17:00～19:00 TTC BlockChain勉強会講演資料

『Blockchain 技術を取り巻く国内外のビジネス動向と将来展望』

～今後のテレコム業界の役割とは?～

2017年9月20日

藤原　洋

株式会社ブロードバンドタワー代表取締役会長兼社長CEO

株式会社インターネット総合研究所 代表取締役所長
一般財団法人インターネット協会理事長・IoT推進委員長
一般社団法人データサイエンティスト協会理事

IA japan

一般社団法人
データサイエンティスト協会

【目次】

１．ブロックチェーンが拓く未来とは？

～何のためのどんなテクノロジーなのか？～

●ブロックチェーンは、ビットコイン（FinTech）の要素技術として登場

●インターネットの基本概念『自律・分散・協調』を前提

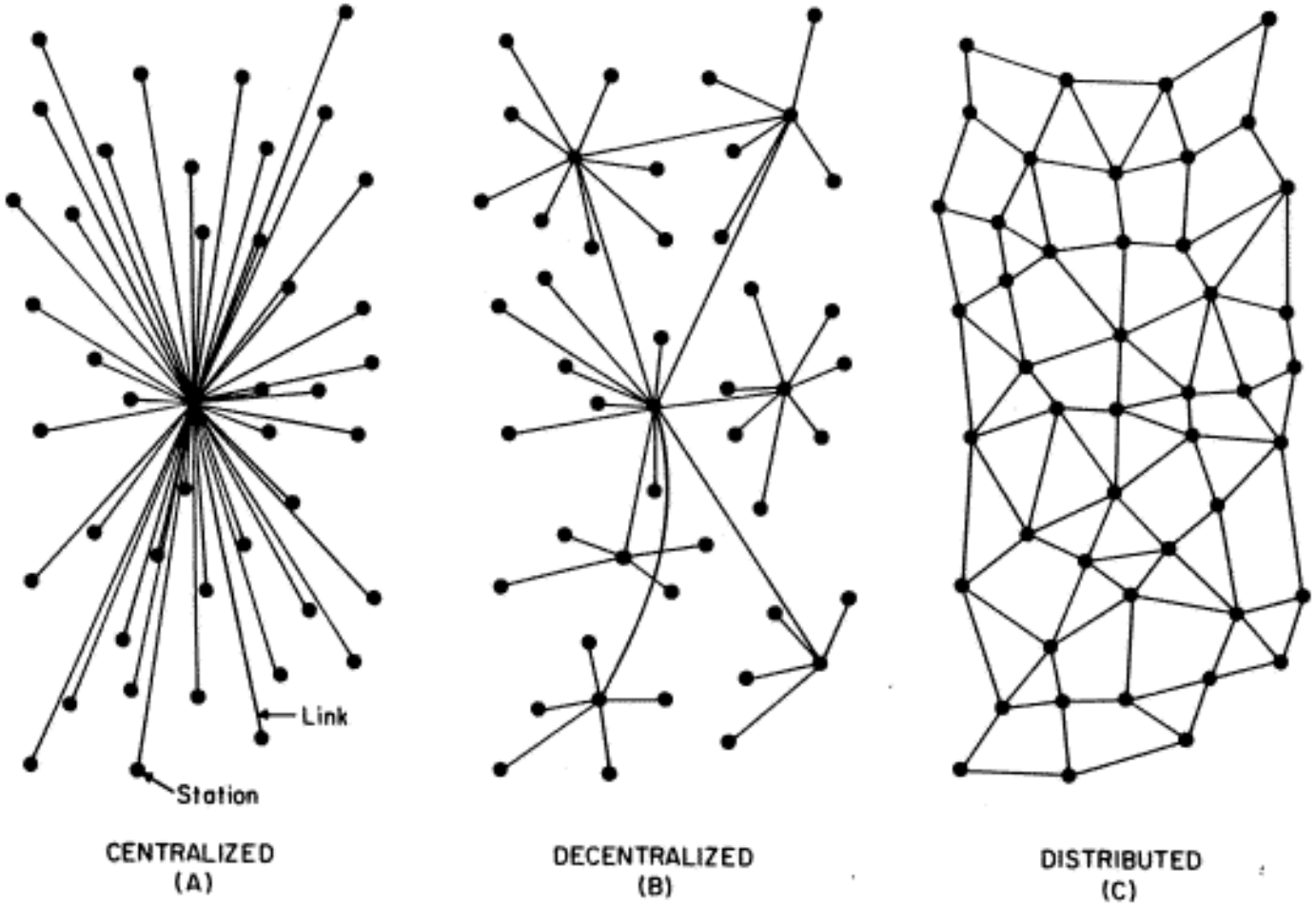


FIG. 1 — Centralized, Decentralized and Distributed Networks

http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography//atlas/baran_nets_large.gif

●インターネットを支える基盤技術の変遷

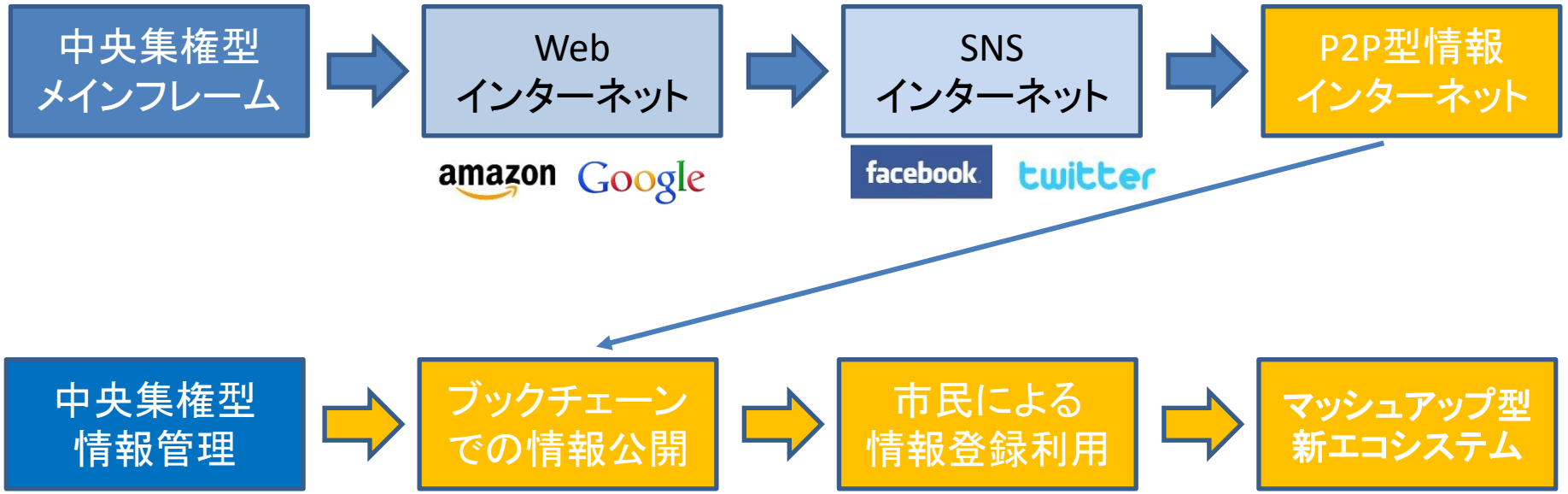
パケット交換
（1969年）

TCP/IP
（1982 年）

Web
（1989年）

Block Chain
（2008年～）

●コンピュータ・ネットワークにおけるインターネットの対比
VS
金融システムにおけるビットコイン（FinTech）
VS
情報管理におけるブロックチェーン



ブロックチェーンの持つ可能性は、分散/集中（囲い込み）/
分散への回帰現象としてのFinTechを超えた情報管理革命！

● ブロックチェーン技術の展開が有望な事例とその市場規模 （67兆円）

- 幅広い分野へ影響を与える可能性がある

出典：経済産業省「平成27年度 我が国経済社会の 情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに 関する国内外動向調査）」報告書概要資料

●イノベーションの起こる可能性

〇インターネットの商用化1990年（基本技術は1969年）

⇒Amazon1995年、Google1998年、Facebook2004年

〇スマートフォン2007年（GPS情報の自動アップロード）

⇒Uber2010年、

〇ブロックチェーン2008年（改竄のない情報発信）【ビットコインとして】

⇒様々な情報をブロックチェーンに記録するアイデアが増加

⇒簡単なアプリというよりもインターネット・インフラ技術としての
ブロックチェーンの基盤技術に習熟したエンジニア育成が必要

⇒シリコンバレー型“Fail First”よりも“Proof First”文化の育成が必要

ブロックチェーン**技術実装**の４つの基本原則

①非中央集権的情報管理
②改竄（かいざん）のない情報管理
③時系列的な変更履歴管理
④全ての人々による公開検証

⇒ビットコイン・プロトコルから中央管理なしに様々なアプリケーション開発の可能性が2014年に始動

●ブロックチェーンの由来

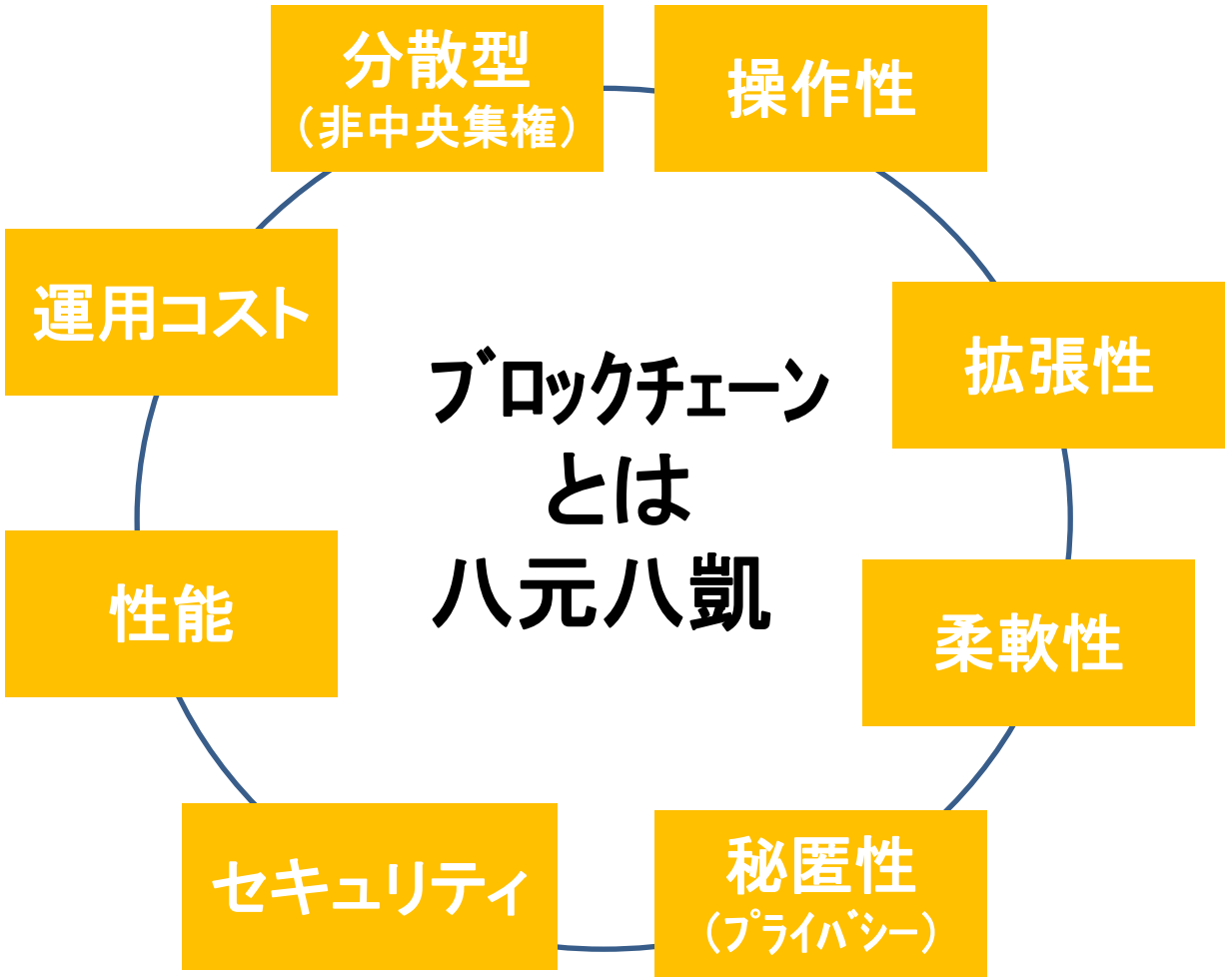
⇒複数の取引情報が「ブロック」という単位にまとめられ、
ブロックが1本に連なった「チェーン」状になって管理

