Tokenization Request for Proposal

Blockchain Concerns

RFP 2024

Revision 1.0

03 Apr 2024

Approved

Document History

Revision	Published	Author(s)	Summary of Changes
1.0	11 APR 2024	Nasdaq	First revision.

Table of Contents

General Information 4
- **0.1 Tokenization RFP** 4
  - **0.1.1 Blockchain Protocol / Platform** 4
  - **0.1.2 Primary Use Case** 6
  - **0.1.3 Proof of Concept** 7
  - **0.1.4 Capabilities** 9

Technology 11
- **1.1 Protocol Technology** 11
- **1.2 Interoperability** 21
- **1.3 Compliance and Token Management** 23
- **1.4 Security** 26
- **1.5 Additional Questions** 28

General Information

Nasdaq, Inc. ("Nasdaq") is proposing a trading infrastructure for the full lifecycle of purchases and sales in digital assets ("Regulated DA Ecosystem"). The intent of the Regulated DA Ecosystem is to provide market participants the ability to issue, trade, settle, and custody digital assets in a regulatorily compliant environment subject to standards that investors in U.S. capital markets expect and that Nasdaq brings to bear to other asset classes.

Please provide detailed technical information with your responses and any relevant documentation.

0.1 Tokenization RFP

This RFP is due by close of business on Monday, April 22, 2024. Please email the RFP submission to:

1. Christopher.Harrsch@nasdaq.com
2. Matthew.Savarese@nasdaq.com
3. Daniel.Carrigan@nasdaq.com

0.1.1 Blockchain Protocol / Platform

Please provide an overview of your blockchain protocol / platform, emphasizing its core architecture strengths and features.

Anatoly Yakovenko, cofounder of Solana, CEO of Solana Labs, and author of the original Solana whitepaper, has been using Nasdaq as a point of reference since Solana mainnet beta went online in March 2020. **Please watch this 1 minute video of Toly talking about Nasdaq and Solana over the years.** Consensus at the speed of light has been a north star for Solana blockchain development – focusing on improvements to optimize speed, cost, and scalability for a global, layer 1 global state machine. The results of this has created the best blockchain option suited to support Nasdaq-scale applications:

- Current measured & proven throughput of **65,000 TPS**[1]

[1] The 65,000 TPS figure refers to a Solana Permissioned Environment; Throughput on mainnet beta is up to 20,000 TPS. The independent Firedancer validator client, currently being developed by Jump Crypto, has processed 1.2 million TPS in a test environment. Firedancer is live on testnet and is expected to be live on mainnet beta soon.

- Transaction fees of **$0.001 USD**[2]
- Settlement & optimistic finality times **under 1 second**[3]

Given these attributes, payments and finance have been the “killer app” to build on the Solana blockchain, and other financial institutions have noticed. In selecting Solana for stablecoin settlement with merchant acquirers Worldpay and Nuvei, Visa wrote that Solana “holds promise [...] due to its speed, scalability and low transaction costs, helping to make it a good candidate for efficient blockchain settlement rails using stablecoins.” Visa isn’t alone. Paxos recently issued a stablecoin on Solana regulated by New York State Department of Financial Services (NYDFS).

Overall, there was $1.4 trillion of stablecoin volume on Solana in March 2024[4], more than 2x that of Ethereum mainnet, and 20x that of Avalanche and Polygon *combined*. Even beyond stablecoins, Solana uniquely enables true real-time buyer-seller markets using Central Limit Order Book protocols, which saw over $94 billion in DEX trading volume in March 2024[5].

The Solana Foundation would make Nasdaq their top priority, working together to deliver enterprise grade solutions to support Nasdaq’s tokenizations platform. We are prepared to provide the following as part of this proposal:

- **$45MM USD** in funding
- A **dedicated team of 5+** comprised of two backend engineers, two frontend engineers, a product manager, and fractional designer, and project management resources to co-build with Nasdaq
- Executive sponsors at the Solana Foundation with **deep legal, regulatory, and tokenization experience** to ensure success of the Nasdaq product post-launch

We look forward to presenting our proposal in greater detail. Thank you!

[2] The median transaction fee of 0.00001 SOL at a price of $173 is $0.001. Source: https://dune.com/queries/3200383/5348645
[3] This is 50ms in a Solana Permissioned Environment, and 400ms in mainnet beta.
[4] Source: https://app.artemis.xyz/stablecoins?stablecoinBreakdown=chain&granularity=monthly
[5] Source: https://dune.com/queries/3612812?start+date_d83555=2024-01-01+00%3A00%3A00

0.1.2 Primary Use Case

Describe your protocol/platform's primary use cases and any notable projects exemplifying them.

Developers, applications, and enterprises have used the Solana blockchain for a large variety of use cases that take advantage of Solana's high throughput and low fees. The verticals with the most activity are DeFi, Payments / Commerce, NFTs, Games, and DePIN:

- **DeFi**: The vibrant Solana ecosystem has become the highest trading volume platform out of any layer 1 blockchain. This has come as a result of strong builders creating fantastic user experiences, as seen in popular protocols such as Orca, Jupiter, and the more than a dozen projects built on top of the OpenBook protocol. Central Limit Order Book functionality is uniquely possible on Solana due to its speed and low cost. Additionally, there is a growing RWA market, which includes Ondo Finance doing treasuries, Homebase doing real estate, and Credix doing private credit.

- **Payments / Commerce:** Both web3 and traditional companies are taking advantage of the Solana network's speed and low cost (as well as unique tools such the open Solana Pay protocol) to build crypto-based payment and merchant settlement rails. Some example companies include Visa, Mastercard, Stripe, and Helio's Shopify plugin. Additionally, many companies are building global P2P apps on Solana, including Sling. The Solana network is even enabling new use cases such as streaming payments (sending fractions of a dollar every second for example) from companies like Streamflow and next-generation loyalty programs as piloted by shoe company ASICS and restaurant chain Boba Guys.

- **NFTs**: High throughput means that there is a thriving NFT ecosystem on Solana, from the traditional artists and collections to new use cases . There have been over 450 million NFT mints on Solana, held by 41 million wallets. Most notably, DRiP has sent over 150 million NFTs to 2 million wallets for about 878 SOL at a unit cost of $0.0001 per NFT by leveraging the Solana protocol's unique state compression technology. Beyond compression, the NFT space has seen a number of community-led innovations, such as Coral's xNFTs (NFTs that can execute programs) or XP.xyz's tpNFTs ("Tamperproof" NFTs that can be used for event ticket markets). Other examples of cutting-edge companies that use NFTs in nontraditional ways include smart messaging app Dialect, social network

Primitives, and marketplace Exchange Art.

