CSS2019

 1

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

2019年10月22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。

 2

説明項目一覧

（1）暗号資産の概況
　　暗号資産　時価総額ベスト20
　　匿名暗号資産　時価総額ベスト10
（2）匿名性に関するリスク
　　暗号資産トランザクションの匿名性に関する要件
（3）匿名化プロトコル
　　匿名暗号資産ブロックチェーンの主要な匿名化プロトコル
（4）Monero（RCTTypeSimple）ブロックチェーンの匿名性
（5）Zcash（Sapling）ブロックチェーンの匿名性
（6）Grinブロックチェーンの匿名性
（7）Monero（RCTTypeSimple）、Zcash（Sapling）、Grin
　　のブロックチェーンの匿名性に関する比較評価
（8）おわりに

2

（1）暗号資産の概況

 3

暗号資産　時価総額ベスト20

順位	名称	記号	時価総額	単価
1	Bitcoin	BTC	$154,350,254,221	$8,582.94
2	Ethereum	ETH	$20,828,475,950	$192.71
3	XRP	XRP	$12,122,217,124	$0.28
4	Bitcoin Cash	BCH	$4,304,022,687	$238.47
5	Tether	USDT	$4,133,537,994	$1.01
6	Litecoin	LTC	$3,757,845,494	$59.24
7	EOS	EOS	$3,030,696,668	$3.24
8	Binance Coin	BNB	$2,783,053,077	$17.89
9	Bitcoin SV	BSV	$1,635,072,693	$91.58
10	Stellar	XLM	$1,266,712,158	$0.06
11	TRON	TRX	$1,133,257,161	$0.02
12	Cardano	ADA	$1,102,390,058	$0.04
13	Monero	XMR	$993,329,021	$57.58
14	Chainlink	LINK	$974,560,592	$2.78
15	UNUS SED LEO	LEO	$968,202,555	$0.97
16	Huobi Token	HT	$803,567,546	$3.27
17	IOTA	MIOTA	$778,516,603	$0.28
18	Dash	DASH	$676,092,607	$74.40
19	Tezos	XTZ	$620,201,777	$0.94
20	Ethereum Classic	ETC	$580,111,034	$5.08
21	Cosmos	ATOM	$551,305,361	$2.89

2019年10月10日現在2396通貨（資産総額 $235.66 B　約25兆円）

出典：All Cryptocurrencies　https://coinmarketcap.com/all/views/all/

世界の現金通貨総額は102.3兆円、預金通貨を含めると世界の通貨総額は797.6兆円
（2019年8月の日銀のマネーストック速報）

（1）暗号資産の概況

 4

匿名暗号資産　時価総額ベスト10

順位	名称	記号	時価総額	単価
13	Monero	XMR	$993,329,021	$57.58
29	Zcash	ZEC	$289,672,991	$38.14
65	Bytecoin	BCN	$78,299,493	$0.00
66	HyperCash	HC	$71,946,511	$1.62
73	Verge	XVG	$60,790,136	$0.00
83	Zcoin	XZC	$50,969,311	$5.96
94	Electroneum	ETN	$36,710,505	$0.00
99	Beam	BEAM	$34,695,565	$0.87
105	Grin	GRIN	$31,125,902	$1.35
135	Enigma	ENG	$23,938,181	$0.32

