SCIS2019　4E2-1　ブロックチェーン(5)　2019年1月25日

仮想通貨の匿名性の現状と課題

（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）仮想通貨の概況 ✔

仮想通貨一覧 [2]

2019年1月18日現在2112通貨
（資産総額 122.94 Bドル）

世界の貨幣・紙幣発行量推移 [4]
2013年　5Tドル（5Bドル）
2015年　7.6Tドル（173Bドル）
注：（、）内は仮想通貨時価総額推移

（参考 [4]）
世界の金保有総量約18万トン
現時点の時価総額は、約7Tドル

順位	名称	記号	時価総額
1	Bitcoin	BTC	$64.32 B
2	XRP	XRP	$13.52 B
3	Ethereum	ETH	$12.92 B
4	Bitcoin Cash	BCH	$2.30 B
5	EOS	EOS	$2.28 B
6	Stellar	XLM	$2.08 B
7	Tether	USDT	$2.04 B
8	Litecoin	LTC	$1.91 B
9	TRON	TRX	$1.69 B
10	Bitcoin SV	BSV	$1.37 B
11	Cardano	ADA	$1.17 B
12	IOTA	MIOTA	$875.06 M
13	Binance Coin	BNB	$829.36 M
14	Monero	XMR	$763.85 M
15	Dash	DASH	$620.95 M
16	NEM	XEM	$515.42 M
17	NEO	NEO	$510.78 M
18	Ethereum Classic	ETC	$486.80 M
19	Maker	MKR	$335.89 M
20	USD Coin	USDC	$323.35 M

仮想通貨　時価総額ベスト20 （2019年1月18日現在）

 2

（1）仮想通貨の概況 ✔

主要な匿名仮想通貨23通貨 [3]
時価総額 1.55 Bドル（約1696億円）
（2019年1月18日現在）

順位	名称	記号	時価総額
14	Monero	XMR	$763.85 M
21	Zcash	ZEC	$310.98 M
40	Bytecoin	BCN	$119.05 M
48	Verge	XVG	$103.66 M
70	Electroneum	ETN	$50.65 M
75	PIVX	PIVX	$44.42 M
95	Zcoin	XZC	$34.66 M
215	NavCoin	NAV	$10.91 M
288	DigitalNote	XDN	$7.13 M
317	CloakCoin	CLOAK	$6.14 M

匿名仮想通貨 時価総額ベスト10 （2019年1月18日現在） [2]

（1）仮想通貨の概況 ✔

主要な匿名仮想通貨の
匿名化技術・仕組みおよび秘匿対象

匿名仮想通貨名称	主要な技術・仕組み	利用者の秘匿	支払額の秘匿
Monero[5]	リング署名、リングCT、Kovri、ワンタイムアドレス（CryptoNoteプロトコル）	○	○
Zcash[6]	zk-SNARKプロトコル（Zerocashプロトコル）	○	○
Bytecoin[7]	ワンタイムアドレス、ワンタイムリング署名（CryptoNoteプロトコル）	○	×
Verge[8]	ステルスアドレス（Wraithプロトコル）、TorやI2P	○	×
Electroneum[9]	ワンタイムアドレス、ワンタイムリング署名（CryptoNoteプロトコル）	○	×

（2）ビットコインシステムにおける匿名性 ✔3分

ビットコインの匿名性の問題

（1）一定レベルの匿名性（公開鍵、ビットコインアドレス）
➔匿名性の犯罪での利用が社会問題
（マネーロンダリング、テロリストの資金源、
違法サービスの決済手段）

（2）不十分な匿名性
➔プライバシー・機密情報保護問題
（所有者の支払・受取行動、資産は公開）

仮想通貨における匿名性と特定・追跡性の両立の必要性
＜EU第5次マネーロンダリング対策指令[21]（2018年7月9日施行）
“仮想通貨のアドレスとその仮想通貨の所有者のIDを
紐づけられる情報を各国の金融情報機関は得るべき”＞

（2）ビットコインシステムにおける匿名性 ✔

ビットコインシステムにおける匿名性に対するリスク一覧と対策例

(1)仮想通貨取引所のリスク➔取引所の守秘義務/セキュリティ対策

(2)取引所管理ウォレットのリスク➔公開鍵/アドレスをクライアント側

(3)対面取引のリスク➔支払の都度、アドレスを変更し利用

(4)ビットコインブロックチェーンのリスク
➔格納情報の匿名性を高める仕組み

(5)ブロックチェーン検索時のリスク➔ブルームフィルタ使用時の工夫
（偽陽性発生確率の増大を覚悟し、適合対象を拡大）

(6)ビットコインネットワークアクセス時のリスク➔Tor等の利用

ビットコイントランザクションに含まれる匿名性に関連する情報

入力欄		出力欄	
入力項目1	使用する資金の指定(1)	出力項目1	支払先(受取者)の指定(3)
	指定資金の使用権の証明(2)		支払額の指定(4)
入力項目2	使用する資金の指定	出力項目2	支払先(受取者)の指定
	指定資金の使用権の証明		支払額の指定
.....		.....	
入力項目n	使用する資金の指定	出力項目m	支払先(受取者)の指定
	指定資金の使用権の証明		支払額の指定

