２Ｃ１５

ブロックチェーン×ビジネス

－IoT 分野への適応を例題として－

○高橋　浩（B-frontier 研究所）

１．ブロックチェーン導入の目的

最近、多数の新技術が登場している。AI,IoT,BD,ブロックチェーン他。これらの新技術は最初は技術自体への関心から出発するが、適応進展、適用領域拡大に伴い新技術×ビジネス、即ち、どれだけビジネスとして成立しうるか、あるいはどれだけ有用性や将来性があるかの視点からの評価段階に入る。

ブロックチェーン技術も最初は Bitcoin の斬新性から出発したが、2015 年登場のスマートコンタクト実装 Ethereum などを契機に適応分野が格段に広がり、様相は一変した。その変化の中で、ブロックチェーンは IoT に相性が良いとの認識も登場した。その結果、【ブロックチェーン for IoT】×ビジネスが現在注目されている。本稿はこのような問題認識で考察する。

その状況を端的に示すため、ブロックチェーン導入の IoT 先行アプリケーション（表１）で、「ブロックチェーンは何故使われたのか？」の使用目的探索から開始する。

表１．ブロックチェーン導入 IoT 先行アプリ一覧

アプリケーション	使用目的	キーワード
ADEPT(2015)	スマート契約とネットワーク合意の活用	分散化,自律化
スマートシティ(2016)	信頼性向上とフォールトトレランス向上	信頼性
ファームウェア更新(2016)	ファームウェア検証時のデータの完全性、データ認証、否認防止の確実な実施	分散化,信頼性,効率化
スマートホーム(2016)	分散信頼と、IoTデバイスとそのデータへのアクセス制御の共通プラットフォーム化	分散化＆アクセス制御
VANETS(2016)	分散型自己管理システムの構築	自律性
eBusiness(2016)	スマート契約に基づく透明な自己管理と自己調整システムの実現	分散化＆自律性
SCM(2016)	偽造できないことによるオブジェクト追跡や所有権記録の実施	トレーサビリティ（信頼性）
Slock.it(2015)	分散型管理とスマート契約実行能力の実現	自律性

ＡＤＥＰＴ：自律分散型ピアツーピア遠隔測定システム(by IBM)
ＶＡＮＥＴＳ(Vehicular ad-hoc network)：自己管理車両アドホックネットワーク

事例は ADEPT、Slock.it、スマートシティ、スマートホームなど先行例としては著名なものである[1]。当然、予想されるように Bitcoin ブロックチェーンの特性である分散化、信頼性などが主流を占める。その中から、先行 IoT アプリケーションで期待されていたと推定されるブロックチェーンの特性を図１にまとめる。

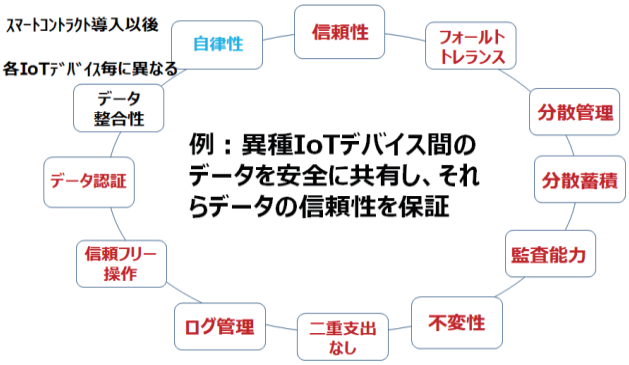

図１．先行 IoT アプリで期待されていた特性

Bitcoin ブロックチェーンは、独特のコンセンサスルール使用によって中央当局または第三者による調停無しに不特定者間の送金などを実現可能にしていた。そこで開発された仕組みで登場した特性はほぼ IoT に継承されるが、Ethereum で初登場したスマートコントラクトによる自律性、各種 IoT デバイスのデータ整合性などは追加される。【ブロックチェーン for IoT】は、これら特性を総合的に活用して、異種 IoT デバイス間のデータを安全に共有し、それらデータの信頼性を保証することで、多様な IoT 分野へのブロックチェーン技術の適用が目指されていた。

