IoTへのブロックチェーンの適用に関する現状と課題

四條能伸

大阪大学 / IFA株式会社

DPF 研究会

2019/12/26

自己紹介

四條能伸（しじょう よしのぶ）

大阪大学 博士後期課程

IFA株式会社 執行役員CTO

仮想通貨 c0ban を扱うサービス・仮想通貨取引所を運営する株式会社LastRoots執行役員CTOを務めた後、ブロックチェーンを専門に扱うフリーランサーとしてコンサルティング・システム設計/開発などに従事。2018年10月より大阪大学博士後期課程に入学しブロックチェーン×IoTをテーマにした研究を開始。2019年7月より、IFA株式会社に入社し、ブロックチェーンを活用した分散型情報銀行の設計・開発等に従事。

本講演の背景

- IoT への注目が日に日に高まってきている
  - 低遅延広帯域ネットワークやデバイス製造コストが安価になってきた
  - 2022年には500億を超えるデバイスが接続されると予想されている
- IoT のデバイスやサービスの固有の特徴による新たな課題
  - デバイスの多様性、資源制約
  - 垂直統合型ではなく水平統合型サービスのサービスへの転換
- ブロックチェーン技術による課題解決
  - 既に様々なユースケースも出てきている
- ブロックチェーン × IoT という組み合わせならではの課題

本講演の目的

① ブロックチェーンと IoT のデバイスやサービスなどの基礎を解説した上で、IoT 固有の問題についてブロックチェーンを適用することにより解決する方法を説明

② IoTとブロックチェーンを組み合わせることによって生じる新たな課題とその課題解決に向けたアプローチを解説

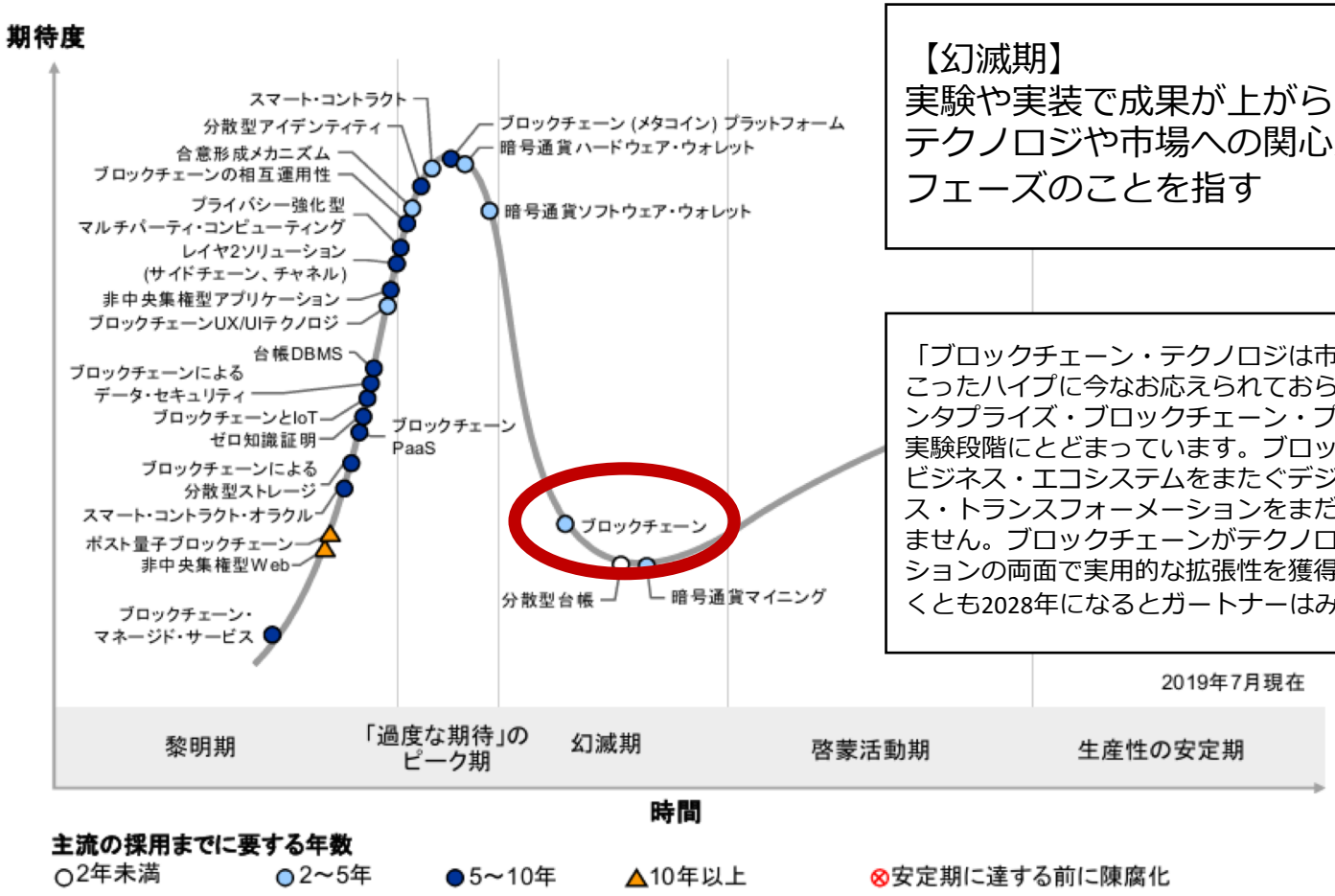
ブロックチェーン技術の推移

仮想通貨のために開発されたブロックチェーンは、金融分野への適用を経て、
非金融分野への適用が積極的に進められている段階

出典) GrowShip Partners ブロックチェーン活用事例 https://www.growship.com/blockchain/

ブロックチェーンのハイプサイクル (2019)

実験や実装で成果が上がらないため幻滅期に突入。
研究開発を推進することによる幻滅期からの脱却が求められている。



【幻滅期】
実験や実装で成果が上がらないため、テクノロジや市場への関心が薄れたフェーズのことを指す

「ブロックチェーン・テクノロジは市場で巻き起こったハイプに今なお応えられておらず、大半のエンタプライズ・ブロックチェーン・プロジェクトは実験段階にとどまっています。ブロックチェーンは、ビジネス・エコシステムをまたぐデジタル・ビジネス・トランスフォーメーションをまだ実現できていません。ブロックチェーンがテクノロジとオペレーションの両面で実用的な拡張性を獲得するのは、早くとも2028年になるとガートナーはみています」

出典) ブロックチェーン・テクノロジのハイプ・サイクル：2019年
https://www.gartner.com/jp/newsroom/press-releases/pr-20191018

ブロックチェーンの可能性

ブロックチェーンは様々な業界に大きなインパクトを与えうる新興テクノロジーとして注目されており、将来大きな市場を形成する可能性がある

グローバル市場

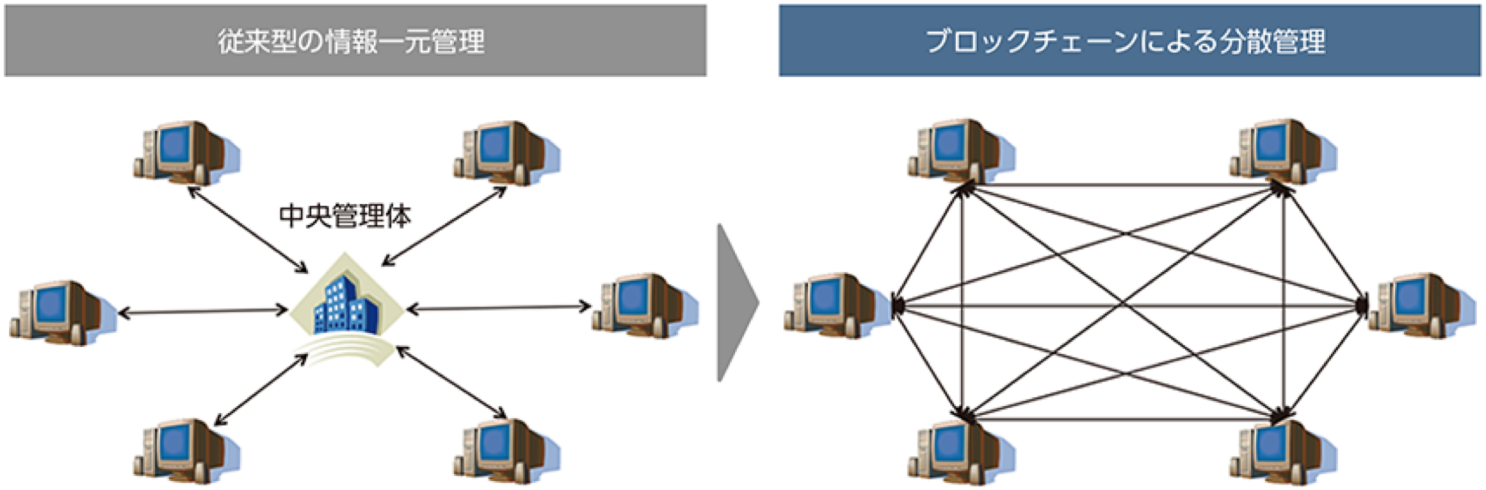
300兆円規模*1

*1：3.1兆ドル(2030年時点の予想値)「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(平成28年4月28日 経産省)」(GARTNER)より抜粋
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（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」）

ブロックチェーンの概要

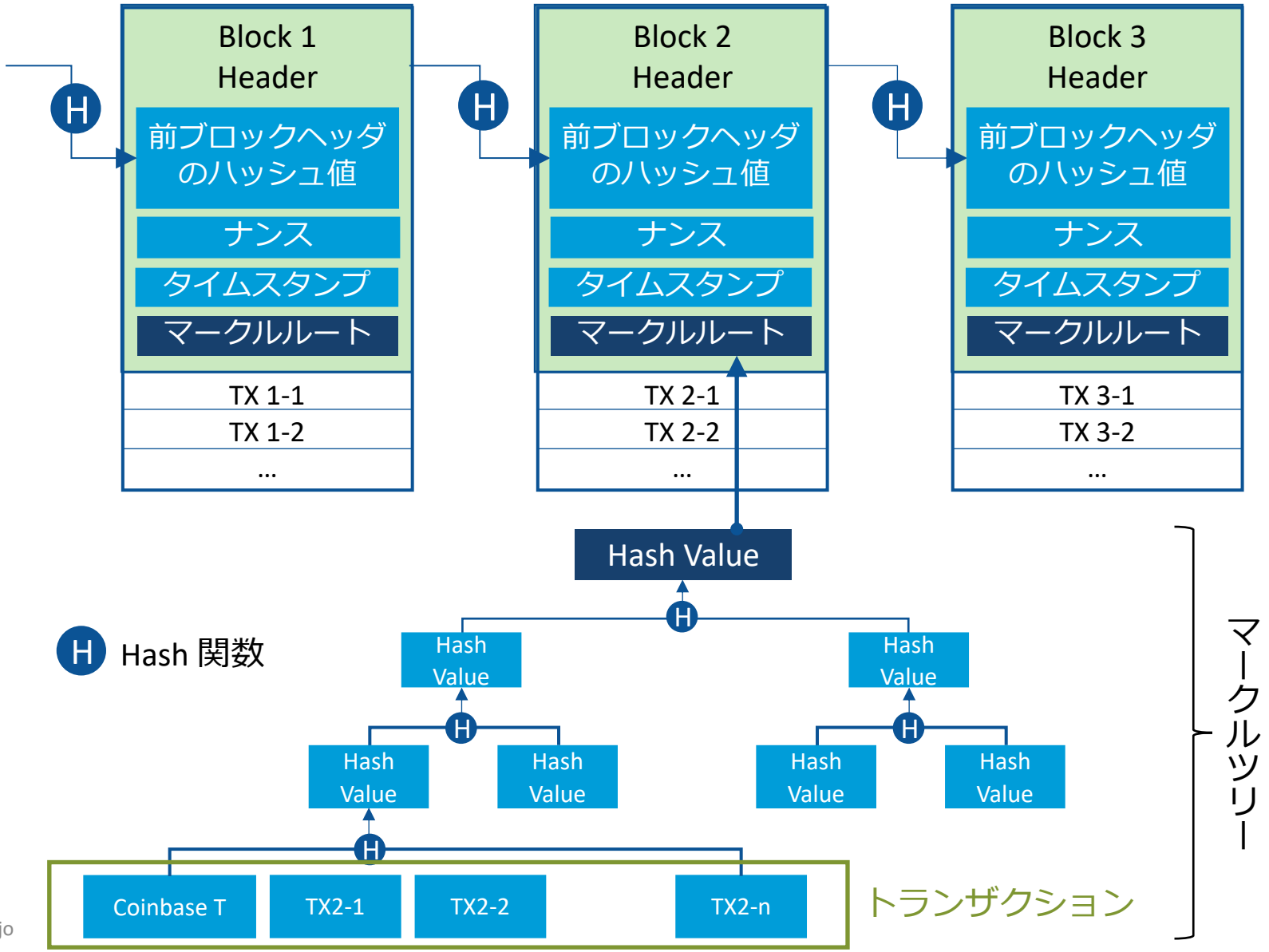
（一般社団法人日本ブロックチェーン協会による定義）
電子署名とハッシュポインタを使用し**改竄検出が容易なデータ構造**を持ち、且つ、当該データを**ネットワーク上に分散する多数のノード**に保持させることで、高可用性及び**データ同一性等を実現**する技術

