暗号通貨と
ブロックチェーン技術

筑波大学システム情報系 准教授
面 和成
omote@risk.tsukuba.ac.jp

品川フロントビル会議室 B1F
2020年2月12日（水）

本発表の内容

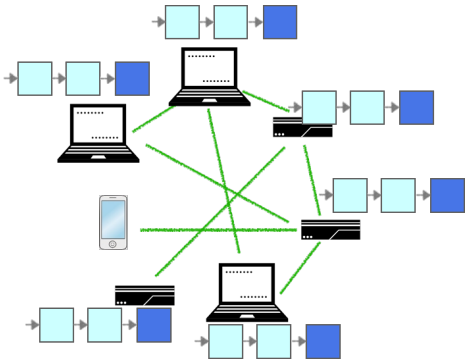
- 暗号通貨の特徴
- 暗号通貨のセキュリティリスク
  - NEM流出事件
  - ブロックチェーンポイズニング攻撃
- 対策に向けての取り組み
  - ウォレットアドレスへの信頼性付与
  - 匿名信頼性付与手法

暗号通貨の特徴

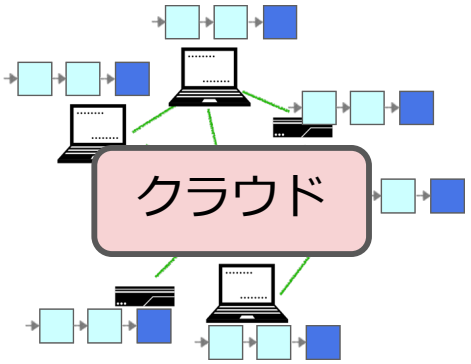
- 銀行を介さない個人間送金が国境を越えて可能
  - 銀行に頼らなくてよい
    - 銀行口座を持たなくても送金が可能
  - 国内では，銀行を介さない個人間送金は別手段で存在（e.g., 楽天キャッシュ）
  - 暗号通貨は個人間送金の世界統一化に向けた1つの解決策
- 管理主体なしに完全性・透明性を保証
  - 暗号技術を用いて取引データの完全性を保証
  - 誰でもアルゴリズムや取引の内容を確認可能
- システム的な単一障害点がない
  - 分散管理されている
    - 世界中のP2Pネットワークで支えられている
  - 部分的にダウンしてもシステムが持続可能

中央集権 vs 非中央集権

- P2Pネットワーク上のブロックチェーン
  - 管理主体がいないという意味で非中央集権化
  - 単一障害点がないという意味で非中央集権化



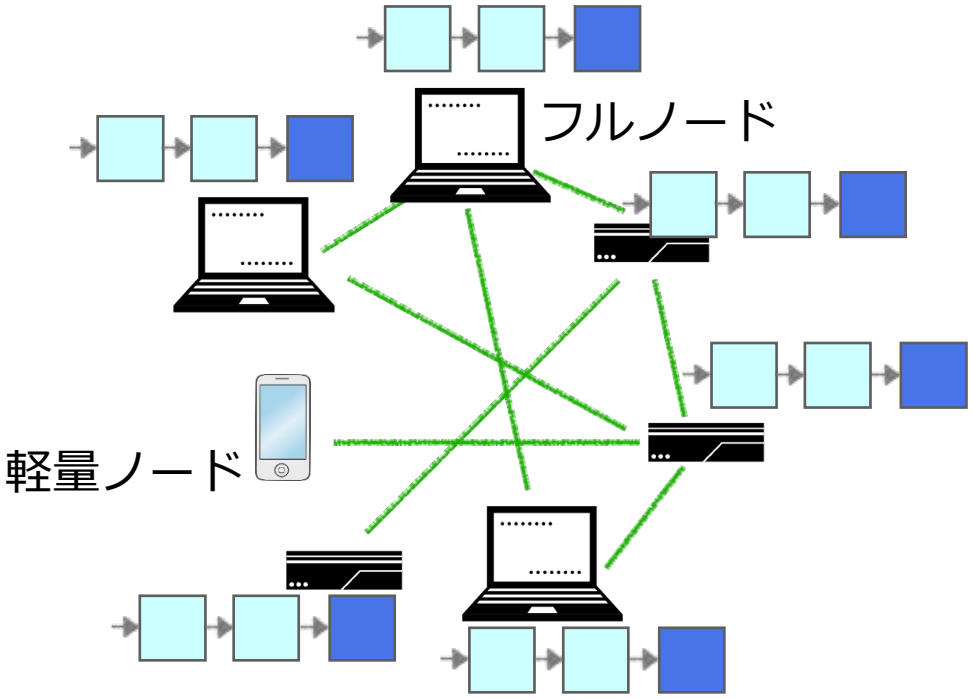
- クラウド上のブロックチェーン
  - 管理主体が存在するという意味で中央集権化
  - 単一障害点がないという意味で非中央集権化



