JAPAN
SMART
CHAIN

WHITEPAPER

バージョン 1.0.0 | 2024年 11月

免責条項:

このホワイトペーパー及びその内容はいかなるトークンの売買の申込み又は勧誘ではありません。本書面のいかなる内容も、JSC若しくはそのトークン（それがあれば）又はMizuhiki Protocolがどのように発展するのか、利用されるのか、又は価値を有するようになるのかについて、保証又は約束するものと判断又は解釈されるべきものではありません。Japan Smart Chain Foundation（JSCF）[及び/又はAltX Research 株式会社（AltX）]は現状の計画の概要を説明しているに過ぎず、当該計画は自らの裁量で変化しうるものであり、それが成功するかは、我々のコントロール外の様々な要因に依ります。そのような将来についての言及は必然的に既知又は未知のリスクを含むものであり、そのようなリスクは、将来、実際の成果や結果を、我々が本ホワイトペーパーにおいて記載し又は意味するものとは大きく異なるものにする可能性があります。JSCF[及び/又はAltX]はその計画のアップデートをする義務を負いません。実際の結果や将来の事象は大きく変わりうるため、本ホワイトペーパーのいかなる記載も、将来、正確であると判明する保証はありません。将来についての言及に過度の信頼を置かないようにお願いいたします。

はじめに

日本におけるブロックチェーンサービスの発展は、一時的な成長と停滞を繰り返してきました。ビットコインの初期時代には日本が世界をリードする立場にあったものの、現在のWeb3時代においては他国に遅れをとっています。

グローバルに見ると、ブロックチェーン産業は成熟しつつあり、決済、分散型金融（DeFi）、実世界資産（RWA）、投票システムなど、スケールのある革新的なサービスが提供されています。

にもかかわらず日本での**Web3**サービスの普及を妨げる主要な要因の一つは、日本の金融規制、データの国内保管、消費者保護に最適化されたブロックチェーンインフラの不足だと考えています。

これらの重要な要素が整備されれば、日本の有力企業が長期的な投資を安心して行い、決済やロイヤルティ、実世界の資産など、ブロックチェーンを活用したコスト削減や顧客満足度の向上に貢献できるサービスを提供することが可能となるでしょう。

私たちのビジョンは、日本国内でバリデートされ、海外の政治的・地理的・社会的・技術的・経済的影響を受けない、パブリックなレイヤー1（L1）ブロックチェーンの構築です。

ひとことで言えば、**Japan Smart Chain**（**JSC**）は「日本主権型」のL1です。

JSCは日本のための主権型ブロックチェーン[1]なのです。

[1] 日本主権型ブロックチェーンの定義：

(イ) データはすべて日本国内に保存される。
(ロ) すべてのバリデータノードが日本国内で稼働し、その情報は公開される。
(ハ) 外国の規制当局（SECを含む）の干渉を受けない。JSCは日本のみの指針に従う。
(ニ) JSCのすべての運営が日本国内で行われる。JSCのリサーチラボと財団は、それぞれ株式会社と一般社団法人として日本に登録されている。

「日本のほぼすべての企業や政府機関は***Web3***を活用したいと考えていますが、信頼性が高く、適切にガバナンスが行われ、評判が良く、さらに主権型のレイヤー***1***ブロックチェーンが存在しないため、実験や構築に踏み出せないでいます。」

伊藤 穣一
Japan Smart Chain

解決すべき問題

重要なインフラは「主権型」である必要があります。つまり、外部の政府や規制当局の干渉を受けないことが求められます。これまで、電力網、通信、交通ネットワークといった分野が重要インフラの典型例とされてきましたが、人工知能やWeb3が進化するデジタル時代において、デジタル主権の重要性がますます明確になっています。

日本政府は最近、デジタル資産の利用やその推進に関する規制環境の整備に注力していますが、大手企業や大規模なサービスプロバイダーは依然としてWeb3の活用に消極的であり、新たな消費者体験を提供したり、日本国民のために新たな価値を創出したりすることに踏み切れていません。

私たちが解決したい核心的な課題は、既存のブロックチェーンにおいて、サーバーが世界のどこに設置されているのか、またユーザーがどの国の規制に従うべきかという不確実性と、パブリックなブロックチェーンが提供する透明性、相互運用性、オープンソースの利点を両立させることの間にある緊張関係です。

私たちは、日本の高度なデジタルセキュリティ、プライバシー、安全性への需要に応えるため、外部の政府や規制当局、または単一障害点の影響を受けない主権型ブロックチェーンインフラの早急な開発が必要だと考えています。

ソリューション

「日本のデジタル新幹線」

Japan Smart Chain（JSC）は、日本国内で日本の産業リーダーによってバリデートされる、**Ethereum**完全互換のレイヤー1（L1）ブロックチェーンです。日本の法規制と消費者保護に最適化されており、外国の法規制や外部からの不当な影響を受けないように明確に設計されています。

JSCは外部の干渉を排除するだけでなく、日本のブロックチェーンエコシステムと顧客体験全体を効率化することにも注力しています。特に、アプリケーション層で顕在化する消費者の課題を、L1レベルでより効果的に解決することを目指しています。私たちの主なターゲット分野は、コストが高く、顧客に不便を強いる、または複数のアプリケーション間で繰り返されるプロセスです。

初期段階として、デジタル決済、分散型自律組織（DAO）、およびその他の規制されたオンチェーンユースケースにおけるeKYCの負担をアプリケーション層から軽減することを目指します。

さらに、効率化を図り、消費者に新たな満足を提供できる分野を継続的に模索していきます。

新幹線が既存の鉄道の枠組みを活用しながら、卓越した速度と世界クラスのサービスを提供しているように、**JSC**は**Ethereum**ブロックチェーン技術を基盤に、埋め込まれたデジタルプロトコルを活用することで、**JSC**の利用者が安全かつ合法的に、既存サービスを凌駕するコストでトランザクションを行える環境を提供します。

日本のための主権型Ethereum完全互換性

JSCのセキュリティとスケーラビリティの原則に基づく取り組み

JSCは、主権型**Ethereum**完全互換性の先駆けとして、Ethereumメインネットのセキュリティ、拡張性、技術革新を完全に踏襲しつつ、すべてのバリデータインフラが日本国内に所在し、名前が公開された状態で稼働する構成を実現します。

