Position Paper

SWIFT と分散型台帳技術

Delivering an industry-standard platform through community collaboration

目次

概要

ブロックチェーン技術と分散型台帳技術（DLT: Distributed Leader Technologies ）の出現以来、金融業界はこれらの技術をいかにしてビジネスに応用できるかという問いに関心を寄せてきました。当該技術の導入や適用領域の調査は、今や大手金融機関の研究開発・新規事業開発チームの注力分野であり、トランザクションビジネスやその他データ処理が中心となる業務の戦略を探る企業経営者にとっても重要な焦点となっています。

SWIFT は金融業界の協同組合として、DLT が成熟し、安定したビジネスの適用領域が形成された際に、SWIFT の 11,000 以上のメンバーに DLT を基盤としたサービスを提供するプラットフォームを確立させるために、技術力、運用力、ビジネス遂行能力の強化に注力しています。SWIFT が提供するサービスの基盤となる将来のDLTが、エンド・ツー・エンドにおけるプロセスの自動化と、従来の運用プロセスとの互換性を実現し、金融業界のニーズと期待と一致するよう、特定された要件への対応に注力しています。

DLT の普及を実現するには、業界と連携しながら標準的な DLT を開発することが望ましいのは明らかです。SWIFT は業界内の協働を推進してきた実績を生かし、独自の強み（標準化に関する比類ない見識、セキュリティにおける実績、強力なガバナンス、業務効率性、信頼性やネットワーク）を活用して、SWIFT コミュニティにメリットをもたらす優れた DLT プラットフォームを提供したいと考えています。

本書は、SWIFT がアクセンチュアとの協力のもとで実施した現在の DLT に関する綿密な評価の結果をまとめたものです。本評価では、DLT が金融業界に新たなビジネス機会をもたらし、効率化を実現する可能性を持つことが実証されました。DLT の主な強みは以下のとおりです。

- 分散型システム特有の信頼性の高さ
- 効率的な情報同報送信
- 徹底した取引履歴管理
- 照合の簡略化
- 耐障害性の高さ

ただし、本評価にて一部の DLT ソリューションは機能検証において効果が確認されたとは言え、現在の DLT は金融コミュニティの要件を満たすほど成熟していないことも実証されました。金融業界での普及を実現するにあたり、DLT が満たすべき主な要件として以下が特定されました。

- 強力なガバナンス
- データ制御
- 規制要件の遵守
- 標準化
- 本人確認体制
- セキュリティおよびサイバーディフェンス
- 信頼性
- 拡張性

評価の結論として、金融界が求める基準で DLT を導入するには、上記の各領域にて一層の研究開発が必要になります。

DLT の成功にはビジネスの標準化が不可欠です。いかなる技術であっても、複数の関係者が携わる環境では、共有データの有意性には、透明性の確保と、またその関係者による合意が必須となります。ISO　20022 を中心とする既存の標準では、業界共通のデータ定義のソースとして、また金融メッセージングシステムなどの既存技術と DLT の相互運用を実現するツールとして重要な役割を果たすことになります。

本評価では、DLT が業務上の全ての問題を解決する特効薬として見なされるべきではないという点も浮き彫りになりました。技術の主要な長所を組み合わせてビジネス上の問題を解決できるか否かを判断するために、常に想定される適用領域を評価すべきです。

SWIFT は研究開発プログラムの一環として積極的に DLT の実験を行い、コミュニティと連携して DLT がメリットをもたらす業務の特定に取り組んでいます。SWIFT Innovation Lab は、基盤技術を利用した様々なシステム体系において、DLT の機能検証を行っています。また、SWIFTはリナックス・ファウンデーション・ハイパーレッジャー・プロジェクトの理事会メンバーとして、金融業界と協働してオープンソースのブロックチェーン技術の強化と、分散型台帳の本格導入に向けた基盤構築に取り組んでいます。さらに、SWIFT はイノベーションへ向けた独自の施策である Innotribe を通じて、SWIFT メンバーとフィンテック企業の協力体制を推進しています。SWIFT は研究開発を進める上で、引き続きコミュニティとの連携を図っていきます。

SWIFT の DLT に関する取り組みの詳細については、DLT@swift.com までお問い合わせください。

現在の DLT の技術評価

SWIFT とアクセンチュアは、現在の DLT について綿密な評価を行い、現在の技術と、金融業界が新しいソリューションに求める要件を対比しました。複数分野の専門家によって構成される SWIFT の評価チームは、DLT がガバナンスやコンプライアンスに及ぼす影響に加え、DLT のセキュリティ、信頼性、耐障害性、旧システムとの互換性、標準化などの技術的側面について調査しました。なお、本調査は DLT の運用面に着目しているため、DLT に関する法的な影響は対象外となります。また、本評価は複数の金融機関における、SWIFT のサービスを利用している金融機関内の適用領域に焦点を当てています。従って、SWIFT が関与せず金融機関内で完結するような DLT アプリケーションは対象としていません。

