JAPAN
SMART
CHAIN

WHITEPAPER

VERSION 1.0.0 | NOVEMBER 2024

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 white paper 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 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. The JSC Block Builder wraps around the execution client and the consensus client[3], securing compliant transactions and prioritizing essential transactions such as stablecoins. The JSC-specific validator requirements are set only once in the Genesis block. This ensures that JSC's core software can be upgraded in lockstep with Ethereum.

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.

[3] The JSC Block Builder interposes itself between the RPC layer and between the peer-to-peer (P2P) connectivity of the validator nodes.

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 layer.

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 Identity Protocol

Aligning with JSC's Principles of Safety and Sovereignty

In-line with JSC's vision of addressing consumer pain points in the Layer 1 rather than the application layer, JSC offers its pioneering **Mizuhiki Protocol**, which introduces a user-controlled identification method[4] matched with a suite of eKYC[5] tools and services, **offered for free to Japan Smart Chain projects and end-users**.

JSC enhances 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 Protocol ensures that 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 permission to their verified credential[6] 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 KYC 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 Protocol by: (a) limiting company access to unnecessary personal information, (b) abstracting credentials (such as age or university graduation status) from their natural personhood identities, and (c)

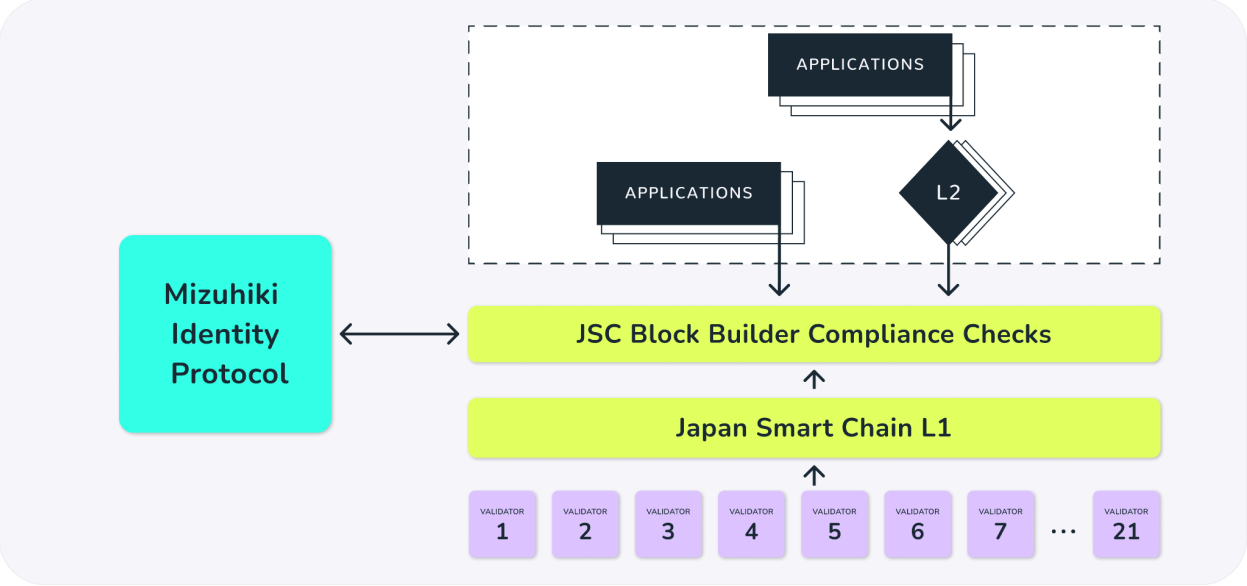
[4] Decentralised Identifiers (DID), a W3C recommendation, will be used as our user-controlled identification mechanism, allowing users to take back ownership of their data while also securely abstracting the necessary credentials required to transact safely in Japan.
[5] Electronic Know Your Customer. eKYC is used interchangeably throughout this paper with "Know Your Customer" (KYC)
[6] A verifiable credential is a nationally recognised credential that proves a customer's eligibility to participate in a certain activity. For example, a credential may include a job-seeker's GPA, or a consumer's age eligibility to purchase alcohol. Once the credential has been witnessed by an attestor, the verifiable credential may be considered a *verified* credential for a limited or unlimited time period.

allowing users to revoke permissions to their DIDs and/or verified credentials in a single click.