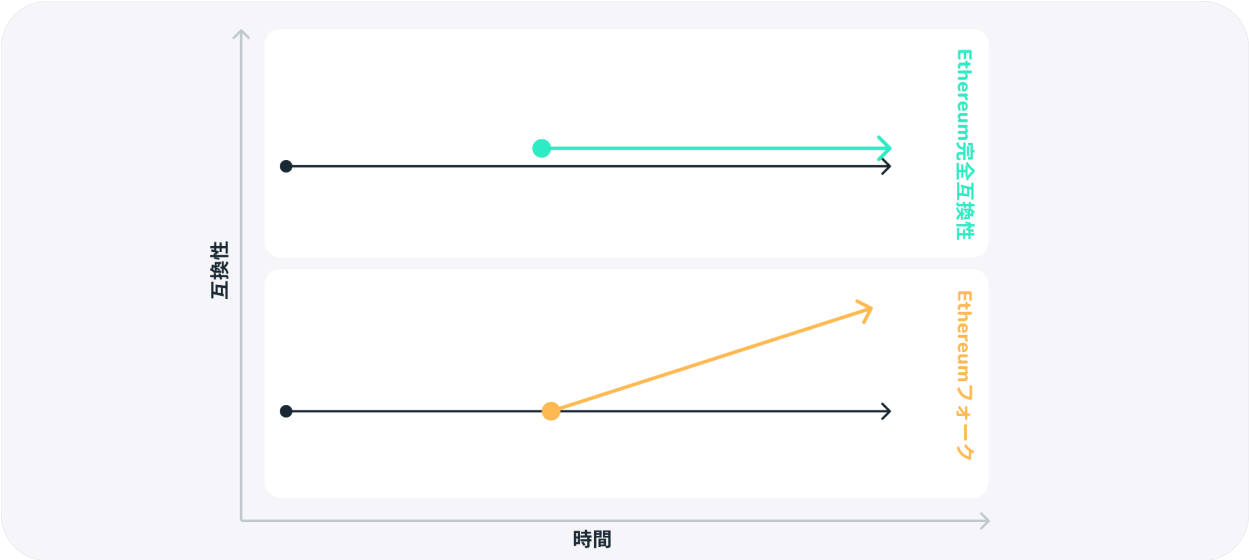
このアプローチは、AI分野の計算サービスにおける選択肢に似ています。共有クラウドサービスから専用リソース、そして最も機密性の高いユースケース向けの完全オンプレミス型インフラまで、多様な提供形態が存在する中で、JSCは日本国内オンプレミス型のパブリックでオープンなブロックチェーンです。

日本主権型ブロックチェーンインフラ

Ethereum完全互換性は、Ethereumの「フォーク」とは異なります。フォークでは、Ethereumのコードベースの一部または全部を変更しなければならず、独自のクライアントソフトウェア、プロトコル、セキュリティアップデートを維持・開発する必要があります。このため、フォークはクライアントの多様性に欠け[2]、既存・新規顧客をサポートする際に膨大なコストが発生しがちです。

[2] 集中リスクを回避するためには、ネットワーク上で複数の独立したブロックチェーンクライアントソフトウェアの実装が稼働していることが理想的である。Ethereum Mainnetでは5つ以上の独立したクライアント実装が維持されているが、多くのEthereumフォークでは1つの実装しか維持できていない。

JSCはEthereumのエコシステムに完全に互換性を持ち、過去・未来にわたるツール群のすべてに対応可能です。



*Ethereum*完全互換性とフォークの比較

JSCは、主権型かつ規制に準拠したブロックチェーンのニーズに対応しながらも、Ethereumとの相互運用性を損なうことはありません。JSCのBlock Builderは、Ethereumの実行クライアントとコンセンサスクライアントをラッピングする形で設計されており[3]、規制に準拠したトランザクションを保護し、ステーブルコインなどの重要なトランザクションを優先します。JSC特有のバリデータ要件は、ジェネシスブロックで一度のみ設定されるため、JSCのコアソフトウェアはEthereumの進化と同期してアップグレード可能です。

Ethereumや関連するブロックチェーン上でローンチされたプロジェクトは、即座にEthereum互換のJSC上でも展開可能です。この互換性は、Ethereumのレイヤー2（L2）ブロックチェーンエコシステム全体にも及びます。また、EthereumとJSCのオープンソース開発は互換性があり、どちらかのチェーンで行われた進化が相互に恩恵をもたらします。さらに、JSCは適切な場合、Ethereumの上流開発を支援することを予定しています。

[3] JSC Block Builderは、RPC層とバリデータノード間のピアツーピア（P2P）接続の間に介在するものである。

JSCの指針となる4つの原則

JSCが日本でWeb3の普及を促進するために独自に設計した枠組みは、以下の4つの指針に基づいています。

1. 主権
   主権とは、日本の統制下にあり、外部の規制機関や地政学的な影響を受けないことを意味します。これはJSCの根幹を成す重要な要素です。

   JSCは日本の主権型L1であり、日本の主要な産業リーダーによって日本国内でバリデートされています。JSCは、日本の法規制を遵守し維持するために設計されており、可能な限り外国の法規制や外部の干渉を排除しています。

2. 情報セキュリティ
   デジタル資産の安全性を確保することは、JSCの中核的な目標です。JSCは**Ethereum**完全互換であり、日本の優れたエンジニアリング力を活用して、Ethereumの優位性をさらに強化する堅牢なインフラを提供します。

3. 安全性
   規制対象のオンチェーンサービス（例：ステーブルコイン）の顧客は、アカウントが認証されていることや、日本のマネーロンダリング防止および反社会的勢力排除の方針がインフラ層に組み込まれていることを前提に、安心して他者と取引を行えます。

4. スケーラビリティ
   増え続ける顧客基盤のニーズに応える能力は、プラットフォームの発展に不可欠です。JSCはローンチ時から「L2 as a Service」を提供し、既存および将来のL2プロジェクトが大幅に低コストで準拠したインフラを採用できる環境を整えます。

MIZUHIKI（ミズヒキ）アイデンティティ・プロトコル

安全性と主権の原則に基づくJSCの新しい基盤

JSCは、アプリケーション層ではなくレイヤー1で消費者の課題に対応するというビジョンに基づき、革新的な**MIZUHIKI**プロトコルを提供します。このプロトコルは、ユーザーが自身で制御できる認証方法[4]を提供し、eKYC[5]ツールとサービスを組み合わせたもので、**JSC**プロジェクトやエンドユーザーに対して無料で提供されます。

JSCは単一で再利用可能なKYCプロセスを通じてユーザーの利便性を高め、消費者の時間を節約し、JSC上のアプリケーションにおけるコストを削減します。このプロセスにより、ブロックチェーンプラットフォームの新しい基準を確立し、日本におけるWeb3の普及を妨げる2つの重要な課題、すなわちユーザーエクスペリエンスと情報セキュリティに直接対応します。

MIZUHIKIプロトコルは、ステーブルコインの送金、金融取引、DAO管理、その他の規制対象活動において、日本の法規制を満たすブロックチェーンアプリケーションを実現します。ユーザーは必要な情報をアプリケーションに提供し、安全に取引を行うことができるだけでなく、アプリケーションの利用を中止したい場合には、検証済み資格情報[6]の権限を取り消すことも可能です。

これらすべてのケースにおいて、個人識別情報（個人を特定できる情報）がオンチェーンで公開されることはありません。これは、従来の各アプリケーションに直接**PII**を共有する仕組みとは対照的です。

MIZUHIKI　KYCは、JSCを利用するブロックチェーンアプリケーション開発者、ユーザー、企業に主な機能として以下を提供します。

- プライバシーの管理をユーザーの手に取り戻す：ユーザーは　(イ)　不要な個人情報への企業アクセスを制限、(ロ) 年齢や大学卒業資格などの証明を自然人のアイデンティ