- **Games**: Blockchain games leverage Solana not only for its speed and low costs, but also for its capacity to support entire economies and ecosystems at scale. For instance, Photo Finish LIVE (an official partner of the Kentucky Derby) implemented the complex horse racing economy onchain. In the most recent "season" (4 week period), stable owners generated a collective $700k in revenue. Even more ambitious, Parallel (Web3 Game of the Year in 2023) announced their upcoming title, Colony, where AI agents will autonomously transact onchain and navigate blockchain ecosystems on their own which will be build on Solana. Eventually, blockchain games could go much deeper than ownership of digital items and collections. Play-and-own games are ones where players own their data and progression across games, platforms, and publishers.

- **DePIN**: High throughput and low fees make Solana uniquely qualified to host token-incentivized networks. These DePIN (decentralized physical infrastructure networks) projects allow communities to build much-needed alternative infrastructure from the ground up. Some prominent examples include Helium's 5G and IoT wireless network coverage, Hivemapper's decentralized mapping, Teleport's rideshare protocol, and Render's distributed GPU compute network.

This is just a sample of some of the use cases that already exist in the Solana ecosystem.

0.1.3 Proof of Concept

Provide examples of proof-of-concept projects or applications that have been developed on your platform.

Several financial institutions and large organizations that have built or are building applications on the Solana blockchain:

- **Paxos** and **GMO** have both issued NYDFS-regulated stablecoins on Solana (USDP, ZUSD, GYEN) using the token extensions program.

- **Visa** is utilizing the Solana blockchain to expand their stablecoin settlement capabilities with Circle's USDC, adding pilot programs with merchant acquirers Worldpay and Nuvei.

- **Stripe** built a crypto on-ramp on Solana that is used by many large applications, including Magic Eden. The majority of their volume is coming from Solana transactions. Stripe's rationale for launching with Solana was their assessment of demand and active users in the Solana ecosystem.

- **Google Cloud** is currently running a block-producing validator in South America, indexing Solana data for use within bigQuery, serving Solana archival data from BigTable, and is launching a self-hosted validator in Google Cloud Platform via their Blockchain Node Engine product.

- **Amazon Web Services** is currently running multiple validators, has tested and benchmarked Solana validator performance and specifications on both RPC and voting validators configurations, and developed one click deployment scripts for Solana validators.

- **Helium,** a decentralized wireless IoT network, migrated to Solana in Q2 2023 to enhance its infrastructure. By Q3 2023, Helium launched an unlimited mobile phone data plan, starting with a $5 per month pilot in Miami that quickly extended to a $20 per month nationwide plan.

- **Jump Crypto** is building a standalone validator client on Solana, built from the ground up in C/C++ and designed to work with commodity hardware. Its parent company Jump Trading has largely been constrained by the speed of light, and they recognize Solana is facing similar constraints for consensus on everything occurring on the Solana network. Given their belief in the network they see the need to add additional resiliency to the network by increasing throughput with a new standalone validator.

- **Brave** built wallet infrastructure that scales with the volume of their user base on Solana, allowing their 50m users to earn cryptocurrency rewards (Brave Attention Tokens, or BAT) by viewing ads.

- **Helio's Shopify x Solana Pay plugin** eliminates bank fees, chargebacks, and holding times while enabling immediate, direct payment settlement of USD stablecoins compatible with Solana, making it easy for Shopify merchants to get

real-time access to their money and greater ability to manage working capital, liquidity, and liability protection.

- **Pyth**, a high-frequency oracle built using Solana ecosystem technology, presents a compelling use case in data sharing for decentralized finance, offering products like real-time price feeds and benchmarks to be used by a host of financial service providers. Its ecosystem is a thriving community hub where users can leverage information contributed by vetted data providers, become providers themselves, or simply access desired statistics from the network.

0.1.4 Capabilities

How do these projects demonstrate the platform's capabilities in real-world applications?

Each of these projects demonstrate use cases that are only possible on Solana and do not — and cannot — exist on other blockchain networks. For example:

- **Visa**, in their explanation of why they chose to expand their stablecoin pilot to Solana, wrote, “[Solana] holds promise for payments due to its speed, scalability and low transaction costs, helping to make it a good candidate for efficient blockchain settlement rails using stablecoins like USDC. The Solana blockchain network incorporates a number of key features and novel innovations that are worth unpacking for anyone interested in payment technologies.”

- **Helio’s Solana Pay x Shopify** plugin has been adopted by over 500 Shopify merchants, with cumulative volumes well over 7 figures.

- In their announcement, **Brave** wrote, “We chose Solana as the ideal network for the launch of on-chain Brave Rewards given its high transaction speed and low fees, which help reduce the costs associated with distributing BAT earnings to hundreds of thousands of users. For example, a single transaction on Solana costs on average $0.002 USD, while a single transaction on Ethereum, or on its most popular layer-2 scaling solution, Arbitrum, costs on average $1.00 and $0.10 respectively.”

- **Pyth's** Solana Permissioned Environment instance produces blocks every 400 milliseconds, allowing it to distribute real-time market data, including 292 feeds in cryptocurrencies, 68 in equities, 16 in foreign exchange, two in commodities, and eight in fixed income/rated, across more than 45 blockchains.

- **Helium's** IOT network now encompasses over 900k onboarded hotspots, of which 410k are actively providing coverage in 50k cities spread across 175 countries. Helium Mobile has since attracted over 80k subscribers across over 200 countries.

- **Firedancer from Jump Crypto** is now live on Solana testnet, and has shown to process 1.2m transactions per second in a test environment.

Technology

1.1 Protocol Technology

1. What consensus mechanism does your platform use, and why was this particular mechanism chosen?

Solana is a Proof of Stake blockchain network. The protocol uses Tower BFT (Byzantine Fault Tolerance) as its consensus algorithm. All validators participating in consensus are considered voting validators. On the Solana network, validators will take turns producing blocks on the network according to a predefined schedule known as the leader schedule. When an individual validator (voting validator) sees a block produced by another validator (the leader), then the voting validator will vote to include that block in the blockchain (assuming the block is valid).

