JAPAN
SMART
CHAIN

WHITEPAPER

VERSION 1.0.1 | AUGUST 2025

Legal Disclaimer:

This white paper and its contents are not an offer to sell, or the solicitation of an offer to buy, any tokens. Nothing in this document should be read or interpreted as a guarantee or promise of how the JSC or its tokens (if any) or Mizuhiki Protocol will develop, be utilized, or accrue value. The Japan Smart Chain Foundation (JSCF) [and/or AltX Research KK (AltX)] only outline its current plans, which could change at its discretion, and the success of which will depend on many factors outside of its control. Such future statements necessarily involve known and unknown risks, which may cause actual performance and results in future periods to differ materially from what we have described or implied in this white paper. JSCF [and/or AltX] undertakes no obligation to update its plans. There can be no assurance that any statements in the whitepaper will prove to be accurate, as actual results and future events could differ materially. Please do not place undue reliance on future statements.

Introduction

The development of blockchain services in Japan has proceeded in fits and starts, with periods when Japan was a global leader (early Bitcoin era) and periods when Japan has lagged behind other parts of the world (current web3 era).

Globally, the blockchain industry is maturing with innovative consumer offerings at scale, including payments, decentralized finance, real-world assets, and voting.

We believe one of the main constraints to the widespread adoption of web3 services in Japan is the lack of blockchain infrastructure optimized for Japanese financial regulations, Japanese data residency, and consumer protections.

With these critical elements in place, we believe that leading Japanese companies will be comfortable making long-term investments into services that leverage blockchain to unlock cost savings and consumer delight in payments, loyalty, real world assets and other areas.

Our vision is a public Layer 1 (L1) blockchain validated onshore in Japan, without exposure to offshore influence, whether political, geographic, societal, technical, or economic.

Simply stated, **Japan Smart Chain (JSC)** is an L1 that is “Japan-sovereign”.

This is THE sovereign blockchain for Japan[1].

[1] **We define a Japan-sovereign blockchain as:**

(a) Data residency all onshore in Japan.
(b) Every validator node operates onshore in Japan and is publicly disclosed.
(c) Beyond reach and interference of foreign regulators, including the SEC. JSC responds to Japan only.
(d) All JSC operations onshore in Japan. JSC’s Research Lab and Foundation are both registered *kabushiki kaisha* (KK) and *ippan shadan houjin* respectively.

“Nearly every company and government agency in Japan wants to leverage web3, but many are stymied by the lack of a trustworthy, well-governed, reputable, and SOVEREIGN Layer 1 blockchain upon which to experiment and build.”

— Joi Ito, Japan Smart Chain

Problem Statement

Critical infrastructure needs to be sovereign – that is, beyond the reach of outside governments or regulators. While electricity grids, communications and transportation networks have historically upheld the paradigm of what constitutes “critical infrastructure”, the importance of digital sovereignty is becoming increasingly clear as the world moves into the digital age of artificial intelligence and web3.

Even with Japan’s recent government focus and work to clarify the regulatory climate around the use and facilitation of digital assets, major companies and large-scale service providers remain reluctant to leverage blockchains to offer compelling new consumer experiences and unlock new value for the people of Japan.

The core problem we want to address is the tension between a lack of certainty of where blockchain servers are located globally, and which nation’s regulations its users ought to respond to for existing blockchains, while still achieving the same transparency, interoperability and open-source benefits that public, permissionless blockchains offer.

We believe that the high digital security, privacy, and safety needs of Japan call for urgent development of a public, open and available to use for any project globally, **sovereign** blockchain infrastructure that is beyond the reach of outside governments, regulators, or single points of failure.

Solution

“Japan’s Digital Shinkansen”

Japan Smart Chain (JSC) is an **Ethereum Equivalent** Layer 1 (L1) blockchain, validated onshore in Japan by Japanese industrial leaders, and optimized for Japanese regulations and consumer protections. JSC is explicitly designed to avoid exposure to foreign regulations or undue outside influence.

In addition to being protected from outside influences, JSC is committed to streamlining the Japanese blockchain ecosystem and overall customer experience by focusing on consumer pain points in the application layer that can be better addressed at the L1. **Our primary target areas are those processes that are expensive, cause customer inconvenience, or are repetitive across applications.**

Initially, we are aiming to minimize the burden of eKYC in the application layer for digital payments, decentralized autonomous organizations (DAOs) and other regulated on-chain use cases.

We will continuously look for other areas where efficiencies and consumer delight can be unlocked.

Just as the Shinkansen leveraged the existing paradigm of rail travel with exceptional speed and world-class service, JSC augments the Ethereum blockchain technology with embedded digital protocols to ensure JSC users can transact both safely and legally at costs unparalleled by existing services.

Sovereign Ethereum Equivalence for Japan

Aligning with JSC's Principles of Security and Scalability

JSC is pioneering **Sovereign Ethereum Equivalence**, a deployment of Ethereum that follows all the security, scaling, and technology innovations of Ethereum Mainnet, but critically on validator client infrastructure that is all known, named, and located onshore in Japan.

We view this approach as analogous to the spectrum of computational service offerings in the AI world, ranging from shared cloud services, to co-located dedicated resources, to fully on-premises infrastructure for the most sensitive use cases. JSC is a public and open blockchain, but with validation specifically "on-premise" in Japan.

Japan-sovereign blockchain infrastructure

Ethereum Equivalence distinguishes itself from a "fork" of Ethereum. Ethereum forks, which make changes to some or all of the Ethereum codebase, must develop and maintain client software, protocol, and security updates independently. Forks typically have less client diversity[2], and struggle to support new and existing customers without incurring massive costs.

[2] To avoid concentration risk it is ideal to have multiple independent implementations of blockchain client software running on the network. Ethereum Mainnet maintains over five independent client implementations, while most Ethereum forks are only able to maintain one.

JSC is fully backward and forward-compatible with the full ecosystem of Ethereum tooling.

