ブロックチェーン技術とシステム監査

2018年6月30日

日本情報システム・コンサルタント協会
副理事長　永田　淳次
Junji.Nagata@gmail.com

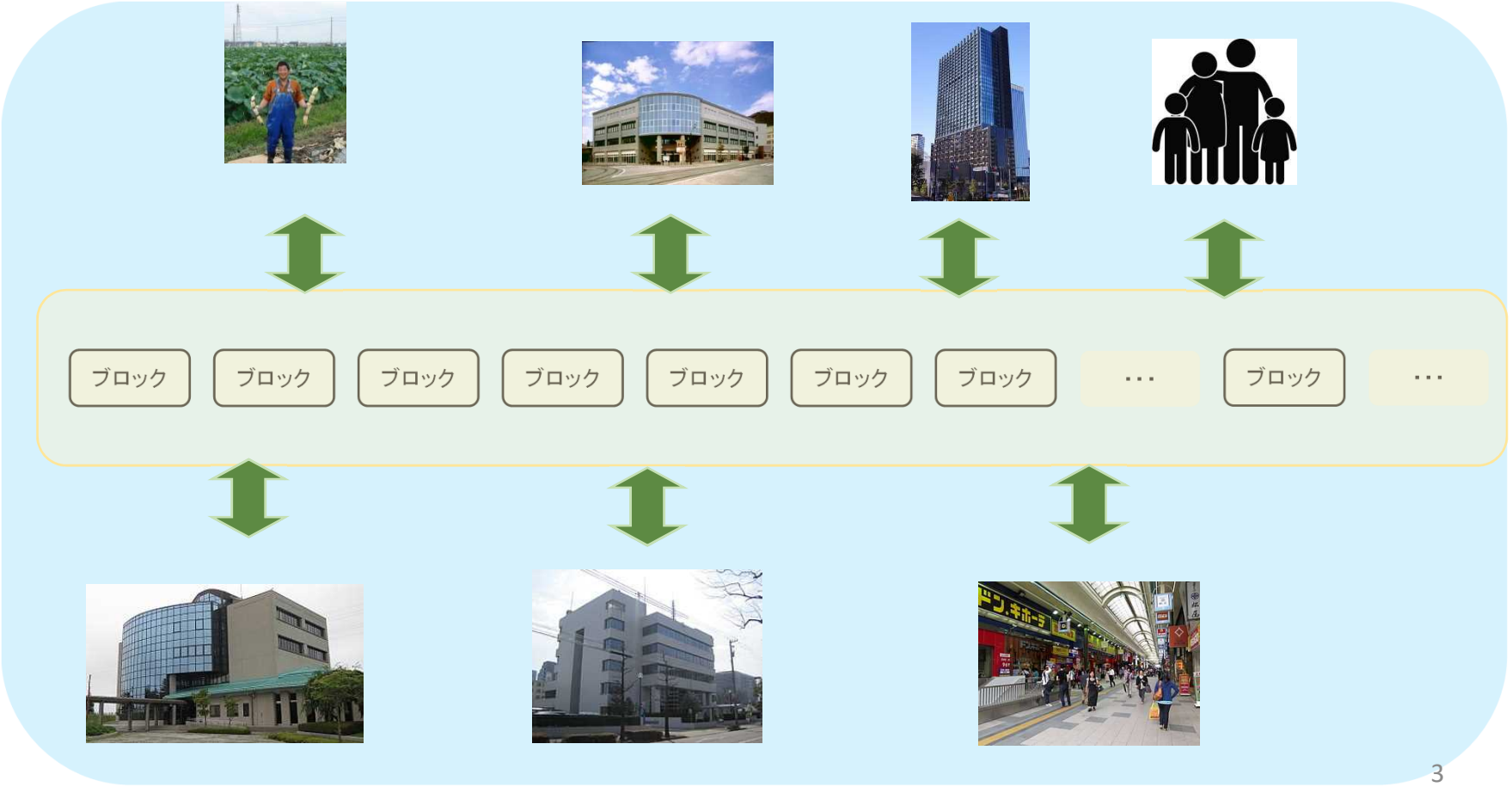
ビットコインアドレス
bitcoin:1LsJPU6APpqwNKi5jHgW819bQoefGVtURc

発表要旨

- ブロックチェーン技術
- ブロックチェーンの特徴
  - 台帳、Wallet、Github、トラストレス、インセンティブ
- ブロックチェーンの展開の方向
  - 情報の記録
  - 通貨、価値交換
  - 正しい情報の記録
- 情報の記録とシステム監査
- 通貨、価値交換とシステム監査
- 正しい情報の記録とシステム監査
- まとめ

ブロックチェーン技術とは

- 定義は定まっていない
  - 分散台帳とも区別されていない
- 暗号通貨Bitcoinシステムの中核技術群



ブロックチェーンの特徴

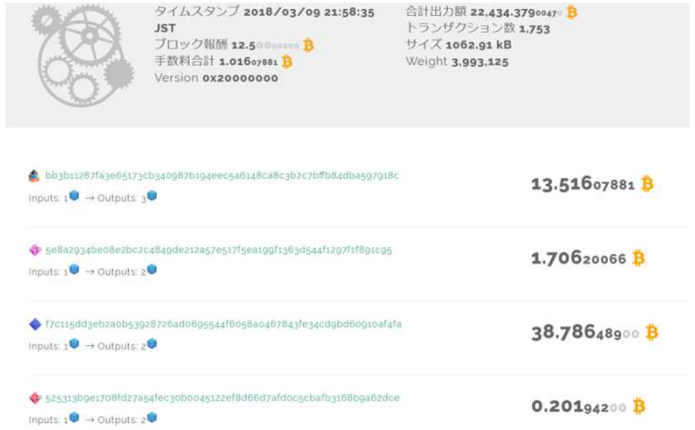
- 全ての正しい取引を記録し全員で共有する「台帳」
- 「鍵」で個人情報をコントロールする「Wallet」
- 大衆が実力発揮可能な環境「Github」
- トラストレスでトラストを実現
- システムを維持するインセンティブの存在

Bitcoinシステムでの台帳

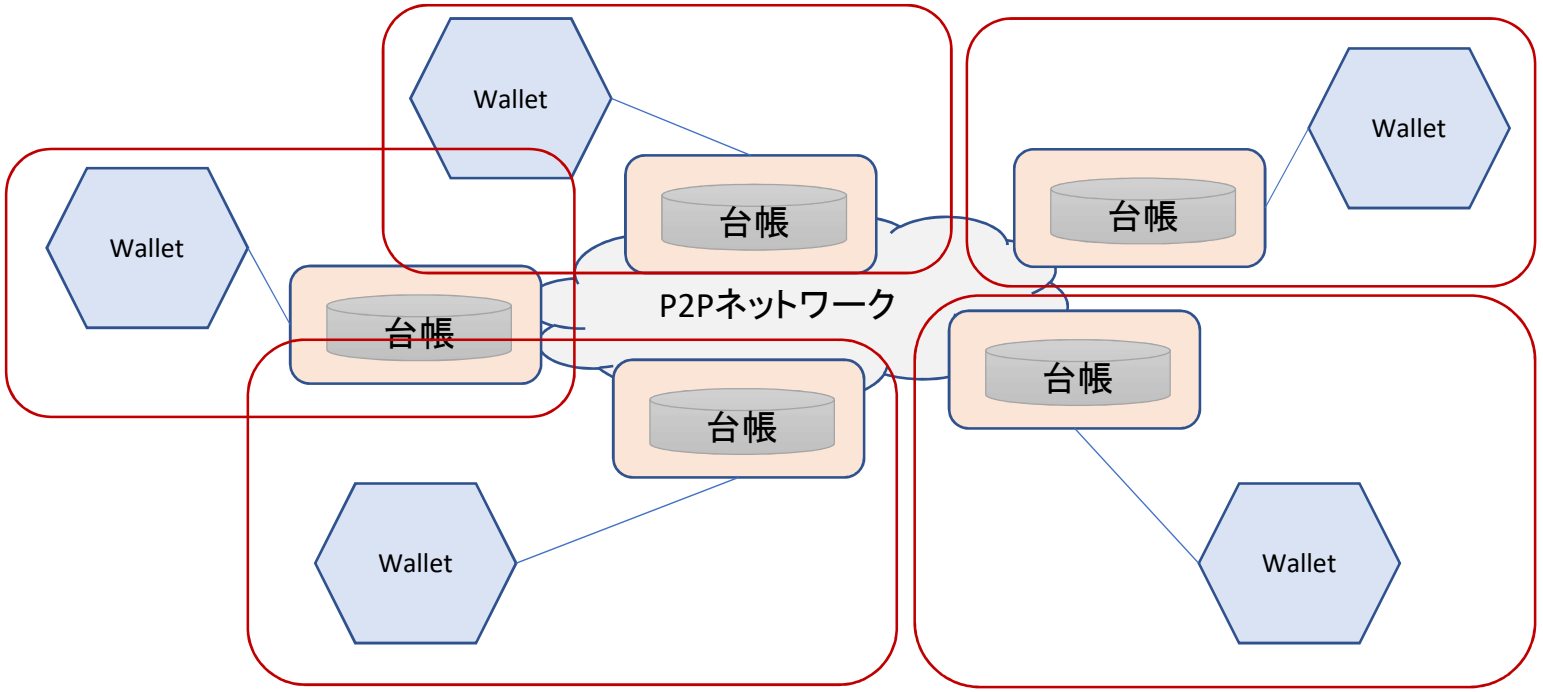
- 「 BTCいくらを、誰それから、誰それへ」という「取引」の全てを記録する
- 正当な取引のみを台帳に書込む
  - 正当性：　本人に使用する権利がある
    二重取引じゃない等々
  - 台帳に書込む前に、皆で、その正当性を確認し、合意する
- 書込んだ取引は、消さない、変更しない
  - 時間軸上につないでいく