DLT の強み

我々の分析では、DLT が金融業界に新たなビジネス機会と効率化をもたらす潜在性があることを示しています。DLT の主な強みは以下のとおりです。

- **情報伝搬：**ネットワーク全体に最新の情報が反映され、常にその状態が保たれる効率的な手段が提供されます。分散型台帳ではほぼリアルタイムにデータが更新・複製されるため、すべてのノード（各 PC やサーバー等の通信端末）は真正な同一のデータを参照、活用できます。
- **追跡可能性：**参加者、及び規制当局等の正当な信頼できる第三者機関が、全ての取引履歴を確認できます。参加者は分散型台帳に情報を追加できますが、削除ができないため、情報の改ざんは不可能になります。台帳の情報には、取引のオーナー、取引履歴、共有台帳に保管された情報のデータ系列などが含まれます。
- **照合の簡素化：**情報は相互的であり、全ての参加者がリアルタイムまたはほぼリアルタイムで同じデータを利用できることから、完全且つ検証済みのデータへのローカル・アクセスは照合プロセスを簡素化します。ネットワークの通信待ち時間（Latency）や大幅な手作業が伴う現行の照合プロセスは改善されるか、場合によっては不要になります。
- **信頼性の高い分散型システム：**中央集約型システムによるデータ管理に依存することなく、台帳上のデータの信頼性を信用することができます。取引はデジタル署名され、各ノードに個人間（P2P: Peer-to-Peer）ネットワークの参加者間で台帳を複製する専用ソフトウェアが搭載され、そのネットワーク上で分散型台帳の保守と検証が行われ、台帳の完全性が確保されます。
- **耐障害性：**システムは継続的に稼働可能であり、サービスの可用性が中央集約型システムに左右されません。処理が分散化されるため、特定参加者の端末に障害が起きた場合でも、他の参加者は業務を継続できます。台帳上のデータは拡散し、永続性を備え、安定した分散型ストレージが構築されることから、特定の端末で障害が起きた場合でも分散型台帳から取引データの復元ができます。つまりシステムは非常に強力なデータ内臓式の耐障害性を保有することになります。

現在の DLT の技術評価

金融サービス業界における DLT の適用

DLT は金融業界に多くのビジネス機会をもたらす潜在的な可能性を持っています。しかし、DLT は第三者の仲介なしに価値移転を非集中的に行う手段として、暗号通貨を交換する消費者間（C2C: Consumer-to-Consumer）マーケットから発生しています。当然ながら、代替的な価値移転手段を求める個人消費者への適用に比べ、より広範な金融業界はまったく違う要件を抱えています。本技術評価の一環として、金融界における広範な普及のために DLT が満たすべき主な要件として以下を特定しました。

- **強力なガバナンス：**様々な当事者の役割責任、ビジネス及び技術運用ルールを明確に定義するガバナンスモデル
- **データ制御：**データへのアクセス制御、データ機密性保護の有意性
- **規制要件の遵守：**規制要件（経済制裁や KYC 等）を遵守する能力
- **標準化：**ストレート・スルー・プロセッシング（STP：Straight Through Processing）、相互運用性、及び旧システムとの互換性を保証するための全ての階層における標準化
- **本人確認体制：**金融取引の責任所在及び否認防止を確保するため、関係者の本人を確認する能力
- **セキュリティーとサイバーディフェンス：**規模と複雑性が増すサイバー攻撃を検知、防止、抵抗する能力
- **信頼性：**金融サービスの業務遂行に不可欠なサポートが可能な体制
- **拡張性：**毎秒数百から数千件の取引を処理するサービスへの拡張が可能な体制

次のセクションでは、上記要件の詳細、また各要件に対する DLT の現在の成熟度を示します。業界が求める要件と現在の DLT 機能のギャップを埋めるために必要となる研究開発を確認し、本技術評価の結論を述べます。

強力なガバナンス

業界要件

あらゆる金融サービスは、そのサービスに関わる各当事者の役割や責任に加え、特定のビジネスサービスを支える、ビジネス及び技術運用ルールを明確に定義する強力なガバナンスモデルに依存しています。効果的、予測可能であり安定的な金融サービスの提供には、強力なガバナンスが不可欠です。

DLT の現状

DLT は暗号通貨から発生し、参加者主体のガバナンス・モデルを利用しています。このモデルは暗号通貨の運用においては効果的かもしれませんが、金融業界が求める信頼性、透明性、明確な責任所在の水準には達していないと SWIFT は考えています。本評価ではガバナンス関連の問題がいくつか特定されました。DLT は、誰でも取引を実行・閲覧できる完全にオープンなモデル（つまり参加許可不要の台帳）です。この特性は消費者間ビジネスにおいては望ましいかもしれませんが、SWIFT は、権限を与えられた参加者のみがサービスにアクセスできき、また事前のビジネスにおける合意や台帳の技術的制約の範囲内で参加者間の取引が行われるかどうかによってアクセスするモデルを選好します。「許可制台帳」はこのモデルの実現に向けた一歩となるものの、ユーザー権限の精緻化が、アクセス制御や参加者間取引に必要となります。

現在導入されている許可制台帳は、一般的な読取権限と書込権限、金融資産のトークン化、限定的な検証手段といった基本的な機能のみ保有しています。

今後の研究開発

金融サービスに DLT を応用するにあたり、オープンソースに対して規定の業務ルールに沿って分散型台帳を作成・運営する中央集約型モデルか、またはコンソーシアム（共同）モデルを採用すべきかについて盛んに議論されています。中央集約型モデルであれば参加者が安心する強力なガバナンスが提供される一方、コンソーシアムモデルと比べると DLT の機能が制限され、メリットが抑制されると考えられます。中央集約型モデルとコンソーシアムモデルのどちらが妥当かについては、さらなる検討が必要です。とりわけ、ガバナンスの適正水準を決定するために、規制要件対応や当局宛報告の観点からの検討が重要となります。

データ制御

業界要件

金融取引で交換されるデータの多くは機密情報です。受取人などの（個人情報保護関連法の対象となる）個人情報や、参加者の業務に関わる競争上慎重に扱うべき情報を引き出すことができる情報を含むためです。したがって、データの機密保護はあらゆる金融ソリューションの必須要件であり、権限を付与された者にのみ関連データへ排他的にアクセスする強固な制御機能が必要となります。

DLT の現状

台帳データは全ての DLT 参加者によって保有され、データはすべての参加者に同報送信されます。取引に関わる当事者は理論上は匿名になりますが、個人名や社名の代わりに匿名アドレスが利用されるため、、企業間（B2B: Business-to-Business）取引ではこの匿名性の確保が課題となる可能性があります。企業間取引では、アドレスを個人または会社と瞬時に紐付できるよう、参加者は取引相手の「匿名」アドレスを把握している必要があるため、台帳の情報がすべて可視化されることになります。

