SCIS 2019 2019 Symposium on Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics, Information and Communication Engineers

仮想通貨の匿名性の現状と課題
Current status and issues about anonymity of virtual currency

才所 敏明[*1] 辻井 重男[*2] 櫻井 幸一[*3]
Toshiaki Saisho Shigeo Tsujii Kouichi Sakurai

あらまし 仮想通貨及び多くのブロックチェーン応用では、確実な匿名性の保証と確実な特定・追跡性の保証の両立が不可欠である。本稿では、仮想通貨および匿名仮想通貨の現状を概観し、ビットコインを対象に、ブロックチェーン上の情報の匿名性強化のために提案されている技術・仕組み、具体的にはワンタイムビットコインアドレス、コンフィデンシャルトランザクション、コインミキシング、エスクロー、リング署名等の技術や仕組みと、それらの利用の現状・課題を整理した。

キーワード 仮想通貨，ブロックチェーン、ビットコイン、コンフィデンシャルトランザクション、コインミキシング、エスクロー

Abstract In virtual currency and many Blockchain applications, we believe that it is indispensable to ensure both anonymity and identifiability / traceability. In this paper, we'll overview the current status of virtual currencies and anonymous virtual currencies. And then, we'll report on the present situation and issues of anonymity of Bitcoin which is the representative of the virtual currency. And then, we'll clarify the technology and mechanism proposed for strengthening the anonymity of information on the Blockchain, such as one-time bitcoin address, confidential transaction, coin mixing, escrow and ring signature, and report their current status and issues.

Keywords Virtual currency，Crypto currency，Blockchain，Bitcoin，Confidential Transaction，Coin Mixing，Escrow

1 はじめに*

仮想通貨の元祖であるビットコインは Satoshi Nakamoto が 2008 年に投稿した論文（[1]）で公開され、2009 年に運用が開始された。以来、2100 もの多数の仮想通貨が登場（2018 年 11 月 6 日現在）、活発な取引が行われている。その中でも仮想通貨の元祖であるビットコインが現在も時価総額は 1 位であり、シェアも 50%前後を占めている（[2]）。

仮想通貨による取引は一般にブロックチェーン上に公開されているため、その公開情報から、取引内容や取引者（支払者、受取者）の情報が第三者に漏れるリスクが存在する。多くの仮想通貨では取引内容や取引者の匿名性の重要性が指摘され、匿名性強化の技術・仕組みが提案されており、また強い匿名性を特徴とする匿名仮想通貨（[3]）も数多く出現している。

本稿では、匿名仮想通貨を含む仮想通貨を概観し、仮想通貨の代表として、ビットコインの匿名性に関する現状・課題を整理の上、公開されているビットコインブロックチェーン上の取引データ（トランザクション）の匿名性を強化する主要な技術・仕組みについて整理する。

2 仮想通貨の現状

仮想通貨は 2018 年 11 月時点で 2100 程度発行されている（[2]）。仮想通貨全体の時価総額は約 215B ドルとな

*1 IT 企画 http://advanced-it.co.jp/
mail:toshiaki.saisho@advanced-it.co.jp
*2 中央大学研究開発機構
mail: tsujii@tamacc.chuo-u.ac.jp
*3 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
mail: sakurai@INF.kyushu-u.ac.jp

っている。図1に主要な仮想通貨、時価総額でベスト20を示している。

順位	名称	記号	時価総額
1	Bitcoin	BTC	$111,603,653,485
2	Ethereum	ETH	$21,686,983,353
3	XRP	XRP	$21,316,167,697
4	Bitcoin Cash	BCH	$9,727,964,629
5	EOS	EOS	$5,062,917,548
6	Stellar	XLM	$4,788,815,193
7	Litecoin	LTC	$3,206,426,163
8	Cardano	ADA	$2,035,116,446
9	Monero	XMR	$1,862,296,670
10	Tether	USDT	$1,765,995,152
11	TRON	TRX	$1,587,865,830
12	Dash	DASH	$1,402,210,855
13	IOTA	MIOTA	$1,392,612,570
14	Binance Coin	BNB	$1,268,969,483
15	NEO	NEO	$1,083,622,072
16	Ethereum Classic	ETC	$1,001,089,213
17	NEM	XEM	$847,260,851
18	Tezos	XTZ	$811,902,521
19	Zcash	ZEC	$636,914,783
20	VeChain	VET	$593,250,850

図1　仮想通貨時価総額ベスト20
（2018年11月6日）

仮想通貨時価総額と世界の貨幣・紙幣全体の発行総額を比較すると、2013年時点で5Bドルに対し5Tドル（5000Bドル）、2015年時点で173Bドルに対し7.6Tドル（7600Bドル）という報告がある（[4]）。仮想通貨の役割はまだまだ微々たるものではあるが、大きな伸びを示している。また、法定通貨もいずれは仮想通貨へと移行するという見通しもある。仮想通貨は匿名性が不十分なことによる課題、逆に匿名性が強いが故にマネーロンダリング等の不正・不法な目的に悪用される課題を抱えているが、このような課題を克服した安心・安全な仮想通貨への期待は強いと考えられる。

