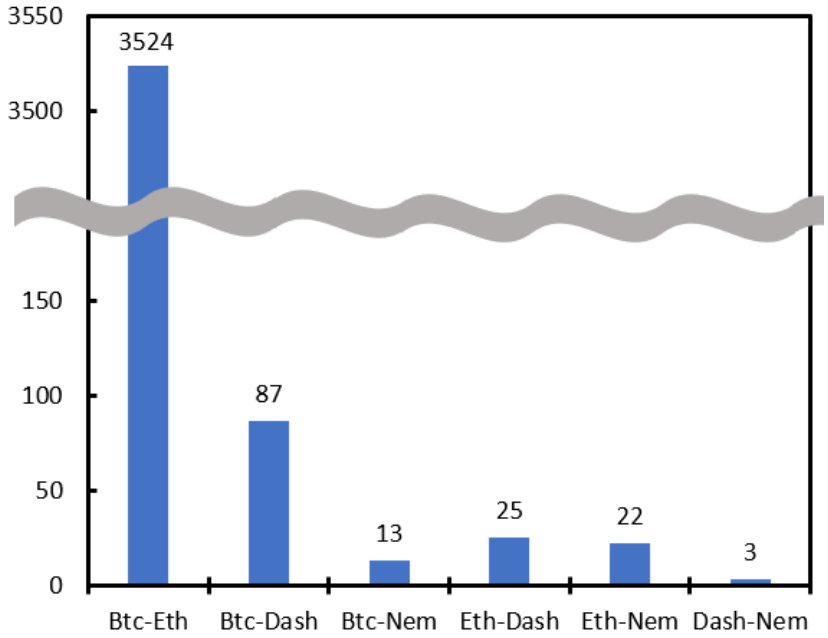


図1　2種類の通貨で重複したノード数

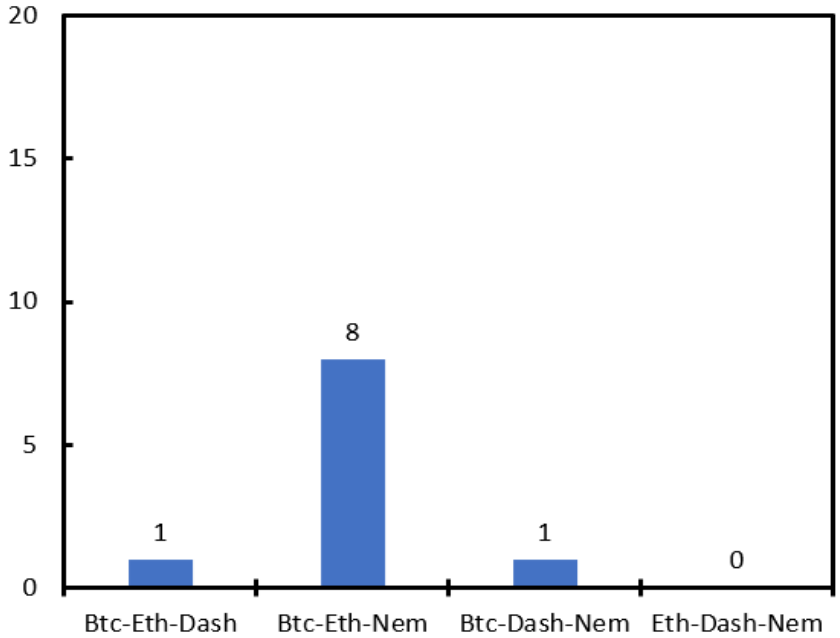


図2　3種類の通貨で重複したノード数

各仮想通貨ネットワーク間に重複するノードが存在

- これらは同一端末で複数の仮想通貨ネットワークに参加し、ウォレットと秘密鍵を複数所持している可能性

リスク大

結果：重複ノード数

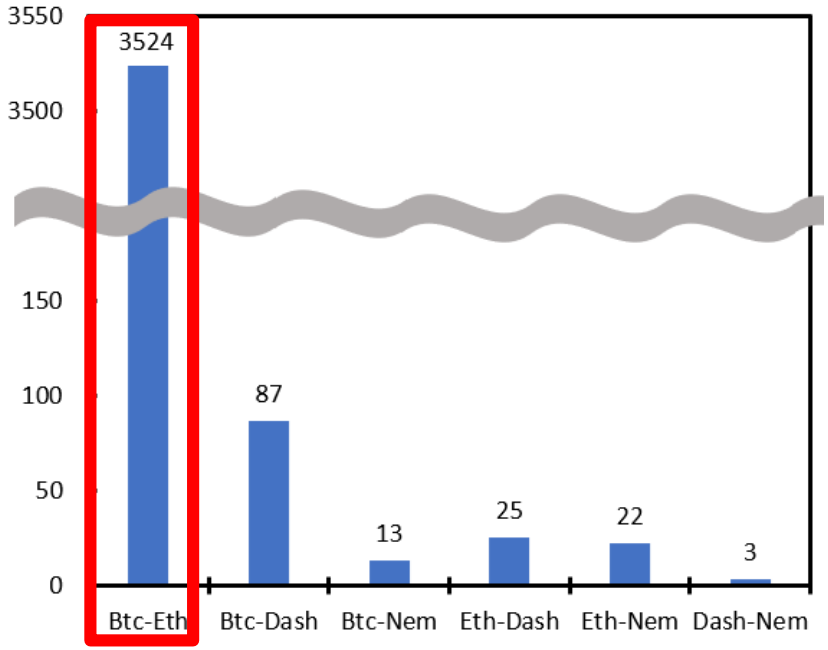


図1　2種類の通貨で重複したノード数

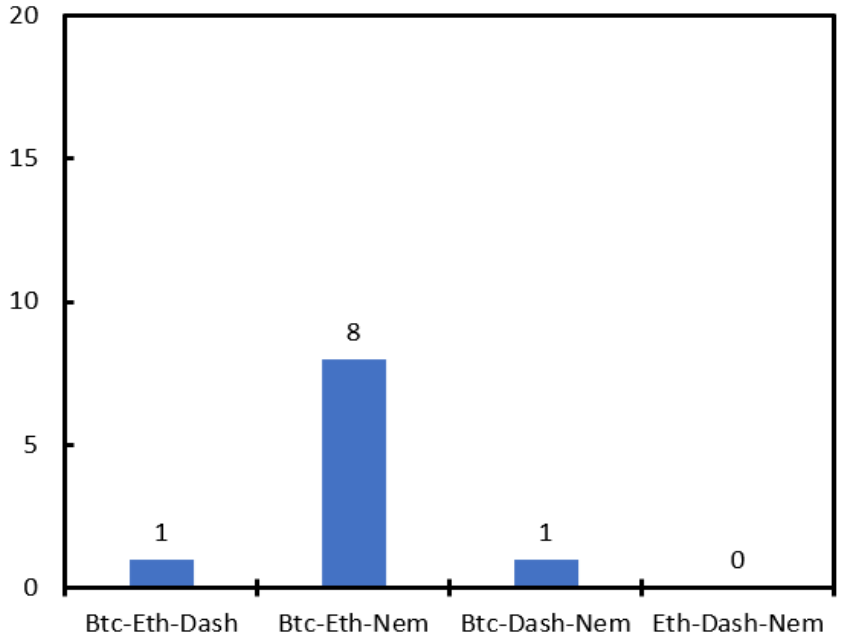


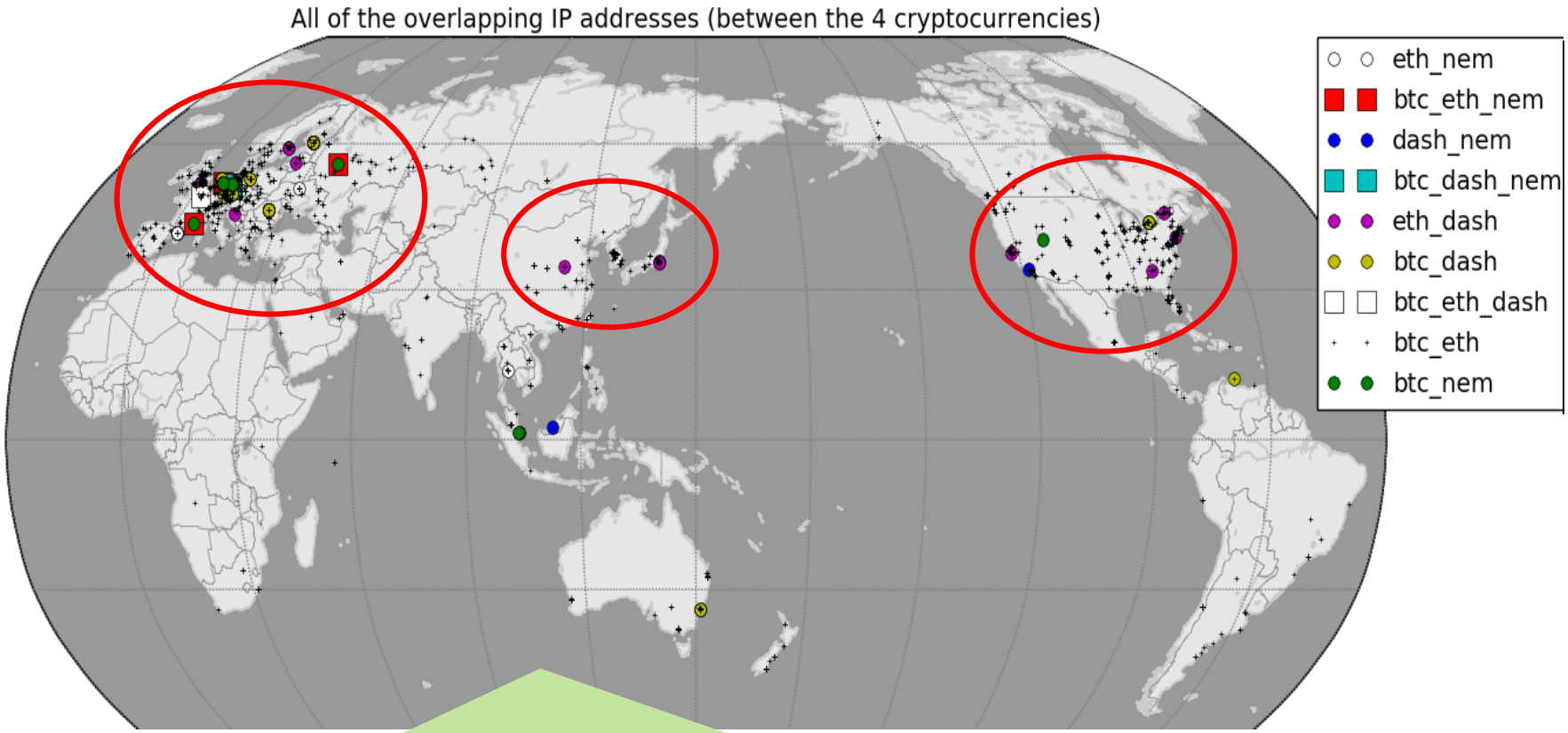
図2　3種類の通貨で重複したノード数

最も重複の多い Btc-Eth の場合，
→ Bitcoin 系列ネットワークの 約 2%のノードが重複あり.

テックビューロ社にてBtcを含む複数の仮想通貨が不正流出(2018/9)
→運用管理上のリスクについて検討する必要がある

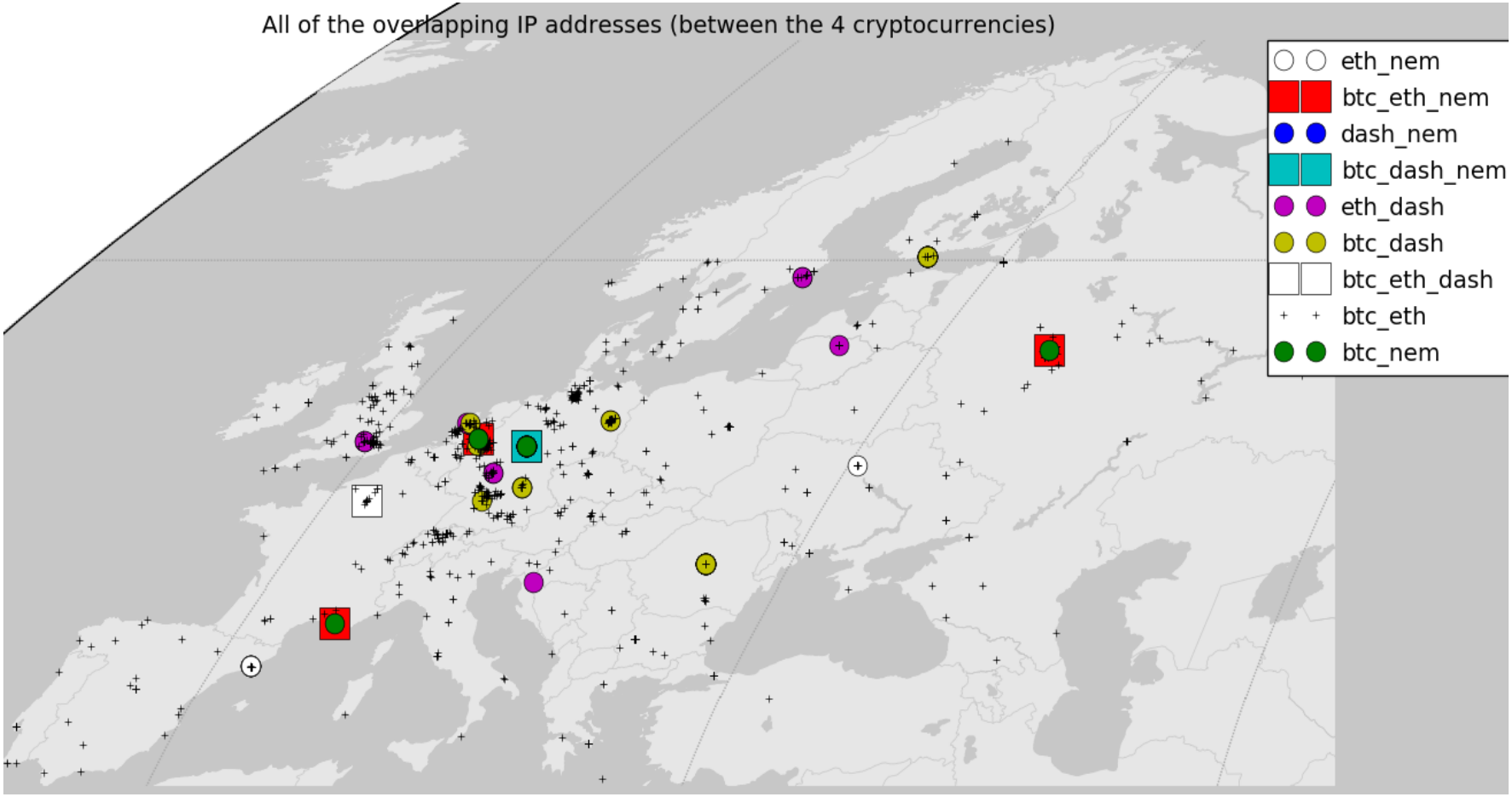
結果：全重複ノードの地理的分布

BitcoinとEthereumの重複(国別集計：全重複ノード)

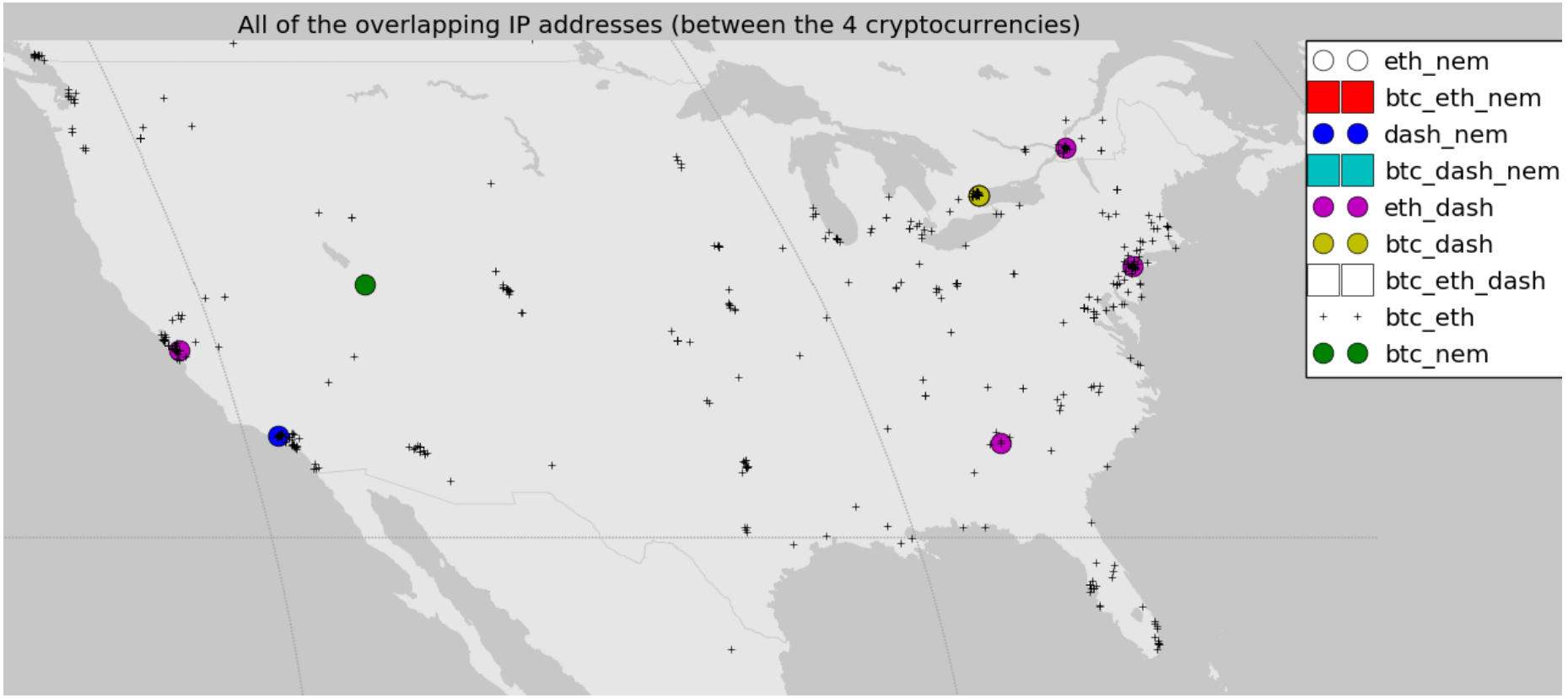


米国，欧州，東アジアの先進国を中心に多く分布

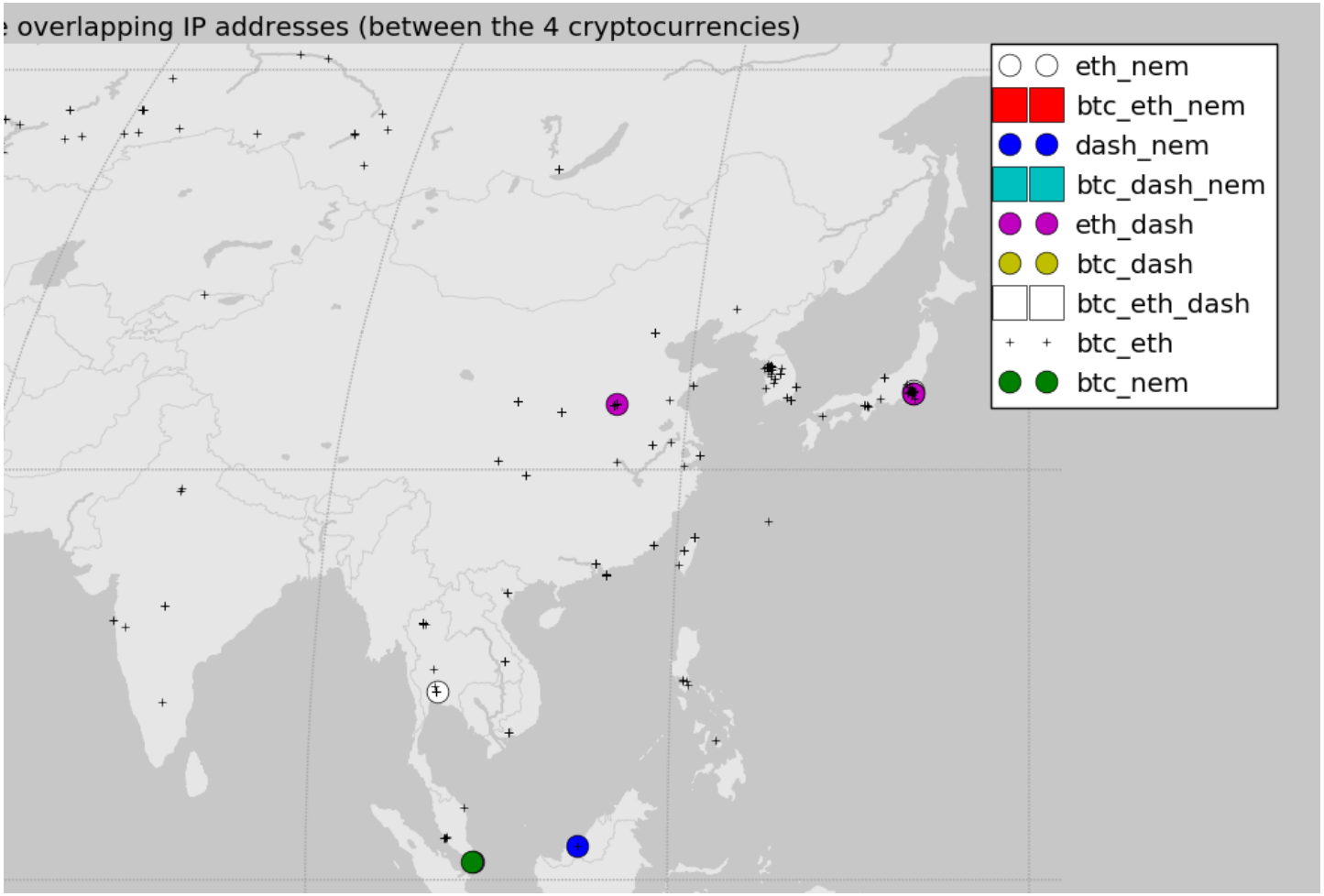
結果：重複ノードの地理的分布(欧州)



結果：重複ノードの地理的分布(米国)

