CONFIDENTIAL PRIVATE PLACEMENT MEMORANDUM

QURANIUM ASSOCIATION
A SWISS NON-PROFIT ASSOCIATION

Up to $500,250
(Rule 506(c) of Regulation D)

Up to 7,500,000 of QRN Tokens

The date of this Memorandum is September 10, 2025.

TABLE OF CONTENTS

SECURITIES DISCLOSURES

THE SECURITIES OFFERED HEREBY HAVE NOT BEEN APPROVED OR DISAPPROVED BY THE SECURITIES AND EXCHANGE COMMISSION (THE "**SEC**"), ANY STATE SECURITIES COMMISSION OR ANY OTHER REGULATORY AUTHORITY, NOR HAVE ANY OF THE FOREGOING PASSED UPON OR ENDORSED THE MERITS OF THE OFFERING OR THE ACCURACY OR ADEQUACY OF THIS CONFIDENTIAL PRIVATE PLACEMENT MEMORANDUM (THE "**MEMORANDUM**").

THE SECURITIES HAVE NOT BEEN AND WILL NOT BE REGISTERED UNDER THE SECURITIES ACT OF 1933, AS AMENDED (THE "**SECURITIES ACT**"), OR ANY OTHER LAW OR REGULATION GOVERNING THE OFFERING, SALE OR EXCHANGE OF SECURITIES IN THE UNITED STATES OR ANY OTHER JURISDICTION. THE SECURITIES OFFERED HEREBY MAY NOT BE SOLD, TRANSFERRED OR OTHERWISE DISPOSED OF BY AN INVESTOR UNLESS THEY ARE REGISTERED UNDER THE SECURITIES ACT AND WHERE REQUIRED, UNDER THE LAWS OF OTHER JURISDICTIONS, UNLESS SUCH PROPOSED SALE, TRANSFER OR DISPOSITION IS EXEMPT FROM SUCH REGISTRATION.

A PURCHASE OF THE SECURITIES INVOLVES A HIGH DEGREE OF RISK, INCLUDING THE RISK OF A TOTAL LOSS OF PRINCIPAL, VOLATILITY AND ILLIQUIDITY. A PROSPECTIVE PURCHASER SHOULD THOROUGHLY REVIEW THE CONFIDENTIAL INFORMATION CONTAINED HEREIN AND THE TERMS OF THE APPLICABLE OFFERING DOCUMENTS, AND CAREFULLY CONSIDER WHETHER A PURCHASE OF THE SECURITIES IS SUITABLE TO SUCH PROSPECTIVE PURCHASER'S FINANCIAL CONDITION AND GOALS. SEE "RISK FACTORS" BELOW.

SECURITIES RISK FACTORS AND SUITABILITY DISCLOSURES

INVESTORS SHALL BE REQUIRED TO REPRESENT THAT THEY ARE FAMILIAR WITH AND UNDERSTAND THE TERMS, RISKS AND MERITS OF THE OFFERING DESCRIBED IN THIS MEMORANDUM AND ALL THE ATTACHMENTS HERETO. THE SECURITIES IS BEING OFFERED IN A PRIVATE OFFERING TO A LIMITED NUMBER OF INDIVIDUALS OR ENTITIES MEETING CERTAIN SUITABILITY STANDARDS. THIS OFFERING INVOLVES A HIGH DEGREE OF RISK AND PROSPECTIVE INVESTORS SHOULD BE AWARE THAT THEY MAY SUSTAIN A LOSS OF THEIR ENTIRE INVESTMENT.

PURCHASES WILL BE ACCEPTED ONLY FROM "ACCREDITED INVESTORS," AS DEFINED IN RULE 501 OF REGULATION D (SEE "**INVESTOR SUITABILITY STANDARDS**"). THE SECURITIES OFFERED HEREBY ARE SPECULATIVE AND INVOLVE A HIGH DEGREE OF RISK. NO INVESTMENT IN THE SECURITIES SHOULD BE MADE BY ANY PERSON WHO IS NOT IN A POSITION TO LOSE THE ENTIRE AMOUNT OF SUCH INVESTMENT. IN MAKING ANY INVESTMENT DECISION, INVESTORS MUST RELY ON THEIR EXAMINATION OF US AND THE TERMS OF THIS OFFERING, INCLUDING THE MERITS AND RISKS INVOLVED.

EXCLUSIVE NATURE OF THE PRIVATE PLACEMENT MEMORANDUM

NO ENTITY HAS BEEN AUTHORIZED TO GIVE ANY INFORMATION OR TO MAKE ANY REPRESENTATIONS OTHER THAN THOSE CONTAINED IN THIS MEMORANDUM. ANY INFORMATION OR REPRESENTATION NOT CONTAINED HEREIN MUST NOT BE RELIED

UPON AS HAVING BEEN AUTHORIZED BY THE COMPANY. MOREOVER, NEITHER THE DELIVERY OF THIS MEMORANDUM NOR THE SALE OF THE SECURITIES SHALL UNDER ANY CIRCUMSTANCES CREATE ANY IMPLICATION THAT THERE HAS BEEN NO CHANGE

THE COMPANY DISCLAIMS ANY AND ALL LIABILITIES FOR REPRESENTATIONS OR WARRANTIES EXPRESSED OR IMPLIED, CONTAINED IN, OR OMISSIONS FROM, THIS MEMORANDUM, OR ANY OTHER WRITTEN OR ORAL COMMUNICATION TRANSMITTED OR MADE AVAILABLE TO THE RECIPIENT. EACH INVESTOR SHALL BE ENTITLED TO RELY SOLELY ON THOSE REPRESENTATIONS AND WARRANTIES WHICH MAY BE MADE TO THE INVESTOR IN ANY FINAL PURCHASE OR TOKEN PURCHASE AGREEMENT RELATING TO THE SECURITIES. THE DELIVERY OF THIS MEMORANDUM DOES NOT CONSTITUTE AN OFFER IN ANY JURISDICTION TO ANY PERSON TO WHOM SUCH OFFER WOULD BE UNLAWFUL IN SUCH JURISDICTION.

THIS MEMORANDUM DOES NOT PURPORT TO BE ALL-INCLUSIVE OR TO CONTAIN ALL OF THE INFORMATION THAT A PROSPECTIVE INVESTOR MAY DESIRE IN EVALUATING AN INVESTMENT IN THIS OFFERING OR THE SECURITIES OFFERED HEREIN. INVESTORS MUST CONDUCT AND RELY ON THEIR OWN EVALUATIONS OF THE COMPANY AND THE TERMS OF THE OFFERING, INCLUDING THE MERITS AND RISKS INVOLVED IN MAKING AN INVESTMENT DECISION WITH RESPECT TO THE SECURITIES. THE RISK FACTORS SHOULD BE CONSIDERED IN CONNECTION WITH THE PURCHASE OF THE SECURITIES. NEITHER THE DELIVERY OF THIS MEMORANDUM AT ANY TIME, NOR ANY SALE OF THE SECURITIES HEREUNDER, SHALL UNDER ANY CIRCUMSTANCES CREATE AN IMPLICATION THAT THE INFORMATION CONTAINED IN THIS MEMORANDUM IS CORRECT AS OF ANY TIME SUBSEQUENT TO ITS DATE.

JURISDICTIONAL (NASAA) LEGENDS

FOR RESIDENTS OF ALL U.S. STATES: THE PRESENCE OF A LEGEND FOR ANY GIVEN STATE REFLECTS ONLY THAT A LEGEND MAY BE REQUIRED BY THAT STATE AND SHOULD NOT BE CONSTRUED TO MEAN AN OFFER OR SALE MAY BE MADE IN A PARTICULAR STATE. IF YOU ARE UNCERTAIN AS TO WHETHER OR NOT OFFERS OR SALES MAY BE LAWFULLY MADE IN ANY GIVEN STATE, YOU ARE HEREBY ADVISED TO CONTACT THE COMPANY. THE SECURITIES DESCRIBED IN THIS MEMORANDUM HAVE NOT BEEN REGISTERED UNDER ANY STATE SECURITIES LAWS (COMMONLY CALLED "**BLUE SKY**" LAWS). THESE SECURITIES MUST BE ACQUIRED FOR INVESTMENT PURPOSES ONLY AND MAY NOT BE SOLD OR TRANSFERRED IN THE ABSENCE OF AN EFFECTIVE REGISTRATION OF SUCH SECURITIES UNDER SUCH LAWS, OR AN OPINION OF COUNSEL ACCEPTABLE TO THE COMPANY THAT SUCH REGISTRATION IS NOT REQUIRED.

THE PRESENCE OF A LEGEND FOR ANY GIVEN STATE REFLECTS ONLY THAT A LEGEND MAY BE REQUIRED BY THE STATE AND SHOULD NOT BE CONSTRUED TO MEAN AN OFFER OF SALE MAY BE MADE IN ANY PARTICULAR STATE. THE DISCLOSURES SET FORTH ON **SCHEDULE A** ARE SUBJECT TO REVISION OR MODIFICATION, AND THE INVESTOR IS ADVISED TO SEEK INDEPENDENT LEGAL ADVICE IN THEIR JURISDICTION.

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

THIS MEMORANDUM CONTAINS ESTIMATES AND FORWARD-LOOKING STATEMENTS. ALL STATEMENTS OTHER THAN STATEMENTS OF HISTORICAL FACT ARE FORWARD-LOOKING STATEMENTS. THE WORDS "MAY," "MIGHT," "WILL," "COULD," "WOULD," "SHOULD,"

“EXPECT,” “PLAN,” “ANTICIPATE,” “INTEND,” “SEEK,” “BELIEVE,” “ESTIMATE,” “PREDICT,” “POTENTIAL,” “CONTINUE,” “CONTEMPLATE,” “POSSIBLE,” AND SIMILAR WORDS ARE INTENDED TO IDENTIFY ESTIMATES AND FORWARD-LOOKING STATEMENTS. SUCH FORWARD-LOOKING STATEMENTS, INCLUDING THE INTENDED ACTIONS AND PERFORMANCE OBJECTIVES OF THE COMPANY AND THE SECURITIES ARE BASED LARGELY ON CURRENT EXPECTATIONS AND PROJECTIONS ABOUT FUTURE EVENTS AND TRENDS.

THESE FORWARD-LOOKING STATEMENTS ARE SUBJECT TO A NUMBER OF KNOWN AND UNKNOWN RISKS, UNCERTAINTIES, ASSUMPTIONS, AND OTHER IMPORTANT FACTORS, INCLUDING THOSE DESCRIBED UNDER “**RISK FACTORS**”, THAT COULD CAUSE THE ACTUAL RESULTS, PERFORMANCE, OR ACHIEVEMENTS OF THE COMPANY OR THE SECURITY TO DIFFER MATERIALLY FROM ANY FUTURE RESULTS, PERFORMANCE, OR ACHIEVEMENTS EXPRESSED OR IMPLIED BY SUCH FORWARD-LOOKING STATEMENTS. ALTHOUGH WE BELIEVE THAT THE EXPECTATIONS REFLECTED IN OUR FORWARD-LOOKING STATEMENTS ARE BASED ON REASONABLE ASSUMPTIONS, ACTUAL OUTCOMES COULD DIFFER MATERIALLY FROM THOSE SET FORTH OR ANTICIPATED IN OUR FORWARD-LOOKING STATEMENTS. FACTORS THAT COULD CAUSE OUR FORWARD-LOOKING STATEMENTS TO DIFFER FROM ACTUAL OUTCOMES INCLUDE, BUT ARE NOT LIMITED TO THOSE DESCRIBED UNDER THE SECTION ENTITLED “**RISK FACTORS**”.

SAFE HARBOR STATEMENT UNDER THE PRIVATE SECURITIES LITIGATION REFORM ACT

WITH THE EXCEPTION OF THE HISTORICAL INFORMATION CONTAINED IN THIS MEMORANDUM, THE MATTERS DESCRIBED HEREIN CONTAIN FORWARD-LOOKING STATEMENTS THAT INVOLVE RISK AND UNCERTAINTIES THAT INDIVIDUALLY OR MUTUALLY IMPACT THE MATTERS HEREIN DESCRIBED INCLUDING, BUT NOT LIMITED TO, FINANCIAL PROJECTIONS, PRODUCT DEMAND AND MARKET ACCEPTANCE, THE EFFECT OF ECONOMIC CONDITIONS, THE IMPACT OF COMPETITIVE PRODUCTS AND PRICING, GOVERNMENTAL REGULATIONS, TECHNOLOGICAL DIFFICULTIES AND/OR OTHER FACTORS OUTSIDE THE CONTROL OF THE COMPANY.

CERTAIN SERVICE PROVIDERS

NONE OF OPENDEALBROKER LLC DBA OPENDEALBROKER OR THE CAPITAL R (“**ODB**”) (NOR HAVE ANY OF THEIR AFFILIATES) INVESTIGATED THE DESIRABILITY OR ADVISABILITY OF AN INVESTMENT IN THIS OFFERING OR THE INTERESTS OFFERED HEREIN. NONE OF ODB OR ITS AFFILIATES MAKE ANY REPRESENTATIONS, WARRANTIES, ENDORSEMENTS, OR JUDGEMENT ON THE MERITS OF THE OFFERING OR THE SECURITIES OFFERED HEREIN. THE CONNECTION OF ODB AND/OR ITS AFFILIATES TO THE OFFERING IS SOLELY FOR THE LIMITED PURPOSES OF ACTING AS A SERVICE PROVIDER. AN INVESTOR SHOULD HAVE KNOWLEDGE AND UNDERSTANDING OF SOPHISTICATED AND COMPLEX INVESTMENTS TO MAKE A SELF-DETERMINATION OR SEEK ADVICE ELSEWHERE. ODB MAY INVITE OTHER BROKER/DEALERS TO PARTICIPATE IN THIS OFFERING UNDER SIMILAR TERMS AND CONDITIONS.

ZERO HASH LLC, THE PAYMENT PROCESSOR FOR THIS OFFERING, AND ITS SUCCESSOR OR ASSIGN, HAS NOT INVESTIGATED THE DESIRABILITY OR ADVISABILITY OF

PARTICIPATION IN THIS OFFERING OR THE INTERESTS OFFERED HEREIN. ZERO HASH MAKES NO REPRESENTATIONS, WARRANTIES, ENDORSEMENTS, OR JUDGMENTS ON THE MERITS OF THE OFFERING OR THE INTERESTS OFFERED HEREIN. ZERO HASH'S CONNECTION TO THE OFFERING IS SOLELY FOR THE LIMITED PURPOSE OF ACTING AS A SERVICE PROVIDER AND DOES NOT CONSTITUTE INVESTMENT ADVICE. ZERO HASH SHALL NOT BE LIABLE FOR ANY LOSSES OR DAMAGES ARISING FROM PARTICIPATION IN THIS OFFERING.

* * *

SUMMARY OF THE OFFERING AND THE PURCHASE AND CLOSING PROCESS

Quranium Association, a Swiss non-profit association (the "**Company**", "**we**" or "**us**") is offering (the "**Offering**") under Section 4(a)(2) and Rule 506(c) of Regulation D promulgated under the Securities Act up to $500,250 ("**Maximum Offering Amount**") of the Company's QRN Tokens ("**Tokens**") to qualified investors as set forth in the "**Terms of the Offering**," below.

The Token is the native unit of value built upon our and for intended use on the Quranium Chain, which is our layer-1 blockchain protocol (the "**Network**" or "**Protocol**") designed as a secure, decentralized platform for smart contracts and decentralized applications (dApps) (together with the Network, the "**Platform**"), at a $0.0667 per Token (the "**Offering Price**"). The date the Tokens are initially broadly publicly released by the Company for use on the Platform, if ever, shall constitute the "**Token Integration Event**" or "**TIE**".

Best Efforts Basis. This Offering is being conducted on a "best efforts" basis through a platform found at https://republic.com, which is operated for the benefit of OpenDealBroker LLC d/b/a OpenDealBroker or the Capital R ("**ODB**"). ODB is a registered FINRA/SEC broker dealer. ODB is not purchasing the securities, except as otherwise set forth herein, and is not required to sell any specific number or dollar amount of securities in this Offering. Since there is no minimum offering amount of the Tokens required to be sold in this Offering, all funds received from purchases under the Offering will immediately become assets of the Company, and available for use by the Company, upon acceptance of the purchases by the Company. The Company may increase or decrease the amount of the Maximum Offering in its sole discretion. The Company may reject purchases in whole or in part, in its discretion. If the Company accepts purchases for the Maximum Offering, the Company expects the proceeds therefrom to equal as follows:

	Offering Price	Commissions[1]	Fees[2]	Proceeds to Company
Minimum Offering Amount	**$ 100,000**	**$ 12,000**	**$ 7,500**	**$ 80,500**
Maximum Offering Amount	**$ 500,250**	**$ 24,015**	**$ 7,500**	**$ 468,735**

(1) The cash fee paid to ODB from the proceeds of this Offering will be the greater of: (A) $12,000 or (B) zero percent (0%) of the total dollar value of the Tokens sold in the Offering up to but not in excess of $100,000.00 and six percent (6%) of the total dollar value of the Tokens sold in the Offering greater than $100,000.00. *See* "**Certain Relationships and Related-Party Transactions**".
(2) Legal fees

Purchase Process.

Each investor must complete such documentation as may be requested through the offering platform at https://republic.com/quranium (the "**Republic Platform**") on behalf of the Company, which may include, without limitation:

1. the execution and delivery of the token purchase agreement (the "**TPA**" and together with any other documents, agreements and instruments, the "**Offering Documents**"), which shall identify the investor's purchase amount (the "**Purchase Amount**");

2. completion of investor qualification requirements (such as accreditation status verification, if applicable);

3. completion of Know-Your-Customer/Anti-Money Laundering ("**KYC/AML**") and/or Know-Your-Business ("**KYB**") screening requirements; and

4. confirmation by ODB of clearance from its regulation best interests requirements and of receipt of funds by the financial institution providing cryptocurrency payment services for the Offering, which presently is Zero Hash LLC (the "**Payment Servicer**" and the foregoing requirements, collectively, (collectively, the "**Closing Requirements**").

The Company shall have the sole discretion to accept or reject any investor purchase and determine whether or not Closing Requirements have been satisfied.

Closing Process; Purchase Payment.

Upon acceptance by the Company of any purchase from qualified investors, the Company shall have the right at any time and prior to the Offering Deadline (as defined below), to effect periodic closings (each a "**Closing**") for purchases in this Offering from investors until the earlier of (i) the date upon which purchases for the Maximum Offering offered hereunder have been accepted, (ii) the Offering Deadline, or (iii) the date upon which the Company elects to terminate the Offering.

Subject to satisfaction of the Closing Requirements, an investor shall make payments in USD Coin ($USDC) or Tether ($USDT) via any $USDC or $USDT supported network during the Offering Period (as defined in "**Terms of the Offering**," below).

