暗号資産の封印・償還における利用者の匿名性および特定・追跡性の考察

2021年1月19日

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

共　著　者

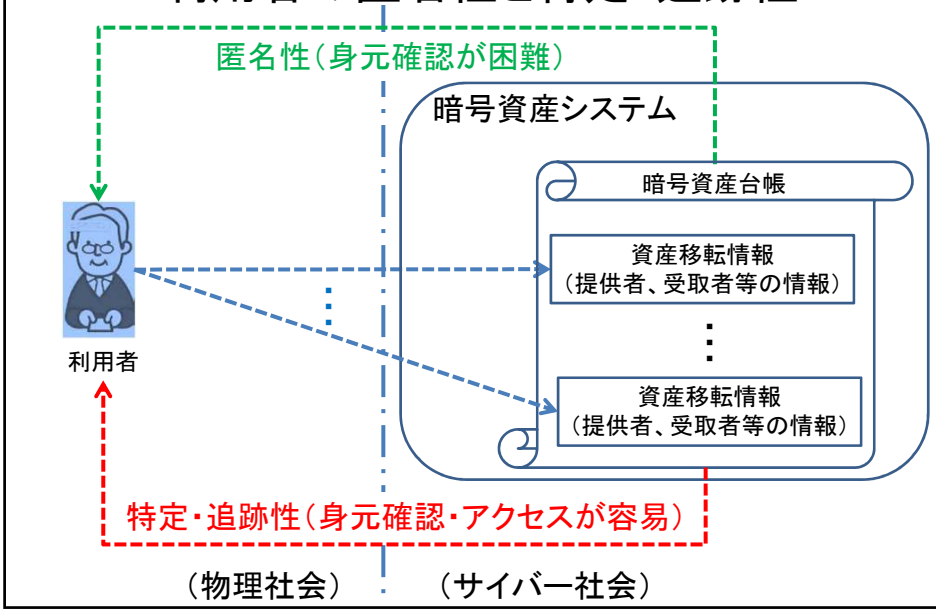
辻井重男
中央大学研究開発機構

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

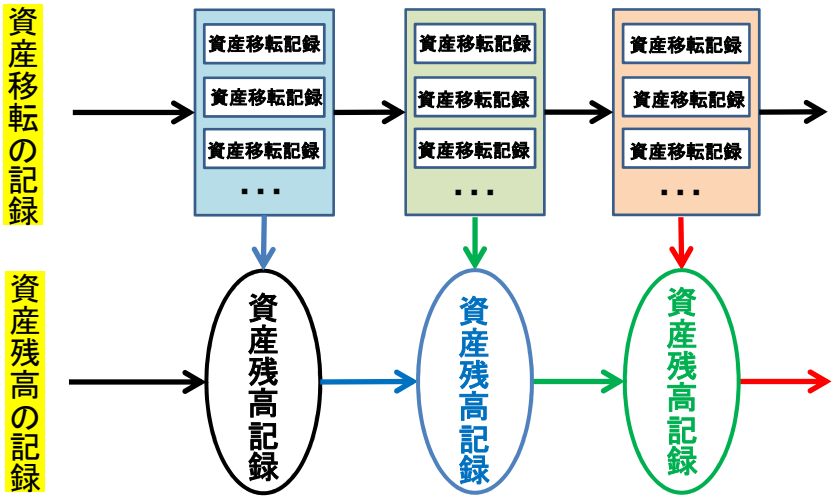
謝辞　本研究の一部は JSPS科研費 基盤(B) JP18H03240 の支援を受けている。

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



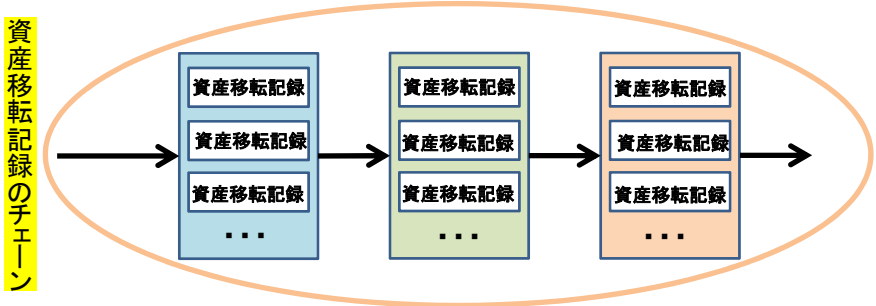
暗号資産台帳で登録・管理される情報



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・管理する方式（TCAMS）

（TCAMS:Transaction based CryptoAsset Management System)



