CSS2020

 1

暗号資産の匿名性要件の整理と対応レベルの比較

2020年10月27日

（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．はじめに

 2

暗号資産の分類

匿名性 / チェーン技術	暗号資産	匿名暗号資産
ブロックチェーン技術ベース	Bitcoin	Monero Zcash Grin
DAGチェーン技術ベース	IOTA Obyte Nano Hedera Hashgraph	Aidos Kuneen Dero Tangram

取引情報の構成
（匿名性に関連する情報のみ）

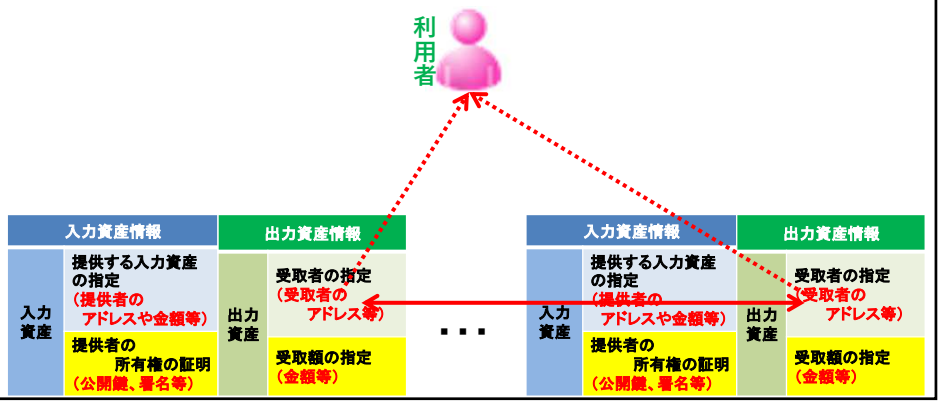
入力資産情報		出力資産情報	
入力資産1	提供する入力資産の指定（提供者のアドレスや金額等）	出力資産1	受取者の指定（受取者のアドレス等）
	提供者の所有権の証明（公開鍵、署名等）		受取額の指定（金額等）
入力資産2	提供する入力資産の指定	出力資産2	受取者の指定
	提供者の所有権の証明		受取額の指定
.....		.....	
入力資産n	提供する入力資産の指定	出力資産m	受取者の指定
	提供者の所有権の証明		受取額の指定

暗号資産の匿名性に関する要件（1）
Pseudonymity of User Identification Information(UII)
（利用者識別情報の仮名性）

