新時代を切り拓く ブロックチェーンに関する シンポジウム＆交流会

ブロックチェーンと 暗号技術の役割について

2019年5月17日
才所敏明
（株）IT企画・代表取締役社長
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

 1

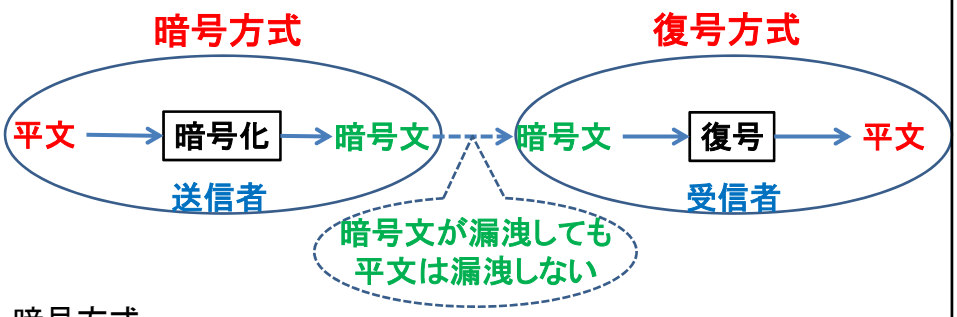
自己紹介

1966年　東京大学理科一類入学－＞工学部・計数工学科・数理コース
1970年　東芝入社
　社内計算機利用環境企画・構築・活用指導・支援
　　スーパコン～PCを利用した技術開発環境構築・活用推進（1969UNIX）
　　インターネットの企業活動への活用推進
　　（1974Internet　1984JUNET　1987InetClub　1992商用サービス）
　情報セキュリティ研究開発企画・推進、事業支援（1995）
　　暗号・認証技術等の事業への活用推進　（1999IoT）
2007年　（株）IT企画設立
　事業支援活動（顧問・相談役）：2社（日、米）
　大学教育活動（情報セキュリティ）：九大、慶応
　研究開発活動（研究員）：中央大学研究開発機構
　　暗号・認証、バイオメトリクス、電子メールセキュリティ、
　　IoTシステムセキュリティ、FinTech（仮想通貨、ブロックチェーン）
　　ビッグデータ、AI

 2

（1）暗号技術

暗号技術とは



暗号方式
　定められたルールに従い、
　意味が分かる文章（平文）を、意味の分からない文章（暗号文）へ
　変換する方式
復号方式
　暗号文を元の平文へ戻す方式（それぞれの暗号方式に対応）
暗号技術
　平文を暗号化でき、また復号できる、暗号方式および復号方式の対

 3

（1）暗号技術

暗号技術発展の歴史
古代暗号から近代暗号

人類の歴史は紛争の歴史
　人類・社会の歴史の陰に、暗号に関する熾烈な戦いが存在
　　その勝敗が人類・社会の歴史を形作ってきた

古代暗号：ヒエログリフ（紀元前3000年頃、世界最初の暗号）
　　シーザー暗号（紀元前100年頃）
古典暗号：（外交活動の活発化による暗号の普及期へ）
　　女王メアリ暗号（ノーメンクラタ暗号、16世紀ごろ）
　　上杉暗号（戦国時代、16世紀ごろ）
近代暗号：（暗号の作成・解読は、手作業から機械へ）
　　エニグマ暗号（第2次世界大戦でドイツ使用、英国解読）
　　パープル暗号（第2次世界大戦で外務省使用、米国解読）