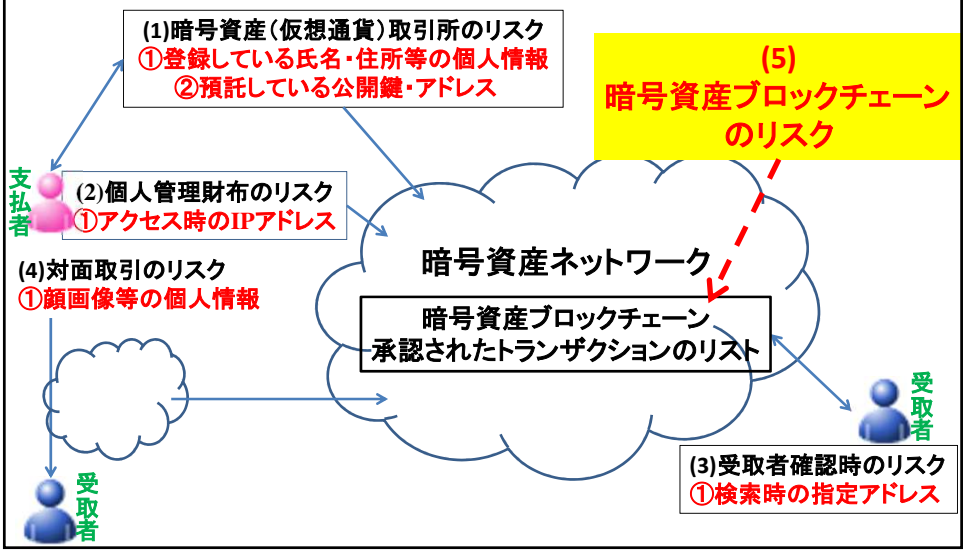
2019年10月10日現在

出典：All Cryptocurrencies　https://coinmarketcap.com/all/views/all/

（2）匿名性に関するリスク

 5

暗号資産システムにおける匿名性に関するリスク



（2）匿名性に関するリスク

 6

トランザクションの構成（匿名性に関連する情報のみ）

入力関連情報		出力関連情報	
入力項目1	使用する資産の指定（提供者のアドレス、金額等が指定されている位置）	出力項目1	受取者の指定（受取者のアドレス等）
	指定資産の使用権の証明（公開鍵、署名等）		提供額の指定（金額等）
入力項目2	使用する資産の指定	出力項目2	受取者の指定
	指定資産の使用権の証明		提供額の指定
.....		.....	
入力項目n	使用する資産の指定	出力項目m	受取者の指定
	指定資産の使用権の証明		提供額の指定

（2）匿名性に関するリスク

暗号資産トランザクションの匿名性に関する要件

要件名称	要件内容
Pseudonymity（利用者識別情報の仮名性）	**利用者識別情報から実在する利用者の実名等の推定が困難であること**
Unlinkability（利用者識別情報間の非連結性）	**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**
Untraceability between Transaction（トランザクション間の暗号資産/利用者の非追跡性）	**受取時の暗号資産と提供に使用する暗号資産との対応の推定が困難であること**
Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）	**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こと**
Concealment of 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**

（3）匿名化プロトコル

匿名暗号資産ブロックチェーンの主要な匿名化プロトコル

匿名化プロトコル	構成要素技術	採用している主要な匿名暗号資産
CryptoNote	リング署名，ワンタイムアドレス，鍵イメージ	Monero，Bytecoin，Electroneum，DigitalNote
Zerocash	ゼロ知識証明zk-SNARKs	Zcash，Komodo，Ethereum（Zcoin，PIVX）
Mimblewimble	コンフィデンシャルトランザクション，CoinJoin	Grin，BEAM
（その他）	Verge（TOR/I2P，Wraith）、Enigma（sMPC）	

5分■

（4）Monero

 9

Moneroトランザクションを構成する情報

（RCTTypeSimpleの匿名性に関連する情報のみ）

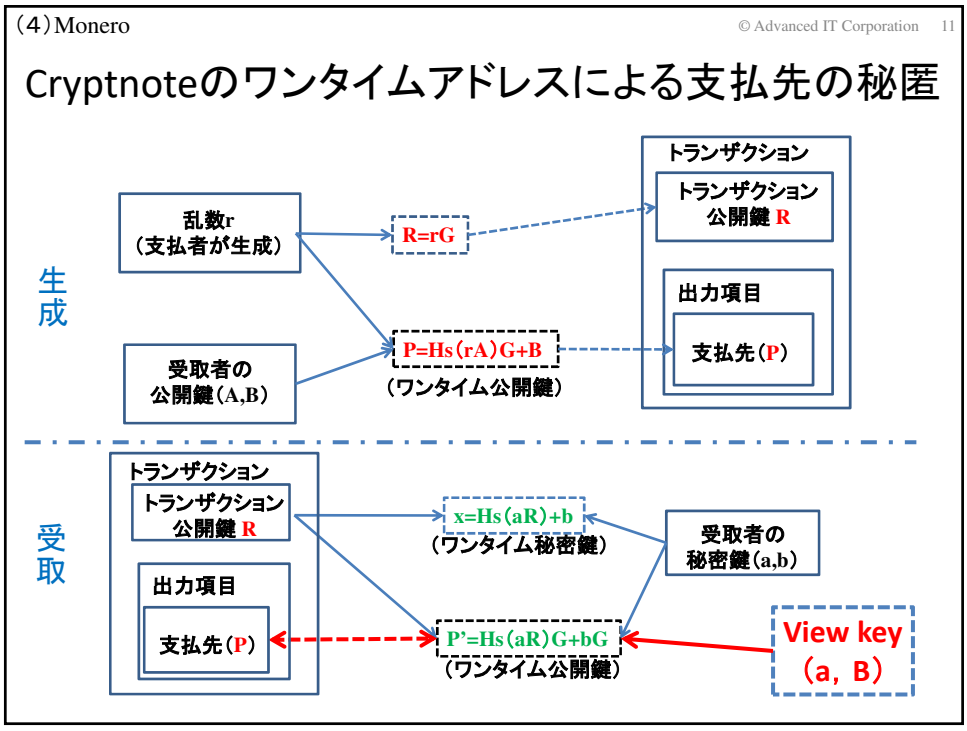
入力関連情報		出力関連情報	
入力項目1	使用する資産の金額指定（通常、0）	出力項目1	受取者の指定（受取者のワンタイムステルスアドレス）
	使用する資産候補の指定（各入力項目とも同じ数の候補）		提供額の指定（金額を乱数でマスクしたペダーセンコミットメント）
入力項目2	使用する資産の金額指定	出力項目2	受取者の指定
	使用する資産候補の指定		提供額の指定
.....		.....	
入力項目n	使用する資産の金額指定	出力項目m	受取者の指定
	使用する資産候補の指定		提供額の指定
入力・出力項目関連情報			
トランザクションパブリックキー（受取者のワンタイムステルスアドレス生成に使用した秘密鍵（乱数）に対応する公開鍵）			
入力項目1の情報	ワンタイムリング署名（使用資産の特定の困難化、）	鍵イメージ（2重使用のチェックに使用）	
.....			
入力項目nの情報	ワンタイムリング署名	鍵イメージ	