- どちらが良いかは一概には言えない
  - 管理主体を置けない背景の考慮も重要
  - 世界統一化を実現するために管理主体を置けない場合がある

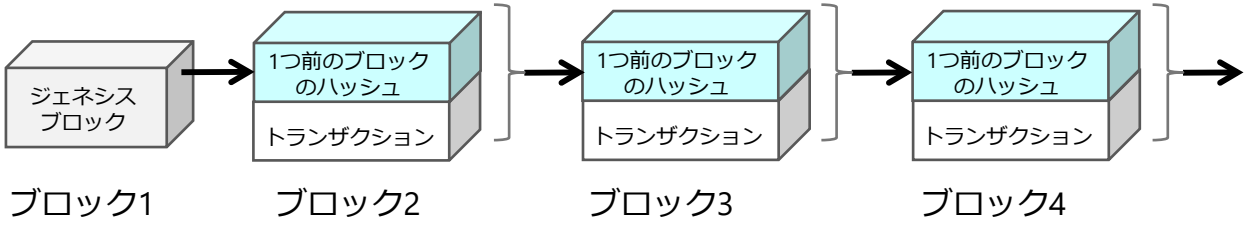
暗号通貨における登場人物

- フルノード
  - ブロックチェーンを持つ
  - ストレージ容量大
  - マイニングも行える
  - サーバ・クラウド的な役割
- 軽量ノード（SPV）
  - ブロックチェーンを持たない（ブロックヘッダのみ）
  - ストレージ容量小
  - プールマイニングが可能
  - クライアント

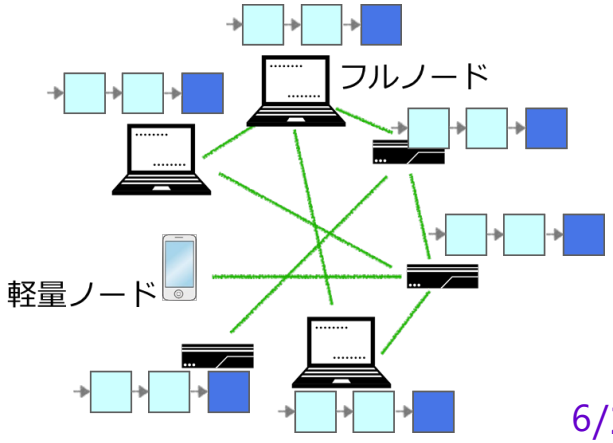


暗号通貨のセキュリティ

- 耐改ざん性
  - 暗号学的ハッシュ関数とディジタル署名の利用
  - ハッシュチェーンによりチェーン途中の改ざんが事実上不可能
  - 欠点：悪意あるデータが格納されると，ハードフォークしない限り格納され続ける

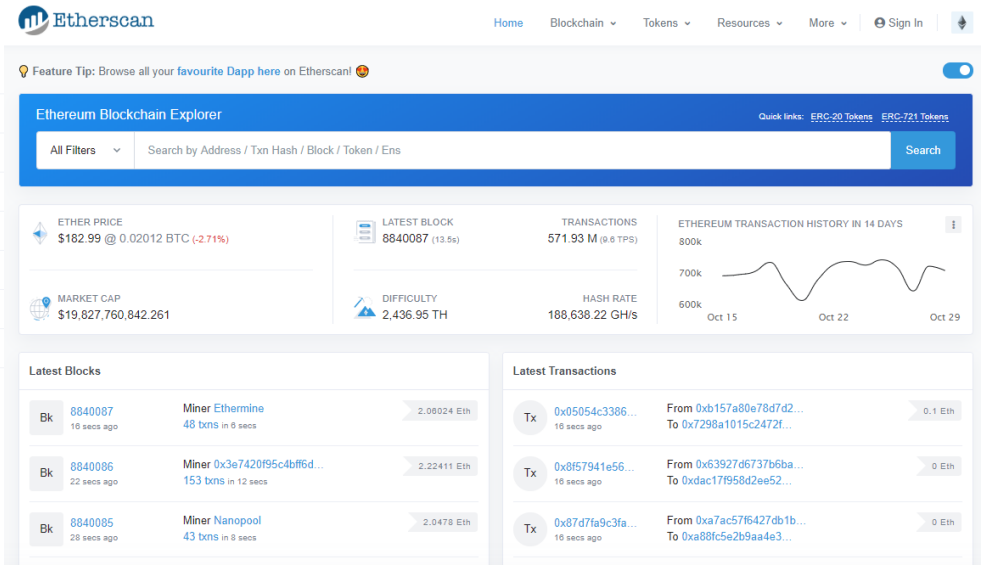


- 高可用性
  - 世界中のフルノードがブロックチェーンのコピーを持つ（多重化）
  - ダウンタイムがゼロに収束する
  - 欠点：停止したくても停止できない



