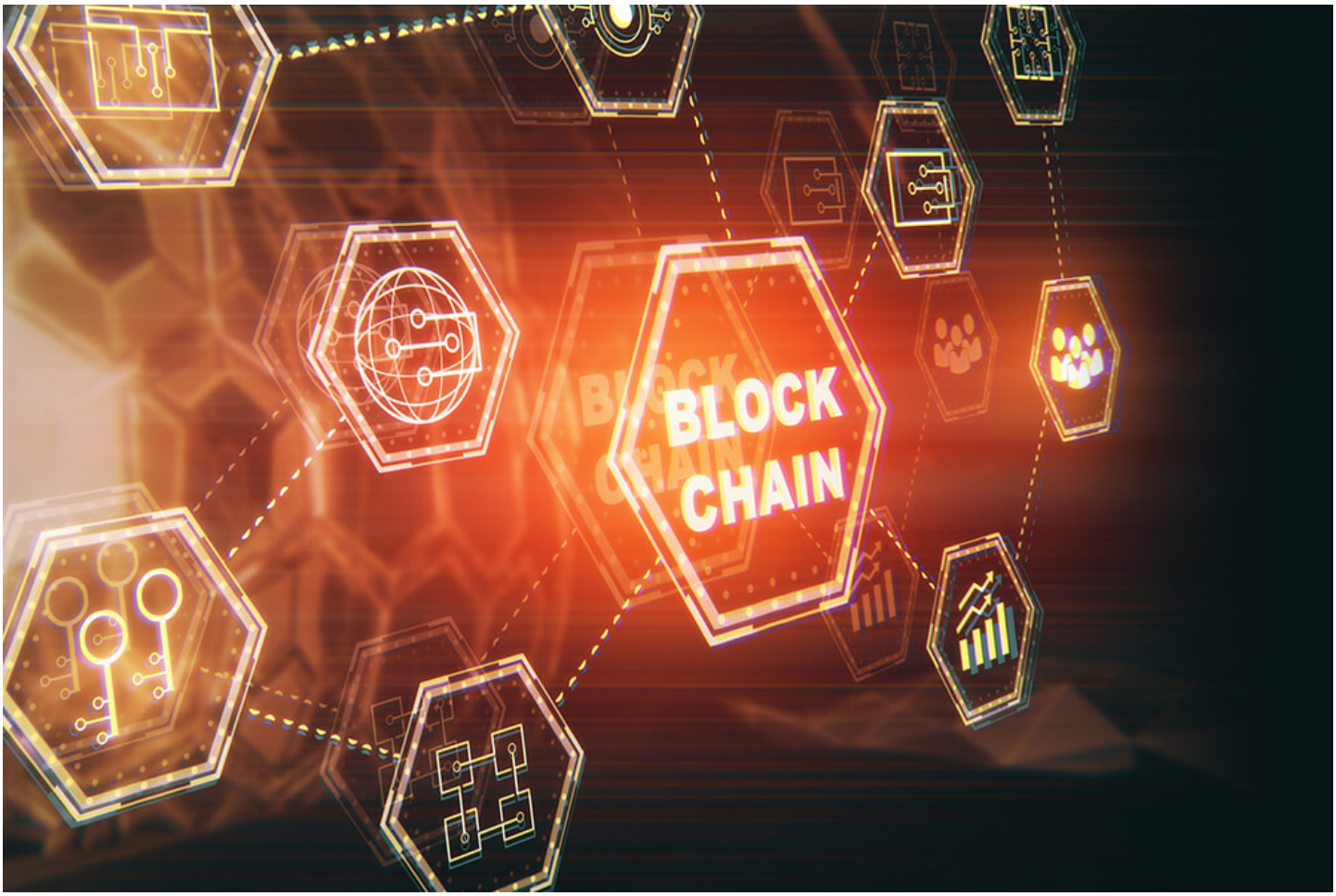
ビットコインだけじゃない、どんどん拡がるブロックチェーンの世界とその仕組み

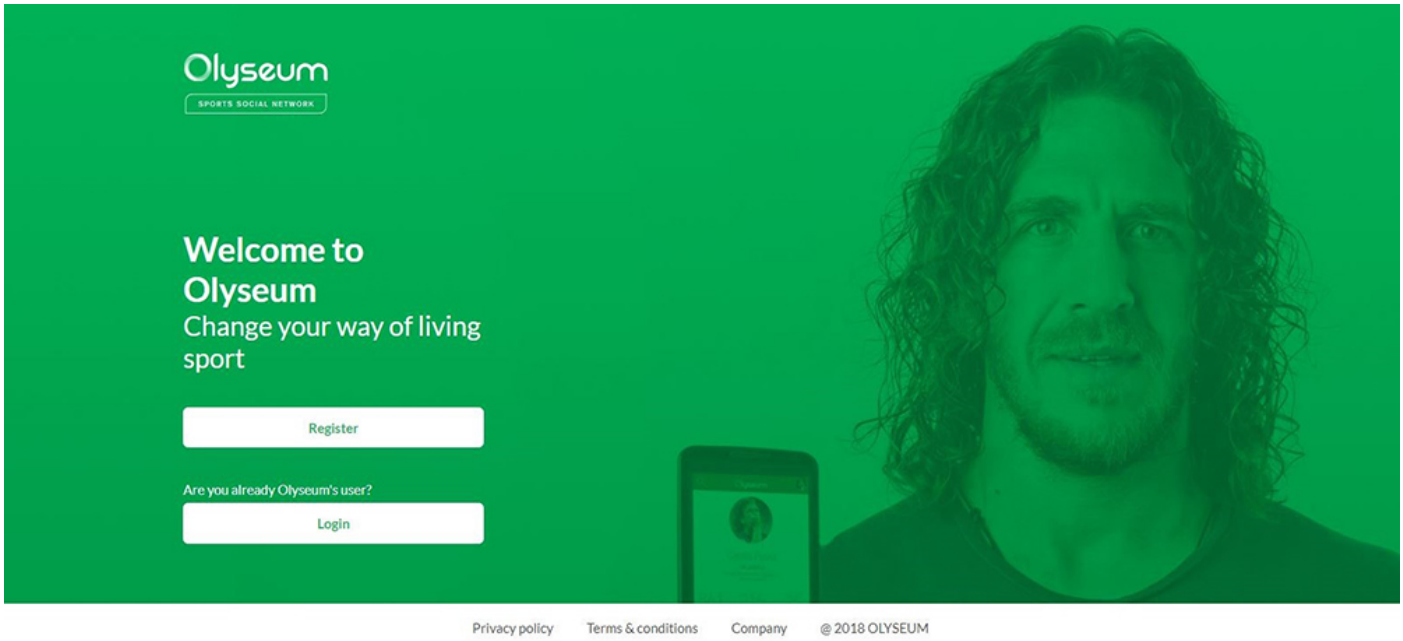
――仮想通貨の実現技術がなぜ他の産業でも活用されるのか――

FUJITSU JOURNAL / 2018年7月10日



4年に1度のサッカーの祭典、寝不足に悩まされた方は多かったことでしょう。今回は日本代表の決勝リーグ進出で大変な盛り上がりを見せました。迫力ある選手のプレーはもちろんですが、世界各国のサポーターの熱い応援も話題となりました。そんな中、世界的なサッカー選手がこのタイミングで"ブロックチェーン型のソーシャルネットワークを始めた"というニュース報道があったことをご存じでしょうか。2018年6月、Jリーグのヴィッセル神戸に所属するスペイン代表ミッドフィールダーのイニエスタ選手が、元スペイン代表ディフェンダーでFCバルセロナのキャプテンとしても大活躍したプジョル氏らと一緒に、スポーツファンに向けたソーシャルネットワーク