The Company may elect to accept other forms of payment on an as-converted to USD basis in its sole discretion and subject to acceptance by the Payment Servicer. The Company will not accept payment by any fiat currency, including, for the avoidance of any doubt, United States dollars, whether by wire, automated-clearing house or otherwise. The Company reserves the right to discontinue accepting any type of consideration in its sole discretion.

The USD exchange rate for USDC or USDT other forms of payment shall be determined solely by the Company or its assignee or agent in accordance with reasonable and accepted market practices. Such currencies are subject to fluctuations in the rate of exchange and, in the case of digital assets, the exchange valuations. Such fluctuations may have an adverse effect on the value, price or returns of a purchase. Purchasers may receive a number of Tokens rounded down to two (2) decimal places.

Delivery of Tokens only upon Token Integration Event.

The Company plans to deliver Tokens on or after the date of the Token Integration Event, as such date may be extended or modified by the Company in its sole discretion (the "**TIE Date**"), as identified in the **Terms of the Offering**, below.

If there is no Token Integration Event on or before the TIE Date, the Company shall repay investors an amount equal to the purchase amount set forth in the investor's TPA (the "**Returned Purchase Amount**"), as soon as reasonably practicable after the TIE Date, to the extent funds are available for such lawful repayment at that time. If there is insufficient capital to refund the investors' Returned Purchased Amount on the TIE Date, the Company will repay Purchasers with equal priority and on a pro-rata basis among the investors based on the relative value of their respective Purchase Amount on the date of receipt by the Company of such Purchase Amount. *See* "**Use of Proceeds**" below for further discussion of the Company's use of any capital raised in the Offering.

* * *

TERMS OF THE OFFERING

The summary below describes the principal terms of the offering. Certain of the terms and conditions described below are subject to important limitations and exceptions. Prospective investors should review the entirety of the document to be entered into in connection with the Offering. The summary below is qualified in its entirety by reference to the actual text of the form of the applicable Offering Document.

Company:	Quranium Association
Tokens:	QRN Token
Expected Date of Token Integration Event:	Such date as determined by the Company, which may be extended or modified by the Company in its sole discretion
Offering Size:	The expected number of Tokens to be sold in this Offering is 7,500,000. Such amount may be modified by the Company in its sole discretion. The total amount of Tokens allocated for public sale is 63,000,000, all of which may be offered and sold by the Company in its sole discretion through the Republic Sale and through other platforms, including digital asset exchanges.
Offering Price:	$0.0667 per Token
Offering Period:	September 10, 2025, at 9:00 am prevailing Eastern Time ("**ET**") through September 21, 2025, at 4 pm ET, subject to the Company's discretion to extend the Offering (the "**Offering Period**"). Purchasers who are on the Company's "allowlist" or presales are eligible to participate in this Offering starting on September 10, 2025, at 9:00 am ET. The Company reserves the right to reject any payments not made within the Offering Period. The Offering Period may be extended or shortened in the Company's sole discretion posting a supplement to the Memorandum on the Offering Website.
Purchase Amounts:	Minimum purchase amount is $50. Maximum purchase amount is $500,250. Such amounts may be modified by the Company in its sole discretion.
Form of Purchase Agreement:	Token Purchase Agreement (the "**TPA**")
Manner of Payment of Purchase Amount:	The Purchase Amount can be paid in USD Coin ($USDC) or USD Tether ($USDT). The US dollar exchange rate for any cryptocurrencies used for the Purchase Amount shall be determined as set forth in the TPA.

	Purchasers must access the Republic Platform at https://republic.com/quranium and be subject to the Offering Documents. Purchases in USDC through Payment Servicer will incur a total fee equal to the greater of $2,500 (minimum fee) or 0.1% of the total payment volume. The above fees for Payment Servicer will ultimately be borne by the Company. The fee is added to the total amount of the investment at checkout. Purchasers in the offering will not have the right to revoke their purchase at any time. If a purchase is rejected for any reason, it will be refunded without interest or deduction save any applicable fees. Purchasers will follow instructions for completing payment when making their purchase via the Republic Platform that is operated by ODB for the benefit of the Offering. Cryptocurrencies and digital assets received in connection with purchases pursuant to this Offering are directed to an account maintained by the Company. If a purchase is rejected for any reason, including if ODB is unable to verify the KYC of the Purchaser, and if payment was made in the specifically approved cryptocurrency or digital asset, a refund of the purchase price will be made in USDC, and such refunds will be based upon the USD-denominated value of the Purchase Amount only, regardless of the type and amount of the approved cryptocurrency or digital assets paid, or any volatility in their prices, and subject to certain fees (i.e. the amount of cryptocurrency originally sent may vary from the amount of cryptocurrency refunded due to exchange rate variations). Gas fees or miner fees for refunds, which are paid to validators on a blockchain network, will be deducted from the amount of the refund sent. Purchasers in the Offering will not have the right to revoke their purchase at any time. Gas costs and miner fees paid in the original purchase will not be refunded. For all accepted purchases, the Company will bear the cost of any gas costs and/or other fees to deliver the tokens to the Purchaser. The Company will not accept payment by any fiat currency, including, for the avoidance of any doubt, United States dollars, whether by wire, automated-clearing house or otherwise.
Investor Suitability:	Each Purchaser must be an "Accredited Investor," as defined in Rule 501 of Regulation D under the Securities Act and such accreditation must be verified in accordance with the verification standards set forth in Rule 506(c) of Regulation D, *see also* "**Investor Verification Standards,**" below.
Offering Documents and Requirements:	In order to complete the closing process in this Offering, each Purchaser will be required to complete such documentation as may be requested by ODB on behalf of the Company, which may include, without limitation:

	1. the execution and delivery of the TPA and any other Offering Documents, which shall identify the investor's Purchase Amount; 2. completion of investor qualification requirements (such as accreditation status verification, if applicable); 3. completion of KYC/AML and KYB screening requirements; and 4. confirmation by ODB of clearance from its regulation best interests requirements and of receipt of funds by Payment Servicer.
Token Delivery:	After the closing of the Offering, and subject to the satisfactory completion of KYC/AML or KYB screening requirements applicable to the Offering and the collection of Payment Amounts, and if there is a Token Integration Event on or before the TIE Date, Tokens will be delivered to a compatible wallet address designated by each Purchaser in the TPA as follows: • 10% at Token Integration Event, followed by linear monthly vesting over 10 months. ERC-20 compatible wallets are the only wallets compatible with and able to receive the Tokens.
Lockup / Market Standoff:	The Purchaser will not offer, sell, pledge, or otherwise assign or transfer any rights under the TPA or the Tokens, unless, where applicable in compliance with securities laws, including Rule 144 of the Securities Act.
Restrictions on Transfer:	No transfer or resale except as permitted under the Securities Act and applicable state securities laws, pursuant to registration or exemption therefrom. Appropriate legends will be implemented.
Dissolution Event:	Any of the following events shall be deemed to be a "**Dissolution Event**": (i) a voluntary termination of the operations of the Company, (ii) a general assignment of all or substantially all the Company's assets for the benefit of the Company's creditors, or (iii) any other liquidation, dissolution or winding up of the Company, whether voluntary or involuntary. Upon the occurrence of a Dissolution Event prior to the TIE Date, the Company shall pay, after the payment of all other creditors, the Returned Purchase Amount due and payable to the Purchaser immediately prior to, or concurrent with, the occurrence of the Dissolution Event, to the extent funds are lawfully available and prior to paying any amounts to any equity holders of the Company. If immediately prior to the occurrence of the Dissolution Event, the assets of the Company that remain lawfully available for payment to the Purchaser and all holders of all other TPAs (collectively, the "**TPA Parties**"), as determined in good faith by the governing body of the Company , are insufficient to permit the payment to the TPA Parties of their respective Returned Purchase Amounts, then the remaining assets of the Company lawfully available for payment shall be paid with equal priority and pro rata among the TPA Parties based on the relative value (in

	the Purchase Price currency of the Tokens as set out herein) of each TPA Party's respective Purchase Amount on the date of receipt by the Company of such Purchase Amount and calculated by reference, as applicable, to the applicable exchange rate as at such date (and the claims of the Purchaser against the Company shall abate accordingly and any further claims of the Purchaser on the Company shall be extinguished). The Company will make commercially reasonable efforts but shall not be required to pay the Returned Purchase Amount to the Purchaser in the original currency of the Purchase Amount.
No Registration Rights:	The Company will not be required to register any securities under this Offering. Resales will be subject to, among other things, Rule 144 under the Securities Act.
Broker/Dealer:	This Offering is being conducted on the platform found at https://republic.com, which is operated for the benefit of ODB, which is a registered FINRA/SEC broker dealer.
ODB Fees:	*See* "**Certain Relationships and Related-Party Transactions**," below.
Governing Law:	Switzerland
Use of Proceeds:	*See* "**Use of Proceeds**," below

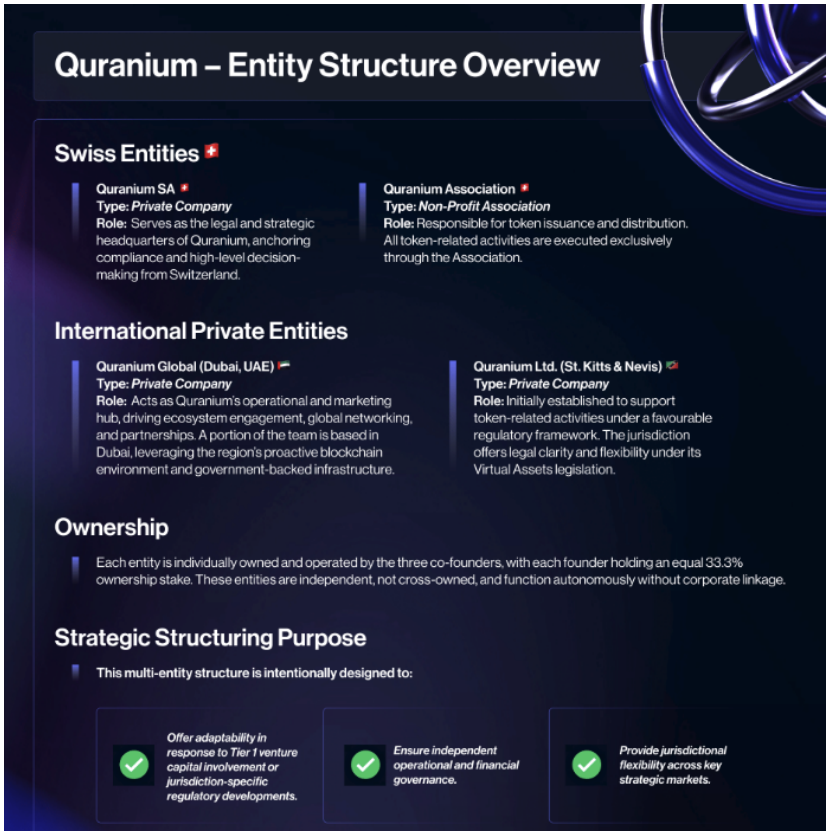
* * *

COMPANY OVERVIEW

*This overview highlights selected information that is presented in greater detail elsewhere in this Memorandum. This overview does not contain all of the information you should consider before participating in the Offering contemplated by this Memorandum. You should carefully read this Memorandum in its entirety before purchasing any Tokens, including the "**Risk Factors**". Some of the statements in this Memorandum constitute forward-looking statements, see the section titled "**Special Note Regarding Forward-Looking Statements**." Unless otherwise indicated herein, all references to the number of Tokens set forth in this Memorandum refers to the number of Tokens that will be created in the minting processes.*

BACKGROUND AND OVERVIEW

Quranium - Entity Structure



The Company is a Swiss Association with no share capital, is the fund-raising and token-issuing entity. Committee members of The Company are Kapil Dhiman (President and Signing Authority), Zeeshan Khan, Yaduvendra Singh and Bernard Jahrmann.

There is one operating company, Quranium SA, a Swiss company, with 45 full-time employees. The founders are also directors of Quranium SA. Bernard Jahrmann also serves as director of Quranium SA. All operational activities take place under the Quranium SA.

As of July 2025, the Company is in the final phase of mainnet preparation and protocol activation.

- Testnet of POS layer 1 is live

- Official mainnet launch of Quranium Layer 1 scheduled in September 2025.
- Deployment of the final version of the Qsafe Wallet, incorporating staking functionality for Quranium and other supported assets - September 2025.
- Finalization and launch of QDEX following the mainnet activation - September 2025.
- Activation of the NFT module, enabling minting, transfers, and seamless integration with Qsafe - July 2025.

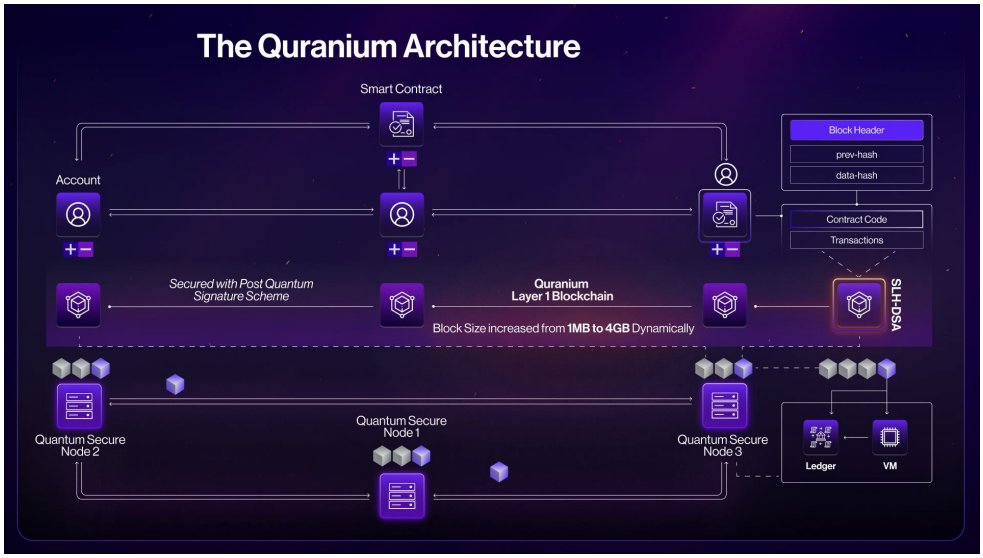
The Company's PQC choices are guided by ongoing developments from the NIST post-quantum cryptography standardization process, ensuring compatibility with emerging global standards. Additionally, the protocol is being developed with formal security modeling to address quantum adversaries, and external reviews by security firms and academic partners (e.g., CertiK) are part of the validation process.

The Company has established partnerships with companies such as PwC, Quantum Basel, ANKR, Polytrade, Galxe, Matter ID, Circle of Games, Happy Bridge, Turf, Metasig, Luma World, AssureDeFi, ExeQuantum, and ICP.

Quranium SA has raised approximately $6.15 million to date across several structured token financing rounds, with no debt or loans.

- Quranium Fundraising Overview
    - **Pre-Seed:** $300K (filled & closed)
    - **Seed:** $3M at $50M FDV (filled & closed)
    - **Strategic:** $3M at $75M FDV ($2.25M remaining) - Will be closed before the public pre-sale
    - **Private:** $6M at $100M FDV ($3.9M remaining) - Will be closed before the public pre-sale
    - **Public Pre-Sale:** $4.2M at $140M FDV
    - **Exchange IEO:** $1.5M at $150M FDV
- Notable institutional investors include Animoca Brands and Hyperscaled Ventures.
- Retail participation has been strong, with contributions from over 2,500 individual investors across South Korea and the UAE.
- Quranium SA also completed a node sale of 2500 nodes at 0.07 Eth/Node. 3 month-cliff with 10-month vesting.
- **Vesting & Alignment:** All contributors follow a unified vesting structure: 0% unlocked at TIE 3-6 month cliff Linear vesting over 18 months depending on the round

Overview



Quranium Chain is a layer-1 blockchain protocol designed as a secure, decentralized platform for smart contracts and decentralized applications (dApps). Built upon Proof of Stake as foundational principles, Quranium introduces a quantum-resistant cryptographic framework with the Stateless Hash-based Digital Signature Algorithm (SLH-DSA). This document provides a comprehensive overview of Quranium's architecture, components, cryptographic mechanisms, consensus protocol, and operational details.

Quranium Chain is a public PoS, permissionless blockchain enabling developers to deploy smart contracts and build dApps with high security and scalability. By implementing SLH-DSA, a quantum-resistant signature scheme, Quranium addresses potential vulnerabilities from quantum computing while preserving Ethereum's robust ecosystem. The native cryptocurrency, QRN Coin, facilitates transactions, gas fees, and staking within the network.

- Provide a quantum-resistant layer-1 blockchain: Quranium mitigates vulnerabilities posed by future quantum computers, ensuring long-term cryptographic robustness. The SLH-DSA algorithm is designed to provide efficient key generation, signing, and verification, all while being resistant to both classical and quantum attacks. This makes Quranium future-proof as global industries transition to quantum-aware infra.

- Maintain compatibility with Ethereum's smart contract and dApp ecosystem: Quranium retains full compatibility with Ethereum’s EVM, allowing developers to port existing smart contracts, decentralized applications (dApps), and tools with minimal or no code changes. All Solidity-based applications, standards (e.g., ERC-20, ERC-721, 4337, 6551, 7702 and all other ERCs, EIPs), and developer workflows (e.g., Hardhat, Truffle, Remix) work seamlessly. The only adjustment lies in the cryptographic signing method, handled internally by Quranium-compatible wallets and libraries. Quranium will also have QIPs to maintain the top standard upgradability.

- Ensure decentralization, security, and scalability: Decentralization is maintained through an open, permissionless Proof-of-Stake consensus layer, ensuring staked participants can contribute to network validation without requiring permission or stake. Security is enhanced through SLH-DSA’s resistance to brute-force and quantum attacks. Scalability is approached through gas optimization, efficient SLH-DSA verification via precompiled contracts, and future extensibility into Layer 2 and rollup solutions. Quranium’s layered architecture supports modular upgrades and robust peer-to-peer networking.

- Support a vibrant developer and user community with familiar tools and interfaces: Quranium will support a wide range of developer tools and interfaces from the Ethereum ecosystem, lowering the barrier to entry for onboarding developers. Wallets, Q-Remix IDEs, testing frameworks, and analytics dashboards can all be adapted to Quranium with simple SLH-DSA integrations. A community-driven governance model encourages contributions, ecosystem grants, hackathons, and documentation standards, fostering innovation and user adoption across global regions.