(1) 使用する資金

トランザクションIDとその出力欄の何番目の出力項目を資金として使用するかを指定

(出力項目には、支払先(受取者)のビットコインアドレスおよび支払額が指定されている)

(2) 指定資金の使用権証明

原資として指定された資金の使用権を保有していることを示す情報を指定

(ビットコインアドレス生成の元になった公開鍵を指定すると共に、対応する秘密鍵によるトランザクションへの署名を指定する)

(3) 支払先(受取者)

受取者のビットコインアドレスを指定

(4) 支払額

支払額を指定

ビットコインブロックチェーンの匿名性に関する要件を三つに整理

（1）ビットコインアドレス/公開鍵の匿名性の確保

（2）支払者・受取者の対応（資金の流れ）の秘匿

（3）支払額（受取額）の秘匿

(1) ビットコインアドレス/公開鍵の匿名性の確保

現状：ブロックチェーン上には、公開鍵、ビットコインアドレスで表現されている膨大な支払記録（トランザクション）が公開

課題：同一の、公開鍵、ビットコインアドレスの利用状況の分析により所有者が推定されるリスク

対策：公開鍵、ビットコインアドレスを使用の都度変更することが望ましい

➔ ワンタイムビットコインアドレス

(2)支払者・受取者の対応（資金の流れ）の秘匿

現状：ブロックチェーン上では、支払者-受取者/受取者-支払者の対応関係が、公開鍵/ビットコインアドレスで表現

課題：資金の流れの追跡・分析により、支払者・受取者（所有者）が推定されるリスク

対策：資金の流れの追跡・分析を困難にすることが望ましい

- ➔ **コインミキシング（支払者➔受取者）**
- ➔ **エスクロー（支払者➔受取者）**
- ➔ **リング署名（受取者➔支払者）**

(3) 支払額（受取額）の秘匿

現状：トランザクションには、支払者−受取者間の支払額が明記

課題：支払額の分析により、支払いの目的や支払者、受取者が推定されるリスク

対策：支払額は秘匿することが望ましい
一方、正しいトランザクションとして承認されるためには、入力金額の合計と出力金額（支払額）の合計の一致をマイナーが確認できる必要がある

- ➔ **コンフィデンシャルトランザクション（CT）**

（4）主要な提案技術・仕組み ✔

(1)ワンタイムビットコインアドレス

＜支払者・受取者のビットコインアドレス/公開鍵の匿名性の確保＞

乱数による鍵生成

受取者は、自分が使用する秘密鍵・公開鍵のペアを多数生成しておき、受取の都度、対応するビットコインアドレスを連絡する方法。

Hierarchy Deterministic (HD) 鍵生成

1つのシードからマスター秘密鍵・公開鍵を生成し、その鍵ペアから順次下位の鍵ペアを生成する仕組みで、受取りの都度、新たな鍵ペアを生成、対応するビットコインアドレスを連絡する方法。

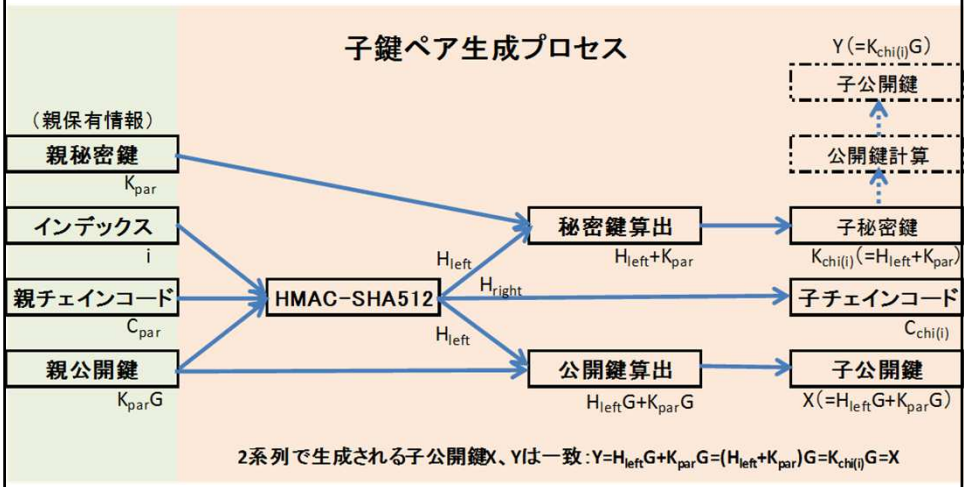
CryptoNoteの鍵生成

支払者は生成した秘密の情報をDH鍵共有の仕組みを利用し受取者へ伝えると共に、その秘密の情報を利用し受取者のワンタイムビットコインアドレスを生成し、支払先に指定する方法。

