IPSJ第81回全国大会　7G-03　2019年3月16日

暗号仮想通貨における匿名化技術の現状と展望

（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）仮想通貨の概況

仮想通貨　時価総額ベスト10
（2019年2月22日現在）

順位	名称	記号	時価総額
1	Bitcoin	BTC	$69.75 B
2	Ethereum	ETH	$15.44 B
3	XRP	XRP	$13.32 B
4	EOS	EOS	$3.48 B
5	Litecoin	LTC	$3.00 B
6	Bitcoin Cash	BCH	$2.55 B
7	Tether	USDT	$2.03 B
8	Stellar	XLM	$1.72 B
9	TRON	TRX	$1.66 B
10	Binance Coin	BNB	$1.53 B

2019年2月22日現在2082通貨（資産総額 $134.35 B　約15兆円）

出典：All Cryptocurrencies　https://coinmarketcap.com/all/views/all/

（1）仮想通貨の概況

匿名仮想通貨　時価総額ベスト10）
（2019年2月22日現在）

順位	名称	記号	時価総額
13	Monero	XMR	$870.53 M
20	Zcash	ZEC	$327.00 M
39	Bytecoin	BCN	$126.57 M
51	Verge	XVG	$97.60 M
65	Electroneum	ETN	$63.99 M
75	PIVX	PIVX	$44.64 M
91	Zcoin	XZC	$37.38 M
236	NavCoin	NAV	$10.38 M
321	DigitalNote	XDN	$6.88 M
392	Aeon	AEON	$4.86 M

出典：All Cryptocurrencies　https://coinmarketcap.com/all/views/all/

 3

（2）仮想通貨の匿名性

仮想通貨の匿名性の現状

（1）一定レベルの匿名性が存在

利用者は公開鍵、アドレスにより表現され、一般に特定は困難

➔匿名性の犯罪での利用が社会問題

各国での規制が強化される方向、EUでは統一規制の動きも

仮想通貨システムへの特定・追跡性への要求

EU第5次マネーロンダリング対策指令（2018年7月9日施行）

“仮想通貨のアドレスとその仮想通貨の所有者のIDを紐づけられる情報を各国の金融情報機関は得るべき”

仮想通貨の流れを追跡する技術開発が活発

追跡をサービスとして提供するビジネスの発展

ELLIPTIC（英国）、CHAINANALYSIS（米国）

顧客：法執行機関、徴税機関、金融情報機関等

警察庁、取引履歴を追跡するシステム導入へ（昨年8月）.

 4

（2）仮想通貨の匿名性

仮想通貨の匿名性の現状

（2）一般の仮想通貨の匿名性は脆弱

プライバシー・機密情報の確実な保護は困難

➔通貨としての本格活用は困難

匿名性強化のための技術開発が活発、匿名仮想通貨の発展

匿名仮想通貨名称	主要な技術・仕組み	利用者の秘匿	支払額の秘匿
Monero[5]	リング署名、リングCT、ワンタイムアドレス、Kovri （CryptoNoteプロトコル）	○	○
Zcash[6]	zk-SNARKプロトコル （Zerocashプロトコル）	○	○
Bytecoin[7]	ワンタイムアドレス、ワンタイムリング署名（CryptoNoteプロトコル）	○	×
Verge[8]	ステルスアドレス（Wraithプロトコル）、TorやI2P	○	×
Electroneum[9]	ワンタイムアドレス、ワンタイムリング署名（CryptoNoteプロトコル）	○	×