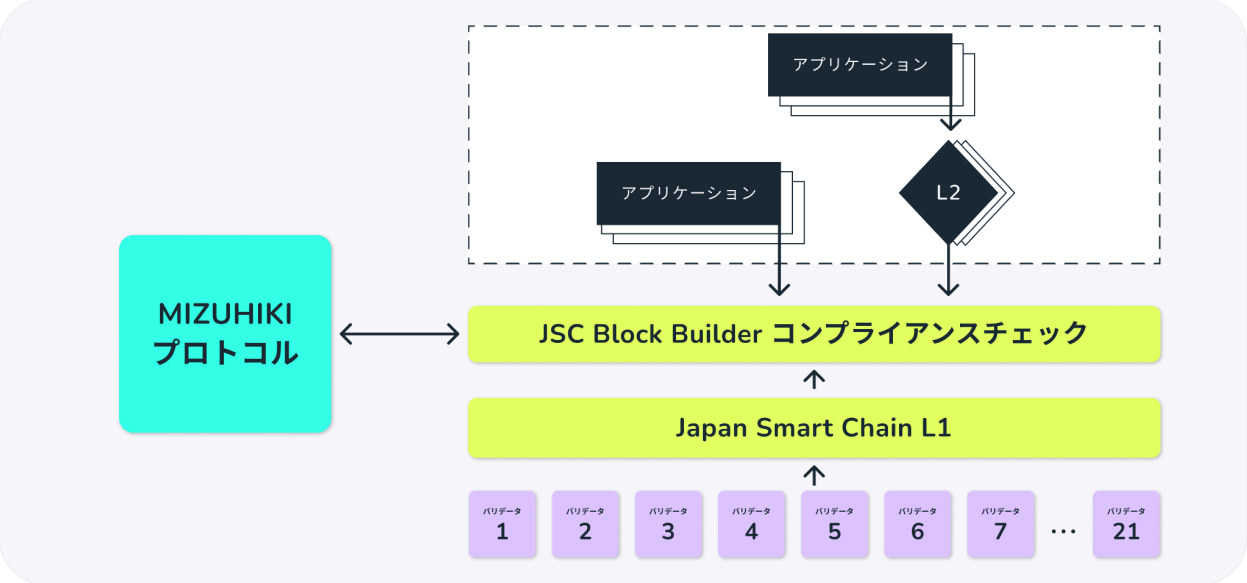
[4] W3Cによる推奨仕様である分散型識別子（Decentralised Identifiers, DID）は、ユーザー制御型の識別メカニズムとして採用される。これにより、ユーザーは自身のデータの所有権を取り戻しつつ、安全なトランザクションを行うために必要な資格情報を抽象化し、セキュアに管理することが可能となる。
[5] 電子KYC（Electronic Know Your Customer）。本書では「Know Your Customer（KYC）」と同義として使用される。
[6] 検証可能な資格情報とは、特定の活動に参加するための顧客の適格性を証明する、国家的に認められた資格情報のことである。例えば、求職者のGPA（成績平均点）や、消費者がアルコールを購入する年齢要件を満たしているかどうかを示す資格情報が含まれる場合がある。資格情報が証明者（アテスター）によって認証されると、その資格情報は検証済み資格情報（*Verified Credential*）として扱われる。この認証の有効期間は限定的である場合もあれば、無期限である場合もある。

ティから抽象化、 (ハ) DIDや検証済み資格情報の権限をワンクリックで取り消す、といった方法でMIZUHIKIプロトコルを通じて情報共有を制御できます。

- 簡易な**KYCとAML**チェックの統合：JSCは最新のセキュリティおよびプライバシー基準を遵守し、文脈に応じたKYC（顧客確認）およびAML（マネーロンダリング防止）チェックをプログラムに組み込んでいます。
- 継続的なコンプライアンス：規制されたユースケースに対する日本の法規制に準拠した仕組みがJSCに組み込まれています。これにより、ユーザー体験をシンプルなものにするとともに、プロトコルレベルでの効率的な規制実施を実現します。この仕組みはプロジェクト全体のコンプライアンス負担とコストを大幅に削減し、イノベーターがアプリケーションの構築に集中できる環境を提供します。

Japan Smart Chainは、Block Builderにプログラムされた継続的なコンプライアンスを通じて、アイデンティティ認証および日本の法規制遵守コストを削減することに注力しています。このインフラにより、既存および将来のイノベーションに必要なコンプライアンスコストを最小限に抑え、従来ならコスト面で実現困難だった新たなユースケースやビジネスチャンスを開拓します。

私たちの目標は、規制遵守を妥協することなく、ユーザーの満足度を向上させるとともに、金融ユースケースにおけるイノベーションの強固な基盤を築くことです。



JSCの構成要素の概要

ガバナンス構造

JSCエコシステムは、以下の2つの主要な運営組織によって構成されています。

- ジャパンスマートチェーン財団（**JSCF**）：JSCFは、日本の一般社団法人として設立された財団であり、JSCのガバナンス基準の維持およびエコシステムの発展を継続的に管理する法的主体です。この財団は、JSCのバリデータや広範なコミュニティと密接に連携し、ネットワークの強化に努めます。
- **AltX Research**株式会社（**AltX**）： AltXはJSCブロックチェーンを開発するラボ企業として、JSCブロックチェーンバリデータネットワークを構成する21のバリデータノードの運営支援を担当しています。

トークノミクス

Japan Smart Chain（JSC）のネイティブトークンであるJSCトークンは、JSCエコシステム内で以下の2つの役割を果たします。

1. スマートコントラクトとブロックチェーンアプリケーションの実行：JSCトークンは、JSC上でのスマートコントラクトやブロックチェーンアプリケーションの実行を支えるネイティブトークンとして機能します。

2. ネットワークのセキュリティ確保：バリデータとステーカーは、JSCトークンをステークし、ネットワークのセキュリティを維持する役割を果たします。その見返りとして、JSCトークンで報酬を受け取ります。報酬は、ネットワークが稼働を開始してから最初の10年間にわたり、定められた割合で得られるほか、JSCユーザーが支払うトランザクション手数料からも供給されます。

ステーキング・エコシステム

JSCのバリデータネットワークは、日本国内に配置された21の「日本主権型」バリデータノードで構成されています。

JSCは、デリゲート（委任）型ステーキングおよびリテール型ステーキングを通じて、数百万の企業や個人が参加する強固なステーキング・オーナーシップエコシステムを構築することを目指しています。21のバリデータノードは、フルノード、デリゲート型ステーキング、リテール型ステーキングの3つのカテゴリに割り当てられます。

2025年メインネットローンチからの最初の5年間（2025-2030年）における21のJSCバリデータノードの割り当ては以下の表*1*の通りです。

ノードタイプ	企業タイプ	割当てノード数	ノードあたりのステーカー数	最初の5年間の想定年利（APY）
フルノード	日経100企業	8〜10	1	20%
デリゲート型（信頼できるデリゲートパートナーによる運用）[7]	中〜大規模企業	8〜10	数百〜数千	約10%〜15%
リテール型（AltX Researchによる運用サポート）	中小企業および個人（国内外）	3〜5	最大数百万	変動金利
バリデータノード数計	-	21	-	-

表*1*：ステーキングとバリデータエコシステム

[7] 日本国内の大規模企業および中小企業の多くは、高度なセキュリティを備えたブロックチェーンインフラの導入において、技術的な支援を必要とする場合がある。そのため、デリゲート型ステーキングは、堅牢で活発なステーキングエコシステムを構築する上で重要な要素となる。この仕組みにおいては、専門の第三者が技術的な課題や一部の会計業務を代行することで、企業がスムーズに参加できる環境を提供する。

トークン発行

JSCトークンの初期総供給量は500億枚に設定されています。

以下の表2において、初期トークン供給量の配分表を示し、各グループへの割り当て、権利確定条件、およびロック解除スケジュールを説明します。

グループ	配分割合	トークン数（単位：百万枚）
バリデータ	21%	10,500
AltX Research	15%	7,500
JSCF - トレジャリー（コミュニティ基金）	25%	12,500
JSCF - パブリックセール	34%	17,000
JSCF - 開発者エンゲージメント	5%	2,500
Total	100%	50,000

表2：JSCトークン配分

バリデータ（21%）

各バリデータは、初期総供給量の1%に相当するトークンを購入しステーキングする必要があります。これらのトークンはバリデータスマートコントラクトにデポジットされ、ロックされたままとなります。