信頼できないノードからなる分散システムにおいて、
ただ１つの状態への合意形成を図り
その結果の改ざんあるいは紛失を防ぐ技術



図は総務省「ICTによるイノベーションと新たなエコノミー形成に関する調査研究」（平成30年）より引用

データ構造


Block 1
Header
前ブロックヘッダのハッシュ値
ナンス
タイムスタンプ
マークルルート
TX 1-1
TX 1-2
...
Block 2
Header
前ブロックヘッダのハッシュ値
ナンス
タイムスタンプ
マークルルート
TX 2-1
TX 2-2
...
Block 3
Header
前ブロックヘッダのハッシュ値
ナンス
タイムスタンプ
マークルルート
TX 3-1
TX 3-2
...
H
Hash 関数
Hash Value
Coinbase T
TX2-1
TX2-2
TX2-n
トランザクション
マークルツリー

トランザクションデータの完全性

下記 2 つの方法でトランザクションデータの完全性を保証している

マークルツリー

- マークルツリーの性質により、トランザクションを変更すると、マークルルートの値が変わる
- ブロックにマークルルートが保存されているため、その値と突き合わせることで、トランザクションが変更されたことがわかる

- 変更されたトランザクションに基づいたマークルルートを計算し、ブロックを生成することで回避可能

ブロックハッシュによる単方向リスト

- 1 つ前のブロックヘッダのハッシュ値をポインタとしてブロックに含めることで、単方向リストを実現している
- トランザクションが変更されることでマークルルートが変更されると、ブロックヘッダのハッシュ値も変更される。すると、ポインタの参照先がなくなり、ブロックのチェーン構造が崩壊する。

ブロックチェーンのワークフロー（ビットコインの場合）

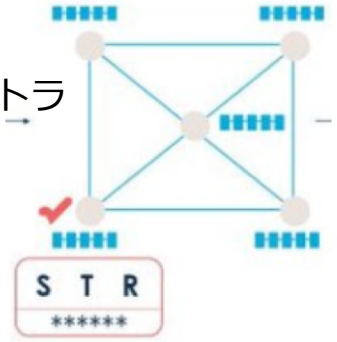
トランザクションの処理

トランザクションの発行・共有

- 送信元、受信先、処理内容を記述したトランザクションの発行
- トランザクション発行者の証明として「電子署名」を付与
- ブロックチェーンネットワークへとトランザクションの送信

トランザクションの確認

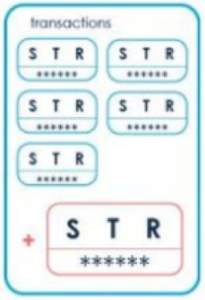
- 署名の検証
- 処理内容の確認
- ブロックへの追加候補としてトランザクションプールへと追加



ブロックに対するコンセンサスの形成

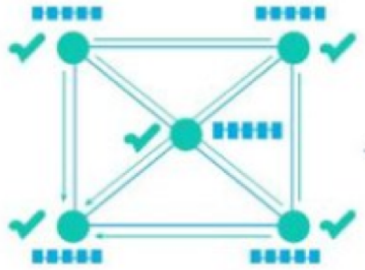
ブロックの生成

- トランザクションをブロックの中に入れる
- 「マイニング」によるブロック生成の労働証明を付与する
- ブロックを送信する



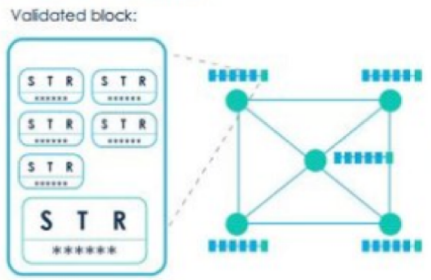
ブロックの確認

- トランザクションの確認
- 労働証明の確認
- 前ブロックハッシュ値の確認



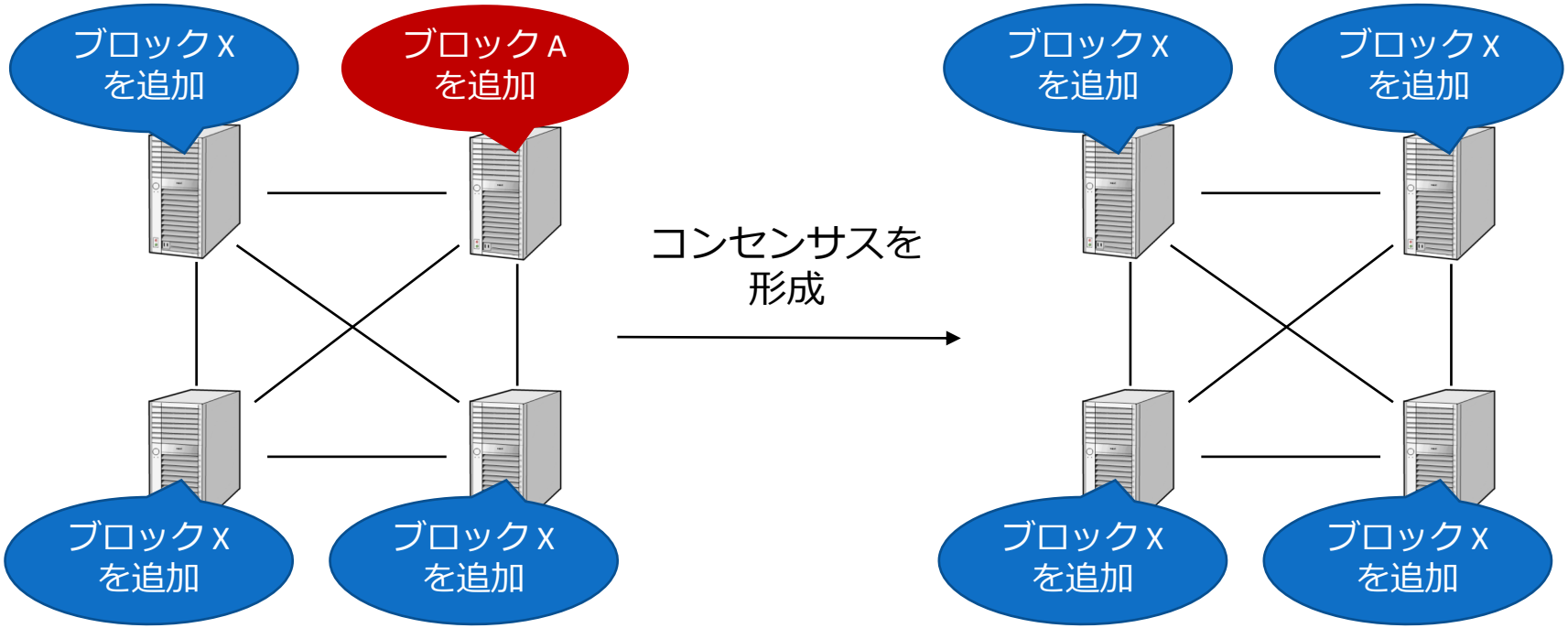
チェーンへの連結

- 新しいブロックとしてチェーンに連結する



ブロックチェーンにおけるコンセンサスアルゴリズム

- ビザンチン故障が発生しうる環境下において、分散ネットワーク全体でただ1つの共通のブロックチェーン情報を共有するためのアルゴリズム



- ノードの参加権限やブロック生成権利によって、大きく2つに分けられる
  1. 非決定的：一度チェーンに追加されたブロックが無効になる可能性がある
  2. 決定的：一度チェーンに追加されたブロックはその時点で確定する

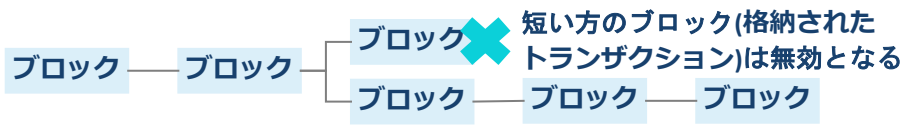
非決定的なコンセンサスアルゴリズム

- 任意のノードがコンセンサスに関与可能であることが前提
- 故意的にコンセンサスを阻害するノードを含む多様な環境であるため、
  コストとインセンティブに基づくアプローチを採用

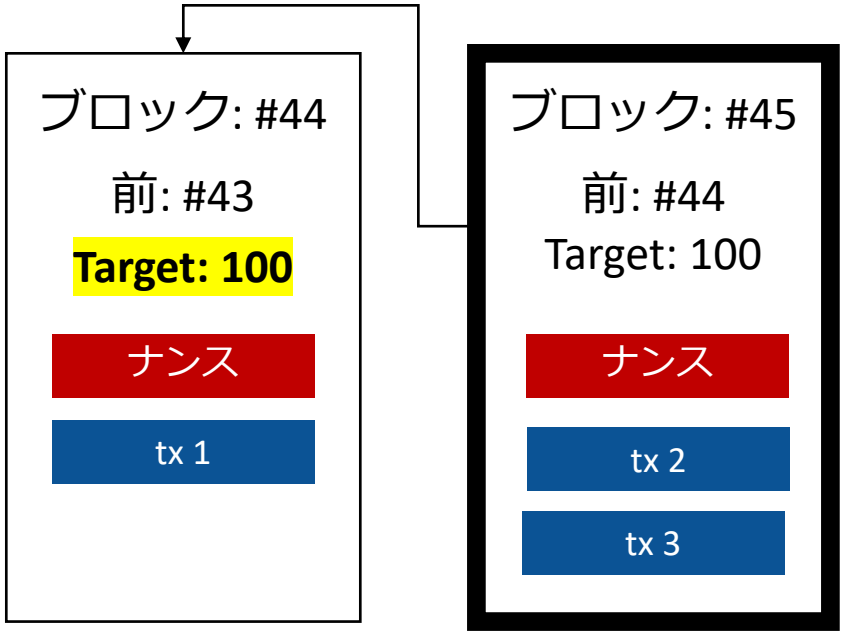
- 何らかのコストをかけたノードが優先的にブロックを追加可能
- 対価として金銭的な報酬を付与

