Vol.2018-DPS-176 No.17
Vol.2018-EIP-81 No.17
2018/9/14

# なぜブロックチェーン？

岸上順一[1,a)]

**概要**：これまで新しい技術が出るたびに繰り返される，法と技術の対立軸はブロックチェーンにおいてもおなじように繰り返されようとしている．一方でデジタルトランスフォーメーションということばが流行りつつある中，我々はバランスをとるというもっとも苦手なことを実現しなければならない．プライバシー，コンプライアンスというのは人によってとらえ方の違うものであるだけでなく，国によっても違い，さらにビジネス戦略から見るともっと重要な意味を持つ．それではブロックチェーンを用いたビジネスやサービスのバランスとはどういうことだろうか，いくつかの例を挙げながら考えてみたい

**キーワード**：Layer 2, ブロックチェーン, 法規制, RFID, コンプライアンス OECD

# Why do you want the Blockchain?

Jay Kishigami[1,a)]

***Abstract:*** The emerging technology, icluding the Blockchain, has been recognized the severe confrontational structure between a technology and a regulation. Many brand new technologies have been imported from mainly USA regardless a tough contradiction, if that gives a notable merit to users. On the other hand, we are intend to reluctant to install such a technology in front of the controversial argument. At this opportunity, shall we discuss on this issue for the Blockchain technology vrom a various aspect?

***Keywords:*** Blockchain, Layer 2, regulation, RFID, compliance, OECD

## 1. はじめに

ビットコインのバブル的な変動や ICO は世の中の注目を引くには充分であるが，その技術を担うブロックチェーンの動きにも興味深いものがある．残念ながらバズワードになった多くの言葉がそうであるように，ブロックチェーンも有名になりすぎたために極端な論調が散見され，多くの誤解を呼んでいる．古くは 2014 年に CEO が顧客のビットコインを着服し 115 億円もの損失を出した Mt.Gox 事件，今年の 1 月に秘密鍵を盗まれたためやはり 500 億円相当分がなくなった NEM 事件，これらは取引所の脆弱性が狙われたもの，さらに最近起こった日本初のコインであるモナコインへの攻撃で 1000 万円程度の損失がでたことなどネガティブなニュースが駆け巡る中，確実に新しい技術として金融，流通，教育など様々な取り組みが行われている．ここで今一度冷静に振り返ってみよう．

[1] 室蘭工業大学
Mizumotocho, Muroranshi, 0508585, Japan
[a)] jay@csse.muroran-it.ac.jp

## 2. ブロックチェーンをめぐる期待と技術的な問題点

### 2.1 3 つの自律的な技術がもたらす新しい産業

そもそもブロックチェーンとは何か．この説明の困難さが多くの誤解を生んでいる分散台帳という言葉が一番近い用語であろう．参加者全員が同じ台帳を持って，だれかが何か新しいことを台帳に書くと，それが正しいものかどうかを特殊な方法 (マイニング) で確認して，それをみんなで確認しあう (合意形成) という仕組みである．

サトシ・ナカモトが考えだしたこのアルゴリズムはそれまでにあった様々な仮想通貨の問題点を解決する画期的なものであった．その後いろんな問題を起こしながらも 8 年にわたって使われ，その価値が非常に大きくなっているこ

とからもその優秀さが分かる．この信頼性は理論的なものであるためトラストレスという言葉がよく使われる．つまり信用を裏付ける第三者の存在を必要としないのである．お札は日本銀行券ともいわれるように，日銀がその信頼性を裏書きしている．ビットコインにはそれがない．つまりその仕組み自体が信頼なのである．

ブロックチェーンはいったん中に書かれた (台帳に書かれた) ものを改ざんすることが原理的にできない．全世界のすべての参加者が持っている内容を書き換えることができればそれは可能であるが (実際には全コンピュータパワーの 51%を支配できれば可能)．

このような真正性があり，トラストレスなアルゴリズムを提供するブロックチェーンはある意味では GAFA(Google, Apple, Facebook and Amazon) に対するユーザー間での取引が重要になるという概念で考えるとわかりやすいかもしれない．これが大革命を起こすかもしれないと言われているコアである．