AltX（15%）

AltXへの割り当ては、JSCの創設者、株主、開発者、コアチームメンバーへのインセンティブとして設けられています。この割り当ては、プロジェクトの長期的な成功と成長への貢献を認識し、利害の一致を図ることを目的としています。

ジャパンスマートチェーン財団 – トレジャリー（25%）

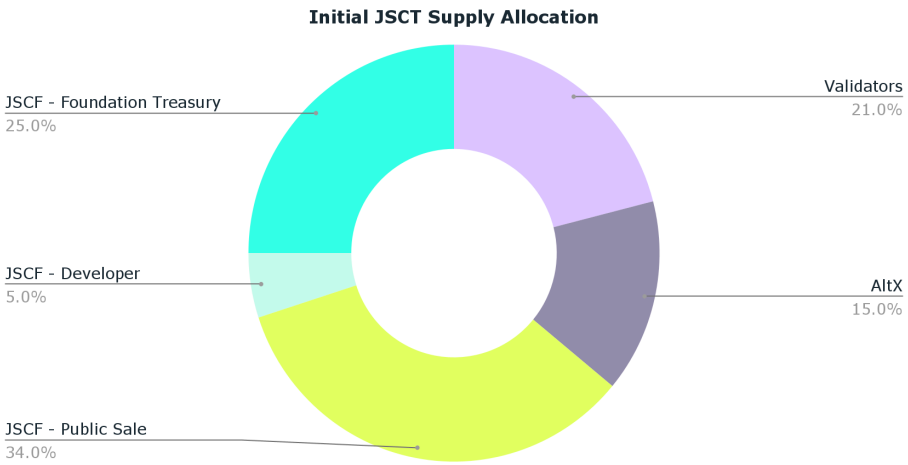
初期供給量の25%は、JSCFの財団トレジャリーに割り当てられ、コミュニティ基金として特別に指定されています。この割り当ては、コミュニティ主導のプロジェクト、イベント、取り組みを資金援助することで、JSCトークンエコシステムの成長と発展を支援し、参加の促進、イノベーションの奨励、コミュニティメンバーの積極的な関与を誘発する財源として機能します。

ジャパンスマートチェーン財団 – パブリックセール（34%）

初期供給量の34%は、国内外の取引所でのパブリックセール用にJSCF準備金に割り当てられます。この公開販売分は、時間をかけてトランシェ方式で投資家に提供され、JSCトークンへのアクセスと流動性を確保します。販売は取引所リストや提供を通じて行われるため、このトークンには権利確定が設定されていません。

ジャパンスマートチェーン財団 - 開発者エンゲージメント基金（5%）

開発者エンゲージメント基金は、新規および既存のJSCコミュニティ開発者にトークンを分配するために設けられています。この基金は、JSCレイヤー1（例：MIZUHIKIプロトコルやその他の日本規制準拠技術）の開発、JSCアプリケーション開発、トークン流通、リワードロイヤリティ、開発者のエンゲージメント強化を含むJSCの活動を促進することを目的としています。



ステーキング報酬

JSCのバリデータは、ネットワークのセキュリティ確保に積極的かつ誠実に参加することで報酬を受け取ります。JSCの運用開始から最初の10年間、バリデータはインフレーションによる発行報酬とトランザクション手数料の両方で報酬を得ます。

10年後には、トランザクション量が十分に増加し、トランザクション手数料のみでネットワークのセキュリティ確保に対する報酬がまかなえる状態を目指しています。

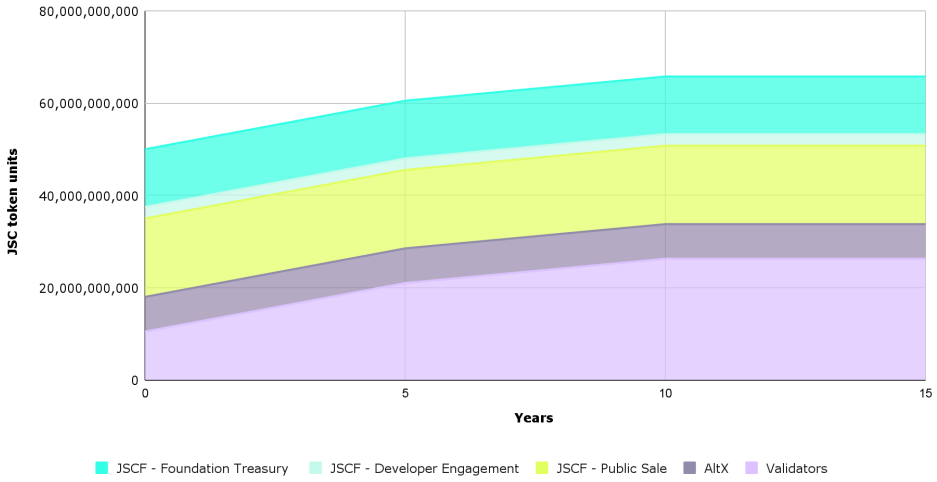
インフレーション率は時間の経過とともに段階的に減少し、**10**年後にはゼロになるよう設定されています。

JSCのブロックタイムは6秒[8]であるため、1ブロックあたりの発行報酬は400 JSCトークンです。この発行報酬により、JSCの年次インフレーション率は、1年目で4.04%、10年目で1.6%に減少し、その後は0%になります。

各バリデータが初期に5億JSCトークンをステーキングし、21のバリデータ全体で105億JSCトークンをステーキングした場合、発行報酬は以下の通りです。

- 1～5年目：年利20%の発行報酬（年間21億JSCトークン発行）
- 5～10年目：年利10%の発行報酬（年間10.5億JSCトークン発行）

フルノードオペレーターは、バリデータのステーキング報酬全額を受け取ります。一方、ステーキングプール内のステーカーは、自身のステーキング量に比例して報酬を受け取ります。

