

WG4 ディスカッション資料 ステ이블コイン

ステーブルコインの技術面での現況について

2025.3.25

株式会社NTTデータ 次世代決済技術推進室

計算リソースが空気や水のように遍在化する現代

スペック的には一昔前の基幹系システムと同等以上の性能、リソースを備えたデバイスが
遥かに高速・低遅延なネットワークに常時接続され、天文学的ともいえる数が世界にあまねく普及した世界



1974年
(Intel 8080)

2MHz

64KB

6μm
(6000個)

300bps

0台

2024年
(Apple A18)

4GHz

8GB

3nm
(数十億個～)

20Gbps(5G)

12億4,000万台/年 (全スマホ・世界)

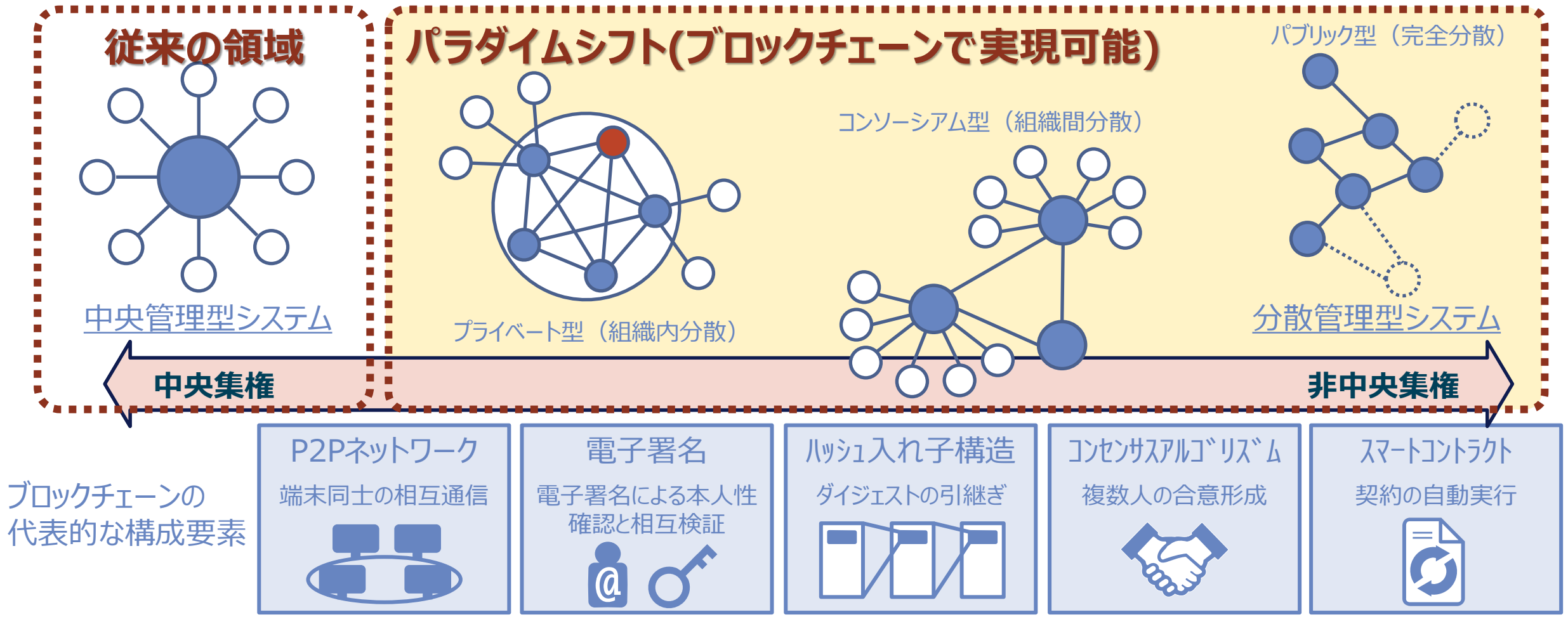


2024
iPhone16 Pro

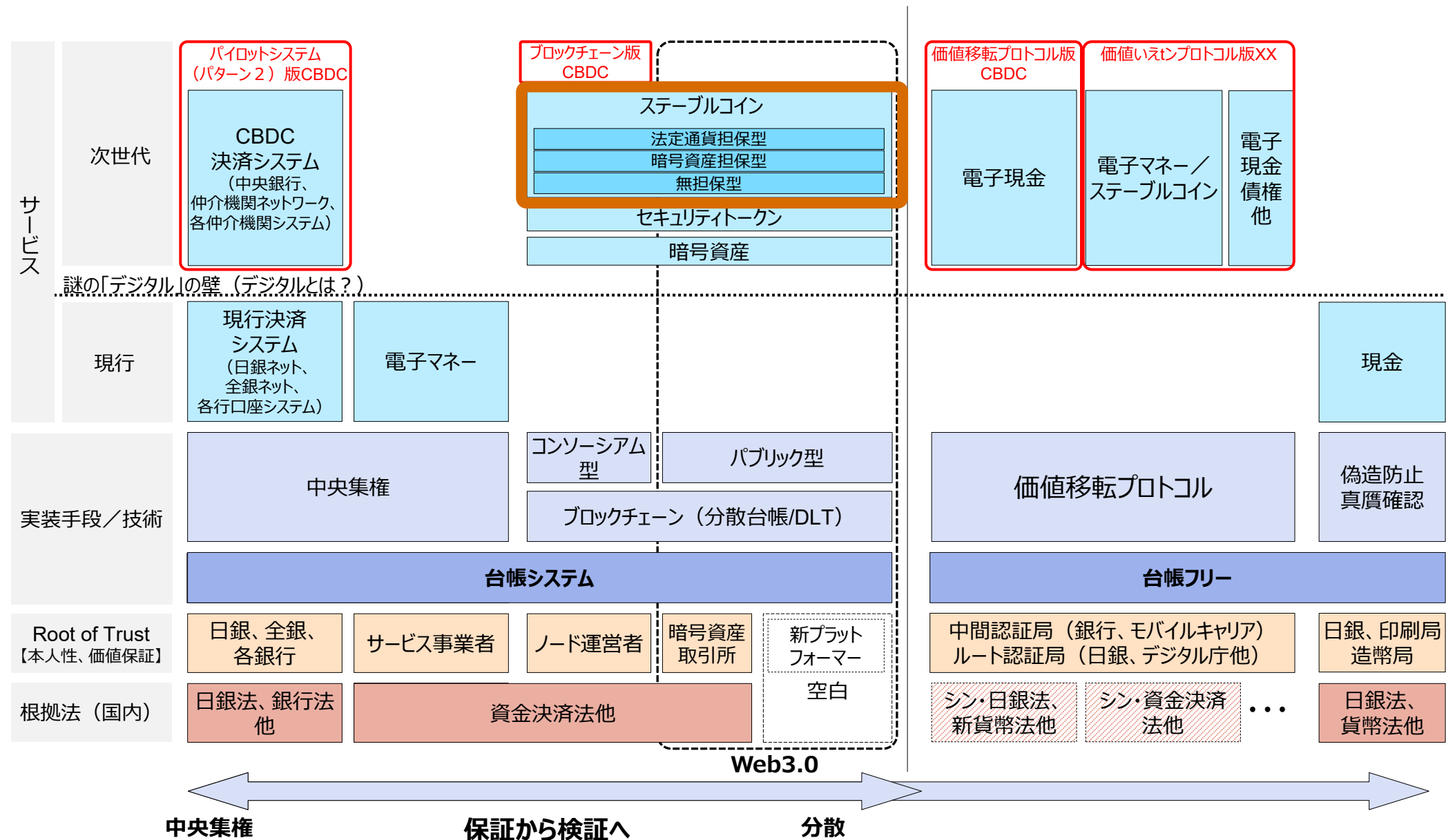
ネットワークによって“**遍在する**” 計算リソース・・・イーテル(**Ether**) → **Ethernet, Ethereum**

ブロックチェーンの一側面：計算リソースの偏在化を背景としたパラダイムシフト

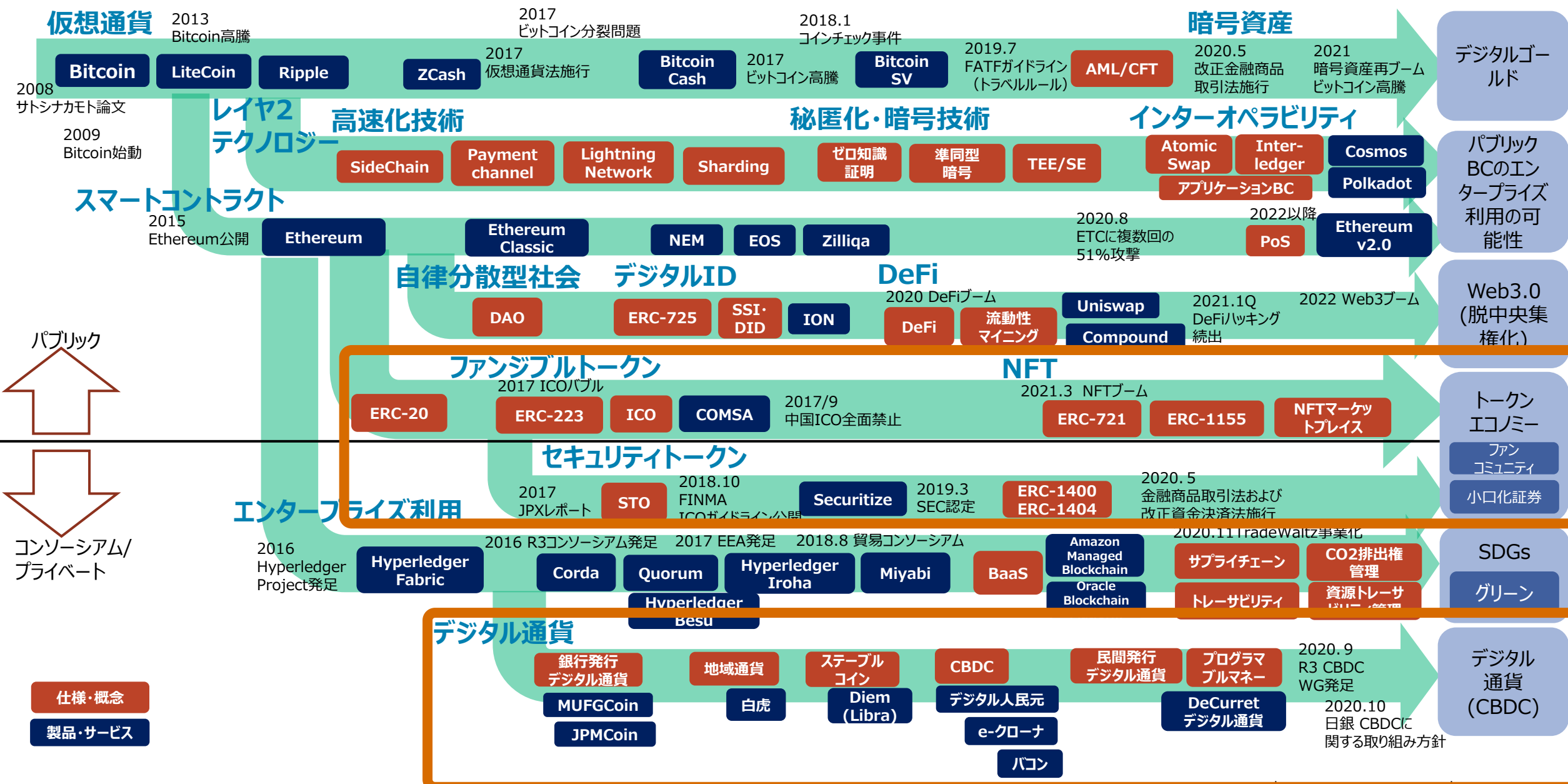
複数主体の合意形成により、流通・共有するデータの信頼性を確保し、非中央集権でのシステム形態を実現可能とした一連の技術的アプローチ