「Olyseum」のテストサイトを立ち上げました。ファンと選手のコミュニケーションを深める活動をするためにブロックチェーン技術を採用したそうです。

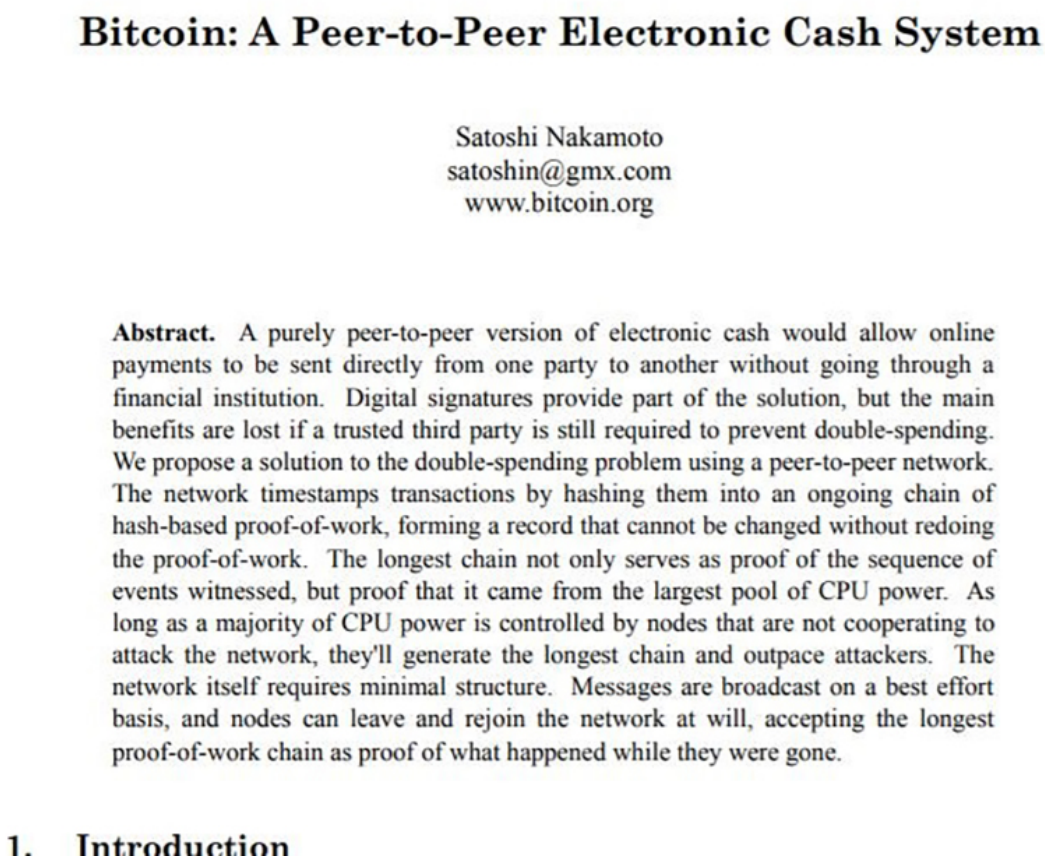


プジョル氏がユーザー登録を薦める*Olyseum*のトップ画面
（出所：*https://www.olyseum.com/welcome/init*）

もしかしたら、このニュースを聞いて「あれ？　ブロックチェーンって仮想通貨のために開発された技術だよね。ソーシャルネットワークと関係あるの？」と思われた方がいるかもしれません。ブロックチェーンは、仮想通貨を実現するために産み出された技術ではありますが、取引記録を安全に保存できる「分散台帳」を実現した技術としても魅力的です。それに加えて、新しい機能開発が進められたことで、今では様々な業務システムを支える汎用的なシステム技術として発展しています。今回は、身近なアプリケーションでの活用が始まっているブロックチェーンについて見ていくことにしましょう。

インターネットユーザーのための少額決済を目指したビットコイン

ブロックチェーンは、仮想通貨「ビットコイン」を実現するために考え出された、インターネット上でピアツーピア（P2P）接続（一対一での通信）した大量のコンピュータ群（コンピュータ同士が対等な関係でつながっているシステム）で実現する分散システム技術です。その原点と言える論文は、2008年にSatoshi Nakamoto名義で発表された「Bitcoin: A Peer-to-Peer Electronic Cash System」です。



