

BBLウェビナー プレゼンテーション資料

2023年3月29日

DXの思考法とスタートアップ：
「DXの思考法」セミナーシリーズ総集編

経済産業省大臣官房Web3.0政策推進室
課長補佐 板垣 和夏

Web3.0事業環境整備の考え方

2023年3月29日

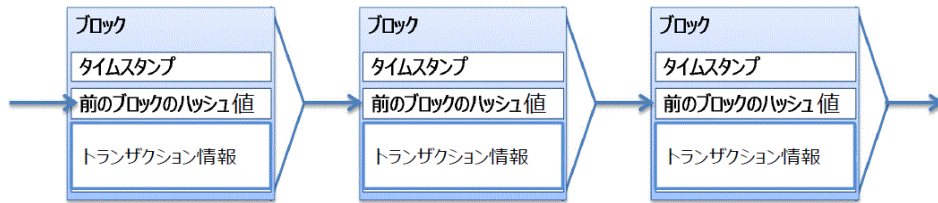
大臣官房 Web3.0政策推進室

板垣 和夏

ブロックチェーン技術について

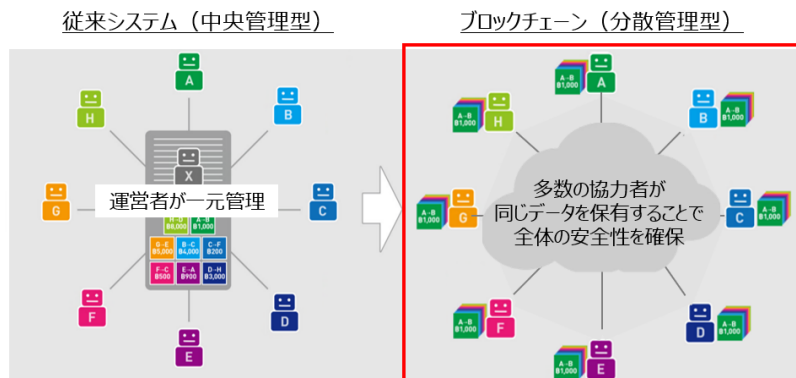
- 一つ一つの取引履歴（ブロック）が1本の鎖のようにつながる形で**情報を記録する技術**。過去の特定のブロックを改ざんするには、それ以降に発生した全ての取引について改ざんが必要であり、**改ざんが極めて困難であるため、安全性が高い**とされる。
- また、**全ての完全な取引データを幾つかの主体が同時に管理・保存**するシステムを採用。仮に、一つのデータが破壊されても、別の主体が持っているデータが無事であれば、当該システムの稼働には問題が生じず、**システム稼働の連続性も確保**される。

ブロックチェーン概念図



あるブロックが少しでも改ざんされるとそれ以降のブロックのハッシュ値*が全く異なる値をとるため、改ざんが困難となる。

*任意のデータから一定の計算手順により求められた特定の長さの値。



ブロックチェーンの特徴 ※パブリック型の場合

- | | | |
|---|------------|--|
| 1 | 分散性 | 中央管理者ではなく複数の主体が全ての完全な取引データを保持（分散管理） |
| 2 | 改ざんが極めて困難 | 過去の特定のブロックを改ざんするには、それ以降に発生した全ての取引について改ざんが必要
※悪意のある者が協力して承認者の51%以上を占めた場合改ざん可能である点は留意 |
| 3 | 永続性 | 一つのデータが破壊されても、別の主体が持っているデータが無事であれば、システム稼働の連続性が確保（企業の倒産等にデータの保持が左右されない） |
| 4 | 透明性 | ブロックチェーン上のデータは、検証性を高めるため公開されており、誰でも閲覧可能 |
| 5 | スマートコントラクト | プロセス・取引の自動化が可能（ある条件を満たした場合の自動的なプログラム実行が可能） |

