SCIS 2020 2020 Symposium on
Cryptography and Information Security
Kochi, Japan, Jan. 28 – 31, 2020
The Institute of Electronics,
Information and Communication Engineers

# DAG 技術ベースの暗号資産の匿名性に関する考察
# Notes on anonymity of DAG-based CryptoAssets

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

**あらまし** Bitcoin 以来，ブロックチェーン技術に基づく多くの暗号資産が出現し活発に取引されているが，ブロックチェーン技術の大きな課題の一つにスケーラビリティ問題がある．この課題の克服が期待される技術の一つに DAG（Directed Acyclic Graph）技術があり，DAG 技術ベースの暗号資産も既に数多く提案され取引されつつある．我々は，このような DAG 技術ベースの暗号資産である IOTA，Obyte，Nano，Hedera Hashgraph の匿名性について調査を実施した．調査には，ブロックチェーン系暗号資産に対し提案した 5 項目の匿名性要件を適用した．その結果，タングル型の DAG 系暗号資産（IOTA，Obyte）は Bitcoin と同程度の匿名性であること，ラティス型の DAG 系暗号資産（Nano，Hedera Hashgraph）は Bitcoin よりも匿名性が低いことを確認した．暗号資産の高い匿名性への期待は大きく，スケーラビリティとは分権化/分散化とともにトリレンマの関係にある匿名性を強化した DAG 系暗号資産も，今後増加するものと考えられる．

**キーワード** 仮想通貨，暗号資産，ブロックチェーン，DAG，Directed Acyclic Graph，タングル，ラティス，ブロックラティス，IOTA，Obyte，Nano，Hedera Hashgraph，匿名性，匿名性要件，スケーラビリティ，トリレンマ

Abstract Since Bitcoin, many crypto assets based on blockchain technology have emerged and are actively traded, but the biggest challenge of blockchain technology is lack of scalability. Many crypto assets based on DAG (Directed Acyclic Graph) technology that can overcome this problem are being proposed and traded. In this paper, we report the survey results on the anonymity of each of the major DAG technology-based cryptographic assets IOTA, Obyte, Nano, and Hedera Hashgraph. For the anonymity survey, we applied the five anonymity requirements proposed for blockchain crypto assets. As a result of the survey, tangle-type DAG crypto assets (IOTA, Obyte) are as anonymous as Bitcoin, and lattice-type DAG crypto assets (Nano, Hedera Hashgraph) are less anonymous than Bitcoin. I understood. Security including anonymity has a trilemma with scalability and decentralization / decentralization, but some DAG crypto assets with enhanced anonymity have already been proposed. The trend of strengthening anonymity while maintaining the scalability that is characteristic of DAG crypto assets is expected to become more serious in the future.

**Keywords** CryptoAssets, Anonymity, DAG, Directed Acyclic Graph , Tangle, Lattice, Block Lattice, IOTA, Obyte, Byteball, Nano, RaiBlocks, Hedera Hashgraph, Anonymity Requirements, Scalability, Trirennma

## 1 はじめに

Bitcoin 以来，ブロックチェーン技術に基づく多くの暗号資産（以下，ブロックチェーン系暗号資産と略記）が出現し活発に取引されているが，ブロックチェーン系暗号資産の大きな課題の一つにスケーラビリティ問題がある．この課題の克服を可能とする DAG（Directed Acyclic Graph）技術ベースの暗号資産（以下，DAG 系暗号資産と略記）も続々と登場している．

DAG 系暗号資産の特徴であるスケーラビリティの良

[*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

さは, PoW に代わるコンセンサスアルゴリズムやシャーディングの仕組みなどの活用等に起因するものと考えられているが，スケーラビリティ向上と匿名性を含むセキュリティ強化は，分権化/分散化も含めトリレンマと呼ばれており，この三つの目標を同時に達成するのは難しい課題でもある．

そこで，我々はスケーラビリティの良さに特徴がある現在の主要な DAG 系暗号資産が，Bitcoin と比べどの程度の匿名性を維持しているのかについて調査した．調査対象とした DAG 系暗号資産については，次章にて具体的に述べるが，タングル型およびラティス型の代表的な DAG 系暗号資産を対象とした．また，匿名性の評価には，ブロックチェーン系暗号資産の匿名性評価に使用した暗号資産の匿名性要件（[1]，[2]，[3]）を使用した．