次に AI(人工知能) があげられる．70 年ほど前に名前を付けられて，何回かの失敗ののち 2012 年くらいからトロント大学，Google を中心に急速に進展してきている．基本的には膨大なコンピュータパワーを持ちいて，学習をコンピュータにさせ，人間の判断と同様あるいは条件を限ればそのはるか上の能力を引き出すことができてきている．最初はゲームの世界で人間よりも強くなったことがセンセーショナルに取り上げられていたが，次第にマーケティングや自動運転などに欠かせない技術として市民権を得つつある．

そして IoT である．ここでは詳細は述べないが，センサーをネットワークで接続し様々な情報を採りながら適切に対応していくという概念は自動車においてもっとも進んでいるように見える．

### 2.2 現在のブロックチェーンの問題点

(1) マイナーの偏りによる脅威

ビットコインの整合性を保証する極めて優れた手法がマイニングである．現在その 80%以上が中国にあり，上位 4 社で全マイニングパワーの半分以上を占める状態 [*1] になっている (図 1)．これはよく知られたビットコインの脆弱性である 51%問題に直接影響しており，全体の信頼性を損なう可能性を含んでいる．最近中国政府がマイニングの禁止を通達したというニュースもあり，その影響が懸念される．

(2) 増え続けるデータ量

ビットコインがはじめて使われたのは，2010 年にピザを 1 万 BTC で購入したのが始まりだと言われている．それ以降ブロックは 7 年弱の間に 150GB[*2] 以上

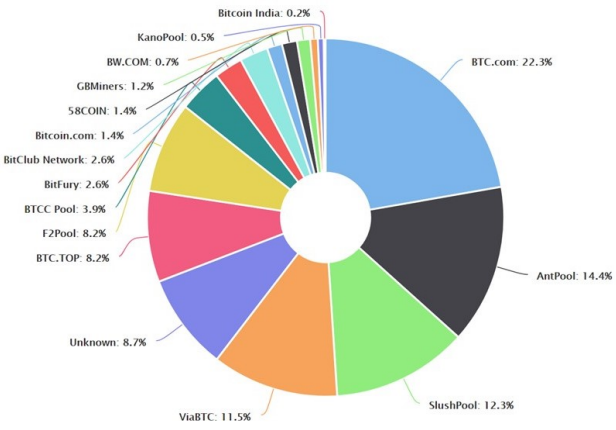


図 1 Mining Pool の実態

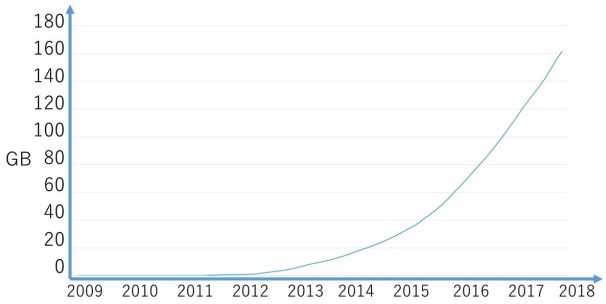


図 2 Blockchian のサイズの増加

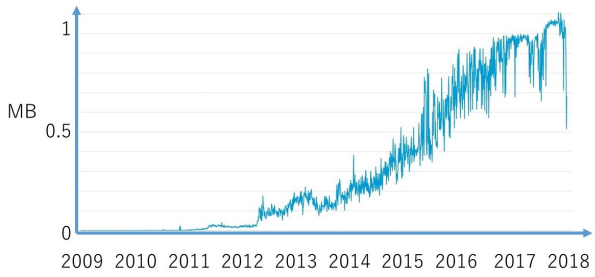


図 3 Block のサイズの増加

に増加している (図 2)．全世界で稼働しているすべての台帳を保管しているフルノード数は 1 万弱であり，Segwit の関係で増加気味ではある，しかし Ethereum はそれ以上の勢いで伸びている．[*3]