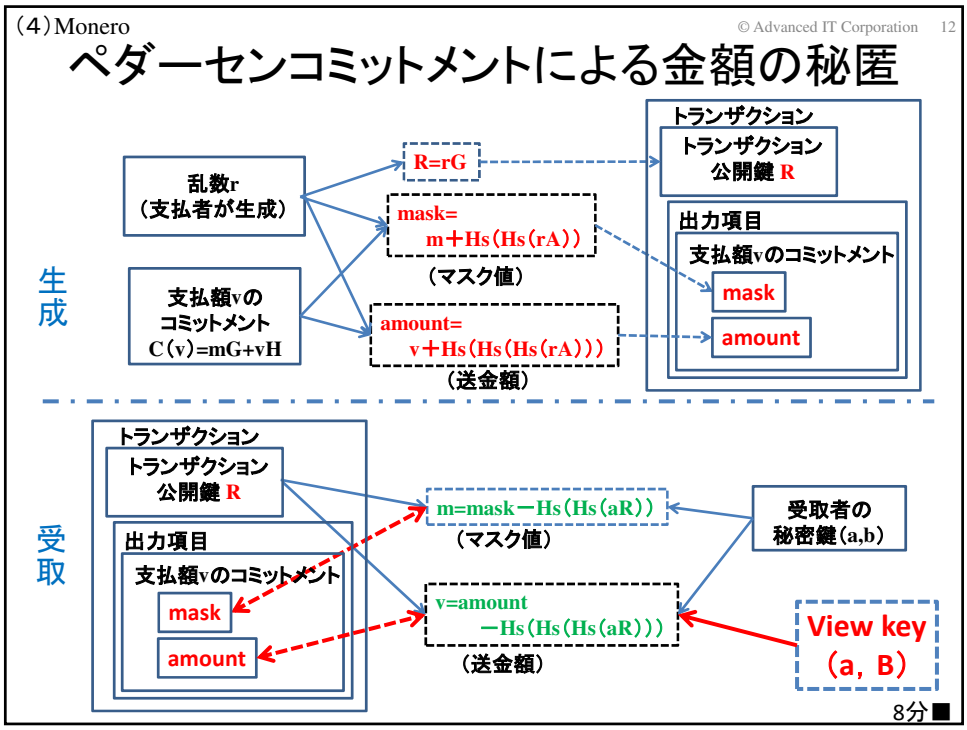
（4）Monero

 10

Moneroブロックチェーンの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity（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を使用しない
Unlinkability（利用者識別情報間の非連結性）	○	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（ワンタイムアドレス）を生成し使用する
Untraceability between Transaction（トランザクション間の暗号資産/利用者の非追跡性）	△	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（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）
Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）	△	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 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（RCTTypeSimple）


