情報通信システムセキュリティ研究会（ICSS）

 1

ビットコイン利用者の特定・追跡の仕組みに関する考察

2021年3月2日

（株）IT企画　才所敏明

toshiaki.saisho@advanced-it.co.jp

http://www.advanced-it.co.jp

共　著　者

辻井重男
中央大学研究開発機構

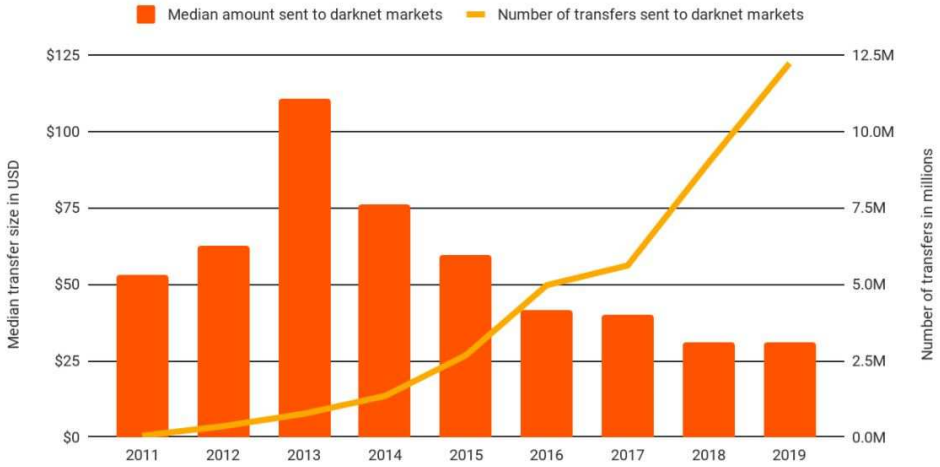
櫻井幸一
九州大学　大学院システム情報科学研究院
＆サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所

謝辞　本研究の一部は　JSPS科研費 基盤(B) JP18H03240　の支援を受けている。

1．暗号資産の悪用の現状

 2

暗号資産の悪用件数が急増



Currencies included: BCH, BTC, LTC, USDT

https://blog.chainalysis.com/reports/darknet-markets-cryptocurrency-2019

1．暗号資産の悪用の現状

ビットコインの悪用の現状

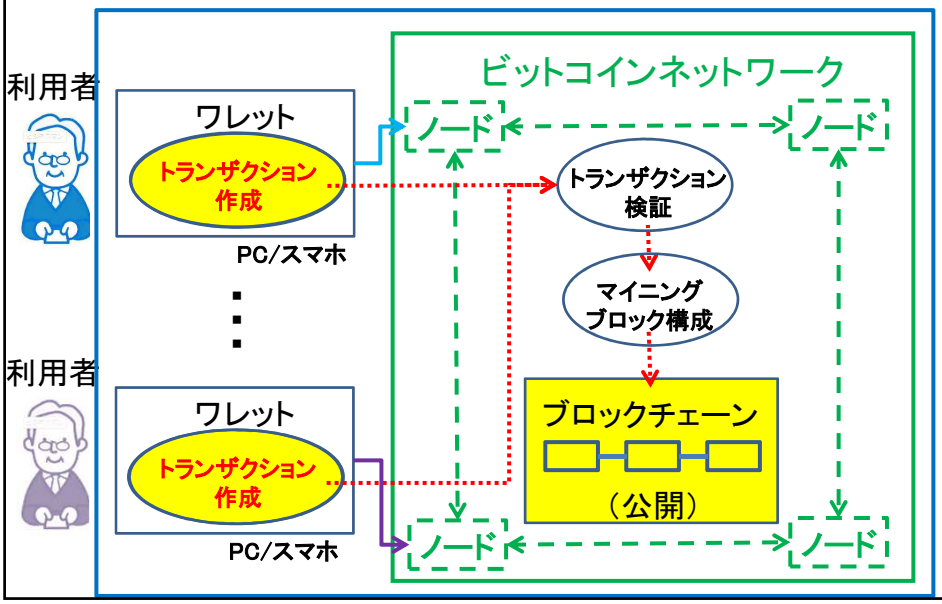
Group/subgroup	Users	Transaction count (mil)	Holding value ($mil)	Number of addresses (mil)	Volume ($bil)
1. All users	106,244,432 (100.00%)	605.69 (100.00%)	2,964.66 (100.00%)	221.71 (100.00%)	1,862.51 (100.00%)
2. Observed illegal users	6,223,359 (5.86%)	196.11 (32.38%)	1,342.43 (45.28%)	58.38 (26.33%)	241.46 (12.96%)
2A. Seized users	1,041 (0.00%)	23.83 (3.93%)	9.39 (0.32%)	8.30 (3.74%)	17.51 (0.94%)
2B. Black market users (not in 2A)	6,221,870 (5.86%)	157.30 (25.97%)	1,324.32 (44.67%)	49.71 (22.42%)	220.91 (11.86%)
2C. Forum users (not in 2A or 2B)	448 (0.00%)	14.98 (2.47%)	8.72 (0.29%)	0.38 (0.17%)	3.03 (0.16%)
3. Other users	100,021,073 (94.14%)	409.58 (67.62%)	1,622.23 (54.72%)	163.33 (73.67%)	1,621.05 (87.04%)