パブリックチェーンの始まり：暗号資産「ビットコイン」

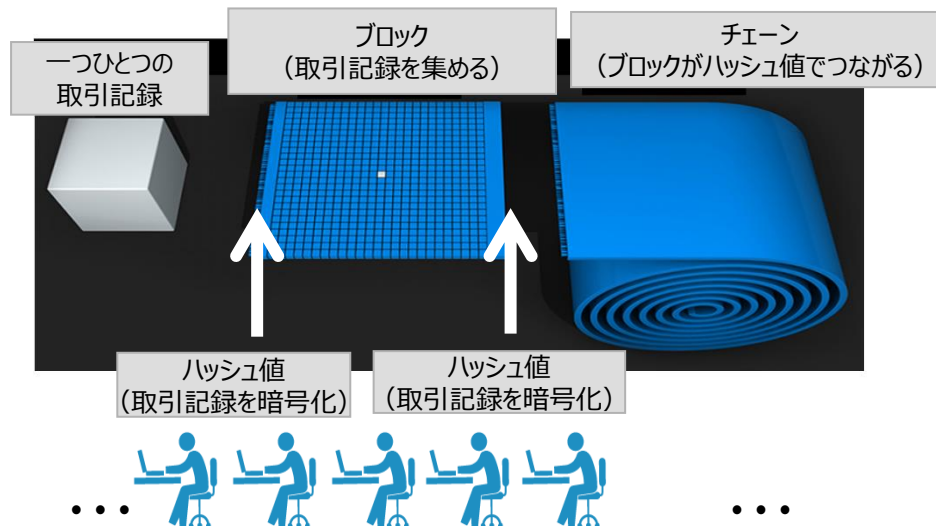
- 2008年に“Satoshi Nakamoto” 名で公開された「ホワイトペーパー」をもとに、コア開発者群によってブロックチェーン技術で開発・公開されたビットコイン（BTC）の発行プログラムが、コインの自動発行を始めた。
- ビットコインでは、原則、「口座Aから口座Bに1BTCを送金する」といった決済に利用される。なお、取引はBlockchain.com等の公開サイトから常時閲覧可能・追跡可能だが、匿名性があり個人に紐づけはされない。

“マイナー”が取引をブロックチェーンに記録し、BTCを得る

「口座Aから口座Bに1BTCを送金」といった取引記録を「ブロック」にまとめ、取引情報の文字列をハッシュ値（※）に転換して記録することで、ブロックを一本の「チェーン」としてつなげる。

その後、あるブロックが改ざんされると、それ以降つながるブロックのハッシュ値が全く異なる値をとるため、改ざんを防げる。

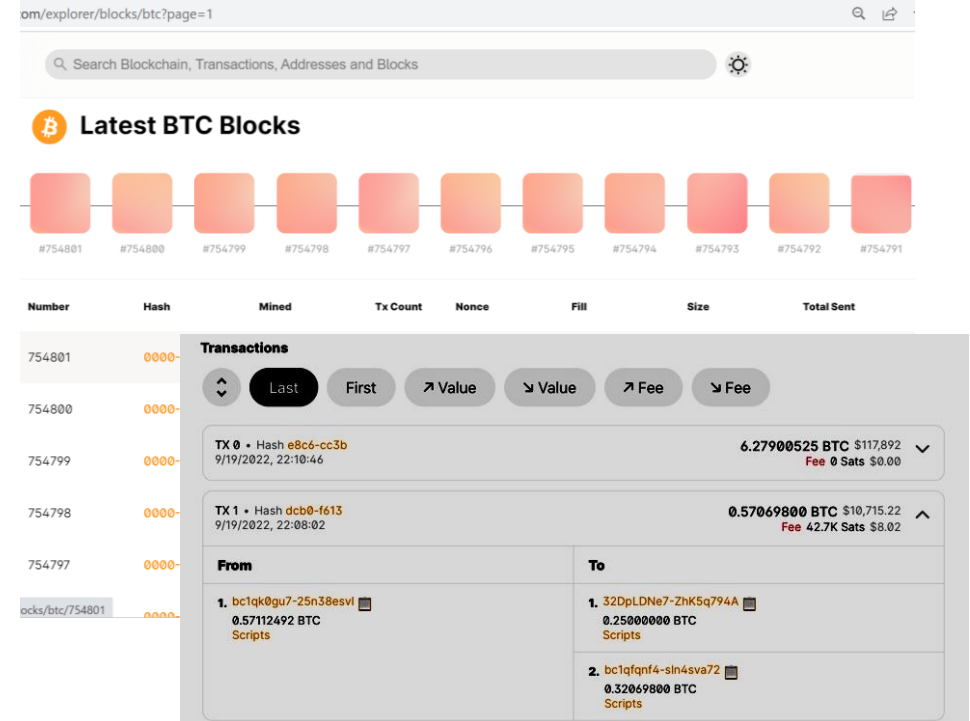
※ハッシュ値：「口座Aから口座Bに1BTCを送金」という取引記録の文字列を、一定の計算手法で特定の長さの値に暗号化した値。



