NEM Catapult

ロン・ウォン
Dragonfly Fintech Pte Ltd.
（ドラゴンフライフィンテック）
NEM コアチームメンバー
E-mail: hwong@dfintech.com
2016年11月

アブストラクト: 現行の金融機関の抱える大きな問題は、そのシステムが複数の台帳を管理することに伴う非効率性にあります。様々な資産を複数の台帳で管理するためにブロックチェーンテクノロジーによる解決策を用いることは、この種の問題に対して抜本的な変革をもたらします。我々は本文書において、元々のNEMのテクノロジーとコンセプトに基づき、全く新しいCatapultというブロックチェーンソリューションプラットフォームを提案します。このオープンプラットフォームにより、実装と所有に伴うコストは減り、現在、そして未来におけるブロックチェーン主導のソリューションが推進されることでしょう。Catapultはほぼすべてのアプリケーションと簡単に統合可能なように設計されており、ゆえに既存の銀行業務のスタンダードと齟齬をきたしません。ブロックチェーンのインスタンス間の相互運用性を高めることで、共有可能なデータと不可能なデータとが単一の環境で共存することを可能にします。この文書は様々な立場の人々に広く読まれることを意図したものです。

キーワード: Catapult, Mijin, NEM, Tech Bureau, テックビューロ, Dragonfly Fintech, ドラゴンフライフィンテック, blockchain, ブロックチェーン, smart contract, スマートコントラクト, permissible chain, open system blockchain, banking standards, multi-ledger

1. イントロダクション

NEMのブロックチェーンテクノロジーが世に出てから２年が経ちます。NEMは世間で主流となるアプリケーションとしての使用を念頭にデザインされていますが、それゆえに我々チームはもっとも拡張可能な形でのソリューションを開発する必要がありました。
これまでNEMプロジェクトはブロックチェーンテクノロジーのパワーを解き放ち、そのプラットフォーム上にプロジェクトがアプリケーションを素早く作り上げられるようにすることを最優先にフォーカスしてきました。

我々の見立てでは、現在ブロックチェーンテクノロジーは産業界のどこに収まるかが定かではなく、その適用と標準化は一貫性を欠いたものとなっています。マーケットを見渡すと、新進のブロックチェーン技術のほとんどは分散台帳を中心として発達しており、いずれもブロックチェーンの運用の仕方と雰囲気ががわずかに異なる程度のものです。

我々のアプローチは一味違います。パワフルなブロックチェーンのための機能と特性だけではなく、それと同じくらい重要でありながら見過ごされがちな点にも注力しました。例えば

1. いかなるソリューションであろうとも、その上に独立に構築することができる。
2. 完備なAPIを備えた抽象化層を用意することで統合を容易にし、それによってブロックチェーンの分散台帳のもたらす力を制御する。
3. 且つスケーラビリティをもたらす。

です。この文書の目的は、NEMがいかにしてこれらを達成しているのかを説明することと、NEMというソリューションがブロックチェーン技術としていかに重要な役割を果たすかというだけでなく、いかに新しいスタンダードを提供するかという点を説明することにあります。

2. 従来型システムの問題点

ブロックチェーンテクノロジーは台帳ソリューションです。台帳なのですから、その特徴的な機能は金融業界と関係が深いということは自然とわかります。全ての金融機関はその業務のもっとも重要なソリューションに台帳を用いているためです。

しかし残念なことに、現行の台帳の上に乗る種々の金融サービスは、プロプライエタリな台帳システムと密に結合しているということは周知の事実です。台帳システムとアプリケーションの数は年々増加の一途を辿っており、それらの折衷が喫緊の課題となっています。

銀行間でトランザクションをやり取りする場合、多数派となるシステムとの互換性が保証できないため、さらに複合的な影響とリスクが存在します。それらのシステムは数十年に渡って使用されているうちに密結合の塊と化しており、効率化は多くの場合不可能であるか、あるいは非常に高くつく作業となっています。全ての銀行にとって、新しいサービスやソリューションを展開することは、その塊に新たにパッチを貼る作業にほかなりません。新た

なシステムが旧来のシステムと齟齬をきたさないことを確認する、というのが頻繁に見られるリスクの回避方法です。

技術的な観点から見るとこれは、密結合の塊と、その上部に存在する台帳間を飛び回る通信レイヤの雑多な情報との間に存在するミドルウェア層が分厚くなることを意味しています。これにより、オペレーションのリスクが高まるだけでなく、トランザクションの引き起こす問題・エラーに対処するリソースの浪費をももたらします。

既存の銀行業務の中核を標準化することは必須です。現時点では、この標準化はミドルウェアのレイヤで起きており、システム間の連携はこのレイヤに依存しています。

銀行間トランザクションの処理は外部のメッセージングシステムに依存しており、これは多くの場合標準化に向かいます。現在主流なのはSWIFT[1]と呼ばれるものです。これは40年以上前にデザインされたものですので、実績は確かかもしれませんが、今日の標準から見ると恐ろしく非効率です。というのも多数のスイッチオーバーやルーティングを行うにあたって一部のメッセージを手動で管理する必要が生じる場合があるからです。