A key innovation in the Solana protocol is the Proof of History algorithm, which uses a verifiable delay function that timestamps blocks with cryptographic proofs that symbolize the passage of time on the network. This allows the protocol to come to a consensus on the validity of blocks to include in the network without having to synchronize to wall clock time, allowing validators to validate much faster than peer L1s.

See the following documents for details on the implementations of Tower BFT, Proof of History, Optimistic Confirmations, and commitments.

2. How does your consensus mechanism impact scalability and security?

Solana's Proof of History consensus mechanism creates a verifiable record of time, allowing nodes to agree on the order of transactions without constant communication. This frees up resources and enables parallel processing, significantly boosting transaction speeds and throughput, with a current potential capacity of 65,000 TPS.

From a security perspective, Solana utilizes Proof of Stake, where validators with the most staked SOL tokens have a higher chance of being selected to create new blocks. This incentivizes validators to act honestly, as slashing penalties exist for malicious behavior.

It is important to note that any concerns around scalability or security are mitigated by the fact that Nasdaq will likely utilize a Solana Permissioned Environment, whereby you can create a secure environment that can achieve higher thresholds of throughput than the permissionless mainnet environment may be able to achieve.

3. What virtual machine(s) does your platform use? Please elaborate on its compatibility with token standards.

Solana uses the Solana Virtual Machine (SVM, formerly known as Sealevel) that compiles down to a generic LLVM. Learn more here.

The SVM is unique in that it is capable of parallelizing execution of non-overlapping transactions to dramatically increase the transaction throughput across Solana. In combination with Proof of History, Solana is effectively streaming portions of a block (called “entries”) across the entire fleet before requiring the notion of block consensus.

The SVM enables some fundamentally different constructs relative to EVM:

Mempool-less
The SVM does not use a mempool, allowing for the fast and reliable transmission of transactions on the network. Transactions are sent with a “recent blockhash” and have up to 150 blocks to get confirmed on the network (1 slot ~= 400ms; 150 blocks ~= 1 minute). This is an intentional design choice to make it simpler for the same address to send multiple transactions at once without the use of a nonce. Transactions are submitted directly to the leader and can be retried until the blockhash expires.

Transactions that are included in a block get voted on by the network. Optimistic confirmations (agreed upon by 66%+ of the network) can occur within 1 second, after which reorgs are economically infeasible. Finalization (100% of stake) occurs within about 10 seconds.

The use of expireable transactions (rather than nonces) makes it simpler for validators to check if a transaction was submitted more than once. This means that a user doesn’t have to worry that if a given transaction wasn’t included in a previous block that some bad actor could replay that same transaction later without such user’s knowledge.

In the context of DeFi, quick price movements could mean that a certain transaction can be profitable now, but incur great losses in the future. A mempool-less design protects against this. Read more about transaction confirmation on Solana.

Parallelizable transactions

The SVM is designed for maximum throughput. Programs on the Solana blockchain are stateless – all relevant read / write data are passed as parameters to the program, allowing for parallelized execution of transactions that are not writing to the same state.

In the context of Nasdaq, this means tens of thousands of transactions between individuals and merchants can be executed in parallel. Moreover, there are no “global gas fees,” just gas fees local to contentious state. For the purposes of this RFP there’s likely little-to-no requirement to consider non-deterministic transaction fees since many transactions would be parallelizable.

Account Abstraction

The account model designed into the SVM lends itself naturally to features typically understood as “account abstraction”: programmatic accounts that can facilitate transactions across a number of user-friendly products. These have been in place on Solana for years. These “smart contract wallets” can handle anything from daily transaction rate limits, increased signature requirements over certain thresholds, as well as signing via other mechanisms besides Ed25519 (Ethereum, passkeys, etc).

Solana Program Library

The SVM is preloaded with several programs that make up the Solana Program Library (SPL) which enable some of the most common use cases for the Solana blockchain, like tokens and state compression. These programs are open source and routinely audited by third-party security firms. Some programs, like Token Exchanges, can only be upgraded via validator software updates which require a majority stake change.

Two important programs in the SPL are the Token and Token-2022 programs. These two programs manage 100% of the tokens currently used on the Solana network, and are what constitutes the “SPL Token Standard”. Using just these two programs to handle everything related to tokens on Solana means that users can trust that transferring any specific SPL token is not able to include malicious code capable of stealing their funds. The SPL Token

Standard enables minting, burning, freezing, delegating tokens, and provides a concrete implementation.

From the developers standpoint, this makes composability more straightforward. With a single program interface (Token / Token-2022 share the same Application Binary Interface) that exposes the token mint, burn, and transfer functions, other smart contracts can "compose" with these Token programs safely. These programs do not require "preapproval" flows to allow the transfer of tokens, reducing the risk related to using DeFi smart contracts and ensuring that users cannot be exploited using stale approvals.

CLOBs

Central Limit Order Books (CLOBs) are the one of the most efficient financial primitives for price discovery, but require low latency and high transaction throughput in order for market participants to be able to update their orders as quickly as price changes on different markets. Solana's high throughput, low latency, and low transaction fees makes it the perfect environment to host such primitives that would previously be relegated to centralized servers. With the throughput enabled by parallelization, a new programming model using the SVM with native account abstraction and a composable token program makes Solana the perfect environment to innovate with novel DeFi primitives.

4. Detail the token standards supported by your platform. Include noted partnerships if applicable.

The first SPL (Solana Program Library) Token program is a concrete implementation of a token program designed to allow for the basic capabilities needed by most tokens: minting, burning, freezing, delegating, transferring.

Third-party ecosystem protocols like Metaplex can be composed with SPL Tokens to provide additional functionality like providing metadata and other access control paradigms.

Token extensions (enabled by Token-2022) is a new token program on the Solana blockchain that enables a set of modular extensions for token issuers that can add advanced functionality and frameworks to tokens. Token extensions are built into the core protocol level of Solana and apply to both fungible and non-fungible tokens. This program is a strict superset of the capabilities of the original SPL Token program.

There are more than a dozen audited token extensions currently live on mainnet. Token issuers – from game developers to stablecoin issuers – can choose to enable any combination of token extensions, gaining advanced capabilities that in some cases were previously not possible on public blockchains such as privacy support, compliance frameworks, and the ability to charge fees. Token extensions give native support for the enterprise features without any additional tooling, vendor lock-in, or requirement to convince other teams to support your token(s). They reduce the work needed from engineering teams by removing the complexity into developing, auditing, and deploying custom token contracts, allowing those resources to deploy elsewhere.