（2）仮想通貨の匿名性 5分

仮想通貨における匿名性と特定・追跡性

匿名性の必要性

プライバシー保護、企業秘密保護のために

特定・追跡性の必要性

犯罪者早期逮捕、犯罪利用抑止のために

公平な徴税のために

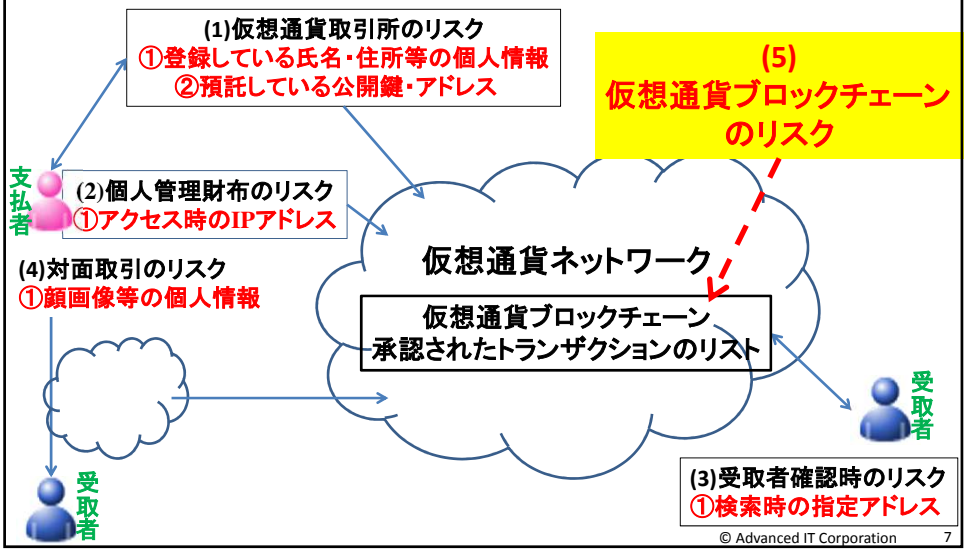
監査可能性を保証するため

➔安心・安全な仮想通貨システムのためには、

匿名性と特定・追跡性の両立は不可欠！

（3）仮想通貨システムの匿名性に関するリスク概観　4分

仮想通貨システムにおける匿名性に関するリスクの現状



 7

（4）仮想通貨ブロックチェーンの匿名性に関する要件

トランザクション内に格納されている匿名性に関連する情報

入力欄		出力欄	
入力項目1	使用する資金の位置（支払者のアドレス、金額が指定されている）	出力項目1	支払先（受取者）の指定（受取者のアドレス）
	指定資金の使用権の証明（公開鍵、署名）		支払額の指定（金額）
入力項目2	使用する資金の位置	出力項目2	支払先（受取者）の指定
	指定資金の使用権の証明		支払額の指定
・・・・・		・・・・・	
入力項目n	使用する資金の位置	出力項目m	支払先（受取者）の指定
	指定資金の使用権の証明		支払額の指定

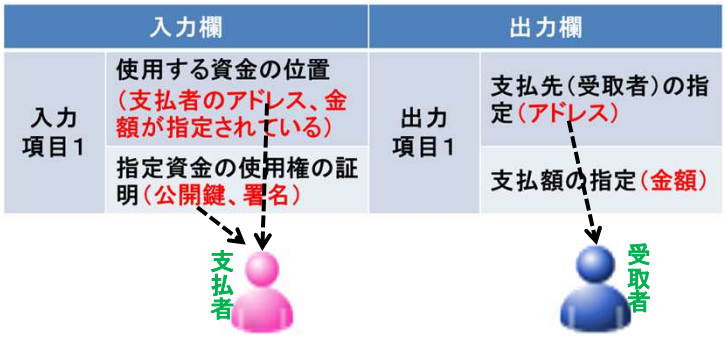
＜入力欄：今回の支払いで使用する原資を指定＞
＜出力欄：今回の原資による支払先・支払額を指定＞

 8

（4）仮想通貨ブロックチェーンの匿名性に関する要件

仮想通貨ブロックチェーンの匿名性に関する要件（1）

公開鍵/アドレスからの利用者の特定不能性

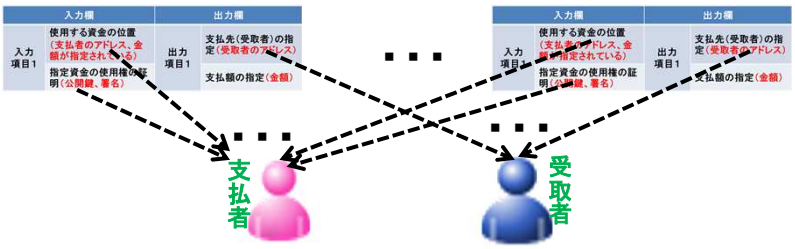


公開鍵、アドレスの生成には、利用者の情報は使用しない。
一般には仮名から利用者を推定するのは困難と考えられる。
➔仮名性 (Pseudonymity)により、一定レベルの匿名性は保証

