Bitcoinの技術的課題の整理と議論
2014.6.2

セコム株式会社 IS研究所
暗号・認証基盤グループ
佐藤　雅史

Bitcoinの技術的課題の整理と議論
2014.6.2

日本ネットワークセキュリティ協会
電子署名WG サブリーダー
佐藤　雅史

セコムIS研究所
Intelligent Systems Laboratory

自己紹介

- 佐藤　雅史　（さとう　まさし）
- 普段は主に電子署名屋さんです。
- 標準化とかやっています。
  - JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル
  - JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル
  - ISO 14533-1:2012, Long term signature profiles – Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
  - ISO 14533-2:2012, Long term signature profiles – Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
  - ISO 14533-3 (計画中)
- 主な活動の場
  - JNSA, TBF(Time Business Forum), JIPDEC

ビットコインの特徴（簡単なおさらい）

セコムIS研究所 Intelligent Systems Laboratory

- コイン所有権の移動をトランザクションの履歴で管理する。
  - コインの使用を表明するのに電子署名を用いる。
- トランザクションの存在を証明するためにブロック（台帳のようなもの）を生成しネットワーク参加者で共有する。
  - ブロック生成者は新しいコインや発生した取引手数料を獲得できる（マイニング）。
- コイン発行や使用に関してコントロールする中央の機関は存在しない。

いきなり余談ですが…
（電子署名屋さんぽいことを…）

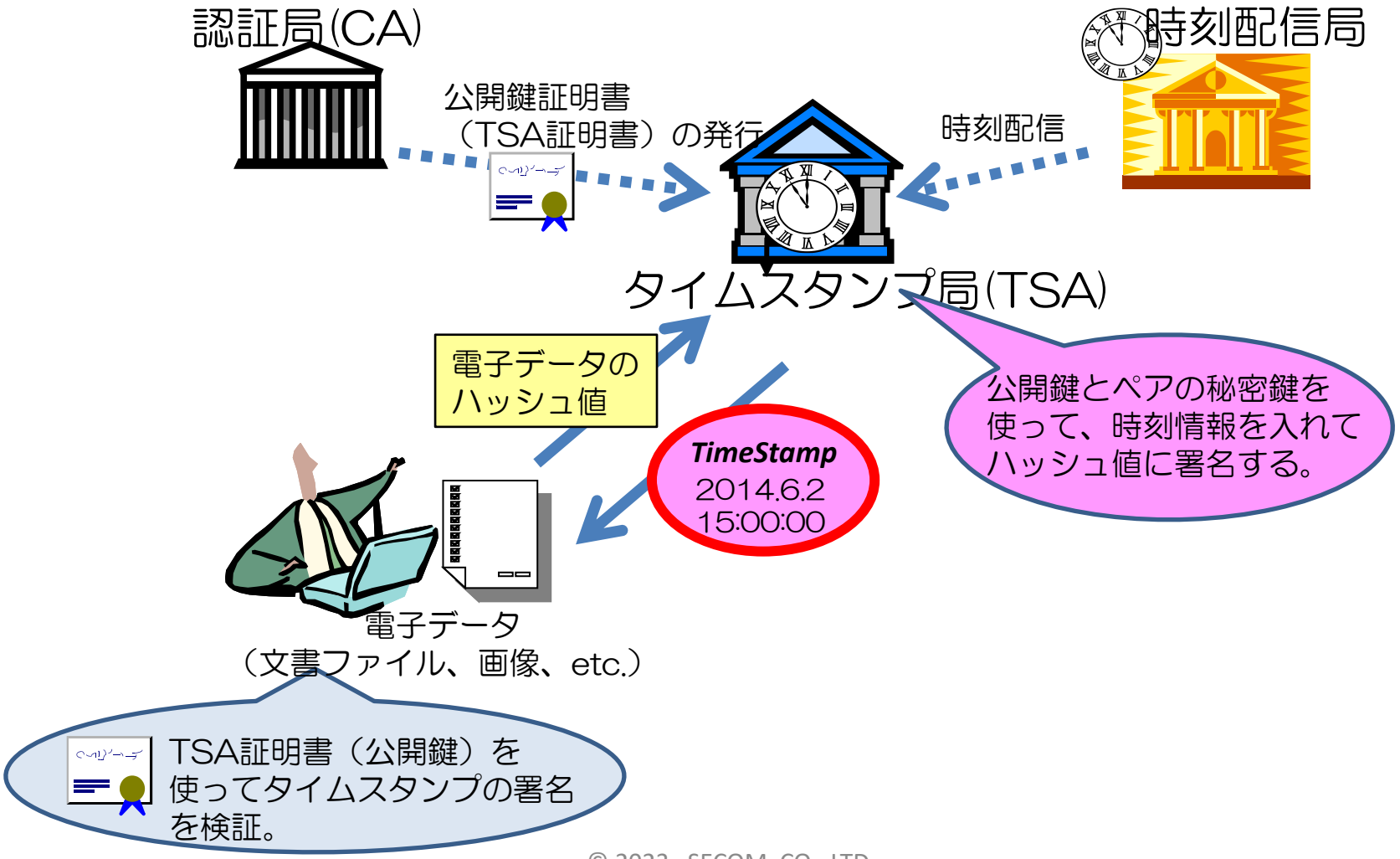
電子署名屋さんから見たビットコイン

- タイムスタンプ
  - 第三者的に証明可能な電子データの存在証明。（ある時間にそのデータが存在した証明）
  - よく電子署名と組み合わせて使われる。
- ビットコインはP2P型のタイムスタンプ