DAG 系暗号資産は今後急増するであろう IoT 分野での活用も期待されている．図 1 に IoT 向け暗号資産として期待されている主要な暗号資産の一覧を示している．また，DAG 系暗号資産も量子コンピュータへの対応が進められている．図 2 に耐量子性あるいは耐量子性を計画している主要な暗号資産一覧を示している．図 1，図 2 の赤字枠で示しているのが，DAG 系暗号資産である．

本稿では，このような DAG 系暗号資産の匿名性に的を絞り調査した結果を報告する．

| 順位 | 名称 | 記号 | 時価総額 |
|---|---|---|---|
| 20 | IOTA | MIOTA | ¥59,007,350,027 |
| 100 | Golem | GNT | ¥3,460,854,210 |
| 121 | Waltonchain | WTC | ¥2,433,151,549 |
| 143 | IoTeX | IOTX | ¥2,076,967,194 |
| 170 | Robotina | ROX | ¥1,571,508,337 |
| 177 | Cortex | CTXC | ¥1,488,534,667 |
| 190 | Cindicator | CND | ¥1,265,786,490 |
| 306 | IoT Chain | ITC | ¥871,932,031 |
| 337 | Davinci Coin | DAC | ¥709,779,142 |
| 356 | Nucleus Vision | NCASH | ¥628,249,406 |

**図 1　IoT 分野での活用が期待される主要な暗号資産**
**(2019 年 11 月 25 日時点の[12]および[13]を参考に作成)**

| 順位 | 名称 | 記号 | 時価総額 |
|---|---|---|---|
| 13 | Cardano | ADA | ¥95,938,478,257 |
| 17 | NEO | NEO | ¥67,039,403,526 |
| 20 | IOTA | MIOTA | ¥59,007,350,027 |
| 80 | HyperCash | HC | ¥5,123,412,789 |
| 348 | Quantum Resis... | QRL | ¥653,283,462 |
| 1203 | SHIELD | XSH | ¥27,912,850 |
| 2033 | Aidos Kuneen | ADK | ¥? |

**図 2　耐量子性が期待（予定）される主要な暗号資産**
**(2019 年 11 月 25 日時点の[12]および[14]を参考に作成)**

## 2　DAG 系暗号資産の特徴

ブロックチェーン系暗号資産は資産の取引をブロックの 1 次元の連鎖で記録しているが，DAG 系暗号資産は有向非巡回グラフ（DAG：Directed Acyclic Graph）による 2 次元の連鎖で資産の取引を記録している．

現在の DAG 系暗号資産は，大きくタングル型とラティス型に分類される．

タングル型では，承認を期待する新たな資産取引を示すトランザクションを登録する際に既存の複数のトランザクションを承認することにより，その新たなトランザクションが DAG へ追加され承認の対象となる仕組みである．このように，承認作業をブロックチェーン系暗号資産の場合のようにマイナーという第三者に依頼するのではなく，トランザクション登録者あるいは少数の管理者が担当するため手数料は不要または少額となる．またブロックという概念がなくトランザクション単位の承認のため, ブロック構成･承認のための遅延も発生しない．

一方，利用者の資産はブロックチェーン系暗号資産と同様，DAG 内のトランザクションに点在し，使用する場合はその資産の位置と所有権を示す情報を指定する．承認時には，指定された資産の所有権を確認の上，更に 2 重使用ではないことの確認も必要となる．

ラティス型では，ブロックチェーンが複数共存し，資産の取引記録がそれぞれのブロックチェーンあるいは対象となるブロックチェーンに登録される．登録される取引記録（トランザクション）あるいはその集合体であるブロックが格子の形状となることからラティス型と呼ばれている．ラティス型では，タングル型と異なり，利用者の暗号資産はアカウント(アドレス)ごとに合算され，管理される，合算された暗号資産を提供に使用する場合は，利用者が指定したアカウントの資産残高が提供資産額以上であることを確認すればよく，2 重使用の確認は原則必要ない．