因みに一つのブロックのサイズは Bitcoin の場合 1MB と決められているがその上限に張り付いている．昨年実施された segwit 以降少し減少の傾向も見受けられる．(図 3)

(3) トランザクションの速度

ビットコインのトランザクションは 1 秒間に 7 程度が限度と言われており，PoW(合意形成) を待つ時間が約

[*1] https://www.buybitcoinworldwide.com/mining/pools/
[*2] https://blockchain.info/charts/blocks-size?timespan=all
[*3] https://blockchain.info/ja/charts/avg-block-size?timespan=all

10 分，系全体が安定するまでには日のオーダーになることも珍しくなくなってきている．

(4) ビットコイン以外のサービスが出ないこと
ビットコインはまさに暗号通貨としての最適化を行った結果，上記のような問題点を内包しながらも順調に拡大しているといえる．ブロックチェーンの技術は数年前から大きな期待感を持って迎えられているが，ビットコイン以外のサービスはなかなか始まらない．

このように現在のブロックチェーンは多くの問題点を含みながらビットコイン一人勝ちの様相で進んでいる．しかしブロックチェーンの技術は分散データベース的で，実は同じものをみんなが持つという一見矛盾したアーキテクチャ故の魅力があり，その可能性を技術的に健康な状態で育成すべく，BSafe.network[*4] あるいは ScalingBitCoin[*5] というグローバルな動きが起こってきている．これに対し，我々は 2017 年 7 月に Base アライアンス [*6] という日本初のアカデミアをベースとするブロックチェーンのアライアンスを立ち上げ，技術的な観点からその健全な発展に貢献するべく活動を始めた．

### 2.3 オフチェーンの意味

ビットコイン技術は暗号通貨の流通に特化したものであるため，ブロックの大きさが 1MB に制約されている．実際の取引の値が限りなくこの値に近づいたため Segwit が提案された．またトランザクションにはハッシュ値と BTC 値などの限られた 300Byte ほどのものがやり取りされるだけである．Ethereum はスマートコントラクトという自律的に実行できる仕組みを内包し，gas と呼ばれているコストを支払えば原理的にはいくらでも大きなファイルを扱うことができる．しかし現実的には，非常にコストがかかるためこのような使い方をするようなサービスは考えられない．

これらの状況からビットコインでは Lightning network, Plasma あるいは Ethereum における Raiden network と呼ばれている Layer 2 の概念が出てきた．ここでいう Layer 1 とはブロックチェーンそのものである．すなわちトランザクションのメインは従来のブロックチェーンで行うものの，日々のトランザクションはオフチェーンと呼ばれる，独立した，しかしメインのトランザクションと連携した方法で行う．別名として state channel とも呼ばれるこの方法はまさに State(状態) をマルチシグネチャーを用いてオフラインにロックし，メインとは別に行った結果を再度メインのブロックチェーン に戻す方式である．この方式はまだまだ開発途上であるためいくつかの問題点を持っている．その一つが参加者の一人はオンラインを保たなければならないことである．

Layer 2 の技術は単にトランザクションのスピードを上げたり，少額の決済が可能になるだけでなく，多くの可能性を秘めていると考えている．我々は複数のブロックチェーン間を接続するアーキテクチャに応用することを考えている．

その後ビットコイン関連では Lightning Network[*7] の発表が 2016 年に行われた．これは HTLC(Hashed Time-Lock Contract) と呼ばれる取引により，途中に知らない第三者が介在するような取引でも最終のステークホルダーが生成したランダム数をベースにしたハッシュ値を期限付で取引 (トランザクション) に載せることにより，信用を担保できる．実はビットコインのブロック容量問題で昨年脚光を浴びた Segwit は，もう一つの機能が重要である．即ち容量を増やすためにデータとハッシュ値を分離して格納することが出来ることだ．このため Transaction Malleability(トランザクション展性) の問題を解決できる．即ち電子署名の改ざんリスクを低減できるのである．そういう意味でこの 2 つの相性は良い．図 4 に概念イメージを示す．通常は第三者間で有効期限と最終ユーザーから示されたハッシュ値をやりとりしていくのだが，途中で図のように Bob と Carol の間で取引が成立しないときは親のブロックチェーンに戻るということになる．