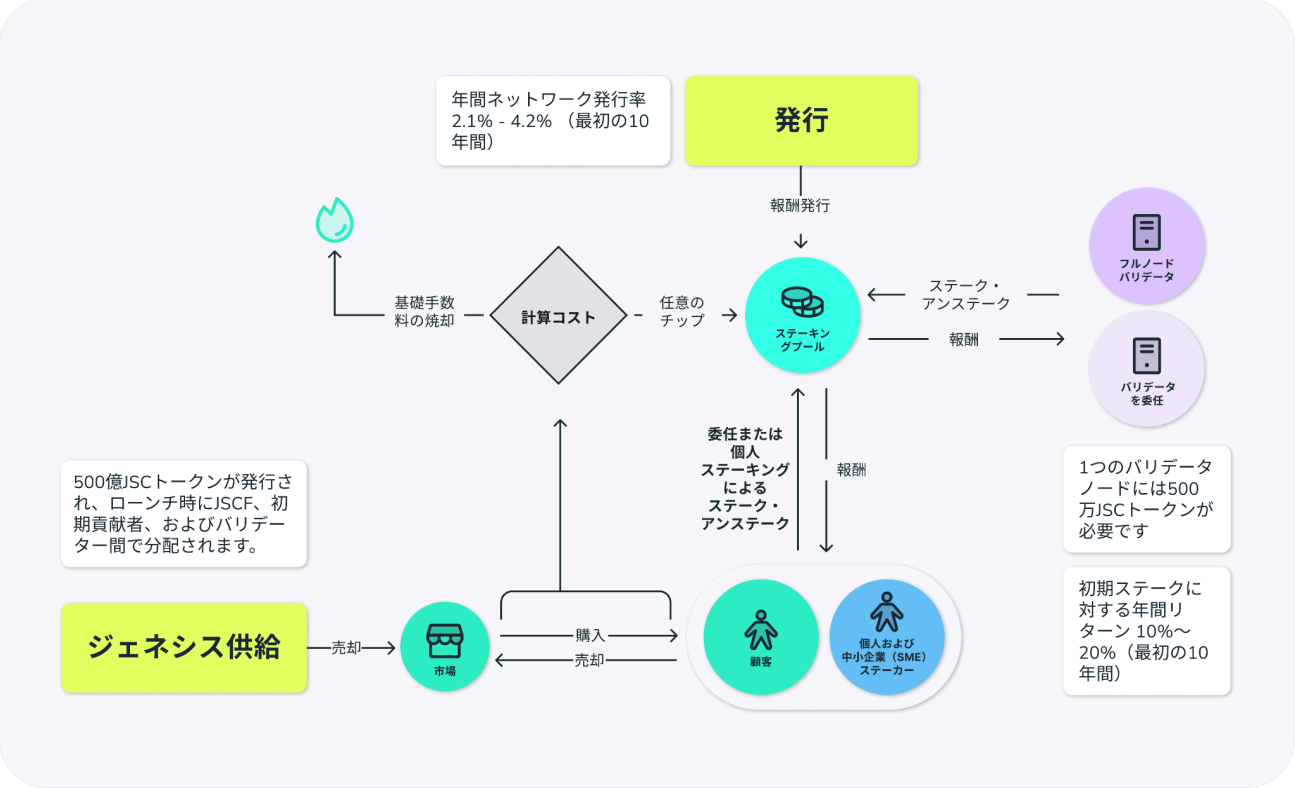


[8]平均ブロックタイムは初期設定で6秒に構成されており、これにより顧客のトランザクション速度と、21のバリデータ間での安全なデータ伝播のバランスが取れるようになっている。

JSCユーザーは、ブロックチェーン上のトランザクション処理のためにJSCトークンで手数料を支払います。Ethereumと同様に、トランザクションには処理費用を賄うための基本手数料と、トランザクション優先度を高めるための優先手数料（任意）が含まれます。基本手数料はバーン（焼却）され流通から除外されることで、バリデータと顧客の間の共謀[9]を防ぎます。

ジャパンスマートチェーン財団（JSCF）は、ステーブルコインやその他の重要なユースケースのトランザクション手数料を、JSCブロックビルダープロトコルに組み込まれた仕組みを通じて補助することを選択する場合があります。

以下のフローチャートは、JSCエコシステム内の経済的な動態を示しています。



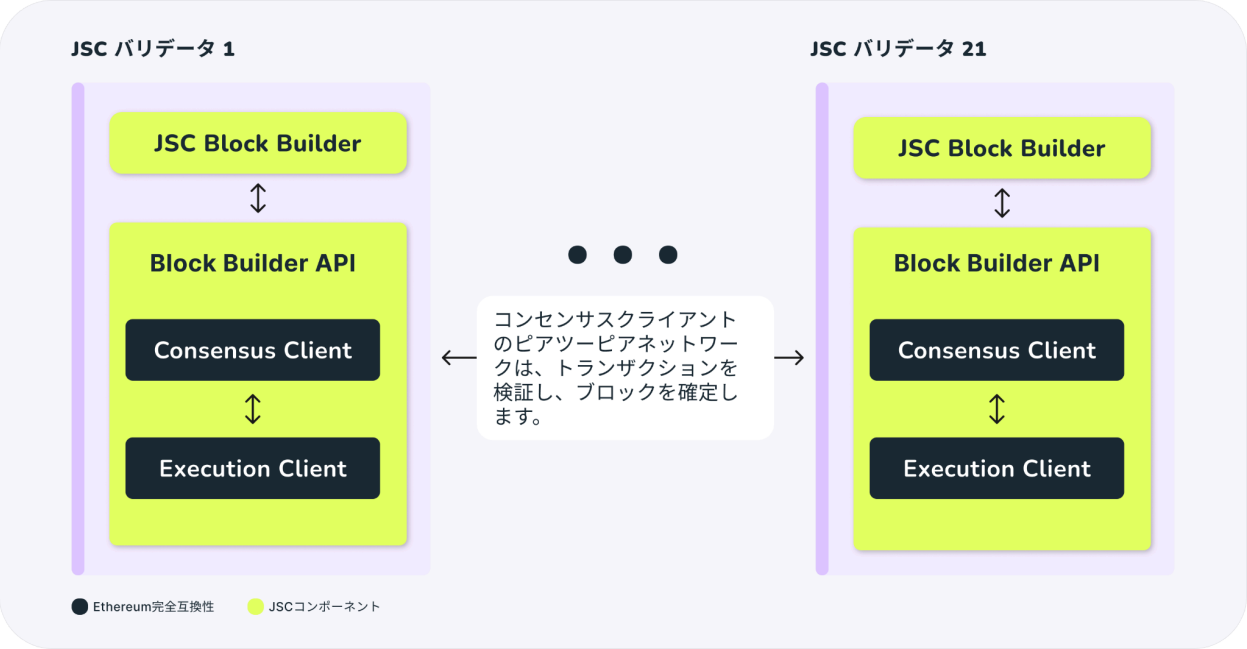
JSCトークノミクスの概要

[9] 出典：Roughgarden, Tim. "Transaction fee mechanism design for the Ethereum blockchain: An economic analysis of EIP-1559." *arXiv preprint arXiv:2012.00854* (2020)

技術的詳細情報

ノードアーキテクチャ

JSCのバリデータノードのアーキテクチャは、Ethereumの実行およびコンセンサスプロトコルの最新の進展と変更を取り入れながら、MIZUHIKIの継続的な規制遵守を維持できるよう設計されています。



JSCバリデータアーキテクチャ

JSCバリデータノードは実行クライアント（Execution Client）、コンセンサスクライアント（Consensus Client）、JSC Block Builderの3つのコンポーネントで構成されています。実行クライアントとコンセンサスクライアントは標準的なEthereumソフトウェアコンポーネントですが、JSC Block BuilderはJSC特有の機能を持っています。

- **JSC Block Builder**
  - トランザクションが法規制を満たしていることを継続的に確認する仕組みを内蔵しています。
  - コンセンサスクライアント向けにトランザクションブロックを構築します。
    - 規制対象の活動（例：ステーブルコイン）の場合、トランザクションがコンセンサスクライアントに送信される前に法規制に準拠していることをチェックします。

    - 標準化されたBlock Builder APIを通じてコンセンサスクライアントと通信します。

- コンセンサスクライアント
    - 他のバリデータやネットワーク参加者とP2Pネットワークでコンセンサスメッセージをやり取りします。
    - 耐障害性を持つ状態機械複製（FT-SMR）を提供します。
    - 標準化されたBlock Builder APIを通じてJSC Block Builderと通信します。

- 実行クライアント
    - コンセンサスクライアントから受け取ったブロック内のトランザクションを実行します。
    - ブロックチェーン状態の外部クエリを処理します。
    - 検証可能な形式でブロックチェーン状態を保存します。
    - Ethereum Virtual Machine（EVM）を実行します。