さて，図 3 に主要な DAG 系暗号資産を，時価総額順に示している．

| 順位 | 名称 | 記号 | 時価総額 |
|---|---|---|---|
| 20 | IOTA | MIOTA | ¥59,007,350,027 |
| 40 | Holo | HOT | ¥13,149,824,493 |
| 47 | Nano | NANO | ¥10,649,007,809 |
| 80 | HyperCash | HC | ¥5,123,412,789 |
| 155 | Fantom | FTM | ¥1,841,928,035 |
| 161 | Hedera Hashgraph | HBAR | ¥1,692,095,702 |
| 188 | Constellation | DAG | ¥1,282,062,213 |
| 260 | Obyte | GBYTE | ¥1,332,713,823 |
| 306 | IoT Chain | ITC | ¥871,932,031 |
| 322 | HYCON | HYC | ¥780,201,587 |

**図 3　主要な DAG 系暗号資産**
**(2019 年 11 月 25 日時点の[12]より作成)**

今回の調査では，この DAG 系案資産の中で，タングル型の暗号資産として最大の時価総額を誇る IOTA および Obyte（旧 Byteball）の 2 つを，また，ラティス型の暗号資産として最大の時価総額を誇る Nano および Hedera Hashgraph（以下，Hedera と略記）の 2 つを調査の対象とした．

## 3　DAG 系暗号資産のトランザクションの匿名性要件

ブロックチェーン系暗号資産の個々の資産移転を示すトランザクションには，一般に図 4 に示す情報が登録されている．ブロックチェーン系暗号資産の匿名性に関する考察（[1]～[3]）ではこのような情報を前提に，暗号資産の匿名性要件を 5 項目提案(以下の①～⑤) した．今回の調査においても，このブロックチェーン系暗号資産の匿名性要件を DAG 系暗号資産の匿名性評価に適用した．

| 入力欄 | | 出力欄 | |
|---|---|---|---|
| 入力項目1 | 使用する資金の位置（提供者のアドレスや金額等の情報が格納されている） | 出力項目1 | 提供先(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） | | 提供額の指定(金額情報) |
| 入力項目2 | 使用する資金の位置 | 出力項目2 | 提供先(受取者)の指定 |
| | 指定資金の使用権の証明 | | 提供額の指定 |
| ····· | | ····· | |
| 入力項目n | 使用する資金の位置 | 出力項目m | 提供先(受取者)の指定 |
| | 指定資金の使用権の証明 | | 提供額の指定 |

**図 4　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)**

**①Pseudonymity**

トランザクションには一般に暗号資産を提供する利用者（提供者）の識別情報，それを受け取る利用者（受取者）の識別情報が含まれている．

このような利用者識別情報 (UII:User Identification Information)から実在する利用者の実名等の推定が困難であるという要件を，Pseudonymity of UII（利用者識別情報の仮名性)，と定義する．

**②OneTime-ness**

同一利用者による暗号資産の利用の都度，トランザクションに格納される利用者識別情報が同一であれば，利用者識別情報の Pseudonymity 要件が満たされていたとしても，同一利用者の複数の暗号資産の利用状況が把握され，その分析から実在する利用者の推定に繋がる恐れがある．

利用者が使用する利用者識別情報が相互の関連が推測されないよう毎回変更され，同一利用者の複数の暗号資産の利用状況からも，利用者識別情報に紐づけられている実在する利用者の推定が困難であるという要件を，OneTime-ness of UII (利用者識別情報のワンタイム性)，と定義する．

**③Unlinkability between Transactions**

トランザクションに存在する利用者識別情報に紐づけられた暗号資産は，保有者が新たなトランザクションにてその暗号資産の位置や所有権を示す情報等を提示し，新たな受取者への提供に使用される．保有する暗号資産と提供に使用する暗号資産の対応関係が判ると，同一利用者による暗号資産の受取・提供の流れが把握でき，また複数の受取資産を原資として使用した場合は利用者識別情報の OneTime-ness が満たされていたとしても,使用された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可能性も高く，その分析から実在する利用者の推定に繋がる恐れがある．

受取時の暗号資産/受取者と提供に使用する暗号資産/提供者との対応の推定が困難であるという要件を，Unlinkability of UIIs/assets between Transactions（トランザクション間の利用者/暗号資産の非連結性)，と定義する．