Current mint extensions include:

- **Confidential transfers**: Allow transfers between participating users without revealing the amount of the transfer. This is not “private” — source, destination, and token type are public. Only the transferred amount is encrypted, and an optional auditor account can be assigned to encrypt amounts if needed for compliance purposes. Both the sender and receiver must opt-in for a transfer to be confidential.

- **Transfer fees**: Allow transfer fees to be charged on each transfer and withheld for another authority to claim.

- **Interest-bearing tokens**: Allow setting a continuously compounding, global interest rate on a token.

- **Non-transferable tokens**: Restricts a token from being transferred.

- **Permanent delegate**: The permanent delegate has ownership privileges over any account for that token, which means that it can burn or transfer any amount of tokens. Some examples of this could be used include the ability to seize assets from a sanctioned entity or repossess a token with an unpaid balance.

- **Transfer hook**: Allows a program to be invoked upon every transfer, which can express functionality such as requiring KYC at source / destination, address include-/exclude-lists, daily rate limits, restrictions on trading hours, etc.

- **Metadata pointer**: Allows token creators to designate an address that describes the canonical (official) metadata for the token. This can even be the mint itself (see the Metadata extension below).

- **Metadata**: Allows metadata to be incorporated natively into tokens through custom fields.

Current account extensions include:

- **Required memo on transfer**: Requires an attached memo as a message during each token transfer. This could be used for regulatory compliance, reporting, and enhanced audit trails.

- **Immutable owner**: Makes it impossible to reassign ownership of an account.

- **Default account state**: Freezes all new token accounts so that users must interact with the project in some way to unfreeze the accounts/tokens.

- **CPI guard**: Restricts how other programs can interact with your token by prohibiting certain actions inside cross-program invocations.

- **Reallocate**: Some extensions can be enabled after account creation. Reallocate allows owners in this situation to reallocate their token account to create room for more extensions.

5. What is the primary programming language for developing on or with your platform?

Solana uses the LLVM compiler infrastructure and smart contracts (called “programs” in Solana parlance) may be written in any programming language that can target the LLVM's BPF backend. Most smart contracts on Solana are written natively in **Rust**, **C++** or **C**.

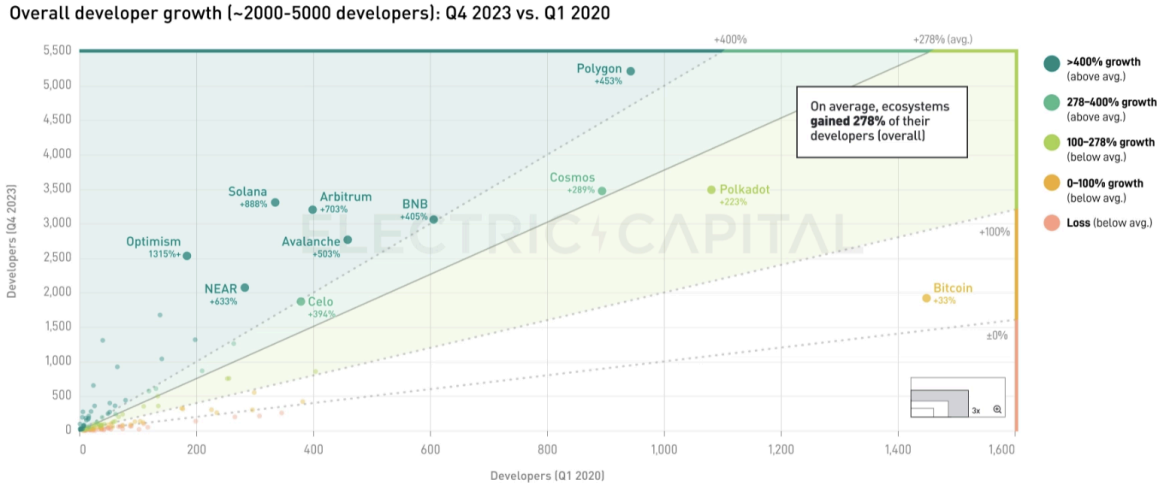
Anchor is a popular community-maintained framework for writing Solana smart contracts in Rust. Programs can also be written in **Python** using Seahorse, a community-led project built on top of Anchor. Learn more about SDKs available for Solana development.

Support for **Move** is in active development.

6. Describe the size and engagement level of your development community.

There are approximately 1,615[6] monthly active developers working on open source projects that build on top of Solana. The number of active developers in the ecosystem is likely much larger than 1,615, since that number does not capture developers that are working on closed source projects. Solana's growth rate in developers from Q1 2020 to Q4 2023 was 888%[7], among the highest growth rate of any chain (see chart below).

Solana Hackathons act as a barometer for Solana developer interest, and each successive hackathon has seen steady growth from the previous. For example, Solana Renaissance, which concluded in early April 2024, had over 8,000 participants build over 1,000 projects. This is more than the late 2023 hackathon, Solana Hyperdrive, which saw more than 7,000 participants build over 900 projects.



7. What solutions exist to improve throughput and/or latency? (i.e., As additional products launch)

[6] Source: https://www.developerreport.com/ecosystems/solana
[7] Source: https://www.developerreport.com/developer-report

The Solana network has processed over 270 billion transactions, and on a daily basis is processing over 25 million transactions[8] – more than all EVM chains combined.

For the open mainnet beta, the Solana benchmarking tool bench-tps is able to reach 20,000 transactions per second of atomic transactions that are composed of single transfers between independent parties, when run on the Solana testnet network with over 2,000 validators. A closed Solana Permissioned Environments (SPEs) can reach up to 65,000 TPS.

In practice, the highest transactions per second reached was over 8,000 TPS on mainnet, although this is well below capacity. Any reported TPS numbers on Solana are merely a reflection of demand, not a restriction of capacity. And with the implementation of the QUIC protocol and fee markets, Solana is able to maintain a high TPS even during times of heavy network load.

Looking to the future, Jump Crypto's independent Firedancer validator client has processed more than 1.2m TPS in test environments, and is currently available on testnet. It is anticipated to be available for mainnet beta soon.

It's important to look beyond TPS as a raw metric. With a targeted slot time of 400ms and supermajority finality within ~1.5 seconds, transactions on Solana are snappy and not subject to reorganization following confirmation by the network.

