ブロックチェーン技術の最前線と中銀デジタル通貨

ソラミツ株式会社 代表取締役社長　宮沢和正氏

今日は、ブロックチェーンの最前線の話をしていきます。基本的な話については、もうご存じの方もいらっしゃると思いますが、おつきあいをお願いします。

ブロックチェーンとは何か

まず、ブロックチェーンでは、今までは中央集権的なシステムで管理していたものを、分散型で全ての取引履歴を皆で共有して確かめ合います。これによって安全な「分散型台帳」を実現し、信頼性を担保します。

仕組みは、ハッシュ値、ハッシュ関数を使用して、データを要約して固定長の数値に変換します。取引のリスト、タイムスタンプ、作成者の署名をまとめてハッシュ値を取り、それをブロックに書き込みます。これがチェーンでつながっているので、ブロックチェーンです。ブロックの中の取引リストを改ざんするとか、タイムスタンプを改ざんするとハッシュ値が変わり、矛盾が生じて、改ざんが分かります。ブロックの中身の書き換えや、消去はできませんが、間違った情報は、追記により正しいデータに変えることができ、誰がいつ改訂したかという履歴が全て残ります。

ブロックチェーンの特徴は、瞬時にデータを共有できる、改ざんの防止、システムが止まらない、の３つです。データセンターがないため、各参加者は対等の立場で順次増えるという性質を持っています。複数のサーバーで共有することにより、データが常に最新で他と共有されます。改ざんができないため、高い信頼ができます。スマートコントラクトとして、契約の内容をプログラム化して書き込むと、確実に実行されます。システムが止まらないため、一部のサーバーが故障しても、他のサーバーが動き続け、災害対策にも有意です。また、つながりやすいという性質があり、世界中で連携が広がります。

ブロックチェーンは管理主体の存在によって、パブリック型とプライベート型（コンソーシアム型）の 2 つに分類されます。

パブリック型には管理主体が存在せず、プログラムが自動的に実行しています。代表的な事例は、ビットコインとかイサリウムといった仮想通貨です。それから、分散型の金融のシステム、NFT(Non-fungible token)という、唯一無二のトークンが実行できます。プログラムが実行するので誰かを信頼する必要がない一方、誰も止められない、一度動き出すと、永遠に動き続けます。

プライベート型は管理主体が存在し、主体が複数の場合はコンソーシアム型、単独の場合プライベート型と呼びます。管理者がデータの改ざんはできないものの、全てのシステムを止めることができることが、デメリットのひとつです。代表的な事例としては、ハイパーレジャーとかリップルがあります。

また、パブリック型では、データを正しいと判断するか、間違っていると判断するかの検証に、自由に参加できて、その参加者の数が不明で、日々増えています。プライベート型の方は許可制ですので、検証の参加者が分かっていて、代表者が検証します。

そして、結果に対する合意形成については、パブリック型では、マイニングという非常に電力を使う作業を行って、最初に回答を得た人に優先権があります。プライベート型、コンソーシアム型の方は参加者が決まっており、多数決で決定できます。

合意形成アルゴリズムが、パブリック型ですと PoW（プルーフ・オブ・ワーク）、プライベート型ですと BFT（ビザンチン・フォールト・トーレラント）といった仕組みです。ビットコイン等で使用される PoW は、一国と同程度の消費電力です。一方で、プライベート型ですと消費電力の問題を解決しています。処理時間についても、パブリック型のビットコイン等は一回の処理に 10 分かかり、また１秒間に７件しか処理できません。しかし、ソラミツが開発した Hyperledger Iroha（「いろは」）（プライベート型）は、２秒で処理ができ、また１秒間に 5,000 件ぐらいの処理ができ、全銀ネットの３倍の処理能力となります。

また、PoW では Finality と呼ばれる一度決まった内容が、覆る可能性があります。これは計算競争をして、ときどきブロックが同時に生成されることがあり、そのときに２つに結果が分かれます。この場合は、どちらが正しいのかというのを判断するのに１時間ぐらいかかります。BFT 方式ですと、投票によって一瞬で結果が出ます。

ブロックチェーンの利用法には、ヒト・モノ・カネの管理があります。ヒトの管理では、「デジタル ID」によって本人確認をし、公証やタイムスタンプ、医療とか教育とか行政を一元管理することを考えています。スマートシティの中で ID を管理することに使われています。