3　匿名仮想通貨の現状

2100の仮想通貨全体の中で主要な匿名仮想通貨24の2016年11月6日時点の時価総額は3.35Bドルと推定され、仮想通貨時価総額全体の1.5%程度となっている。図2に、匿名仮想通貨の時価総額ベスト10を示している（[2]，[3]）。

順位	名称	記号	時価総額
9	Monero	XMR	$1,862,296,670
19	Zcash	ZEC	$636,914,783
37	Bytecoin	BCN	$245,387,856
42	Verge	XVG	$207,256,627
52	Electroneum	ETN	$151,134,314
82	PIVX	PIVX	$76,286,056
105	ZCoin	XZC	$57,709,632
198	NavCoin	NAV	$23,457,756
224	DigitalNote	XDN	$19,619,618
300	CloakCoin	CLOAK	$13,500,579

図2　匿名仮想通貨時価総額ベスト10
（2018年11月6日）

匿名性を悪用した不正・不法目的の利用の増加のため、匿名性の強い仮想通貨の取引への制限が各国で強化される見込みであるが、今後も一定程度の伸長が期待されている。図2の匿名仮想通貨について、以下に匿名性に関する特徴を整理しておく。

(1)Monero（[5]）

Moneroの匿名性は、CryptoNoteで提案された匿名化技術を改良し実現されている。採用されている匿名化技術は、リング署名、リングCT（コンフィデンシャルトランザクション）、Kovri、ワンタイムアドレス（ステルスアドレス）である。取引データの支払者、受取者、支払額を秘匿することができる。

(2)Zcash（[6]）

Zcashの匿名性は、Zerocashプロトコルにより実現されている。ゼロ知識証明として知られているzk-SNARKプロトコルが採用されている。取引データの支払者、受取者、支払額を秘匿することができる。

(3)Bytecoin（[7]）

ByteCoinはCryptoNoteで提案された匿名化技術を採用しており、ワンタイムアドレスおよびワンタイムリング署名である。取引データの支払者、受取者のみを秘匿し、支払額を秘匿する機能はない。

(4)Verge（[8]）

Vergeで採用されている匿名化技術は、ステルスアドレス（Wraithプロトコル）、ネットワーク上の通信内容の秘匿や通信の追跡を困難にするTorやI2Pの技術である。取引データの支払者、受取者のみを秘匿し、支払額を秘匿する機能はない。

(5)Electroneum（[9]）

ElectroneumはCryptoNoteで提案された匿名化技術を採用しており、ワンタイムアドレスおよびワンタイムリング署名である。取引データの支払者、受取者のみを秘匿し、支払額を秘匿する機能はない。

(6)PIVX（[10]）

PIVXは、2016年にDASHからのフォークで生まれた仮想通貨である。採用されている匿名化技術は、DASHから引き継いだPrivateSendによるミキシング技術CoinJoinと、Zerocoinプロトコルである。取引データの支払者、受取者のみを秘匿し、支払額を秘匿する機能はない。

(7)Zcoin（[11]）

Zcoinの匿名性は、ミント&スペンドのエスクローの仕組み等、Zerocoinプロトコルにより実現されている。取引データの支払者、受取者のみを秘匿し、支払額を秘匿する機能はない。

(8)NavCoin（[12]）

NavCoinで採用されている主な匿名化技術は、ブロックチェーン上での支払者/受取者の秘匿のためのエスクローの仕組み（Navtech Server Cluster）、サブチェーン（サイドチェーン）上での情報の秘匿のための暗号化である。取引データの支払者、受取者、支払額を秘匿することができる。

(9)DigitalNote（[13]）

DigitalNote も CryptoNote で提案された匿名化技術を採用しており、ワンタイムアドレスおよびワンタイムリング署名である。取引データの支払者、受取者のみを秘匿し、支払額を秘匿する機能はない。

(10)CloakCoin（[14]）

CloakCoin で採用されている主な匿名化技術は、オフチェーン上で実施されるミキシング、匿名通信のための TOR、内容の秘匿に暗号技術、ステルスアドレス等である。取引データの支払者、受取者のみを秘匿し、支払額を秘匿する機能はない。

4　ビットコインの匿名性

匿名仮想通貨は、匿名性を特徴として新たに開発され発展してきたが、現時点でも匿名性が不十分な仮想通貨が仮想通貨時価総額の 98%近くを占めている。その中でも、仮想通貨の元祖であるビットコインは依然として仮想通貨時価総額の 50%以上を占めており、このような市場支配の状況からビットコインへの匿名性強化の研究開発も活発に展開されている。