Ethereum Equivalence vs a Fork of Ethereum

Adjustments to cater to the needs of a sovereign and compliant blockchain do not compromise JSC's interoperability with Ethereum. Customisation to the blockchain is under research and development, with the two primary goals being (1) blocking blacklisted transactions, and (2) prioritizing essential transactions such as stablecoins. The remaining JSC-specific network configurations are specified in the Genesis state, which improves forward-compatibility with major Ethereum changes.

Any project that launches on Ethereum or an Ethereum-adjacent blockchain can immediately launch on the Ethereum Equivalent JSC. This includes the full ecosystem of Ethereum Layer 2 (L2) blockchains. In addition, open-source development work on Ethereum and JSC is compatible: advancements made to either chain are mutually beneficial, and we anticipate that JSC will sponsor upstream development work on Ethereum, where appropriate. JSC will also post back regular checkpoints to Mainnet Ethereum as a way to further anchor the security of JSC to Ethereum.

Guiding Principles

JSC's unique approach to creating the conditions for web3 adoption to thrive in Japan lies in its four guiding principles as defined below:

1. **Principle of Sovereignty**
   Sovereignty – being within the control of Japan and beyond the influence of outside regulatory and geopolitical forces is key for JSC.

   JSC is Japan's sovereign L1: it is validated onshore in Japan by key leaders in Japanese industry, and it is built to comply with and uphold Japanese regulations. JSC is beyond the reach of foreign regulators and outside forces to the greatest extent possible.

2. **Principle of Security**
   The quality of one's digital assets being secure. JSC is **Ethereum Equivalent**, and leverages Japan's top engineering talent to fortify Ethereum's excellence with robust infrastructure.

3. **Principle of Safety**
   Customers of regulated on-chain services (such as stablecoins) can safely interact with others, knowing that accounts have been verified and Japan's anti-money laundering and anti-social compliance policies have been embedded at the infrastructure layers.

4. **Principle of Scalability**
   The ability of the platform to meet the needs of an ever-growing customer base. JSC will offer L2 as a service from launch, allowing pre-existing and future L2 projects to adopt compliant infrastructure at a significantly lower cost to what is being currently offered.

Mizuhiki Suite

Aligning with JSC's Principles of Safety and Sovereignty

In-line with JSC's vision of addressing consumer pain points in the infrastructure layer, JSC offers its pioneering **Mizuhiki Suite**, which introduces a universal identification method matched with a suite of eKYC[3] tools and services, **offered for free to Japan Smart Chain projects and end-users**.

The Mizuhiki Suite tooling aims to enhance user convenience through a single, reusable KYC process, saving time for consumers and cost for applications on JSC. It sets a new standard for blockchain platforms by directly addressing two critical aspects of web3 adoption in Japan: **user experience** and **security**.

The Mizuhiki Suite is designed to help blockchain applications meet Japanese regulations regarding stablecoin transfers, financial transactions, DAO administration, and other regulated activities. Users are able to provide applications with the necessary information required to transact safely, but also revoke access permission to their information via verifiable credentials or other on-chain abstracted identity tokens if they wish to discontinue application usage.

In all cases, no Personally Identifiable Information (PII) is exposed on-chain. This contrasts with the current paradigm of sharing PII with every application directly.

Mizuhiki provides the following key features for blockchain application developers, users, and businesses using JSC:

- **Privacy control back in the hands of the user:** Users are able to control their information-sharing via the Mizuhiki Suite by: (a) limiting application access to only the user's necessary personal information, (b) abstracting credentials (such as age or university graduation status) from their natural personhood identities, and (c) revoking access permissions to their **DIDs** and/or **verifiable credentials** (VCs) with a single click.
- **Effortless KYC and embedded AML checks:** JSC ensures the latest security and privacy standards by embedding KYC, AML, and other context-specific

[3] Electronic Know Your Customer. eKYC is used interchangeably throughout this paper with "Know Your Customer" (KYC)

compliance checks programmatically into compliance and risk management toolkits provided by the Mizuhiki Suite.

- **Continuous compliance:** Japan Smart Chain is committed to driving down the cost of identity verification and of compliance with Japanese regulations through **programmatic continuous compliance**. Our intention is to create infrastructure where the cost of compliance for existing and future innovation is *de minimis*, opening up new use cases and business opportunities that would otherwise be prohibitively expensive.

To address challenges faced by end-users and enterprises, the Mizuhiki Suite will consist of three core components:

(1) Mizuhiki Identity

A user's eKYC-verified identity, DIDs, and verifiable credentials, making identity self-managed, portable, and enforceable on-chain.

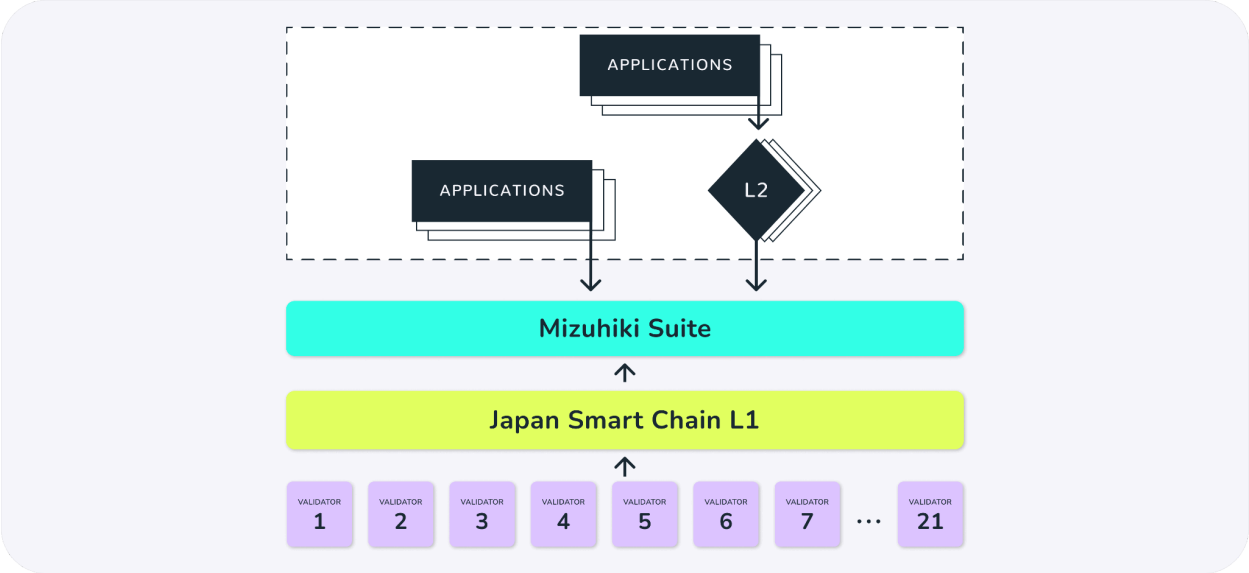
(2) Mizuhiki Compliance

A third-party compliance validation and insurance: a source of truth that applications can tap into. Enforces external regulatory frameworks (e.g., JFSA rules) through a hybrid on- and off-chain approach by surfacing compliance signals and proofs.