### 2.4 IPFS との連携

現在のブロックチェーンにおける Layer 2 の技術はビットコインに引っ張られる形で暗号通貨のトランザクションを高速にする方向に注目が集まっている．FinTech の場においては重要なことであろう．しかし，IoT(WoT) などの通貨以外の場面，あるいは通貨以外とビットコインなどの暗号通貨を接続することを考えるとき，これまでの提案では不十分だ．Ethereum におけるスマートコントラクトのデータ (プログラム) を用いて様々な情報を流通させる際の Layer 2 を考えるといくつかの要求条件が考えられる．

(1) 大容量コンテンツの持ち方
(2) 権利の流通など流通途中でコンテンツ (データ) が変化する場合の取り扱い
(3) トランザクション速度
(4) マイナーのインセンティブ

IPFS(InterPlanetary File System) はこれらの要求を実現する重要な技術だ．これはファイルシステムを現在の HTTP プロトコールの代わりに Qm で始まるデータのハッシュ値で表現するものであり，データの変遷 (バージョン管理) なども内包されている．データ自体は自分自身から計算されるハッシュ値をアドレスとし，完全に分散されて

[*4] http://bsafe.network/
[*5] https://scalingbitcoin.org/
[*6] http://base-alliance.org/ja/
[*7] https://lightning.network/lightning-network-paper.pdf

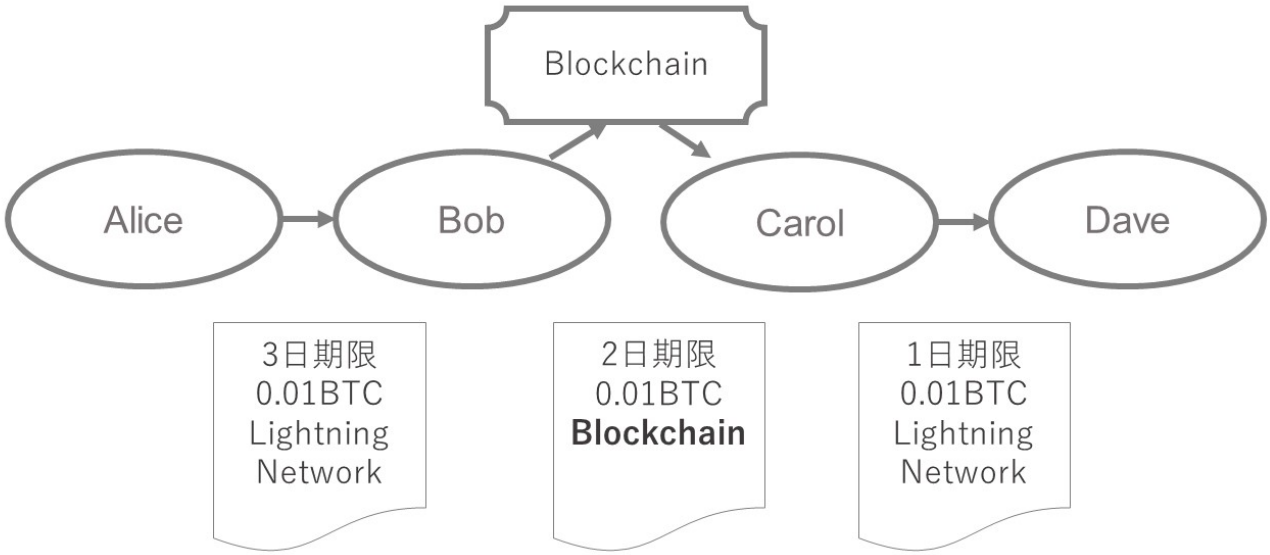


図 4　Lightning Network 概念図

蓄積することが可能だ．これはブロックチェーンの分散システム，特にこれまで述べた Layer 2 のアーキテクチャと親和性があることが分かる．

### 2.5　ブロックチェーン Bridge

今後様々なブロックチェーンネットワークが出てくることが予想される．そこで異なるブロックチェーンを接続するために，Layer 2 におけるネットワークを通じてデータの一貫性を保証し，またできるだけ軽いトランザクションを実現するために IPFS の仕組みを内包したアーキテクチャが重要であろう．これが現在の HTTP と親和性があるかどうかは分からないが，少なくとも広い意味でのコンテンツのメタデータに当たるハッシュ値の流通はブロックチェーンで保証し，コンテンツ自体はそれとハッシュ値で紐ついた形で保持されるアーキテクチャが考えられる