ビットコインシステムでは、支払データ（トランザクション）をブロックチェーンで記録し管理しており、インターネット上に公開されている。多くの仮想通貨も同様の仕組みで運用されている。トランザクションやブロックチェーンの保護のために暗号技術が利用されているため、仮想通貨は暗号通貨とも呼ばれている。

本章では、4.1 にてビットコインシステムにおける匿名性上のリスクについて概要を述べる。4.2 では、ビットコイントランザクションに含まれる匿名性に関わる情報について、4.3 ではその情報に基づく匿名性のリスクを述べる。4.4 においては、ビットコイントランザクションの匿名性を強化する主要な対策技術（仕組み）の概要を紹介し、4.5 にてそれらの対策技術の現状・課題を、また 4.6 にて対策技術の実装方式に関し整理している。

4.1　ビットコインシステムにおける匿名性の現状

現状のビットコインシステムに存在する主要な匿名性のリスクを以下に列記する。

(1)仮想通貨取引所のリスク

日本の仮想通貨取引所は、アカウント開設時に本人確認（KYC）を求められている（取引所への個人情報の登録や証明書類の提出、実住所への郵送物の受け取り確認等の手続きが必要）ため、取引所でビットコインアドレス（公開鍵）と本人情報の紐づけがなされている。（海外では未だ確実な本人確認がなされていない仮想通貨取引所も多いが、多くの国ではマネーロンダリング等の不法な資金移動の検知の仕組みの必要性が議論されている。）

(2)ウォレットのリスク

一般には、鍵ペアおよびビットコインアドレスは個人管理下のクライアント内または専用のウォレットに格納しておくのが望ましいが、取引所にビットコインアドレスを預託するウェブウォレット等の場合は、取引所にてビットコインアドレスと本人情報との対応が管理されている。

(3)対面取引のリスク

対面でのビットコインを利用した取引相手には、ビットコインのアドレスと本人の関係を知られてしまう。

(4)ブロックチェーン/トランザクションのリスク

公開されているブロックチェーン/トランザクションから、ビットコインアドレス間のビットコインの移動および支払額が把握できる。

＝＞トランザクションの情報の匿名性を高める仕組みを利用する（詳細は次節以降）。

(5)ブロックチェーン検索時のリスク

SPV（Simplified Payment Verification）ウォレットの場合、必要なトランザクションの情報収集に使用するブルームフィルタから、ウォレットに紐づけられているビットコインアドレスが特定され、更に利用者が特定されるリスクがある。

(6)ビットコインネットワークアクセス時のリスク

ビットコイン・ネットワークに接続する際の IP アドレスから、利用者が特定されるリスクがある。

4.2　ビットコイントランザクションの構成

ビットコインのトランザクションに含まれている匿名性に関連する情報は以下の通りである。

＜入力欄：今回の支払いで使用する原資を指定＞

＊使用する資金の指定(1)

＊指定資金の使用権の証明(2)

＜出力欄：今回の原資による支払先・支払額を指定＞

＊支払先（受取者）の指定(3)

＊支払額の指定(4)

入力欄		出力欄	
入力項目1	使用する資金の指定（1）	出力項目1	支払先（受取者）の指定（3）
	指定資金の使用権の証明（2）		支払額の指定（4）
入力項目2	使用する資金の指定	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	使用する資金の指定	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

図 3　トランザクションの論理構成
（匿名性に関連する情報のみ）

(1) 使用する資金の指定

新たにトランザクションを発行する支払者はその支払の原資とする資金をトランザクションの入力欄に指定する。使用する資金は、過去にその支払者宛に支払われ未だ使用されていない資金であり、入力欄にはその資金が定義されているブロックチェーン上のトランザクション ID と

その出力欄の何番目の出力項目かを示すポインタを指定する。

ポインタが示す出力項目には、支払先（受取者）のビットコインアドレスおよび支払額（受取者の受取額）が指定されている。ビットコインアドレスは、その資金の受取者を示す情報で、一般には受取者の公開鍵から生成されたコードである。支払額（新たなトランザクションを発行する支払者の受取額）は、平文のまま指定されている。

(2) 指定資金の使用権の証明

支払者は、原資として指定された資金の使用権を保有していることを示す情報を指定する。支払者が原資として指定した出力項目には、ビットコインアドレスで受取者が指定されている。支払者は、そのビットコインアドレスが支払者自身のものであり、その資金を使用する権利を保有することを示す必要がある。

そのため、支払者は、ビットコインアドレス生成の元になった公開鍵を指定すると共に、対応する秘密鍵による新たに発行するトランザクションへの署名を指定する。

使用する資金の原資は複数の場合もあり、入力欄には資金の指定および使用権の証明から構成される入力項目が複数指定されることもある。

(3) 支払先（受取者）の指定

支払者は、支払先（受取者）を受取者のビットコインアドレスにより指定する。

(4) 支払額の指定

支払者は、支払先（受取者）へ支払う金額を指定する。支払額は、平文のまま指定する。

4.3 ブロックチェーン/トランザクションの匿名性

ブロックチェーン上で公開されるトランザクションには、3 章で述べた情報が格納されている。匿名性の観点から期待される要件に関するビットコインのブロックチェーン/トランザクションの課題および対応策は、以下の通りである。

