ブロックチェーン市場調査　報告書

この報告書について

この報告書は、ブロックチェーン技術の最新動向として、特に以下の2つにフォーカスして調査をおこなったものである。

- ブロックチェーンの金融向けの応用についての動向
- コンソーシアム型ブロックチェーンの現状と今後の方向性
- ブロックチェーンのインターオペラビリティの動向
- Identityに関する動向
- ISO TC307などの国際標準化、日本国内の動向、および国際会議における新規技術開発の方向性

本報告書の内容は、2020年3月25日時点のものであり、その後の動向については反映されていないことに注意が必要である。

金融への応用の動向

2019年を通じたブロックチェーンの金融分野への応用は、主に2つの流れがある。1つは規制に適合していないグレーゾーンのICOが多発したことへの反動としての、規制に準拠したブロックチェーンベースの金融の構築、もう1つは、Facebook Libraにみられるように、金融包摂に向けた民間発行のグローバル通貨への動きである。

規制に準拠したブロックチェーンベースの金融の構築

2017年にブームとなったInitial Coin Offering（ICO）は、クラウドファンディングのような形で企業が資金調達する方法として注目を集めたが、投資家への情報開示の不備による投資家保護上の問題、資金決済法の扱いになる暗号資産とのグレーゾーンを利用した金融商品取引法の潜脱として考えられるため、厳しい規制がかかるようになった。
そこで、いわゆる企業の資金調達のための、流通性のある暗号資産については「電子記録移転権利」として整理され、金融商品取引法の規制対象とされることになった。

ICOへの批判に対応する形で、最初に新しく提案された形式はInitial Exchange Offering（IEO）であり、取引所にトークンを委託して資金調達するという形である。さらに、トークンそのものを、既存の有価証券と同じように流通できるようにしたものが、Security Token Offering（STO）となる。従来の有価証券の発行による資金調達に比べてSTOが優れいてる点は、Ethereumなどのスマートコントラクトが可能なプラットフォーム上でトークンが発行されているために、透明性が高く、仲介コストが低減された、高度な取引の実現が期待できるか

らである。このようなSTOのためのプラットフォームを開発し、提供するスタートアップも数多く登場しており、Securitize, Polymathなどはその代表例である。

日本では、2020年改正、2021年施行の改正金融商品取引法で、STOについても自主規制団体による自主規制ルールのもとで、規制されたブロックチェーン上の金融サービスとして実施できるようになる。現在、証券会社を中心とする日本STO協会が自主規制ガイドラインを取りまとめ、認定自主規制団体に名乗りを上げている。本報告書の執筆段階では、自主規制団体の認定についての決定は出ていないが、6月に予定される施行の前には、自主規制のフレームワークも定まると想定されている。

金融包摂に向けた民間発行のグローバル通貨

2019年のブロックチェーンの金融応用の一番のトピックはFacebook Libraの登場と、規制当局との軋轢である。Facebook Libraは、Libra協会に属する30あまりのメンバーによるコンソーシアム型ブロックチェーンを元に、複数のFIAT通貨のバスケットを元にしたステーブルなコインを発行し、実際のメンバー企業を通じたトランザクションの処理は、Layer2のように別の処理を行い、必要な処理性能を確保する方式とされている。Libra協会自身は、将来的にコンソーシアム型ブロックチェーンから、パブリック型のブロックチェーンへの移行を行うとしている。これは、米国の規制当局への対応として、Libra協会のガバナンスから有価証券としての規制を受けないようにするための措置と考えらえる。

Facebook Libra自体は、銀行口座を持てないUnbankedな人を対象に金融サービスを提供する、いわゆる金融包摂の実現をその目的としている。しかし、この目的、および、その他の金融規制の関係で、米国政府、議会、金融規制当局と大きな論争となっているのには、以下の点があると考えられる。

(1) Facebookのようなテックジャイアントの存在に関わる論点
Libraに対して政府や規制当局が大きな反応を見せている理由のひとつが、Libraの主要プレイヤーがテックジャイアントの一角であるFacebookである、ということである。ケンブリッジアナリティカの事件に象徴されるようにプライバシー保護の問題や、政治への介入のツールとして使われるようになったことなど、国家や市民を脅かす存在となったことや、広告モデルによるビジネスがプライバシーの侵害に結びついていることなど、同社が社会インフラとして影響力が大きくなっているにもかかわらず、その担い手としての適格性に大きな疑義があることによる。

(2) 金融システムとしての論点
　金融システムとして見たときの課題には、大きくは3つの論点がある。1つ目はフリーバンキングと呼ばれるもので、国家による管理や規制を受けずに、銀行機能と通貨発行権を持ち得るのかという点だ。この点について、過去のフリーバンキング排除の歴史を踏まえ、まずはフリーバンキングを許容するような社会環境変化や技術的発展が成し遂げられたのかを慎重に検討する必要があるだろう。また、規制当局側の視点で見れば、足元の社会的・技術的環境において過去のようにフリーバンキングを排除することができるのかといった現実的な問題も生じ

る可能性もある。2つ目の論点は、通貨バスケットによるステーブルコインが成立しうるのかという点だ。ステーブルコイン自体が、継続的にバスケットに対する交換比率を維持することができるのかは重要な論点である。また、こうした新しいタイプの通貨が成立しうる場合に広く金融政策やマクロ経済政策への影響が生じる可能性がある点にも留意が必要だろう。そして、3つ目は、国家をまたがる決済が、国家の管理外で行われるようになることに起因して発生するマネーロンダリング対策の問題だ。これは、後述のビジネスモデル上の問題だけでなく、プライバシーと国家による検閲の問題など広範な社会的含意のある論点であり、単に勧善懲悪的な問題ではないことに留意が必要となるだろう。

(3) Libraのビジネスモデルにおける論点
1つ目の懸念は、Libraが掲げているunbankedな市民の金融へのアクセスである。これ自体は、Financial Inclusion（金融包摂）の文脈からは非常に重要なことだ。ビットコインやブロックチェーンを利用した新たな金融にも大きく期待されているところで、この目標自体は歓迎すべきことだ。一方で、LibraにおけるIdP（Identity Provider）の扱いは不明確である。Facebook自体には、IdPの機能を担う、あるいは独占する大きなインセンティブがあるが、もしFacebookがIdPの機能を独占するとすれば、この金融システムの参加の権利を同社が左右することを意味する。つまり、Facebookが新たにunbankedな人を作り出すことができるかもしれない。近年SNSでも、通報制度などを含めてアカウント停止が多くなされるようになる中で、IdPの扱いは極めて重要だ。もし本当のFinancial Inclusionを実現したいのであれば、複数のIdPを切り替えられるようなAPIが実装される必要があり、またSelf Sovereign Identityの仕組みも必要だろう。一方で、広告収入をベースとするFacebookのビジネスモデル上、同社や株主がそれを許容するかは不明だ。Libraは、一定期間後にパーミッションレスブロックチェーンへの移行を表明しているが、その一定期間内にある種の独占が生まれないかどうかは、大きな論点である。

　また、そもそも、Libraのビジネスモデルで本当にUnbankedな人への金融システムへのアクセスを提供することができるのかと言った問題もあるだろう。例えば、途上国の人々がFacebookのサービスにアクセスできるような高度な端末を有しているのか、マイナー通貨でLibraを販売するような認定販売所が現れるのかといった点は実際に目標を達成するに当たっての大きな障害となる。