※2つ合わせて「マイニング」と呼ぶ

- トランザクションプールから任意のトランザクションを選択しブロックを作成
- そのブロックに対し、コストがかかる証明を付与
  - 計算コスト、信頼コスト、経済的コスト、etc...
- 正しいブロックを作成したノードには、金銭的な報酬を付与する
  - 「マイニング報酬」とも呼ばれる
  - 不正なブロックを生成するとコストのみがかかり無駄になる。
    そのためノードには正しいブロックを生成するインセンティブがある。
- 分散環境ゆえ、同タイミングで異なる有効なブロックが生成される可能性がある。
  そのため一時的にチェーンが2つに分裂する可能性があるが、
  長いチェーンを有効というルールを定める。短いブロックは無効になる。

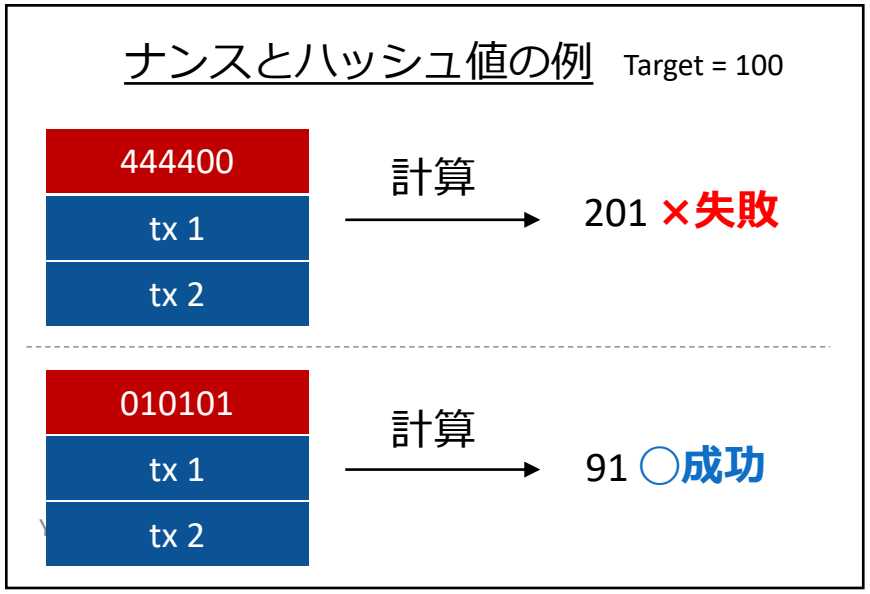


（参考） Proof of Work によるマイニング



ブロック #45 を生成する時…

1. ブロックに含める取引をまとめる
2. ノンスと呼ばれる値を適当に選ぶ
3. 取引とノンスを結合してハッシュ値を計算する
4. 計算結果が…
   Target以下: 成功
   Target以上: ノンスを変えて再計算



ポイント

- ネットワークの全ノードが同時に計算しても10分に1回しか計算に成功しないようにTargetが調整されている

  → ブロック生成は天文学的な難しさ

決定的なコンセンサスアルゴリズム

- 事前に指定されたノードのみがコンセンサスに関与可能であることが前提
- 少数の信頼できるノードのみが含まれる環境であることを考慮したアプローチが利用可能

- 多数決、あるいは代表者によるブロックの生成と追加

「ブロックの承認」と「ブロックチェーンへの追加」を多数決に基づきフェーズを分けて実施することで、トランザクションの決定性を保証することが多い

- ブロックの生成
  任意のトランザクションを選択してブロックを作成。作成したブロックを事前に定められた他のノードに共有。
- ブロックの承認
  ブロックに対してある一定以上の賛成票(署名による投票)が投じられればそのブロックは、チェーンに追加されるブロック候補となる
- チェーンへの追加
  ブロック候補をブロックに繋いで他のノードへと送信。そのタイミングで再度一定以上の賛成票が投じられればそのブロックは可決。そうでなければ棄却。(決定的)

（参考） PBFT による合意形成

トランザクションの共有

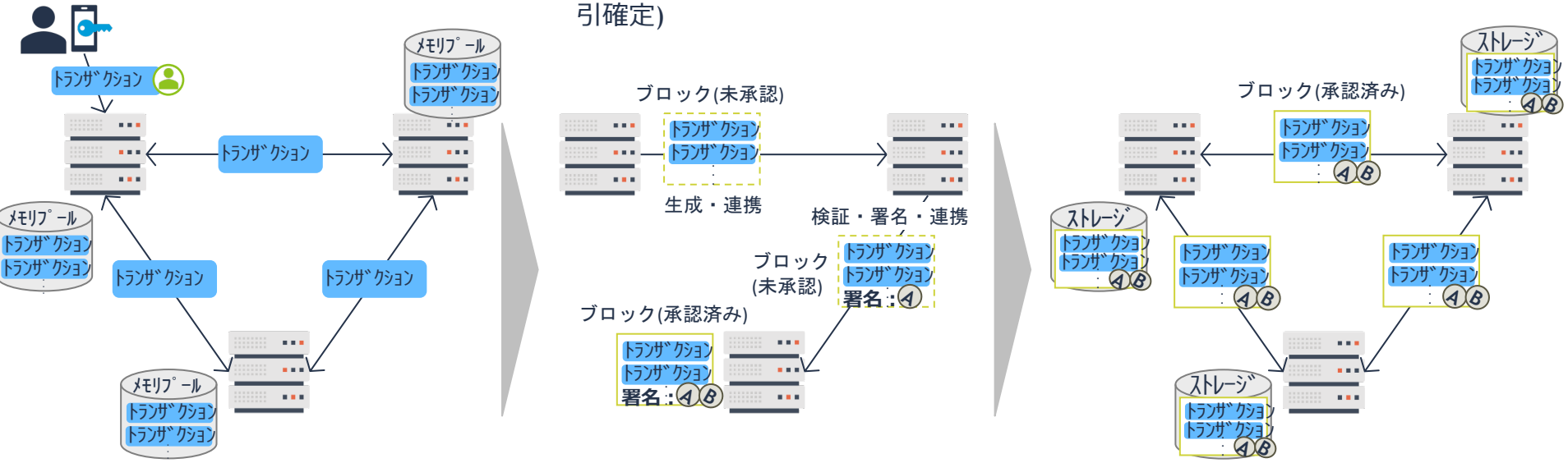
- 参加者はトランザクションを生成してノードへ連携
- ノードは形式チェックのうえ、トランザクションを全ノードへ連携
- ノードは受取ったトランザクションを各自が保持するメモリプールへ格納

ブロックの生成・承認

- ノードはメモリプール内のトランザクションを取出し、署名・残高・二重払い等チェックのうえ、ブロック(未承認)を生成して他のノードへ連携
- 他のノードはブロックを検証して正当と判断すると、これに自身の署名を付与
- これを繰返し、規定数のノードの署名が付与されるとブロック承認 (取引確定)

チェーンへの追加

- ノードはブロック(承認済み)を全ノードへ連携
- 受取ったノードはアドレスの残高状態等を更新し、承認済みトランザクションをメモリプールから削除のうえ、最新のブロックをブロックチェーンに繋げる
- 次のブロックの生成／検証に向け準備



ブロックチェーンの分類

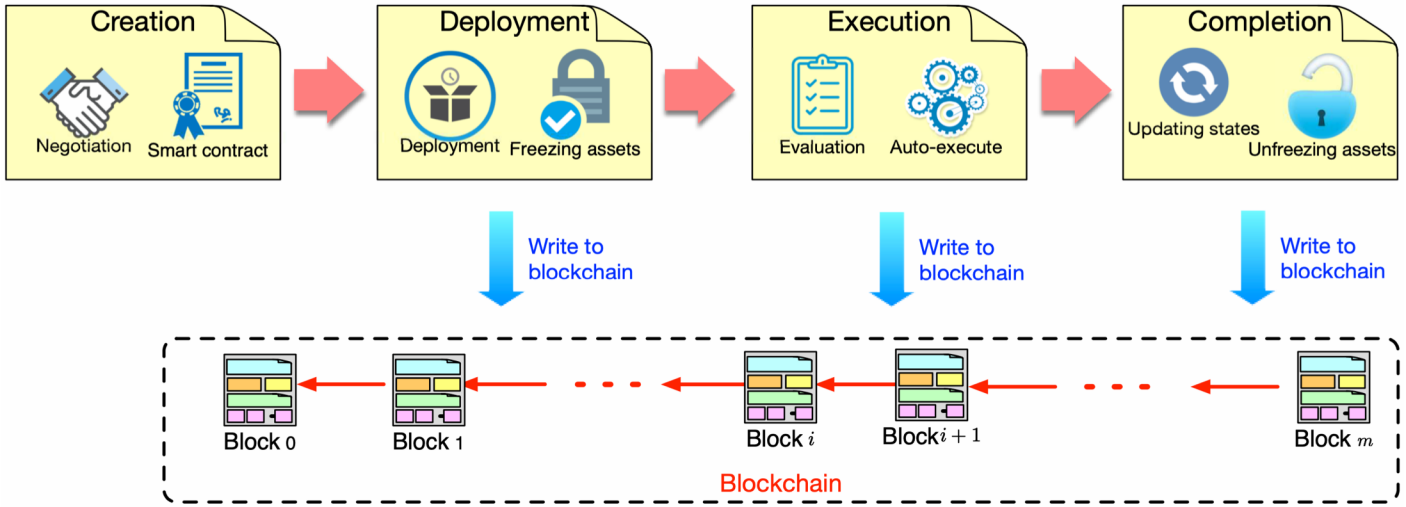
コンセンサスに関与可能なノードの種類に応じて 3 つに分類可能

	Public	Consortium	Private
コンセンサスに関与可能なノード	自由	事前に指定	事前に指定
ノードの管理者	多様	複数組織	単一組織
ノードの信頼	信頼できない	多少信頼できる	信頼できる
コンセンサスアルゴリズム	PoW, PoS, PoI, etc...	PBFT, PoA, PoET	PoA, Ripple
非中央集権性	○	△	×
ノードスケーラビリティ	○	×	×
トランザクションスケーラビリティ	×	△	○
ブロック生成までの時間	長い	比較的短い	短い
トランザクション手数料	必要	不要	不要

スマートコントラクト

- 「契約」を自動執行する仕組みのこと
- コンピュータプログラムの形式で契約内容を記述。条件を満たした時に処理が実行される。
- ブロックチェーンにおいては「契約内容」「処理の実行」「結果に応じたデータの書き換え」のそれぞれがトランザクションとしてブロックチェーンに保存される。通常のトランザクション同様、ノードによる検証が行われる。

