暗号資産の匿名性要件の整理と対応レベルの比較

才所 敏明[*1]　　辻井 重男[*2]　　櫻井 幸一[*3]

概要： 暗号資産は，大きくブロックチェーン技術ベースの暗号資産，DAG チェーン技術ベースの暗号資産に分類できる．本稿では，匿名性を強化した DAG 技術ベースの匿名暗号資産 Aidos Kuneen，Dero，Tangram について，匿名性の調査・分析結果を報告する．匿名性の評価にあたっては，5 項目の匿名性要件，①利用者識別情報の仮名性，②利用者識別情報間のワンタイム性，③トランザクション間の暗号資産/利用者識別情報の非連結性，④トランザクション内の暗号資産/利用者識別情報の非連結性，⑤移転資産額の秘匿，を使用し実施した．次に，報告者らがこれまで実施してきたブロックチェーン技術ベースおよび DAG チェーン技術ベースの主要な暗号資産 Bitcoin，Monero，Zcash，Grin，IOTA，Obyte，Nano，Hedera Hashgraph の匿名性の比較を示し，考察結果を報告する．

キーワード: 仮想通貨, 暗号通貨, 暗号資産, 匿名暗号資産, ブロックチェーン, DAG チェーン, Directed Acyclic Graph, Aidos Kuneen，Dero，Tangram，Bitcoin，Monero，Zcash，Crin，IOTA，Obyte，Nano，Hedera Hashgraph，CryptoNote，AKShufll，Schnorr NIZK proof，匿名性，特定・追跡性

Organizing CryptoAsset Anonymity Requirements and Comparing Compliance Levels

Toshiaki Saisho[*1]　　Shigeo Tsujii[*2]　　Kouichi Sakurai[*3]

Abstract: Generally, Crypto Assets can be classified into blockchain technology-based Crypto Assets and DAGchain technology-based Crypto Assets. In this paper, we report the results of anonymity survey and analysis on Aidos Kuneen, Dero, and Tangram, an anonymous Crypto Asset based on DAGchain technology with enhanced anonymity. Anonymity was evaluated using the following five anonymity requirements: (1) Pseudonymity of User Identification Information(UII), (2) OneTime-ness of UIIs, (3) Unlinkability of Assets/UIIs between Transactions, (4) Unlinkability of Assets/UIIs within Transaction, (5) Concealment of Asset Amount. Next, we present and discuss the results of anonymity comparison of the major blockchain technology-based and DAGchain technology-based crypto assets Bitcoin, Monero, Zcash, Grin, IOTA, Obyte, Nano, and Hedera Hashgraph that we have been conducted.

Keywords: Virtual currency, Crypto currency, Crypto Assets, Blockchain, DAGchain, Directed Acyclic Graph, Aidos Kuneen，Dero，Tangram，Bitcoin，Monero，Zcash，Crin，IOTA，Obyte，Nano，Hedera Hashgraph，CryptoNote，AKShufll，Schnorr NIZK proof，Anonymity，Identifiability，Traceability

1. 暗号資産の匿名性

Satoshi Nakamoto が 2008 年に投稿した論文で公開し，2009 年に運用が開始された最初の暗号資産である Bitcoin 以来，多くの暗号資産が登場し，消滅した暗号資産もあるが，“All Cryptocurrencies”（[8]）のデータによると 2020 年 7 月 12 日現在，2713 個の暗号資産が公開され，活発な取引が行われており，暗号資産全体の時価総額は約 29 兆円となっている．

一般に暗号資産の取引記録（トランザクション）にはある程度の匿名性があるが，プライバシー保護の観点からは不十分であり，匿名性を強化する技術を導入する暗号資産も多く，また匿名性を強化した新たな暗号資産も多く登場している．

