ブロックチェーンの向かう先を冷静に見つめて

ブロックチェーン技術は暗号通貨からその他領域に適用できる技術として注目されており，以前話題であった技術的な課題は改善され続けています．特に，合意形成方式ではProof of Work以外の方式も実装され始めました．しかし，ビジネス面では商用サービスは少なく，このままブロックチェーンを利用すべきか判断が迫られています．ここでは，ブロックチェーンの現在を技術，ビジネスの両面から見るとともに，今後の展望について紹介します．

ブロックチェーン技術の現状

ブロックチェーン技術については，現在も新たな技術が世界中で登場し続けています．一方，既存のブロックチェーン実装についても性能問題の解決に向けた改良など改善活動が進んでいます．ここでは昨今検討が進んでいる改善活動について紹介します．

■合意形成方式

仮想通貨に利用されているProof of Workは計算リソースの大量消費という課題があったため，以前よりほかの合意形成方式が検討されてきました．最近は，これらの構想がいよいよ実装に移っています．そして，既存の枠組みに組み込まれ，利用され始めています．特にEthereum[(1)]は，数年前に提案されていたProof of Stakeの利用がみえてきました．

Proof of Stakeは，所有している通貨の保有量に比例して，新たにブロックを生成，承認する確率を決める形式です．通貨を大量に保有している参加者が勝つ確率が高くなるように設計されています．これは，Proof of Workのようなマイニングによるリソースの大量消費を抑えることや，悪意あるマイナーによる51%攻撃の可能性を下げることが期待されています（**図1**）．

一方，通貨を大量に所有している参加者が勝ち続ける可能性やチェーンのフォークが発生した後，それぞれのチェーンが伸び続ける可能性があります(Nothing at Stake問題)．それらの課題に対しては，通貨の保存期間（coin age）の設定や不正なチェーン操作に関するペナルティの導入といった対策も組み込まれています．coin ageは，所有して

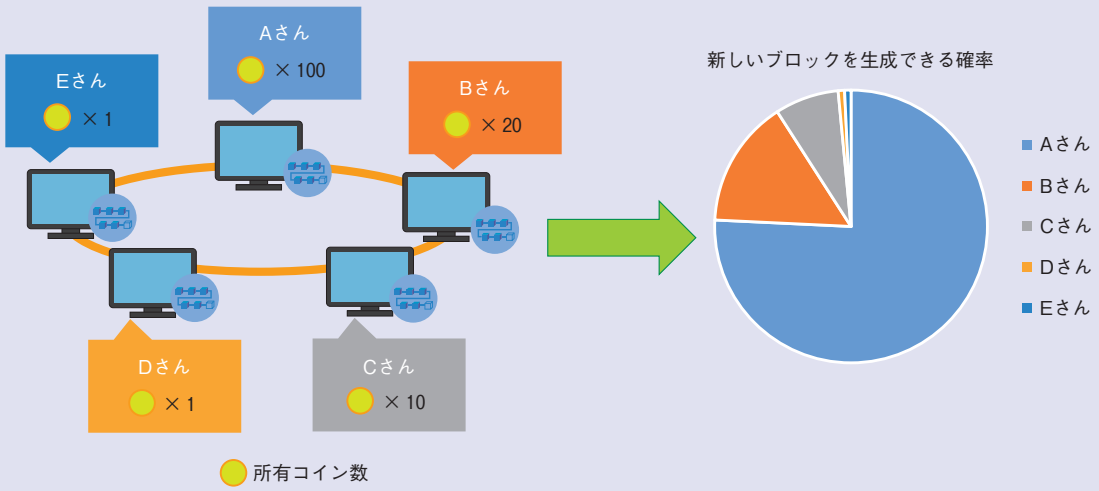


図1　Proof of Stakeの仕組み

いる通貨の所有期間を組み込み，勝者となった参加者の所有期間を調整して，連続して勝者となる確率を調整します．ペナルティの導入はEthereumのSlasher[2]のように，不正なチェーンを操作する場合に対処するよう実装が進んでいます．

Proof of Stake適用に向けての活動は継続しています．今後もこの活動について注目です．

■シャーディング

スループットの課題を解決するための開発も進んでいます．レイヤ2のような仕組みを導入してメインチェーンの外で処理する動きもあれば，シャーディングを実装するものもあります．