**④Unlinkability within Transaction**

トランザクションには一般に提供者と受取者の情報が格納されているが，暗号資産の提供者と受取者の対応関係が判るとそれぞれの利用者の推定に繋がる恐れがある．

トランザクション内の提供者と受取者の対応の推定が困難であるという要件を，Unlinkability of UIIs/assets within Transaction（トランザクション内の利用者/暗号資産の非連結性)，と定義する．

**⑤Concealment of Asset amount**

暗号資産の提供額・受取額も，提供者，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でもある．

暗号資産の提供額・受取額の推定が困難であるという要件を，Concealment of Asset amount（資産額の秘匿)，と定義する．

## 4　IOTA の匿名性

IOTA では，暗号資産の移転の記録はタングルと呼ばれる DAG で表現され格納されている．資産の移転は複数のトランザクションから構成されるバンドルで表現されている．資産移転を示すトランザクション/バンドルは図 5 のようにタングルに格納されている．

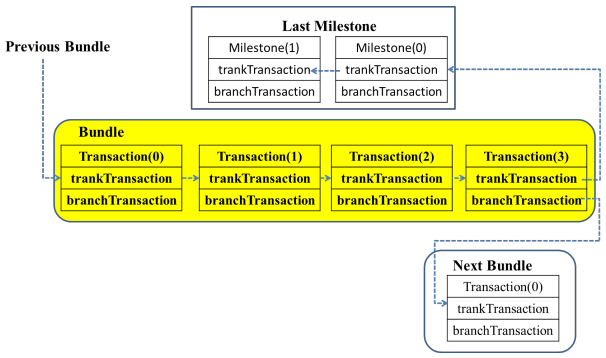


**図 5　IOTA タングル内の**
**トランザクション/バンドルの繋がり**

資産移転を示すバンドルを構成するトランザクショ

ンに格納されている情報を図 6 に示している.

| | Transaction (0) | Transaction (1) | Transaction (2) | Transaction (3) |
|---|---|---|---|---|
| sigMF | | UTXO使用権を示す署名(前半) | UTXO使用権を示す署名(後半) | |
| address | 受取人アドレス | 使用するUTXOアドレス | 使用するUTXOアドレス((1)と同じ) | 差額の送金先アドレス |
| value | 送金額 | 減額する額 | 0 | 差額 |
| currentindex | 0 | 1 | 2 | 3 |
| lastindex | 3 | 3 | 3 | 3 |

**図 6　IOTA 資産移転バンドルを構成するトランザクションに格納されている情報**

IOTA 資産移転トランザクション/バンドルの匿名性について，以下，3 章でまとめた匿名性に関する要件ごとにまとめている.

**①Pseudonymity**

IOTA では，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，IOTA 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.

**②OneTime-ness**

IOTA では，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 UII（利用者識別情報のワンタイム性）要件を満たしている.

**③Unlinkability between Transactions**

IOTA では，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 UIIs/assets between Transactions(トランザクション間の利用者/暗号資産の非連結性）要件は満たしていない.

**④Unlinkability within Transaction**

IOTA では，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は，提供者と受取者のアドレスが直接指定されており，その対応は容易に把握でき，Unlinkability of UIIs/assets within Transaction（トランザクション内の利用者/暗号資産の非連結性)要件は満たしていない.

**⑤Concealment of Amount**

IOTA では，暗号資産の提供額，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.

## 5　Obyte の匿名性

Obyte は，タングル型の DAG 系暗号資産である. Obyte を構成するストレージユニットは過去のストレージユニットのハッシュ値を 1 つ以上含むことにより相互に連結され，Obyte データベースではストレージユニットが DAG 形式で表現され格納されている. 暗号資産の移転の記録を示すトランザクションもストレージユニットの形式で格納されている（図 7）.