 4

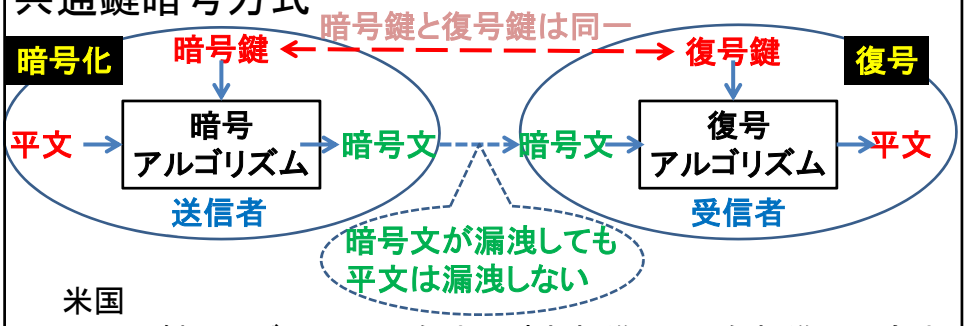
（1）暗号技術

暗号技術発展の歴史
現代暗号（第2次世界大戦以降）

現代暗号：（暗号の作成・解読は、計算機利用へ）（1943コロッサス　1946ENIAC）
- 特徴：コンピュータ/ネットワークの発展➔暗号利用分野の拡大
  - 軍事的・政治的利用から、産業活動・生活活動での利用へ
    - 多くのベンダによる開発競争、相互運用性の保証
  - 従来は“暗号方式を公開しない”ことで安全性を確保
    - 従来とは異なる安全性を確保する仕組みが必要に！
  - 現代暗号では暗号方式を暗号アルゴリズムと暗号鍵に分離
    - 現代暗号は、暗号アルゴリズムを公開しても
      暗号鍵を公開しなければ安全性が確保できるよう、
      暗号アルゴリズムが設計されている

現代暗号は、共通鍵暗号方式と公開鍵暗号方式の2方式に分類

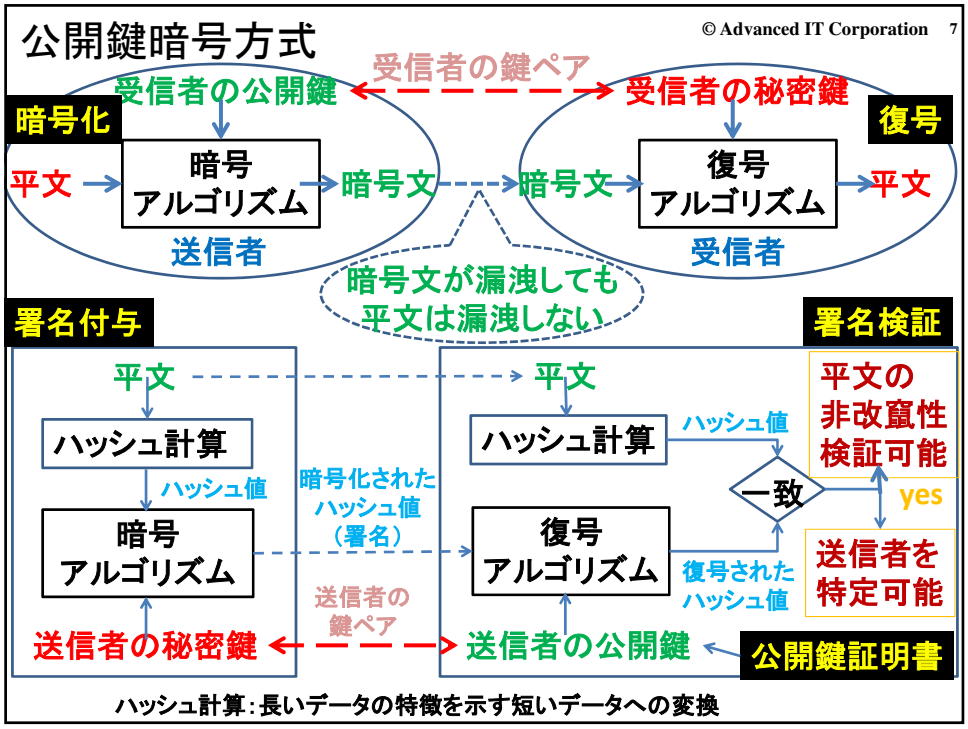
共通鍵暗号方式



米国
- DES：鍵長56ビット、1976年米国連邦標準、2005年標準から除外
- AES：鍵長128、192、256ビット、2001年米国連邦標準

日本
- NTT：1985年FEAL（64ビット）　2003年Camellia（128ビット）
- 三菱：1995年MISTY（128ビット）
- 東芝：1999年Triplo（128ビット）、2003年Hierocrypt-3（128ビット）

日本での活用事例
- 有料放送（1991年）：限定受信システム（CAS：Conditional Access System）
- PCでDVD視聴（1998年）：DTCP（Digital Transmission Content Protection）