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

ブロックチェーンの原典と言える*Satoshi Nakamoto*名義の論文
（出所：*https://bitcoin.org/bitcoin.pdf*）

ビットコインは、インターネットユーザーがネット上で商取引する際に、安い手数料で安全に使えることを目指して開発された仮想通貨です。電子的な支払いを実行する際に重要視される問題に「多重支払い」があります。現金払いと違って、電子的な商取引では購入と支払いに時間差が生じるので、支払請求や支払行為が多重化しない仕組みが欠かせません。このためインターネットユーザーがネットで商取引をするときは、多重支払いが生じない仕組みを構築した仲介業者に手数料を支払って、その仕組みを使うのが一般的です。これに対してビットコインは、多重支払いが生じない仕組みをP2Pシステムに組み込むことで、仲介業者を介さない電子決済（ビットコインの送金）を実現します。システムを維持するための手数料は必要になるのですが、仲介業者に支払うような大きな金額ではありません。
ビットコインは、世界中のインターネットユーザーが自分のコンピュータでビットコイン専用のソフトウエアを動かすことで作り上げるP2Pシステムで運用されています。重要なポイントは、集中管理するための特定のサーバーを設置するのではなく、P2Pシステムを構成するすべてのコンピュータ上にビットコインのすべての取引記録（送金ログ）が保存されることと、保存データを簡単に改ざんできない仕組みが組み込まれていることです。すべての送信記録が保存されていて、その改ざんが不可能となれば多重支払いという事態は発生しません。

取引はブロックとして記録、ブロックをつなげて取引台帳を作る

ブロックチェーンは、ビットコインを実現するP2Pシステムに組み込まれた「多重支払いが生じないシステム技術」のことです。ブロックチェーンの登場によって、これまで国や企業に頼っていた「貨幣の価値・信用」を、システムが備える技術で実現できることが示されたことで、国や企業の制約を受けない仮想貨幣を発行・運用できる可能性が出てきたわけです。実際、2013年に発生した「キプロス・ショック」と呼ばれる金融危機の時は、国の信用失墜の影響を受けず、いつでも取引出来るビットコインの価値が高まりました。

多重支払いが生じない仕組みはどのようなものなのでしょうか。その本質は、一定時間ごとの取引記録を「ブロック」と呼ぶ特殊なデータの塊にしたことと、ブロック相互を時系列に関連付けて「チェーン」のようにつないでいくことにあります。つまりビットコインは、「ブロックとチェーン」でビットコイン全体の取引台帳を作っているのです。

新たにブロックを作るときは、その直前のブロック内の情報を活用して作ります。ブロックは一定時間ごとに作り続けられ、そのたびに全体の整合性チェックが実施されます。あるブロックの内容だけを改ざんする場合でも、台帳全部を書き直さなければならないというこの仕組みによって、実質的に改ざん不可能なシステムとして運用できるわけです。

ビットコインの運営には、インターネット上でP2Pシステムを構成する大量のコンピュータが必要になります。それらのコンピュータは24時間365日動作し、世界中の取引データを一定時間ごとにブロックにまとめて記録しなければなりません。このシステムを安定させるために持ち込まれたのが、運用のために大量の計算処理を実行した参加者へのインセンティブです。多くの計算処理を実行した参加者にビットコインが発行され、取引手数料も提供されます。このシステム維持のための計算処理作業は、ビットコインの獲得につながることからマイニング（採掘）と呼ばれています。報酬を獲得するには、他の参加者よりも早く計算処理を終える必要があるため、今では多くの企業がビットコインのシステム運用のために大量のコンピュータを設置し、計算処理能力の増強を競っています。

システム維持にインセンティブを導入したことは、二つの観点でシステムに安定をもたらします。一つは、多くの参加者がシステム増強の競争を続けることになるため、システム全体が強化され続けることになること。もう一つは、仮に改ざんできるだけの圧倒的な計算能力を持つ参加者が登場しても、それだけの計算能力を獲得するために費やした投資を考えると、貨幣価値を毀損しかねないリスクをはらんだ改ざんで利益を得るより、システム運用に貢献して安定的に正当な報酬を獲得した方が安全かつ効率的となることです。

ちなみに、前述のNakamoto論文にブロックとチェーンという単語は出てきますが、ブロックチェーンという名称は登場しません。ブロックチェーンという言葉は、ビットコインのコア技術がブロックをチェーンのようにつなげていることから、仮想通貨の研究者の間で使われるようになって普及しました。