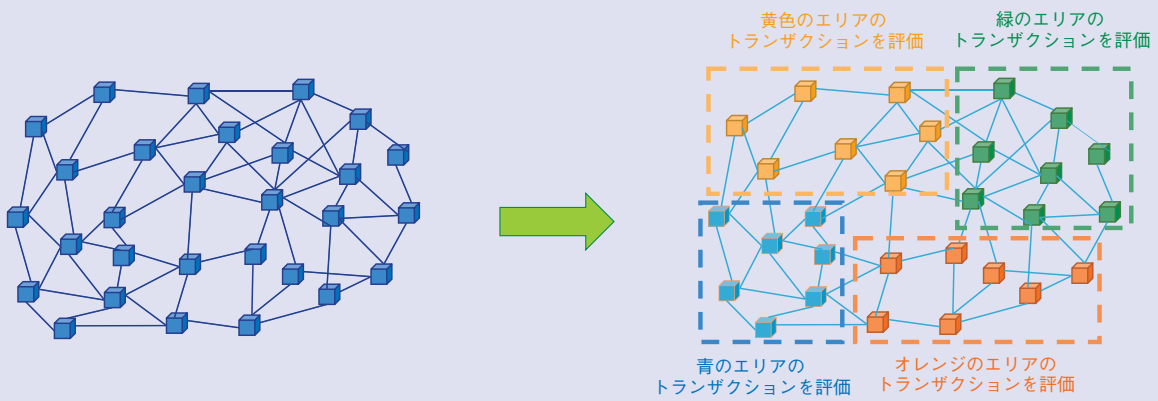
シャーディングはデータベースを利用する場合での負荷分散方法として利用されていましたが，ブロックチェーンにおいても実装されています．

参加者をいくつかのグループに分けて，ネットワーク全体で実施する処理もグループごとに分けることで，負荷分散しスループットの向上を図っています（**図2**）．

Ethereumや他のブロックチェーン技術でシャーディングの導入に向けて実装が進んでいます．特にサブネットワークのバランスを考慮するために，例えば1つのグループに1000程度の参加者になるようにネットワーク全体で調整され，グループは定期的に更新されるといったアイデアも検討されています．

さらに，ブロックチェーンネットワークを階層構造化し，スループットを高める動きもあります．EthereumのPlasma[3]のように開発が続けられています．

多くのブロックチェーン技術は，これまでに発生した課題を解決すべく，日々改善活動が続いています．今後高度な利用をするために，最新の技術動向は継続して注目しましょう．



ネットワーク上のすべてのトランザクションを評価するため時間を要する

(a)　シャーディングなし

シャーディングによって同時に評価できるトランザクション数が増加，スループット向上を図る

(b)　シャーディング適用

図2　シャーディングの仕組み

ブロックチェーンビジネスの現状

ビジネス面において，現在の動向はどうでしょうか．日本では，2019年5月に改正資金決済法が成立しました．仮想通貨という呼称が暗号資産に代わること，暗号資産の扱いに関する法律整備がポイントです．この法律は2020年4月から施行される予定です．今後は暗号資産が重視され，幅広く浸透していくでしょう．

また，2016年に経済産業省が発行したレポート[(4)]にて，ブロックチェーンが既存のビジネスに影響を与える金額は67兆円と述べられていました．この数字の影響は大きく，レポートに記載されていたテーマを中心に，多くのPoC（Proof of Concept）が実施されました．そのPoCの多くはすでにITシステムとして確立している既存の業務をブロックチェーンで実施した場合の評価というものでした．データベースで扱っていた処理をブロックチェーンに置き換えるというものはもっとも多いテーマだといえます．

これらのテーマについては，PoCの1つのフェーズを完了したものの，次に進むためのハードルは高いです．すでにITシステムとして成立しているテーマに対し，ブロックチェーンを導入する理由がないからです．

ブロックチェーンの特徴の1つとして分散台帳があります．分散台帳とはネットワークに参加する複数の利用者がそれぞれで台帳を所有し，台帳内のデータを合意によって同期する仕組みです．つまり，“複数の参加者の台帳のデータをそれぞれの合意によって同期させるような業務”に適用させることが大切といえます．

例えば，企業間で書類をやり取りしてきた業務は，適用を検討すべきテーマといえます．記載ミスなどのエラーについては，ITシステムによるチェックを組み込むことで，エラーを低減できます．一方，書類から変わることによる業務への影響も考慮が必要です．PoCではITシステム導入の効果だけでなく，企業間での業務の見直しも考慮に入れなければなりません．

分散台帳のメリットは，ネットワークへの他の参加者もそのデータに容易にアクセスできる点にあります．データ操作の流れが他の参加者が確認できることにより，第三者による監査，チェックが容易になるという点です．例えば，製品を原料から製造の過程を記録するとします（**図3**）．その情報を第三者が速やかにアクセスできることで，製品の信用を維持できるようになります．問題が発覚した後にデータを収集して対処するよりも，速やかに対処できるよ