価値移転の世界観 過去・現在・未来



ブロックチェーンを用いたビジネスモデルと技術の変遷



(参考) 金融庁「デジタル・分散型金融への対応のあり方等に関する研究会」

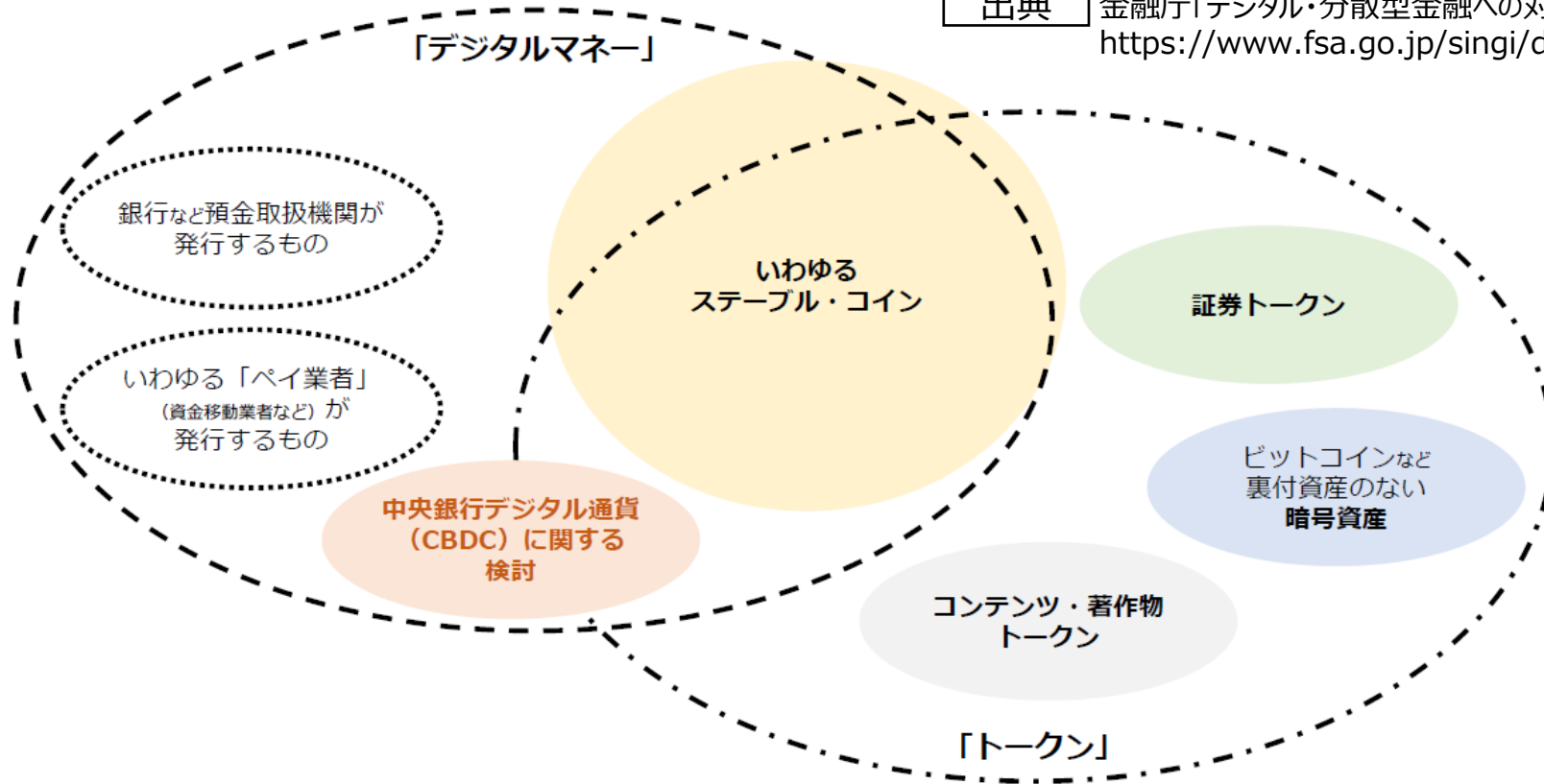
関連する最近の取組み (イメージ)

出典

2021/7/26

金融庁「デジタル・分散型金融への対応のあり方等に関する研究会」

<https://www.fsa.go.jp/singi/digital/gijiroku/20210726.html>



デジタル・アセットの取引等のプラットフォーム

「分散型金融 (DeFi)」

特定の管理者がいない (またはいないと称する) もの

新興企業・既存企業 (特定の管理者) によるもの

2

ステーブルコインとは

◆ 概要

- USDやEURなどの法定通貨と同等の価値を持つように設計された暗号通貨トークン
- 2014年に、米ドルを担保とし常に1:1での交換を保証する形で、最初のステーブルコインTetherが誕生
- ビットコインやその他の暗号通貨が持つ高いボラティリティに対応するためのソリューションとして生まれた背景

◆ 変遷

- 2017年以降、Ethereumブロックチェーンを主な発行先として選ぶステーブルコインが多数誕生
- 2018年から19年にかけては、暗号通貨取引所CoinbaseのUSDC, BinanceのBUSD, HuobiのHUSDなど、取引所が関連するステーブルコインの流通が拡大
- 2020年から現在にかけては、より資本効率を追求したステーブルコインが模索されている

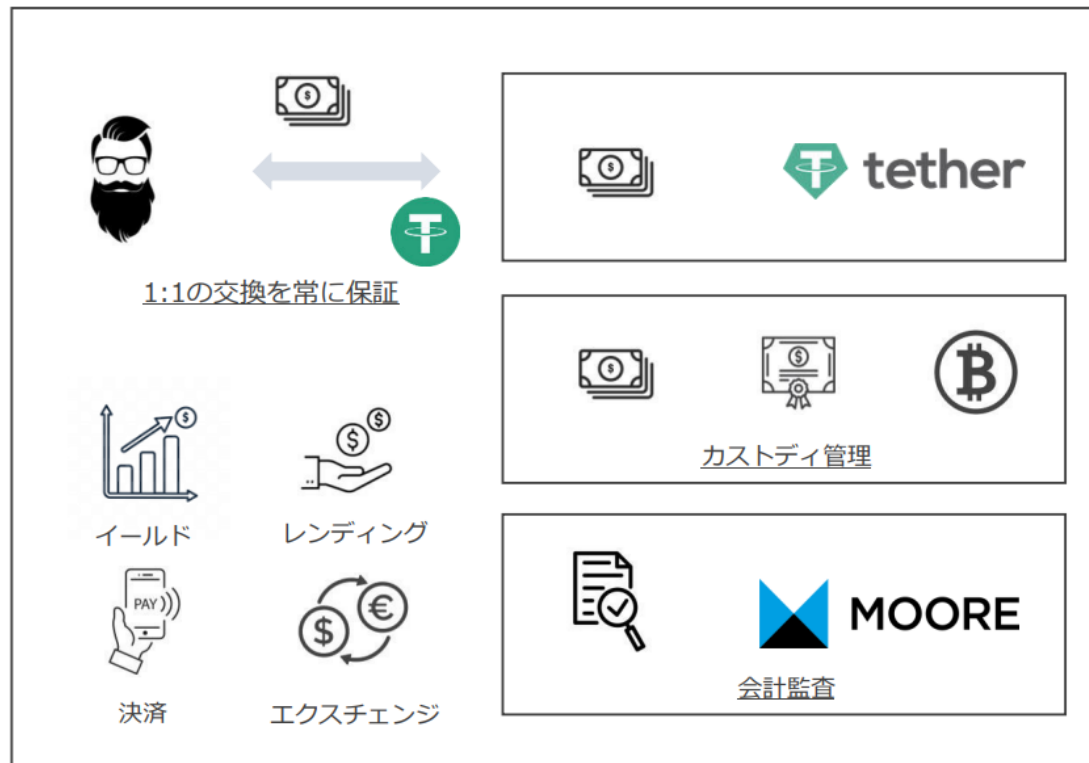


CT AnalySSI, 『ステーブルコインの概要と現状 動向調査レポート』 <https://crypto-times.jp/ctanalySSI-20/>

類型①：法定通貨担保型ステーブルコイン

現金のUSDや現金同等物を担保とすることで1:1の価値の裏付けを維持

フィアット担保の構造(USDTの場合)