台帳（ブロックチェーン）の概要

https://chainflyer.bitflyer.jp/



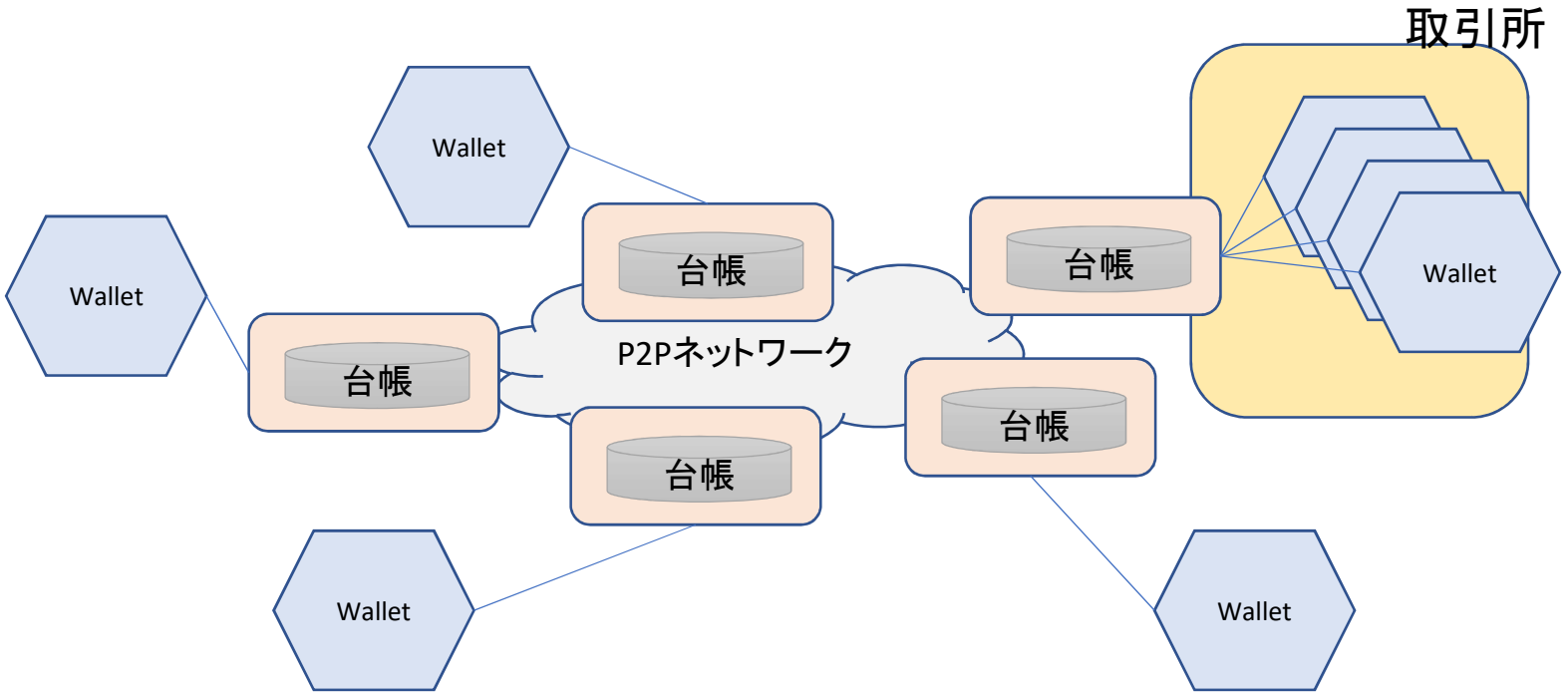
台帳とWallet



- 全員が同じ台帳を共有
  - 新たなブロックが生成されると、全員がすぐに共有
  - P2Pネットワークで通信

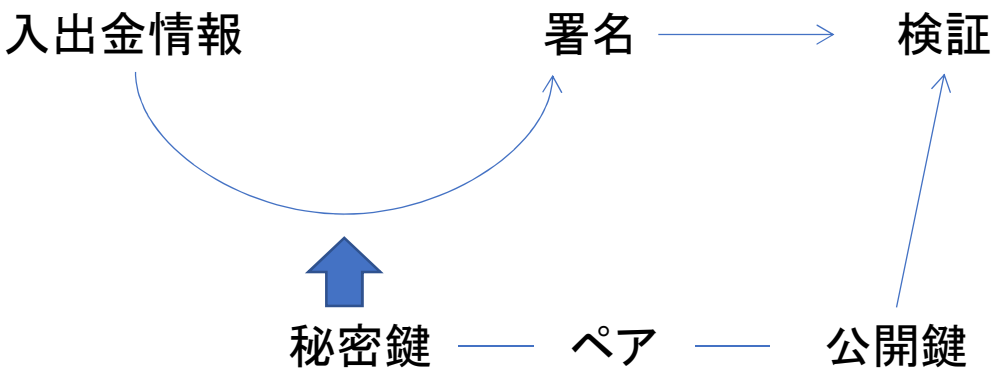
暗号通貨と法定通貨との交換

- BTCの入手には、マイニング
  - ブロックをつなぐことでBTCが生成され、つないだ人がそれをもらえる
  - つないだ人は取引の入金合算値と出金合算値の差がもらえる
- マイニングしない場合
  - （Bitcoinシステムには法定通貨との交換機能はない）
  - BTCをすでに獲得している人から入手する
    - 直接取引
    - 取引所の利用



公開鍵、秘密鍵（１）

- 台帳（すべての取引）は公開、だが個人情報は鍵で秘匿
  - 自分の情報を秘匿しているが
  - 自分のものであるという主張ができ、
  - 他の人が「そだねー」という判断が簡単にできること、そのために
  - 公開鍵暗号方式を採用
    - 公開鍵と秘密鍵のペア
    - 秘密鍵で署名することで、「自分もの」であるという主張
    - 「署名と公開鍵」を参照して「秘密鍵を持ってるんだよねー」と判断