(1)支払者・受取者のビットコインアドレス/公開鍵の匿名性の確保

支払者は、原資となる資金を指定する際に、その資金の支払先（受取者）として指定されたビットコインアドレスが支払者自身のものであることを主張し、その資金の使用権を保有することを示すため、ビットコインアドレス生成の元になった公開鍵を示し、かつ署名を示すことにより、その公開鍵に対応する秘密鍵を保有していることを示す仕組みとなっている。そのため、ブロックチェーン上のトランザクションには支払者・受取者の公開鍵やビットコインアドレスが格納され、公開されることになる。

一般に、公開鍵やビットコインアドレスから支払者・受取者を特定することは困難であるため、**仮名性（Pseudonymity）**によりある程度の匿名性は確保されていると考えられる。しかし、ブロックチェーン上に記録されている膨大なトランザクションの情報から、その公開鍵/ビットコインアドレスを利用した支払・受取を把握でき、その支払・受取行動の特徴分析等から、支払者・受取者をある程度推定することも可能である。実際、同様の分析をサービスとして提供する企業も存在する。

特に、支払者・受取者の公開鍵（およびビットコインアドレス）が固定の場合は、複数のトランザクションにおける支払者・受取者の連結性（Linkability）により、支払・受取行動の特徴分析等から、支払者・受取者の推定が容易となるため、支払者・受取者が使用する公開鍵は都度変更することが望ましい。そのために、**ワンタイムビットコインアドレス（4.4.1 を参照）**の仕組みにより**非連結性（Unlinkability）**を実現する方法が複数提案されており、既にウォレットに実装されている仕組みもある。

(2)支払者・受取者の対応（資金の流れ）の秘匿

ブロックチェーン上のトランザクションにおいて、支払者と受取者の対応関係がわかると、支払者・受取者の特定・追跡につながりかねない。資金の流れの追跡を困難にすることが望ましい。

ビットコインでは、トランザクション内に示す資金の流れ、支払者と受取者の関係を秘匿する方法として、複数人の支払者による支払いを一つのトランザクションにまとめる**ミキシング（4.4.2 を参照）**、トランザクションの仲介者・システムへの迂回を利用した**エスクロー（4.4.3 を参照）**など、トランザクション内の資金の流れの**非追跡性（Untraceability）**を実現する方法が提案されている。

また、トランザクション間で、支払先に示された受取者が受取者であることを証明する際に、受取者の特定・追跡を困難にする**リング署名（4.4.4 を参照）**など、トランザクション間の**非追跡性（Untraceability）**を実現する方法が提案されている。

(3) 支払額（受取額）の秘匿

支払額が支払者・受取者の特定・追跡に直接つながるケースは少ないと考えられるが、同一支払額の多数のトランザクションが存在した場合はトランザクションの発行時期や発行頻度から、取引内容の推定、更には支払者・請負者の推定につながりかねず、トランザクション内の支払額（出力項目に指定）の秘匿も望ましい。一方、正しいトランザクションとして承認されるためには、検証者であるマイナーは、個々の入力金額、出力金額（支払額）を知る必要は無いが、入力金額の合計と、出力金額の合計が一致するかどうか確認できる必要がある。

ビットコインでは、このように個々の入力金額（受取額）、出力金額（支払額）の値を公開せず、受取額の合計と支払額の合計が一致することを示すために、**コンフィデンシャルトランザクション（4.4.5 を参照）**が提案されている。

4.4 トランザクションの匿名性強化策として提案されている技術・仕組み

4.4.1. ワンタイムビットコインアドレス（ステルスアドレス）

支払者・受取者の公開鍵（およびビットコインアドレス）

が固定の場合は、支払・受取行動の特徴分析等から、支払者・受取者の推定が容易となるため、支払者・受取者が使用する公開鍵は都度変更することが望ましい。具体的には、トランザクションの出力項目の支払先としては都度異なるビットコインアドレスを指定してもらうのが望ましい。そのために、ワンタイムビットコインアドレスを使用する仕組みが提案されており、既にウォレットに実装されている仕組みもある。

代表的なワンタイムビットコインアドレスの仕組みは以下の通り。

(1)乱数による鍵生成

受取者は、自分が使用する秘密鍵・公開鍵のペアを多数生成しておき、受取の都度、異なる公開鍵から生成されるビットコインアドレスをその支払者にオフチェーンで連絡し、支払先として指定を依頼する方法である。

(2)Hierarchy Deterministic (HD) 鍵生成（[15]）

HD 鍵生成は、１つのシードからマスター秘密鍵を生成し、その秘密鍵から更に子の秘密鍵を生成、という具合に、順次下位の秘密鍵を生成する仕組みで、管理するのは、シード（またはマスター秘密鍵）のみで良い、という特徴がある。