（4）仮想通貨ブロックチェーンの匿名性に関する要件

仮想通貨ブロックチェーンの匿名性に関する要件（2）

多数のトランザクションの公開鍵/アドレスからの利用者の特定不能性

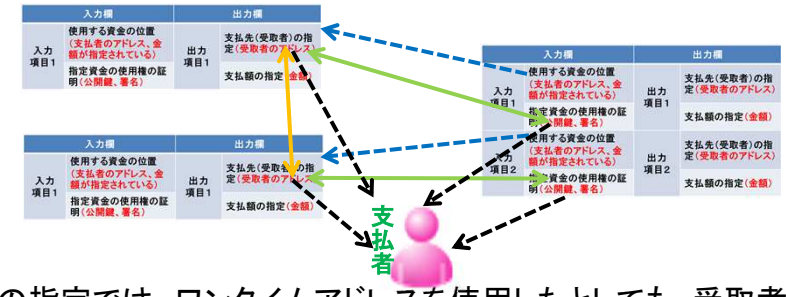


長期的に公開されるブロックチェーンには、同一の公開鍵、アドレスが記録され、支払パターン、受取パターンの分析より利用者が推定される恐れがある。
➔支払/受取の都度、異なるアドレス/公開鍵を使用する
（ワンタイムアドレス、ステルスアドレス）

（4）仮想通貨ブロックチェーンの匿名性に関する要件

仮想通貨ブロックチェーンの匿名性に関する要件（3）

トランザクション間の受取者・支払者の特定不能性



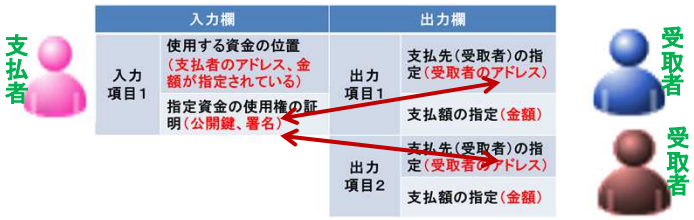
原資の指定では、ワンタイムアドレスを使用したとしても、受取者としてのアドレス、支払者としての公開鍵が同一の利用者に属することを公開することになり、利用者が推定される恐れがある。

➔原資として使用する資金が特定されない仕組みを使用する（CryptoNoteのワンタイムリング署名）

（4）仮想通貨ブロックチェーンの匿名性に関する要件

仮想通貨ブロックチェーンの匿名性に関する要件（4）

トランザクション内の支払者・受取者の対応の特定不能性



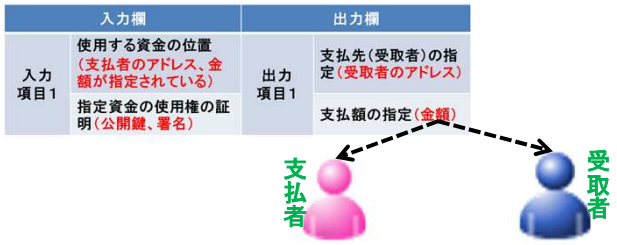
トランザクションは1人の利用者が作成し、複数の受取者への支払いを指定する。その結果、支払者と受取者の対応を公開することになり、利用者が推定される恐れがある。