（1）暗号技術

主要な公開鍵暗号方式

1978年RSA暗号：大きな素数の積の
素因数分解問題の難しさを利用

1985年楕円曲線暗号：楕円曲線上の
離散対数問題の難しさを利用

日本での活用事例

2001年クレジットカード（EMV仕様、RSA暗号）

2006年ICパスポート（ICAO準拠、RSA暗号、楕円曲線暗号）

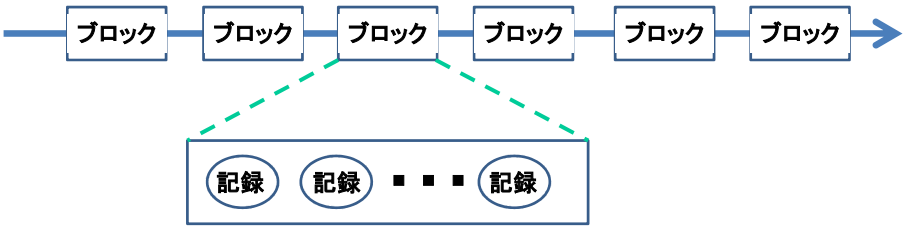
2016年マイナンバーカード（RSA暗号）

 8

（2）ブロックチェーンと暗号技術

ブロックチェーン

記録（支払等）を（複数）格納しているブロックの連鎖



（1）中央管理組織の無い記録技術

（2）記録消失の危険性が極めて低い記録技術

（3）過去の記録の改ざんが難しい記録技術

 9

（2）ブロックチェーンと暗号技術

ブロックチェーンの特徴（1）
中央管理組織の無い記録技術

未登録の複数の記録を集めたブロックを構成し、
**　ブロックチェーンに追加（ブロックを承認）する人・組織の選定方法をあらかじめ決めておくことが必要**
**　＝＞　コンセンサスアルゴリズム**

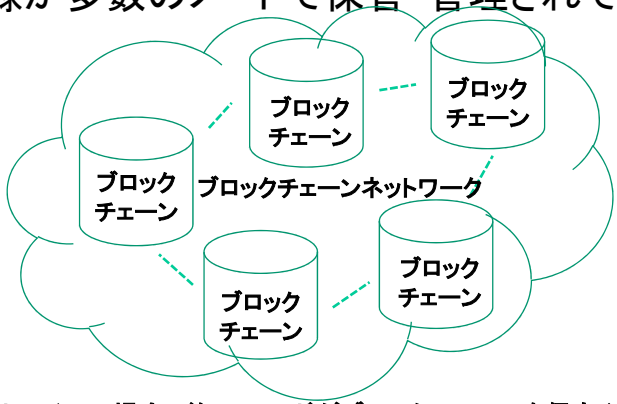
コンセンサスアルゴリズムの例
**　PoW（Proof of Work）：作業により目的を最初に達成した場合に、承認権と報酬**
**　PoS（Proof of Stake）：保有量に応じて、承認権と報酬**
**　PoI（Proof of Importance）：保有量に加えて、使用量に応じて、承認権と報酬**

 10

（2）ブロックチェーンと暗号技術

ブロックチェーンの特徴（2）
記録消失の危険性が極めて低い記録技術

記録が多数のノードで保管・管理されているため



参考：ビットコインの場合、約1万ノードがブロックチェーンを保有（2019年2月時点）
データ量：210GB＋5～10GB/month

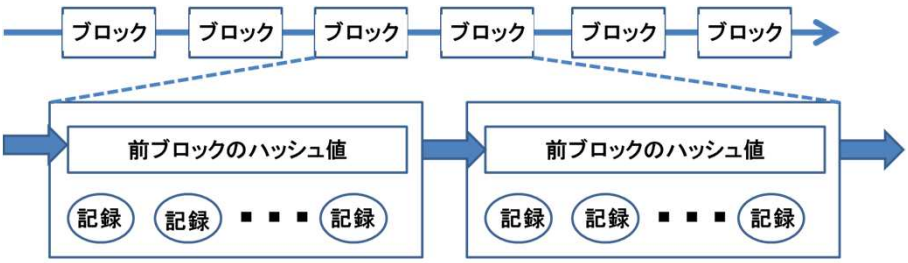
 11

（2）ブロックチェーンと暗号技術

 12

ブロックチェーンの特徴（3）
過去の記録の改ざんが難しい記録技術

過去の記録の情報（ハッシュ値）が
以降の記録に反映されているため



ハッシュ値：対象となるデータの特徴を一定の長さのデータに変換したもの。
対象となるデータが1ビットでも変われば、ハッシュ値も変わる。
ハッシュ値から元のデータの復元は不可。ハッシュ関数は一方向性関数。