Explorer

https://www.blockchain.com/ja/explorer



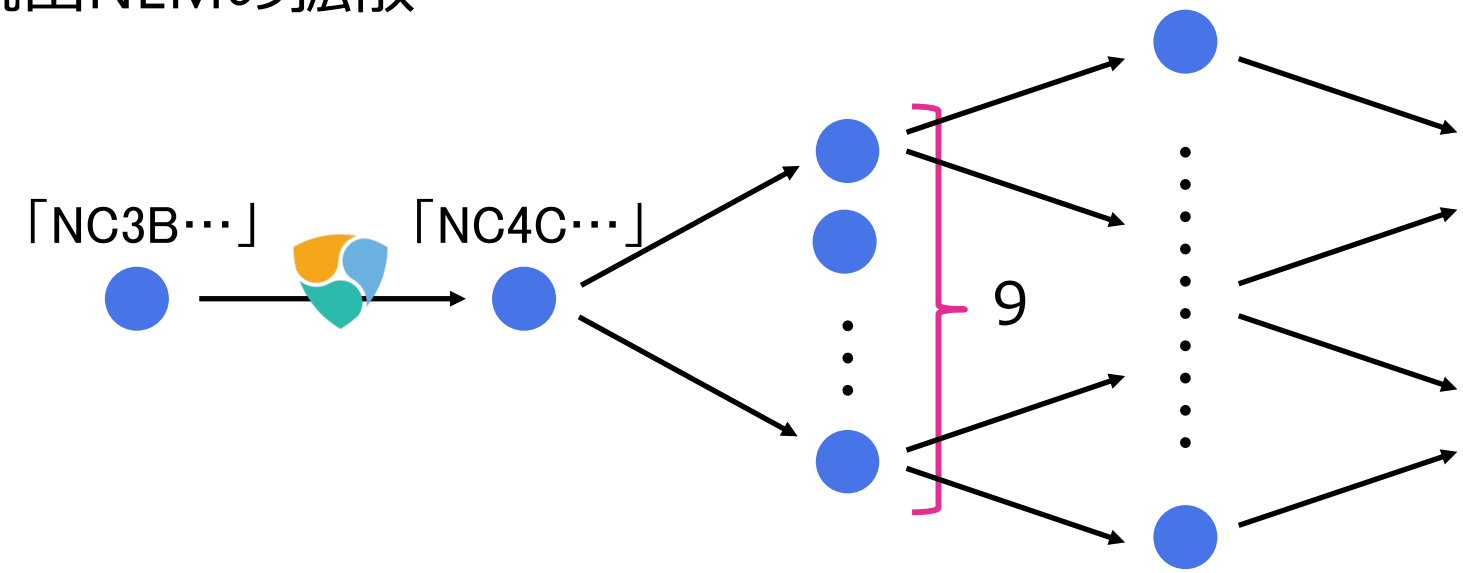
https://etherscan.io/

- ブロックチェーンを持たないユーザにとって便利
- フィルタリングをかけることが可能
- Webサーバの信頼性に依存

暗号通貨のセキュリティリスク

NEM流出事件（1/3）

- 2018年1月26日0時2分頃からコインチェック社のウォレットから顧客のNEM（当時日本円で約580億円）が流出
  - コインチェック社のウォレットアドレス
    - NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ
  - 最初の犯人のウォレットアドレス
    - NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
- 流出NEMの拡散



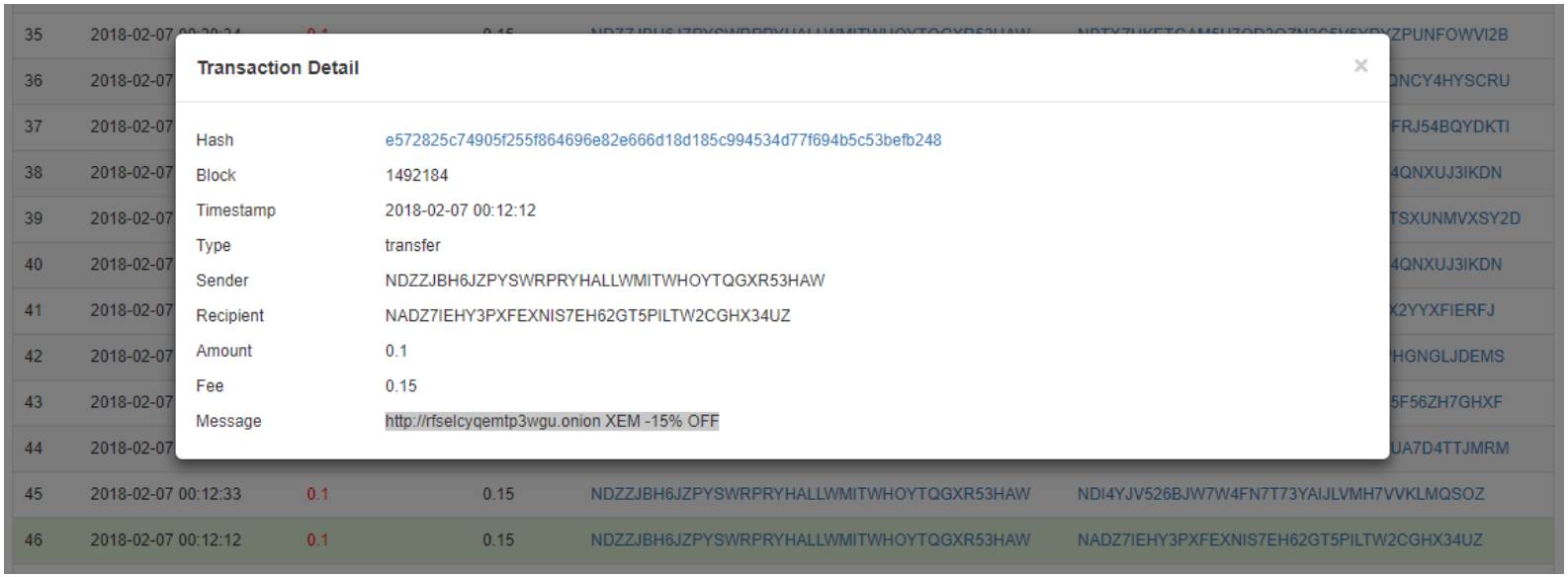
NEM流出事件（2/3）

234	2018-01-26 03:29:54	92,250,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NA6JSWNF24Y7DVIUVPKRNAY7TPOFJJ7G2URL7KU5
235	2018-01-26 03:28:44	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NDDZVF32WB3LWRNG3IVGHCOCAZWENCNRGEZJVCJI
236	2018-01-26 03:18:07	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NB4QJJCLTZWVFWRFBKEMFOONOZFDH3V5IDK3G524
237	2018-01-26 03:14:09	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NDZZJBH6JZPYSWRPRYHALLWMITWHOYTQGXR53HAW
238	2018-01-26 03:02:12	750,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NBKLQYXEIVEEGARYPUM62UJIFHA3Y6R4LAPU6NP4
239	2018-01-26 03:00:33	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NDODXOWEIZGJSMAEURXACF4IEHC2CB7Q6T56V7SQ
240	2018-01-26 02:58:42	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NA7SZ75KF6ZKK267TRKCJDJBWP5JKIC2HA5PXCKW
241	2018-01-26 02:57:24	30,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NCTWFIOOVITRZYSYIGQ3PEI3IMVB25KMED53EWFQ
242	2018-01-26 00:21:14	3,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
243	2018-01-26 00:10:36	20,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
244	2018-01-26 00:09:22	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
245	2018-01-26 00:08:21	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
246	2018-01-26 00:07:04	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
247	2018-01-26 00:06:46	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
248	2018-01-26 00:04:56	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
249	2018-01-26 00:02:13	10	0.05	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG