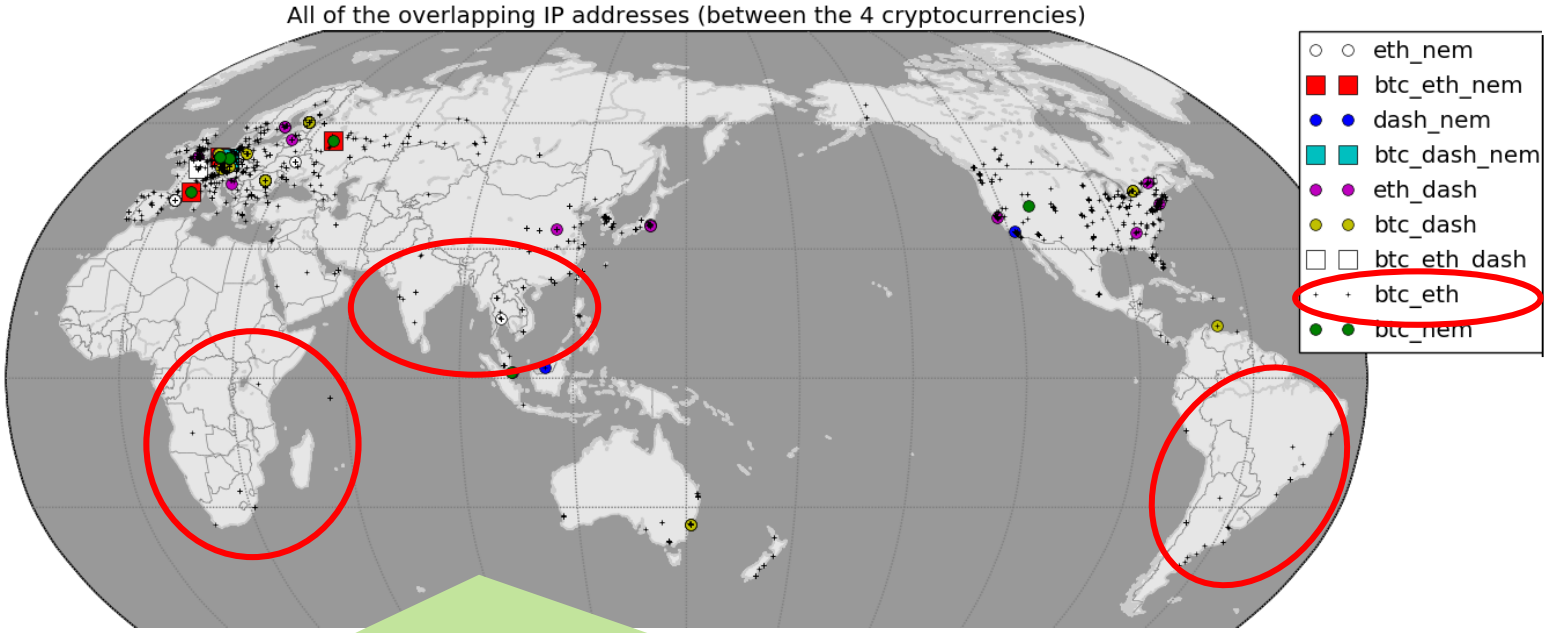


結果：重複ノードの地理的分布(アジア)



結果：重複ノードの地理的分布

BitcoinとEthreamの重複(国別集計：全重複ノード)

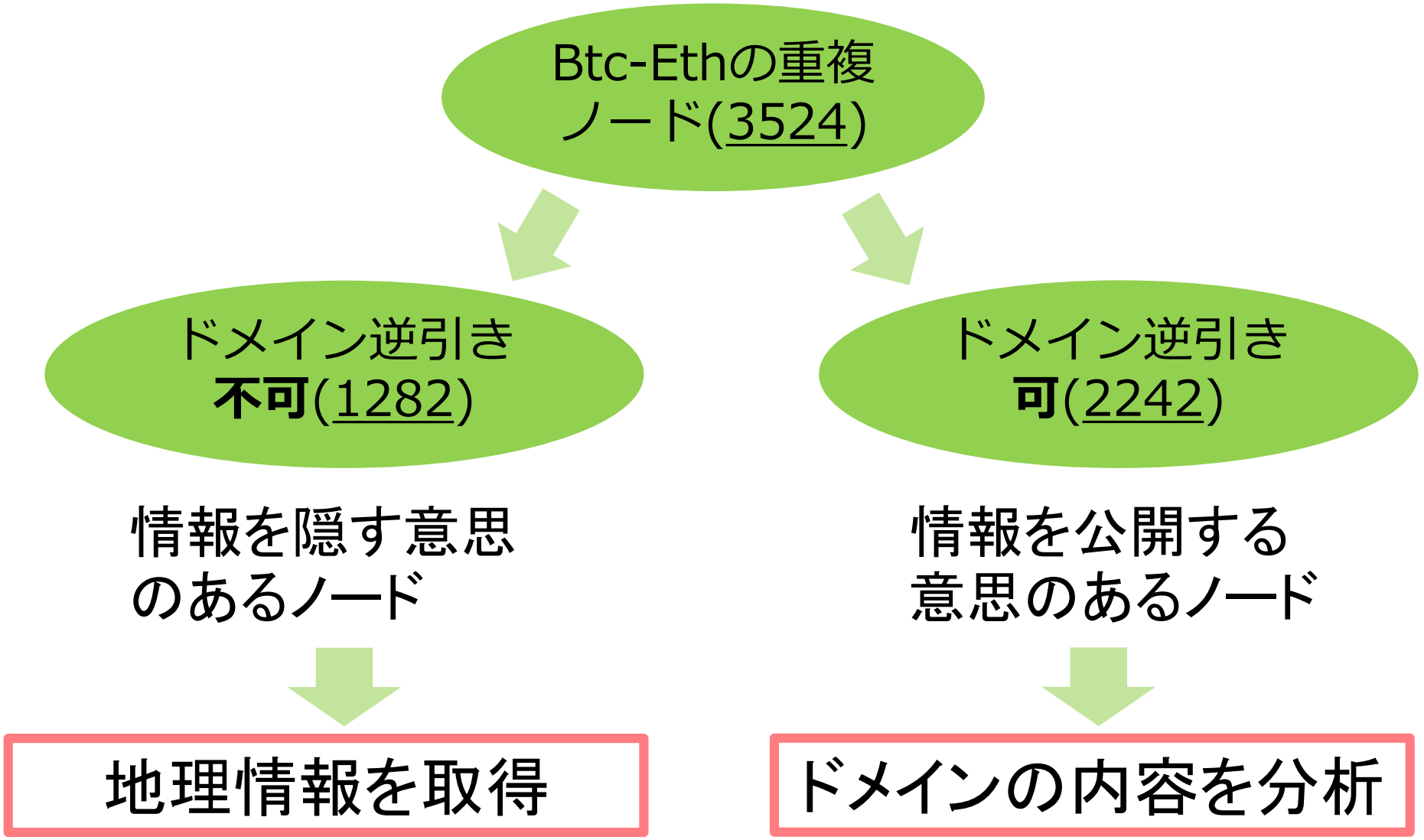


Bitcoin_Ethereumの重複ノードは発展途上国にも!

認知度の高いサービス ▶ 地域に関係なく存在.

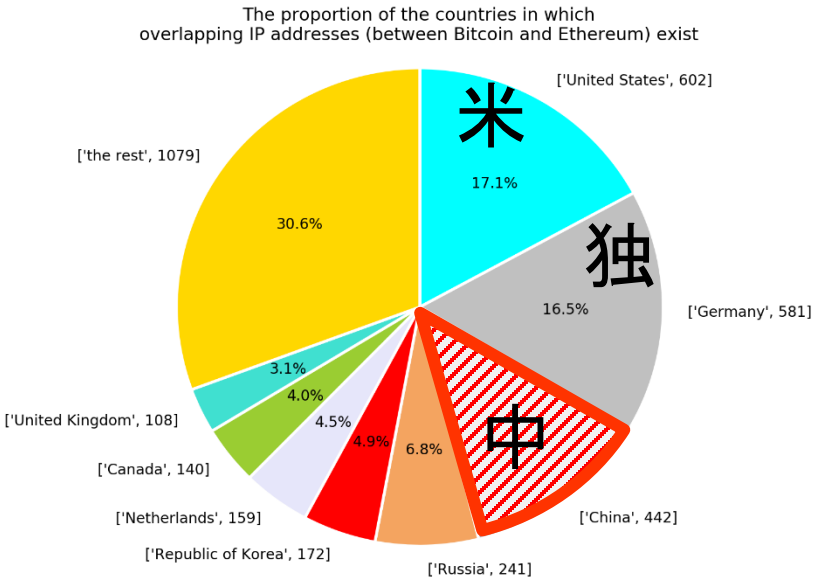
全域的な視点で検討するべき課題である

考察:ドメインの逆引きによる分析

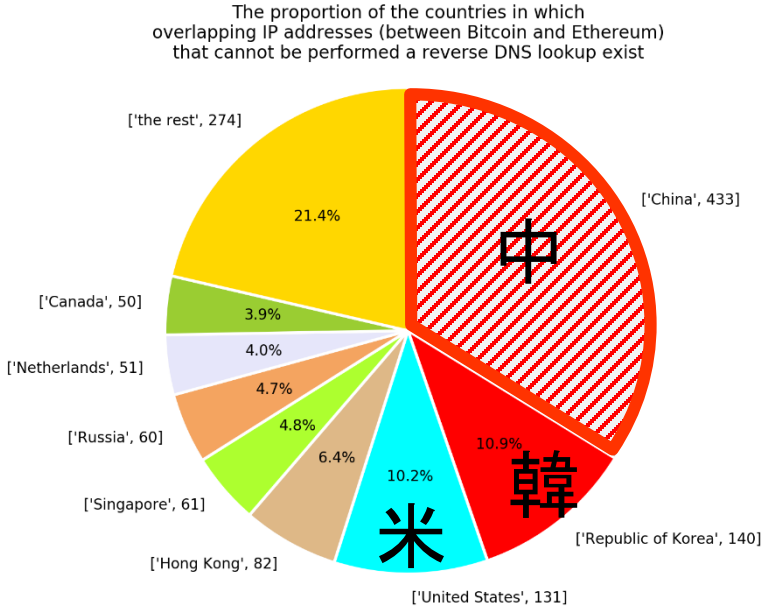


考察:ドメインの逆引きによる分析

全重複ノード



逆引き不可



逆引き不可ノードでは，全体に占める中国の割合が大きくなる

中国ではBitcoinの取引が原則禁止されている.
個人を特定しにくいよう，逆引き不可の設定で利用しているのでは？

考察:ドメインの逆引きによる分析

Btc-Ethの重複
ノード(3524)

ドメイン逆引き
不可(1282)

ドメイン逆引き
可(2242)

情報を隠す意思
のあるノード

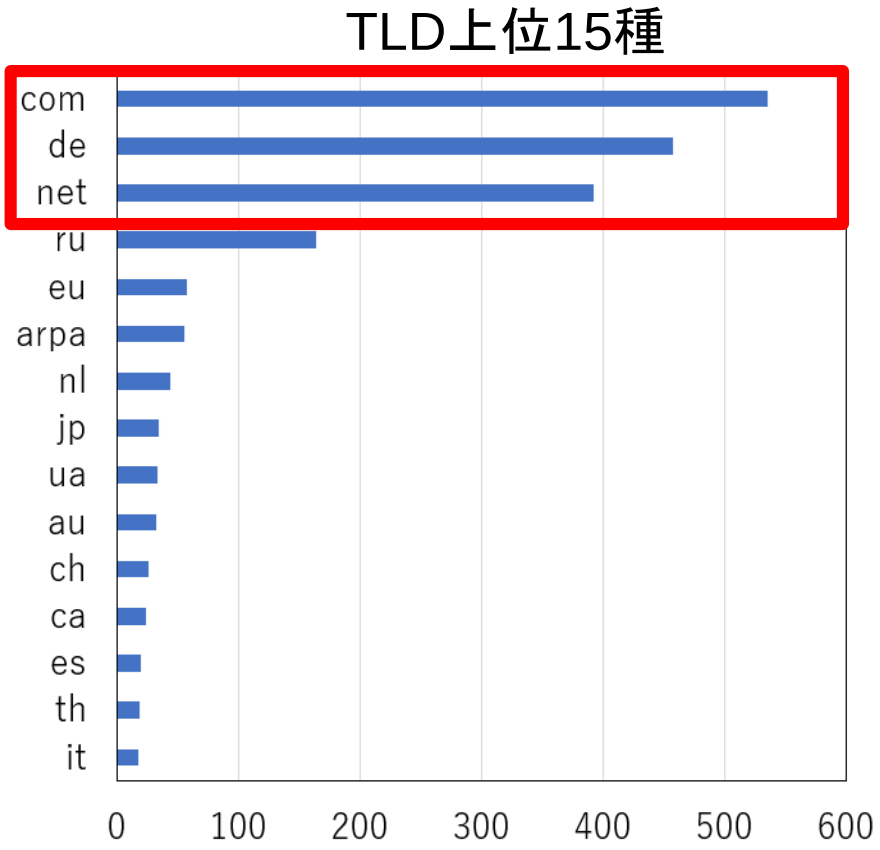
情報を公開する
意思のあるノード

地理情報を取得

ドメインの内容を分析

考察:ドメインの逆引きによる分析

TLD(Top Level Domain)を抽出



- .com　.net

  誰でも登録可能
  （汎用ドメイン）
  企業などで多く使われる

- .de　(ドイツ)

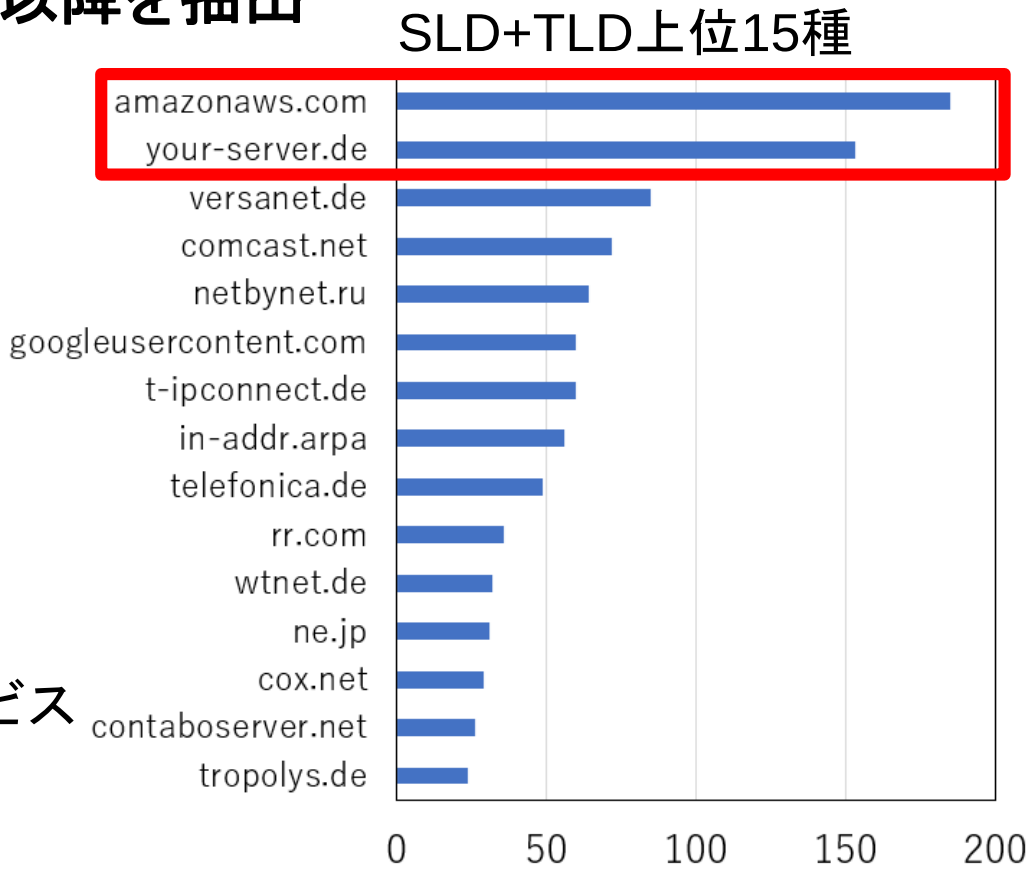
  ドイツのクラウドサービス
  やVPSの利用が多いため

- 数は少ないが、教育機関向けgTLDである.eduも存在

考察:ドメインの逆引きによる分析

SLD(Second Level Domain)以降を抽出

- amazonaws.com
  amazonのクラウドサーバーサービス
- your-server.de
  YOURSERVER社のVPS(Virtual Private Server)サービス



- **匿名性を重視した取引が多く行われている可能性**

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

- 最大で3種類までの仮想通貨ネットワークで**重複ノードを確認**
- Bit_Ethの重複ノードは全域的な視点で対応するべき課題である.
- 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
- ドメインが取得できたものにはクラウドサーバやVPSが多い
  → 匿名性を重視した取引が好まれている

- 攻撃発生時に複数の仮想通貨が流出するリスク
- サービス依存度による障害範囲が拡大するリスク

今後の課題

- 大きな流出時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可能.

  → 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

- BitcoinとEthereumの重複は全域的に分布したため先進国以外の分布について調査が必要である.

参考文献

[1] 仮想通貨で90%以上の暴落を味わった猫のブログ
https://www.bitcoin77777.com/2017/12/11/153310

[2] Wikipedia, ビットコイン
https://ja.wikipedia.org/wiki/ビットコイン

[3] BITPOINT, イーサリアムの特徴とは？ビットコインにはない優れた機能
https://www.bitpoint.co.jp/column/tips05/

[4] 仮想通貨ネム（NEM/XEM）特徴と将来性｜ビットコインとの比較
http://vtuka.jp/nemshourai

[5] 仮想通貨DASH（ダッシュ）とは？特徴・仕組み・チャートから将来性を徹底解説！
https://coinotaku.com/?p=7246

[6] コインチェックHP
https://corporate.coincheck.com/

[7] 韓国の取引所ビッサム（bithumb）で仮想通貨33億円が流出～
https://bitcoin-newstart.com/bithumb-news0620

[8] bitfinex取引所がハッキングを受けビットコインが盗難被害（12万BTC）
https://bitcoin-newstart.com/bitfenix-incident

[9] BITFINEX
https://www.bitfinex.com/

[10] IPアドレスとは
http://pc-tablet-smartphone.com/aboutipaddress

参考文献

[11] IPアドレスから何がわかるのか？IPアドレスを知られる危険性と仕組み
https://24ch.biz/2017/05/08/post-522/

[12] Norton by Symantec Blog
https://japan.norton.com/ip-address-8394

Thank you

筑波大学
University of Tsukuba

btc-eth			
全体		逆引き不可	
United States	602	China	433
Germany	581	Republic of Korea	140
China	442	United States	131
Russia	241	Hong Kong	82
the other	1658	the other	496
計	3524	計	1282

btc-dash			
全体		逆引き不可	
Germany	32	Canada	2
Romania	25	Romania	16
Finland	20	Netherlands	1
Australia	4	Germany	1
the other	6		
計	87	計	20

btc-nem

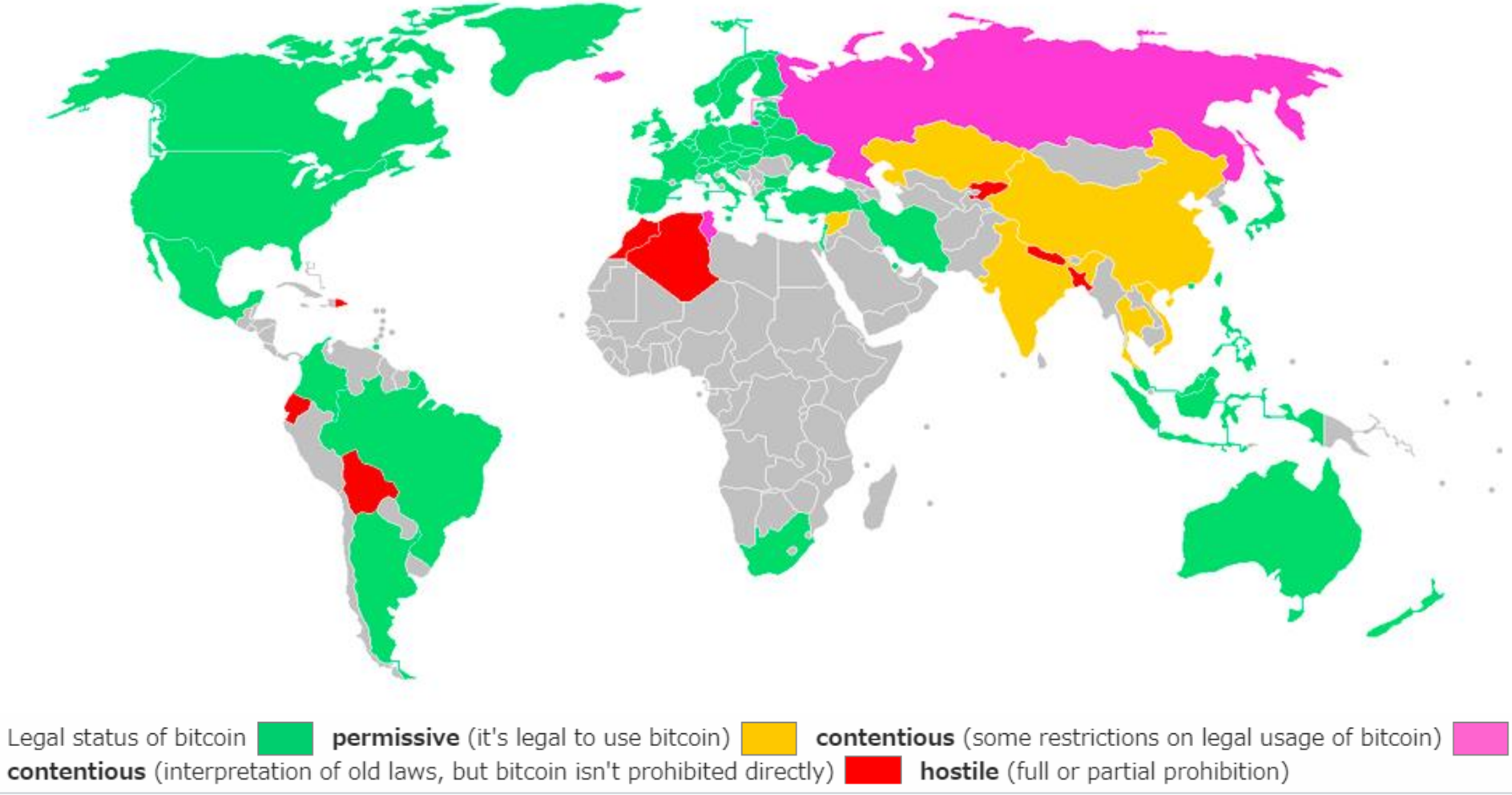
全体		逆引き不可	
Germany	9	United States	1
United States	1		
Singapore	1		
Russia	1		
France	1		
計	13	計	1

eth-dash

全体		逆引き不可	
Netherlands	4	Netherlands	3
United States	3	United Kingdom	2
Germany	3	Canada	1
Canada	2	Republic of Lithuania	1