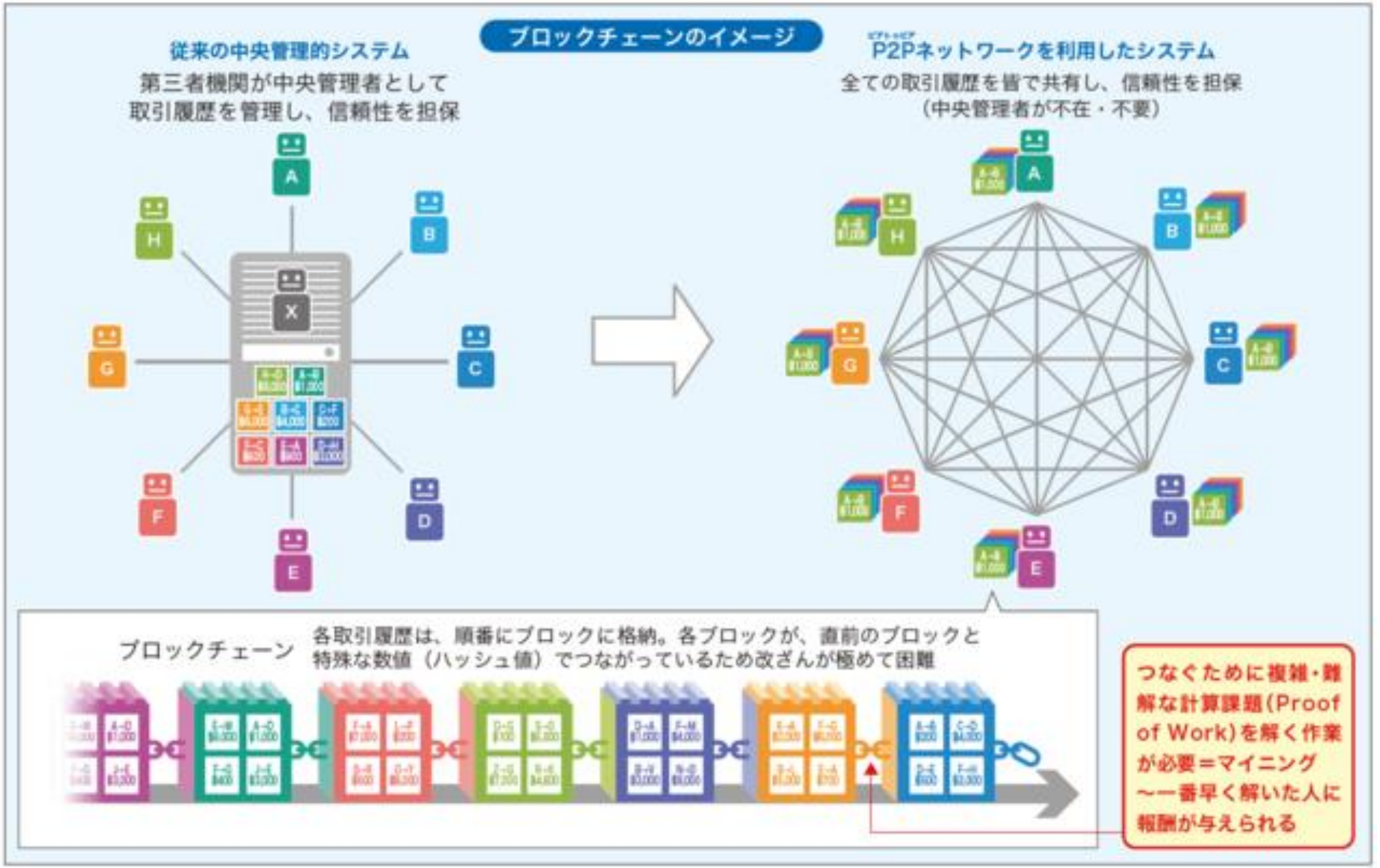
⇒日々発生する新たな取引がブロック単位にまとめられ
ブロックチェーンの最後尾に次々と追加される

⇒ブロック間をハッシュ値という特殊な数値でつなぐことで、
ブロック内容の改竄を防止

●ブロックチェーンが実現すべきこととは？

【八元八凱(はちげんはちがい):「元」は善、「凱」は高い徳】
〔高い徳を持っていて、清く正しい心の人物〕





出典：経済産業省「ブロックチェーン技術を利用したサービスに関する国内外動向調査」

●ブロックチェーンを支える3つの基本技術

①P2P

②公開鍵暗号

③ハッシュ関数

①P2P（Peer-to-Peer）

⇒ネットワーク上で対等な関係にある端末間を相互に直接接続し、データを送受信する通信方式。

⇒その通信方式を用いて通信するソフトウェアやシステムの総称

⇒データの送り手と受け手が分かれているクライアントサーバ方式等と対比される用語で、利用者間を直接つないで音声やファイルを交換するシステムなどが実用化されている

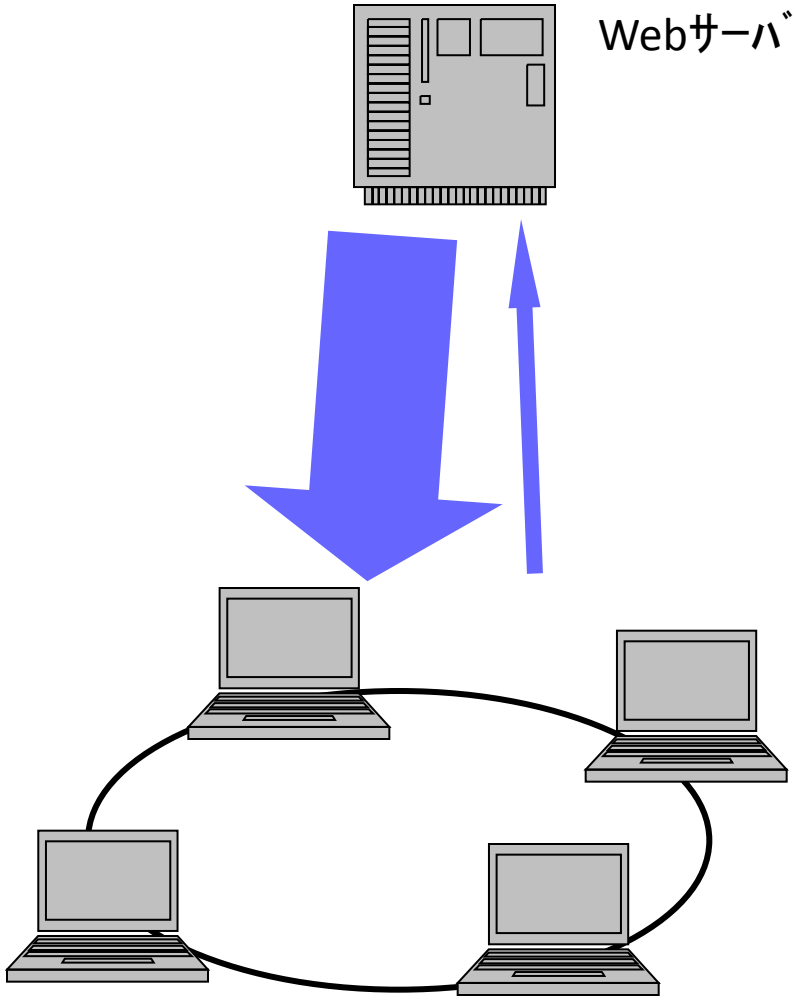
⇒P2Pシステム：データの種類、利用者参加方法により様々な種類

⇒特定利用者間をつなぐ1対1で音声通話、メッセージの送受信を行うインスタントメッセンジャー、インターネット電話、
バケツリレー式インターネット放送システム、不特定多数の利用者の匿名ファイル共有ソフト

【P2Pネットワークの本質】

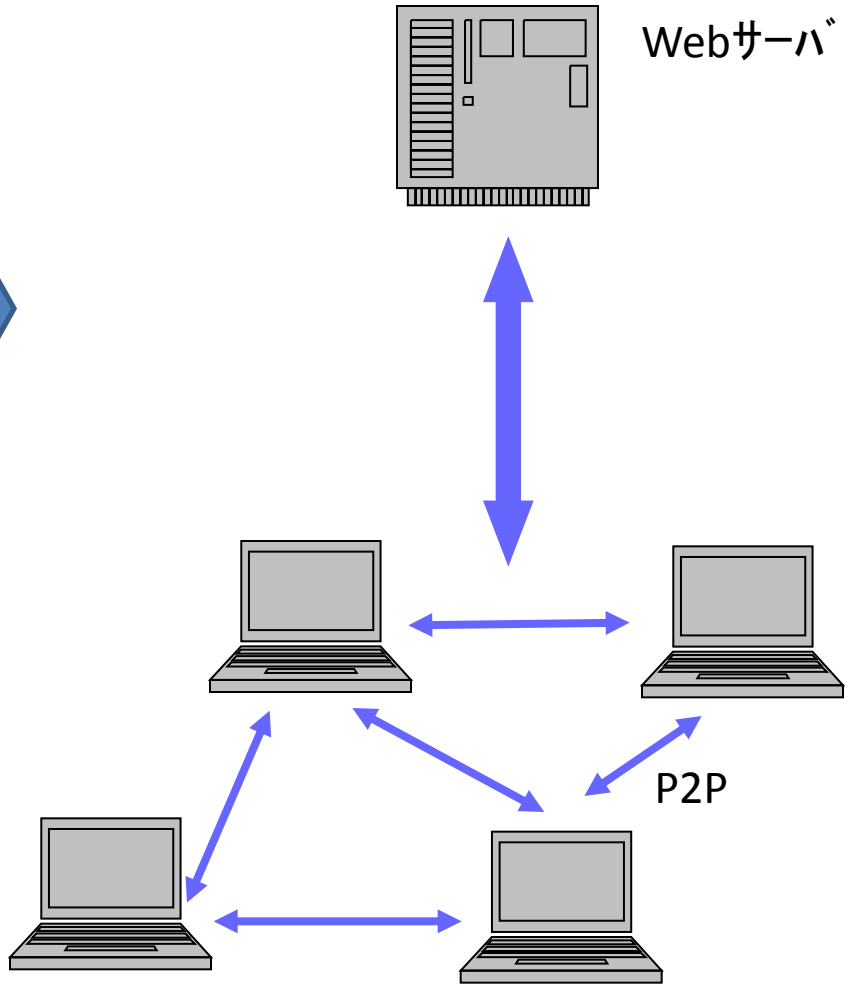
○現在のインターネット

＝非対称トラフィック



○今後のインターネット

＝対称トラフィックへ



②公開鍵暗号【 public key cryptosystem 】非対称鍵暗号 / asymmetric key cryptosystem

⇒対になる2つの鍵を使ってデータの暗号化・復号を行う暗号方式
（1976年にWhitfield DiffieとMartin E. Hellmanが基本原理を考案）
〔当時、各々、スタンフォード大学の研究員、教授〕