「デジタル資産管理」では、例えば、お金の価値そのものとなるデジタル通貨や、決済、それから保険とか証券といった資産の管理を行います。不動産とか契約、あるいは貿易等の管理、電力の管理や、唯一無二のデジタルコンテンツのアートの管理に使われています。

モノの管理では、例えば、食の安全ということで、バーコードをスキャンすると、豚肉がどこで育てられて、どういう加工工場を通ってきたかが、全部トレースできます。改ざんができないために、食の安全を守るとか、原産地証明ができます。天然ゴムの例では、違法に伐採されていないかどうかを GPS とブロックチェーンで管理して、合法的なものしか買い上げないことが可能です。あるいは車両トレーサビリティということで、中古車の事故履歴とか整備履歴の全て改ざんができない形で管理できます。

情報共有する場合に、ブロックチェーンのデータ共有には中心がありません。主導権争いもなく、対等の立場で参加ができ、データが瞬時に共有される、これがブロックチェーンの本質的な意義だと考えています。

ソラミツの会社概要と技術

ソラミツは５年前に設立されたベンチャー企業で、従業員数 100 名、日本からスタート

して、持株会社がスイスにあり、ロシア、カンボジア、中国にも子会社があります。ミッションは「ブロックチェーン技術で産業にイノベーションを起こし、社会課題を解決する」とし、グローバルに活動をしております。

ソラミツが開発したブロックチェーン「いろは」は、最初から世界で使えるように開発しました。Linux Foundation でブロックチェーンの世界標準を決める際に、全世界 260 社が応募して、IBM とインテルとソラミツの 3 社の技術を世界標準としていくとされました。

2019 年 5 月に、セキュリティの監査・安定性・耐久性等、さまざまな機関がテストして、政府、自治体、金融機関が使えるということで認定され、商用バージョンを発行しました。

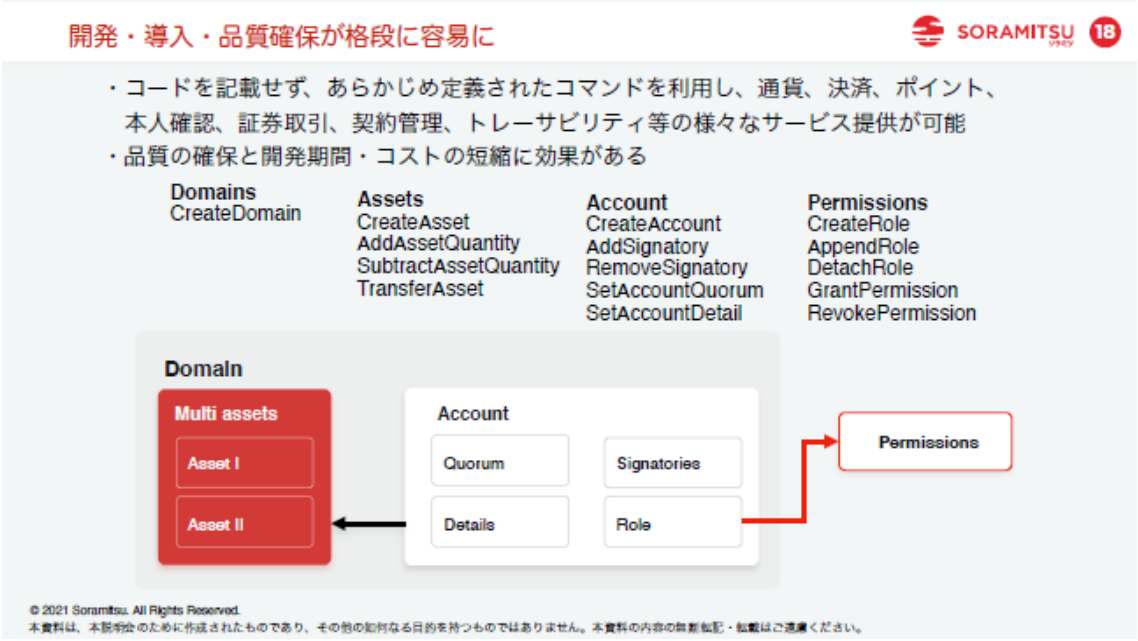
もう一つの特徴は、オープンソースで、ソラミツだけではなく、世界中のエンジニアが一緒に開発しています。仮にソラミツが消滅しても、このコンソーシアムの中で多くの技術者がアップグレードを続けていくことで、技術の継続提供が保証されています。また、海外のエンジニアが多数参加しておりますので、海外のデジタル通貨とか他のブロックチェーンとの相互接続も進んでいます。