タイムスタンプ技術（１）
～　PKI（公開鍵基盤）方式　～

セコム IS 研究所
Intelligent Systems Laboratory

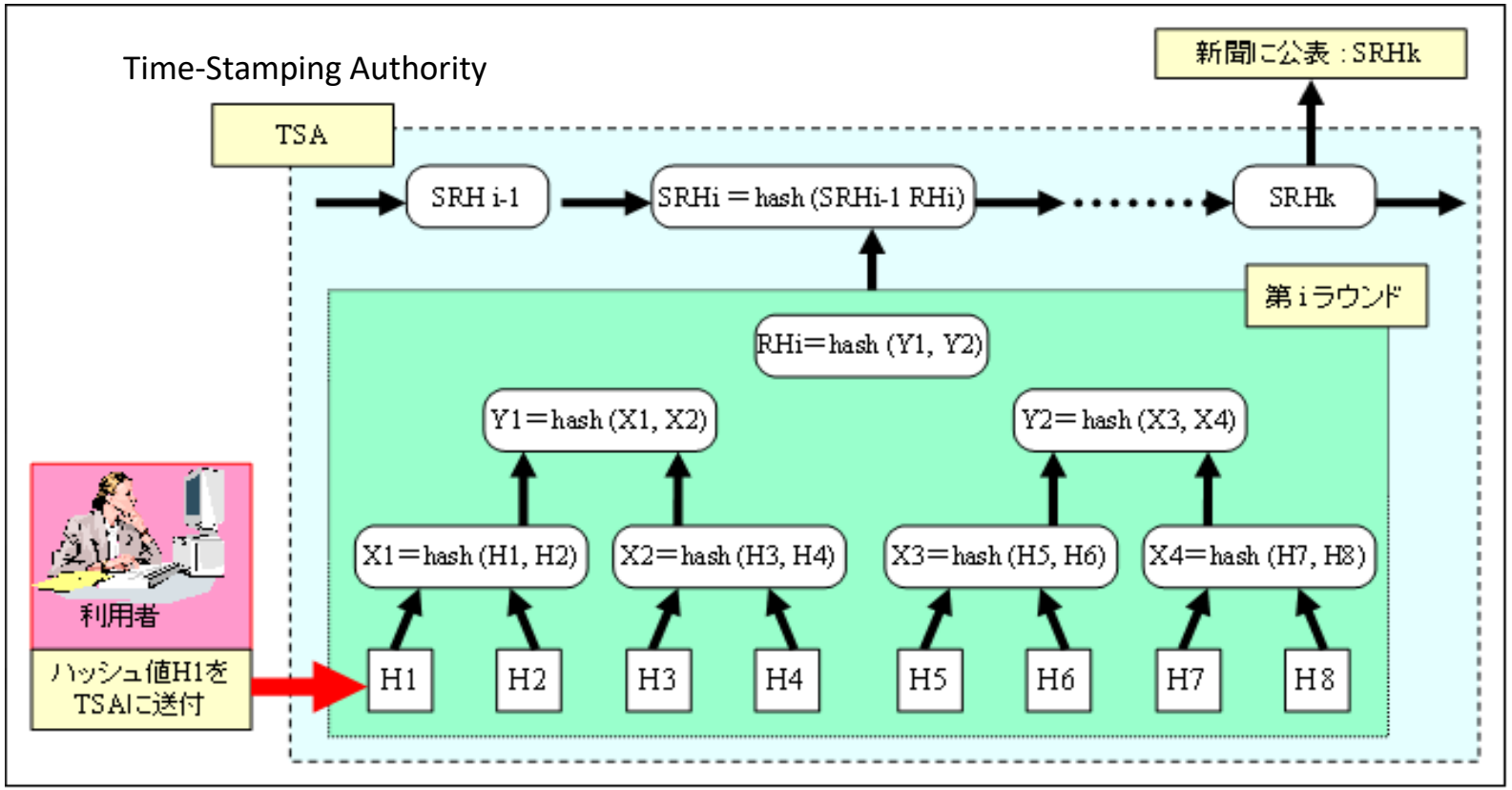
標準規格：RFC 3161, ISO/IEC 18014-2



タイムスタンプ技術（2）
～　リンキング方式　～

セコム IS 研究所
Intelligent Systems Laboratory

標準規格：ISO/IEC 18014-3

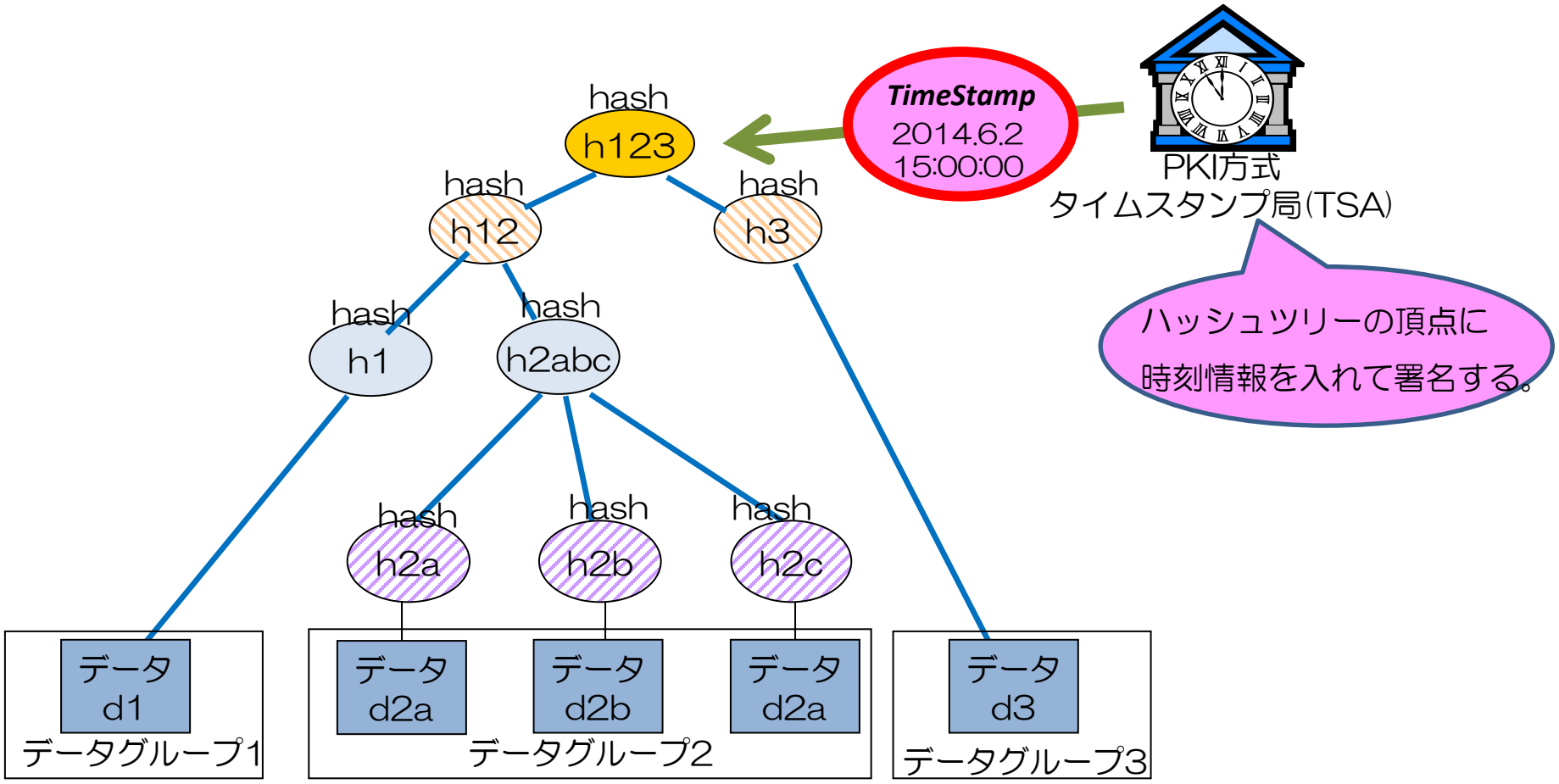


引用元：https://www.ipa.go.jp/security/pki/093.html

ハッシュアルゴリズムが脆弱化しない限り有効。
逆に言えば、ハッシュアルゴリズムの移行が困難。
（ビットコインも同様の問題がある？）

タイムスタンプ技術（３）
～　ERS(Evidence Record Syntax)方式　～

標準規格：RFC 4998, RFC 6283



PKI方式タイムスタンプを用いたリンキングのような仕組み。
ハッシュアルゴリズムの移行ができる。

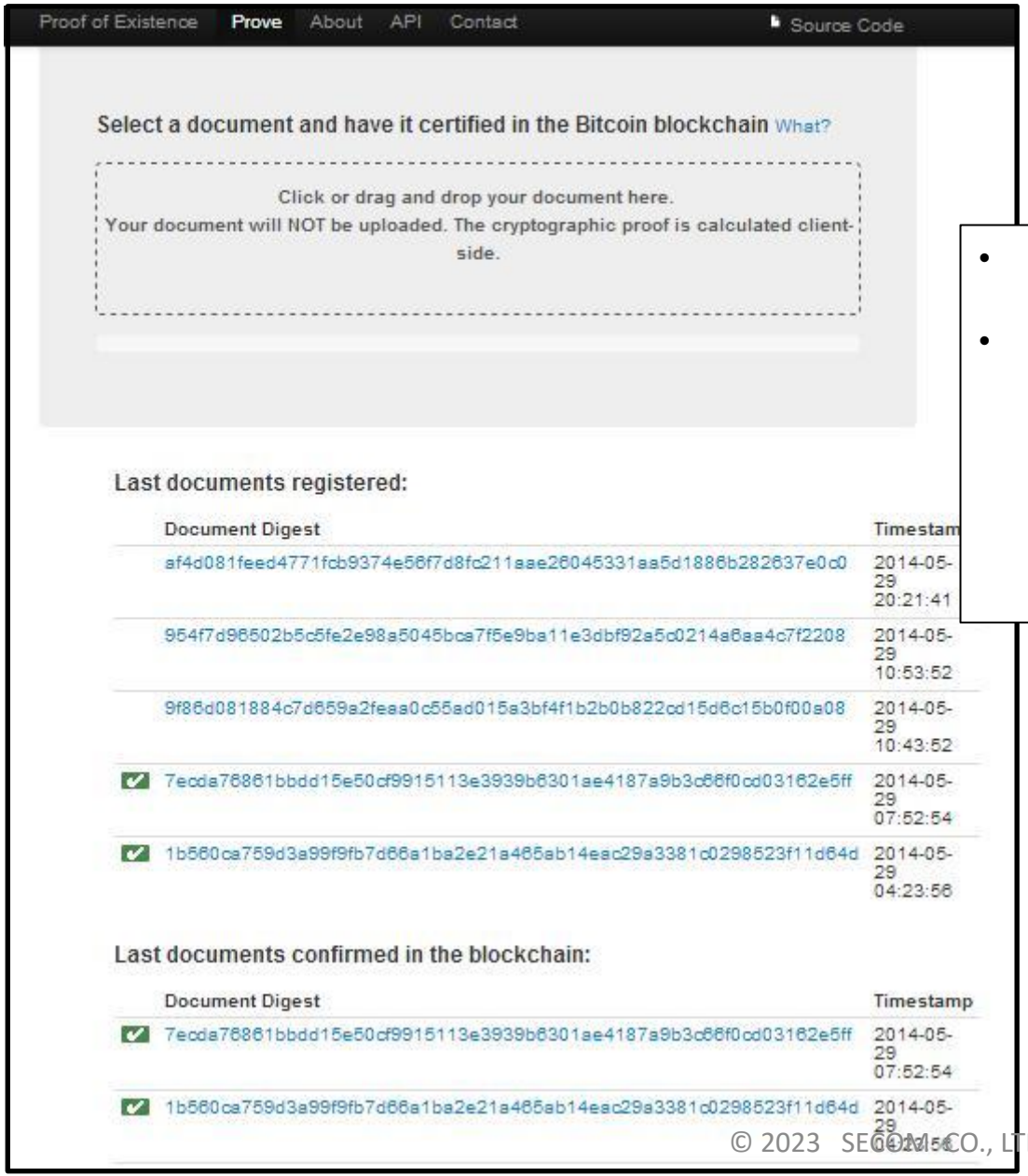
ビットコインのタイムスタンプ

セコムIS研究所
Intelligent Systems Laboratory

	従来のタイムスタンプ	ビットコインのタイムスタンプ
信頼のモデル	信頼できる第三者機関が存在する。	中央の機関は存在しない。多数決による合意。
対象とするデータ	任意の電子データ。（文書、画像データ、ログ等)	ビットコインのトランザクション（基本的には…）。
ビジネスモデル	タイムスタンプ付与者または検証者への課金。	利用者は無料(minerが獲得する発掘コインとTransaction Fee)

ビットコインを用いた存在証明①
～Proof of Existence～

セコムIS研究所
Intelligent Systems Laboratory

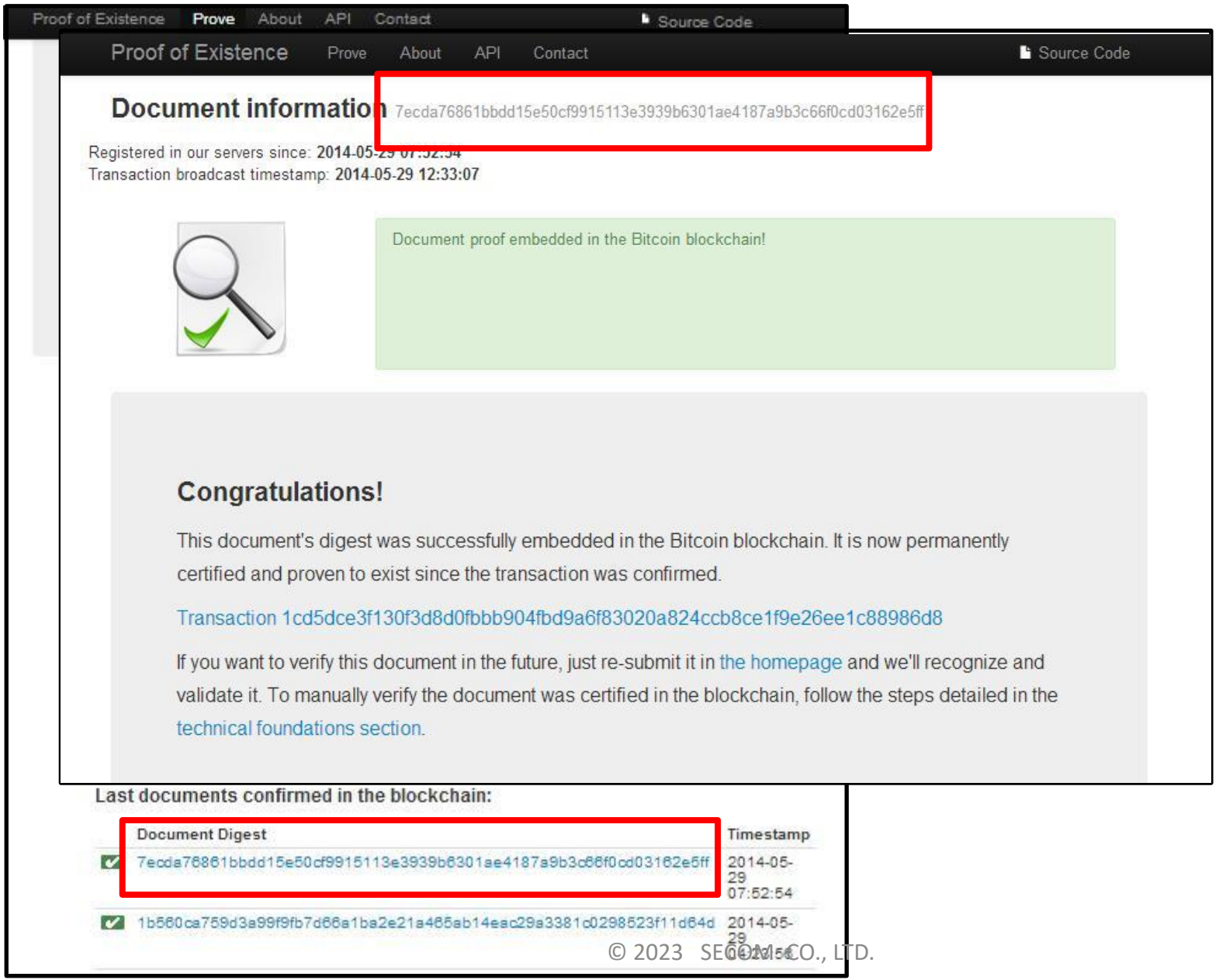


http://www.proofofexistence.com/

- 存在証明したい文書のハッシュ値(SHA256)を作る。
- 文書のハッシュ値とマーカーをビットコイントランザクションのOutput Scriptに格納する。
  - Output Scriptの格納にはOP_RETURNを用いる。
  - OP_RETURNの後ろには任意のデータ(40bytesまで)を入れられる。