しかし、Bitcoin のような暗号通貨分野と IoT 適応分野の環境は著しく異なる。IoT デバイスの置かれた環境は保護されていないことが多く、IoT セキュリティ達成は重要な課題となる。また、リアルタイム性能が重要なケースが殆どで、IoT セキュリティ要件と IoT パフォーマンス要件のトレードオフやバランスが重要になる。また、Bitcoin と異なり、Private 型（許可型）ブロックチェーンとの親和性が高く、IoT で適応が進んでいるクラウド適応との優劣・利害得失評価も重要になる。クラウド型は集中型による信頼性・障害対応・高コストへの懸念があるが、ブロックチェーン技術はこれらに対応する能力が有ると同時に、関連技術が日々進化

している。以下、このような状況の下、個別課題にどのように取組んで行くかに有用な指針抽出を試みる。

2．IoT へ導入の要件

IoT システムの適応範囲は広い。システムは Internet を中核に、車などを含むゲートウェイ付き分散ネットワーク、スマホなどと接続するゲートウェイ付き無線センサーネットワーク、情報家電機器、市販 IoT 機器などを含む。そして、これら多様なネットワークを介して相互接続する異種デバイス混在環境でのセキュリティ順守などが要件になる。このような IoT システムの特異性は下記などである。

【IoT の特異性】

・IoT デバイスのリソース制約が非常に厳しい（例：データストレージ容量、処理能力、限られた電力など）
・バラバラなサイズ、能力、役割の異種デバイスが混在する。
・その一方、IoT システム全体としてのセキュリティ要件充足は必須な状況にある。
・大半の適用領域ではリアルタイム性も必須である。
・しかも、将来的にはとんでもない規模のスケーラビリティが求められる。

また、既存 IoT 市場はまだまだ発展途上にあり、その理由は下記などである[2][3][4]。

【IoT 市場は発展途上】

・各 IoT システムは専門性が高い。
・IoT プラットフォームにおける一方のサイドがデバイスなので、ネットワーク効果によるプラットフォーム拡大や寡占化が起き難い。
・その結果プラットフォームが乱立し市場の断片化が発生し易い。
・ビジネスモデル構造が個別化するので、工夫を凝らした IoT プラットフォーム活性化が必要になる。
・唯一の IoT プラットフォームで活性化が不充分な場合、他プラットフォームとの連携が模索される。
・但し、連携コストは高い。
・その結果、スケール化が限定される。

従って、【ブロックチェーン for IoT】においては適切なスケール化とコスト削減効果も強く期待される。このような幅広いニーズに答えるための IoT 参照モデルは各種提案されている[5][6][7][8][9]。それらのモデル概要一覧を図２に示す[1]。

