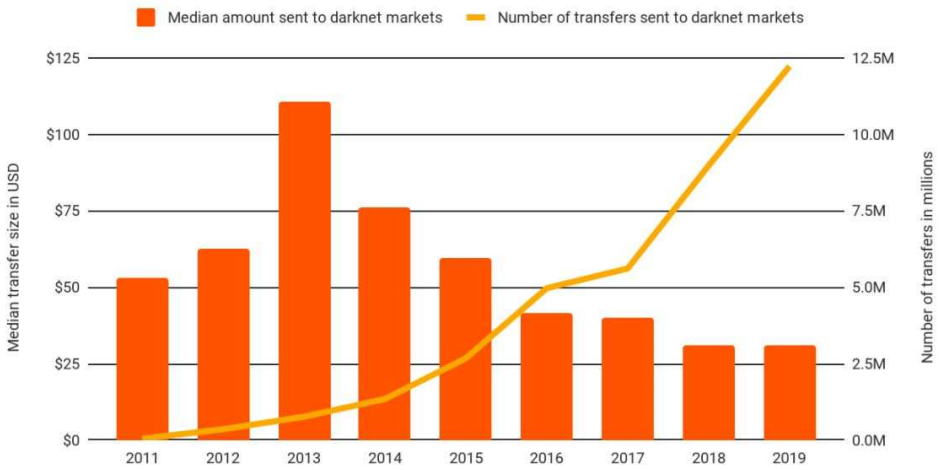


③暗号資産の課題とその克服のための新たな仕組みに向けて
ー　ビットコインを例に　ー

2021年6月30日
才所敏明
（株）IT企画・代表取締役社長
中央大学研究開発機構・研究員
（株）ZenmuTech顧問
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

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

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

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）

2015年6月　G7サミット
　仮想通貨等への適切な規制の導入等を宣言
2018年3月　G20財務大臣・中央銀行総裁会議
　暗号資産についてマネーロンダリング等の
　　問題提起等の声明
2018年10月　FATF勧告15「新技術」の改訂
　暗号資産交換事業者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
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月に制定された新ルール）

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

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

暗号資産システムへの規制強化 日本の対応・・・犯罪収益移転防止法

犯罪収益移転防止法（2007年公布）
犯罪者による資金洗浄(マネーロンダリング)を防止するために、
金融機関や資金の流れに関わるその他の業者が
従うべきルールを定めた法律

2016年の法改正
暗号資産交換事業者も対象に
（確実な本人確認(KYC)の実施、記録の保存が義務化）

2020年の法改正
本人確認方法の厳格化
（利用者の本人確認の際、本人確認書類を2点提出要）

2021年3月31日　金融庁が2022年4月を目処に「トラベルルール」導入か
暗号資産（仮想通貨）交換業協会（JVCEA）に対し、
「トラベルルール」導入を進めるための体制整備を要請

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

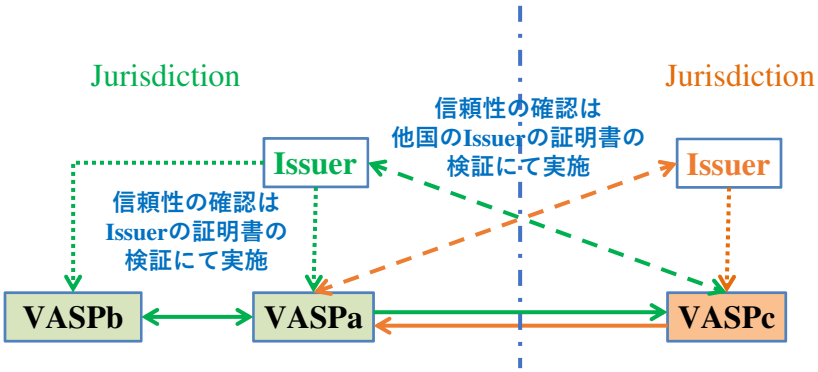
for decentralized VASP-to-VASP　connection