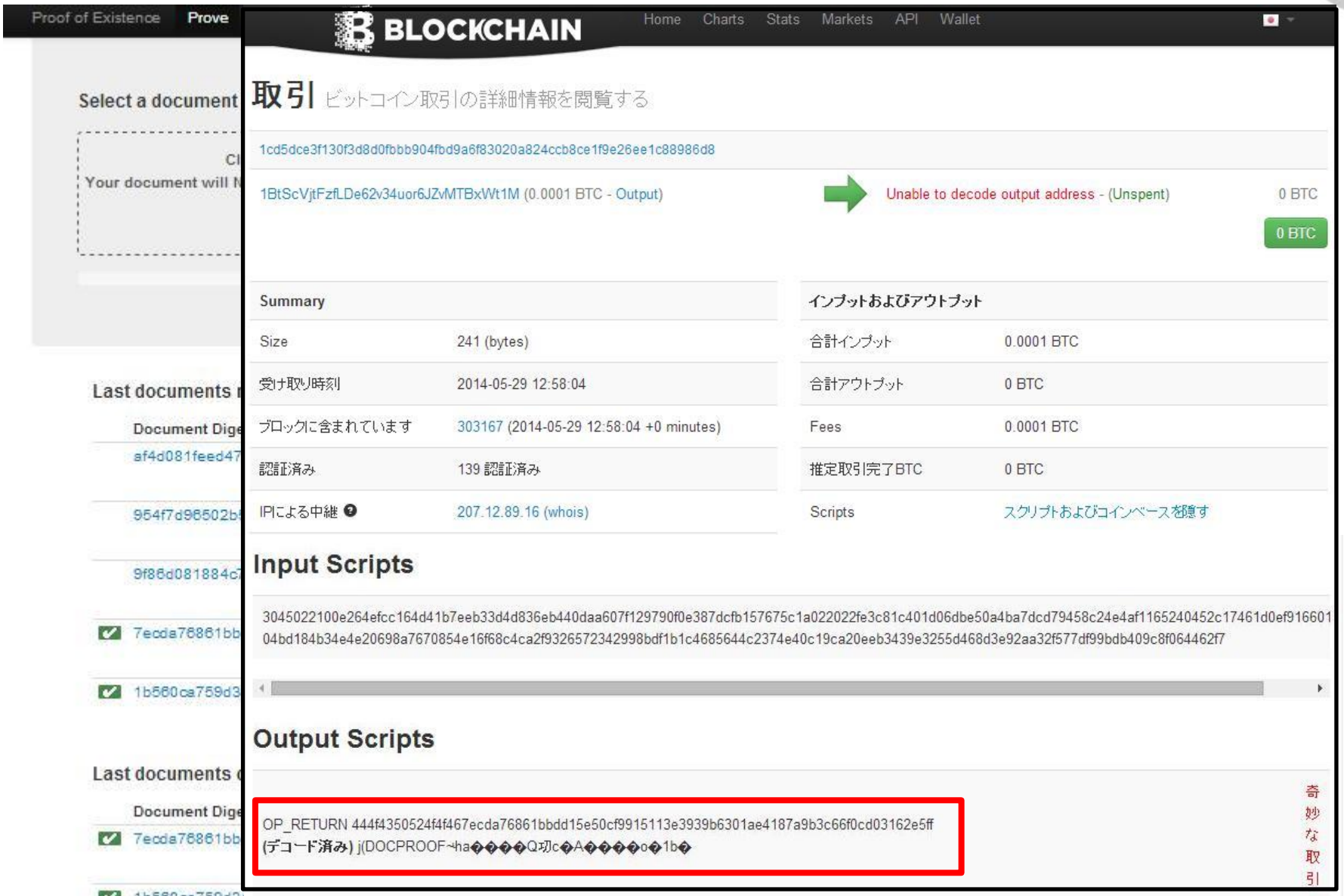
ビットコインを用いた存在証明①
～Proof of Existence～

セコムIS研究所
Intelligent Systems Laboratory



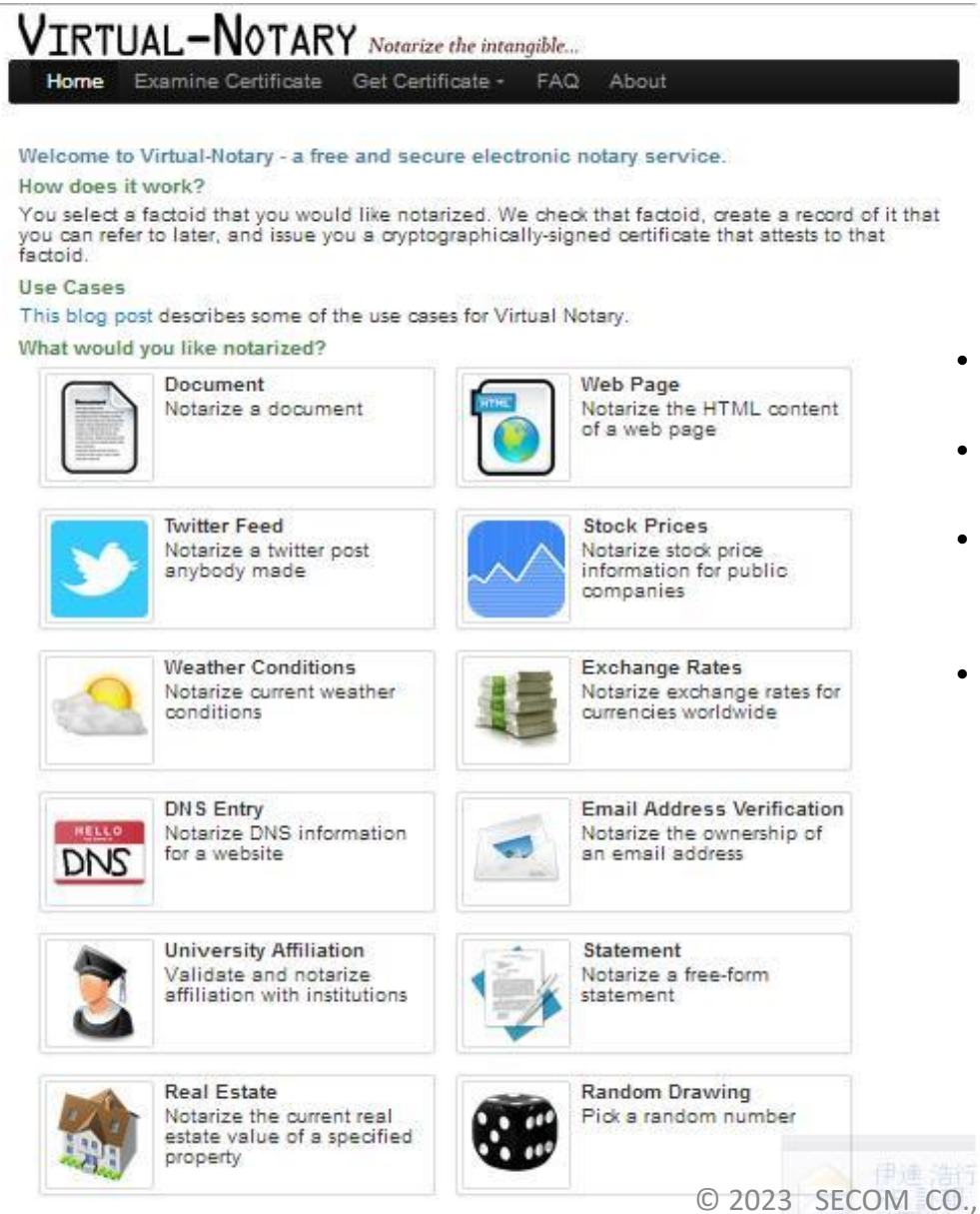
ビットコインを用いた存在証明①
～Proof of Existence～

セコムIS研究所
Intelligent Systems Laboratory



ビットコインを用いた存在証明②
～Virtual Notary～

セコム IS研究所
Intelligent Systems Laboratory



http://virtual-notary.org/

Cornell University
Computer Science Department

- 存在証明したい文書やWebサイトに対して X.509属性証明書を発行する。
- X.509属性証明書のハッシュチェーンを作り、順序関係を担保する。
- ハッシュチェーンの最新状態をTwitterとビットコインネットワークに流すことで第三者証明を可能にする。
- 24時間ごとにビットコイントランザクションのOutput Script(たぶんOP_RETURN)にその時の最新ハッシュ値を埋め込んで流す。

セコムIS研究所
Intelligent Systems Laboratory

本題に入ります

ビットコインの気になるところ

セコム IS研究所
Intelligent Systems Laboratory

- ビットコインに対する攻撃
  - ビットコインの盗難
  - ビットコインの二重使用
  - ビットコインの二重取り（トランザクション展性）
- ブロックチェーンの肥大化
- 暗号アルゴリズムの脆弱化
- etc.

今日触れるのは
このあたりのお話

ビットコインを不正に得るには？

- 人様のビットコインを盗む
- 自分のビットコインを不正に増やす
  （二重使用）
- 他者から二重取りする
  （コイン受領の否認）

ビットコインの気になるところ

セコム IS 研究所
Intelligent Systems Laboratory

- ビットコインに対する攻撃
  - ビットコインの盗難
  - ビットコインの二重使用
  - ビットコインの二重取り（トランザクション展性）
- ブロックチェーンの肥大化
- 暗号アルゴリズムの脆弱化

ウォレット盗難の脅威

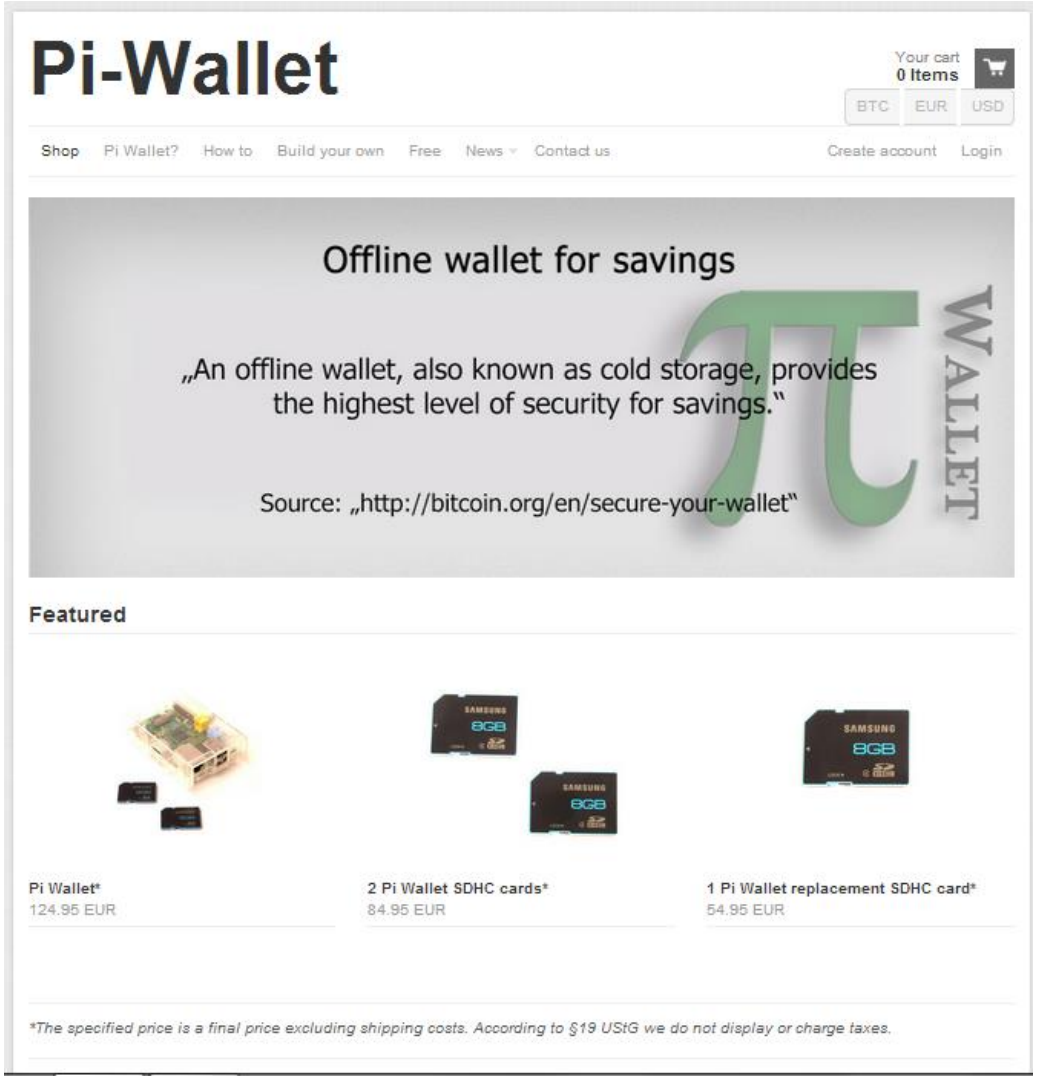
ウォレット（トランザクションの署名に使う秘密鍵）の管理はとっても大事！

- PC/デバイスでの管理
  - マルウェア感染によるウォレット流出の脅威
  - 暗号（パスワード）はかけられるが、キーロガーを仕掛けられたり、ウォレット取得後にブルートフォースを掛けられたら…
  - ウォレットのバックアップについても注意が必要
    - 盗難ではないが、古いバックアップをリストアしてしない新しい鍵が消失してしまう事故も…
- オンラインサービスでのウォレット管理
  - そのサービスに脆弱性があった場合の秘密鍵流出や不正使用など
  - そもそも、そのサービスは信用できるのか？

オフライン管理による保護①

- オンラインPC（ネットワーク接続したトランザクション受信専用PC）とオフラインPC（ネットワークに接続しない署名専用PC）の２台に分割して管理する。
- 送金する場合には、オンラインPCで生成したトランザクションデータ（署名なし）に対してオフラインPCで署名を行う。トランザクションデータはUSBキーを用いて移動させる。
- 専用ウォレット管理ソフト ARMORY
  https://bitcoinarmory.com/

オフライン管理による保護②



- http://www.pi-wallet.com/
- 前述のARMORYをRaspberry Piに組み込んだもの
- オフラインウォレットのために別のPCを用意する必要がなくなる。

ビットコインの気になるところ

セコム IS 研究所
Intelligent Systems Laboratory

- ビットコインに対する攻撃
  - ビットコインの盗難
  - ビットコインの二重使用
  - ビットコインの二重取り（トランザクション展性）
- ブロックチェーンの肥大化
- 暗号アルゴリズムの脆弱化