著者らは，暗号資産における匿名性の現状を把握すべく，5 項目の暗号資産の匿名性要件（2 章）を定義し，ブロックチェーン技術ベースの暗号資産 Bitcoin，匿名性が強化されたブロックチェーン技術ベースの暗号資産 Monero，Zcash，Grin，および DAG チェーン技術ベースの暗号資産 IOTA，Obyte，Nano，Hedera Hashgraph について，5 項目の匿名性要件への対応状況を報告してきた（[1]～[4]）．

本稿では，匿名性が強化された DAG チェーン技術ベースの暗号資産 Aidos Kuneen，Dero，Tangram について，5 項目の匿名性要件への対応状況を報告（3 章），更にこれまでの調査結果も含め 5 項目の匿名性要件への対応状況の比較を示し，主要な暗号資産の匿名性の現状，匿名化技術と匿名性の関連等を考察し報告する（4 章）．

2. 暗号資産の匿名性要件

暗号資産の移転を示す情報としては，一般に図 1 に示す

*1　（株）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
【 論文原稿：上記*の文字書式「隠し文字」 】

情報がトランザクションに記録されている．

図１　暗号資産の移転を示すトランザクション情報（匿名性に関連する情報のみ）

このような資産の移転を示す情報の匿名性要件を，本稿では図２の５項目に整理している．

要件名称	要件内容
Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性）	利用者の実名等の推定が困難な利用者識別情報（公開鍵、アドレス等）であること
OneTime-ness of UIIs（利用者識別情報のワンタイム性）	毎回異なる利用者識別情報が使用され、複数の利用者識別情報が同一の利用者に紐づけられていることの推定が困難であること
Unlinkability of Assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）	トランザクション間の、提供者の受取を示す出力資産情報とその提供を示す入力資産情報の対応から、暗号資産および利用者識別情報の対応の推定が困難であること
Unlinkability of Assets/UIIs within Transaction（トランザクション内の暗号資産/利用者識別情報の非連結性）	トランザクション内の、提供者の入力資産情報と受取者の出力資産情報の対応から、提供者/受取者の暗号資産/利用者識別情報の対応の推定が困難であること
Concealment of Asset Amount（移転資産額の秘匿）	暗号資産の提供額・受取額の推定が困難であること

図２　暗号資産の匿名性要件

3. DAG チェーン技術ベースの主要な匿名暗号資産

DAG チェーン技術ベースの主要な暗号資産を図３に示している．この中の，IOTA，Hedera Hashgraph，Nano，Obyte の匿名性については，SCIS2020 の報告（[1]）を参照願いたい．

図３の赤字（斜字）で示した暗号資産 Aidos Kuneen，Dero が，匿名性を強化した DAG チェーン技術ベースの匿名暗号資産である．本稿では，この二つの暗号資産に加え，開発途上の暗号資産 Tangram の匿名性について考察する．

名称	記号	時価総額
IOTA	MIOTA	$694,058,681
Hedera Hashgraph	HBAR	$197,302,800
Nano	NANO	$135,017,645
Holo	HOT	$118,207,058
HyperCash	HC	$57,062,211
Fantom	FTM	$20,735,164
Aidos Kuneen	*ADK*	*$18,225,532*
Obyte	GBYTE	$15,394,458
Constellation	DAG	$12,903,131
IoT Chain	ITC	$9,896,749
Dero	*DERO*	*$9,691,234*

図３　主要な DAG チェーン技術ベース暗号資産一覧（2020 年 7 月 12 日現在の時価総額順）

3.1 Aidos Kuneen

Aidos Kuneen は，IOTA のコードの 70%を流用して開発された DAG コインだが，その後の開発過程でソースコードも一新された模様．しかし，IOTA の特徴である DAG（Directed Acyclic Graph）およびトランザクション/バンドル構造（ブロックレス）は継承している．

Aidos Kuneen では，暗号資産の移転を示すトランザクション情報に対する匿名性を強化するため，詳細内容は公開されていないが耐量子非対話型ゼロ知識証明プロトコル ZKBoo を利用した AKShuffle という仕組みが用意されている．