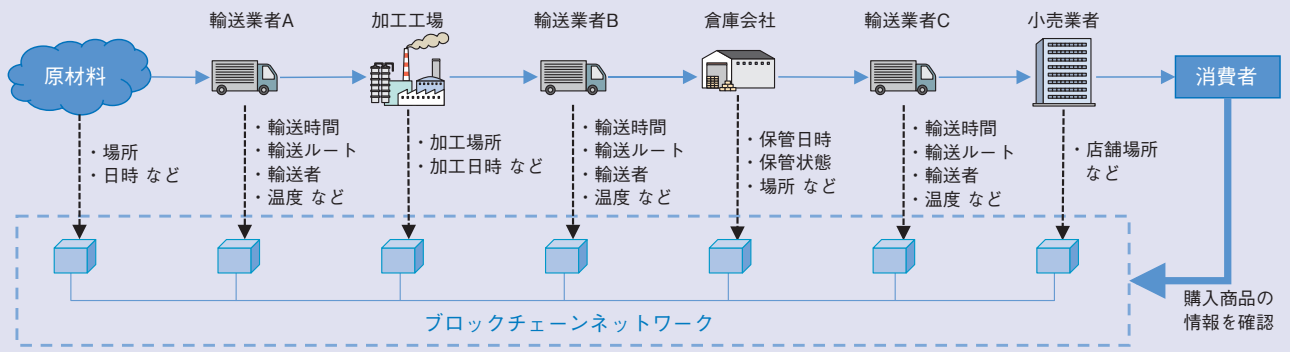


図3　商品のトレーサビリティ

うになります．そして，問題の発生を予防することも可能となるでしょう．

このような検討を進めるには，一社単独での検討は難しいです．工程にかかわる他の企業の参加，第三者としての役割を持つ企業の参加が大切です．テーマによっては競合となる企業の参加も促し検討を進める必要があるでしょう．そして，複数の参加者で台帳を共有することに加え，第三者もその台帳を共有することが大切です．第三者のアクセスの必要性を考慮して適用する業務を検討してみてください．

次のステップに進むためには，自社だけでなく関係する企業の巻き込みや同じような課題を持つ企業との連携など，より実践的な検討が求められることでしょう．

今後の発展に向けた課題

ブロックチェーンの実用化の検討が進むにつれ，そのネットワークを維持するための課題が顕在化します．ここではいくつか考えられる課題について述べます．

■実データの扱い

ブロックチェーンと実データをどのように紐づけるか課題となります．いくつかのブロックチェーン技術は，NoSQL技術と組み合わせてデータを管理するものもあります．他のアプローチとしてブロックチェーン技術とP2Pベースのファイルシステムを組み合わせる方式もあります．どちらの場合も実データを管理するための環境，データへのアクセス方法，故障によりデータが欠損する場合の影響など，本格的に利用する場合に想定される課題について考慮が必要です．

■データの投入方法

ブロックチェーン上に導入するデータが誰かによって意図的に改ざんされている場合，誤った情報を利用することになります．そのため，データの投入も意図的に改ざんされないようにしなければなりません．センサや装置から人の手を介さずデータを送信し，ブロックチェーンでデータを管理するといった仕組みが必要です．

■ノードの所有

適用したい業務によっては，なぜノードを所有しなくてはならないのかという課題も出てくると考えられます．実際に必要なのは仮想通貨を管理するウォレットのようなアプリケーションであって，分散台帳のデータを管理するノードではないかもしれません．ノードを管理するということは，管理コストや運用コストが発生します．クラウドベンダによるマネージドサービスの普及により，以前に比べるとそのコストは減少しているものの，ノード所有の必要性とそのコストは定期的な見直しが必要となるでしょう．

おわりに

ブロックチェーンは，技術面については現在も発展し続けています．以前は対応していなかった技術的な課題が，現在解消されているものも少なくありません．一方，ビジネス面においては，どのように利用するかの模索が続いている中，少しずつ商用サービスも出てきています．最新のトレンドを把握しつつ，ブロックチェーンは自社のどのような課題を解くために利用できるか継続して検討を進めることが大切です．

■参考文献

(1) https://www.ethereum.org/
(2) https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/
(3) https://plasma.io/
(4) https://www.meti.go.jp/press/2016/04/20160428003/20160428003.html

◆問い合わせ先

NTTデータ
技術革新統括本部　システム技術本部
デジタルテクノロジ推進室
TEL　050-5546-9404
E-mail　blockchain-contact@kits.nttdata.co.jp