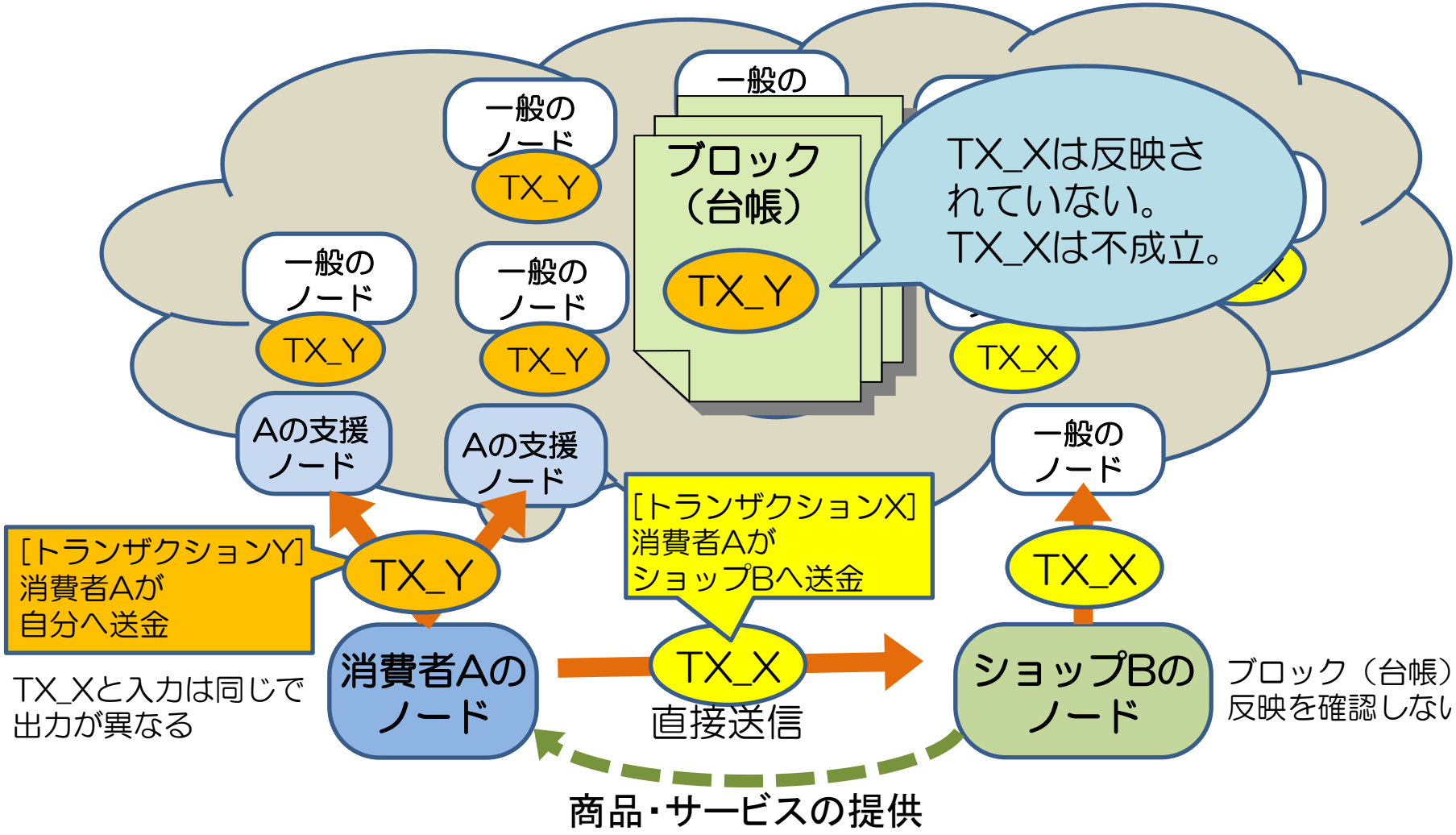
コインの二重使用

ホントは自分のコインを使っちゃったんだけど、使ったことをみんなに内緒にできれば…

無限に使えるコインができるじゃないか！

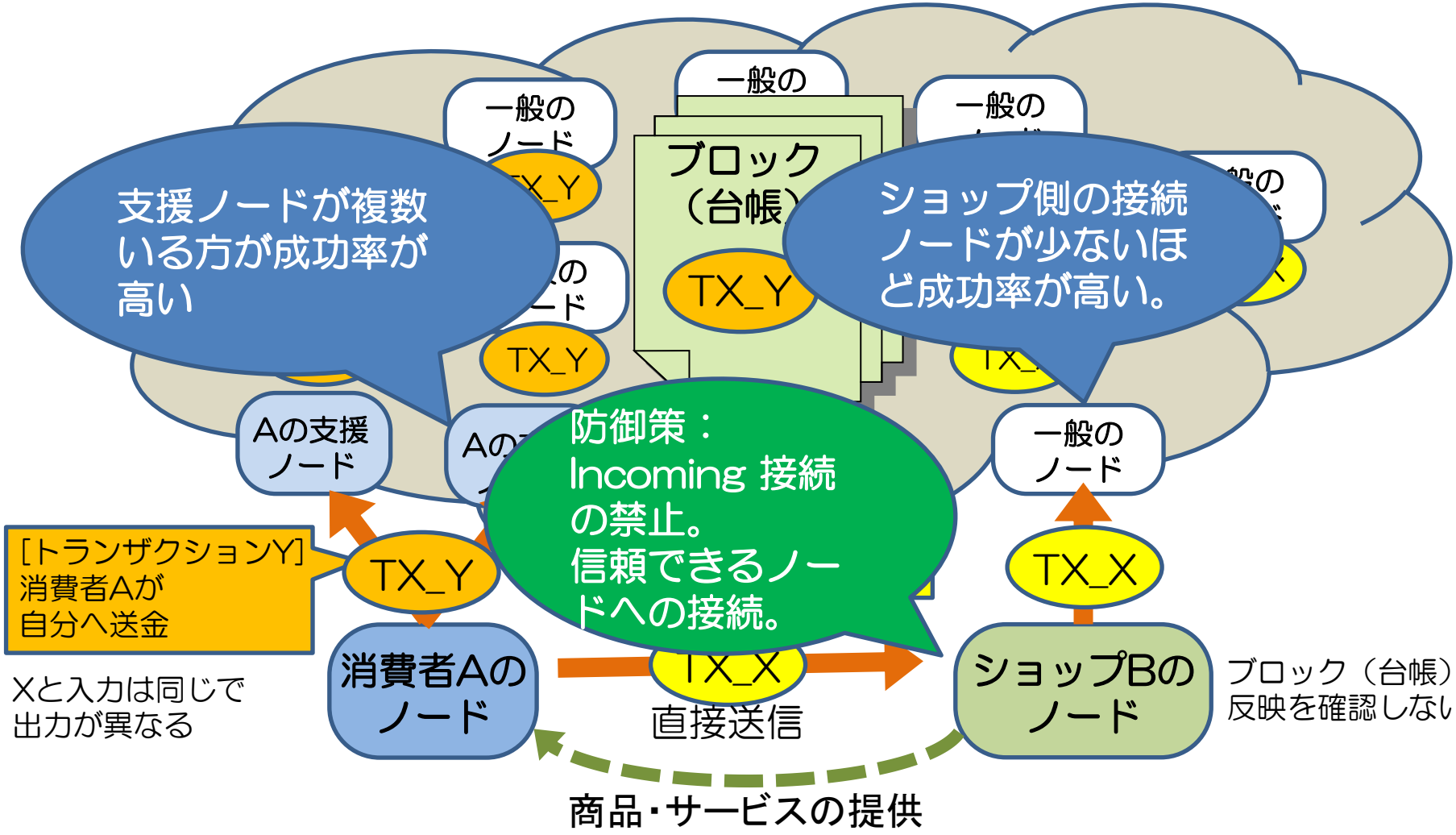
0-confirmation (Fast) payment におけるコイン二重使用

セコムIS研究所
Intelligent Systems Laboratory



（参考）“Two Bitcoins at the Price of One? Double –Spending Attacks on Fast Payments in Bitcoin “, Ghassan O. Karame , Elli Androulaki, Srdjan Capkun

0-confirmation (Fast) payment におけるコイン二重使用

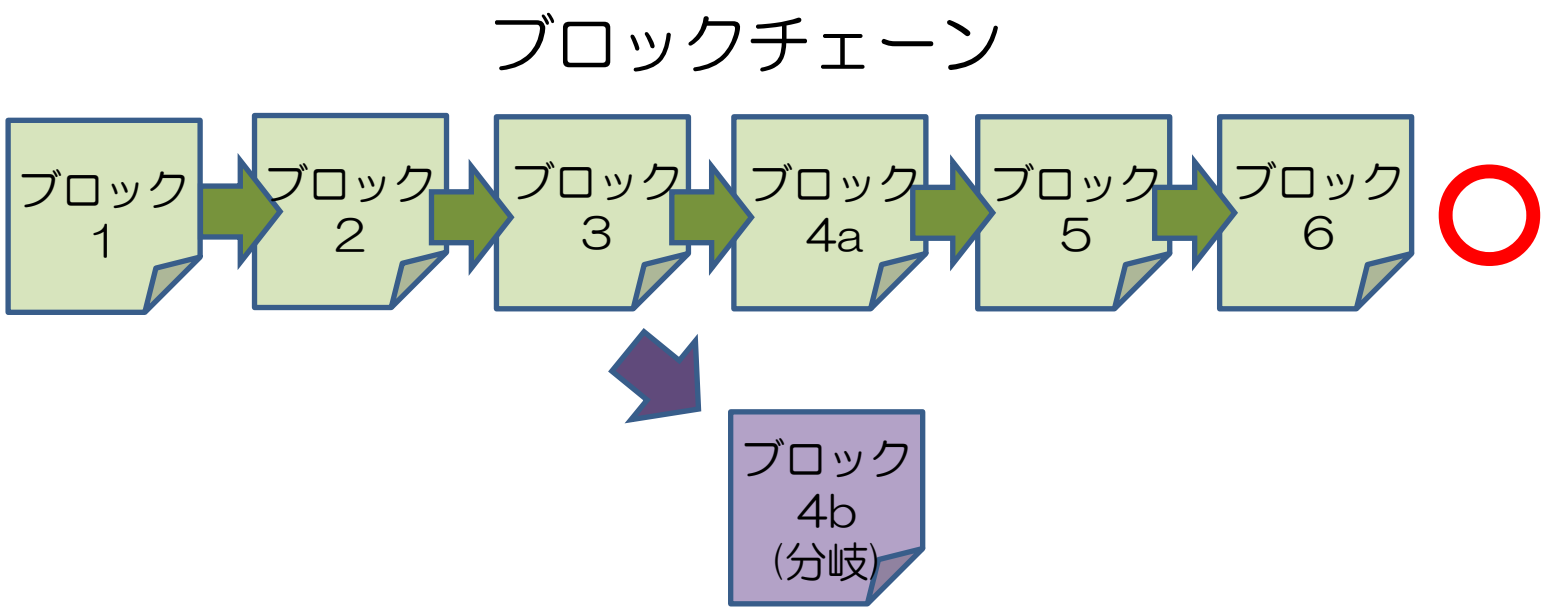


（参考）“Two Bitcoins at the Price of One? Double –Spending Attacks on Fast Payments in Bitcoin “, Ghassan O. Karame , Elli Androulaki, Srdjan Capkun

N-Confirmations

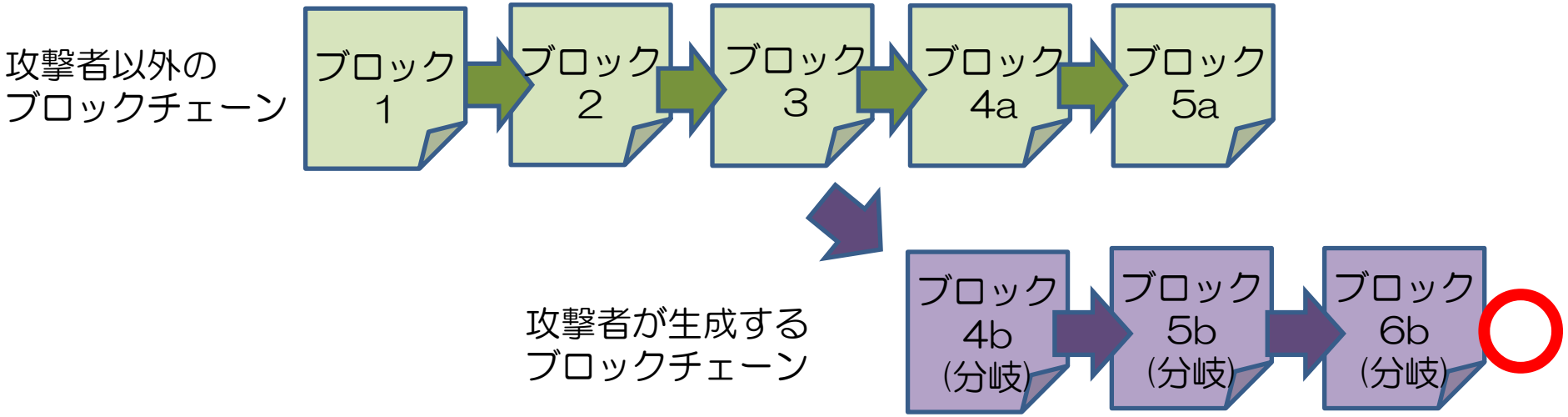
- 0-Confirmationによる取引はリスクを考慮する必要がある。高額取引には推奨されない。
- トランザクション発生後、N個のブロック生成を待った後にトランザクションの確認を行ったほうがよい（N-Confirmations）。
  - 例えば、bitcoinオリジナルクライアントでは6 confirmationsが設定されている。
- N-Confirmationsに関する考察
  - Analysis of hashrate-based double-spending, Meni Rosenfeld, Dec 2012