　2つ目の懸念は、金融規制の目標にもあるが、マネーロンダリング対策などの金融インフラとして必要な機能を、誰がどのような実装し、運営するかという問題である。もし、Known Your Customer（KYC）と呼ばれる顧客管理や、疑わしい取引の検知を含めたマネーロンダリング対策の実装と運営が、コンソーシアムの各会社の責任で行う形となるのであれば、それらの会社の運営費は莫大になり、持続的な運用を行うにはビジネス上成り立たない可能性が出てくる。すると、それらの会社はコンソーシアムを脱退する可能性があり、ビジネスモデル自体が成り立たない。Facebookにとっては、実は決済の手数料収入はなくてもよく、そういった決済システムの泥臭い部分をやらずに、自社のサイトのアクセス時間（＝広告収入）を増やすことができるだけでもメリットがあるかもしれない。そういった、参加する会社それぞれのビジネスモデルと、インセンティブモデルの分析は必要である。

一方で、Facebook Libraは、数多くのレガシーを残す可能性も大いにある。その1つは、コン

ソーシアム型ブロックチェーン上に、新たなスマートコントラクト用のプログラミング言語を構築し、layer2のようなスケーラビリティのための工夫がされたソフトウエアが、オープンソースで開発されていることで、仮にLibraがビジネス的に頓挫したとしても、これらのプログラム資産は後々生かされる可能性は高いと考えられる。

コンソーシアム型ブロックチェーンの現状と今後の方向性

ビットコインのような、パーミッションレスな支払いを目指したブロックチェーンは、もともとの金融サービスとしての規制上の問題、スケーラビリティ問題のような技術的問題、管理者が不要であることが故にマネタイズのためのポイントがないことなど、エンタープライズ向けの用途では、すぐにはビジネスになる応用が見当たらないという課題がある。

一方で、共有のデータを複数のエンティティで処理しながらアップデートしていく、というパーミッションレスブロックチェーンの技術的特徴を生かしながら、ブロックチェーンの維持の責任を一定のエンティティで賄うことで、性能問題の解決とビジネス性を持たせたものが、コンソーシアム型ブロックチェーンである。

ビットコインのブロックチェーンの主なメリットは、支払いの帳簿の更新という情報処理を行うにあたって、信頼できる第三者が不要になるというところである。一方で、コンソーシアム型ブロックチェーンは、参加するメンバーが多くの場合固定されている少数のノードで、それぞれのノードにビットコインのノードに比べると多くの管理責任が発生する。そのようなトラストモデルの観点では、パーミッションレスブロックチェーンと、コンソーシアム型のブロックチェーンは別の技術と考えることが適切である。トラストモデルの観点では、コンソーシアム型ブロックチェーンは、暗号的タイムスタンプサービスのタイムスタンプサーバを分散させ、タイムスタンプに書き込むデータの情報処理にルールを付加したものである。

コンソーシアム型のブロックチェーンについては、R3やHyperledgerなどのプラットフォームや、それらを利用したMarco Poloのようなドメインを限ったプロジェクトが存在する。このようなコンソーシアム型ブロックチェーンが登場した当初は、パーミッションレスブロックチェーンが、ノード運営費用やエコシステムの維持費用を、コインの報酬で代用していたことと混同し、パーミッション型でも同じようなコスト低減が実現できるように宣伝されていた。しかし、実態としては、コンソーシアム型ブロックチェーンのメンバーは、タイムスタンプ局を運営するようなコストと責任を追うため、プラットフォームを利用して実現できる手間の削減と、維持費用の比較を精緻に行う必要がある。コンソーシアム型ブロックチェーンを実際のアプリケーションに適用した時の経済的便益についてのフレームワークの研究を始めている大学もあるが、これらの研究を進める必要があるだろう。

一方で、故障に強く、幅広いビジネスロジックを実現できる帳簿用のタイムスタンプ技術として考えると、現在のビジネスのデジタル化にはそのまま適用可能でもある。その際に、ビジネス上必要なのは、タイムスタンプの有効性を規定しているe文書法の改正を行い、コンソーシ

アム型ブロックチェーンにおける処理の有効性を法的に担保できるようにして、この技術を利用した時のメリットを大きくすることが挙げられる。例えば、現在でもe文書法で認められたタイムスタンプを使うと、領収書のスキャン画像が税務申告に利用できるようになる。これらを画像ではなくて、広範囲な取引データに対しても認められるような法改正を求めることは重要なステップである。

また、Facebook Libraの項で述べたように、Facebook Libraのプログラムコードは大きなレガシーになることが見込まれる。ID管理やAMLなどの観点で検討不足ではあるが、基本的なアイディアについては優れたものが多いため、Libraのコードをベースに新たな応用を研究開発することは有望な方向である。

ブロックチェーンのインターオペラビリティについて

異なるブロックチェーン上の帳簿のデータを相互に取り扱えるようにする、インターオペラビリティは、ブロックチェーン普及上の大きな課題である。ISO TC307においてもインターオペラビリティのStudy Groupが立ち上がっている。一方で、インターオペラビリティの指し示す定義が曖昧で、何が保たれることがインターオペラビリティの確保になるのかが現時点で不明である。

この混乱の大きな原因の1つは、ブロックチェーンにおけるトラストの境界の問題が挙げられる。Bitcoinであれば、支払いの足し算引き算の演算に限って、信頼できる第三者がなくてもトラストが保たれる。Ethereumも、同じく限定された範囲において帳簿の更新におけるトラストが形成される。しかし、それらは限られた系の中での話であり、他のトラストモデルとの連携があった場合に保たれる保証はない。端的な例は、スマートコントラクトにおけるOracle問題であり、帳簿と別の系とのやりとりの中で、データそのものではなくトラストが損なわれない事を証明するのは困難である。

インターオペラビリティを実現するためには、2つの要素が必要である。1つは、異なるトランスの系のデータを扱う時のトラストの依存関係を表現し、扱えるようにする記述言語とトラストの可視化ができるようにすることである。もう1つは、異なるブロックチェーンに記述された個別のトランザクションの識別子を正しく付与し、いつでも誰でも識別できるようにする事である。このような議論が、ISOを含めたインターオペラビリティの議論に必要とされると考えられる。

Identityに関する動向

ブロックチェーンの金融以外のアプリケーションの中で有望視されているのは、広い意味での包摂を実現するSelf-Sovereign Identityである。通常、Identityは、Identity Provider (IdP)がコントロールしているため、ある人がシステムの中でIdentityを確立できるかは、他者に委ねられることになる。簡単な例としては、SNSにおいてサービス提供主体がIDを停止、あるいは削除してしまう（アカウントBan）の問題がある。また、IDに関する情報が他者に集約されている

と、そこからの情報漏洩において、プライバシや自分自身を証明する手段が冒される可能性がある。このようなIdentityに関する課題を、単一障害点を持たないパーミッションレスブロックチェーンの特性を用いて実現しようとするプロジェクトが複数存在する。

- Onename
  OnenameはBlockstack社が開発する、Bitcoin Blockchain上に構築したSelf-Sovereign Identityのプラットフォームで、Bitcoinのアドレスと、Onenameのアカウントと、SNSなどのアカウントを結びつけて、個人のIDが失われない形で保持する。

- uPort
  uPortは、Consensysによる、Ethereum blockchain上に構築したSelf-Sovereign Identityのプラットフォームである。スマートコントラクトの形で、IDの管理を実現している。