Component	Quranium (QRN)
Base Protocol	Quranium Layer 1 compatible to EVM
Currency	QRN
Crypto Signature	SLH-DSA
VM	QVM compatible to EVM Smart contracts
Consensus	Proof-of-Stake
Chain ID	4062024
Max Gas per Block	30,000,000

Core Components & Process

Blockchain Structure

Quranium operates as a proof-of-stake (PoS) blockchain. The blockchain consists of:

- Block Header: Metadata including previous block hash, timestamp, nonce, and Merkle root
- Transactions: Signed operations (e.g., QRN transfers, smart contract executions) using SLH-DSA
- State Trie: A Merkle Patricia Trie storing account states (balances, nonces, contract code)

Table 1: Quranium Block Structure

Field	Description
Previous Hash	SHA-256 hash of the previous block
Timestamp	Block creation time (Unix epoch)
Merkle Root	Root of the transaction Merkle tree
State Root	Root of the state trie
Transactions	List of SLH-DSA-signed transactions

Cryptographic Framework: SLH-DSA

Quranium implements SLH-DSA, a NIST-standardized, quantum-resistant signature scheme based on hash functions, providing robust security against both classical and quantum attacks.

Key Generation

- Private Key: A randomly generated seed (typically 256 bits for standard security levels) and secret seeds for various components (e.g., pseudo-random function, one-time signatures). These are used to derive all necessary values for the hash-based signature scheme.
- Public Key: Composed of the Merkle tree root and a seed for the public pseudo-random function. The Merkle tree root is derived from the private key components and represents the top of a carefully constructed hash tree.

Signature Generation and Verification

- Signing: To sign a message, a hash of the message is computed. A specific one-time signature (OTS) key pair is selected and used to sign the hashed message. The signature includes the OTS signature, the public key of the OTS, and an authentication path (Merkle path) that proves the OTS public key is a valid leaf within the Merkle tree whose root is part of the public key. Additionally, a randomized element is included to ensure security.
- Verification: The verifier recomputes the Merkle root using the provided OTS public key, the authentication path, and the public key components. This recomputed root is then compared with the public key's Merkle root. The verifier also checks the validity of the OTS signature on the message hash using the OTS public key. If all checks pass, the signature is deemed valid, ensuring message integrity and authenticity.

Quantum-Resistant Key Generation and Account Management

Quranium distinguishes itself as a forward-thinking, quantum-resistant distributed ledger, providing robust security against both classical and future quantum computing threats. This fundamental security is primarily achieved through its innovative approach to Externally Owned Account (EOA) key generation and signature mechanisms, which are built upon the Stateless Hash-based Digital Signature Algorithm (SLH-DSA), a NISTstandardized Post-Quantum Cryptography (PQC) primitive.

Account Creation and SLH-DSA Key Generation

Unlike traditional cryptographic schemes that face potential vulnerabilities from quantum algorithms, Quranium's EOAs are rooted in SLH-DSA, offering a fundamentally secure digital identity. The key generation process for a Quranium EOA involves:

1. **Seed Generation**: The foundation of an SLH-DSA key pair is a cryptographically strong, random 96-byte seed value. This seed acts as the initial entropy from which all subsequent key components are deterministically derived. The generation of this seed is performed using a high-quality, cryptographically secure pseudo-random number generator (CSPRNG), ensuring unpredictability and uniqueness for each account.
2. **Private Key Derivation**: From this 96-byte seed, the full 128-byte SLH-DSA private key is generated. This private key, while larger than those in pre-quantum schemes, encapsulates all the necessary secret information required to generate valid signatures, including internal seeds for one-time signature schemes and the current state counter for managing the signature tree.

3. **Public Key Derivation**: Concurrently, the 64-byte SLH-DSA public key is derived from the same initial seed and private key components. This public key consists of a pseudo-random function (PRF) seed and the root hash of a Merkle tree. This Merkle tree represents a vast collection of one-time signature (OTS) keys, which are consumed sequentially with each signature. The public key is the cryptographic anchor that verifiers will use to confirm the authenticity of signatures.

4. **Quranium Address Generation**: The unique 20-byte Quranium account address is then deterministically generated by taking the last 20 bytes of the Keccak-256 hash of the 64-byte SLH-DSA public key. This address serves as the public identifier for the account on the Quranium network, analogous to a street address for a physical location.

Key Storage and Security Paradigm

The SLH-DSA private key is the sole mechanism for controlling an EOA and authorizing transactions. Therefore, its secure storage is paramount to account security on Quranium.

1. **Encrypted Keystore Files**: To safeguard the sensitive 128-byte private key, it is never stored in an unencrypted format. Instead, it is immediately encrypted using robust symmetric encryption algorithms, typically AES-128-CTR, and saved into a keystore file. Access to this encrypted private key requires a user-defined, strong passphrase, which is used to derive the encryption key via a computationally intensive key derivation function (like Scrypt).4

2. **Decentralized User Control**: Private keys and their corresponding keystore files are stored locally by the user, not on the Quranium network itself. This architecture places full ownership and responsibility of key management directly with the user, embodying the principles of decentralization and self-sovereignty.

3. **Mnemonic Phrases for Recovery**: For enhanced usability and disaster recovery, most wallet implementations generating SLH-DSA keys will also provide a mnemonic phrase (a human-readable sequence of words). This phrase, derived from the initial 96-byte seed, allows for the deterministic regeneration of the entire SLH-DSA key pair, offering a crucial backup mechanism. Protecting this mnemonic phrase with utmost care is as critical as protecting the encrypted keystore file.

By integrating SLH-DSA from the ground up, Quranium provides a forward-looking and inherently quantum-resistant foundation for digital asset ownership and transaction authentication, positioning the network for long-term security in the evolving cryptographic landscape.

Table 2: SLH-DSA Parameters

Parameter:	Value
Security Level:	256-bit (post-quantum)
Signature Size:	49 KB (variable based on parameter set)
Public Key Size:	64 bytes
Private Key Size:	128 bytes (seed)

Hash Function:	SHA-256

Consensus Mechanism

Quranium employs a Proof-of-Stake (PoS) consensus mechanism, identical to Ethereum's Gasper protocol, combining Casper FFG and LMD-GHOST for finality and fork choice.

- Validators: Stake QRN and Q-Node Key to participate in block proposal and attestation
- Epochs: Time periods (6.4 minutes) for validator assignments and finality
- Rewards/Penalties: Validators earn QRN for honest behavior and face slashing for malicious actions

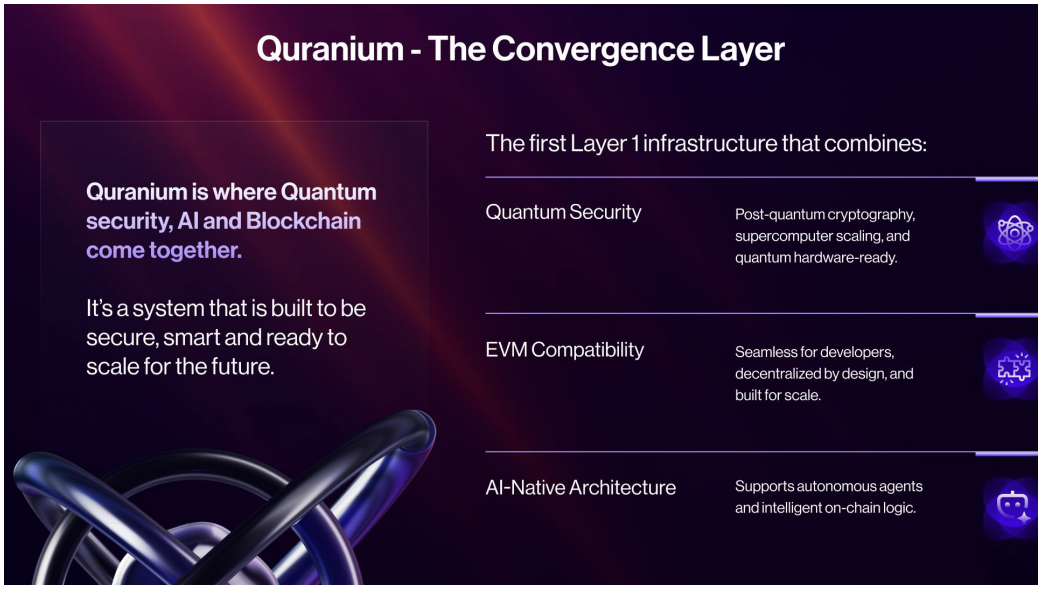
Virtual Machine

The Quranium Virtual Machine (QVM) mirrors the Ethereum Virtual Machine (EVM), executing smart contracts written in Solidity or Vyper with identical opcodes. This allows whole EVM developers to deploy contracts to Quranium Chain as well.

- Gas: Computational effort measurement, paid in QRN
- State Transitions: Contract execution updates the global state trie
- Compatibility: Supports existing Ethereum Development Experience

Layered Stack Explanation

- **Application Layer**: This layer comprises decentralized applications (dApps), wallets, and user interfaces. It’s where end-users interact with Quranium through various applications built on top of the protocol. It leverages standard Web3 interfaces and supports Solidity-based frontends.
- **Execution Layer**: The execution layer powers the EVM compatible Quranium virtual Machines, responsible for processing smart contracts, computing state transitions, and executing all on-chain logic. It ensures compatibility with Ethereum's existing dApp ecosystem to onboard community faster
- **Consensus Layer**: Quranium uses a Proof-of-Stake mechanism to achieve consensus. This layer ensures that all nodes agree on the blockchain state, provides Sybil resistance, and secures the network from manipulation and strictness of Penalties for running a chain
- **Networking Layer**: Built on DevP2P and optionally enhanced with Libp2p, this layer manages peer discovery, message propagation, and node communication across the decentralized network.
- **Cryptography Layer**: Quranium replaces traditional ECDSA with SLH-DSA, a stateless hash-based signature scheme designed to resist quantum attacks. This layer underpins address creation, transaction signing, and block validation with quantum-secure cryptography.



Contract Creation

In Quranium, contracts are deployed using the Quranium Virtual Machine (QVM) . Contract creation is a core operation that results in the generation of a new account with associated executable code. The process follows a deterministic mechanism, ensuring predictable and unique contract addresses.

Key Parameters

- Deployer Address: The account initiating the contract creation.
- Nonce: The deployer's transaction count (used for CREATE).
- Salt: A 32-byte value provided by the deployer (used for CREATE2).
- Initialization Code: The bytecode executed during contract deployment.
- Endowment: The amount of QRN sent to the contract during creation.

Contract Address Calculation

The contract address is derived from a deterministic function based on the creator's address and additional parameters:

For CREATE

- address =Keccak256(RLP(sender, nonce))[12:]

Where:

- **sender**: The account deploying the contract.
- **nonce**: The sender's transaction count.

For CREATE2

- address =Keccak256(0xff + sender + salt +Keccak256(init_code))[12:]

Where:

- **0xff:** A constant prefix to avoid collisions.
- **sender:** The account deploying the contract.
- **salt:** A 32-byte user-provided value.
- **init_code:** The initialization bytecode for the contract.

Rationale

- **CREATE** ensures sequential addresses per deployer based on nonce.
- **CREATE2** provides predictability, enabling off-chain precomputation of contract addresses before deployment. This facilitates advanced use cases such as counterfactual deployments.

Transaction Execution

Transaction execution in Quranium is the core process that transforms the blockchain's global state by applying a transaction. It ensures correctness, deterministic behavior, and verifiable effects across nodes, while enforcing signature validity, nonce ordering, balance sufficiency, and gas metering.

Overview

Each transaction is applied to the current world state to produce a new state:

$$\text{NewState} = \text{ExecuteTransaction}(\text{CurrentState}, \text{Transaction})$$

This process validates the transaction, deducts the appropriate gas and balance from the sender, performs the operation (such as a transfer or smart contract call), and finalizes the resulting state.

Signature Model

Quranium uses the SLH_DSA_SHAKE_256f signature scheme, replacing traditional elliptic curve signatures. Each transaction includes:

- A signature of 49856 bytes
- A public key of 64 bytes

These are combined into a single sig field of 49920 bytes.

Sender address is derived by hashing the public key using Keccak-256 and taking the last 20 bytes. This eliminates the need for (r, s) values and provides post-quantum security.

Transaction Fields

A transaction in Quranium includes:

- Nonce: Prevents replay; must match sender's account nonce
- To: Recipient address (or null for contract creation)
- Value: Amount of native token to send
- Data: Payload or contract init code
- gasLimit: Maximum gas the sender is willing to spend
- maxFeePerGas and maxPriorityFeePerGas: Fee configuration
- Sig: SLHDSA signature + public key

- V: Chain ID

Validity Checks

Before execution, the transaction must satisfy:

- Correct formatting and encoding
- Valid SLHDSA signature over the transaction payload
- Correct sender derivation
- Nonce matches sender's current state
- Gas limit is sufficient for intrinsic gas
- Sender's balance can cover fees and value transfer
- Fee caps conform to protocol rules

Intrinsic Gas Calculation

Each transaction has a **base gas cost** depending on:

- Payload size
- Number of zero/nonzero bytes in data
- Whether it creates a contract
- Size of init code (if any)
- Intrinsic gas is calculated before execution begins and must be less than or equal to the gas limit.

Upfront Cost and Fee Logic

Quranium supports both legacy and dynamic fee structures.

- **Effective gas price** is the minimum of maxFeePerGas and baseFee + maxPriorityFeePerGas
- **Upfront cost** = gasLimit × gasPrice + value

If the sender cannot cover this cost, the transaction is rejected before execution.

Execution Phases

1. **Initial State Changes**
    a. Deduct gasLimit × gasPrice from sender
    b. Increment sender's nonce
2. **Execution Context Setup**
    a. Compute availableGas = gasLimit − intrinsicGas
    b. Initialize temporary substate to track:Self-destructed contracts
    c. Logs
    d. Touched accounts
    e. Refunds
    f. Accessed accounts and storage keys

Core Operation

Based on the to field:

- If to is empty → contract creation
- If to is present → message call

The smart contract VM (or native execution logic) is invoked to process the transaction.

Post-execution Refund

Remaining gas is calculated

- A portion of unused gas is refunded (up to 20%)
- The rest is burned or distributed as miner/validator reward
- Refund is credited back to sender's balance

Final State Update

- Apply substate changes
- Delete accounts marked for self-destruction
- Remove empty touched accounts
- Commit logs for indexing and filtering

Receipt and Output

Execution produces:

- **Gas used**: total gas minus refund
- **Logs**: emitted during execution
- **Status**:1 for success, 0 for failure

These are used to create the transaction receipt and are committed to the state trie.

NETWORK OPERATIONS

Accounts and Transactions

Quranium supports two account types:

- Externally Owned Accounts EOAs): Controlled by SLHDSA private keys
- Contract Accounts: Controlled by code, activated by transactions like ERC 4337 smart accounts, ERC 6551 Smart Contract Wallets

Transactions include:

- Nonce: Transaction counter
- Gas Price/Limit: Fee parameters in QRN
- Recipient: Target address
- Value: QRN amount
- Data: Contract input data
- Signature: SLHDSA signature
- V Chain Id

Network Topology

Quranium operates as a peer-to-peer P2P decentralized network, closely following the architectural principles of Ethereum. The network is designed for high availability, censorship resistance, and efficient transaction propagation. It uses a Kademlia-based Distributed Hash Table DHT for node discovery and routing, enabling scalable communication across thousands of nodes.

Kademlia-Based Peer Discovery

Quranium nodes discover and communicate with peers using a Kademlia-like DHT protocol, which is also employed by Ethereum. Each node has a unique 256-bit Node ID, and the network organizes connections based on the XOR distance between node IDs.

- **Routing Table**: Nodes maintain k-buckets that store peer information by proximity, allowing for efficient lookup and routing.
- **Recursive Lookups**; Peers are discovered via iterative queries across the network, typically requiring only logarithmic steps (O(log n)) to find a peer.
- **Resilience**: The DHT structure offers robustness against churn (nodes joining/leaving), making the network fault-tolerant.

Node Types

Quranium supports multiple node types that cater to different use cases, storage capabilities, and hardware requirements.

1. **Full Nodes**
    a. **Definition**: Full nodes store the entire Quranium blockchain, including all transactions, receipts, and state transitions. They independently verify and validate every block and transaction.
    b. **Consensus Participation**: Full nodes validate according to Quranium's consensus rules (e.g., Proof-of-Stake, or in future upgrades, other consensus models).
    c. **Peer Services**:
        i. Broadcast new transactions and blocks
        ii. Respond to state and data requests from light clients
    d. **Storage**: Can prune old states but retain full block and receipt history
    e. **Example**: Similar to Ethereum Geth or Nethermind in full-node mode

2. **Light Nodes (Light Clients)**
    a. **Definition**: Light nodes only download block headers and rely on full nodes to provide the necessary Merkle proofs to validate transactions.
    b. **Protocol**: Use a Light Client Protocol to query full nodes on-demand.
    c. **Use Cases**: Faster sync and lower storage cost
    d. **Trust Model**: While more lightweight, they inherit a semi-trusted relationship with the full nodes they rely on

3. **Archive Nodes**
    a. **Definition**: Archive nodes retain the entire blockchain history, including every state at every block height—not just the latest state.
    b. **Functionality**:
        i. Allow querying of smart contract states at any historical block
        ii. Crucial for explorers, forensic tools, analytics, and indexing services
    c. **Storage Demand**: Extremely high, often reaching several terabytes depending on chain growth
    d. **Comparison**: Like Ethereum's archive mode in Geth (e.g., -gcmode=archive)

Node Interaction Model

- **Gossip Protocol**: Quranium uses a modified devp2p protocol for transaction and block propagation.
- **Transaction Pool**: All full nodes maintain a mempool of pending transactions which are broadcast across peers until mined. There is added UserOps Mempool for Account Abstraction transactions as well.
- **Header Chain**: Light clients sync and verify only block headers and request proofs when needed.

Node Synchronization Modes

Like Ethereum, Quranium nodes support various sync modes to optimize for user needs:

- **Full Sync**: Processes every block from genesis, reconstructs full state
- **Fast Sync** (default for many nodes): Downloads blocks and state trie up to a recent checkpoint, then validates state transitions
- **Snap Sync** (if implemented): Syncs recent state snapshots for faster bootstrapping
- **Light Sync**: Syncs only block headers; relies on full nodes for state and transaction data

Summary Table

Node Type	Stores Full Blocks	Stores State History	Validates Transactions	Peer Discovery	Storage Need
Full Node	✅	Latest State Only	✅	✅	Medium
Light Node	Headers Only	❌	SPV-style	✅	Low

Archive Node ✅	✅ Full State)	✅	✅	Very High

This layered node topology ensures that Quranium maintains decentralization, supports diverse participants (from mobile users to institutional indexers), and remains efficient even as the blockchain grows.

SECURITY CONSIDERATIONS

Quranium is designed with a strong emphasis on security, resilience, and future-proofing, especially against emerging threats such as quantum computing and economic manipulation.