## 3.　新しい技術の日本における展開

### 3.1　RFID

2000 年代に入り RFID の活用が盛んになってきたころ，その推進を総務省の委員会で行っていた．そこでは日本としてどのような制度が健全なビジネス展開に必要かというもので結局 1980 年に制定された OECD(経済協力開発機構) の 8 原則 [*8] が基本となって珍しく総務省，経産省の合同でガイドラインを発表した．(電子タグに関するプライバシー保護ガイドライン) [*9]．実際の運用には様々な例外規定も設けられているが，概して使いにくいシステムになっているのも否めない．因みに OECD の 8 原則とは下記のとおりである．

(1) 収集制限の原則
(2) データ内容の原則
(3) 目的明確化の原則
(4) 利用制限の原則
(5) 安全保護の原則
(6) 公開の原則
(7) 個人参加の原則
(8) 責任の原則

### 3.2　ストリートビュー

Google が 2005 年に始めた Google Maps さらにその 2 年後に開始したストリートビューは当初，プライバシーが脅かされるなどの議論があり，極めて批判的な世論であった．同じようなサービスは他の機関からも提案されていたが，ことごとくこれらの世論を前に断念せざるを得なかった．しかし，今日 NHK をはじめ多くのマスコミは Google Earth などのサービスからの映像を高い頻度で用いており，個人レベルでもスマホの利用アプリの中で常にトップ 5 に入るくらいの人気である．企業や大学は一般道路だけでなくキャンパス内や建物の中までも積極的に公開するようになってきた．プライバシーをめぐる議論はどこにいったのだろうか．

[*8] http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/oecd8198009.html
[*9] http://www.meti.go.jp/policy/it_policy/tag/privacy-gaid.pdf

### 3.3 ビジネスセキュリティ

2020 を前にセキュリティをめぐる議論が活発化しており，政府も多くのリソースをそれに割いている．勿論歓迎すべきことではあるが，企業におけるコンプライアンスとともに IT 立国をめざす日本のそれをけん引する企業の多くが，世界と競争のできる状況でない問題が出てきている．細かいことをみれば，なぜか多くの企業でファイルの転送に暗号化された添付ファイルを用い，そのパスワードを平文で続いて送られるメールで示すという状況，暗号を定期的に変えましょうという呼びかけの前にかえって暗号を破りやすくしている状況，さらにブラック化を恐れ硬直した勤怠管理を行い生産性を損なっている状況などなど，いったい何から何を守ろうとしているのかが分からない．

### 3.4 AI がもたらす顔認証，AI スピーカー

2017 年から Amazon の Alexa の技術をはじめ，Google などいくつかの企業がいわゆる AI スピーカーのサービスを始めた．簡単で自然なことばで AI スピーカーが反応し，音声認識の上，AI を用いたシステムがパーソナライズした対応をするので一旦使い始めたらやめられない魅力を持っている．しかし当初個人のプライバシー情報を集め，それを他の用途に使うという話が絶えなかった．サービサーが個人の行動様式を自動的に集められるという点では今でも問題点は山積している．

### 3.5 監視カメラ

毎日のように繰り返される多くの犯罪を未然に防いだり，犯人を見つけるのに今や監視カメラは欠かせない存在になった．監視カメラがコンビニに設置された 1999 年頃は，個人の行動を自動的に監視される「気持ち悪さ」からプライバシーの問題がずいぶん取り上げられた．その後デジタル化され，ネットワーク化されることにより同時に多くの情報を収集することが可能となってきた．警察の車両の監視をする N システムも同様である．しかし，今監視カメラの活躍は，これなしでは，犯罪天国になるのではないかと思われるくらい浸透している．ここに監視カメラがありますという提示だけは守られているが，もはやそれを気にする人も少ない．