⇒暗号化鍵と、復号鍵を分離
（暗号化鍵で復号をできず、片方から一方を割り出すことは困難）

⇒鍵の持ち主は復号鍵のみを他人に知られないように管理し、
暗号化に使う鍵は公開（暗号化鍵は公開鍵、復号鍵は秘密鍵）

⇒公開鍵暗号で秘密メッセージを送受信する場合、送信者は受信者が公開している公開鍵を入手して暗号化し暗号化されたメッセージは受信者の秘密鍵でしか復号できないため、途中での第三者傍受で中身を解読されない
（公開鍵暗号考案まで、暗号化と復号に同じ鍵を用いる秘密鍵暗号〔共通鍵暗号、対称鍵暗号〕だけ）

②公開鍵暗号（つづき）

⇒秘密鍵暗号ではメッセージの送信者と受信者が同じ鍵(暗号表など)を共有するため、鍵を安全な経路で相手に届けなければならない。

⇒公開鍵暗号では暗号に使う公開鍵は第三者に知られても解読されないため、鍵の輸送が不要で、安全性が高い。

⇒公開鍵暗号は秘密鍵暗号よりも複雑でより多くの計算資源が必要

⇒暗号通信の場合、暗号化には即興で鍵を生成した秘密鍵暗号を使い、その鍵を送信者と受信者の間で安全に交換するために公開鍵暗号を使うといった使うことが多い

⇒公開鍵暗号は非対称な鍵を用いる特徴から、デジタル文書の正当性を保証するデジタル署名にも応用

*公開鍵暗号を実装するための具体的な暗号方式で有名なのは、巨大な整数の素因数分解の困難さを利用したRSA暗号、他に、離散対数問題の解の困難さを利用したElGamal暗号、楕円曲線上の離散対数問題を利用した楕円曲線暗号等。

③ハッシュ関数

【 hash function 】メッセージダイジェスト関数 / message digest function

⇒与えられた入力値から、規則性のない固定長の値を生成する演算手法。得られた値は「ハッシュ値」と呼ぶ。

⇒ハッシュ関数には、同じ入力値からは必ず同じ値が得られるが、少しでも異なる入力値からは全く違う値が得られるのが特徴

⇒不可逆な一方向関数を含み、ハッシュ値から入力値の割出し不可

⇒入力値がハッシュ値より長い場合、複数の異なる入力値から同じハッシュ値が得られる(ハッシュ値の衝突)が、ある入力値を元に、同じハッシュ値になる別の入力値を探索することは不可

⇒データの伝送、複製を行なう際に、入力側と出力側でハッシュ値を計算し一致すれば、途中で改ざんや欠落などが起こっていない

⇒暗号、認証、デジタル署名などの要素技術として利用されている。

●ハッシュ(hash)とは？

「今日はブロックチェーン勉強会です。」

d5a4508fdc93cac73a5eb91ab96c020e

⇒それだけでは意味不明の数値をハッシュ値という。
（ハッシュとは、データを投入して生成される数値のこと）

⇒元来、データに誤りがないかを確認するためのもの。

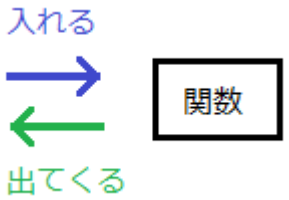
⇒通信速度が遅く、通信中にエラーも起きやすかったとき
送信者はデータと一緒にハッシュも送り、受信者は送られてきた
データを共通の計算式を利用してハッシュ値に変える。
その数値が一致していたら、OK問題なし！

⇒ハッシュは送信者、受信者のデータが一致しているか判断する
ために使用。

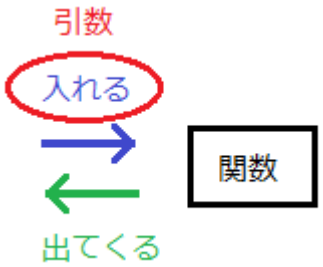
●ハッシュ関数 (hash function)とは

入力データに対して、適当に見える値（特定のルールに沿って、意味不明な値）を返してくれる関数

関数には、一般的には、入力を受けて処理を行い、その結果として出力がある。



関数に入れる値は「引数」（プログラムや関数に渡す値）と言う。



● ブロックチェーンの最初の応用＝ビットコイン

〇2008年にナカモト・サトシと名乗る人物により発表された論文に基づき
2009年に運用が開始された仮想通貨

〇P2Pネットワークにより運営されるため、トランザクション（所有権移転の取引）
はユーザー間で行われる。トランザクションの履歴を記録するのが、
公開分散元帳であるブロックチェーン

〇「誰でも閲覧可能な帳簿を用いて、人対人の決済を可能にしたシステム」

〇ビットコインの持つ革新性＝「中央管理が無い」「世界共通の通貨」

〇ビットコインはビットコイン取引所で購入可能（国内11か所）

bitFlyer　coincheck　bitbank Trade　bitbank　Zaif　BITPOINT

QUOINE　BTCBOX　みんなのビットコイン　Lemuria Bitcoin Exchange　GMOコイン

〇ビットコインを取引所で購入しビットコインウォレットというビットコイン専用
の財布にしまう。

●ブロックチェーンが最初にビットコインで用いられたか？

○電子マネーなどの研究は、1997年から約3年NTTと日本銀行で取り組んだ電子マネーや日立製作所が取り組んだ電子マネーのプロジェクトがあった頃が、最初の電子マネーブーム

○「Financial Cryptography」という名前の、暗号技術を金融サービスに応用する技術に関する国際会議が1997年にスタート。

○暗号技術の国際学会での暗号技術が、ビットコイン登場の背景。

○NTTデータが電子情報の原本性保証を行うサービスとして提供している「SecureSeal」（重要文書・データを電子化して保存する場合「いつから存在し、内容が現在まで全く変更されていない」ことを証明するタイムスタンプによる時刻認証と非改ざん証明 ）では、ブロックチェーンに近くハッシュ値をリンクして非改ざんを証明する技術を利用。

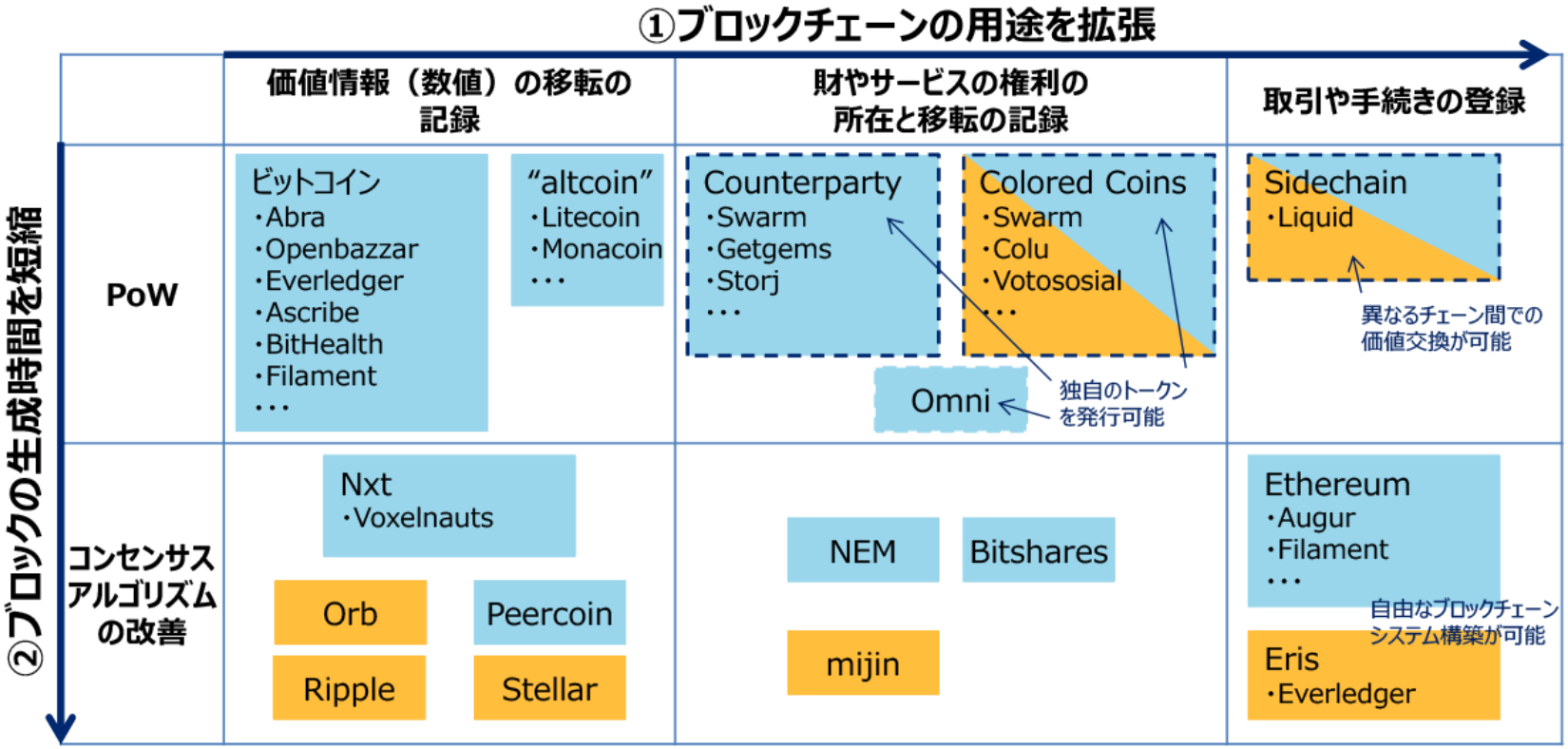
○1990年に学会で発表され、「ISO/IEC 18014-3（リンクトークン式タイムスタンプ）」として国際標準化されている技術。

○ビットコインは、ISO/IEC 18014-3にある考え方を使い、あるドキュメントの前後関係をハッシュの署名を連鎖させて確認できるサービス。

○トランザクションの開始から現在に至るまでのやり取りの一連を確認できるこの仕組みが、ブロックチェーンという技術の中核。

● ブロックチェーン技術の発展トレンド

- 3つの軸（注）で、ブロックチェーン技術の改変・発展が進んでいる



（注） 3軸の説明
①記録内容を数値に限らず、権利や契約条件等にも拡大
②ﾌﾞﾛｯｸ生成時間の短縮のための承認アルゴリズム等の改善
③ﾌﾞﾛｯｸ生成時間短縮やシステム堅牢性の負担軽減のため参加者を限定

6

出典：経済産業省「平成27年度 我が国経済社会の 情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに 関する国内外動向調査）」報告書

●ブロックチェーンが「分散型台帳（元帳）」技術と呼ばれる理由は？

〇ビットコインは、ブロックチェーンの応用形態で銀行の残高元帳を分散させたもの。

〇ブロックチェーンとは、公開検証可能なオープンデータに対して、誰もが新た情報を登録して確認できる技術。

〇信頼できる事業者がいなくても様々なサービスが実現できるため、スマートコントラクト（契約）分野での利用が拡大中。

〇物流のための情報をマッチングする中間業者や証券取引所等を代替するイノベーション。

●安全性の向上

〇未熟な技術で、セキュリティ要件やセキュリティを確認する手法は固まっていない

⇒2016年6月17日午後「The DAO」のハッキング事件が発生

⇒Dao事件：自律分散型投資ファンド「The DAO」が取引基盤とするイーサリアムベースのブロックチェーンがハッキングを受け

⇒The DAOのアカウントから仮想通貨イーサリアム（ETH）が流出。その後Slock.it（The DAOの発案元）は、The Ethereum Foundation（ETHの運営元）やEthereum　開発者との議論とコミュニティの協力でハードフォーク（該当仮想通貨のルールを変える際に旧ルールを無視し、新ルールを新たに適用することで旧ルールの互換性が無くなること）によって本件に対する対策

⇒このフォークの際にイーサリアムクラシック（ETC)が誕生
（フォーク前のイーサリアムはイーサリアムクラシックに名前を変え、
　新しいイーサリアムがそのまま名前をイーサリアムとした）