- **Effortless KYC and embedded AML checks:** JSC ensures the latest security and privacy standards by embedding context-specific compliance, KYC, and AML checks programmatically into the blockchain.
- **Continuous compliance:** Compliance with Japanese laws for regulated use cases is built into JSC, streamlining user experience while ensuring efficient implementation of Japanese regulations at the protocol level. This built-in compliance significantly reduces the overall compliance burden and cost for projects, enabling innovators to focus on building applications.

Japan Smart Chain is committed to driving down the cost of identity verification and of compliance with Japanese regulations through **programmatic continuous compliance** in the block builder. 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.

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 validators 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 operators of the 21 validator nodes that make up the JSC blockchain 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. Validators 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 defined 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 is 21 Japan-sovereign validator nodes, all onshore 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 nodes, 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 nodes will allocated as follows:

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)[7]	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 Nodes		21		

Table 1: Staking and Validator Ecosystem

[7] 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.

Issuance

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)
Validators	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

Validators (21%)

Each validator must purchase their validator stake, which is equal to 1% of the total initial supply. **These tokens are deposited into the validator smart contract and as such 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,

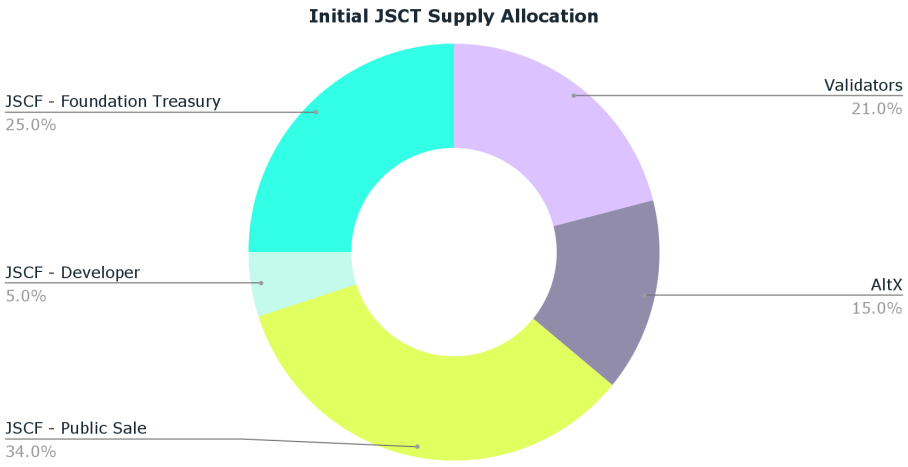
events, and initiatives. It serves as a financial reservoir to incentivize participation, foster innovation, and encourage the active involvement of community members in the project's expansion and success.

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 (including but not limited to the Mizuhiki Protocol and other Japan compliance technologies), JSC application development, token circulation, reward loyalty, and enhanced developer engagement.