 13

（4）主要な提案技術・仕組み

Hierarchy Deterministic (HD) 鍵生成



 14

（4）主要な提案技術・仕組み

CryptoNoteの鍵生成

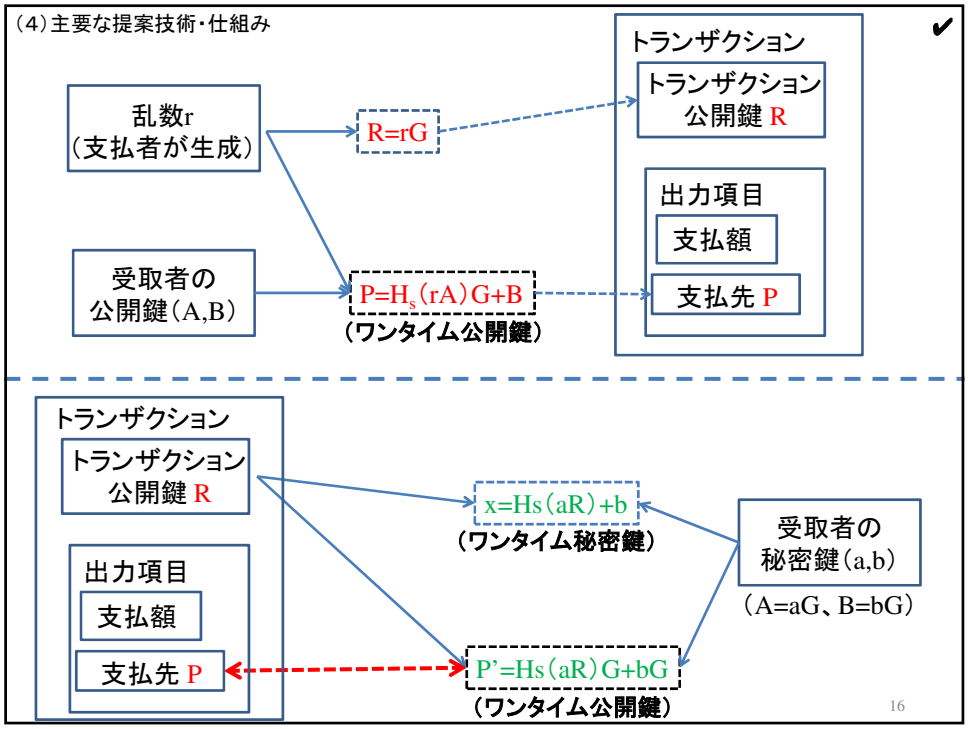
＜前提＞
受取者は2つの秘密鍵a, b、それに対応する公開鍵A(=aG), B(=bG)を保有

＜支払者＞
①トランザクション公開鍵Rを次式で生成し、トランザクションに追加で格納
R=rG　　r：生成した乱数　G：生成元
②受取者のワンタイム公開鍵Pを次の式にて生成し、ビットコインアドレスに変換の上、支払先として格納
$P = H_s(rA)G + B$　　：H_sは暗号ハッシュ関数

＜受取者＞
①次式により、P'を計算する。
$P' = H_s(aR)G + B$
（受取者が正しいa, bを保有していれば、P'=Pとなる。）
②次式により、ワンタイム秘密鍵xを計算する。
$x = H_s(aR) + b$

注1：秘密鍵xを利用し、受取者は使用権を示すことができる。
注2：トラッキング鍵（秘密鍵aと公開鍵B）により、
受取者（秘密鍵aの保有者）であることを確認できる。

 15



現状・課題

①乱数鍵生成およびHD鍵生成は、多くのワレットに実装され利用。

課題は、両方式とも、受取者が生成したワンタイムビットコインアドレスを事前に支払者へ連絡することが必要な点。

②CryptoNote鍵生成は、支払者が受取者の公開鍵を利用し受取者のワンタイムビットコインアドレスを生成する。事前連絡は不要。

課題は、トランザクションに新たにトランザクション公開鍵を格納する必要があり、トランザクションの構造が変わること。（ビットコインネットワーク参加者の合意が得られていない。）

(2)コインミキシング（Coin Mixing）

＜支払者➔受取者の対応（資金の流れ）の秘匿＞

<u>コインジョイン（CoinJoin）</u>

複数の支払記録（トランザクション）を一つにまとめ、
支払者と受取者の対応の特定を難しくする方法

<u>チャウミアン・コインジョイン（Chaumian CoinJoin）</u>

トランザクションを統合するシステム（タンブラー）に対しても、
支払者と受取者の対応を秘匿にできる仕組み

（4）主要な提案技術・仕組み

Chaumian CoinJoin

①支払者は以下の情報をタンブラーに渡す。
　㋐自分が支払う元となる資産（原資）の所在
　㋑その資産の使用権の証明
　　（公開鍵と対応する秘密鍵による署名）
　㋒支払額と暗号化された支払先（受取者）のアドレス
②タンブラーは、
　有効なトランザクションを構成することを確認後、
　暗号化された受取者のアドレスにブラインド署名を付与し、
　支払額と共に支払者に返す。
③支払者は、
　受取者のアドレスをタンブラーの署名付きのまま復号し、
　支払額と共に、受取者に渡す。