「今までのブロックチェーンの課題」をあげると、処理能力が低い、プライバシーがない、秘密鍵を紛失すると二度と使えなくなる等があります。また、大量に電力を消費するとか、特殊な言語を使って非常に開発が難しい上、開発できる人員も非常に少ないという問題もあります。

そのため、ブロックチェーンは導入が難しく、用途が限定されるのではないかという議論が行われてきましたが、ここ数年、大幅に技術が進歩しました。われわれも問題を解決しようとして取り組んできた結果、高速大量処理とか、プライバシーの保護、鍵の復活が可能になりました。消費電力も少なく、開発導入が、Python とか Java という一般的な言語でできるようにしました。

また、スケーラビリティに大きな特徴があり、IBM の Hyperledger Fabric とか米国の R3 の Corda、あるいは Ethereum、Facebook LIBRA と比較しても、処理件数が 10 倍から 100 倍の性能です。

開発が簡単な理由として、「いろは」ではデータモデルが規定されています。まず Domain があって、その中に複数の Asset があり、その中に Account があって、利用者が複数いるという構造です。Account のユーザーは Permissions として、何ができる、何ができないかの権利が与えられています。権利に対し、Role という役割が規定されているという構造です（図表 1）。



図表 1

デジタル通貨を作ってそれを送金する場合には、この Assets 内の TransferAsset というコマンドを使うことによって、1 行でＡさんからＢさんへの送金処理ができます。相手の受け取る権利とか、反社会組織でないかとか、十分な資産を持っているかといったチェックのような複雑な事は、裏で処理します。こうした数百のコマンドを使うことによって、簡単に高度なシステムを開発することができ、これらのコマンドは全て品質の確保がされております。

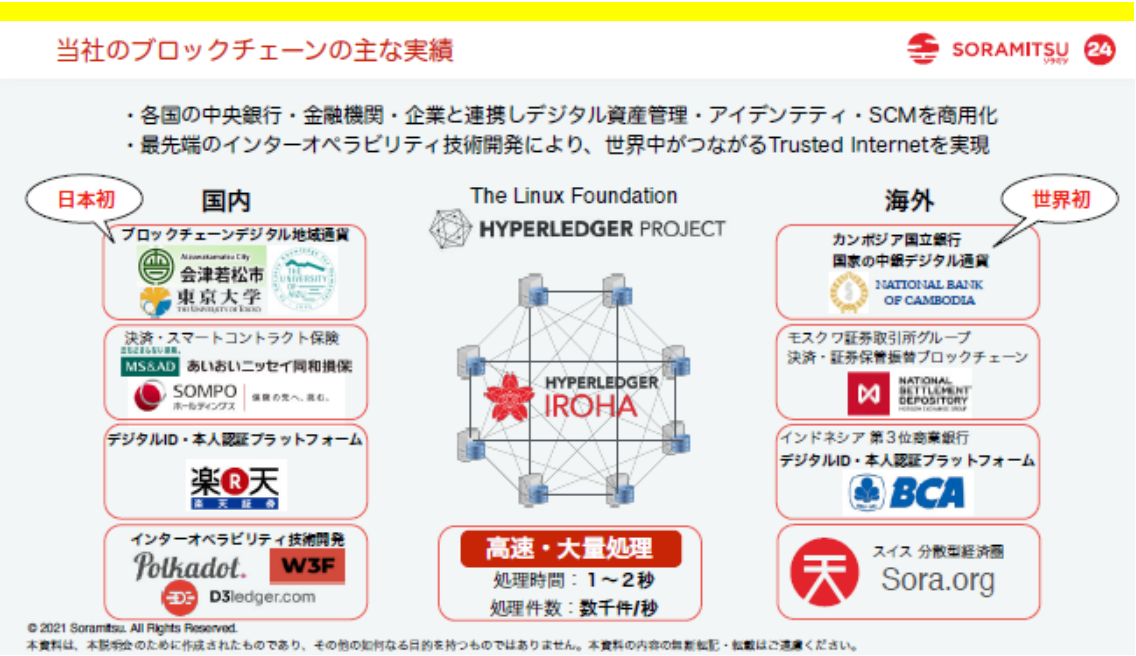
「いろは」では、送金はできるけれども、通貨の作成はできないという設定ができます。Role という役割を定義し、この Role をアカウントにアサインして、複雑な権限管理とかアクセスコントロールを簡単にします。他のブロックチェーンの場合は、全てコードで書かなければいけないので、複雑なプログラムになりますが、それが簡単にできる Role Bases Access Control(RBAC)という考え方を取り入れています。