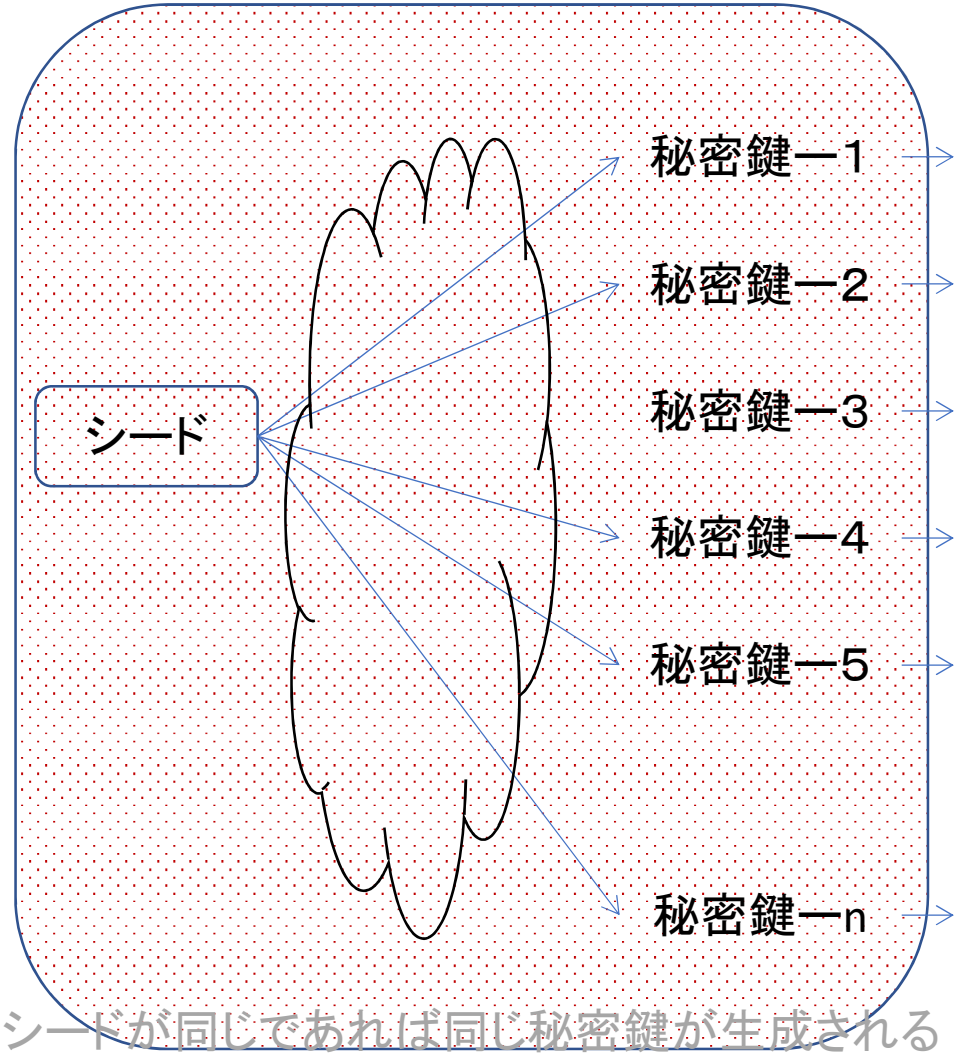


公開鍵、秘密鍵（２）

- 暗号通貨Bitcoinシステムでは
  - Walletで公開鍵と秘密鍵のペアを生成
  - 公開鍵からビットコインアドレスを生成
  - 取引はビットコインアドレスで
    - ビットコインアドレスでBTCの支払い、受取り
    - ビットコインアドレスとペアとなる秘密鍵を持っているものだけが、取引の結果を利用できる
    - 秘密鍵を利用した署名で所有者であることを証明
  - 秘密鍵を失うと
    - 取引ができない　→　BTCを失う

Walletでの鍵の管理

ビットコインアドレスは使い捨てが可能
←保有量を不明にするため



秘密鍵ー1 → 公開鍵ー1 → ビットコインアドレスー1

秘密鍵ー2 → 公開鍵ー2 → ビットコインアドレスー2

秘密鍵ー3 → 公開鍵ー3 → ビットコインアドレスー3

秘密鍵ー4 → 公開鍵ー4 → ビットコインアドレスー4

秘密鍵ー5 → 公開鍵ー5 → ビットコインアドレスー5

秘密鍵ーn → 公開鍵ーn → ビットコインアドレスーn

シードが同じであれば同じ秘密鍵が生成される

Github（１）

https://en.wikipedia.org/wiki/Vitalik_Buterin

- 質問　１　VITALIK BUTERIN氏
  - 現在24歳（1994年1月31日生まれ）
  - 19歳のときに「ETHEREUM」（イーサリアム）を考案
  - メディアや一部の人は、彼のことを天才というが．．．
- 質問　２　アルトコイン（ビットコイン以外の暗号通貨）
  - アルトコインはすでに1500を超す
  - 何故．．．

Github（２）

- Githubとは
  - 成果物の管理や共有
    - ソースプログラムやドキュメント
  - 誰もが簡単に参照、利用できる
  - 暗号通貨も同様
    - 例えばMonacoin
    - http://bitcoin.clock-up.jp/contents/admin/monacoinを参照

- Bitcoinシステムのソースプログラムも Github上で公開
  - https://github.com/bitcoin/bitcoin
- オープンにしたことにより
  - Bitcoinシステムの利用、普及が急速に拡大
  - Bitcoinシステムの動作原理や知識が浸透
  - 専門家による改良、改善が継続
  - 新たなアイデアを議論しながら実装
  - Bitcoinシステムのソースプログラムを利用したアルトコインが出現

インセンティブの存在

- OSS（Open Source Software）の問題の一つ
  - インセンティブがない
  - ボランティア精神にタダ乗り
  - 企業による寄付、投げ銭で、開発、保守、運用
    ↓
  - 安定した運用保守の困難性が内在
    - バグフィックス
    - バージョンアップ
    - 運用の破綻
    - 身勝手なフォーク
- Bitcoinシステムにはインセンティブが存在
  - ブロックをつないだことによって得られる報酬
  - 入金と出金の差額が報酬
    ↓
  - 上記問題（ossの問題）を解決する可能性を有す