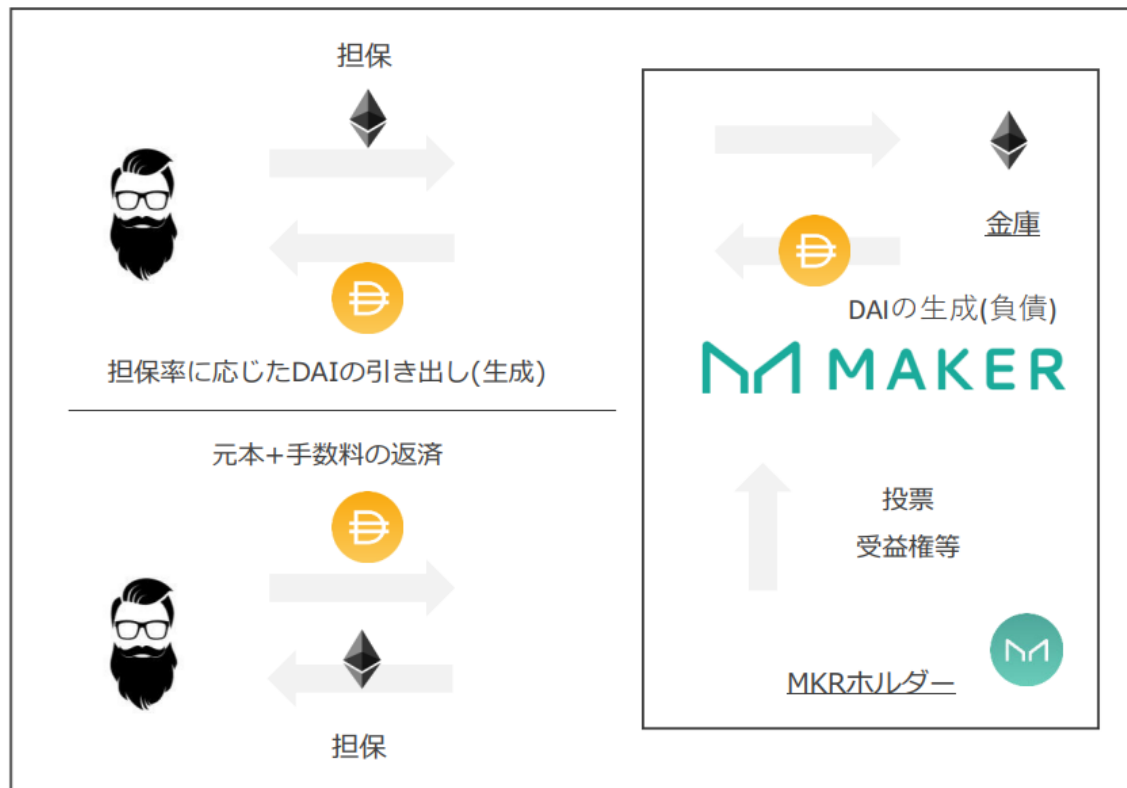


- 一般的に、発行体とカストディへの信頼を前提としており、**発行者が常にユーザーの要求に応じて暗号通貨トークンを1:1で償還可能な状態としておくことが価格の安定につながっている**
- 発行体としての透明性を維持するため、多くのケースでは第三者の会計監査機関による監査が行われ、担保資産の内訳等が公開されている
- **発行母体の国の法律・規制に準拠した形で発行される点**も特徴の一つとされる

類型②：暗号通貨担保型ステーブルコイン

ビットコインやイーサリアムなどの暗号通貨の価値で過剰担保の状態を作ることによって発行

暗号通貨担保の構造(MakerDAOのケース)



CT Analysis, 『ステーブルコインの概要と現状 動向調査レポート』 <https://crypto-times.jp/ctanalysis-20/>

- オンチェーン資産(暗号通貨)による担保により発行される
- 担保となる資産の価格変動リスクが懸念されるため、一般的には過剰担保の状態がシステム側で監視・維持される
- 発行体が第三者ではなく、自律的に動くコントラクトとなるため、コストディを介さず誰もが自分で発行を行うことが可能
- 透明性に関しても会計監査等を必要とせず、エクスプローラー等で常にリアルタイムの状態を監視することができる
- 相場の急落による清算、コントラクトのバグ、法定通貨担保型ステーブルコインの担保組み込みによる二階建て構造などが主なリスク

類型③：無担保型（アルゴリズム型）ステーブルコイン

担保資産を持たず、価格の変動リスクを経済モデル等で調整し常に1ドルに近づける

- アルゴリズムや別のトークンを利用したエコノミクスにより、1ドル付近での価格安定を試みる
- 発行の条件や形態は様々であるが、基本的にはシステムで需給に応じてダイナミックに供給が調整されるようなエコノミクスを導入している
- 無担保であるため価格の崩壊リスクに対する理解も必要とされる
- トークン自体に投機的な需給のスパイクが発生するほか、ペッグの崩壊による不安から売り圧が売り圧を呼ぶスパイラルが発生する可能性

【LUNA-USTの仕組み】

コインの供給量をアルゴリズムでコントロールすることで価格を安定

例：USTの価格が

- ペッグを上回っているとき ($1\$ < 1\text{UST}$)にはUSTの供給量を増加（新規発行）
- ペッグを下回っているとき ($1\$ > 1\text{UST}$)にはUSTの供給量を減少（バーン）



Terra/LUNA事件について ～あるアルゴリズム型ステーブルコインの終焉～

UST価格下落とLUNA価格下落の連鎖によりドルペッグが崩壊



LUNA-USTショック – その他のステーブルコインへの影響

- Tether (USDT) : 一時マイナス乖離、供給量減
- USDC : 供給量増

■ USDT 対 USD



■ USDT時価総額



■ USDC 対 USD



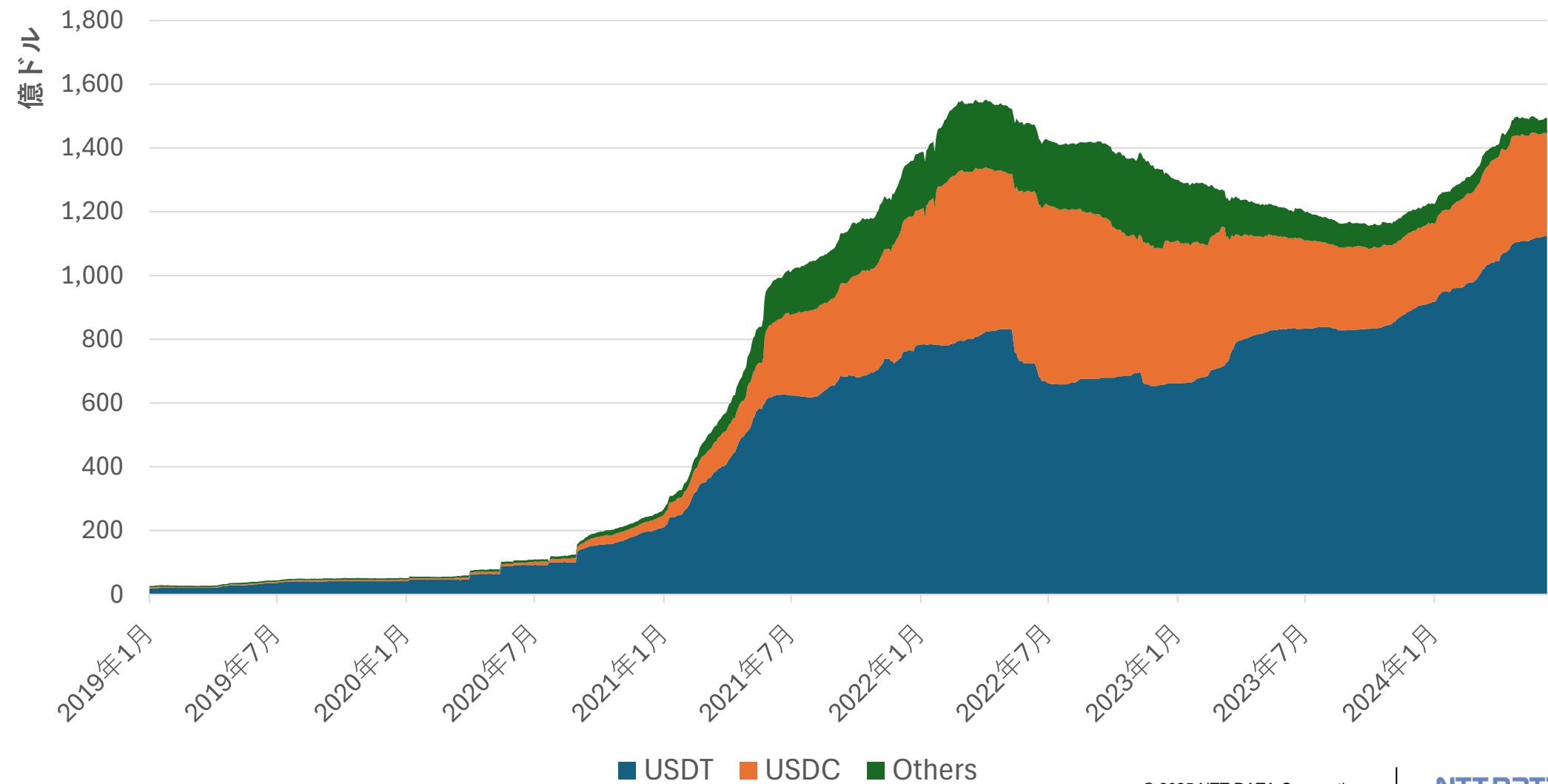
■ USDC時価総額



ステーブルコインの時価総額と内訳

ステーブルコインの市場占有率的にはUSDT、USDCの二つによる寡占状態

ステーブルトークンの時価総額推移



ステーブルコインはどの程度“ステーブル”なのか

代表的な法定通貨担保型（USDT）とアルゴリズム型（USDD）の比較



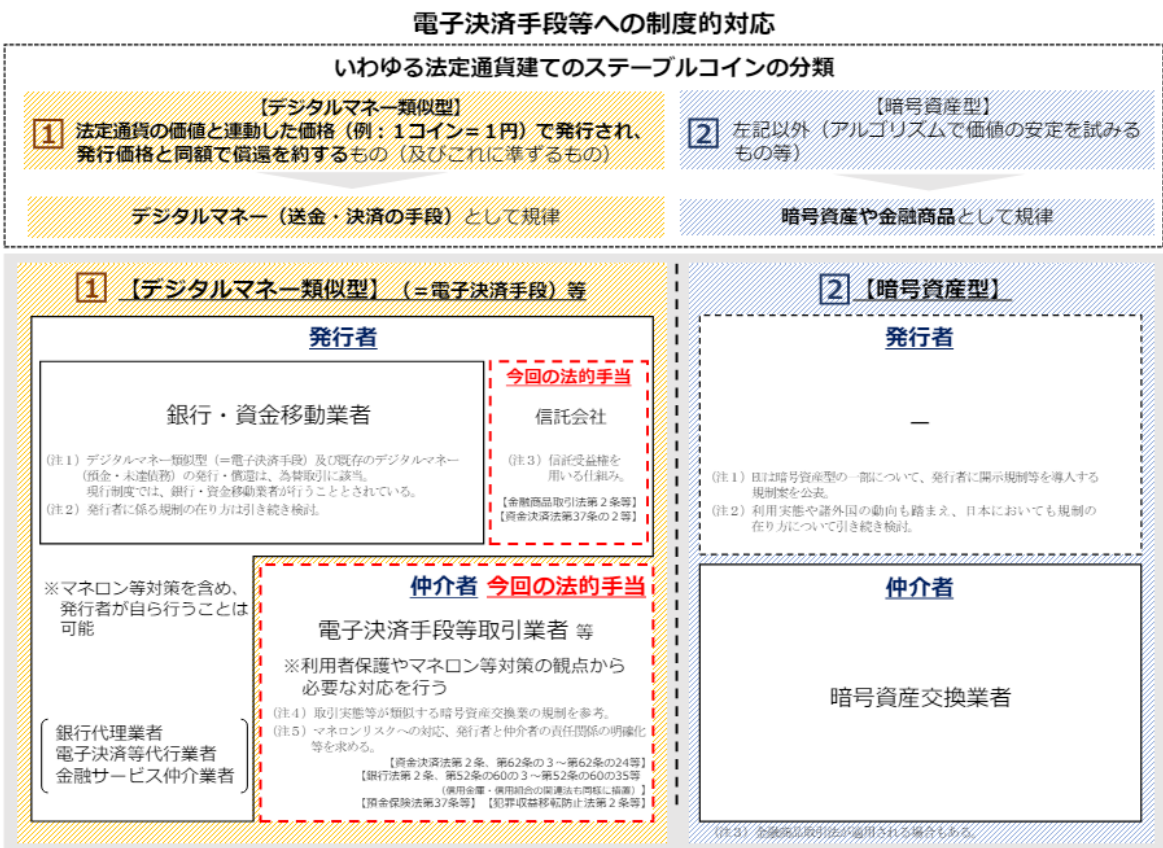
日本でのステーブルコインの法律上の位置づけ

- 2023年6月1日に施行された改正資金決済法において、ステーブルコインは暗号資産とは異なる「**電子決済手段**」に定義された

- ステーブルコインの定義や法規制は世界各国でも曖昧な状況である国が多いため、**日本は世界に先駆けて定義を示したことになる**

- パーミッションレスブロックチェーンを利用して電子決済手段を発行する場合、**相応のAML/CFT対応義務が求められる**
(自民党：web3 政策に関する中間提言より)