➔支払者と受取者の対応が特定されない仕組みを使用する（チャウミアンコインジョイン（ミキシング）、タンブルビット（エスクロー））

（4）仮想通貨ブロックチェーンの匿名性に関する要件

仮想通貨ブロックチェーンの匿名性に関する要件（5）

支払額の特定不能性（秘匿）



トランザクションには、支払者-受取者間の支払額が明記され公開されている。大量のトランザクションの支払額の分析により、支払いの目的や利用者が推定される恐れがある。

➔支払額を秘匿しつつも、トランザクションが承認される仕組みを使用する。　　（コンフィデンシャルトランザクション）

（4）仮想通貨ブロックチェーンの匿名性に関する要件　10分

匿名性要件強化策として提案されている主要な技術・仕組み

匿名性に関する要件	主要な提案技術・仕組み
（1）公開鍵/アドレスからの利用者の特定不能性	ー
（2）多数のトランザクションの公開鍵/アドレスからの利用者の特定不能性	①CryptoNoteのワンタイムアドレス
（3）トランザクション間の受取者・支払者の特定不能性	②CryptoNoteのワンタイムリング署名
（4）トランザクション内の支払者・受取者の対応の特定不能性	③チャウミアンコインジョイン ④タンブルビット
（5）支払額の特定不能性（秘匿）	⑤コンフィデンシャルトランザクション（CT）

