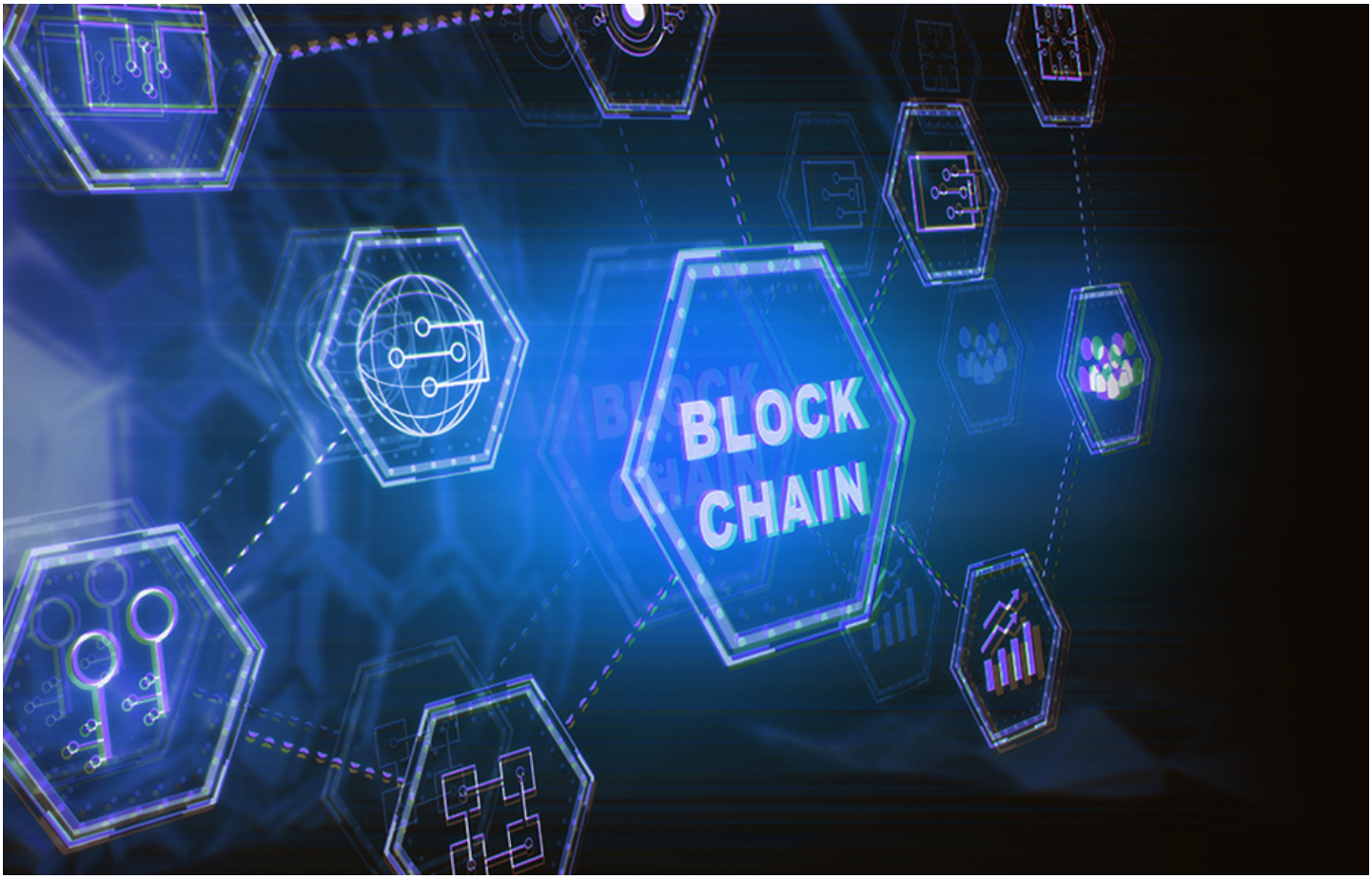
ブロックチェーンによる電子投票がつくば市で実施、処理能力向上やIoT対応に向けた次世代ブロックチェーンも続々登場