そういったソリューションにはオペレーションリスクに加え、遅く怠慢なものになるという可能性があります。銀行や企業はSWIFTを使い続けるために、毎年数億ドルを浪費しているのです。もう少し詳しく述べると、ルーティングシステム単独で見ればインターネットと言うのは非常に優れたシステムですが、スイッチオーバーに対処するとなるとそれは非常に難しいタスクとなり、多くの人月と資源を奪うものとなります。

この問題に対処するために様々な試みや提案がなされたにも関わらず、このような密結合のシステムが金融機関の多数派を占めていることが、今日見られるようなオペレーションのリスクや非効率性をもたらしているという証拠はいまや枚挙に暇がありません。

3. 目的

こういった問題は近年になって生じたものではありません。バンキングシステムのコアに対して金融関係のサービスが付け加えられていくにつれて、毎年繰り返し問題視されてきたことです。さらにサービスの内容が年々複雑なものとなってきていることが状況をさらに悪化させています。

ブロックチェーン技術は、コストの削減、決済のファイナリティ、コンプライアンス遵守の効率化、監査能力とトレーサビリティの増加、プロセスの明確化の促進(近年スマートコントラクトと呼ばれているもの)、グローバル・ローカルなトランザクション双方における複数パーティへの依存度の低下、といったものに対して長期的なソリューションを提供します。

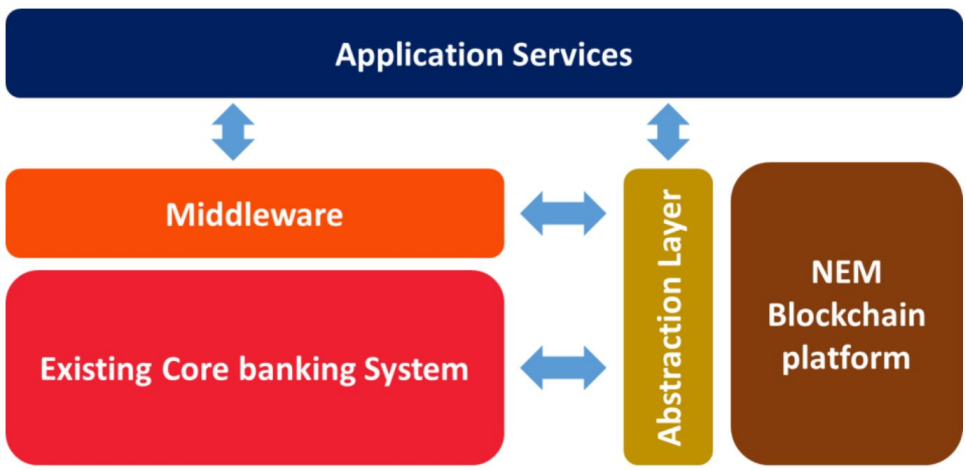
いまだ未解決のこれらの需要を満たすためにブロックチェーン技術を導入すれば、いかなる金融機関であろうともすぐにその利点に気付くことでしょう。ブロックチェーンプラットフォームはそれ自体標準化されているもので、業界標準のコンプライアンス規約を守りつつ任意のアプリケーションと統合することが可能です。

[1] Society for Worldwide Interbank Financial Telecommunication

我々は、ブロックチェーン技術のもたらす衝撃と、それがいかなる役割を果たすことができるかを、金融業界自身よりも早い3年前から調査してきました。

この３年間に及ぶ分析・調査によって我々は極めて重要な結論に達し、ついに最終的な解決策となるブロックチェーンプラットフォームを発表するに至りました。このゴールは以下のような結論の上に導き出されたものです。

- スマートコントラクトは全金融機関において長らく存在しており、銀行業務の中核にプログラム(自動化)されているか、内外のパーティ間のプロトコルや合意に基いて手動で実行されているかのいずれかであった。こういったスマートコントラクトのインフラを幾年にも渡って管理することに金融機関は数十億ドルのコストをかけており、新規システムへの移行にあたってはさらにリソース・時間の浪費とリスクを被っている。これらは複雑に絡み合った複数の仕事の上に成り立っているので、単純な方法では即決の変更をもたらすことはできない。NEMはそれを理解しているので、異なる方向からのアプローチを試みている。そのアプローチとはすなわち、中央集権的(つまり現在のシステムと同等な状態を維持しつつ)、あるいは分散的に、スマートコントラクトを外部のコンポーネントへと括り出すことである。これらのスマートコントラクトのアウトプットはセキュアなトランザクションのプロセスを経て台帳に記録される。
- 最小限のリスク、時間、資源で、且つ最低限の介入のもとで通常通りの銀行業務を行いながらのデプロイを可能にするシステム — これにより有機的な成長が可能になる。
- 複数の台帳とユースケースに(相互排他的であるか否かに関わらず)対応したシステムを作る。同時に台帳間のトランザクションが摩擦を引き起こさないようにする。
- 既存のいかなる銀行業務システム・ソリューションと統合可能な単一の抽象化層を作る。
- プライバシーに憂慮し、個々の金融機関が固有のブロックチェーンプラットフォームを管理することを可能にする。
- 高価で標準化されたプロトコル主導のメッセージングシステムを新たに実装する必要なしに、シームレスなクロスプラットフォームのトランザクション、送金、決済を可能にする。結果として、調整業務、リスク、エラーの少ない決済のファイナリティをより簡素化されたインフラシステムで実現できる。