（5）匿名性強化のための技術・仕組み　10分

①ワンタイムアドレス

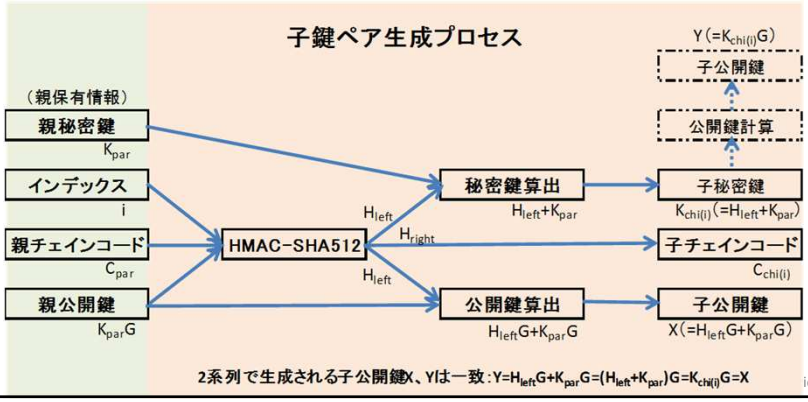
受取者生成方式

①乱数による鍵生成方式

②Hierarchy Deterministic (HD) 鍵生成方式

マスターの鍵ペアは乱数で生成し、

マスター鍵ペアから子鍵ペア、孫鍵ペアと順次生成する方式



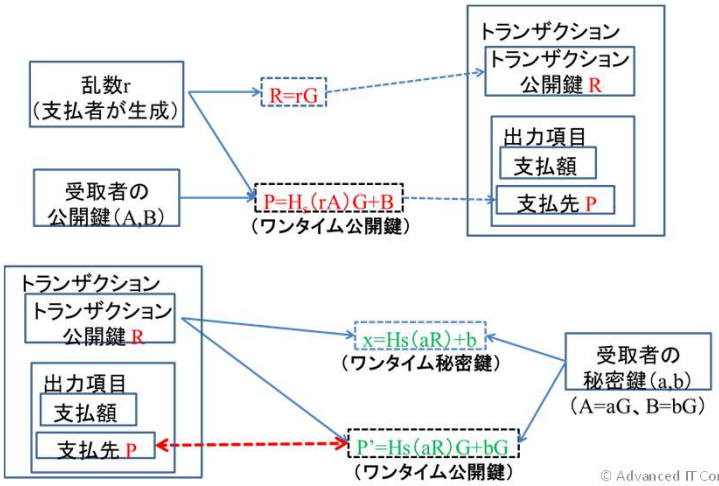
ion　15

（5）匿名性強化のための技術・仕組み

①ワンタイムアドレス

支払者生成方式

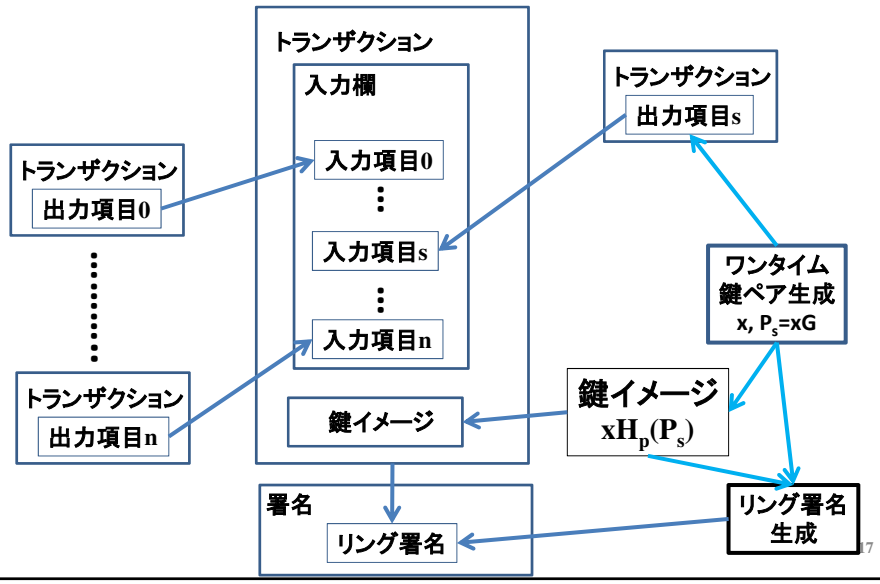
①CryptoNoteワンタイム鍵生成方式（DH鍵共有の仕組みを利用



　16

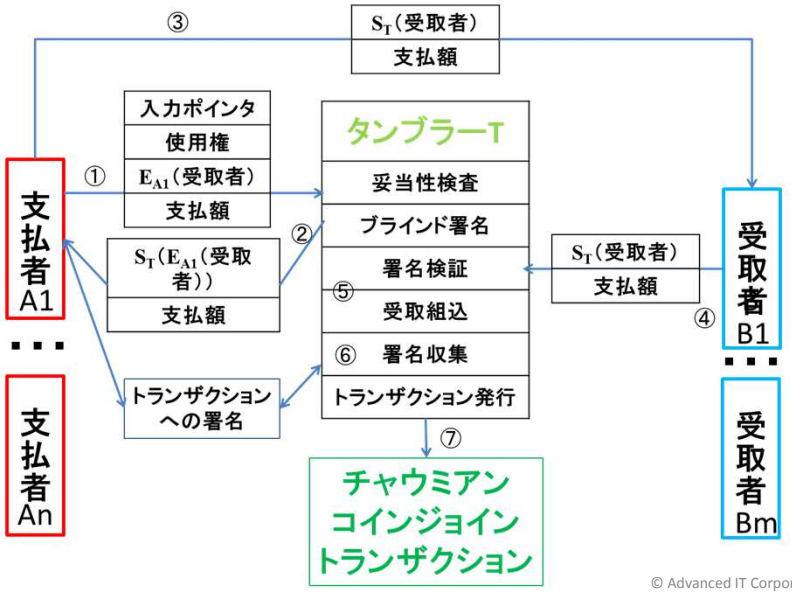
（5）匿名性強化のための技術・仕組み

②CryptoNoteのワンタイムリング署名



（5）匿名性強化のための技術・仕組み

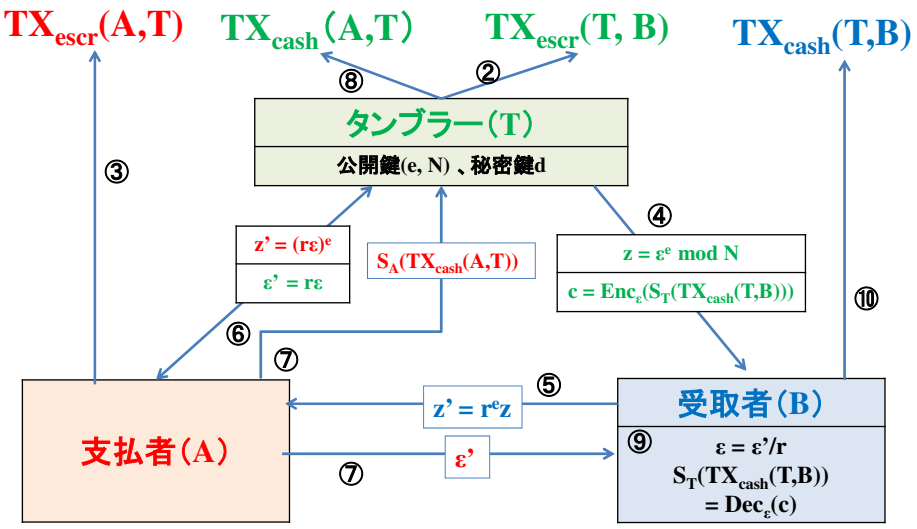
③チャウミアンコインジョイン方式（ミキシング）



 18

（5）匿名性強化のための技術・仕組み

④タンブルビット方式（エスクロー）



 19

（5）匿名性強化のための技術・仕組み

⑤コンフィデンシャルトランザクション（CT）

＜前提＞

入力金額を$a_i(i=1,\ldots,n)$、出力金額を$b_j(j=1,\ldots,m)$とする。

（出力金額には手数料も含めておく。）

＜CT＞

入力金額、出力金額を、乱数を加えたコミットメントで表現する。

$C^{in}_i = a_iG + \alpha_iH$　：G、Hは生成元、α_iは乱数

$C^{out}_j = b_jG + \beta_jH$　：G、Hは生成元、β_jは乱数、

但し、$\beta_m = \Sigma_{i=1}^{n}\alpha_i - \Sigma_{j=1}^{m-1}\beta_j$

入力金額の総額と出力金額の総額の一致は、コミットメントで表現された入力金額の総額と出力金額の総額が0であることを確認すれば良い。

$$\Sigma(a_iG+\alpha_iH) - \Sigma(b_jG + \beta_jH) = (\Sigma a_i - \Sigma b_j)G$$