また、鍵がなくなっても復活できる仕組みを業界初で作っております。簡単に言うと、錠前屋さんという機能をつくり、錠前屋さんと本人が立ち会って、新しい鍵と錠に付け替えることが、プログラムでできます。Grant Permission といって、管理者（Administrator）に限定して、自分の鍵を付け替えていいという権限を最初に移譲します。しかし、その他のこと、自分の財布の中身を見たり、お金を他者に移動するということは、Administrator にはできません。

Administrator が相当力を持つ可能性があるので、三権分立という、国家と同じような仕組みがこのプロセスの中に入っております。例えば、中央銀行であっても、国民の権利をもちろん奪うことはできませんし、勝手に決めることはできない。司法とか立法と相談

しながら、コマンドを実行していく形です。三権分立の機能分担は、憲法として記載します。それを Genesis Block という、ブロックチェーンの最初のブロックの部分に書き込みます。これは、追記による改訂はできますが、改ざんはできません。

主な実績として、海外では、カンボジアの国立銀行でデジタル通貨に使用されております。また、モスクワ証券取引所の証券保管振替、いわゆる「ほふり」のブロックチェーン化をしました。インドネシアの商業銀行の本人確認のプラットフォームや、スイスで分散型の仮想通貨交換所でも使用されています。国内では、ブロックチェーンを使ったデジタル地域通貨を、東京大学、会津大学と共同開発して、会津若松市で昨年 7 月から運用をしております。また、あいおいニッセイ、損保ホールディングスとはスマートコントラクトを使った保険、楽天証券とは、本人認証のプラットフォームに取り組んでいます（図表 2）。



図表 2

デジタル ID と地方創生

デジタル ID については、令和 2 年 9 月から、内閣官房の IT 総合戦略室主催の官民推進会合でデジタル ID、分散型 ID の基盤構築・提供、トレーサビリティへの利活用などが討議されました。具体的には、マイナンバーカードと紐づけをした、分散型 ID をスマートフォン等に入れて、国民全員が持つ、新たなデジタル ID にしていく議論をしました。この分散型 ID を、マイナンバーカードや、法人 ID、登記と結び付けて、健康情報、交通、購買あるいは身分証明といった様々なサービスの認証に使っていくための共通 ID についても検討しました。

分散型 ID は、World Wide Web Consortium (W3C)が制定した、デジタル ID の世界標準です。ID 発行する企業に依存することを避け、中立的で、なおかつ世界標準である技術を

採用しようと働きかけており、国でも、それを認めるようになってきました。

分散型 ID の特徴は、東京、会津若松、あるいはカンボジアで、地域ごとにばらばらに発行しても重複することがありません。そのため、将来データ連携をするときに都合が良い。個人の ID となった上、グローバルに一意です。また、中央認証局の必要がありません。こうした特徴から、全ての個人のサービスを一元管理して、グローバルに活用できる可能性があります。

分散型 ID とマイナンバーカードとの位置付けは、マイナンバーカードは一種の実印のような役割を果たします。分散型 ID はスマホに格納して認印、銀行印のように手軽に使う。法的な制限もなく、さまざまな用途に活用できると期待されております。

分散型 ID では、「Verifiable Credentials(VC:検証可能な資格情報)」という技術を使います。検証可能な資格情報とは、ユーザーの資格情報(JSON)を作り、それに秘密鍵で署名する形で信頼します。全体、ある JSON の資格情報と当該の署名をくっ付けたものを VC と呼び、その VC をユーザーに対して発行します。ユーザーは、自分のスマートフォンに、この VC を格納し、自分の意思で必要な相手に渡します。渡された側は、正しい情報か、改ざんされてないかどうかを、ブロックチェーン上に書き込まれた発行者の公開鍵を使って検証します。ユーザーが自分の意思で情報を渡していくため、ヨーロッパの GDPR にも合致しており、個人情報上も問題がないということで、このような仕組みが主流になっていくのではないか、と言われています。