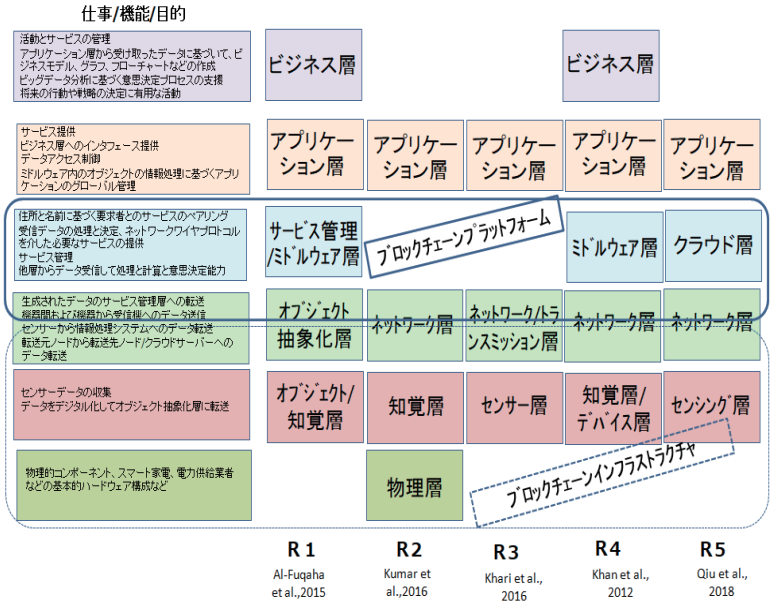

図２．IoT へブロックチェーン導入時の層構造

ブロックチェーンプラットフォームの代表例は Bitcoin, Ethereum,Hyperledger-Fabric の３種である。IoT 向けには Private 型（許可型）の Ethereum, Hyperledger-Fabric などが代表例と言える。

一方、ブロックチェーンインフラストラクチャの状況は通常の IT 環境や金融系ブロックチェーンアプリケーション環境とは大きく異なる。その状況を図３に示す。

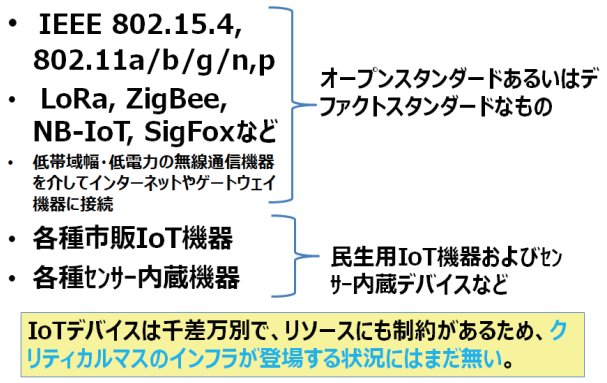

図３．ブロックチェーンインフラストラクチャの状況

即ち、IoT デバイスは千差万別で、リソースにも制約があるため、クリティカルマスのインフラストラクチャ登場にはほど遠い。一方、既存 IT 環境やブロックチェーン金融分野では、特にスマホが共通機器として浮上した結果、それがクリティカルマスに規模拡大し、インフラとして機能する強力な計算とネットワーキングデバイスを形成した。この相違は極めて大きい。この相違に基づく指針が明確に意識され正確に整理されなければならないと考える。

３．適応に向く領域

IoT 適応環境は厳しい。異種デバイスの混在に対応しながら、リソース制約のあるデバイスも含めた全体として高度な IoT セキュリティを実現し、スケーラブルでリアルタイム性能が良く、そして、安くて安全なシステム構築が目標になる。

ビジネス環境は絶えず変化し、これらを支える標準の策定も課題が継続的に存在して、全体としては完備しないことを前提にする必要がある。このような変化する環境の中でも市場ニーズに対応する時々のソリューションを継続的に提供して行くことが求められる。

その中で、ブロックチェーン視点での IoT セキュリティ項目は明示されているが、充足は不充分で今後の対応を待つ。また、ブロックチェーン視点での IoT パフォーマンス項目も不充分で、最もトランザクションスループットが高い Hyperledger-Fabric の場合でも高々 3500TPS 程度である。

それでも、今後に向けて、IoT へブロックチェーン導入の研究は盛んである。そこで、IoT 先行アプリケーションで「ブロックチェーンは何故使われたのか？」（表１）だけで無く、次の３つの質問を探索する。

1) どのブロックチェーンプラットフォームが使われているか？
2) 従来のどのような問題が解決されたか？
3) ブロックチェーンのどのような問題が解決されたか？

それぞれの調査結果を以下に示す[1]。

1) 全８アプリケーション（表１）中、Ethereum 採用が３個と相対的には多いものの、別の３種は独自方式を構築しており、現プラットフォームでの不充分性を示唆する。
2) 解決された課題は使用目的とほぼ対を成しており、信頼性、分散化などの評価が高い。
3) ブロックチェーン問題への対応ではスケーラビリティ、待ち時間、エネルギー消費、アクセス制御、プライバシーなどの評価が高かった。