- ERC725/735
  ERC725/725は、Ethereum上でSelf-Sovereign Identityを扱うための技術仕様で、ERC725がインターフェース、ERC735がIDの処理を定義している。uPortと同様に、スマートコントラクトの形でSelf-Sovereign Identityを実現している。ERC725 Allaianceのメンバーであるorigin Protocolがでもコードを公開している。

- Sovrin Foundation
  Sovrin Foundationは非営利団体であり、Self-Sovereign IdentityであるSovrin IDと、そのための分散ネットワークであるSovrin Networkの開発と運用をしている。ボードメンバーも多様性を持たせており、NECの佐古和恵氏もボードメンバーになっている。もともと、Evernym社の分散台帳であるIndyを用いて開発を行なっていたが、のちに譲り受け、Hyperledger Indyという形で、Hyberledgerにも採択されている。独自のブロックチェーンを運営しているのが特徴。

Self-Sovereign Identityを実現するためには、識別子が分散された状態でも一意である必要がある。そのための仕組みとしてDistributed Identifier（DID）があり、W3Cにおいて議論されている。Self-Sovereign Identityについては、エコシステム上のエンティティの役割の定義と、プライバシ保護に関する要求条件の標準的な議論が今後必要である。もう1つの課題は、Self-Sovereign Identityの運営について、そのエコシステムが持続的に作れるか、という点である。一般にSelf-Sovereign Identityのプラットフォーム自体に、マネタイズを行うポイントは存在しない。直近では、Sovrin Foundationが資金不足から、運営モデルの変更の検討を余儀なくされている（https://sovrin.org/the-status-of-the-sovrin-foundation/）。
そのため、ビジネスモデルの検討と合わせて、技術と標準設計を行う必要がある。

標準化に関する動向

ISO TC307の現状

ISO TC307は、ISOにおいてブロックチェーンおよびDLT(分散台帳技術）の標準化を行う技術委員会であり、2017年の4月にシドニーで第1回目の国際会議が開催されて以来、東京（2017年11月）、ロンドン（2018年5月）、モスクワ（2018年11月）、ダブリン（2019年5月）、ハイデラバード（2019年11月）と計6回開催されている。
現在、TC307の組織は以下のように構成されている。

WG1: Foundations

WG1では、3つの標準文書が作成されている。

- ISO 22739: Terminology and concepts
  Blockchain技術とDLTに関する語彙を定義することを目的とした文書であり、3月14日のバージョンでは125の単語の定義が記述されている、規格文書の主要なパートはClause 3 Terms and definitionsである。現在FDIS投票に掛けられている。

- ISO 23257: Reference Architecture
  Blockchain技術とDLTの参照アーキテクチャを定義することを目的とした文書。参照アーキテクチャの中には、概念、アーキテクチャの観点、機能別コンポーネント、役割、動作とその関係について述べられている。現在3回目のCD投票にかけられている。2020年3月8日現在のバージョンでは、5つの性質（Storage Architecture, Control Architecture, Sub setting, Permissions, implementation）による部類、基本コンセプトとして、システム、ネットワークと通信、システムインターフェース、合意、イベント、台帳コンテンツのIntegrity、台帳管理のIntergrity、Sub chainとSidechain、DLTアプリケーション、DLTソリューション、そしてスマートコントラクトが定義され、その上で、アーキテクチャの全体像と各要素についての解説、レイヤ、参照システム構成などが記述されている。

- ISO TS 23258: Taxonomy and Ontology BlockchainとDLTに関する分類学とオントロジの文書が作成されている。現在WD段階である。

WG2: Security, privacy and identity

WG2は、セキュリティ、プライバシ、アイデンティティを議論するWGである。しかし、2018年5月のロンドン会議において、プライバシとアイデンティティについては、ISO/IEC JTC1 SC27/WG5からのインプットとレビューが必要ということになり、2018年11月のモスクワ会議から、JWG4が発足し、そちらに移管されている。現在WG2で議論されているのは、以下のTRとStudyだけである。

- ISO TR 23576: Security management of digital asset custodians
  コインチェック事件などを受けて、2018年5月のロンドン会議で提案されて承認されたTechnical Report.
  いわゆる仮想通貨交換取引所を含む、カストディ機能を持ったエンティティのセキュリティのプラクティスをTRとして策定。現在TR2のコメントを受付中。

- Study: Security_Evaluation_of_Consensus_Models
  ブロックチェーンで用いられるProof of Workなどの合意アルゴリズムのセキュリティの関する研究をするStudy Period.

WG3: Smart contracts and their applications

WG3は、Smart Contracts and their applicationというタイトルで、スマートコントラクトに関する文書を作成するWGである。SG5から引き継いでいる。 現在、Technical Reportとして、"Overview of and interactions between Smart Contracts in blockchain and DLT systems"のPreliminary Versionを作成中である。このTRでは、スマートコントラクの概要、その動作と運用、そして効用が書かれるとともに、複数のスマートコントラクトの間の連携についても議論される予定である。このTRには技術的観点と法的観点の両方が含まれる。 さらに、Technical Specificationとして、"legally binding smart contracts"を作成する。このTSは、法的拘束力をもつスマートコントラクトを構成するための、モデル、構成要素、構造とワークフローについて定義を行うことを目指している。 また、このWGのスコープとして、サプライチェーンと貿易金融に関する検討も含まれている。共に、WDフェーズである。

JWG4: Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques

- ISO TR 23244 Overview of privacy and PII protection
  BlockhainとDLTを使った際のプライバシとPII（Persinally Identifiable Information）の保護に関する文書である。現在、関連する31の単語の定義を行っている。また、フレームワークの検討に当たっては、ISO/IEC JTC1/SC27 WG5 SD2（Official Privacy Documents References）や既存のISOの標準を参照している。その上で、BlockchainとDLTに特有の課題、BlockchainとDLTにおけるプライバシ情報の取り扱い方法についての記述と、利用可能なPrivacy Enhancing Technologyの記述を行っている。DTR投票の結果出版がApproveされた。

- ISO TR 23245 Security risks and vulnerabilities
  セキュリティ上のリスクと脆弱性に関する現状を提供する文書である。内容としては、BlockchainやDLTについて、参照アーキテクチャのリスク分析や、現状指摘されている攻撃、関連する既存の標準等が記載されている。DTR投票でapproveされ、DTR投票のコメントを反映した後出版することになった。また、次回会合から新しい改版が行われる予定で、revisionが開始されている。

- ISO TR 23246 Overview of identity
  BlockchainとDLTに関連するIdentityに関する整理を行う文書であったが、進捗が思わしくないためプロジェクトがキャンセルになった。

- New TR on overview of existing DLT systems for identity management
  TR23246のキャンセルに伴い、新しいスコープで、既存の分散台帳システムのIdentity管

理への応用についてのTechnical Reportの作成が、ハイデラバード会合で決議された。現在、Call for Contributionsが行われている。

WG5: Governance

Governanceに関する検討は、東京会合の結果新しく新設されたStudy Groupで始められ、"Governance of blockchain and distributed ledger technology systems"というタイトルがつけられている。元となる議論は、ISO/IEC 38500:2015のGovernance of IT for the organizationと、ISO/IEC 38505:2017のIT Governance of Data - Part 1 : Application of ISO/IEC 38500 to the Governance of Dataが下敷きになる方向である。そのため、ISO/TC 309 - Governance of organization、ISO/IEC JTC 1/SC 40 IT Service Management and IT Governanceとリエゾンを組むことがきめられた。ロンドン会合の結果、WG5が作られることになった。現在、ISO TS 23635 "Guidelines for governance"を作成中であり、WD段階である。