ブロックチェーンのブランチ



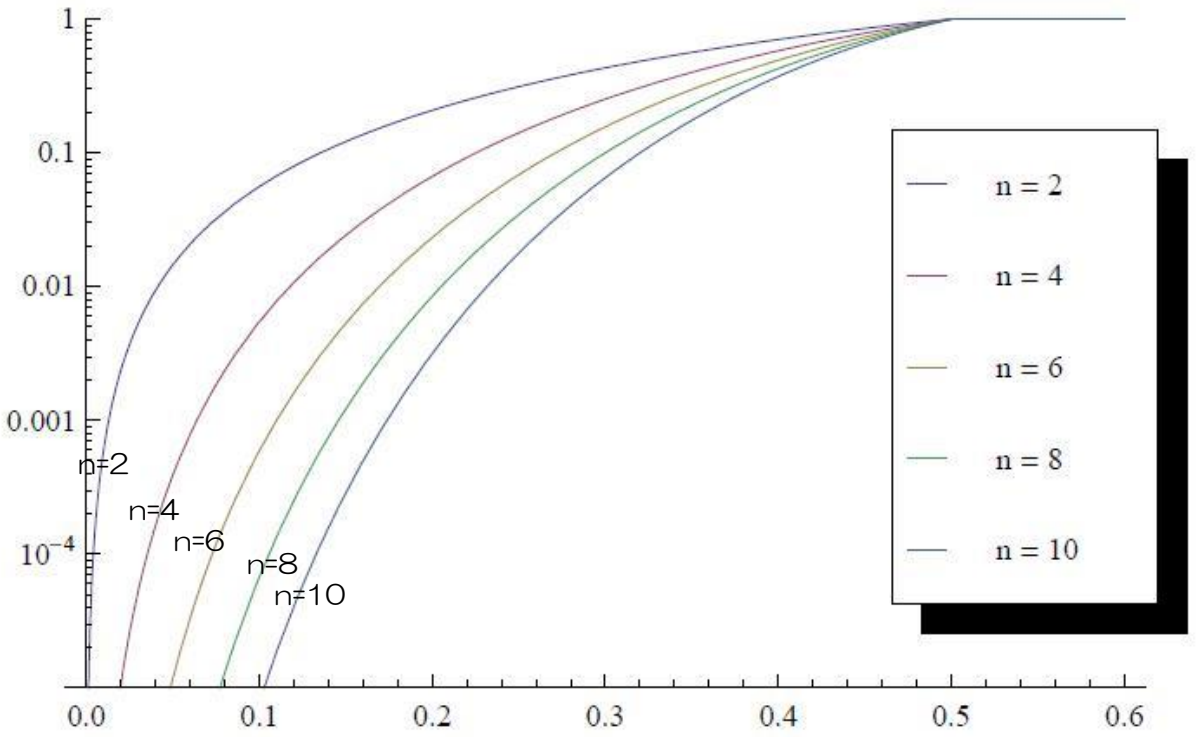
ブロックチェーンが分岐しても、ビットコインネットワークは最長の
ブロックチェーン（緑のブロック）を受け入れる。

ブロックチェーンのキャッチアップ



攻撃者が他のノードよりも先にブロック生成を行い、
最長のブロックチェーンを作り出すことができれば、
攻撃者にとって都合の良いブロックを認めさせることができる。
（例えば、自分のコインの2重使用を可能にするトランザクションを含める等）

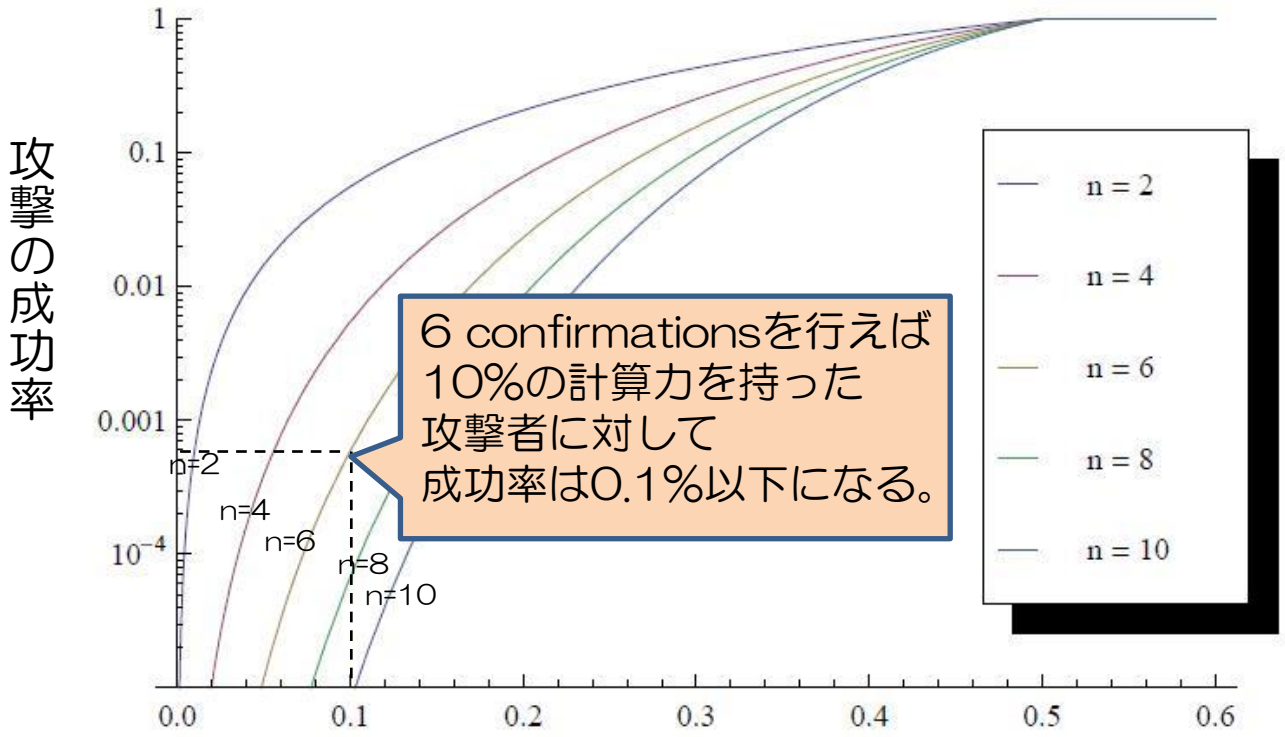
ブロックチェーン乗っ取りによる攻撃の成功率



nはコイン取得者が
実施するconfirmation
(確認するブロック)の数

（引用元）“Analysis of hashrate-based double-spending”, Meni Rosenfeld

ブロックチェーン乗っ取りによるコイン二重使用の成功率

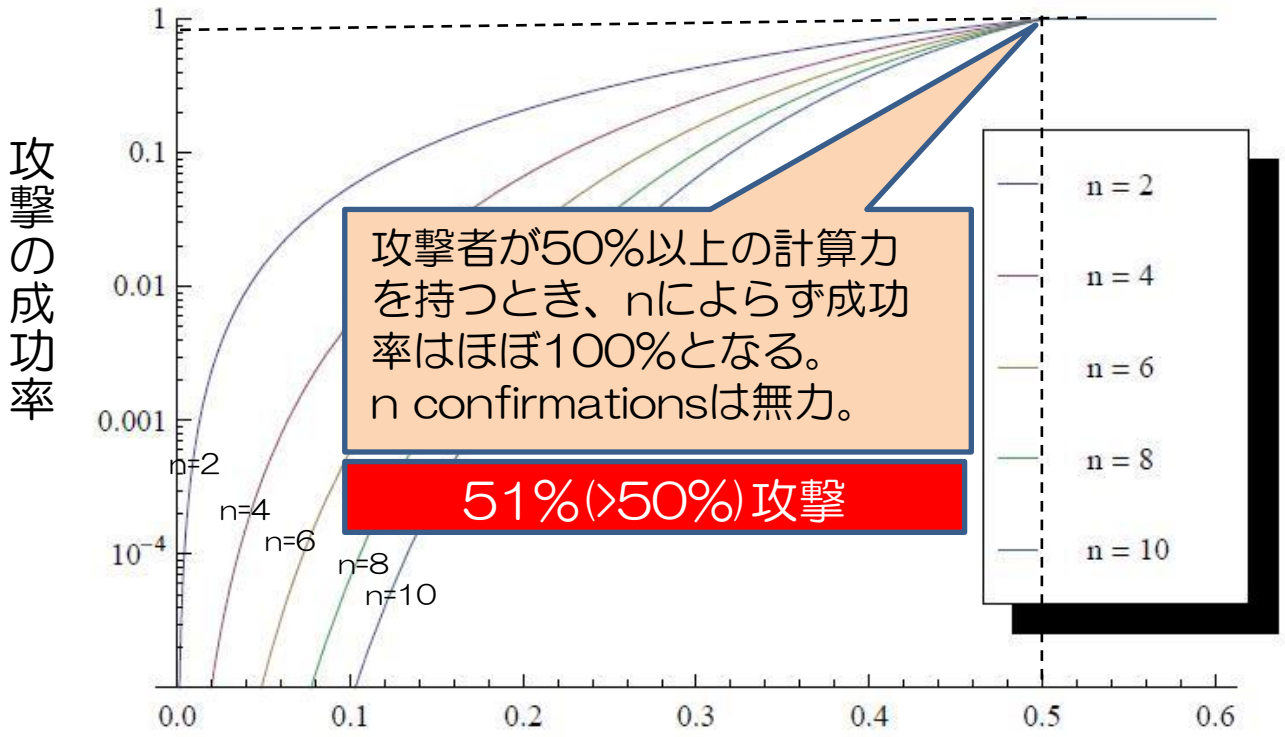


nはコイン取得者が
実施するconfirmation
(確認するブロック)の数

（引用元）“Analysis of hashrate-based double-spending”, Meni Rosenfeld

ブロックチェーン乗っ取りによるコイン二重使用の成功率

セコムIS研究所
Intelligent Systems Laboratory

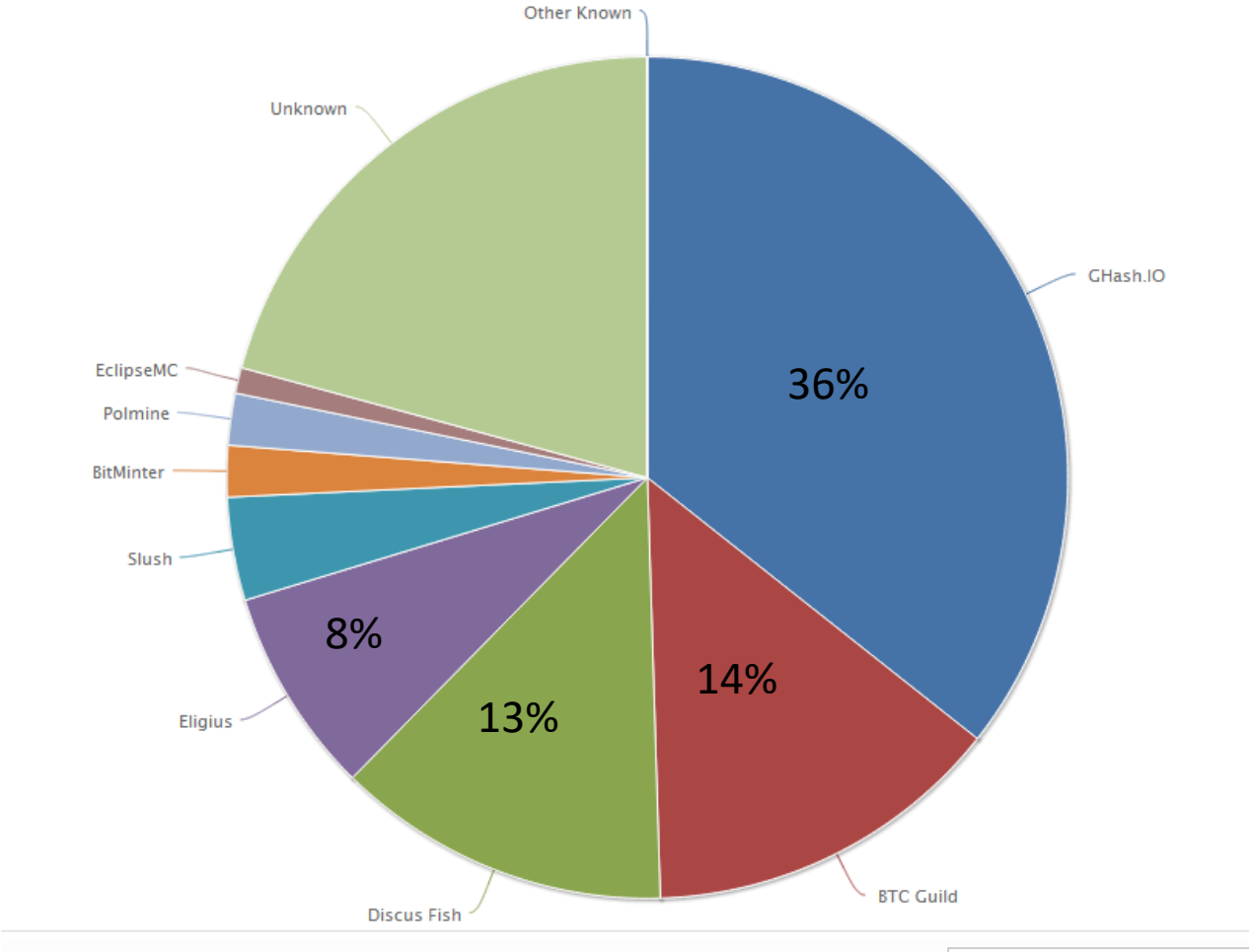


（引用元）“Analysis of hashrate-based double-spending”, Meni Rosenfeld

N-Confirmations

- 0-Confirmationによる取引はリスクを考慮する必要がある。高額取引には推奨されない。
- トランザクション発生後、N個のブロック生成を待った後にトランザクションの確認を行ったほうがよい（N-Confirmations）。
  - 例えば、bitcoinオリジナルクライアントでは6 confirmationsが設定されている。
  - 51%攻撃が実行されないという前提が必要か
- N-Confirmationsに関する考察
  - Analysis of hashrate-based double-spending, Meni Rosenfeld, Dec 2012