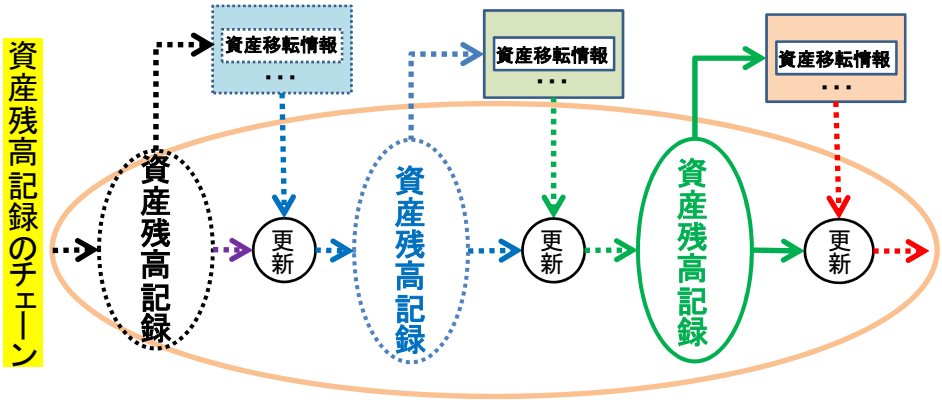
ブロックチェーン：　Bitcoin、Monero、Zcash、Grin

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・管理する方式（BCAMS）

（BCAMS：Balance based CryptoAsset Management System）



DAGチェーン：　Nano、Hedera Hashgraph、Tangram

台帳データ表現方法に基づく11種の暗号資産の分類

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. 新たな暗号資産の分類

台帳に登録される情報に基づく 11種の暗号資産の分類

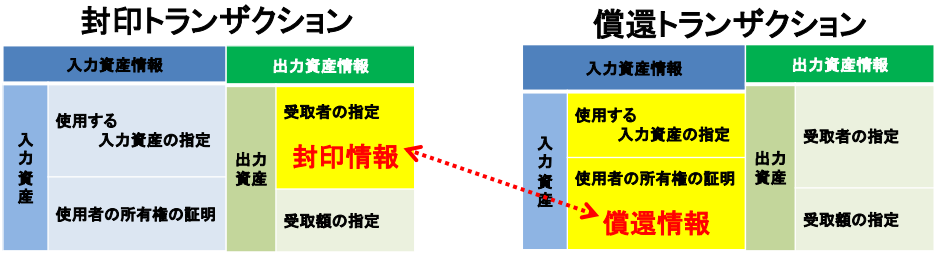
台帳管理情報	暗号資産	匿名暗号資産
TCAMS （資産移転記録）	Bitcoin IOTA Obyte	Monero Zcash Grin Aidos Kuneen Dero
BCAMS （資産残高記録）	Nano Hedera Hashgraph	Tangram

3. TCAMSにおける資産移転

資産移転記録方式TCAMSにおける 暗号資産台帳上の 資産移転記録例（Bitcoin等）

入力資産情報		出力資産情報	
入力 資産1	使用する入力資産の指定 （使用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）
	使用者の所有権の証明 （公開鍵、署名等）		受取額の指定 （金額等）
入力 資産2	使用する入力資産の指定	出力 資産2	受取者の指定
	使用者の所有権の証明		受取額の指定
.....		.....	
入力 資産n	使用する入力資産の指定	出力 資産m	受取者の指定
	使用者の所有権の証明		受取額の指定