WG6: Use Cases

ユースケースに関するStudy Groupであり、昨年までSG2であったが、Working Groupになった。収集されたユーケースとして、ヘルスケアデータ、相続手続き、証券、スマートコントラクトによるエネルギー取引、データのアカウンタビリティと典拠の追跡、そして登記が挙げられている。また、検討の対象とされたビジネスドメインとしては、IDマネジメント、金融、ヘルスケア、製造、知的財産管理、IoT、サプライチェーンと在庫管理、エネルギー、政府と公共セクター、不動産、税金と関税が挙げられており、アプリケーションの種類としては、資産管理、トランザクションの公証とタイムスタンプ、電子的証明の保管と追跡、そしてスマートコントラクトが挙げられている。その他、SG2では、ユースケースを記述するテンプレートを作成している。この結果をISO TR 3242としてTechnical Reportとしてまとめてお理、現在CD段階である。

SG7: Interoperability of blockchain and distributed ledger technology systems

SG7は、東京会合の結果新しく新設されたStudy Groupで、"Interoperability of blockchain and distributed ledger technology systems"というタイトルがつけられている。WG1（SG1）で議論している参照アーキテクチャに書かれているInteroperabilityについての検討を行う。ISO 19941の記述を下敷きに、以下の5つの領域についての検討を行う予定である。

1. Policy, trust and Organization
2. Transport
3. Data syntactics

4. Data semantics

5. Behavioral Semantics

N150 参照アーキテクチャドラフト、N117 ガバナンスベース文書、N119 ガバナンスに関するデンマーク寄書、N120 UKによる寄書をレビューするとともに、ISO/IEC 19941 Cloud Computing Interoperability & Portabilityと、将来の寄書をレビューしている。ハイデラバード会合の結果、Interoperability FrameworkのNWIPを最終化するために、2020年6月までの延長が決議されている。

新規グループの開設

分散台帳に基づくシステムを監査するためのフレームワークとガイダンスについての議論を行うために、新しくAdhoc Group（AHG2）の開設が決議され、Preliminary Work Itemが作られた。

今後の予定

TC307の将来の国際会議は以下のように予定されているが、COVID-19のためキプロス会合はキャンセルされた。また、ISO/IEC JTC1 SC27と合同で行われるJWG4についても、SC27のサンクトペテルスブルグ会合が同じ理由でキャンセルされた。オンラインを含めて、今後の会議がどのように行われるかは、本報告書の執筆時点では未定である。

- 2020年11月：シンガポール
- 2021年5月：ジャマイカ

マルチステークホルダーガバナンスに向けた動き

背景

ビットコインに端を発したパーミッションレスブロックチェーンは、特定の運営主体が存在しないことから、金融規制当局にとって規制の対象組織が存在しないという大きな問題がある。例えば、ビットコインのソフトウエアは、Bitcoin Coreと呼ばれるオープンソースのスタイルを取る開発者のコミュニティによって開発されているが、特定の法人格をもったり、契約関係があるわけではないため、ソフトウエアの動作と運営について責任を追う主体にはならない。また、ビットコインの論文が、Cipher Punkメーリングリスト上に査読なしに公開されたように、草の根の開発者が作成し、公開され、デプロイしたソフトウエアによって、自由に新たらしい金融のための情報システムができるようになった。通常であれば、金融機関が新しいサービスを開始する場合には、金融規制当局との対話や交渉の末、許可されたシステムのみが稼働することができたが、ビットコイン以降ではその秩序が通用しくなってしまった。これは、規制当局の従来の規制の手段が及びにくくなっているという問題である。

一方で、パーミッションレスブロックチェーンに基づく分散金融は、金融当局が実現したい規制の目標の達成を困難にしている。ここで言う規制の目標は、金融安定、金融犯罪の防止、そして消費者（投資家）保護である。金融安定という意味では、前述のFacebook Libra以前は、いわゆる暗号資産の流通量が法定通貨の流通量に比べて極めて小さかったためあまり問題にはされなかったが、Facebook Libraの登場により、ブロックチェーンが金融安定に与える影響が無視できなくなってきている。金融犯罪の防止という観点では、特に匿名性を提供するような暗号資産においてはマネーロンダリングのための道具として利用されたり、テロリストへの資金提供の道具になる可能性がある。そして、消費者保護の観点では、暗号資産取引所における暗号資産の流失であったり、実態のないICOプロジェクトへの投資勧誘などが発生している。パーミッションレスブロックチェーンの登場により、規制の目標が達成できない新しいケースが登場している。

以上より、ここの規制目標において達成のハードル上がっているという状況と、規制のエンフォースメントができなくなるという2つの面に置いて、規制当局にとっては新たな規制の形を模索する必要性が出てきている。

ここで注目されているのが、マルチステークホルダー型のガバナンスである。これは共同規制とも呼ばれ、エコシステムに関係する全てのステークホルダーによる合意に基づいてガバナンスを決めていくという考え方である。インターネットにおいては、技術と運用の標準はInternet Engineering Task Force（IETF）で合意が図られ、IPアドレスやドメイン名などのリソースについてはInternet Corporation for Assigned Names and Numbers（ICANN）が管理をしている。その両者の運営のための法人としてInternet Society(ISOC)が存在する。ISOCやICANNは非営利団体であり、ICANNやIETFへの参加は全て個人の資格で行われており、政府機関であったとしてもステークホルダーの1つにすぎない。

パーミッションレスブロックチェーンにおけるステークホルダーは大きく分けて4つ存在する。

- オープンソース型の開発を行うエンジニア
- 金融規制当局
- ブロックチェーンを利用したビジネスの主体
- 消費者

これらのステークホルダー間の協力は必ずしも良好ではない。Bitcoin Coreなどのエンジニアはもともと政府による監視に反対するCipher Punksなどを源流としており、政府や規制当局と対話をもつインセンティブがない。規制当局とエンジニアが対話をするチャネルはほとんどない状態であり、さらに両者の間では言葉が合わないことが多い。ビジネスサイドは、規制当局からの過剰な規制を受けたくなく、なるべく規制は減らすことを要望する一方で、ビジネス上の事情から技術や規制が成熟する前にビジネスを開始したいと考える。このスピードについていくのが難しくなっている。そして、消費者保保護の観点では、消費者に提供される金融サービスには透明性が求められるが、数多くの詐欺的なICOプロジェクトに見られるように、ブロックチェーンのプロジェクトの多くは第三者による検証に耐えられないレベルのホワイトペーパーで資金を集めるケースが多く、仮にプログラムコードがGitHubで公開されていたとし

ても、その正当性を検証できる人はほとんどいないのが現状だ。ステークホルダー間の協調が極めて不足していると言える。

FSBレポートとG20

上述の背景から、G20の配下の組織であるFinancial Stability Board（FSB）は、2020年6月に福岡で行われたG20財務大臣中央銀行総裁会合への提出資料として、6月6日にReport on Decentralized Financeを公開した。このレポートでは、分散金融の普及による金融規制への影響を広汎に議論しているが、レポートの多くの部分を割いて、分散金融における規制とガバナンスのあり方について記述している。とりわけ、前述の背景に述べたように、パーミッションレスブロックチェーンと分散金融の普及により、規制のあり方に変更が迫られることを記述した上で、同じくグローバルで許可のいらないネットワークとして発展してきたインターネットのガバナンスが整備される過程を細かく研究し、インターネットと同様の、マルチステークホルダー型のガバナンスの必要性を記述している。