(3) Mizuhiki Risk Management

Allows enterprises to support their operational and transactional control that is separate from, but complementary to, external regulatory compliance. Policies such as transaction limits, asset gating, and approvals are codified and enforced on-chain for efficiency and transparency.

Our aim is to enhance user satisfaction while also establishing a strong foundation for future innovation without compromising regulatory adherence for financial use cases.



Overview of the JSC components

Governance Structure

The JSC ecosystem comprises two main operating entities:

- **The Japan Smart Chain Foundation (JSCF)** is a Japanese foundation (*ippan shadan houjin*) that will be the legal entity responsible for securing and maintaining JSC governance standards and managing ecosystem development over time. The entity will work closely with JSC Validator Client Operators and the wider community to bolster the network.
- **AltX Research KK (AltX)** is the labs company that is producing the JSC blockchain and is responsible for supporting the 21 Validator Client Operators that each run a validator client and make up the *JSC Validator Network*.

Tokenomics

Japan Smart Chain token, JSC's native token, serves a dual purpose within the Japan Smart Chain ecosystem:

1. JSC tokens function as the native token of JSC, powering the execution of smart contracts and blockchain applications.

2. Validator clients and stakers stake JSC tokens and are rewarded in JSC tokens for their role in securing the network. Rewards in JSC tokens are earned at a target rate for the first ten years of the network being live, alongside transaction fees paid by JSC users.

Staking Ecosystem

The design of the JSC Validator Network consists of 21 Validator Client Operators, with validator client infrastructure all on-shore in Japan.

JSC wants to drive a robust staking/ownership ecosystem, with millions of companies and individuals in Japan via delegate and retail staking. Amongst the 21 validator clients, JSC will split the allocation between full node, delegate, and retail staking services.

For the first five-year phase from Mainnet launch (2025-2030), the 21 JSC validator clients will be allocated the following staking options:

Node Type	Entity Type	Allocated Nodes	Stakers per Node	Year 0-5 Expected APY
Full Node	Nikkei 100	8-10	1	20%
Delegate Staking (Supported by trusted delegate partners)[4]	Medium to Large Enterprises	8-10	100s to 1,000s	~10% to 15%
Retail Staking (Supported by AltX Research)	Small businesses and Individuals worldwide	3-5	Up to millions	Floating Rate
Total Validator Clients		21		

Table 1: Staking Ecosystem

[4] Both large and small companies in Japan may require assistance with the technical aspects of onboarding high-security blockchain infrastructure. Delegate staking, where technical and some accounting issues are handled by specialized third parties, is thus an important part of how we can develop a robust and active staking ecosystem.

Token Supply

The total initial supply of JSC tokens has been set at 50 billion units.

Below, we detail the JSC token allocation chart, outlining how the initial supply of tokens is distributed among different roles, each with specific vesting conditions and unlock schedules.

Group	Allocation	Token units (in millions)
Validator Client Operators	21%	10,500
AltX Research	15%	7,500
JSCF - Treasury	25%	12,500
JSCF - Public Sale	34%	17,000
JSCF - Developer Engagement	5%	2,500
Total	100%	50,000

Table 2: JSC token allocation

Validator Client Operators (21%)

Each Validator Client Operator (“Operator”) must purchase the minimum stake required to become an Operator, which is equal to 1% of the total initial supply. **These tokens are deposited into the validator smart contract and will remain locked.**

AltX (15%)

The AltX allocation is set aside as an incentive for the JSC founders, shareholders, developers, and core team members to recognize their contributions and align their interests with the project’s long-term success and growth.

JSC Foundation - Treasury (25%)

Of the initial token supply, 25% will be allocated to the JSCF treasure specifically earmarked for the Community Fund. This allocation is designed to support the growth and development of the JSC token ecosystem by funding community-driven projects,

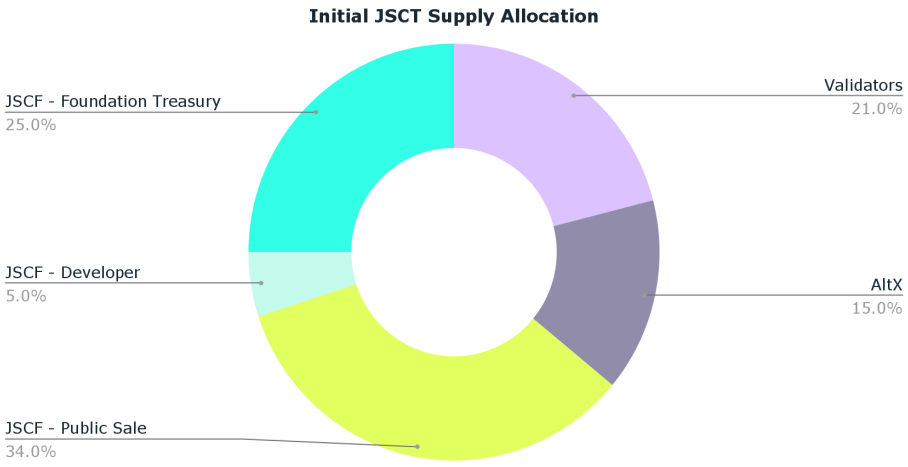
events, and initiatives. It serves as a financial reservoir to incentivize participation, foster innovation, and encourage the active involvement of community members in the project's expansion and success.