Staking Rewards

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

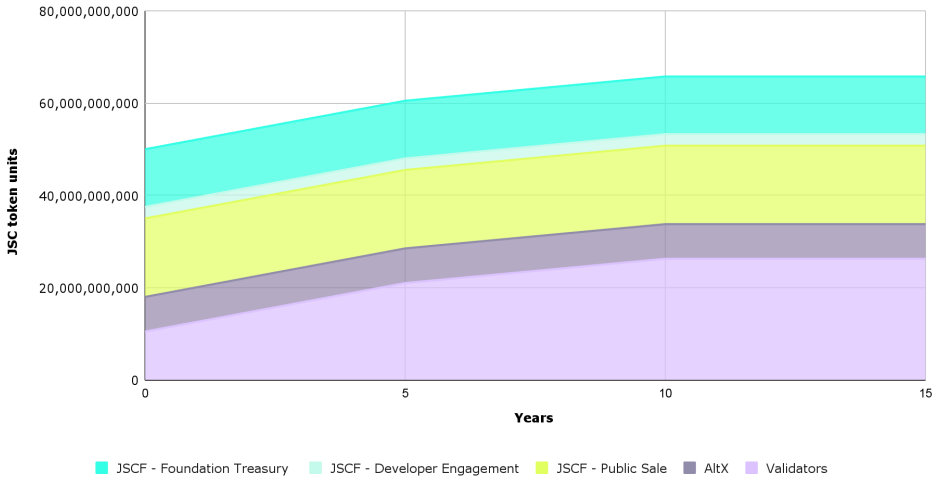
Inflation has been programmed to decrease over time, reaching zero after 10 years.

Given the JSC block time of 6 seconds[8], the issuance reward will be 400 JSC tokens per block. The issuance rewards for validators will make JSC's annual inflation 4.04% in year 1, decreasing to 1.6% in year 10, and 0% thereafter.

Assuming each validator has an initial stake of 500 million initial JSC tokens, a total of 10.5 billion JSC tokens across all 21 validators, 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 operators will receive the entirety of their validator's staking reward, while stakers in staking pools will receive the reward proportionate to their stake in the pool.