このレポートを受けて、G20における金融革新に関するハイレベルセミナーにおいて、全てのステークホルダーを集めて、マルチステークホルダーガバナンスの必要性についての議論が行われ、マルチステークホルダーガバナンスの有効性が確認された。このセミナーにおけるパネルディスカッションの登壇者は以下の通りである。

- 村井純（慶應義塾大学教授・モデレータ）
- Klass Knot (President, De Nederlandsche Bank, and Vice Chair, Financial Stability Board)
- Adam Back（Co-founder and CEO, Blockstream）
- 松尾真一郎（ジョージタウン大学研究教授）
- Brad Carr（Senior Director, Digital Finance, Institute of International Finance）

このパネルディスカッションの結論を受けて、G20財務大臣・中央銀行総裁会合で、分散金融におけるガバナンスについての議論も行われ、コミュニケに以下が明記された。

「13.　暗号資産の基礎となるものを含む技術革新は、金融システム及びより広く経済に重要な便益をもたらし得る。暗号資産は、現時点でグローバル金融システムの安定に脅威をもたらしていないが、我々は、消費者及び投資家保護、マネーロンダリング及びテロ資金供与への対策に関するものを含め、リスクに引き続き警戒を続ける。我々は、マネーロンダリング及びテロ資金供与への対策のため、最近改訂された、仮想資産や関連業者に対する金融活動作業部会（FATF）基準を適用するというコミットメントを再確認する。我々は、FATFが今月の会合にて、解釈ノート及びガイダンスを採択することを期待する。我々は、消費者及び投資家保護や市場の健全性に関し、暗号資産取引プラットフォームについてのIOSCOの報告書を歓迎する。我々は、FSBの暗号資産当局者台帳や、暗号資産における現在の取組、規制アプローチ、及び潜在的なギャップに関する報告書を歓迎する。我々は、FSBと基準設定主体に対して、リスクを監視し、必要に応じ追加的な多国間での対応にかかる作業を検討することを要請する。我々はまた、分散型金融技術、それが金融安定性や規制、ガバナンスにもたらす潜在的な影響、及び当局が広範なステークホルダーとの対話をどのように強化できるかについてのFSBの報告書を歓迎する。我々は、サイバーの強靭性を高める努力を強化し続けるとともに、サイバー攻撃

への対応や復旧のための効果的な取組を明らかにするFSBのイニシアティブの進捗を歓迎する。」

規制当局がマルチステークホルダー型のガバナンスを導入し、1ステークホルダーとなるということは、規制権限を一部手放すことになるため、通常起こりにくことであるが、政府と規制当局のグループであるG20でこのような合意がなされたことは、歴史的である・

Blockchain Global Governance Networkの設立

G20のハイレベルセミナーにおいて、ステークホルダー間の対話を促進するための舞台として、中立なアカデミアのグループを活用することが議論された。これを、受けて14カ国、34の大学のブロックチェーン研究ネットワークであるBSafe.networkが中心となり、各国でマルチステークホルダーによる予備議論のワークショップが行われた。これは、ブロックチェーンに関するイベントが各地で行われるのに合わせて、各国のエンジニア、規制当局、ビジネスセクター、そしてアカデミアなどのステークホルダーを集めて共通の話題を、アンカンファレンス形式で議論するものである。主に、Identity、プライバシ、鍵管理、FATF Travel Ruleなど、現在規制当局とビジネスセクターで議論となっているテーマが取り上げられた。行われたワークショップの一覧は以下の通りである。

- June 13, 2019, G20 meets G-20 Vancouver, Canada
- September 3, Fin/sum Tokyo, Japan
- September 8, Decentralized Finance Architecture Tel Aviv, Israel
- November 11, Security Standardization Research London, UK
- November 12, Multi-stakeholder Workshop for Financial Diversity Dublin, Ireland
- February 14, 2020 CoDeFi 2020 Kota Kinabaru, Malarysia
- February 18, 2020 Stanford Blockchain Conference Palo Alto, USA
- February 26, 2020 Workshop at Cardozo Law New York, USA

これらの議論を経て、インターネットにおけるIETFやICANNのようなマルチステークホルダーによる会議体設立の機運が高まり、2020年3月10日に行われたBlockchain Global Governance Conference (BG2C)の特別セッションにおいて、この会議体であるBlockchain Governance Initiative Network (BGIN)の設立が発表された。この会議体の詳細は、これからオープンな議論の上決められる予定である。BGINは、バックグラウンド、地域、性別など、様々な面で多様性とバランスが考慮された23人の発起人によって立ち上げられた。発起人の一覧は以下の通りである。

- Julien Bringer (Kallistech)
- Brad Carr (Institute of International Finance)
- Michele Finck (Max Planck Institute for Innovation)
- Joaquin Garcia-Alfaro (Institut Mines-Télécom / Institut Polytechnique de Paris)
- Byron Gibson (Stanford Center for Blockchain Research)
- Hui Li (Huobi Blockchain Academy)
- Philip Martin (Coinbase)

- Shin’ichiro Matsuo (BSafe.network / Georgetown University)
- Jumpei Miwa (Financial Services Agency, JAPAN)
- Katharina Pistor (Columbia Law School)
- Nii Quaynor (Ghana Dot Com Ltd)
- Jeremy Rubin (Bitcoin Core Engineer)
- Danny Ryan (Ethereum Foundation)
- David Ripley (Kraken)
- Nat Sakimura (OpenID Foundation)
- Kazue Sako (Sovrin Foundation)
- Mai Santamaria (Ireland Department of Finance)
- Yuji Suga (CGTF)
- Shigeya Suzuki (BSafe.network / Keio University / WIDE Project / BASE alliance)
- Yuta Takanashi (Financial Services Agency, JAPAN / ex-Georgetown University)
- Robert Wardrop (Cambridge Center for Alternative Finance)
- Pindar Wong (VeriFi (Hong Kong) Limited)
- Aaron Wright (Cardozo Law School)

BGINのホームページには、概要の資料、およびManifestoとToRの作成のためのGitHubレポジトリへのリンクが存在する。BGIN全体のActing co-chairには、Mai Santamaria（アイルランド財務省）と松尾真一郎（ジョージタウン大学）が就任し、BGINそのもののガバナンスを議論するワーキンググループ（acting co-chairs: Aaron Wright（Cardozo Law School）、鈴木茂哉（慶應義塾大学））、Identity/privacy/key managementの活動項目を議論するスタディグループ（acting co-chairs: Katharina Pistor（コロンビア大学）、崎村夏彦（OpenID Foundation））が就任する。本格的な活動は2020年秋以降に予定されている。

日本国内での取り組み

CGTF (Cryptoasset Governance Task Force)