(4)Monero
© Advanced IT Corporation 11
Cryptnoteのワンタイムアドレスによる支払先の秘匿
生成
乱数r
(支払者が生成)
R=rG
トランザクション
トランザクション
公開鍵 R
出力項目
支払先(P)
受取者の
公開鍵(A,B)
P=Hs(rA)G+B
(ワンタイム公開鍵)
受取
トランザクション
トランザクション
公開鍵 R
出力項目
支払先(P)
x=Hs(aR)+b
(ワンタイム秘密鍵)
受取者の
秘密鍵(a,b)
P'=Hs(aR)G+bG
(ワンタイム公開鍵)
View key
(a, B)


(4)Monero
© Advanced IT Corporation 12
ペダーセンコミットメントによる金額の秘匿
生成
乱数r
(支払者が生成)
支払額vの
コミットメント
C(v)=mG+vH
R=rG
mask=
m+Hs(Hs(rA))
(マスク値)
amount=
v+Hs(Hs(Hs(rA)))
(送金額)
トランザクション
トランザクション
公開鍵 R
出力項目
支払額vのコミットメント
mask
amount
受取
トランザクション
トランザクション
公開鍵 R
出力項目
支払額vのコミットメント
mask
amount
m=mask−Hs(Hs(aR))
(マスク値)
v=amount
−Hs(Hs(Hs(aR)))
(送金額)
受取者の
秘密鍵(a,b)
View key
(a, B)
8分■

（5）Zcash

 13

Zcash（Sapling）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）

トランザクションに関する情報	
資産のバランス	Saplingによる使用資産額と提供資産額の差
・・・・・	
使用資産情報	使用資産の数（n）
	使用資産1
	・・・・・
	使用資産n
・・・・・	
提供資産情報	資産提供先の数（m）
	資産提供先1
	・・・・・
	資産提供先m
・・・・・	
トランザクションの署名	A signature on the SIGHASH transaction hash, to be verifed as specifed in § 5.4.6.2 ‘Binding Signature’ on p.63.

資産の移転を示すノートに対するコミットメント（note commitment）

資産の2重使用のチェックに使用されるヌリファイア（nullifier）

（5）Zcash

 14

Zcash（Sapling）トランザクションの使用資産情報

使用資産情報（1・・n）	
使用資産額に対するコミットメント	使用する資産（入力ノート：$(d, pk_d, v^{old}, rcm^{old})$）で指定されている金額に対するバリューコミットメント：cv^{old}
使用資産内容に対するコミットメント	使用する資産（入力ノート）で指定されている内容に対するノートコミットメントcm^{old}が含まれるツリーのルート：rt
使用資産内容に対するユニークなコード	使用する資産の2重使用の検査に使用するユニークなコード（ヌリファイア）：nf^{old}
使用資産の使用権を示すのに使用される公開鍵	使用する資産の使用権を示す秘密鍵askをランダマイズし生成した秘密鍵rskに対応する公開鍵：rk
使用資産の使用権の証明	cv^{old}、rt、cm^{old}、nf^{old}、rk、および使用する資産（入力ノート）で指定されている受取者を示すワンタイム公開鍵pk_d、の正当性を示す証明
使用資産情報への署名	rskによる署名（署名検証により、使用権を示す秘密鍵askの所有を証明）

（5）Zcash

 15

Zcash（Sapling）トランザクションの提供資産情報

提供資産情報（1・・m）	
提供資産額に対するコミットメント	提供する資産（出力ノート：$(d, pk_d, v^{new}, rcm^{new})$）で指定されている金額に対するバリューコミットメント：cv^{new}
提供資産内容に対するコミットメント	提供する資産（出力ノート）で指定されている内容に対するノートコミットメントcm^{new}の位置：cm_u
提供資産内容暗号化時の暗号鍵生成に使用される公開鍵	提供資産内容（出力ノート）の暗号化のために生成された秘密鍵eskに対応する公開鍵：epk
暗号化された提供資産内容	受取者を示すワンタイム公開鍵pk_dおよびesk、epk等から生成した暗号鍵K^{enc}により暗号化された提供資産内容（出力ノートのテキスト）：C^{enc}
暗号化された提供資産内容の復号を可能にする情報	cv^{new}、cm_u、cm^{new}、提供資産内容の復号に使用する公開鍵epk等からランダムに生成される暗号鍵ockにより暗号化されたpk_dおよびesk
提供資産情報の正当性の証明	ノートコミットメント、バリューコミットメント、暗号化された提供資産内容（出力ノートのテキスト）の復号に使用する公開鍵epk等の正当性を示す証明