ブロックチェーンにプログラムを埋め込める「スマートコントラクト」

ビットコインのブロックチェーンは公開鍵暗号方式（一組の暗号化鍵と復号鍵を用いる暗号方式。一つを公開し、もう一つを秘密鍵として所有する。ブロックチェーンでは秘密鍵で個人認証を実行している）やハッシュ関数（任意の長さのビット列から規則性のない固定長のビット列を生成する関数のこと。生成したビット列から元データを見つけ出すことができないという特徴を持つ。元データを暗号化した上で何らかの処理を効率よく実施する場面で用いられる）を活用しており、取引データや参加者の個人情報を秘匿する仕組みを備えています。ただし、その目的が仮想通貨の実現であることから、そこでしていることはビットコインの取引記録を正確に残すことだけです。

2013年、新たな機能を備えるブロックチェーンに基づく仮想通貨が登場しました。イーサリアムです。新たな機能とは、ブロックチェーンの中にプログラムを埋め込めるようにしたことです。イーサリアムは、イーサという仮想通貨の運用システムの事を指しますが、その目指すところはイーサという仮想通貨を活用した新しい電子商取引のプラットフォームになることです。

イーサリアムの公式サイトのトップ画面　エーサリアムがブロックチェーン・アプリケーションのプラットフォームであることを宣言している
（出所：*https://www.ethereum.org/*）

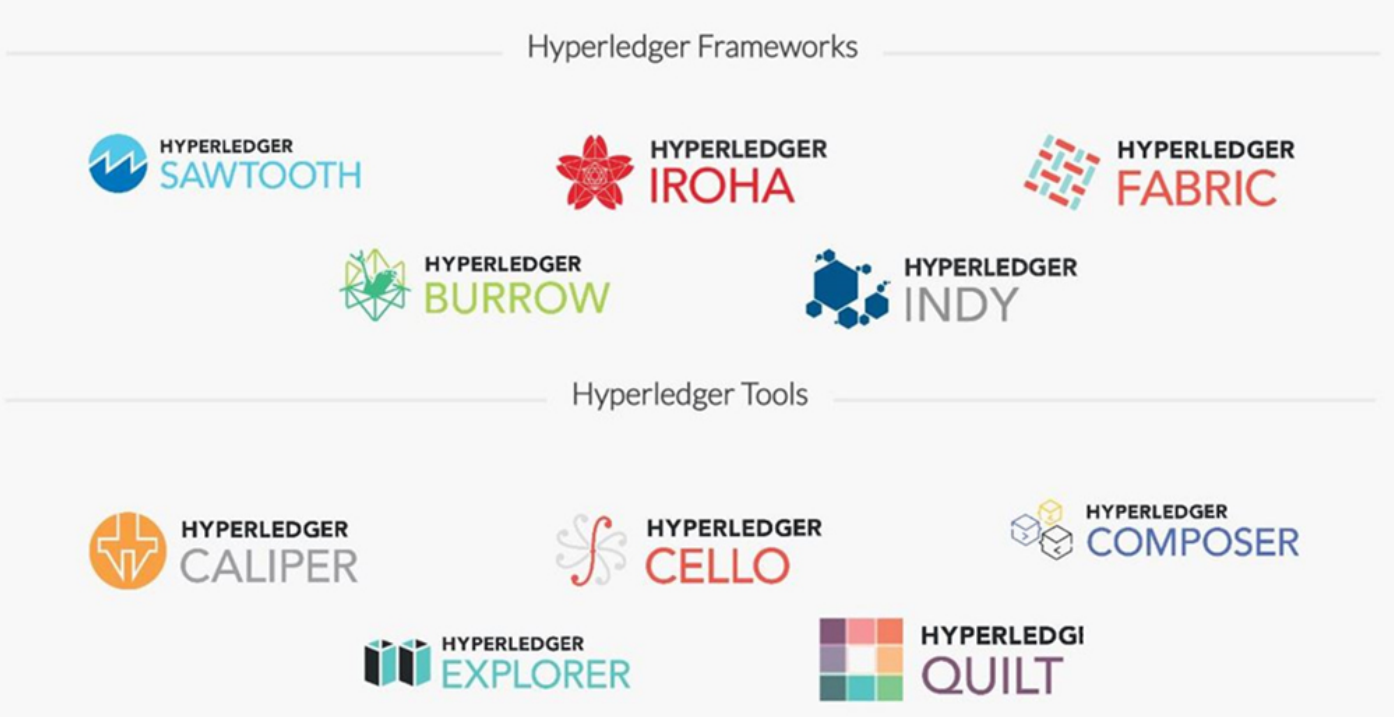
イーサリアムのブロックチェーンには、「スマートコントラクト」と呼ぶアプリケーション実行機能が組み込まれているので、これを利用することでインターネット上にイーサリアム・ユーザー向けの"自動販売機"を作ることができるのです。