コインチェックによる暗号資産の流出事件が2018年1月に発生したことを契機に、仮想通貨交換取引所のセキュリティ確保とガバナンスの確立が急務となった。これを受けて、日本のセキュリティ専門家と一部のブロックチェーン事業者の有志で、任意団体VCGTF（Virtual Currency Governance Task Force）が設立された。その後、金融庁の「仮想通貨交換業等に関する研究会」において、仮想通貨の代わりに暗号通貨という新しい呼称を用いる方針となったため、この任意団体の名称はCGTF（Cryptoasset Governance Task Force）に変更となった。金融庁は、仮想通貨交換取引所について、業界団体などによる自主規制を行う方針を取っている。一方で、仮想通貨交換取引所、およびブロックチェーン事業者としての業界団体が複数設立され、自主規制団体としてまとまった意思決定や行動ができる状態になっておらず、公式な自主規制の方針や基準ができないまま、コインチェックによる事件が発生した。公式な自主規制団体の設立と自主規制基準の作成が遅れたことが、仮想通貨交換取引所におけるインシデントの発生の可能性を高めたとも言える。

そのため、VCGTFが設立された当初は自主規制団体が存在しなかったが、将来、自主規制団体が設立されることを想定して、自主規制団体におけるセキュリティの基準として参照される文書を作成すること、必要によっては金融庁などに直接参照される文書を作成することがCGTFの目標である。

CGTFでは、主に仮想通貨交換取引所が、ISMS（ISO/IEC 27000シリーズ）に準拠したセキュリティマネジメントプロセスを実施することができるように、同標準に基づいたセキュリティ確保のためのプラクティスを記述した文書を作成している。その他に、暗号資産に関わる用語の定義を行う文書、ブロックチェーンシステムで使用しているウォレットに関する調査報告書を作成している。

仮想通貨交換所のセキュリティ対策についての考え方

この文書は、仮想通貨交換取引所のセキュリティマネジメントについて、ISO/IEC 27002で規定されたフォーマットに従い、仮想通貨交換所システムのリスク分析を行い、セキュリティ対策のプラクティスをまとめている。現状、仮想通貨交換所のシステムについては、共通のアーキテクチャなどは存在せず、各事業者が自己流でシステムの設計、構築、運用を行なっている。そのため、この文書の作成に当たっては、可能な限りのブロックチェーン事業者からヒアリングを行い、システムのモデル化を行なった上で検討している。そのため、その他の仮想通貨交換所のシステムのセキュリティをカバーするためには、追加のヒアリング等が必要である。

この文書は、IETFのInternet Draft（I-D）として公開されている。またこの文書は、ISO TR23576（Security management of Digital Asset Custodians）にも入力されている。

- [IETF] General Security Considerations for Cryptoassets Custodians, https://datatracker.ietf.org/doc/draft-vcgtf-crypto-assets-security-considerations/
- [ISO TR23576] Blockchain and distributed ledger technologies -- Security management of digital asset custodians, https://www.iso.org/standard/76072.html

Terminology for Cryptoassets

この文書は、仮想通貨（暗号資産）の技術文書を作成するにあたり、必要な用語の定義を行うために作られている。

この文書は、IETFのInternet Draft（I-D）として公開されている。

- [IETF] Terminology for Cryptoassets, https://tools.ietf.org/html/draft-nakajima-crypto-asset-terminology-01

暗号資産の署名鍵を取り扱うサービスに関する調査

この文書は、暗号資産に関する内閣府令の改正のパブリックコメント対応に泡sて、暗号資産

における署名鍵の管理の実態調査を行い類型化したものである。

- 栗田 青陽, 暗号資産の署名鍵を取り扱うサービスに関する調査, https://cgtf.github.io/publications/20191216/dp2019-02/dp2019-02.pdf

CGTFの詳細について、https://vcgtf.github.io から参照することができる。

その他の動向

標準化団体

ITU-T

ITU-Tでは、Focus Gruopとして、2017年5月にFocus Group on Application of Distributed Ledger Technologyが設立された。このFGは、Telecommunication Standardization Advisory Group (TSAG)の中に作られている。
　このFGの目的としては、以下の3つが挙げられている。

- DLTを利用した応用とサービスを特定し分析する
- 上記のアプリケーションとサービスをグローバル規模で実装するためのベストプラクティスとガイダンスを記述する
- ITU-TにあるStudy Groupにおける関連する標準化作業における今後の進め方を提案する
  　その上で、相互互換性をもったDLTを用いたサービスのための標準化のロードマップを作成するとしている。
  　Terms of Referenceによると、FG DLTは、関係するステークホルダーのための、知見、ベストプラクティス、標準化フレームワークを定めることに資する知見などを集める、オープンプラットフォームになることを目指している。ここでのステークホルダーとは、通信に関する規制当局、金融に関する規制当局、サービスプロバイダ、プラットフォームプロバイダ、ネットワーク事業者、国際機関、産業界のフォーラムやコンソーシアムである。取り扱う項目の例として、ユースケースとアプリケーション、実装上の要求事項、規制と政策の観点、その他が挙げられている。
  　また、Terms of Referenceに記述されているこのFGのObjectiveは以下の通りである。
- DLTに関する標準化活動に貢献できる他の組織とのリエゾンと関係の確立
- DLTを利用した応用とサービスのためのエコシステムを記述し、このエコシステムにおけるステークホルダーの役割と責任を明らかにする
- DLTを利用した応用とサービスの実装のためのユースケースを明らかにする
- 将来のITU-Tの検討課題とTU-T内のStudy Groupにおけるアクションを示すこと
  - DLTを利用したサービスのコンセプト、範囲、ビジョン、およびユースケース

    - DLTを利用したサービスの性質と要求事項
    - DLTを利用したサービスのアーキテクチャフレームワークと通信技術
    - DLTの現状分析、評価と成熟度
    - DLTを利用した応用とサービスに関連するセキュリティとプライバシの面の検討
    - ブロックチェーンの応用を進めるエンタープライズと複数の産業や経済セクタの規制当局の間での、ブロックチェーンによって生じる政策と規制に関する意味の議論のプラットフォームの提供
    - SG17が将来協力できるステークホルダーの特定と将来の方向性

活動の結果、以下のドキュメントが公開されている。その上で、2019年の8月を持って活動を停止している。

- Technical Specification FG DLT D1.1 DLT terms and definitions
- Technical Report FG DLT D1.2 DLT overview, concepts, ecosystem
- Technical Report FG DLT D1.3 DLT standardization landscape
- Technical Report FG DLT D2.1 DLT use cases PDF
- Technical Specification FG DLT D3.1 DLT reference architecture
- Technical Specification FG DLT D3.3 Assessment criteria for DLT platforms
- Technical Report FG DLT D4.1 DLT regulatory framework
- Technical Report FG DLT D5.1 Outlook on DLTs

IETF

IETFでは、直接ブロックチェーンに関連する標準化アイテムがあるわけではないが、現在IRTFにおいて、Decentralized Internet Infrastructure Proposed RG (dinrg)というResearch Groupが構成されている。これ以前に、当初Blockchain, Distributed Data & Service Federationという形で提案され、IETF99（1017年7月17日　プラハでで行われたBoF meetingにおいて議論されている。2017年9月21日に、このResearch Groupの設立が提案され、Charterが同11月11日に承認された上でGroupが設立された。Charterの主な内容は以下の通りである。