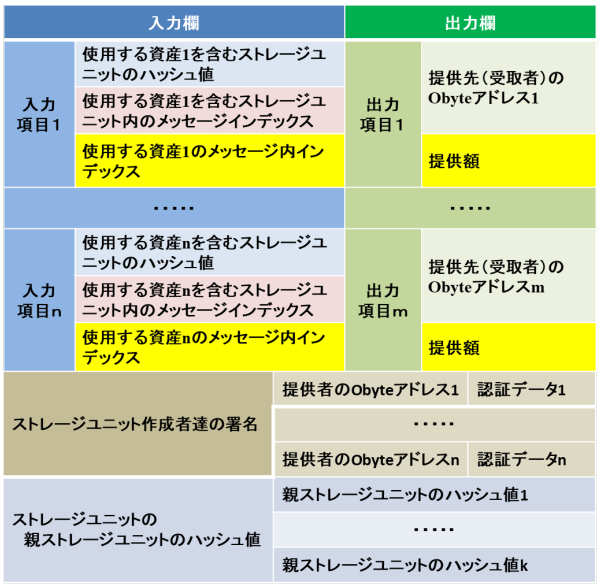


**図 7　資産移転を示すトランザクションのストレージユニット構成**

Obyte では，さまざまのオプション機能を利用者が選定し利用できるが，本稿では高い匿名性を前提とした利用形態に限って，匿名性を評価する. 例えば，図 6 の出力欄の受取者のアドレスとして，利用者が指定したニックネームやメールアドレスの指定も可能であるが，乱数から生成される Obyte アドレスの利用を前提とし評価する.

また，Obyte では，Byte と BlackByte の 2 つの資産（通

貨）が定義されているが，BlackByte の取引は公開される 0byte データベースには登録されずワレット間で直接取引される．本稿では公開される取引記録の匿名性の評価が目的であるため，0byte データベースに登録される Byte の取引のみを対象とし評価する．

0byte 資産移転トランザクション/ストレージユニットの匿名性について，以下，3 章でまとめた匿名性に関する要件ごとにまとめている．

**①Pseudonymity**

0byte では，必要の都度，乱数により新たな鍵ペアが生成され，公開鍵より 0byte アドレス（利用者識別情報）が生成される．このように，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，アドレス（利用者識別情報）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．

**②OneTime-ness**

0byte では，同じアドレスを繰り返し使用することは推奨されておらず，原則，①で示したように毎回乱数からアドレスを生成し使用することになる．利用者識別情報であるアドレスは毎回異なり，生成される複数のアドレスが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 UII（利用者識別情報のワンタイム性）要件を満たしている．

**③Unlinkability between Transactions**

Gbyte では，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はその未使用資産が存在する位置（トランザクションのハッシュ値およびその中の位置）を指定する．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 UIIs/assets between Transactions（トランザクション間の利用者/暗号資産の非連結性）要件は満たしていない．

**④Unlinkability within Transaction**

0byte では，複数の提供者，複数の受取者から構成されるトランザクションの生成も可能で，その機能を利用することにより提供者が提供に使用する資産と受取者が受け取る資産の対応を困難にすることができる．しかし，参加する提供者，受取者の数には限度があり，提供者と受取者の対応の推定には高い困難さを期待できない．一般に，一定の Unlinkability of UIIs/assets within Transaction（トランザクション内の利用者/暗号資産の非連結性）要件を満たしてはいるが，限定的である．

**⑤Concealment of Amount**

0byte では，暗号資産の提供額，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．

## 6　NANO の匿名性

Nano はラティス型の DAG 系暗号資産である．利用者は資産の管理単位であるアカウントを複数保有できる．アカウントには，公開鍵と秘密鍵の 1 組が対応し，公開鍵から生成されるアカウントアドレスにより，そのアカウントへの資産の移転が指定され，秘密鍵によりそのアカウント資産の使用（提供）が可能である．

アカウント間の資産移転は，2 つのトランザクション，資産提供（送信）のためのトランザクション（図 8）と資産受取（受信）のためのトランザクション（図 9），で実施される．提供（送信）トランザクションは提供アカウントのアカウントチェーンに登録され，受取（受信）トランザクションは受取アカウントのアカウントチェーンに登録される（図 10）．

| 提供（送信）トランザクション | |
|---|---|
| トランザクションの型 | “send” |
| 提供先のアカウントアドレス | 受取アカウントのアドレス |
| 提供アカウントの残高 | 提供アカウントの今回の送信後の残高 |
| 提供アカウントのアカウントチェーンの直前のトランザクション | 当該トランザクションのハッシュ値 |
| Nonce（Proof of Work） | 条件を満たすNonce（スパム対策） |
| 署名 | 提供アカウントのトランザクションへの署名 |