ソラミツでも 4 年前からこの技術に着目して、2016 年に楽天証券で最初に導入し、そこから金融庁と一緒に実証実験をやりました。最初に実用化されたのが、インドネシアの銀行で、2019 年 5 月に、この方式で、銀行が発行した VC を保険会社やクレジットカード会社、証券会社に提供し、簡単に口座開設、保険会社の申し込みができるようになりました。

DID、分散型 ID、それから自己主権型アイデンティティは、本人認証の未来であると言われております。中央集権ではなくて分散型でさまざまな情報を管理しようというのが、この DID という思想で、それを一歩一歩実現していきます。例えば、マイナンバーを持っている人が、スマートフォンにマイナンバーをかざすだけでデジタル ID の登録ができ、その鍵を生成できるようにして、その鍵で地域でのあらゆる登録や認証を行うという取組みが始まっています。

カンボジア中央銀行デジタル通貨

仮想通貨には、裏付け資産はなく、価格が乱高下することもあり、決済には使いづらく、投機用資産として活用されてきました。ブロックチェーンと技術が進化する中で出てきたのが、デジタル通貨です。これには裏付け資産が 100%あり、価格が一定しています。従って、便利な支払い手段として利用できるようになりました。

ソラミツが共同開発した「バコン」が、カンボジアの中央銀行によって、世界初で、2020 年 10 月 28 日に正式運用開始されました。カンボジアでは銀行口座開設率が 2 割ぐらいし

かないので、銀行口座番号ではなく、電話番号を使った送金や、QR コードで店舗支払いができます。

「バコン」は、複数の通貨、カンボジアのリエルや US ドルといった現金と同等の価値を持っております。また、全ての個人・企業に提供されており、銀行口座がなくても、オンライン・匿名でデジタル通貨の口座開設ができます。一日の上限金額が US250 ドルに設定されていますが、銀行で本人確認のうえ口座開設すると、上限金額が上がります。デジタル通貨を現金にしたい場合には、銀行に行って交換できます。いつでも交換できるので、店舗等にとっては資金繰りの問題もなくなります。

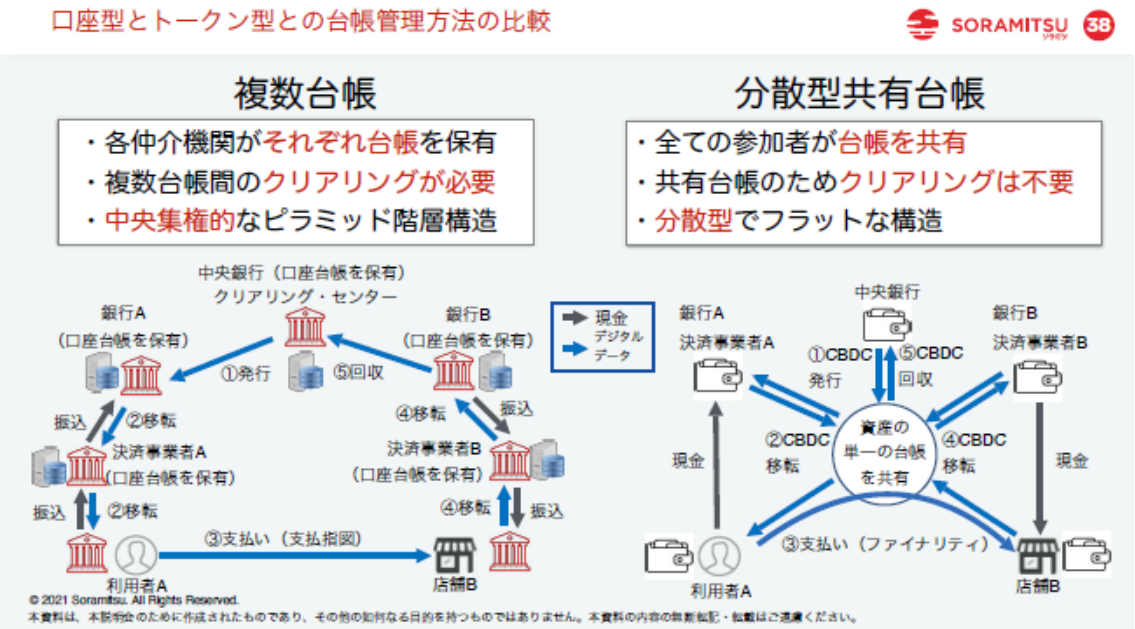
国全体をカバーし、ホールセールといわれる何億円とか何十億円の銀行間決済も、リテール決済の 100 円、1,000 円という決済も全て同じシステムで扱います。仕組みが非常に簡素化されて、送金手数料、振込手数料、加盟店手数料は無料になりました。これは、システムへの投資金額が、これまでの 10 分の 1 から 20 分の 1 ぐらいのコストになり、運用コストも下がったために可能になりました。カンボジアからの出稼ぎが多いタイやマレーシアとの送金決済を安く早くできるように、クロスボーダーの送金・決済についても開発中です。

