第94回CSEC研究会

 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（2）
ー BITFRAの提案 ー

2021年7月19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

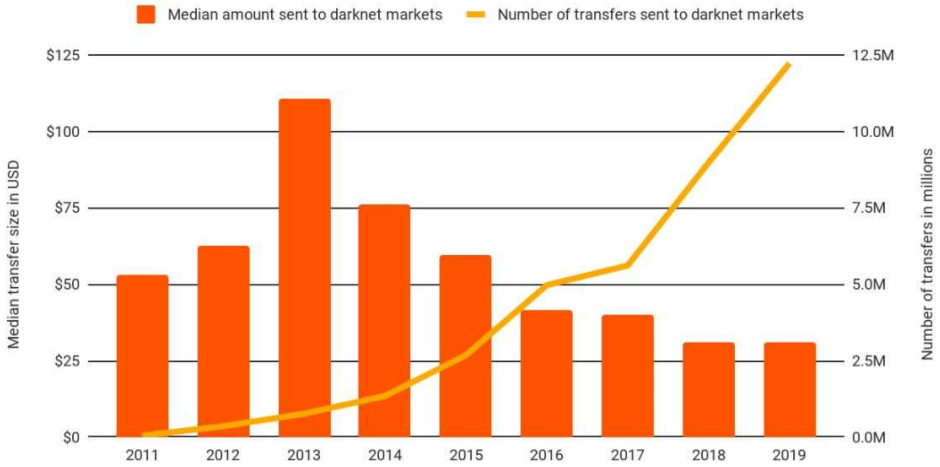
櫻井幸一
九州大学　大学院システム情報科学研究院
＆サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所

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

 3

ビットコインの悪用の現状
（2017年4月時点のビットコインブロックチェーンが分析対象）

ユーザ分類		ユーザ数	トランザクション数（百万）	保有資産（百万ドル）
全ユーザ		106,244,432	605.69	2,964.66
		（100%）	（100%）	（100%）
観察された違法なユーザ		6,223,359	196.11	1,342.43
		（5.86%）	（32.38%）	（45.28%）
	拘束された違法ユーザ	1,041	23.83	9.39
		（0.017%）	（12.151%）	（0.699%）
	ブラックマーケットユーザ	6,221,870	157.3	1,324.32
		（99.976%）	（80.210%）	（98.651%）
	フォーラムユーザ	448	14.98	8.72
		（0.007%）	（7.639%）	（0.650%）

＜下記論文のデータから作成＞
Sex, Drugs, and Bitcoin How Much Illegal Activity Is Financed through Cryptocurrencies（2019）
https://academic.oup.com/rfs/article/32/5/1798/5427781