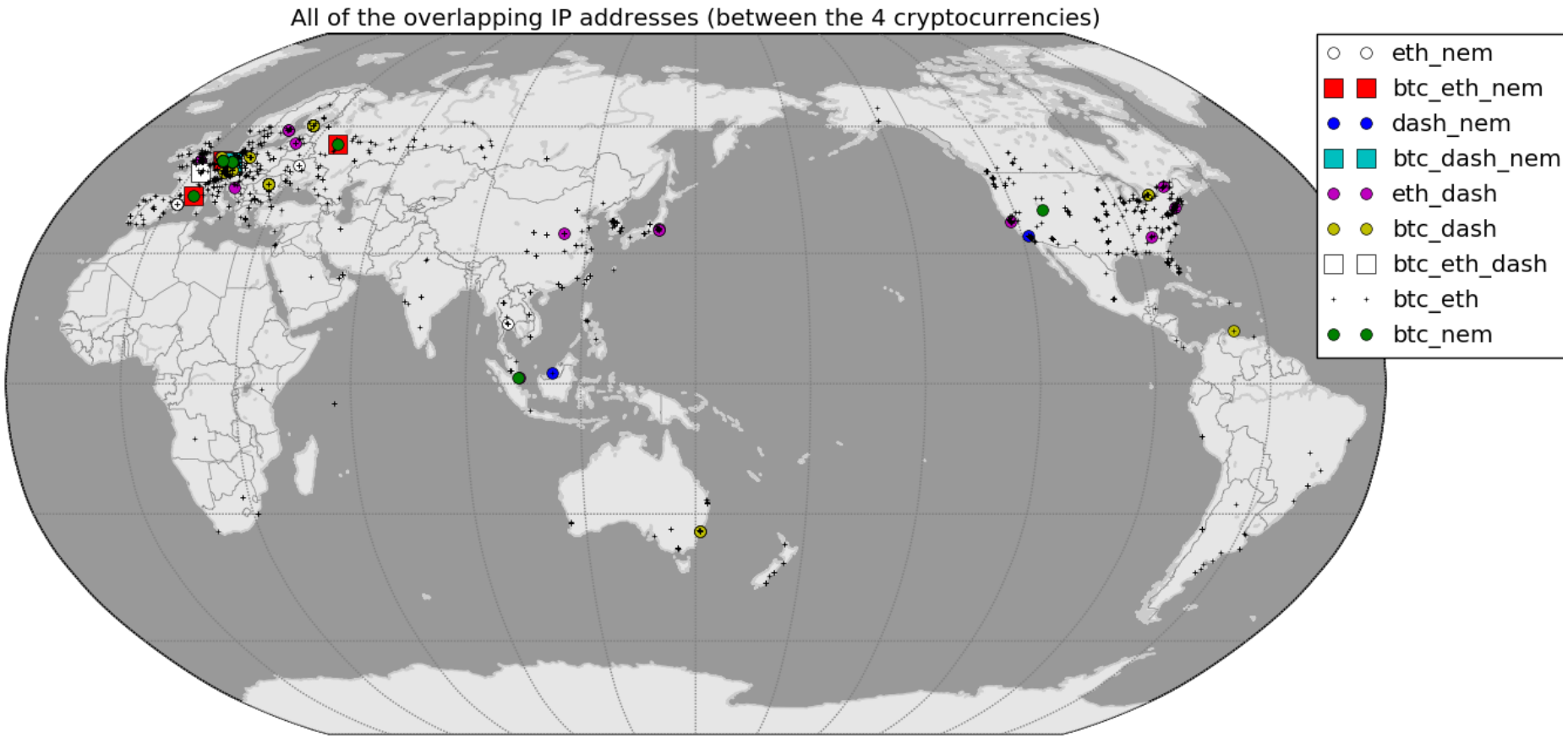
eth-nem			
全体		逆引き不可	
Spain	9	Germany	1
Germany	7		
Ukraine	1		
Finland	1		
the other	5		
計	22	計	1
dash-nem			
全体		逆引き不可	
United States	1	Malaysia	1
Malaysia	1		
Germany	1		
計	3	計	1

btc-eth-nem			
全体		逆引き不可	
Germany	6	-	-
Russia	1		
France	1		
計	8	計	0
btc-eth-dash			
逆引き可		逆引き不可	
France	1	-	-
計	1	計	0
btc-dash-nem			
逆引き可		逆引き不可	
Germany	1	-	-
計	1	計	0

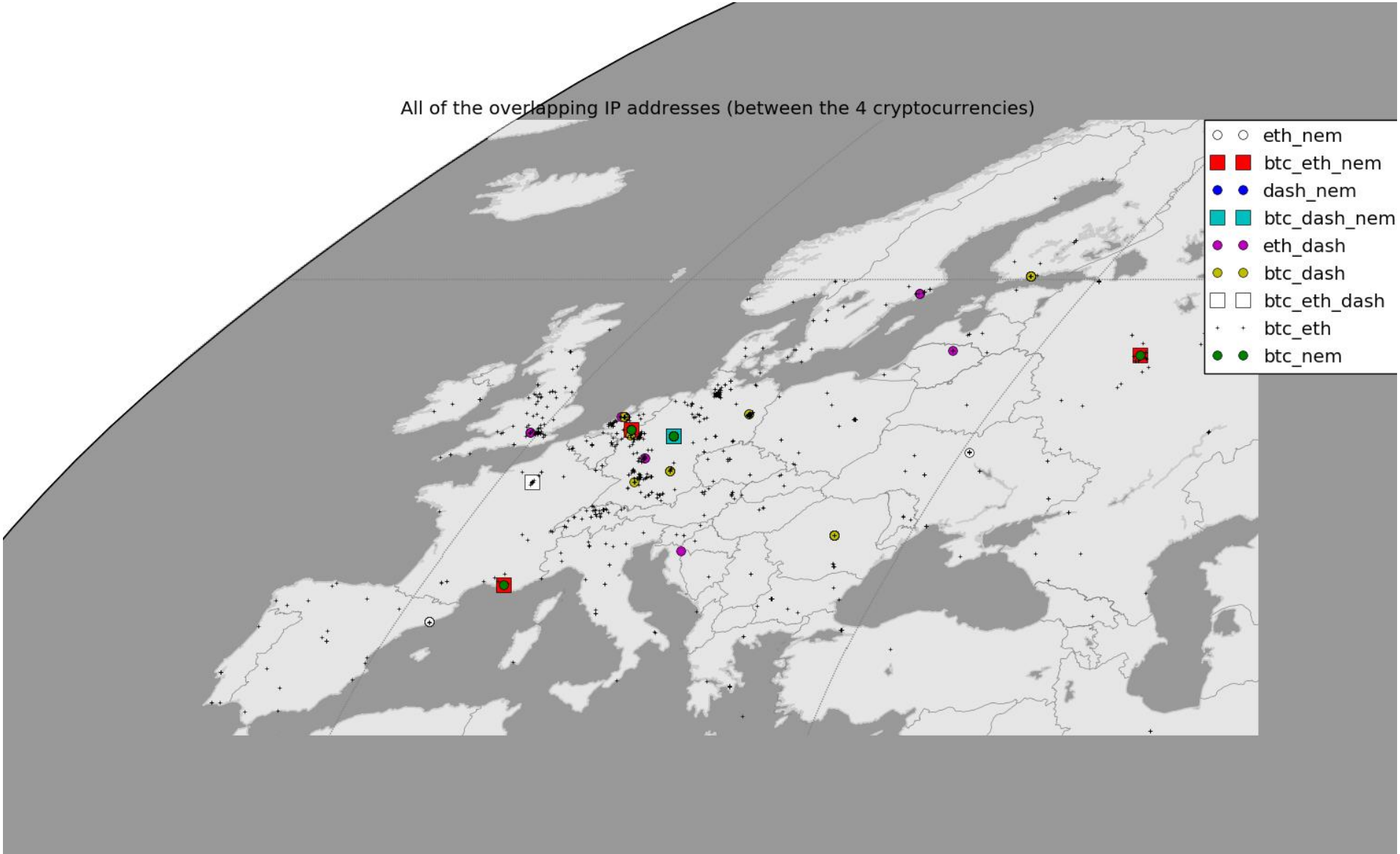


https://ja.wikipedia.org/wiki/%E5%90%84%E5%9B%BD%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8B%E3%83%93%E3%83%83%E3%83%88%E3%82%B3%E3%82%A4%E3%83%B3%E3%81%AE%E6%B3%95%E7%9A%84%E3%81%AA%E6%89%B1%E3%81%84#/media/File:Legal_status_of_bitcoin_(new).png

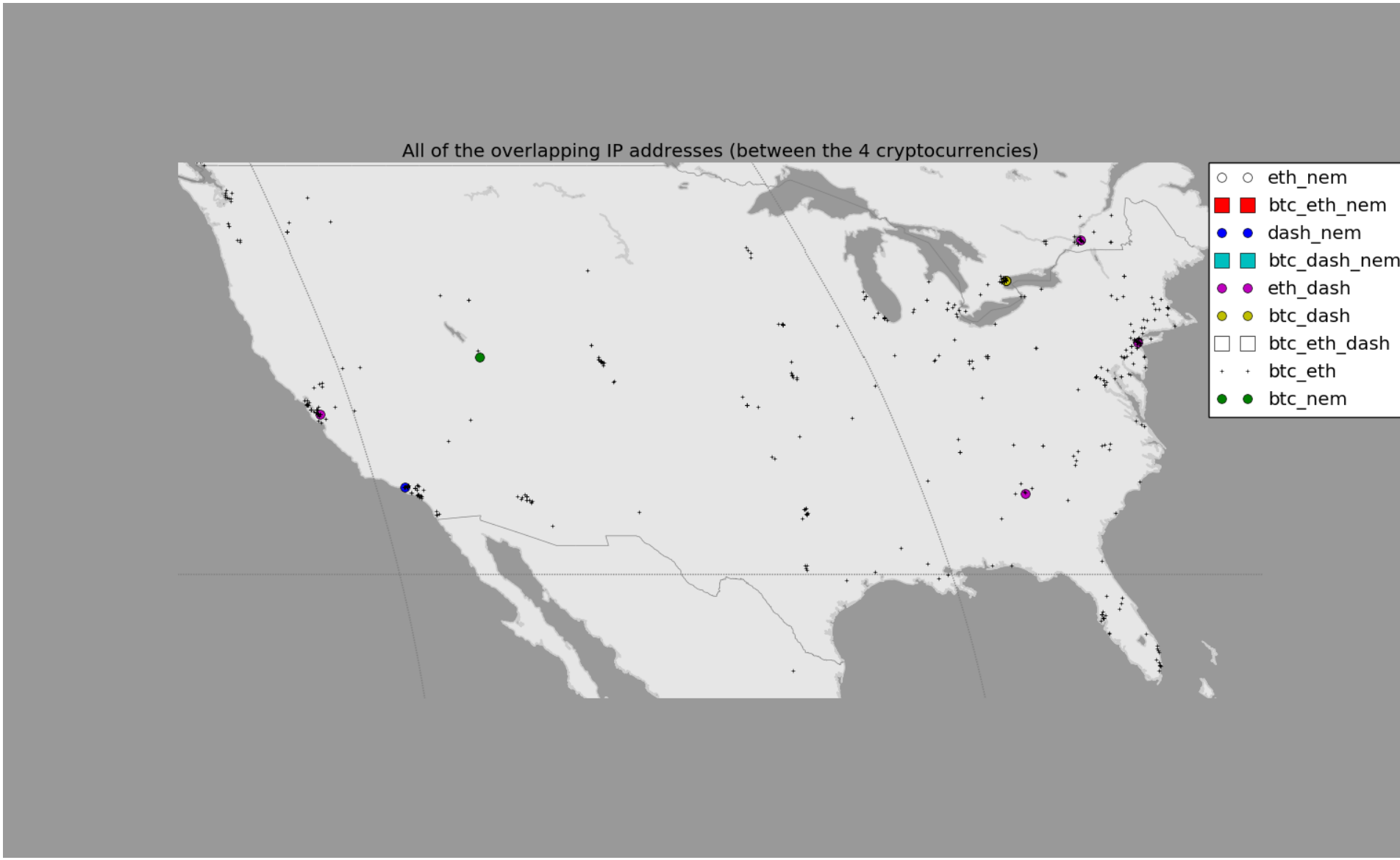
全体(世界)


All of the overlapping IP addresses (between the 4 cryptocurrencies)
eth_nem
btc_eth_nem
dash_nem
btc_dash_nem
eth_dash
btc_dash
btc_eth_dash
btc_eth
btc_nem

全体(拡大:ヨーロッパ)


All of the overlapping IP addresses (between the 4 cryptocurrencies)
eth_nem
btc_eth_nem
dash_nem
btc_dash_nem
eth_dash
btc_dash
btc_eth_dash
btc_eth
btc_nem

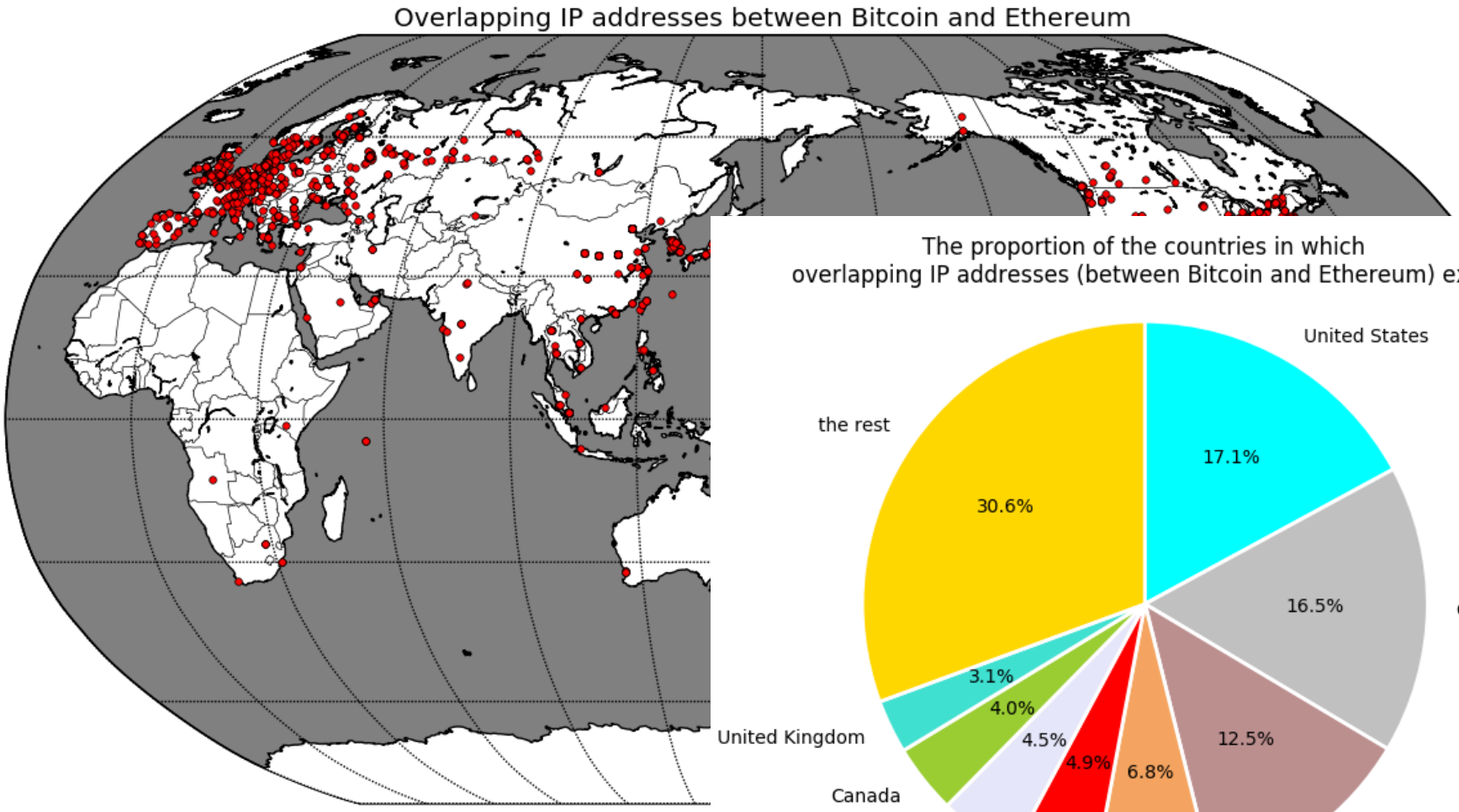
全体(拡大:アメリカ)


All of the overlapping IP addresses (between the 4 cryptocurrencies)
eth_nem
btc_eth_nem
dash_nem
btc_dash_nem
eth_dash
btc_dash
btc_eth_dash
btc_eth
btc_nem

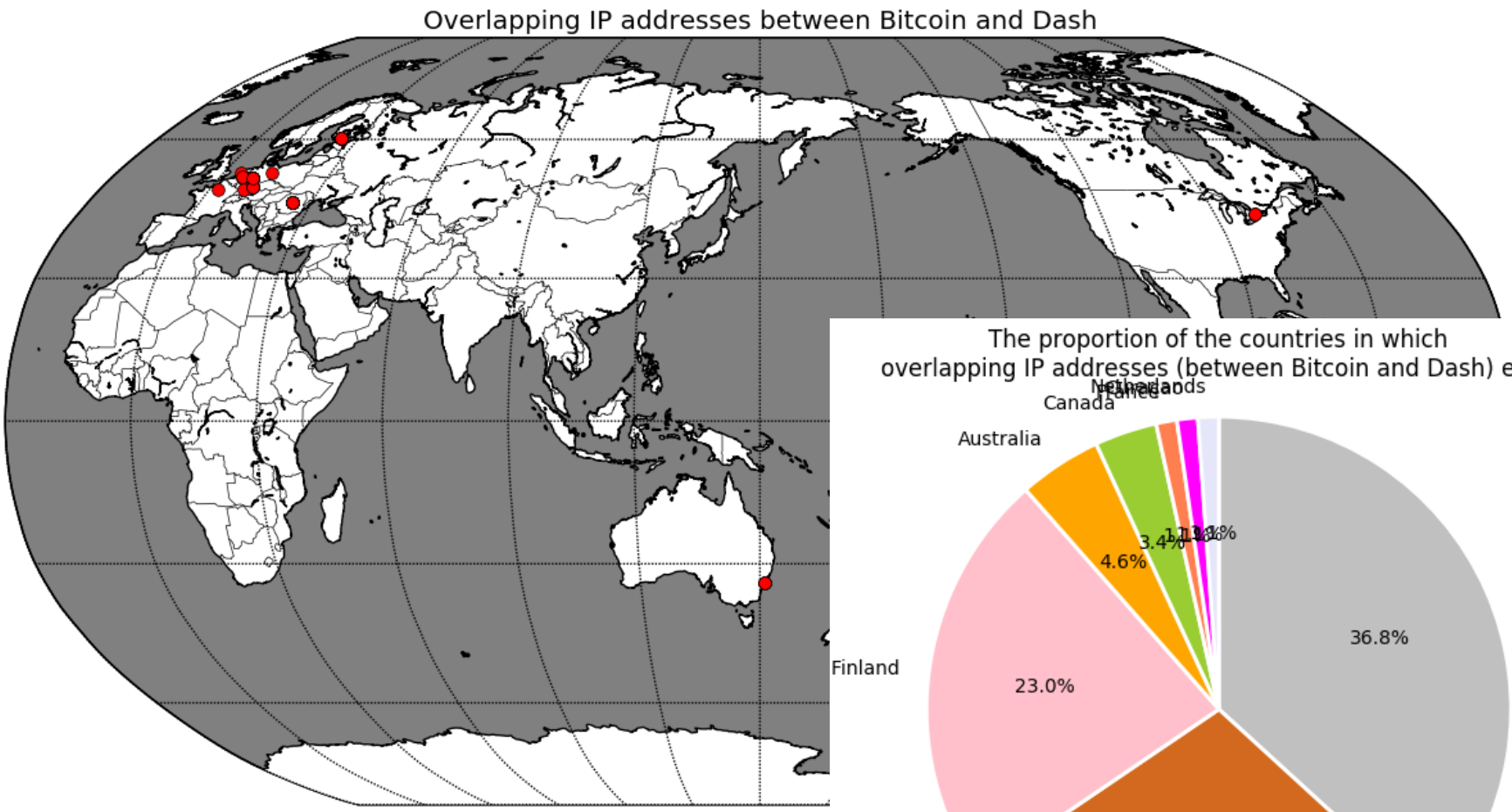
全体(拡大：東アジア)


All of the overlapping IP addresses (between the 4 cryptocurrencies)
eth_nem
btc_eth_nem
dash_nem
btc_dash_nem
eth_dash
btc_dash
btc_eth_dash
btc_eth
btc_nem