今までのキャッシュレスと違うのは、例えば、Suica や PayPay では、利用者が店舗で使ったときには、お金の価値は移動していません。「使用した」というデジタルデータ、支払指図のデータだけが店舗に行き、それを 1 カ月に一回とかの一定期間で決済事業者に上げ、決済事業者が翌月に銀行振り込みをします。そのため、お金はあくまでも銀行口座の中で動き、複数の銀行を経由する場合に、どうしてもコストと時間がかかります。

デジタル通貨では、デジタル情報自体にお金の価値があります。ブロックチェーンの技術によって、コピーできない、改ざんできないとなり、人類史上初めて通貨がデジタル情報になりました。紙幣から、1,000 年かかって通貨の形が変わりました。

台帳管理の仕方で比較すると、現在の金融システムは、複数台帳方式といって、中央銀行を頂点としたピラミッド構造になっており、クリアリングをしながら決済が動いています。ブロックチェーンによって共有台帳にすると、サーバーは複数あっても、一つの台帳に中央銀行も銀行も決済事業者も利用者も店舗もみんなアクセスして、そこで残高を書き換えます。よって、クリアリングが不要になり、非常にスピーディーに動き、コストも非常に安い。これが新しい新時代の金融システムの形だと考えています（図表 3）。

使用する際の課題は、拡張性、利用者保護やプライバシーなどで、こういった課題を全て解決して、カンボジア中銀デジタル通貨が実現できました。



図表 3

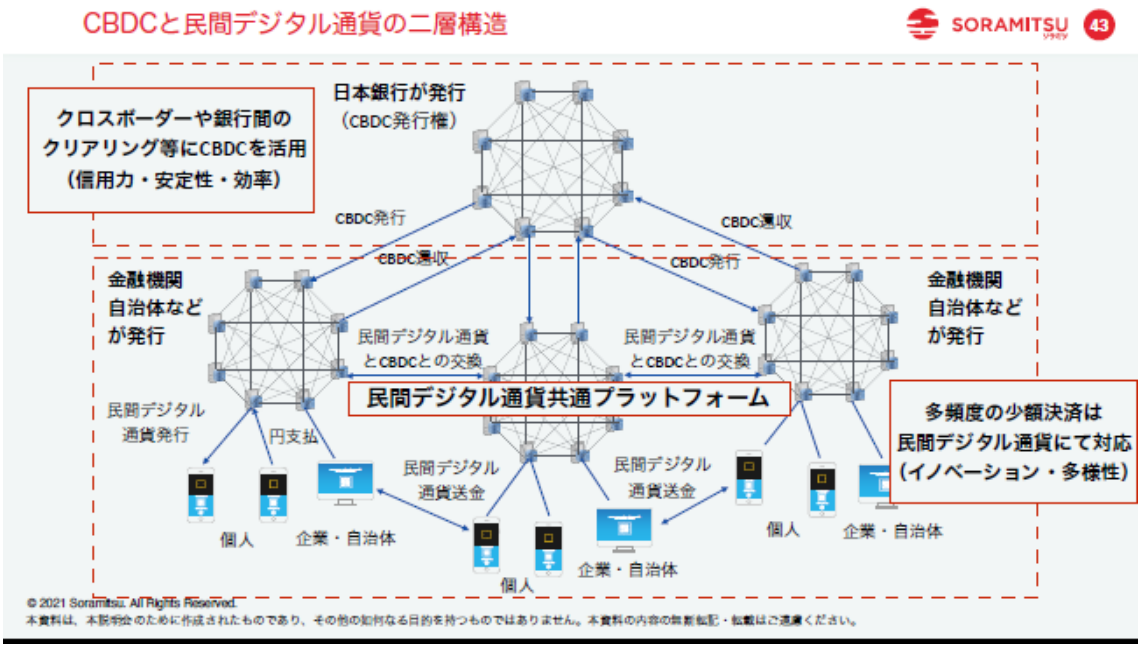
日本におけるデジタル通貨

日本でも、2020 年 7 月から、日銀主催の「デジタル通貨分科会」が開催される等、デジタル通貨の検討が始まっています。

カンボジアと状況が違うのは、「目指すべき方向性」として、日本の場合は、民間のデジタル通貨と CBDC（政府のデジタル通貨）との両立・連携が前提になります。これは、民業圧迫をしないことと、イノベーションしやすい民間がまずやり、民間ができない事を政府がやるという姿勢で検討が進んでおります。