The following security strategies form the core of Quranium's architecture:

Quantum Resistance

Quranium integrates **SLH-DSA (Stateless Hash-based Digital Signature Algorithm)** as its native digital signature scheme to achieve quantum resistance.

Why Quantum Resistance Matters:

Quantum computers threaten traditional cryptographic algorithms like ECDSA and RSA by potentially breaking them using Shor's algorithm. This would allow malicious actors to forge signatures, reverse private keys, and compromise wallets or entire networks.

Quranium's Approach:

- **SLH-DSA**, based on SPHINCS+, provides provable security grounded in hash-based cryptographic constructions.
- Unlike elliptic curve-based signatures (like Ethereum's secp256k1), SLH-DSA does not rely on number-theoretic assumptions and is considered safe against quantum adversaries.
- Quranium wallets, node software, and contracts are being adapted to support post-quantum-compatible transaction formats, preparing the network for a seamless transition.

This ensures Quranium is "quantum-hardened by default", future-proofing user accounts, smart contracts, and validators against next-gen threats.

Resistance to 51% Attacks

Quranium uses a **Proof-of-Stake (PoS)** consensus model, designed to resist majority (51%) attacks through economic disincentives and slashing mechanisms.

Mitigation Strategies:

- **Slashing Conditions**:
  - Validators who propose conflicting blocks or sign malicious attestations can be penalized or slashed, losing part or all of their staked assets.
  - This creates a strong economic deterrent against double-spending, reorgs, or censorship.
- **Sybil Resistance**:
  - The staking requirement makes it costly to spin up a large number of validator nodes, reducing the risk of Sybil attacks.
- **Finality Checkpoints**:
  - Quranium may include finality gadgets (similar to Ethereum's Casper FFG) that make certain finalized blocks irreversible unless an overwhelming portion of the stake misbehaves.
- **Decentralized Validator Set**:

- Staking is open and globally distributed, ensuring no single entity can easily acquire a controlling stake.

By aligning validator incentives with honest behavior and introducing automated punishment for malicious actions, Quranium maintains network integrity and liveness, even under adversarial conditions.

Smart Contract Security

Quranium is EVM-compatible with replacement of ecrecover to slhrecover, meaning it supports the Ethereum Virtual Machine and inherits a rich history of smart contract tooling, standards, and battle-tested infrastructure. However, it enhances security through stricter guidelines and optional advanced features.

Key Safeguards:

- **Audit Recommendations**:
  - Quranium strongly recommends (and may eventually require) third-party smart contract audits for all mainnet deployments.
  - The Quranium ecosystem will support integration with formal verification tools like Slither, MythX, and Certora.

- **Secure Language Standards**:
  - Quranium supports Solidity and Vyper, with best practice enforcement via contract linter tools.
  - Development kits will include predefined safe templates to prevent common vulnerabilities (reentrancy, overflows, etc.)

- **Permissioned Features**:
  - Quranium supports modular account abstraction and optional multi-sig controls for contracts handling large amounts of funds.

- **Runtime Protections**:
  - Static gas limits, opcode restrictions, and call-depth controls help prevent Denial-of-Service (DoS)attacks at the EVM level.

Quranium builds on Ethereum's hard-earned lessons in contract safety, with proactive auditing and developer tooling to foster a secure smart contract ecosystem.

Additional Protections

- **Network-Level Encryption**:
  - Quranium encourages TLS-like encryption for P2P traffic and gossiped data to reduce metadata leakage.
- **Replay Attack Protection**:
  - Transaction formats include chain ID protections, preventing cross-chain replay attacks.
- **DoS and Spam Resistance**:
  - Quranium includes fee markets, gas pricing, and rate limits to mitigate spam transactions and DoS vectors targeting validators or nodes.

Summary

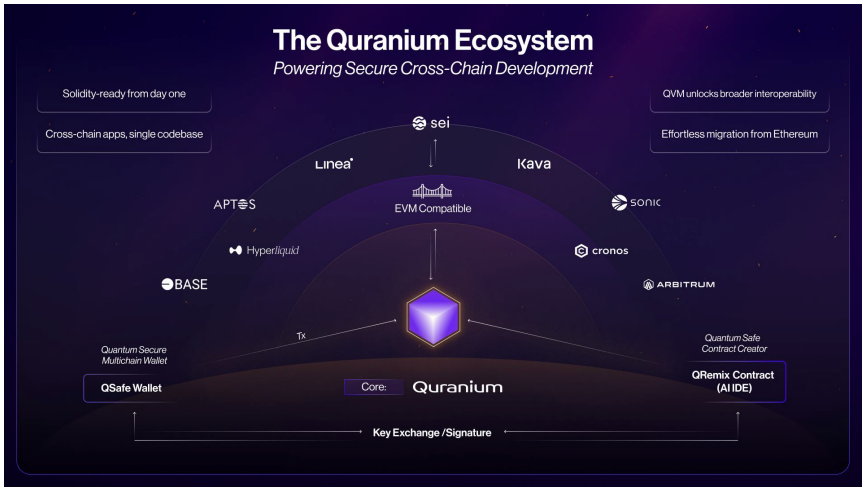
Threat Type	Quranium Mitigation

Quantum Attacks	SLH-DSA (hash-based post-quantum signatures)
51% Attacks	PoS +Slashing +Economic Disincentives
Smart Contract Bugs	EVM Compatibility +Auditing Tools +Secure Templates
Sybil/DoS Attacks	Staking Barriers +Fee Markets +Rate Limiting
Replay Attacks	Chain ID Enforcement

DEVELOPER ECOSYSTEM

Quranium has been purposefully designed to empower developers by offering a familiar, Ethereum-compatible environment while integrating advanced cryptographic primitives like SLH-DSA for post-quantum security. This enables both Web3-native and security-conscious developers to build confidently on the Quranium platform.

The ecosystem is designed around maximum compatibility, tooling extensibility, and future-proof architecture to accelerate decentralized application (dApp) and protocol development.

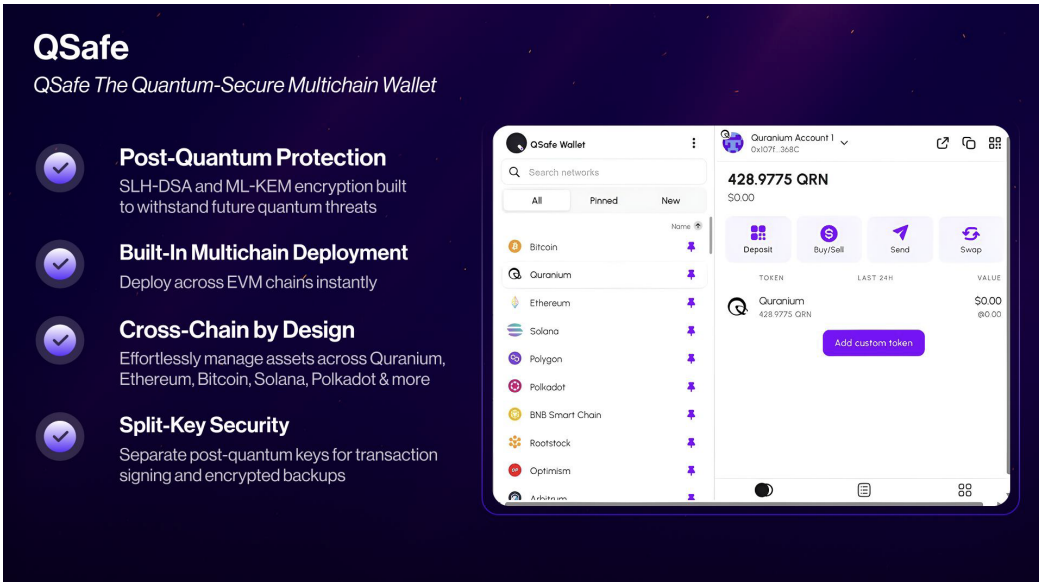


Wallet Support

Quranium supports leading Ethereum wallets as well as its own custom wallet implementations, with enhanced capabilities for quantum-resilient signatures.

QSafe Wallet

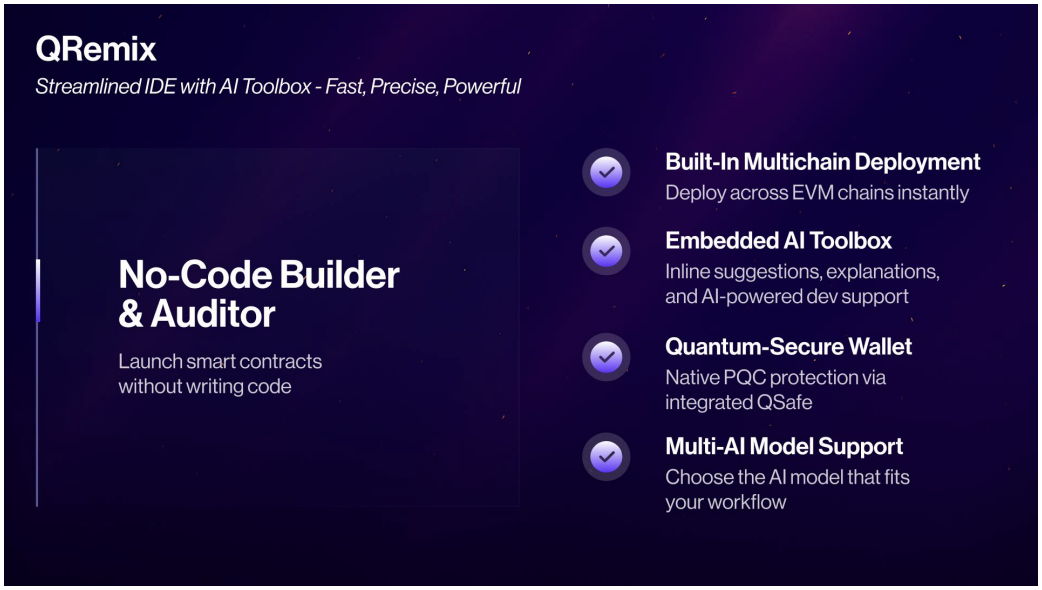
- QSafe Wallet is Quranium's native wallet, designed for secure multi-chain use. It supports all major chains and provides a complete solution for managing SLH-DSA keys and transactions.
- Key features of QSafe Wallet include:
    - SLH-DSA key generation for quantum-resistant signature generation and transaction signing.
    - Multi-account management for handling multiple Quranium accounts.
    - Customizable gas fees and transaction parameters, allowing users and developers to fine-tune their transactions.
    - Ledger and hardware wallet integration (planned for future releases), enhancing the security of key storage.
- QSafe Wallet is available in CLI, browser extension, and mobile versions, with ongoing development to expand its features.



Smart Contract Development Frameworks

Quranium ensures out-of-the-box support for the most widely used smart contract development frameworks in the Ethereum ecosystem.

Q-Remix IDE



The Next-Gen Quantum-Secure Smart Contract Development Environment.

Q-Remix IDE is a web-based smart contract development environment, built on the foundational architecture of Remix IDE, but reimagined for a post-quantum era. With built-in post-quantum cryptographic support, AI-assisted coding, and project-level automation, Q-Remix empowers developers to build secure, scalable, and intelligent Web3 applications for the future.

What It's For

- Writing, compiling, deploying, and testing quantum-secure smart contracts.
- Creating entire decentralized application (DApp) projects using natural language prompts.
- Learning, experimenting, and prototyping secure smart contracts with the help of an AI assistant.
- Ensuring forward-compatibility with quantum-resilient blockchain ecosystems.

How It Works

QRemix functions like Remix IDE in terms of:

- Solidity coding with syntax highlighting.
- Compilation and ABI generation.
- Deployment and interaction with smart contracts.
- File management and console output.

But it adds powerful new layers:

Quantum-Secure Infrastructure:

- Every cryptographic operation (e.g., signatures, key exchange) can optionally use post-quantum algorithms such as CRYSTALSKyber, Dilithium, or SPHINCS where applicable.
- Ensures resistance against future quantum computers without sacrificing developer usability.

Inline AI Assistant (Ctrl + I):

- Pressing Ctrl + I opens an inline prompt window.
- You type a request like *"create an ERC20 token with burn functionality"*.
- AI suggests smart contract code directly in your current file.i
- The newly inserted code is visually highlighted, giving you the option to Accept or Reject it.
- On acceptance, the code blends seamlessly into the file; on rejection, it disappears without trace.

Built-In Chatbot (Bottom-right):

- Ask coding questions like *"What's a fallback function?"* or *"Explain modifiers in Solidity."*
- Also supports contextual queries like *"Why am I getting this compiler error?"*
- Provides debugging hints, code explanations, and best practices.

Project Generator via Chatbot:

- Type a prompt like *"Create a voting DApp with frontend and backend folder structure"*.
- The chatbot replies with:
    - A brief project overview.
    - A clean project architecture diagram.
    - Preview of auto-generated folder/file structure with logic inside.
- You can then Confirm to auto-save it in your workspace with all files populated and ready.

Hardhat

- Quranium is fully compatible with Hardhat, a powerful development environment for writing, testing, and deploying Solidity smart contracts.
- Custom Hardhat plugins are available to:
    - Deploy contracts to Quranium testnet/mainnet. Integrate SLHDSA accounts into deployment scripts.
    - Run simulations with Quranium-specific gas parameters.

Foundry

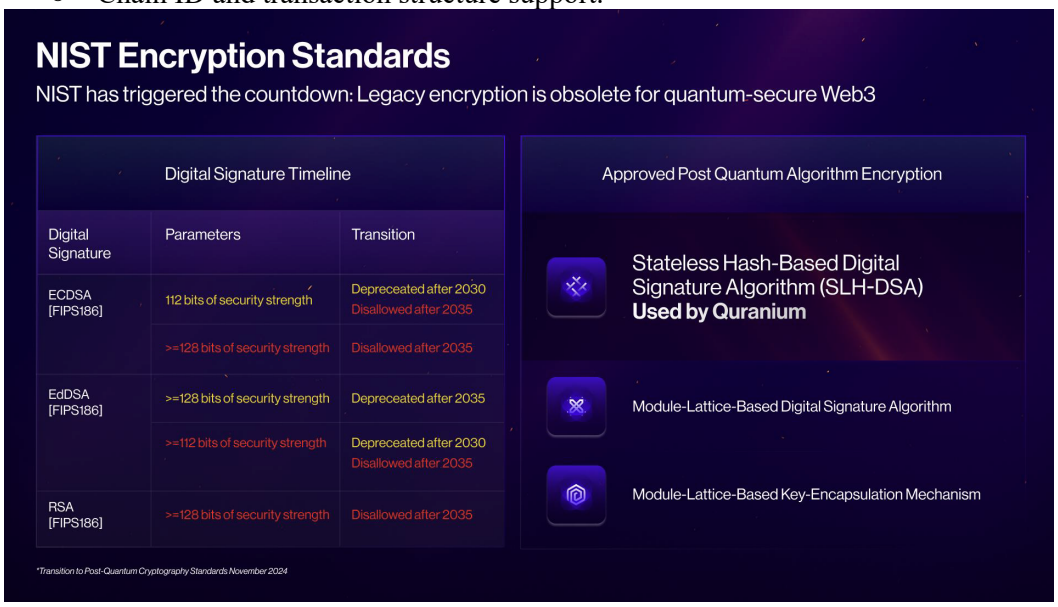
- Quranium also supports Foundry, a fast, Rust-based development toolkit. Developers can write contracts in Solidity and test them using Forge and Anvil.
- Foundry's modularity makes it easy to add Quranium-specific signer types, including SLHDSA key management.
- Both frameworks include Quranium-specific templates and starter kits to speed up onboarding.

APIs and Libraries

Developers building on Quranium can use familiar Ethereum libraries with minor adaptations to support its unique signature scheme.

Web3.js

- Quranium will support web3.js, the legacy JavaScript library for interacting with Ethereum nodes.
- A Quranium-patched version is available that adds:
    - SLHDSA signing hooks.
    - Quranium-specific JSONRPC support.
    - Chain ID and transaction structure support.



ethers.js (SLH-DSA-Compatible)

- Quranium will provide a modified version of ethers.js:
    - Seamless integration of SLHDSA key signing for wallets.
    - Support for Quranium node providers and RPC interfaces.
    - Includes QuraniumSigner and QuraniumProvider abstractions.

Developers can write dApps using familiar code like provider.sendTransaction() or contract.connect(signer) — with post-quantum protection built-in.

Tooling & IDE Plugins

- VS Code Extensions: Quranium extensions enhance Solidity support and enable SLHDSA-based signing for test transactions.
- Remix IDE Plugin: Quranium plugin for Remix allows developers to compile, deploy, and interact with contracts using the Quranium testnet directly.
- Chain Explorers: Quranium has its own blockchain explorer with support for SLHDSA transaction decoding and contract verification.

Developer Resources & Community

- **Quranium Docs**: Comprehensive documentation hub (GitBook) covering everything from SLH-DSA cryptography to node setup and smart contract guides.
- SDKs: Quranium SDKs available for JavaScript/TypeScript, Rust, and Python.
- Grants & Hackathons: Quranium Foundation will support open-source developers via hackathons, bounty programs, and ecosystem grants.
- **Support Channels**: Active Discord, Telegram, and GitHub discussions for developer Q&A and ecosystem coordination.

Summary Table

Tool / Feature	Ethereum-Compatible	SLHDSA Support	Quranium Ready
QSafe Wallet	🔶 (native)	✅	✅
Hardhat	✅	✅	✅
Foundry	✅	✅	✅
ethers.js	✅ Will be patched)	✅	✅
web3.js	✅ Will be patched)	✅	✅
QRemix Plugin	✅	✅	✅
VS Code Tools	✅	✅	✅

By offering a familiar yet forward-looking development stack, Quranium ensures that developers can start building immediately with tools they already know, while embracing the post-quantum era with SLH-DSA and scalable infrastructure.

PROOF-OF-STAKE (POS) GAS MODEL

Quranium's PoS gas model integrates both economic incentives and transaction efficiency to provide an optimal user experience while ensuring network security and scalability. The gas system works similarly to Ethereum's gas model but incorporates PoS-based adjustments.