コンセンサスプロトコル

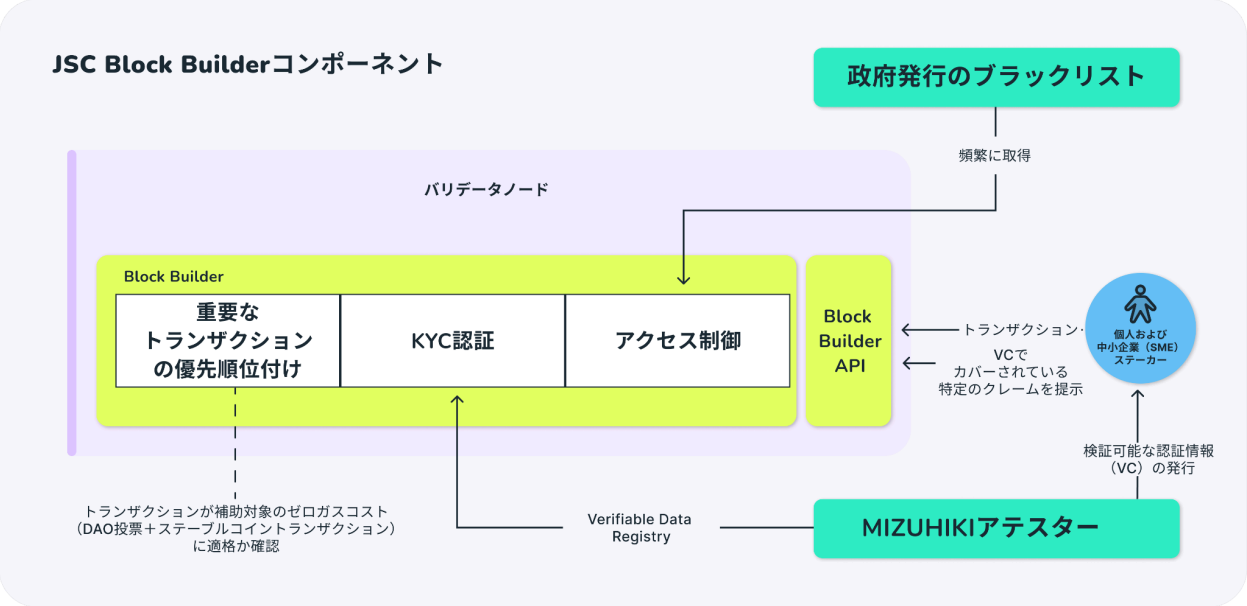
JSCは、Proof of Stake（PoS）コンセンサスプロトコルを採用したEVM互換のブロックチェーンネットワークです。このブロックチェーンは、日本国内で厳格なハードウェアおよびソフトウェア基準に基づいて管理される、21の選定されたバリデータノードによってバリデートされます。これらの基準は、ジャパンスマートチェーン財団（JSCF）によって設定されています。

JSCの21バリデータは、標準的なEthereumコンセンサスクライアントを実行しますが、バリデータの選定、リーダーの選定、報酬分配、アンステーキングプロセスに関してスマートコントラクトに調整が加えられています。

JSCはコンセンサススマートコントラクトに限り以下の改良を加えています。

- ステーキングコントラクト：ネットワークで一時的に有効な21の承認済みアクティブバリデータを選定する仕組みを調整しています。
- リーダーの選定：ブロック提案者となる単一のバリデータを選定するためのコンセンサスメカニズムを採用し、21のバリデータ間で公平にリーダーの役割が分配されるようにブロック高を調整しています。
- アンステーキングコントラクト：JSCはアンステーキングおよびボンディング期間の詳細を変更しており、これには報酬分配の仕組みの調整も含まれています。

JSC Block Builder：MIZUHIKIプロトコルの統合



JSCブロックビルダーの構成要素

MIZUHIKI（ミズヒキ）は、JSCネットワーク向けに最適化されたユーザー制御型のアイデンティティプロトコルです。このプロトコルは、JSCの顧客が**MIZUHIKIアテスター**[10]によって自分のブロックチェーンアドレスに1つのシンプルな検証可能な資格情報（**Verifiable Credential, VC**）を発行される手順を規定しています。顧客は、そのVCに基づいて特定の主張（Claim）をJSCバリデータに提示することができます。

JSCブロックチェーン上にデプロイされるアプリケーションは、MIZUHIKIで認証されたアドレスと安全に相互作用しながら、日本の法規制を遵守することができます。

JSC Block Builderは、JSCブロックチェーン上のすべてのトランザクションで継続的な規制遵守を実現するために、以下の3つの確認を行う必要があります。

1. アクセスコントロール - ブラックリストに登録されたアドレスがトランザクションを実行することを防ぎます。

[10] アテスターは、日本主権型のネットワークであり、適切なライセンスを持つMIZUHIKIプロトコルのアテスターで構成される。これらのアテスターは、個人、機関、その他の主体の実世界のアイデンティティとデジタルアイデンティティの結びつきを確立する「信頼の根幹（root of trust）」を担う。

2. **KYC認証** - 活動が規制対象である場合、KYC認証を通じて、トランザクションの署名ウォレットが適切な検証済み資格情報を持っているかを確認します。適切な検証済み資格情報が存在しない場合、トランザクションは失敗します。

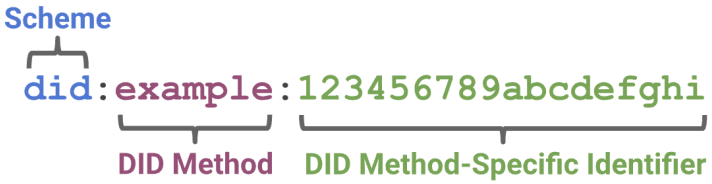
3. 重要なトランザクションの優先順位付け - トランザクションのガスが、ジャパンスマートチェーン財団によって定義されたガス補助政策に従って補助されるかを確認します。

検証可能な資格情報に関連するプライベートデータは、**JSC**バリデータには表示されません。JSCの顧客は、検証可能な資格情報の真実性のみを明示し、その他のプライベート情報を開示することなく、特定のオンチェーンアクションを実行するための資格を証明するゼロ知識証明をバリデータに提出することができます。

分散型識別子と検証可能な資格情報

分散型識別子（Decentralized Identifiers, DID）は、分散環境での主体の認証可能な識別を目的に、W3Cワーキンググループ[11]によって推奨されたデジタル識別子です。

各DIDはURIとして構造化されており、識別子によって参照される文書を解決および検証するための方法に関する情報を含んでいます。



分散型識別子（*DID*）の一例[12]

検証可能な資格情報（Verifiable Credentials, VC）は、分散型識別子を利用して資格情報を発行、保持、提示、および検証するためのもう1つのW3C仕様に基づいています[13]。資格情報には、大学の卒業証明書、運転免許証、身分証明書など、さまざまな文書が含まれる可能性があります。