図表 4 の下の方が民間で、金融機関、自治体などが発行するデジタル通貨がどんどんつながっていって共通で使えるようにします。多頻度や少額決済は、民間のデジタル通貨で対応して、イノベーションや多様性に対応します。民間ではできない部分については、日本銀行が、銀行間のクリアリングといった信用力が必要な部分、海外との取引で、将来 CBDC を発行するかもしれません。

民間デジタル通貨共通プラットフォームの作成者として、いくつかの企業が名乗り上げ、検討が進んでいます。その一つが、ソラミツも出資している Digital Platformer 社です。全国金融機関とか自治体が、相互運用性があるデジタル通貨とデジタル ID を発行するための「共通プラットフォーム LITA」を同社が開発し、4 月から稼働しています。デジタル通貨による給与払いに対応して、カンボジアの仕組み、それから会津若松の仕組みの技術を使っています。



図表 4

Digital Platformer 社は、短期的には「プレミアム付デジタル地域振興券」を全国の地方自治体等と進めております。また、自治体の「健康ポイント」とか「ふるさと納税感謝券」をブロックチェーンで発行しようとしています。

プレミアムを付けて地域通貨を発行する場合、今までの商品券だと、一回お店で使っておしまいです。ところが、デジタル通貨の場合だと、転々流通という特徴を生かし、ぐるぐると地域内を回り、経済循環乗数効果によって、助成金の 30 倍から 40 倍ぐらい経済効果があったという情報があります。お金が早く動いてコストが掛からないのは、あらゆる地域で経済の活性化につながります。

また、プログラムが可能なので、プレミアムの有効期限を設定し早く使ってもらって経済活性化するとか、他の地域でも使えるけれども、プレミアムは他地域で使えないようにして囲い込みと広域利用の安心感を与えることができます。データを地元に残し、個人のデータや法人のデータを使って、最適な融資、資金調達に使おうという検討がされております。

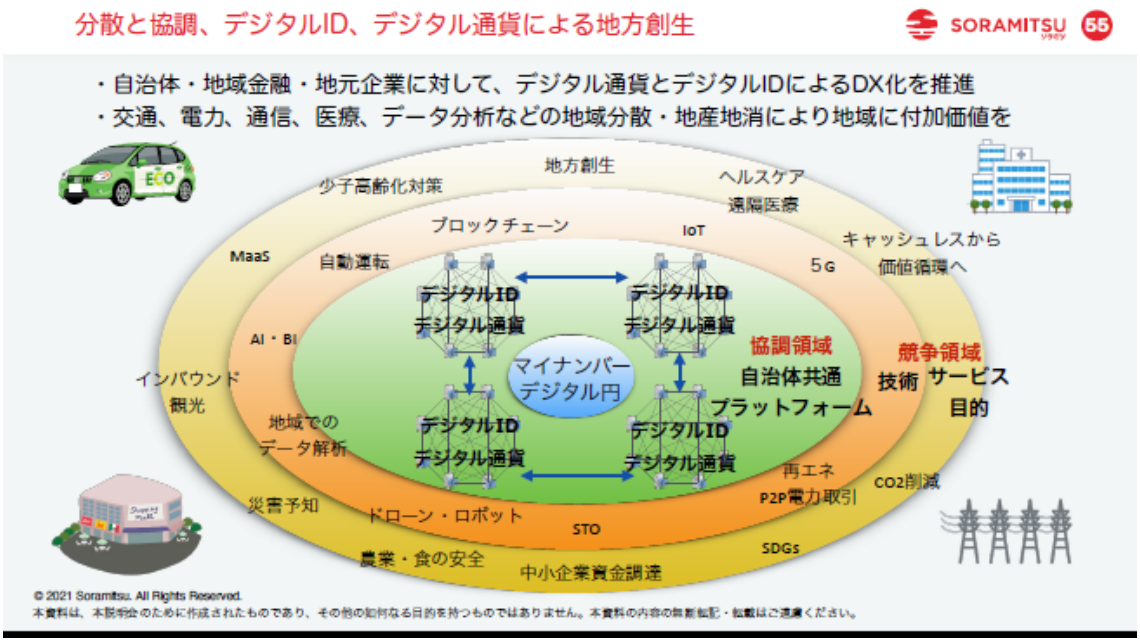
マイナンバーとの連携を考えると、デジタル ID にすると、一つのアプリでデジタル商品券とか健康ポイントとかマイナンバーの認証とか、さまざまな事が全部できて、これによって地域の発展に寄与できると考えております。