FUJITSU JOURNAL / 2018年9月20日



2018年8月、ブロックチェーンとマイナンバーカードを用いた国内初のインターネット投票の実証実験が実施されました。主催したのは茨城県つくば市。同市は民間の創意工夫をいかしたIoT・AI・ビッグデータ解析等の革新技術を社会実装するためのトライアル（実証実験）を公募し、優れたトライアルを支援する取り組みを進めていました。今回、応募トライアルの中から「つくばSociety 5.0社会実装トライアル支援事業」を選定するための最終審査で、インターネット投票システムを活用しました。マイナンバーカードは投票者認証のためのものです。

公平なインターネット投票の基本条件は次の四つです。第一は、投票者の正当性の確認、第二は投票内容の秘匿、第三は複数投票の防止、そして第四は投票結果の改ざん阻止です。

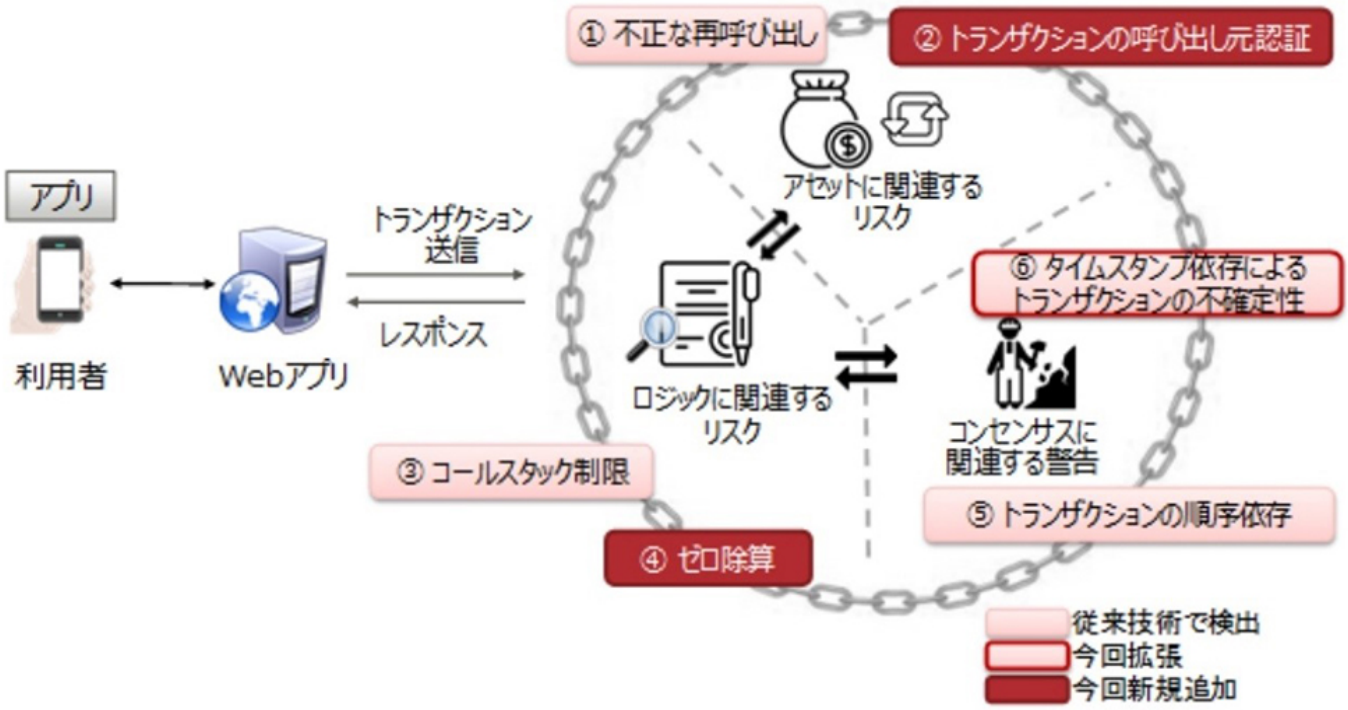
ブロックチェーンの特徴は、「参加者の取引行為（この場合は投票）の秘匿性を確保した上で、改ざんされることなくすべての取引結果を記録する」ことです。ですからブロックチェーンに投票者認証の仕組みを組み合わせれば、四つの基本条件をクリアするインターネット投票システムを実現できます。
つくば市のインターネット投票は、あらかじめ用意した投票所内の端末で投票する形で運用されましたが、技術的には自宅や出先からも投票できるシステムとして作られています。こうした取り組みが進んでノウハウが蓄積されれば、将来的には自宅や出先からインターネット投票で私たちの代表を選べるようになるかもしれません。