【図1】中核を担う台帳システムとして用いられるにあたって、まずは既存システムへの付加によるブロックチェーンプラットフォームの導入

4. CATAPULT

Catapult[2]は、2015年3月にローンチしたNEMブロックチェーンテクノロジーの拡張技術である第2版です。Catapultは2017年の第一四半期から段階的にリリースする予定です。先行のソリューションはMijinと呼ばれ、こちらも厳しいテストをくぐり抜けています。Mijin、Catapultともにプライベート化可能なブロックチェーンですが、違いはMijinがパブリックブロックチェーンであるNEMの拡張であるのに対し、２つ目のバージョンであるCatapultはその逆、つまりプライベートチェーンのNEMへの拡張とみなすことができる点にあります。ブロックチェーンに対して、よりクリティカルな機能・特性を必要としている金融機関をサポートするのに特価した設計をしているのです。

4.1 特徴の要約

CatapultはNEMの核となるコンセプトを継承しつつ全コードをC++で書き直しており、NEMの初版リリースから学んだ経験にもとづき、それらのコンセプトに拡張と修正を加えています。最終目標はハイパフォーマンス且つセキュアで、外部接続が容易なエンタープライズクラスのソリューションとなることです。現在Catapult用に開発中の機能として特筆すべきものには以下があります。

- 業界標準のWEBアーキテクチャに基いて設計されたことによるより高いスケーラビリティ。既存のブロックチェーンソリューションでこれを包括的な形で達成したものは今のところ存在しない。
- 外部接続性の高い、高パフォーマンス且つスケーラブルなAPIゲートウェイサーバのレイヤ
- トランザクションに対するリアルタイムなビッグデータ分析を可能とする、ハイスループットなメッセージ・キュー
- ハイスピードなメッセージングに適した、APIレイヤにおけるNoSQLデータベースの採用
- ブロックチェーン上でアセットを取引するための、組み込み型の預託(エスクロー)サービス。トランザクション型コントラクト。
- 高いトランザクション処理能力(秒間3,000トランザクション以上)
- アクセス権限管理可能なアカウント。すなわち各ユーザーは自分から見える範囲にしかアクセスできないという特徴。
- 高い相互運用性。外部の分散・非分散アプリケーションやスマートコントラクトソリューションとブロックチェーン上でトランザクションを行うことを可能にする。
- ビジネスルール — 確実に問題のないことが確かなトランザクションによってのみ、明確且つ決定的なオブジェクトの状態変更が行われるルール。特に事前に定められた改変不可能且つイミュータブルなトランザクション料金との整合性の検証

[2] CatapultとMijinはテックビューロ株式会社によって開発されたパーミッションドブロックチェーンです。CatapultはオープンソースソリューションのコアとしてテックビューロよりNEMに提供されます。

- メタデータ — アカウントとアセットは変更可能なメタデータのフィールドを持つ

上記に加えて、最新版のNEMが持つ既存の機能や特色を改善した上でCatapultプロジェクト上にも移植する予定です。これは以下を含みます。

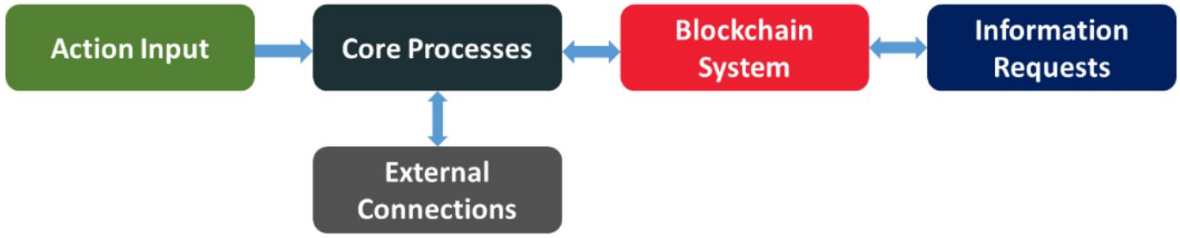
- ビルトインのメッセージングソリューション。
- プロセス駆動、あるいは手動でアクティベートされるトランザクション機能。必要に応じて多重認証を必要とするようにすることが可能。
- 単一のブロックチェーン上における、複数の対応アセットを持つ複数台帳の管理
- 全アカウントが複数台帳上で複数アセットを持ち、従って銀行の提供するあらゆるサービス用に用いることが可能である。例えば一つのアカウントで米ドル、ユーロ、ポンド、金、金利スワップ、投資信託などを持つことができる。もちろんそれぞれトランザクションとバランスシートの履歴を保持した状態で、である。
- 全アカウントは金融機関によるコントロールの元に置くことができる。これによりコンプライアンスの適用とマネーロンダリング対策として、トランザクションのマネージメントが可能になる。
- アカウントの凍結。
- 説明責任を果たしつつ、監査証跡可能なトランザクションの取り消し。

