暗号仮想通貨における匿名化技術の現状と展望

才所　敏 明[†1]　　辻井　重男[†2]　　櫻井　幸一[†3]

(株)IT 企画　　中央大学研究開発機構　　九州大学大学院システム情報科学研究院

（株）国際電気通信基盤技術研究所

1　仮想通貨の現状

ビットコインは Satoshi Nakamoto が 2008 年に投稿した論文で公開され、2009 年に運用が開始された仮想通貨である。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おり、仮想通貨全体の時価総額は約 215B ドルとなっている。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。

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。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。

仮想通貨は匿名性が強く、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。

一方、プライバシー保護の観点からは、仮想通貨の不十分な匿名性への懸念も強く、匿名性を更に強化した仮想通貨も多数発行されている。

主要な匿名仮想通貨 24 の 2015 年時点の時価総額は 3.35B ドルと推定され、仮想通貨時価総額全体の 2%程度となっている。図 1 に、匿名仮想通貨の時価総額ベスト 10 を示している。

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通しであるが、プライバシー保護を重視した匿名仮想通貨は今後も一定程度の伸長が期待されている。

順位	名称	記号	時価総額
9	Monero	XMR	$1,862,296,670
19	Zcash	ZEC	$636,914,783
97	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 1　匿名仮想通貨時価総額ベスト 10
（2018 年 11 月 6 日）

2　仮想通貨における匿名性のための要件

本稿では、仮想通貨の匿名性を、仮想通貨による支払いの記録（トランザクション）から利用者（支払者あるいは受取者）を特定する難しさ、と定義する。

トランザクションには、一般に、支払者が使用する原資の情報、原資の使用権を支払者が保有することを示す情報、受取者の情報および支払う金額が指定されている。

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 2　トランザクションの構成
（匿名性に関連する情報のみ）

2.1　利用者の仮名性

図 2 の(2)および(3)の情報には、利用者に関する情報が含まれているが、利用者が特定されないよう工夫が必要となる。なお、仮想通貨では一般には利用者固有の、しかし利用者とは直接は結びつかないように生成される公開鍵あるいは公開鍵から生成されるアドレスが使用されており、仮名性により利用者の一定の匿名性を確保する工夫が既になされている。

2.2　公開鍵/アドレスの非連結性

しかし、仮名とはいえ、同一の公開鍵/アドレスがブロックチェーン上の多くのトランザクションで使用されていると、連結されたトランザクションの特徴分析等から利用者の推定が可能になる場合もあり、公開鍵やアドレスを都度変更するワンタイム公開鍵、ワンタイムアドレス（ステルスアドレス）の使用が望ましい。

2.3　トランザクション間の利用者の追跡不能性

Current status and future prospect about anonymization technology in crypt virtual currency

[†1]Toshiaki Saisho　Advanced IT Corporation
[†2]Shigeo Tsujii
Research and Development Initiative, Chuo University
[†3]Kouichi Sakurai
Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University
Advanced Telecommunications Research Institute international (ATR)

支払者の原資の指定と、その原資の所有者、使用権を示す情報は、原資使用の妥当性を確認する検証者（マイナー等）には必要な情報ではあるが、利用者の受取/支払行動が追跡され、利用者の推定につながりかねない。原資として使用する受取とその原資による支払の対応を秘匿することが望ましい。

2.4　トランザクション内の利用者間の資金移動の追跡不能性

トランザクションには支払者と受取者の情報が格納されているが、支払者と受取者の対応関係もまた利用者の推定に利用されかねない。利用者の特定を難しくなるよう対応関係を秘匿することが望ましい。

2.5　支払額の秘匿

支払額も支払者、受取者の推定に繋がる恐れもあり、またプライバシー上の問題もあり、秘匿することが望ましい。

3.　仮想通貨の匿名性を強化する技術

本章では、2 章で示した匿名性に関する要件の実現のために提案・実装されている技術・仕組みについて述べる。

3.1　利用者の仮名性

利用者の仮名は、一般に生成した乱数に基づく公開鍵生成と各仮想通貨のルールに従った公開鍵のアドレスへの変換により生成される。このような仮名生成方式では利用者固有の情報を使用しないので、利用者の特定を困難にする工夫は必要無い。

3.2　公開鍵/アドレスの非連結性

ワンタイムの仮名として使用される公開鍵・アドレスの生成には、受取者生成方式と支払者生成方式が提案されている。

受取者生成方式としては、必要時に乱数による鍵を生成する方式と、マスターの秘密鍵・公開鍵ペアは乱数で生成し、必要時に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である Hierarchy Deterministic (HD) 鍵生成方式([1])が提案され、実際に利用されている。

支払者生成方式としては、DH 鍵共有の仕組みを利用したワンタイム公開鍵生成方式([2])が提案されている。鍵共有のための情報（トランザクション公開鍵）をトランザクションに加える必要があることが課題である。

なお、ワンタイム公開鍵/アドレスを使用していたとしても、支払者が複数の原資を使用した場合、それぞれの原資で使用されているワンタイム公開鍵/アドレスが全てその支払者に紐づけられることになり、注意が必要である。

3.3　トランザクション間の利用者の追跡不能性

支払者が使用する原資の特定を困難にするための技術として、ワンタイムリング署名([2])が提案されている。金額が同じの複数の原資を指定し、リング署名によりどの原資が実際に使用されるかの特定を困難にする方法である。トランザクションには、ダミーの原資指定、リング署名格納のための大きなスペースが必要となり、また署名検証のために処理時間が必要となる。

3.4　トランザクション内の利用者間の資金移動の追跡不能性

トランザクション内の支払者と受取者の対応を困難にする方法として、複数のトランザクションを一つにまとめるコインミキシング方式と仲介者の介在によるエスクロー方式が提案されている。コインミキシングとしてはチャウミアン・コインジョイン方式が、エスクロー方式としては、TumbleBit([3])が提案されている。

チャウミアン・コインジョイン方式の場合は、実装方法にもよるが、サービスを提供する事業者やシステムへの一定の信頼性が前提となっている。TumbleBit の場合は、1 件の支払が複数のトランザクションにより実現されるため、手数料負担増が問題となる。

3.5　支払額の秘匿

トランザクションの検証時には、入力金額の合計と出力金額の合計が一致するかどうかの確認が必要である。個々の金額を秘匿しつつも、入力金額の合計と出力金額の合計の一致を確認可能な方法として、コンフィデンシャルトランザクション([4])が提案され、利用されている。

4.　おわりに

本稿では、暗号仮想通貨の利用者の匿名性に関する、トランザクションに格納されている情報の要件を整理し、匿名性強化のために提案されている技術・仕組み整理した。

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]Pieter Wuille,”Hierarchical Deterministic Wallets”. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
[2]Nicolas van Saberhagen,"CryptoNote v2.0",2013. https://cryptonote.org/whitepaper.pdf
[3]Ethan Heilman, etc., "TumbleBit:An Untrusted Bitcoin-Compatible Anonymous Payment Hub",2016. https://eprint.iacr.org/2016/575.pdf
[4]Greg Maxwell,"Confidential Transactions",2016. https://people.xiph.org/~greg/confidential_values.txt