なお、対応する公開鍵は各秘密鍵からも生成できるが、マスター公開鍵から同様の仕組みで順次下位の秘密鍵に対応する公開鍵を生成することも可能である。いずれにせよ、受取者は、受取りの都度、異なる子公開鍵から生成されるビットコインアドレスをその支払者にオフチェーンで連絡し、支払先として指定を依頼する必要がある。

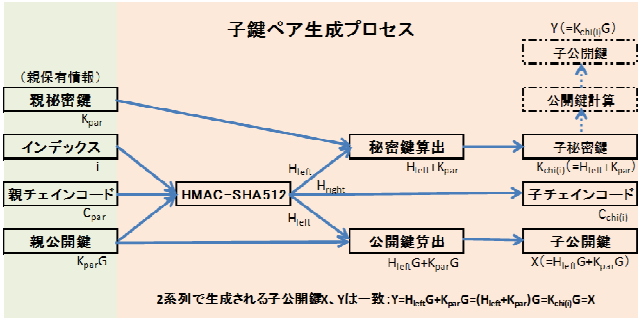

図４　HD 鍵生成の仕組み

(3)CryptoNote の鍵生成

上述の(1)、(2)は、ワンタイムビットコインアドレス/公開鍵を受取者側が生成するため、支払者への事前の連絡が必要である。Nicolas van Saberhagen が提案している鍵生成では、支払者側が受取者のためのワンタイム公開鍵を生成し受取者として指定の上、受取りのための秘密の情報を受取者だけに知らせる仕組みを利用するので、支払者・受取者間の事前の連絡が不要な方法である（[16]）。

前提として、受取者は 2 つの秘密鍵 a, b、それに対応する公開鍵 A(=aG), B(=bG)を保有しているものとする。

支払者は、生成した乱数 r と生成元 G を利用し、トランザクション公開鍵 R(=rG)をトランザクションに追加で格納する。次に支払者は、支払先（受取者）の 2 つの公開鍵と生成した乱数 r を利用し、下記のワンタイム公開鍵 P を生成し、受取者を指定する領域に格納する。

$$P = H_s(rA)G + B \qquad : H_s \text{ は暗号ハッシュ関数}$$

受取者は、保有する秘密鍵 a, b とトランザクションに格納されているトランザクション公開鍵 R を利用し、次式で P’を生成する。受取者が正しい 2 つの秘密鍵 a, b を保有していれば、P＝P’となる。

$$P' = H_s(aR)G + bG$$

また、保有する秘密鍵 a,b とトランザクションに格納されているトランザクション公開鍵 R を利用しワンタイム秘密鍵 x を下記の式にて算出できるので、受取者は支払額を使用することができる。

$$x = H_s(aR) + b$$

4.4.2.　コインミキシング（Coin Mixing）

通常のトランザクションは、一人の支払者が発行する。その結果、支払先（受取者）へ支払うのはトランザクションの発行者であり支払者であることは明白である。

そこで、複数人の支払者の支払データを一つのトランザクションにまとめることにより、支払者と受取者の対応を難しくする、というアイデアに基づく方法である。

(1)コインジョイン（CoinJoin）

コインジョインは、Gregory Maxwell が発表した方法である。

公開されるブロックチェーン上のトランザクションには、複数の支払者の入力項目がランダムに並んだ入力欄と、それぞれの支払者の支払先の全てを含む出力項目がランダムに並べられた出力欄が格納され、支払者を示す入力項目と受取者を示す出力項目の対応を難しくする方法である。

しかし、個々の入力項目の金額や、出力項目の金額が異なっている場合、その金額から対応が推測されるリスクがある。そこで、コインジョインでは、一般に金額を同じにする、あるいは金額が同じのものをまとめる、という工夫が必要である。

(2)チャウミアン・コインジョイン（Chaumian CoinJoin）

チャウミアン・コインジョインも、Gregory Maxwell が発表した方法である。

(1)のコインジョインでは、複数人の支払データをまとめるシステムは、支払者と受取者の対応を知ることができる。チャウミアン・コインジョインは、支払データを統合するシステム（タンブラー）に対しても、対応を秘匿にできる仕組みである。なお、チャウミアン・コインジョインにおいても、出力金額を同じにする等の工夫は必要である。