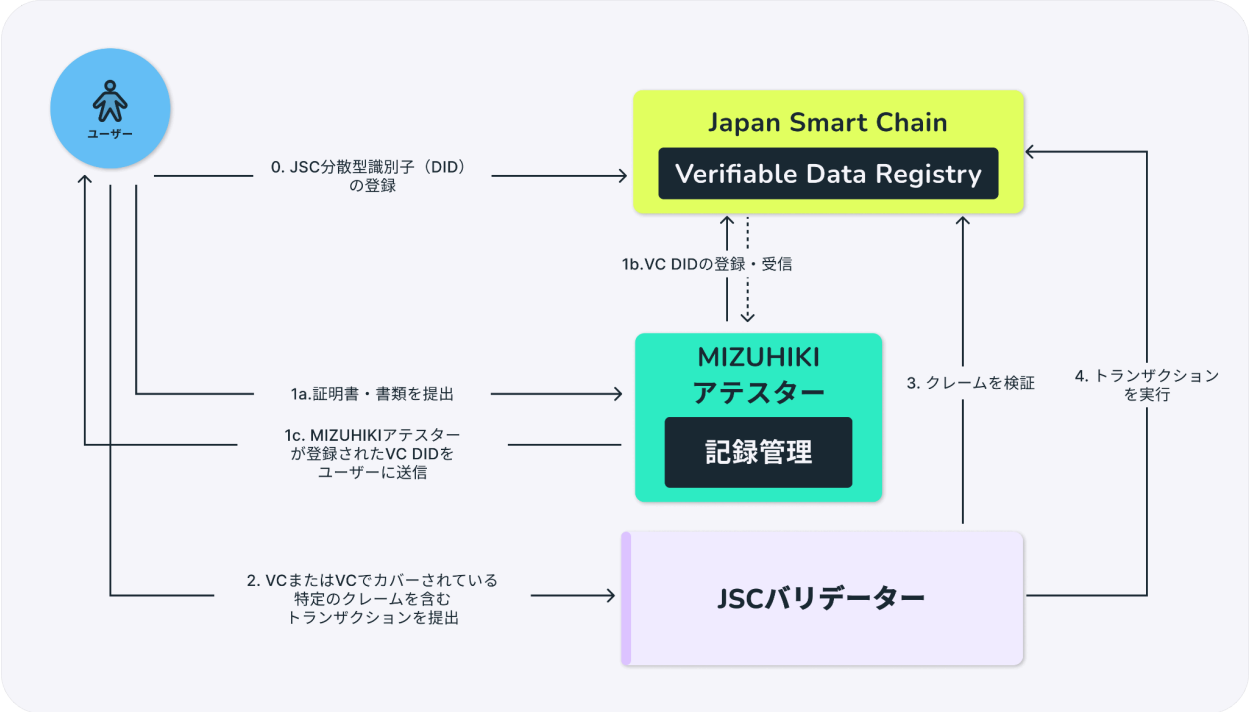
この仕様はまた、異なる状況で同じ資格情報を表現するための検証可能なプレゼンテーション（**Verifiable Presentations**）も定義しています。その中にはゼロ知識表現があり、資格情報

[11] 出典：*Decentralized Identifiers (DIDs)*, W3C Recommendation, v1.0, July 2022. [Online] https://www.w3.org/TR/did-core/
[12] 同書
[13] 出典：*Verifiable Credentials Overview*, W3C Group Note, October 2024. [Online] https://www.w3.org/TR/2024/NOTE-vc-overview-20241022/

の内容に関連する主張の真実性だけを証明し、資格情報そのものを公開せずに提示できます[14]。

JSCネットワークとMIZUHIKIプロトコルは、KYC認証を標準化された方法で表現するために、検証可能な資格情報（VC）と分散型識別子（DID）を使用します。これにより、KYC文書に関連する主張を検証する際、バリデータやアプリケーション運営者にプライベート情報を開示することなく確認が可能です。さらには、ゼロ知識資格情報の表現をスマートコントラクト内で検証できるため、JSCアプリケーションの開発者や顧客は、MIZUHIKIプロトコルを日常的に追加の負担なく利用できます。

エンドユーザー向けMIZUHIKIプロトコル利用手順



MIZUHIKIプロトコルのエンドユーザー向けフロー

MIZUHIKI eKYCプロセスを完了するためのエンドユーザーのフローは以下の通りです。

0. ユーザーDIDの生成と登録

ユーザーは、JSCウォレットアドレスを使用してローカルでDIDを生成します（例:　JSC上にデプロイされたスマートコントラクトを利用）。生成されたDIDはオンチェーンに登録されます。

[14] 出典：*Verifiable Credentials Data Model - Zero Knowledge Proofs*, W3C Candidate Recommendation Draft, October 2024. [Online] https://www.w3.org/TR/vc-data-model-2.0/#zero-knowledge-proofs

1a. 必要書類をMIZUHIKIアテスターに提出

ユーザーはMIZUHIKI認証プロセスを開始し、MIZUHIKIアテスターに必要書類とステップ0で登録したDIDを提出します。MIZUHIKIアテスターは、ユーザーのプライバシーを保護するため、すべての本人確認および書類チェックをオフチェーンで実施します。

1b. MIZUHIKIアテスターによる検証可能な資格情報のオンチェーン登録

ユーザーの書類およびDIDの確認が完了すると、MIZUHIKIアテスターは書類の検証を正式化し、検証可能な資格情報をJSC上（特に**Verifiable Data Registry**[15]）に登録します。このVCはユーザーのDIDと埋め込まれており、他者による不正使用を防止します。

1c. 検証可能な資格情報のユーザーへの送信

ユーザーは、検証済み資格情報（VC）に含まれる特定の主張を必要に応じて他者に共有することができます。

2. ユーザーが検証可能な資格情報を含むJSCトランザクションを送信

ユーザーがJSC上で規制対象の活動（例: 金融取引）に参加する場合、検証済み資格情報（およびその適格性）をJSCアプリケーションに提示します。

ゼロ知識証明[16]が使用される場合、ユーザーのプライバシーが保護され、公開されることなくMIZUHIKIアテスターによって検証可能です。

検証可能な資格情報には生年月日、GPA、住所などの主張が含まれる場合があります。ユーザーはこれらの主張の一部のみ（例: 生年月日だけ）を提示することも可能です。このプロセスを検証可能なプレゼンテーション（Verifiable Presentation, VP）と呼びます。

3. バリデータによる主張の検証

JSCバリデータ（特にバリデータノード内のBlock Builder）が、**Verifiable Data Registry**を通じてVCに含まれる主張を検証し、トランザクションが日本の法規制に準拠していることを確認します。

[15] MIZUHIKI Verifiable Data Registryは、JSCバリデータや規制対象アプリケーションが、MIZUHIKIアテスターに直接連絡することなく、検証可能な資格情報（VC）の有効性を確認するために使用するオンチェーン情報レジストリである。
[16] 出典：13参照

4. トランザクションの実行

すべてのMIZUHIKIプロトコル検証を通過したトランザクションは、リードバリデータによってブロックに追加され、その後JSCブロックチェーン上で実行されます。

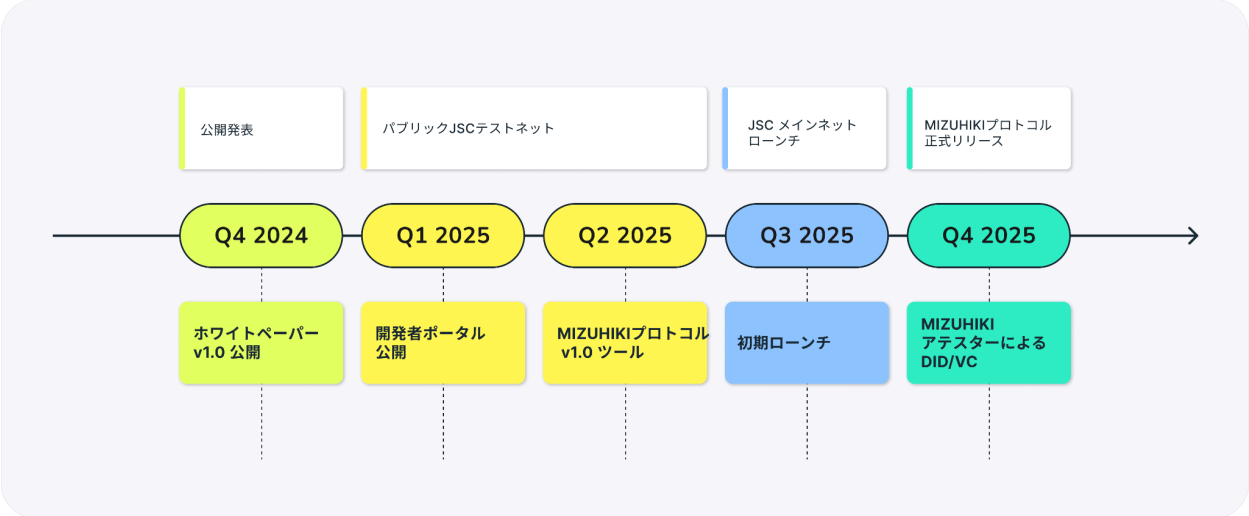
ロードマップ

このプロジェクトのロードマップは段階ごとに分かれており、まずはパブリックテストネット、開発者のオンボーディング、続いてバリデータダッシュボードやブロックエクスプローラーといった主要なツールの構築が行われます。