Gas Mechanism

1. **Gas Price & Gas Limit:**
    a. Gas Price: The amount of native cryptocurrency (e.g., QRN tokens) users pay to process transactions. It fluctuates based on network congestion and validator preferences.
    b. Gas Limit: The maximum amount of gas a user is willing to pay for a transaction. This is determined by the user based on the complexity of the transaction (e.g., smart contract execution, transfers, etc.).
2. **PoS Influence on Gas:**
    a. Staking Mechanism: Validators stake QRN tokens as collateral to propose new blocks. Higher staking increases a validator's chance to propose a block.
    b. Gas Auction Model: Validators and network participants can set their gas price dynamically in real-time. Gas prices may vary slightly depending on network activity and validator-staked amounts.
    c. Lower Gas Fees during Low Activity: In a low-traffic environment, the gas price will decrease since validators are more incentivized to propose new blocks to receive staking rewards.
3. **Gas Efficiency & Scaling:**
    a. PoS allows for more efficient block production because it is less resource-intensive than Proof-of-Work (PoW).
    b. Dynamic gas adjustments help prevent overpricing and keep transaction costs manageable even during peak periods.

Gas Limit for Transactions

- **Transaction Gas Limit:** Each transaction has an upper gas limit. For standard transactions like transfers, this limit is predefined. Complex operations, such as executing a smart contract, will require higher gas limits based on the complexity.

- **Block Gas Limit:** This refers to the total gas limit for all transactions within a block. Validators have the option to adjust the gas limit based on network activity and overall stake.

PENALTY RULES

Penalty mechanisms in Quranium are implemented to maintain network integrity, prevent malicious behavior, and ensure that validators and nodes behave in the best interest of the system.

Validator Penalties

Validators in Quranium are crucial to maintaining the PoS consensus and confirming blocks. Malicious actions or misbehavior can result in penalties.

1. **Slashing:**
    a. Slashing is the most common penalty for validators who are caught misbehaving, such as by proposing invalid blocks or double-signing. A portion of the staked QRN tokens is forfeited, making malicious behavior costly.
    b. Double Signing: If a validator signs conflicting blocks (e.g., signs two blocks at the same block height), it will result in a slashing penalty.
    c. Downtime Penalty: Validators that frequently go offline or fail to validate transactions for extended periods will be penalized by having a portion of their staked tokens slashed. This ensures validators remain online and responsive.

2. **Missed Block Production:**
    a. Validators who miss block production (i.e., fail to propose a new block within the allowed time window) will receive minor penalties. This could also influence their ability to propose future blocks.
    b. Underperformance: If a validator consistently fails to participate in the consensus process, it may experience a reduction in the staking rewards it receives.

3. **Inactivity Leak:**
    a. Inactivity Leak penalizes validators who do not participate in consensus for long periods. The leaked amount increases if a validator's inactivity continues without active participation in the network. This encourages continuous engagement from validators.

4. **Incentive for Honest Behavior:**
    a. Honest validators are rewarded with staking rewards, allowing them to earn transaction fees and block rewards.
    b. Validators who act maliciously are penalized and lose the ability to earn rewards and may lose their staked QRN tokens.

Transaction Penalties

- **Failed Transactions**: If a user's transaction is unsuccessful due to insufficient gas or an invalid contract execution, the gas fee is still deducted, but the transaction does not get confirmed. The penalty here is that the gas spent is non-refundable.

- **Non-compliant Smart Contracts**: Smart contracts that are written in a way that is either computationally inefficient or malicious may lead to a penalty in execution fees. For instance, a smart contract that intentionally performs unnecessary operations will be charged higher gas fees and could be flagged by the network for audit.

ATTACK PREVENTION MECHANISMS IN QURANIUM

Quantum Resistance

Quranium uses SLH-DSA (Post-Quantum Digital Signature Algorithm) to provide quantum resistance for its transactions and smart contracts. This ensures that even if powerful quantum computers emerge in the future, they will not be able to break the cryptographic security of Quranium's blockchain.

- **SLH-DSA Signatures:** SLH-DSA replaces traditional elliptic curve signatures, which are vulnerable to quantum computing-based attacks, with a quantum-resistant alternative. This is crucial to ensure long-term security.
- **Safe Smart Contracts:** Even after quantum computers become a practical reality, the cryptographic schemes used in Quranium will protect users' assets and smart contracts, preserving blockchain integrity.

Proof-of-Stake (PoS) Consensus to Mitigate 51% Attacks

A 51% attack in Proof-of-Work (PoW) systems can lead to malicious actors controlling the majority of the network and double-spending coins. Quranium mitigates the risk of such attacks through its Proof-of-Stake (PoS) consensus mechanism, which is more resistant to 51% attacks than PoW.

- **Slashing:** Validators who act maliciously (e.g., double-signing blocks or attempting to create conflicting forks) are penalized by having a portion of their staked tokens slashed. This discourages dishonest behavior by making attacks economically infeasible.
- **Economic Incentives:** Validators are incentivized to behave honestly, as they earn rewards for proposing and validating blocks. Malicious activity results in loss of rewards and staked tokens, ensuring that honest behavior is always the most profitable.
- **Validator Participation:** Since the likelihood of controlling a significant portion of staked assets is low, the attacker's cost increases substantially. A validator needs to stake a large amount of QRN tokens to take over the network, which becomes prohibitively expensive.

Transaction Validation & Smart Contract Auditing

Quranium inherits the battle-tested Ethereum Virtual Machine (EVM), which is known for its robust transaction validation process and widespread security auditing. Smart contracts on Quranium can leverage existing tools and processes used in Ethereum to prevent vulnerabilities.

1. **Smart Contract Auditing:**
    a. Quranium encourages the auditing of smart contracts using best practices, third-party auditors, and established tools (e.g., MythX, Slither, Oyente) to check for security vulnerabilities like reentrancy attacks, overflow/underflow errors, and other common smart contract issues.
    b. Custom smart contract vulnerabilities are minimized by the use of established, secure coding practices within the ecosystem.

2. **Automatic Bug Detection:**

    a. As part of the development environment, tools like Hardhat and Foundry can be used for extensive testing and simulation, ensuring that smart contracts are properly tested for edge cases before deployment.

    b. Quranium also integrates a bug bounty program, where the community can report potential vulnerabilities.

Protection Against Sybil Attacks

Sybil attacks occur when an attacker creates multiple fake identities to gain control of the network. Quranium uses PoS to prevent this kind of attack in a few key ways:

1. Validator Staking To participate in consensus, validators must stake QRN tokens. This means that an attacker would need to stake a significant amount of QRN tokens to create fake identities and influence the consensus, which is economically expensive and risky.

2. Reputation & Slashing Validators with a history of misbehavior or Sybil-like activity can be penalized by slashing, reducing their staked tokens and preventing them from participating in future block validation.

3. Quorum-based Decision Making By ensuring that multiple validators are required to come to a consensus, Quranium prevents a single or a small group of malicious actors from overtaking the network.

Distributed Denial of Service (DDoS) Prevention

Quranium's architecture, which is based on distributed nodes and decentralized consensus, makes it inherently resilient against traditional DDoS (Distributed Denial of Service) attacks, where attackers flood the network with traffic to overwhelm it.

1. **Decentralized Network:** Quranium's P2P network ensures that even if one or several nodes are attacked, the rest of the network remains intact and operational.

2. **Light Nodes & Full Nodes Distribution:** By using a combination of light and full nodes, Quranium distributes the computational load and storage requirements, making it harder to launch a successful DDoS attack on a single point.

3. **Validator Redundancy:** Since validators are spread across the network and block proposals require a quorum of validators to agree, attacking a single validator node does not disrupt the entire consensus process.

Double-Spending Attack Prevention

A double-spending attack occurs when an attacker tries to spend the same tokens multiple times by exploiting the delay in the system's transaction processing. Quranium prevents double-spending through a combination of PoS and effective transaction validation mechanisms:

1. PoS Security Validators must stake QRN tokens to participate in block production and transaction validation. Double-spending would require controlling more than 50% of the staked tokens, making such an attack highly expensive and risky.

2. Finality Mechanism Quranium uses finality guarantees in its PoS protocol to ensure that once a transaction is included in a block, it cannot be reversed. This reduces the chance of double-spending occurring after the block is finalized.

3. Transaction Mempool Transactions are first placed in the mempool, where they are checked for validity, including double-spending attempts. Invalid transactions are rejected before they even enter the block validation process.

Front-running & Transaction Ordering Attacks

Front-running occurs when an attacker sees a pending transaction and executes their own transaction before it, benefiting from the price change or market information.

1. **Anti-Front-running Mechanisms:**
    a. Quranium can use commit-reveal schemes for sensitive transactions to prevent front-running. In these schemes, users commit to their transaction by submitting a hashed version of the transaction data, which is revealed later, preventing attackers from observing and acting on the transaction details.

    b. Time-based Commitments: Quranium can implement time delays and transaction ordering algorithms to prevent malicious actors from exploiting transaction data ahead of time.

Denial of Service via Smart Contract

Malicious actors can attempt to overload the network through inefficient smart contract code. Quranium employs a combination of gas mechanisms and smart contract audit recommendations to mitigate such risks.

1. **Gas Limits:** Every transaction and smart contract execution has a gas limit. Transactions that require excessive computation will fail if they exceed the set gas limit, preventing resource exhaustion attacks.

2. **Audit Tools & Best Practices:** Developers are encouraged to use the best practices for smart contract development. Static analysis tools such as Slither and Mythril are integrated into the ecosystem to automatically scan for vulnerabilities and ensure contracts are optimized for efficiency.

Insider Attacks

In the case of insider attacks, where validators or network participants with high privileges exploit their position, Quranium has security measures to minimize such risks:

1. **Transparency and Auditing:** All validators' activities and block proposals are visible to the entire network, and suspicious actions can be reported and investigated. This ensures that there is no centralized control over the network.

2. **Slashing for Malicious Behavior:** Validators who act maliciously, including collaborating with insiders to manipulate blocks or transactions, are penalized through slashing of staked tokens.

3. **Democratic Governance:** Validators are regularly rotated and elected by the stakers to ensure no single party can gain excessive control over the network.

Network Forking Prevention

Quranium prevents malicious forks from splitting the network through finality mechanisms in the PoS protocol, ensuring that once a block is validated and included in the chain, it is final and cannot be reversed.

- **Forking Resistance:** Quranium uses a finality gadget in its PoS consensus to ensure that a fork cannot occur unless it has the support of more than 50% of the staked QRN tokens.
- **Quorum-Based Consensus:** The network requires a majority of validators to agree on each block, ensuring that a minority cannot hijack the chain and create an alternate history.

Key, Signature Generation & Verification Time Analysis

Overview:

This test generated 10, 100, and 1000 key pairs using SLHDSA to observe the time taken for key generation, signing and verifying operations. Each key pair signed a 'Hello, World!' message, allowing for a performance comparison at different scales.

SLHDSA - C Implementation:

The following tests are conducted on machine with the following specifications,

- Model name: 11th Gen Intel(R) Core(TM) i5-1135G7 @2.40GHz
- CPU(s): 8
- RAM:16GB
- ROM:512 GB
- Architecture: AVX-512

The below table shows average performance metrics per operation (based on 1000 iterations) for key generation, signing, and verification

S. No	Algorithm	Key Size Bytes)	Key Gen (ms)	Sign (ms)	Verify (ms)	Size Bytes)
1.	SLHDSA SHAKE256f	SK 128 PK 64	4.6463	93.10492	2.479921	49,856
2.	SLHDSA SHAKE256s	SK 128 PK 64	71.60378	848.6832	1.176295	29,792
3.	SLHDSA SHAKE128s	SK 64 PK 32	68.73005	528.5192	0.519581	7,856
4.	Modified SLH DSASHAKE 128s with n = 32 instead of 16	SK 128 PK 64	142.0908	1038.354	0.996826	22,880

SLHDSA - SHAKE 256F

10 Keys, Signature & Verification 1
100 Keys, Signature & Verification 1
1000 Keys, Signature & Verification 1

SLHDSA - SHAKE 256s

10 Keys, Signature & Verification 1
100 Keys, Signature & Verification 1
1000 Keys, Signature & Verification 1

SLHDSA - SHAKE 128s

10 Keys, Signature & Verification 1
100 Keys, Signature & Verification 1
1000 Keys, Signature & Verification 1

SLHDSA - SHAKE 128s with n = 32 instead of 16

10 Keys, Signature & Verification 1
100 Keys, Signature & Verification 1
1000 Keys, Signature & Verification 1

TOKEN DISTRIBUTION

A total supply of Tokens will be capped at 2,100,000,000 Tokens and reaches close to full circulation after 48 months (largely due to a 5% liquidity allocation that is unlocked as needed)**.** Tokens will be created as part of the minting processes, *see* "**Description of the Tokens**" for additional detail below.

Token supply and vesting for different groups are as follows below.

Tokenomics

Stage	Price	Discount from list price	Raise Amount	Valuation	Tokens Sold	Percent of supply	Release on TGE (%)	Release on TGE ($)	Release on TGE (qty)
Pre Seed	$0.0048	92.86%	$300,000	$10,000,000	63,000,000	3%	0.00%	$0	0
Seed	$0.0238	64.29%	$3,000,000	$50,000,000	126,000,000	6%	0.00%	$0	0
Strategic	$0.0357	46.43%	$3,000,000	$75,000,000	84,000,000	4%	0.00%	$0	0
Private	$0.0660	1.00%	$6,000,000	$100,000,000	126,000,000	6%	0.00%	$0	0
Public Pre-Sale	$0.0667		$4,200,000	$140,000,000	63,000,000	3%	10.00%	$450,000	6,300,000
Exchange IEO	$0.0715		$1,500,000	$150,000,000	21,000,000	1%	100.00%	$1,500,000	21,000,000
		Total:	$18,000,000						

Initial Market Cap (excl. liquidity)	$6,891,885
Fully Diluted Valuation	$150,000,000
Total Supply	2,100,000,000
Circulating Supply on TGE (excl. liquidity)	4.59%

The Company is currently in discussions with several centralized exchanges, including KuCoin, MEXC, INEX, Kraken, Binance and Bybit. Final exchange confirmations will be announced closer to the launch date.

Distribution Schedule

The distribution schedule for the Tokens at the Token Integration Event is described below.

Token Distribution

Article	Allocation	Quantity of tokens	% on TGE	Quantity on TGE	Cliff/Lock-up	Vesting	Vesting Type	
Pre Seed	3%	63,000,000	0%	0	6	18	Linear Monthly	6 months cliff, then linear monthly unlock over 18 months
Seed	6%	126,000,000	0%	0	3	18	Linear Monthly	3 months cliff, then linear monthly unlock over 18 months
Strategic	4%	84,000,000	0%	0	3	18	Linear Monthly	3 months cliff, then linear monthly unlock over 18 months
Private	6%	126,000,000	0%	0	3	18	Linear Monthly	3 months cliff, then linear monthly unlock over 18 months
Public Pre-Sale	3%	63,000,000	10%	6,300,000	0	10	Linear Monthly	10% at TGE, then linear monthly unlock over 10 months
Exchange IEO	1%	21,000,000	100%	21,000,000	0	0	Linear Monthly	100% at TGE
Ecosystem Growth	33%	693,000,000	8%	55,440,000	0	36	Linear Monthly	Linear monthly unlock over 36 months
Foundation	10%	210,000,000	0%	0	12	36	Linear Monthly	12 month cliff, then linear monthly unlock over 36 months
Team	20%	420,000,000	0%	0	12	36	Linear Monthly	12 months cliff, then linear monthly unlock over 36 months
Advisors	5%	105,000,000	5%	5,250,000	6	24	Linear Monthly	5% at TGE, 6 months cliff, then linear monthly unlock over 24 months
Marketing	4%	84,000,000	10%	8,400,000	0	24	Linear Monthly	10% at TGE, then linear monthly unlock over 24 months
Liquidity	5%	105,000,000					Linear Monthly	Unlocked as needed
Total:	100.00%	2,100,000,000						

At the Token Integration Event, the following core functionalities will be live: token transfers, staking and delegation mechanisms, payment of transaction and network fees, and early access to selected ecosystem products and services including:

- QRN Scan: A Quranium blockchain explorer
- Q-Remix: An IDE for Smart Contracts and dApps on Quranium
- QSafe: A multichain wallet that supports Quranium Chain.

The Company has a large community: Twitter (84.2K), Discord (16.1), Telegram (56.1K).

Initial Launch of the Tokens

The Company expects to enter into TPAs on an ongoing basis through the Offering Period. The Company is targeting a Token Integration Event on or before the TIE Date. However, there can be no assurance that the Tokens will be issued as of such date.

Overview of Transfer Restrictions Discussed in this Memorandum

This Memorandum describes the legal and contractual transfer restrictions applicable to the Tokens. Purchasers should carefully review this Memorandum, including the transfer restrictions described under "**Notice to Purchasers**" which contain important information regarding the Tokens. Purchasers should consult with their own legal and financial advisors regarding the transfer restrictions to which they will be

bound. The summary below is intended to provide a summary overview of applicable transfer restrictions and are qualified by reference to the transfer restrictions set forth under "**Notice to Purchasers**".

USE OF PROCEEDS

The Company estimates that the maximum net proceeds from this Offering, unless the Offering amount is subsequently amended by the Company in its discretion, and any other contemporaneous Token offerings on Republic (together, the "**Republic Offerings**") may be approximately $450,000 after deducting estimated offering expenses, less any marketing and legal expenses.

The Company intends to use the proceeds of the Republic Offerings, net of any federal and state income taxes, primarily for: Tech Development and R&D, Business Development and Partnerships and Educational Awareness and Community Growth. It is anticipated that the proceeds raised in this Offering will extend our operating runway by 3.5 months in addition to the existing runway and planned additional capital we are raising.

Accordingly, our management will have broad discretion over the application of the proceeds received from the Republic Offerings and may spend the proceeds from the Offering in ways with which investors may not agree with or that do not yield a favorable return, if at all. We cannot predict whether this allocation invested will yield a favorable return. If management does not invest or apply the proceeds of this Offering in ways that benefit the Tokens, the future value and utility of Purchasers' Tokens may be adversely affected. Our failure to apply such funds effectively could have a material adverse effect on our business, financial conditions, and results of operations. We cannot specify with certainty all of the particular uses for the net proceeds to be received upon the closing of the Republic Offerings. In addition, the amount and timing of our actual expenditures will depend upon numerous factors. Pending other uses, we may allocate the proceeds to interest-bearing instruments, direct or guaranteed obligations of the U.S. government, crypto assets, or hold as cash.

We cannot guarantee that we will be able to sell any or all of the Tokens in the Republic Offerings. If we do not sell any of the Tokens, we will not obtain any usable proceeds from the Republic Offerings and our ability to continue as a going concern may be called into question.

The Company reserves the right to alter the use of proceeds of the Republic Offerings.