Catapultの提供するブロックチェーンソリューションの最終的な形は、金融機関が長期に渡って中核業務のプラットフォームの基礎として使用できる強力でカスタマイズ性の高いものとなります。

銀行システムがよりよいものとなるためのブロックチェーンソリューションの普遍的な基礎を担えるものにする、というのが設計に当たっての原則です。また、現行のシステムとの不均衡を引き起こさず、徐々にサブシステムを移行していくことが可能でなくてはならないという前提の元に設計されています。周辺的、または必須でない機能の移行時に銀行システムをリスクに晒すことはありません。機能の新旧を問わず、より複雑性の低いプロダクト・サービスをブロックチェーンを用いて、開発、移行、ローンチすることができます。

このように、オーダーメイドでありながらフレキシビリティの高いシステムにより、金融機関はブロックチェーン手動のシステムに向かって成長していきながら、ソリューションを手軽に実装し、システムに慣れる事ができます。

CatapultのAPIゲートウェイにより、他のシステムとブロックチェーンが容易に組み合わせ可能なものとなります。他のシステムとは(新旧を問わず)中央集権的なものと、あるいは(他機関の実装したコンセンサス手動のソリューションによる)分散的なものを含み、スマートコントラクトシステム、内部プロセス手動のソリューション、決済、支払い、精算システムなどがあります。



【図２】設計の原則。シンプル且つフレキシブルに。

4.2 コンセンサス

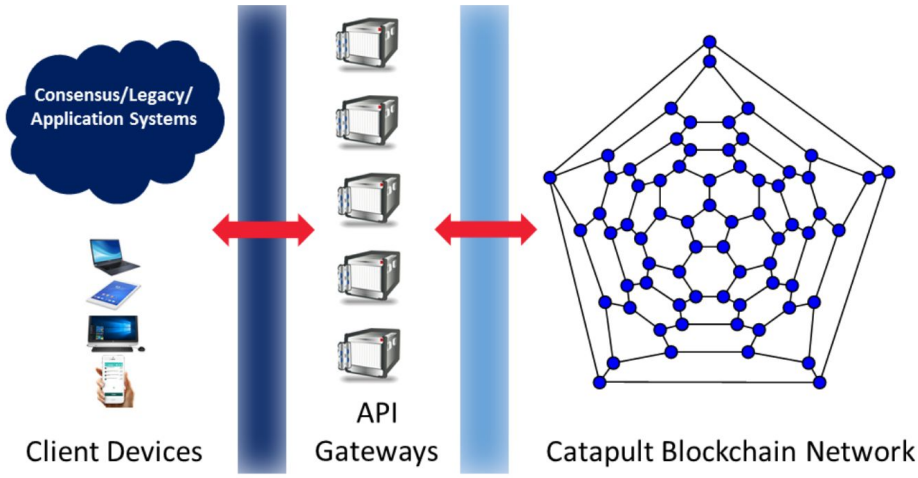
他の多くのブロックチェーンシステムと同様、Catapultにおけるブロックチェーンプラットフォームもまたコンセンサスメカニズムに基づいたものです。パーミッションが必要なノードと不必要なノードがP2Pネットワークで結びついたネットワークから構成されます。トランザクションはP2Pネットワークをブロードキャストされてノードにたどり着き、ノードによって検証されます。ブロックタイムと呼ばれる周期的なインターバルごとに、これらのトランザクションはひとまとまりにされてハッシュ関数の引数として与えられ、デジタル指紋が作成されます。これによって直前のブロックと紐付けられ、新たな情報のブロックとしてブロックチェーンに加えられます。パーミッションが必要な台帳はマイニングの必要がなく、制御されたProof-of-Stakeアルゴリズムに従い、パーミッションが必要ないパブリックチェーンの場合はProof-of-Importance[3]と呼ばれるアルゴリズムに従います。

NEMブロックチェーンソリューションに組み込まれた機構(Eigentrust++ 評判管理アルゴリズム)では各P2Pノードの評判が管理できること、またそれゆえに利己的な振る舞いができないことが保証されています。
また、NEMブロックチェーンソリューションは完全に新規のP2Pによる時計同期アルゴリズムが搭載されており、これにより各ノードのタイムスロットがずれないことも保証されています。

4.3 ユースケースの展望

Catapultのブロックチェーンは、業界標準のJSON RESTful APIを用いたオープンシステムであることを意図して設計されています。従ってISO20022やFpMLマークアップ言語といった旧来の標準を用いるシステムとも問題なく統合可能です。Catapultはこれらを、トランザクションをブロードキャストしたり台帳をアップデートしたりするための、きちんと定義されたアウトプットを伴うプロセスとして扱います。この統合様式と高い相互運用性により、レガシーなアプリケーション・ソリューションとの再利用が可能になります。