受け取った暗号資産を直接第三者への提供に使用した場合，その暗号資産の出所（提供者のアドレス）が容易に把握されてしまうことになるため，AKShuffle では，使用する前に受け取った暗号資産をシャッフルアドレスに送信すると，提供者の特定を困難化するシャッフル処理後，再び本人の別のアドレスへ暗号資産が戻される．シャッフル処理後に受け取った暗号資産は，提供者候補として同一金額の暗号資産を保有する複数のシャッフルアドレス（公開鍵）が指定され，そのうちの一つの公開鍵に対応する秘密鍵を提供者が所有していることを示すゼロ知識証明が付与されている．

AKShuffle はこのような TumbleBit のエスクローや CryptoNote のリング署名に類似した仕組みにより，使用する暗号資産の出所（提供者）の特定を困難にしている．

Aidos Kuneen のトランザクションの匿名性について，以下，２章で整理している匿名性に関する要件ごとにまとめている．

① Pseudonymity

Aidos Kuneen では IOTA と同様，利用者が選定したランダムなシード 81 トライトと未使用のインデックスから秘密鍵が生成される．秘密鍵はセキュリティレベル 1～3 に応じ 2187 トライトにセキュリティレベルを乗じた長さである．秘密鍵は 81 トライトのセグメントに分割され，それぞれのセグメントは 26 回ハッシュ関数を通し，それらの結果を繋いだ値をダイジェストと称し，更にそのダイジェストを 2 回，ハッシュ関数を通し 81 トライトのアドレスを得る．

以上のように，Aidos Kuneen のアドレスは乱数から生成され，その生成プロセスでは利用者固有の情報は使用されないため，利用者識別情報であるアドレスから利用者を推定するのは難しく，Pseudonymity of UII（利用者識別情報の仮名性）要件を満たしている．

② OneTime-ness of UIIs

Aidos Kuneen では，IOTA と同様，何度も同じアドレスを送金に使用することは秘密鍵漏洩に繋がりかねず，原則，毎回異なるアドレスを生成し受け取ることになる．①で示したアドレス生成手順において，毎回異なるインデックスを指定することにより，毎回異なるアドレスを生成し使用

する．結果として，利用者識別情報であるアドレスは毎回異なり，また生成される複数のアドレスが同一のランダムシードから生成されていること，つまり同一の利用者に紐づけられていること，を第三者が確認することは難しく，OneTime-ness of UIIs（利用者識別情報のワンタイム性）要件を満たしている．

③　Unlinkability of Assets/UIIs between Transactions

Aidos Kuneen では，暗号資産の第三者への移転においては IOTA と同様，本要件のための対策は行っていない．トランザクションで使用する資産の指定には未使用の資産が存在するアドレス（受取時のアドレス）を直接指定する．受取時の資産と提供に使用する資産との対応を容易に確認できるため，Unlinkability of assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）要件は満たしていない．

しかし，Aidos Kuneen では，AKShuffle という仕組みが用意されており，提供に使用する資産として，第三者から受け取った暗号資産ではなく，シャッフル処理後の，提供者の特定が困難な暗号資産を使用することができる．AKShuffle の利用により，受取時の資産と提供に使用する資産との対応の特定を困難にすることができるため，Unlinkability of assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）要件は一定レベル満たしているといえるが，そのレベルはシャッフルに使用されるダミーの未使用暗号資産の数に強く依存することになる．

④　Unlinkability of Assets/UIIs within Transaction

Aidos Kuneen では，本要件のための個別の対策は行っていない．しかし，②のワンタイムアドレスの使用による受取者を示す利用者識別情報からの受取者特定の困難化，および③の AKShuffle による提供者に対応する利用者識別情報の特定の困難化により，提供者と受取者の対応の特定を困難にすることができる．

しかし，③で述べたように Unlinkability of Assets/UIIs between Transactions 要件への対応レベルはシャッフルで使用するダミーの暗号資産の数に依存し，Unlinkability of Assets/UIIs within Transaction（トランザクション内の暗号資産/利用者識別情報の非連結性）要件への対応レベルもそれに準じたレベルとなる．