この問題の対応策は多方面から検討されていますが、基本的な機密保護要件を満たす対応策は今後さらなる取り組みが必要となります。データの暗号化は典型的な解決策ですが、次の点に留意しなければいけません。

- 複数の当事者がデータにアクセスする場合には、当事者のペアごとにキーを発行することになるため、暗号化・暗号解読キーの管理が運用上の課題となる。当事者が 2 社を超えると非実用的となる。
- データの暗号化によって取引が検証できなくなる可能性がある。取引内容が過度に暗号化されてしまうと、ネットワーク上で取引を検証できない、あるいは台帳に情報が同報送信されない可能性がある。

今後の研究開発

台帳に含めるデータ種類と参加者に送信するデータ種類をより明確に定義する必要があります。各取引の参加者にのみデータを配信する代替的なモデルを模索する必要があります。これには個人間通信などプライバシーを確実に保護するソリューションを活用することが考えられます。

「ゼロ・ナレッジ・プルーフ（ゼロ知識認証）」アルゴリズムは、取引内容を把握せずに内容を認証できるアルゴリズムであり、データのプライバシー問題への対応として現在取り組まれている有望な解決策です。

規制要件の遵守

業界要件

金融界は厳格に規制されており、規制対応に対する圧力は増大しています。すべてのソリューションは、金融機関による規制要件の遵守と、コンプライアンス業務（経済制裁や KYC に対応した取引・顧客フィルタリングなど）の遂行をサポートすることが求められるます。同時に情報の機密性と透明性を両立させることも求められています。

DLT の現状

DLT の規制要件への対応は大部分が調査未済であり、今後一層の取り組みが必要となります。今後、誰が誰を規制するかといった重大な問題についても、分散型台帳の非集中的かつグローバルな性質により、明快な回答を得るに至っていません。また、分散型台帳に既存の規制を適用すべきなのか、それとも新たな規制を策定すべきなのかもまだ不明です。この問いについては、現行の規制の枠組み（メッセージング、役割定義、プロセスなど）を引き継ぐべきだという考え方と、すべてをいったん白紙にして新たな枠組みを策定すべきだという 2 つの考え方があります。前者の考え方は、規制当局の同意を得やすいでしょう。DLT に対する関心が高まり、本番環境での適用領域が形成されるにつれ、規制当局の関心も高まるはずであり、引き続き注目すべき論点だと言えます。

今後の研究開発

分散型台帳に係る規制対応関連の研究開発については、金融機関と規制機関双方の協力が必要となります。

- 参加者は、DLT を活用することで当局への報告や監査要件対応にどのような影響があるかを理解すべきです。上記以外に注目すべき点としては、現行の規制要件に対する報告データの精度、個人情報保護の関連法に抵触しない適正なレベルでのデータの明細提供、という点です。
- 規制当局は金融業界による DLT ソリューションの検討、開発、方針策定には関与しませんが、金融サービス・プロバイダーの施策に対しては適宜意見を述べます。直近ではいくつかの規制当局が DLT に対して非常に前向きなコメントをしています。例として、最近では米商品先物取引委員会（CFTC）が分散型台帳の開発を奨励し、規制機関は技術革新を抑止するべきではないと述べています。また、DLT は規制機関の技術要件や人材スキルにも影響をもたらすことから、一部の規制機関は DLT が自らの業務に与える影響について調査し始めています。

標準化

業界要件

複数のシステム間または参加者間の STP と相互運用性を確保するために、また交換するデータを正確に解釈するためには標準化が不可欠です。相互運用性の確保のため、現在の金融業界は、国際標準化機構（ISO）、国際スワップデリバティブ協会（ISDA：デリバティブ取引の XML プロトコルである FmPL を管轄）、FPL（FIX Protocol Limited：金融情報交換プロトコルである FIX を管轄）などの標準規格に大きく依存しています。

DLT の現状

現在の DLT 環境では、通信プロトコルから、台帳データや取引データの形式、スマートコントラクトに至るまで、あらゆる階層で標準化が未整備となっています。また、DLT は、ISO、ISDA、FPL などの標準化機関からは独立して開発されてきました。標準化が不在の状況では、各分散型台帳間の相互運用は成立せず、台帳情報が市場の標準や慣行と一致しないことになります。DLT 環境と旧システムの統合は容易ではなく、例え可能であっても大掛かりな変換作業やデータのデータの充実が必要になると思われます。

DLT やスマートコントラクトの標準化に関する議論の多くは通信プロトコルにのみ焦点が当てられてきましたが、他の分野でも今後さらなる取り組みが必要となります。標準化に向けた取り組みが進むにつれ、ビジネスにおける適用領域や自動化の標準に直ぐに注目が注がれるでしょう。DLT ソリューションと既存アプリケーションとの互換性を確保するためには、現在、ISO 20022 への統合が急速に進んでいる、より広義の取引自動化の領域との統合も必要となります。

今後の研究開発

標準化に際して、根本的な問題が存在します。

- 分散型台帳はすべて標準化すべきなのか、または他の分散型台帳や旧式の台帳と十分に相互運用可能な異なる DLT ソリューションが存在しても問題ないか？ペイメント処理スピード、コスト、普及度合を最適化するため、ソリューション間でデータや取引を交換する際の要件策定が必要となる。ISO 20022 といった既存のメッセージングやリファレンスデータは、どのように再利用するのが最も良いか？
- 一定の期間において一部の金融サービス・プロバイダーのみ DLT 環境で取引の清算及び決済が可能な一方、その他技術を採用していない金融機関では旧インフラ上で取引を継続します。このような状況では、決済時間の相違により市場価格に歪みを生じさせ、市場の分断を招きます。異なる環境間の相互運用性については、オペレーションおよび規制の両観点から検討すべきです。自動実行される分散型台帳上の金融資産に埋め込んだロジックの機能に依存する金融サービス分野において、スマートコントラクトの是非が問われています。革新的な概念であり、多くの潜在的適用領域が考えられます。しかし「うまくいかなかった場合」に何が起きるのか、またその際のエラーや例外にどう対応するべきか、従来の契約に対するスマートコントラクトの法的権限の相違、スマートコントラクトのコンピューター言語の標準化等に精通するため、多大な時間と労力が必要になります。