（対象は、2017年4月時点のビットコインブロックチェーン）

Sex, Drugs, and Bitcoin How Much Illegal Activity Is Financed through Cryptocurrencies（2019）
https://academic.oup.com/rfs/article/32/5/1798/5427781

2．ビットコインの匿名性

ビットコインシステム構成概要



トランザクション内の資産移転にかかわる情報

入力資産情報	
入力資産1	①提供者が使用する入力資産の指定
	②提供者が使用する入力資産の所有権の証明
入力資産2	①提供者が使用する入力資産の指定
	②提供者が使用する入力資産の所有権の証明
.....	
入力資産n	①提供者が使用する入力資産の指定
	②提供者が使用する入力資産の所有権の証明

出力資産情報	
出力資産1	③受取者の指定
	④受取額の指定
出力資産2	③受取者の指定
	④受取額の指定
.....	
出力資産m	③受取者の指定
	④受取額の指定

トランザクションの匿名性（P2PKHによる資産移転情報の匿名性）

①提供者が使用する入力資産の指定（提供者の公開鍵のハッシュ値と金額へのポインタ）➔利用者（提供者）の高い匿名性

②提供者が使用する入力資産の所有権の証明（提供者の公開鍵、対応する秘密鍵による署名）➔利用者（提供者）の高い匿名性

③受取者の指定（受取者の公開鍵のハッシュ値）➔利用者（受取者）の高い匿名性

④受取額の指定➔利用者（受取者）の高い匿名性

➔トランザクションは利用者の高い匿名性！

➔利用者の特定・追跡が困難

➔ビットコインの悪用が氾濫する要因

（多くの暗号資産も同様！）

暗号資産利用者の特定・追跡への対応例
犯罪収益移転防止法（日本）

犯罪収益移転防止法（2007年公布）の2016年の法改正
　暗号資産交換事業者も、確実な本人確認(KYC)の実施、
　　および記録の保存が義務化

しかし、多くの暗号資産は
　暗号資産交換業者を経由せずに資産移転が可能

➔不正・不法な暗号資産の移転を行う
　　利用者の特定・追跡に対する効果は限定的！

暗号資産利用者の特定・追跡の現状
トラベルルール（FATF Recommendation 16）
（2019年6月　新ルール制定）

目的：テロリストやその他の犯罪者が資金を移動するための電信送金に自由にアクセスできないようにし、そのような誤用が発生したときにそれを検出することが可能なこと

具体的要件：電信送金の発信者と受益者に関する以下の基本情報をすぐに利用できるようにすること

1) 資産提供者の名前
2) トランザクションの処理に利用される資産提供者のアカウント番号
3) 資産提供者の地理的な住所および国固有の個人識別番号等
4) 資産受取者の名前
5) トランザクションの処理に利用される資産受取者のアカウント番号

FATF（Financial Action Task Force）：1989年にマネーロンダリング・テロ資金対策等に取り組む主要国政府による枠組みとしてOECDに事務局を設置し発足した金融活動作業部会