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

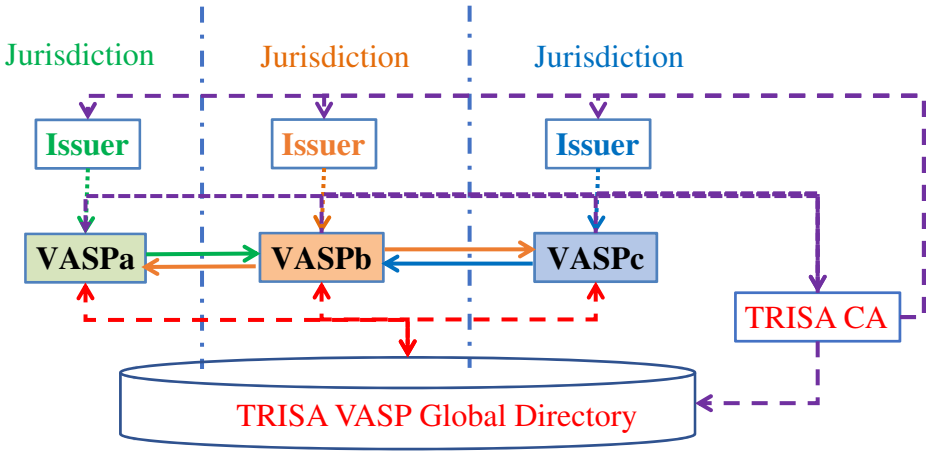
OpenVASPにおけるVASP間の信頼性確認



（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

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。

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

⇩

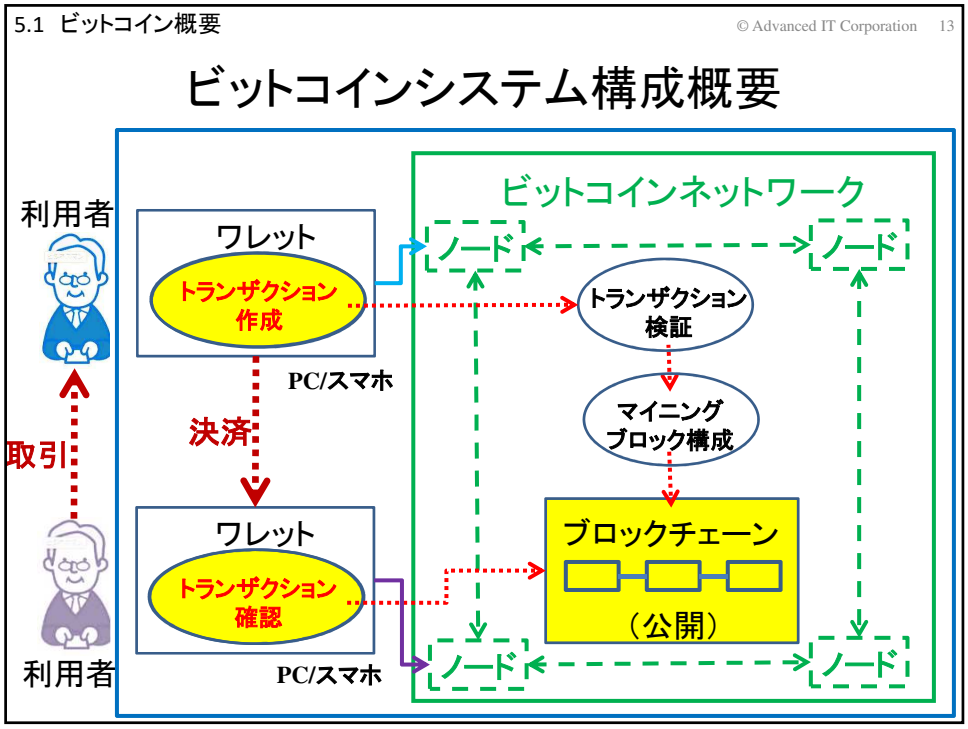
不正・不法な暗号資産利用者の
特定・追跡に対する効果は限定的！

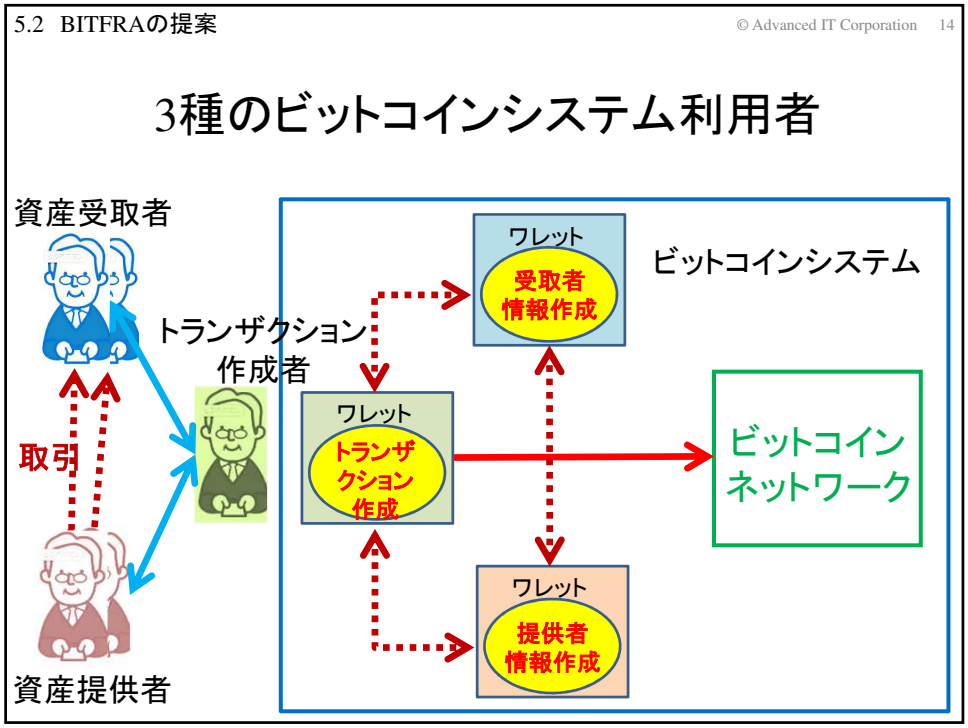
報告者らのアプローチ（2018年より）
安心・安全な暗号資産システムを目指して

（1）利用者の個人情報の保護を目指した研究
➔ 利用者の匿名性の要件定義、匿名化技術の調査・評価
➔ 活発な研究・実装が進められていることを確認

（2）暗号資産システムの悪用防止・抑止を目指した研究
➔ 利用者の特定・追跡の仕組みの現状・課題把握
➔ 多くの暗号資産で考慮されておらず、研究も少ない

＜暗号資産システムにおける
利用者の特定・追跡の仕組みの研究＞
①TCAMSの代表であるビットコインを対象に、
具体的な仕組みを考案


5.1 ビットコイン概要
© Advanced IT Corporation 13
ビットコインシステム構成概要
利用者
ワレット
トランザクション作成
PC/スマホ
決済
取引
ワレット
トランザクション確認
PC/スマホ
利用者
ビットコインネットワーク
ノード
ノード
トランザクション検証
マイニング ブロック構成
ブロックチェーン
（公開）
ノード
ノード


5.2 BITFRAの提案
© Advanced IT Corporation 14
3種のビットコインシステム利用者
資産受取者
トランザクション作成者
取引
資産提供者
ワレット
受取者情報作成
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
ワレット
提供者情報作成