前述のように、これまでの DLT 開発は、金融サービスの効率化をけん引する現行の標準規格とは独立して行われてきました。そのため、DLT プロセスと従来の業務プロセスの統合、新旧の DLT 環境の双方で取引される金融資産間の調整、また旧システムの廃止においても様々な問題が生じると考えられます。

本人確認体制

業界要件

特定のビジネスサービスに従事する関係者の身元を確認し、様々な参加者の活動の否認防止を確保するためには、強力な本人確認の仕組みが必要となります。当該仕組みは、システムの信頼性の確立、責任所在の明確化といった全ての権利実行に不可欠です。また、KYC（Know-Your-Customer）やコンプライアンス業務の前提条件にもなります。

DLT の現状

データの機密性に関連して、本人確認運用における問題が発生します。現在の DLT の一部では参加者は擬似匿名を利用していますが、このステータスは規制産業において利用が許されません。取引参加機関と取引を実行する社員、即ちアクセスを許可された者の本人確認がコントロールされた環境下で追跡可能である必要があります。2008 年の金融危機以来、金融業界は取引主体識別コード（LEI）に投資しており、LEI の活用も不可欠な要素となります。

また、当事者本人を特定するために DLT が使う暗号化キー管理システムは、暗号化キーの復元・失効ができない自己署名の証明書に依拠しています。そのため、以下の影響が予想されます。

- 特定の暗号化キーが特定の個人または企業と紐付くことを認証・保証する中立的な第三者がいないため、その暗号化キーがその個人または企業と紐づくという確証が得られない。
- 暗号化キーを逸失した場合には暗号化キーを復元できないため、資産所有者が確認できず、台帳上で資産が永久に凍結されることになる。
- 暗号化キーが盗難・漏洩した場合、当該キーを無効化できない。また、特定のキーが信頼できないものであり、システム上受け入れられないことを他の参加者に伝える手段がない。

今後の研究開発

暗号化キーの発行、本人確認、復元を含む運用全般について、綿密な調査が必要となります。現在の DLT 環境の構想においては、暗号化キーの無効化リストを管理し、復元機能を提供する認証機関と提携することが考えられます。なお、この認証機関は中立的な第三者機関でなければいけません。これは多くの金融機関が活用している手段であり、既存のインフラやプロセスによってサポートされており、米連邦情報処理標準規格（FIPS）レベル 2 または 3 のセキュリティ標準規格に対応し、パフォーマンス、セキュリティ、操作性において確立した利用実績が認められます。本人確認の要件対応のために、既存の枠組みの利用は自然な流れですが、DLT に利用する場合には、同様に機能を発揮させるため更なる研究開発が必要です。

セキュリティーとサイバーディフェンス

業界要件

サイバー犯罪の脅威は金融業界にとって非常に切迫したものであり、かつてない程に拡大しています。DLT ソリューションは、サイバー攻撃の標的になり得るとの前提のもと設計されるべきであり、サイバー攻撃を検知し、自らを防御できなければなりません。また、サイバー攻撃の数と複雑さが増していることから、防衛メカニズムの評価、テスト、改善を定期的に実施する必要があります。

DLT の現状

DLT はオープンシステムとして開発されていますが、取引認証と台帳更新に耐障害性アルゴリズムを用いていることで、サイバー攻撃の脅威に対して強固な仕組みになっています。当該アルゴリズムは、悪意を持つ参加者が多数存在するという前提のもと設計されています。金融界で数多く利用されている標準的な暗号アルゴリズムによって DLT ソリューションのセキュリティは確保されています。しかし、サイバー攻撃に対して現在の高水準の耐性とセキュリティを維持するには大きなコストがかかります。通常、オープンソースの分散型台帳は「プルーフ・オブ・ワーク（Proof of Work: 作業量による証明）」アルゴリズムを使用するこで、暗号解析のためにコンピューターのリソースを大量に使った参加者が台帳を更新する裏付により、高水準のセキュリティを保証しています。したがって、サイバー攻撃を実行するには同等のコンピューターの処理能力とリソースが必要となり、サイバー攻撃の経済合理性が得られない仕組みになっています。

しかし、同モデルは金融業界には適用できません。同モデルを維持するコストは大きく、導入による効果を上回ることになるからです。拡張性や通信待ち時間の問題に言及せず、システムの安全を保証する代替手段を模索すべきです。最近においては、金融業界では参加者のアクセス権限を厳しく制御し、取引認証を代替的な「合意形成アルゴリズム」に基づいて実行する、非公開かつ許可制の台帳に依存する方向性にあります。このアルゴリズムは、アクセス制御メカニズムと併用することで、同水準のセキュリティを確保しつつ、処理能力の迅速化とリソースの大幅な削減を目指すものです。

今後の研究開発

台帳は参加者に配信されるため、暗号化されていないデータを保護する責任は各参加者に委ねられます。これに伴い、台帳へのアクセス制御がある非公開台帳であってもデータ漏洩のリスクは増大します。このリスクに対応するために、データの暗号化または限定配信を通じて、一部または全データの保護を可能とする取組みが必要となります。

また、以下のシナリオの影響を確認のために、更なる研究開発が必要です。

- DLT 環境において、サーバー攻撃の構成にどのような変化があるか？
- 単一障害点（Single Point of Entry）を取り除くことで、同時並行処理 (Multiple Points of Entry) の開発は可能か？
- サイバー攻撃者は、システムを遅延または混乱させるために、大量の偽取引による攻撃を行うことで、サービス妨害を行うことは可能か？
- 分散型環境におけるサイバー攻撃の検知及び防御の問題点として、システムを保護するために特定のノードを隔離できるか？できる場合にはどのようにして隔離するか？
- 許可制の環境において、悪意のある人がハッキングまたは KYC 規定を迂回することで、新しいノードを作成するためにシステムにアクセス権限を得ることがないことを、誰が保証するのか？