[3] NEMのテクニカルリファレンスを参照 - https://www.nem.io/NEM_techRef.pdf



【図3】他のシステム、あるいはクライアントの端末と接続するためのAPIゲートウェイを用いたアーキテクチャ。現行の標準と齟齬をきたさない。

4.3.1 投資信託のトランスファーエージェント

ここでは典型的な投資信託の購入と決済に対するソリューションを検討します。

典型的な投資信託のシナリオでは以下の主体が登場します。

1. ファンドマネージャー
2. トランスファーエージェント
3. 顧客

投資信託の適法契約にあたっては、キーポイントとなる区分がいくつか登場します。これらはアセットのユニットごとの収入と支出を構成する概念で、以下が全てではありませんがその一部となります。

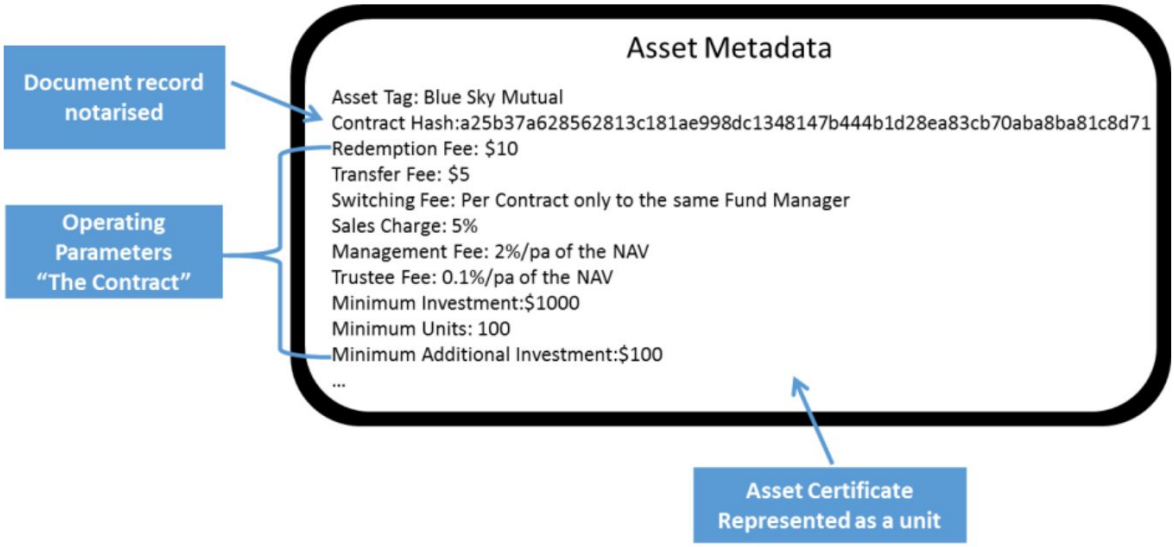
1. 純資産総額(Net Asset Value, NAV)
2. 投資の内訳とその状況
3. 配当
4. ディスカウント
5. マネージメント料金
6. 信託報酬
7. トランスファー料金
8. 手数料

従来の考え方ではこういった契約は、会計処理のアプリケーションへと翻訳されます。そしてそのアウトプットはデータベースへの一つ以上の書き込みを行い、それが引き続く一連の自動あるいは手動のアクションを引き起こします。

売買のプロセスによって、手動で処理されるか自動的にいくつかのオペレーションを引き起こすリクエストが発行されます。これらのオペレーションは実際に結果をもたらします。購入プロセスの場合、その結果とは以下のようなものです。

1. 決済期間まで待つ
2. 決済に基いて、ユニットごとにアセットを移譲(トランスファー)する
3. 所有権の証明書を発行する

トランスファーエージェントの役割はこのような、アセットの購入、売却、配布を取り仕切る事にあります。面倒且つ高価になりうる仕事です。



【図4】アセットの証明書はそれ自体新たなアセットとしてブロックチェーン上に登録されます。

投資信託のユニットを購入すると、それをブロックチェーン上で保持していることを示す証明書がユニットごとに必ず生成されます。各トランザクションは改竄と取り消しが不可能なものとなります。

従って配当・料金・報酬の計算は、ブロックチェーンを介したAPI呼び出しによって、別のアプリケーションから取り出される形になります。

そしてオリジナルの契約書類は、ハッシュ値をブロックチェーン上に保持した上で、分散ファイルシステムで管理することができます。(会計処理の)アウトプットがAPI呼び出しによってブロックチェーン上で処理される他の例として、注文の計上があげられます。
また、同一のフロントエンドアプリケーションから、API呼び出しを介してユーザーのバランスシートをブロックチェーンから引き出すことも可能です。他にも、前述のように上位レイヤにビッグデータ解析基盤を実装し、APIメッセージキューによる呼び出しによって引き出されたブロックチェーン上のデータを解析することができます。支払いと決済は通常通りユーザーアカウントから直接ブロックチェーン上で実行されます。