ブロックチェーンの課題は、リアルタイム、処理能力、セキュリティ

金融業務からインターネット投票まで、さまざまな経済・社会活動のデジタル化・システム化をドライブすることが期待されているブロックチェーンですが、完璧な技術として完成したわけではありません。ビットコインの検討が始まったのは2008年ですから、ブロックチェーンの技術開発は始まったばかりとも言えます。解決しなければならない課題は多く、高いポテンシャルはあるものの、その真価を発揮するには、今後多くの新技術が組み込まれる必要があります。
ブロックチェーンが抱える課題はいくつかありますが、ここでは代表的なものを三つ紹介します。第一は「リアルタイム処理」に弱いことです。ブロックチェーンは、一定時間ごとに取引記録をブロックにまとめて記録するというプロセスがあります。また、複数のコンピュータが同時にブロックチェーンを別々に作ってしまうケースが発生するため、一定時間が経過した後に、一番長いブロックチェーンを正式なものとするというルールがあります。このため、ブロックチェーンにおいて正式な記録であると判定できる状態になるまでに時間がかかるので、厳しいリアルタイム性が求められる取引には向いていません。
第二の問題は、「処理能力」が小さいことです。これは、ブロック当たりのデータ量が決まっていることと、一定時間ごとに記録することに関係しています。瞬間的に大量の取引が発生すると、データ量に収まらない分の取引は次のブロックに回すことになります。ブロックチェーンを構成するコンピュータ群は大量の計算処理を実行してブロックを生成しますが、そのコンピューティングパワーは他のコンピュータより早く計算して報酬を得るために使われています。単位時間当たりの処理件数は、コンピュータの処理能力には関係なく、ブロックチェーンの仕組みによって決まっているのです。
第三の問題は、セキュリティです。特に危険性が指摘されているのは、プログラムの実行環境としてブロックチェーンを利用するスマートコントラクトについてです。スマートコントラクトでは、プログラムをブロックチェーンに埋め込むことによって、ブロックチェーンに参加するすべてのコンピュータにプログラムを配布・実装することができます。悪意あるプログラムを配布することのないように、取り扱うプログラムの安全性を発見する仕組みの継続的な開発が求められます。