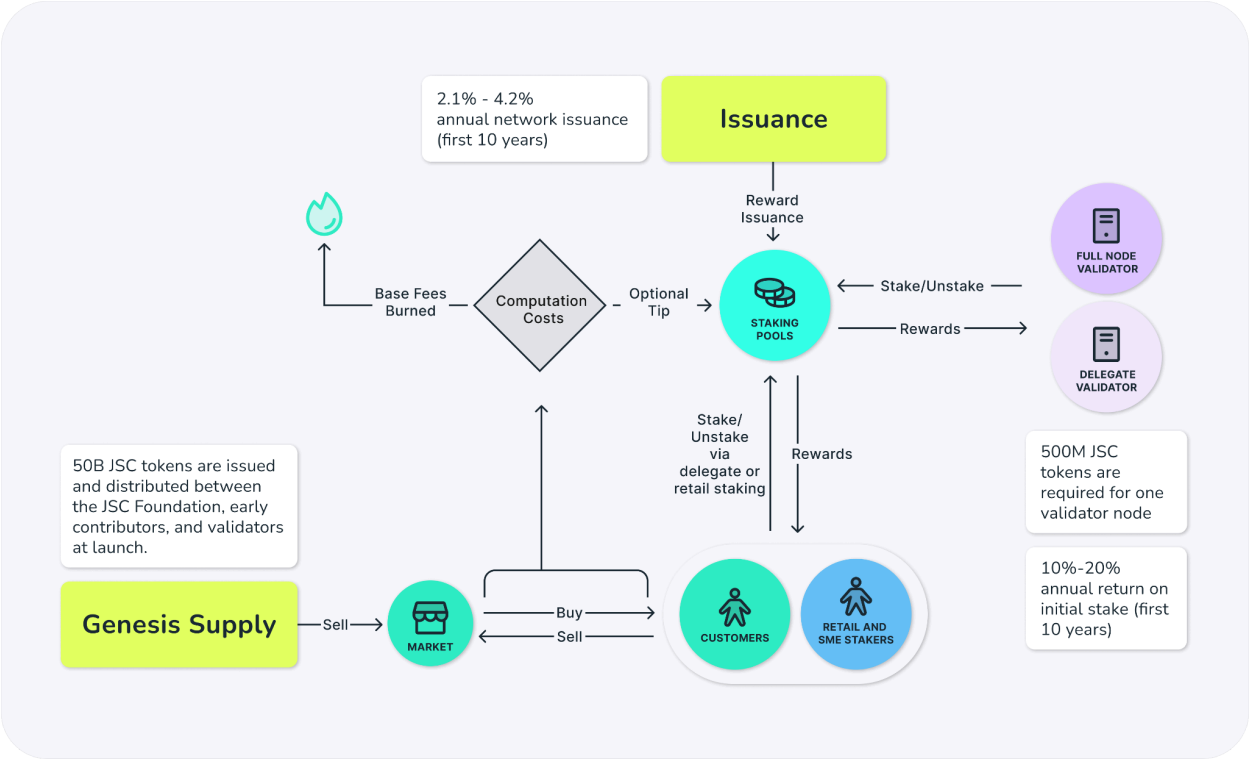


[8]Average block time will be initially configured to six seconds, balancing the customer's transaction speed with secure data propagation across the 21 validators.

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 priortisation. Base fees are burned, or removed from circulation, to avoid collusion between validators and customers[9].

The JSC Foundation may choose to subsidize transaction fees for stablecoins and other essential use cases through mechanisms built into the JSC Block Builder protocol.

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



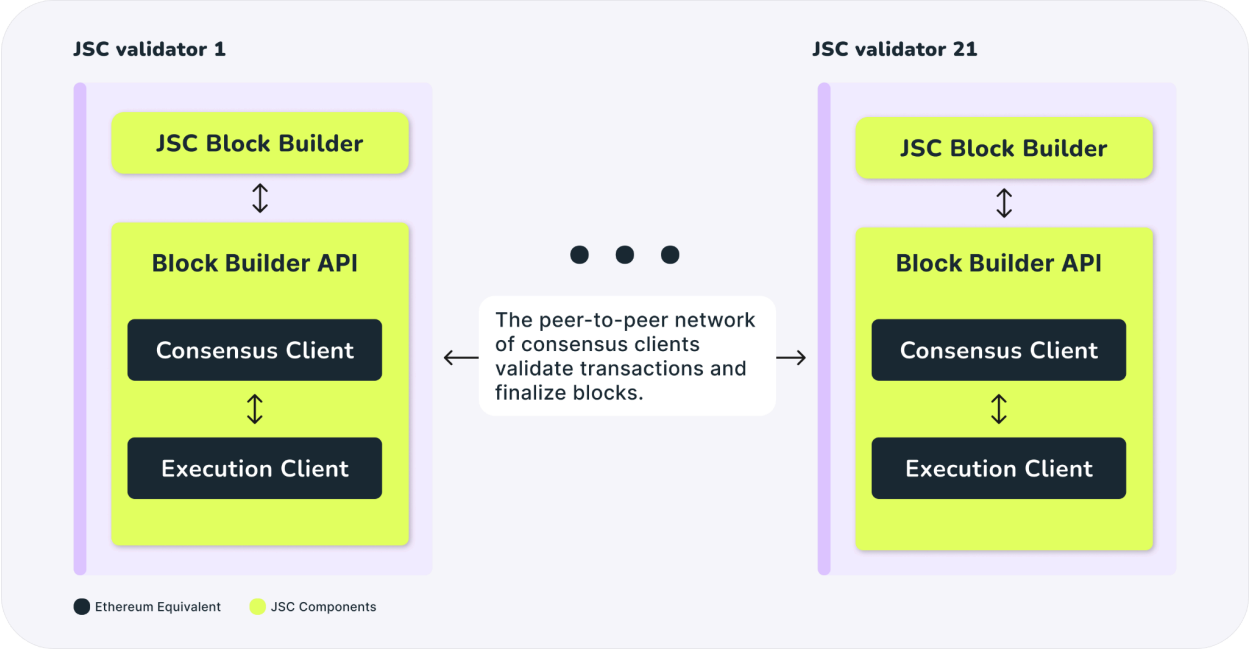
High-level overview of JSC tokenomics

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

Technical Details

Node Architecture

The architecture of the JSC validator node was designed to allow the adoption of the latest developments and changes to the Ethereum execution and consensus protocols while preserving Mizuhiki's continuous compliance.