出典：http://explorer.nemchina.com

NEM流出事件（3/3）

- Hidden Service （ダークウェブ）上に独自の取引所を開設
- 2018年2月7日に，2次送金先のウォレットの1つに対して，「http://rfselcyqemtp3wgu.onion XEM -15% OFF」というメッセージが送信され，割安なレートでNEMとbitcoin, lightcoinを交換することが可能になっていた
- 他の通貨に交換されるとトレースが難しくなる



モザイクについて（1/2）

- モザイク
  - 通貨のようにやりとりが可能なトークン
  - NEM＊XEM（NEMがネームスペース，XEMがモザイク名）
  - XEMはLevy（税金）の設定なし
- 追跡用モザイク
  - mizunashi.coincheck_stolen_funds_do_not_accept_trades＊owner_of_this_account_is_hacker
  - ts＊warning_dont_accept_stolen_funds
  - Levy（税金）の設定あり
    - 誰も持っていない別のモザイクをLevyとして設定
      - mizunashi.coincheck_stolen_funds_do_not_accept_trades＊levy_to_lock_assets
      - ts＊locker_levy
    - Levyを支払えないので追跡用モザイクを送れない
- Levy
  - モザイク送信時に税金のようなものを課す機能
  - モザイク，量，受け取りウォレットアドレスを設定

モザイクについて（2/2）

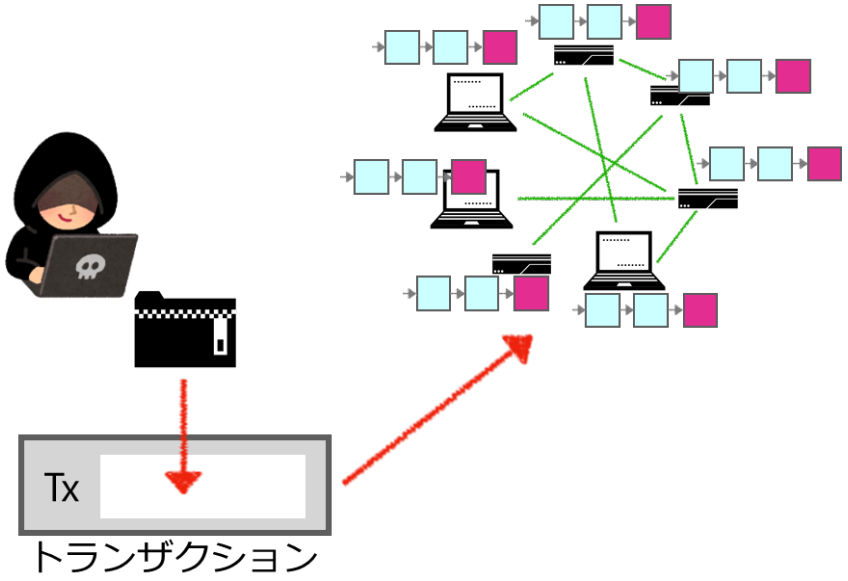
- 「NC4C…」のモザイク付与状況

Transactions | Mosaic Transactions

#	Timestamp	Mosaic	Quantity	Sender	Recipient
1	2018-03-01 16:07:31	ts:warning_dont_accept_stolen_funds	1	NCU63AYO6RS2ISG4UEP5CALTKVQOB4FUTYIYXUAV	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
2	2018-02-05 05:38:04	nem:xem	1.000000	NCVGXTCV7YYGCUTOWRSEALEVHVTDFRJ54BQYDKTI	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
3	2018-01-31 00:10:21	cat_my_boss:nekoboss	11	NBPEASRPODP56JEQYUWY36JK4NOBZGIQ347Y4JD2	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
4	2018-01-29 12:25:14	serendipity:coin	100.000	NCGLWE2SVA5DP2X4TO7JBOM65PRIFZZPSPSHDGU4	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
5	2018-01-28 01:27:18	mm:lektoken	100,000	NBY32IX3KZOPTVVAOVIP5TLWJZDQNTZ5HZ3L3NU3	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
6	2018-01-28 00:21:03	namuyan:faucet	1	NBKCVZ2BU3D5XLUZD4BAI2EVIXE3MRYKEVINPWYQ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
7	2018-01-27 17:24:42	friend.vegetable:carrot	1.00	NCJQZIGJLMVPCOZAUUSI7V7BJ6MOGO2TTZCQFPHC	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
8	2018-01-26 17:23:58	mizunashi.coincheck_stolen_funds_do_not_accept_trades:owner_of_this_account_is_hacker	1	NCVGXTCV7YYGCUTOWRSEALEVHVTDFRJ54BQYDKTI	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG

Bitcoinブロックチェーンへの非金融データの格納

- 複数の非金融データの格納手法が存在
  - OP_RETURN(80B)，Coinbase(100B)（公式な手法）
  - 通常のトランザクション (57.34～96.70KiB)（非公式な手法）
  - 規格外のトランザクション(96.72KiB) （非公式な手法）
- 利点
  - 文書の存在証明
  - ログ等のフォレンジック
- 欠点
  - 著作権侵害，プライバシー侵害
  - マルウェア，違法コンテンツ



[MHHZMHW18] R. Matzutt et al. "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin", FC2018.

