2020年電子情報通信学会ソサイエティ大会

暗号資産台帳の匿名性と特定・追跡性についての考察

2020年9月17日

（株）IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp

共　著　者

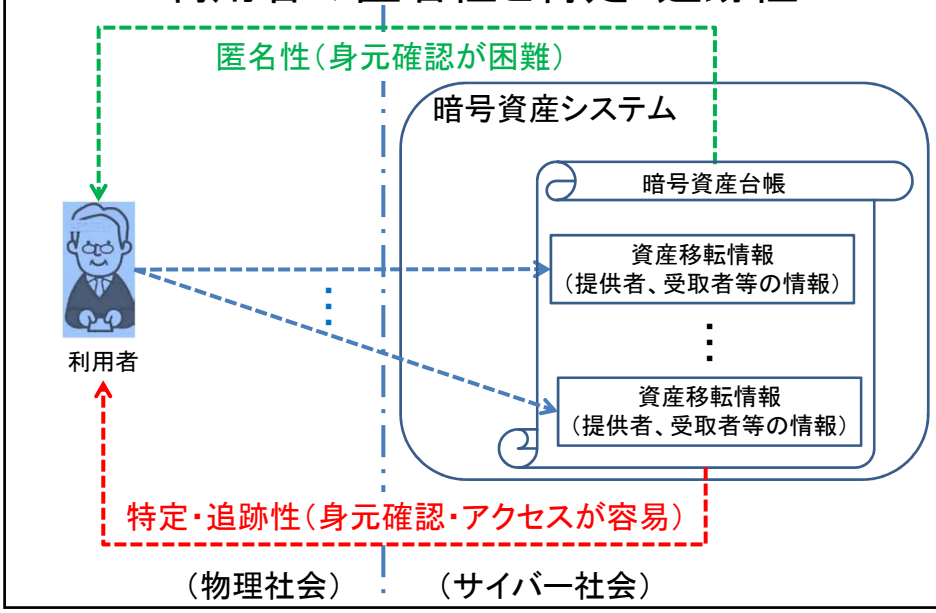
辻井重男
中央大学研究開発機構

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

暗号資産システムにおける利用者の匿名性と特定・追跡性



1. はじめに

 3

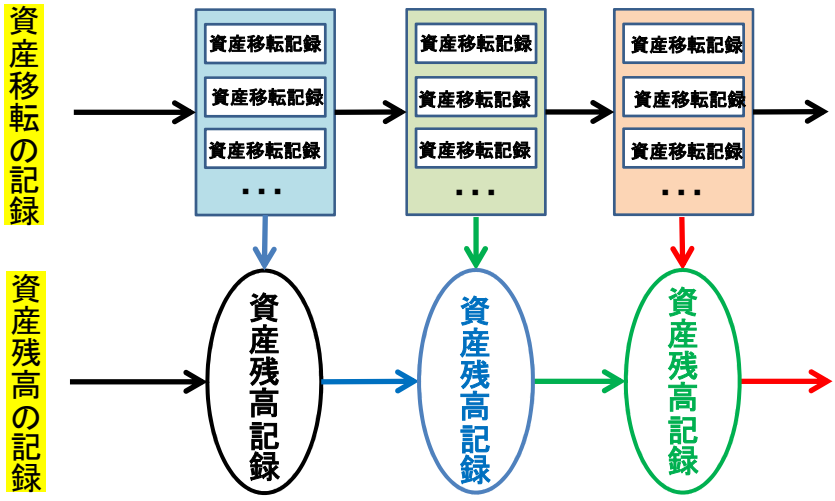
一般的な暗号資産の分類

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

2. 暗号資産の分類方式の提案

 4

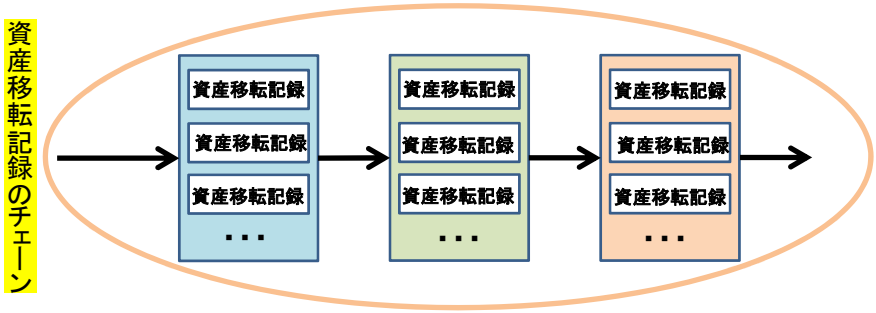
暗号資産台帳で登録・管理される情報



暗号資産台帳登録・管理情報による暗号資産の分類

（1）資産移転情報を台帳に登録・管理する暗号資産（TCAMS）

（TCAMS:Transaction based CryptoAsset Management System)