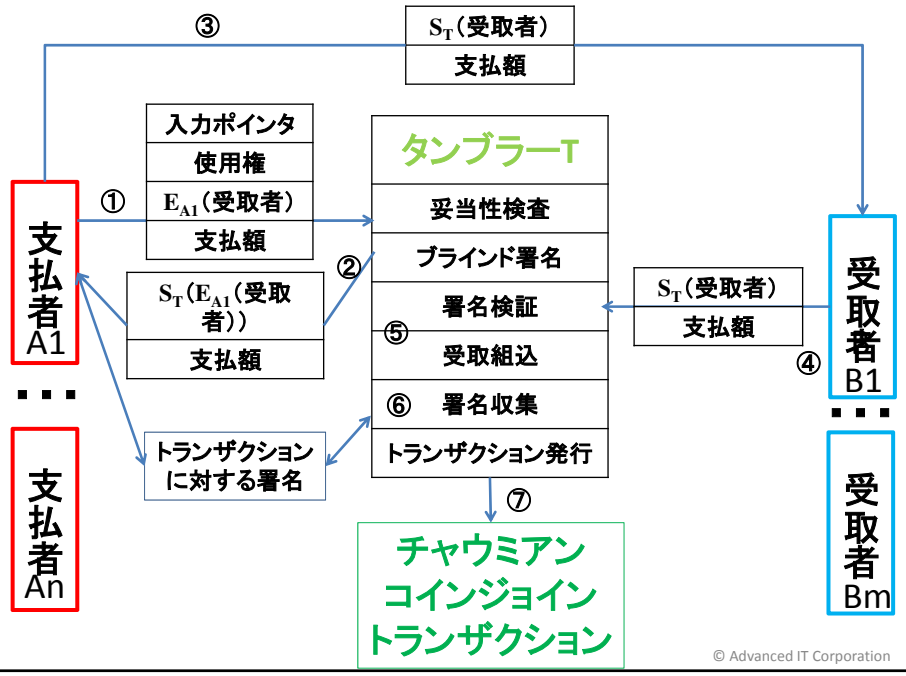
 19

（4）主要な提案技術・仕組み

④受取者は、
　復号されたタンブラーの署名付き受取者アドレスと
　受取額をタンブラーへ渡す。
⑤タンブラーは、
　受取者のアドレスにタンブラーが付与した
　　署名が付与されていることを確認し、
　受取額（支払額）が同一の出力項目の支払先として組み込む。
⑥タンブラーは、
　出力項目に格納すべき支払先（受取者）の
　　アドレス、支払額が集まったら、
　統合したコインジョイントランザクションを作成する。
⑦タンブラーは、
　コインジョイントランザクションに支払者全員の署名を求め、
　署名済みの有効なトランザクションをブロードキャストする。

 20

（4）主要な提案技術・仕組み ✔



 21

（4）主要な提案技術・仕組み ✔

現状・課題

①ビットコインのためのミキシングサービス/システムは、
多数存在（オフチェーンでのサービス）

②コインジョインの課題は次の2つ。
入力項目・出力項目の金額の対応から、
支払者と受取者の対応が推定されるリスク
コインジョインシステム/サービス事業者には、
支払者と受取者の対応を隠ぺいできないリスク

③チャウミアンコインジョインの課題は、
入力項目・出力項目の金額の対応から、
支払者と受取者の対応が推定されるリスク

 22

（4）主要な提案技術・仕組み

ビットコインミキシング方法の比較（例）

比　較　項　目	
Correctness	正しく機能するための仕組み
Anonymity	匿名性のレベル
Deniability	ミキシング参加の否認可能性
Scalability	ユーザ数に応じたオーバヘッド
Cost-efficiency	ミキシングコスト＋トランザクションコスト
Applicability & Usability	ビットコインへの適用容易性

Approach	Correctness	Anonymity			Deniability	Scalability	Costs	Applic.
1st *Generation* [9, 13]	None	0	$> n - c$	$>> n$	✓	$> 1000s$	Mix + 2 TX	✓
Mixcoin [15]	Accountability	0	$> n - c$	$>> n$	✓	$> 1000s$	Mix + 2 TX	✓
Blindcoin [56]	Accountability	n	$n - c$	n	I	$> 1000s$	Mix + 4 TX	(✓)
CoinJoin [40]	Group TX	0	$n - c$	n	✗	$\sim 10s - 100s$	1 TX	✓
CoinShuffle [52]	Group TX	n	$n - c$	n	✗	$\sim 100s$	1 TX	✓
SMC [51, 60]	Group TX	n	$n - c$	n	✗	-	1 TX	✗
ZeroCoin [5, 22, 44]	ZKPs	All ZeroCoin users			✓	-	2 TX	✗
CoinParty	2/3 honest	n	$> n - c$	$>> n$	✓	$\sim 100s - 1000s$	2 TX	✓