Additionally, the Solana protocol is designed to process transactions in parallel, greatly enhancing throughput and efficiency of the chain. All transactions with disjoint addresses can be executed in parallel, perfect for Nasdaq where transactions occur primarily between two distinct parties rather than a single party paying out to a large number of people. Other chains cannot make that distinction.

8. What architecture or implementation decisions can negatively impact throughput and/or latency?

[8] Source: https://app.artemis.xyz/project/solana

It's important to note that Nasdaq's implementation of Solana in a Solana Permissioned Environment will not be subject to the same risks that could impact throughput or latency as on Solana mainnet beta. As referenced above, in a controlled environment, SVM based infrastructure using the Agave client can do on the order of 65,000 TPS, and Firedancer has the potential to reach up to 1m TPS.

When considering the impact of the infrastructure, one needs to consider what are the target applications and how closed should a system be. For a Nasdaq SPE, one can consider the geo-proximity of the several nodes, this means that block times can be further reduced compared to mainnet. Depending on hardware configurations further optimizations could be made on compute per block and number of banking threads to allow more parallel processing. All of these optimizations that can't trivially be done on mainnet would have a tremendous impact on trading applications reducing latencies and increasing throughput that could match centralized trading exchanges.

No matter how much one optimizes the infrastructure of a system, it's still going to be bottlenecked at the application level if its design completely disregards the underlying infrastructure design. For this matter, Solana programs require some level of attention to make sure they take full advantage of the parallelization provided by the runtime, such as reducing the scope of the hotspots and making sure written resources aren't used globally on a program. When dealing with extreme hot spots (e.g. CLOBs) the frameworks and languages used to write the programs must be carefully considered, these abstractions usually lead to higher overhead which means that programs written in vanilla rust will be able to process more transactions for the same compute compared to programs that use Anchor.

Today, CLOBs are still evolving on Solana. OpenBook was a novel DEX for a blockchain that was enabled by Solana's speed, low costs and fast block times. More recently Phoenix innovated further by creating a new crankless design that further improves the performance of a CLOB in a blockchain.

9. What solutions exist to prevent transaction fees from being prohibitive to scaling or expanding the coverage of logic that occurs on-chain.

At 0.000005 SOL per-signature and at the recent SOL price of approximately $173, a penny can fund 10 transactions on Solana mainnet beta (The Solana Foundation recommends Nasdaq implement a Solana Permissioned Environment, where fees can be toggled to near zero or obfuscated entirely).

Median transaction fee for payment transfers will remain 0.000005 SOL. Solana isn't near capacity today, and there are proposed changes that will make some of the non-payment transactions more expensive, like increasing cost of compute, while making most transactions cheaper.

State compression is a Merkle tree-based storage structure on Solana that allows the use of individual transactions as storage containers for data. While state compression has been utilized mostly to reduce the cost of minting NFTs on Solana by over 24,000x, it can be generalized for other uses.

For example, the primitive can be generalized to allow the publication of a Merkle root that is produced off-chain and stored on-chain, and as long as provided off-chain data can be verifiably proven against the Merkle root, it can be expanded / utilized as on-chain data. For example, rather than requiring the issuance of 500k transactions to issue payouts, one could pre-compute the final state (500k "claimable" payouts) and provide the data / proofs to clients to be able to make lazy claims against that computed state.

a. E.g. Can blockchain instances be "gasless" or otherwise use a valueless token, is there a method for account abstraction, etc.?

Yes, gasless transactions can be executed both with a stablecoin as well as funded by a third-party signing service. In both cases, the "fee payer" property is the first signature on a transaction and can cover fees related to the transaction, including signatures and rent. The transaction is created as usual on the client and submitted to the signing service, which sets the fee payer and signs the transaction. The signing service is not required to be the one to send the transaction. These are not "meta transactions" or "wrapped transactions" — fee paying is a first-party property of the Solana transaction model.

When translating transaction fees to stablecoins, onchain swaps can be baked into the transaction where the central signing service continues to fund the part of the network fee

covered in the SOL token. See Octane, a reference implementation of a transaction relayer maintained by Anza, as an example of stablecoins being used to pay for transactions.

10. Do you work with any technology vendors for additional functionalities? If so, please list them and describe how their feature set interacts with or compliments your own.

The Solana Foundation has strong relationships with Amazon Web Services. AWS has tested and benchmarked Solana validators running on AWS in both RPC and voting validators configurations. AWS can also seamlessly support a Solana Permissioned Environment.

1.2 Interoperability

1. Does your platform have native interoperability functionality? If so, please describe the mechanism.

Multiple bridges support cross-chain transfers to the Solana network:

- Wormhole
- Allbridge
- DeBridge
- Mayan Finance
- Circle's Cross Chain Transfer Protocol
- *Coming soon: Support from LayerZero and Axelar*

Solana does not employ any concept of sharding, subnets, or supernets. The monolithic global state of Solana mainnet is accessible to all parts of the network, and transfers are simply transactions that finalize within a single block (~400ms). All addresses on the network can be credited, but must provide a signature from a private key or be a program to issue debits.

It is important to note, however, that a Solana Permissioned Environment would need to use a bridge protocol in order to interface with Solana mainnet.

2. What are the prerequisites for a chain to be compatible with your interoperability features?

There are multiple ways for smart contracts deployed on other chains to use Solana features. The use of a bridge can help sync deployments over multiple chains (see above).

While the Solana network uses SVM, not EVM, there are a number of ways for EVM projects to connect with Solana. See this detailed guide from the Solana Foundation.

Neon EVM is an Ethereum Virtual Machine (EVM) empowering developers to build and deploy dApps seamlessly from EVM chains to Solana, all from their existing codebase. Neon allows developers to deploy Solidity code directly to Solana using the Neon Virtual Machine makes interoperability easy and simple.

The Hyperledger Solang compiler can be used to easily transition Solidity code to the SVM.

Wormhole and other bridges automatically translate most assets on Solana (e.g. fungible tokens and NFTs) to their ERC equivalents. Any ERC 721 that is translated over to Solana will be interoperable as an NFT to the rest of the NFT ecosystem like marketplaces, NFT lending, etc.

The use of cloning can support interoperability with Solana mainnet beta and other SVMs.

- Any SVM can clone code to any other SVM chain directly from the bytecode. This means there it isn't necessary to copy/paste any code, change code or get it audited.
- The same cloning will work for messaging programs like LayerZero (coming soon) and zk bridges (in development).
- Other compatible technologies that can create permissioned bridge standards. For example, Squads is a formally verified program on mainnet beta that can be cloned.