現在のハッシュレート
(2014.6.1現在)



51%(>50%)攻撃による効果

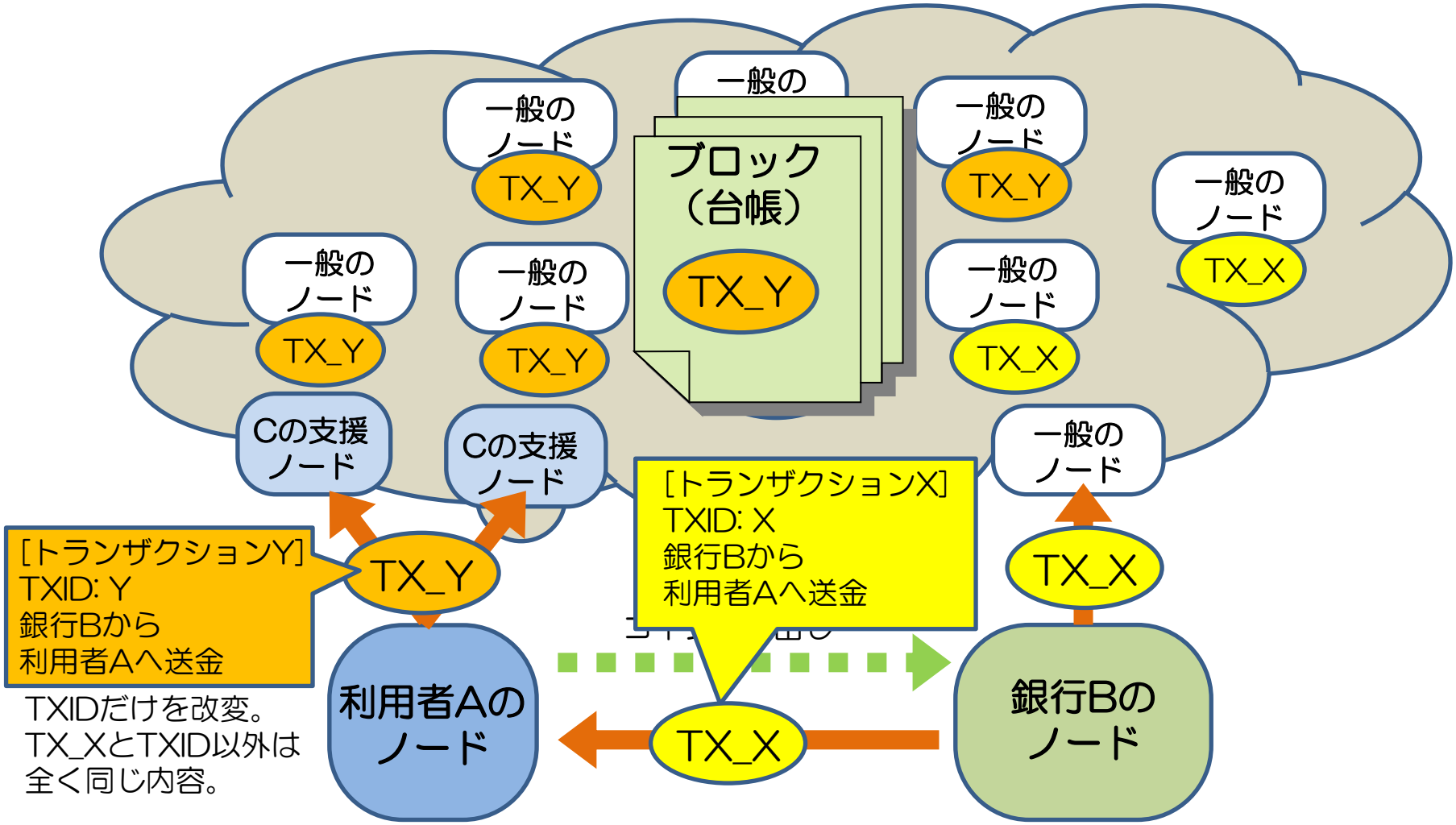
- 二重使用以外にも攻撃者に都合よく仕向けることができる。
  - 他者のトランザクションのconfirmationを妨害できる。
  - 他者のマイニングを妨害できる。

ビットコインの気になるところ

セコムIS研究所
Intelligent Systems Laboratory

- ビットコインに対する攻撃
  - ビットコインの盗難
  - ビットコインの二重使用
  - ビットコインの二重取り（トランザクション展性）
- ブロックチェーンの肥大化
- 暗号アルゴリズムの脆弱化