（5）Zcash

 16

Zcash（Sapling）ブロックチェーンの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity（利用者識別情報の仮名性）	○	利用者識別情報である秘密鍵Spending Keyの生成には利用者固有の情報を使用しない
Unlinkability（利用者識別情報間の非連結性）	○	Spending Keyから生成される受取参照鍵ivkにより、受け取りの都度生成されるDiversified Transmission Keyから構成されるSapling Shielded Payment Addressをワンタイムの利用者識別情報として使用

（5）Zcash

 17

Zcash（Sapling）ブロックチェーンの匿名性評価

要件名称	評価	評価の根拠
Untraceability between Transaction（トランザクション間の暗号資産/利用者の非追跡性）	○	トランザクションで使用する暗号資産は暗号化された状態で指定されるため、受取時の暗号資産の受取者と使用する暗号資産の提供者との対応の特定は困難
Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）	○	トランザクションで使用する暗号資産は暗号化された状態で指定されるため、提供者と受取者の対応の特定は困難
Concealment of Amount（移転資産額の秘匿）	○	暗号化およびPedersen Commitmentの利用により、提供額・受取額の秘匿が可能

11分■

（6）Grin

 18

Grinブロックを構成する情報

ブロックに関する情報			
カーネルオフセット	トランザクションカーネルオフセットの合計		
入力情報	入力1	使用する出力1 (pedersen commitment)	使用権の証明1 (signature for commitment with blinding factor)
	・・・・・・・・・・・・・・・		
	入力n	使用する出力n	使用権の証明n
出力情報	出力1	出力コミットメント1 (pedersen commitment)	出力の非負の証明1 (range proof of output 1)
	・・・・・・・・・・・・・・・		
	出力m	出力コミットメントm	出力の非負の証明m
トランザクションカーネル情報	カーネル1	カーネルエクセス1 (pedersen commitment)	トランザクション署名1 (signature for transaction with kernel excess)
	・・・・・・・・・・・・・・・		
	カーネルk	カーネルエクセスk	トランザクション署名k

（6）Grin

Grinブロックチェーンの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity（利用者識別情報の仮名性）	○	固定の利用者識別情報は存在せず、出力ごとに乱数から生成される秘密の情報が利用者を示し、利用者固有の情報を使用しない
Unlinkability（利用者識別情報間の非連結性）	○	利用者を示す秘密の情報は，出力ごとに乱数より生成され毎回異なる
Untraceability between Transaction（トランザクション間の暗号資産/利用者の非追跡性）	×	提供者は受け取った資産を提供資産としてそのまま指定するため、受取資産と提供資産の対応は公開されることになる
Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）	△	提供者と受取者の対応の特定を困難にするため，CoinJoinの仕組みによりブロック内のトランザクションを統合している
Concealment of Amount（移転資産額の秘匿）	○	Pedersen Commitmentにより，個々の資産額は秘匿されている

14分■

（7）比較評価

匿名性に関する比較

要件名称	Monero（RCTTypeSimple）	Zcash（Sapling）	Grin
Pseudonymity（利用者識別情報の仮名性）	○	○	○
Unlinkability（利用者識別情報間の非連結性）	○	○	○
Untraceability between Transaction（トランザクション間の暗号資産/利用者の非追跡性）	△	○	×
Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）	△	○	△
Concealment of Amount（移転資産額の秘匿）	○	○	○

（8）おわりに

 21

特定・追跡性について

利用者が第三者へ提供する情報により、一定範囲のトランザクションの利用者の受取資産・提供資産を把握できる仕組みが存在するかどうか（第三者による未使用資産の流用（使用）のリスクが発生しない仕組み）

	利用者の協力の元	利用者の協力無し
Monero（Sapling）	○（View Key）	×
Zcash（RCTTypeSimple）	○（Full Viewing Key）	×
Grin	×	×

16分

（7）比較評価

 22

おわりに

①匿名暗号資産ブロックチェーンの匿名性に関して

Monero（RCTTypeSimple）、Zcash（Sapling）、Grin
のブロックチェーンは高い匿名性

Zcash（Sapling）が最も匿名性が高く、
Monero（RCTTypeSimple）、Grinの順に高い匿名性

匿名暗号資産システムとしての匿名性は別途評価要

②匿名暗号資産ブロックチェーンの特定・追跡性に関して

Monero（RCTTypeSimple）、Zcash（Sapling）には、
利用者が資産の不正使用を防ぎつつ、
暗号資産の提供・受取状況の監査を可能とする仕組みが
一部用意されているが、Grinには全く用意されていない

③安心・安全な暗号資産ブロックチェーンの要件

利用者の匿名性の保証と、
必要な場合はしかるべき組織による特定・追跡性の保証が必要

終