3. How is cross-chain communication incentivized, and what measures are in place to prevent censorship by infrastructure providers?

All of the cross-chain communication bridging protocols have some subset of node operators who manage the process of facilitating cross-chain asset transfers or message passing. Similar to other infrastructure you may be familiar with, each of these protocols utilize a native token (such as $W for Wormhole) to incentivize the Node Guardians who process and validate these transfers.

The node operators are financially and reputationally incentivized to act in good faith and process transactions accordingly. If they do not, they risk being removed from the system by the independent node parties helping operate the bridge. For instance, if a Guardian or group of Guardians was seen censoring transactions, it would be visibly apparent to the other node operators. In order for colluding nodes to achieve a goal of censorship, they would need to corrupt 66% of the Guardians, which is nearly as hard as corrupting the Bitcoin, Ethereum and Solana blockchains themselves.

4. Are cross-chain payloads encrypted, or can infrastructure operators view message contents?

There are multiple fully private transaction providers on Solana, including Elusiv and Light Protocol that use different combinations of zk proofs and have their own operational characteristics.

The token extension confidential transfers can be utilized to obfuscate transferred amounts.

All data on the chain is publicly readable by any participant, although there is no restriction on that data being encrypted.

1.3 Compliance and Token Management

1. Describe the compliance features available on your platform, including token recovery and seizure mechanisms.

Token extensions can be used to support compliance and privacy features. Some examples of how they can be utilized include:

- **Native confidential payments with auditing**: Using confidential transfers, account balances and transfers of tokens can be masked using zero knowledge proofs, so that third parties cannot see the amounts onchain while issuing audit rights, in case of a regulator subpoena.

- **Freeze and seize:** Using the freeze authority and delegate authority extension, tokens can be configured to freeze the balance of a token account and seize the asset, in case of law enforcement action or token recovery.

- **Permissioned gatekeeping:** Using delegate authority, tokens can be configured to add a program dependency on transfers, which acts as a gatekeeper on whether a sender or receiver can do such actions, in case of sanctions.

2. How does your platform ensure regulatory compliance, particularly in the context of asset tokenization?

Interaction with a public, permissionless blockchain carries an inherent expectation that all activity will be made public. However, there are applications and smart contracts that can be tailored with a view towards compliance with data privacy and data protection laws.

For example, token extensions enable confidential transactions protecting users from sharing account balances and transfer amounts while also allowing the issuer of the token to have audit rights and freeze / seize capabilities if required by regulatory action (See above).

Given that the Nasdaq deployment would be on a Solana Permissioned Environment, the implementation will be under the full control of Nasdaq and any other parties elected to run

validator nodes on the network. By doing so, Nasdaq would maintain full control, and therefore discretion on compliance, over the entire userbase interacting with the network.

3. Is there support for address-based allowlisting? If so, describe the mechanism. Describe the scope and granularity of address-level allowlisting (e.g., ability to transact generally or with specific tokens, ability to deploy smart contracts, etc.)?

The transfer hook token extension and transfer hook Interface introduce the ability to create Mint Accounts that execute custom instruction logic on every token transfer. This unlocks many new use cases for token transfers, including black or white list wallets that can receive tokens.

Importantly, allowlisting comes native with a Solana Permissioned Environment. Nasdaq and any individuals operating nodes on the network have full discretion over the users of the platform.

Address-based allowlisting can occur on multiple levels:

- On both mainnet beta and in an SPE:
    - Tokens can be configured with a transfer hook that constrains transfers to either an allowlist or excludelist (or even more complex logic like constrained transfers over a certain limit).
    - Smart contract wallets can be used to constrain the ability to transfer funds to certain addresses, requiring multiple levels of authorization for certain actions.

- Only in an SPE:
    - Modifications can be made to a strict allowlist to:
        - Deploy programs
        - Operate a node on the network

4. Detail the transaction privacy features your platform offers and how they are implemented.

The confidential transfer token extension provides confidential (but not anonymous) payments, taking advantage of zero-knowledge proofs called “bulletproofs” to obscure

token types and amounts. The token extension program allows the issuer of the token to have audit rights on the confidential payments in the case of regulatory requirements.

Mints may be configured for confidential transfers, so that token amounts are encrypted, but the account owners are still public. Exchanges may configure token accounts to send and receive confidential transfers to hide user amounts.

There are multiple fully private transaction providers on Solana, including Elusiv and Light Protocol, that use different combinations of zk proofs and have their own operational characteristics.

All data on the chain is publicly readable by any participant, although there is no restriction on that data being encrypted.

5. Is there support for selective transparency to comply with regulatory requirements?

Token extensions support confidential transfers between participating users without revealing the amount of the transfer. This is not “private” — source, destination, and token type are public. Only the transferred amount is encrypted, and an optional auditor account can be assigned to encrypt amounts if needed for compliance purposes. Both the sender and receiver must opt-in to receive confidential transfers.

6. Is there support for identity verification or are other KYC methodologies employed? (e.g., non-transferable identity tokens)?

The non -transferable token extension makes it possible to create tokens that cannot be transferred. This enables the creation of "soul-bound" tokens, where digital assets are intrinsically linked to an individual. While these tokens cannot be transferred, the owner can still burn tokens and close the Token Account. This prevents users from being "stuck" with an unwanted asset.

Civic, Gateway, Albus Protocol and Blockpass also offer third party KYC solutions, some of which are open source and could be easily forked and copied over to the Nasdaq SPE environment.

An example implementation is Solrise Dex Pro, an onchain decentralized exchange on Solana with permissioned access based on digital identity. Solrise DEX Pro uses Civic to determine which participants meet their rigorous standards for verification prior to allowing them the ability to trade.

1.4 Security

1. What security protocols and measures are in place to protect against common blockchain vulnerabilities and threats?

Solana uses the popular dalek cryptography rust crates for the implementations of the standardized Ed25519 signature scheme, encryption, and (bulletproofs) zero-knowledge proof system. These crates are actively monitored for security related issues. The parts of the code where we rely on these crates are also audited by multiple auditing firms. The audit reports are publicly available.

Regarding post-quantum cryptography (PQC), the NIST PQC standardization process is actively monitored, as well as new developments in academic research (eprint, IACR conferences, etc.) relating to the topic. While core engineers are not currently in a rush to move to PQC, there is likely sufficient engineering capability and expertise in the ecosystem to make the shift when the industry as a whole starts to move towards PQC.