Bitcoinブロックチェーン内の汚染データ

- 著作権侵害
  - 書籍，Bitcoin論文，2つのホワイトペーパー，2つの秘密鍵，違法素数
- プログラム
  - （無害な）JavaScript，マルウェアは発見できず
- プライバシー侵害
  - 結婚式の写真，集合写真
  - チャットログ，メール，マネーロンダリングに関するフォーラム投稿
  - 第三者機関からの漏洩
    - 電話番号，住所，銀行口座，パスワードなど
- 政治上のセンシティブなコンテンツ
  - アメリカ外交公電ウィキリークス流出事件のバックアップ

[MHHZMHW18] R. Matzutt et al. "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin", FC2018.

Ethereumブロックチェーンへの非金融データの格納

- extraData領域
  - Ethereumブロックのヘッダに存在する領域
  - マイナーのみがデータを埋め込むことが可能
  - 最大で32B

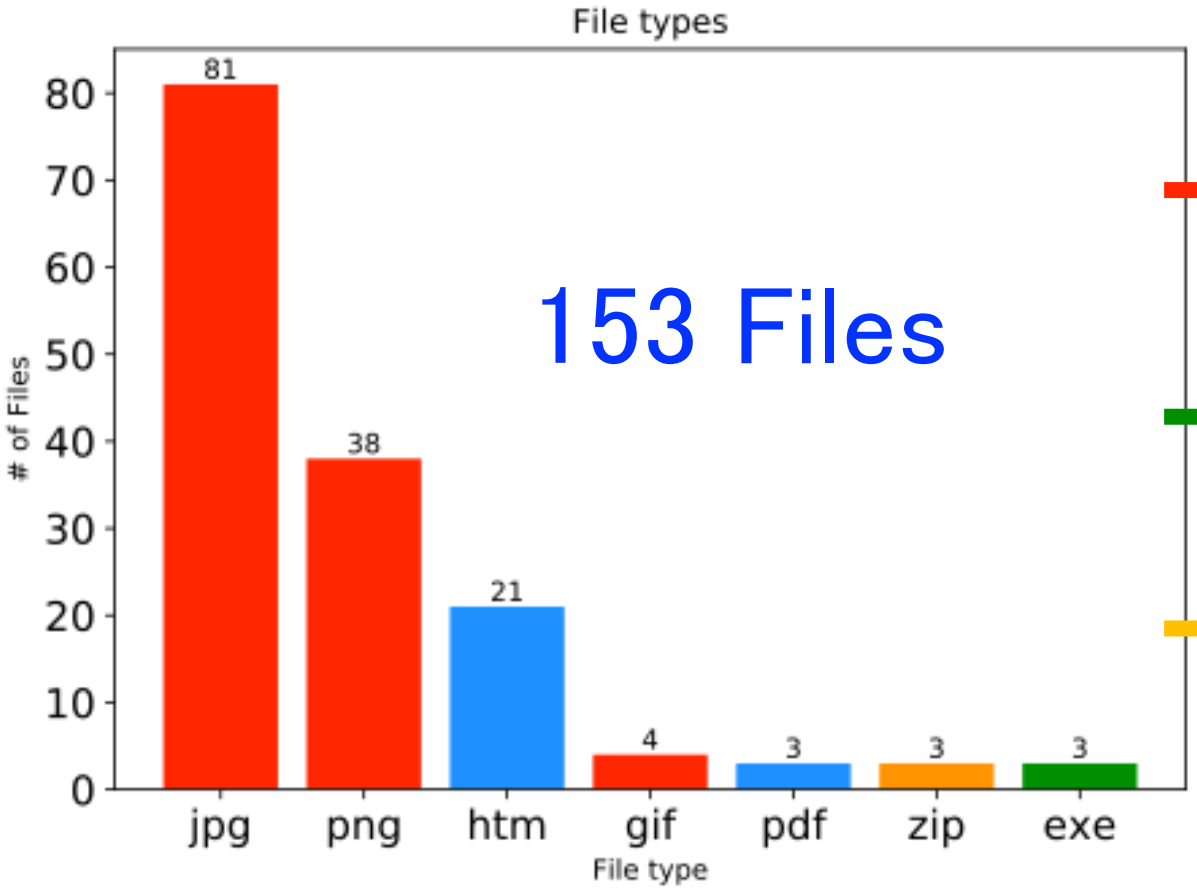
- Init/data領域
  - スマートコントラクトの生成・利用などに使用される領域
  - 理論的には埋め込みサイズに制限はない
  - 実質的には数百kBのデータを一つのトランザクションに埋め込み可能

[SIO19] T. Sato, M. Imamura and K. Omote, “Threat Analysis of Poisoning Attack against Ethereum Blockchain”, WISTP2019.