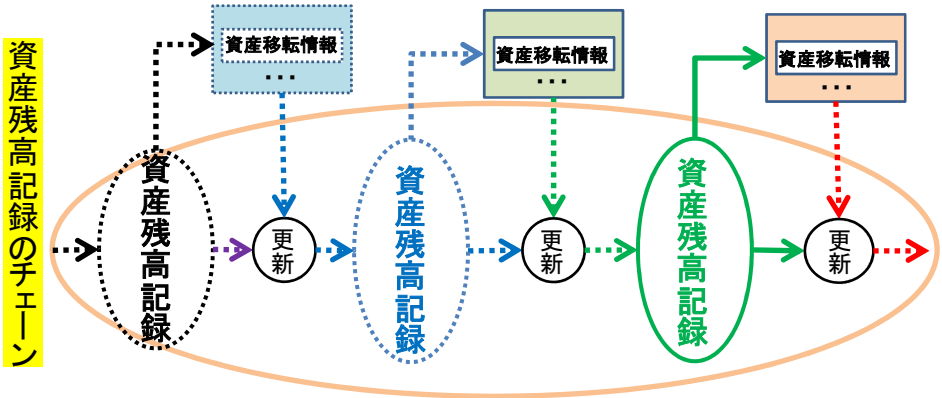
ブロックチェーン：　Bitcoin、Monero、Zcash、Grin

DAGチェーン：　IOTA、Obyte、Aidos Kuneen、Dero

暗号資産台帳登録・管理情報による暗号資産の分類

（2）資産残高情報を台帳に登録・管理する暗号資産（BCAMS）

（BCAMS：Balance based CryptoAsset Management System）



DAGチェーン：　Nano、Hedera Hashgraph、Tangram

新たな分類方式に基づく暗号資産の匿名性に関する現状

台帳管理情報	暗号資産	匿名暗号資産
TCAMS （資産移転記録）	Bitcoin IOTA Obyte ➔公開鍵のランダム性、ワンタイム性による匿名性	Monero Zcash Grin Aidos Kuneen Dero ➔加えて、リング署名、コインミキシング、ゼロ知識証明による匿名性
BCAMS （資産残高記録）	Nano Hedera Hashgraph ➔資産管理IDのランダム性による匿名性 （繰り返し利用が匿名性のリスク）	Tangram ➔加えて、ゼロ知識証明による匿名性

主要な暗号資産の匿名性比較結果（詳細はCSS2020にて発表）

匿名性要件名称	TCAMS								BCAMS		
	ブロックチェーン				DAGチェーン				DAGチェーン		
	Bitcoin	匿名性強化			IOTA	Obyte	匿名性強化		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
②匿名暗号資産が採用する匿名性強化技術は多様
③ゼロ知識証明が高い匿名性を実現

➔ **安心・安全な暗号資産のためには、匿名性の強化が必須！**

4. 特定・追跡性の現状

新たな分類方式に基づく暗号資産の特定・追跡性に関する現状

台帳管理情報	暗号資産	匿名暗号資産
TCAMS （資産移転記録）	Bitcoin IOTA Obyte ➔具体的な提供機能無し（ワンタイム公開鍵と利用者の対応情報が必要）	Monero Zcash Grin Aidos Kuneen Dero ➔Monero、Zcashには若干の機能があるが、他には一切無し（匿名化の仕組みの解除が必要）
BCAMS （資産残高記録）	Nano Hedera Hashgraph ➔具体的な提供機能無し（資産管理IDと利用者の対応情報が必要）	Tangram ➔具体的な提供機能無し（匿名化の仕組みの解除が必要）

5. おわりに

安心・安全な暗号資産台帳システムに期待される機能

（1）基本機能：安全・確実な暗号資産保全、暗号資産移転

（2）利用者のプライバシー保護➔利用者の確実な匿名性の実現
多くの暗号資産の匿名性は不十分！

（3）不正・不法な暗号資産利用防止
➔利用者・資産の特定・追跡性保証
多くの暗号資産では、特定・追跡性への配慮が欠如！
匿名性強化の仕組みには、特定・追跡性要件への対応も必須！
なお、利用者・暗号資産の
特定・追跡性要件の明確化も今後の課題！
（監査の観点、徴税の観点、犯罪捜査の観点・・・）

終