（2）ブロックチェーンと暗号技術

ブロックチェーンの例としての ビットコインブロックチェーンの紹介

ブロックチェーン技術を 最初に具現化したのがビットコイン！

ビットコインの歴史

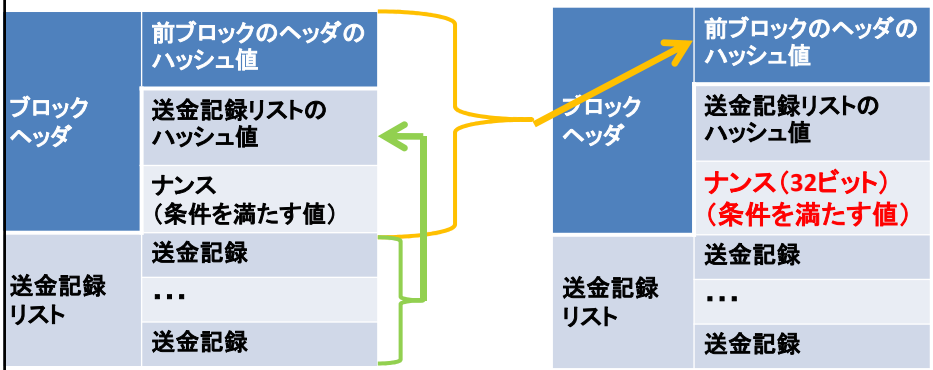
2008年10月　サトシ・ナカモトがインターネット上で論文発表

2009年1月　ビットコインソフトウェアが開発され運用開始
（その直後に、最初のトランザクションが発行された）

2010年5月　現実世界で初めて決済に使用された
「ピザ2枚（約25ドル）＝1万BTC」で取引が成立（1BTC≒0.2円）
（1BTC≒85万円：2019年5月14日）

（2）ブロックチェーンと暗号技術

ビットコインにおけるブロックの連鎖



検証者は、それぞれ自分で構成したブロックに対しハッシュ値を計算、
条件*を満たすナンス探索作業を実施する必要がある（マイニング）
条件*：ブロックのハッシュ値（256ビット）の先頭に16個の0が並ぶこと
ハッシュ関数は一方向性のため、ナンスを次々と変えて
ハッシュ値を計算して探索する方法しかない➔膨大な計算量/電力消費
ビットコイン1トランザクションの電力消費量：VISAの32万倍
年間電力消費量は、世界で4位の日本の1/5

ビットコインにおける送金記録の連鎖

使用する送金記録ID=n			
入力		出力	
入力元	所有権	出力金額	出力先
		8	Aのアドレス

使用する送金記録ID=m			
入力		出力	
入力元	所有権	出力金額	出力先
		7	Aのアドレス

出力先（送金先）は、
受取者の公開鍵から生成される
ビットコインアドレス（27～34文字）で指定

Aが新たに作成する送金記録			
入力		出力	
入力元	所有権	出力金額	出力先
ID=n Out=2	公開鍵（256ビット）、署名	10	B
ID=m Out=1	公開鍵（256ビット）、署名	5	C