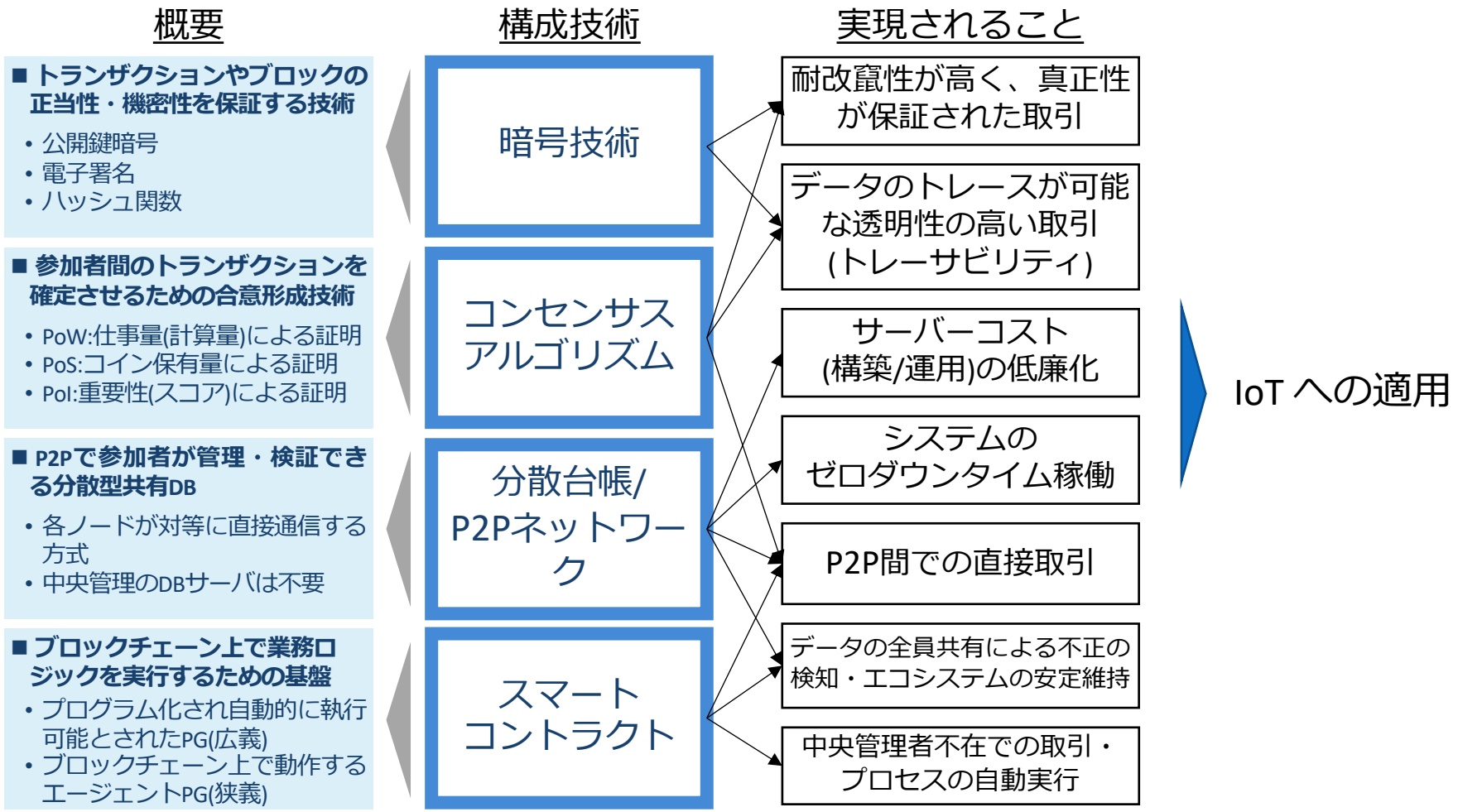
管理者であっても、プログラムを不正に実行したり、
その結果を改ざんすることができなくなる



※図は Honh-Ning Dai, et., al, “Blockchain for Internet of Things: A Survey” より引用

ブロックチェーンのまとめ

様々な技術を組み合わせることで、**信頼できないノードからなる分散システム**において、有益な性質を実現している



出典) GrowShip Partners ブロックチェーン活用事例 https://www.growship.com/blockchain/

（参考）ブロックチェーン技術の今後

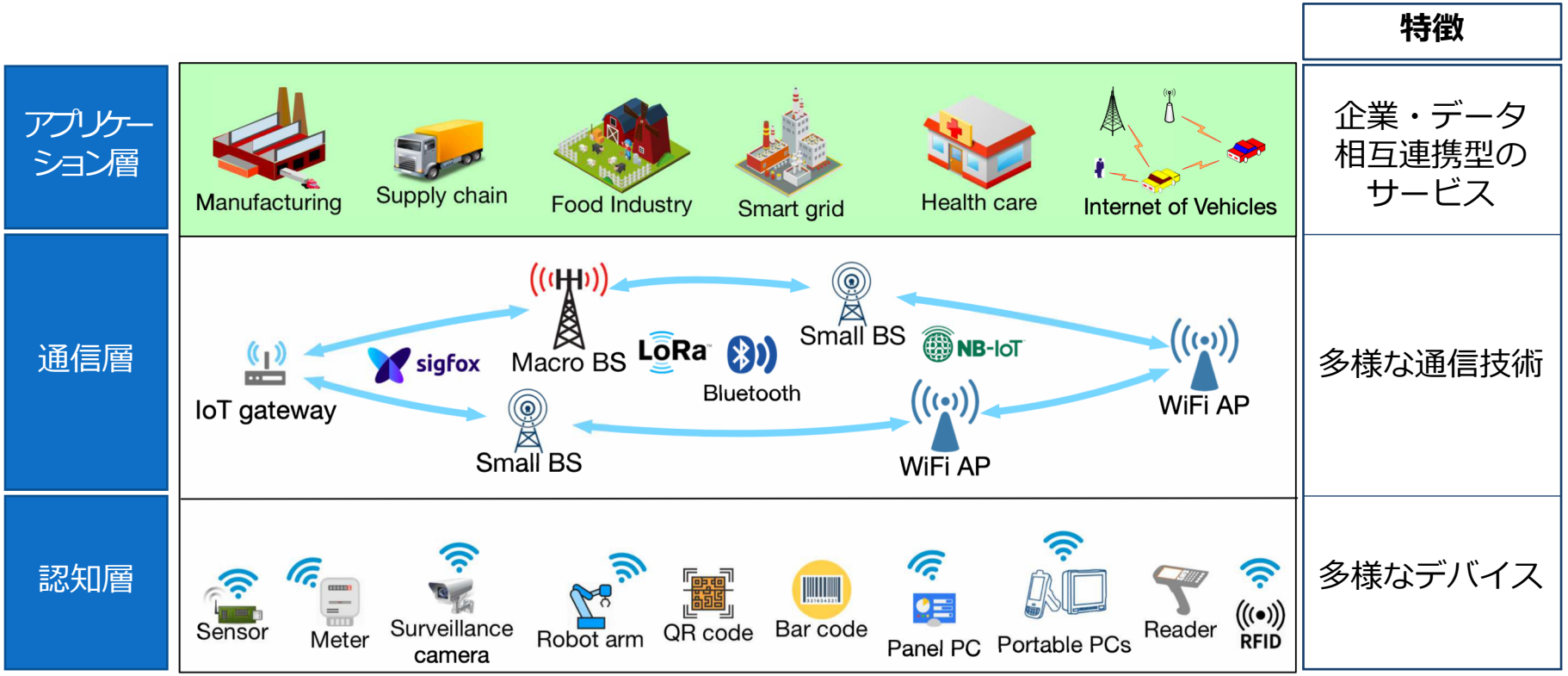
- 特にスケーラビリティとプライバシーの問題への取り組みが盛ん

	課題	アプローチ
スケーラビリティ	• ストレージ容量の逼迫する • 秒間あたりのトランザクション処理速度が遅い	• 高速なコンセンサスアルゴリズムの開発 • サイドチェイン • シャーディング • オフチェーントランザクション • Lightning Network, Plasma

プライバシー	• トランザクションの内容が公開されてしまう
	• トランザクションとトランザクション発行者が密に紐付けられてしまう
		• 秘匿化・匿名化
		  • 秘匿化：トランザクションの内容を隠蔽する
		  • 匿名化：トランザクションの発行者を隠蔽する
		• ゼロ知識証明の活用
		• MPC(Multi Party Computation) の活用

IoT: Internet of Things

- あらゆる「モノ」をネットワークに接続し、ネットワーク経由でセンサー情報の取得、アクチュエータの制御を実施するシステム・概念
- 「IoT のデバイスやシステム」と「 IoT プラットフォームサービス」のそれぞれにおいて、固有の特徴・課題がある



※図は Honh-Ning Dai, et., al, “Blockchain for Internet of Things: A Survey” より引用

IoTデバイス・システムの特徴・課題

- データの多様性
  - 種類・形式の双方において様々なパターンが存在する
- 相互運用性
  - 同じ性能・性質だがインターフェースなどが異なる場合がある
- スケーラビリティ
  - デバイスの数は増え続ける
- データの完全性・可用性の担保
  - センサーデータの改ざん、消失などが発生する
  - 誤ったデータに基づいた運用・判断がされる可能性がある
- プライバシー
  - 例えば個人情報と位置情報データが関連付けられ利用されないか？
- セキュリティ
  - 認証、認可、通信暗号化
- デバイスの多様性
  - 処理方式、稼働方式、実装センサー・アクチュエータ、etc...
- リソース制約
  - 処理、ストレージ、ネットワーク、バッテリーが非力な場合がほとんど
- ハードウェア故障
  - 長期間、低頻度のメンテナンス環境下で運用されることが多い
- 物理的な障害
  - デバイスの盗難、不正操作
  - 周辺環境の変化などの影響

IoTデバイス・システムの特徴・課題

- データの多様性
  - 種類・形式の双方において様々なパターンが存在する
- 相互運用性
  - 同じ性能・性質だがインターフェースなどが異なる場合がある
- スケーラビリティ
  - デバイスの数は増え続ける
- データの完全性・可用性の担保
  - センサーデータの改ざん、消失などが発生する
  - 誤ったデータに基づいた運用・判断がされる可能性がある
- プライバシー
  - 例えば個人情報と位置情報データが関連付けられ利用されないか？
- セキュリティ
  - 認証、認可、通信暗号化

- デバイスの多様性
  - 処理方式、稼働方式、実装センサー・アクチュエータ、etc...
- リソース制約
  - 処理、ストレージ、ネットワーク、バッテリーが非力な場合がほとんど
- ハードウェア故障
  - 長期間、低頻度のメンテナンス環境下で運用されることが多い
- 物理的な障害
  - デバイスの盗難、不正操作
  - 周辺環境の変化などの影響