●安全性の向上（つづき）

〇The DAOのハッカーが巨額な利益を手にする時が来ている。

⇒ハッカーのアドレスを監視、追い続けているKhooという人物

⇒$100,000のETC（約1060万円）がハッカーのアドレスから移動され
2333ETCずつに分けて、更に別のアカウントへ送金し、ShapeShiftを使って
ビットコインに両替

⇒Koo氏によると、これはハッカーが今回初めて仮想通貨を現金として引き出そうとしている

⇒3.5ミリオンは換金されずにこのアドレスに残されたまま

⇒ハッカーはETC→ETH→BTCの順で資金を移動中

●安全性の向上（つづき）

〇The DAOはプログラム同士が取引をしたり、投資をしたり、自律的に経済活動をする世界観を実証しようとするプロジェクト

〇「Ethereum」というThe DAOが動作するプラットフォームの脆弱性（バグ）を突かれ、思ってもみないお金の流出が起きた事件

〇スマートコントラクトは、まだまだ運営も実現も困難との認識。

〇ブロックチェーンとしての安全性向上策

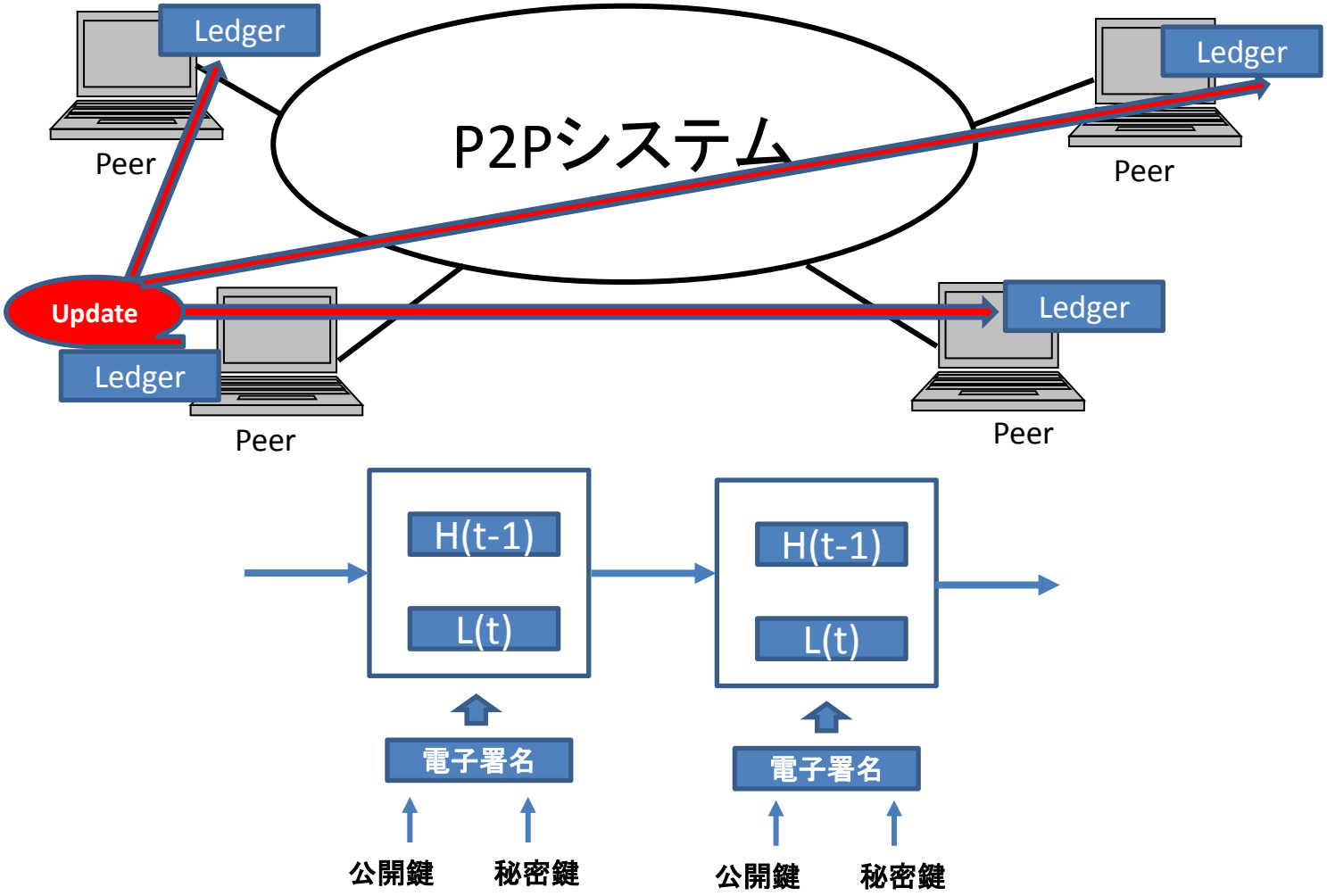
⇒P2Pのネットワークで繋がったユーザーが、公開管理されたレッジャー（元帳）に変更を加えていく。

⇒それらの記録は逐次伝搬されチェーンのように連鎖することと前後関係を証明

⇒その過程で電子署名が与えられ悪意ある改ざんを防ぐ。

●ブロックチェーンと公開元帳との関係

Ledger(元帳)は、Peer-to-Peerネットワークで各Peerに分散公開管理され、内容が更新されると即座に共有され、連鎖的な電子署名で内容が保証される。



●ブロックチェーン技術のポイント

〇分散システム＝支配的な権限がなく集中管理システムが不要

〇ビットコイン＝発行体が存在しない通貨ながら、法定通貨との交換を行うための取引所ができ利用者の秘密鍵が保存

⇒想定していない支配的な権限を持つ人が生まれる可能性があり不完全

⇒「Mt.Gox」事件：本来ビットコインが持つ非中央集権という性質を悪意のある取引所が行った

〇非中央集権を保ちながらアプリケーションを増やせるようにする改良が必要

〇スマートコントラクト的には、プログラム言語を堅牢なものに作り直す

⇒バグを減らすデバッガーやチェッカー（安全性検証）

⇒プロトコル自体の脆弱性を下げるためのフォーマル・ベリフィケーション（形式検証）が重要

●ブロックチェーン技術のトレードオフ

〇セキュリティを強めると運用コスト/操作性/性能が低下

〇ブロックチェーンの場合：さらに・・・

「どれくらい非中央集権を高めるのか？」

〇2015年あたりから、ビットコインのブロックサイズをどれくらいに変えるか？が論点

⇒現在ビットコインの仕様、1つのブロックのデータサイズには現在1MBの上限

⇒1ブロックは10分に1回作成

⇒1GBにすればスケーラビリティが劇的に向上
（7トランザクション/secのブロックチェーンの処理速度向上）

●ビットコインのスケーラビリティ

①新ブロックは1回/10分しか生成されない。

②ブロックサイズは1MBが上限。

③トランザクション数の上限7/秒（⇔VISAカード：10000トランザクション/秒）

現状：　トランザクション・スケーラビリティの向上が課題

スケーラビリティが上がらないと、使い勝手が悪く、クローズドな仕組みが出る！

速度が向上して利便性が上がると、パブリックブロックチェーンへ自然に移行！

２．ブロックチェーン技術の概要

2.1　ブロック-チェーン（block chain）とは？（その1）

〇インターネットで相互接続されたコンピュータに、公開鍵暗号などの暗号技術を組み合わせ、取引情報などのデータを同期して記録する手法。

〇ビットコインなどの暗号通貨に用いられる
　基盤技術。

〇一部のコンピューターで取引データを改竄(かいざん)
　しても、他のコンピューターとの多数決等の相互チェックによって
　正しい取引データが選ばれる。

〇取引情報の履歴が鎖状につながれていることに由来。

〇分散型台帳（元帳）。

〇金融取引などの記録をコンピュータのネットワーク上で管理する技術で、インターネット上の複数のコンピューターで取引の記録を互いに共有し、検証し合いながら正しい記録を鎖(チェーン)のように繋いで蓄積する仕組み。

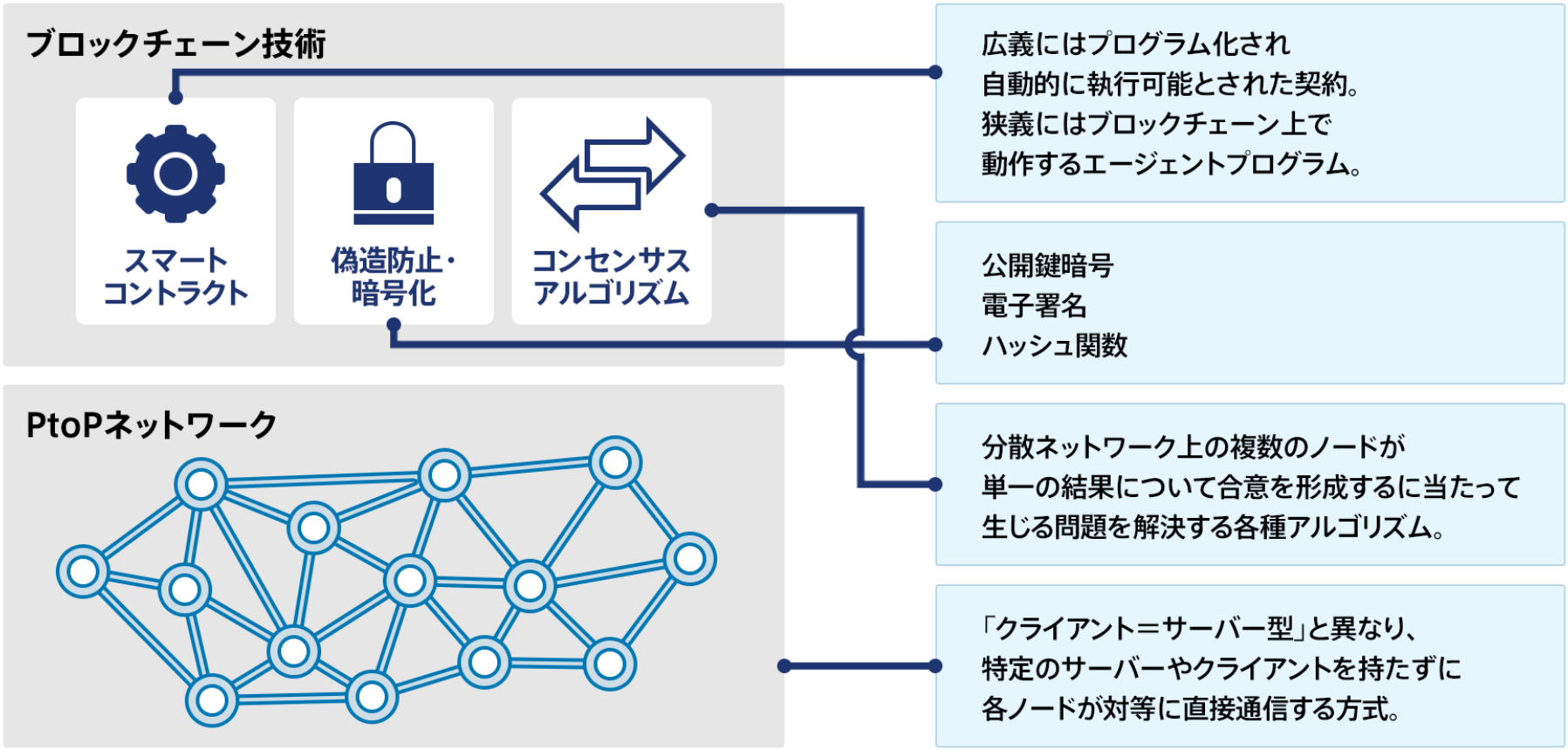
〇「分散型台帳」ともいわれ、記録を共有し、検証し合うため、記録改ざんや不正取引が防げる。