“Secure and anonymous decentralized Bitcoin mixing”（2018年4月）

（4）主要な提案技術・仕組み ✔

(3)エスクロー（Escrow）

＜支払者➔受取者の対応（資金の流れ）の秘匿＞

支払者と受取者の間にエスクロー（第三者・仲介者・サービス）が入り、その対応関係の特定を難しくする仕組み

<u>TumbleBit（[8]）エスクローシステム</u>

信頼できないタンブラーを利用しつつも、
支払者・受取者の対応をタンブラーに暴露される心配も無く、
ビットコインがタンブラーに盗まれることも無く、
またタンブラーに勝手な支払を発生されることも無いこと
が保証された仕組み

（4）主要な提案技術・仕組み

TumbleBit

＜預託フェーズ＞

①支払者(A)と受取者(B)の間で、タンブラー(T)の利用に関し合意を得る。（TはRSA暗号の公開鍵(e, N) および対応する秘密鍵dを保有）

②BはTとのチャネルを開設する。Tは、TとBの両者の署名が付与されたトランザクション(TX)で1BTCを受け取れる2-of-2エスクロートランザクションTX_{escr}(T, B)をブロードキャストし、Tは1BTCを預託する。

③AはTとのチャネルを開設する。Aは、AとTの両者の署名が付与されたTXで1BTCを受け取れる2-of-2のTX_{escr}(A,T)をブロードキャストしブロックチェーンに登録、Aは1BTCを預託する。

④Bは、Tとの間で実行される暗号プロトコル(PPP: Puzzle Promise Protocol)を通じ、Tよりパズルz (= ε^e mod N)と共に、キャッシュアウトトランザクションTX_{cash}(T,B)に対するTの署名σを暗号化したc (= $Enc_{\varepsilon}(\sigma)$)を得る。

（4）主要な提案技術・仕組み

＜支払フェーズ＞

①Bは、Tから得たパズルzにブラインディングファクタrを付けz' (= $r^e z$)に変換し、Aへ伝える。

②Aは、Tにz' (= $r^e\varepsilon^e = (r\varepsilon)^e$)の答えε' (= $(Z')^d = (r\varepsilon)^{ed} = r\varepsilon$)を依頼する。Tは、Aへz'の答えε'を伝える。

③Aは、ε'がz'の正しい答えであることを確認した上で、Bへε'を伝えると共に、TX_{cash}(A,T)を作成し署名の上、Tへ渡す。

＜受取フェーズ＞

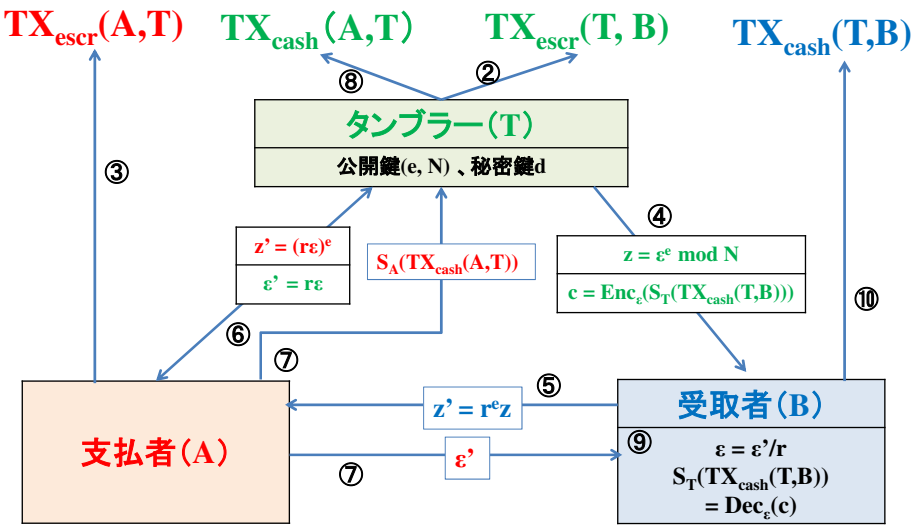
①Tは、TX_{cash}（A,T）に署名し、ブロックチェーン上にブロードキャストし、1BTCを得る。

②Bは、Aから得たパズルz'の答えからパズルzの答えε (= ε'/r)を得る。

③Bはεを利用したcの復号(σ = $Dec_{\varepsilon}(c)$)によりTX_{cash}(T,B)に対するTの署名σを得て、TX_{cash}(T,B)を完成させブロードキャストし、Tから1BTCを得る