JSC Validator Architecture

JSC validator nodes consist of 3 components: the execution client, the consensus client, and the JSC Block Builder. The execution client and the consensus client are standard Ethereum software components, while the JSC Block Builder is unique to JSC.

- **JSC Block Builder**
  - Incorporates the continuous compliance framework for transactions.
  - Builds blocks of transactions for the consensus client.
    - In the case of a regulated activity, such as stablecoins, the block builder checks that the transactions are compliant before they are submitted to the consensus client.
  - Communicates with consensus clients through the standardized Block Builder API.

- **Consensus Client**
  - Exchanges consensus messages in a peer-to-peer (P2P) network with other validators and other network participants.
  - Provides fault-tolerant state-machine replication (FT-SMR).
  - Communicates with the JSC Block Builder through the standardized Block Builder API.

- **Execution Client**
  - Executes each transaction in a block received from the consensus client.
  - Runs external queries of the blockchain state.
  - Stores blockchain state in a verifiable manner.
  - Runs the Ethereum Virtual Machine (EVM).

Consensus Protocol

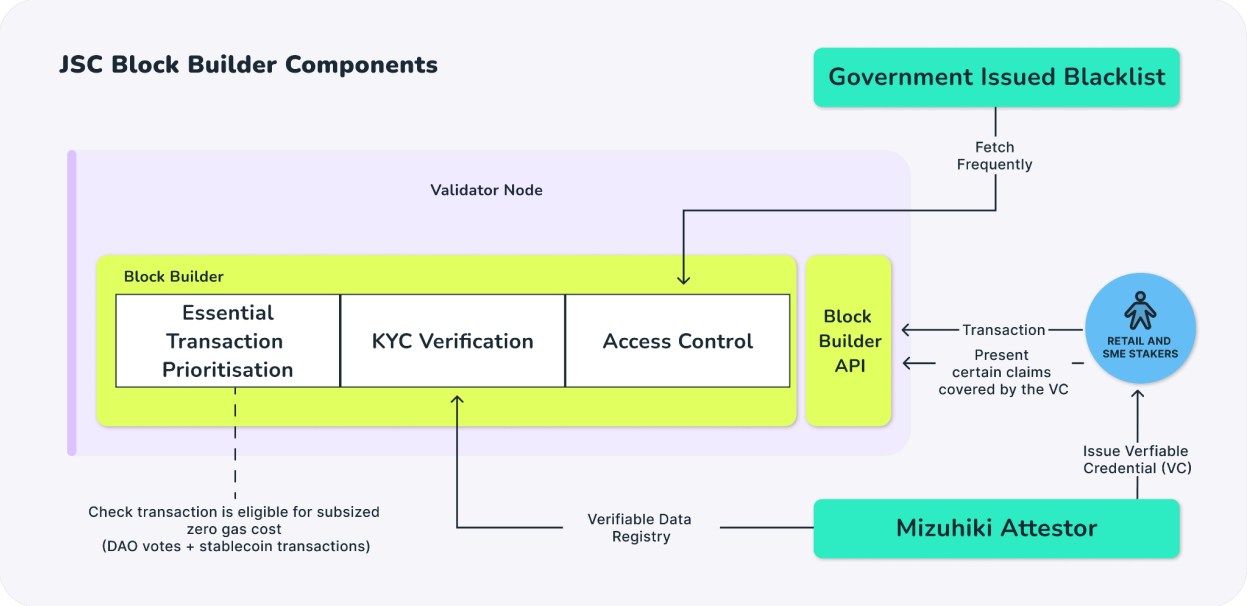
JSC is an EVM blockchain network powered by a Proof of Stake (PoS) consensus protocol. The blockchain is validated by a selected set of 21 validator nodes, maintained onshore in Japan according to stringent hardware and software criteria set by the Japan Smart Chain Foundation (JSCF).