Ethereumブロックチェーンのデータの分析

- 実際にファイルが埋め込まれているかを確認
- init/data領域の調査方法
  1. Ethereumブロックチェーンからトランザクションを抽出
  2. それぞれのトランザクションのinit/data領域を抽出
  3. ファイルカービングによって，init/data領域に埋め込まれたファイルの有無を確認・ファイルの取り出し
- ファイルカービングの対象としたファイル：
  - jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, html, cpp の18種類

Ethereumブロックチェーンの汚染



画像ファイル（8割）

マルウェア

zipファイル

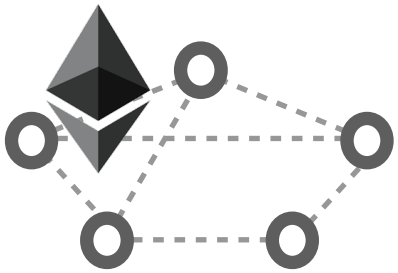
調査期間　2015年7月30日 ~ 2018年11月30日

[SIO19] T. Sato, M. Imamura and K. Omote, “Threat Analysis of Poisoning Attack against Ethereum Blockchain”, WISTP2019.

ブロックチェーン汚染による攻撃の容易性

Ethereumネットワーク

Explorer等Webサイト

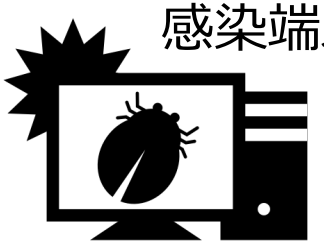


Ethereumネットワーク
から情報取得

METAMASK等

攻撃者

感染端末等



Ethereumネットワークに接続
Ethereumブロックチェーンに情報埋め込み

Explorerに接続し情報を取得

[SIO19] T. Sato, M. Imamura and K. Omote, “Threat Analysis of Poisoning Attack against Ethereum Blockchain”, WISTP2019.

対策に向けての取り組み

アドレスの信頼性問題

- アドレスだけから信頼性を判断するのは難しい
  - ウェブアドレス：フィッシングサイト
  - メールアドレス：偽造されたメールアドレス
  - IPアドレス：偽装された送信元IPアドレス
- 掲載されたウォレットアドレスの信頼性
  - ウェブに掲載されたウォレットアドレス
  - メールに記載のウォレットアドレス

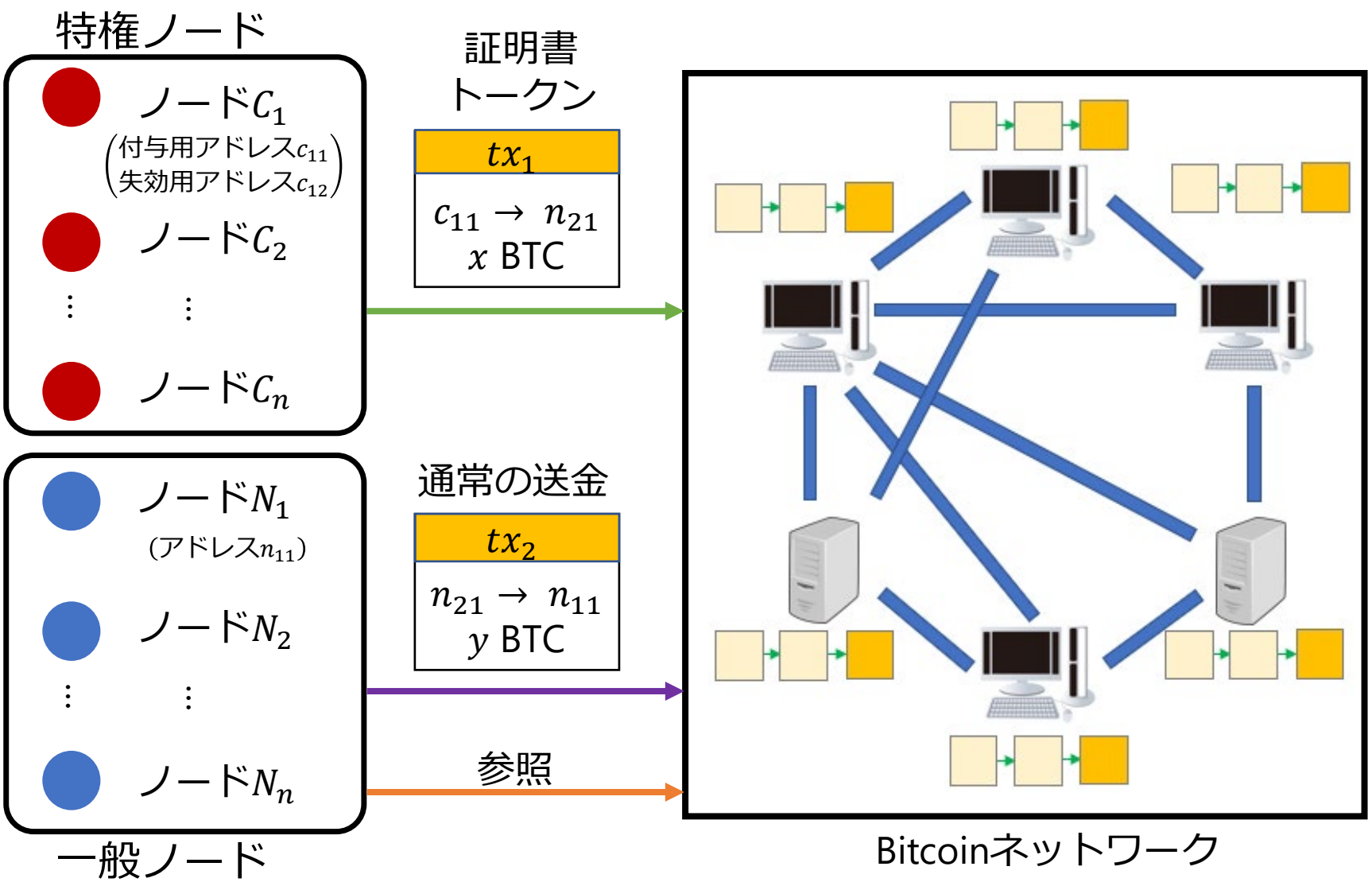
日本赤十字社 Bitcoin募金画面
（出典：https://bitcoindonations.bitflyer.com/#）