JSC Foundation - Public Sale (34%)

Of the initial token supply, 34% will be allocated to the JSCF treasury for sale to the public on international and domestic exchanges. The Public Sale portion is the share of tokens that will be offered in tranches over time to investors. It provides access and liquidity to the JSC tokens, while the Foundation ensures this sale aligns with the JSCF mission. These tokens are not vested as this sale will be conducted through an exchange listing and offerings.

JSC Foundation - Developer Engagement Fund (5%)

The Developer Engagement allocation distributes tokens to new and existing JSC community developers to increase participation in JSC Layer 1 development and application development - including but not limited to the Mizuhiki Suite and other Japan-focussed compliance technologies - and to enhance token circulation, reward loyalty and further support developer engagement.



Issuance and Rewards

JSC stakers are rewarded for their active and honest participation in securing the network. For the first 10 years of JSC's operation, stakers will earn rewards in the form of **issuance rewards** and **transaction fees**.

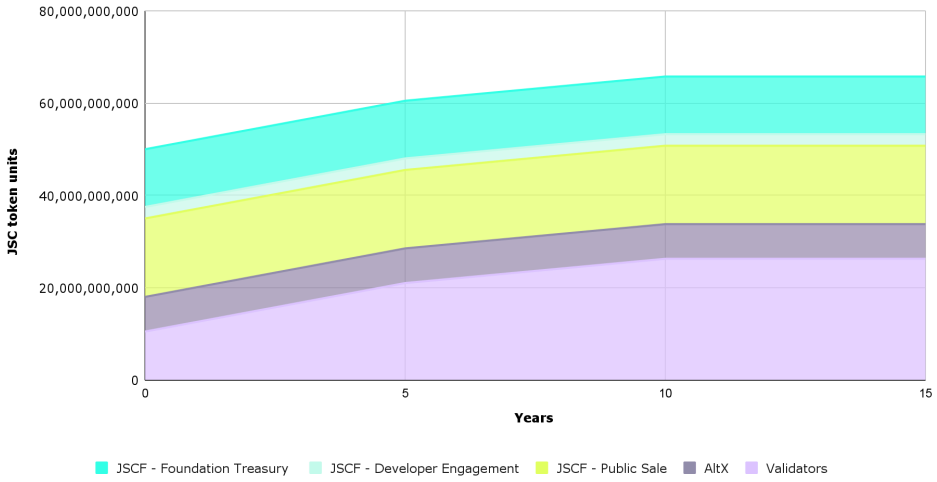
After 10 years, we envision a high level of transaction volume will be sufficient to reward validators for their securing of the network via transaction fees alone.

Issuance is set to decrease over time, with the goal of reaching zero after 10 years.

Given the JSC block time of 6 seconds[5], the issuance reward will be 400 JSC tokens per block. Assuming each validator client has an initial stake of 500 million initial JSC tokens, thus a total of 10.5 billion JSC tokens across all 21 validator clients, the issuance rewards are as follows:

- Year 1-5: 20% APY issuance reward (2.1 billion JSC tokens issued per year)
- Year 5-10: 10% APY issuance reward (1.05 billion JSC tokens issued per year)

Full node stakers (i.e., Validator Client Operators) will receive the entirety of their validator client's staking reward, while stakers in staking pools will receive the reward proportionate to their stake in the pool.

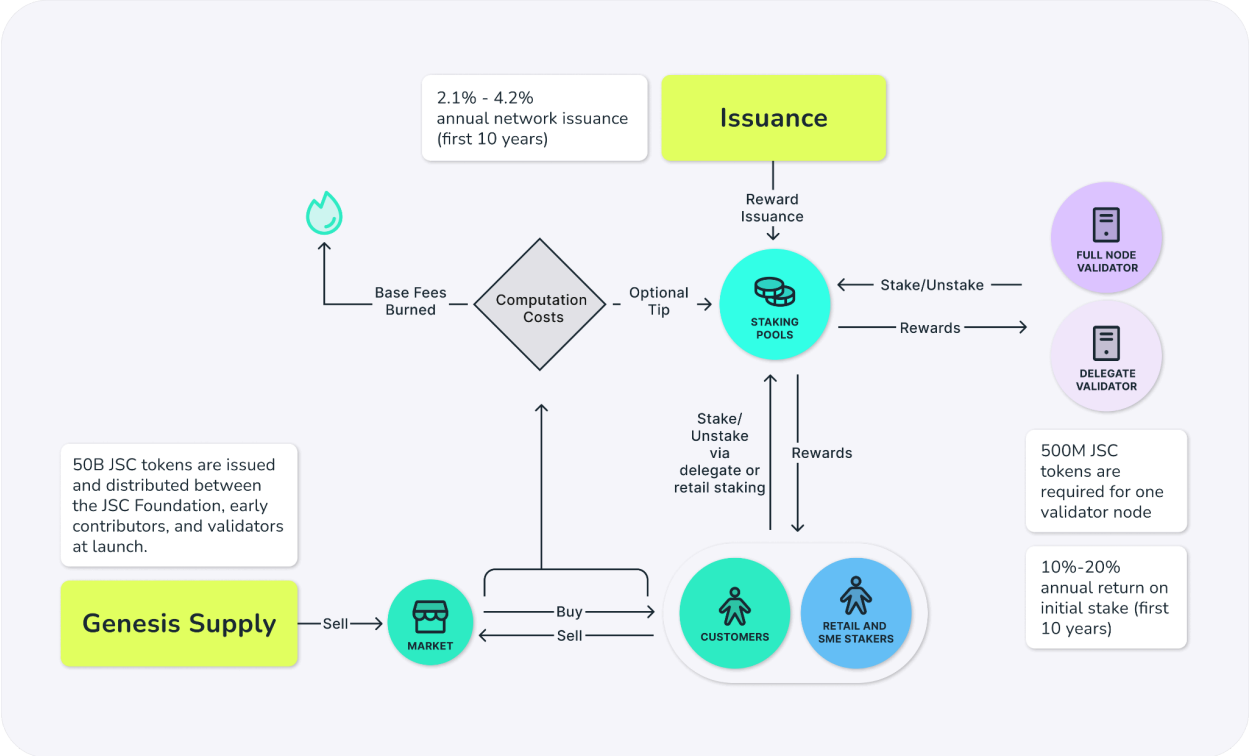


[5]Average block time will be initially configured to six seconds, balancing the customer's transaction speed with secure data propagation across the 21 validators.