署名は受取者だけが保有する秘密鍵
により作成（楕円曲線暗号の利用）

 15

作成された送金記録の検証（1）

ビットコインアドレスと公開鍵が一致するかどうか

Aが作成した送金記録		
入力		
入力元	所有権	
ID=n Out=2	指定した公開鍵（256ビット）	秘密鍵による送金記録への署名

使用する送金記録ID=n	
出力	
出力金額	出力先
8	Aのビットコインアドレス

参照

ハッシュ計算

ハッシュ値（160ビット）

アドレスへ変換

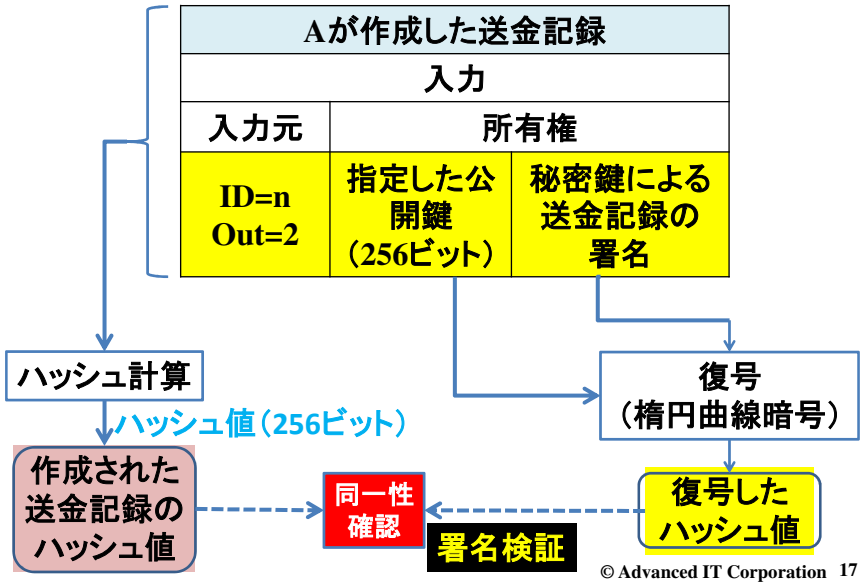
ビットコインアドレス
（27～34文字）

同一性確認

 16

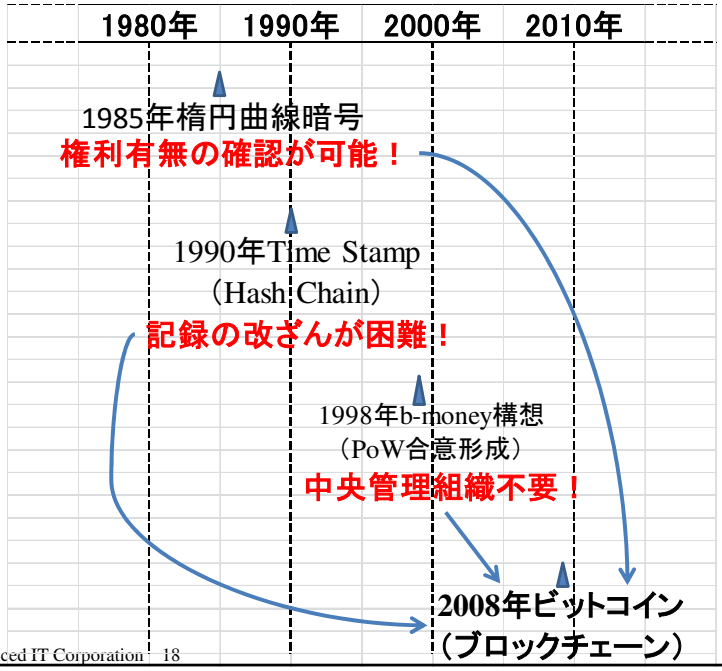
作成された送金記録の検証（2）

公開鍵に対応する秘密鍵で署名されているかどうか



 17

暗号技術の研究成果に支えられたブロックチェーン



 18

（3）ブロックチェーンの応用

ブロックチェーンの応用を考える前に

（1）ブロックチェーンのタイプ

管理：パブリック、コンソーシアム、プライベート

申請、参照：パーミッションド、パーミッションレス

（2）スマートコントラクト

ブロックチェーンに実装するビジネスロジック

（ビジネスロジックに応じたリアクションを実装可能）

スマートコントラクトは2013年に19歳のロシア人青年

Vitalik Buterinが発表したイーサリアムで初めて実装

スマートコントラクトという考え方は

暗号学者Nick Szaboが1996年に発表

（暗号学者Nick Szaboは1999年、”Bit Gold”構想を発表、

Satoshi NakamotoのBitcoinよりも半年以上前に仕様発表）

（3）ブロックチェーンの応用

ブロックチェーン応用 適用範囲による型の定義

型	目的	管理対象
保証	データの真正性保証	ハッシュ値のみ
保全	データの保全	実データも含め
履行	プロセスの自動実行	ビジネスロジックまで

（3）ブロックチェーンの応用

保証型：データ/システムの真正性保証技術としての応用

政府の記録データ、医療データ（カルテ）の真正性保証
　エストニアのe-Governmentを支えるX-Roadプラットフォーム
　で扱われている政府の記録（データ）は全てKSI署名で保護
　　KSI：Keyless Signature Infrastructure（guardtime）
　　キーレス署名は従来のPKI署名とは異なる代替方式で、
　　暗号鍵を使わないため、鍵の安全な管理を必要としない署名方式

データの所有者、データのアクセス権等の認証
　企業向け、金融機関向けの
　　認証だけのブロックチェーン（Keychain）

（3）ブロックチェーンの応用

保全型：記録技術としての応用

価値（資産）の移転の記録
　仮想通貨（現在2000種程度）
　美術品（作品の出所、所有に関する履歴の透明性確保）
　不動産（登記申請から登記審査、登記記録、自由な閲覧）
製造・調達プロセスの記録
　ダイヤモンド（スキャンし固有IDの付与、鑑定書他、原産地から
　　消費者までの全取引の透明性確保、自由に閲覧可能）
　農産物・畜産物・水産物等の加工商品・パッケージ商品
　医薬品、ソフトウェア、ハードウェア
権利・資格の記録
　医療ライセンス証明、学歴証明
重要情報の記録
　医療カルテ、公文書