暗号資産利用者の特定・追跡の現状
トラベルルールへの対応状況

本ガイドラインの順守に向けての活動
　各国の政府は法制度の整備
　暗号資産関連事業者は管理・運用面の対応の検討
まだまだ緒に就いたばかり
　その完全順守の見通しは立っていない

しかし、そもそも、現在の多くの暗号資産システムが、
　事業者の関与無しに、個人間で取引が可能なため
　事業者への運用・管理面での法制度による規制だけでは、不十分

➔暗号資産システム側の技術面の対応が必要
　加えて、管理・運用面の対応、それらを支える法制度面の対応
　の連携が必要

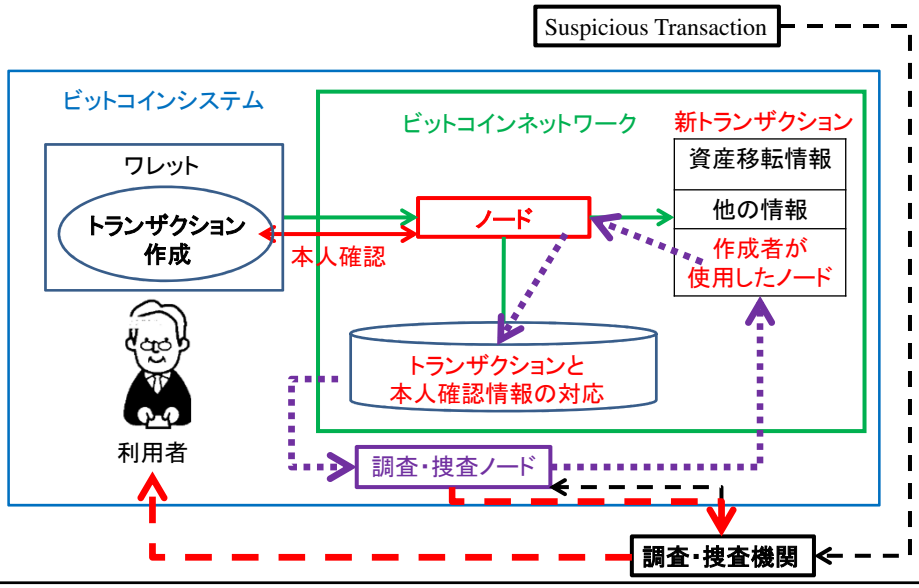
ビットコインシステムにおける
利用者の特定・追跡の仕組み（提案）

対象トランザクション：ビットコインのP2PKHによる
　　資産の移転を行うトランザクション
対象利用者：トランザクション作成者（発行者）

提案方式
　A:ビットコインネットワークのノード活用方式
　B：本人確認ノード導入方式
　C：本人確認ノード経由方式
　D：本人確認基盤利用方式

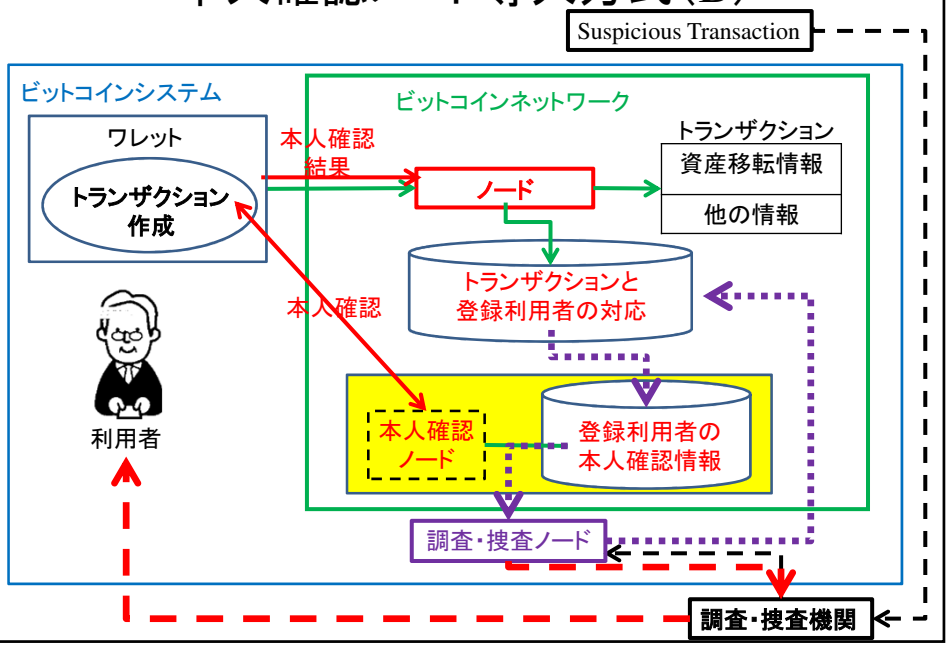
 11

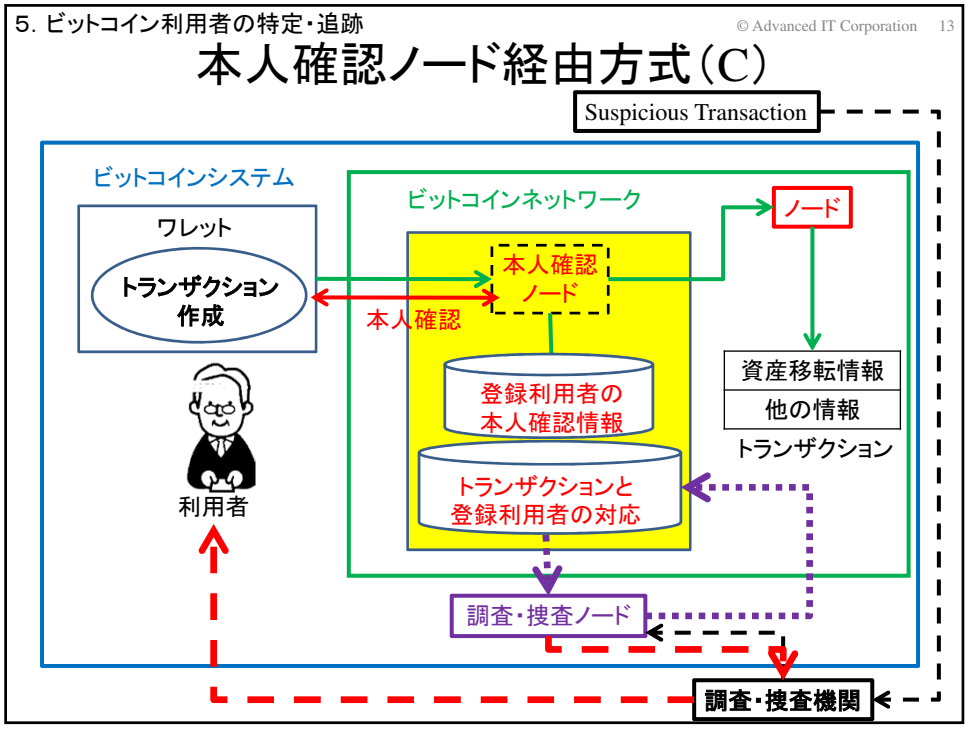
ビットコインネットワークのノード活用方式（A）

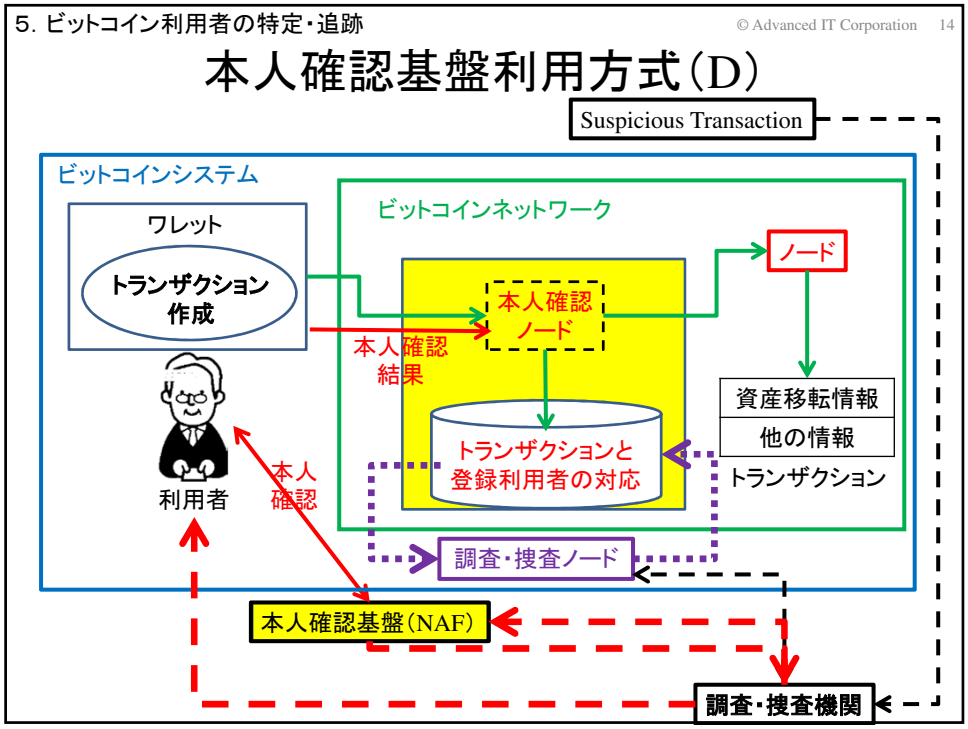


 12

本人確認ノード導入方式（B）