Blockchain transaction fees are paid by JSC users in JSC tokens. Like Ethereum, transactions will include a base fee to pay for the processing of the transaction, and an optional priority fee for transaction prioritization. Base fees are burned, or removed from circulation, to avoid collusion between validators and customers[6].

The JSC Foundation is actively researching how transaction fees may be subsidized for stablecoins and other essential use cases through mechanisms embedded at the Layer 1 level.

The flowchart below breaks down the economic dynamics within the JSC ecosystem:



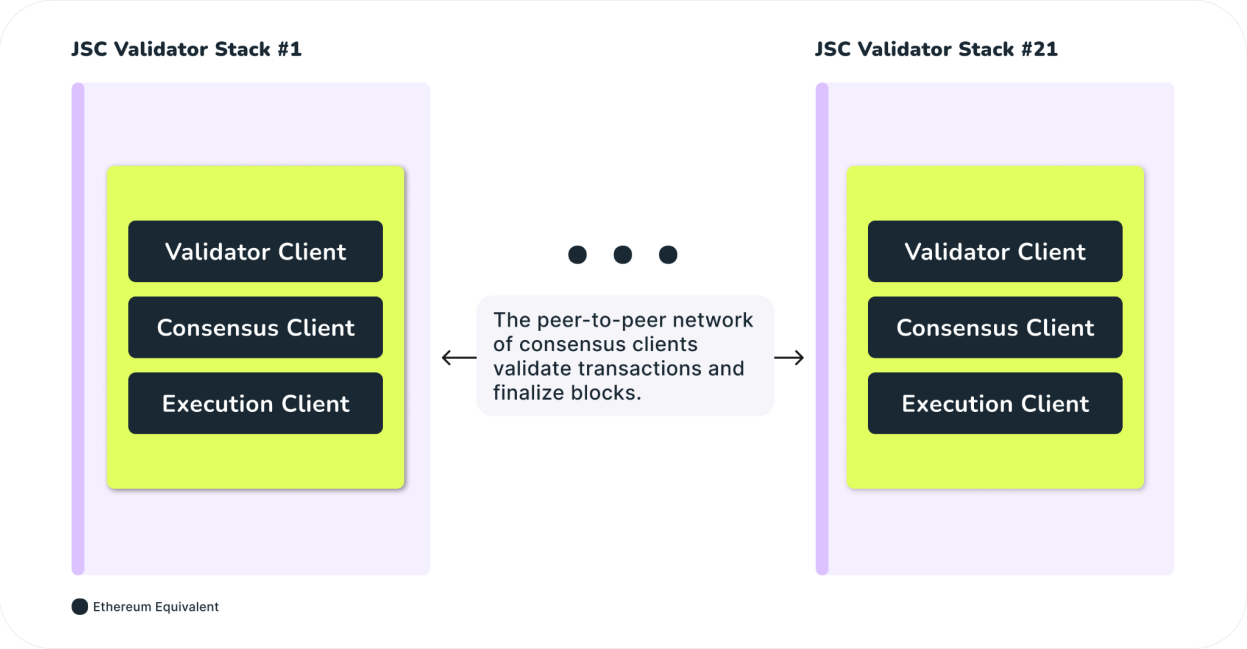
High-level overview of JSC tokenomics

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

Technical Details

Validator Stack Architecture

The architecture of the JSC "Validator Stack"[7] was designed to allow the adoption of the latest developments and changes to the Ethereum execution and consensus protocols whilst also allowing for a permissioned set of validator clients and a basic level of compliance.



JSC Validator Stack Architecture

A JSC Validator Stack consists of 3 components: the execution client, the consensus client, and a validator client. The execution client and the consensus client are standard

[7]Since Ethereum's transition to Proof of Stake, the words "validator", "validator node", and "full node" have been used interchangeably leading to justifiable confusion amongst developers and policymakers. To help distinguish between a "validator client", "full node", and a permissioned system operator on JSC we have decided to use the term "Validator Stack" to refer to an infrastructure setup running all three software clients (execution client, consensus client and validator client), and "Validator Client Operator" to refer to the title of a permissioned validator client operator on JSC. Those who are not designated Validator Client Operators are not permitted to run validator clients, and may only run execution and consensus clients without permission. Grammatically, we will initially use *Validator Stack* as a proper noun until it is integrated into the Ethereum lexicon. "Validator client" will continue to refer to the individual software client. We will refrain from using the term "validator" on its own to maintain clarity. Please see Appendix A for further definitions.

Ethereum software components and may be operated separately by those who have not been designated a Validator Client Operator seat, mostly in a “read-only” capacity on the JSC network.

- **Validator Client**
  - Entities running validator clients are deemed the true “stakers” on the network. JSC has set a high token threshold as well as a whitelist for those who are allowed to run a validator client.
  - The protocol rewards them for securing the network and maintaining consensus.
  - The main role of a validator client is to propose blocks, attest to the validity of blocks, and provide the ability for *light clients*[8] to sync with the network.

- **Consensus Client**
  - Manages the “beacon” state for the validator client with the proof of stake consensus protocols - this includes fork choice and state finality.
  - Coordinates multiple validator clients, passes messages, and handles duty assignment (such as block proposing duties).
  - Exchanges consensus messages in a peer-to-peer (P2P) network with other consensus clients.

- **Execution Client**
  - Receive and gossips pending transactions over its P2P network of other execution clients.
  - Packages pending transactions into payloads to be proposed by validator clients.
  - Executes blocks in the Ethereum Virtual Machine and updates the blockchain state.
  - Exposes the JSON-RPC API for blockchain users to interact with the blockchain (i.e., submit transactions, read the blockchain via a blockchain explorer, etc).
  - Holds logic defining the Ethereum Virtual Machine (EVM).