（3）ブロックチェーンの応用

履行型：自動取引技術としての応用

著作権管理

音楽配信（中間業者を通さずに音楽を売買、
透明・確実な利益配分）

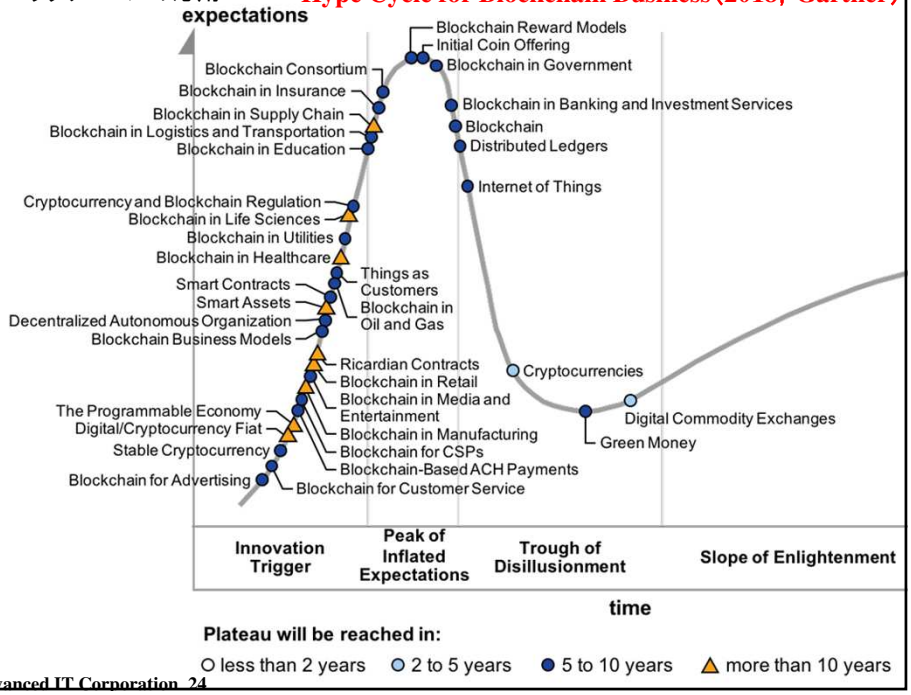
不動産取引（売主、買主、不動産業者のマッチング、
透明性のあるスピーディな取引）

電力流通決済システム

（30分ごとの入札、需給のマッチング、約定結果の記録）

（3）ブロックチェーンの応用

Hype Cycle for Blockchain Business（2018，Gartner）



（4）ブロックチェーンの新技術動向

BigchainDB（BigData+Blockchain）

開発元：BigchainDB GmbH（ベルリン）　発表：2016年2月
概要：大企業が求める処理能力、大容量、多様な検索・アクセス制御等の
　　データ管理機能に加え、ブロックチェーンの特徴機能
　　（記録データの不変性、分散コントロール、資産の登録・移転等）を提供
実現方式：ビッグデータ管理システム（MongoDB：NoSQL DBMS）へ
　　ブロックチェーンの特徴機能を付加
現状：オープンソースとして公開（機能強化は継続中）
　　世界で20社以上がパートナー企業となり、
　　応用PJが進行中（日本企業：リクルート、トヨタ）
　　トヨタは、MITのメディア・ラボ、ブロックチェーン技術企業と提携
　　具体的には、TRI（Toyota Research Institute）が主導
　　BigchainDBは、自動運転や自動運転テストの
　　データの安全な共有にための分散暗号化DBとして利用