⑤　Concealment of Asset Amount

Aidos Kuneen では，IOTA と同様，暗号資産の使用額，受取額を秘匿する対策は行っていない．Concealment of Asset amount（資産額の秘匿）要件は満たしていない．

3.2　Dero

2017 年 12 月に開発に着手された DERO は，PoW（Proof-of-Work）と DAG（Directed Acyclic Graph）を組み合わせた最初の暗号資産であり，Google で設計されたオープンソースのプログラミング言語 Go でスクラッチから開発された暗号資産である．

Dero では，暗号資産の移転を示すトランザクション情報に対する利用者の匿名性を強化するため，CryptoNote で提案されている匿名化技術（ワンタイムアドレス，リング署名，鍵イメージ）ベースであるが，リング署名の代わりに，暗号資産の使用額・受取額の秘匿のためのペダーセンコミットメント，それに伴うリング署名の改良版 MLSAG（Multi-layered Linkable Spontaneous Anonymous Group signature）から構成されるリング CT（Confidential Transaction）を採用している．

入力資産情報		出力資産情報	
入力資産1	入力資産1の候補群の指定（複数）	出力資産1	受取者1の指定（受取者1のワンタイムステルスアドレス）
	ワンタイムリング署名1（候補群内に所有権を有する資産の存在の証明）		受取額1の指定（金額を乱数でマスクしたペダーセンコミットメント）
入力資産2	入力資産2の候補群の指定	出力資産2	受取者2の指定
	ワンタイムリング署名2		受取額2の指定
·····		·····	
入力資産n	入力資産nの候補群の指定	出力資産m	受取者mの指定
	ワンタイムリング署名n		受取額mの指定
トランザクションパブリックキー			
受取者のワンタイムステルスアドレス生成に使用した秘密鍵（乱数）に対応する公開鍵			

図４　Dero のトランザクションを構成する情報
（匿名性に関連する情報のみ）

Dero のトランザクションの匿名性について，以下，2 章で整理している匿名性に関する要件ごとにまとめている．

①　Pseudonymity

Dero では，利用者固有の 2 組の公開鍵暗号の鍵ペアが使用され，そのうちの 256 ビットの二つの公開鍵が利用者識別情報に該当する．二つの公開鍵は共に乱数から生成される秘密鍵経由生成され，その生成プロセスでは利用者固有の情報は使用されないため，二つの公開鍵（利用者識別情報）のいずれからも利用者を推定するのは難しく，Pseudonymity of UII（利用者識別情報の仮名性）要件を満たしている．

②　OneTime-ness of UIIs

Dero では，トランザクションでの受取者の指定には，上述の利用者固有の二つの公開鍵をそのまま使用するのではなく，二つの公開鍵とトランザクションごとに生成する乱数から新たな公開鍵を作成し使用する．このように受取用公開鍵は毎回異なるため，DAG チェーン上のトランザクション内に指定されている複数の利用者識別情報が同一の利用者に紐づけられていることを特定するのは困難で，OneTime-ness of UIIs（利用者識別情報のワンタイム性）要件を満たしている．

③　Unlinkability of Assets/UIIs between Transactions

Dero では，トランザクションで使用する暗号資産が特定されないよう，リング CT が採用されている．使用する暗

号資産候補として未使用の暗号資産を多数指定し，どの暗号資産が使用されるかはわからないようにしつつも，一つの暗号資産が使用されることを保証することができる．また，使用暗号資産の鍵イメージの登録・利用により使用資産の特定を防ぎつつ，資産の 2 重使用のチェックを可能としている．

リング CT により Unlinkability of Assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）要件に対応する仕組みは用意されているが，その要件への対応のレベルはダミーとして指定する未使用暗号資産の数に強く依存することになる．

④ Unlinkability of Assets/UIIs within Transaction

Dero では，本要件のための個別の対策は行っていない．しかし，②のワンタイム公開鍵の使用による受取者を示す利用者識別情報からの受取者特定の困難化，および③のリング CT による提供者に対応する利用者識別情報の特定の困難化により，提供者と受取者の対応の特定を困難にすることができる．