いくつかの技術とそれを用いたサービスの社会的受容性の変化を見てきた．一言で言うと当初新しい技術は，何らかの気持ち悪さとともに，まずプライバシーの問題が取り上げられる．しかし，しばらくたつとそれが社会にとって必要べからざる存在になり，空気のようにそのネガティブな面が忘れられ，効用がしばしば取り上げられる．これはこれまでの長い歴史を見ても，同じことが繰り返されているだろう．ここで大きな問題は，新しい技術が出てきたとき，日本では過度に規制の方向に走り，アメリカなどで技術が高められ，それを用いたサービスが輸入されるという構図である．当初は決して日本が遅れていたわけではないのに，日本での研究開発が過度な規制などでやりにくくなり，研究資金が集められず，海外から逆輸入されるという例は多い．

## 4. ブロックチェーン，Ai，IoT の自律的発展

### 4.1 現在の状況

2017 年度くらいから総務省，経産省をはじめブロックチェーンに対する大きな，時には過渡な期待が高まってきている．2009 年くらいから徐々に広がったこの技術は，当初説明の困難さからなかなか携わる研究者，開発者あるいはビジネス関係者が居なかった．さらに Mt. Gox 事件や CoinCheck 事件などがビットコインに対してネガティブな印象，ダークなイメージを植え付け一部の研究者を除き，関心を持たれることは少なかった．しかし 2012 年には 1,000 円程度だった BTC(ビットコイン) が 2017 年には一時 200 万円を超える値が付き一気に世間の注目を浴びだした．同時にその基本的な技術であるブロックチェーンの先進性が再び着目され，2018 年現在はすでにバズワード化してきている．

毎年ガートナー社から発表される Hype Cycle の技術予想図は，それぞれの技術がどの程度期待され，それが今後どうなっていくかを占ういい指標になっている．2017 年度の図 5 ではブロックチェーンは図に示すように，最高の期待度から少し，過ぎたところに位置している．勿論これはアメリカ中心に見た例であるが，多くの関係者の理解と一致する．多くの問題になっていることがブロックチェーンを導入することによって一気に解決するような雰囲気が今の日本にはあるが，さすがにそれはと思う．

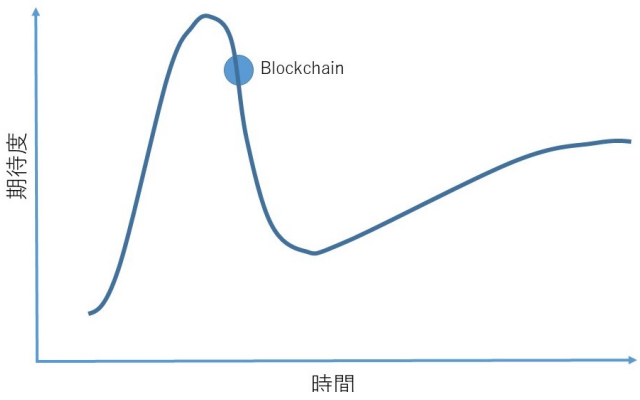


図 5 2017 年ガートナー社による Hype Cycle 上の Blockchain の位置

### 4.2 想定される問題

(1) もし多くの関係者の期待通り，多くのブロックチェーンを用いたサービスが開始された時，これら複数のシステム間の連携をどのように実現するのであろうか
(2) ISOC や W3C などでブロックチェーンの標準化の話は出ているが，まだ不完全な状態である技術に標準化は足を引っ張るだけにならないだろうか
(3) ブロックチェーンの特徴の一つは過去のチェーンをトラッキングできることである．過去にさかのぼって履歴がすべて残ることは「忘れ去られる自由」() と矛盾することにならないだろうか
(4) ビットコインが暗号通貨としてますます力をつけてきたとき，FIAT との関係はどうなるのだろうか
(5) コミュニティをベースに発展しているシステムを社会的に受け入れられるだろうか