2．規制強化（1）

 4

安心・安全な社会に向けた暗号資産システムへの規制強化の動き（1）

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

2018年10月　FATF勧告15「新技術」の改訂

暗号資産交換事業者VASPにはマネーロンダリング等の規制が課されなければならないことを規定

（注）VASP：Virtual Asset Service Provider

2019年6月　FATF勧告16「電信送金」の改訂

トラベルルール：電信送金の発信者と受益者に関する基本情報の確認・保存をVASPへ要求

トラベルルール（FATF(注) Recommendation 16）（2019年6月に制定されたルール）

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
以下の基本情報を電信送金に含めておくこと

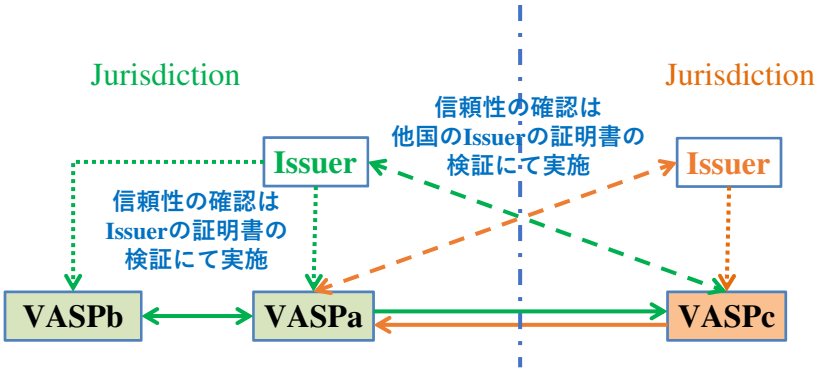
1) 資産提供者の名前
2) トランザクションの処理に利用される資産提供者のアカウント番号
3) 資産提供者の地理的な住所および国固有の個人識別番号等
4) 資産受取者の名前
5) トランザクションの処理に利用される資産受取者のアカウント番号

暗号資産システム側の規制強化への対応の動き

OpenVASP（Open Virtual Asset Service Provider）
OpenVASP Association （2019年　スイス） Bitcoin Swiss
Blockchain-based Protocol
for decentralized VASP-to-VASP connection

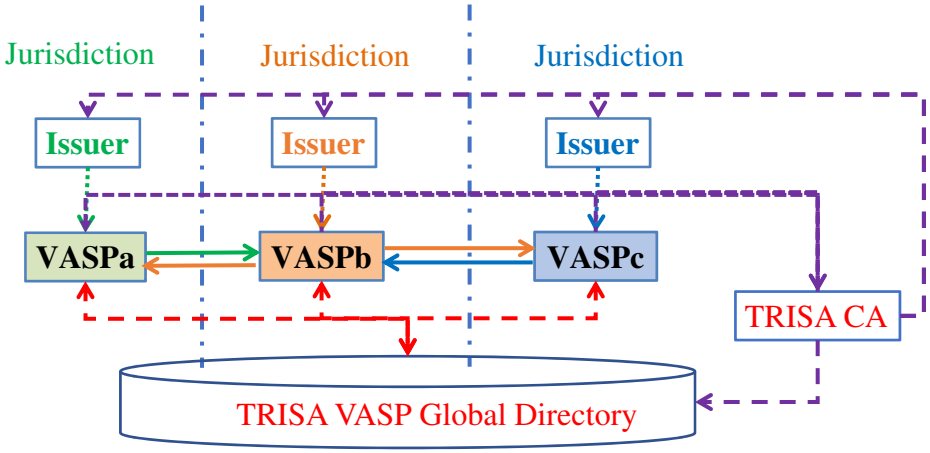
TRISA（Travel Rule Information Sharing Architecture）
TRISA Alliance （2019年　米国） CypherTrace、Shyft Network
PKI- based Solution：TRISA認証局、TRISA VASP ディレクトリ

OpenVASPにおけるVASP間の信頼性確認



（1）各国のVASPは、自らの情報を第三者発行の証明書等も含め
ブロックチェーン上に登録されることを想定
（2）通信相手のVASPが信頼できるかどうかは、
各国の法制度等に基づき各Issuerが発行する証明書等利用し、
VASP自らの確認と責任で判断する方式を想定

TRISAにおけるVASP間の信頼性確認



（1）各国のVASPは、TRISA CAへ登録申請。
TRISA CAは、各国の各種証明書発行機関の確認内容、信頼性等を検証の上、
TRISA VASP Global Directoryへ登録。
（2）通信相手のVASPが信頼できるかどうかは、TRISA VASP Global Directoryを参照し、
TRISA CA発行の証明書の検証により判断する方式を想定

4. 規制強化(1)への対応

 9

OpenVASP、TRISA比較・考察

(1)VASP間信頼性確認

OpenVASPは、Blockchain-based Protocolによる信頼性確認
TRISAは、PKI-based Frameworkによる信頼性確認

➔ 各国の事情・法制度に基づく、
VASPの存在確認、FATFトラベルルール準拠確認の
妥当性検証は個々のVASPに依存するのではなく
専門機関で実施するのが望ましいと考える。