「マイナー」（ハッシュ値の計算競争で、6.25BTC（現時点）の報酬を獲う“コイン採掘人”）

全ての取引情報は「匿名」だが、閲覧・追跡可能

ブロックチェーンに記録された全ての取引記録（ビットコインアドレスと取引価値）は常時公開されており追跡も可能だが、ビットコインアドレス（口座）は個人に紐づけできない。

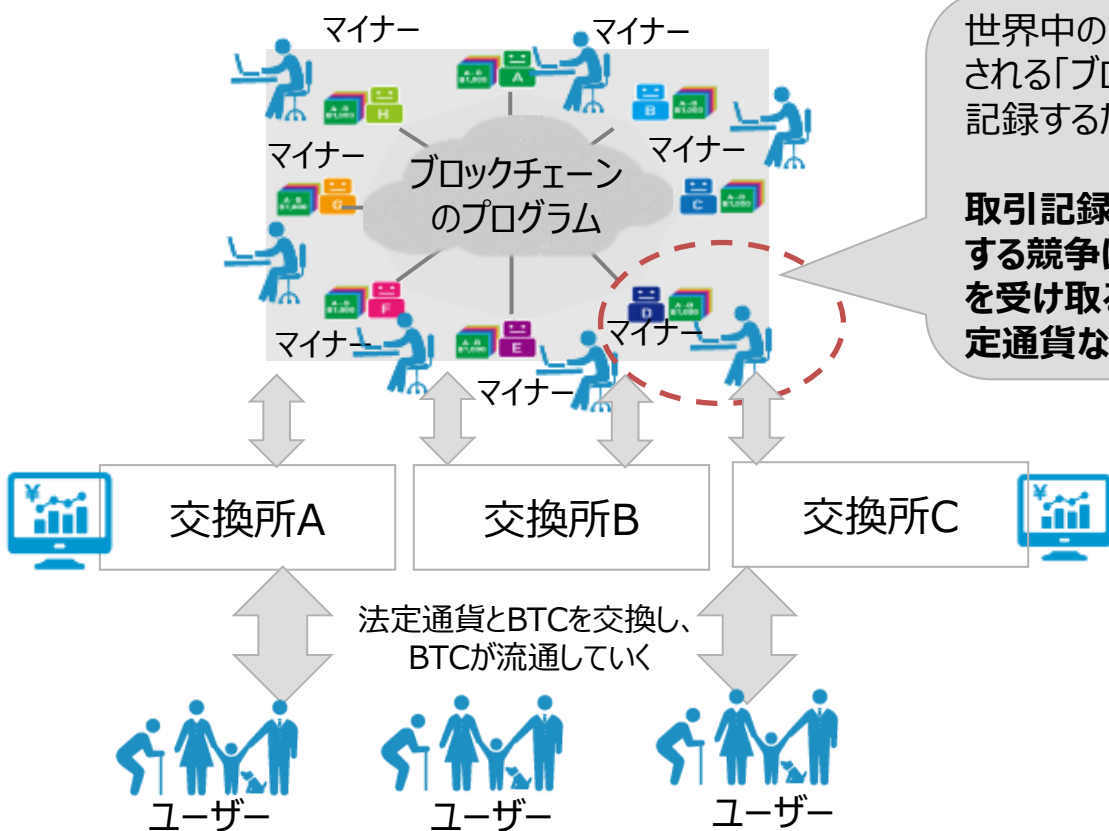


ビットコインの発行と流通の仕組み

- 膨大なコンピュータパワーを用意してビットコイン取引の承認・記録作業を競う“マイナー（コイン採掘人）”に、**報酬として新規ビットコイン（2022年11月末時点で6.25BTC＝約1,400万円）が自動発行される仕組み。**
- ビットコインは、①「発行上限」は2,100万BTC（2021年秋時点で9割弱は発行済）、さらに②概ね4年に1度「マイナー報酬の半減期」が訪れることもプログラム化されており、**通貨価値の下落防止を意図。**