信頼性

業界要件

特定の金融サービスは世界経済の金融安定化に不可欠であるため、最高水準のサービスレベルが求められます。即時グロス決済システム（RTGS）や証券集中保管機関（CSD）など、業務遂行に必要不可欠なアプリケーションをサポートするためには、非常に高い可用性と大規模障害発生時の復旧可能手段を保証するよう設計されたエンタープライズソリューションが必要となります。

99,999%

DLT の現状

分散型システムは耐障害性に優れ、データを喪失することなく障害から回復する高い能力を持ち合わせます。しかし、中央集約型システムは、通常 99%を超える、高い可用性水準を達成しています。

中央集約型システムがなければ、分散型システムのサービス可用性は各参加者のインフラの可用性に依存し、中央管理のコントロールが不在になります。可用性要件を満たす義務は各参加者に移されるので、各参加者が規定の可用性水準を満たすためのコントロールが必要になります。各参加者がソフトウェア更新を担うため、厳格なソフトウェアの開発、認定、リリース管理が必要になります。例えば、暗号通貨のソフトウェアのリリース認定管理プロセスが脆弱だったため、多数の問題が発生しました。台帳の分岐（所謂「Folk」と言われる現象）を回復するために緊急にソフトウェア修正が必要となり、その結果相互運用性や旧システムとの互換性に問題が派生しました。中央集約型システムであれば、ソフトウェア更新は中央で管理されるため、各参加者のソフトウェア更新の負担を軽減できます。

また、分散型システムの信頼性には限界があることが知られています。詐欺行為を行うユーザーの構成比がある上限を超えると、分散型システムの整合性が失われます。ネットワーク通信の問題が発生した場合、分散型システムは分断の影響を受けやすくなり、結果、参加者が互いに独立して運用する 2 つ以上のグループに分断されます（所謂「パーティション」と言われる現象）。そのような状況では、孤立した参加者の構成比がある上限値を超えると、ネットワークの通信問題が回復した際に、台帳の整合性を修復ができなくなります。

分散型システムの信頼性の限界は、ビジネスユーザーが当該事項を認識し、また上限値を超過した場合のリスクを評定し、また事業継続計画を策定できるよう、理解可能な形でサービス内容に明記される必要があります。

今後求められる研究開発

DLT を基盤としたソリューションが今後数年または数十年にわたって十分な信頼性を確保するために、情報技術基盤ライブラリー（ITIL）など業界のベストプラクティスに倣い、分散型環境向けの適切なソフトウェア管理とリリース管理方針を策定するための研究開発が必要となります。

また、重要な金融システムの障害がもたらすシステミックリスクを踏まえて、事務運用の側面からも検証が必要になります。具体的には、必須ソフトウェアの定期的な更新や、バグ・セキュリティ違反に対する緊急修正の適用をいかに徹底させるか、規則を遵守しないノードをいかに除外するか、参加者が分断された場合にどのように通知するか、ローカルにおける問題が速やかに解決され、サービス内容合意書で定義された運用が復旧された場合に、元帳からデータをいかに回復等になります。

拡張性

業界要件

毎秒数百件から数千件の取引を処理する金融システムは多数存在します。したがって、金融業界向けの DLT ソリューションは、適用領域の規模への対応が保証される必要があります。

DLT の現状

ブロックチェーンから発生した分散型台帳によるプルーフ・オブ・ワーク・アルゴリズムの利用の結果、極めて控えめな TPS（1 秒で処理される取引件数）に制限されています。同アルゴリズムによって、台帳が分岐し、参加者が違うバージョンの台帳を持つ可能性があります。通常、分岐は台帳が何度か更新されるうちに自動訂正されるますが、訂正プロセスは長く、取引が「完了」（Finality）状態になるまでにかなりの時間がかかります（一部の暗号通貨については、1 時間程度を要する）。

前述の代替的な合意形成アルゴリズムを活用することで、この 2 つ問題は解決されます。現在、ソリューションプロバイダー数社が大量取引処理の実験を行い、有望な結果を得ています。しかし、上記実験の数値は慎重に扱うべきです。本番環境では世界各地で何百人もの参加者が同時に取引を行うことから、処理能力と通信待ち時間に大きな影響を及ぼすと考えられます。現行ソリューションは、HFT（High Frequency Trading）など、高い処理能力と非常に短い通信待ち時間を要するシステムを支援できるほどの十分な安定性と拡張性はないかもしれませんが、これらの実験結果は有望なものであり、今後多数のアプリケーションへの適用が期待されます。なお、分散型台帳の基本概念のひとつとして情報の永久保存があります。取引量の増加に伴い、ストレージとネットワーク回線容量に大きな課題が生じると予想されます。

今後の研究開発

現実的かつ代表的なビジネスにおける処理能力要件に対して、様々な合意形成アルゴリズムや認証方法を評価するため研究開発を実施することが必要となります。例外シナリオや負荷の大きい状況におけるアルゴリズムの安定性を評価するために、テスト環境ではなく本番環境における諸条件のもとでテストを行う必要があります。なかでも次の項目は重点的にテストを行うべきです。

- 分散型システムの根底にある CAP 定理に対する各種 DLT システムの検証。検証を通じて、整合性、可用性、分断耐性が保証されなくなる限界値と、その限界値を超えた場合の回復方法を理解する必要がある。
- WAN 環境における DLT の動作のシミュレーション。WAN 環境ではネットワークが中断されやすく、物理的な位置とネットワーク接続状況によって各参加者の通信待ち時間に大きな差が出る可能性がある。