しかし，③で述べたように Unlinkability of Assets/UIIs between Transactions 要件への対応レベルはリング CT で使用するダミーの暗号資産の数に依存しているため，Unlinkability of Assets/UIIs within Transaction（トランザクション内の暗号資産/利用者識別情報の非連結性）要件への対応レベルもそれに準じたレベルとなる．

⑤ Concealment of Asset Amount

Dero では，リング CT により，個々の暗号資産の使用額，受取額を公開せずに，使用額の合計と受取額の合計が一致することを示すことができる．使用額・受取額の秘匿が可能となり，Concealment of Asset Amount（移転資産額の秘匿）要件を満たしている．

3.3 Tangram

2018 年 2 月に Sneak という名称で開発に着手されたプライバシー重視の DAG 技術ベースの暗号資産である．2018 年 6 月に Tangram へ変更された．

Tangram では，トランザクションは送金者のワレット（財布）内で作成され，暗号化されたトランザクションは検証を担当するノードでゼロ知識証明を利用し使用するコインの存在，所有権等を確認後，コインの生成に使用される．生成されたコインはノードで承認後，台帳（Ledger）に登録される．

フィールド名称	格納されている情報
masterKey	コインの現所有者（提供者）のマスター鍵
toAddress	コインの受取者の一時公開鍵から生成されたアドレス
amount	提供者から受取者に転送する金額
encryptedMemo	提供者が利用可能なオプションデータフィールド

図５　Tangram のトランザクションを構成する情報

属性名称	属性が示す情報
Hash	コインのハッシュ値
Hint	コインの世代 ＜Version、Amount、Principleで定義＞
Keeper	コインの鍵 （マスター鍵と関連付け 所有権を取得するための鍵） ＜Version、Stamp等で定義＞
Principle	コインの所有者および コインが本物であることの証明 ＜Version、Stamp等で定義＞
Stamp	コインの識別子（シリアルナンバー） ＜Amountおよび秘密の乱数鍵で定義＞
Version	コインのバージョン番号

図６　Tangram のコインを構成する情報

以上のように，Tangram の台帳にはトランザクションは登録されず，生成されるコインが登録されるため，要件の評価はコインを対象とし実施した．以下，2 章で整理している匿名性に関する要件ごとにまとめている．

① Pseudonymity

Tangram では，そもそも資産（コイン）の受取者の情報を含むトランザクションは台帳に登録されず，所有権が移行されたコインのみが登録される．コインには，所有者を識別する情報（利用者識別情報）は明示的には含まれていない．なお，コインには所有権を示すマスター鍵から生成された情報が含まれるが，その情報はマスター鍵の他，コイン生成プロセスの様々の情報のハッシュ値から生成されるため，コインの情報からマスター鍵保有者（利用者）を推定することは困難で，Pseudonymity of UII（利用者識別情報の仮名性）要件を満たしている．

② OneTime-ness of UIIs

Tangram では，①で述べたように，そもそも資産（コイン）の所有者を明示的に示す利用者識別情報は登録されない．また，コインには所有権を示すマスター鍵（利用者識別情報）から生成された情報が含まれるが，その情報はマスター鍵の他，コイン生成ごとに異なる生成プロセスの様々の情報のハッシュ値から生成され各コインで異なるため，コインの情報から同一の利用者に紐づけられていることを特定するのは困難で，OneTime-ness of UIIs（利用者識

別情報のワンタイム性）要件を満たしている．

③　Unlinkability of Assets/UIIs between Transactions

Tangram の台帳に登録されるコインには，そのコインの所有者の情報は明示的には含まれず，コイン固有の属性が格納されている．所有者のみが所有権を示す情報を提示でき，検証ノードはゼロ知識証明により，所有者の所有権を確認できる．台帳には，コインを利用した資産の移転を示すトランザクションは登録されず，移転結果を示すコインのみが登録されているので，Unlinkability of Assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）要件を満たしていると考えられる．