①支払者は以下の情報をタンブラーに渡す。

㋐自分が支払う元となる資産（原資）の所在

㋑その資産の使用権の証明（公開鍵と対応する秘密鍵による署名）

㋒支払額と暗号化された支払先（受取者）のアドレス

②タンブラーは、有効なトランザクションを構成することを確認後、暗号化された受取者のアドレスにブラインド署名を付与し、支払額と共に支払者に返す。

③支払者は、受取者のアドレスをタンブラーの署名付きのまま復号し、支払額と共に、受取者に渡す。
④受取者は、復号されたタンブラーの署名付き受取者アドレスと受取額をタンブラーへ渡す。
⑤タンブラーは、受取者のアドレスにタンブラーが付与した署名が付与されていることを確認し、受取額（支払額）が同一の出力項目の支払先として組み込む。
⑥タンブラーは、出力項目に格納すべき支払先（受取者）のアドレス、支払額が集まったら、統合したコインジョイントランザクションを作成する。
⑦タンブラーは、コインジョイントランザクションに支払者全員の署名を求め、署名済みの有効なトランザクションをブロードキャストする。

4.4.3. エスクロー（Escrow）

エスクローとは、一般には取引の安全性を保証するために売り手と買い手の間に入る第三者（仲介者・サービス）を意味する。仮想通貨の世界では、支払者と受取者の対応を難しくするために、このエスクローの仕組みが利用されている。

支払者はエスクローへ支払い、エスクローが支払者に代わって受取者へ支払う。本来は支払者から受取者への支払いを示すトランザクション 1 つの発行で済むところを、2 つのトランザクションに分け発行することにより、支払者と受取者の対応を難しくする仕組みである。なお、この仕組みにおいても、支払額から支払者と受取者の対応が推定されるリスクもあり、金額を同じにする工夫は必要である。

エスクローの仕組みを利用したシステムの一つが、Ethan Heilman の研究者グループによって提案された TumbleBit（[20]）である。Chaumian CoinJoin との違いは、仲介するシステムの信頼性に依存しないことである。信頼できないタンブラーを利用しつつも、匿名性を損なうことも無く、ビットコインが盗まれることも無く、また勝手な支払いを発生されないことも保証された仕組みである。TumbleBit は、1BTC（ビットコイン）単位の、オフチェーンによる高速支払いを可能とし、結果はブロックチェーンに記録される。

4.4.4. リング署名

ビットコインでは、支払者が原資として使用する資金の指定には原資の所在地（トランザクション ID および出力欄の何番目の出力項目か）が使用され、その出力項目には受取者のビットコインアドレスが格納されている。また、その原資の使用権を証明するために、入力項目にはビットコインアドレスに対応する公開鍵と、その公開鍵に対応する秘密鍵による署名を指定する。

ビットコインでは、入力項目に格納されている公開鍵からビットコインアドレスを生成し、そのビットコインアドレスが原資として指定されたビットコインアドレスとの一致の確認により、またその公開鍵による格納されている署名の検証により、公開されているブロックチェーン上のトランザクション間のリンクを検証者が確認できる。このような、異なるトランザクション間の支払者と受取者の同一性の公開は、支払者・受取者の特定に繋がりかねない。そこで、どの支払者とどの受取者が同一であるかの特定を困難にする方法が望まれ、リング署名を利用した方法が提案されている。

リング署名を利用した仕組みの一つが、ビットコインの匿名性強化のための技術として、Nicolas van Saberhagen が CryptoNote（[16]）にて発表したワンタイムリング署名である。

4.4.5. コンフィデンシャルトランザクション（CT）

コンフィデンシャルトランザクションは、Gregory Maxwell が発表した、支払額（出力項目に指定）の秘匿と、第三者による入力金額の合計と出力金額（支払額）の合計の一致を検証可能とする仕組みである（[17]）。コンフィデンシャルトランザクションは、以下に例を示すペダーセンコミットメントおよびボロミアンリング署名を利用し構成されている。

(1)ペダーセンコミットメント

入力項目が n 個ありそれぞれの入力金額を $a_i(i=1,\ldots,n)$、出力項目が m 個ありそれぞれの出力金額を $b_j(j=1,\ldots,m)$とする。出力金額には手数料も含まれているものとする。

入力金額の合計と出力金額の合計の一致を示すには、$\Sigma_i(a_i)=\Sigma_j(b_j)$を示せばよいが、そのためには入力金額、出力金額がそのまま格納されている必要があり、出力金額（支払額）が全て公開されてしまうことになる。

CT では、楕円曲線上の点を使用し構成されるペダーセンコミットメントを利用する。j 番目の出力金額 b_j は、2 つの生成元 G、H とブラインディングファクタ（乱数）β_j を利用し、コミットメント　$C^{out}_j = b_jG + \beta_jH$　で表現する。i 番目の入力金額 a_i は、同様に 2 つの生成元 G、H とブラインディングファクタ α_i で、それぞれ格納されているものとする。なお、最後の出力金額のブラインディングファクタ β_m は　$\beta_m = \Sigma_{i=1}^{n}\alpha_i - \Sigma_{j=1}^{m-1}\beta_j$　とする。