(2)VASP間利用者情報送信

OpenVASPおよびTRISA共に、FATFトラベルルール指定の
利用者の個人情報をそのまま、通信相手のVASPへ送信

➔ 法域を超えた個人情報の授受は好ましくない
取引前に授受する個人情報で必要な確認事項、
取引後に調査・捜査時に必要な確認事項を整理し、
法域を超えた個人情報の授受方式の検討が必要と考える。

5. 規制強化(1)の課題

 10

現行の「トラベルルール」の課題

「トラベルルール」
暗号資産関連事業者 (VASP)における
確実なKYCおよびKYTと、その確実な記録により、
暗号資産利用者の特定・追跡を可能とし
不正・不法な暗号資産移転の抑止・防止を目指す

⇩

しかし、多くの暗号資産は、
暗号資産関連事業者を経由せずに利用者が直接資産移転が可能

⇩

不正・不法な暗号資産利用者の
特定・追跡に対する効果は限定的！

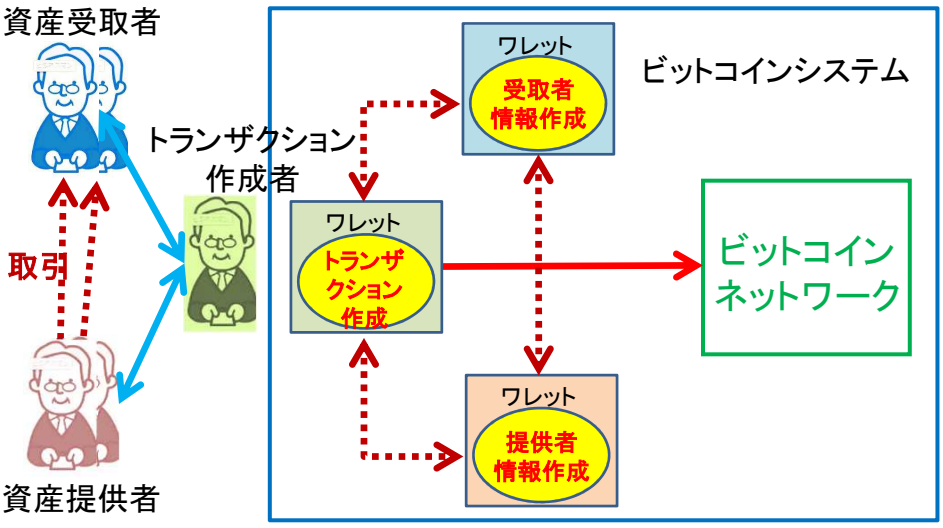
BITFRAの提案
ビットコインシステム利用者の特定・追跡方式
Bitcoin User Identifying and Tracking Framework