パブリックテストネットのフェーズでは、ハードウェアおよびソフトウェアのセットアップ、ウォレットやステーブルコインSDK（Sign in with JSC）の開発を通じてメインネットローンチの準備が行われます。

次のフェーズでは、JSCメインネットがリリースされます。このフェーズでは、EIP（Ethereum Improvement Proposals）への対応やコアインフラコンポーネントの実装を継続的に行います。

最終フェーズでは、オンチェーン検証コントラクト、ブロックチェーンアプリケーションのホワイトリスト化、MIZUHIKIアテスターの移行といった機能をリリースすることで、Japan Smart Chainのビジョンを完全に実現します。詳しい内容は下図の通りです。



Japan Smart Chain ロードマップ

付録A：用語集

- マネーロンダリング防止（**Anti-Money Laundering, AML**）
  金融機関やその他の規制対象機関が、金融犯罪、特にマネーロンダリング活動を防止、検出、報告するための政策と実践のセットを指す。
- ブロックチェーン（**Blockchain**）
  非中央集権型で分散されたデジタル台帳。多くのコンピュータでトランザクションを記録し、安全かつ不変の方法で保管する。
- 分散型自律組織（**Decentralized Autonomous Organization, DAO**）
  コンピュータプログラムとしてエンコードされたルールによって運営され、中央集権的なリーダーシップ構造を持たない組織。
- 分散型識別子（**Decentralized Identifiers, DID**）
  分散型環境における主体の検証可能な識別のために設計されたデジタル識別子。
- 電子**KYC**（**Electronic Know Your Customer, eKYC**）
  顧客の個人識別情報（Personal Identifiable Information, PII）を電子的に検証するプロセス。マネーロンダリング防止やその他の法規制に準拠するために使用される。一般的なeKYCの実装例として、スマートフォンやコンピュータのカメラを使用した顔認証等が挙げられる。
- イーサリアム仮想マシン（**Ethereum Virtual Machine, EVM**）
  Ethereumブロックチェーン上でスマートコントラクトを実行する仮想マシン。バイトコードの実行環境を提供する。
- イーサリアムメインネット（**Ethereum Mainnet**）
  Ethereumの本番環境「メインネットワーク」。
- **JSC**メインネット（**JSC Mainnet**）
  Japan Smart Chainの本番環境「メインネットワーク」。
- **KYC**／身元認証（**Know Your Customer**）
  企業やその他の団体が顧客の個人識別情報（PII）を検証し、マネーロンダリング防止（AML）やその他の法規制に準拠するプロセス。
- レイヤー**1**（**Layer 1, L1**）
  ブロックチェーンの中でも、トランザクションの決済とコアインフラの維持を行う基礎的なブロックチェーンネットワーク（例: Ethereum、Bitcoin）。

- レイヤー2（**Layer 2, L2**）
  スケーラビリティとトランザクションスループットを向上させるために、レイヤー1ブロックチェーン上に構築されたセカンダリプロトコル。

- **MIZUHIKI**アイデンティティプロトコル／**MIZUHIKI**プロトコル
  JSCが提供するユーザー制御型の識別メソッドで、ユーザーの利便性、安全性、ネットワークセキュリティを強化する。

- **MIZUHIKI**アテスター（**Mizuhiki Attestors**）
  JSCにおける「認証機関（Certificate Authority, CA）」に相当する存在。ワールドワイドウェブ（WWW）のパラダイムでは、CAは信頼された第三者として機能し、デジタル証明書の所有者（主体）およびその証明書に依存する者の双方から信頼されている。MIZUHIKIアテスターは、MIZUHIKIプロトコルを実装する。

- 個人識別情報（**Personal Identifiable Information, PII**）
  氏名、生年月日、メールアドレス、生体情報など、個人を特定できる情報。

- プルーフオブステーク（**Proof-of-Stake, PoS**）
  一部のブロックチェーンネットワークがトランザクションを検証し、新しいブロックを作成するために使用するコンセンサスメカニズム。バリデータは暗号通貨をステーキングすることでコンセンサスのプロセスに参加すり。

- スマートコントラクト（**Smart Contract, SC**）
  事前に決められた条件が満たされた際に自動的に実行されるデジタル上のコントラクト（契約）／命令セット。ブロックチェーン上に保存される。

- ステーブルコイン（**Stablecoin**）
  価格変動を最小限に抑えるよう設計された暗号通貨。しばしば米ドルやコモディティなどの安定した資産にペッグされる。

- ステーカー（**Staker**）
  JSCネットワークにJSCトークンをステーキングする個人や団体。

- シビル攻撃（**Sybil Attack**）
  単一の個人や団体が複数のアイデンティティを作成し、ネットワークに過度な影響を与えようとする攻撃。

- テストネット（**Testnet**）
  各チェーンのメインネットの動作をシミュレートする「テストネットワーク」。開発者や試験利用者が現実世界の金銭的影響を排除しながら、本番環境のプロセスやメカニズムを安全にテストできる環境。

- バリデータノード（**Validator Node**）
  日本国内に設置されたブロックチェーンノードのハードウェアおよびソフトウェアインフラを組み合わせたもので、トランザクションを収集し、それをブロックに組み込み、ネットワークのすべての参加者にそのブロックを伝播することで、JSCブロックチェーンを実装および保護する役割を果たす。バリデータノードは、1人または複数のステーカーで構成される。本書では、バリデータノードを「ノード」または「バリデータ」として同義的に使用する。

- 検証可能な資格情報（**Verifiable Credentials, VC**）
  分散型環境で検証可能なデジタル資格情報。通常、認証には分散型識別子（DID）が使用される。

- 検証可能なプレゼンテーション（**Verifiable Presentation, VP**）
  認証可能な資格情報の一部または暗号的に抽象化された形式で、規制対象またはルールベースの活動を実行するために必要最小限の情報のみを開示するためのもの。

- **Verifiable Data Registry**（**VDR**）
  Japan Smart Chain上で検証可能な資格情報データを管理するレジストリ（個人を特定できる情報は含まない）。信頼できる発行者レジストリとも呼ばれ、MIZUHIKIアテスターによって発行された検証可能な資格情報の正確な記録を表す。VDRは改ざん防止機能を備えており、MIZUHIKIアテスターによって発行された検証可能な資格情報の正確な記録を保持する。

- ゼロ知識（**Zero-Knowledge, ZK**）／ゼロ知識証明（**~ Proof, ZKP**）
  ある主張が真であることを、追加情報を一切開示することなく証明する現代的な暗号手法。現代の暗号技術の一種であり、一方の当事者が、他方の当事者に対して、追加の情報を一切開示することなく、ある主張が真実であることを証明する方法を指す。