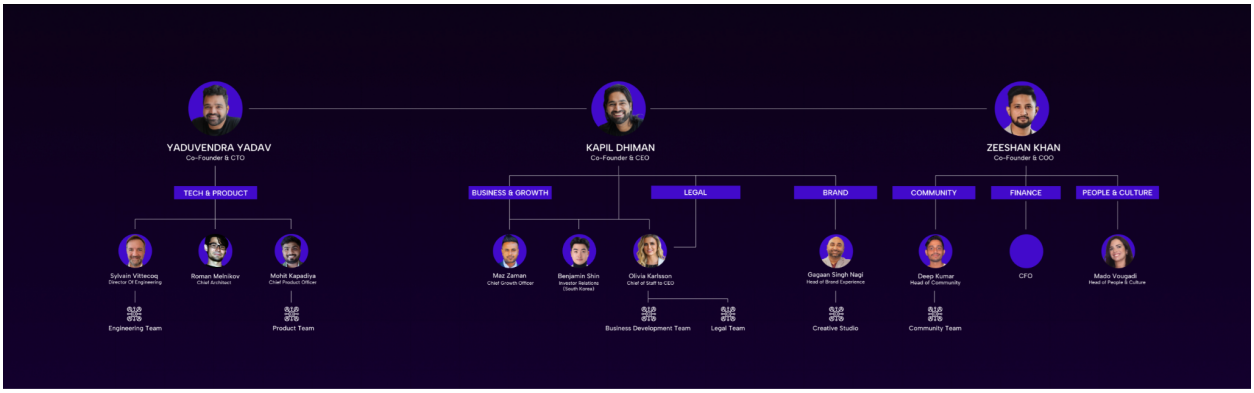
DILUTION

The following table summarizes the differences between the total consideration and the price per token paid by existing tokenholders who have purchased or acquired Tokens or rights thereto, prior to the date of this Memorandum and participants participating in this Offering at the price, or deemed price, to the public of $0.0667 per Token, before deducting estimated expenses in connection to this Offering:

	Tokens Previously Purchased or Acquired	Total Consideration	Price Per Token
Pre-Seed Investors	63,000,000	$300,000	$0.0048
Seed Investors	126,000,000	$3,000,000	$0.0238
Strategic Investors	84,000,000	$3,000,000	$0.0357
Private Round Investors	126,000,000	$6,000,000	$0.0476
Tokens offered in this Offering	7,500,000	$500,250	$0.0667

MANAGEMENT OF THE COMPANY

Name	Age	Position
Kapil Dhiman	**33**	Co-Founder, CEO and Board Member
Zeeshan Khan	**34**	Co-Founder, COO and Board Member
Yaduvendra Singh	**34**	Co-Founder, CTO and Board Member
Bernard Jahrmann	**58**	Board Member



Committee Composition and Risk Oversight

The Committee of the Company is currently composed of 4 board members**.** There are no family relationships among the board members or any of the executive officers.

CERTAIN RELATIONSHIPS AND RELATED-PARTY TRANSACTIONS

ODB Offering Engagement

We are currently party to an offering engagement agreement with ODB, effective as of July 10, 2025 (the "**Engagement Agreement**"), who has agreed to provide certain offering facilitation services, including executing and delivering evidence of the interests sold in this Offering to each Purchaser and the use of the Republic Platform. ODB has made no commitment to purchase all or any part of the securities. The term of the Engagement Agreement will continue until the later of the date on which (i) all proceeds in the Offering are disbursed and the TPAs are no longer being listed on the Republic Platform or (ii) all fees due to ODB being remitted unless otherwise terminated by either party upon thirty (30) days' prior written notice or for cause pursuant to the Engagement Agreement.

ODB is not purchasing any of Tokens in this Offering and are not required to sell any specific number or dollar amount of securities but will instead arrange and manage this Offering on their fundraising platform, www.republic.com.

Reimbursable expenses in the event of termination. Termination fees are due for any termination in the event of ODB's uncured breach, or the expiration of the term of the Engagement Agreement. The Company shall at the date of termination pay the (a) termination fee of $15,000, (b) Business Advisory Service Fee, and (c) any incurred Payment Processing Fees.

Commission and Expenses. The cash fee paid to ODB from the proceeds of this Offering will be the greater of (i) $12,000 or (ii) pursuant to the following schedule: (A) for the dollar value of the Tokens issued to Purchasers pursuant to the combined proceeds of each Offering up to but not in excess of $100,000.00, zero percent (0%) and (B) for the dollar value of the Tokens issued to Purchasers pursuant to the combined proceeds of each Offering greater than $100,000.00, six percent (6%) (the "**Cash Commission**"). In addition to the Cash Commission, ODB will be entitled to a Tokens commission equivalent to two percent (2%) of the dollar value of the Tokens issued to Purchasers pursuant to the combined proceeds of each Offering at the time of closing.

For each executed transaction resulting from off-platform services for Purchasers introduced to the Company via an introduction notice (each, an "**Off-Platform Purchaser**"), the Company shall pay ODB: (i) a cash payment of six percent (6%) of the dollar value of the Tokens issued to the Off-Platform Purchaser ("**Off-Platform Cash Commission**"), and (ii) two percent (2%) of the total number of Tokens of the same type issued to the Off-Platform Purchaser ("**Off-Platform Tokens Commission**"). Together, these payments are the "**Off-Platform Services Commissions**." Off-Platform Services Commissions are payable to ODB even after termination, unless for cause.

ODB has agreed, with respect to the TPAs issued to it as part of its commission, not to: (a) sell, transfer, assign, pledge or hypothecate any securities obtained pursuant to the ODB Engagement Agreement for a period of one hundred eighty (180) days following the date on which this Offering is qualified by the SEC to anyone other than (i) its affiliates or any selected dealer that may participate in the Offering, or (ii) a bona fide officer of ODB or of any such selected dealer, in each case in accordance with FINRA Conduct Rule 5110(e)(1), or (b) cause such Tokens to be the subject of any hedging, short sale, derivative, put or call transaction that would result in the effective economic disposition of such TPAs, except as provided for in FINRA Rule 5110(e)(2). On and after one hundred eighty (180) days after the date on which this Offering is qualified by the SEC, transfers to others may be made subject to compliance with or exemptions from applicable securities laws. There are no registration rights offered to ODB.

Under the Engagement Agreement, ODB may also pass through certain administrative expenses related to payment processing in the event of a withdrawn offering. The Company is responsible for all costs related to Purchaser payment disputes. The Company will pay to ODB various fees, which are not considered underwriting compensation. ODB has the right to assign the Engagement Agreement to an affiliate or successor.

Business Advisory Service Fees: We have agreed to pay ODB $17,500 within 7 days of the effective date of the Engagement Agreement, for services including standard, additional, or enhanced reviews of KYC, AML, diligence, compliance monitoring, CIP, financials, offering documents, and the appropriate time and effort undertaken to perform such reviews. ODB may provide additional guidance regarding the Offering's size and structure, market conditions, and provide suggestive participation into other possible circumstances that may affect the Company. This participation is not deemed to be absolute or as legal advice and does not serve as a substitute for Company's own legal and regulatory representation.

Payment Processing Fees. The Company shall pay to ODB, irrespective of the outcome of each Offering, all payment processing fees. If the Offering has launched, these fees are typically the greater of $2,500 or approximately two percent (2%) of an Offering's proceeds. The Company shall reimburse ODB for administrative fees associated with the Offering.

Any overpayment amounts of less than $25 shall be deemed a nonrefundable gift from the applicable subscriber to the Company.

Indemnification and Control: The Company has agreed to indemnify ODB against any and all liabilities, obligations, losses, damages, claims, actions, suits, costs and expenses (including professional fees and expenses) of any kind and nature whatsoever concerning, relating to, arising out of or from the (i) Engagement Agreement, (ii) Tokens, (iii) Offering, or (iv) violation of law, any acts or omissions, negligence or willful misconduct of the Company. ODB and their respective affiliates are engaged in various activities, which may include securities, trading, commercial and investment banking, financial advisory, investment management, investment research, principal investment, hedging, financing, and brokerage activities. ODB and their respective affiliates may in the future perform various financial advisory and investment banking services for us, for which they received or will receive customary fees and expenses.

SECURITY OWNERSHIP OF THE COMPANY

Quranium Association, a Swiss Association with no share capital, is the fund-raising and token-issuing entity. Committee members of Quranium Association are Kapil Dhiman (President and Signing Authority), Zeeshan Khan, Yaduvendra Singh and Bernard Jahrmann.

DESCRIPTION OF THE TOKENS

Ownership of Tokens

We are offering TPAs in this Offering in accordance with the terms outlined under "**Terms of the Offering**" above, which entitles the holders thereof to purchase Tokens at a fulfillment price of $0.0667 per Token. The TPAs and the Tokens are subject to transfer restrictions as described under "**Terms of the Offering**" above.

Token

As a layer-1, Quranium primarily generates revenue from gas fees. For a standard transaction on the Quranium network, the average gas fee is approximately 0.00001 – 0.00006 QRN, though this may vary slightly with network demand.

Token Utility:

- **Transaction fees**: Used to pay for transactions and smart contract execution on the Quranium blockchain.
- **Staking and network security**: Token holders can stake to help secure the network and receive rewards in return, supporting decentralization and overall network integrity.
- **Ecosystem incentives**: The token is used to incentivize builders, validators, and community contributors, encouraging active participation and long-term ecosystem growth.
- **Access to services**: Holders can access premium features and services within the ecosystem, such as the quantum-resistant wallet (QSafe), launchpad participation, and future enterprise-level tools.

Revenue generated from these fees is shared between Quranium SA and the wider ecosystem. A portion is allocated to Quranium SA to support ongoing protocol development and core operations, while the remaining share is distributed to ecosystem contributors, such as validators and community initiatives, to encourage decentralization and network growth. The exact split of revenue share has not been determined at the time of diligence.

Future potential revenue streams on top of the protocol include stablecoins and money market products, however these are still in ideation/development and the timeline for availability is unknown.

Token Supply

The maximum supply of Tokens is 2,100,000,000 tokens. The total supply of Tokens will be allocated as described in "**Plan of Distribution**".

Limited Token-Related Rights

Tokens will not provide you with any enforceable rights against the Company, or any third-party developer, including any rights to receive payments, any control rights or any claims on assets. Holders of Tokens will not receive a right to any repayment of principal or interest, any interest in the profits or losses of the Company, its affiliates, or any third-party developer. Holders of Tokens may not have any right to vote on any matters relating to the Company, its affiliates, or any third-party developer. Further, we are not aware

of any binding obligation on the Company with respect to the Tokens or the holders of Tokens following the delivery of Tokens.

PLAN OF DISTRIBUTION

This Offering of Tokens will be deemed to be fully subscribed once the aggregate purchase amount (of TPAs) meets the Offering Size (see "**Terms of the Offering**").

Distribution of Tokens

The 2,100,000,000 Tokens, consisting of the initial minted supply of Tokens will be distributed as follows:

Pre-Seed Round – 3% (63 million Tokens)

- 6-month cliff, followed by 18-month linear vesting
- 0% released at Token Integration Event (TIE)

Seed Round – 6% (126 million Tokens)

- 3-month cliff, followed by 18-month linear vesting
- 0% at TIE

Strategic Round – 4% (84 million Tokens)

- 3-month cliff, followed by 18-month linear vesting
- 0% at TIE

Private Round – 6% (126 million Tokens)

- 3-month cliff, followed by 18-month linear vesting
- 0% at TIE

Public Pre-Sale – 3% (63 million Tokens)

- 10% unlocked at TIE, followed by 10-month linear vesting

Exchange IEO – 1% (21 million Tokens)

- 100% unlocked at TIE

Ecosystem Growth – 33% (693 million Tokens)

- 8% at TIE, 36-month linear vesting (no cliff)
- Allocated to incentivize builders, validators, developers, and long-term adoption

Foundation – 10% (210 million Tokens)

- 12-month cliff, followed by 36-month linear vesting

Team – 20% (420 million Tokens)

- 12-month cliff, followed by 36-month linear vesting

Advisors – 5% (105 million Tokens)

- 5% at TIE, 6-month cliff, followed by 24-month linear vesting

Marketing – 4% (84 million Tokens)

- 10% at TIE, followed by 24-month linear vesting

Liquidity – 5% (105 million Tokens)

- Unlocked as needed to ensure exchange and market depth support

Republic Sale (Regulation D). A total number of 7,500,000 Tokens are allocated to investors in the Republic Sale (Regulation D). The Company reserves the right to increase or decrease this allocation, in its sole discretion and without further amendment to this Memorandum, by re-allocating Tokens from the unused allocation. Tokens under this distribution category are subject to delivery restrictions. Purchasers will each enter into a TPA with the Company. At the time of entering into the TPA, the Purchaser will designate a network address where such Purchaser wishes to receive delivery of the Tokens. Tokens in this distribution category will be delivered to an Ethereum compatible wallet address designated by each Purchaser in the TPA as follows: 10% at Token Integration Event, followed by linear monthly vesting over 10 months.

Republic Sale (Concurrent Offering). The Company may conduct, during or after this Offering, one or more offerings of its securities to certain investors satisfying the eligibility requirements of the applicable exemption from the registration requirements of the Securities Act, including, but not limited to, Regulation S (any such offering, a "**Concurrent Offering**"). Investors solicited through this Offering, or with whom the Company had not established a substantive relationship prior to the commencement of this Offering, may not be permitted to participate in any Concurrent Offering, except as otherwise permitted under the Securities Act, Regulation S and, if applicable, the non-exclusive safe harbors set forth in Rule 152(b). The Company reserves the right to increase or decrease such allocation for the Concurrent Offering, in its sole discretion and without further amendment to this Memorandum, by re-allocating Tokens from the unused allocation. Tokens under this distribution category are subject to delivery restrictions. Purchasers will each enter into a TPA with the Company. At the time of entering into the TPA, the Purchaser will designate a network address where such Purchaser wishes to receive delivery of the Tokens. Tokens in this distribution category will be delivered to an Ethereum compatible wallet address designated by each Purchaser in the TPA as follows: 10% at Token Integration Event, followed by linear monthly vesting over 10 months.

Token Supply Release Schedule

The release of Tokens will follow a structured vesting schedule over a period of up to 48 months, beginning from the Token Integration Event.

- **Pre-Seed, Seed, Strategic, and Private Rounds**: These investor allocations represent 19% of the total token supply. They are subject to cliffs of 3 to 6 months, followed by linear monthly vesting over 18 months. No Tokens are unlocked at TIE.
- **Public Pre-Sale**: Representing 3% of total supply, this category is subject to a 10% unlock at TIE, followed by linear monthly vesting over 10 months.
- **Exchange IEO**: Comprising 1% of total supply, this allocation is fully unlocked at TIE and intended for immediate liquidity and exchange listing.
- **Team and Foundation**: These two categories together represent 30% of total supply. Both are subject to a 12-month cliff followed by linear vesting over 36 months, ensuring long-term alignment with project success.

- **Advisors**: Representing 5% of supply, subject to a 6-month cliff and 24-month linear vesting thereafter, with 5% unlocked at TIE.
- **Ecosystem Growth**: The largest allocation at 33%, released monthly over 36 months, without a cliff. This supports grants, bounties, validator incentives, and other ecosystem programs.
- **Marketing**: Comprising 4%, with 10% unlocked at TIE and the remaining 90% vesting linearly over 24 months.
- **Liquidity**: 5% of the supply is reserved for liquidity provisioning and may be deployed on an as-needed basis. No fixed vesting is applied.

Purchaser Qualifications

Only persons of adequate financial means who have no need for present liquidity with respect to this purchase should consider purchasing the Tokens offered hereby because: (i) a purchase of the Tokens involves a number of significant risks (see "**Risk Factors**"); (ii) no market for the Tokens currently exists; and (iii) there is no established trading market for the Tokens and it is possible that a public market will never develop for the Tokens or, if one were to develop, it may develop without the involvement of the Company. The sale of Tokens as described herein is intended to be exempt from registration under the Securities Act and applicable state securities laws.

This Offering is limited solely to Purchasers who are accredited investors as defined in Regulation D under the Securities Act, meaning only those persons or entities coming within the definition in Rule 501 of Regulation D, including *among others,* any one or more of the following categories:

(i) Any bank, as defined in Section 3(a)(2) of the Securities Act, or any savings and loan association or other institution defined in Section 3(a)(5)(A) of the Securities Act, whether acting in its individual or fiduciary capacity; any broker-dealer registered pursuant to Section 15 of the Exchange Act; any insurance company, as defined in Section 2(a)(13) of the Securities Act; any investment company registered under the Investment Foundation Act of 1940 or a business development company, as defined in Section 2(a)(48) of that Act; any Small Business Investment Foundation licensed by the United States Small Business Administration under Section 301(c) or (d) of the Small Business Investment Act of 1958; any plan established and maintained by a state, its political subdivisions or any agency or instrumentality of a state or its political subdivisions for the benefit of its employees, if such plan has total assets in excess of $5,000,000; and any employee benefit plan within the meaning of the Employee Retirement Income Security Act of 1974, if the investment decision is made by a plan fiduciary, as defined in Section 3(21) of such Act, that is either a bank, savings and loan association, insurance company or registered investment advisor, if the employee benefit plan has total assets in excess of $5,000,000 or, if a self-directed plan, with investment decisions made solely by person(s) that are accredited investor(s);

(ii) Any private business development company as defined in Section 202(a)(22) of the Investment Advisors Act of 1940;

(iii) Any organization described in Section 501(c)(3) of the Internal Revenue Code of 1986, as amended, any corporation, Massachusetts or similar business trust, or company, not formed for the specific purpose of acquiring the Common Stock, with total assets in excess of $5,000,000;

(iv) Any director or executive officer of the Company;

(v) Any natural person whose individual net worth, or joint net worth with that person's spouse, exclusive of the value of the person's primary residence net of any mortgage debt and other liens, at the time of his or her purchase exceeds $1,000,000;

(vi) Any natural person who had an individual income in excess of $200,000, or joint income with that person's spouse in excess of $300,000, in each of the two most recent years and who reasonably expects to reach the same income level in the current year;

(vii) Any trust with total assets in excess of $5,000,000, not formed for the specific purpose of acquiring the Common Stock, whose purchase is directed by a sophisticated person as described in Rule 506(b)(2)(ii) of Regulation D;

(viii) Any entity all of whose equity owners are accredited investors;

(ix) Any entity of a type not listed in paragraphs (i), (ii), (iii), (vii), or (viii) above, not formed for the specific purpose of acquiring the securities offered, owning investments in excess of $5,000,000;

(x) Any natural person holding in good standing one or more professional certifications or designations or credentials from an accredited educational institution that the Commission has designated as qualifying an individual for accredited investor status;

(xi) Any natural person who is a "knowledgeable employee," as defined in rule 3c-5(a)(4) under the Investment Foundation Act of 1940, of the issuer of the securities being offered or sold where the issuer would be an investment company, as defined in section 3 of such act, but for the exclusion provided by either section 3(c)(1) or section 3(c)(7) of such act;

(xii) Any "family office" as defined in rule 202(a)(11)(G)-1 under the Investment Advisers Act of 1940"

a. With assets under management in excess of $5,000,000;

b. That is not formed for the specific purposes of acquiring the securities offered, and

c. Whose prospective investment is directed by a person who has such knowledge and experience in financial and business matters that such family office is capable of evaluating the merits and risks of the prospective investment; or

(xiii) Any "family client," as defined in rule 202(a)(11)(G)01 under the Investment Advisers Act of 1940, of a family office meeting the requirements in paragraph (xii) above and whose prospective investment in the issuer is directed by such family office pursuant to paragraph (xii)(c) above.