（4）主要な提案技術・仕組み ✔

一定の支払額に対応したTumbleBit



（4）主要な提案技術・仕組み ✔

現状・課題

①エスクローの利用は、一般に支払者によるエスクローへの支払い、エスクローによる受取者への支払いの、2つのトランザクションが発行される（TumbleBitの場合は、4つのトランザクション）

②支払額を均一にする等、金額からエスクローを介した支払者と受取者の対応が推定できないような工夫が必要

③Stratis（マイクロソフトがサポートする仮想通貨）上にTumbleBitが実装され、ビットコインの匿名取引を実現

 ✔

(4)リング署名

＜受取者➔支払者の対応（資金の流れ）の秘匿＞

原資として使用する資金の候補を複数指定し、原資候補の全ての受取者の公開鍵および真の受取者（今回の支払者）の秘密鍵による署名を利用することによって、その中の誰が対応する秘密鍵を使用し署名を作成したかを困難にすることにより、その受取者とそれを使用する支払者との対応を困難にする仕組み

<u>CryptoNoteワンタイムリング署名</u>

CryptoNoteのワンタイムリング署名

＜諸元生成フェーズ＞

秘密鍵x、公開鍵P_s（= xG）およびもう一つの公開鍵I（= $xH_p(P_s)$：鍵イメージ）を生成する。なお、H_pはハッシュ値をx座標とする楕円曲線上の点を返す。