④　Unlinkability of Assets/UIIs within Transaction

Tangram では，③で述べたように，コインには，そのコインの所有者の情報は明示的には含まれず，また台帳にはコインを利用した資産の移転を示すトランザクションは登録されず，移転結果を示すコインのみが登録されているので，Unlinkability of Assets/UIIs within Transaction（トランザクション内の暗号資産/利用者識別情報の非連結性）要件を満たしていると考えられる．

⑤　Concealment of Asset Amount

Tangram の台帳に登録されるコインには，金額の情報はペダーセンコミットメント等を利用し表現され，所有者のみが金額を確認できる．Concealment of Asset Amount（移転資産額の秘匿）要件を満たしている．

4.　主要な暗号資産の匿名性に関する考察

暗号資産の匿名性に関する調査・分析の一連の報告（[1]～[4]）および今回の結果から，報告者らが定義している匿名性要件への対応レベルで調査対象暗号資産の匿名性を比較したのが図 7 である．また，結果についての考察は①～④にまとめている．

なお，複数の暗号資産移転の仕組みが存在する暗号資産については，オンチェーンで提供されている匿名性の高い仕組みの中で，標準的と想定される使い方を評価の対象としている．

匿名性要件名称	ブロックチェーン				DAGチェーン						
	Bitcoin	匿名性強化			IOTA	Obyte	Nano	Hedera Hashgraph	匿名性強化		
		Monero (TypeSimple)	Zcash (Sapling)	Grin					Aidos Kuneen	Dero	Tangram
Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性）	○	○	○	○	○	○	○	○	○	○	○
OneTime-ness of UIIs（利用者識別情報のワンタイム性）	○	○	○	○	○	○	×	×	○	○	○
Unlinkability of Assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）	×	△	○	×	×	×	×	×	△	△	○
Unlinkability of Assets/UIIs within Transaction（トランザクション内の暗号資産/利用者識別情報の非連結性）	×	△	○	△	×	△	×	×	△	△	○
Concealment of Asset Amount（移転資産額の秘匿）	×	○	○	○	×	×	×	×	×	○	○

図 7　主要な暗号資産の匿名性要件対応レベルの比較

①　Nano，Hedera Hashgraph は Bitcoin より低い匿名性

優れたスケーラビリティに特徴がある DAG チェーン技術ベースの暗号資産の中で，タングル型の IOTA，Obyte は Bitcoin と同程度の匿名性を有するが，ラティス型の Nano，Hedera Hashgraph は Bitcoin に比べても匿名性が低いことを確認した．

DAG チェーン技術ベース暗号資産のタングル型とラティス型との匿名性のレベルの違いは，タングル型が Bitcoin と同様，暗号資産のデータはトランザクション内にのみ格納されているのに対し，ラティス型の場合，アカウント ID（利用者識別情報）の再利用を前提とし，アカウント ID 間の資産の移転の結果は，アカウント ID ごとの資産残高として別途の台帳で管理されていることにある．

このようなアカウント ID の再利用を前提とした資産残高管理方式は，資産の 2 重使用のチェックやトランザクションの長期保存を不要とする資産の効率的な移転の管理を可能とするが，今回調査した Nano，Hedera Hashgraph はともにアカウント ID や資産残高の匿名性強化の仕組みが導入されていないために，匿名性は低くなっている．

なお，Tangram でも資産残高管理方式を採用しているが，ワレット単位の資産残高管理，ワレット内で必要に応じ新たなコインが定義可能，台帳に登録されるコインには所有者の情報は明示的には含まれていないこと等により，コインの所有者間の連結特定を困難とし，匿名性を強化している．

②　匿名暗号資産が採用する匿名性強化技術は多様

調査対象の匿名暗号資産で利用されている主要な匿名化技術は以下の通りである．

Monero：CryptoNote（リング署名，ワンタイムアドレス，鍵イメージ）ベースであるが，リング署名の代わりに，ペダーセンコミットメントおよび MLSAG 署名を使用したリング CT を利用