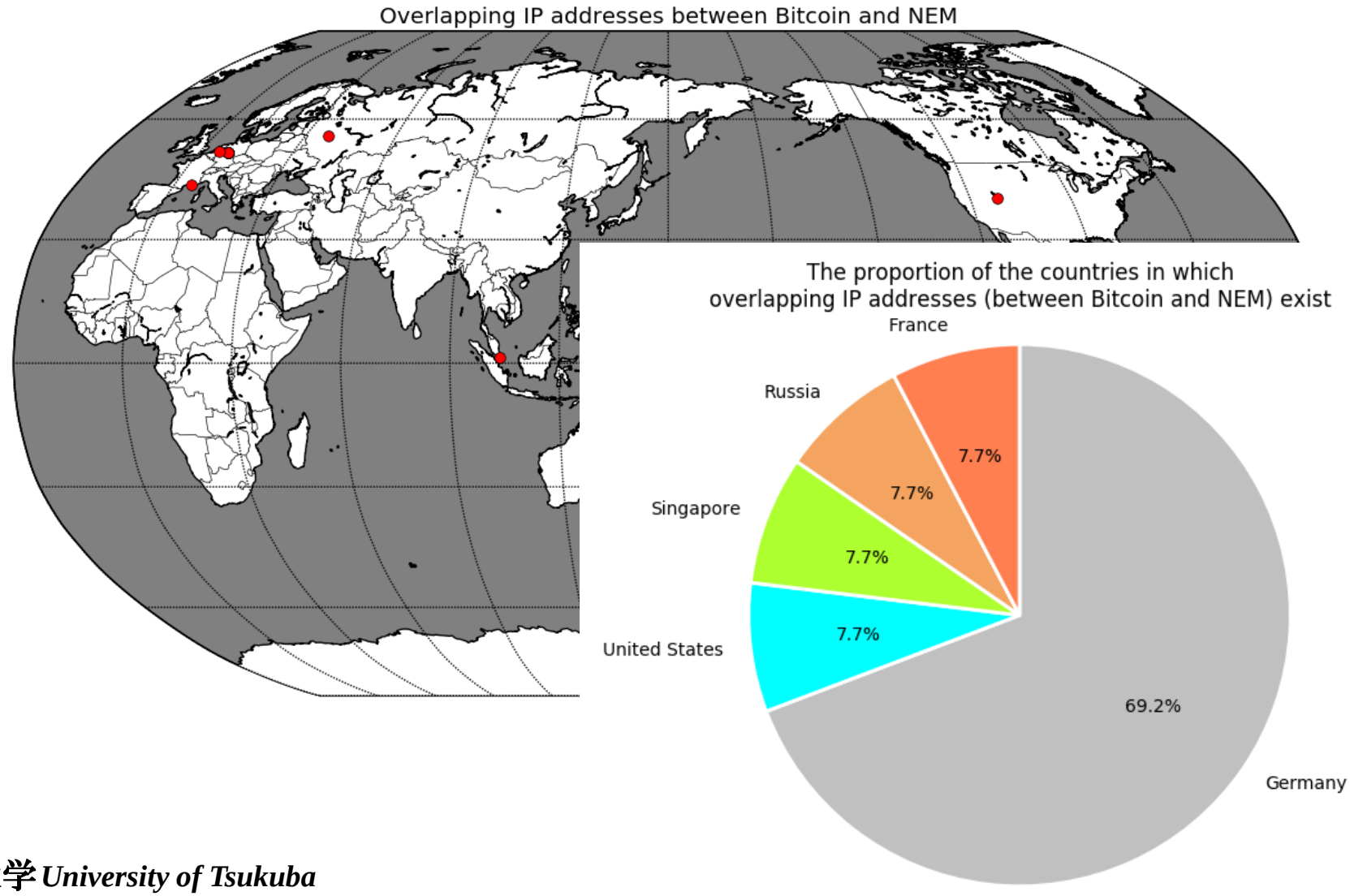
Bitcoin_ethream



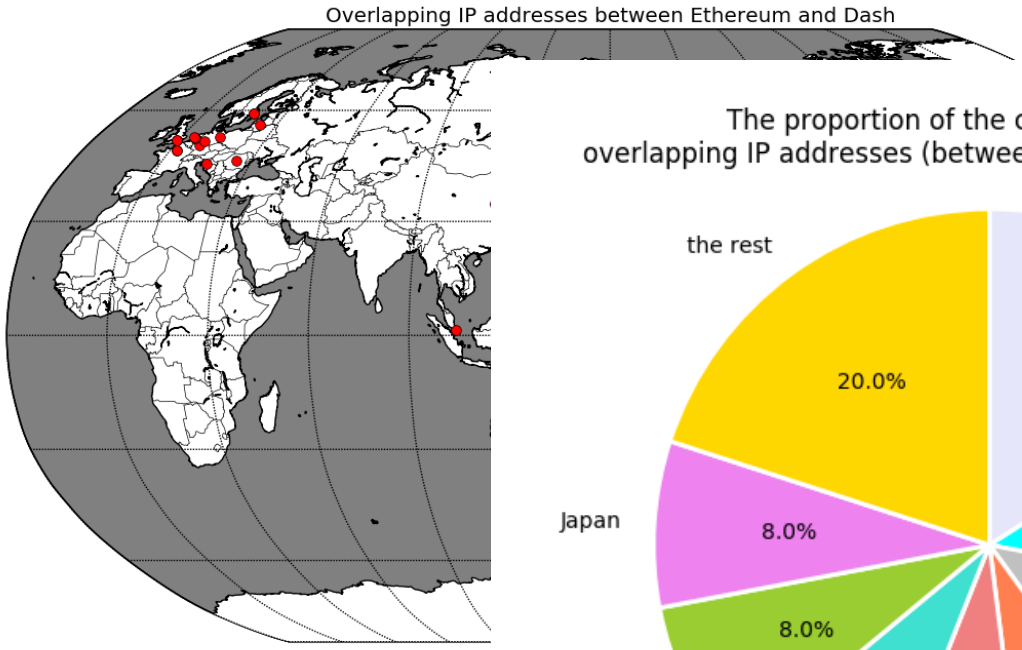
Bitcoin_Dash

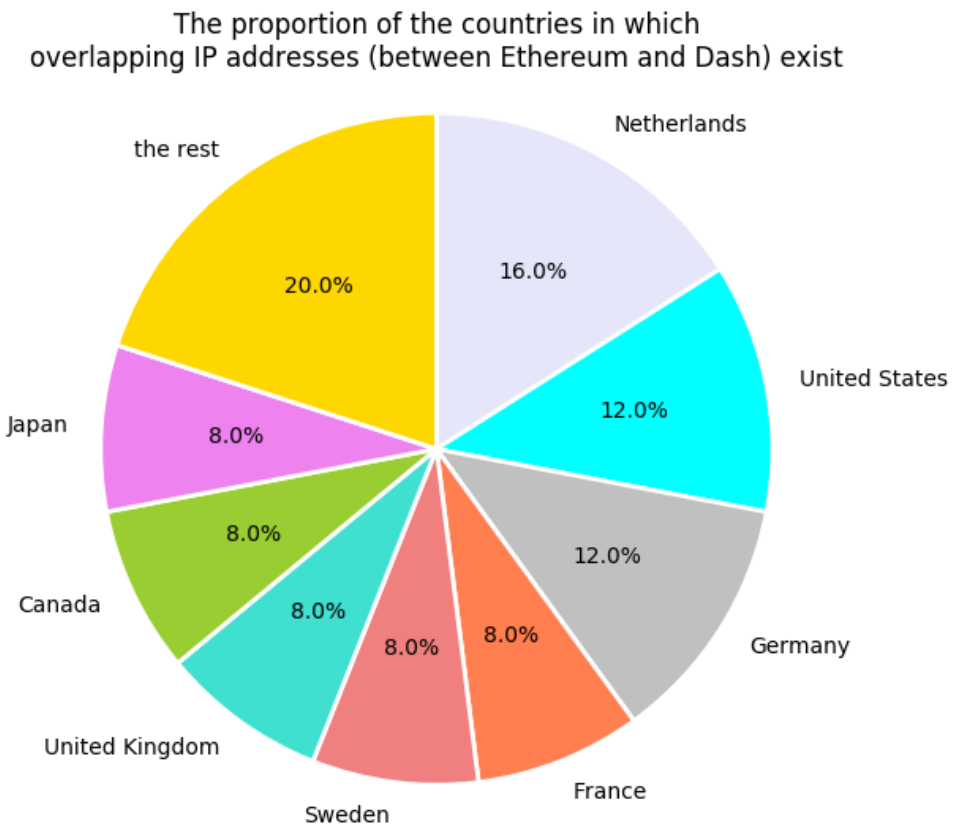


Bitcoin_nem

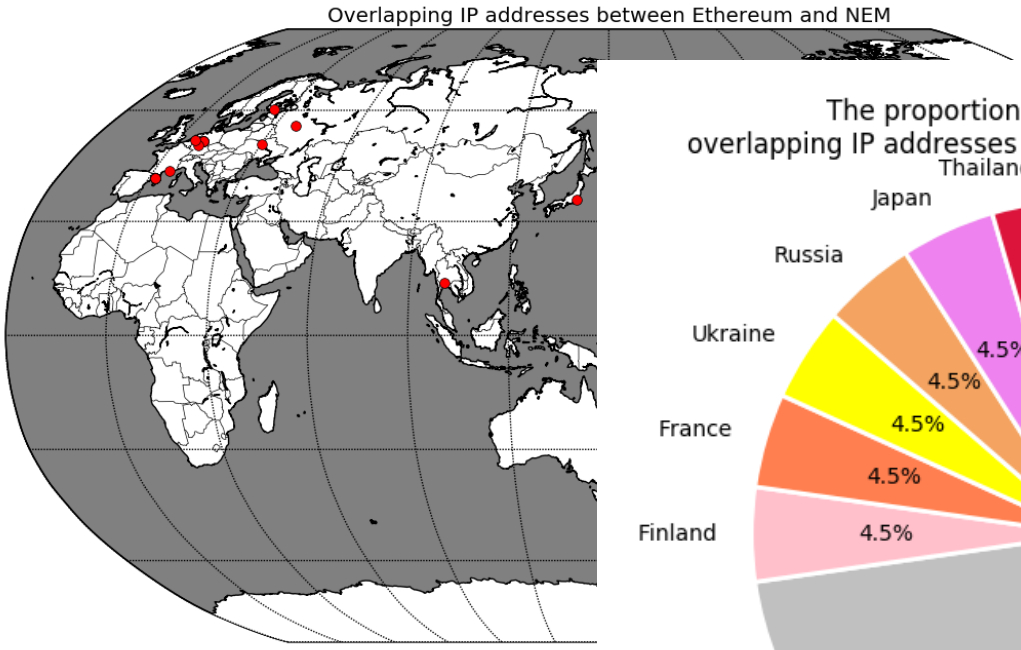

Overlapping IP addresses between Bitcoin and NEM
The proportion of the countries in which
overlapping IP addresses (between Bitcoin and NEM) exist
France
Russia
Singapore
United States
Germany
7.7%
7.7%
7.7%
7.7%
69.2%

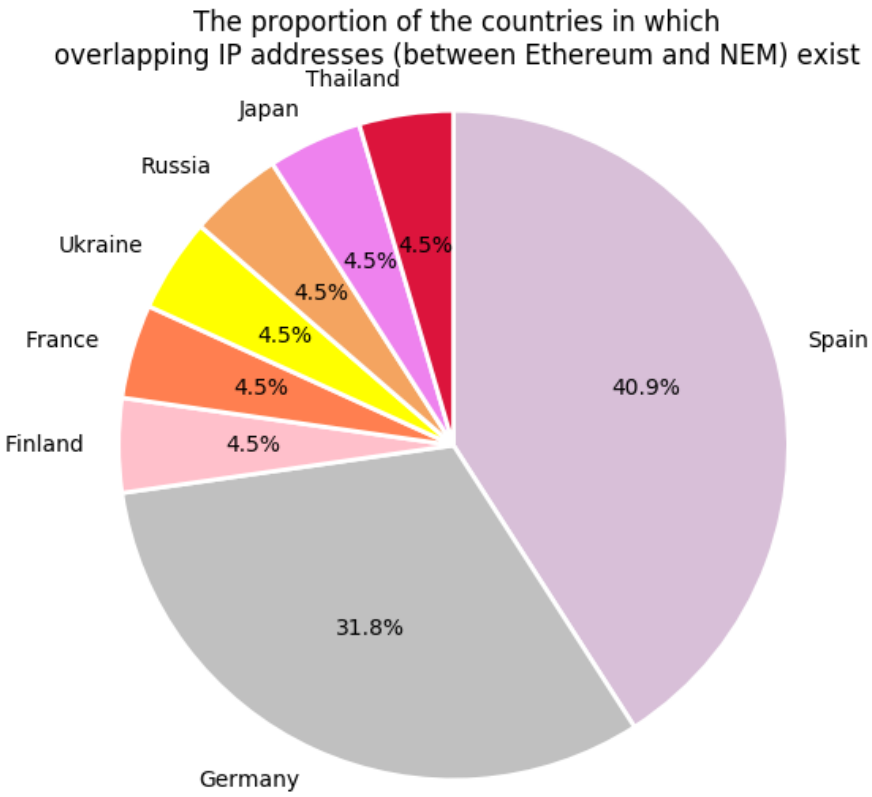
Ethream_Dash



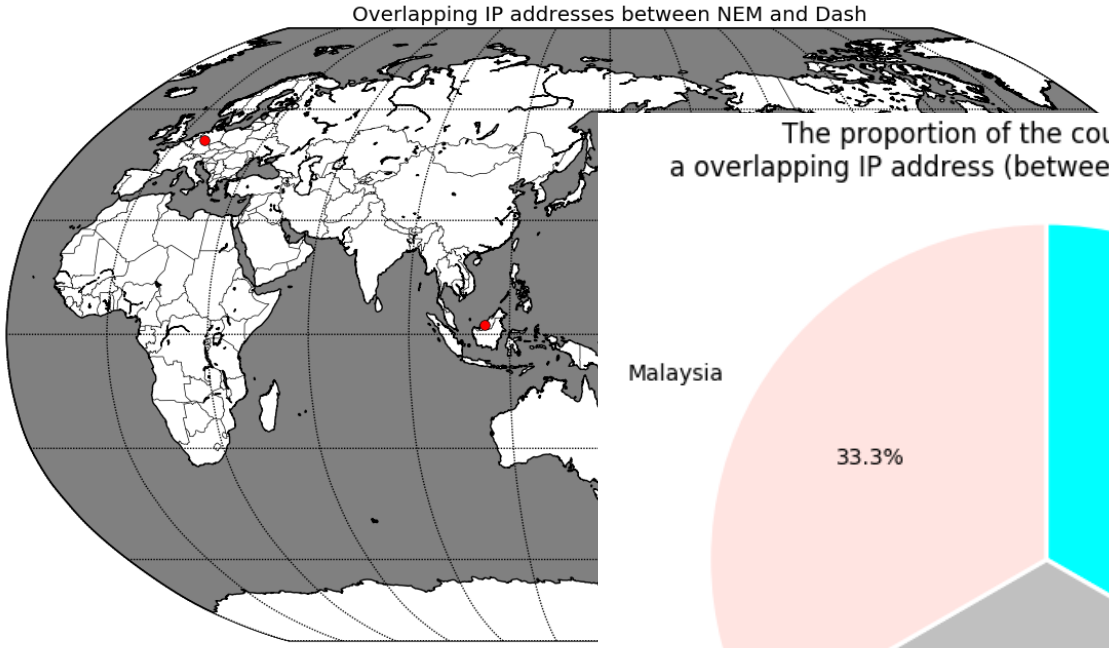


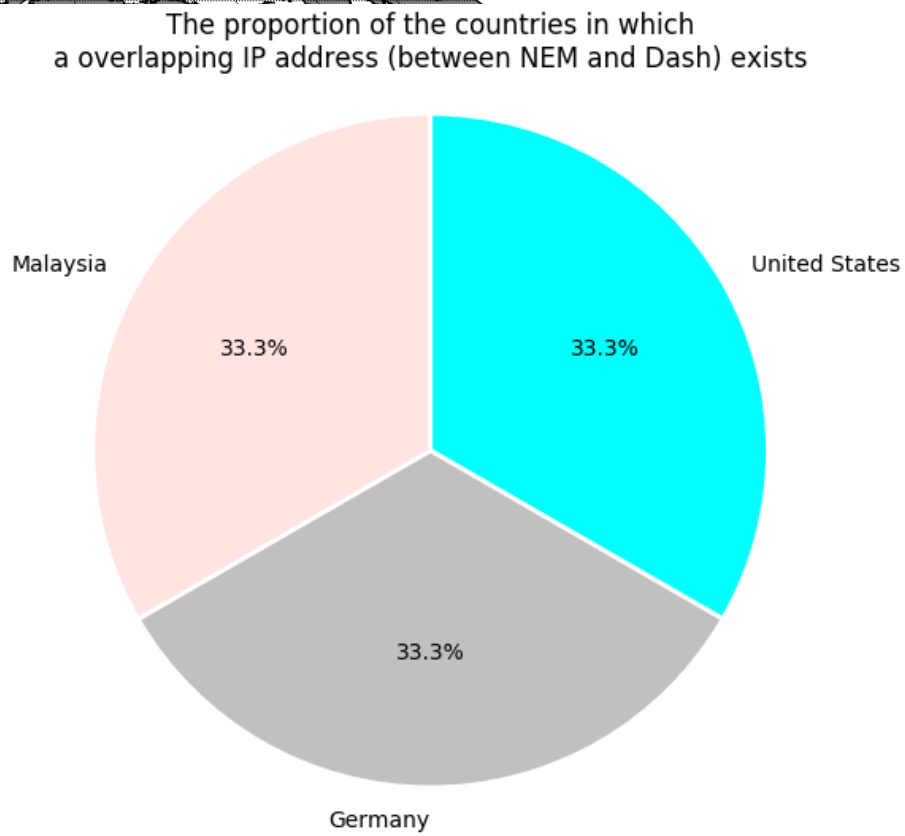
Ethream_NEM


Overlapping IP addresses between Ethereum and NEM

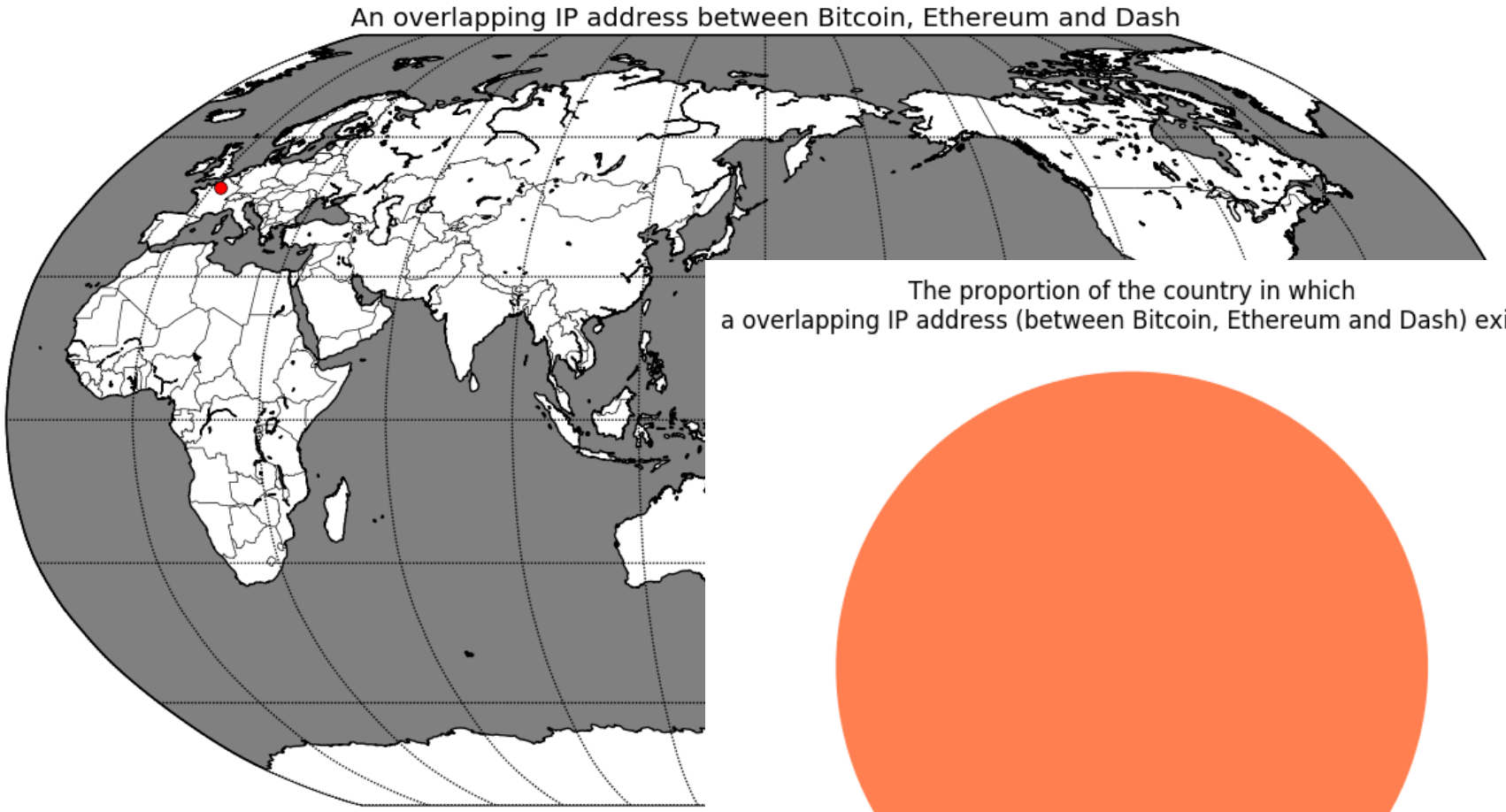

The proportion of the countries in which
overlapping IP addresses (between Ethereum and NEM) exist
Thailand
Japan
Russia
Ukraine
France
Finland
Germany
Spain
4.5%
4.5%
4.5%
4.5%
4.5%
4.5%
40.9%
31.8%

NEM_Dash


Overlapping IP addresses between NEM and Dash

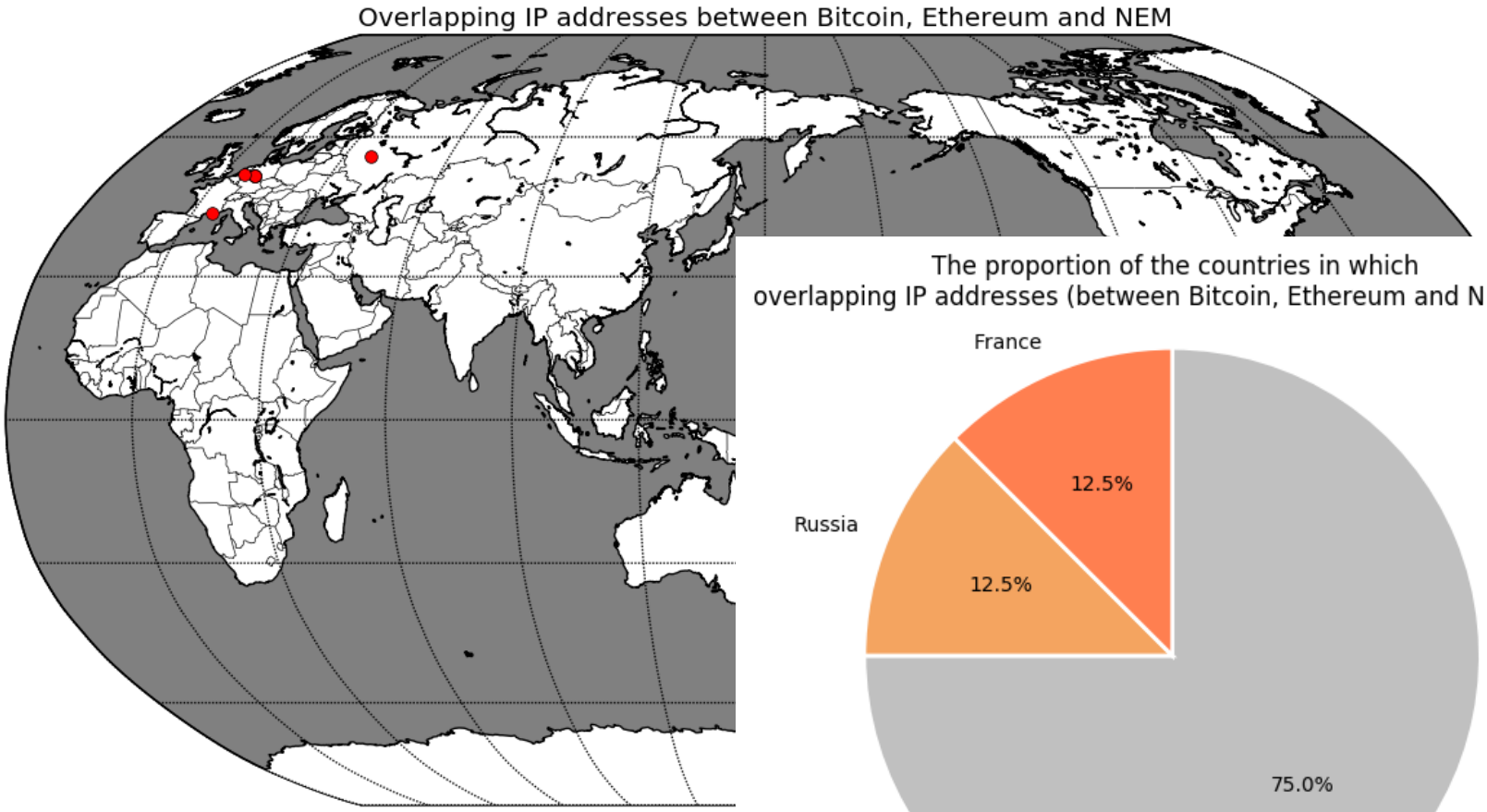

The proportion of the countries in which
a overlapping IP address (between NEM and Dash) exists
Malaysia
United States
33.3%
33.3%
33.3%
Germany