ブロックチェーンシステムに国境は関係なく、また単一のノードで複数台帳を管理することも可能です。これは海を超えて複数の国にまたがる、とてもパワフルなシステムを作ることができるということを示しています。分散的・非分散的に、(スマートコントラクトの)条件を実装しつつ、その国のルールに則った形で運用することができるためです。

スマートコントラクトのテンプレートはあらゆるファンドに構築、適用することができます。

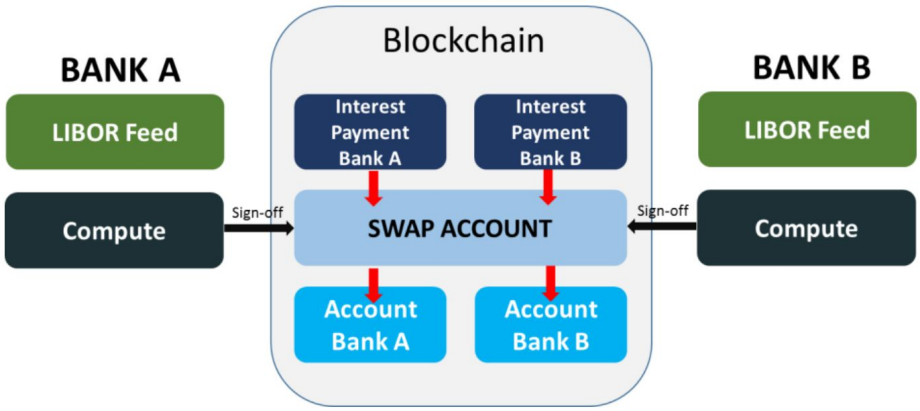
ブロックチェーンソリューションにおいては決済のメカニズムが容易に自動化できるため、決済時間をほぼ瞬時に、干渉が入らないままに行うことができます。

このソリューションそれ自体はNEMプロジェクトのバージョン1にすでに存在するものでしたが、Catapultでは、パフォーマンスの向上と上述のような改善によって一つ上のレベルに到達することでしょう。

4.3.2 金利スワップ(Interest Rate Swap, IRS)の仲介

２つのパーティが金利スワップの契約を結ぶ場合、まずはじめに、関係のあるパーティ間で結果をどう処理するか、定量的な形での合意を取り付ける必要があります。この合意はデジタル化された文書として書き下されて分散ファイルシステムに保持され、ダイジェストハッシュ値はブロックチェーン上に保持されます。

【図5】定量的結果に基いたIRSの合意の例



【図6】ブロックチェーン上での金利スワッピング

計算結果である出力は、テンプレート化された分散スマートコントラクト上で、あるいは参加者が別途計算するかによって合意に至ることができます。いずれにせよ、これらの計算結果のアクションをトリガーとしてブロックチェーンが精算をします。

4.4 エクステンション

上記の2つは、NEMブロックチェーンを用いて実装可能なユースケースのうちのごく一部に過ぎません。金融機関では、あらゆるプロセスの中心に台帳が登場します。会計の調整、遅延、失敗のリスクは多くの場合、複数のサブ台帳が単一のプラットフォーム上で協調して働くための中心となる台帳システムが存在しないことに起因してます。たとえ存在していても、それぞれのサブ台帳が個別に中心にある台帳をアップデートする必要があるようなシステムの場合、システムのインテグレーションは悪夢と化し、さらなる問題を引き起こす可能性があります。

この問題の根源を明らかにし、必要なプラットフォームを提供することは、問題の発生するリスクを低減するだけでなく、金融機関により新しく複雑なサービスを提供するための余裕を与えるものでもあります。

NEMテクノロジーはこの問題を解決します。さらにそのデザインによってトランザクションはファイナリティと完全性を保証され、イミュータブルで取り消し不可能なものになります。トランザクションの取り消しは正反対の内容を持つ新たなトランザクションによってのみ行われるため、完全な監査証跡が可能になります。

APIサーバゲートウェイの存在によって、ブロックチェーンが、台帳を必要とするアプリケーションの中核として振る舞うことができます。これにより、オープンなシステムであることと、スタンダードに従うレガシーシステムと分散化された新世代のスマートコントラクトシステムとの両方が台帳と円滑に接続できることが保証されます。

Catapultは、それぞれの金融機関、あるいは経営主体が1種類ずつのプライベートブロックチェーンを持つという仮定の元にデザインされています。共通の分散台帳システムを持ちいて法人間の相互運用性を高めるためのルーティングシステムに関しては、NEMイニシアティブ内で並行して進められているプロジェクト[4]があります。この汎用的分散台帳ソリューションによってNEMブロックチェーン技術のパワーがより引き出され、シームレスなトランザクションが可能になり、複数段階の必要な決済や支払いのシステムを仲介する必要がなくなります。トランザクションを介すことで、アカウント間での支払いのやり取りが最小限のメッセージングで直接的に行うことができるようになるという新たな地平を切り開くことでしょう。