実際の検討や導入については、会津若松を中心に磐梯町、須賀川市や仙台市がデジタル地域通貨の導入をすでに発表しております。会津若松では、2020 年の 7 月から正式稼働し、磐梯町では、デジタル地域通貨を使った町ぐるみの活動が、2021 年 7 月からスタートします。

仙台市、東北大学のスーパーシティの構想では、参画事業者に Digital Platformer 社やソラミツも選定され、デジタル通貨、デジタル ID の検討が進んでおります。

関西では、大阪商工会議所とか京都市がプロジェクトを始動しております。デジタル ID とデジタル地域通貨が車の両輪と考え、このデジタル ID に、健康情報とか、交通情報を結び付けて一元管理をします。将来的には 2025 年の万博に向けて、全てデジタル通貨での決済とか ID による認証を行う構想があります。

各地域でデジタル ID、デジタル地域通貨が実用化されると、標準化されていないとお互いにつながらず、データ連携ができなくなります。デジタル ID、デジタル地域通貨を標準化して、図表 5 の中の協調領域で、自治体共通プラットフォームを提供して地方創生を考えます。一番中心には、マイナンバーと、日銀が発行する「デジタル円」があり、それらと連携をして、核となる技術の提供をしていきます。その外側では、競争領域でさまざまなイノベーションを起こすために、各地域がデータの地産地消とか、そういうことができるインフラを、各地域が作り始めています。



図表 5

スマートコントラクト、プログラマブルマネーと NFT

スマートコントラクトは、契約の自動化です。契約の条件確認とか履行まで自動的に実行できて、非改ざん性が保証されています。決済期間の短縮やコストの削減にもつながります。

証券とか不動産とか保険とかを小口化して、ブロックチェーンで管理して、簡単に売買するときに、何で払うのかという課題があります。そこで、デジタル通貨でスマートコントラクトによって売買を同時に実行する方法を模索しています。権利の移転と決済を同時

に行う Delivery Versus Payment(DVP)が、ブロックチェーンを利用し、スマートコントラクトで実現できるようになってきています。モスクワの証券取引所で、DVP で、証券トークンと決済の同時に実行を、活用していただいております。

スマートコントラクトを使った契約の自動実行も可能です。損保ホールディングスでは「天候デリバティブ」という商品の契約の実行、支払いが行われています。また、あいおいニッセイでも少額短期保険、「ペット保険」とか「乗っただけ保険」が、スマートフォンだけで申し込みから保険金の支払いまでできるようになっております。

もう一つ話題になっているのが、NFT で、代替不可能な唯一無二の「一点物」の価値を生み出すトークンです。コピーや改ざんはできません。デジタルアート作品に、「これは私が作ったもので唯一無二です。他にはありません。真正なものです」という NFT 証明書を付けた、デジタルコンテンツの販売が最近進んでいます。今まで、デジタルコンテンツは、簡単にコピーができるために価値が希釈化されてきました。新しい Web3.0 の考え方では、コピーや改ざんができなくなり、全てのデジタルアセットに価値を与えます。

NFT の規格には、ERC-721 という標準規格があり、ソラミツでもこれにのっとって開発をしています。ただ、取引手数料の高騰、コンテンツのフォーマットの標準化、仮想通貨での支払いといった問題があります。NFT を実現することや、Oct-Pass という標準仕様、法定通貨で支払うことができるプラットフォームの作成によって解決しようとしています。

最後に、こういった技術を国内だけではなく、世界中とつないでいく必要があります。すでに、「いろは」とビットコインとか Ethereum はつながっており、今後、さまざまなブロックチェーンもつながってきます。ブロックチェーンの国際標準化についても、ソラミツも審議に参加しております。

本日ご説明したようなかたちで、産業イノベーションを起こし、社会課題を解決していこうという意識をもって取り組んでおります。本日は、ありがとうございました。