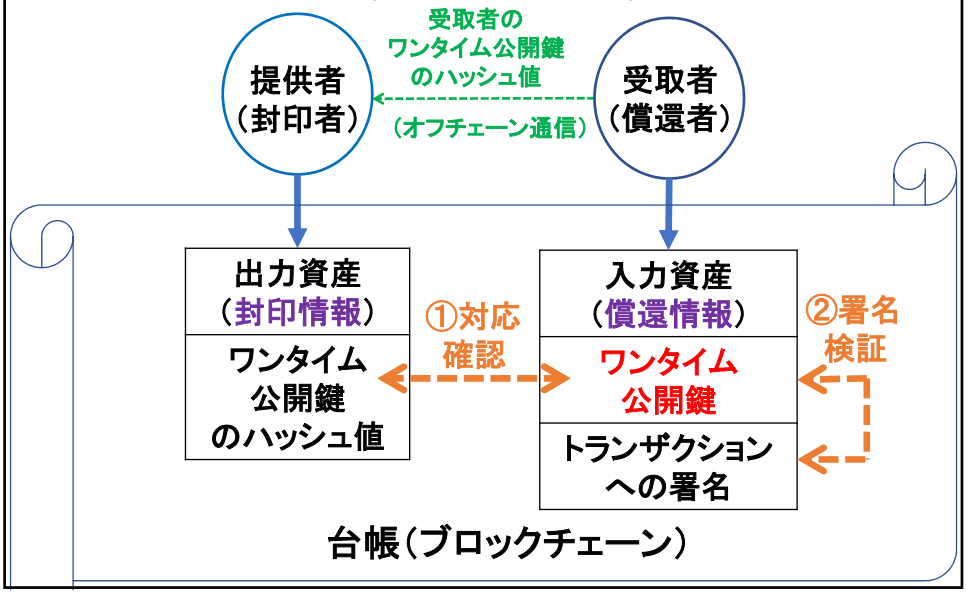
資産移転記録方式TCAMSにおける封印・償還による資産移転

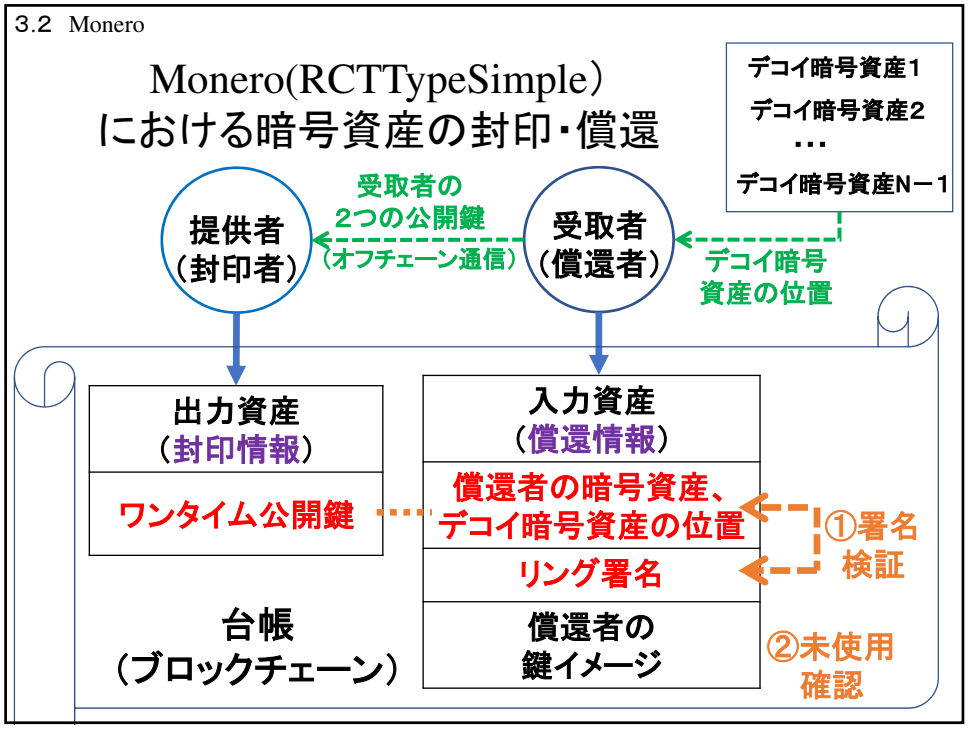


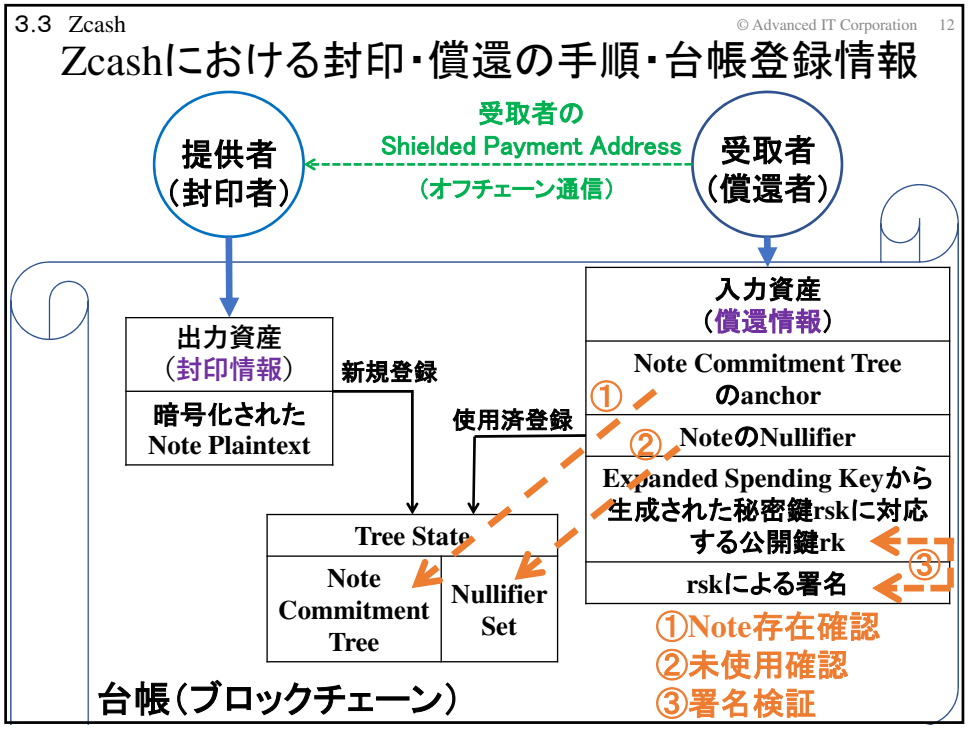
封印情報：提供する資産の受取者を指定する情報
償還情報：受取者が資産を受け取るために指定する
正当な受取者であることを示す情報

Bitcoinにおける暗号資産の封印・償還

P2PKH（Pay-to-Public-Key-Hash）




3.2 Monero
Monero(RCTTypeSimple)
における暗号資産の封印・償還
デコイ暗号資産1
デコイ暗号資産2
…
デコイ暗号資産N－1
提供者
(封印者)
受取者の
2つの公開鍵
(オフチェーン通信)
受取者
(償還者)
デコイ暗号
資産の位置
出力資産
(封印情報)
ワンタイム公開鍵
入力資産
(償還情報)
償還者の暗号資産、
デコイ暗号資産の位置
リング署名
償還者の
鍵イメージ
①署名
検証
②未使用
確認
台帳
(ブロックチェーン)


3.3 Zcash
© Advanced IT Corporation 12
Zcashにおける封印・償還の手順・台帳登録情報
提供者
(封印者)
受取者の
Shielded Payment Address
(オフチェーン通信)
受取者
(償還者)
出力資産
(封印情報)
暗号化された
Note Plaintext
新規登録
使用済登録
入力資産
(償還情報)
Note Commitment Tree
のanchor
①
NoteのNullifier
②
Expanded Spending Keyから
生成された秘密鍵rskに対応
する公開鍵rk
③
rskによる署名
Tree State
Note
Commitment
Tree
Nullifier
Set
①Note存在確認
②未使用確認
③署名検証
台帳(ブロックチェーン)