プライベートブロックチェーンを自身で一つ管理するという選択肢が各金融機関に与えられる事によって、データのプライバシーがその機関外にもれないということが保証されます。さらに共有台帳の存在によって、金融機関同士の相互運用性が高まり、支払いや決済を機関同士でスムーズに行うことができるようになります。

[4] Dragonfly Fintech は、複数のブロックチェーンのインスタンスを結びつけることで、チェーン間の相互運用性を高める単一のソリューションを開発しています。

実際のところ、共有台帳システムはそれ自身単独で運用可能なものですので、各銀行は参加するためにプライベートブロックチェーンを持つ必要はありません。結局のところ、それは決済と支払いを可能にするトランザクションとレコードの台帳にすぎないのですから。

伝統的なやり方とは若干異なる決済と支払いの方法ではありますが、現在用いられているものとよく適合しやすいということは付け加えておきましょう。

要約すると、NEMブロックチェーンテクノロジーは、金融機関が、伝統的ソリューションからブロックチェーンテクノロジーによって支えられたものへと移行するのを助ける手段を提供していると言えるでしょう。

NEMプロジェクトチームは、これこそが最適な移行であると強く確信しています。金融機関がブロックチェーンテクノロジーを迎えるにあたって、参入コストを下げつつ、ブロックチェーンに触れながら慣れていくことを可能にします。

5. サマリー

Catapultはすでに実装の終盤に入っています。段階的にリリースし、その段階ごとに4.1節で述べた機能を追加していく予定です。最初のリリースは2017の最初の四半期を予定しています。ソリューションの拡張はユニーク且つパワフルで、ブロックチェーンのデザインに新しいスタンダードをもたらすものとなるでしょう。

Catapultの強力な抽象化レイヤは、インストール済みのソリューションを妨害せず、円滑に結合できることを意図して設計されているため、現行の金融システムの基準と齟齬をきたしません。FpMLやISO20022といった業界のスタンダードにしたがって現在運用されているシステムは、ブロックチェーンから抽象化レイヤを介してアウトプットされた出力を使用するだけでかまわないのです。こういった実装方法によって、金融機関は彼らのビジネス業務にとってより適切な時系列（旧来の特定の標準への依存を減少させたタイミング）で、システムをブロックチェーンプラットフォームへ移行することが可能になります。同時に、Catapultのソリューションによって金融機関はブロックチェーンの使用によるより高速且つ安価な移行を促進し、成長、拡大、新規プロダクトの開発を行うことができます。

6. その他のイニシアティブとの比較

Catapultはユニークな立ち位置を占めており、先行のソリューションであったMijinの第2版でもあります。その他のプロジェクトのほとんどは、既存のブロックチェーンソリューションの派生物ないしはそれに機能を追加したもので、包括的な機能を提供しようとすると不細工な形になってしまうでしょう。

ここではNEMプロジェクトの対象と関係する可能性がある３つのイニシアティブについて触れます。EthereumとBitcoinはすでにプロダクションフェーズに入っていますが、Cordaは本文執筆時点では構想の段階です。

6.1 ETHEREUM[5]

このプロジェクトは、独自の言語により記述されたスマートコントラクトの履行にあたって仮想マシンの使用を前提としています。一度ブロックチェーン上にロードされたスマートコントラクトコードは変更・取り消しを行うことができず、条件分岐にバグが見つかった場合は厄介なことになります。加えて、ステートの変更を行うプログラムに入力を与える際、オラクルと呼ばれる外部データへの依存が頻繁に発生します。変更後のステートはブロックチェーンストレージに書き込まれます。

こういった機能をいかにして取り込むか、あるいは別途処理するか、と言った問題は銀行側の判断に任せるべき、というのが我々の見解です。ですので我々のソリューションにはスマートコントラクトそのものの機能はありません。ある意味で我々は、ブロックチェーンが何のために設計されたのかに立ち戻り、その目的を達成するために最適な解を出そうとしているのです。すなわち台帳管理、複数台帳の管理です。これに多数の機能を追加して、金融業だけでなく他業種のアプリケーションにも対応できる、汎用的なソリューションを開発することです。その過程で、簡便に使用できるいくつかのスマートな機能もブロックチェーン上に開発しています。例えば、マルチシグ（複数鍵）ソリューションや、所有権移譲の管理にサードパーティが必要ないスマートエスクローソリューション等がそうです。このエスクローソリューションは、アセットを交換するにあたって双方のパーティが署名をしなくてはならず、それが片方だけの場合は交換は行われないというものです。

変更・取り消しが不可能な状態でスマートコントラクトが存在するというEthereumの形式は、システム移行にかかる労力が増すのみです。100%正しいということの保証やテストが必要な場合はとりわけその傾向が強まります。普通のソフトウェアソリューションの場合、こういったことは想定されていません。プロジェクトが複雑になればなるほど、バグを抱えるリスクは高まっていきます。ほんの些細なミスが体系的な失敗につながる可能性があり、いかなる金融機関であろうと、そのようなリスクは絶対に許容してはならないものです。