JSC's 21 validators run the standard Ethereum consensus client, with adjustments to the smart contracts specifying validator selection, leader selection, reward distribution, and unstaking processes.

The JSC modifies only the consensus smart contracts:

- Staking contract: Adjusts validator selection to a group of 21 *authorized,* active validators on the network at a given time.
- Leader selection is a consensus mechanism for choosing a single validator to propose a block. The JSC approach ensures a fair distribution of consensus leaders across block heights among the 21 validators.
- Withdrawal contract: JSC modifies the specifics of the unstaking and bonding periods, including reward distribution.

JSC Block Builder: Integrating the Mizuhiki Protocol



JSC Block Builder components

Mizuhiki is the user-controlled identity protocol optimized for the JSC network. The Protocol specifies the procedure enabling JSC customers to be issued a single, simple **Verifiable Credential (VC)** to their blockchain address by a **Mizuhiki Attestor**[10]**.** The customer is able to present certain claims covered by the VC to JSC validators, as required.

Applications deployed on the JSC blockchain are able to safely interact with Mizuhiki-verified addresses while complying with Japanese regulations.

The block builder needs to verify three things to deliver continuous compliance for all transactions on the blockchain:

1. **Access Control** - Prevent blacklisted addresses from performing transactions.
2. **KYC Verification** - If the activity is regulated, KYC verification checks that the transaction's signing wallet has the appropriate verified credential, registered by a known Mizuhiki attestor. The absence of the appropriate verified credential results in transaction failure.

[10] Mizuhiki Attestors are a Japan-sovereign network of compliant, licensed Mizuhiki Protocol attestors which establish a "root of trust" about the binding of the real identity and the digital identity of individuals, institutions and other entities.

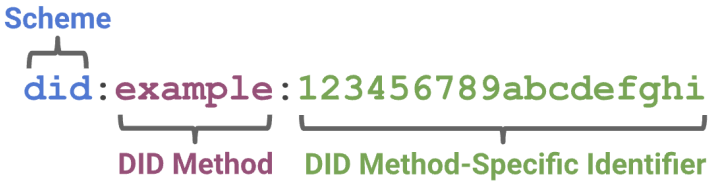
3. **Essential Transaction Prioritization** - Checks whether the transaction's gas can be subsidized according to a gas subsidization policy defined by the Japan Smart Chain Foundation.

The private data linked with **Verifiable Credentials is not visible to the JSC validators**. JSC customers are able to present a zero-knowledge proof to validators to prove their eligibility to perform certain on-chain actions, **without disclosing any private information** besides the truthfulness of their Verifiable Credential.

Decentralized Identifiers and Verifiable Credentials

Decentralized identifiers (DID) 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].

Verifiable Credentials (VC) result from another W3C specification that utilizes decentralized identifiers for issuing, holding, presenting, and verifying credentials[13]. Credentials could include various documents, such as university diplomas, driving licenses, identity documents, and so on.