The term "net worth" means the excess of total assets over total liabilities, exclusive of the value of your primary residence net of any mortgage debt and other liens. In determining income, you should add to your adjusted gross income any amounts attributable to tax-exempt income received, losses claimed as a limited partner in any limited partnership, deductions claimed for depreciation, contributions to an IRA or Keogh retirement plan, alimony payments and any amount by which income from long-term capital gains had been reduced in arriving at adjusted gross income.

As a condition to completing a purchase of the Tokens, you will be required to represent to the Company in writing that you are an accredited investor under Regulation D, as described above, and provide certain documentation in support of such representation. See the section titled "**Regulation D Rule 506(c) Investor Verification Stands**" in this Memorandum for additional information.

Other Requirements

In addition to submitting documentation to confirm one's status as an accredited investor all potential investors of the Tokens will need to complete requisite know-your-customer and anti-money laundering procedures to purchase Tokens.

You should check the Office of Foreign Assets Control (the "OFAC") website at https://www.treas.gov/ofac before marking the following representations to the Company: You represent that the amounts paid by you in this sale of Tokens as described herein were not and are not directly or indirectly derived from any activities that contravene Federal, state or international laws and regulations, including anti-money laundering laws and regulations. Federal regulations and Executive Orders administered by the OFAC prohibit, among other things, the engagement in transactions with, and the provision of services to, certain foreign countries, territories, entities and individuals. The lists of the OFAC-prohibited countries, territories, individuals and entities can be found on the OFAC website at https://www.treas.gov/ofac. In addition, the programs administered by the OFAC (the "**OFAC Programs**") prohibit dealing with individuals or entities in certain countries, regardless of whether such individuals or entities appear on any OFAC list;

(i) you represent and warrant that none of (1): you; (2) any person controlling or controlled by you; (3) if you are a privately-held entity, any person having a beneficial interest in you; or (4) any person for whom you are acting as agent or nominee in connection with this purchase is a country, territory, entity or individual named on an OFAC list, or a person or entity prohibited under the OFAC Programs. Please be advised that the Company may not accept any purchase amounts from a prospective Purchaser if such prospective Purchaser cannot make the representation set forth in the preceding sentence. You agree to promptly notify the Company should you become aware of any change in the information set forth in any of these representations. You are advised that, by law, the Company may be obligated to "freeze the account" of any Purchaser, either by prohibiting additional purchases from it, declining any redemption requests and/or segregating the assets in the account in compliance with governmental regulations, and that the Company may also be required to report such action and to disclose such Purchaser's identity to the OFAC;

(ii) you represent and warrant that none of: (1) you; (2) any person controlling or controlled by you; (3) if you are a privately-held entity, any person having a beneficial interest in you; or (4) any person for whom you are acting as agent or nominee in connection with this purchase is a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure, as such terms are defined in the footnotes below; and

(iii) if you are affiliated with a non-U.S. banking institution (a "**Foreign Bank**"), or if you receive deposits from, make payments on behalf of, or handle other financial transactions related to a Foreign Bank, you represent and warrant to the Company that: (1) the Foreign Bank has a fixed address, and not solely an electronic address, in a country in which the Foreign Bank is authorized to conduct banking activities; (2) the Foreign Bank maintains operating records related to its banking activities; (3) the Foreign Bank is subject to inspection by the banking authority that licensed the Foreign Bank to conduct its banking activities; and (4) the Foreign Bank does not provide banking services to any other Foreign Bank that does not have a physical presence in any country and that is not a regulated affiliate.

The Company is entitled to rely upon the accuracy of each of your representations. The Company may, but under no circumstances shall it be obligated to, require additional evidence that a prospective investor meets the standards set forth above at any time prior to its acceptance of a prospective investor's purchase. You are not obligated to supply any information so requested by the Company, but the Company may reject a purchase from you or any person who fails to supply such information. In addition, if at any time after

completion of the sale of the Tokens the representations concerning Purchaser's compliance with the OFAC Programs becomes untrue, the Company may be required to take certain actions, including refusal to deliver the Tokens after Listing and reporting the transaction(s) to the relevant governmental authorities.

ODB

ODB provides hosting and operational services for the Offering. ODB's connection to the offering is solely for the limited purposes of acting as a third-party service provider. ODB and its affiliates do not provide tax, accounting or legal advice — all recipients are advised to consult with their own advisers. Neither ODB nor its affiliates have investigated (nor have any of its affiliates investigated) the desirability or advisability of participation in this offering or the securities offered herein. ODB and its affiliates make no representations, warranties, endorsements, or judgment on the merits of the offering or the securities offered herein.

Delivery of Tokens

On the Token Integration Event, the Tokens will be minted and delivered to Purchasers according to the terms specific to their TPA. The Tokens will be delivered to either a wallet address provided upon contribution or will be made available by other means as agreed upon among the Company, ODB, and the applicable Purchaser.

Transfer Restrictions

The Company's governance documents and the TPA place restrictions (or outright prohibition) on the transfer of the Tokens. Only accredited investors that can tolerate an illiquid investment should invest in the Tokens.

Prior Offerings

The Company has entered into prior sales agreements with various investors for Tokens. Such agreements may include confidentiality, non-use and/or non-disclosure obligations.

NOTICE TO PURCHASERS

This Offering has not been registered or qualified under the securities laws of any jurisdiction anywhere in the world. The Tokens, if issued, are being offered and sold only in jurisdictions where such registration or qualification is not required, including pursuant to applicable exemptions that generally limit the Purchasers who are eligible to purchase the Tokens, if issued, and that restrict the Tokens' resale. **The Tokens delivered may not be offered, sold, assigned, transferred, pledged, encumbered, or otherwise disposed of except as permitted under applicable securities laws and the additional restrictions imposed on the Tokens hereunder. In addition, holders of Tokens will not be able to transfer their Tokens until such Tokens have been released from any delivery restrictions to which they are subject.**

Procedures for Subscribing

We plan to market this Offering to potential Purchasers through the Republic Platform. We will hold a closing after ODB has received notification that the terms have been met. We generally will close on proceeds based upon the order in which they are received but reserve the right to accept or reject any purchase. We will consider various factors in determining the timing of any additional closings.

Closing Requirements

In order to complete the closing process in this Offering, each Purchaser will be required to complete such Closing Requirements as may be requested by ODB on behalf of the Company, which may include, without limitation: (1) the execution and delivery of a Token Purchase Agreement; (2) completion of investor qualification requirements (lack of status as an accredited investor under Regulation D and KYC/AML or KYB (if applicable)) screening requirements; (3) clearance from ODB's regulation best interest requirements, and (4) confirmation by ODB of receipt of funds, if applicable.

Notice Concerning the Securities Act

The Tokens have not been registered under the Securities Act or any securities laws of any state, and unless so registered, the Tokens may not be offered or sold except pursuant to an exemption from, or in a transaction not subject to, the registration requirements of the Securities Act or such other applicable securities laws. Accordingly, the Tokens are being initially offered and sold only to (1) "accredited investors" (as defined under Regulation D), in each case, in a private transaction in reliance on, and in compliance with, the exemption from the registration requirements of the Securities Act provided by Rule 506(c) of Regulation D under the Securities Act, and (2) non-U.S. persons outside the United States in offshore transactions in reliance upon Regulation S under the Securities Act.

As used herein, the terms "United States", "U.S. person" and "offshore transactions" have the meanings given to them in Regulation S under the Securities Act.

Representations and Warranties of Purchasers

In addition to the representations, warranties, and covenants in the TPA, each investor that executes a TPA will also be deemed to have acknowledged, represented, and warranted to, and agreed with, the Company as follows:

(1) It understands and acknowledges that (i) the Tokens, has not been and will not be registered under the Securities Act or any other applicable securities law, unless required by applicable law, (ii) the Tokens are being offered for sale in transactions not requiring registration under the Securities Act

or any other applicable U.S. state securities law, (iii) the Tokens, if issued, will be issued in transactions not requiring registration under the Securities Act or any other applicable U.S. state securities law, (iv) the TPA's are non-transferable and may not be offered, sold, assigned, transferred, pledged, encumbered or otherwise disposed of, unless so authorized, and (v) the Tokens may not be offered, sold or otherwise transferred or disposed of, except in compliance with the registration requirements of the Securities Act and any other applicable securities law, or pursuant to an exemption therefrom and, in compliance with the conditions for transfer set forth in paragraphs (5) and (9) below.

(2) It acknowledges that this Memorandum relates to an offering that is exempt from registration under the Securities Act and may not comply in important respects with SEC rules that would apply to an offering document relating to a public offering of securities.

(3) Purchaser must acknowledge that it is an "accredited investor" (as defined in Regulation D) acquiring the TPA, and it is aware that the TPA and the Tokens, when issued, are being issued in reliance on an exemption from the registration requirements of the Securities Act.

(4) It acknowledges that the execution of a TPA is also the purchase of Tokens, if, as, and when they are issued.

(5) In addition to all applicable transfer restrictions under applicable securities laws, it acknowledges and agrees that: (i) holders of the TPA's may never offer, sell, assign, transfer, pledge, encumber, or otherwise dispose of the TPA and (ii) the Tokens may not be offered, sold, assigned, transferred, pledged, encumbered or otherwise disposed of until such time as the Company (A) designates or creates a Designated Exchange and notifies tokenholders thereof or (B) notifies tokenholders that peer-to-peer transfers will be permitted and provides holders with the requirements and conditions to effect peer-to-peer transfers.

(6) It acknowledges that neither the Company, nor any of its representatives or affiliates, have made any statement, representation, or warranty, express or implied, to it other than the information contained in this Memorandum, which has been delivered to it and upon which it is solely relying in making its decision with respect to the Tokens. It has had access to such financial and other information concerning the Company and the Tokens as it has deemed necessary in connection with its decision to participate in the Offering, including an opportunity to ask questions of and request information from the Company, and such information has been made available to it.

(7) It is the Tokens, when issued, for its own account, or for one or more Purchaser accounts for which it is acting as a fiduciary or agent, in each case for investment, and not with a view to, or for offer or sale in connection with, any distribution thereof in violation of the Securities Act or any other applicable securities laws, subject to any requirement of law that the disposition of its property or the property of such Purchaser account or accounts be at all times within its or their control and subject to its or their ability to resell the Tokens, when issued, pursuant to Rule 144A if applicable, Section 4(a)(6), Regulation S, or any other exemption from registration available under the Securities Act, in each case, subject to the conditions set forth in (9).

(8) Each holder of the Tokens acknowledges that the Company is not making any representations as to the availability of Securities Act Rule 144 if applicable for resale of the Tokens, when issued.

(9) Each holder of a TPA acknowledges that:

The TPA will contain a legend substantially to the following effect:

> THIS SECURITY AND ANY TOKENS WHEN ISSUED PURSUANT TO IT (THE "**TOKENS**"), HAVE NOT BEEN AND WILL NOT BE REGISTERED UNDER THE SECURITIES ACT OF 1933, AS AMENDED (THE "***SECURITIES ACT***"), OR THE SECURITIES LAWS OF ANY STATE OR OTHER JURISDICTION. NEITHER THIS SECURITY, NOR ANY INTEREST OR PARTICIPATION HEREIN, MAY BE OFFERED, SOLD, ASSIGNED, TRANSFERRED, PLEDGED, ENCUMBERED OR OTHERWISE DISPOSED OF UNDER ANY CIRCUMSTANCES. EACH HOLDER OF THIS SECURITY, BY ITS ACCEPTANCE HEREOF REPRESENTS THAT (A) IT IS AN "ACCREDITED INVESTOR" (AS DEFINED IN REGULATION D UNDER THE SECURITIES ACT) OR (B) IT IS NOT A "U.S. PERSON" AND IS ACQUIRING THIS SECURITY IN AN OFFSHORE TRANSACTION WITHIN THE MEANING OF REGULATION S UNDER THE SECURITIES ACT AND IN ACCORDANCE WITH THE LAWS APPLICABLE TO IT IN THE JURISDICTION IN WHICH SUCH ACQUISITION IS MADE.
>
> HEDGING TRANSACTIONS INVOLVING THE TOKENS MAY NOT BE CONDUCTED UNLESS IN COMPLIANCE WITH THE SECURITIES ACT.
>
> **REGULATION D ONLY** (THE "**REGULATION D LEGEND**"): THE HOLDER OF ANY TOKENS AGREES TO OFFER, SELL OR OTHERWISE TRANSFER SUCH TOKENS ONLY IN COMPLIANCE WITH THE SECURITIES LAWS, INCLUDING, WHERE APPLICABLE, (A) PURSUANT TO SECURITIES ACT RULE 144, (B) PURSUANT TO A COMPLIANT REGULATION S RESALE OR (C) PURSUANT TO A REGISTRATION STATEMENT THAT HAS BEEN DECLARED EFFECTIVE UNDER THE SECURITIES ACT, SUBJECT, IN EACH OF THE FOREGOING CASES, TO ANY REQUIREMENT OF LAW THAT THE DISPOSITION OF ITS PROPERTY OR THE PROPERTY OF SUCH PURCHASER ACCOUNT OR ACCOUNTS BE AT ALL TIMES WITHIN ITS OR THEIR CONTROL AND, IN EACH CASE, IN COMPLIANCE WITH APPLICABLE SECURITIES LAWS, INCLUDING SECURITIES LAWS OF ANY U.S. STATE OR ANY OTHER APPLICABLE JURISDICTION.
>
> THE HOLDER OF THIS TPA BY ITS ACCEPTANCE WILL BE DEEMED TO HAVE REPRESENTED AND WARRANTED THAT EITHER (1) NO PORTION OF THE ASSETS USED BY SUCH HOLDER TO ACQUIRE OR HOLD THE TOKEN OR INTERESTS CONSTITUTES THE ASSETS OF AN EMPLOYEE BENEFIT PLAN THAT IS SUBJECT TO TITLE I OF THE U.S. EMPLOYEE RETIREMENT INCOME SECURITY ACT OF 1974, AS AMENDED ("**ERISA**"), A PLAN TO WHICH SECTION 4975 OF THE U.S.

INTERNAL REVENUE CODE OF 1986, AS AMENDED (THE "**CODE**") APPLIES (INCLUDING AN INDIVIDUAL RETIREMENT ACCOUNT), AN ENTITY WHOSE UNDERLYING ASSETS ARE CONSIDERED TO INCLUDE PLAN ASSETS OF ANY SUCH EMPLOYEE BENEFIT PLAN, OR PLAN, A GOVERNMENTAL PLAN (AS DEFINED IN SECTION 3(32) OF ERISA), A CHURCH PLAN (AS DEFINED IN SECTION 3(33) OF ERISA) THAT HAS NOT MADE AN ELECTION UNDER SECTION 410(D) OF THE CODE, OR A NON-U.S. PLAN, OR (2)(A) THE HOLDER IS, OR IS USING, THE ASSETS OF A GOVERNMENTAL PLAN, A CHURCH PLAN THAT HAS NOT MADE AN ELECTION UNDER SECTION 410(D) OF THE CODE, OR A NON-U.S. PLAN AND (B) THE ACQUISITION AND HOLDING OF THE TOKEN OR INTEREST WILL NOT CONSTITUTE A VIOLATION UNDER ANY APPLICABLE PROVISIONS UNDER ANY FEDERAL, STATE, LOCAL, NON-U.S. OR OTHER LAWS OR REGULATIONS THAT REGULATE SUCH PLAN'S INVESTMENTS.

Each Purchaser of a TPA acknowledges, such Purchaser agrees to be bound by the legends set forth in this paragraph (9) notwithstanding any differences appearing in the legend appearing on the TPA previously delivered to such Purchaser. The legends set forth in this paragraph (9) shall be deemed to be set forth on any such TPA delivered prior to the date of this Memorandum.

(10) It agrees that it will not transfer Tokens unless it is given reasonable assurance that each person to whom it transfers Tokens receives notice of any restrictions on transfer of such Tokens.

(11) If it is an acquirer in a transaction that occurs outside the United States within the meaning of Regulation S, it acknowledges that until the expiration of the Distribution Compliance Period (as defined in Regulation S under the Securities Act), any offer or sale of the Tokens within the United States or to a U.S. Person by a dealer (whether or not participating in the offering) may violate the registration requirements of the Securities Act.

(12) It acknowledges that the Company or its transfer agent, for the Tokens will not be required to accept for registration of transfer any Tokens, except upon presentation of evidence (including an opinion of counsel) satisfactory to the Company and the Transfer Agent, that the restrictions set out therein have been complied with.

(13) It understands that no action has been taken in any jurisdiction in the U.S. or elsewhere by the Company that would result in a public offering of the Tokens or the possession, circulation or distribution of this Memorandum or any other material relating to the Company or the Tokens in any jurisdiction where action for such purpose is required. Consequently, any transfer of the Tokens will be subject to the transfer restrictions set forth under this "Notice to Purchasers."

(14) It (a) is able to act on its own behalf in the transactions contemplated by this Memorandum, (b) has such knowledge and experience in financial and business matters as to be capable of evaluating the merits and risks of its prospective purchase of the securities and (c) (or the account for which it is acting as a fiduciary or agent) has the ability to bear the economic risks of its prospective purchase of the Tokens, and can afford the complete loss of such purchase.

(15) It acknowledges that the Company will rely upon the truth and accuracy of the acknowledgements, representations, warranties, and agreements set forth in this "Notice to Purchasers" section and agrees that,

if any acknowledgements, representations, warranties, and agreements deemed to have been made by its participation in the Offering are no longer accurate, it will promptly notify the Company.

(16) If it is acquiring the Tokens as a fiduciary or agent for one or more Purchaser accounts, it represents that it has sole investment discretion with respect to each such account and that it has full power to make the acknowledgements, representations, warranties, and agreements set forth in this "Notice to Purchasers" section on behalf of each such Purchaser account.