〇取引記録を集中管理する大規模コンピューターが不要なため、運営コストが割安なのが特徴。

〇仮想通貨「ビットコイン」の取引を成立させるために開発された技術、金融にIT技術を活用するフィンテック分野を中心に応用が多様化。
（住信SBIネット銀行、横浜銀行、りそな銀行など「国内外為替の一元化検討に関するコンソーシアム」は、年内に新送金サービスを開始）

●ブロックチェーン技術の概要

公開鍵暗号＋Hash関数＋P2Pネットワーク技術によるチェーン構成！



出典：NTTデータ

●「ハッシュ関数」と「ハッシュ値」

○データの受け渡しの際、改変されていないかを確認する技術

○元のデータと受け取ったデータを比較すればよいが、処理の簡素化のため、「ハッシュ関数」を使って、「ハッシュ値」と呼ばれるデータを作り、それを比較

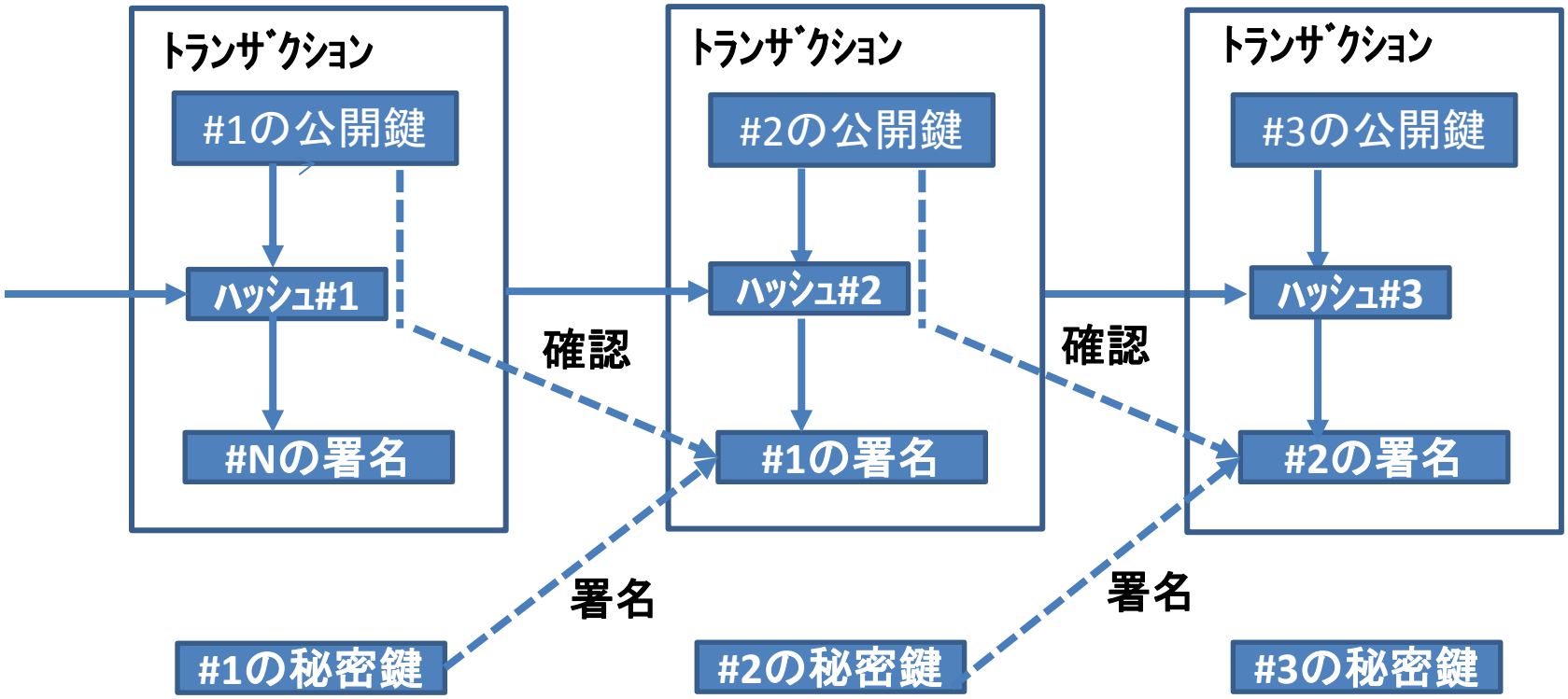
○一定の法則でデータを短くして同じ長さに揃えたもの＝「ハッシュ値」
⇒この方法＝「ハッシュ関数」

○違うデータから同じハッシュ値ができない、ハッシュ値から元のデータを復元できない
⇒元データを送る際にハッシュ値も送信し、受信者は受け取ったデータからハッシュ値を計算し、同じになればデータが改変されていないことになる！

○ハッシュ関数には複数方式があり、ハッシュ値が大きいほど安全性が高い
⇒以前は、MD5（ハッシュ値：128ビット）と短く使われない。（Message Digest 5）
⇒その後SHA-1（ハッシュ値：160ビット）：　Secure Hash Algorithm
⇒現在は SHA-2（224、256、384、512ビット）へ移行を推奨
＊ SHA-2は、アメリカ国家安全保障局(NSA)によって設計され、2001年にアメリカ国立標準技術研究所 (NIST)によってFIPS PUB 180-4として標準化された暗号学的ハッシュ関数

●ブロックチェーン技術の本質

各トランザクションは、前のトランザクションのハッシュ値、新たな所有者の公開鍵を含み、元のコインの所有者の暗号鍵によって電子署名される！



2.2 P2P技術の世界

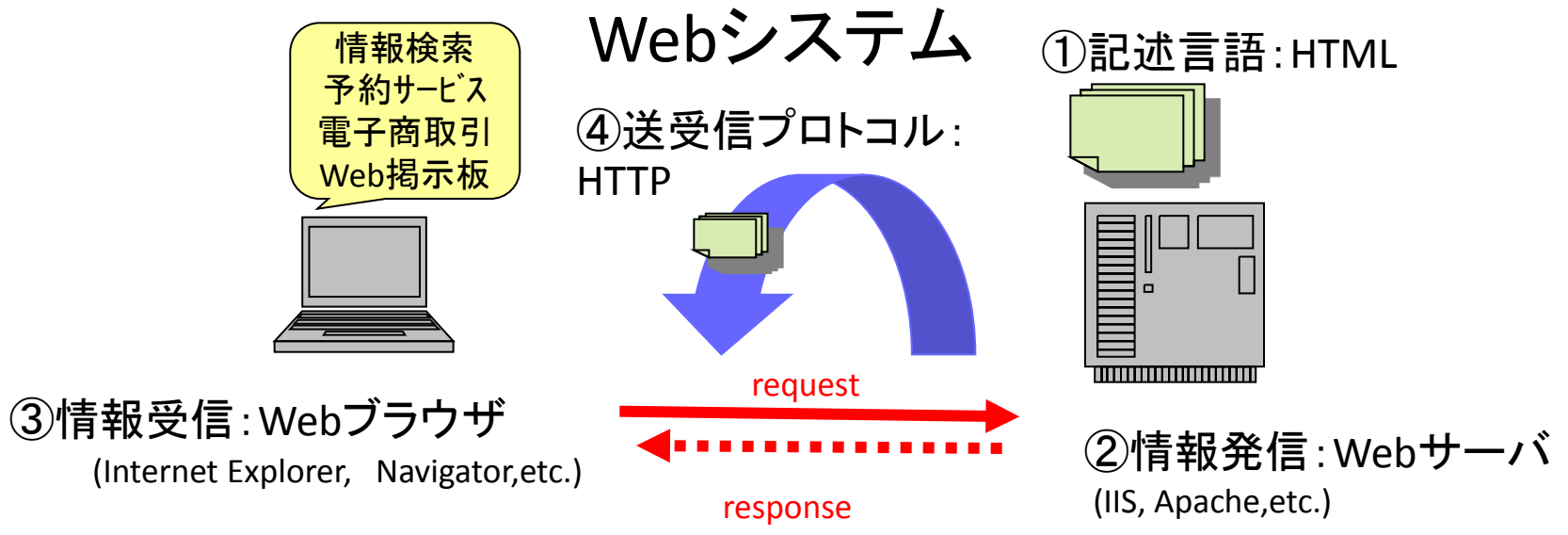
P2Pとは？　　P2P＝Peer to Peer

Peer とは同等の人、対等の人、同僚、友人、仲間

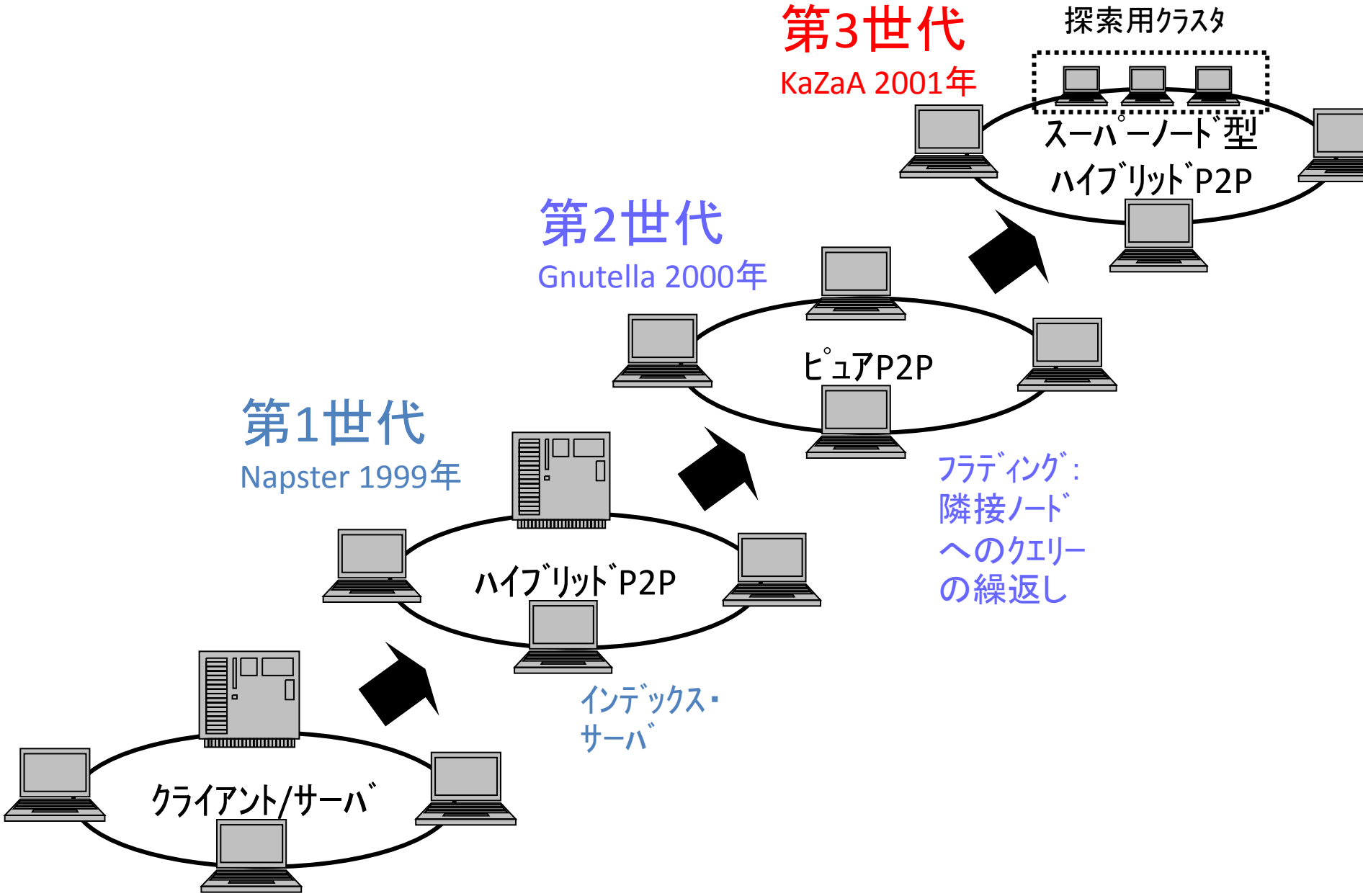
対立概念：　P2Pシステム　⇔ｸﾗｲｱﾝﾄ/ｻｰﾊﾞｼｽﾃﾑ

ｸﾗｲｱﾝﾄ/ｻｰﾊﾞｼｽﾃﾑの例＝World Wide Web

WebとP2Pとの相違



P2Pの発展経緯


第3世代
KaZaA 2001年
探索用ｸﾗｽﾀ
ｽｰﾊﾟｰﾉｰﾄﾞ型
ﾊｲﾌﾞﾘｯﾄﾞP2P
第2世代
Gnutella 2000年
ﾋﾟｭｱP2P
ﾌﾗﾃﾞｨﾝｸﾞ：
隣接ﾉｰﾄﾞ
へのｸｴﾘｰ
の繰返し
第1世代
Napster 1999年
ﾊｲﾌﾞﾘｯﾄﾞP2P
ｲﾝﾃﾞｯｸｽ・
ｻｰﾊﾞ
ｸﾗｲｱﾝﾄ/ｻｰﾊﾞ