For the Solana blockchain itself, there are no major cryptographic assumptions other than the security of SHA256 and Ed25519 signatures. Ed25519 is a standardized digital signature scheme that relies on the hardness of discrete log over Curve25519 (Edwards representation) in the random-oracle model.

There can be additional assumptions at the application level. In particular, the confidential transfer token extension uses authenticated encryption, ElGamal encryption and Bulletproofs over Curve25519 (Ristretto representation). Each of these components require the following assumptions:

- **Authenticated encryption (AES-GCM-SIV)** relies on the security of AES128.

- **ElGamal encryption** relies on the hardness of the Decision Diffie-Hellman (DDH) assumption over Curve25519.

- **Bulletproofs** relies on the hardness of discrete log over Curve25519 and the security is proved in the random-oracle model (Sha3 is used for the hash function).

No trusted setup or knowledge assumptions (generally required for SNARKs) are required for the confidential transfer extension to SPL tokens.

2. How does the platform handle smart contract audits, and what best practices are recommended for developers to ensure security?

Changes to the protocol are audited on every minor release. While the protocol itself has no way of detecting a security breach, like all permissionless and public blockchains, the Solana network maintains a full history of all activity on the chain. In addition, core engineers across multiple companies regularly monitor network activity and performance. Any transactions done onchain can be reviewed at any time.

3. Have any third-party security audits or penetration testing exercises been conducted?

There are several security companies that have audited Solana programs, including:

- Trail of Bits
- Neodyme
- Zellic
- Halborn
- OtterSec
- Sec3

An additional list of audits can be found at solana-labs/security-audits.

4. What data security and handling standards or policies do you follow? (e.g., the handling of PII).

The Solana blockchain itself is open and permissionless. Solana Foundation is a non-profit organization and does not own or operate the Solana blockchain, nor does it collect any PII through the Solana blockchain. The only PII collected by the Solana Foundation is for marketing purposes through websites it manages, which feature its own privacy policies.

1.5 Additional Questions

1. Discuss any planned upgrades or roadmap features that could affect the answers to the above questions.

Jump Crypto's independent Firedancer validator client is live on testnet and expected to be available on mainnet beta soon. With potential hardware acceleration as well as high performance C code, the Firedancer project has shown promising demos processing 1.2m TPS. Watch a demo.

A recent testnet release by Anza is designed to improve Stake-weighted QoS reliability in v1.17 of the Agave validator client.

The best way to keep up to date about major changes to the protocol include:

- **Solana Improvement Documentation (SIMD)** for defining the next major changes to the core protocol.
- **The sRFC system** for non-protocol changes that are standard based enhancements (similar to Ethereum ERC).
- **The @Solana X account**, maintained by the Solana Foundation, for other general news and updates.

2. How does the platform support migration or transition from other platforms if a project decides to switch?

There are several ways to migrate onto Solana. By design, the Solana runtime uses an LLVM compiler, so any language (including Solidity) that compiles down to LLVM can be used.

See the Solana Foundation's complete EVM to SVM guide.

For EVM teams looking to expand or move with minimal work, third party providers such as Neon can provide EVM-compatibility layers on Solana by creating a translation tool that maps EVM constructs to SVM primitives, using the Neon RPC network to allow Ethereum-compatible wallets to communicate to the Neon network. This should enable simple re-deployment of code already running on EVM chains.

For EVM teams that wish to rewrite code to take advantage of the full Solana UX, Hyperledger Solang can be used to write in Solidity.

A notable example of a large-scale migration to Solana is Helium, which migrated their original, proprietary L1 network to Solana. Read more about it here.

3. Have you applied for or obtained any state or sovereign regulator license approval?

In 2023, the New York Department of Financial Services (NYDFS) approved the issuance of USDP, ZUSD, and GYEN, US-dollar and Japanese Yen based stablecoins on the Solana blockchain. This made Solana one of two non-Ethereum blockchains to be approved by NYDFS for stablecoin issuance in New York state.

In 2024, the Abu Dhabi Global Market (ADGM) and the Solana Foundation signed a Memorandum of Understanding (MOU). The MOU marks the start of a joint exploration of initiatives and projects related to the development of the blockchain ecosystem in Abu Dhabi.

Business Partnership

1. Can you detail the level of development, support, and capital resources your organization is willing to commit to our project? Please specify the types of resources available (e.g., developers, infrastructure).

The Solana Foundation views this opportunity as a major priority for adoption of the Solana network. As such, we are willing to make an investment of **over $45MM** to ensure the

success of this project. We have proposed below a set of allocations for this investment, but are open to discussing specifics in greater detail:

- **$30MM investment in assets deployed on the Regulated DA Ecosystem**

- **$6MM USD for announcement / launch tied to milestones:**
  - **Milestone 1 (33%): Announcement.** Upfront payment for a joint announcement that Solana is the exclusive chain for Nasdaq's Regulated DA Ecosystem at or prior to Solana's Breakpoint conference Sept. 19-21, 2024. (The announcement must be exclusive to Solana, with no other chains referenced.)
  - **Milestone 2 (33%): SPE Launch.** Nasdaq's Regulated DA Ecosystem is live on a Solana Permissioned Environment and available for use. The milestone is considered complete upon the first successful third party SPE transaction on or prior to April 22, 2025.
  - **Milestone 3 (33%): Mainnet Launch.** Nasdaq's Regulated DA Ecosystem is live on Solana mainnet and available for use. The milestone is considered complete upon first successful third party mainnet transaction on or prior to April 22, 2026.

- **$4MM USD tied to adoption / transaction volume on Solana:**
  - **Milestone 1 (50%):** $50 billion of monthly trading volume based on trailing 3 month period on the Regulated DA Ecosystem on a Solana Permissioned Environment on or prior to April 22, 2026.
  - **Milestone 2 (50%):** $50 billion of monthly trading volume based on trailing 3 month period on the Regulated DA Ecosystem on Solana mainnet on or prior to April 22, 2027.

- **$4MM for a dedicated Nasdaq pod:**
  - The Solana Foundation will staff a dedicated Nasdaq pod with support from ecosystem partner organizations:
    - 4+ engineers (two backend, two frontend) to build with Nasdaq team, and support the team ongoing for the term of the agreement
    - 1 dedicated product manager to support the development of the Regulated DA Ecosystem
    - 0.5 designer
    - 0.5 project manager lead

- **$1MM for a Solana Permissioned Environment cluster**
  - 4 machine cluster
  - Leased bare metal hardware

2. Are you open to co-developing features or custom solutions that are specific to our needs? If so, how do you manage and prioritize feature requests, bug fixes, and updates for clients' projects?