具体的に説明しましょう。イーサリアムのブロックチェーンは、その中に「契約内容を記述したルール」と「契約内容を実行するプログラム」を埋め込むことができます。例えば企業Aがコンテンツ販売を企画し、10イーサでコンテンツをダウンロード販売することを考えたとします。その場合、「Aは、Xさんから10イーサを受け取ると、Xさんにコンテンツのダウンロードを許可するパスワードを送る」というルールと、それを実行するプログラムをイーサリアムのブロックチェーンに書き込みます。ブロックチェーンの仕組みで、このルールとプログラムがイーサリアムの構成するすべてのコンピュータに行き渡ります。誰かに決済を仲介してもらうことなく、イーサリアム・ユーザー向けのコンテンツ自動販売を始められるのです。

電子決済の仕組みを切り離し、ブロックチェーンの普及を目指す「Hyperledger」

ビットコインとイーサリアムは、仮想通貨を実現するためにブロックチェーンを用いていますが、仮想通貨とは切り離した分散台帳技術としてブロックチェーンを活用する試みも始まっています。その代表例と言えるのが、2015年12月にLinux Foundationが始めた「Hyperledgerプロジェクト」です。Linux FoundationはLinuxの普及促進を目的に、オープンソースコミュニティにさまざまな支援を実行している非営利組織です。

Hyperledgerプロジェクトの目的は、ブロックチェーンの「P2Pシステムで作る分散台帳」に着目し、これを活用して様々な産業分野におけるシステム課題を解決することです。この活動を推進するために、ブロックチェーンのオープンソース化に向けてフレームワークやツールを開発しています。開発テーマごとに個別プロジェクトを立ち上げており、2018年6月時点でフレームワーク関連とツール関連でそれぞれ5つのプロジェクトが誕生しています。個別プロジェクトでは、構成メンバーが自ら開発したブロックチェーン・ソフトウエアを提供するなどして、オープンソース化の作業を進めています。