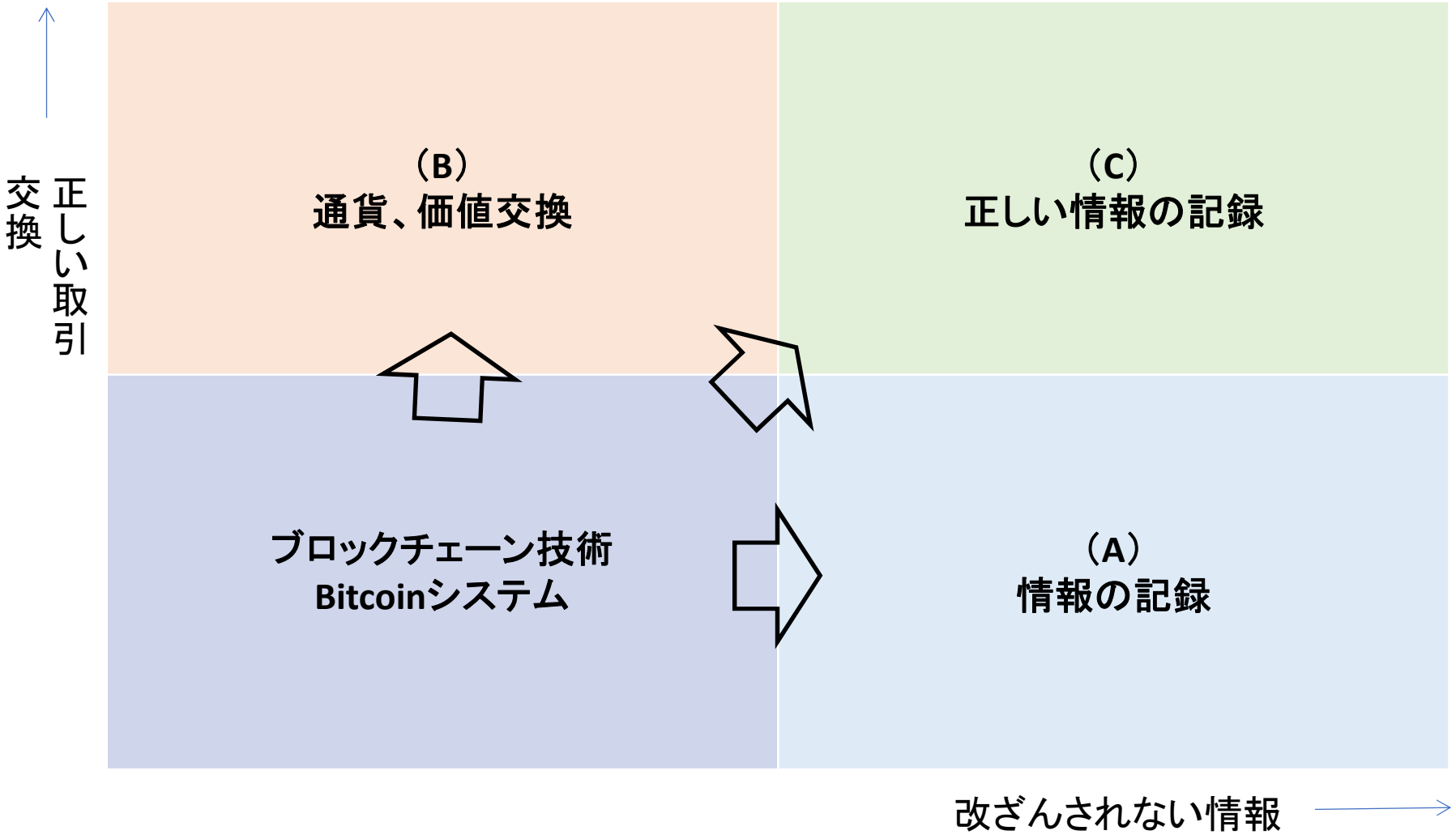
トラストレスでトラストを実現

- インターネットは誰が管理しているのか？
  - JPNIC？　W3C？　IETF？　→　管理主体が非存在
  - 管理主体は存在しないが、インフラとして定着
    - 参加者が、それぞれの持ち場、立場で信頼性を確保、維持
      ↓
    - 管理主体が非存在だが「トラスト」がある

- トラストレスでトラスト
  - 暗号通貨で語られるキーワードの一つ
  - 管理主体はないが参加者の力で信頼性を確保
    - PoW
    - P2Pネットワーク
    - 鍵
  - 非中央集権、民主主義

- 「Code is Law」という考え方
  - 人間が恣意的に「何かすること」を排除
  - ルールに則った行動

ブロックチェーン展開の方向



「(A) 情報の記録」とシステム監査

- 「追加しか」しない情報の記録
  - 改ざんがない（できない）
  - （必ずしも）ブロックをチェーンする構造でなくてもよい
- 参考になる過去の実績
  - 特許（実用新案）、公証役場や登記所
  - ジャーナル、ログ機能
  - タイムスタンプサービスやWeb魚拓
  - Wikipediaの履歴
  - Github
    - （事例）GitHubで雑誌・書籍を作る https://www.slideshare.net/inao/githubkaigi
  - 消さないTwitterや消さないブログ
- 監査ログとして利用
  - 監査ログの蓄積
  - 監査証跡として利用
- 課題
  - 何をどのタイミングで記録し、それをどう利用するのか
  - 有用な情報として抽出する方法や自動化、見える化
  - 記録されたものの正しさをどう確保するのか（認証機能）

「(B) 通貨、価値交換」とシステム監査

- 暗号通貨システムをどう監査するか
  暗号通貨システムの利活用に対してのシステム監査
  - これから利用する企業へのシステム監査
  - すでに利用している企業へのシステム監査
  - 複数企業が共有して利用する場合の、システム監査

- クラウドサービスを監査する場合と同じ考え方が適用可能か
  - チェックリストによる外部からのシステム監査
  - サービスを提供する会社も含めたシステム監査
  - 内部統制保証報告書サービス（SOC1、SOC2）等の利用

「(B)通貨、価値交換」とシステム監査

これから利用する企業に対して

- 価値として扱うことの明確化
- 技術、知識の理解度
  - 法定通貨や証券とは違うことの認識
  - BTC、アルトコイン、トークン等実現方式の評価
  - 安定性や実績の評価
- リスクの認識
  - 発生可能性のあるリスクの洗い出しとその対策の検討
    - 盗難や鍵漏えいによる価値の喪失リスク
    - 操作ミス等による送金先の間違い等
    - 相場の高下による価値の棄損
  - リスクヘッジの可能性
- グローバルの場合
  - 海外起点のリスクの評価
  - 自国法律への適合性
  - 現地法律への適合性

「(B)通貨、価値交換」とシステム監査

すでに利用している企業に対して

- 他の資産との関係や連携
  - （暗号通貨に適した）内部統制の有無
  - 内部統制に沿った運用
- 秘密鍵（やシード）の管理方法
  - ハードウエアWallet
  - ペーパWallet
  - 二段階認証
- 暗号通貨システム運用主体がある場合
  - 内部統制保証報告書の提出
  - その内容の適正さの確認

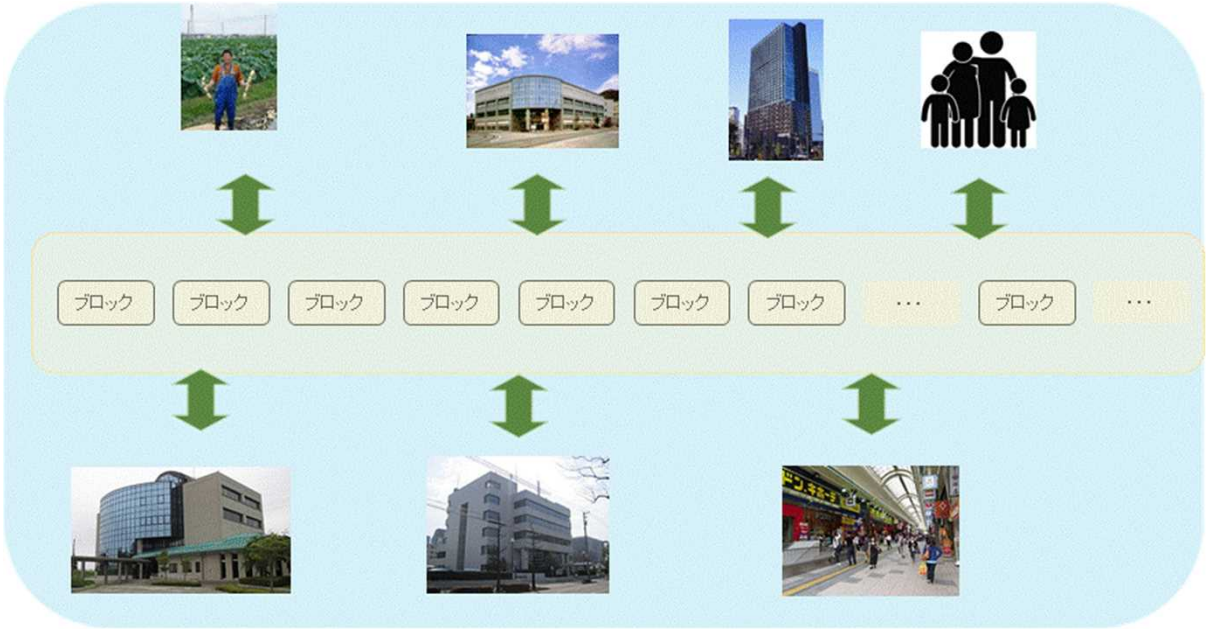
「(B)通貨、価値交換」とシステム監査

複数企業が共有して利用する場合

- 特定の管理者がいないという特徴
  - 内部統制保証報告書はない
  - 暗号通貨システムそのもののシステム監査は可能か？
- 格付け（今、思いつくのは以下の方法）
  - ソースの公開性
  - コアメンバーの評価
    - 暗号通貨システムを維持する関係者
      - 初期メンバ：暗号通貨を大量に保有
      - コア開発者：暗号通貨を保有
      - マイナー：暗号通貨を新規に獲得
      - 取引所：法定通貨等との交換による手数料
    - 関係者それぞれが
      - 暗号通貨の価値を維持、向上させるよう行動し、
      - そうなるようなメカニズムが整備されているか