[8]Light clients are execution and/or consensus clients that request data from the blockchain as necessary instead of storing local copies, making the hardware requirements for running a light client much lower than a full execution or consensus client.

Consensus Protocol - Proof of Stake

JSC is an EVM blockchain network powered by a proof of stake (PoS) consensus protocol. The blockchain is validated by a selected set of 21 Validator Client Operators running validator clients, maintained onshore in Japan according to stringent hardware and software criteria set by the Japan Smart Chain Foundation (JSCF).

JSC applies proof of take consensus where the permissioned set of validator clients are routinely assigned consensus duties, and rewarded for performing them correctly and in a timely manner, and are penalised for either missing their duties or provably doing them incorrectly.

Mizuhiki Suite: Use of Decentralised Identifiers and Verifiable Credentials

Mizuhiki is the universal identity protocol optimized for the JSC network. The core of this suite revolves around “Mizuhiki ID”, which enables JSC customers to be issued a simple **verifiable presentation (VP)** or **soulbound token (SBT)** to their blockchain address by a trusted **Mizuhiki Attestor.**

Mizuhiki Attestors are a Japan-sovereign network of compliant and licensed Mizuhiki Suite attestors. They establish a "root of trust" that binds the real identity and digital identity of individuals, institutions, and other entities. Mizuhiki Attestors can issue verifiable credentials to a user's Decentralized Identifier (DID). The personal data contained in a verifiable credential **is never stored on-chain and never visible to any JSC client operator**. JSC customers are able to present a zero-knowledge proof to verifiers to prove their eligibility to perform certain on-chain actions, **without disclosing any private information** beyond the validity of their verifiable credential. This may take the form of a **verifiable presentation** and/or **soulbound token.**

Verifiable credentials result from a W3C Recommendation, and is designed to be complemented with decentralized identifiers for issuing, holding, presenting, and these credentials[9]. Verifiable credentials can represent various documents, such as university diplomas, driving licenses, identity documents, and so on. The **Mizuhiki ID** toolkit in particular provides a verifiable presentation called “Mizuhiki Verified”[10] that demonstrates a “proof of KYC” on-chain: this claims that the user controlling a particular JSC address has undergone the specific KYC and screening procedure in Japan, enabling them to interact with regulated on-chain applications.

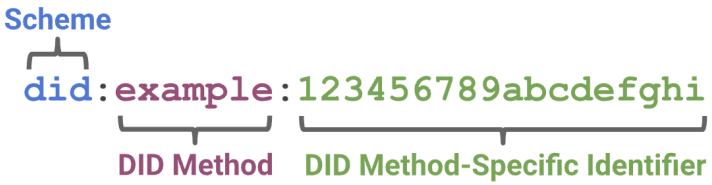
Mizuhiki’s use of verifiable credentials, verifiable presentations and soulbound tokens (which may be thought of as a type of verifiable presentation), is enabled by the use of **Decentralised Identifiers.**

[9] *Verifiable Credentials Overview*, W3C Group Note, October 2024. [Online]. Available: https://www.w3.org/TR/2024/NOTE-vc-overview-20241022/

[10] Verifiable Presentations, which are used to represent the same credentials in different situations. One representation is a zero-knowledge representation, which allows the credential owner to prove only the truthfulness of the statement related to the credential contents without revealing the credential. See more. See more: *Verifiable Credentials Data Model - Zero Knowledge Proofs*, W3C Candidate Recommendation Draft, October 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/#zero-knowledge-proofs

Decentralized Identifiers (DIDs) are digital identifiers recommended by the W3C working group[11] specifically for the verifiable identification of subjects in a decentralized environment.

Each DID is structured as a URI containing information on methods for resolving and verifying the documents referred to by the identifier.



A simple example of a decentralized identifier (DID)[12].

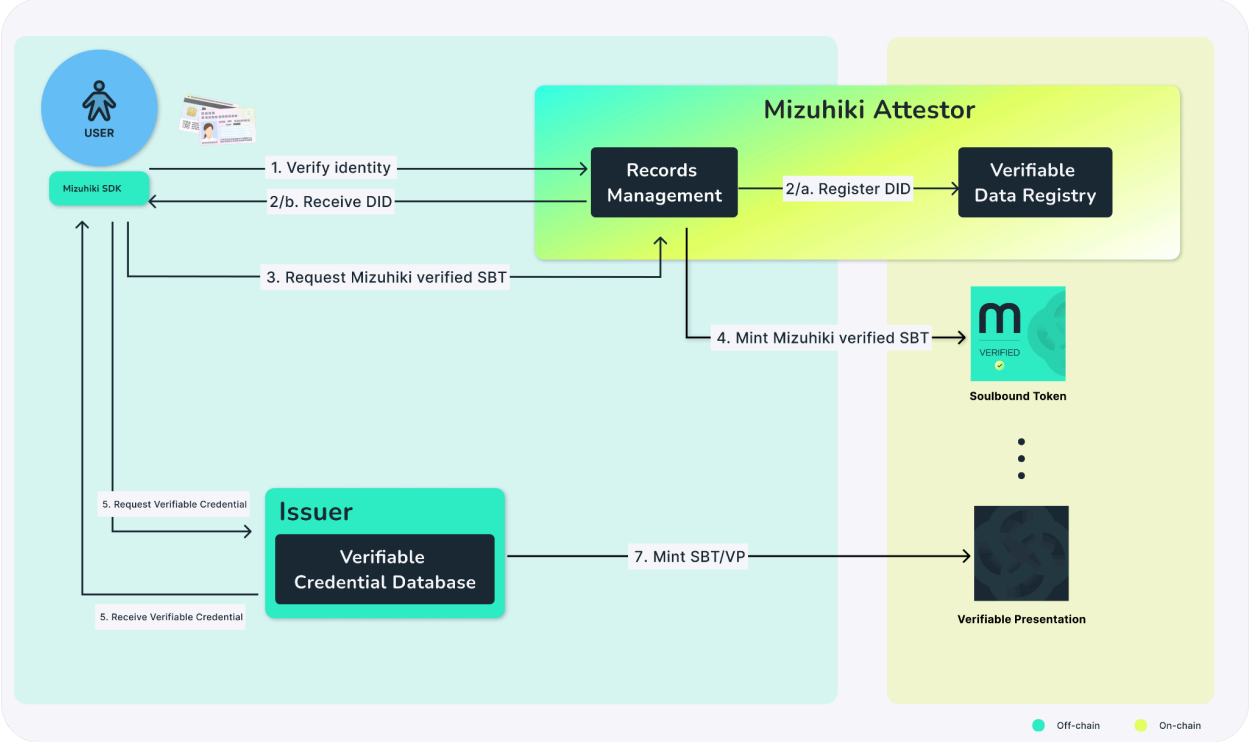
The Mizuhiki Suite features its own DID Method, which conforms to W3C specifications and is referred to as the "Mizuhiki DID" or "Mizuhiki DID Method." This method encompasses the syntax, resolution, verification, and authorization processes for Decentralized Identifiers (DIDs) and DID documents that start with the prefix `did:mizuhiki`.