暗号資産の匿名性に関する要件（2）

OneTime-ness of UIIs

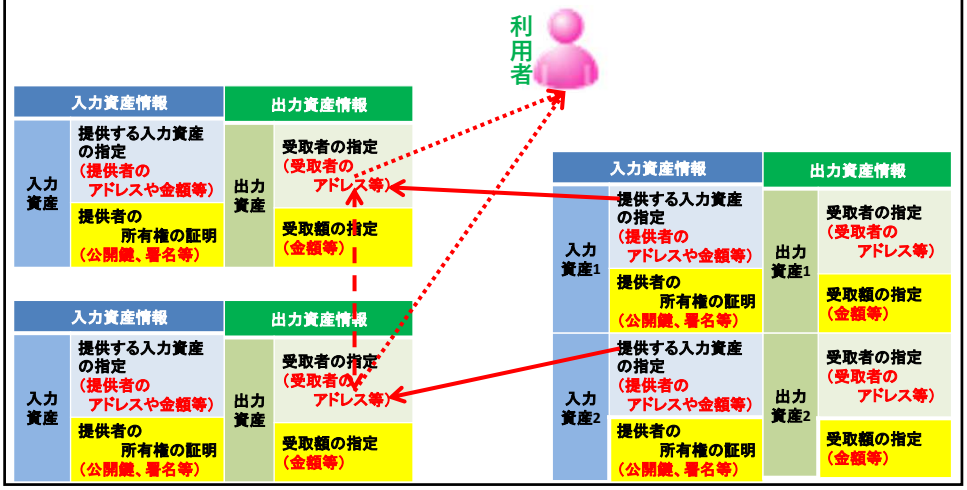
（利用者識別情報のワンタイム性）



暗号資産の匿名性に関する要件（3）

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）



2. 匿名性要件

 7

暗号資産の匿名性に関する要件（4）

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）

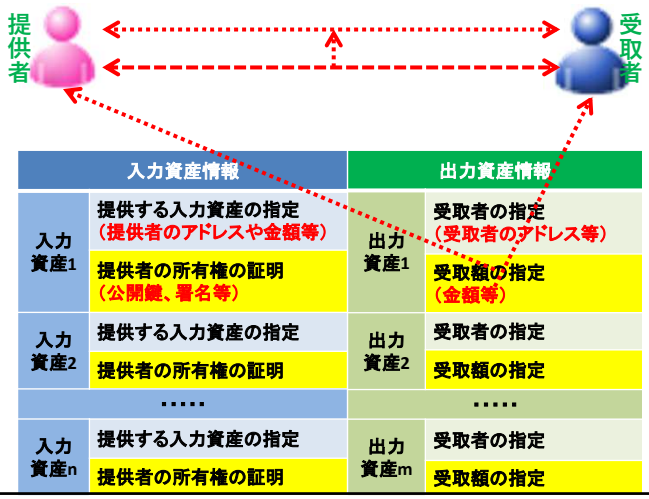
2. 匿名性要件

 8

暗号資産の匿名性に関する要件（5）

Concealment of Asset Amount

（移転資産額の秘匿）



暗号資産の匿名性に関する要件

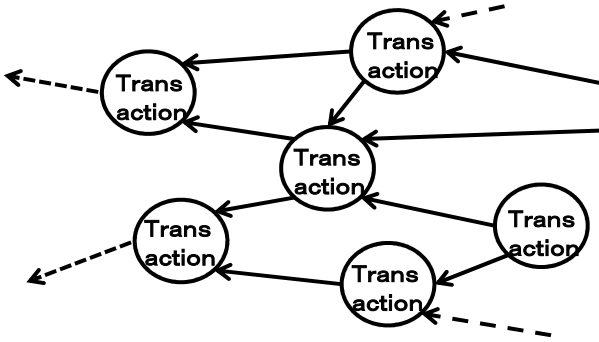
要件名称	要件内容
Pseudonymity of User Identification Information(UII) （利用者識別情報の仮名性）	利用者の実名等の推定が困難な利用者識別情報（公開鍵、アドレス等）であること
OneTime-ness of UIIs （利用者識別情報のワンタイム性）	毎回異なる利用者識別情報が使用され、複数の利用者識別情報が同一の利用者に紐づけられていることの推定が困難であること
Unlinkability of Assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）	トランザクション間の、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

DAGチェーン技術ベースの暗号資産

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*

Aidos Kuneen

概要：IOTA技術をベースにシンプルなトランザクション構造を採用
匿名化技術：ゼロ知識証明（ZKBoo）を利用した匿名転送AKShuffle



Aidos KuneenのDAGチェーン

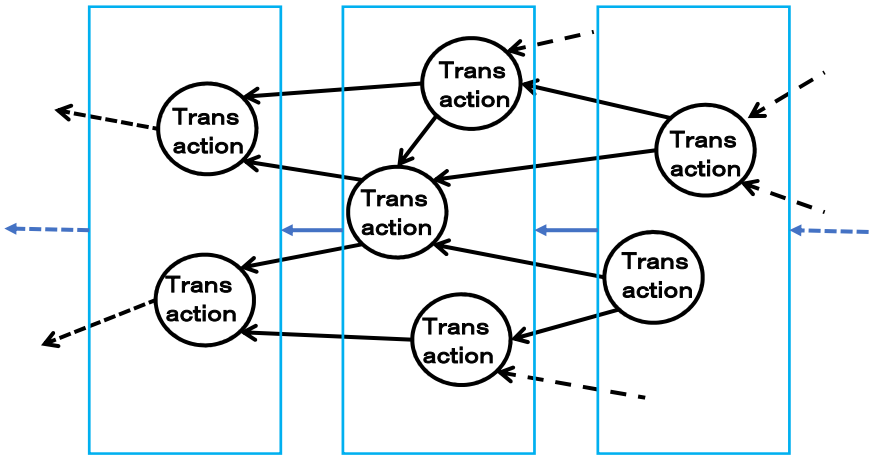
Transaction
From address
To address
Value
Signature
Previous transaction 1
Previous transaction 2