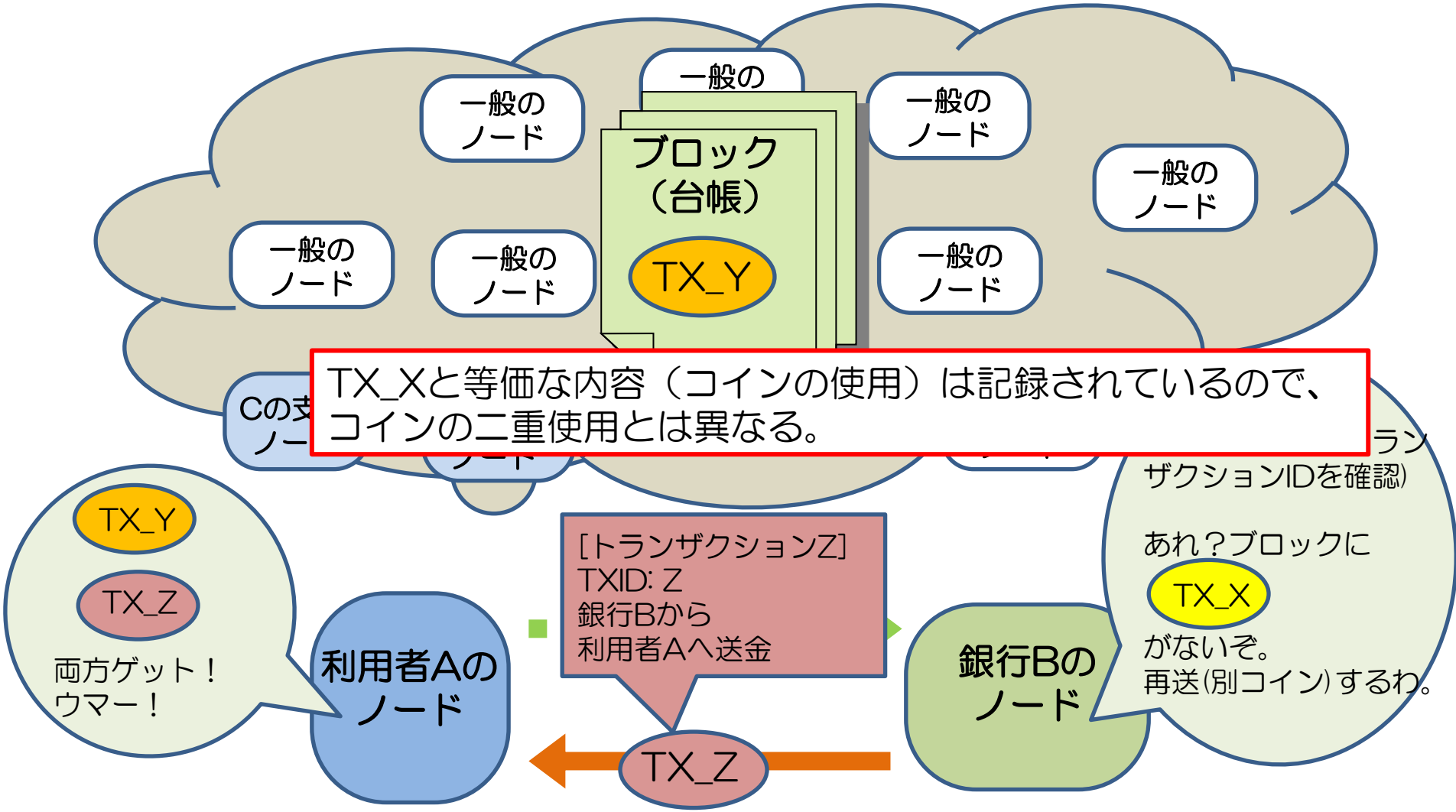
コインの二重取り



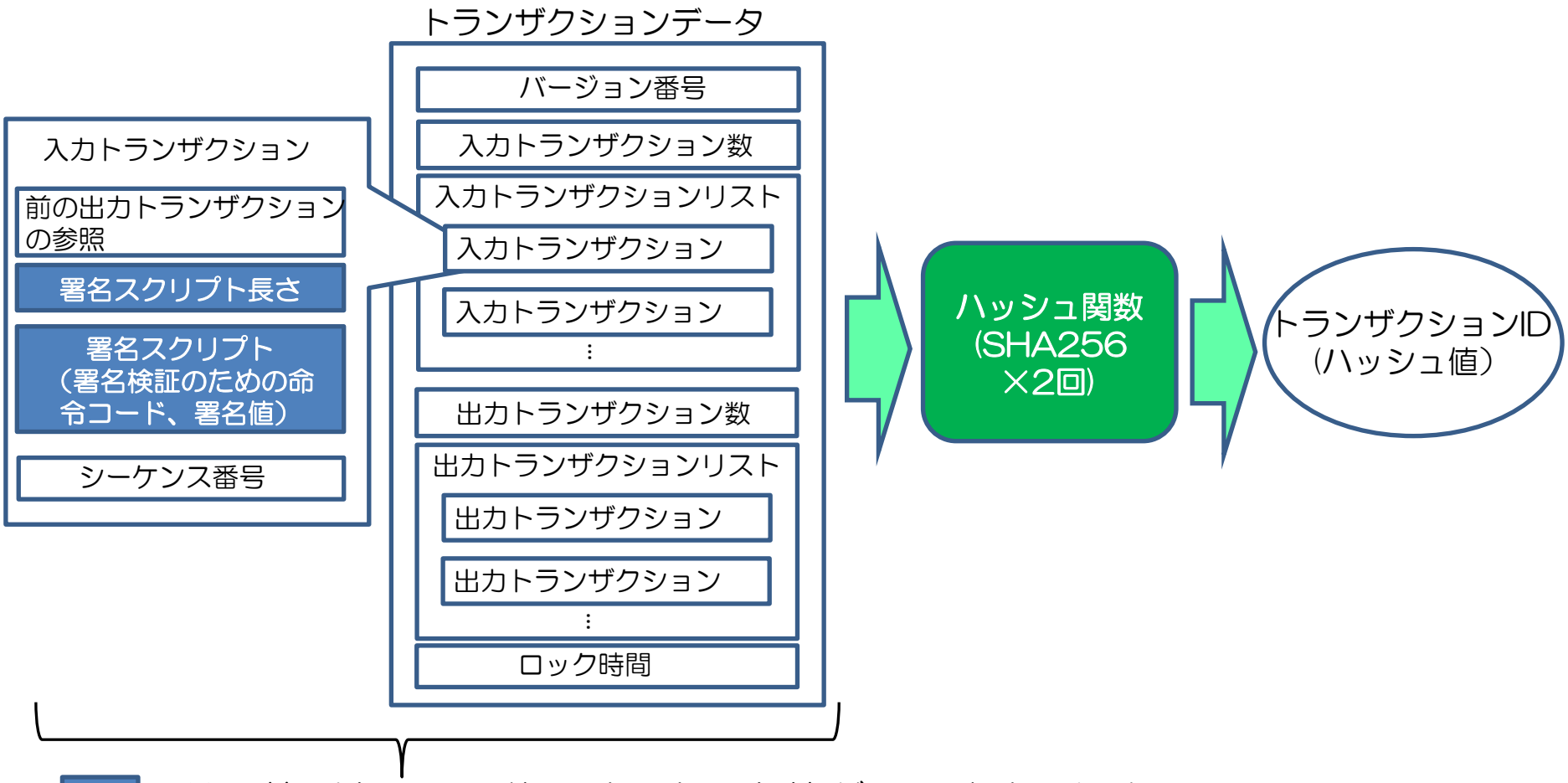
TXIDだけを改変。
TX_XとTXID以外は
全く同じ内容。

※図の都合上、TX_Xを直接送る絵になってます。

コインの二重取り

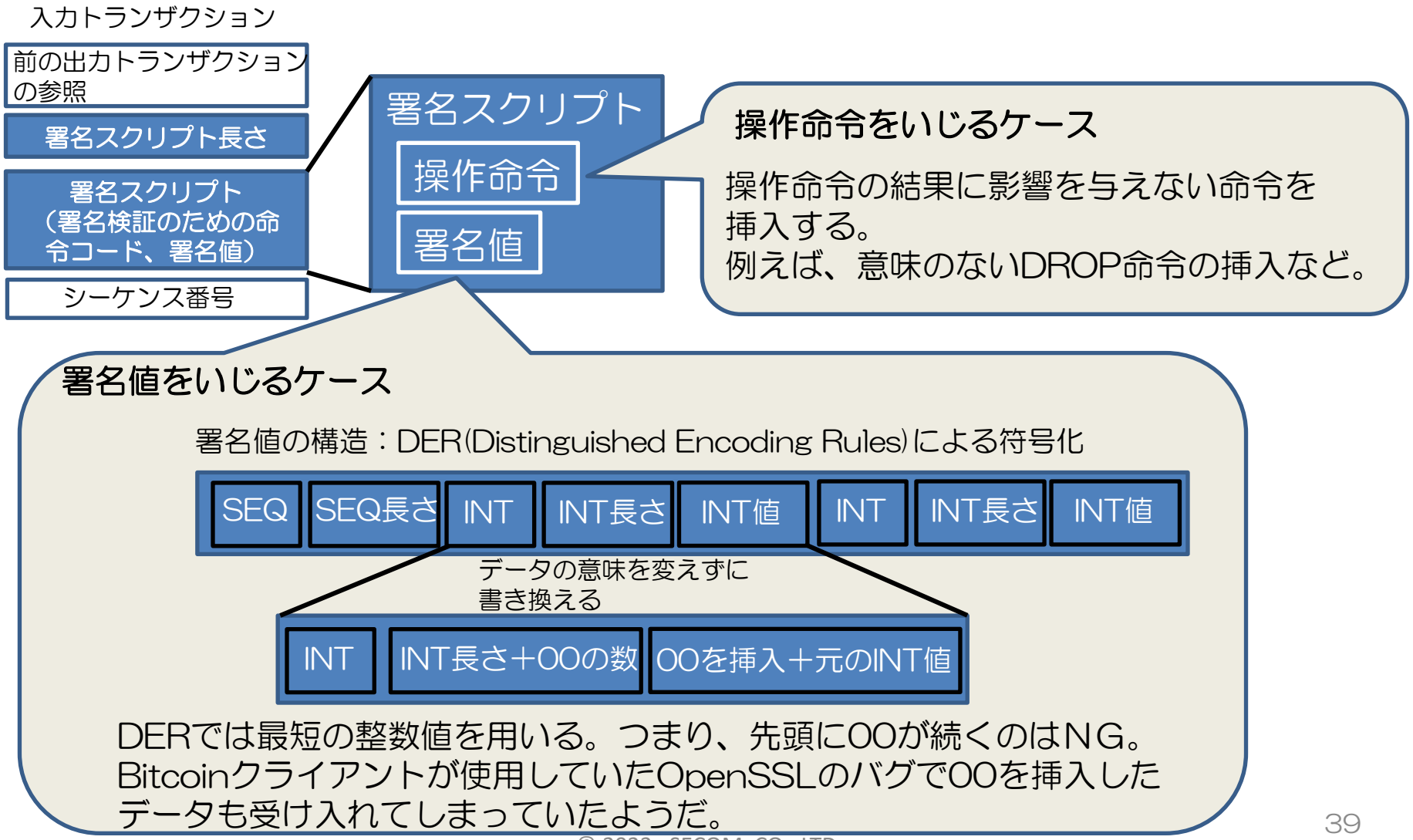


トランザクションIDに対する不正な操作
～トランザクション展性(Transaction Malleability)～



以外の箇所を不正に修正すると署名値が不一致するため、
データ改ざんとして検知される。署名値を変えても検知される。
署名値の内容を変えずに の箇所を微調整できれば、全く異なるハッシュ値（ID）を生成させることができる（ハッシュ関数の性質）。

トランザクションIDの改変方法例①（署名値の操作）

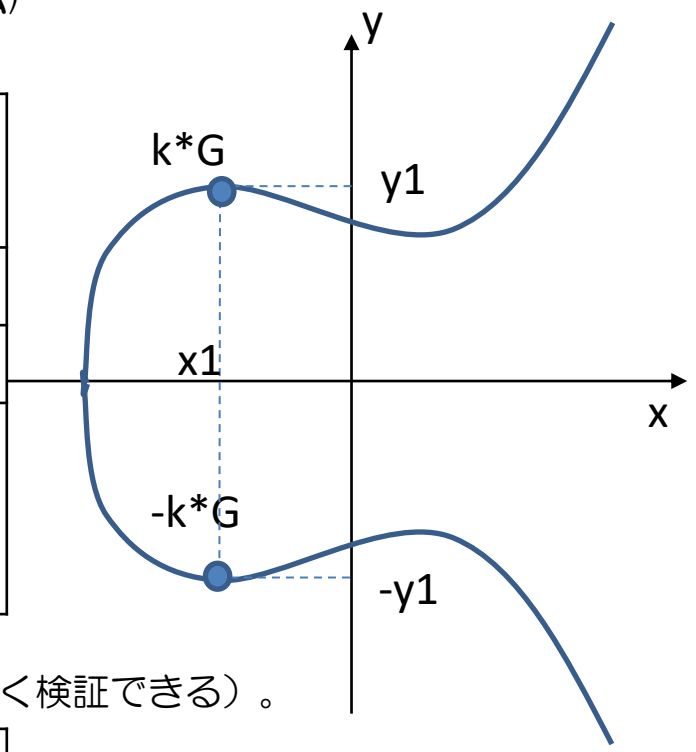


トランザクションIDの改変方法例②（異なる署名値への置換）

セコム IS研究所 Intelligent Systems Laboratory

ECDSA（楕円曲線暗号を用いた署名アルゴリズム）による署名生成

共通パラメータ	・楕円曲線の関数 ・楕円曲線上の点G ・Gの位数n
署名に使う秘密鍵	d
検証に使う公開鍵	Q=d*G
署名値 （署名対象データ:M）	点 k*G=(x1, y1)（k ∈[1, n-1]）を決めて以下を計算。 r = x1 mod n s = (hash (M) + dr)/k mod n



-k*G=(x1, -y1)を使って
署名値だけ変えられる（これも正しく検証できる）。

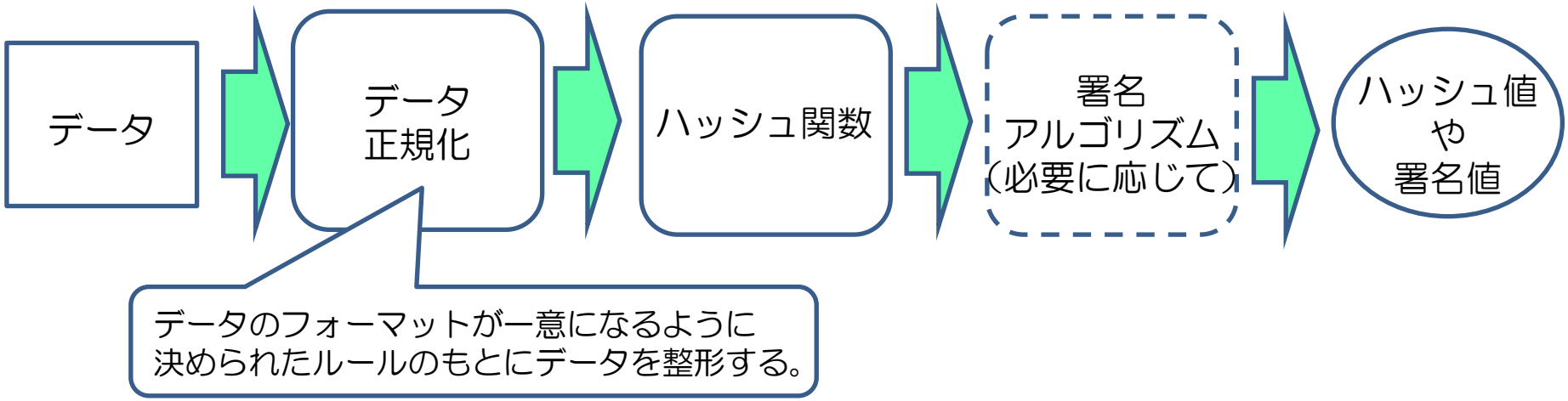
署名値 （署名対象データ:M）	k’ = -k mod nに置換すれば r はそのまま s’ = -s mod n

トランザクション中の署名値をS→S’に置換すれば、署名を無効化せずに、トランザクションID(ハッシュ値)を変えることができる。

データ正規化の必要性

セコムIS研究所
Intelligent Systems Laboratory

一般的にデータに対してハッシュ関数や署名演算をかけるときには、
同じデータに対して出力される値が一意になるようにデータの正規化を行う。
（電子署名屋さんにとっては常識？）



ビットコインはデータ正規化が甘かったのかも（当初は複数の実装がなかったせい？）。
一部のデータ正規化については、オリジナルクライアントは対応済(v0.8, 2013年頃)。
その他の正規化は？　オリジナルクライアント以外の実装は？？？

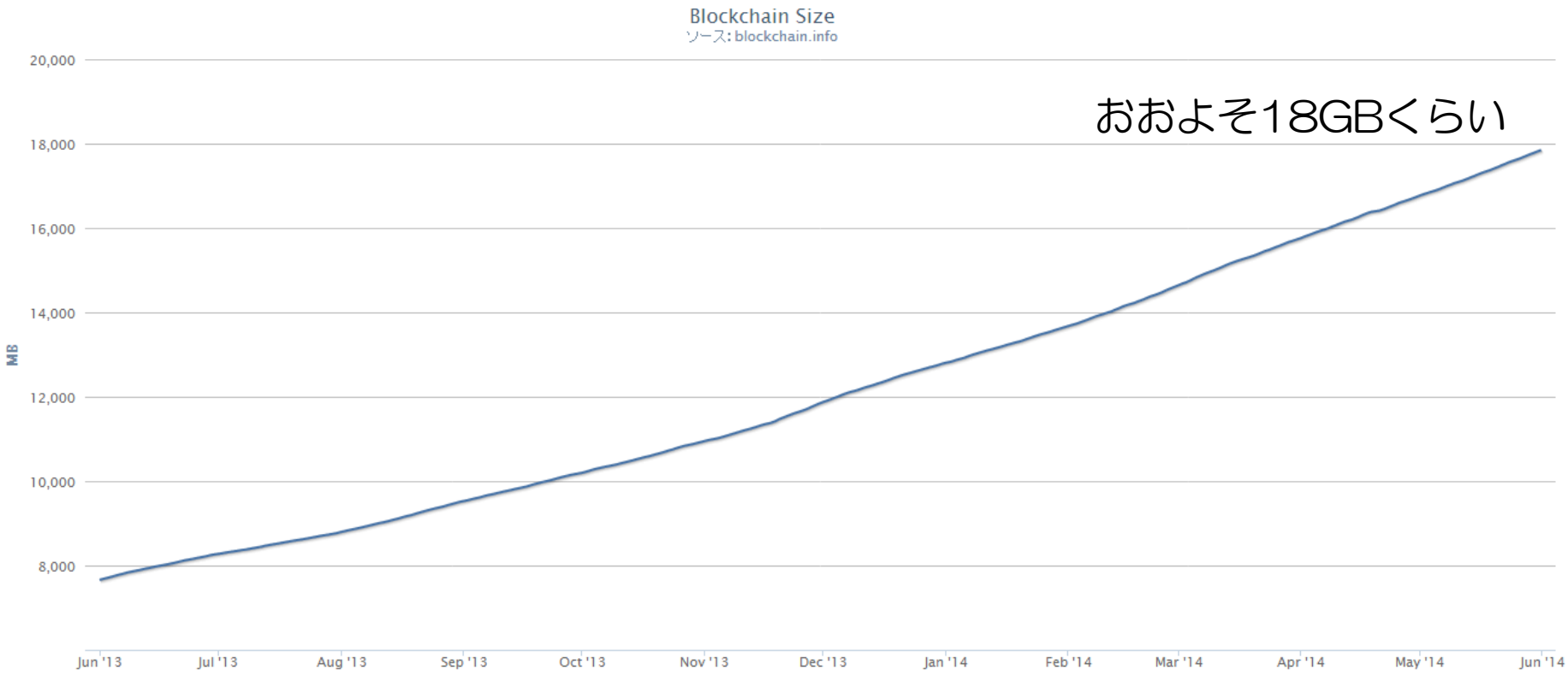
ビットコインの気になるところ

セコム IS 研究所
Intelligent Systems Laboratory

- ビットコインに対する攻撃
  - ビットコインの盗難
  - ビットコインの二重使用
  - ビットコインの二重取り（トランザクション展性）
- ブロックチェーンの肥大化
- 暗号アルゴリズムの脆弱化