●P2P技術の概要

1．ハイブリッドP2P（Napster：音楽MP3ファイル交換訴訟に)

・データの場所を探索するインデックス・サーバ

・データアクセスはサーバに集中しない

・Napster：　Shawn Fanning(Northeastern Univ.学生)が開発

2．ピュアP2P（Gnutella：米Nullsoft社、サービス主体不明で未訴訟)

・データの場所を探索するフラディング技術

・隣接ノードへ探索クエリーを発行（TTL：Time to Live/ Gnutella＝7)

・ Gnutella：　Justin Frankel とTom Perpper

3．スーパーノード型ハイブリッドP2P（蘭FastTrack社）

・データの場所を探索するスーパーノード・クラスター

・一般/スーパー・ノード数割合＝一定

・ライセンスビジネス⇒Skypeが利用

●P2Pの特長

①冗長性：　全ノードがバックアップ機能）

②拡張性：　アクセス集中がない

③オーバーレイ機能：　セグメント境界の意識不要

④非同期アクセス機能：　ローカル・データ処理機能

⑤オフラインアクセス機能：　同上

⑥アドホック構成：　参加者同士の合意で参加が成立

●P2Pを支えるオーバーレイ・ネットワーク技術

①下位のネットワークレイヤ（IP）を抽象化する

②IPレイヤ（IP）：ルータ、スイッチ、ファイアウォール
などでセグメント化され、セグメント間のノード同士の
直接接続は通常は不可

③通常のアクセス：サーバ名/フォルダ名/ファイル名
【データの所在は、固定的に】
⇒データを複数ノードに分散設置し同一IDでアクセス
⇒位置透過技術

●P2P技術の社会への波及

1. 個人利用では「インターネットの匿名性」と連動

   ⇒情報を匿名で入手可能

   ⇒情報の入手経路が特定困難

   ⇒P2Pファイル交換による違法コピーが流行

2. ビジネス利用で用途が拡大

   ⇒Groove社（Microsoftが買収）のP2Pグループウェア：

   サーバ不要の企業横断型情報共有環境

   ⇒BitTorrentのP2P型CDN　(Contents Delivery Network)

3. ビットコインと共にブロックチェーンが登場

   ⇒ビットコインからFinTech市場が創生

   ⇒新産業創出への期待

●ノード探索技術（１）

フラッディング

（洪水、氾濫などの意味。IT用語では、ネットワークに接続されたシステムに許容量を超えるデータが流入する現象。P2Pではノード探索技術の１つを指す。）

〇バケツリレー

〇探索クエリー：情報保有ノードへ到達すると来たルートを帰る

〇帰りルートのノードに保有場所をキャッシュ記憶する

〇同一クエリーを再転送しない

〇TTL (Time To Live)を設定

〇カテゴリーリスト作成し一括してクエリー発行

●ノード探索技術（２）【DHT方式】

○情報保有ノード固定方式の欠点

⇒フラッディング（大規模化困難）

インデックスサーバ方式（負荷集中）

○DHT (Distributed Hash Table:分散ﾊｯｼｭﾃｰﾌﾞﾙ）登場

○Hash値＝一方向性変換で得られる固定長値

○Hash関数：あるデータが与えられた場合にそのデータを代表する数値を得る操作、又は、その様な数値を得るための関数のこと。

○Hash値は、元データとHash関数が同一なら同値

○DHT探索：Hash値を求めHash値と情報所在のﾏｯﾋﾟﾝｸﾞ

●ノード探索技術（３）【DHT方式】

○DHT (Distributed Hash Table:分散ﾊｯｼｭﾃｰﾌﾞﾙ）方式

ハイブリッドP2P方式と同様にデータ追加時に登録必要

○登録：　Hash値と情報保存場所の組

○登録先：　複数が分散配置（固定でない）

○インデックスノード：複数の分散配置された管轄の領域のHash値と所在場所ﾃｰﾌﾞﾙを保有

○情報保有ノード：対象データのHash値に近いHash値を持つインデックスノードに登録

●ノード探索技術（4）【DHT方式】

○DHT (Distributed Hash Table:分散ﾊｯｼｭﾃｰﾌﾞﾙ）方式
　における探索はインデックスノードへのアクセスで開始

○インデックスノード中で最もHash値の近いHash値を持つ
　ノードへクエリーを発行

○該インデックスノードが管轄でない時更にHash値の近い
　インデックスノードへクエリーを転送（繰り返す）

○対数的に収束：　100万ノードで20回

○フラッディングのように発散せず効率的

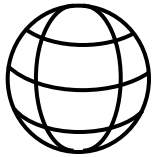
●P2Pルーティング技術（１）

「インテリジェント・ルーティング」

- ○　FastTrack社が実装
- ○　Skype（IP電話）の基本[当初、現在はクラウド】
- ○ 常に複数のルーティングパスを保持
- ○ 通話中でもより広帯域パスを見つけて切替
- ○ 耐ネットワーク障害性に優れる

●P2Pルーティング技術（2）

「オニオン・ルーティング」



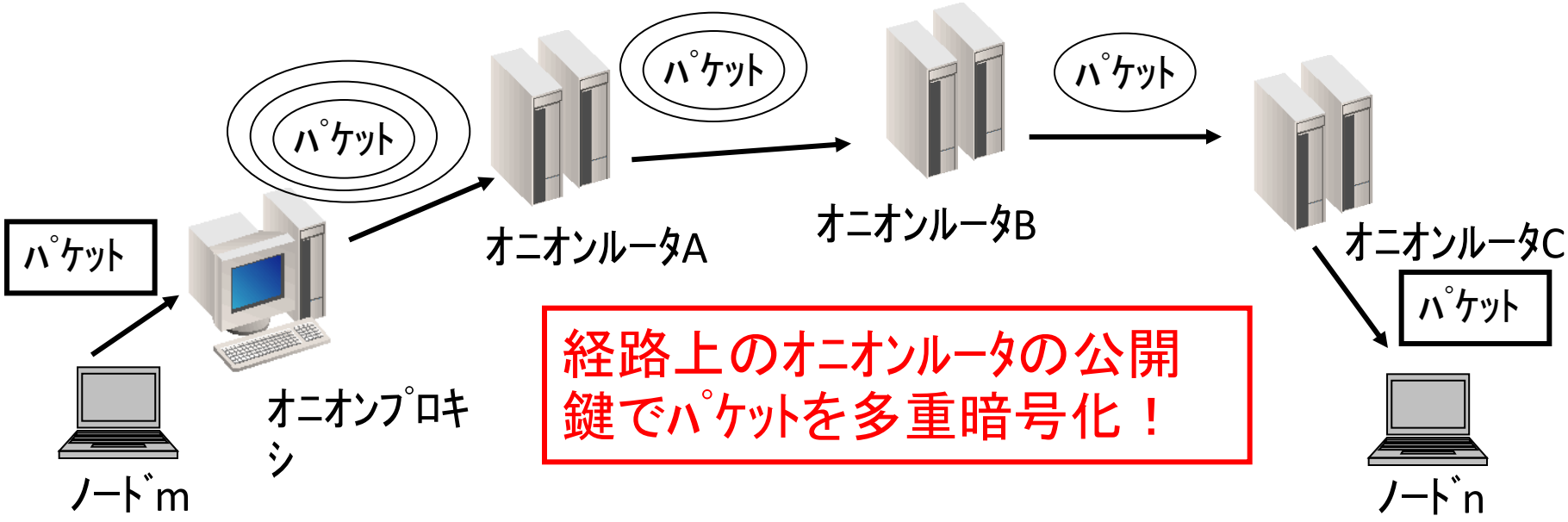
○TCP通信路を暗号化

○ IPアドレス部も含めて暗号化

○何重にも皮を被せた暗号化＝オニオン

○オニオンルータ＝１ペアのPKI（公開鍵基盤）の公開鍵と秘密鍵を保有

○オニオンルーティング・ユーザーは、ローカル常駐のオニオンプロキシに一任



2.3 Bitcoinとは？【ブロックチェーンの最初のアプリケーション】

〇銀行という中央を経由せず、直接、1対1での「通貨」を取引できる仕組み。

〇クライアントモデル/サーバーモデルによる信用なしに、取引可能。

〇P2P（Peer-to-peer）技術と、公開鍵暗号などの暗号技術で実現。

〇Bitcoinによってはじめて実現されたが、現在、Bitcoinの他にも多数存在。

⇒「暗号通貨」（Cryptocurrency; クリプト・カレンシー）

⇒ファイル共有やVoIP等P2P技術には、様々な方式が存在するが、Bitcoinは、単純で通信の暗号化もないP2Pのネットワークを形成。

●Botcoin「通貨」の表現＝P2Pでの「取引履歴」

○すべての取引履歴のかたまりとして表現

○「トランザクション」(取引)を定義

⇒各トランザクションは、前のトランザクションのハッシュ値と新たな所有者の公開鍵を含み、元のコインの所有者の暗号鍵によって電子署名される。

⇒全トランザクション情報は、P2Pネットワーク全体で共有

○ハッシュ値は、必ず任意のデータを同じ長さのデータになる値

〇取引データを単に保存しているだけのデータベースと異なり、
鎖のようにデータを結びつける！

⇒鎖のようにというのは、一つ前のブロックのハッシュ値を次の
ブロックの中に含めている からそう呼ばれる
（ハッシュ値とは任意のデータ を変換し同じ長さのデータ になる値）

⇒元データを変更すると変換後のハッシュ値は全く違ったデータに

⇒この特徴を利用して、ブロックチェーンでは、ハッシュ値は、
取引記録の改ざん対策 として利用

⇒一つ前のブロックのハッシュ値を次のブロックに含めることで、
前のブロックが改ざんされると、次のブロックの中に含まれる
ハッシュ値も変わり、そのブロックのハッシュ値も変わる