- トラストマネジメント、IDマネジメント、名前解決、資源オーナーシップマネジメント、リソース発見などのインターネットのインフラサービスの非中央集権化のための研究を行う。
- ユースケースと分散した状態で実装する際の要求事項を検討する
- スケーラビリティ、性能、セキュリティなどのインターネットレベルでのデプロイメントの問題
- 技術的解決とベストプラクティスのドキュメント化
- スケーラビリティの問題と、かけているコンポーネントの示すためのツールと指標の作成
- IETFにおける将来の課題の定時
- 技術と解決方法について中立

以下の項目がResearch Challengeとして挙げられている。

- スケーラビリティ
- 非中央集権的な通信環境におけるトラストマネジメント
- プライバシと、目的に限定した検証可能な開示
- 分散台帳と関連技術の、異なるユースケースと環境における適用可能性
- インターネットインフラしストラクチャに関する特定のシナリオにおけるコンセンサスアルゴリズム
- 合意すべき情報を完全な格納したり処理できないノードの可能性と取り扱い
- 分散化されたトラストと代理コンピューティング
- 非中央集権的なネットワークインフラストラクチャのための経済的ドライバ
- 技術に対する共通的な要求と性質の特定
- 1つあるいはそれ以上の共通目的のためのインフラシステムのデザインと実装
- 1つあるいはそれ以上の実装のデプロイと運用

基本的には、Blockchainそのものをとりあげるというよりも、ネットワークインフラストラクチャにフォーカスを当てており、Blockchainの要素技術や考え方をインターネットのアーキテクチャに取り込む方法や考え方について、検討を行うことを目的としている。
2019年3月27日の会合では、Transport Issues for End-System Multicast and Message Propagation in Distributed Ledger Technologiesで、P2Pマルチキャストを使った台帳データの送信についての議論が行われた。また、2019年7月24日の会合では、以下の項目が議論された。

- Leandro Navarro MeshDApp: Blockchain-enabled Crowdsourced Internet Access Platform for Mesh Networks" （スマートコントラクトのメッシュネットワーク管理への応用）
- Shen Yan, "A Blockchain based Testbed for BGP Verification" （DII（分散インターネットインフラ）によるBGPの検証のためのブロックチェーンの応用）
- Lixia Zhang, "Decentralization: from the ground up"（Named Data Networkingの提案）

ITEF106(2020年3月)でのセッションは、コロナウイルスによる遠隔開催への以降のため行われないことになった。

W3C

World Wide Web Consortium (W3C)は、Web技術に関する標準を議論するコンソーシアムである。多くの場合、Webブラウザに影響のある技術領域や技術仕様についての議論が行われる。
W3Cでは、ブロックチェーン技術に関連して、BLOCKCHAIN COMMUNITY GROUP（Blockchain CG）が設立されている。ブロックチェーン技術そのものは、データやトランザクションの取り扱いに関する基盤的な技術であるため、直接Webブラウザに関係する領域は多くないと考えられるが、Web技術全体として考えたときに、Webアクセスとブロックチェーン上の情報のやり取りにおいて、フォーマット等の標準化が必要になると考えられる。
Blockchain CGの主なISO20022をベースにメッセージフォーマットを決めることと、torrent, パブリックブロックチェーン、プライベートブロックチェーン、サイドチェーン、CDNなどにおけるストレージ利用のガイドラインなどを議論することである。

W3Cでは、さらにW3C Decentralized Identifier (DID) Working Groupが作られた。目的は、Distributed IDにおけるURIのスキーム、DIDのドキュメントにおけるデータモデルとsyntax、DIDのスペックのための要求条件を議論することである。

DIDワーキンググループのWebページ：
https://www.w3.org/2019/did-wg/

OECD BEPAB

OECDは、OECDの目的であるグローバルなポリシーの策定の一環として、ブロックチェーンのエコシステムとその応用についての議論を、OECD Blockchain Policy Centerの設立、および年次のGlobal Blockchain Policy Forumを開催している。そして、2019年のGlobal Blockchain Policy Forumの後に、OECDとしてのブロックチェーンに関する原則（Principle）を策定するために、Blockchain Expert Policy Advisory Board (BEPAB)を組織した。2019年から対面、非対面の会合を5回行い、2020年の夏頃に、原則の文案を公開する予定である。

PEPABのメンバーは　https://www.oecd.org/daf/blockchain/OECD-Blockchain-Expert-Policy-Advisory-Board-List-of-Participants.pdf　から参照できる。
日本からは、松尾真一郎（ジョージタウン大学）、吉田明彦（金融庁）が参加している。

学術会議の動向

Financial Cryptography 2020

Financial Cryptography 2020は、2020年2月10日から14日まで、マレーシアのコタキナバルで開催された。昨年より、併催のBitcoin WorkshopがFinancial Cryptographyにマージする形となった。今夏は、併催のワークショップとして、ブロックチェーンに関連するところでは4th Workshop on Trusted Smart Contractsと、1st Workshop on Coordination of Decentralized Financeが行われた。今回も、セッションと論文の過半数がブロックチェーンに関連するもので、Financial Cryptographyのビジネスミーティングでは、発表分野の多様性についても議論が起こった。次回以降、プログラムの割合として何らかの配慮があるのは現時点では不明である。

ブロックチェーンに関するセッションと論文は以下の通りである。

Session 2: Attacks

Session Chair: Ross Anderson

- Leveraging Bitcoin Testnet for Bidirectional Botnet Command and Control Systems. Federico Franzoni (Universitat Pompeu Fabra), Vanesa Daza (Universitat Pompeu Fabra),

Iván Abellán (Universitat Pompeu Fabra)

- Security Analysis on dBFT protocol of NEO. Qin Wang (Swinburne University of Technology), Jiangshan Yu (Monash University), Zhiniang Peng (Qihoo 360 Core Security), Vancuong Bui (Swinburne University of Technology), Shiping Chen (Csiro, Data61), Yong Ding (Cyberspace Security Research Center), Yang Xiang (Swinburne University of Technology)

Session 3: Consensus

Session Chair: Stefanie Roos

- Selfish Mining Re-Examined. Kevin Alarcón Negy (Cornell University), Peter R. Rizun (Bitcoin Unlimited), Emin Gün Sirer (Cornell University)

- Fairness and Efficiency in DAG-based Cryptocurrencies. Georgios Birmpas (University of Oxford), Elias Koutsoupias (University of Oxford), Philip Lazos (Sapienza University of Rome), Francisco J. Marmolejo Cossío (University of Oxford)

- Stake Shift in Major Cryptocurrencies: An Empirical Study. Rainer Stütz (Austrian Institute of Technology), Peter Gaži (IOHK), Bernhard Haslhofer (Austrian Institute of Technology), Jacob Illium (Chainalysis)

- Coded Merkle Tree: Solving Data Availability Attacks in Blockchains. Mingchao Yu (University of Southern California), Saeid Sahraei (University of Southern California), Songze Li, Salman Avestimehr (University of Southern California), Sreeram Kannan (University of Washington), Pramod Viswanath (University of Illinois at Urbana-Champaign)

Session 4: Cryptoeconomics

Session Chair: Roger Wattenhofer

- Decentralized Privacy-Preserving Netting Protocol on Blockchain for Payment Systems. Shengjiao Cao (Ant Financial), Yuan Yuan (Ant Financial), Angelo De Caro (IBM Research), Karthik Nandakumar (IBM Research), Kaoutar Elkhiyaoui (IBM Research), Yanyan Hu (IBM Research)

- The Arwen Trading Protocols. Ethan Heilman (Boston University/Arwen), Sebastien Lipmann (Arwen), Sharon Goldberg (Boston University/Arwen)