このような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の差は、

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

となり、この式の値が 0 となることの確認が、入力金額の総額と出力金額の総額が一致していることの確認となる。

以上のように、金額をコミットメントとして表現することにより金額を公開することなく、入力金額の総額と出力金額の総額が一致することを示すことができる。

なお、出力金額 b_j は適切な金額、つまり b_j がビットコインで金額を格納する 8 バイト（64 ビット）で表現できる範囲内にあることが前提であるが、$(\Sigma a_i - \Sigma b_j) = 0$ の確認だけでは、全ての出力金額 b_j がその範囲内にあることは確認できないため、ボロミアンリング署名を利用した「数値の範囲の証明（Range Proofs）が別途必要である。

4.5 提案されている技術・仕組みの課題・現状

本章では、4.4 で述べた各技術・仕組みの課題・現状について、整理する。

(1)ワンタイムビットコインアドレス

乱数による鍵生成およびHD鍵生成の場合は、既に多くのウォレットに実装され、利用されている。課題は、両方式とも、受取者が生成したワンタイムビットコインアドレスを事前に支払者へ連絡することが必要な点、である。

一方、CryptoNoteの鍵生成の場合は、支払者が受取者の公開鍵を利用し受取者のワンタイムビットコインアドレスを生成するので、事前の連絡は不要である。課題は、本方式の場合、トランザクションに新たにトランザクション公開鍵を格納する必要があり、トランザクションの構造が変わること、である。

ワンタイムビットコインアドレスの共通の課題は、ワンタイムビットコインアドレスで受け取った資金を複数まとめて支払うトランザクションを発行した場合、指定された複数のワンタイムビットコインアドレスの連結性を暴露することになること、である。

(2)コインミキシング（Coin Mixing）

ビットコインのためのミキシングサービス/システムは、多数存在し利用されている。

コインジョイン方式の場合の課題は、ミキシングサービス/システムがトランザクションの情報を知り得ると共に操作できる立場であるため、支払者と受取者の対応を暴露されたり、資金が意図しない受取者に流れたりするリスクが存在することである。

チャウミアン・コインジョイン方式の場合も、支払者と受取者の対応を暴露されるリスクは回避できるが、資金が意図しない受取者に流れたりするリスクが存在することである。

(3) TumbleBitによるエスクロー（Escrow）

TumbleBitは、ミキシングサービス/システムとは異なり、受取者と支払者の対応が暴露されるリスク、資金が意図しない受取者に流れたりするリスクが存在しないことである。

Stratis（マイクロソフトがサポートする仮想通貨）のサイドチェーン上にTumbleBitが実装され、ビットコインの匿名取引を実現している。

(4)CryptoNoteのワンタイムリング署名

ビットコインでの利用の動きは無いが、他の仮想通貨の基盤として利用されている。

課題は、多数のダミーの入力項目が必要で、リング署名の格納に大きなスペースが必要、検証には大きな計算量が必要、という点である。

(5)コンフィデンシャルトランザクション（CT）

ビットコインのサイドチェーンElements Alphaにてテスト/評価されており、ビットコインへ組み込む動きもある。

4.6 提案されている技術・仕組みの実装方式

ビットコインブロックチェーンの匿名性強化のための技術・仕組みの実装方式を、メインチェーンでの実装、サイドチェーンとしての実装、オフチェーンとしての実装の三つに分類し、それぞれの方式の特徴と4.4で述べた各技術・仕組みの実装あるいはその取り組みとの関連を整理しておく。

(1)メインチェーン（オンチェーン）での実装

ビットコインブロックチェーンの仕様変更により、新たな機能・仕組みを実装する方法である。ビットコインブロックチェーンの基本仕様を変えずに、残されている拡張性や可変部分の修正により改良・拡張するソフトフォーク、ビットコインブロックチェーンの基本仕様の変更を伴うハードフォークによる方法がある。

メインチェーンでの実装は、ビットコインブロックチェーンの仕様変更を伴い、ビットコイン・ネットワークの参加者であるビットコインコア開発者、マイニング事業者（マイナー）、仮想通貨取引所、仮想通貨による売買・決裁事業者、仮想通貨利用者の合意が必要である。このようなビットコイン・ネットワーク参加者の利害・意見は往々にして一致せず、メインチェーンでのビットコインの匿名性強化の実現には時間がかかるものと推察される。

(2)サイドチェーンとしての実装

サイドチェーンとは、メインチェーンから生成されるブロックチェーンで、両ブロックチェーン間のデータのやり取りが可能な技術・仕組みである。メインチェーンの場合とは異なり、匿名性を強化する新たな技術・仕組みの実装を容易に実施可能で、実証の場としての活用が可能である。

TumbleBitは、ビットコインのサイドチェーンStratisに実装され、ビットコインの匿名取引を実現している。また、コンフィデンシャルトランザクション（CT）も、サイドチェーンElements Alphaに実装され、テスト/評価されている。CTは、メインチェーンへのソフトフォークによる実装の提案もなされているが、未だ具体化していない。