⇒そのブロックのハッシュ値が変わると次のブロックのハッシュ値も
変わる！

〇取引を表現することで通貨としての多くの特性を表現できる

⇒あるコインについて元の所有者の許可なくコインを本人以外が勝手に譲渡することはできない

⇒第三者が、他人同士のコインの譲渡を、客観的に確認可能

〇この仕組みだけでは、これを通貨として用いることは不可

⇒二重譲渡の防止の仕組みがないため

〇二重譲渡とは、元のコインの持ち主が、二人以上の相手に、全く同じコインを譲渡すること

⇒どちらかの譲渡を、ネットワーク全体で、正しい取引として決定

⇒一般的には、時系列的に後の取引を無効とみなすのが自然

⇒P2Pネットワーク上でなされるので、どちらが先か決定不可

○ブロックチェーンで二重譲渡を防ぐ

⇒ネットワーク全体で、特定のどちらか一方のみを一貫して、正しい
　取引であると決定できること

⇒不正を働くことができるのは、コインを持っている人だけ

⇒矛盾する二つの取引のあるとき、厳密にどちらの取引かは、あまり重要でない。

⇒Bitcoinで導入されたのが、「ブロックチェーン」という仕組み。

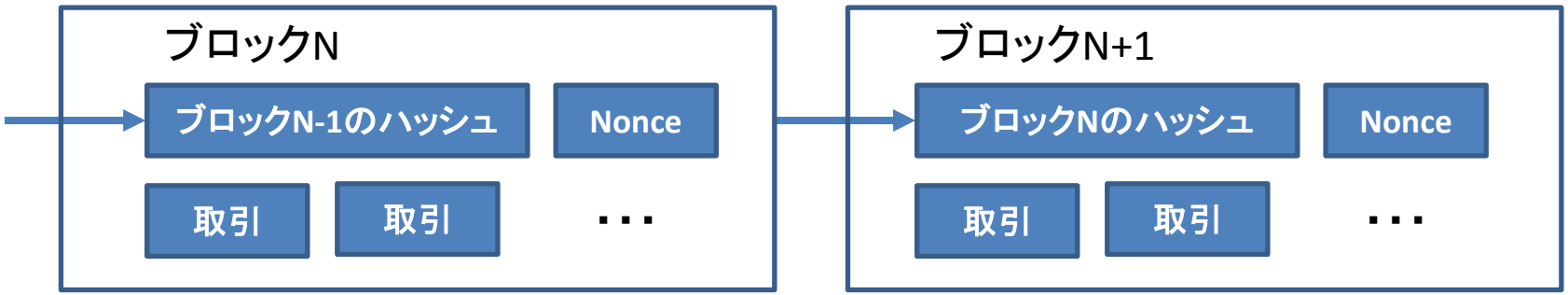
⇒「ブロック」は多くのトランザクションと、「ナンス」と直前ブロックのハッシュを持つ

＊Nonce:暗号通信で用いられる、使い捨てのランダム値、認証の過程で使われ、リプレイ攻撃を阻止。
具体例として、HTTPのDigest認証では、パスワードのMD5ダイジェストを計算する過程でナンスを使用

⇒「ブロック」に含まれた取引のみを「正しい取引」と認めることにする。

⇒ネットワーク全体で「唯一のブロックの鎖」を持つようにする。

⇒以上で一貫した取引履歴を全体が共有できる＝ブロックチェーン



●ブロック生成の仕組み

○「特権的立場を持った存在のいない平等な通貨」という性質から特定の誰かにブロックを生成する権限を与えることはない。

○誰でも無条件でブロックを生成できるとすると、「唯一の正しいブロックの鎖」なのか、誰にも分からなくなるため無条件生成はない。

○「仕事の証明」（Proof-of-Work, PoW）の仕組み。

⇒各ブロックについて、SHA-256ハッシュを取る。

⇒ハッシュの先頭に、一定の数以上の0が並んでいるブロックのみを、「正しいブロック」として、ネットワーク全体で認める

⇒ブロックには、ナンスと呼ばれる特別な値が含まれており、ナンスを変えることで、ブロック全体のSHA-256ハッシュを変化させることができるため、条件を満たすハッシュを持ったブロックを作成可能。

●SHA-256などのような暗号学的ハッシュ関数

⇒ハッシュ値から、簡単にデータを逆算できないように設計

⇒全探索・総当り以外の方法で条件を満たすようなナンスを探すことは不可

⇒計算資源を使わないと、条件を満たすブロックを生成することができない

⇒ブロックの作成に「誰でも作成できず、特定の誰かのみが作成する権限を持つこともない

⇒P2Pネットワーク上の各ノードは、ナンス値を変化させながら、全探索・総当りで条件を満たすブロックを発見しようと努力し、見つけたノードは、そのブロックを他ノードに配信し、ネットワーク上の全てのノードがこれを認める。

⇒ブロック生成の難易度は、過去のブロック生成速度に応じて、およそ10分に1個のブロックが発掘されるよう、適切な値が設定されいる。

⇒コンピュータの性能はムーアの法則で向上し、探索の難易度（つまり、ハッシュの先頭にいくつ0が必要か）が一定のままだとすると、やがてブロックはただ同然の計算資源で生成できるようになってしまう

⇒一方、ネットワークに参加するノードが増えるにつれてブロックの生成速度が次第に速くなっていってしまうということも意味し、望ましくない

⇒コンピュータの性能の共に難易度を変化させる必要あり

ブロック（例）

Hashes	
Hash	00000000000000000358fa848b19facc99fa1d6d56775eeee5025d8f34f77b31f
Previous Block	00000000000000009197fd818efbc538a31f5fd35e4b2c5bfd6e2fbec851620d

ブロック #289683（例）

概要	
取引件数	256
合計出力	2,596.80678367 BTC
推定取引量	659.24214953 BTC
取引手数料	0.02779968 BTC
ブロック高	289683 (主鎖)
タイムスタンプ	2014-03-09 09:24:56
受け取り時刻	2014-03-09 09:25:07
中継所	50.159.45.177
難易度	3,815,723,798.81
ビット	419504166
サイズ	122.449 KB
バージョン	2
ナンス	3258658318
ブロック報酬	25 BTC

3. ブロックチェーンの応用分野

3.1 FinTechとは？　FinTechサービスとは？

●FinTechとは？

FinTech = Finance（金融）× Technology（技術）

金融とITを掛けあわせた領域 ⇒特にインターネット技術

●FinTechサービスとは？

〇既存の「金融」機関がオンライン「テクノロジー」を使ったサービスは、「FinTech」サービスではない！

〇「インターネット企業」による金融サービスが、「FinTech」サービスである！

FinTechが登場した技術的背景

①5大DT（デジタルトランスフォーメーション）技術（「ポータル」「SNS」「IoT」「ビッグデータ」「AI」）を中心とするテクノロジーを駆使した「FinTech」サービスが、既にシリコンバレーを中心とした新興企業によって、続々と登場

②新興企業による「FinTech」は、従来の金融機関が独占的に提供し、変わりばえのしない金融商品や金融サービスを、
ネットユーザー視点で、「安く、早く、便利」に変化させたもの！

③FinTechも第4次産業革命の潮流の1つ！
ここで生まれた新たなテクノロジーが「ブロックチェーン」

●テクノロジー視点のFinTechとは？

〇FinTechとは、「FinanceとTechnologyを組み合わせた造語で、スマートデバイス、ビッグデータ分析、人工知能（AI）など新世代のITを活用した金融サービスを指す」と定義

〇FinTechの起源は、リーマンショックから始まった世界金融危機後、米国シリコンバレーにおいてベンチャー起業家が、既存の金融サービスが行き詰ったことをビジネスチャンスととらえ、いち早く新たな金融サービスの開発に取り組んだことにある

⇒こうして生まれた企業を「FinTech企業」と呼び、シリコンバレーから全世界に波及

インターネット企業がFinTechサービスを提供

主体が独立した「インターネット企業」だからこそ、各金融機関の壁を取り払い、横断的な「お金」に関するサービスを提供可能

「金融機関」がFinTechサービスを提供

金融機関が行うと、どうしても自らの金融商品を推すため、中立性に欠け、ユーザーに最適なサービスを提供不可（？）

社会的には「金融機関」と「インターネット企業」の協力関係が必要！

●米国でFinTechサービスが成長する背景

〇個人投資が積極的で、借り手／貸し手のニーズが明確
〇クレジットカード上の債務の借り換えニーズが高いにも関わらず、
　リーマンショックで金融機関が個人融資に対応できなった
〇現在の定型的なFinTechサービスを分類
　融資、預金、家計簿・会計ソフト、資産運用、決済、モバイルPOS（スマートデバイスでのクレジットカードやデジタルマネー支払い）、
　PFM（Personal Financial Management、個人のお金に関わる情報に関する統合管理）、銀行インフラ、ロボ・アドバイザー（AI活用投資助言サービス）、仮想通貨（特殊なバーチャルコミュニティで流通する電子マネー）、マーケットプレイス・レンディング（資金の貸し手と借り手の仲介サービス）等

⇒FinTechサービスは、ネット・ユーザーに対して、既存金融機関によるサービスとは異なる、新たな価値を提供
⇒先進的な消費者に加えて、個人事業主、中小企業を中心にビジネスの分野での利用が急拡大

●「融資」サービス

「レンディング・クラブ（Lending Club）」

借り手と貸し手を仲介するマーケットプレイス型のクラウドファンディング・サービス

⇒Lending ClubがC2Cモデルで成長した結果、ネットオークションサイトを企業が利用するのと同様に、機関投資と金融機関が新たな資金運用手段として活用し同社の成長を加速

⇒同サイトの利用手順
①借り手が自身の情報をLending Clubサイトに登録
②Lending Clubが借り手を独自基準で審査し借り手を「格付け」
③貸し手がLending Clubサイトに表示される借り手の中から条件に合致する借り手を選択し資金を貸すことで資金運用

⇒借り手の格付けに応じて金利水準が異なるため、貸し手はリスクと運用利回りを総合的に判断した分散投資が可能

●「融資」サービス

「キャベッジ（Kabbage）」

インターネット上のクラウド会計サービスやイーコマースサイトのデータを活用し、オンライン与信判断を実施することで、既存の金融機関と比較し、短期間での借り入れを可能に。

FinTech融資の特徴は、審査スコアを公開することで、従来金融機関による融資審査の不透明性を払拭したこと！

●「預金」サービス

「ネオ・バンク」

普通預金概念を刷新した、第三者提携型（他金融機関の金融商品を利用）銀行モデルを提供する、「シンプル（Simple）」「ムーヴン（Moven）」が注目。

「アトムバンク（Atom Bank）」

アプリ銀行を標榜しているところが注目

⇒セキュリティ上の問題と、ユーザーが銀行取引に求めるニーズは、よりスマートフォンやタブレット寄りになり、アプリのみの利用に注力していることに起因

「スマーティピッグ（Smartypig）」、「ダイム（Dyme）」

SNSを利用して積立預金を可能にしたことに注目

⇒貯蓄口座を持たないデジタルネイティブ世代を対象に、貯金の目標額を設定しておき、会話形式のSMSでフォローアップし貯金意欲を向上

「ディジット（Digit）」

米国のPFMだが、自動的に節約し貯めるユーザーに向けたアプリで、独自のアルゴリズムに基づき、日常的に使っている銀行口座から、自動的に貯金用口座に、小額を移す機能を有しており、月収の約5.5%貯めた例が報告。

●「送金」サービス

「ドゥオラ（DWOLLA）」

銀行口座ベースの送金が可能なP2P決済サービス事業を展開しており、2015年4月にスペイン大手BBVAのグループの米国BBVA Compass銀行と提携、自行顧客向けにリアルタイム送金サービスの提供を開始。

⇒BBVA Compass顧客は、自行内もしくは、ドゥオラ・アカウントを持つ利用者同士は、24時間リアルタイム送金が可能。

「（ベンモVenmo）」

友人同士での送金で急成長、2013年にPayPalが買収したBraintree社の運営する個人間送金サービス

⇒送金額が2016年には、10億ドル/月を突破。ユーザーは、銀行口座やクレジットカードをウォレット に連携すれば、簡単に送金ができるアプリ。操作が簡単で、SNS的（「AさんがBさんに支払った」というフィードが流れる）

●「送金」サービス

「ワールドレミット（WorldRemit）」（英国）

従来の銀行送金イメージを転換した新たなサービス

欧米では、出稼ぎ労働者など銀行口座を持てない層も多く、母国への送金にFintechサービスを利用する例が急増

スマートフォンだけの個人向けの国際送金サービスを提供

次のような3つの手順で実行
①“現金”ではなく、「Airtime」（携帯電話のプリペイドチャージ）を送る
②送金人は、受取人の携帯番号、金額、送金資金の受取方法を入力
③受取人には送金を知らせるSMSが送られ、Airtimeを追加

⇒「WorldRemit」サービスでは、国により、Airtime追加ではなく、銀行口座への入金、取次店での現金受取り等も可能。銀行口座がなくてもスマートフォンさえあれば送金できるため新興国向けの送金インフラとして成長