Zcash：ゼロ知識証明 zk-SNARKs

Grin：Mimblewimble（ペダーセンコミットメントを利用した CT およびコインをミキシングする CoinJoin）に加え，ブロック内の中間的な資産の移転記録を破棄するカットスルーを採用

Aidos Kuneen：AKShuffle（セロ知識証明 ZKBoo およびエスクロー，リング署名に類似した仕組み）

Dero：Monero とほぼ同じで，CryptoNote ベースであるが，リング署名の代わりに，ペダーセンコミットメントおよび MLSAG 署名を使用したリング CT を採用

Tangram：ゼロ知識証明 Schnorr NIZK

③　ゼロ知識証明が高い匿名性を実現

ゼロ知識証明を採用している暗号資産 Zcash, Tangram が高い匿名性を実現している．なお，Aidos Kuneen もゼロ知識証明を利用しているが，提供者が指定暗号資産候補群のいずれかの秘密鍵の保有の証明にのみ利用されているため，匿名効果は限定的である．

ダミーの暗号資産を利用するリング CT を採用している暗号資産 Monero，Dero では，ダミーの暗号資産の数に応じ実際に使用される暗号資産の特定は困難となる．ダミーの暗号資産の数に応じた匿名化の効果となり，実現できる匿名性はゼロ知識証明に比べ低い．

コインミキシングにより入力資産/提供者と出力資産/受取者の対応の特定を困難にする CoinJoin を採用している暗号資産 Grin でも，ミキシングするコイン（トランザクション）の数に応じ入力資産/提供者と出力資産/受取者の対応の特定が困難となるが，ミキシングするコインの数に応じた匿名化の効果となり，実現できる匿名性はゼロ知識証明に比べ低い．

5. おわりに

筆者らは暗号資産の匿名性に着目し，暗号資産の匿名性要件を定義，その匿名性要件への対応状況から主要な暗号資産の匿名性の現状および匿名性強化に採用されている技術を調査している．本稿では，今回の調査対象である DAG チェーン技術ベースの匿名暗号資産 Aidos Kuneen，Dero，Tangram の調査結果とともに，これまでの調査結果（[1]～[4]）も含め，調査対象暗号資産の匿名性要件への対応状況整理し，その結果に対する考察結果を報告した．

暗号資産に関する技術はまだまだ発展途上であり，匿名性強化のための新たな仕組みもまた出現するものと考えられ，今後も注目したい．

一方では，暗号資産/利用者の特定・追跡性も重要である．非合法な取引の決済，マネーロンダリング，脱税等，暗号資産の不正目的の利用の多発や，暗号資産による資産移転（取引）の第三者機関による監査困難性等が，暗号資産の社会での活用の障害となっている．KYC/KYT 等の社会の要請に応えるべく，暗号資産/利用者の特定・追跡のための仕組みも検討されつつあるが，緒に就いたばかりという状況である．今後，暗号資産の特定・追跡性の検討にあたっては，監査組織や徴税機関への利用者の協力の元あるいは利用者主導での台帳情報の開示による暗号資産の特定・追跡，あるいは利用者の協力が得られない徴税機関や捜査機関による強制的な暗号資産/利用者の特定・追跡に分け，検討する必要があろう．

インターネット社会で安心して使用できる安全な暗号資産の実現には，そのための暗号資産に求められる要件，その要件実現のための仕組み等，今後の更なる研究開発が必要となろう．

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] 才所敏明，辻井重男，櫻井幸一，“暗号資産台帳の匿名性と特定・追跡性についての考察”，電子情報通信学会ソサイエティ大会，2020.

[2] 才所敏明，辻井重男，櫻井幸一，” DAG 技術ベースの暗号資産の匿名性に関する考察 ”，暗号と情報セキュリティシンポジューム（SCIS2020），2020.