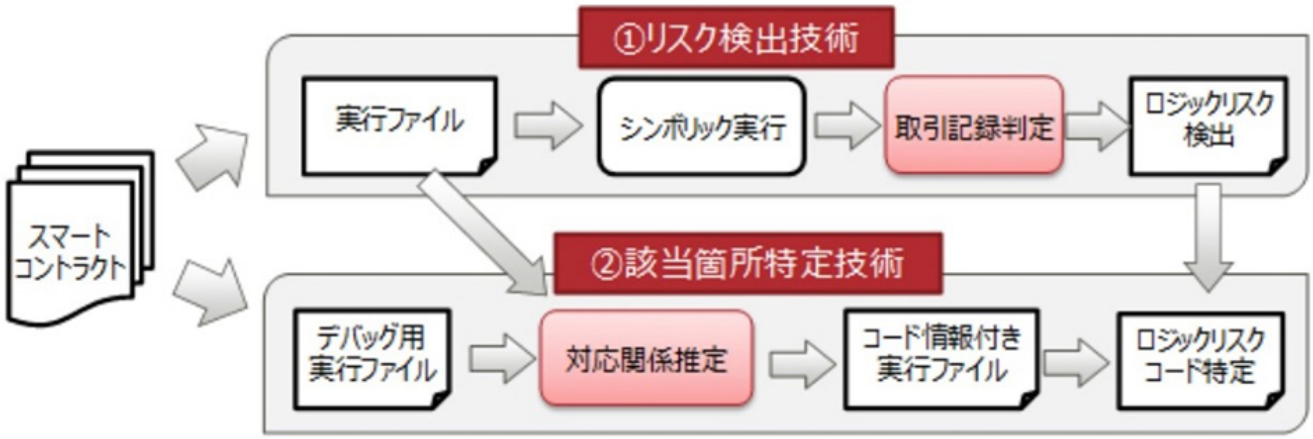
スマートコントラクトのリスクをチェックしてソースコードの該当箇所を見つける

ブロックチェーンの問題解決に向けた取り組みは世界中で活発に進められています。例えばスマートコントラクトのセキュリティ問題については、富士通研究所と中国富士通研究開発中心の開発事例があります。両社は共同で、スマートコントラクトのリスクを事前に検証した上で、検証で見つけたリスクがプログラムのどの部分にあるのかを特定する技術を開発しています。
具体的には、ブロックチェーンアプリケーションの実行基盤の一つであるイーサリアム上においてリスクのある取引の流れを特定するアルゴリズムを開発し、人手では見逃す可能性のあったスマートコントラクトのさまざまなリスクを網羅的に検出できるようにしました。



富士通研究所と中国富士通研究開発中心が検証可能にしたスマートコントラクトのリスク

他にもリスクの発見に加えて、発見したリスクが元のソースコードのどの部分にあるのかを高い精度で特定する技術も開発しました。実行ファイルと、ソースコード情報が付加されたデバック用の実行ファイルの対応関係を推定することで、発見されたリスクのあるソースコードの該当箇所を見つけます。この技術を組み込んで運用すれば、スマートコントラクトのセキュリティは大幅に高まるでしょう。



富士通研究所と中国富士通研究開発中心が開発したリスク検出技術と該当箇所特定技術

高い処理能力で格付け機関からの高評価を得るEOS

ブロックチェーン技術はビットコインという仮想通貨を実現する技術として誕生しました。以降、ビットコインのブロックチェーンを改良・強化した新しいブロックチェーン技術が続々と登場し、それぞれ独自の仮想通貨を生み出しています。世界中で発行されている仮想通貨の取引価格や取引量、時価総額などを発表しているCoinMarketCapによると、2018年8月時点で1900以上の仮想通貨が発行されています。

これらの新しいブロックチェーンの中には、ビットコインのブロックチェーンが抱えていた課題を克服したものもあります。例えば2017年6月に創設されたEOSは、参加者の投票で選ばれた人が効率的にブロックを生成する仕組みを取り入れるなどして、処理速度の高速化を実現しました。ビットコインのブロックチェーンが処理できる取引件数は1秒間に数件でしたが、EOSは1秒間に何百万件規模の件数を扱えるようにすることを目指しています。

EOSは、企業が事業活動で活用できるスマートコントラクト向けの分散型プラットフォームの実現を目指して創設されました。この考え方はイーサリアムに似ていますが、イーサリアムにない特徴があります。それは、手数料が無料であることです。

EOSは技術的な評価が高いという特徴もあります。例えば、中国では中国情報産業省電子情報産業発展研究院（CCID：China Center for Information Industry Development）が仮想通貨の評価指標「国際パブリックチェーン技術評価指標」に基づいた評価結果を発表していますが、2018年6月発表の評価結果ではEOSが総合第一位となりました。同ランキングは技術、適用性、革新性の観点で評点したものですが、EOSは技術部門でも第一位でした。ちなみに総合第二位はイーサリアムでした。