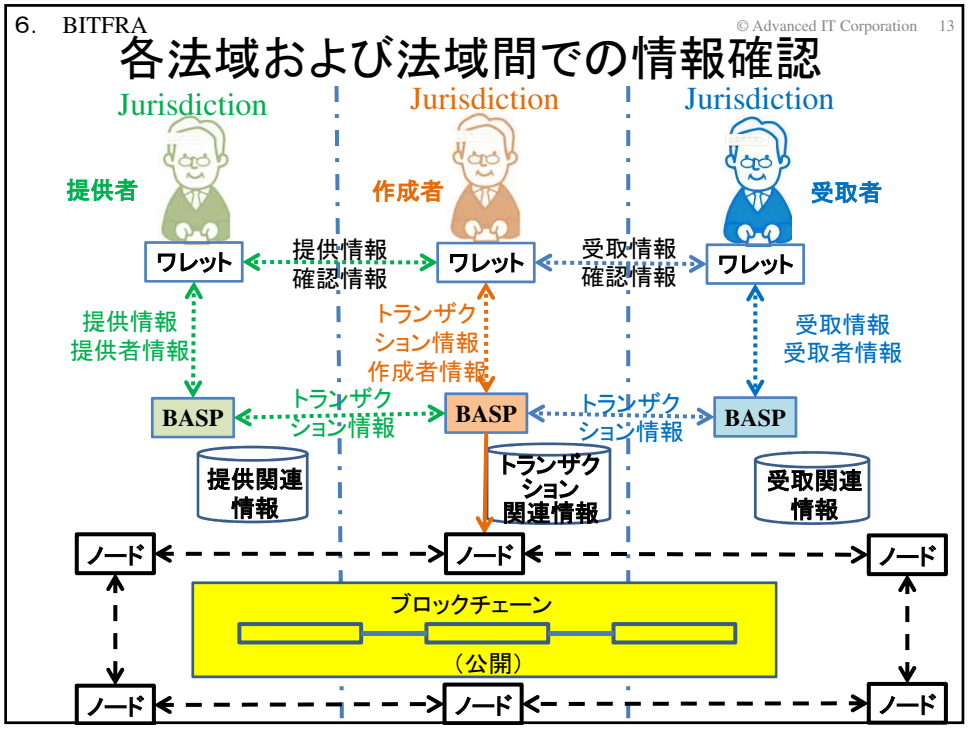
トラベルルールおよびその順守の仕組みでは対応できない、
暗号資産利用者の特定・追跡の仕組みの研究

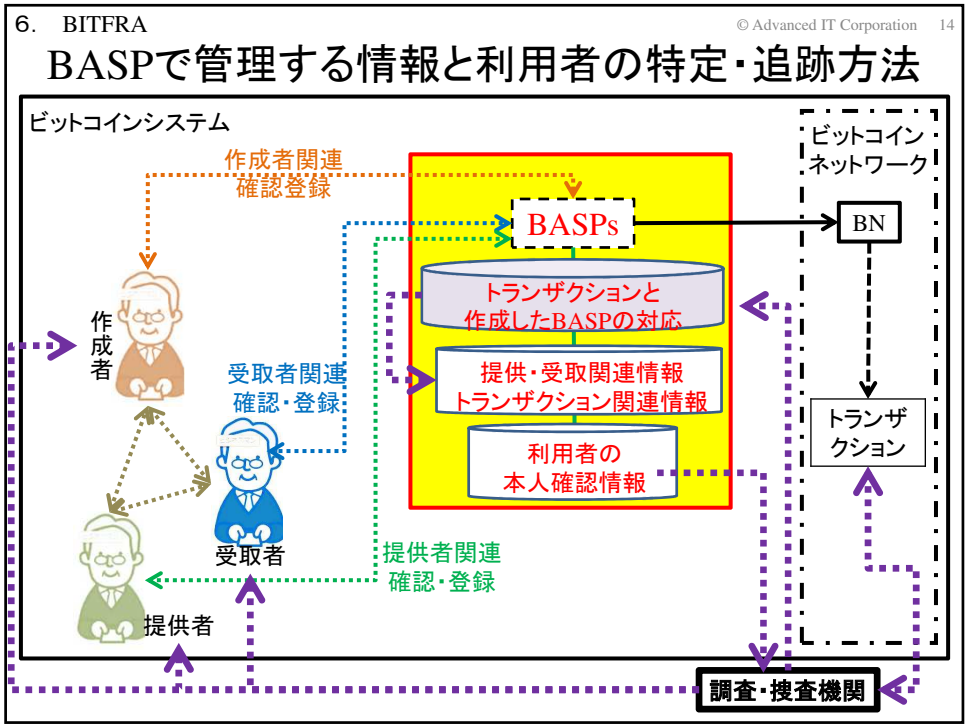
代表的暗号資産であるビットコインを対象に具体的に研究

基本方針
①ビットコインネットワークへの影響を最小化
②各国の法制度に準拠した利用者の個人情報保護
③複数の暗号資産システムの利用を支援する
統合環境への発展を想定