これらは次の点を示唆する。

・セキュリティ要件とパフォマンス要件両立の領域にブロックチェーンでカバーすべき領域が存在すると思われるが、既存解はまだ発展途上で要件に合わせて個別対応しているケースが多い状況にある。
・分散化はスケール化とコスト効率化をもたらす可能性があり、スケール化×コスト化の評価がブロックチェーンに相応しい領域の特定に有用な可能性がある。これらを踏まえ、セキュリティ要件×パフォーマンス要件の適応図式を図４、スケール要件×コスト要件の適応図式を図５．に示す。

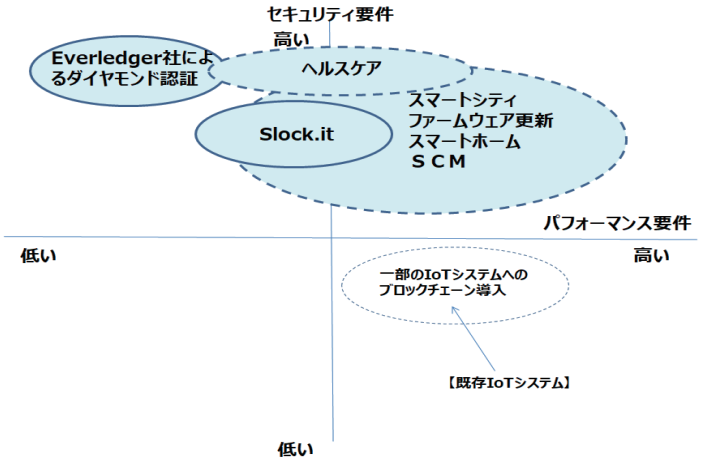

図４．セキュリティ要件×パフォーマンス要件適応図

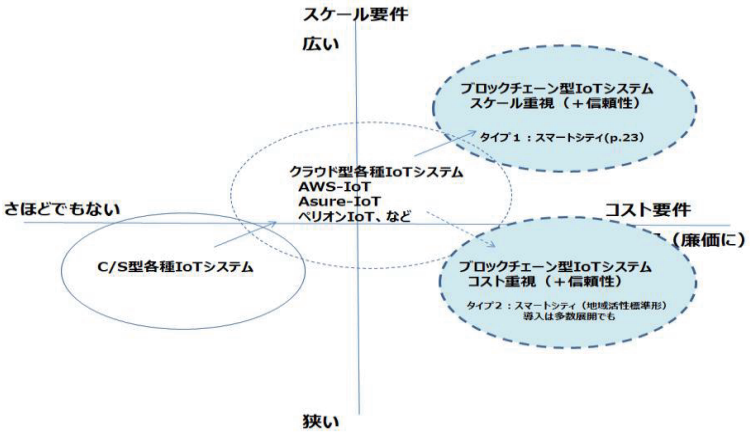

図５．スケール要件×コスト要件適応図

図４．においては、セキュリティ要件に重点的に特化した Everledger 社のダイヤモンド認証のような事例が実用化が早かった。やや類似の領域にヘルスケアがあるかもしれない。標準的にはセキュリティ要件・パフォーマンス要件を両立させる領域が最大のターゲット領域と思われるが、本格的適応事例拡大にはまだ新たな技術の開発が必要と推定される。

図５．においてはスケール拡大・低コストの両立だけでなく、上手い適応対象の絞り込みによって、低コスト・適正スケールの試みの有効性も示唆される。

４．今後の方向性

ブロックチェーンの IoT 分野への本格導入にはまだ幾つか大きな課題がありそうである。例えば、IoT 環境にフィットするコンセンサスルールはまだ無いと言える。そして、暗号通貨向け要件とは明確に異なる要

件が存在する。代表的なセキュリティ要件、パフォーマンス要件は下記などが期待される。

セキュリティ系の要件例： IoT 重視のトランザクション検証ルール、シビル攻撃の回復力、即時性の高いコンセンサスルール、フォークの回避、最大障害ノード数の許容、デバイスの整合性チェック、DoS 攻撃の回避、など