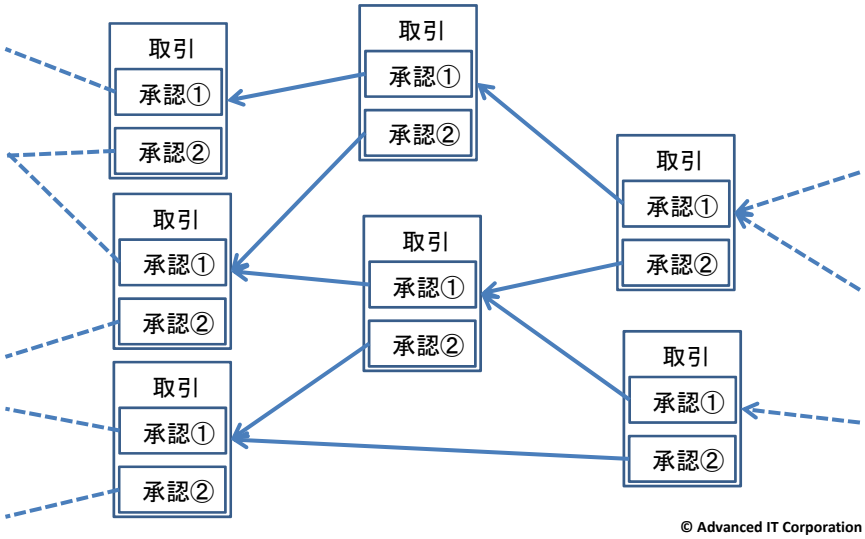
（4）ブロックチェーンの新技術動向

ブロックチェーンに変わる新技術？　DAG IOTA

開発元：IOTA Foundation（ドイツ）　発表：2016年7月
概要：機械と機械が直接取引を行うことを想定した、
　　IoT向けの仮想通貨/決済プロトコル
　　特徴は、マイナーが不要で、取引手数料がかからないこと
実現方式：既存のブロックチェーンとは少し異なり、
　　Tangle（DAG：Directed acyclic graph：有向非巡回グラフ）を使用
現状：オープンソースとして公開（機能強化は継続中）
　　2017年11月、IOTA上で分散型データ販売市場確立のため
　　20社以上とパートナーシップ契約
　　（マイクロソフト、富士通、シスコ、フォルクスワーゲン、サムスン等）

（4）ブロックチェーンの新技術動向

Tangle（イメージ）



 27

（5）おわりに

おわりに

（1）ブロックチェーンは仮想通貨ビットコインで初めて具現化された技術
　　資産の所有権が保証されるよう、暗号技術に支えられた仕組み
（2）ブロックチェーンの仮想通貨以外への応用の取り組みも活発
　　しかし、仮想通貨を超えるブロックチェーン応用は未だ存在せず
（3）ブロックチェーン関連技術の開発は活発
　　匿名性、追跡可能性、適用性（機能）、実用性（性能）、課題特化
（4）ブロックチェーン活用の要点は、適用対象分野の将来像の把握
　　ブロックチェーン技術は道具、目標に応じ開発、適否も判断
（5）国際標準化活動が活発化
　　ISO/TC307：2021年までに第1版、用語、コンセプトは2020年に
　　INATBA（EC：100以上の企業・団体）：2019年4月3日立上げ
（6）課題は、量子コンピュータ時代への準備
　　ブロックチェーンを支える暗号技術の危殆化への対応

 28

エストニア共和国

首都タリン
人口132万

IT立国を目指すIT先進国。安定した経済成長、政府主導のデジタル戦略、スタートアップ環境の整備等により、優秀な起業家・エンジニアの誘致に成功、欧州圏のIT市場のオフショア開発拠点へ。

e-Government構想：エストニア国民はICチップ入りの国民カード1枚で、投票から医療、教育、納税、銀行、警察関連など全ての手続がオンライン上で完結。

e-Resident構想：外国人もエストニアのデジタル市民となり、オンラインで行政サービスを利用したり、起業したり等が可能。（約165か国の5万人以上が登録済み（日本人も約2500人）。

Estcoin構想：国の公式通貨としての計画はとん挫
（欧州中央銀行総裁：ユーロ圏の通貨はユーロのみ）
エストニア大統領が ”e-Residency2.0”構想2018年12月発表
（e-Residencyコミュニティ内での利用を目指す模様）