- 外国発行のステーブルコインを取り扱う場合、取引業者において十分な**利用者保護措置**が求められる



金融庁の資料より <https://www.fsa.go.jp/common/diet/208/03/setsumei.pdf>

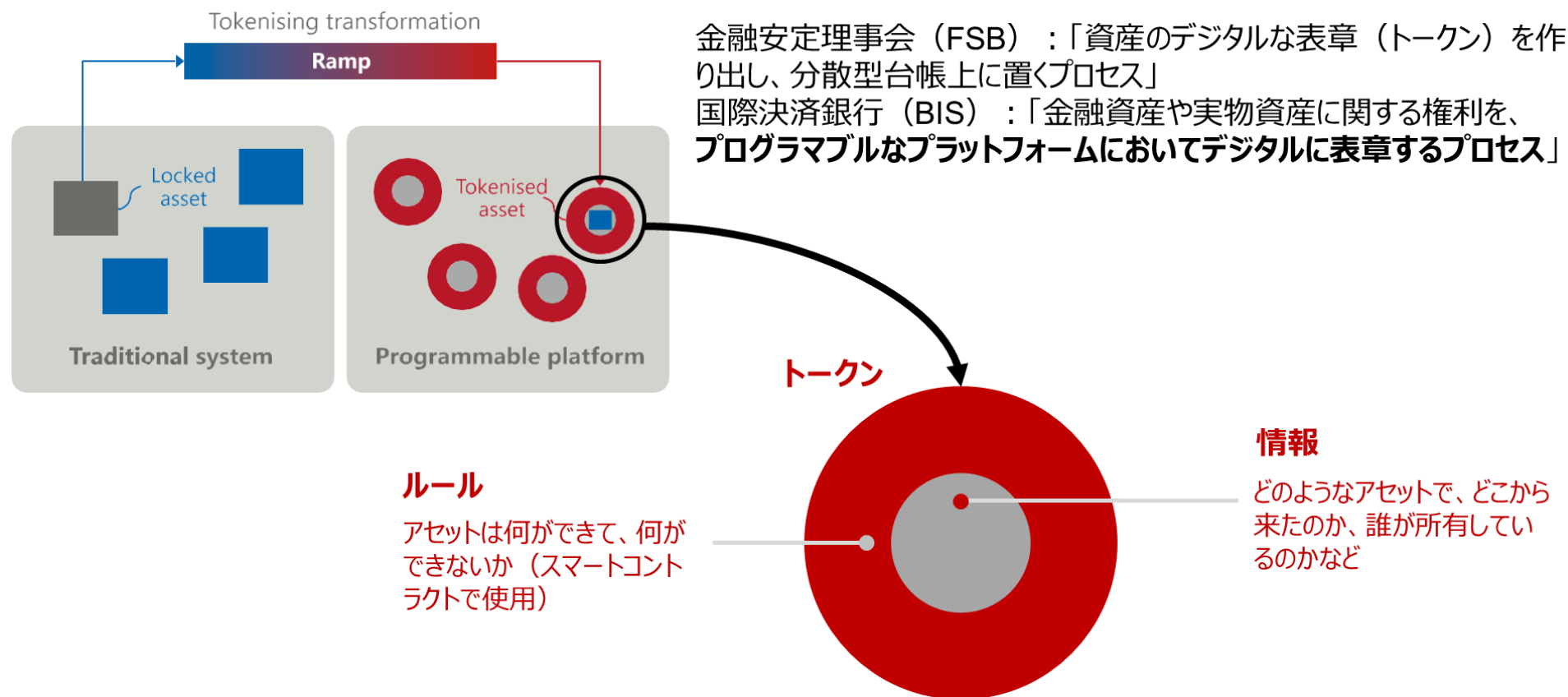
“デジタル”という言葉が意味するところ

“トークン化”と“プログラマビリティ”

トークン化とは

高いプログラマビリティの実現を目指して

「従来の伝統的決済システム上の価値」を「**プラットフォーム自体が実行環境となるシステム上のトークン**」に置き換えるプロセス



集権的な管理者のいない、自律分散的な環境が支えるWeb3

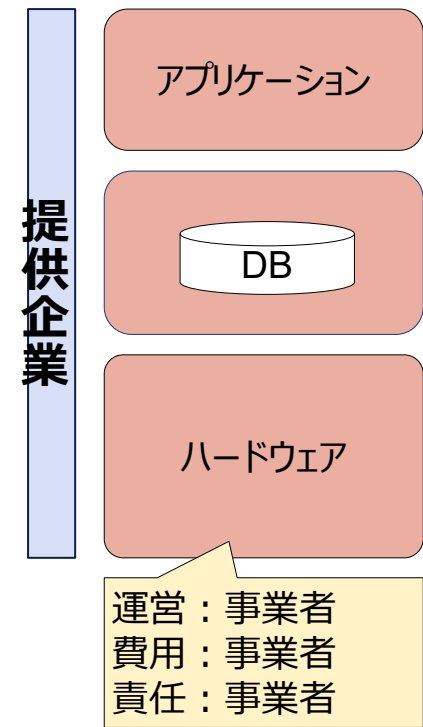
DeFiやNFT等、Web3の多くはスマートコントラクトによって実装・運用される。

スマートコントラクトはブロックチェーンプラットフォームを基盤として動作する。

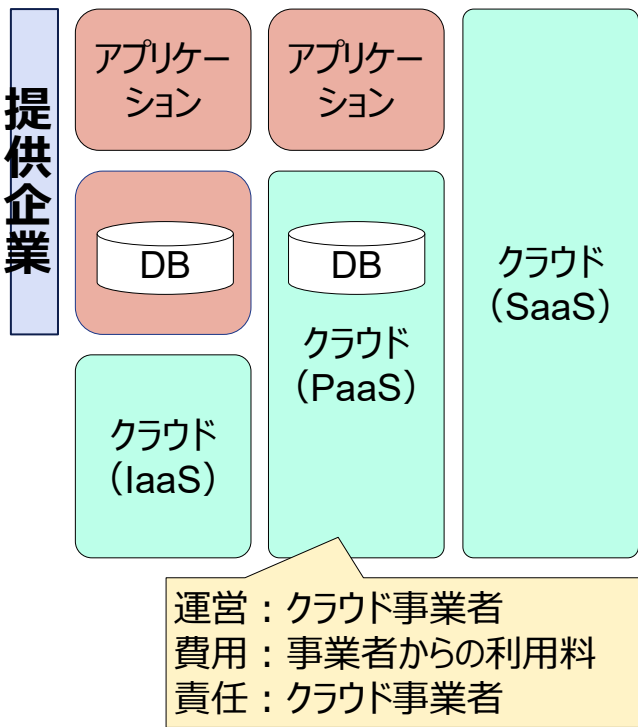
プラットフォームはマイナーによって維持運営される。

Web 3 サービスの運営主体は集権的な存在を排除した**自律分散組織（DAO）**を謳うことが多い

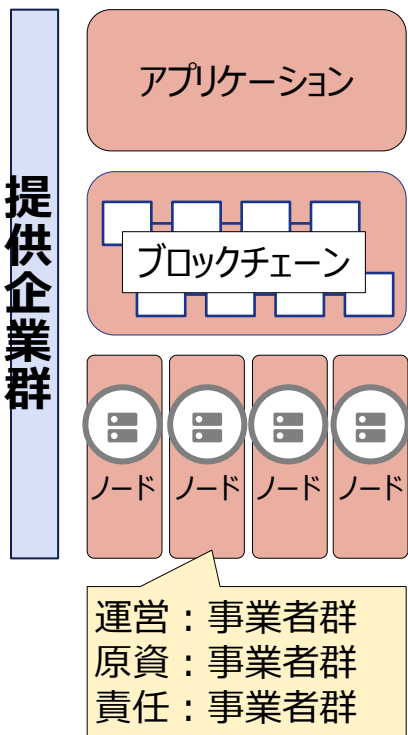
オンプレ環境上に構築



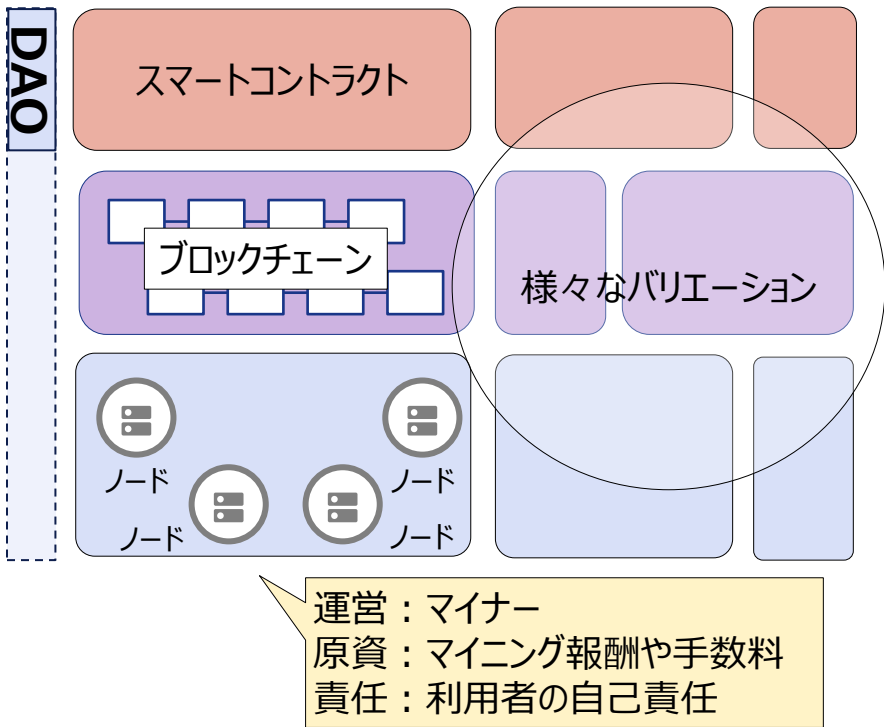
クラウド上に構築



コンソーシアムブロックチェーン



パブリックブロックチェーン上に構築
(Web3、DeFi)