A Mizuhiki DID registry is a smart contract registry that records the unique DIDs and DID Document metadata of users who have undergone KYC under Japan's Act on the Prevention of Transfer of Criminal Proceeds.

KYC is performed by a "Mizuhiki Controller", which must be a registered JPKI Service Provider[13].

[11] *Decentralized Identifiers (DIDs)*, W3C Recommendation, v1.0, July 2022. [Online]. Available: https://www.w3.org/TR/did-core/
[12] Ibid.
[13] Japan Public Key Infrastructure (JPKI) Service Provider. [Online]. Available: https://www.jpki.go.jp/jpkiguide/index.html

End-user Mizuhiki ID procedure



Mizuhiki End-User flow

The end-user flow for completing the Mizuhiki ID procedure, including the process for obtaining a “Mizuhiki Verified” address on JSC, involves the following steps:

DID Generation and Registration

1. The user starts the Mizuhiki Identification process with a **Mizuhiki Controller** (“Controller”), providing the necessary documents for identity verification. A Mizuhiki Controller conducts all identity and document checks completely off-chain with the goal of preserving user privacy.

2. The Mizuhiki Attestor generates and registers a DID on-chain via the Mizuhiki SDK (in development).

Mizuhiki Verified Soulbound Token

3. Using the Mizuhiki SDK or application, and once authorized as the owner of the respective DID, the user can issue a "Mizuhiki Verified" soulbound token (SBT) to their JSC address.

4. The SBT is issued by the Mizuhiki Controller, and is non-transferable but burnable by the Controller and/or the user. Importantly, the soulbound token does not contain any personally identifiable information (PII), including the DID.

Verifiable Credentials

5. A user may want to use *verifiable credentials* to manage other credentials. In this case, a user must request a credential from a trusted entity - such as a university or registered institution - that supports the Mizuhiki DID method and the W3C Verifiable Credential specification. We refer to such an entity as a “Mizuhiki Attestor”.

6. After receiving a VC request, the Mizuhiki Attestor may issue verifiable credentials to the user. Verifiable credentials are mapped to the user’s Mizuhiki DID off-chain, in a completely private and secure manner. The verifiable credential is able to be accessed by the DID subject by completing *authorization* to a verification method contained in their DID’s *verification methods*.

A verifiable credential may contain a set of claims, such as date of birth, GPA, or residential address. A user may only want to forward a subset of these claims to the verifier, i.e., a verifiable presentation. This means the user could reveal their age bracket without revealing their birthdate, or their residential area without disclosing their full address.

Verifiable Presentations

7. Users may generate and issue *on-chain-compatible* verifiable presentations to their JSC addresses or other applications on JSC - perhaps in the form of a soulbound token - based on their verifiable credentials via the Mizuhiki SDK. Verifiable presentations may be issued by the user holding the verifiable credential or the issuer of the credential. On-chain VPs should not have any personally identifiable information contained in them, including the DID itself. Verifiable presentations are also available off-chain and in this case may include PII.

Compliance & Risk Management Rule Engine using SBTs/VCs

If the user wants to engage in a regulated activity on JSC (e.g., a financial transaction), the user can present their SBT/VC (and hence their eligibility) to the JSC application providing the regulated service via the Mizuhiki suite.

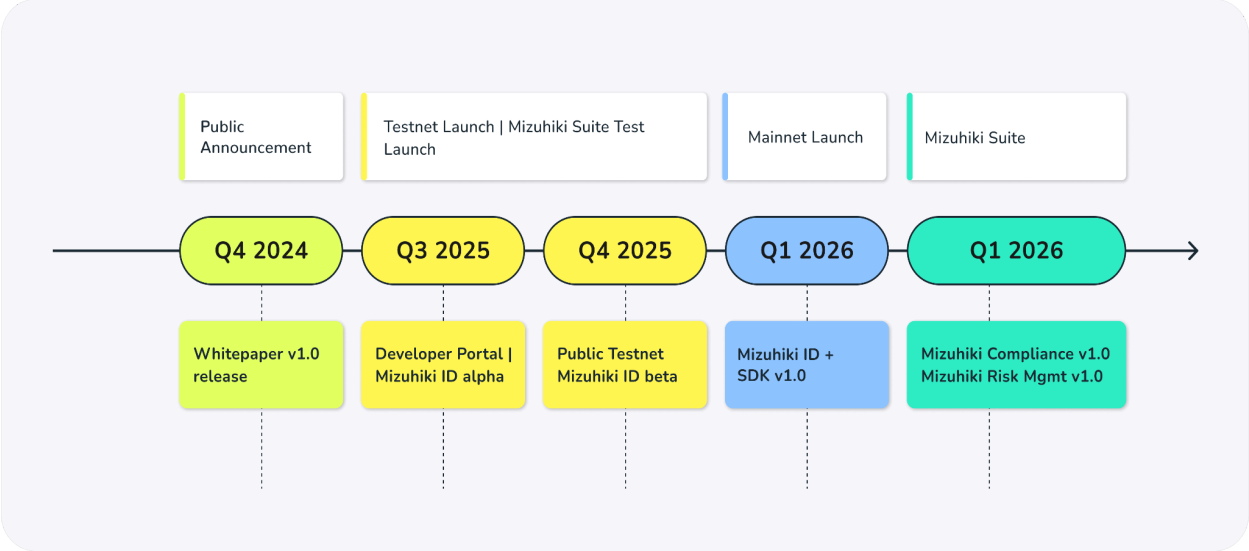
Roadmap

The project's roadmap is divided into phases, starting with a public testnet, onboarding developers, followed by building essential tooling like the validator dashboard, and block explorer.