Aidos Kuneenの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性）	○	利用者識別情報であるアドレスは、利用者が選定したランダムなシードと未使用のインデックスから生成される（利用者固有の情報は使用されない）
OneTime-ness of UIIs（利用者識別情報のワンタイム性）	○	利用者が選定したランダムなシードと未使用インデックスから、毎回異なるアドレスが生成され使用される（同一のアドレスの使用は秘密鍵漏洩に繋がる）
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）	△	ダミーの未使用資産とのシャッフル機能（ZKBooを利用したAKShuffle）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は困難であるが、その困難さは、AKShuffleでダミーとして指定する暗号資産の数に依存する
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）	△	ワンタイムアドレスおよびAKShuffleにより、提供者と受取者の対応の特定は困難であるが、その困難さは提供者のダミーとして指定する暗号資産の数に依存する
Concealment of Asset Amount（移転資産額の秘匿）	×	提供額・受取額を直接指定している

Dero

概要：PoWブロックチェーン技術とDAGチェーン技術の組み合わせ
匿名化技術：ワンタイムステルスアドレス、鍵イメージ、リングCT



DeroのDAGチェーン：BlockDAG

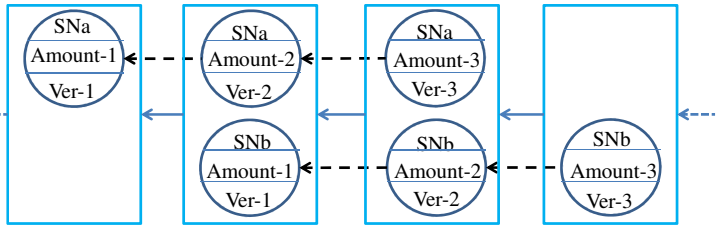
Dero DAGチェーンの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性）	○	固定の利用者識別情報である二つの公開鍵生成には利用者固有の情報は使用されない
OneTime-ness of UIIs（利用者識別情報のワンタイム性）	○	トランザクションごとに生成する乱数と固定の利用者識別情報からワンタイムの利用者識別情報（アドレス）が生成され使用される
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）	△	リングCTが採用され、受取時の資産と提供に使用する資産との対応の特定は困難である（特定の困難さは、リングCTでダミーとして指定する暗号資産の数に依存する）
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）	△	ワンタイムアドレスおよびリングCTにより、提供者と受取者の対応の特定は困難であるが、その困難さは提供者のダミーとして指定する暗号資産の数に依存する
Concealment of Asset Amount（移転資産額の秘匿）	○	ペダーセンコミットメントにより、提供額・受取額の秘匿が可能

Tangram

概要：ブロックチェーン技術とDAGチェーン技術の組み合わせ
匿名化技術：暗号化とゼロ知識証明（シュノアのNIZK）

Tangram のLedger



Coin

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：Version、Stamp等で定義 （マスター鍵と関連付け所有権を取得するための鍵）
Principle	コインの証明：Version、Stamp等で定義 コインの所有者およびコインが本物であることの証明
Stamp	コインの識別子：シリアルナンバーおよびAmount等で定義
Version	コインのバージョン番号

Tangramの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity of User Identification Information(UII) （利用者識別情報の仮名性）	○	コインの所有権を示す情報は、利用者のマスター鍵（利用者識別情報）の他、コイン生成プロセスの情報のハッシュ値から生成され利用者の特定は困難
OneTime-ness of UIIs （利用者識別情報のワンタイム性）	○	コインの所有権を示す情報は、利用者のマスター鍵の他、コイン生成ごとに異なる生成プロセスの情報のハッシュ値から生成され、各コインで異なる
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）	○	台帳（Ledger）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ない
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）	○	台帳（Ledger）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ない
Concealment of Asset Amount （移転資産額の秘匿）	○	提供額・受取額は暗号化されており、 提供額・受取額の秘匿が可能

4. 考察

主要な暗号資産の匿名性比較

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）	×	○	○	○	×	×	×	×	×	○	○

①Nano，Hedera HashgraphはBitcoinより低い匿名性
資産残高記録方式のため、資産管理IDが再利用されるため
②ゼロ知識証明が高い匿名性を実現
リング署名（CryptoNote）、コインミキシング（MimbleWimble)は
使用するダミーの暗号資産の数に応じた匿名性

終

ご清聴、ありがとうございました。