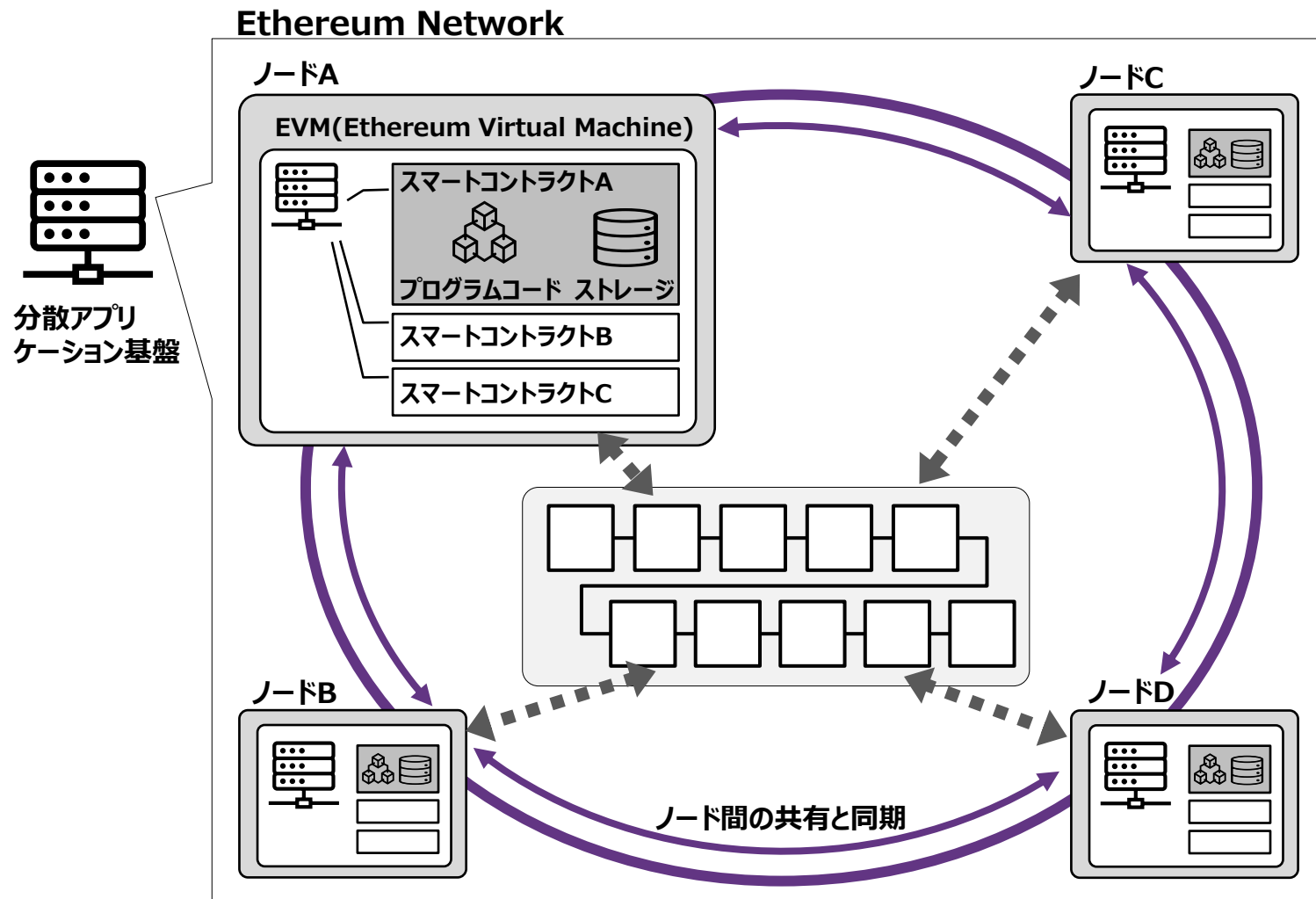


ステーブルコインの技術的側面：プログラマブルなプラットフォーム上での価値移転

基盤としては分散台帳技術とその上で稼動するプログラム技術（スマートコントラクト）を使って実現

トークンの標準規格であるERC-20をベースに実装。Ethereum等のブロックチェーンネットワークを実行環境として動作

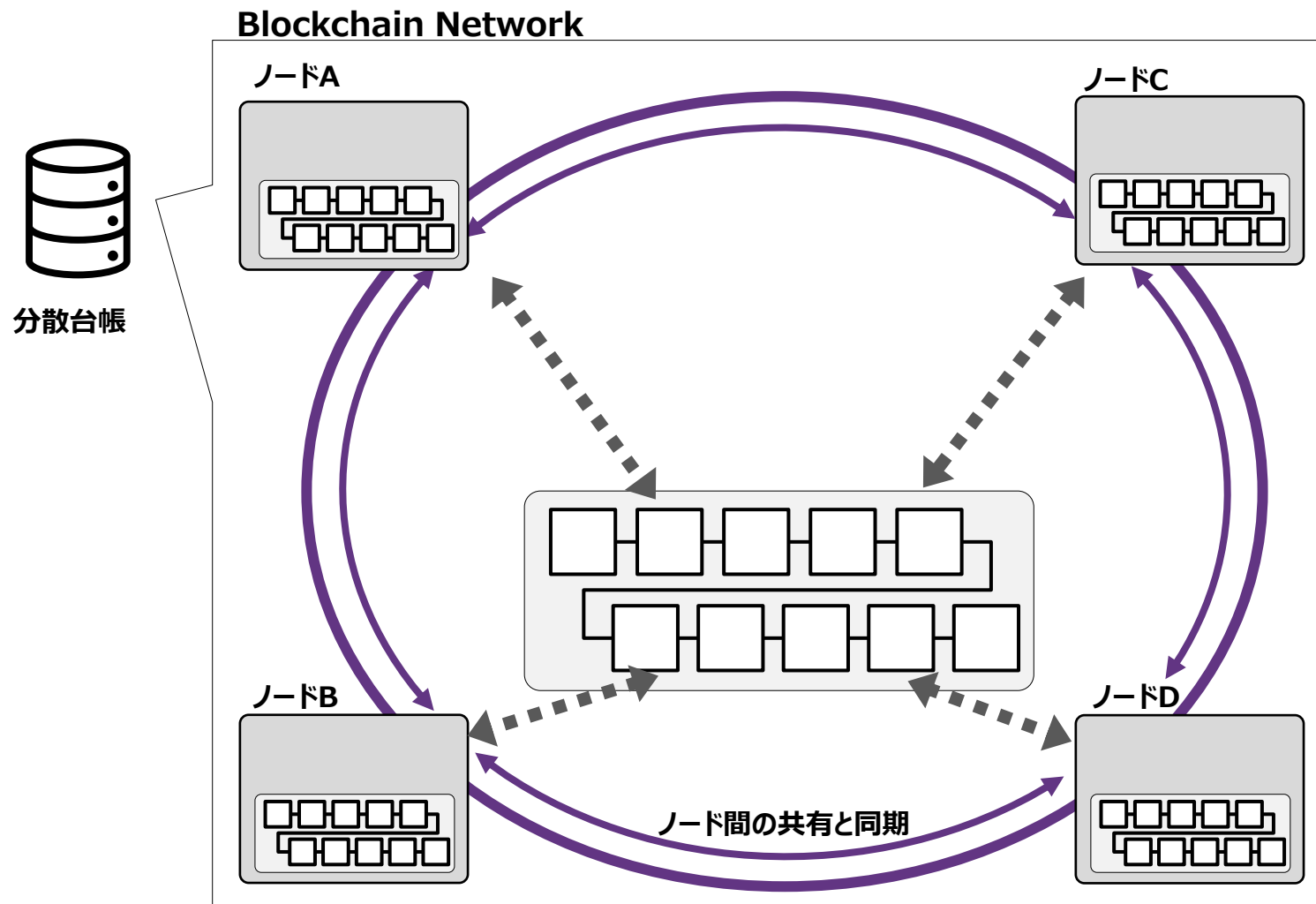
Web3系各種サービスとの連携はEVM等標準規格に則って実現できるため親和性が高い