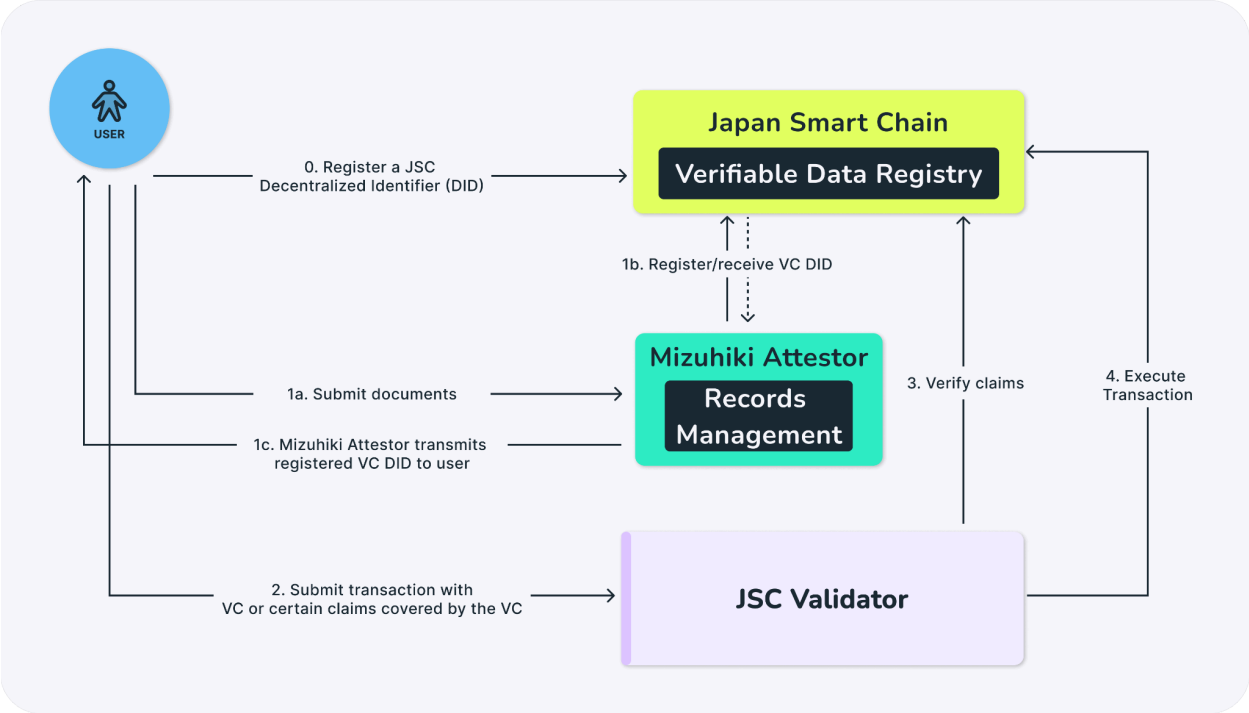
The specification also defines **Verifiable Presentations**, which are used to represent the same credentials in different situations. One representation is a zero-knowledge

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

representation, which allows the credential owner to prove only the truthfulness of the statement related to the credential contents without revealing the credential[14].

The JSC network and Mizuhiki Protocol use verifiable credentials and decentralized identifiers to represent KYC attestations in a standardized way. This allows verifying statements related to KYC documents without revealing private information to validators and application operators. Additionally, verification of the zero-knowledge credential representations is possible in smart contracts, allowing JSC application developers and customers to benefit from the Mizuhiki Protocol on a daily basis at no extra difficulty.

End-user Mizuhiki Protocol procedure



Mizuhiki Protocol end-user flow

The end-user flow for completing the Mizuhiki eKYC requires the following steps:

0. User DID generation and registration

The user generates a DID locally (e.g., through a smart contract deployed on JSC), using their JSC wallet address and registers the DID on-chain.

[14] *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

1a. Submit necessary documents to Mizuhiki Attestor

The user starts the Mizuhiki Identification process with a Mizuhiki Attestor, providing the necessary documents for credential verification alongside the DID registered in Step 0. A Mizuhiki Attestor conducts all identity and document checks completely off-chain with the goal of preserving user privacy.

1b. Mizuhiki Attestor registers Verifiable Credential DID on-chain

Once the user's document and DID checks are complete, the Mizuhiki Attestor formalizes the document verification by registering a Verifiable Credential on JSC (specifically, in the **Verifiable Data Registry**[15]). This Verifiable Credential is embedded with the user's DID registered in step 0 so that no one else is able to use this Verifiable Credential.

1c. Verifiable Credential is transmitted to the user

The user is now able to share selected claims contained in the Verified Credential with anyone.

2. User submits JSC transaction with Verifiable Credential

If the user wants to engage in a regulated activity on JSC (e.g., a financial transaction), the user can present their Verified Credential (and hence their eligibility) to the JSC application providing the regulated service.