マイナーが記録作業報酬として獲得したBTCが、転々流通していく仕組み

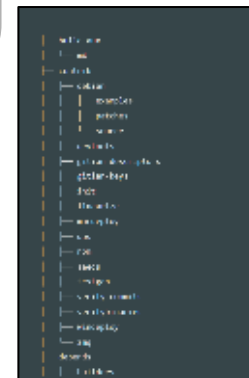
Satoshi Nakamoto名のホワイトペーパーに基づきコア開発者群が開発・公開したブロックチェーンのプログラムが、ビットコインを自動発行する。



世界中のマイナーが、10分に1回のペースで生成される「ブロック」（取引記録の集合体）を承認し記録するため、ハッシュ値の計算競争を行う。

取引記録を集めたブロックを「ハッシュ値」に転換する競争に勝ったマイナーは、対価として6 BTCを受け取る。これが様々な交換所などを通じて法定通貨などと交換され、一般に転々流通する。

```
// Copyright (c) 2009 Satoshi Nakamoto
//
// Permission is hereby granted, free of charge, to any person obtaining a copy
// of this software and associated documentation files (the "Software"), to deal
// in the Software without restriction, including without limitation the rights
// to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
// copies of the Software, and to permit persons to whom the Software is
// furnished to do so, subject to the following conditions:
//
// The above copyright notice and this permission notice shall be included in
// all copies or substantial portions of the Software.
//
// THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
// IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
// FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT
// SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR
// OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
// FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
// IN THE SOFTWARE.
```



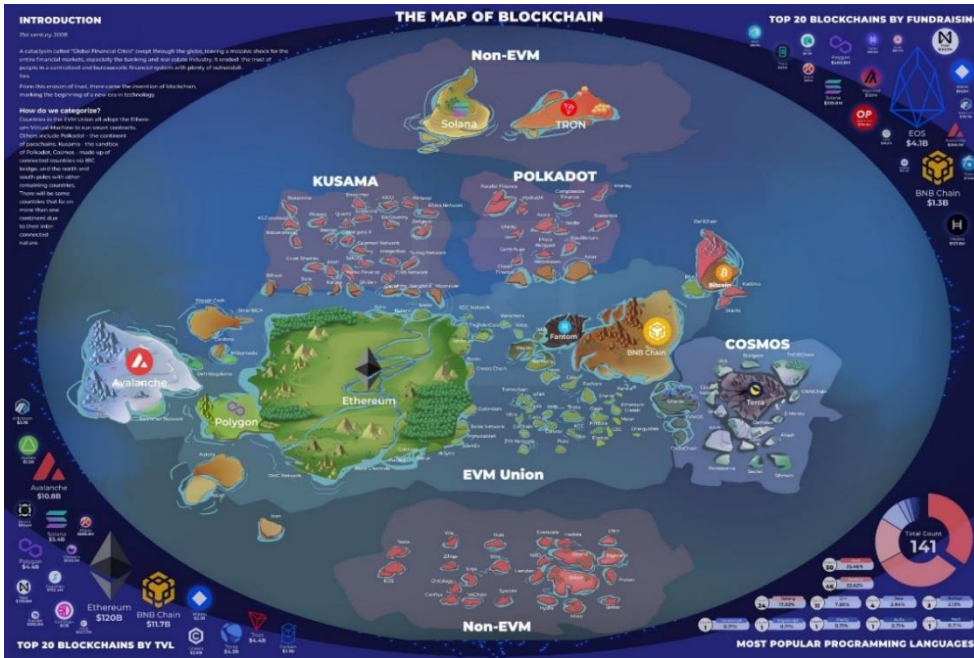
ビットコインのホワイトペーパー（左）とソースコード（右）
※インターネット上で公開