「(C) 正しい情報の記録」とシステム監査

- Bitcoinシステムでは「取引」の部分は正しさの確認がされる
  - 「取引」以外の部分は正しさの確認が行われているわけではない



- 正しい情報を記録することができれば
  もしくは正しいことの保証ができれば
  - システム監査にとって有用な情報の宝庫となる

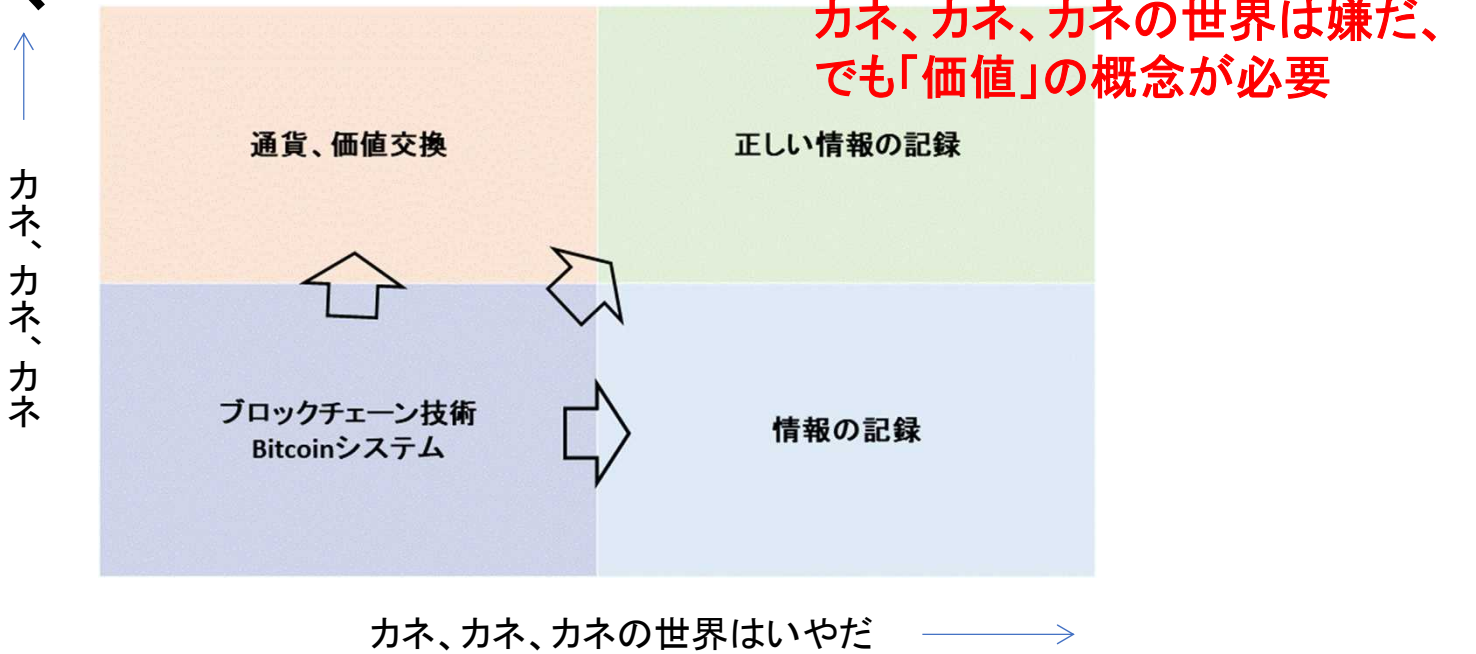
「(C)正しい情報の記録」とシステム監査

ブロックチェーン技術を利用するメリット

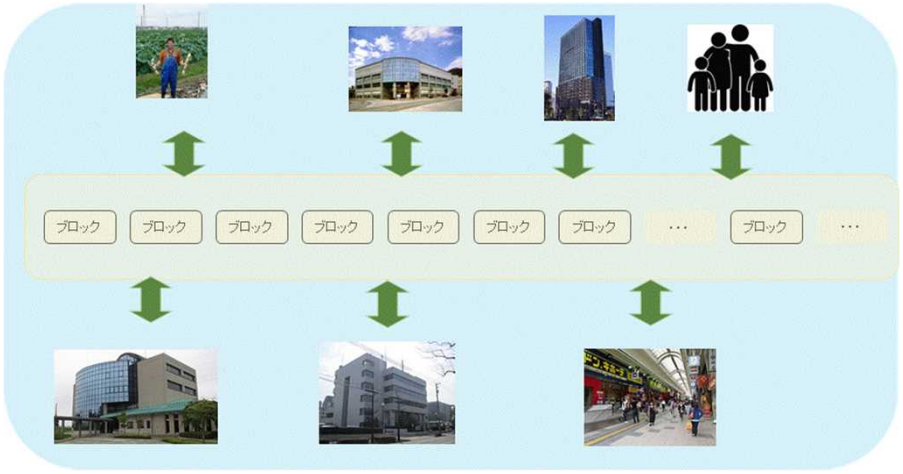
- コストの削減
  - 大型機、サーバがほとんど不要
    - PC程度でも参加可能
  - 分散化が容易
  - バックアップが不要
- 時間軸をたどることで有意義な情報の獲得が可能
  - 監査が容易
  - フォレンジックが容易
- 楽な管理監督
  - 意識の高い従業員が不要
  - 堅牢な建物、停電対策が不要
- （デメリット）
  - 鍵の管理の重要性の増加

「(C)正しい情報の記録」とシステム監査

ジレンマ



カネ、カネ、カネの世界は嫌だ、
でも「価値」の概念が必要



＜特徴を再掲＞
全ての正しい取引を記録し全員で共有する台帳

「鍵」で個人情報をコントロールする「Wallet」

大衆が実力発揮可能な環境「Github」

トラストレスでトラストを実現

システムを維持するインセンティブの存在

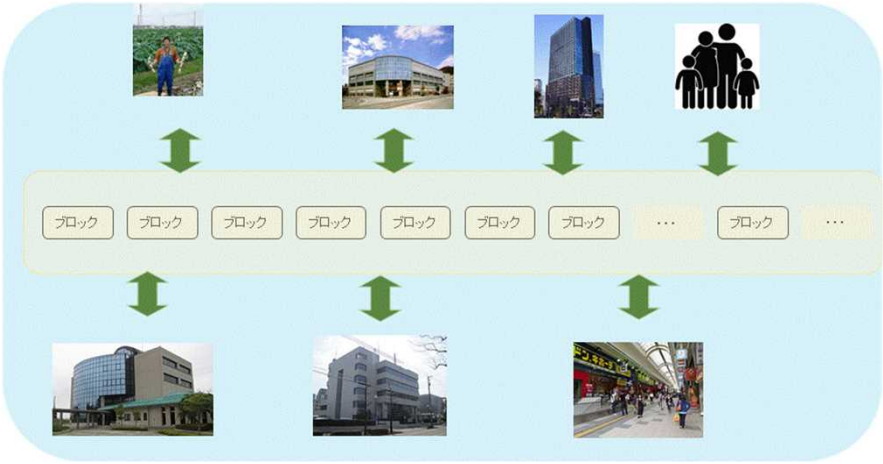
「(C)正しい情報の記録」とシステム監査

適用のために

- **データの正しさを保証できる**
- 複数の企業・組織や個人がデータベースを共有する
- 改ざんされていないため、皆にメリットがある
- 共有するデータベースの維持にインセンティブがある

↓

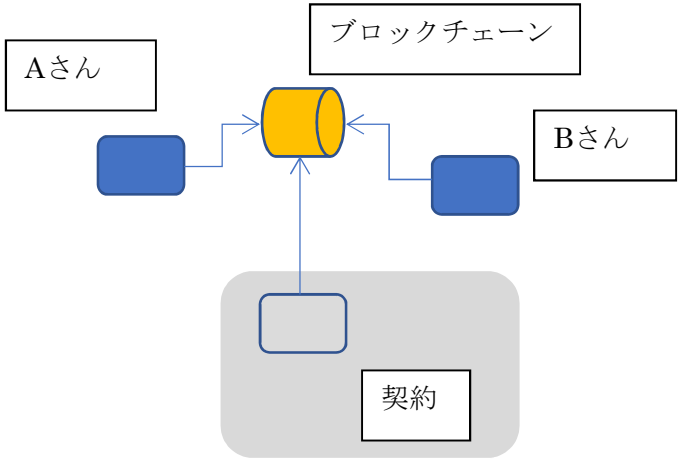
- 必要とされる技術開発
  - スマートコントラクト
  - InterOperability
  - レイヤー2アプリやAPI