ブロックチェーンの肥大化

1年間（2013年6月～）

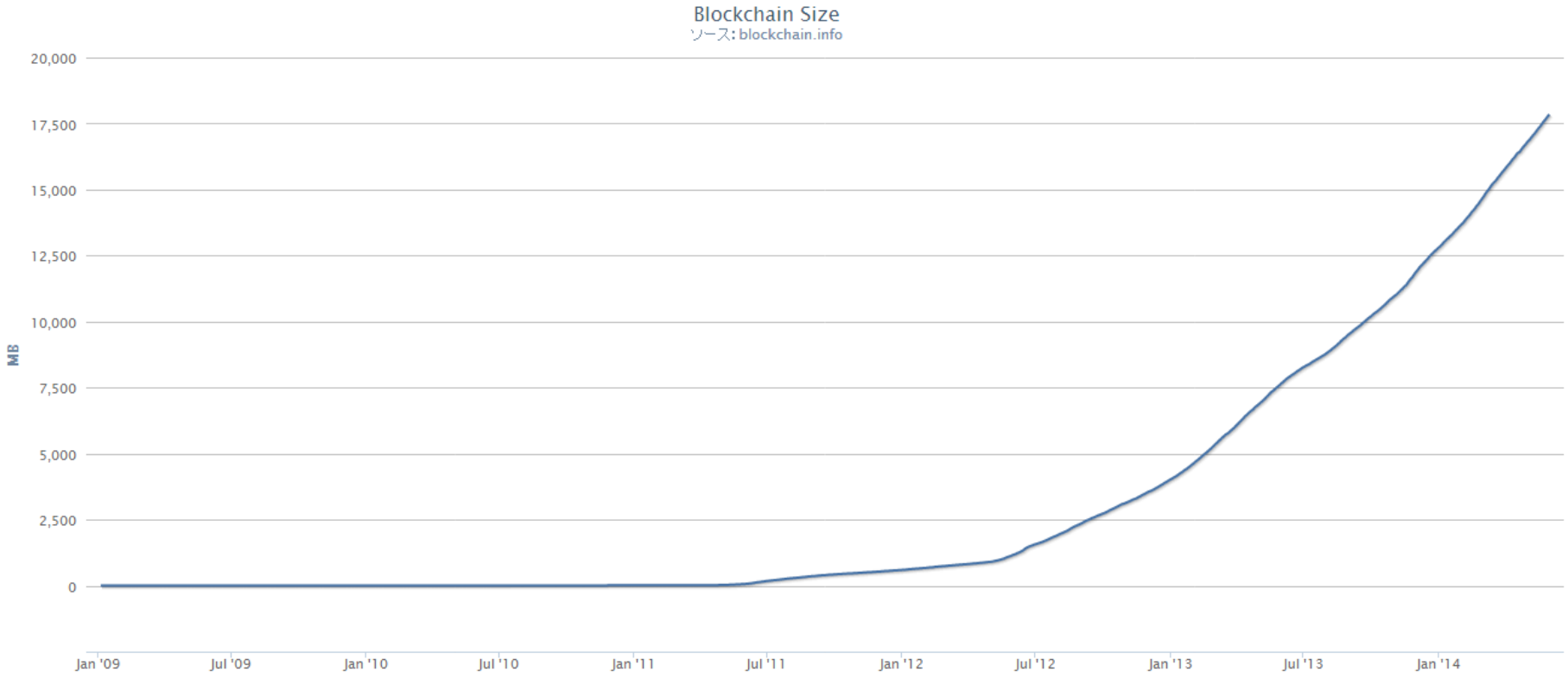


おおよそ18GBくらい

現在、全ブロックチェーンをダウンロードしようとすると
結構な時間がかかります（数日とか…）

ブロックチェーンの肥大化

全期間（2009年～）



ここ1年くらいの伸びがすごい！

ブロックチェーンの肥大化への対策

セコムIS研究所 Intelligent Systems Laboratory

- ビットコインネットワーク上でのブロックチェーンの圧縮が必要？
  - すでに検討されている？
- アプリケーションによる必要なトランザクションデータの抽出
  - 軽量クライアント用に既に拡張されている。
    - Bloom filterを使って自分に関係しそうな（プライバシーへ配慮）トランザクションデータのみをダウンロードする。
    - トランザクションデータを提供するノードへの依存性が高くなる。
    - Multibit, BitCoin Walletでサポート
- 将来、ブロックの蓄積や検証についても分業化が進む可能性がある？

ビットコインの気になるところ

セコム IS 研究所
Intelligent Systems Laboratory

- ビットコインに対する攻撃
  - ビットコインの盗難
  - ビットコインの二重使用
  - ビットコインの二重取り（トランザクション展性）
- ブロックチェーンの肥大化
- 暗号アルゴリズムの脆弱化

ビットコインの暗号やハッシュ

- 暗号が使われている箇所
  - トランザクションへの署名[公開鍵暗号]
  - 署名鍵（ウォレット）の保護[共通鍵暗号]
- ハッシュ関数が使われている箇所
  - ビットコインアドレス（公開鍵のハッシュ値）
  - トランザクションのハッシュ（ハッシュツリー、トランザクションID）
  - ブロックチェーン生成（マイニング）

ビットコインの暗号やハッシュ

- 暗号が使われている箇所
  - トランザクションへの署名[公開鍵暗号]
  - 署名鍵（ウォレット）の保護[共通鍵暗号]
- ハッシュ関数が使われている箇所
  - ビットコインアドレス（公開鍵のハッシュ値）
  - トランザクションのハッシュ（ハッシュツリー、トランザクションID）
  - ブロックチェーン生成（マイニング）

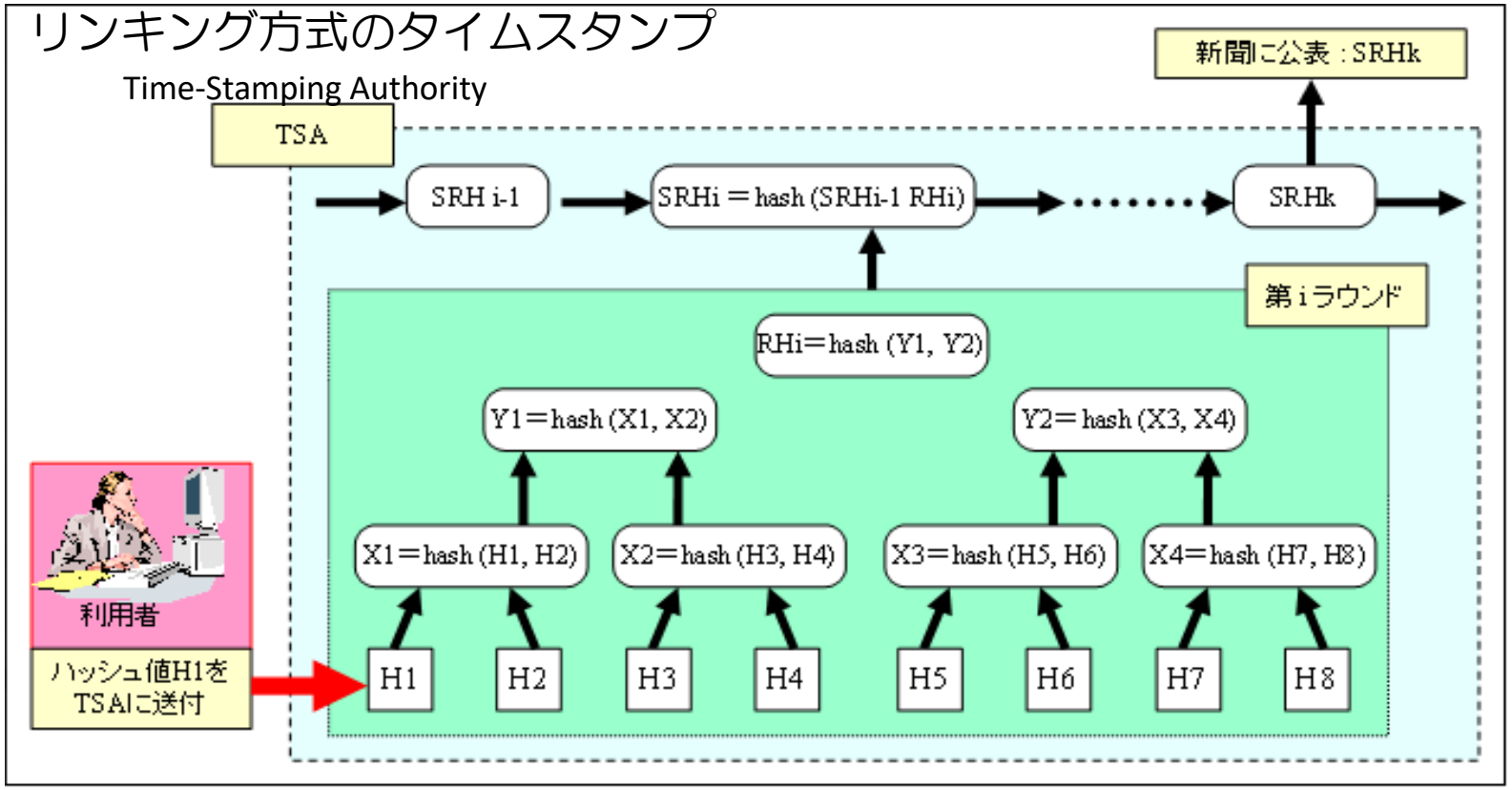
暗号やハッシュが脆弱化すると？

- 将来、暗号解読方法の解明や、計算能力の向上、実装ミスの発覚などによって、使用されている暗号やハッシュが弱体化するかも？
- そうなると、次のようなことが可能になるかも？（あくまで可能性の話）。
  - 秘密鍵の所有者以外の者がウォレットを盗むことなく同じ秘密鍵を得る（例えば、公開鍵から秘密鍵を作り出すとかetc.）
  - ブロックチェーン上のあるブロックや、一部のトランザクションを後から不正に入れ替える
- 暗号/ハッシュの弱体化がすぐにビットコインネットワーク崩壊につながるというわけではない。暗号/ハッシュの弱体化の内容とその影響度、他のビットコインネットワークのメカニズムと照らし合わせて、実際にどのようなリスクがあるのか考える必要がある。

暗号やハッシュの移行は可能か？

- ビットコインのプロトコルとソフトウェアを更新し、単純に新しい暗号/ハッシュアルゴリズムに入れ替えることで、その更新以降から生成されるトランザクションやブロックはより強力な暗号/ハッシュを利用できるようになるだろう。
- ただし、その場合、過去に作られたトランザクションやブロックは脆弱なままと言える。
  - 例えば、過去に放置したままにしているコインの所有者はどうなるか？

ハッシュアルゴリズム移行を考えるときのヒント？



引用元：https://www.ipa.go.jp/security/pki/093.html

この形式のタイムスタンプは過去に作られたハッシュ値を新しいハッシュアルゴリズムで再生成するのは事実上困難。
ビットコインのケースにおいても、過去のものをすべて作り直すことは難しいだろう。どこまで対策すべきなのか、どのようなリスクがあるか検討が必要。

おわりに

セコムIS研究所
Intelligent Systems Laboratory

- ビットコインは中央の機関に依存しない仕組みであるため、それゆえの難しい問題も生じている。
- ビットコインで生じた数々の問題は、開発コミュニティによって解決が試みられてきている。
  - それらの問題の中には、ビットコインだけでなく他のシステム等を考えるうえで参考になるものもあるかも。
- ビットコインのプロトコルも拡張されているので、決済以外の用途にも使えてくると面白そう。
  - 一方で、他の既存のビジネスへの脅威になる恐れも？
- 電子署名屋さんとしては、秘密鍵の管理や暗号アルゴリズム移行などに興味があるので、今後もう少し深掘りして考えてみたい。

セコムIS研究所
Intelligent Systems Laboratory

ご清聴ありがとうございました。