イーサリアム以降の「Web3.0」へ

- 2013年に、暗号資産ETH（イーサ）を基軸通貨とするブロックチェーン「イーサリアム」が登場。
- 「NFTの転売手数料の●%を原作者に渡す」などの契約（スマート・コントラクト）を自動実行できるブロックチェーン上で①NFT取引、②ゲーム（GameFi）、③分散型金融（DeFi）等のアプリケーションが次々に誕生する「Web3.0」の時代が始まった。
- その後、ポルカドット(DOT)、アバランチ(AVAX)、ソラナ(SOL)など「イーサリアム・キラー」と呼ばれる様々なブロックチェーンが群雄割拠。その上で動くアプリケーションが発行するプロトコルトークンも流通。

Web3.0の「群雄割拠」

ポルカドット、アバランチ、ソラナなど様々なブロックチェーンと固有のネイティブトークンが生まれ、同時に互換性追求の動きも進む。



Web3.0のレイヤー構造

プロトコルトークン：各アプリケーションの中で使われる暗号資産

例) Aave
GST



アプリケーション：各ブロックチェーン上で動くサービス

例) Aave
STEPN



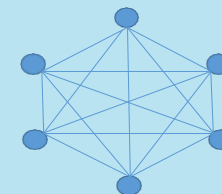
ネイティブトークン：各ブロックチェーン固有の基軸となる暗号資産

例) ETH（イーサリアム）
DOT（ポルカドット）
SOL（ソラナ）
AVAX（アバランチ）



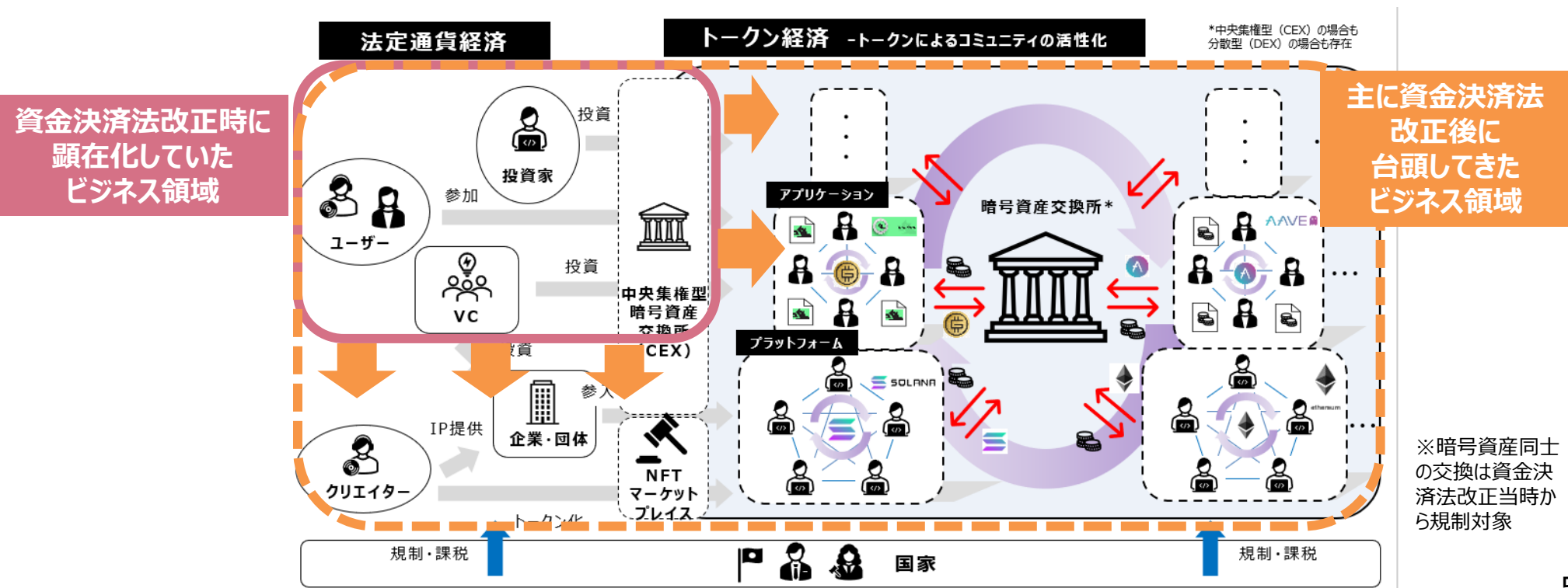
ブロックチェーン

例) イーサリアム
ポルカドット
ソラナ
アバランチ 等



法規制の基本的考え方：世界に先駆けた法規制の課題

- 日本は世界に先駆けて暗号資産に関する法規制を導入。ビットコイン等の決済機能を持つ暗号資産を念頭に置き、暗号資産と法定通貨の交換や暗号資産同士の交換を行う暗号資産取引所等を規制。
- 規制導入時は「イーサリアム以降」の世界が顕在化しておらず、「イーサリアム以降」のアプリケーションやトークンについて、資金決済法や金商法の規制がどこまで適用されるのか不明確（例えば、デジタルアート等に紐づいたNFTなどについて、同種のものが複数存在する場合、暗号資産に該当するかが不明確との指摘がある）。
- 税制や会計も、資金決済法上の暗号資産を念頭に置いた設計となっており、暗号資産の発行体やV C等への期末時価評価課税等の問題が生じている。



政府全体で検討すべき政策の全体像

- 政府全体では、健全な市場の発展のため、投資家保護やマネロン対策等にも取り組みつつ、Web3.0やブロックチェーン技術の発展のための事業環境を整備する必要。

金融

- 投資家保護
- マネーロンダリング・テロ資金供与
- 既存金融秩序との共存

文化経済

- 賭博罪該当性
- 無断NFT対策（著作権保護）

地方創生