Zero-knowledge proofs[16] may be employed to keep the user's identity secret from the public while still being verifiable by the Mizuhiki Attestor.

Additionally, 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, which we refer to as a **Verifiable Presentation.** This means the user could reveal their date of birth without revealing their GPA or residential address.

[15]The Mizuhiki Verifiable Data Registry is an *on-chain* information registry used by JSC validators and regulated applications to confirm the validity of a Verifiable Credential without needing to contact the Mizuhiki Attestor directly.
[16]See 13.

3. Validator checks claims

A JSC validator (specifically, the Block Builder within the validator node) verifies the claims[17] covered by the Verifiable Credential via the **Verifiable Data Registry** and ensures the transaction is compliant with Japan's regulations.

4. Transaction is executed

Once the transaction passes all Mizuhiki Protocol checks, the lead validator adds the transaction to a block which is thereafter executed on the JSC blockchain.

[17]Typically, a verification check performed by the JSC validator will include checking the identity of the Mizuhiki Attestor that registered/issued the Verifiable Credential, the integrity of the Verifiable Credential, and the validity of the Verifiable Credential (ensuring it has not expired or been revoked).

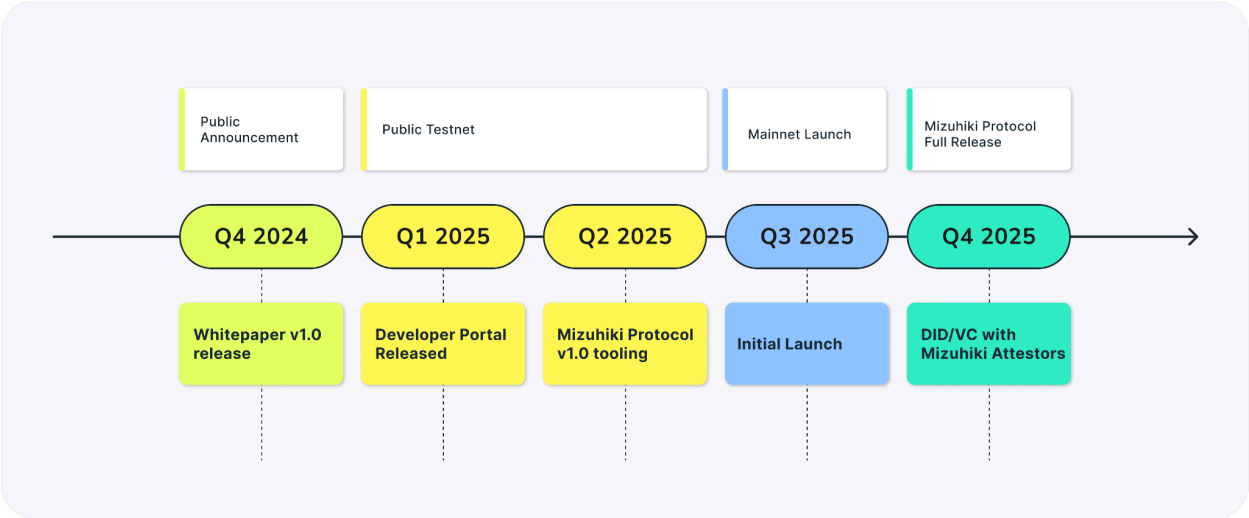
Roadmap

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 mainnet launch by setting up hardware and software, the JSC block builder with Mizuhiki Protocol v1.0 tooling, and developing wallet and stablecoin SDKs (sign in with JSC).

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 Protocol 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 Identity Protocol / Mizuhiki Protocol**: JSC's proprietary protocol that introduces an user-controlled identification method 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 Protocol.
- **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.
- **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 Node:** 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 nodes are composed of one or more stakers. Throughout this paper we refer to validator nodes as “nodes” and “validators interchangeably.

- **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