ブロックチェーンの基本形

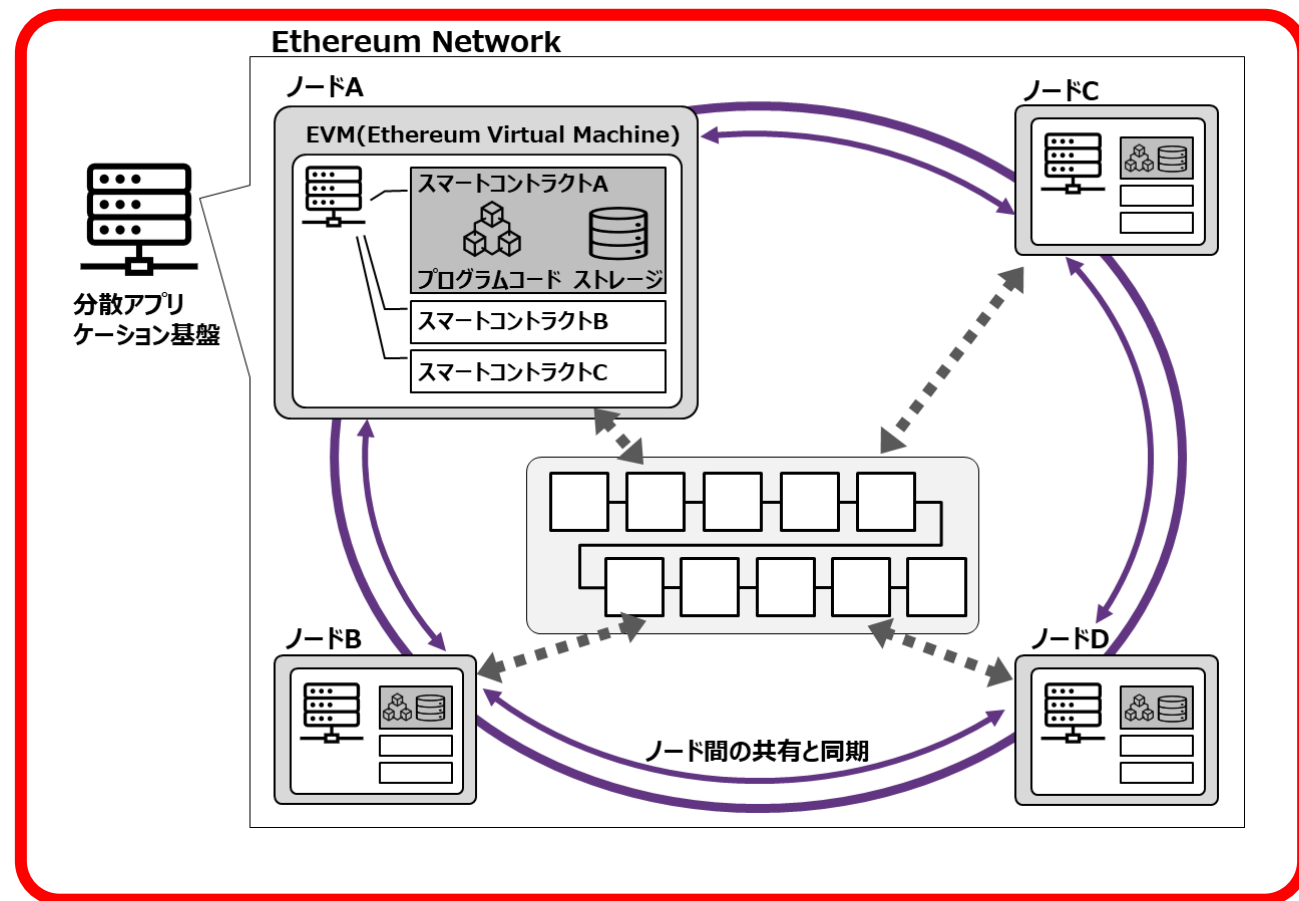
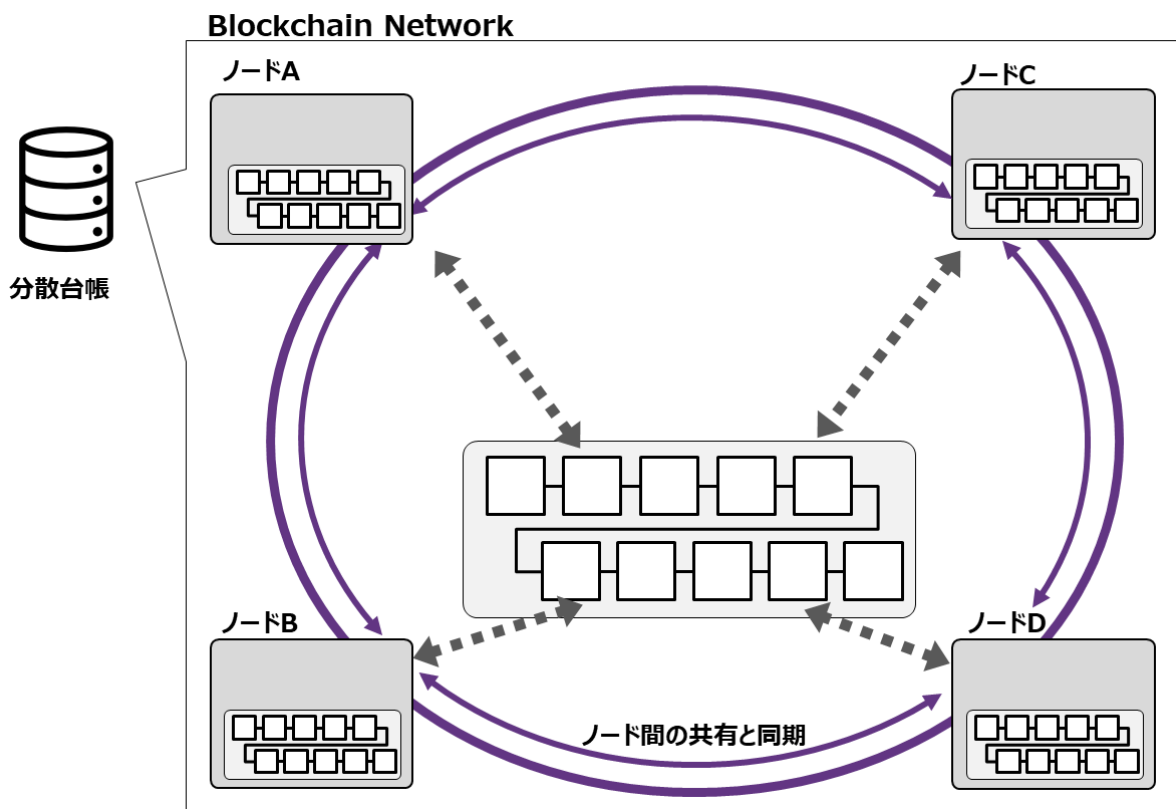
分散台帳としてのBlockchain Network。スマートコントラクトの実行を前提としていない。

ビットコインはこのタイプ（近年は進化してきている）。**ネットワーク全体があたかも一つの台帳であるかのように振る舞う**



スマートコントラクトの実行環境としてのブロックチェーンネットワーク

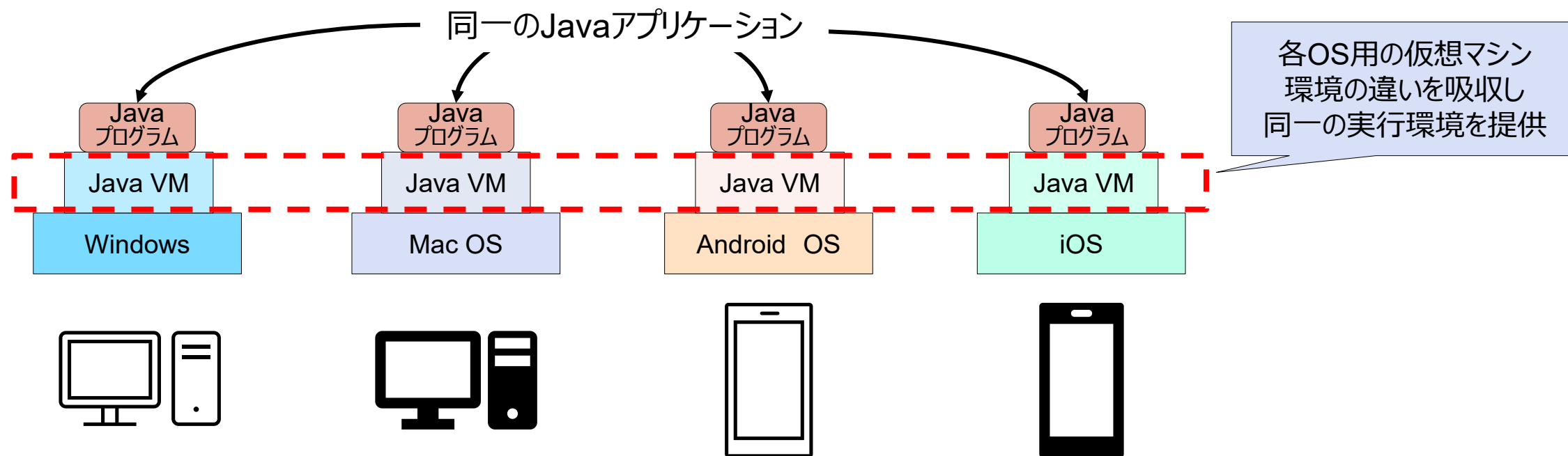
Ethereum等では各ノードにEVM（Ethereum Virtual Machine）と呼ばれる仮想マシンが組み込まれている。
各ノードのEVM上で動作するスマートコントラクトのプログラムソースや処理結果等はブロックチェーン技術によって同期され
ネットワーク全体があたかも一台のコンピュータであるかのように振る舞う（分散アプリケーション基盤）



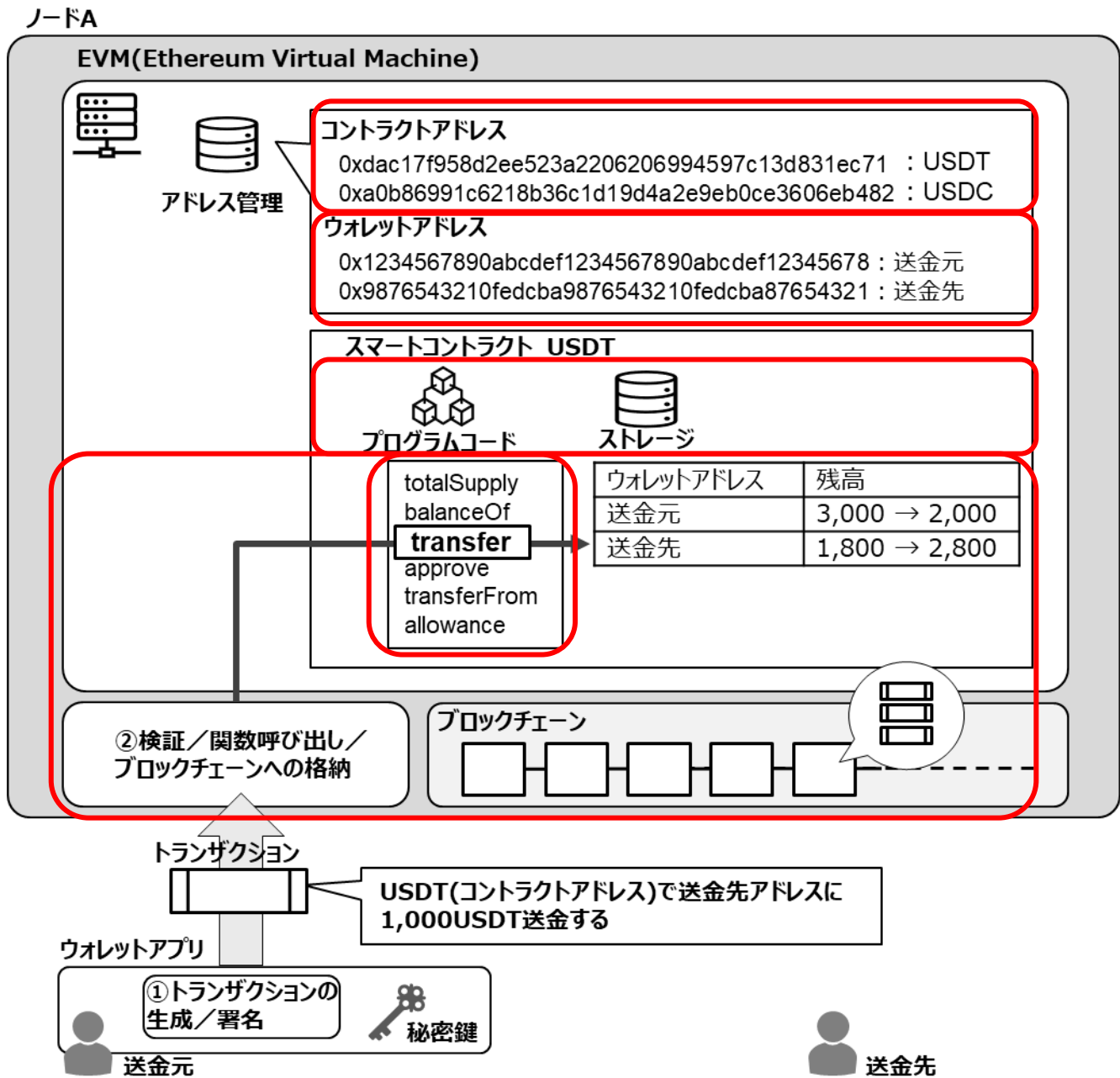
仮想マシン（Virtual Machine）とは

異なる環境（OS等）において同じプログラムが同じように正しく実行できるようにするため、各環境で共通仕様のコンピュータをエミュレートして、その上でプログラムを実行するもの