＜署名付与フェーズ＞

①他のユーザn-1人の公開鍵P_i（i=1,…,n、i≠s）の集合をS’、S’にP_sを加えた集合をSとする。

②乱数で{q_i：i=1,…,n}、{w_i：i=1,…,n、i≠s}の値を決め、以下を計算する。

$L_i = q_iG$ if i=s、 $L_i = q_iG+w_iP_I$ if i≠s

$R_i = q_iH_p(P_i)$ if i=s、$R_i = q_iH_p(P_i)+w_iI$ if i≠s

③次式により、Cを得る。

$C = H_s(m,L_1,…,L_n,R_1,…,R_n)$

④次式により、{c_i：i=1,…,n}、{r_i：i=1,…,n}を計算する。

$c_i = w_i$ if i≠s、$c_i = C - (c_1+…+c_{i-1}+c_{i+1}+…+c_n)$ if i=s

$r_i = q_i$ if i≠s、$r_i = q_s-c_sx$ if i=s

⑤署名を σ=$(I,c_1,…,c_n,r_1,…,r_n)$ とする。

（4）主要な提案技術・仕組み

＜署名検証フェーズ＞

メッセージm、公開鍵の集合 S を利用し、署名 σ を検証する。

①i=1,…,nに対し、以下を計算する。

$L_i'=r_iG+c_iP_i$、$R_i'=r_iH_p(P_i)+c_iI$

②C'を次式より得る。

$C'=H_s(m,L_1',\ldots,L_n',R_1',\ldots,R_n')$

③次の式が成立すれば、署名検証は成功となる。

$C'=\Sigma_{i=1}^{n}c_i$

＜リンク確認フェーズ＞

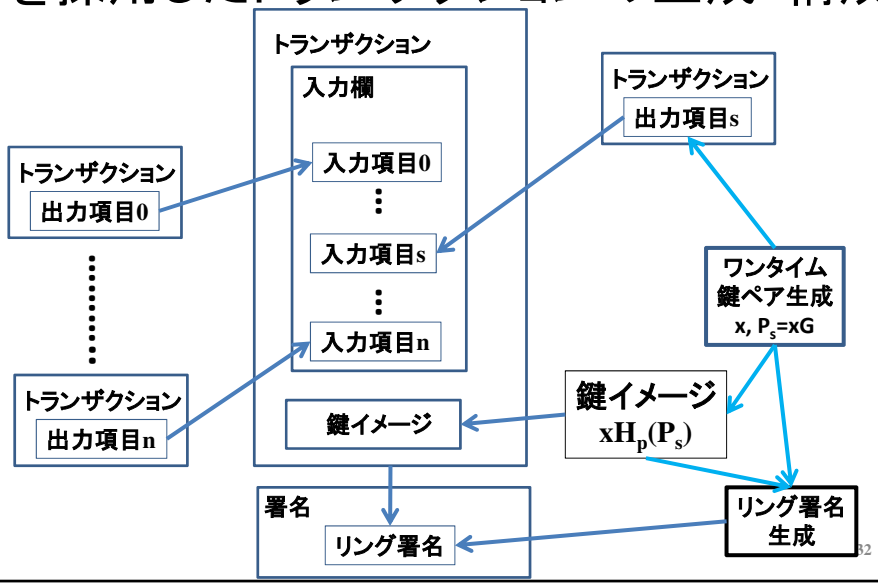
鍵イメージIが過去使われた鍵イメージと一致するかどうか確認する。

過去に使われていた鍵イメージと一致した場合は、指定された原資は2重使用であるため、検証は失敗とする。

 31

（4）主要な提案技術・仕組み

CryptoNoteのワンタイムリング署名を採用したトランザクションの生成・構成



現状・課題

①ビットコインでの利用の動きは無いが、他の仮想通貨の基盤として利用されている。

（Monero、Bytecoin、Electroneum、DigitalNote等）

②課題は、多数のダミーの入力項目が必要で、リング署名の格納に大きなスペースが必要、検証には大きな計算量が必要、という点。

(5)コンフィデンシャルトランザクション（CT）

＜支払額（受取額）の秘匿＞

コンフィデンシャルトランザクションは、Gregory Maxwellが2016年に発表した、入力金額・出力金額の秘匿と、第三者による入力金額の合計と出力金額（支払金額）の合計の一致を検証可能とする仕組み

<u>コンフィデンシャルトランザクション（CT）</u>

次の技術から構成

- **ペダーセンコミットメント**
- **範囲の証明**
- **ボロミアンリング署名**

（4）主要な提案技術・仕組み

ペダーセンコミットメント（PC）

＜前提＞入力金額を$a_i(i=1,\ldots,n)$、出力金額を$b_j(j=1,\ldots,m)$とする。

＜課題＞

入力金額の合計と出力金額の合計の一致$\Sigma_i(a_i)=\Sigma_j(b_j)$を示す必要。

一方、入力金額、出力金額の公開は避けたい。

＜CT＞

j番目の出力金額b_jは、2つの生成元G、Hとブラインディングファクタ（乱数）β_jを利用し、コミットメント　$C^{out}_j = b_jG + \beta_jH$　で表現する。

i番目の入力金額a_iは、同様に2つの生成元G、Hとブラインディングファクタα_iを利用し、、コミットメント　$C^{in}_i = a_iG + \alpha_iH$　で表現されているものとする。

なお、最後の出力金額のブラインディングファクタは $\beta_m = \Sigma_{i=1}^{n}\alpha_i - \Sigma_{j=1}^{m-1}\beta_j$ 。

コミットメントで表現された入力金額の総額と出力金額の総額の差は、

$$\Sigma(a_iG+\alpha_iH) - \Sigma(b_jG + \beta_jH)= (\Sigma a_i - \Sigma b_j)G$$

となり、入力金額の総額と出力金額の総額が一致する場合、0となる。

このようにして、入力金額、出力金額を秘匿したまま、それぞれの和が一致することを示すことができる。

（4）主要な提案技術・仕組み

範囲の証明（Range Proof）

＜課題＞出力金額b_jが適切な範囲内にあるかどうか確認できない

＜Range　Proof＞コミット対象の値が想定範囲内にあることを証明

値域を検証する整数Vを以下のように展開する。

$V=v_0+v_1 2^1+v_2 2^2+\ldots+v_{63}2^{63}$

Vが64ビットで表現できる整数値であることを示すには、$v_o,\ldots,v_{63}$の全てが、0か1であることを示せばよい。

整数Vに対しペダーセンコミットメント$P=VG+\gamma H$を作成（γは乱数）。

各v_iに対してペダーセンコミットメント$P_i=v_i2^iG+\gamma_iH$　を作成（γ_iは乱数）。

最後のγ_{63}のみ、$\gamma_{63} = \gamma - \Sigma_{i=0}^{62}\gamma_i$ とする。（$P=\Sigma_{i=0}^{63}P_i$となることを確認）。

さて、v_iが0場合、公開鍵P_iの秘密鍵はγ_iとなり、v_iが1の場合、公開鍵$P_i - 2^iG$ の秘密鍵がγ_iとなる。

（$v_i=0$の場合：$P_i=\gamma_iH$、$v_i=1$の場合：$P_i - 2^iG = v_i2^iG +\gamma_iH - 2^iG=\gamma_iH$）

v_iが0か1の場合のみ、2つの公開鍵[Pi, $P_i - 2^iG$]のどちらかの公開鍵に対応する秘密鍵がγ_iとなる。このことを利用し、ボロミアンリング署名を作成し、署名検証により、v_iが0か1であることを確認できる。

（4）主要な提案技術・仕組み

ボロミアンリング署名

＜前提＞i番目の集合に属する公開鍵がm_i個とするn個の公開鍵の集合を$\{\{P_{1,1},P_{1,2},\ldots,P_{1,m_1}\},\ldots,\{P_{n,1},P_{n,2},\ldots,P_{n,m_n}\}\}$とする。