4. 比較・考察

 13

暗号資産封印・償還方式の“利用者の確実な匿名性”の観点からのまとめ

	匿名性へのリスクが想定される台帳登録・公開情報	利用者の確実な匿名性の観点からのリスク
Bitcoin（P2PKH）	利用者（償還者）のワンタイム公開鍵とそのハッシュ値	複数の入力資産指定の場合の、ワンタイム公開鍵間の連結性
Monero	利用者（受取者）のワンタイム公開鍵（受取者のワンタイム公開鍵の特定はデコイ暗号資産の数に応じ困難）	複数の入力資産指定の場合の、指定された複数のワンタイム公開鍵間の連結性（但し、償還者のワンタイム公開鍵の特定はデコイ暗号資産の数に応じ困難）
Zcash	匿名性へのリスクが想定される台帳登録・公開情報は無い（利用者に関する情報は、暗号化、ハッシュ化、ランダム化されている）	ー

高い匿名性の実現には、暗号化＋ゼロ知識証明の活用

4. 比較・考察

 14

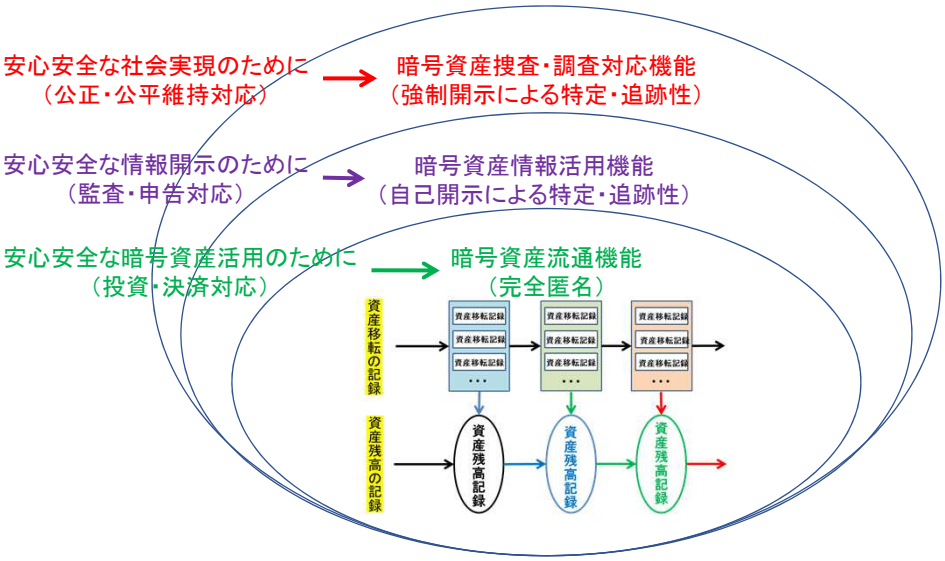
暗号資産封印・償還方式の利用者協力の元の“利用者の特定・追跡性”の現状・課題

	可能な方法	できること（できないこと）	リスク
Bitcoin（P2PKH）	利用者によるワンタイム公開鍵の提供	＊ワンタイム公開鍵で受け取った資産の特定、使用済み/未使用の特定 ＊資産保有額の把握（すべてのワンタイム公開鍵を提供した場合）	＊利用者の提供情報が正しいかどうか
Monero	利用者によるワンタイム公開鍵の提供	＊ワンタイム公開鍵で受け取った資産の特定（当該資産の使用済み/未使用の特定は不可）	＊利用者の提供情報が正しいかどうか
	利用者によるtracking keyおよび鍵イメージの提供	＊受け取った資産の全ての使用・未使用の特定、資産保有額の把握	
Zcash	利用者によるIncoming Viewing Keyの提供	＊受け取った資産の全ての特定および資産保有額の把握	＊利用者提供情報が正しいかどうか ＊利用者宛メッセージ公開のリスク

①利用者の特定・追跡性についての検討はこれからの課題
②現状では、利用者の協力無しでは“利用者の特定・追跡”は困難

5. おわりに

期待される暗号資産システム
匿名性と特定・追跡性の両立



終

（ご清聴、ありがとうございました）