3種のビットコインシステム利用者




6. BITFRA
© Advanced IT Corporation 13
各法域および法域間での情報確認
Jurisdiction
Jurisdiction
Jurisdiction
提供者
作成者
受取者
ワレット
提供情報
確認情報
ワレット
受取情報
確認情報
ワレット
提供情報
提供者情報
トランザクション情報
作成者情報
受取情報
受取者情報
BASP
トランザクション情報
BASP
トランザクション情報
BASP
提供関連情報
トランザクション関連情報
受取関連情報
ノード
ノード
ノード
ブロックチェーン
（公開）
ノード
ノード
ノード


6. BITFRA
© Advanced IT Corporation 14
BASPで管理する情報と利用者の特定・追跡方法
ビットコインシステム
作成者関連
確認登録
BASPs
ビットコイン
ネットワーク
BN
トランザクションと
作成したBASPの対応
作成者
受取者関連
確認・登録
提供・受取関連情報
トランザクション関連情報
トランザクション
利用者の
本人確認情報
受取者
提供者関連
確認・登録
提供者
調査・捜査機関

提案方式BITFRAの評価・考察（3つの基本方針の観点から）

①「ビットコインネットワークへの影響を最小化」
- ○ビットコインブロックチェーンの構造には影響を与えない。
- ×各ビットコインノードには追加の処理が必要となる。
  - 正規のBASPにより利用者の特定・追跡性が確認された
  - トランザクションであるをBASPの署名の検証により確認

②「各国の法制度に準拠した利用者の個人情報保護」
- ○法域を超えた個人情報の移転を伴わないことを想定
  - 登録されているBASPは個人情報の取り扱いに関する
  - 各国（法域内）の法制度に準拠している事業者

③「複数の暗号資産システムの利用を支援する統合環境への発展の可能性」
- ○ビットコインの利用者の特定・追跡の仕組みを、ビットコインネットワークと独立したBASPで実現

提案方式BITFRAの評価・考察（OpenVASP、TRISAとの比較の観点から）

①「分散型か中央集権型か」
- OpenVASPとTRISAの根本的な違い
  - OpenVASP：通信相手のVASPの信頼性は自己責任で確認
  - TRISA：信頼できる第3者機関TRISA CA（Certificate Authority）の通信相手のVASPの信頼性確認結果を利用
- BITFRA：TRISAと同様のPKIベースのフレームワーク

②「個人情報の取扱い」
- OpenVASPとTRISA
  - FATFトラベルルール規定の個人情報をVASP間で送受する方式
- BITFRA：
  - 個人情報の確認・管理を保証する情報を送受する方式
  - （トラベルルール規定の個人情報も必要に応じBASP間で共有できる仕組み）

安心・安全な社会に向けた暗号資産システムへの規制強化の動き（2）

2020年　スイス政府　資金洗浄対策強化の方針
VASPは、ユーザが資金を取引所のアカウントから
認証されていない個人ウォレットへの送金を許可しない、
等の規制案？

2020年12月　米国FinCEN：Financial Crimes Enforcement Network
ユーザ個人のワレットで、一つのトランザクションで3千ドル、
24時間内に合計1万ドルを超える送金または着金の場合、
VASPはレポートを提出要、等の規制案を発表

2021年3月　FATF　トラベルルール改定の動き
P2P取引への規制案を発表

まとめ

（1）ビットコイン利用者の特定・追跡の仕組みBITFRAを提案
（2）提案方式BITFRAの評価・考察実施
（3）今後の検討課題
①新FATFトラベルルールの内容、議論の動向に応じた対応
個人（unhosted wallet）間の資産移転
OpenVASP、TRISAの対応案は未発表
BITFRAは一応想定
②VASP間個人情報送受に関する議論の動向に応じた対応
FATFトラベルルールと個人情報保護の両立
合法的アクセスの仕組み
③BASPのブラッシュアップ（①、②への対応も含め）
仕様の詳細検討
他のTCAM型暗号資産への適用可能性の検証

終