「(C)正しい情報の記録」とシステム監査

スマートコントラクト

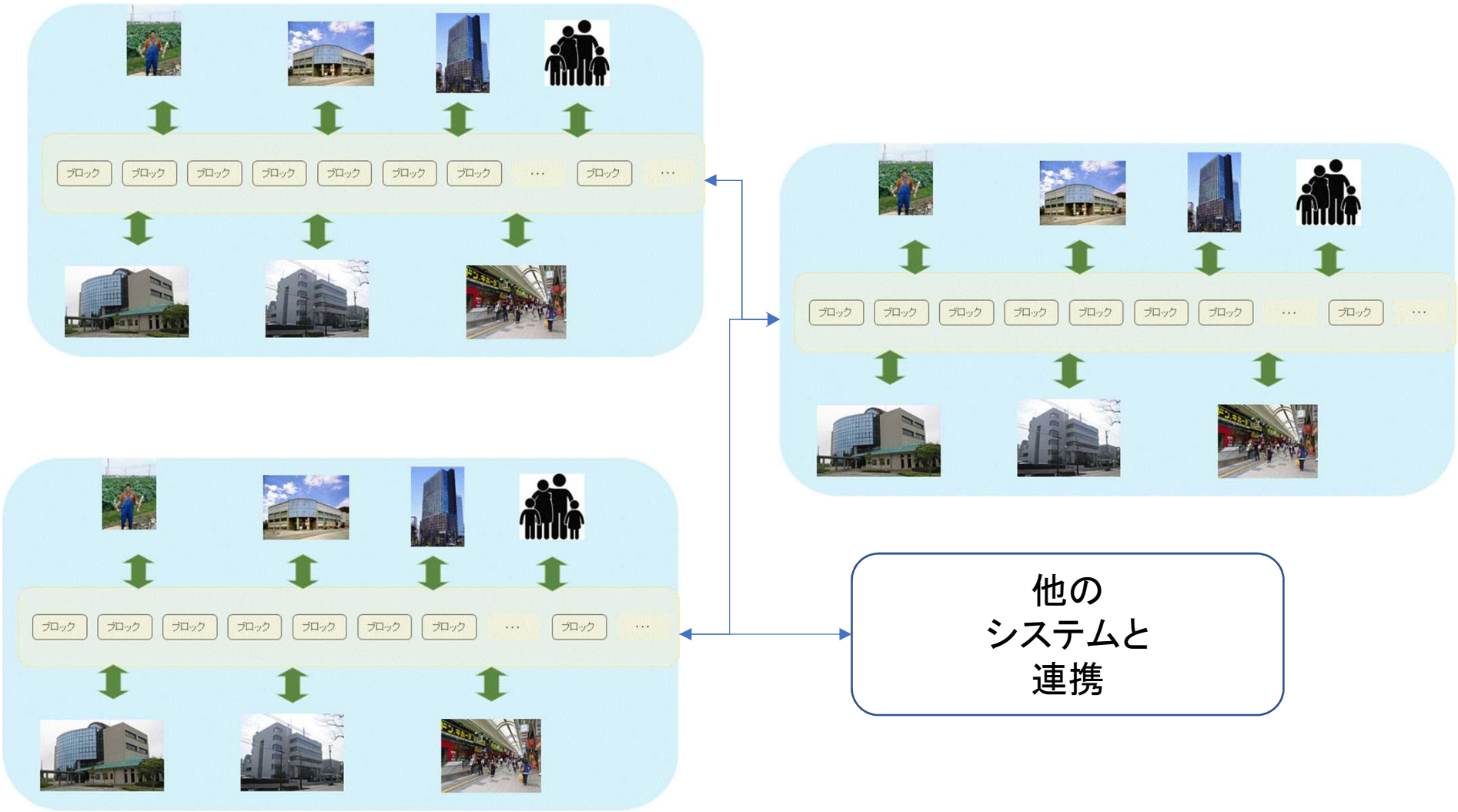
- 「契約」を作成することができる
- 作成した「契約」を登録することができ、登録すると「契約」にもアドレスがもらえる
- 「契約」がエスクロー的役割を果たす
- 他の人が登録した「契約」を利用可能
- Ethereum(イーサリアム)ではコントラクト記述言語「Solidity」が用意されている
  http://gaiax-blockchain.com/solidity



例えばAさんが商品を提供、Bさんが対価を提供を「契約」で行うことを想定
Aさんから「契約」に商品を提供したとの「取引」を、
Bさんから「契約」に、対価に相当する暗号通貨を提供するとの「取引」を、ブロックチェーンに記録する
このような両者（Aさん、Bさん）の取引があると契約が成立し、契約内の「通貨」を利用できるようになる。

「(C)正しい情報の記録」とシステム監査

InterOperability（１）



InterOperability（2）

- ILP（インターレジャープロトコル）
  - 異なる台帳間で資金を移動するための規格
  - 暗号通貨、法定通貨、クレジットカード等の間も
- W3Cで標準化
  - HTTPのエラーコード402（Payment Required支払いが必要である）に、実装か？？？
  - ブラウザにILPとAPIの実装（中？）
    - MS、Google、Apple
- 著作権の管理に適用が可能
  - 著作権保有者は著作物の使用をコントラクトに記載
  - ブラウザで著作者に費用の支払いを可能に
    - 簡便に著作物を利用可能に