- デジタル田園都市国家構想推進交付金等の活用によるユースケース創出

Society 5.0

- グローバルなデータ共有基盤の発展
- トラストを確保したデータ流通

法制度（暗号資産の該当性等）

税制

会計・監査（会計基準の策定/監査法人による適正意見問題）

投資ビークル（LPSによるトークン保有問題）

予算（ユースケース創出、技術系人材育成・研究開発支援）

国際政策（国際カンファレンスによる海外人材呼び込み、国際的な規制議論）

ID認証（DID）

Web3.0政策における主要な論点

- まずは「日本ではWeb3.0関連の事業が困難」とさえ言われる**事業環境の改善**が必須。主要論点は以下。
 - ①**金融規制**：暗号資産の解釈
 - ②**税制**：法人税制（暗号資産の期末時価評価課税）
 - ③**その他**：監査法人による会計監査問題やLPS法、賭博罪該当性、無断NFT対策等
- 加えて、**中長期的観点でブロックチェーン技術の発展のための施策**（研究開発支援・人材育成等）も重要。

規制	1	暗号資産の該当性	✓ ブロックチェーン上で発行されるデジタルなアイテムやコンテンツ等のうち、同種のものが複数存在する場合等の 暗号資産該当性に係る金融庁の解釈指針策定についてサポート する。
	2	法人税制(暗号資産の期末時価評価課税)	✓ 自己発行・自己保有の暗号資産は、期末時価評価課税の対象外 とする税制改正要望 ✓ また、 スタートアップの起業や事業成長を支援する投資家等が保有する暗号資産 についても見直しに向けて検討する
税制	3	監査法人による会計監査問題	✓ 監査法人から受嘱を忌避される事例が複数存在。今後、 金融庁や民間業界団体と連携・協同し、公認会計士・監査法人による監査を受けられるような環境整備を進めていく 予定。
その他	4	LPSによるトークン保有問題	✓ セキュリティトークンが投資対象に含まれるか等のLPS法解釈について整理。トークンへの投資については、資金調達の実態や課題等を調査した上で LPS法の取扱いについて検討
	5	無断NFT対策	✓ 権利者の許諾を得ないコンテンツを使用した「無断NFT」対策の 報告書とりまとめ
	6	NFTの賭博罪該当性の解釈	✓ スポーツDXレポートにおいて、 NFTのランダム型販売と二次流通市場のサービスや、NFTとファンタジースポーツを合わせたサービスの賭博罪該当性についての見解を整理し公表
	7	ユースケース創出支援	✓ コンテンツ業界・スポーツ業界等における 新たなユースケース創出の支援（予算措置）
	8	海外人材呼び込み	✓ 民間と連携してグローバルの第一人者を招いた 国際的なイベントの開催をサポート
	9	研究開発支援・人材育成	✓ ブロックチェーンの 技術的・社会的課題を解決するための研究開発・人材育成等が課題