技術評価の結論

次ページの図にまとめているとおり、本評価では各要件への対応について有望な進展は見られるものの、金融業界が必要とする規模において DLT を適用するには、全ての領域において一層の研究開発が必要となることが判明しました。新しい DLT ソリューションプロバイダーの出現、また既存ソフトウェアの自然な成熟にも拘らず、金融機関による導入に必要な要件をすべて満たす単一の高度な DLT ソリューションは存在せず、課題も山積みされています。DLT はまだ開発の初期段階にあると言えます。DLT の機能と最適な適用領域を十分に理解するためには、さらなる研究、開発、テストが必要となります。

加えて、DLT システムと旧インフラの相互運用性、複数の参加者間での分散型台帳の相互運用性、それを実現するための規制要件、標準化において一層の研究が必要です。

本評価では、DLT が業務上の全ての問題を解決する特効薬として見なされるべきではないという点も浮き彫りになりました。技術の主要な長所を組み合わせてビジネス上の問題を解決できるか否かを判断するために、常に想定される適用領域を評価すべきです。

技術評価の結論

成熟度評価

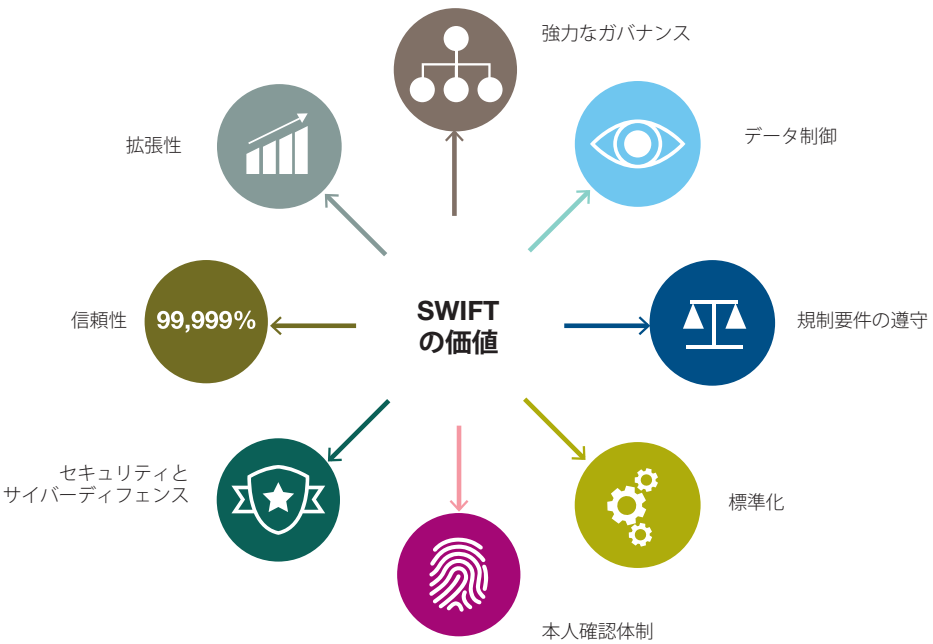
強力なガバナンス	各当事者の役割と責任および、ビジネスと技術運用ルールを明確に定義するガバナンスモデル
データ制御	データへのアクセス制御とデータの機密性を保護する機能
コンプライアンス	規制要件を遵守する機能（経済制裁、KYC対応等）
標準化	STP、相互運用性、旧システムとの互換性を確保するための、あらゆる階層における標準化
本人確認体制	金融取引の責任所在と否認防止を確保するために、関係者の本人確認を行う機能
セキュリティとサイバー攻撃対策	規模と複雑性が増すサイバー攻撃を検知、回避、防御する機能
信頼性	金融サービスの業務遂行に必要不可欠なサポートする体制
拡張性	毎秒数百から数千件の取引を処理するサービスをサポートする拡張性

- 研究は初期の段階であり、未だに対応されていない。
- 限定的対応に留まり、解決策における方向性も明確でない
- 有望な進展は見られるが、一層の研究開発が必要。
- ソリューションは存在するが、業界による評価が未済。
- 金融業界の要件を満たす。

SWIFT の強みを生かした業界標準 DLT の実現

SWIFT は金融業界の協同組合として、DLT が成熟し、安定したビジネスの適用領域が形成れた際に、SWIFT の 11,000 以上のメンバーに DLT を基盤としたサービスを提供するプラットフォームを確立させるために、技術力、運用力、ビジネス遂行能力の強化に注力しています。SWIFT が提供するサービスの基盤となる将来の DLT が、エンド・ツー・エンドにおけるプロセスの自動化と、従来の運用プロセスとの互換性を実現し、金融業界のニーズと期待と一致するよう、特定された要件への対応に注力しています。

SWIFT は 40 年間以上にわたって金融業界向けソリューションを提供してきました。そしてプロダクト・サービスを開発し提供する過程で多くの課題に対応してきました。SWIFT は強力なガバナンス、標準化に関する他に類のないノウハウ、業務の効率性、セキュリティ、信頼性、ネットワークなどの独自の価値と強みを持ち、これらを最大限に活用してコミュニティーのニーズに応えた DLT サービスを開発します。



SWIFT の強みを生かした業界標準 DLT の実現

ガバナンスとアクセス制御

金融業界の協同組合である SWIFT は、コミュニティ主導の独自のガバナンスモデルを通じて業界全体に関わる問題の解決に当たっています。SWIFT のガバナンスは利潤最大化ではなく、コミュニティに貢献するという目的意識のもとで、金融取引を促進する公共的な役割が果たせるように設計されています。SWIFT のガバナンスは、役割と責任の明確な定義、アクセスコントロールのためにサービス管理者が SWIFT ネットワークを介してサービス提供可能とし、また Closed User Group や RMA 認証を通して正式に権限が付与された参加者間の通信を規定する包括的な枠組みにより支えられています。