図 8　資産提供のためのトランザクション

| 受取（受信）トランザクション | |
|---|---|
| トランザクションの型 | “receive” |
| 受け取る提供（送信）トランザクション | 提供（送信）トランザクションのハッシュ値 |
| 受取アカウントのアカウントチェーンの直前のトランザクション | 当該トランザクションのハッシュ値 |
| Nonce（Proof of Work） | 条件を満たすNonce（スパム対策） |
| 署名 | 受取アカウントのトランザクションへの署名 |

図 9　資産受取のためのトランザクション

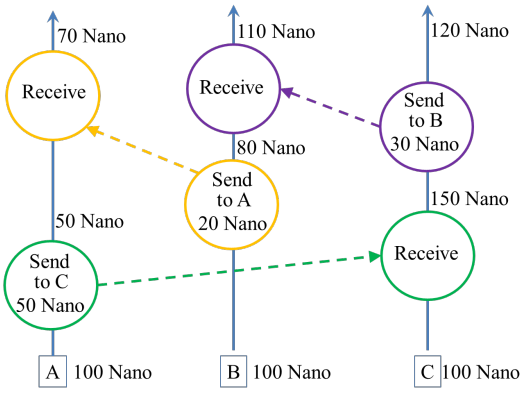


図 10　アカウントチェーンの例

①Pseudonymity

Nano では，個々のアカウントに公開鍵暗号の鍵ペアが対応する．秘密鍵は乱数で生成されるか，乱数で生成されるワレットのシードから生成される．公開鍵は秘密鍵から生成され，公開鍵から利用者識別情報であるアカウントアドレスが生成される．

以上のように，利用者識別情報（アカウントアドレス）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．

②OneTime-ness

Nano では，ワレット内のアカウントアドレスは必要に応じ乱数あるいはワレットのシードに毎回異なるインデックスを加味し生成することができる．この機能を利用し必要の都度アカウントアドレスを生成し使用すれば，利用者識別情報であるアカウントアドレスは毎回異なる（ワンタイムステルスアドレス）ため，OneTime-ness of UII（利用者識別情報のワンタイム性）要件を満たしている．

しかし，一般には，資産受取の際に毎回異なるアカウントを生成することを想定されているわけではない．アカウントごとにアカウントチェーンが構成され，そのアカウントチェーンには同じアカウント宛の資産の受取（受信）トランザクションおよびそのアカウントからの提供（送信）トランザクションが登録され，同一アカウントアドレスを使用したトランザクションが複数存在することになる．このように，Nano の一般的な使い方では OneTime-ness of UII（利用者識別情報のワンタイム性）要件は満たされないことになる．

③Unlinkability between Transactions

Nano の提供（送信）トランザクションでは，使用する資産を受け取った受取（受信）トランザクションを指定する機能はない．そもそも Nano では保有資産は受取（受信）トランザクション内で管理されているわけではなく，アカウントごとに合算され管理されている．従って，タングル型の DAG 系暗号資産と違い，提供者が作成する提供（送信）トランザクションとその原資として使用する受取(受信)トランザクションとの対応は記録されない．しかし，トランザクションには提供者の資産残高と紐づけられているアカウントが直接登録されており，提供に使用する資産を容易に確認でき，Unlinkability of UIIs/assets between Transactions（利用者識別情報間の利用者/暗号資産の非連結性）要件は満たしていない．

④Unlinkability within Transaction

Nano では，提供アカウントチェーンに登録されている提供（送信）トランザクションにて受取アカウントアドレスを直接指定しており，提供者と受取者の対応は容易に把握でき，Unlinkability of UIIs/assets within Transaction（トランザクション内の利用者/暗号資産の非連結性）要件は満たしていない．

⑤Concealment of Amount

Nano では，アカウントチェーンの資産総額，提供（送信）トランザクション内の提供アカウントの残高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．

## 7　Hedera の匿名性

Hedera はラティス型の DAG 系暗号資産である．利用者は資産の管理単位であるアカウントを複数保有できる．アカウントには，公開鍵と秘密鍵の 1 組および Hedera 側で自動的に設定されるアカウント ID により，そのアカウントへの資産の移転が指定され，秘密鍵によりそのアカウントの資産の使用（提供）が可能である．

アカウント間の資産移転は，トランザクション（図 11）で実施される．転送資産額が負の場合は提供，正の場合は受取となる．トランザクション内の転送資産額の合計は 0 になる必要がある．

| トランザクション | | |
|---|---|---|
| 転送$_1$ | アカウントID$_1$ | 転送資産額$_1$ |
| 転送$_2$ | アカウントID$_2$ | 転送資産額$_2$ |
| 署名 | 提供アカウントによる<br>トランザクションへの署名 | |