(3)オフチェーンとしての実装

オフチェーンとは、メインチェーンの外で、独自のブロックチェーンは生成せず、データのやり取りを行う技術・仕組みである。サイドチェーンと同様、匿名性を強化する新たな技術・仕組みの実装を容易に実施可能である。

コインミキシングやエスクローの技術・仕組みがオフチェーン方式で実装され利用されている。

5 おわりに

仮想通貨の匿名性は、プライバシー保護の観点から、今後ますます重要視されるものと考えられる。匿名性が不十分なビットコインにおいても、今後も匿名性強化の研究開発や具体的実装提案が展開される見込みである。

一方、仮想通貨の匿名性は、マネーロンダリングや不法な販売・サービスサイトの支払い手段として活用され大きな社会問題となっており、各国での規制が強化されつつある。実際、EUでは第5次マネーロンダリング対策指令（[21]）が2018年7月9日に施行され、“仮想通貨のア

ドレスとその仮想通貨の所有者の ID とを紐づけられる情報を各国の金融情報機関（Financial Intelligence Units）は得るべきである”と記載されている。

安心・安全な社会を支える通貨としての役割を仮想通貨が担うためには、プライバシーの確実な保護が可能な匿名性と、不正・不法な利用に対してはその行為者に対しタイムリーに法的措置を取れる特定・追跡性が両立できる技術・仕組みが求められている。

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。

参考文献

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2001. https://bitcoin.org/bitcoin.pdf

[2] All Cryptocurrencies https://coinmarketcap.com/all/views/all/

[3] Top 28 Best Privacy Coins 2018 https://kingpassive.com/best-privacy-coins-2018/

[4] All of the World’s Money and Markets in One Visualization http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/

[5] Monero Privacy in the blockchain v1.0 https://eprint.iacr.org/2018/535.pdf

[6] Zcash Protocol Specification https://www.btrade.co.kr/btrade_res/20180507145055652.pdf

[7] Bytecoin (BCN)-Whitepaper https://whitepaperdatabase.com/bytecoin-bcn-whitepaper/

[8] Verge Currency Blackpaper rev 3.0.pdf https://vergecurrency.com/static/blackpaper/Verge-Anonymity-Centric-CryptoCurrency.pdf

[9] Electroneum’s Blockchain and Cryptonote Algorithm Technology https://electroneum.com/technical-white-paper.pdf

[10] Private Instant Verified Transaction - White Paper https://pivx.org/wp-content/uploads/2018/10/PIVX-White.pdf

[11] ZCoin (XZC)-Whitepaper https://whitepaperdatabase.com/zcoin-xzc-whitepaper/

[12] NAV-Coin-Whitepaper https://whitepaperdatabase.com/nav-coin-nav-whitepaper/

[13] DigitalNote http://xdndigitalnote.com/wp-content/uploads/2017/07/whitepaper.pdf

[14] CloakCoin_Whitepaper_v2.1 https://www.cloakcoin.com/user/themes/g5_cloak/resources/CloakCoin_Whitepaper_v2.1.pdf

[15] Hierarchical Deterministic Wallets(BIP-32) https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[16] Nicolas van Saberhagen, "CryptoNote v2.0", 2013. https://cryptonote.org/whitepaper.pdf

[17] Greg Maxwell, "Confidential Transactions", 2016.https://people.xiph.org/~greg/confidential_values.txt

[18] Elements, "An open source, sidechain-capable blockchain platform". https://elementsproject.org/

[19] Gregory Maxwell, Andrew Poelstra, ”Borromean Ring Signature”, 2015. https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf

[20] Ethan Heilman, etc., "TumbleBit:An Untrusted Bitcoin-Compatible Anonymous Payment Hub", 2016. https://eprint.iacr.org/2016/575.pdf

[21] DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843

[22] 穴田啓晃, 櫻井幸一, “ブロックチェーンの暗号論的要素技術の分類”, SCIS2018.

[23] 才所敏明, 五太子政史, 辻井重男, ”「安心・安全電子メール利用基盤（SSMAX）」悪意のあるメールの根絶とメール内容の確実な保護を目指して ”, 情報処理学会論文誌 59 巻 9 月号, 2018.

[24] 才所敏明, 辻井重男, ”安心・安全な IoT システム(SSIoT)に関する考察”, 第 81 回コンピュータセキュリティ研究会（CSEC81), 2018.

[25] Daniel Genkin, Dimitrios Papadopoulos, Charalampos Papamanthou,” Privacy in Decentralized Cryptocurrencies”, Communications of the ACM, June 2018. https://cacm.acm.org/magazines/2018/6/228028-privacy-in-decentralized-cryptocurrencies/fulltext

[26] Mauro Conti,E. Sandeep Kumar,Chhagan Lal,Sushmita Ruj,” A Survey on Security and Privacy Issues of Bitcoin”, IEEE Communications Surveys & Tutorials Vol.20, Issue.4 , 2018. https://ieeexplore.ieee.org/document/8369416