四角い杭は、丸い穴には決して完璧にフィットすることがありません。スマートコントラクトをブロックチェーン上に持ってくるというのはその一例です。今やもう、ほぼすべての金融機関はスマートコントラクトを詳細に設計された中央集権システム上で何年にも渡って動作させています。これらは全てきちんとコントロール下に置かれており、一時停止、バグ修正、再稼働を行うことができ、そのアウトプットは確定的で曖昧さのないものです。そういった二国間、多国間の契約は必ず複数パーティ間で相互承認することができます。ブロックチェーン上でのスマートコントラクトではそれはできません。つまり、一度ブロックチェーン上に記録されたスマートコントラクトは、別のプログラムによって置き換えるということができないのです。

また、スマートコントラクトはそれ単独で動作することができず、外からのインプットやオラクルに依存してしまっています。外部に何もない状態での実行は不可能で、サードパーティからのインプットに依存するのは信用の問題が浮上します。元々信用を置く必要がないプラットフォームを構想していたにもかかわらず、です。これはまさにパラドックスです。

[5] https://www.ethereum.org/

分散化スマートコントラストの一番の売りは、信用を置く必要がないスマートコントラクトプラットフォームである、というところにあったのですが、これは実現不可能なのです。実際には、スマートコントラクトをブロックチェーン上にもってくることは、実装のコストを指数関数的に増大させます。目的は手段を正当化しないのです。

6.2 BITCOIN[6]

ビットコインはトランザクションの処理に分散ブロックチェーン技術が使用できるというコンセプトの実証実験です。Catapultはトランザクションのハッシュ化と保持をブロックチェーン上で行うという点で、最終目的はビットコインと同じです。実際のところ、大抵のブロックチェーンプロジェクトはこの原則を共有しています。

NEMがビットコインと異なるのはまず、データブロック生成の権利を競うその方法にあります。他にも以下のような相違点があります。

- システムのアーキテクチャ — NEMの方がより高いスケーラビリティを持つ
- NEMには「残高」に相当する概念であるunspent transaction output (UXTO)がない。通常の台帳と同じ慣習に従い、複数のバランスシートとアセット —すなわち複数の台帳— を持つアカウントを管理し、全アウトプットとインプットはこのアカウントを介す。
- ビジネスロジック — ビットコインはただの台帳にすぎないが、NEMは例えば、トランザクションのキューイングとブロードキャストする前に署名を行う中央サーバに依存することなく、チェーン上でトランザクションへの署名を行うことができる、という非常に強力な機能を持つ。
- ビットコインは、特定の目的用の複数台帳を管理する機能をネイティブに持たない。
- ビットコインにはノードの評判を管理するソリューションがその中核に組み込まれていない。
- ビットコイン関連サービスの提供する機能の多くはサード・パーティのプロバイダによるパッチに依存したで回避手段あり、それゆえにサービスのレベル、クオリティの依存度、パフォーマンス、セキュリティ、信頼性という面において考慮しなくてはならないレイヤが増える。
- マシン間の競争 — ビットコインはマイニングを念頭に設計されており、ブロックチェーンをセキュアにするためにproof-of-workが必須である。パーミッションドブロックチェーンの場合、ブロックのマイニングのために競争を行う必要はない。ブロックチェーンをセキュアにするためのNEMのアプローチはよりシンプル且つパワフルで、維持にかかる計算資源とエネルギー資源の消費をより少なく抑えている。
- ビットコインは、ファイナンシャルなアプリケーションに用いるにはトランザクションのスループットが低すぎる。ビットコインのトランザクションレートは秒間1桁であるのに対し、NEMのCatapultは秒間4桁トランザクションを処理できる。
- ビットコインの承認時間は長すぎて、金融業界にとって適切とは言えない。

[6] https://bitcoin.org/en/

6.3. CORDA[7]

Cordaは構想の段階にありますが、どうやらオラクルの管理の仕方や、分散台帳上で動作するステートレスな関数を持っていること以外はEthereumと概ね同じ道を歩んでいるようです。ソリューションの実装のためにはJava Virtual Machineを使用することを提案しています。仮にそうなったとしても、おそらくNEMはこれらのEthereum上で処理されたスマートコントラクトの結果を、Catapult台帳システムへと導入し、処理することができるでしょう。

日本語訳: 宮本 丈
E-mail: joemphilips@gmail.com
NBZ5WW-S53QRZ-DO73Z7-B6CA6I-R2PNS4-PLR24N-NKZJ

編集： テックビューロ株式会社　代表取締役　朝山 貴生
http://twitter.com/takaoasayama
NCSPXQ-TU6Q5G-A7QOWJ-VPVAVJ-HG3HA5-7YJ3ZX-QJL5
NEM alias: @takaoasayama

[7] https://r3cev.com/blog/2016/8/24/the-corda-non-technical-whitepaper