Bitcoin_Ethream_Dash

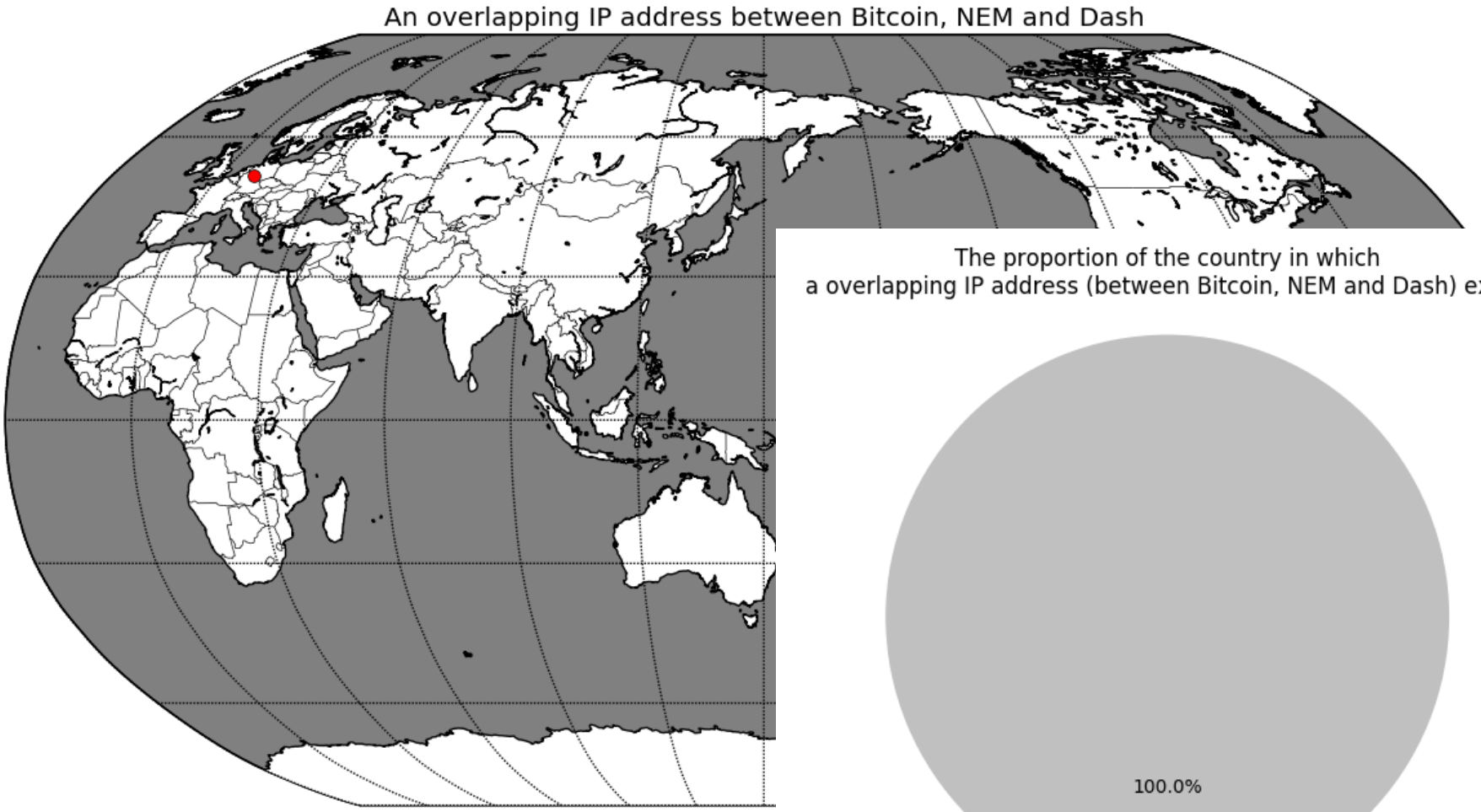


The proportion of the country in which
a overlapping IP address (between Bitcoin, Ethereum and Dash) exists

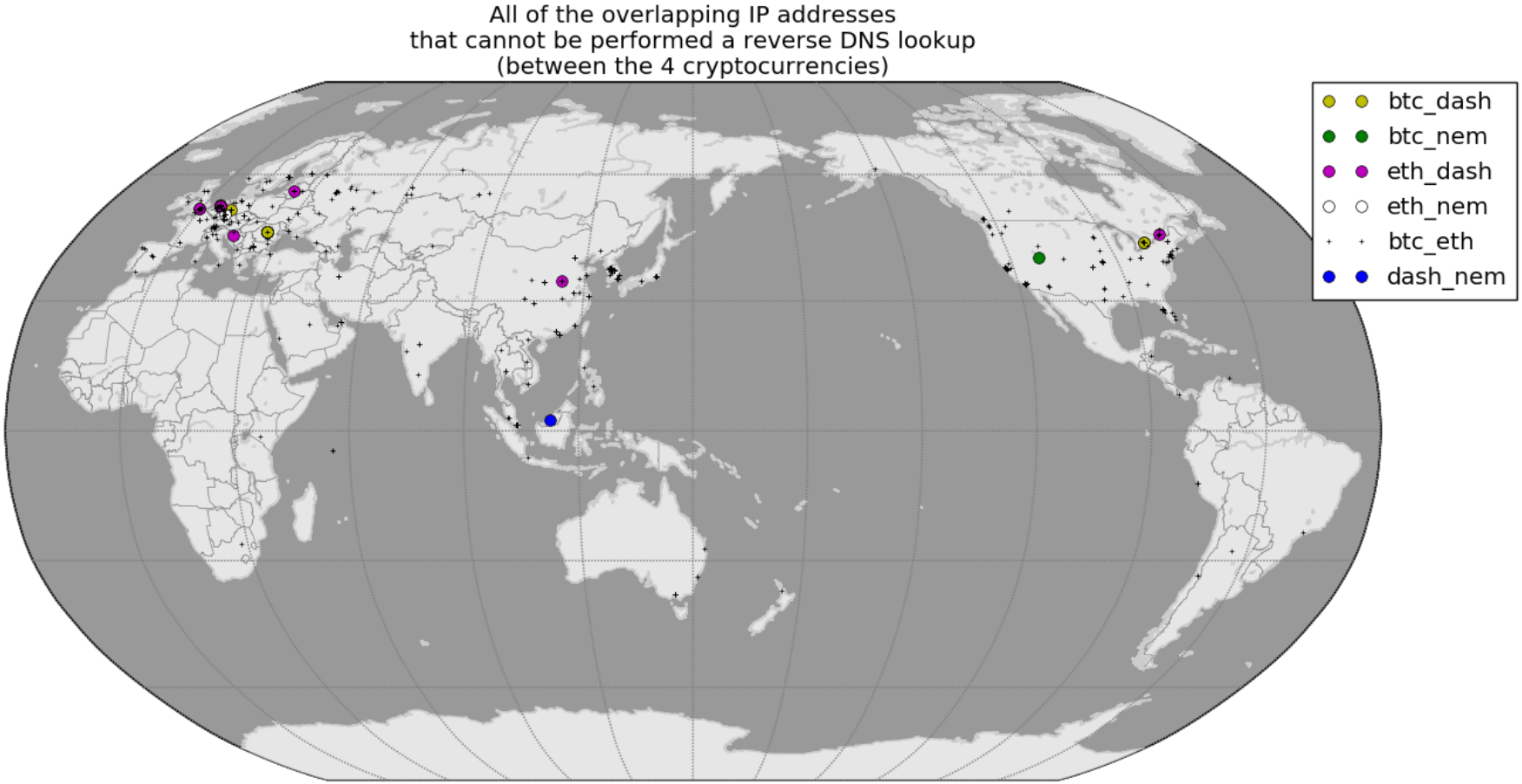
Bitcoin_Ethream_NEM



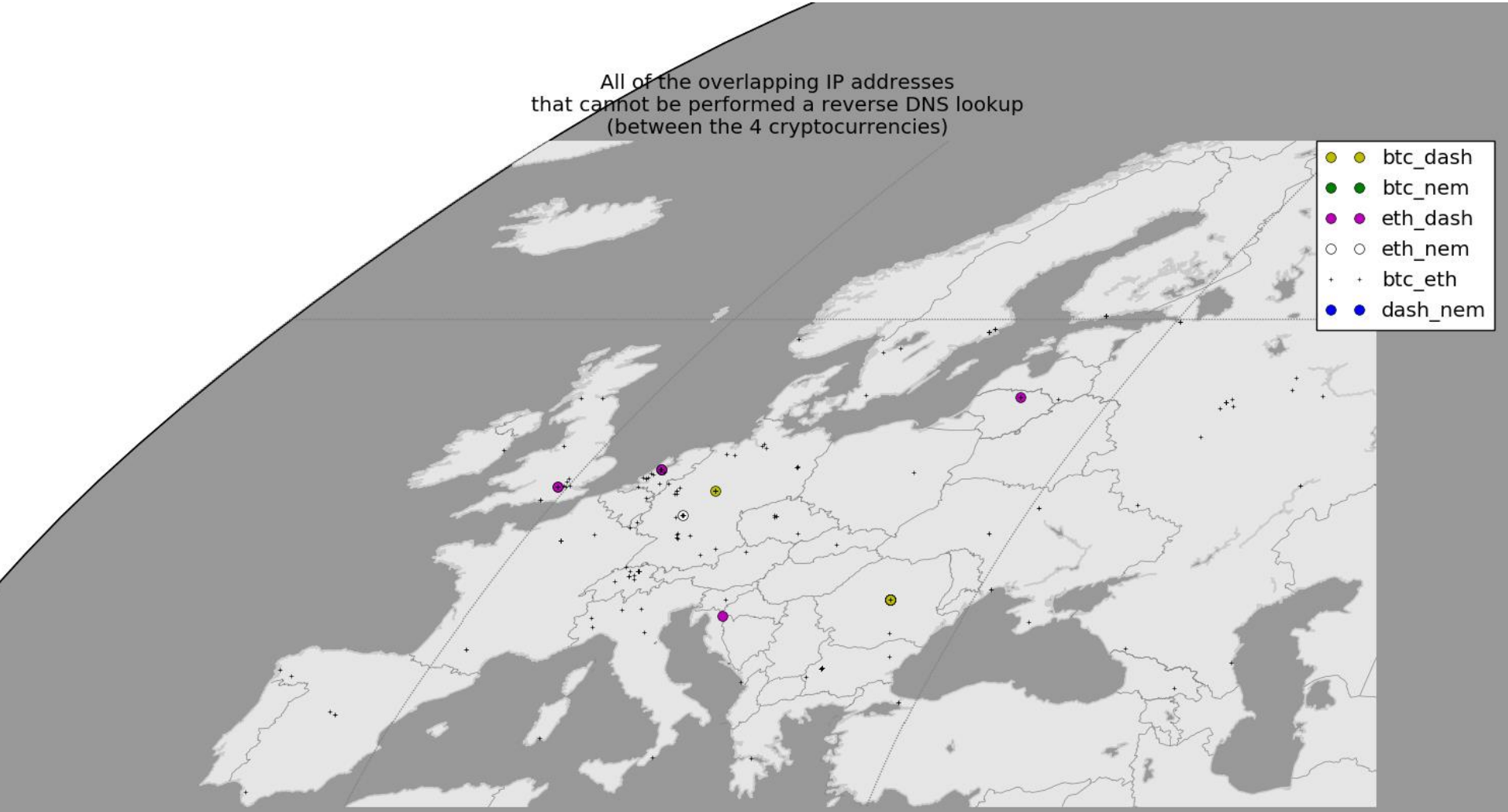
Bitcoin_NEM_Dash



全体(世界)(N/A)


All of the overlapping IP addresses
that cannot be performed a reverse DNS lookup
(between the 4 cryptocurrencies)
btc_dash
btc_nem
eth_dash
eth_nem
btc_eth
dash_nem

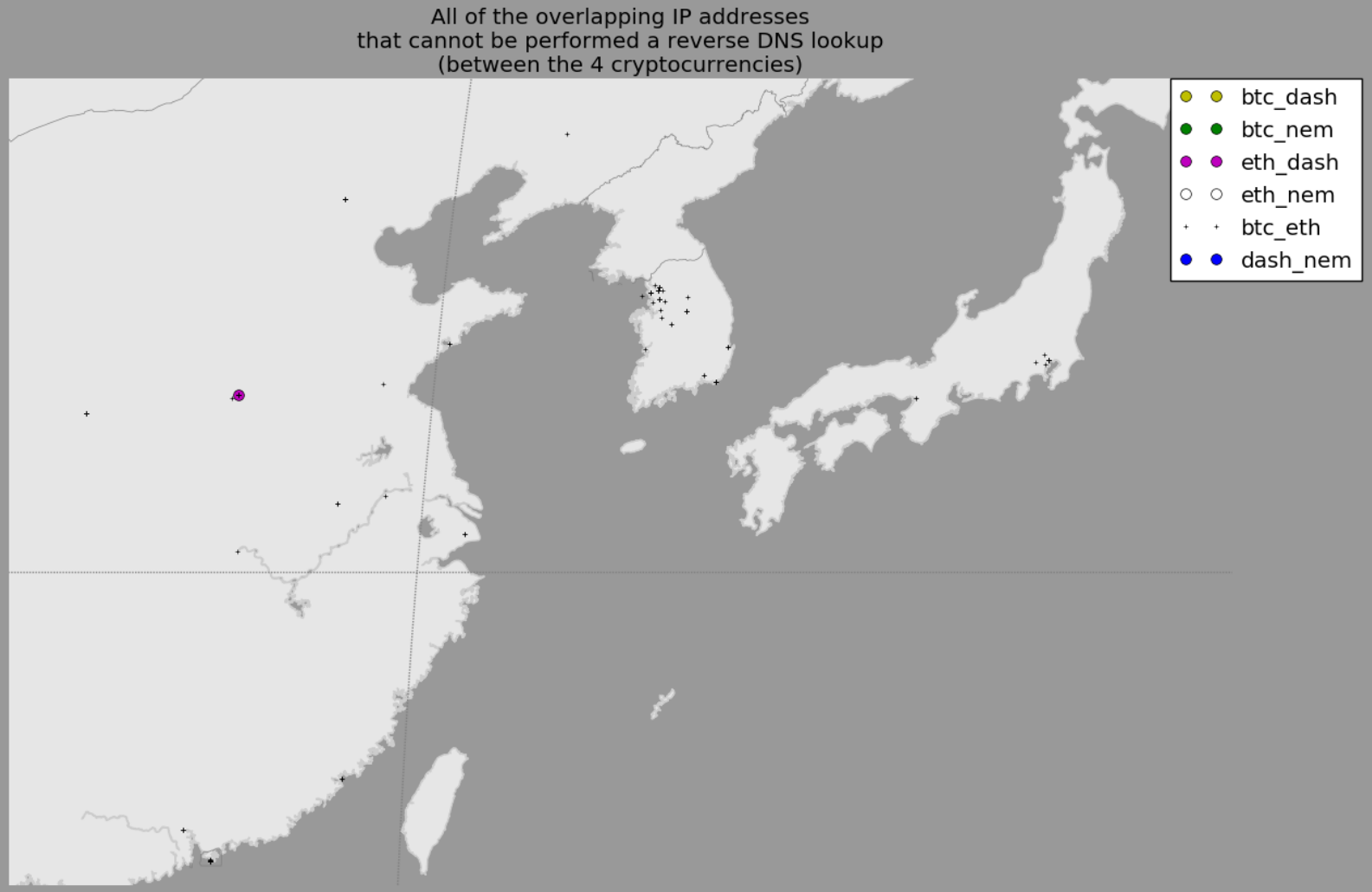
全体(拡大:ヨーロッパ)(N/A)



全体(拡大:アメリカ)(N/A)


All of the overlapping IP addresses
that cannot be performed a reverse DNS lookup
(between the 4 cryptocurrencies)
btc_dash
btc_nem
eth_dash
eth_nem
btc_eth
dash_nem

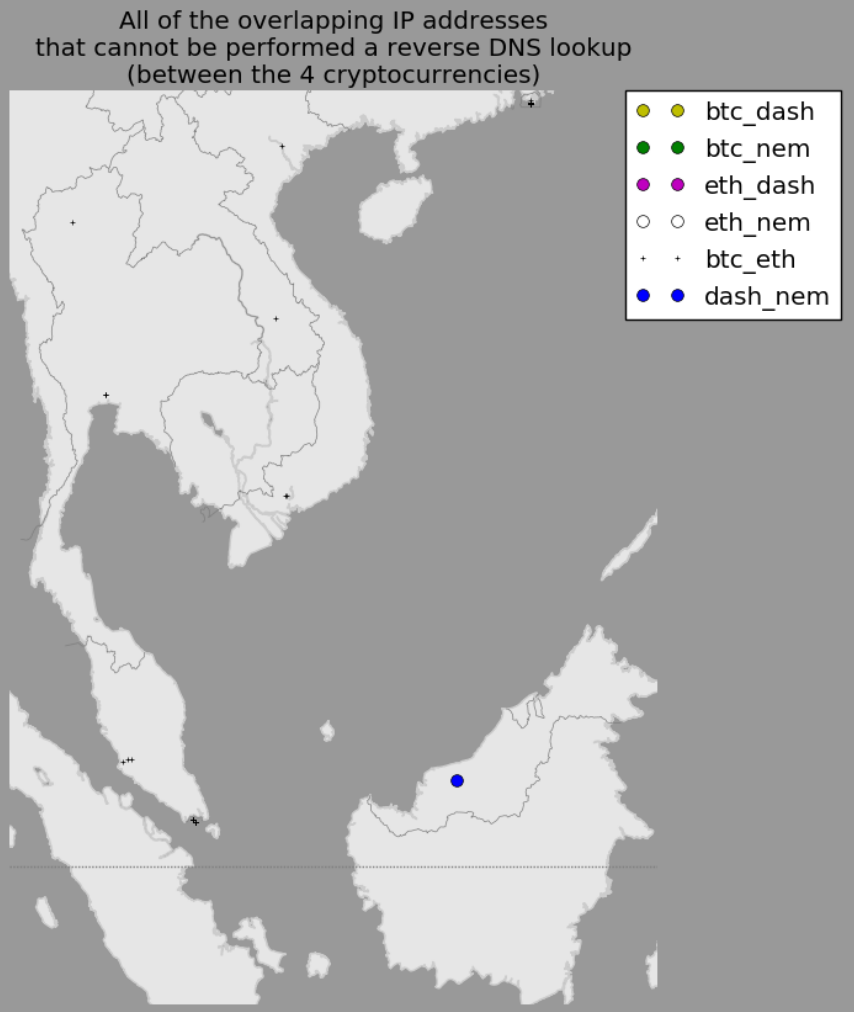
全体(拡大:東アジア)(N/A)


All of the overlapping IP addresses
that cannot be performed a reverse DNS lookup
(between the 4 cryptocurrencies)
btc_dash
btc_nem
eth_dash
eth_nem
btc_eth
dash_nem

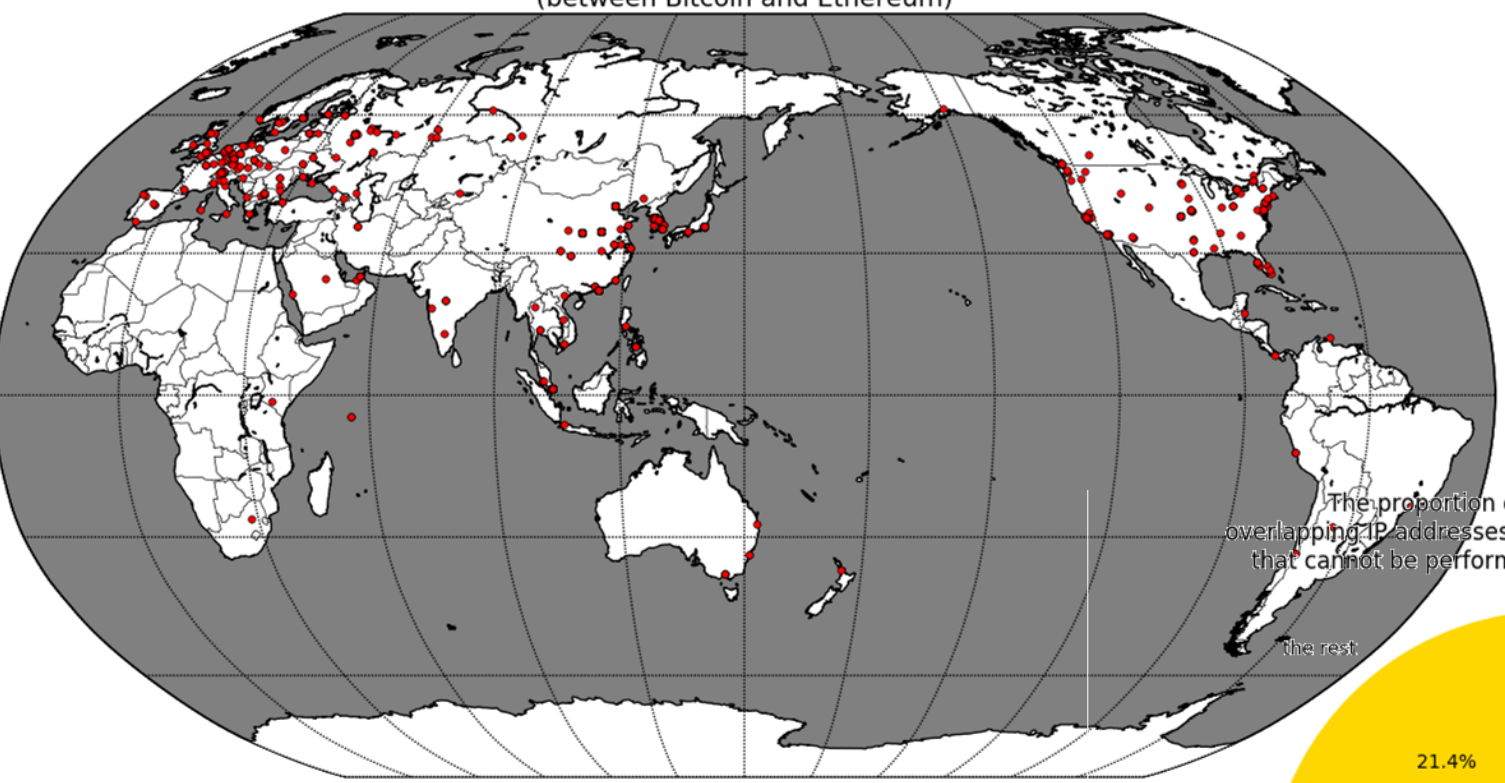
全体(拡大:カリブ)(N/A)

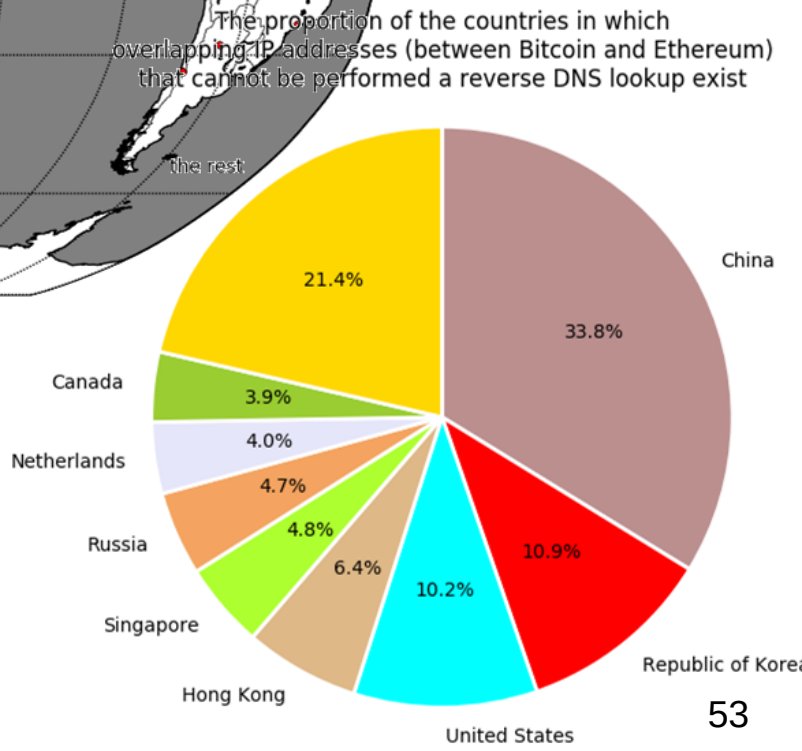

All of the overlapping IP addresses
that cannot be performed a reverse DNS lookup
(between the 4 cryptocurrencies)
btc_dash
btc_nem
eth_dash
eth_nem
btc_eth
dash_nem