**図 11　Hedera トランザクションの例**

トランザクションは，イベントにまとめられノード間の転送により共有される．その上で各ノードにおける内容の確認とトランザクションの順序についてコンセンサスを得る．コンセンサスに到達すると，トランザクションをその順序に従って Hedera State へ適用し更新する．Hedera State には，各アカウント ID の資産残高が記録される．

Hedera 資産移転のためのトランザクションおよび Hedera State の匿名性について，以下，3 章でまとめた匿名性に関する要件ごとにまとめている．

①Pseudonymity

Hedera では，利用者識別情報として，公開鍵およびアカウント ID がある．公開鍵は乱数で生成される秘密鍵より生成される．またアカウント ID は，Hedera 側で自動的に付与される．個々のアカウントに公開鍵暗号の鍵ペアが対応する．

以上のように，利用者識別情報（公開鍵およびアカウント ID）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．

②OneTime-ness

Hedera では，複数のアカウントを利用することができるが，受取の都度，新たな公開鍵やアカウント ID を生成し使用することは想定されていなく，同一アカウント ID

を使用したトランザクションが複数存在することになる．このように，Hedera の一般的な使い方では OneTime-ness of UII（利用者識別情報のワンタイム性）要件は満たされないことになる．

**③Unlinkability between Transactions**

Hedera では，使用する資産を受け取ったトランザクションを指定する機能はない．Hedera では保有資産はトランザクション内で管理されているわけではなく，アカウントごとに合算され管理されている．従って，タングル型の暗号資産と違い，提供者が作成するトランザクションとその原資として使用するトランザクションとの対応は記録されない．しかし，トランザクションには提供者のアカウント ID が直接登録されており，提供に使用する資産を容易に確認でき，Unlinkability of UIIs/assets between Transactions（利用者識別情報間の利用者/暗号資産の非連結性）要件は満たされていない．

**④Unlinkability within Transaction**

Hedera では，トランザクションにて提供アカウント ID および受取アカウント ID を直接指定しており，提供者と受取者の対応は容易に把握でき，Unlinkability of UIIs/assets within Transaction（トランザクション内の利用者/暗号資産の非連結性）要件は満たしていない．

**⑤Concealment of Amount**

Hedera では，アカウント ID の資産総額，トランザクション内の提供および受取資産の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）要件を満たしていない．

## 8　おわりに

DAG 系暗号資産である IOTA，Obyte，Nano，Hedera Hashgraph のトランザクションの匿名性を，3 章に定義を記載している DAG 系暗号資産のトランザクションの匿名性要件に即して評価した結果を図 12 にまとめている．なお，参考までに Bitcoin の匿名性要件に対する評価結果も示している．

| 要件名称 | IOTA | Obyte | Nano | Hedera | Bitcoin |
|---|---|---|---|---|---|
| Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性） | ○ | ○ | ○ | ○ | ○ |
| OneTime-ness of UII（利用者識別情報のワンタイム性） | ○ | ○ | ×(△) | ×(△) | ○ |
| Unlinkability of UIIs/assets between Transaction(トランザクション間の利用者/暗号資産の非連結性) | × | × | × | × | × |
| Unlinkability of UIIs/assets within Transaction(トランザクション内の利用者/暗号資産の非連結性) | × | △ | × | × | × |
| Concealment of Amount（移転資産額の秘匿） | × | × | × | × | × |

**図 12　DAG 系暗号資産のトランザクションの匿名性評価結果**

今回の調査の対象とした DAG 系暗号資産は，Bitcoin をはじめとする一般のブロックチェーン系暗号資産に比べ，タングル型の場合は同程度の匿名性，ラティス型の場合は低い匿名性，という結果であった．

ラティス型の匿名性が低いのは，タングル型が一般のブロックチェーン系暗号資産と同様，DAG 上で UII の OneTime-ness を利用し資産が分散管理されることが想定されているのに対し，ラティス型の場合，資産を（限られた数の）アカウントに集約し管理されることが想定されているため UII の OneTime-ness の維持は困難あるいは限られた範囲での維持となるであろう，という判断に基づいている．