5. ビットコイン利用者の特定・追跡
© Advanced IT Corporation 13
本人確認ノード経由方式（C）
Suspicious Transaction
ビットコインシステム
ワレット
トランザクション作成
ビットコインネットワーク
本人確認ノード
ノード
本人確認
登録利用者の本人確認情報
資産移転情報
他の情報
トランザクション
トランザクションと登録利用者の対応
利用者
調査・捜査ノード
調査・捜査機関


5. ビットコイン利用者の特定・追跡
© Advanced IT Corporation 14
本人確認基盤利用方式（D）
Suspicious Transaction
ビットコインシステム
ワレット
トランザクション作成
ビットコインネットワーク
ノード
本人確認ノード
本人確認結果
資産移転情報
他の情報
トランザクション
トランザクションと登録利用者の対応
利用者
本人確認
調査・捜査ノード
本人確認基盤（NAF）
調査・捜査機関

各方式の評価

評価項目＼方式	A	B	C	D
現状のビットコインシステムへの影響の小ささ	×	△	△	△
利用者の個人情報・プライバシー情報の安全な管理のしやすさ	×	△	△	○
グローバルなビットコインシステムの運用のしやすさ	×	△	△	○
複数の暗号資産システム利用への対応のしやすさ	×	○	×	○
社会実装の容易さ	×	×	○	△

考案した4方式のトラベルルールとの関係

トラベルルール：電信送金の発信者と受益者に関する