全体(拡大:東南アジア)(N/A)

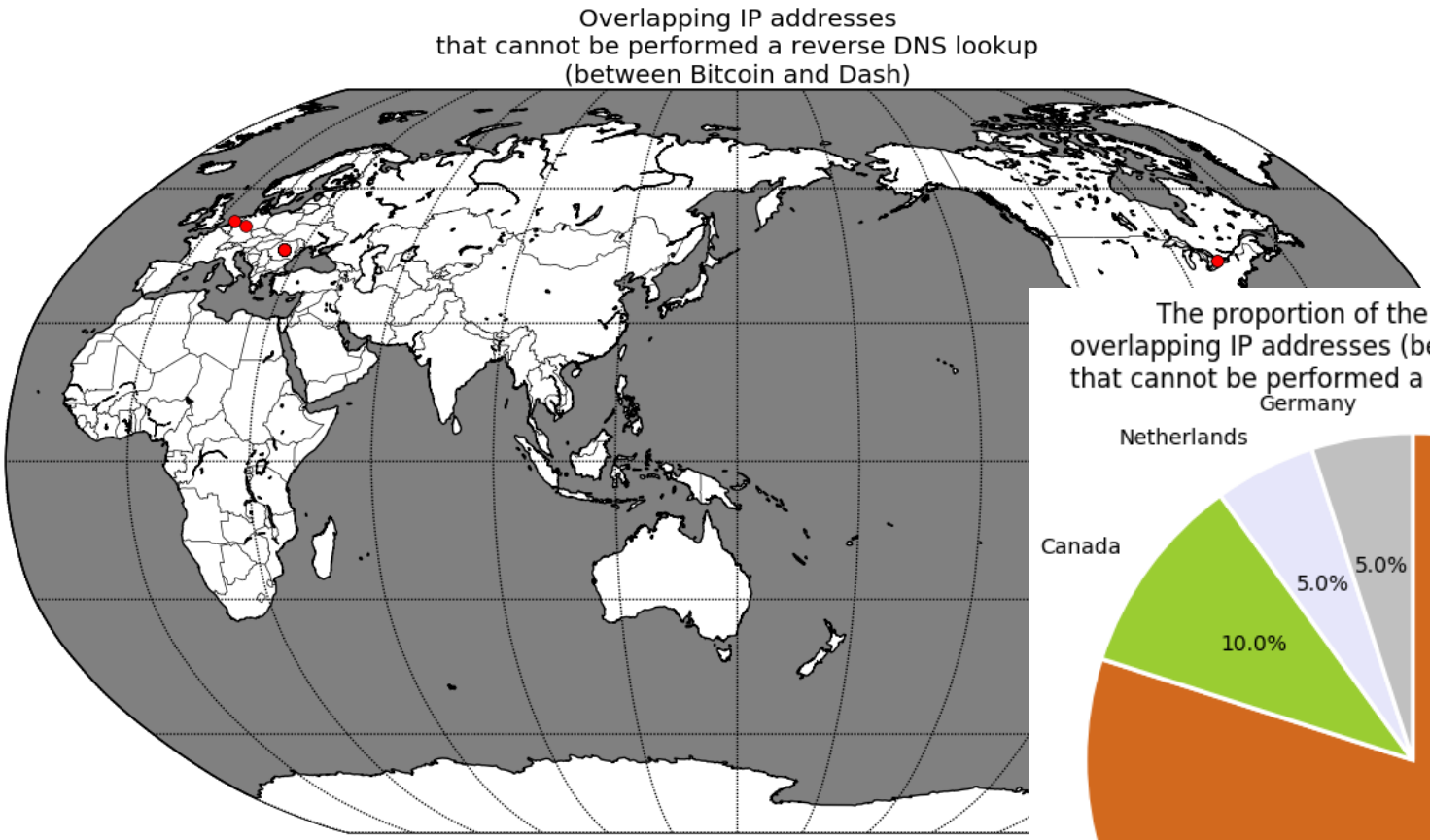


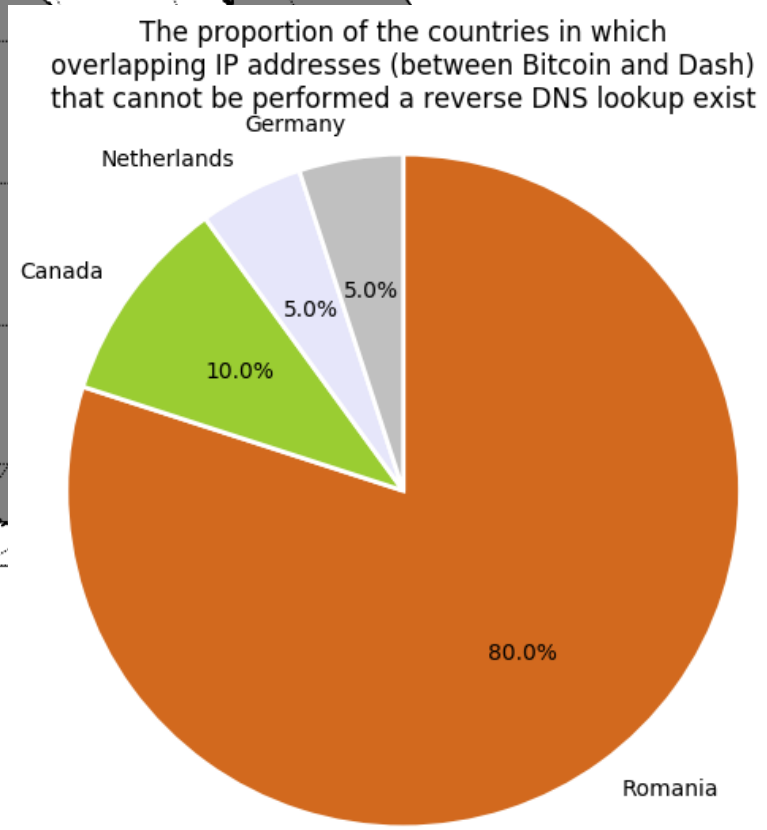
Bitcoin_ethream(N/A)





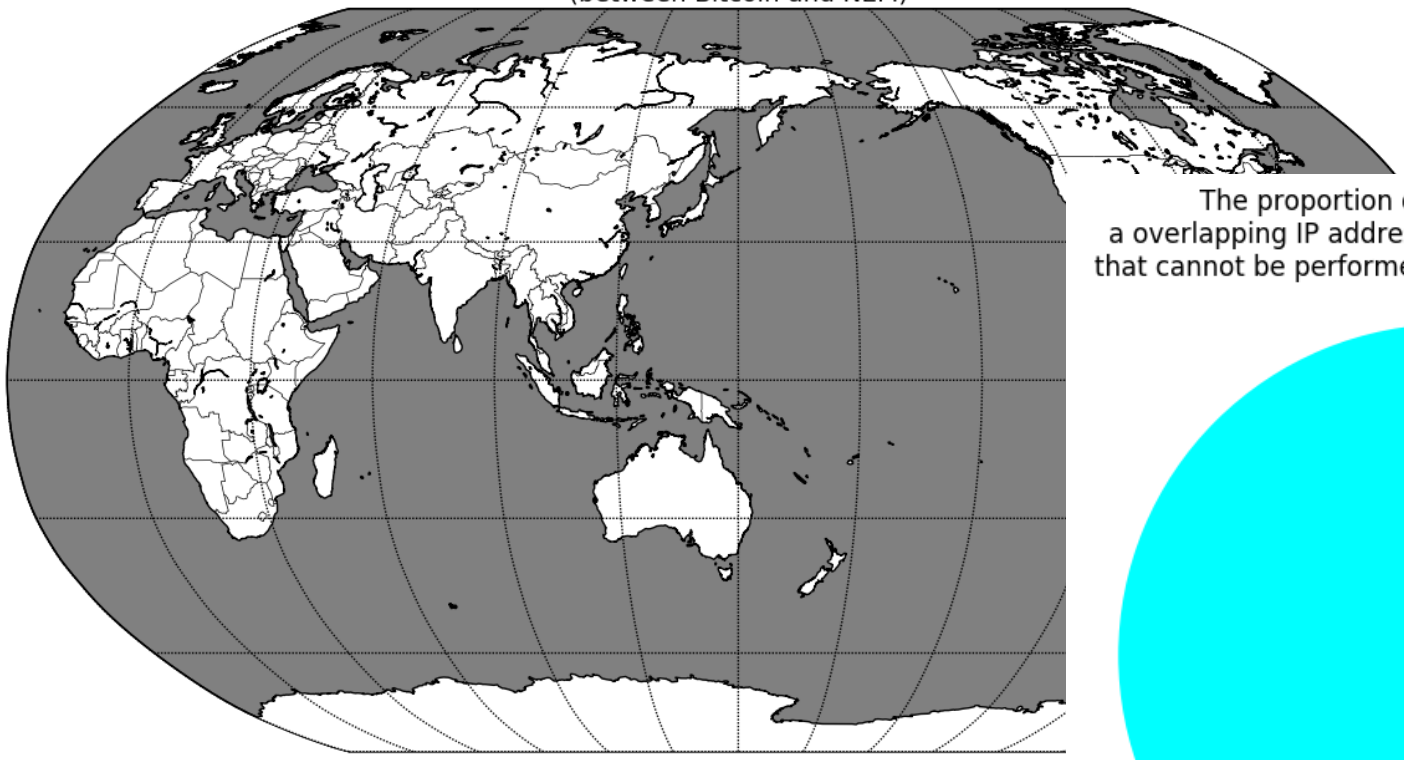
Bitcoin_Dash(N/A)



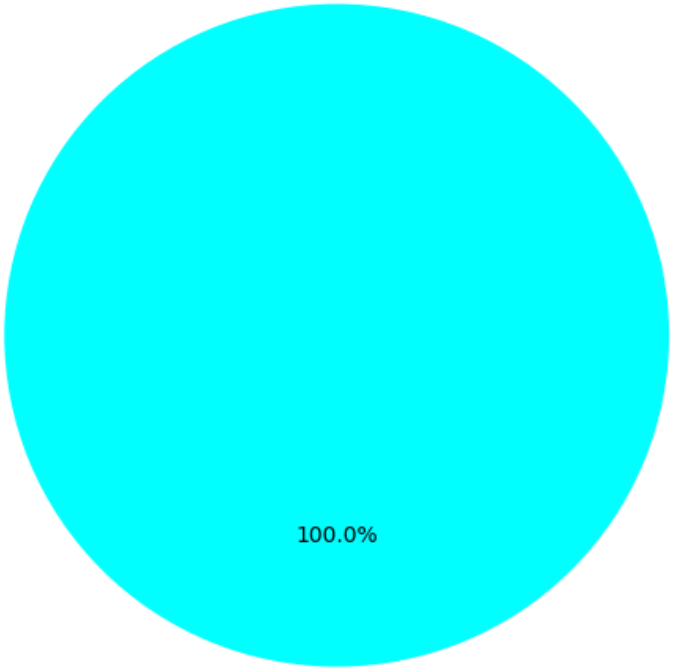


Bitcoin_nem(N/A)

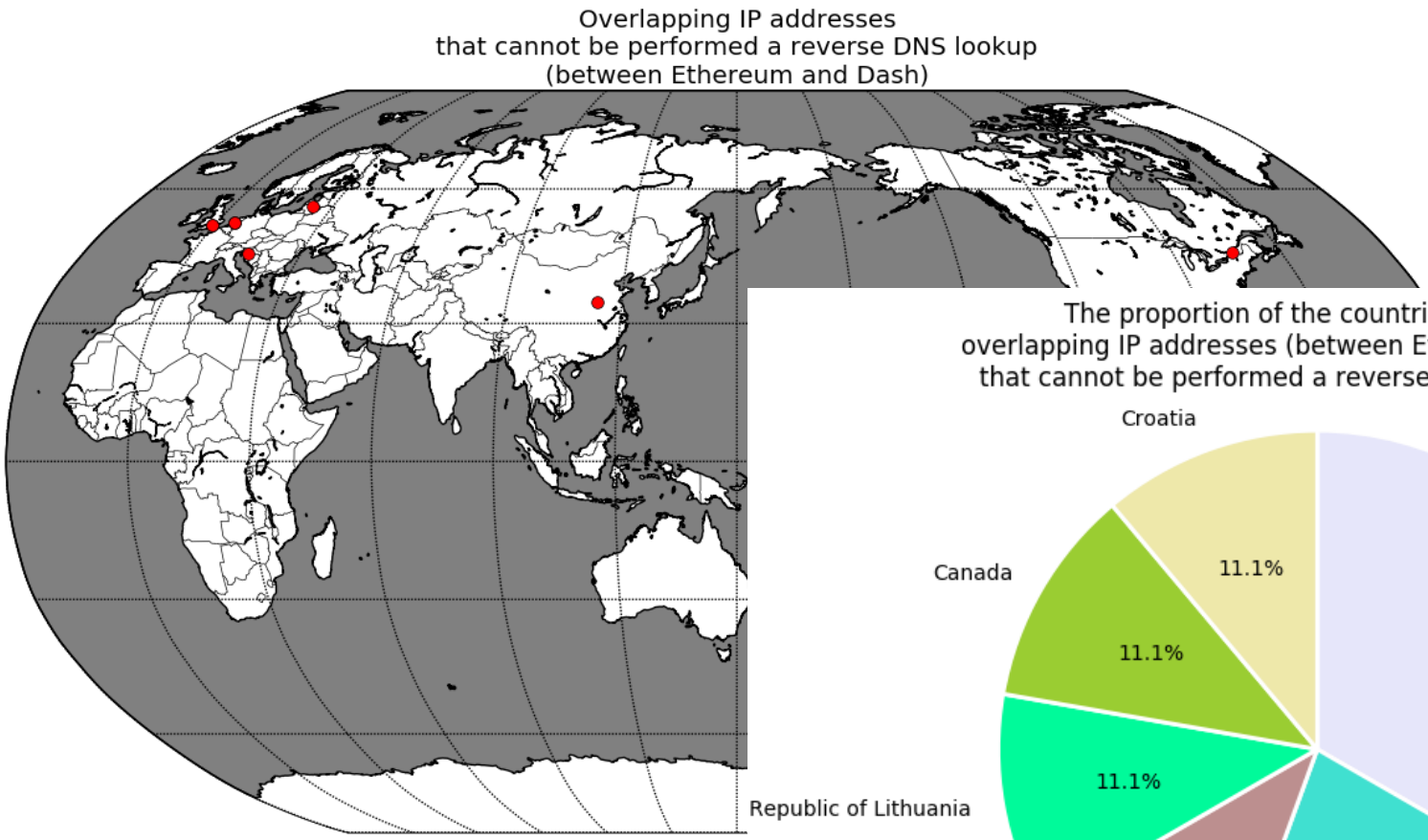
An overlapping IP address
that cannot be performed a reverse DNS lookup
(between Bitcoin and NEM)

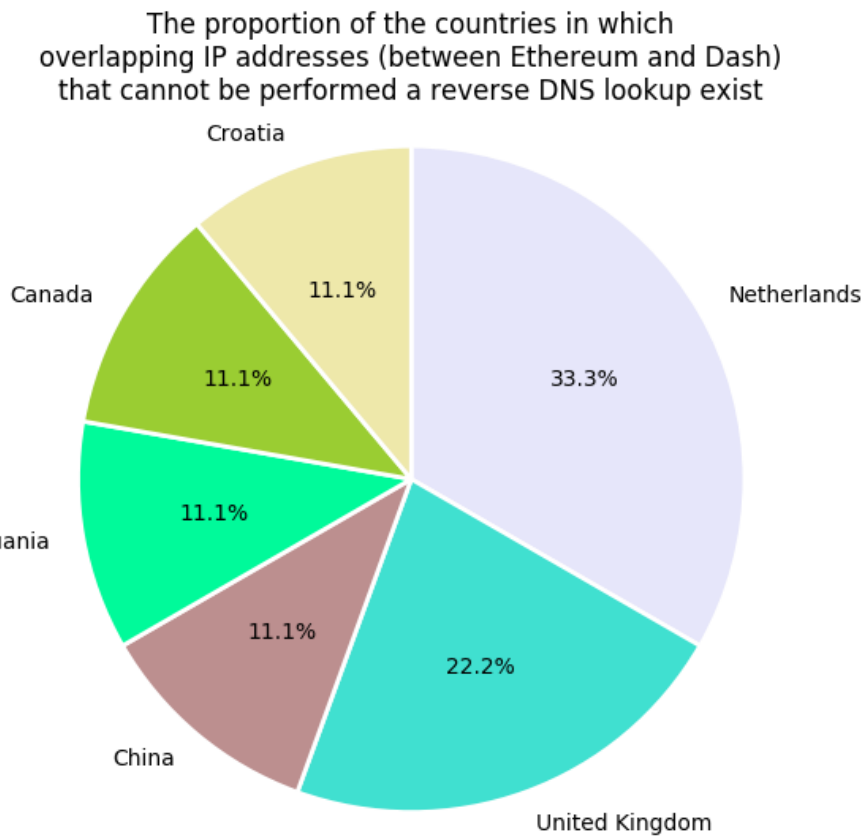


The proportion of the country in which
a overlapping IP address (between Bitcoin and NEM)
that cannot be performed a reverse DNS lookup exists



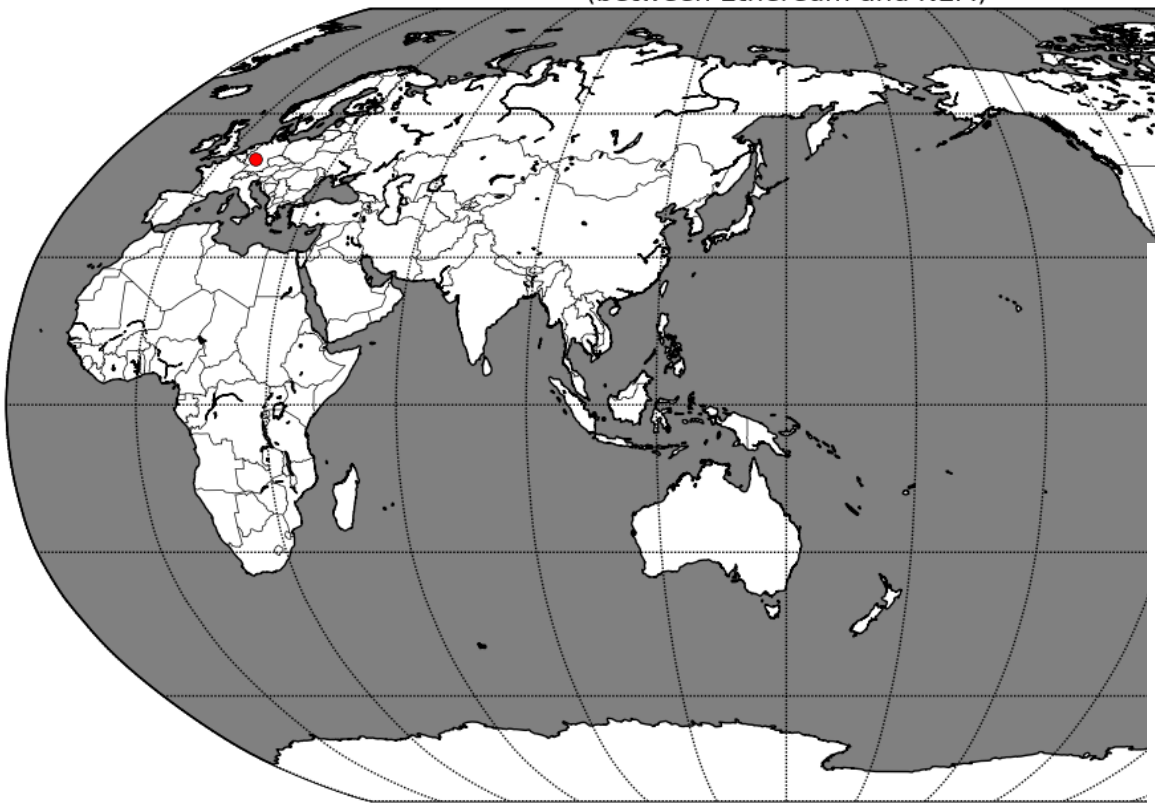
Ethream_Dash(N/A)



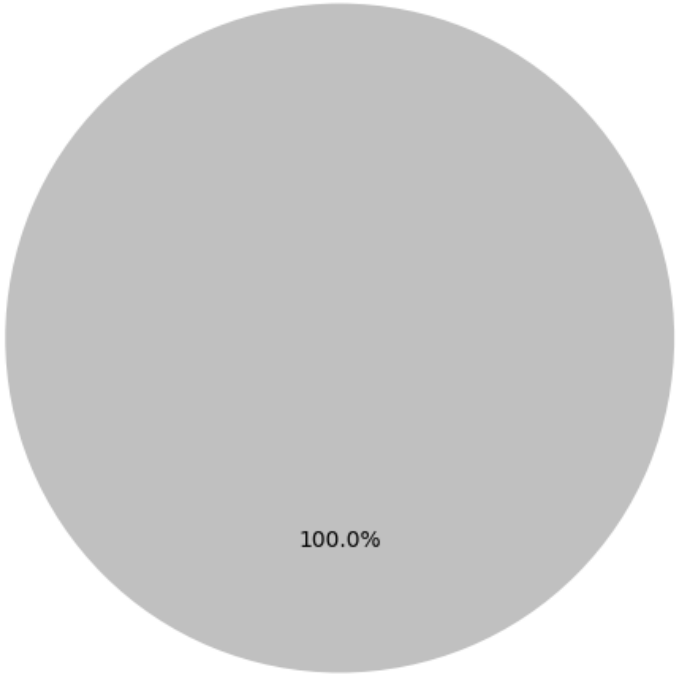


Ethream_NEM(N/A)

An overlapping IP address
that cannot be performed a reverse DNS lookup
(between Ethereum and NEM)