これらはブロックチェーンを適用することで課題の解決ができると期待されている

ブロックチェーンを活用することで得られる利点

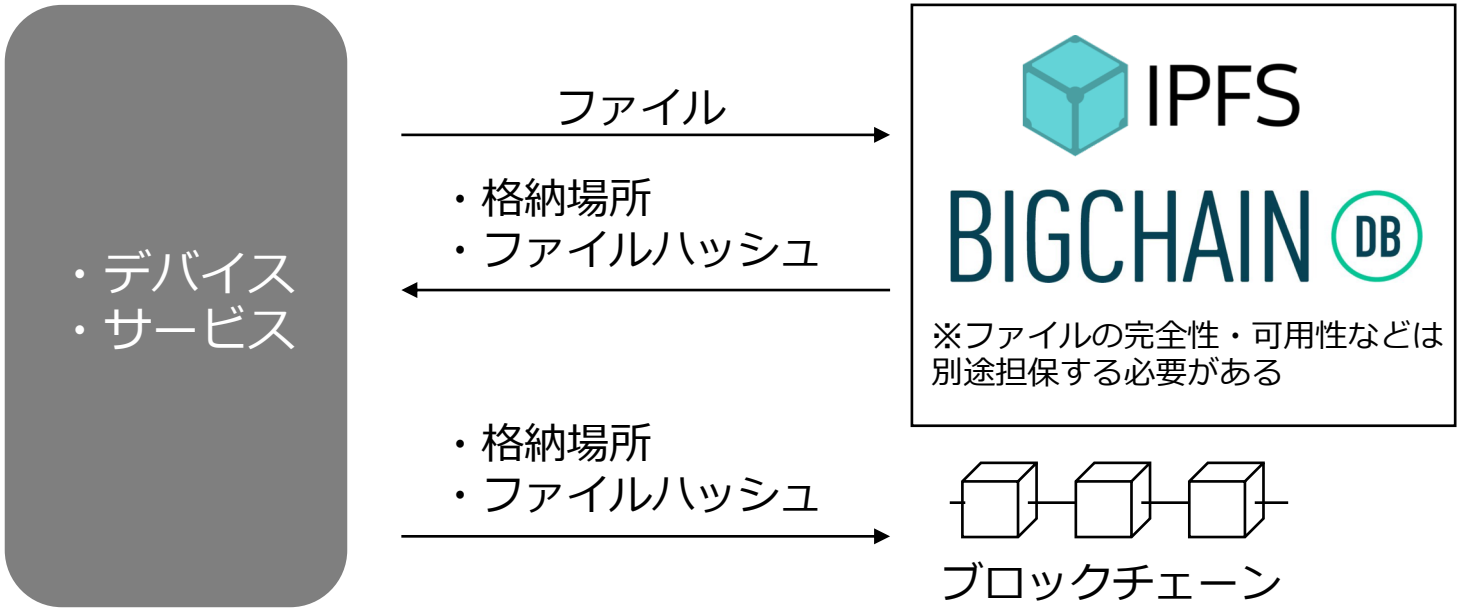
- トラストレスな認証・認可
  - 認証・認可情報を、認証者・認可者の電子署名とともにブロックチェーンに書き込むことで、中央サーバを必要としない認証・認可情報の管理ができる
  - ブロックチェーン上の情報に基づきスマートコントラクトを用いて制御を行う
- データの完全性・可用性
  - ブロックチェーンを分散ストレージとして利用する
  - ブロックチェーン上のデータは改ざん耐性と可用性が保証されている
- 相互運用性の担保
  - ブロックチェーン上のデータと、スマートコントラクトを用いた処理・通信を行う
- 非中央集権性とスケーラビリティ
  - 通信形態やシステムアーキテクチャを P2P 分散型に変更することにより、単一障害点を除去し、データの一極化も防止できる
  - スマートコントラクトを用いた分散的な自動処理によって、ノード数のスケーラビリティを確保できる
- デバイスの自動アップデート
  - スマートコントラクトを用いて、古いファームウェアを利用しているデバイスは自動的にブロックチェーン上に保存されている完全性が担保されたファームウェアを用いてアップデートされる

他にも活用方法は様々ある。

（参考）分散ストレージとしてのブロックチェーン

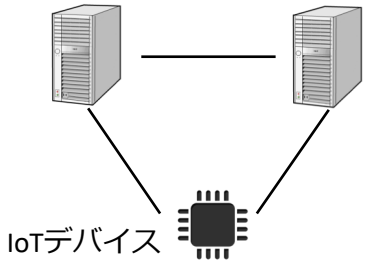
- ブロックチェーン情報を全てのノードで共有するという特徴上、ブロックチェーンそのものはデータ効率が悪いため、そのままではストレージとして利用できない

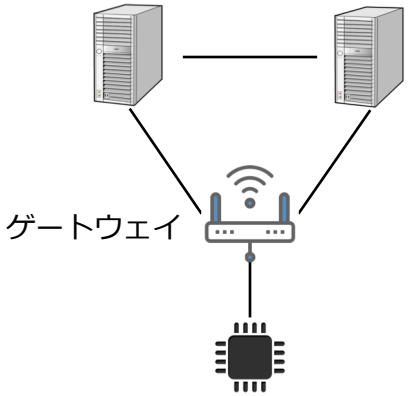
  データは外部の分散ストレージに保存し、ブロックチェーンにはメタデータとファイル場所のみを保存するアプローチが一般的

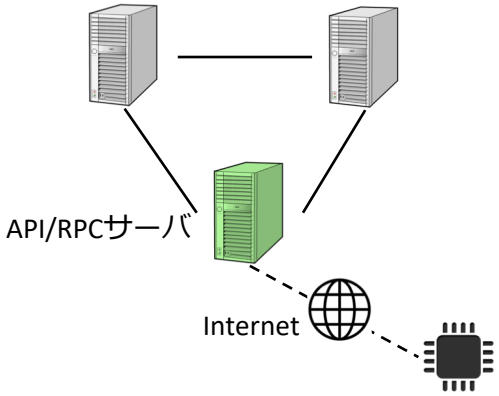


ブロックチェーンノードとの通信方法

- IoT デバイスとブロックチェーンノードとの関係性によって 3 つに分類







直接通信

- IoT デバイスがブロックチェーンノードとして参加する
- トランザクションを直接ブロックチェーンに送信できるため、遅延が少なく、安全。
- ブロックチェーン情報を同期するためストレージを逼迫する

ゲートウェイを介した通信

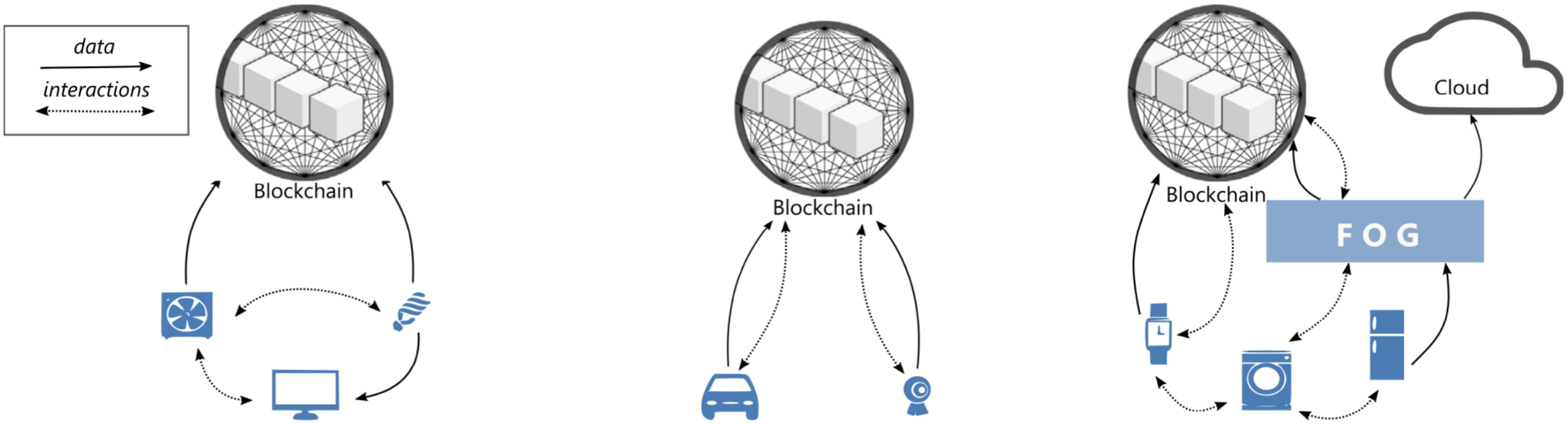
- ゲートウェイを介して通信を行う
- トランザクションはゲートウェイ経由で送信される。ゲートウェイがトランザクションを処理しない等の可能性がある。
- IoT デバイスのリソースを節約できる。

API/RPC を介した通信

- インターネット越しの API/RPCを介して通信を行う
- トランザクションはインターネットを経由するため、消失・盗聴のリスクがある
- デバイス運用者の手間は最も少ない

ブロックチェーンを利用した IoT 機器間の通信方法

- IoT 機器間の通信に対するブロックチェーンの介在方法によって 3 つに分類



IoT - IoT

- IoT機器間はアドホックに通信。ブロックチェーンはデータ保管のためのデータベースという位置づけ。
- IoT 機器が互いに信用できる環境下では有効。

IoT – Blockchain

- 全ての機器間通信はブロックチェーンを通じて実行。
- ブロックチェーンとの通信遅延が生じるが、セキュアな機器間通信を実現可能。

Hybrid

- 信頼できる機器間は直接、そうでない機器間はブロックチェーンを介して通信を実行。
- 設計難易度が高いが、うまく活用できればいいとこ取りができる。

図は Ana Renya, et al., “On blockchain and its integration with IoT. Challenges and opportunities” より引用

事例１｜IoTデバイスへのアクセス権限の制御

Yuanyu Zhang, et al., “Smart contract-Based Access Control for the Internet of Things”

スマートコントラクトでアクセス権限を保持・制御することで、不正なアクセスや権限変更を防止

ACC: Access Control Contract / アクセスコントロールを定義
JC: Judge Contract / ペナルティの執行
RC: Register Contract / ACC や JC の登録・保持

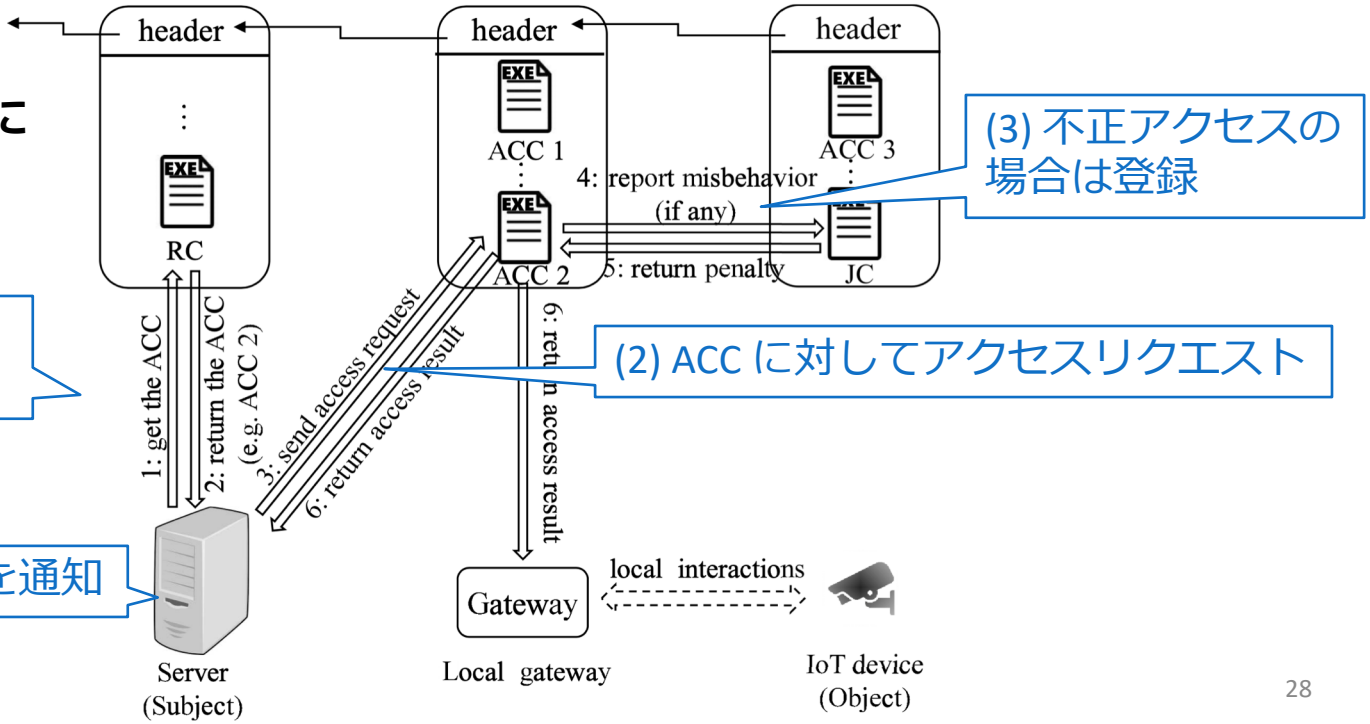
（RCの例）

MethodName	Subject	Object	ScName	Creator	ScAddress
Method 1	Server A	Sensor B	ACC 1	Sensor B	0xca35b7d915458ef540ade6
Method 2	Server A	Sensor B	ACC 2	Sensor B	0xab072c469475346532bf47
Method 3	Sensor B	Server A	ACC 3	Server A	0xb51f6d86d4c998531056a5
JC			Judge		0x3f23c7b929cced4191ef60

（ACCの例）

Resource	Action	Permission	ToLR
file A	read	allow	2017-12-11 16:19
file A	write	deny	2017-12-12 20:34
Program A	execute	deny	2017-12-11 16:19
...	...	...	...