- SoK: A Classification Framework for Stablecoin Designs. Amani Moin (Cornell University), Kevin Sekniqi (Cornell University), Emin Gün Sirer (Cornell University)

Session 5: Layer 2

Session Chair: Andrew Miller

- SoK: Layer-Two Blockchain Protocols. Lewis Gudgeon (Imperial College London), Pedro Moreno-Sanchez (TU Wein), Stefanie Roos (TU Delft), Patrick McCorry (PISA Research), Arthur Gervais (Imperial College London)

- MicroCash: Practical Concurrent Processing of Micropayments. Ghada Almashaqbeh (Columbia), Allison Bishop (Proof of Trading and Columbia), Justin Cappos (New York University)

- LockDown: Balance Availability Attack against Lightning Network Channels. Cristina Pérez-Solà (Universitat Oberta de Catalunya), Alejandro Ranchal-Pedrosa (University of Sydney), Jordi Herrera-Joancomarti (Universitat Autònoma de Barcelona), Guillermo Navarro-Arribas (Universitat Autònoma de Barcelona), Joaquin Garcia-Alfaro (Institut Polytechnique de Paris)

- Ride the Lightning: The Game Theory of Payment Channels. Zeta Avarikioti (ETH Zurich), Lioba Heimbach (ETH Zurich), Yuyi Wang (ETH Zurich), Roger Wattenhofer (ETH Zurich)

Session 6: Layer 2, Part Deux

Session Chair: Patrick McCorry

- How to profit from payments channels. Oguzhan Ersoy (Delft University of Technology), Stefanie Roos (Delft University of Technology), Zekeriya Erkin (Delft University of Technology)

- Boomerang: Redundancy Improves Latency and Throughput in Payment Networks. Joachim Neu (Stanford University), Vivek Bagaria (Stanford University), David Tse (Stanford University)

- DLSAG: Non-Interactive Refund Transactions For Interoperable Payment Channels in Monero. Pedro Moreno-Sanchez (TU Wien), Arthur Blue, Duc Le (Purdue University), Sarang Noether (Monero Research Lab), Brandon Goodell (Monero Research Lab), Aniket Kate (Purdue University)

- Cerberus Channels: Incentivizing Watchtowers for Bitcoin. Zeta Avarikioti (ETH Zurich), Orfeas Stefanos Thyfronitis Litos (University of Edinburgh), Roger Wattenhofer (ETH Zurich)

Session 8: Privacy

Session Chair: Claudia Diaz

- Zether: Towards Privacy in a Smart Contract World. Benedikt Bünz (Stanford University), Shashank Agrawal (Visa Research), Mahdi Zamani (Visa Research), Dan Boneh (Stanford University)

- An airdrop that preserves recipient privacy. Riad S. Wahby (Stanford), Dan Boneh (Stanford), Christopher Jeffrey (Purse.io), Joseph Poon (Lightning Network)

- RingCT 3.0 for Blockchain Confidential Transaction: Shorter Size and Stronger Security. Tsz Hon Yuen (The University of Hong Kong), Shi-feng Sun (Monash University), Joseph K. Liu (Monash University), Man Ho Au (Hong Kong Polytechnic University), Muhammed F. Esgin (Monash University), Qingzhao Zhang (Shanghai Jiao Tong University), Dawu Gu (Shanghai Jiao Tong University)

Session 9: Crypto Foundations

Session Chair: Sven Dietrich

- Non-Interactive Proofs of Proof-of-Work. Aggelos Kiayias (University of Edinburgh and IOHK), Andrew Miller (University of Illinois at Urbana-Champaign), Dionysis Zindros (University of Athens and IOHK)

- Proof-of-Burn. Kostis Karantias (IOHK), Aggelos Kiayias (University of Edinburgh and IOHK), Dionysis Zindros (University of Athens and IOHK)

- Non-interactive Cryptographic Timestamping based on Verifiable Delay Functions. Esteban Landerreche (CWI Amsterdam), Marc Stevens (CWI Amsterdam), Christian Schaffner (University of Amsterdam)

Session 11: Empirical Studies

Session Chair: Jens Grossklags

- Open Market or Ghost Town? The Curious Case of OpenBazaar. James E. Arps (Carnegie Mellon University), Nicolas Christin (Carnegie Mellon University)

- Exploring the Monero Peer-to-Peer Network. Tong Cao (University of Luxembourg), Jiangshan Yu (Monash University), Jérémie Decouchant (University of Luxembourg), Xiapu Luo (The Hong Kong Polytechnic University), Paulo Esteves-Veríssimo (University of Luxembourg)

- Surviving the Cryptojungle: Perception and Management of Risk Among North American

Cryptocurrency (Non)Users. Artemij Voskobojnikov (University of British Columbia), Borke Obada-Obieh (University of British Columbia), Yue Huang (University of British Columbia), Konstantin Beznosov (University of British Columbia)

Session 12: Smart Contracts

Session Chair: Jeff Burdges

- Address clustering heuristics for Ethereum. Friedhelm Victor (Technical University of Berlin)

- What are the Actual Flaws in Important Smart Contracts (and How Can We Find Them)?. Alex Groce (Northern Arizona University), Josselin Feist (Trail of Bits), Gustavo Grieco (Trail of Bits), Michael Colburn (Trail of Bits)

- Characterizing Code Clones in the Ethereum Smart Contract Ecosystem. Ningyu He (Peking University), Lei Wu (Zhejiang University), Haoyu Wang (Beijing University of Posts and Telecommunications), Yao Guo (Peking University), Xuxian Jiang (PeckShield, Inc)

- Short Paper: Smart Contracts for Government Processes Case Study and Prototype Implementation. Magnus Krogsbøll (IT University of Copenhagen), Liv Hartoft (IT University of Copenhagen), Tijs Slaats (University of Copenhagen), Søren Debois (IT University of Copenhagen)

会議用の予稿は会議のWebページからダウンロード可能である。

Scaling Bitcoin

Scaling Bitcoinは、2015年に、主にブロックチェーンのスケーラビリティ向上のための技術について、利害関係を排除し、純粋に技術的な議論をエンジニアとアカデミアが協力して行う会議としてスタートした。2019年は、イスラエルのテルアビブで、2019年9月19日、20日に行われた。

特に注目を浴びた発表は以下の通りである。

- Bandwidth-Efficient Transaction Relay for Bitcoin
  PRESENTER(s): Gleb Naumenko (Chaincode Labs), Gregory Maxwell (Independent Researcher), Pieter Wuille (Blockstream), Alexandra Fedorova, Ivan Beschastnikh (The University of British Columbia)

- BIP: OP_SECURETHEBAG
  PRESENTER(s): Jeremy Rubin (Independent Researcher)

- Applying Private Information Retrieval to Lightweight Bitcoin Clients
  PRESENTER(s): Kaihua Qin, Henryk Hadass, Arthur Gervais (Imperial College London), Joel Reardon (University of Calgary)

- PISA: Arbitration Outsourcing for State Channels
  PRESENTER(s): Patrick McCorry (PISA Research), Surya Bakshi, Andrew Miller (University of Illinois at Urbana-Champaign), Iddo Bentov (Cornell University), Sarah Meiklejohn (UCL)

Scaling Bitcoin 2020の発表スライドとビデオは、Scaling BitcoinのWebページから参照することができる。