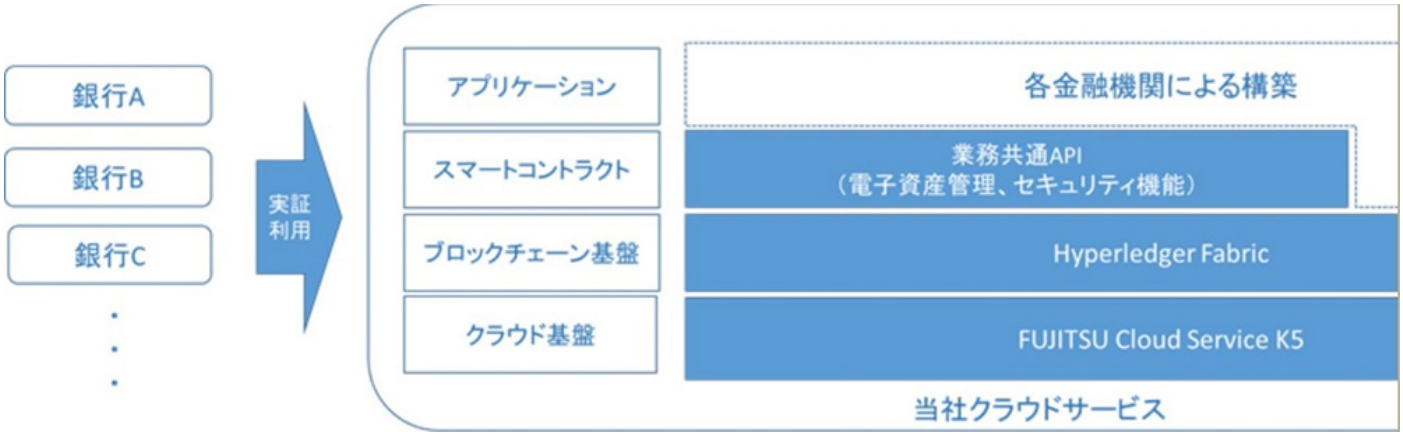


*Hyperledger*プロジェクトが組織しているプロジェクトの一覧
（出所：*https://www.hyperledger.org/projects*）

Hyperledgerプロジェクトのプレミアメンバーには、富士通をはじめとする大手ITベンダーの他、金融大手の米JPモルガンと独ドイツ銀行、クレジットカード大手の米アメリカンエクスプレス、自動車大手の独ダイムラー、航空機大手の仏エアバスが参加しています。

Hyperledgerプロジェクトの成果を活用した実証実験が国内で始動

Hyperledgerプロジェクトの活動成果は、プロジェクトに参加する企業のブロックチェーン関連製品などに反映されます。例えば富士通は2017年6月にブロックチェーンの応用による分散データアクセス制御技術「富士通VPX（Virtual Private digital eXchange）」をベースとするソフトウエアを開発しましたが、これはHyperledger Projectの一つであるブロックチェーンフレームワーク「Hyperledger Fabric」をベースとしています。Hyperledger Fabricのブロックチェーン上で実行される独自のスマートコントラクトを開発することで実現しました。
また、全国銀行協会がブロックチェーン技術を活用した金融サービスの実証実験環境の一つとして採用した富士通のクラウドサービスにも、Hyperledger Fabricが使われています。この実証実験環境「ブロックチェーン連携プラットフォーム」は、Hyperledger Fabricをブロックチェーン基盤として富士通のクラウドサービス「FUJITSU Cloud Service K5」上に実装したものです。



全国銀行協会が実証実験環境として採用した「ブロックチェーン連携プラットフォーム」

ブロックチェーンは今も多くの仮想通貨を支える技術として活躍していますが、スマートコントラクトなどの機能追加と、仮想通貨機能を切り離したHyperledgerプロジェクトなどの貢献によって、幅広い産業分野で用いることができる新しいシステム技術として発展しています。冒頭で紹介したOlyseumは、ファンと選手を結びつける新たな仕組みをブロックチェーンで作る計画があるとのことですが、例えば「投稿者のコメントに一定数の賛同コメントが寄せられた場合、投稿者には選手からの特別メッセージや特別コンテンツが送られる」といった仕組みがスマートコントラクトで実装されるかもしれませんね。
次回は、仮想通貨以外の適用事例を紹介しながら、ブロックチェーン利用のメリットや、今のブロックチェーンが抱える課題などを見ていきます。

著者情報

林哲史

日経BP総研　クリーンテック ラボ　主席研究員

1985年東北大学工学部卒業、同年日経BPに入社。「日経データプロ」「日経コミュニケーション」「日経NETWORK」の記者・副編集長として、通信/情報処理関連の先端技術、標準化/製品化

動向を取材・執筆。2002年「日経バイト」編集長、2005年「日経NETWORK」編集長、2007年「日経コミュニケーション」編集長を歴任。「ITpro」、「日経SYSTEMS」、「ITpro」、「Tech-On!」、「日経エレクトロニクス」、「日経ものづくり」、「日経Automotive」等の発行人を経て、2014年1月に海外事業本部長。2015年9月より現職。2016年8月より日本経済新聞電子版にて連載コラム「自動運転が作る未来」を執筆。2016年12月に「世界自動運転開発プロジェクト総覧」、2017年12月に「世界自動運転/コネクテッドカー開発総覧」を発行。2011年よりCEATECアワード審査委員。

FUJITSU JOURNAL / 2018年7月10日