「(C)正しい情報の記録」とシステム監査

API、レイヤー2アプリ

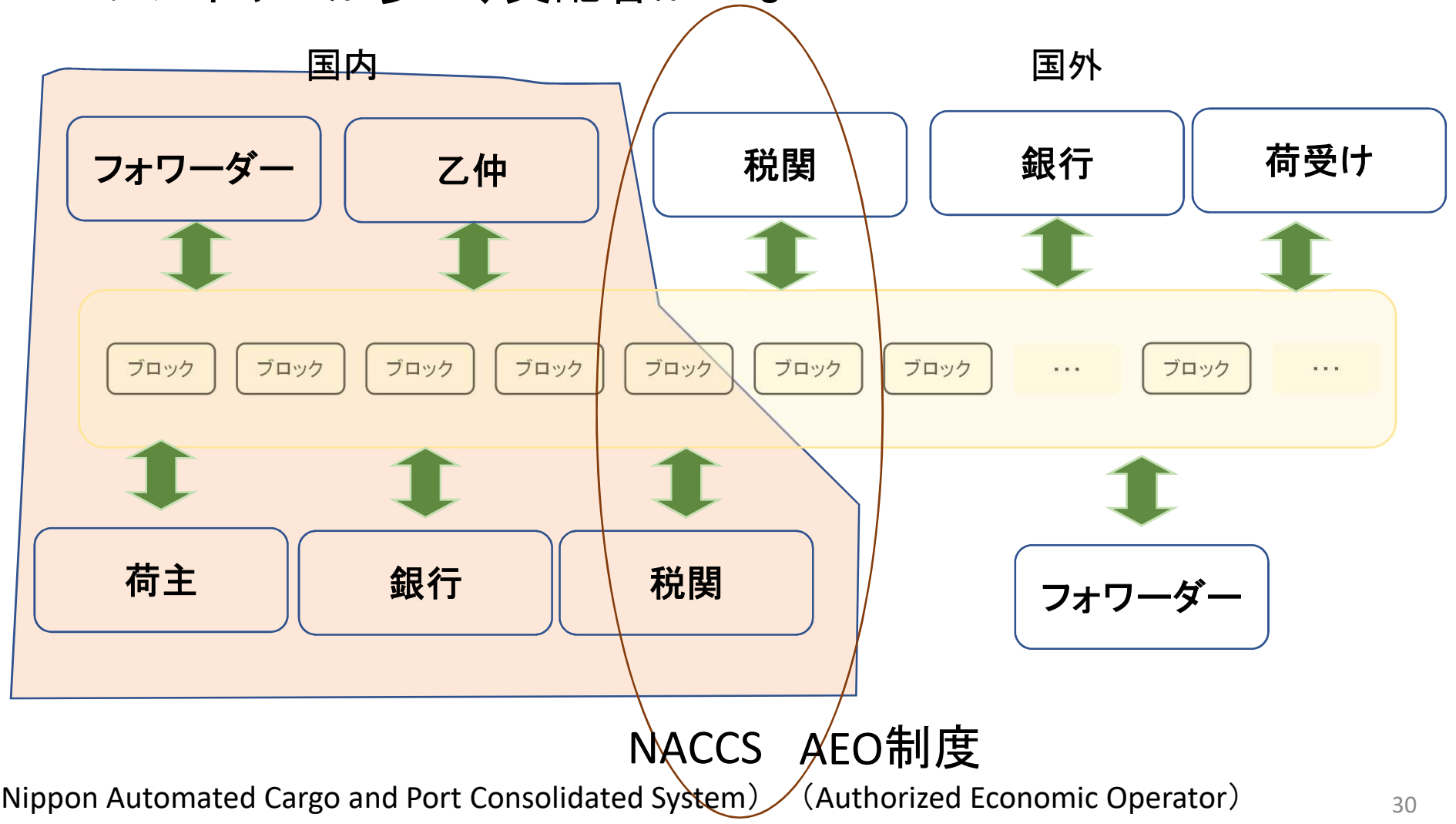
- API
  - ブロックチェーンへのアクセスの簡単化
  - NEMで実装

- レイヤー2アプリ
  - ブロックチェーンをレイヤー1として、Bitcoinシステム等のブロックチェーンの欠点を補完する
  - 但し、レイヤー2側のデータの正しさの証明はブロックチェーンとは別

「(C)正しい情報の記録」とシステム監査

適する領域（海外との商取引）

- プレイヤーが多い、支配者がいない



「(C)正しい情報の記録」とシステム監査

海外の商取引の事例

- **IBMとマースク、ブロックチェーンで合弁会社　貿易手続き効率化のシステム提供（日刊工業新聞（2018年1月17日）より）**
  - https://www.nikkan.co.jp/articles/view/00458209

米IBMと海運世界最大手、デンマークのA・P・モラー・マースクは16日、ブロックチェーン技術を活用した貿易情報ソリューションの合弁会社を設立すると発表した。積み荷の受け渡しや通関について、これまで文書で行っていた手続きをデジタル化し、情報をより効率的かつ安全に、リアルタイムで管理運用できるようになるという。

新会社はニューヨークに本社を置く。ブロックチェーンとクラウドコンピューティングに加え、新しいソリューションには人工知能（AI）やIoT（モノのインターネット）、アナリティクスなどの技術も盛り込む。規制当局の認可を受ける必要があるが、システムは半年以内に提供可能となる予定。税関当局や多国籍企業などへの提供を見込み、米ゼネラル・モーターズ（GM）や米プロクター＆ギャンブル（P＆G）、物流・運送会社などが関心を示しているという。

これに先立ち、IBMとマースクは2016年6月から協力し、ブロックチェーンとクラウドによる貿易管理運用システムの開発をスタート。現在では、米デュポンやダウ・ケミカル、スウェーデンのテトラパック、米ヒューストン港湾当局、オランダ税関、米税関・国境警備局などが両社のソリューションを試験運用している。

両社の発表によれば、海運によって年間4兆ドル（約440兆円）以上の積み荷が出荷され、日常使われている製品の8割以上が船で運ばれているという。ただ、グローバル物流での最大のコストとなっているのが積み荷の受け渡しや通関にかかわる文書手続きと管理運用の部分で、全体の運送コストの約20%を占めると推定されている。

そのため、世界経済フォーラム年次総会（ダボス会議）を主催する世界経済フォーラムからは、こうしたコストが軽減されれば、世界貿易は15%近く拡大し、経済が活性化するとの見通しも出ている。

コメント：記事からはブロックチェーンでなく分散台帳のように見えるが・・・

「(C)正しい情報の記録」とシステム監査

適する領域（教育）（１）

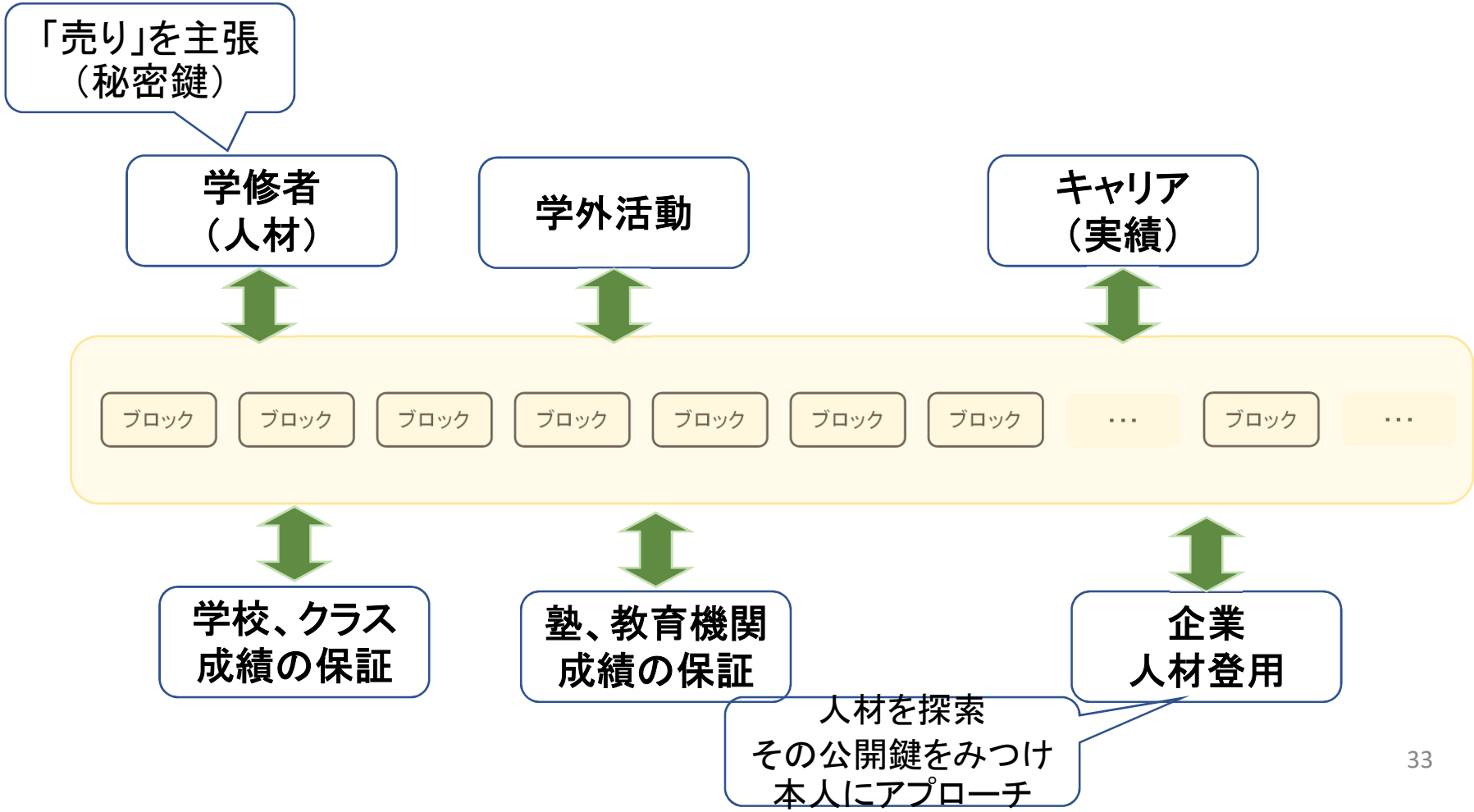
- ヒントの一つとなったシステム（１）
  - MOOK（Massive Open Online Course）オンラインで受講可能な授業
  - 講義映像を提供することから変化しつつある
  - 教育の質の保証（アクレディテーション：Accreditation）の動き
  - 学位、成績の認定→転職、就職に有利
- ヒントの一つとなったシステム（２）
  - 米：MITが「ブロックチェーン学位」の発行開始
    https://qaupdates.niad.ac.jp/2017/11/17/mitblockchain/
  - 学位保持者は進学や就職時に、デジタル学位を任意の第三者とシェアできる
  - MITの確認用サイトで瞬時に確認可能
- ヒントの一つとなったシステム（３）
  - Paiza（https://paiza.jp/guide/career）就職支援サービス
  - 特徴：学修することやプログラミング問題を解くことで、書類選考なしで面接へ進める
    ↓
  - 成績を企業に提供することで就職機会を増大
  - 求める人材のミスマッチが減少
- ポートフォリオや業績をブロックチェーンに記録し、学生の就職活動や育成された人材の採用に利用（次のスライド）