これらはいずれもインターネットの黎明期に起こった問題と似ている．インターネットはそれを IETF や ISOC そして W3C というような団体，コミュニティがうまく解決してきている．残念ながらブロックチェーンにはそれらにあたるものがまだない．

さらにブロックチェーンを社会的に考えると非中央集権とトラストレスという 2 つの概念が重要である．前者は P2P の仕組みの中で，日本銀行と貨幣のような関係がないということである．即ち権威にあたるものが存在せず，あえて言えばブロックチェーンの仕組み自体がそれにあたる．そのため何か強い力で全体を引っ張るということが起こりにくく，究極の民主主義であろう．しかし同時に何か問題があった時にそれを解決するのに多くのコストがかかるということも考えられる．また信頼という，やはり権威によるものが存在しないことも重要である．これも仕組み自体に内包されているという理解が妥当であろう．しかしこの特徴は日本人には少し受け入れにくいかもしれない．何か問題があると必ず自分以外の何かの責任に持っていきがちである．ブロックチェーンでは自己責任になる．

### 4.3 今後の方向性

これからの新しいサービスは単一の技術だけでなく，ブロックチェーンに AI や IoT の技術が自律的に作用して，全く新しい機能を提供してくれるだろう．センサーの情報をもとに AI が自律的に判断した結果をブロックチェーンで管理され，それをベースに IoT システムで新たな環境を作り出すこともあり得るだろう．そこには人が介在することはない．こういう複雑なシステムが自律的に動くということはあまり経験がない．個々の技術は研究者によって確実に伸びていくだろう．それらを組み合わせたサービスの及ぼす影響は今後非常に大きくなる．今後の Autonomous の時代をうまく舵とることが重要だ．

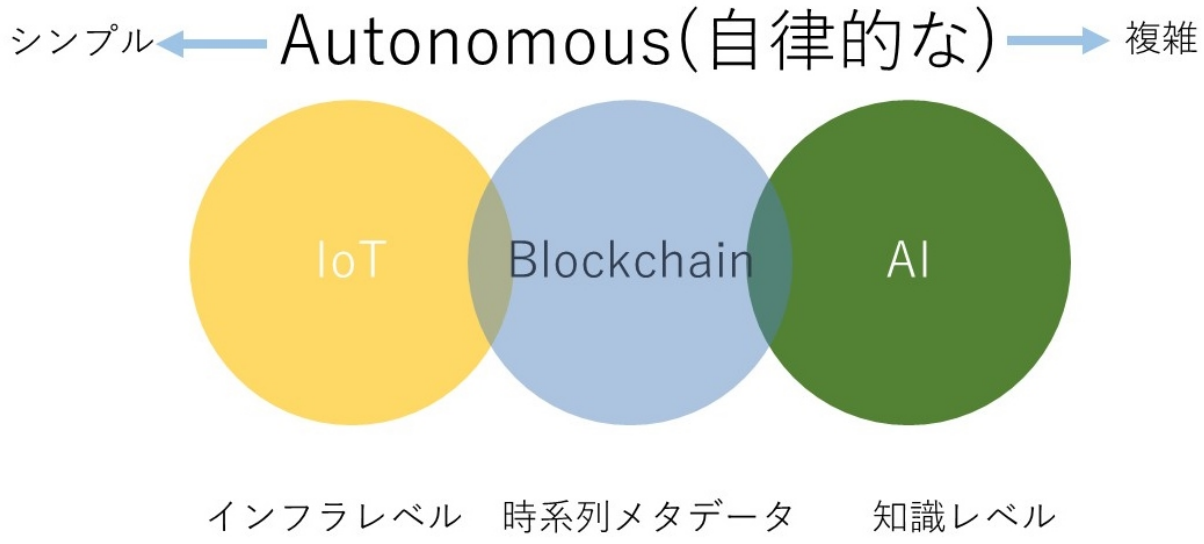


**図 6** Blockchain, AI, IoT による自律的サービス