The Public Testnet phase focuses on preparing for the JSC Mainnet launch by setting up hardware and software, JSC blacklist enabled at the layer 1, Mizuhiki ID beta tooling and testing compliance engines for wallets and stablecoins.

The following phase marks the JSC Mainnet release, with continuous upgrades to keep up with EIPs and the implementation of core infrastructure components.

Finally, the Mizuhiki Suite full release phase aims to implement the full vision of the Japan Smart Chain by releasing features like on-chain verifier contracts, blockchain application whitelisting, and Mizuhiki Attestor migration. Broken down, the phases look like this:



Japan Smart Chain roadmap

Appendix A: Glossary of Terms

- **Anti-Money Laundering (AML):** refers to a set of policies and practices to ensure that financial institutions and other regulated entities prevent, detect, and report financial crime, especially money laundering activities.
- **Blockchain**: A decentralized, distributed digital ledger that records transactions across many computers in a secure and immutable manner.
- **Decentralized Autonomous Organization (DAO)**: An organization that is governed by rules encoded as computer programs and operates without a centralized leadership structure.
- **Decentralized Identifiers (DID)**: Digital identifiers designed for verifiable identification of subjects in decentralized environments.
- **Electronic Know Your Customer (eKYC)**: An electronic process by which private and public institutions verify a customer's Personal Identifiable Information (PII) to comply with anti-money laundering and other regulations. A common implementation of eKYC is facial recognition through smartphone and computer cameras.
- **Ethereum Virtual Machine (EVM)**: A virtual machine that executes smart contracts on the Ethereum blockchain, providing a runtime environment for executing bytecode.
- **Ethereum Mainnet:** The production "main network" of Ethereum.
- **JSC Mainnet:** The production "main network" of Japan Smart Chain.
- **Know Your Customer (KYC)**: A process by which entities verify their customer's Personal Identifiable Information (PII) to comply with anti-money laundering (AML) and other regulations.
- **Layer 1 (L1)**: The base blockchain network, such as Ethereum or Bitcoin, handles transaction settlement and maintains the core infrastructure.
- **Layer 2 (L2)**: A secondary protocol built on top of a Layer 1 blockchain to improve scalability and transaction throughput.

- **Mizuhiki Suite (formerly known as “Mizuhiki Protocol”)**: JSC's proprietary protocol that introduces an user-controlled identification toolkit for enhancing user convenience, safety, and network security.
- **Mizuhiki Attestors:** This is the JSC equivalent of “Certificate Authorities” (CA). In the World Wide Web paradigm, CAs act as trusted third parties—trusted both by the subject (owner) of a digital certificate and by the party relying upon that certificate. Mizuhiki Attestors implement the Mizuhiki ID tooling from Mizuhiki Suite.
- **Mizuhiki Controller:** A registered JPKI Service Provider, and a JSCF-approved entity authorised to issue Mizuhiki DIDs and “Mizuhiki Verified” soulbound tokens.
- **Personal Identifiable Information:** Refers to personally identifiable information such as name, date of birth, email address, or biometric data.
- **Proof of Stake (PoS)**: A consensus mechanism used by some blockchain networks to validate transactions and create new blocks, where validators stake their cryptocurrency holdings to participate in the consensus process.
- **Smart Contract:** Smart contracts are digital contracts/instruction sets stored on the blockchain that are automatically executed when predetermined terms and conditions are met.
- **Soulbound Token (SBT):** A non-fungible token that is non-transferable, but may be revokable by either the recipient of the SBT or the issuer. JSC currently implements the ERC-5484 standard (Consensual Soulbound Tokens).
- **Stablecoin**: A cryptocurrency designed to minimize price volatility, often by being pegged to a stable asset like the US dollar or a commodity.
- **Staker:** An entity that stakes JSC tokens into the JSC network.
- **Sybil Attack:** A type of attack in decentralized networks where a single entity creates multiple identities to gain a disproportionate influence on the network.
- **Testnet:** a “test network” which simulates the behavior of the respective chain’s mainnet. Testnets are used by developers and trial customers to test the processes and mechanisms of the mainnet without real-world financial repercussions.

- **Validator Client Operator:** Validator Client Operators ("Operators") represent the backbone of the JSC network, typically consisting of large Japanese companies and established enterprises that are entrusted with the task of operating validator clients alongside maintaining network infrastructure. Operators maintain physical or cloud-based infrastructure, consensus processes, and contribute to network governance decisions.
- **Validator Stack:** The combination of blockchain node hardware and software infrastructure, onshore in Japan, that is collectively responsible for implementing and securing the JSC blockchain by collecting transactions, building them into blocks, and propagating those blocks to all the participants of the network. Validator Stacks consist of a consensus client, execution client and validator client.
- **Verifiable Credentials (VC)**: Digital credentials that can be verified in a decentralized environment, often using decentralized identifiers (DIDs) for identification.
- **Verifiable Presentation:** A subset or cryptographically abstracted derivation of a Verifiable Credential, with the purpose of disclosing the minimum amount of information required to perform a regulated or rule-based activity.
- **Verifiable Data Registry (VDR):** A Verifiable Data Registry (also known as a *Trusted Issuer Registry*) manages Verifiable Credential data (**not** to be confused with Personal Identifiable Information) on Japan Smart Chain. The VDR is tamper-evident and represents a correct record of Verifiable Credentials issued by Mizuhiki Attestors.
- **Zero-Knowledge (ZK), Zero Knowledge Proof (ZKP)**: Refers to a modern cryptographic method allowing one party to prove to another party that a statement is true without revealing any additional information