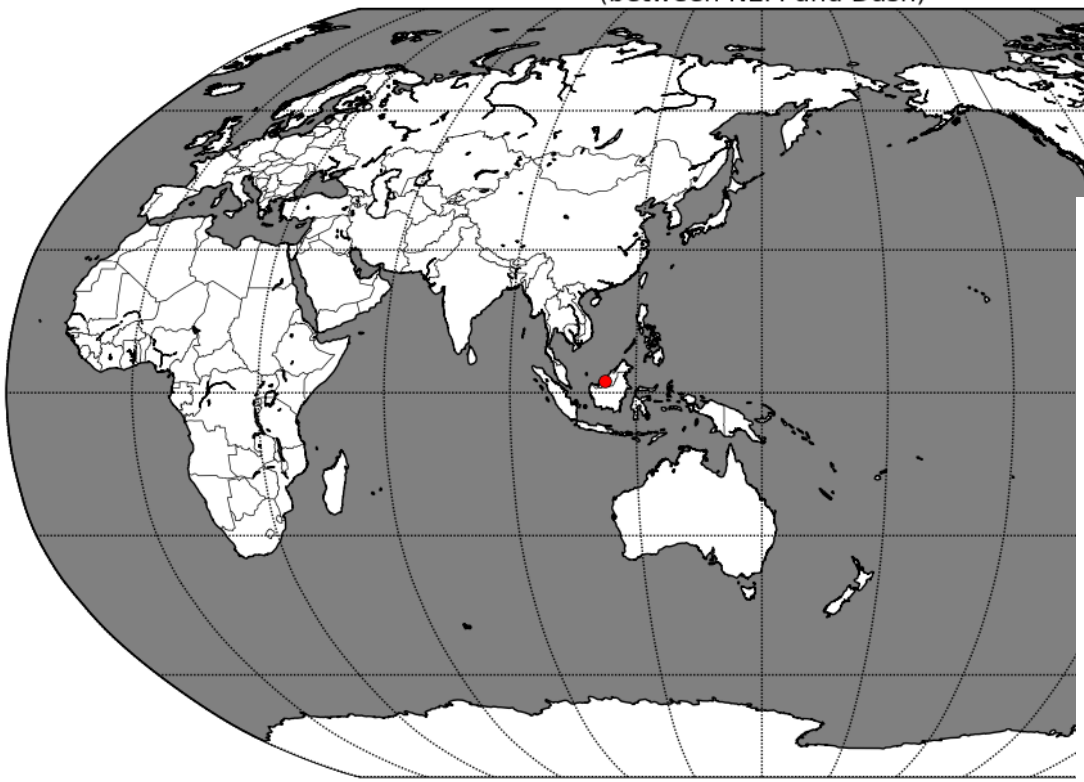


The proportion of the country in which
a overlapping IP address (between Ethereum and NEM)
that cannot be performed a reverse DNS lookup exists

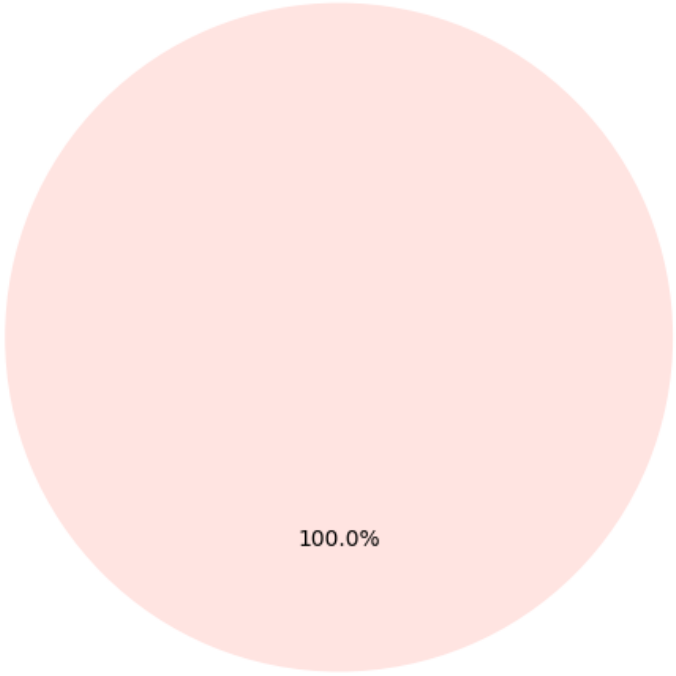


NEM_Dash(N/A)

An overlapping IP address
that cannot be performed a reverse DNS lookup
(between NEM and Dash)



The proportion of the country in which
a overlapping IP address (between NEM and Dash)
that cannot be performed a reverse DNS lookup exists



時価総額ランキング10月19日

仮想通貨時価総額上位100

仮想通貨 ▾ | 取引所 ▾ | ウォッチリスト | JPY ▾ | 次の100 → | すべて見る

#	名前	時価総額	値段	ボリューム（24時間）	循環サプライ	変化（24時間）	値段表（七日間）
1	Bitcoin	¥12,610,356,602,115	¥727,685	¥442,155,338,947	17,329,412 BTC	-0.94%	
2	Ethereum	¥2,347,613,166,040	¥22,868.44	¥154,174,870,343	102,657,316 ETH	-1.70%	
3	XRP	¥2,059,999,012,741	¥51.50	¥53,276,984,667	39,997,634,397 XRP *	-2.07%	
4	Bitcoin Cash	¥854,790,458,022	¥49,098.09	¥37,053,042,357	17,409,850 BCH	-2.69%	
5	EOS	¥545,377,327,339	¥601.80	¥49,062,488,478	906,245,118 EOS *	-0.86%	
6	Stellar	¥507,974,425,448	¥26.89	¥6,687,901,789	18,891,502,889 XLM *	-0.65%	
7	Litecoin	¥347,038,850,603	¥5,903.49	¥32,466,492,517	58,785,402 LTC	-2.03%	
8	Tether	¥233,877,437,175	¥109.99	¥278,693,883,350	2,126,421,736 USDT *	0.83%	
9	Cardano	¥218,578,578,728	¥8.43	¥3,139,868,965	25,927,070,538 ADA *	-2.62%	
10	Monero	¥193,169,484,890	¥11,709.59	¥2,546,595,208	16,496,695 XMR	-1.05%	
11	TRON	¥178,310,117,068	¥2.71	¥12,333,214,748	65,748,111,645 TRX *	-0.75%	

仮想通貨とは

法定通貨

紙幣
硬貨

- 物理的形がある
- 国家がその価値を保証

代替通貨

電子マネー
デジタル通貨
ポイント

- ICチップへの記録
- 運営会社が価値を保証

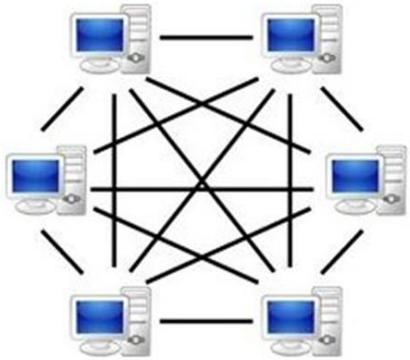
仮想通貨

- 実体がない
- 発行者がいない

bitcoin　Ethereum

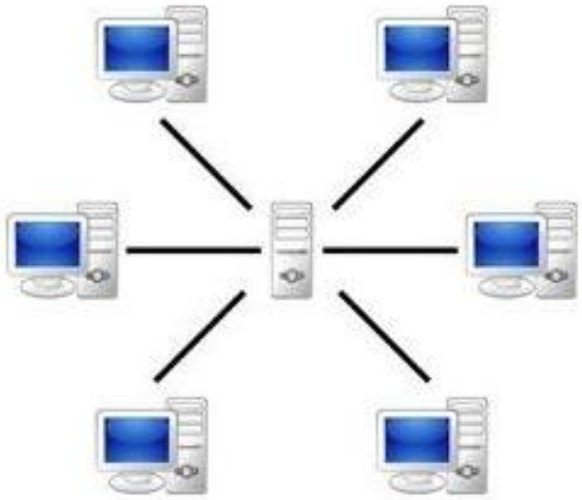
nem　DASH

分散型台帳技術
同じ台帳を参加者全員で共有
→取引を保証

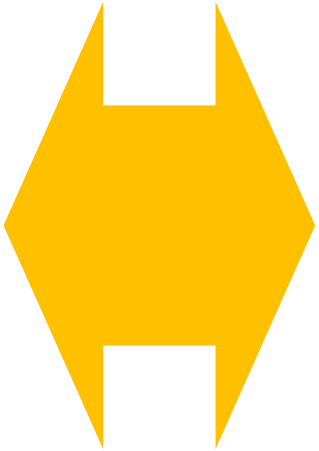


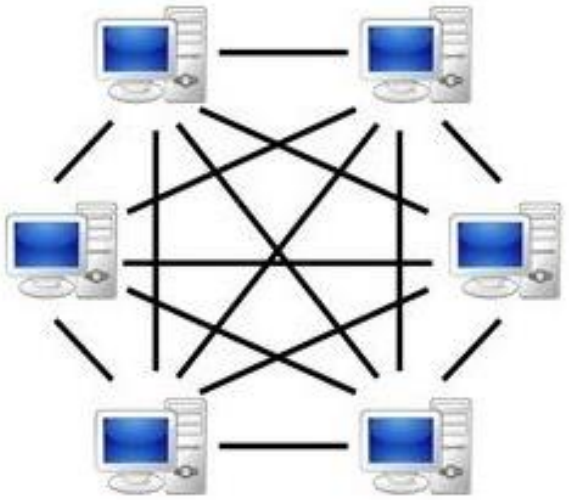
出典[1]

P2Pネットワーク



Server-based





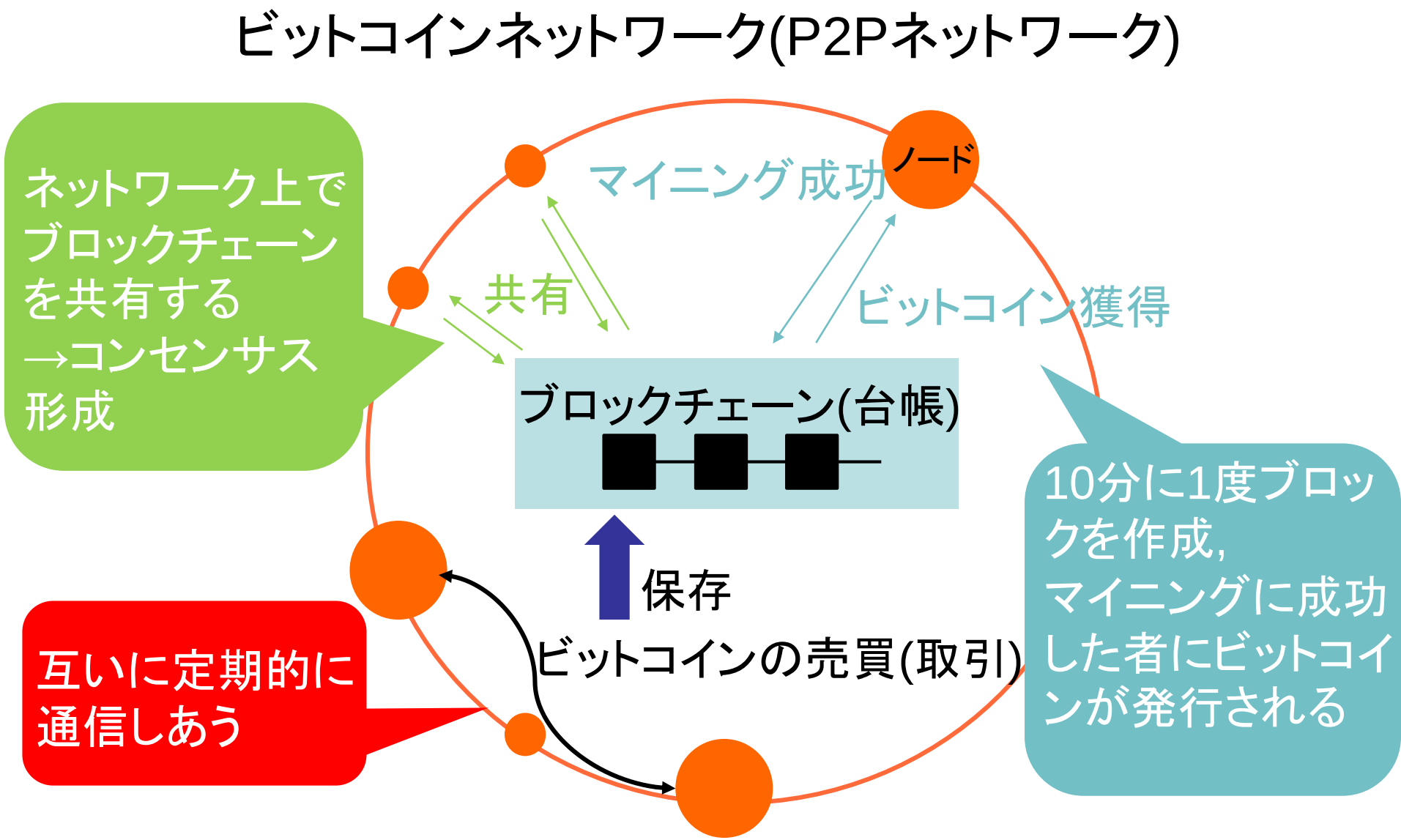
P2P-network

中央管理者(サーバー)
・国家、管理会社など

Peer to Peer
接続先(IPアドレス)のリストを交換し、
ネットワークに参加
定期的に、お互いに通信しあう

出典[1]

仮想通貨の仕組み(ビットコインの例)



研究目的

- 仮想通貨ネットワークはP2Pでつながっており，
  個々のネットワークから成るダイナミズムに特徴が存在する
- ホット・ウォレットは攻撃の標的になりやすい

個々のネットワークに共通または固有の特徴が存在
→セキュリティリスクが存在し、多大な経済損失が発生する可能性

研究目的

複数のネットワーク上にあるIPアドレスの特徴を調査

セキュリティリスクを明らかにする

仮想通貨への攻撃

オンライン上で手続きが完了する

▶攻撃の対象になりやすい

多大な損失

取引所を狙った大きな事件の例

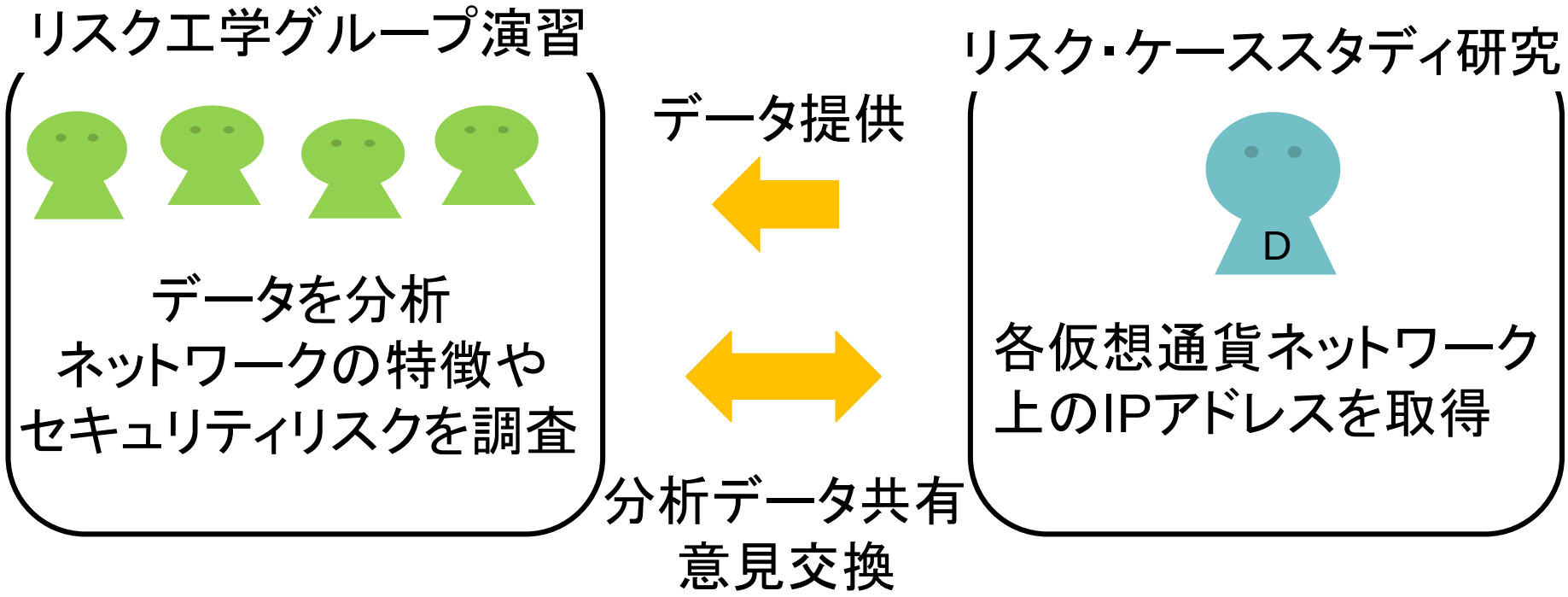
日時	通貨	取引所	被害額
2018/1	NEM	Coincheck	約580億円
2018/6	Ethereum等	Bithumb	約33億円
2016/8	Bitcoin	Bitfinex	約70億円

取引が多いことが分かる

▶ DOS攻撃・サーバー乗っ取りなどの標的に

出典[6], [7], [8], [9]

他授業との連携



- 適宜情報交換を行いながら調査を進めていく

今後の予定

各ネットワークのIPアドレスの取得 → データ処理・分析 → ネットワークの特徴の調査

取得済み

- データにはIPv4・IPv6アドレス・ドメイン名が混在
- 4つネットワークのIPアドレスを全部IPv4又はIPv6に統一(Pythonのライブラリを使用)
- 統一したデータをPythonで分析し、4ネットワークのノードを探し出す

今後の予定

各ネットワークのIPアドレスの取得

データ処理・分析

ネットワークの特徴の調査

取得済み

- IPアドレスから地域を特定し、ネットワークの地域の偏りを評価
- 各仮想通貨ネットワークに共通するノードの数を調査し，ウォレットのリスクを評価

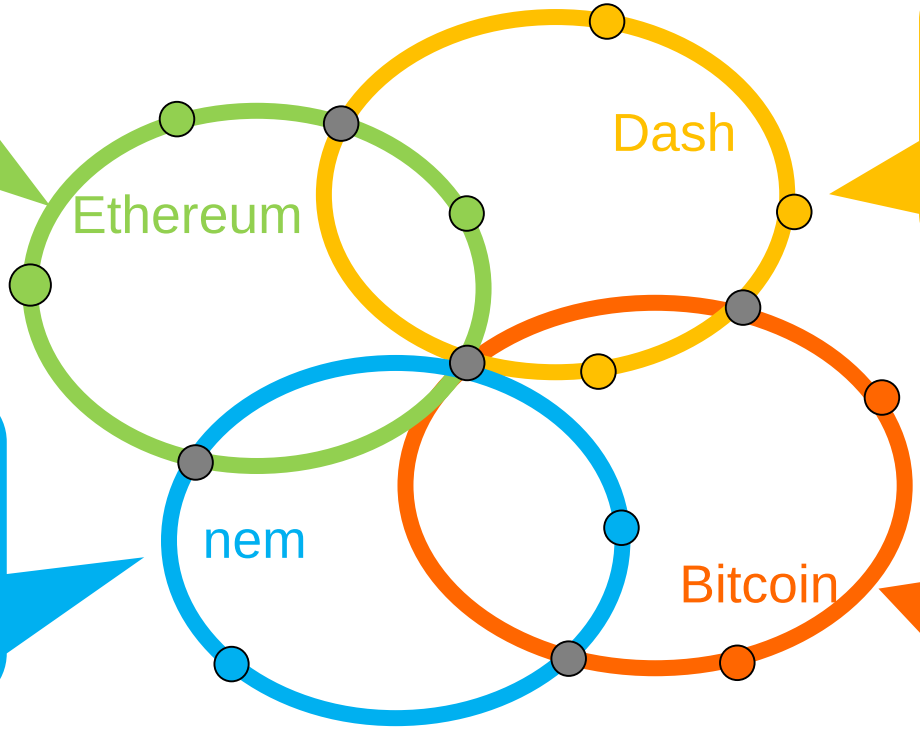
背景ーネットワークの違いー

- 利用目的の違い
- アルゴリズムの違い
- 決済の速さの違い

ネットワークごとに地域の偏りや
振る舞いに違いがあると考えられる

地域によってはリスクが高まる可能性

Proof of Stake
スマートコントラクト
(契約に使える)



Proof of Work
決済目的
匿名性に優れる
決済が速い

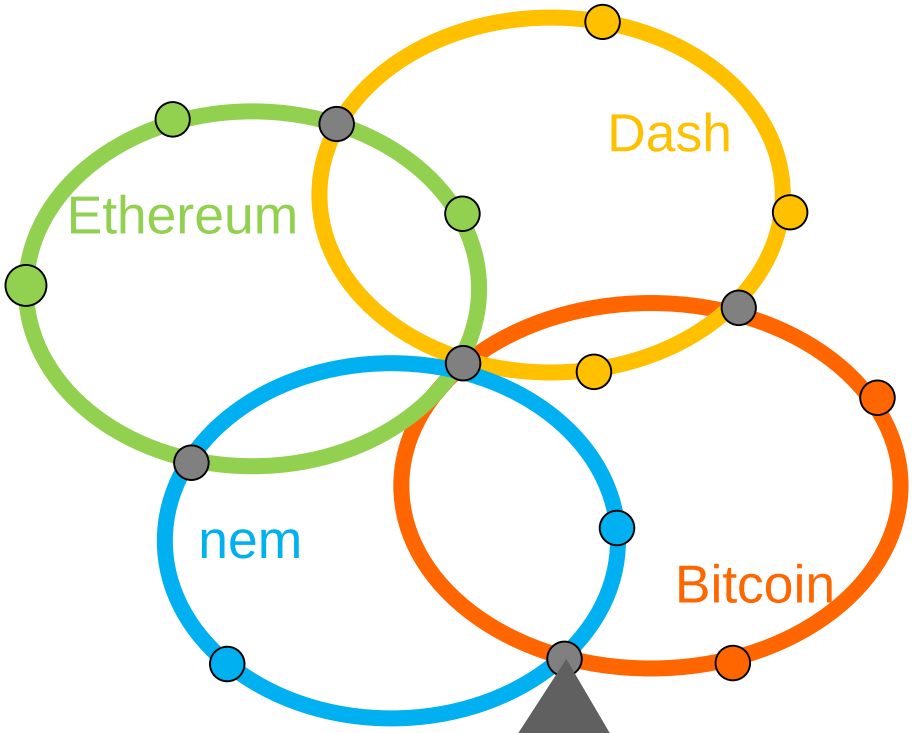
Proof of Importance
積極的にネットワーク
を使う人が多い？

Proof of Work
PC性能の高い人が
利用？
決済目的

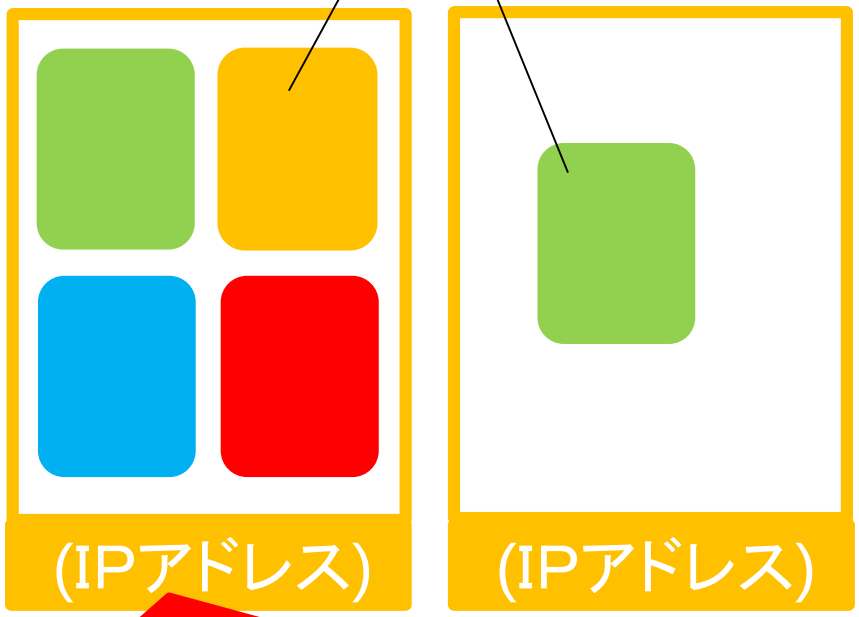
背景ーノードの重なりー

共通のIPアドレスが複数のネットワーク上にある
▶ウォレットを複数所持している・取引所の可能性

各通貨のネットワーク



ウォレット

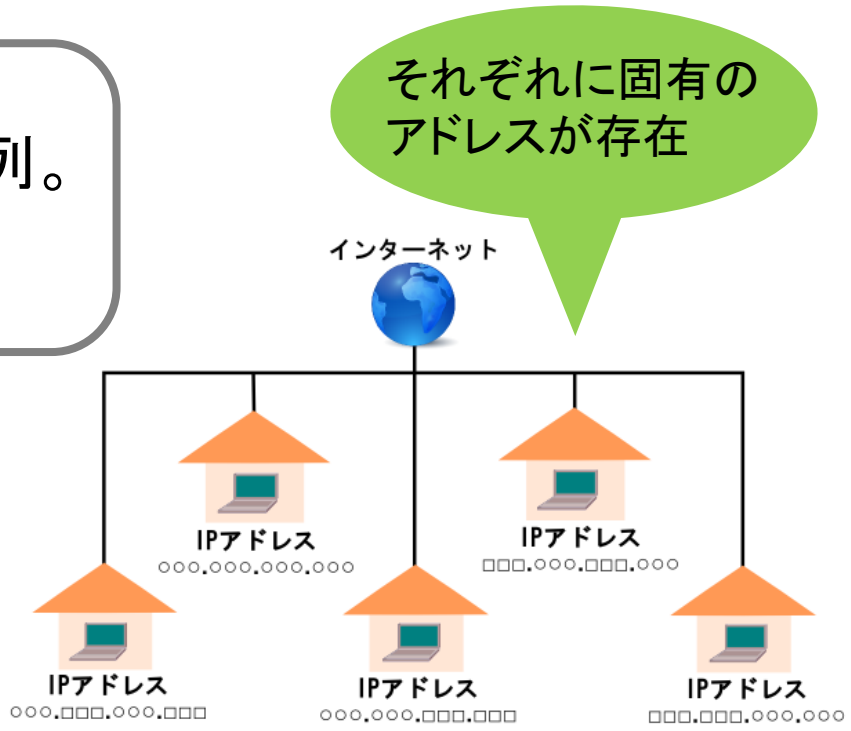


1つのIPアドレス(サーバ)に
複数のウォレット➡リスクが高い
(特に取引所は多額の通貨を扱う)