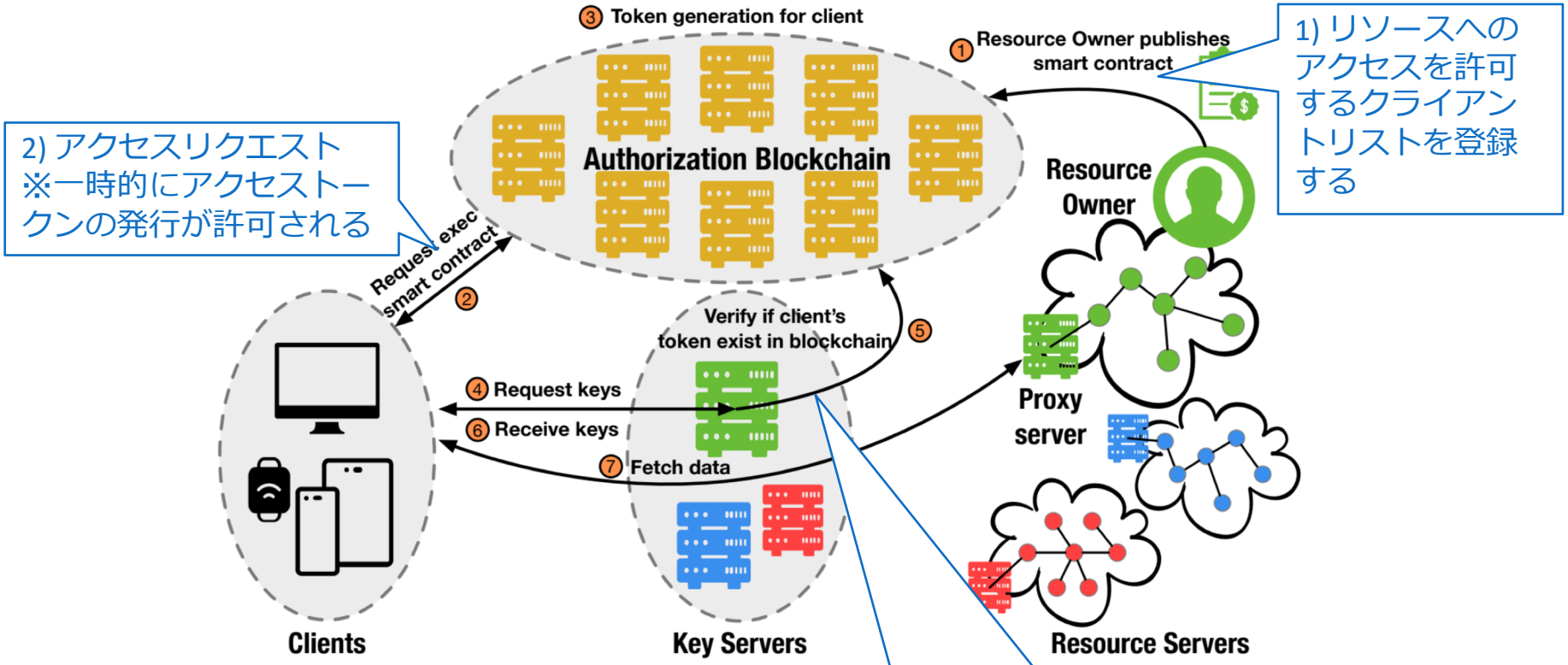
◆**サーバが IoT デバイスにアクセスするケース**



事例２｜リソースサーバへのアクセストークンの発行

Oliver Alphand, et al., “IoT Chain: A Blockchain Security Architecture for the Internet of Things”

センサーデータへのアクセスコントロールを非同期かつ非中央集権的に行うためにブロックチェーンを活用する。膨大なリソースへのアクセス情報も、単一障害点がない完全性が担保されたシステムで管理することができる。



2) アクセスリクエスト
※一時的にアクセストークンの発行が許可される

1) リソースへのアクセスを許可するクライアントリストを登録する

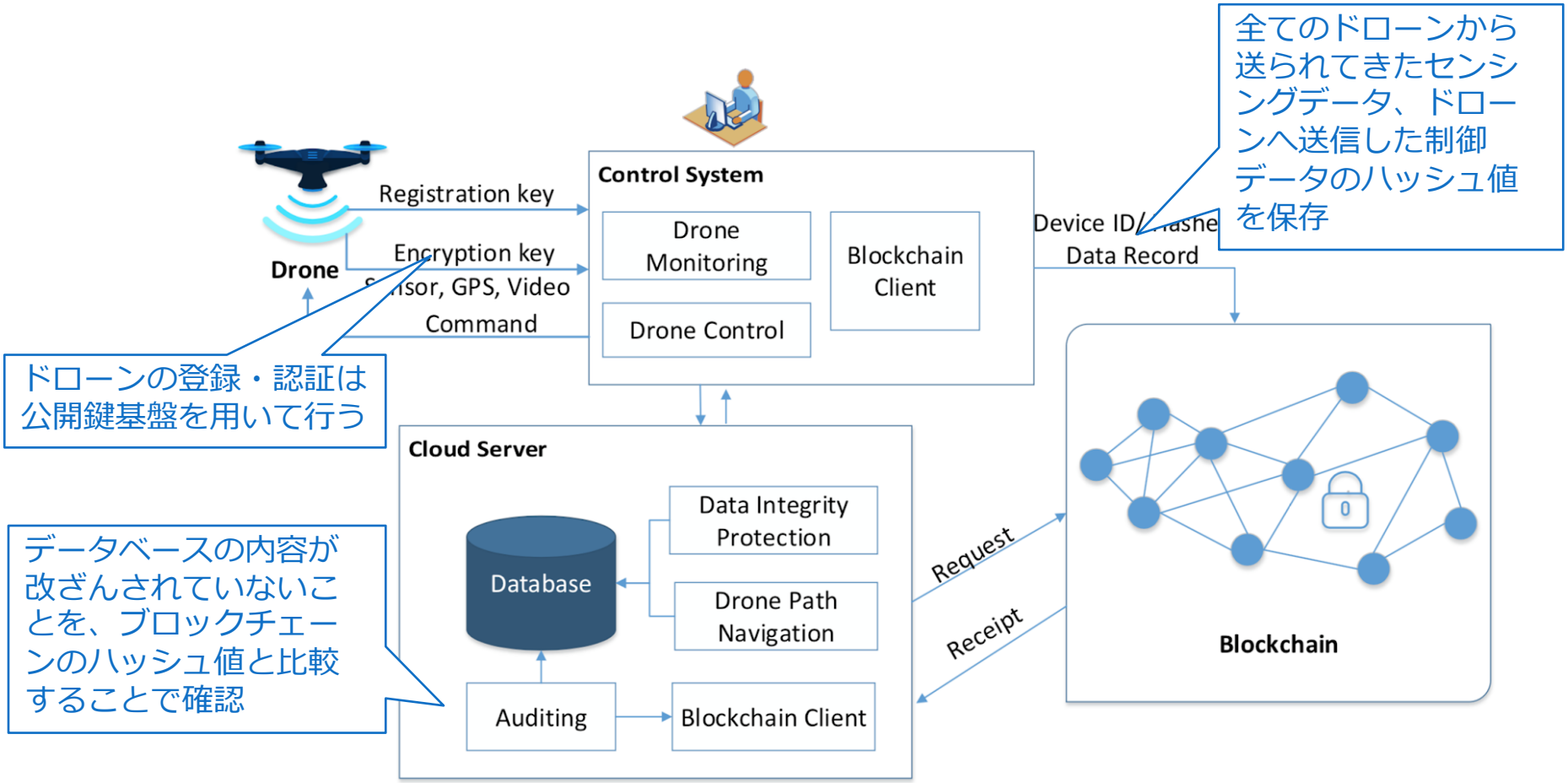
4) 取得したアクセストークンを使ってリソースにアクセスする

3) クライアントのアクセストークン発行が許可されていれば、クライアントにトークンを返す

事例３｜ドローンの制御通信における完全性担保

Xueping Liang, et al., “Towards Data Assurance and Resilience in IoT Using Blochchain”

クラウドで集中制御される IoT 機器は、常にクラウド基盤への攻撃に備える必要がある。特に、過去のデータに基づいて制御が行われるドローンについては、データの完全性を保証することが非常に重要である。完全性担保にブロックチェーンを活用する。



IoT へブロックチェーンを適用する上での課題

- ブロックチェーン情報の容量
  - 過去の全てのトランザクションを保存するため、容量が肥大化していく
    - ビットコイン：254GB、Ethereum：115GB（2019年12月25日）
  - ストレージ制約がある IoT デバイスが直接ブロックチェーン情報を扱うのは現実的ではない
- ブロックの生成間隔 = トランザクションの処理間隔
  - コンセンサスアルゴリズムの処理遅延により、ブロックの最大生成間隔は秒オーダが最速
  - 秒以下の単位でデータを生成し続けるセンサーデバイスと時間のオーダが合わない
- デバイスのリソース制約
  - CPU、メモリ、ストレージ、ネットワーク、バッテリーが貧弱であるため、常時ブロックチェーンネットワークと通信することはできない
- トランザクション手数料
  - パブリック型のブロックチェーンでは、無用なトランザクションの発行を防ぐために手数料を課す場合が多い
  - 数百億台のデバイスにそれぞれ手数料分の暗号資産などを注入しておくことは運用上不可能
- etc...

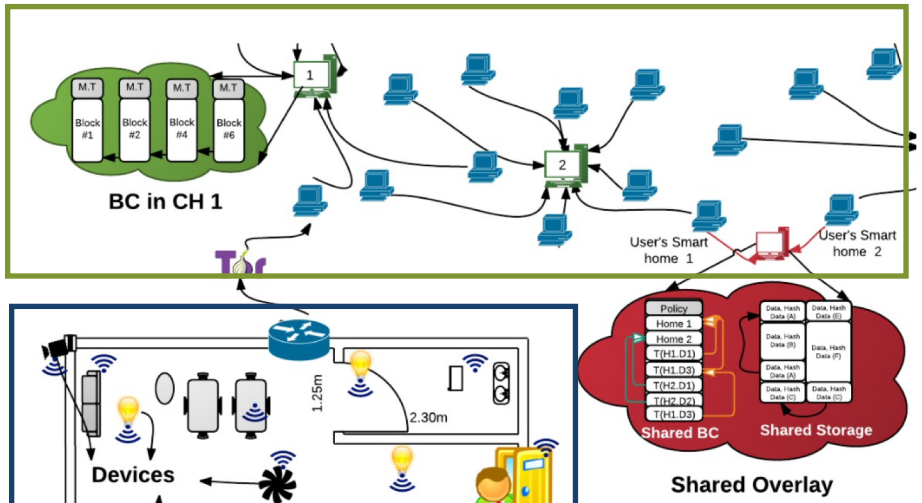
解決策 1 ｜階層型アーキテクチャ

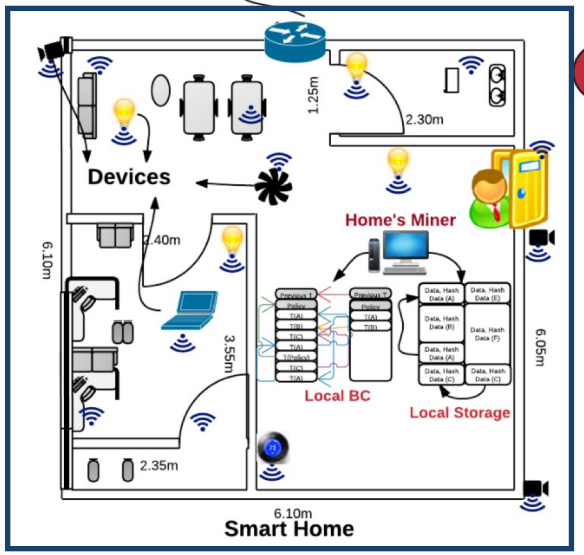
Ali Dorri, et al., “Blockchain in Internet of Things: Challenges and Solutions”