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

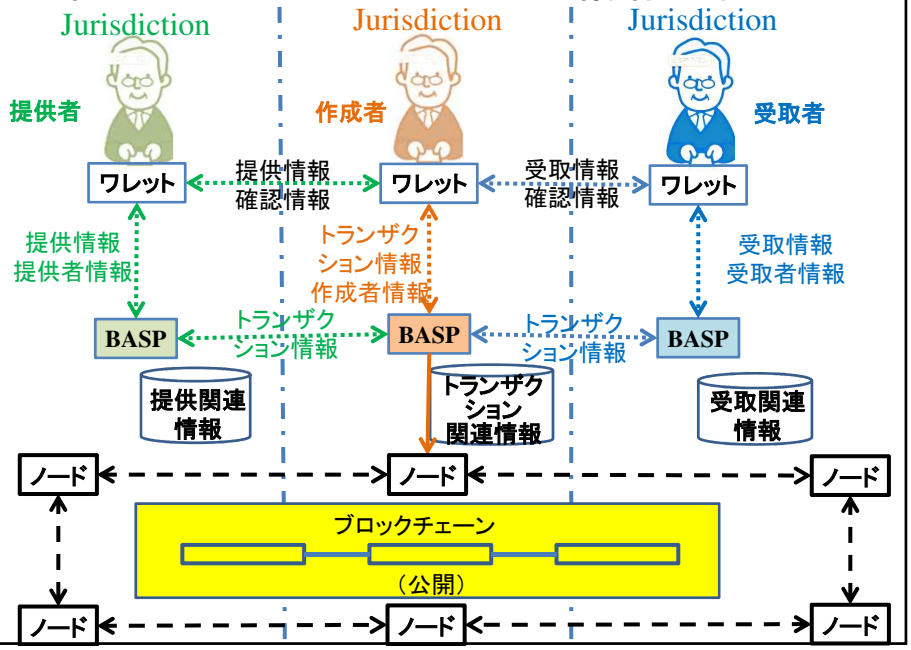
基本方針

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
統合環境への発展の可能性

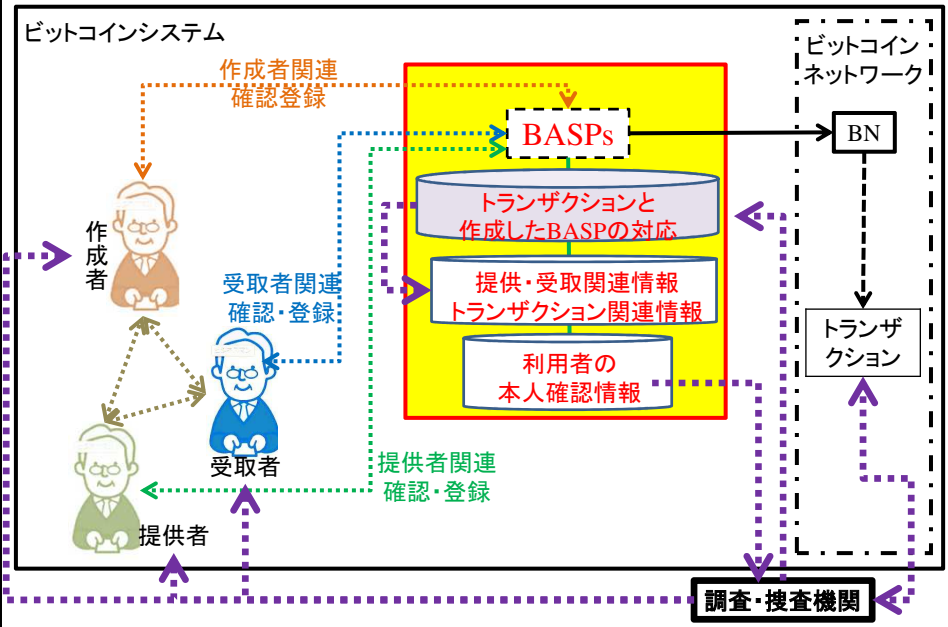
各法域および法域間での情報確認



5.2 BITFRA

 17

BASPで管理する情報と利用者の特定・追跡方法



6. BITFRAの評価・考察

 18

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」

〇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」

〇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」

〇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での実現を想定

資産の移転を示すトランザクションにより資産の移転・残高の管理を行う
TCAMS（Transaction based CryptoAssets Management System）方式の
暗号資産に適用可能と想定

提案方式BITFRAの評価・考察（FATFトラベルルールの観点から）

トラベルルールの具体的要件：
提供者が利用しているVASPは受取者が利用しているVASPへ、提供者と受取者に関する、提供者の名前・アカウント番号・住所・個人識別番号および受取者の名前・アカウント番号等の利用者の情報を、トランザクション（暗号資産移転情報）と共に送付すること

BITFRA：
法域（国）の異なる可能性のあるBASP間での個人情報の送受を回避
①信頼できるBASPによる利用者の情報の確認結果を署名にて
通信相手のBASPへ通知し利用者の特定・追跡性を保証する仕組み
②利用者の個人情報はそれぞれのBASPが格納しており、
必要に応じすべての利用者の個人情報にアクセス可能な仕組み

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
　仮想通貨取引所は、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、
　等の規制か？

2020年12月　米国FinCEN：Financial Crimes Enforcement Network
　ユーザ個人のワレットで、1日に1万ドルを超える送金の場合、
　仮想通貨取引所はレポートを提出要、等の規制案を公表

2021年3月　FATF　トラベルルール改定の動き
　P2P暗号資産取引プラットフォームに規制準備を公表

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