ウォレットアドレスへの信頼性付与

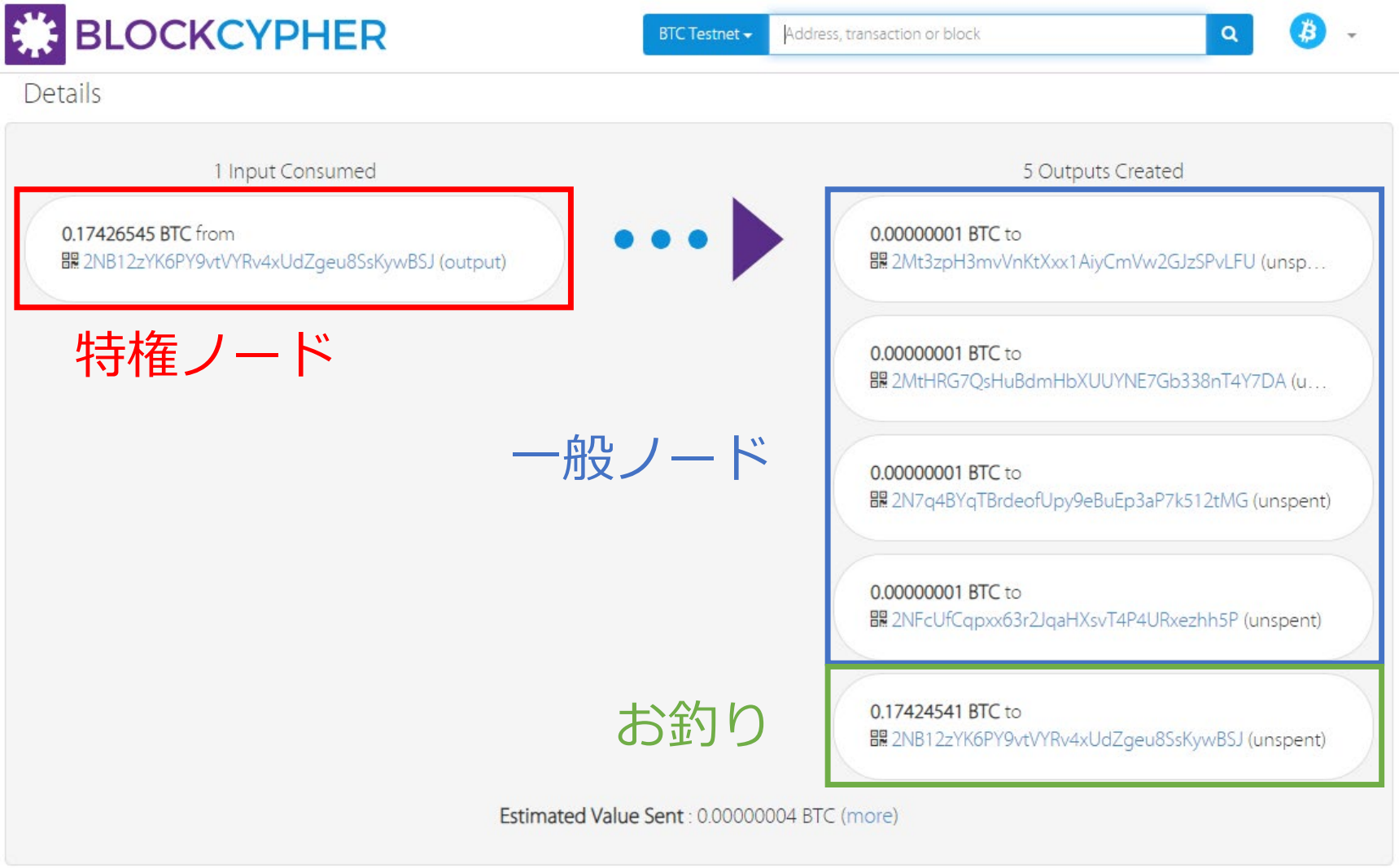
- 暗号通貨のウォレットアドレスに対して信頼性を割り当てる
- 信頼性を割り当てる自明な方法は，第三者機関が公開鍵証明書（クレデンシャル）をウォレットアドレスに割り当てる
  - ブロックチェーンへの非金融データの格納
  - 例えば，EthereumにおけるERC735のClaimを利用した証明書付与など
- 我々は，新たな2つの信頼性付与手法を提案
  - 暗号通貨そのもの（証明書トークン）を利用した簡易的な信頼性付与手法[SSO19]
  - アカウンタブルリング署名を利用した匿名信頼性付与[SEO19, SEO20]

[SSO19] 鈴木, 佐藤, 面,「ビットコインにおけるユーザへの信頼性付与の手法」, ISEC研究会, 2019年7月
[SEO19] 佐藤, 江村, 面,「ブロックチェーンシステムにおける匿名トークン付与に関する一考察」, CSS2019, 2019年10月.
[SEO20] 佐藤, 江村, 面,「ブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価」, SCIS2020, 2020年1月.