パフォーマンス系の要件例： 低遅延時間、低計算コスト、低エネルギーコスト、通信の複雑さが少ない、など

また、IoT 系のトランザクションは独特で、従来型トランザクションと明確に区別する必要がある場合がある。仮想的にスマートホームの場合で例示する。仮に部屋に暖炉があったとすると、カメラまたは任意のセンサーも、その部屋に人間の存在を検知した場合に限り暖炉に点火すべきである。このようにセンサーの読み取り値が環境に依存して検証され、単独では検証されないことを想定しなければならない場合が有り得る（これに類する多様な場面を想定しなければならないとすれば厄介である）。

最後に今後についてまとめる。今後に向けた基本認識として、“IoT が自律的デジタル化経済の未来”と想定されており、世界的合意が共有されている。但し、このような段階に本格的に到達するまでには、設計段階と開発段階双方で概念的変革が必要なように思われ、また、自律的デジタル世界の将来の要件を満たすブロックチェーンベースの IoT システム設計と開発が不可欠のように思われる。

そのような将来の IoT システムは既存の IoT テクノロジーとは結構違って来るであろう。そして、徐々に変化していくと思われるので、互換性も考慮されるべきである。このような変化の中で、ブロックチェーンと IoT デバイスとの統合も重要な課題になると思われる。感知装置のような市販 IoT 機器は費用対効果のため安全な実行環境を持っていないし、将来もこのような機器は次々に登場し、これらもシステムの中に取り込んで行かなければならないだろう。

このような環境を想定すると、当面はフォグコンピューティングのコンポーネント活用が現実的中間解を提供して行くように思われる。その場合には、それぞれの場面で異種 IoT デバイスからのデータをブロックチェーンに送信できる方法の設計・開発も必要になると思われる。

このような状況変化も含めて、デジタル化は新たな姿を提示していくのではないだろうか。なかなか共通のビジョンは描けず、従来の IT 環境での Apple iPhone 寡占モデルのような世界は想定しずらいが、将来の世界は現在のシステムとは異なるレベルの新たな形態のエコシステム登場の世界と思われる。そうであるなら、そのエコシステムの未来を描くことはある程度できると思われる。例えば、パートナー間の新たな摺り合わせや、各種インターフェースの UX/実現手段などにも新たなチャンスが到来してくるかもしれない。そして、このような世界でチャンスを獲得するには、実践的に新たな姿の探求に取組み、ビジネスとの融合に一層熱心に取り組むことが必要になる。このような試みの先に新たなデジタル世界を想定すべきと思われる。

〔参考文献〕

[1]Imran Makhdoom, et al., “Blockchain’s adoption in IoT: The challenges, and a way forward”, Journal of Network and Computer Applications , Vol.125, pp.251-279, 2019.

[2]Tiago M. Fernández-Caramés, Paula Fraga-Lamas, “ A Review on the Use of Blockchain for the Internet of Things”, IEEE Access, May, 2018.

[3] 高橋 浩, “IoT プラットフォーム市場の高付加価値化 －IoT システムはなぜスケール化が難しいのか－”, 横幹, Vol.13, No.1, 2019.

[4] J Mineraud, O Mazhelis, X Su, S Tarkoma, “A gap analysis of Internet-of-Things platforms”, Computer Communications, Vol.89, pp.5-16, 2016.

[5] Al-Fuqaha et al., “Internet of things: a survey on enabling technologies, protocols, and applications”, IEEE Commun. Surv. Tutor., Vol. 17, No.4, 2015.

[6] Kumar et al., “Security in internet of things: challenges, solutions and future directions”, IEEE 49th HICSS, 2016.

[7] Khari et al., “Internet of Things: proposed security aspects for digitizing the world”, 3rd INDIA Com, 2016.

[8] Khan et al., “Future Internet: the internet of things architecture, possible applications and key challenges”, IEEE 10th FIT, 2012.

[9] Qiu et al., “How can heterogeneous Internet of things build our future: a survey”, IEEE Commun. Surv. Tutorials, Vol.20, No.3, 2018.