一方，ブロックチェーン系暗号資産の場合と同様，スケーラビリティに優位性のある DAG 系暗号資産においても，匿名性強化目指す暗号資産が登場してきている．その一つに，DERO（[10]）がある．DERO は，Monero 等の匿名暗号資産の匿名性を強化する仕組みである CryptoNote Protocol（[18]）を採用しており，DAG 系匿名暗号資産の一つである．DERO のブロックやトランザクションの具体的なデータ構造については未公開のようであるが，CryptoNote を採用している Monero と同等の匿名性と推定される．具体的には，Pseudonymity of UII，OneTime-ness of UII はもちろん，リング CT により Unlinkability of UIIs/assets between Transactions および Unlinkability of UIIs/assets within Transaction の要件を一定レベル満たし，更にペダーセンコミットメントにより Concealment of Asset amount の要件も満たしている，と考えられる．

DAG 系暗号資産においても高い匿名性へのニーズは強く，今後多くの DAG 系暗号資産にてスケーラビリティとセキュリティの両立に向けた改良・拡張，あるいは新たな DAG 系匿名暗号資産の登場が期待される．

## 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] 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ウム 2019（CSS2019），

[2] 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.

[3] 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.

[4] 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.
[5] 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
[6] Serguei Popov, “The Tangle”, April 30, 2018.
Version 1.4.3.
https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
[7] Anton Churyumov, “Byteball: A Decentralized System for Storage and Transferof Value”,2016.
https://obyte.org/Byteball.pdf
[8] Colin LeMahieu, “Nano: A Feeless Distributed Cryptocurrency Network”, 2018.
https://nano.org/en/whitepaper
[9] Leemon Baird, Mance Harmon, Paul Madsen, “Hedera: A Public Hashgraph Network & Governing Council”, 2019.
https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf
[10] DERO PROJECT WHITE PAPER, 2018.
https://dero.io/attachment/Whitepaper.pdf
[11] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2001.
https://bitcoin.org/bitcoin.pdf
[12] All Cryptocurrencies
https://coinmarketcap.com/all/views/all/
[13] 最新 IoT 関連の仮想通貨一覧, 2019.
https://www.owl-coin.com/tags/internet-of-things
[14] 耐量子暗号特性の仮想通貨とその技術概要, 2019.
https://www.zbaron-newworld.com/entry/2018/03/11/003001
[15] Top 28 Best Privacy Coins 2018
https://kingpassive.com/best-privacy-coins-2018/
[16] Monero : Privacy in the blockchain v1.0
https://eprint.iacr.org/2018/535.pdf
[17] Zero to Monero: First Edition
https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
[18] Mastering Monero
https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf
[19] Zcash Protocol Specification
https://www.btrade.co.kr/btrade_res/20180507145055652.pdf
[20] Nicolas van Saberhagen, ″CryptoNote v2.0″, 2013.
https://cryptonote.org/whitepaper.pdf
[21] Adam Back, “bitcoins with homomorphic value (validatable but encrypted)”, 2013.
https://bitcointalk.org/index.php?topic=305791.0
[22] Greg Maxwell, ″Confidential Transactions″, 2016.
https://people.xiph.org/~greg/confidential_values.txt
[23] Gregory Maxwell, Andrew Poelstra,” Borromean Ring Signature”, 2015.
https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf
[24] SHEN NOETHER, “RING CONFIDENTIAL TRANSACTIONS”, 2015.
https://eprint.iacr.org/2015/1098.pdf
[25] 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
[26] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova, “Pinocchio: Nearly Practical Verifiable Computation”, 2013.
https://eprint.iacr.org/2013/279
[27] Andrew Poelstra, “Mimblewimble”, 2016.
https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf
[28] Gregory Maxwell, “CoinJoin: Bitcoin privacy for the real world”, 2013.
https://bitcointalk.org/index.php?topic=279249.0
[29] Daniel Wilczynski, “Greg Maxwells Roadmap for Bitcoin Scaling”, 2015.
http://www.danielwilczynski.com/maxwells-scaling-roadmap
[30] 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
[31] Christina Garman, Matthew Green, Ian Miers, ” Accountable Privacy for Decentralized Anonymous Payments”, 2016.
https://eprint.iacr.org/2016/061.pdf