「(C)正しい情報の記録」とシステム監査

適する領域（教育）（2）

受講を受けるメリットはどこに
単位？卒業？就職？知識？

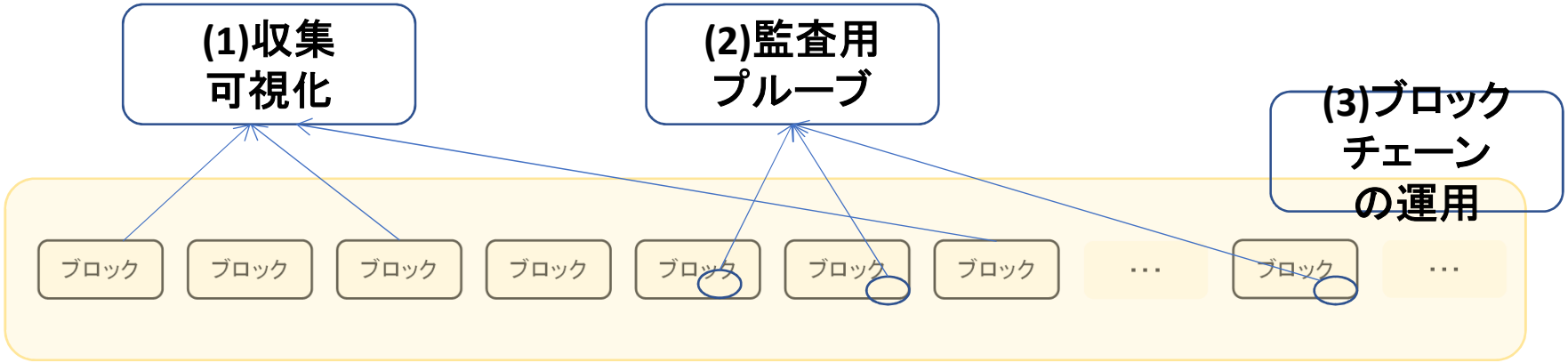
- 学業のポートフォリオの蓄積と活用
- 業務経験のキャリア開発



「(C)正しい情報の記録」とシステム監査

システム監査の方向

- (1) ブロックチェーンからの監査証跡の収集
  - 必要情報の収集
  - 可視化や分析する道具の開発
    - （Walletソフトの改良）
- (2) 設計時点で監査用プルーブの埋め込み
  - （プライバシー）バイデザインの考え方
  - Audit by Design、Inspection by Design
- (3) ブロックチェーン運用のコアメンバになる



「(C)正しい情報の記録」とシステム監査

(2) 設計時点で監査用プルーブの埋め込み

- 〇〇by Design
  - 設計時点から事前に〇〇対策を考慮し、企画から保守段階までのシステムライフサイクルで一貫した〇〇への取組みを行うことを提唱する考え方
  - メリット
    - 自然で無理のない情報の収集が可能
    - 有用となるプルーブの組込みが可能
    - 後からでは、収集不可能な場合がある
    - 出戻りで実現すれば膨大なコストとなる
- Audit by Design、Inspection by Design
  - （具体的には）スマートコントラクトに監査用のプルーブを組込む
    - （会計監査においても有用な情報となるであろう）
    - 課題
      - システム監査の立場で「契約」において、どのような情報を収集すべきか
      - 内部統制と契約（スマートコントラクト）との関係

「(C)正しい情報の記録」とシステム監査

(3) ブロックチェーン運用のコアメンバになる

- システム監査用ブロックチェーンの構築
  - （例えば）システム監査人協会が運用するブロックチェーン
  - 監査情報の第三者預託（エスクロー）サービス
  - 正しい記録であることを、監査人が保証できる
  - 有用で監査に必要とする情報の記録が可能

  - システム監査人が属する組織がマイニング
  - 監査情報を記録することでインセンティブ
  - 会計監査に応用可能なものにする
- メリット
  - システム監査に必要とする情報の確実な記録の実現
  - より正確で的を射たシステム監査報告の作成が可能
  - システム監査に必要とする期間や時間の短縮
  - 俗人性の排除（システム監査人の変更が容易）
  - システム監査実施のノウハウの蓄積
  - システム監査の自動化の可能性

まとめと課題（1）

- ブロックチェーン技術は魔法の技術ではない
  - ブロックチェーンにデータを格納するだけ、それだけで素晴らしいことが起こるわけではない
- 情報にも不正確性が
  - 話題性を得たいがための「ブロックチェーンを利用した〇〇」
  - カネ、カネ、カネだけの人たちも
- 課題は多数
  - 技術者の圧倒的不足（カネカネカネの世界に人材がとられている）
  - 経験や体験不足
    - 概念やそれを実現する技術や知識の不足
    - 実現した結果と、現行の社会資本や制度とのギャップ

まとめと課題（2）将来は楽観的、か？

- 批判的な意見も多い
  - 乱高下
  - おたくのおもちゃ
  - 思惑が多すぎ
  - 通貨発行は国の専権事項
- 1990年頃のインターネットに類似
  - 当時、ネットバブルは弾けると予想する人も多数
  - でも、その後Google、Facebook、Amazonと巨大企業が誕生
    - **ジェフ・ベゾス**（2003年のTEDでの講演）
      - タイトル：次のウェブ・イノベーション
      - ネットバブルはゴールドラッシュと比較されるが
      - 電気産業の初期の頃に似ていると
      - https://www.ted.com/talks/jeff_bezos_on_the_next_web_innovation?language=ja
- ブロックチェーン技術の普及
  - ビットコイン、アルトコインの普及が先でその後様々な場所に応用されると予想
  - 現在は壮大な実験中かもしれない？
  - （幸運にも）時間的余裕はまだある。
  - でもビットコイン、アルトコインの普及の段階でシステム監査（や会計監査）からの考え方を反映することが、後々に大きなメリット

Q&A

- 大きな課題と思うのは何ですか？
  - 技術者の不足
  - 「情報を記録する」と「通貨」とを切り離したいが、それが難しそう
  - 暗号通貨に対する規制がブロックチェーンの普及を阻む可能性
- 将来ブロックチェーンを利活用するには、システム監査人は今何をするといいと思いますか
  - Githubで遊ぶこと
  - スマートコントラクトを設計し、コーディングしてみること
  - ブロックチェーンで記録する情報の洗出しと整理

付録　IsTech（造語）（Fintechだけでなく）

- ITと情報技術
  - IT企業と情報技術会社の違い
- 「情報技術」もITで変革中
  - オンプレミスからクラウドへ
  - アプリケーションプログラムからアプリへ
- 今の若者は、「IT金持ち」
  - メモリも、ディスクも、CPUも、ネットも、使い放題
- 我々のような『「IT成金」の発想』からの脱却が必要
- 事例：テラやペタは当たり前
  - Statcast（AWSを利用）
    - MLBでゲームの情報（選手やボールの動き等）をレーダーを利用してすべてを記録、分析し、興味深い情報を視聴者に提供
      - 1試合当たり**7テラバイト**
      - 1シーズンで**17ペタバイト**
    - 2015年から運用
    - NHKでも、選手（大谷選手を始め日本人プレイヤーも）の分析に利用
    - Amazonサイトに紹介記事と映像
      - https://aws.amazon.com/jp/solutions/case-studies/major-league-baseball-mlbam/