[3] 才所敏明，辻井重男，櫻井幸一，”匿名暗号資産（Monero/Zcash/Grin）ブロックチェーンの匿名性に関する考察 ”，コンピュータセキュリティシンポジューム（CSS2019），2019.

[4] 才所敏明，辻井重男，櫻井幸一，” 暗号仮想通貨における匿名化技術の現状と展望 ”，情報処理学会第 81 回全国大会，2019.

[5] 才所敏明，辻井重男，櫻井幸一，” 仮想通貨の匿名性の現状と課題”，暗号と情報セキュリティシンポジューム（SCIS2019），2019.

[6] 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.

[7] 宇根正志，“暗号資産における取引の追跡困難性と匿名性：研究動向と課題”，金融研究/2019.7.
http://www.imes.boj.or.jp/research/papers/japanese/kk38-3-4.pdf

[8] ブロックチェーンを用いた金融取引のプライバシー保護と追跡可能性に関する調査研究，金融庁，(株)三菱総合研究所，2019.
https://www.fsa.go.jp/policy/bgin/ResearchPaper_MRI_ja.pdf

[9] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.
https://bitcoin.org/bitcoin.pdf

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

[11] Monero : Privacy in the blockchain v1.0
https://eprint.iacr.org/2018/535.pdf
[12] Zero to Monero: First Edition
https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
[13] Mastering Monero
https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf
[14] Zcash Protocol Specification
https://www.btrade.co.kr/btrade_res/20180507145055652.pdf
[15] Nicolas van Saberhagen, "CryptoNote v2.0", 2013.
https://cryptonote.org/whitepaper.pdf
[16] Adam Back, "bitcoins with homomorphic value (validatable but encrypted)", 2013.
https://bitcointalk.org/index.php?topic=305791.0
[17] Greg Maxwell, "Confidential Transactions", 2016.
https://people.xiph.org/~greg/confidential_values.txt
[18] Gregory Maxwell, Andrew Poelstra," Borromean Ring Signature", 2015.
https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf
[19] SHEN NOETHER, "RING CONFIDENTIAL TRANSACTIONS", 2015.
https://eprint.iacr.org/2015/1098.pdf
[20] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer, "From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again", 2011.
https://eprint.iacr.org/2011/443
[21] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova, "Pinocchio: Nearly Practical Verifiable Computation", 2013.
https://eprint.iacr.org/2013/279
[22] Andrew Poelstra, "Mimblewimble", 2016.
https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf
[23] Gregory Maxwell, "CoinJoin: Bitcoin privacy for the real world", 2013.
https://bitcointalk.org/index.php?topic=279249.0
[24] Daniel Wilczynski, "Greg Maxwells Roadmap for Bitcoin Scaling", 2015.
http://www.danielwilczynski.com/maxwells-scaling-roadmap
[25] Serguei Popov, "The Tangle", April 30, 2018. Version 1.4.3.
https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
[26] Anton Churyumov, "Byteball: A Decentralized System for Storage and Transfer of Value", 2016.
https://obyte.org/Byteball.pdf
[27] Colin LeMahieu, "Nano: A Feeless Distributed Cryptocurrency Network", 2018.
https://nano.org/en/whitepaper
[28] Leemon Baird, Mance Harmon, Paul Madsen, "Hedera: A Public Hashgraph Network & Governing Council", 2019.
https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf
[29] Aidos Kuneen - A Blockless and Anonymous Cryptocurrency for the Post-Quantum Era -, Aidos Developer & Aidos Foundation, 2018.
http://www.aidoskuneen.com/files/adk_whitepaper.pdf
[30] DERO PROJECT WHITE PAPER, 2018.
https://dero.io/attachment/Whitepaper.pdf
[31] Tangram: An Introduction, 2018.
https://tangrams.io/wp-content/uploads/2018/12/Tangram_An_Introduction-2018-12-19-03-27.pdf
[32] 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
[33] Christina Garman, Matthew Green, Ian Miers," Accountable Privacy for Decentralized Anonymous Payments", 2016.
https://eprint.iacr.org/2016/061.pdf