なお、が適切な数値（負では無い、64ビットで表現できる数値）であることの確認が別途必要だが、ここでは省略。

 20

匿名性強化策として提案されている主要な技術・仕組みの現状・課題

匿名性に関する要件（1）：公開鍵/アドレスからの利用者の特定不能性

匿名性に関する要件（2）： 多数のトランザクションの公開鍵/アドレスからの利用者の特定不能性	提案技術・仕組み： ①CryptoNoteのワンタイムアドレス名

現状・課題：Monero等の基盤として利用されている。同一支払での複数原資の指定時に、ワンタイムアドレス間の連結性が漏洩。

匿名性に関する要件（3）： トランザクション間の受取者・支払者の特定不能性	提案技術・仕組み： ②CryptoNoteのワンタイムリング署名

現状・課題：Monero等の基盤として利用されている。ダミーの原資指定によるトランザクションサイズ、検証のための計算量が増大。

15分

匿名性に関する要件（4）： トランザクション間の受取者・支払者の特定不能性	提案技術・仕組み： ③チャウミアンコインジョイン

現状・課題：オフチェーン実装で利用されている。支払者と受取者の対応が推定できないよう同一の支払額での利用が必要。

匿名性に関する要件（4）： トランザクション内の支払者・受取者の対応の特定不能性	提案技術・仕組み： ④タンブルビット（エスクロー）

現状・課題：Stratisのサイドチェーンに実装され、ビットコインの匿名取引にも利用可能。支払者と受取者の対応が推定できないよう同一の支払額での利用が必要。

匿名性に関する要件（5）： 支払額の特定不能性（秘匿）	提案技術・仕組み： ⑤コンフィデンシャルトランザクション（CT）

現状・課題：ビットコインのサイドチェーンElements Alphaにてテスト/評価中。Moneroでは、リングCTとして実装。

おわりに

①本稿では、仮想通貨におけるプライバシー保護の観点から、
＊仮想通貨ブロックチェーンの匿名性に関する要件を定義し、
＊要件ごとに、匿名性強化のための
主要な技術・仕組みの現状・課題を整理した。

②仮想通貨はプライバシー保護等の観点からの確実な匿名性の保証と共に、犯罪防止等の観点からの利用者の確実な特定・追跡性の保証、が必要と考えている。

③仮想通貨における匿名化技術の調査・整理・体系化を試み、特定・追跡性との両立方式を検討し、安心・安全な仮想通貨システムのあるべき姿を明らかにしたい。

23

終

 24