スマートホームを題材に、リソースに応じて利用する異なるブロックチェーン (BC) を利用し、それらを階層的に接続することによって、IoT データの完全性を保証し、かつデバイスへの不正なアクセスを排除する

- [前提] スマートホームデバイスはリソースが乏しい。全てのデバイスは、ゲートウェイに接続されている。ゲートウェイは常にオンラインで、リソースが豊富。
- 階層1: スマートホーム内 Private BC
  - ゲートウェイのみがブロックを生成可能な Private型のブロックチェーンを構成
  - デバイスのあらゆる情報は、ブロックチェーンに刻まれ、ゲートウェイのストレージに保存される
- 階層2: スマートホーム間 Public BC
  - ゲートウェイがノードとしてPublic 型のブロックチェーンを構成
  - Private BC のサマリデータを Public BC に書き込むことで、Private BC のデータ改ざんを防止する
  - 自宅外から自宅内にアクセスする際のアクセス権限リストもPublic BCで管理。ゲートウェイが適宜参照することで、不正なアクセスを排除する。

スマートホーム間 Public BC



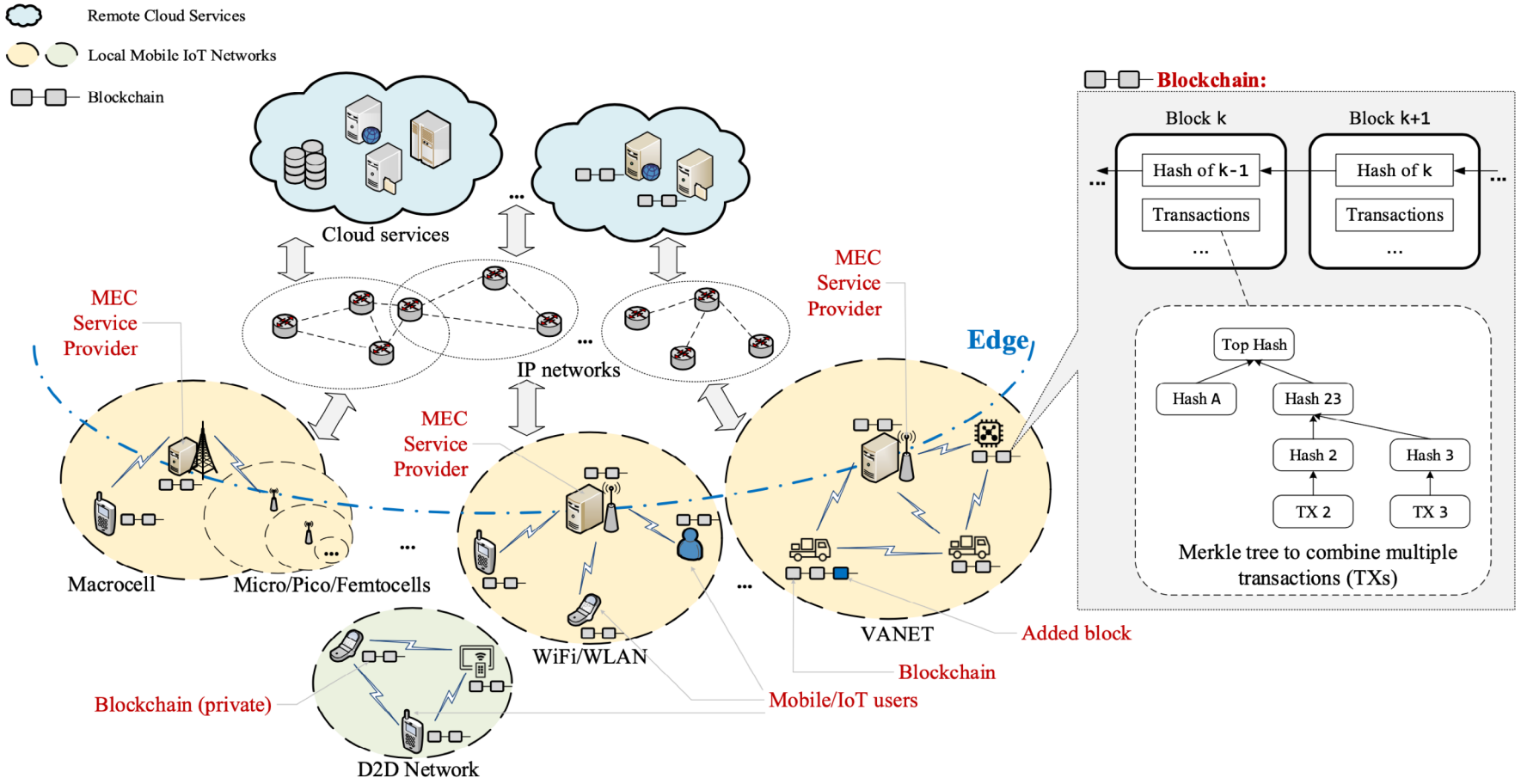


スマートホーム内 Private BC

解決策２｜MEC との協調、計算のオフロード

Zehui Xiong, et al., “When Mobile Blockchain Meets Edge Computing”

移動する IoT デバイスの場合、ブロックチェーンネットワークへのアクセスエンドポイントが高頻度で切り替わる。そこで MEC(Mobile Edge Computing) と協調することで、ブロックチェーンへのアクセスを行う。またマイニング時の計算のオフロードを行う。
MEC のリソース使用量は、暗号資産・トークンで支払う。　※MECの新しいビジネスに繋がる可能性がある



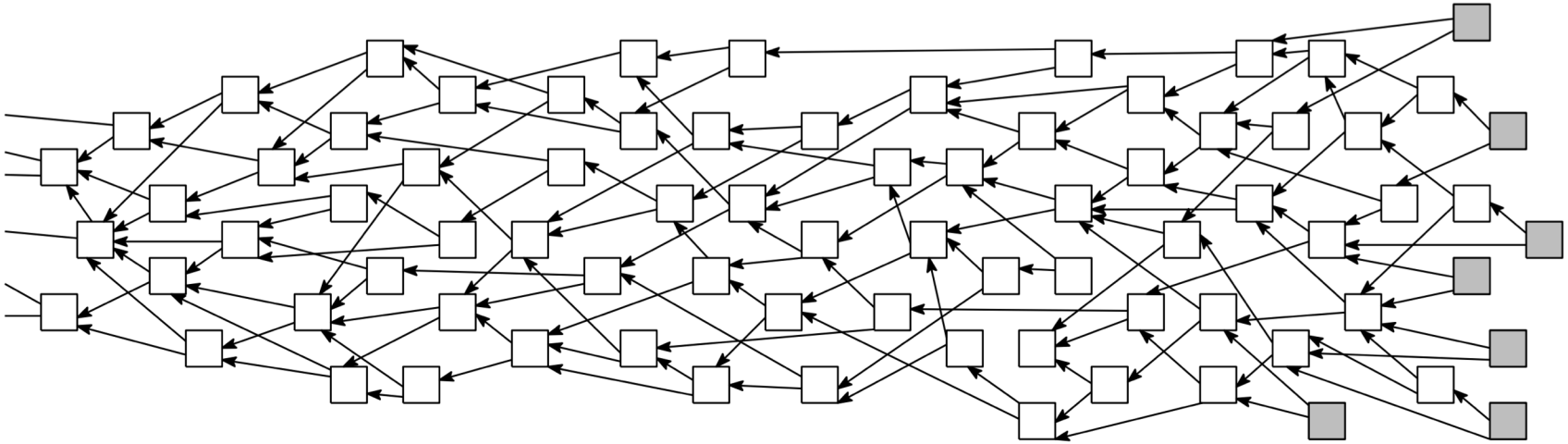
解決策３｜ブロックを生成しないブロックチェーン

Serguei Popov, “The Tangle”

トランザクションが別のトランザクションを PoW にて承認。その対価として、そのトランザクションをネットワークに伝搬できる。そのため手数料が不要。

IOTA における DAG(有向非巡回グラフ) 構造

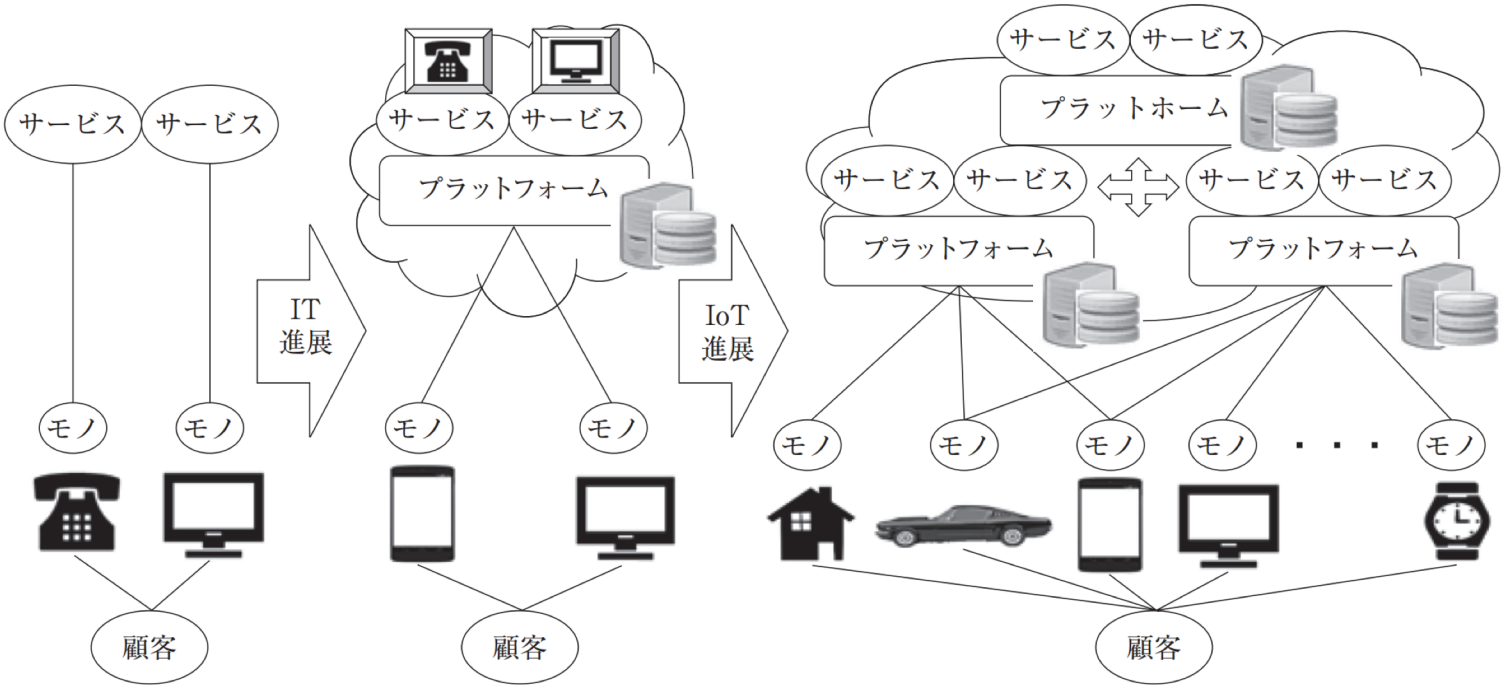
※四角はトランザクションを表現



どのトランザクションも、別の 2 つのトランザクションを承認する

IoTプラットフォーム

- IoTのデバイスやデータを統合管理するためのIoTプラットフォームは、今後より高度なサービスを提供するために、相互に結びつくことが予想される
- 相互接続は肥大化の一途を辿ることが想定されるため、ブロックチェーンを用いた非中央集権型のアーキテクチャが検討されている[経産省2016]
- 中でも、データの相互流通が重要なテーマになっている