赛迪研究院发布全球公有链技术评估指数（第2期）

来源： 作者： 投稿时间：2018-06-21

6月20日上午，赛迪全球公有链技术评估指数（第2期）是在链锁反应（Ⅱ）高峰科技论坛上正式向社会发布的，此次论坛由中国电子信息产业发展研究院为指导单位，赛迪区块链研究院主办，上海泛伍文化传播有限公司承办。EOS位居首位，以太坊屈居次席，比特币位列第17！。

中文名	英文名	分项指数			总指数	综合排名
		基础技术	应用性	创新力		
EOS	EOS	102.0	15.4	44.1	161.5	1
以太坊	Ethereum	85.2	24.9	28.3	138.4	2
NEO	NEO	73.7	27.4	7.9	109.0	3
恒星链	Stellar	78.1	21.2	9.0	108.3	4
应用链	Lisk	66.7	20.8	18.1	105.6	5
星云链	Nebulas	73.5	21.1	10.7	105.3	6
斯蒂姆链	Steem	89.9	7.5	10.1	104.5	7
比特股	BitShares	82.3	10.9	10.9	104.1	8
瑞波链	Ripple	77.1	9.4	16.4	102.9	9

国際パブリックチェーン技術評価指標に基づいた評価結果の報道資料の一部（出所：中国情報産業省電子情報産業発展研究院）

IoTのための新技術はブロックチェーンとは異なる手法で分散台帳を実現

ブロックチェーンの限界を突破するために、ブロックチェーンとは異なる原理の分散台帳技術を開発する活動も始まっています。その代表例と言えるのがIoT向けの仮想通貨として開発が進められているIOTA（アイオータ）です。

IOTAは、IoTデバイス間でのデータのやり取りをする際に用いられることを前提としています。IoTでは大量のリアルタイムデータを瞬時にやり取りすることが求められます。大量のセンサーから情報を収集してビッグデータにすれば情報価値が高まります。ただ、一つ一つのセンサー情報の対価はそれほど大きくありませんし、やり取りそのものは無数に発生します。やり取りを記録するたびに手数料を支払っていたのでは、IOTAの普及は望めません。そこでIOTAでは、リアルタイム性と処理能力を高めるだけでなく、手数料を無料にする仕組みを考えました。それが

「Tangle」です。
Tangleは、取引をしたい人が、他の取引を承認します。そして自らが承認した二つの取引に自らの取引を関連付けて記録します。このため全体的な取引記録は単純なチェーン状ではなく、取引が複雑に関連付けられた形で記録されます。
Tangleにはブロックなどのリアルタイム性と処理性能の足かせになる決まりはないので、個々の参加者は即座に個別に取引を承認できます。しかもオフライン状態での承認も認めているので、リアルタイム性や処理性能を高めやすくなっています。オフライン状態の承認結果を含んだ全体的な整合性は、オンライン状態になったときに同期して確保します。
IOTAを活用したソリューション開発も始まっています。例えば台湾の台北市は、IOTAを主導するIOTA財団と共同で、スマートシティをIOTAで実現する共同プロジェクトを2018年1月から始めています。最初のプロジェクトは、TangleIDを組み込んだデジタル市民カードの開発。デジタル市民カードの用途としては、議決権行使、医療記録情報の提供、政府関連サービスの利用が想定されています。
製造業向けでは、富士通が2018年4月、製造物のトレーサビリティを管理する場面にIOTAを用いるデモンストレーションをハノーバーメッセ2018で実施しました。サプライチェーン全体で製品や部品のトレーサビリティを実施するには、異なるいくつもの管理システムを相互連携させる仕組みが必要になるわけですが、IOTAを用いればIDサプライチェーンをまたがったトレーサビリティを効率よく実行できる可能性があります。
仮想通貨を実現するために誕生したブロックチェーンですが、その技術は急速な発展を遂げています。技術面でも用途面でも、あっと驚く展開が始まる期待があります。インターネットが大きな発展を遂げたように、ブロックチェーンも新しい社会を支えるインフラのプラットフォームとして、生活の中に浸透していくかもしれませんね。

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。