 29

KSI：Keyless Signature Infrastructure

開発元：guardtime（エストニア）　試験：2008年　2012年：実運用

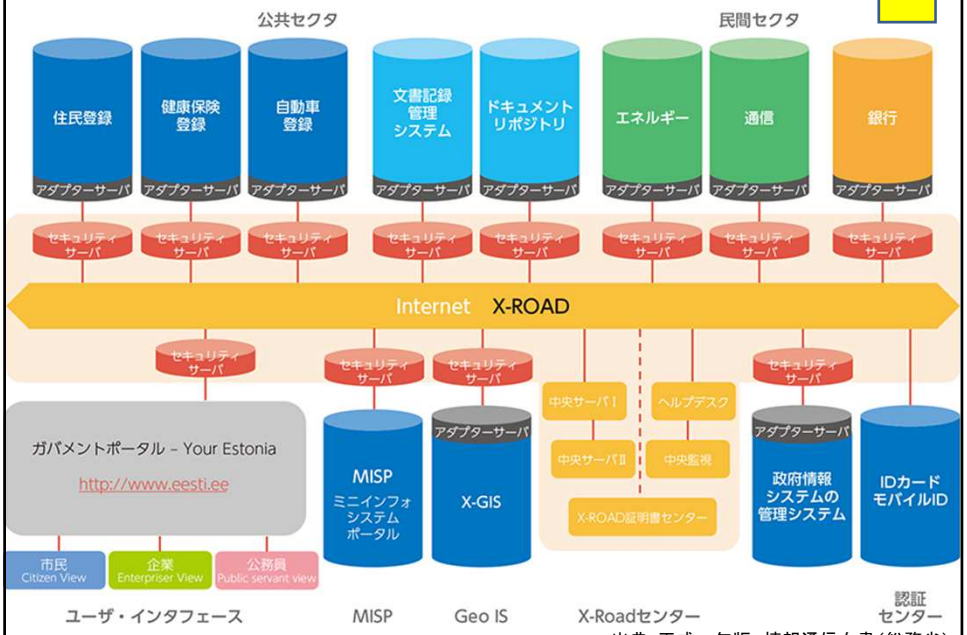
概要：キーレス署名は従来のPKI署名とは異なる代替方式で、
暗号鍵を使わないため、鍵の安全な管理を必要としない署名方式

実現方式：過去からのデータの要約（キーレス署名）をチェーンで結び、
改ざんを検知できる仕組み
（hash-linked time-stamping、データそのものの管理は対象外）

現状：エストニアのe-Governmentを支えるX-Roadプラットフォームで扱う
政府の記録（データ）は全てKSI署名で保護されている

 30

エストニアの電子政府アーキテクチャ



出典：平成27年版　情報通信白書（総務省）

最近の学会発表論文一覧（1/2）

①情報処理学会第81回全国大会
　才所敏明，辻井重男，櫻井幸一，”暗号仮想通貨における匿名化技術の現状と展望”
②2019年暗号と情報セキュリティシンポジューム（SCIS2019）
　才所敏明，辻井重男，櫻井幸一，”仮想通貨の匿名性の現状と課題”
③情報処理学会論文誌59巻9月号
　才所敏明，五太子政史，辻井重男，”「安心・安全電子メール利用基盤（SSMAX）」
　　悪意のあるメールの根絶とメール内容の確実な保護を目指して”
④夏のセキュリティワークショップ2018 in 札幌（CSEC82）
　才所敏明，辻井重男，”インターネット依存社会における
　　情報送信者・情報送信機器の匿名性と特定・追跡性”
⑤第81回コンピュータセキュリティ研究会（CSEC81）
　才所敏明，辻井重男，”安心・安全なIoTシステム(SSIoT)に関する考察”
⑥2018年　暗号と情報セキュリティシンポジューム（SCIS2018）
　才所敏明，辻井重男，”ビッグデータの社会活用推進上の課題に関する考察”
⑦2017年 暗号と情報セキュリティ研究会 (ISEC)
　才所敏明，五太子政史，辻井重男，”社会的課題「安心・安全な電子メール利用環境
　　の実現」のための三止揚・MELT-UP の試み”(ISEC2017-54)
⑧コンピュータセキュリティシンポジューム2017（CSS2017）
　才所敏明，五太子政史，辻井重男，”「安心・安全電子メール利用基盤（SSMAX）」”

最近の学会発表論文一覧(2/2)

⑨2017年 暗号と情報セキュリティシンポジューム（SCIS2017)
　才所 敏明，五太子 政史，辻井 重男，
　　”「安心・安全電子メール利用基盤（SSMAX）」構想”
⑩コンピュータセキュリティシンポジューム2016（CSS2016）
　才所敏明，五太子政史，辻井重男，
　　”標的型メール攻撃に対抗する「組織通信向けS/MIME」”
⑪2016年 暗号と情報セキュリティシンポジューム（SCIS2016)
　才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男，
　　”自治体・医療機関における組織暗号の実証実験”
⑫医療情報学連合大会（JCMI35）
　才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男，
　　”組織暗号の社会的実装に向けて”
⑬コンピュータセキュリティシンポジューム2015（CSS2015）
　才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男，
　　”自治体における組織暗号実証実験報告”
⑭情報処理学会誌論文誌56巻9月号
　才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男，
　　”組織暗号の構成と社会的実装－個人情報の安全な利活用を目指して－”

 33

終

 34