＜署名付与＞

① $1 \le i \le n$ の範囲の各iについて以下を実行する。

ア 乱数 $k_i \leftarrow Zq$ を生成する。

イ $e_{i,j_{i*}+1} = H_s(M\|k_iG\|i\|j_{i*})$ を計算する。

なお、j_{i*}はi番目の公開鍵の集合の中で、
秘密鍵が使用された公開鍵のインデックス

ウ $j_{i*}+1 \le j < m_i$の範囲の各jについて以下を実行する。

乱数 $s_{i,j} \leftarrow Zq$ を生成する。

$e_{i,j+1} = H_s(M\|s_{i,j}G - e_{i,j}P_{i,j}\|i\|j)$ を計算する。

② $1 \le i \le n$ の範囲の各iについて、乱数 $s_{i,m_i} \leftarrow Zq$ を生成する。

③ $e_1 = H_s(s_{1,m1}G - e_{1,m1}P_{1,m1} \|\cdots\| s_{n,m_n}G - e_{n,m_n}P_{n,m_n})$ を計算する。

（4）主要な提案技術・仕組み

④ $1 \le i \le n$ の範囲の各iについて以下を実行する。

ア $1 \le j < j_{i*}$ の範囲の各jについて以下を実行する。

乱数 $s_{i,j} \leftarrow Zq$ を生成する。

$e_{i,j+1} = H(M\|s_{i,j}G - e_{i,j}P_{i,j}\|i\|j)$ を計算する。

なお、$e_{i,1}=e_1 \quad 1 \le i \le n$ とする。

イ $s_{i,j_{i*}} = k_i + x_{i,j_{i*}}e_{i,j_{i*}}$ を計算する。

⑤ 署名を$\sigma = \{e_1,\{s_{i,j} : 1 \le i \le n, 1 \le j \le m_i\}\}$ とする。

<署名検証>

① $1 \le i \le n$ 、$1 \le j \le m_i$ について、以下を計算する。

但し、各iについて $e_{i,1}=e_1$ とする。

$R_{i,j+1} = s_{i,j}G - e_{i,j}P_{i,j}$

$e_{i,j+1} = H(M\|R_{i,j+1}\|i\|j)$

② $e^*_1 = H(R_{1,m1}\|\cdots\|R_{n,mn})$ を計算する。

③ ②の計算結果e^*_1が署名σ中のe_1と一致すれば、署名検証に成功。

（4）主要な提案技術・仕組み ✔

現状・課題

①ビットコインのサイドチェーンElements でテスト/評価中。（ビットコインのメインチェーンでのソフトフォークによる実装、という提案もあるが、具体化していない。）

②匿名仮想通貨Moneroでは、リングCTとして実装。

③課題は、コンフィデンシャルトランザクションの範囲の証明（ボロミアンリング署名）の利用には、トランザクションのサイズが巨大化せざるを得ないこと、検証時間がかかること。

➔ BulletProofsプロトコル

各出力金額ごとの範囲の証明を、
全ての出力金額の範囲の証明を一括実施できる方法

➔ 大幅な、トランザクションサイズの削減、検証時間の短縮

（昨年10月18日、MoneroがハードフォークによりBulletProofs導入、トランザクションサイズ80%減、手数料97%減、という報告有）

（4）主要な提案技術・仕組み ✔15分

トランザクションの匿名性強化策として提案されている技術・仕組み

匿名性に関する要件	主要な提案技術・仕組み
ビットコインアドレス/公開鍵の匿名性の確保	(1)ワンタイムビットコインアドレス
支払者・受取者の対応（資金の流れ）の秘匿	(2)コインミキシング（Coin Mixing） (3)エスクロー（Escrow） (4)リング署名
支払額（受取額）の秘匿	(5)コンフィデンシャル トランザクション（CT）

（5）技術・仕組みの実装方式

提案されている匿名性強化のための技術・仕組みの実装方式の分類

（1）メインチェーンでの実装

ビットコインブロックチェーンの仕様変更により実装する方法

ソフトフォーク：ブロックチェーンの拡張性や可変部分を活用

ハードフォーク：ブロックチェーンの基本仕様の変更による拡張

（2）サイドチェーンとしての実装

メインチェーンと関連するブロックチェーンで実装する方法

TumbleBit：Stratisに実装、ビットコインの匿名取引が可能

CT：Elementsに実装、ビットコイン支払金額の秘匿が可能

（3）オフチェーンとしての実装

メインチェーン外で実装する方法

コインミキシングやエスクローの技術・仕組みは

オフチェーン方式で実装

 41

✔

おわりに

①仮想通貨におけるプライバシー保護の観点から、

＊ビットコインブロックチェーンの匿名性に関するリスクの整理

＊匿名性強化のための主要な技術・仕組みの調査・分析・整理

②本研究活動の目標は、

＊プライバシー・機密情報保護の観点からの確実な匿名性の保証と

＊不正・不法な利用者の確実な特定・追跡性の保証を両立する

安心・安全な仮想通貨システムのあるべき姿を整理すること。

③今後、匿名仮想通貨における匿名化技術の調査・分析・整理を進め

＊匿名化技術の整理・分類（体系化）

＊利用者の特定・追跡性機能の匿名化技術への組込み可能性

等を検討したい。

 42

終

ご清聴、ありがとうございました。