●「決済」サービス

「アファーム（Affirm）」

米サンフランシスコの消費者向けに金融サービス

⇒デジタルネイティブ世代に人気

⇒アファームと提携したオンラインショッピングサイトでは、
　クレジットカードで支払いとアファームで分割払いが設定可能

⇒クレジットカードがなくてもオンラインショッピングサイト決済が可能

●「個人資産管理（PFM）」

「MX」

UI（ユーザーインタフェース）に注力し、ユーザーエクスペリエンスともいえる域に到達

⇒個人の予算管理を直感的に行えるサービス

⇒多くの金融機関が採用

⇒同社のサービスでは、収集した個人の取引履歴を活用しビッグデータ分析機能を充実させ金融機関向けマーケティングサービスを提供

●日本国内のFinTechベンチャー企業

「マネーツリー」：資産管理サービス、金融データのクラウドサービス

「マネーフォワード」：クラウド会計ソフトや資産管理ツール

「Freee」：クラウド会計ソフト

「maneo」：ソーシャルレンディング

「メタップス」：オンライン決済

「 bitFlyer」「bitbank」「coincheck 」： BitCoin＝「仮想通貨」の売買

●富士通、三井住友銀行、三菱東京UFJ銀行他

⇒FinTechに関わるビジネスコンテストを開催し、FinTech企業との連携やビジネスチャンスを模索

○Fintechベンチャー Alpaca社（神戸発シリコンバレー企業）

・AIを利用して、株式のアドバイスタイミング（When）を通知する「キャピタリコ（Capitalico）」と、どの株式(What)を買うかをアドバイスする「アルパカスキャン（AlpacaScan）」をアメリカで提供。
【MUFGのFintechアクセラレータに採用】

①「キャピタリコ（Capitalico）」
Web上で自分が勝てる「チャートパターン」をインプットとして入力し、ディープラーニングでパターン認識から自分の投資アルゴリズムを作成しリアルタイムに売買のタイミングを通知する

②「アルパカスキャン（AlpacaScan）」
ゴールデンクロス、ボリンジャーバンド、RSI、一目クラウド、赤三兵、包足、ローソク足といった投資家に馴染みのあるパターンを、全て実装して、米国の7000あるすべての株を読み込ませ、今どの株を売買するかを指摘する。

○ブロックチェーン技術の応用としての保険

■ブロックチェーンの技術を使い、暗号通貨を利用すると銀行口座を持たない人々でも保健サービスを利用することが可能。

⇒メキシコのモバイル決済プラットフォームのSaldoは、**ブロックチェーンベースの生命保険などの各種保険の契約を行うことができるマイクロ保険サービス「Consuelo」を発表**。

⇒暗号通貨の取り扱いがある企業ということ前提だが、このタイプの保険では、中間業者や保険金調査担当者を排除できる。

■日本でも、東京海上日動火災保険株式会社がこの技術を導入。

⇒外航貨物海上保険で保険証券の電子化を行い、電子化した保険証券をブロックチェーン上にて流通実験中。

○三菱UFJフィナンシャルグループのFinTech

・店舗を中心とした考え方から、店舗とモバイルが融和したような顧客サービスの創出が求められるようになってきたことが起点

・決済、融資、資産運用といった金融機関の基本領域が対象

・計画を立てて、失敗しないことを前提にプロジェクトを進行させるのではなく、「これは有望だ」と感じたサービスは、できるだけ早く、PoC（Proof of Concept=概念実証）を始めていくことが重要

・2015年5月には、IT事業部の名称を、デジタルイノベーション推進部に変更（情報システム部門と兼務せず）

人型ロボット「NAO」：
19カ国語でATMの場所や口座開設を案内します。

・2017年３月三菱UFJフィナンシャル・グループは金融とIT（情報技術）を融合したフィンテックで、ベンチャー企業など外部との連携を加速。
⇒外部の企業が銀行の口座情報などに安全にアクセスできるようにして、新たな金融サービスを展開しやすくする。フィンテック企業が手掛ける送金や資産運用などの新サービスの信頼性を高め、利用者の裾野を広げる。

○みずほ銀行とソフトバンク

FinTech（フィンテック）を活用したレンディングサービスを提供する株式会社J.Scoreを設立

J.Scoreは、顧客からのデータ提供や追加情報入力でスコアアップが可能となるスマートフォン完結の国内初スコア・レンディングサービスを提供する。みずほ銀行のビッグデータやローン審査ノウハウ、ソフトバンクのビッグデータやAIによるデータ分析のノウハウに実現

スコア・レンディングサービスにより審査応諾範囲の拡大、競争力のある金利水準を実現

2017年1月現在、Pepperは11ヵ店まで導入拡大、八重洲口支店、吉祥寺支店、石神井支店、神戸支店、札幌支店、阿倍野橋支店、調布支店、横浜駅前支店、玉川支店、銀座中央支店、東京中央支店。

○三井住友銀行

・AIの実用化に向けた取組について

　JSOL社（2014年Google Cloud Platform Special Contribution Award受賞）と提携しPOC（(Proof Of Concept)、概念実証）のプラットフォームとしてGoogle Cloud Platform（GCP）の活用で技術支援。

①実用可能なAIの早期活用
　AI関連テクノロジーについて、主要ITベンダーやベンチャー企業の最新技術や先進事例を情報収集し、各業務への適用が見込めるAIの実用性を検証。

②業務の高度化・自動化を担う独自のAIを創造

③AI活用のスピード化と利用拡大（AI化）

・2017年2月三井住友銀行は金融とIT（情報技術）を融合したフィンテックを手がけるベンチャー企業との連携を加速。7月をめどに同行の個人顧客の口座情報へのアクセス権をベンチャーに与え、預金残高や入出金などの情報を入手しやすくする。銀行の抱える情報を開放して有望なフィンテック企業をひき付け、新サービスの開発につなげる。

●ビットコインの中核技術として開発された「ブロックチェーン」

〇ブロックチェーンはビットコインを構成するソフトウェアの一部

〇ビットコインは中央集権的な管理機構を持たない通貨で、分散的に管理されているが、それを支える仕組みがブロックチェーン

〇取引の履歴を記録するデータベースを一ヵ所で管理（中央で管理）するのではなく、多くの場所で同じデータベースを保持しながら管理（分散的に管理）し「分散型台帳（元帳）」と呼ぶ。

〇記録する際に情報のブロックを作るため、一つのブロックと次のブロックの繋がりを示す「ハッシュ値」を組み込んで繋ぎ、あたかも鎖の形のように連ねることから命名。

〇ブロックチェーンによって取引を記録・管理することで「改ざんが極めて困難」「実質的にゼロ・ダウンタイム」の安定な高信頼性システム低コストで構築可能。

●米Nasdaq未公開株式取引市場Nasdaq Private Market
「Nasdaq Linq」

株式未公開企業の従業員が、自身で保有している株式を売買でき、その取引の「台帳」を実装する技術としてブロックチェーンを使用。

●米ベンチャー企業＝Gyft Block社
ブロックチェーンを活用して、ポイント交換システムを開発、安価で信頼性の高い、ギフトカードを交換する仕組みを創出。

●米ベンチャー企業＝Factom社
ブロックチェーンを使い文書の存在証明を多くの分野へ展開。医療や保険といった分野での活用が期待されるほか、土地登記謄本といった権利書類の記録管理サービスを提供しており、中国政府が主導するスマートシティ計画に参画。

●豪ベンチャー企業＝Flux社
　ブロックチェーンをベースに選挙システムを構築し、市民の声を政治により反映しやすくさせようとする取り組み。

●英ベンチャー企業＝Everledger社
⇒ダイヤモンドの形状をセンサーで読み取ってデジタル指紋に変換し、ブロックチェーンにダイヤモンドの認定書を記録

⇒ダイヤモンドが消費者に販売されるまでの取引ルートを追跡しブロックチェーンに記録することにより、消費者の盗品購入防止

◎ビットコインの一部として登場した際には、想像もできなかった応用例が出現。今後も様々なアイデアが考案されるだろう。

3.2 ブロックチェーン技術の応用としての電力

●電力での応用としては2016年8月オーストラリアのブロックチェーン最大手企業がソーラーパネルを用いて発電した電力を、**個人同士が自由に売買できる仕組み**の実現を目指し、ブロックチェーン技術の活用実験を継続中。

●電力会社を通しての売買だと仲介料が発生するが、個々人の間であれば、売る側も買う側も損することなく取引可能という概念。

3.3 ブロックチェーン技術の応用としての医療

●医療分野の例としては、ドナー登録や個人情報の保護対策、
さらには医薬品の製造や管理等に活かす研究が進行中。

●情報管理や、改ざんなどの不正を防ぐ手段としてブロックチェーンの技術が大きく作用。

●患者の身体の情報を時系列に記録し、暗号化・匿名化を電子署名
によって守りながら真正性と見読性と保存性の「電子保存3原則」を
保証することを可能にしています。

3.4 まとめ

日本は技術で先行もビジネス面に遅れ金融分野にとどまらずあらゆる分野に応用

【平野洋一郎・ブロックチェーン推進協会（BCCC）理事長インタビュー】

インターネットの世界がその黎明期から技術とビジネスの両面で発展を遂げたのと同様に、ブロックチェーンも、技術とビジネスの両面で普及を促す必要がある。

実は、日本の一部の企業や機関で、世界的に見ても先進的なブロックチェーンの実証実験が行われている。ただ、現時点の日本では、ブロックチェーンのビジネス面での適用例や需要が海外に比して相対的に少ないことから、今のままでは本格的な普及までに海外より多くの期間がかかってしまうと懸念されている状況だ。

その普及を推進するために設立したのがブロックチェーン推進協会（BCCC）である。4月の設立以降、急激に加盟者数が増え、8月には既に80社を突破した。いわゆる技術系企業にとどまらず、ブロックチェーンを活用する立場にあるユーザー企業も増加傾向にある。

今後は流通分野（トレーサビリティ）や製造分野（検査・検証データ）、公共分野（登記、試験履歴）、医療分野（治験データ）など、改ざんが許されない領域を中心に、近い将来、日本でも大きな広がりを見せることだろう。

3.4 まとめ： 全産業分野の「次世代プラットフォーム」へ

●FinTechの次の注目技術だ期待されるブロックチェーン

⇒ビットコインによって可用性の高さが証明

⇒多種多様な拡張アプリケーションが想定
「ブロックチェーン2.0（ビットコイン2.0）」

●経済産業省がブロックチェーンを強調【2016年4月28日発表資料】
「平成27年度我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書概要資料」

⇒ブロックチェーンは「〝フィンテックの次〟の注目技術」」
「あらゆる産業分野における次世代プラットフォームとなる可能性」

3.4 まとめ： 全産業分野の「次世代プラットフォーム」へ（つづき）

●ブロックチェーンの特徴
（1）記録手段として情報の改ざんが極めて困難
（2）ゼロダウンタイムを実現
（3）従来のシステム構築に比べて安価に構築可能

●パブリック型ブロックチェーンで今後トランザクションコストが大幅に削減（企業間の取引コスト）
⇒さらにプライベート型のブロックチェーンによって劇的削減へ。
（企業内オペレーションコスト）

●ブロックチェーン技術を使って金融機関の運営コストを近未来に10分の1未満に削減

⇒可能性としては100分の1も

⇒ブロックチェーンによって劇的に削減されるのは、情報システムそのものの費用だけではなく、システムに携わる要員の人件費

『Blockchain 技術を取り巻く国内外のビジネス動向と将来展望』

～今後のテレコム業界の役割とは?～

日本における「ブロックチェーン」普及の課題

①ブロック形成時間（数秒～10分程度かかる）

②処理件数（単位時間あたりに処理できる取引件数が大手クレジットカード会社のシステムなど既存の決済システムと比して劣る10000倍？）

③実ビジネスでの適用例の少なさ

今後のテレコム業界の役割＝課題解決と安定運用

ご清聴ありがとうございました