The Solana Foundation is open to co-developing custom features and solutions that are tailored to Nasdaq's specific needs. When it comes to managing and prioritizing feature requests, bug fixes, and updates, we follow a structured and transparent process:

Feature Requests and Custom Solutions:

- Solana Foundation conducts a detailed discovery workshop to thoroughly understand your business objectives, pain points, and desired outcomes.
- The product management and engineering teams then collaboratively assess the feasibility, effort, and impact of each feature request.
- Solana Foundation prioritizes features based on factors such as business value, technical complexity, and alignment with Nasdaq's roadmap.
- Throughout the development process, Foundation maintains frequent communication and iterative feedback loops to ensure the solutions meet Nasdaq's expectations.
- The flexible engagement model allows Foundation to allocate dedicated resources and adjust timelines as needed to deliver custom features on schedule.

Bug Fixes and Platform Updates:

- Dedicated Nasdaq pod will actively monitor the platform's performance and stability, proactively identifying and addressing any issues.

- Pod will define an incident response and triage process to ensure critical bugs are resolved quickly, with clear communication to your team.
- For non-critical bugs and maintenance updates, engineers will consolidate them into regular release cycles, keeping you informed of the changes and their impact.
- Engineering practices will include comprehensive testing, version control, and deployment automation to ensure the quality and reliability of platform updates.
- Solana Foundation will provide detailed release notes and offer optional pre-production testing environments to allow the Nasdaq team to validate updates before deployment.

Importantly, the Solana Foundation will maintain a collaborative backlog and roadmap management process that involves Nasdaq stakeholders. This ensures alignment on priorities, transparency into the development pipeline, and the ability to adapt to changing business needs.

3. What ongoing support and maintenance services do you offer post-deployment?

We are committed to providing comprehensive ongoing support and maintenance services to ensure the smooth and reliable operation of your platform. A dedicated pod of 5+, including 4 engineers (2 backend, 2 frontend), product manager, and fractional design and project management resources, will be available 24/7 for triage and incident management using a tool like PagerDuty.

The pod will respond to critical issues within 1 hour, and resolve them within 4 hours. For non-critical issues, they will respond within 4 hours and resolve them within the next business day. Our escalation procedures ensure that senior engineers and subject matter experts are involved as needed to address complex problems.

In addition to reactive support, the team will proactively monitor the platform's health, perform regular software updates and patches, and optimize performance based on usage patterns. The Solana Foundation will collaborate closely with your internal teams to ensure

seamless operations and provide knowledge transfer to build your self-sufficiency over time.

While the Solana Foundation cannot provide a contractual SLA for any underlying network concerns that require independent validator node operators to take certain actions (e.g., upgrading their software) as these entities operate fully independently, we can provide an SLA-like commitment for communications related to anything related to the operation of the network.

4. Do you provide training to ensure client teams can effectively manage the platform?

The Solana Foundation places great importance on empowering teams with comprehensive training to effectively manage and operate Solana Permissioned Environments. We can offer a variety of training formats, including in-person workshops, virtual instructor-led sessions, and self-paced online courses.

The training curriculum can be tailored to address Nasdaq's specific needs, covering topics such as protocol development and administration, user management, monitoring and alerting, troubleshooting, and advanced customization. Upon completing the training program, your team members will have the opportunity to earn certification, demonstrating their proficiency and expertise. We also provide ongoing access to our extensive documentation, video tutorials, and online community forums to support continuous learning and skill development.

5. What types of documentation, tutorials, and learning resources are available?

There is a robust suite of documentation and learning resources for Solana developers, which can be found here. This includes detailed technical documentation, API references, architectural diagrams, and step-by-step implementation guides, all organized in a user-friendly online portal for easy navigation.

Documentation covers a wide range of topics, from platform overview and key features to advanced configuration and troubleshooting. Additionally, we provide interactive

multimedia resources, such as video tutorials, code samples, and webinars, to complement the written material and cater to different learning preferences.

Furthermore, the dedicated Nasdaq team will be available to answer questions, provide guidance, and assist with any issues that may arise. They can be reached through various communication channels, including email, live chat, and a self-service knowledge base.

6. What is your typical engagement model for project collaboration? (e.g., dedicated team, fixed-price project?)

The Solana Foundation's engagement model is centered around a dedicated team of experts[9] that will work seamlessly alongside your internal stakeholders. This multidisciplinary team includes a project manager to oversee the collaboration, software engineers with deep blockchain expertise, a user experience designer, and a product manager to align the solution with your business objectives.

We leverage agile methodologies to ensure transparency, efficient communication, and timely delivery of milestones. Our project management approach includes regular status updates, collaborative planning sessions, and flexible adjustment of team composition, timelines, and scope as needed to address evolving requirements.

While our default engagement model is a dedicated team, we are open to alternative approaches to best suit your preferences and project dynamics. Regardless of the engagement type, our goal is to provide a tailored solution that exceeds your expectations and achieves the desired outcome.

[9] Solana Labs and/or Anza may contribute team members to the project. Solana Labs builds products, tools and reference implementations that can be used on the Solana blockchain. Solana Labs also helps startups building on Solana through its Incubator program, and via investing in companies through its venture arm, Solana Ventures. Anza is the leading Solana dev shop. Anza was founded by the original core and dev tooling teams from Solana Labs, and leverages their deep expertise to help Solana projects level-up and launch first in class protocols. They are the creators and maintainers of Agave, a forked version of the original Solana Labs client validator client. They also develop tooling for dApp developers on Solana, and contribute to the next generation of apps and protocols in the ecosystem.

7. How flexible are you in adjusting the engagement model based on the project's evolving needs?

Recognizing the fluid nature of project requirements, the Solana Foundation maintains a highly flexible engagement model. We are able to swiftly adapt to evolving project needs, whether it involves scaling resources, adjusting timelines, or revising pricing structures. Our goal is to provide solutions that exceed expectations, delivering exceptional value, and driving tangible results for Nasdaq. Our commitment to agility and responsiveness ensures that we will remain aligned with Nasdaq’s objectives throughout the project lifecycle.