例）JVM（Java Virtual Machine）



EVMの中で行われていること



アドレス管理を行って、どのノードでも同じアドレスには同じプログラム（スマートコントラクト）が格納されていることを保証（USDTやUSDCのプログラム）

利用者のウォレットアドレスについても同様にアドレス管理される（送金元や送金先ウォレットのアドレス）

各スマートコントラクトにはプログラムのコードやプログラムの処理対象、処理結果、その他のデータを管理するストレージ等が含まれている

USDTはトークン規格ERC-20をベースにしたトークン进行处理する関数をプログラムに含んでいる

EVMはトランザクション要求を受け取ると上記関数を呼び出して送金処理を実行する

コンピュータの中で行われている基本的なこと

メモリーの中に格納されたプログラムの場所（メモリアドレス）を指定してプログラムを呼び出し、
メモリーの中に格納されているデータを変化させる



コンピュータへの命令：
「C330から格納されているプログラムを
呼び出してC3D0に格納されている
データを変更して」

メモリアドレス

プログラムやデータ

Add	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	Sum
C300	60	69	01	05	07	7C	BA	38	08	20	04	7D	BB	38	02	B7	: 99
C310	C9	29	30	06	B7	ED	52	B7	18	0C	7C	BA	38	08	20	04	: 93
C320	7D	BB	38	02	ED	52	CB	10	0D	20	E6	78	2F	08	4F	08	: A5
C330	0C	20	02	ED	44	37	C9	CD	47	C3	CB	22	CB	13	CB	22	: EE
C340	CB	13	16	00	F0	15	C9	C5	43	1E	73	CD	0D	BA	4A	50	: 89
C350	1E	73	CD	0D	BA	7B	81	5F	30	01	14	7A	CB	10	30	02	: 4C
C360	D6	73	53	5F	C1	C9	C5	E5	79	2F	4F	CD	A8	C2	E1	C1	: FF
C370	CD	BD	C2	C9	00	00	00	00	00	00	00	00	00	00	00	00	: 15
C380	21	00	DE	11	01	DE	01	FF	05	36	00	ED	B0	C9	00	00	: 90
C390	0E	05	06	03	21	30	CC	CD	6A	C7	21	36	CC	11	00	C0	: 2B
C3A0	06	4A	CD	75	C7	06	03	21	00	E3	CD	6A	C7	06	03	21	: 8E
C3B0	7A	CC	CD	6A	C7	11	03	00	06	4A	21	78	CC	CD	75	C7	: 16
C3C0	06	03	21	4A	E3	CD	6A	C7	06	03	21	78	E5	CD	6A	C7	: DA
C3D0	11	03	00	06	42	21	76	E5	CD	75	C7	11	00	C0	06	42	: FA
C3E0	21	7E	E5	CD	75	C7	06	03	21	C8	F9	CD	6A	C7	0E	02	: 86
C3F0	11	FF	FF	21	76	D7	CD	C1	BA	21	7C	D7	CD	C1	BA	21	: A2
Sum:	36	C1	E6	60	1A	FC	35	32	83	E8	73	17	98	A9	47	CC	: 03

EVMの中で行われていることも（すごく大雑把にいて）同様

トークンの標準的規格 “ERC-20”

イーサリアムブロックチェーン上でトークンを発行・管理するための標準規格（Ethereum Request for Comments）
トークンの転送や残高確認、承認などの基本的な機能を提供する関数が定義されている。

関数	説明
totalSupply	トークンの総供給量を返す
balanceOf	指定されたアドレスのトークン残高を返す
allowance	指定されたアドレスが使用できるトークン残高を返す
transfer	トークンを別のアドレスに送信する
approve	指定されたアドレスに一定量のトークンを使用する許可を与える
transferFrom	承認されたアドレスからトークンを送信する

ステーブルコイン向けトークン規格、主要ステーブルコイン概要

トークン規格	説明
ERC-20	- 一般的なFungible Tokenの規格。 - 基本的にFTはこの規格の拡張で実装されている。USDT、USDC、DAIもこの規格に準拠。
ERC-621	- ERC20に供給量変化機能を追加した規格 - EIPにてこの規格が確認できないため、Ethereum財団が正式に承認した規格ではない可能性がある。ERC20から容易に拡張して供給量を変化できるためか、利用事例の確認ができず
ERC-777	- ERC20に各種機能を追加した規格 - 一部機能が悪用される可能性があり使用は非推奨（ERC-777 トークン規格 ethereum.org）

主要ステーブルコイン	説明
USDT	- 法定通貨担保型ステーブルトークン。 - 時価総額が最も大きいステーブルトークン。3カ月ごとに監査レポート公開。
USDC	- 法定通貨担保型ステーブルトークン。 - 時価総額が二番目に大きいステーブルトークン。毎月監査レポート公開。
DAI	- 暗号資産担保型ステーブルトークン。 - MakerDAOによって管理されているステーブルトークン

トークン規格・ステーブルコイン比較の評価軸

- 評価軸選定について
以下の二つの観点で評価軸を選定
 - ERC777はERC621,20を拡張したもののため、ERC777でメソッドとして実装されている機能
残高確認、送金、供給量の変更、オペレーター、フック、誤送金
 - ステーブルコイン・セキュリティトークンで一般的に実装されている機能
ホワイトリスト・ブラックリスト・一時停止・アップグレード

評価軸	評価軸説明
残高確認機能	アドレスを引数として残高を出力するメソッドの有無
送金	宛先アドレスとトークン数を引数としてトークンを送金するメソッドの有無
総供給量の変更	トークンを発行・償却して供給量を変更するメソッドの有無
権限設定機能	指定したアドレスに特権的な権限を付与するメソッドの有無
フック機能	トークンの送受信時に特定の処理させるようにを設定できるメソッドの有無
誤送信防止機能	送金先のアドレスがトークンを扱う機能の有無を確認するメソッドの有無
ホワイトリスト機能	設定したアドレスのみに送信を制限するメソッドの有無
ブラックリスト機能	設定したアドレスへの送信を制限するメソッドの有無
一時停止機能	全てのトークンの送金を一時的に停止させるメソッドの有無
アップグレード機能	コントラクトの実装を後から変更するメソッドの有無

トークン規格比較表・主要ステーブルコイン比較表

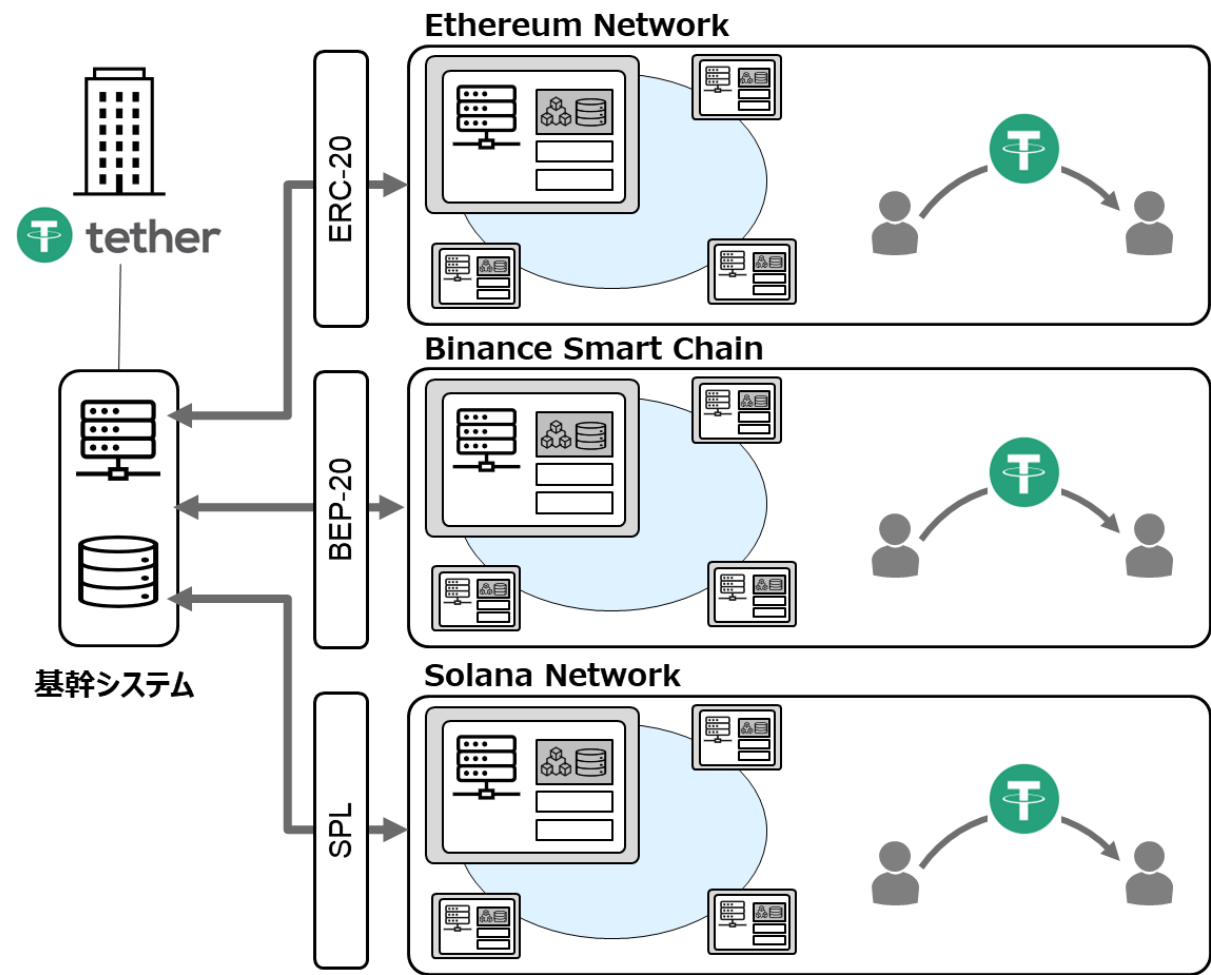
評価軸	トークン規格			主要ステーブルコイン		
	ERC-20	ERC-621	ERC-777	USDT	USDC	DAI
残高確認機能	○	○	○	○	○	○
送金	○	○	○	○	○	○
総供給量の変更	×	○	○	○	○	○
権限設定機能	○	○	○	○	○	○
フック機能	×	×	○	×	×	×
誤送信防止機能	×	×	○	×	×	×
ホワイトリスト機能	×	×	×	×	×	×
ブラックリスト機能	×	×	×	○	○	×
一時停止機能	×	×	×	○	○	×
アップグレード機能	×	×	×	○	○	○