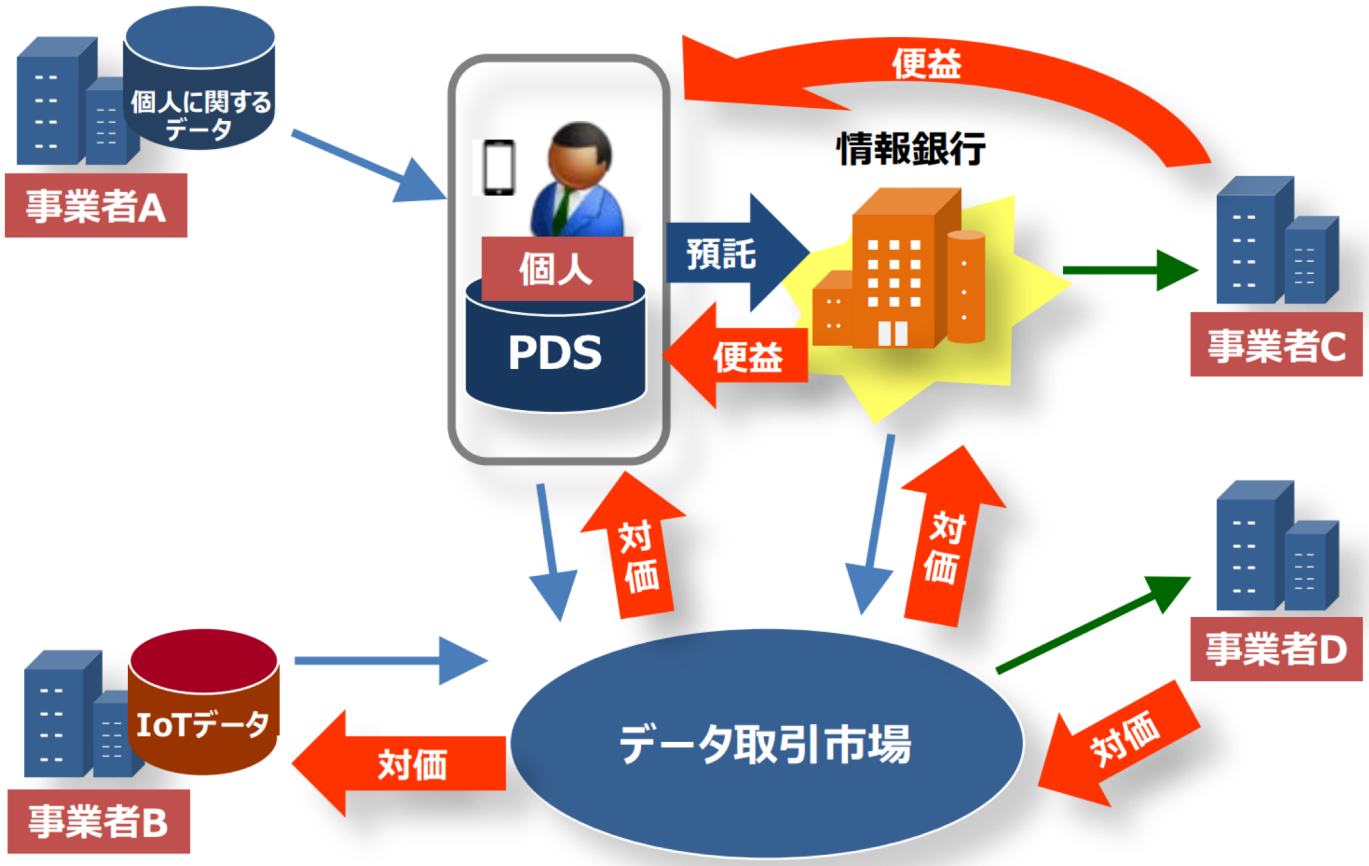


図は下記論文より引用。

北野健太, “IoTにおけるブロックチェーンの適用可能性について –「つながるIoT」プラットフォームの実現に向けて–,” JRIレビュー, Vol. 8, No. 47, 2017.
[経産省2016] 経済産業省 産業構造審議会 情報経済小委員会 分散戦略ワーキンググループ 中間とりまとめ
「IoTの進展による分散型の アーキテクチャ及び社会システム等について」（2016年11月）

（参考）データ取引市場

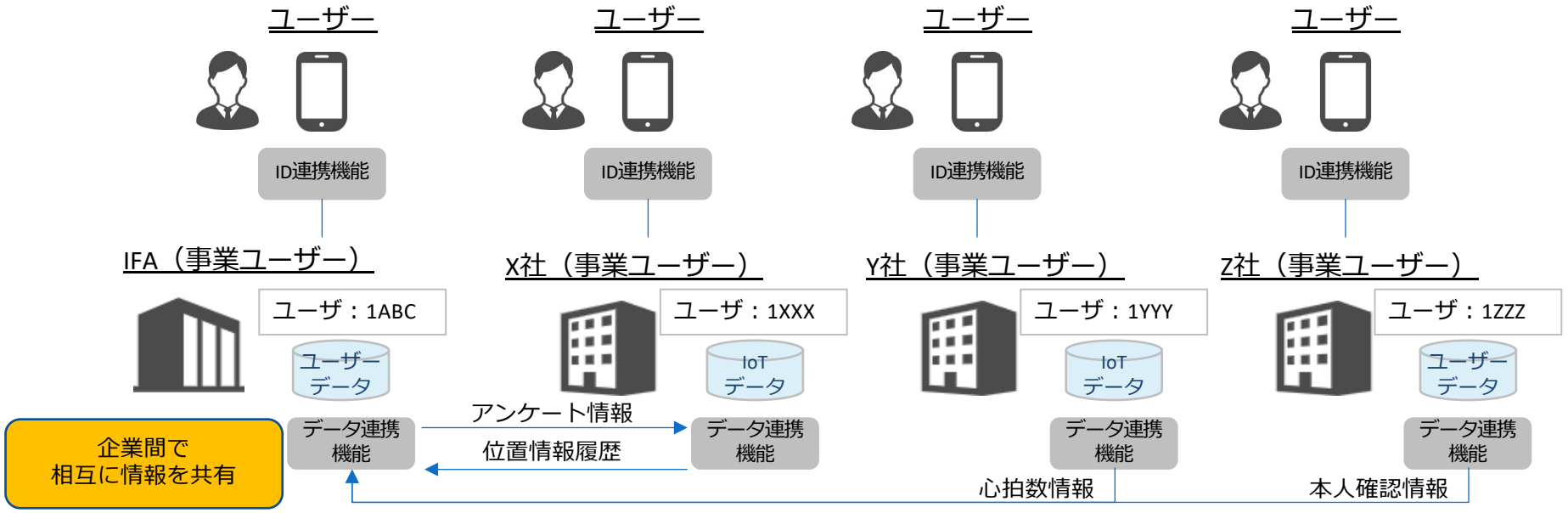
- 日本国としては、事業者による中央集権的なデータ取引市場構想をとりまとめているが、セキュリティ、権限の扱い、透明性の確保、トレーサビリティの確保等の観点で課題があることを指摘している

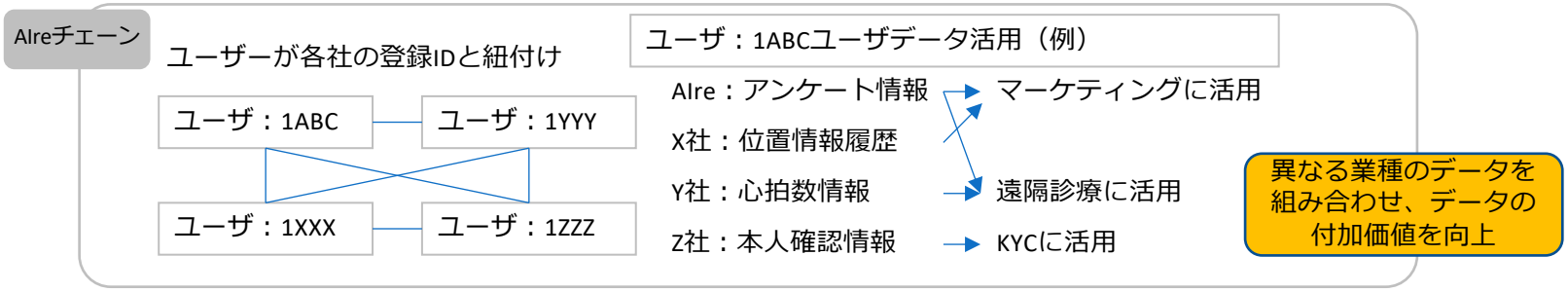


図は「データ流通環境整備検討会 AI, IoT時代におけるデータ活用ワーキンググループ 中間とりまとめ」より引用

企業間情報連携（IFA株式会社における取り組み）

- 各社が保有しているIoTデータなどをブロックチェーンを用いて連携させる
- ブロックチェーンを用いた分散ガバナンスによって、不正なデータ利用を防ぐことが可能





（参考）データ統合によるユースケース

販売者 (デバイス管理者)	データ	購入者	高付加価値情報
国/地方自治体	天候	・旅行会社 ・コンシェルジュサービス会社	・空いている観光スポット ・快適な移動経路
国/地方自治体 自動車メーカー	交通状況		
個人	GPS		
宿泊施設	宿泊施設状況		
個人	ヘルスケア	・保険会社	・保険料金のダイナミックプライシング 例) 体調不良・悪天候・初走行の道 →保険料を高く
国/地方自治体	天候		
自動車メーカー	GPS		
物流倉庫	在庫情報	・農協 ・製造会社	・生産量の調整
店舗	在庫情報		
個人	冷蔵庫の中身		

まとめ

- ブロックチェーンに基礎について解説
  - 信頼できないノードからなる分散システムにおいて、ただ 1 つの状態への合意形成を図りその結果の改ざんあるいは紛失を防ぐことが可能
- IoT のデバイスやサービスについて解説し、ブロックチェーンを適用することによる課題の解決方法について説明。
  また、新たに生じる課題とその解決策のアプローチを説明。
- IoT のプラットフォームについて解説し、ブロックチェーンを用いたデータ連携基盤の実例を紹介。

今後の主要な課題

- IoT デバイスをブロックチェーンと通信させる際の最適なアーキテクチャ
  - セキュリティ、コスト、性能などの観点で比較する必要がある
  - ユースケースにより最適なアーキテクチャは異なるかもしれない
- プライバシーの問題
  - ブロックチェーンでは電子署名を用いたトランザクションの送信元の特定を行うため、システムの稼働時間が長くなるほど、ある送信元に結びつくデータ量が増えるため、プライバシーを侵害する恐れがある
- セキュリティ
  - スマートコントラクトのバグ、ブロックチェーンの構成方法に起因するバグ、etc...
  - ブロックチェーンの抱える潜在的なセキュリティの問題とその対処方法を検討する必要がある
- トランザクションのスケーラビリティ
  - 比較的高速なコンソーシアム型のブロックチェーンでは 2000tps 程度が実際のスループットの限界と言われている
  - スループットを向上させるためのアーキテクチャ、処理様式などを検討する必要がある