以下の基本情報をすぐに利用できるようにすること

1) 資産提供者の名前
2) トランザクションの処理に利用される資産提供者のアカウント番号
3) 資産提供者の地理的な住所および国固有の個人識別番号等
4) 資産受取者の名前
5) トランザクションの処理に利用される資産受取者のアカウント番号

（1）トランザクション作成者が資産提供者の場合、提案の4方式は
当該トランザクションに対して1）～3）を満たすが
4）～5）は、当該トランザクションの受取者が提供者となる
新たなトランザクションが登録されてはじめて満たされる

（2）トランザクション作成者が資産提供者と異なる場合は対応不可
マルチシグ（P2SH）による資産移転のトランザクション
ミキシングサービスにより統合されたトランザクション

まとめ

（1）社会が求める安心・安全な暗号資産システムに向けて、急増する
不正・不法な取引の決済への利用
マネーロンダリング
等に対応するには、利用者・暗号資産の特定・追跡可能性が必要

（2）利用者・暗号資産の特定・追跡のためには
暗号資産関連事業者における確実なKYC、
その確実な実施を求める法制度面の対応だけでは困難
➔暗号資産システム面(技術面）の対応が不可欠

（3）今回は、ビットコインのP2PKHトランザクションを対象に
利用者（トランザクション作成者）の
特定・追跡の仕組みを具体的に考案し考察

（4）暗号資産システムの技術開発グループは
本課題への対応を真摯に検討すべき

終

（ご清聴、ありがとうございました）