ステーブルコインにおけるサイロ化

Ethereumへのスマートコントラクト負荷集中による性能劣化、実行コスト高騰を背景に各種ブロックチェーンネットワークへ分散
一方で各ネットワークの規格互換性の問題や、異なる台帳間の接続性の課題からサイロ化してしまっている

ブロックチェーンネットワーク	時価総額	VM規格	トークン規格
Ethereum (ETH)	\$3148億	EVM	ERC-20
Binance Smart Chain (BNB)	\$762億	BSCVM	BEP-20
Solana (SOL)	\$670億	Solana Runtime	SPL
TRON (TRX)	\$114億	TVM	TRC-20
Avalanche (AVAX)	\$81億	AVM	ARC-20
Polygon (MATIC)	\$40億	EVM	ERC-20
Arbitrum (ARB)	\$18億	EVM	ERC-20
Algorand (ALGO)	\$10億	Algorand VM	ASA
EOS (EOS)	\$7億	EOSVM	EOSIO

ベースは同じでありつつも、独自拡張等のために複数の規格が存在



※ネットワーク間の送金にはブリッジサービスや発行者のツール等を使う方法もあるが、資金洗浄のリスクが指摘されており、取引所経由の送金が現実解か

金融当局サイドから見たステーブルコインの課題

“ステーブルコインは、デジタルの無記名証券に似た、移転可能な発行者の債権で、ステーブルコインを使用したペイメントは、ある所有者から別の所有者へ**発行者の負債の移転**である。

ステーブルコイン発行者のバランスシートを更新する必要はなく、**中央銀行のバランスシートによるセトルメントもない**。ステーブルコインを持っている人は誰でも、発行者に対する債権をもち、発行者の同意や関与を必要とせずに、その債権を移転できる。

ステーブルコインは取引可能だが、その**価値は額面と異なる可能性があり、マネーの単一性を損なう**。ステーブルコイン間で流動性に差異がある、あるいは裏けの質や発行者の特性の違いにより、発行者の信用力に差異が生じる場合、単一性を逸脱する可能性がある。”

これらの理由に加えて、**明確な規制や監督の枠組みがなく、最後の貸し手としての中央銀行が関与しないことにより**、ステーブルコインの価値が裏付けを失った例が複数ある。

BIS「III. Blueprint for the future monetary system: improving the old, enabling the new」
<https://www.bis.org/publ/arpdf/ar2023e3.htm>

現行金融システムの課題とUnified Ledgerによる解決

デジタルマネーは通信ネットワークのエッジにあって、銀行やノンバンクが運営する**サイロ化された独自DB**に存在し、これらのDBと接続するには**外部のメッセージングシステムが必要**である。

メッセージ、照合、セトルメントの分離によって遅延が発生する可能性があり、完了したアクションが参加者には未完了に見えることが多い。その結果、長期間エラーに気づかずに、エラー解決にコストがかかり、運用リスクが増す可能性がある。

これらのことから**ペイメントプロセスはコストがかかり、面倒で、遅く、不透明であり、ユーザー要求の変化に対応できない可能性**がある。

同一プラットフォーム上に民間のトークン化マネーとCBDCを保有することにより、サイロ化したDB間で順次メッセージを送信する必要がなくなる→**2つのアセットを同時に交換**する（相手が送金したときのみ送金する）**アトミックな決済**が可能になる。

上記プロセスにおける、ある仲介機関から別の仲介機関へのペイメントの**ホールセール決済もホールセールCBDCで即時**に行う。

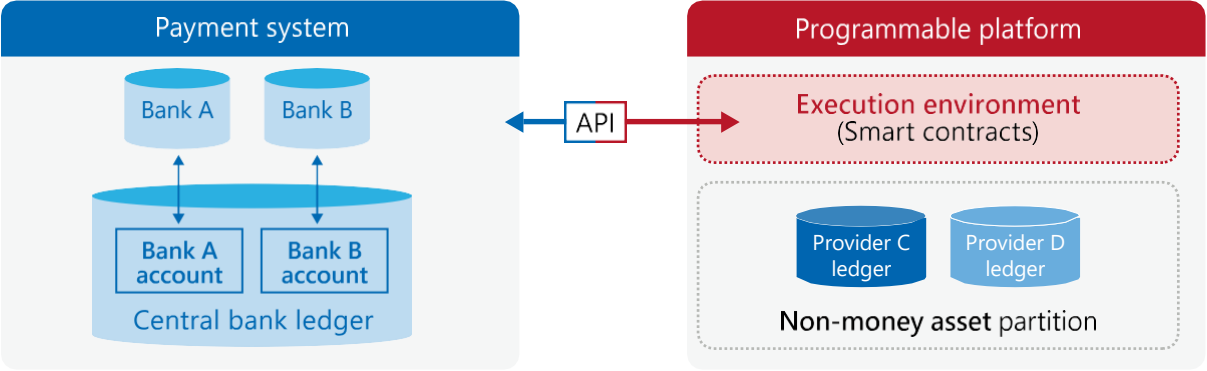
適切なアクセスコントロールを有するパーティション化したデータ環境を使用することで、**取引当事者には完全な透明性を確保して、取引当事者以外には取引を秘密**にできる。

同一プラットフォーム上でメッセージとペイメントレールを結合することで、unified ledgerは**ペイメントプロセスにおける遅延を排除して、決済リスクを軽減**する。

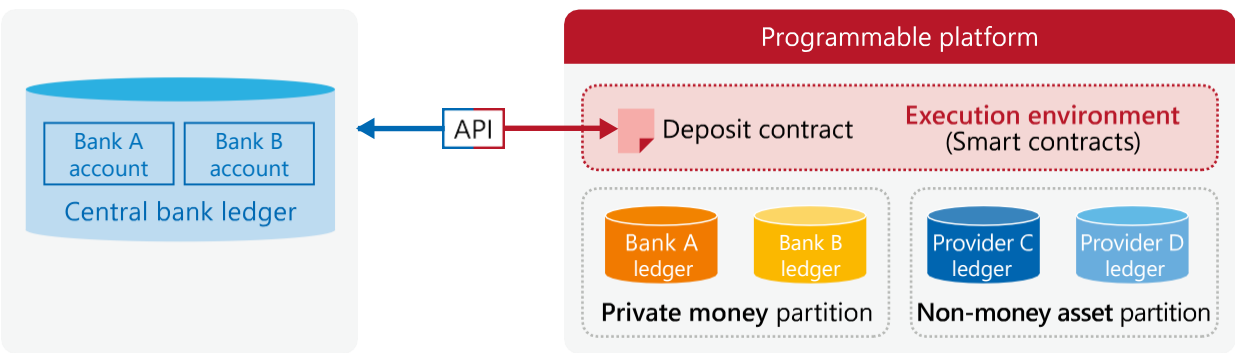
Unified Ledger構想

CBDC、Private Money（デポジットトークン）、アセットトークン等全てを統合した台帳で管理すれば安全性もサイロ化も、様々な課題を解決できるのではないか、という構想

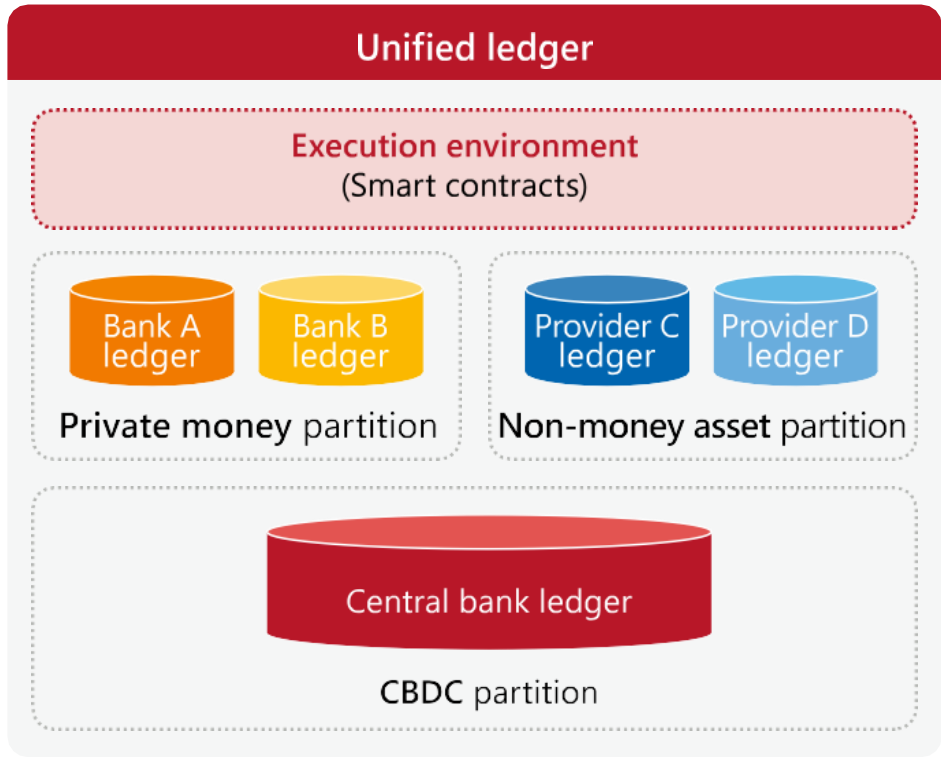
A: ペイメントメッセージモデル



B: 民間トークン化台帳モデル



C: 本格的なunified ledger



BIS「III. Blueprint for the future monetary system: improving the old, enabling the new」
<https://www.bis.org/publ/arpdf/ar2023e3.htm>

The image features a low-angle, wide shot of a modern city skyline under a clear blue sky. Two prominent skyscrapers with white and blue facades dominate the center. Other buildings of varying heights are visible in the background and foreground. The scene includes street-level details like traffic lights, trees, and a small circular structure at the base of the main buildings. The overall tone is professional and urban.

NTT data