データ制御

SWIFT のシステムやプロセスは、コミュニティのデータの機密性が保持されるよう設計、構築、運用、保守されています。データは多階層に暗号化され、データアクセス限定のため十分に文書化された一連の方針に基づく非常に厳格なコントロールが適用されます。これらの方針への SWIFT の遵守状況は毎年外部機関によって監査され、監査結果は ISAE3000 報告書の一部として SWIFT コミュニティ向けに開示しています。

規制要件の遵守

SWIFT はコミュニティの要望に応じて、完結したコンプライアンスポートフォリオの構築に向けて大規模な投資を実施しています。コンプライアンスはすべての金融機関が共通して担う課題であり、また協働して解決に取り組む課題です。金融犯罪コンプライアンス業務への投資は競争力の強化につながらないため、各金融機関が自行のコストとリスクの削減に向けて連携することは有意義であると考えます。

標準化

SWIFT の標準化の取組は、金融業界の DLT 活用に必要な業務自動化の標準定義のために、優れた実績のある技術を結び付ける役割を果たします。SWIFT の ISO 20022 標準に関する取り組み、ビジネスの見識、様々な金融市場に関するノウハウに加え、金融業界とのリレーションシップのみならず業界団体との折衝力も含め、今日の金融業界で見られる高水準の標準化に大きく貢献してきました。

本人確認体制

SWIFT のサービスは、すべての行為に対して、本人確認、履歴管理、責任説明を保証する高度な暗号化機能を利用しています。金融機関は BIC で特定され、取引は公開鍵基盤を使ったデジタル署名は SWIFT 認証局によって認証され、各参加者は取引相手が本人であることを確認できます。暗号化キーは、安全かつ確実なプロセスにより管理され効率的にサービスを提供し、また、消失または漏洩した場合は、証明書の再発行・失効手続きを行います。

セキュリティとサイバーディフェンス

SWIFT 設立以来、セキュリティ対策は SWIFT の DNA の一部となっています。SWIFT の IP ネットワークを保護するサーバー攻撃対策メカニズムは DLT に直結し、保護された非公開の P2P ネットワークにおける参加者の安全な業務遂行に活用できます。

信頼性

SWIFT の最高水準の可用性 [1]、綿密な事業継続計画、基幹業務ソフトウェアの提供力は高く評価されています。SWIFT は業界全体の円滑な業務・システム移行を実現し、そのなかで相互運用性や旧バージョンとの互換性も確保してきました。これらのノウハウや専門知識は DLT にも利用可能であり、ソリューションプロバイダーがユーザーの信頼を得るための必須の資質と考えます。

拡張性

現在、SWIFT は様々なメッセージング・サービスを介して、ペイメント、証券取引、FX、貿易金融のといったビジネスを支えるサービスを提供し、世界中の多岐にわたる金融機関による大量のメッセージを処理しています [2]。SWIFT は最高水準の可用性を維持しつつ、金融界の要件に応じてシステムを拡張してきました。

ネットワーク及び旧システムとの統合

SWIFT の安全な IP ネットワークは金融業界では確固たる地位を保持し、これまでに 11,000 以上の金融機関が接続していることから、DLT を基盤としたサービスを安全に提供するにあたり、自然な選択と考えられます。SWIFT のメッセージングと統合されたサービスポートフォリオは、お客様の既存バックオフィスシステムとの円滑な連携を実現する様々なソリューションを提供しています。これは金融機関内で新しい DLT サービスを旧システムを連携する際に再利用できます。

業界の変革を支援

DLT の採用はビックバン的な形では実現しないと考えられます。現在旧システムが広範囲で普及していることから、DLT の採用は、技術的転換だけはなく、一定の事業変革も伴うことが想定されます。このような変革は時間がかかるものであり、すべての企業や関連団体が同じペースで変革を進めるわけではありません。したがって、長期間にわたり複数システムを同時並行で運用するコストの発生を防ぐために、一定のペースで導入を進める必要があります。

業界全体の変革の舵を取ってきた SWIFT の実績が価値を発揮します。SWIFT はこれまでに何度も技術革新の場面において円滑かつ適時にコミュニティーの移行を成功に導いてきました。SWIFT のガバナンス体系や長年にわたって構築してきたお客様やベンダーとのリレーションシップを最大限に活用した、コミュニケーション力、企画力、実行力の相乗効果による成果です。DLT への移行に際しても、同じ原則が適用できます。

1. SWIFTNet と FIN メッセージング・サービスは 2015 年に 99.999%の可用性を達成
2. 2015 年に交換された FIN メッセージは 61 億件以上

SWIFT による DLT 研究開発

SWIFT は研究開発活動の一環として、積極的に DLT の実験を行っているほか、多くのイニシアティブに取り組んでいます。

コミュニティとの連携

SWIFT は DLT により事業メリットがもたらされる可能性がある証券取引、ペイメント、貿易金融、リファレンスデータなどの各適用領域で、DLT の活用方法を模索するためにコミュニティーとの連携に積極的に資源を投入してきました。この取り組みは、主に数十社の金融機関との二者間協議を通じて進めてきました。

リナックス・ファウンデーション・ハイパーレッジャー・プロジェクト

SWIFT は、DLT の進展を目的とする当オープンソース・プロジェクトの創立メンバーかつ理事メンバーです。SWIFT はコミュニティと連携し、既存の問題や現在の導入における制約事項を克服する、本番環境レベルの DLT の基盤を開発しています。また、SWIFT はイーサリアムのエコシステムに使われる技術検証も積極的に行っています

概念実証（Proof of Concept）

現在、SWIFT Innovation Lab では、DLT 関連の概念実証を数多く実施しています。機能検証を通じてノウハウと専門知識を強化し、ビジネスの適用領域にとらわれない DLT プラットフォームの構築に向けた SWIFT のアプローチを検証しています。現在、以下の機能検証を実施中です。