暗号通貨そのものを利用した簡易的な信頼性付与手法



Bitcoinアドレスへの信頼性付与について



[SSO19] 鈴木, 佐藤, 面,「ビットコインにおけるユーザへの信頼性付与の手法」, ISEC研究会, 2019年7月

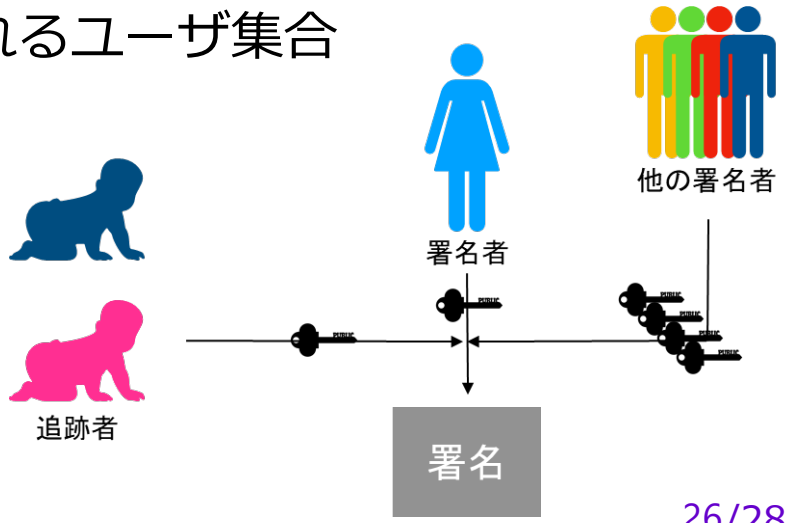
ウォレットアドレスへの信頼性付与手法の問題

- 信頼性付与者のプライバシー
  - 信頼性付与を行う際に付与した者が特定される場合，公正な信頼性付与の妨げになるという問題がある
  - 信頼性付与を目的とした脅迫・危害が加えられる等の可能性

- 信頼性付与者の信頼性
  - 単純に信頼性付与側のプライバシーを守った場合，信頼性付与の公正さが損なわれる
    - 誰によって， どのような基準で信頼性が付与されたか，適切に付与されたかが分からない
  - NEM流出事件では，有志によってモザイク付与が行われたため， どのような基準で付与が行われたのか等の信頼性の面で問題があった

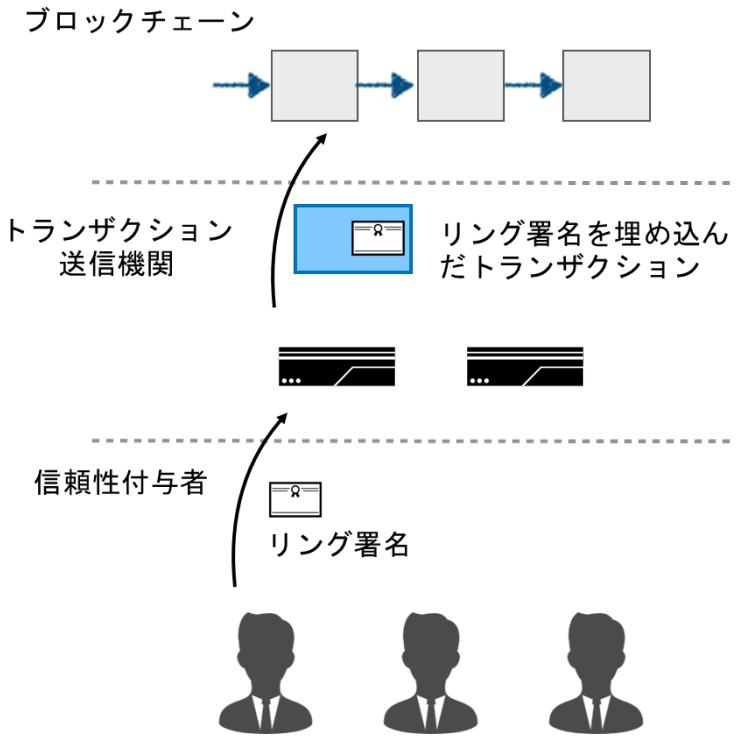
アカウンタブルリング署名

- リング署名とグループ署名の両方の特徴を持つ
  - 署名者が自分で鍵ペアを生成
  - 必要に応じて署名者を追跡できる追跡者が存在
- 署名
  - 署名者は，自身，追跡者，他の署名者の公開鍵集合（リング）を入力として用い，署名者の秘密鍵で署名生成
- 検証
  - 検証者は，署名者がリングで定義されるユーザ集合に含まれることのみ検証可能
- 追跡
  - 指定された追跡者のみが署名者を特定



匿名信頼性付与手法

- ブロックチェーン上で特定のアカウントに信頼性を与える事によって安全な取引を行うための手法
- 従来の手法における下記問題を解決
  - 信頼性付与の信頼性
  - 信頼性付与者のプライバシー
- 提案手法ではアカウンタブルリング署名を用いて，匿名性をもって監査可能な信頼性付与が可能
- トランザクション送信と信頼性付与の権限を分離するためトランザクション送信機関を設置



[SEO19] 佐藤, 江村, 面,「ブロックチェーンシステムにおける匿名トークン付与に関する一考察」, CSS2019, 2019年10月.
[SEO20] 佐藤, 江村, 面,「ブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価」, SCIS2020, 2020年1月.

まとめ

- 暗号通貨の特徴
- 暗号通貨のセキュリティリスク
  - NEM流出事件
  - ブロックチェーンポイズニング攻撃
- 対策に向けての取り組み
  - ウォレットアドレスへの信頼性付与
  - 匿名信頼性付与手法