背景ーIPアドレスー

IPアドレス

コンピュータの住所を表す数値の列。
IPv4とIPv6の2種類が存在。



IPアドレスからわかること

- 国
- 都道府県
- 所有者(企業名など)
- プロバイダー

IPアドレスは公開情報 → セキュリティは端末に依存

▶ セキュリティが甘いと、攻撃によって侵入される可能性

出典[10], [11], [12]

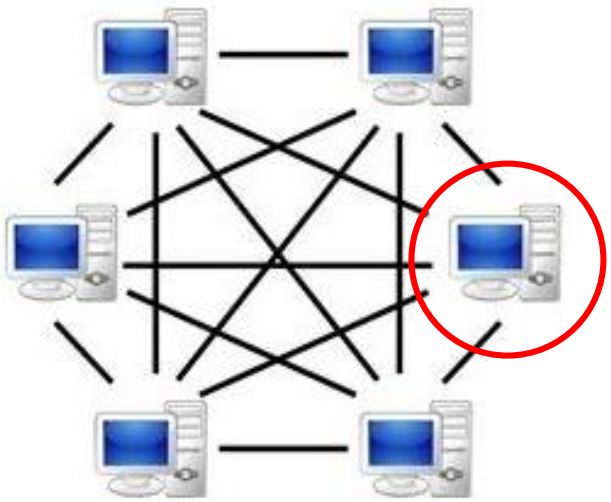
調査内容

異なる仮想通貨のネットワークからIPアドレスを取得
- ブロックチェーンを基盤とするシステムのセキュリティリスクを調査

ネットワークの調査対象

① ネットワークに出現したIPアドレスデータの処理及び解析
② 各仮想通貨ネットワークの特徴を調査(地域の偏りなど)
③ 各ネットワーク同士のつながりを調査

IPアドレスデータの取得方法



ネットワークに参加し、接続先のIPアドレスを取得

直接つながるノードは時間とともに変わるので数日分の接続先データを取得する

ウォレット(仮想通貨のお財布)

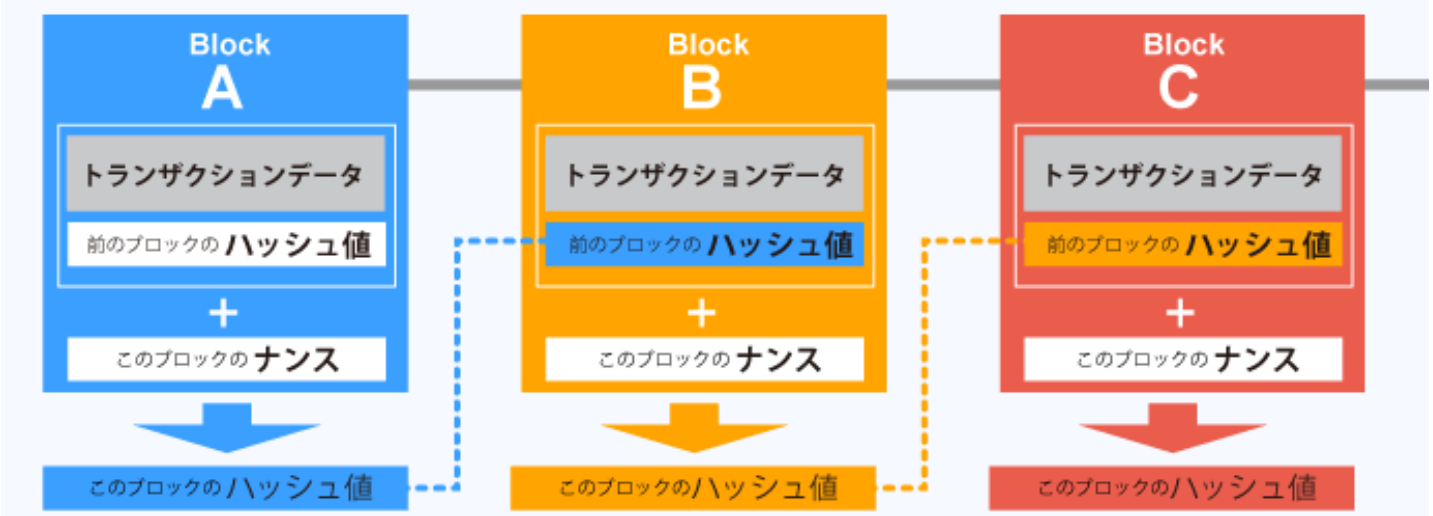
ホット・ウォレット

- インターネットに接続されている
- いつでも入出金が可能(送金がいつでも行える)
- 取引所は常にホットウォレット

コールド・ウォレット

- インターネットに接続されていない
- 送金を行うための秘密鍵がオフライン上に保管
- しかし入出金する際にはネット接続が必要

ブロックチェーンの生成方法



特定のハッシュ値が出るナンスを探す(繰り返し計算)

→ マイニング

Proof of work ➡ 計算力が高いほど

Proof of stake ➡ ETH保有量が多いほど

Proof of importance ➡ 経済的重要度が高いほど

報酬を受け取りやすい

https://blockchain-jp.com/guides/4

アルゴリズムの違い

bitcoin

Proof of work

Proof of stake

Ethereum

大資本をもって計算力の強い
コンピュータを所持している者
が報酬を受け取りやすい
→ 富のある所に富が流れる

Proof of importance

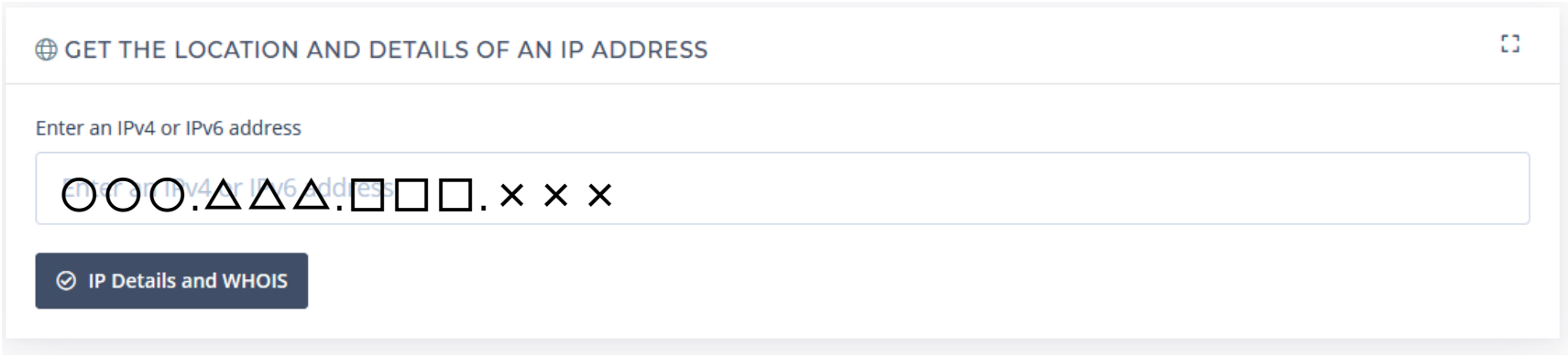
nem

通貨の所有数や取引の頻度によって
ユーザの経済的重要度が決まる
→ 取引を行うことにより富の分配
が行われる

http://bitcoin-richdad.com/nem_xem/#i

ネットワーク特徴の調査方法（例）

WebサイトにてIPアドレスから地域やその他情報が取得可能



ロケーション

Country	Japan
State / Region	Tsukuba
City	Ibaraki

ホスト名

大学

IPアドレスの種類

etc…

https://awebanalysis.com/

異なる仮想通貨P2P間に存在する共通IP

- 複数の仮想通貨を利用しているユーザ

複数の仮想通貨のウォレットを保有している可能性あり。

しかし、全ての仮想通貨をハードウェアウォレットやオンラインウォレットなどのような外部に保管している可能性もあるため、必ずしもウォレットを保有しているとは限らない。

- 取引所及びオンラインウォレット

複数の仮想通貨のウォレットを管理している。

攻撃すれば儲けられる可能性あり。

→IPアドレスが分かれば不正アクセスの可能性が得られる

P2Pネットワーク参加時の他ノードとのやりとり

他ノードとの接続形態によって、P2Pは大きく以下の2種類に分けられる

- ハイブリッドP2P

P2Pに参加しているノードのIPアドレスを管理しているサーバが存在し、そのサーバから他ノードのIPを取得することで他ノードと通信できる。

- ピュアP2P

IPアドレスを管理するサーバが存在しない。その為、ノード探索に関する操作はすべてノードが行う。

ピュアP2Pにおけるノード探索法

ノード探索法によって、ピュアP2Pは以下の2つのネットワーク構造に分けられる

- 非構造化オーバーレイ
- 構造化オーバーレイ

非構造化オーバーレイ

隣接ノードを選定する際の制約が存在しないネットワーク。その為ネットワークトポロジが規定されていない。メッセージをネットワーク上に次々と伝播させ拡散させていくことによりノードの探索を行う。

- メリット

柔軟な探索が可能

- デメリット

メッセージの到達保障性がない

ノード数が増加した場合、ネットワーク上にメッセージが溢れかえりやすい

上記のデメリットを解消する為に、スーパーノードの概念が取り入れられた非構造化オーバーレイも存在する

構造化オーバーレイ

各ノードが接続する相手が決められており、ネットワークトポロジが厳密に規定されているネットワーク。各ノードにはIDが割り当てられ、そのIDに従って接続する相手が決定され、メッセージの転送もIDを用いた経路探索によって実現される。

- メリット

メッセージの到達保障性がある

- デメリット

探索方法に柔軟性がない

P2PにおけるIPアドレス

- IPv4・IPv6ともにグローバルなアドレス

- 固定IPであるとは限らない (しかし固定IPである可能性は 高いと推測される)

→理由:固定IPにすれば、その固定IPアドレスからしか取引所へのログインを受け付けないようにできるため、安全性が高い。また、取引所など仮想通貨に関するサービ スを提供する組織にとっても、自サーバのIPアドレスを 固定にしておかないと、自サーバにクライアントがアクセスできなくなる。

IPv4

枯渇しそうなアドレス資源を節約する為、
グローバルIPアドレスとローカルIPアドレスがある。

- グローバルIPアドレス

インターネット上の住所。重複することはない(一意的)。
ローカルネットワーク外との通信を行うためには必要。

- ローカルIPアドレス

ローカルネットワーク上の住所。
異なるローカルネットワークの機器同士なら、アドレスが重複しても許される
。

IPv6

IPv6にもIPv4でいうグローバルIP・ローカルIPの概念 が存在している。

- グローバル・ユニキャスト・アドレス

IPv4でいうグローバルIP

- ユニーク・ローカル・ユニキャスト・アドレス

IPv4でいうローカルIP

サイバー攻撃の種類

1. 標的型：標的型攻撃・ランサムウェア・水飲み場攻撃・クリックジャッキング・ドライブバイダウンロード
2. APT攻撃
3. OSやソフト，WEBサイトの脆弱性を狙った攻撃：セロデイ攻撃・SQLインジェクション・OSコマンドインジェクション・クロスサイトスクリプティング・バッファーオーバーフロー攻撃・セッションハイジャック・バックドア
4. マルウェア
5. 負荷をかける攻撃：DoS/DDoS攻撃・Ｆ５アタック・ルートキット攻撃
6. パスワード関連のサイバー攻撃：ブルートフォースアタック・パスワードリスト攻撃
7. セッションハイジャック
8. ポートスキャン

https://www.itis.nssol.nssmc.com/blog/nsseint/solution-for-various-cyber-attack.html
https://cybersecurity-jp.com/cybersecurity-guide/14651

事例

年月日	仮想通貨	流出元	被害総額	流出原因
2018/1	NEM	コインチェック	580億円相当	マルウェア感染→秘密鍵→不正送金 コールドウォレット マルチシグ導入せず
2011/6	ビットコイン	マウントゴックス		ハッカーの侵入・遠隔操作 管理体制の甘さ
2014/2	ビットコイン	マウントゴックス	500億円	「トランザクション展性」（取引の2重払い）
2016/6	イーサリアム			「The DAO」 ハードウォークで盗難前の状態に
2018/8	ビットコイン	The Bitfinex		マルチシグの欠陥
	リップル	個人	2500万円	口座への不正ログイン
	Nano	BitGrail	200億円	管理ソフトウェア
2018/5	モナコイン			
				51%攻撃

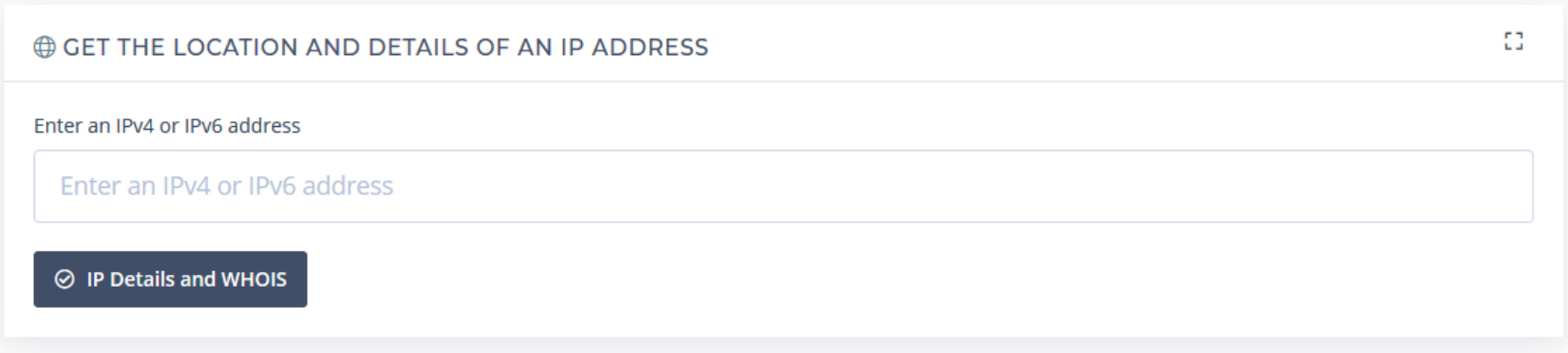
ネットワーク特徴の調査方法

- ドメイン名及びIPv4をIPv6に変換・統一できるサイト

https://awebanalysis.com/

- 2018/4/1-2018/4/7の期間において、Bitcoin,DASH,Ethereum,nemの各仮想通貨ネットワーク上に出現したIPアドレスを調査

→上記のサイトによって、すべてのIPをIPv6に統一して共通IPを調査



仮想通貨への攻撃

仮想通貨がトレンドだが，様々な攻撃を受ける可能性がある

- オンライン上ですべての手続きが完了する仮想通貨は攻撃の対象になりやすい.
- 分散型なのでハッキングリスクは低い.
- しかし，分散型攻撃が増えている？(複数のコンピューターから一斉に送信してサーバーに負担をかけてサービスを停止させるDDoS攻撃)
- 取引所やウォレットへのサイバー攻撃
- 個人のパスワードの盗難
- 51%攻撃
- e.t.c
  - 取引が多いこと(IPアドレス)が分かる→DOS攻撃・サーバー乗っ取り?

DOS攻撃

- ウェブサービスを稼働しているサーバやネットワークなどのリソースに意図的に過剰な負荷をかけたり脆弱性をついたりする事でサービスを妨害する。
- DDoS攻撃（Distributed Denial of Service attack）：トロイの木馬などのマルウェアを使って複数のマシンを乗っ取った上で、DoS攻撃を仕掛ける攻撃.
- DDoS攻撃は通常のDoS攻撃と違い複数のIPを使って行われるので、攻撃対象により大きな負荷をかけることができます。

コインチェック事件

- 2018/1/26
- NEMが流出：約5億2300万XEM(580億円相当)
- 外部からコインチェックの複数の社員宛てに攻撃メールが届き、業務PCがマルウェアに感染．感染したPCを用いて攻撃者が社内ネットワークに侵入し、NEMのサーバにアクセスして秘密鍵を盗み、その秘密鍵を用いて不正送金したことが想定される．
- 流出原因のひとつにコールドウォレットだったこと．
- マルチシグも導入していなかった．
- トップランカーは狙われやすい．海外でも同様．

マウントゴックスビットコイン暴落事件

- 2011年6月
- 日本本社の世界最大の仮想通貨取引所だった.
- ハッカーが管理コンピューターに侵入・遠隔操作し口座に移動.
- ずさんな管理体制

マウントゴックス盗難事件

- 2014年2月
- 「トランザクション展性」とよばれる脆弱性が攻撃された．(取引額の2重払いを受け取る)
- 500億円ぬすまれた
- ビットコインの被害額としては最大.
- 2014年3月
- 三日間で115億円相当のビットコインが消えた.
- 社長が資産を抜き取ったとして逮捕．破綻

リップル流出

- 福島県内の女性が保有していたリップルが不正送金された．口座への不正ログイン．
- 2500万円
- 個人被害は多く，共通のアドレスが送金していることがネット上で指摘されている．

51%攻撃

- 51% 攻撃とは悪意のあるグループまたは個人により、ネットワーク全体の採掘速度の 51%（50% 以上）を支配し、不正な取引を行うことです。ひとつのノードが全体の計算能力の過半数を支配すると、(1)不正な取引の正当化 (2) 正当な取引の拒否 (3) 採掘の独占を行うことが可能となります。現在 51% 攻撃に対する有効な対策はありません。攻撃者は 51% 攻撃を行ったとしても期待値以上の利益を得ることがないことを知っているためノードは 51% 攻撃を行わないと考えられています。51% 攻撃の脅威により、ビットコインの安全性が確保できないため、ビットコインの価値が下がる。攻撃者は価値が下がったビットコインを不正に得ても利益につながらないので攻撃は行われないとされているからです。かつ通常、50% 以上の採掘速度を確保するのは非常に高コストであるため、現実的には難しいとされています。しかしながら 2013 年 12 月には、Ghash.ioというビットコインのマイニングプールの採掘速度が 50% を超えそうになり、この 51% 攻撃が大きな話題となってビットコインの値も下がりました。
- https://bitflyer.com/ja-jp/glossary/fifty_one_percent_attack

2018年5月にビットコインゴールドが標的に
ビットコインゴールドは5月、51%を受けて約20億円分が取引所から盗み出されました。

- 51%攻撃は、ブロックチェーンを強制的に再編成するものだ。セキュリティの欠陥や脆弱性に起因するわけではないが、この攻撃は理論上、あらゆるブロックチェーンに対して仕掛けることができる。
- 脅威をもたらす攻撃者がネットワークの計算能力の50%超を占めることができれば、自身が保有する通貨の取引をブロック上で変更することも除外することもできるようになる。これにより攻撃者は、同じ通貨を2回使う二重支払いができるようになる。
- こういった攻撃を仕掛けるには費用がかかり、膨大な計算能力も必要になるため、利益を上げる唯一の方法は大量の二重支払い取引を試みることであり、必然的に仮想通貨取引所が攻撃対象となる。
- 今回の51%攻撃と関連するウォレットのアドレスは、38万8201BTG（本稿執筆時点で約1750万ドルに相当）を受け取っている。
- 資金の大部分は他のアドレスに移されており、アカウントに残っているのはわずか1万2000BTGほどだ。
- 「標的にされた取引所の1つは、この攻撃者が過去にもBTCの二重支払いを仕掛けようとしたことがあると確信しているとの報告を寄せている。この取引所は、『これが同一人物であることを100%確信しており、両アカウントに多くの関連性があることを発見した』という」（BTG開発チーム）
- 脅威をもたらすユーザーによる攻撃を受けて、多くの仮想通貨取引所が、大規模な取り引きを許可するのに必要な承認の回数を増やしている。

51%攻撃でできることとして、

・トランスアクションが承認されるのを防ぐ

・過半数のハッシングパワーを持っている間、自分のトランスアクションを取り消すことができる（2重支払い）

・マイニングにより得られる10分に一度のブロック報酬（25BTC）を全て自分のものにすることができる。

主に上記３つ．つまり、新しい送金が起こらないように妨害したり、自分が払ったはずの送金を取り消したりすることができるだけ。

逆に51%攻撃でできないことは

・過去のトランスアクションを改ざんする

・ビットコインを新しく無尽蔵に作り出す

・他の人のWalletからビットコインを奪う

モナコイン

- セルフィッシュ・マイニングによる攻撃
- (悪意のあるマイナーがブロードキャストをしないブロックチェーンを作成し，自身が取引所に送った送金を意図的に無効にした．)