- **本人確認とアクセス管理：**DLT ソリューションを、SWIFTNet の公開鍵基盤ソリューションやアクセス制御メカニズム（Closed User Group や RMA など）といった SWIFT の既存プラットフォームや技術と統合することで、本技術評価で明らかになった本人認証やアクセス管理における問題が解決できるかを検証しています。
- **決済口座情報（SSI）：**データの機密保護が不要である OTC 市場のレファレンスデータを対象に SSI データベースを構築し、DLT がもたらすメリットを実証することを目的としています。同時に MT670 や MT671 などの既存の SSI ソリューションとの相互運用性や互換性を調査します。
- **ISO 20022：**DLT に、SWIFT の標準化の専門知識や、ISO 20022 の方法論を適用します。すべてのステークホルダーが分散型台帳を利用していない状況で、旧システムとの相互運用性をいかに実現するかを検証します。債券は仕組が簡素であると同時に、SWIFT の強みが反映されやすい資産クラスであることから、債券発行からサービシング業務に至るライフサイクルを実例として取扱っています。

SWIFT プラットフォームにおける DLT ソリューションをサポートする機能・性能を更なる開発に向け、その他の概念実証も実施中、または実施予定です。標準化され且つ適用領域に依存しない DLT 基盤を構築するために、技術機能の検証及び SWIFT の取組の支援のためには、概念実証の対象分野は実例的に考察されるべきです。

SWIFT による DLT 研究開発

標準化

SWIFT Standards チームは、既存のメッセージングやレファレンスデータの標準をいかにして DLT に適用できるかを検証しています。既存の標準の利用は、以下の 2 つの理由から重要となります。

- 「車輪の再発明」とならないように、ISO 20022 などの既存標準は、業界において承認済みの正確な事業概念の定義が含まれ、DLT にも適用可能であり、DLT ソリューション導入の加速化に寄与します。
- 業務プロセスの一貫性を保つため：複雑な業務プロセスが単一の DLT 環境でカバーされるとは考えにくく、むしろ、DLT はメッセージング・システムや API（Application Programming Interface）などの既存の自動化メカニズムや、他の分散型台帳と連携されることが想定されます。安全かつシームレスな連携を実現するには、DLT と標準が十分に採用されている既存プラットフォーム間において、相互に照合可能で整合的な定義が必要となります。

SWIFT の Standards チームは、DLT 特有の標準についても検討しています。既存のメッセージング標準を再利用できる部分も多くあるが、事業内容からガバナンス業務に至るまでメッセージングとは違う面もあり、業務の自動化に際して形式統一や標準化において多くの課題が存在します。

SWIFT Innotribe

SWIFT の Innotribe プログラムは、SWIFT メンバー、フィンテック企業、SWIFT 社内チームが連携して業界全体に関わる課題やビジネス機会に対応する「Innotribe Industry Challenge」を設立しました。Innotribe Industry Challenge の成果は数多くの概念実証であり、これらは協働による実用的なソリューション構想・設計を可能とします。まず始めに、DLT による証券発行と資産管理業務を検証します。

SWIFT Institute

金融業界における独立研究への資金援助を担う SWIFT Institute は、2016 年に DLT に関する学術的調査報告書を 2 冊刊行する予定です。1 冊目の題材は『The Impact and Potential of Blockchain on the Securities Transaction Lifecycle（ブロックチェーン技術が証券取引ライフサイクルにもたらす影響と可能性）』です。

Global payment innovation initiative (gpii)

SWIFT は gpii の一環として、50 を超える世界の大手決済銀行と連携しながらコルレス銀行取引の長期ビジョンを推進し、DLT などの新技術の導入における協働の可能性について調査しています。2016 年の第 2 四半期と第 3 四半期を通じて、gpii 参加銀行と SWIFT の Bank and Payment Board Committee は「Vision Workshop」を開催する予定です。金融業界における幅広い議論に向けて、ビジョンの草案及びコルレス銀行取引の将来に向けたロードマップを作成し、2016 年 9 月開催の Sibos において提示される予定です。

SWIFT について

SWIFT は金融コミュニティのための協同組合であり、金融業界に新しく画期的な手法でソリューションの提供を担う、信頼性の高いサービス・プロバイダーです。

SWIFT の DLT に関する取り組みの詳細については、DLT@swift.com までお問い合わせください。

SWIFT の詳細については www.swift.com をご参照ください。

swiftcommunity　company/SWIFT

著作権

免責事項

SWIFT は本書を情報提供のみを目的として提供します。本書に掲載される情報は随時変更される可能性あがります。必ず最新版をご参照ください。

アクセンチュアについて

アクセンチュアは世界有数のグローバル・プロフェッショナル・サービス企業であり、経営戦略、コンサルティング、デジタル、テクノロジー、オペレーションの各分野において幅広いサービスとソリューションを提供しています。アクセンチュアは、お客様のパフォーマンス向上と、ステークホルダーに対する持続的な価値の創出を支援するために、事業とテクノロジーの融合に取り組んでいます。

アクセンチュアの詳細については www.accenture.com をご参照ください。

@Accenture　Accenture

Frédéric Le Borne
Managing Director
SWIFT Global Relationship Lead
frederic.le.borne@accenture.com

David Treat
Managing Director
Capital Markets Blockchain Global Practice Lead
david.b.treat@accenture.com

Fernand Dimidschstein
Managing Director
FinTech Innovation Lead
f.dimidschstein@accenture.com

Chris Brodersen
Accenture Research Principal
Capital Markets Blockchain Lead
c.brodersen@accenture.com

免責事項

本書におけるアクセンチュアの役割は DLT の成熟度の現状、主要機能や長所に関する洞察と専門知識の提供に限定されます。我々の判断の基準となる情報源や情報の信頼性を細心の注意を払って確認していますが、アクセンチュアは当該情報源や情報の正確性や完全性を保証しおらず、依拠すべきではない点、予めご了承ください。

また、本書に掲載される結論や推奨は SWIFT の見解を示すものであり、アクセンチュアの見解を反映するものではありません。

57189 - April 2016