(17) Either (i) the Purchaser is not acquiring or holding such Tokens or an interest therein with the assets of (A) an employee benefit plan that is subject to Part 4 of Subtitle B of Title I of ERISA, (B) a "plan" to which Section 4975 of the Code applies (including an individual retirement account), (C) an entity deemed to hold "plan assets" of any of the foregoing by reason of an employee benefit plans or plan's investment in such entity, (D) a governmental plan (as defined in Section 3(32) of ERISA), (E) a church plan (as defined in Section 3(33) of ERISA) that has not made an election under Section 410(d) of the Code, or (F) a non-U.S. plan, or (ii) the Purchaser is acquiring or holding such securities or an interest therein with the assets of (A) a governmental plan, a church plan that has not made an election under Section 410(d) of the Code, or a non-U.S. plan and (B) the acquisition and holding of such securities by the Purchaser, throughout the period that it holds the securities and the disposition of such securities or an interest therein will not constitute or result in a violation of any provisions of any applicable United States federal, state or local laws or non-U.S. laws that regulate such plan's investments.

Limitation of Liability and Indemnification

To the fullest extent permitted by applicable law, (i) in no event will the Company be liable for any indirect, special, incidental, consequential, or exemplary damages of any kind (including, but not limited to, where related to loss of revenue, income or profits, loss of use or data, or damages for business interruption) arising out of or in any way related to this Memorandum, TPAs, or Tokens, regardless of the form of action, whether based in contract, tort, or any other legal or equitable claim (even if the party has been advised of the possibility of such damages and regardless of whether such damages were foreseeable); and (ii) in no event will the liability of the Company, whether in contract, tort, or other legal or equitable claim, arising out of or relating to this Memorandum, Tokens exceed the amount the Purchaser pays to the Company hereunder. The Company shall not be liable or responsible to the Purchaser, not be deemed to have defaulted under or breached this Memorandum, for any failure or delay in fulfilling or performing any provision of this Memorandum, including without limitation, and delivering the Tokens.

Company directors and officers have or will have effective indemnification by the Company against any liability incurred by such directors and officers in connection with any negligence, breach of duty, or breach of trust arising out of their performance as directors and officers of the Company.

Insofar as indemnification for liabilities arising under the Securities Act may be permitted to the president, directors, officers, and controlling persons of the Company pursuant to the foregoing provisions, or otherwise, the Company has been advised that in the opinion of the SEC, such indemnification is against public policy as expressed in the Securities Act and may, therefore, be unenforceable. In the event that a claim for indemnification against such liabilities (other than the payment by the Company of expenses incurred or paid by a president, director, officer, or controlling person of the registrant in the successful defense of any action, suit or proceeding) is asserted by such president, director, officer, or controlling person in connection with the interests being offered, the Company will, unless in the opinion of its counsel the matter has been settled by controlling precedent, submit to a court of appropriate jurisdiction the question whether such indemnification by it is against public policy as expressed in the Act and will be governed by the final adjudication of such issue. We believe that these provisions and agreements are necessary to attract and retain qualified persons as our president, board members, officers, and directors.

At present, there is no pending litigation or proceeding involving our president, directors, or officers for whom indemnification is required or permitted, and we are not aware of any threatened litigation or proceeding that may result in a claim for indemnification.

The Company has agreed to indemnify ODB against liabilities relating to any investigation, claim, or proceeding stemming from the Offering, liabilities arising from breaches of some or all of the representations and warranties contained in the Engagement Agreement, and to contribute to payments that ODB may be required to make for these liabilities.

ODB and their respective affiliates are engaged in various activities, which may include securities trading, commercial and investment banking, financial advisory, investment management, investment research, principal investment, hedging, financing and brokerage activities. ODB and their respective affiliates may in the future perform various financial advisory and investment banking services for us, for which they received or will receive customary fees and expenses.

Potential Conflicts of Interest

This Memorandum does not purport to identify all conflicts of interest. ODB or its affiliates, from time to time, may enter into other transactions not specifically described in this Memorandum with affiliates, officers, managers, members, employees, agents and representatives.

Amounts earned by ODB, including but not limited to success-based commissions, placement fees, and closing fees will be retained by ODB. This includes the administrative fee ODB charges to the purchase at checkout.

TAX CONSIDERATIONS

EACH PURCHASER SHOULD SEEK, AND MUST DEPEND UPON, THE ADVICE OF HIS OR HER TAX ADVISOR WITH RESPECT TO THEIR RECEIPT OF TOKENS, AND EACH PURCHASER IS RESPONSIBLE FOR THE FEES OF SUCH ADVISOR. NOTHING IN THIS PRIVATE PLACEMENT MEMORANDUM IS OR SHOULD BE CONSTRUED AS LEGAL OR TAX ADVICE TO A PURCHASER. PURCHASERS SHOULD BE AWARE THAT THE INTERNAL REVENUE SERVICE MAY NOT AGREE WITH ALL TAX POSITIONS TAKEN BY US AND THAT CHANGES TO THE INTERNAL REVENUE CODE OR THE REGULATIONS OR RULINGS THEREUNDER OR COURT DECISIONS AFTER THE DATE OF THIS PRIVATE PLACEMENT MEMORANDUM MAY CHANGE THE ANTICIPATED TAX TREATMENT TO A PURCHASER. WE WILL NOT OBTAIN ANY RULING FROM THE INTERNAL REVENUE SERVICE WITH REGARD TO THE TAX CONSEQUENCES OF THE RECEIPT OF OR A PURCHASE OF TOKENS.

THE TAX TREATMENT OF TOKENS IS UNCERTAIN AND THERE MAY BE ADVERSE TAX CONSEQUENCES FOR THE COMPANY, ITS AFFILIATES, AND/OR PURCHASERS UPON CERTAIN FUTURE EVENTS. THE ISSUANCE OF TOKENS MAY RESULT IN ADVERSE TAX CONSEQUENCES TO PURCHASERS, INCLUDING WITHHOLDING TAXES, INCOME TAXES AND TAX REPORTING REQUIREMENTS. EACH PURCHASER SHOULD CONSULT WITH AND MUST RELY UPON THE ADVICE OF ITS OWN PROFESSIONAL TAX ADVISORS WITH RESPECT TO THE UNITED STATES AND NON-U.S. TAX TREATMENT OF THE RECEIPT OF AND A PURCHASE OF TOKENS.

INVESTOR VERIFICATION STANDARDS IN RULE 506(C) OF REGULATION D

In purchasing securities through this Offering, the Company is obligated to verify your status as an accredited investor in accordance with Rule 501 of Regulation D. There are three primary methods the Company may employ to comply with the verification standards. Purchasers in this Offering will need to provide the Company with verification that meets the standards and form using one or multiple methods, including, but not limited to:

Income: The Company may verify an individual's status as an accredited investor on the basis of income by reviewing copies of any IRS form that reports net income, such as Forms W-2 or 1099 (which are typically filed by an employer or other third party payor), or Forms 1040 filed by the Purchaser (with non-relevant information permitted to be redacted). Under this method, the Company must review IRS forms for the two most recent years and obtain a written representation from the prospective Purchaser that he or she has a reasonable expectation of attaining the necessary income level for the current year. Where accredited investor status is based on joint income with the person's spouse, the IRS forms and representation must be provided with respect to both the Purchaser and the spouse.

Net Worth: Under this method, the Company will need to review bank or brokerage statements or third-party appraisal reports to verify the Purchaser's assets and a credit report to verify liabilities, in each case dated within the prior three months, and will need to obtain a written representation from the prospective Purchaser that all liabilities have been disclosed. Where accredited investor status is based on joint net worth with the person's spouse, the asset and liability documentation and representation must be provided with respect to both the Purchaser and the spouse.

Reliance on Determination by Specified Third Parties: The Company may satisfy the verification requirement if it obtains a written confirmation from a registered broker-dealer, a registered investment adviser, a licensed attorney, or a certified public accountant that within the prior three months such person or entity has taken reasonable steps to verify that the Purchaser is an accredited investor and has determined that the Purchaser is an accredited investor. Proper verification must be submitted with your purchase for interests in order for the Company to verify your suitability for investment and accept your purchase.

RISK FACTORS

*A purchase of Tokens involves a high degree of risk, including the risk of a total loss of principal, volatility and illiquidity. A prospective investor should thoroughly review the confidential information contained in this Memorandum and the terms of the applicable Offering Documents, and carefully consider whether a purchase of the Tokens or receipt of Tokens is suitable to such prospective investor's financial condition and goals. The following risks entail circumstances under which the Platform, the Tokens, and their related operations and prospects could suffer. They may also be harmed by additional risks and uncertainties not currently known or that we currently do not believe to be material. See "**Risk Factors**" below.*

UNLESS EXPRESSLY SET OUT HEREIN, THE COMPANY SPECIFICALLY DOES NOT REPRESENT AND WARRANT AND EXPRESSLY DISCLAIMS ANY REPRESENTATION OR WARRANTY WITH RESPECT TO THE INFORMATION MATERIALS, THE TOKENS, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY REPRESENTATIONS OR WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, USAGE, SUITABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, OR AS TO THE WORKMANSHIP OR TECHNICAL CODING THEREOF, OR THE ABSENCE OF ANY DEFECTS THEREIN, WHETHER LATENT OR PATENT. THE COMPANY DOES NOT REPRESENT OR WARRANT THAT TOKENS ARE RELIABLE, CURRENT, OR ERROR-FREE, MEET YOUR REQUIREMENTS, OR THAT DEFECTS IN THE TOKENS WILL BE CORRECTED. THE COMPANY CANNOT AND DOES NOT REPRESENT OR WARRANT THAT TOKENS OR THE DELIVERY MECHANISM FOR THE TOKENS IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS.

A significant amount of further work may be required in order for the Company to integrate the Tokens into the Platform and much of that work may be subject to regulatory approval and otherwise reliant on the input or consent of other persons not under the control of the Company. The success of the Tokens is reliant upon the Company (i) raising sufficient resources to fund the ongoing development of the Tokens; and (ii) complying with ongoing funding, reserve and/or regulatory requirements (as relevant) related to the proposed creation and operation of the Tokens (collectively, the "**Regulatory and Funding Requirements**").

There is a significant risk that the Tokens are not developed as envisaged herein. The Company, in the sole and absolute discretion of the Company's governing board or committee (the "**Committee**"), reserves the right to modify, extend, reduce, eliminate, add and/or substitute the scale, scope, business lines, operations, and any other characteristics of the Tokens in order to address any actual or perceived commercial, legal, regulatory or other matters that the Committee, in its sole and absolute discretion, considers relevant at any time.

The Company may issue Tokens even if there are material changes to the scale, scope, business lines, operations, and any other characteristics of the Tokens or the Platform or if the Company or its affiliates have not satisfied (or are unlikely to satisfy) any regulatory and funding requirements or any other regulatory, commercial or legal requirements with respect to the Tokens. No promises of future performance or value are or will be made with respect to the Tokens, including no promise of inherent value, no promise of continuing payments, and no guarantee that the Tokens will hold any particular value.

The Company is developing the Tokens to be used with respect to the Platform. Subject to applicable law and the cautionary statements and risk factors contained in this Memorandum, upon the Token Integration Event, the Platform will accept any duly presented Tokens in exchange for privileges and other benefits related to such Tokens from time to time on the Platform.

The precise terms of the privileges and other benefits of the Tokens will be determined by the Company as the owner of the Platform in its sole and absolute discretion from time to time. Such privileges and benefits

will initially be determined by such person on or around the Token Integration Event and may be amended thereafter at any time and without notice to, or consent from, any holder of Tokens. Any such determination or amendment shall not be a breach of the terms of this Offering.

The Tokens are provided on an "as is" and "as available" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the Token is free of defects, vulnerabilities, merchantable, fit for a particular purpose or non-infringing. Any use of the Tokens shall be at your own risk. In no event shall the Company be held liable in connection with or for any claims, losses, damages, or other liabilities, whether in contract, tort, or otherwise, arising out of or in connection with the Tokens or its operation or use or be under any obligation to support, develop or otherwise maintain or promote the use of the Platform or the integration of the Tokens into the Platform.

While the Tokens are available only to qualified investors, there is the possibility that Tokens could be acquired over time or following changes in the regulatory landscape by persons in other jurisdictions currently restricted from acquiring Tokens and, accordingly, the risk factors set out below may include certain risk factors specific to certain jurisdictions even though the Company will not at present make the Tokens available at this time to persons from such jurisdictions.

BY PARTICIPATING IN ANY ACQUISITION OF TOKENS, YOU EXPRESSLY ACKNOWLEDGE AND ASSUME ALL RISKS RELATED THERETO INCLUDING (WITHOUT LIMITATION) THE RISKS SET OUT BELOW.

GENERAL RISK FACTORS

We may fail to implement our business plan.

We have a short operations record on which you can evaluate our business and prospects. Our prospects must be considered in light of the risks, uncertainties, expenses, and difficulties frequently encountered by companies in their early stages of development. These risks include, without limitation, competition, lack of brand and/or name recognition, product obsolescence or inventory loss, theft or destruction, limited access to additional sales and management talent, and limited access to software and technology development experts, among other factors. We cannot guarantee that we will be successful in executing our business plan, and we may then be forced to cease operations, in which case you may lose your entire investment.

Investor Status and Claims Risk

Investors in the Tokens will not acquire any equity, debt, or other ownership interest in the Company or its affiliates. Holding Tokens does not confer any right to vote, receive dividends, participate in profits, or claim any assets of the Company. Investors should not expect to have any recourse against the Company, its officers, directors, or affiliates for any losses incurred in connection with the Tokens.

There can be no assurance that the Company's business plan will be profitable, and there is no assurance of any returns.

The expenses we incur to expand the business could result in operating losses for the foreseeable future. There is no assurance that we will ever have net income sufficient to cover our expenses. No assurance can be made that any investor will not lose his, her or its entire investment.

As we have a limited operating history, we are subject to business development risks.

The Company has only a limited history upon which an evaluation of its prospects and future performance can be made. Our proposed operations are subject to all business risks associated with new enterprises. The likelihood of the Company's success must be considered in light of the problems, expenses, difficulties,

complications, and delays frequently encountered in connection with the expansion of a business, operation in a competitive industry, and the continued development of advertising, promotions and a corresponding customer base. There is a possibility that the Company could sustain losses in the future. There can be no assurance that our efforts will result in continued successful commercialization or further development of our operations, that our marketing efforts will be successful, or that we will ever achieve significantly higher revenues. Failure to do so could result in investors losing part or all of their money invested.

Our advisors and management have other business interests and obligations to other entities, some of which may conflict with their responsibilities to the Company.

Members of our management and other advisors of the Company may provide services to us on a non-exclusive basis. Such persons are required to provide us with such amount of their time and efforts as they deem necessary to run the business and operations of the Company in a reasonable manner. We are dependent on our team to successfully execute our business plan. Their other business interests and activities could divert time and attention from operating our business. We cannot assure you that some or all of such persons will be able to provide the Company with a sufficient amount of their time or efforts to take advantage of all opportunities that may be available to the Company. Moreover, some of the other entities in which such persons have a material financial interest may enter into agreements with the Company in which there is a potential conflict of interest.

Key man risk and the risk that we may be unable to retain experienced management and personnel could impair our ability to execute on our business strategy and growth plan. Although we intend to recruit additional talent over time, competition for qualified personnel is intense and there can be no assurance that we will be able to retain our personnel or attract additional qualified personnel. We also rely on consultants for systems, software and technology development that we believe are a critical part of our growth strategy as well as our finance functions. We may not be able to continue to attract or retain qualified personnel in the future, and the loss of key members of our team would have a material adverse effect on our business. Any inability to fill vacancies in our management team on a timely basis could impair our ability to implement our business strategy, which would harm our business, results of operations, and the value of your investment.

The Company may engage in business transactions with companies affiliated with one or more members of the management team.

The Company may engage in business transactions with businesses that are affiliated with one or more of the members of the Company's management team. Any such business transactions may or may not be the result of arms-length negotiations and could result in potential conflicts of interest.

We cannot assure you that we will be able to forge and maintain required beneficial relationships with third parties.

We are generally dependent on relationships with strategic partners and vendors, and we may enter into future potential strategic alliances. Our success requires that we secure and maintain beneficial third party relationships. There can be no assurance that such third parties may regard their relationship with us as important to their own business and operations, that they will not reassess their commitment to the business at any time in the future, or that they will not develop their own competitive services or products, either during their relationship with us or after it expires. Accordingly, there can be no assurance that our existing relationships or future relationships will result in sustained business partnerships, successful service offerings, or significant revenues for us.

We may incur business disruptions.

We take measures to reduce the risks of disruptions at our facilities. However, the occurrence of a natural disaster, such as a hurricane, tropical storm, earthquake, tornado, flood, fire, or other unanticipated problems, such as illness of any member of our management or any other employee, contractor or advisor, labor difficulties (including work stoppages or strikes), vendor shortages, equipment failure or unscheduled maintenance, could cause operational disruptions and could materially adversely affect our business, earnings and cash flows. Any losses due to these events may not be covered by our existing insurance policies or may be subject to certain deductibles.

Rapid growth may strain our resources.

Significant and rapid growth in the scope and complexity of our business would place a significant strain on our management team and our financial and other resources. Such growth, if experienced, may expose us to greater costs and other risks associated with growth and expansion. We may be required to hire a broader range of additional employees and outsource certain functions to contractors in order to sustain our operations. We may be unsuccessful in these efforts, or we may be unable to project accurately the rate or timing of these increases. Our ability to manage our growth effectively will require us to continue to improve our operations, to improve our financial and management information systems, and to train, motivate, and manage our future employees. The failure to develop and implement effective systems, or to hire and retain sufficient personnel for the performance of all of the functions necessary to effectively service and manage our business, or the failure to otherwise manage growth effectively, could have a materially adverse effect on our business, financial condition, and results of operations. In addition, difficulties in effectively managing the budgeting, forecasting, and other process control issues presented by such a rapid expansion could result in our inability to maintain quality standards or otherwise harm our business, financial condition, and results of operations.

Our risk management efforts may not be effective which could result in unforeseen losses.

We could incur substantial losses and our business operations could be disrupted if we are unable to effectively identify, manage, monitor, and mitigate financial risks, such as credit risk, interest rate risk, prepayment risk, liquidity risk, regulatory risk, and other market-related risks, as well as operational risks related to our business, assets and liabilities. Our risk management policies, procedures, and techniques may not be sufficient to identify all of the risks to which we may be exposed, mitigate the risks that we have identified or identify additional risks to which we may be subject in the future.

The Company may require additional capital to support its business objectives, and this capital might not be available on acceptable terms, or at all.

At any time, the Company may accept funds from additional lenders, investors, and others to support the growth of its business. Accordingly, it is expected that we will need to engage in additional debt and equity-based financings to secure additional funds. Financial market disruption, the ability to attract business partners and clients, the ability to identify and attract financiers, and general economic conditions in which the credit markets are severely constrained may make it difficult for us to obtain additional financing on terms favorable to us, if at all. Any debt financing secured by us in the future could involve restrictive covenants relating to our capital raising activities and other financial and operational matters, which may make it more difficult for us to obtain additional capital and to pursue business opportunities. If we are unable to obtain adequate financing, or financing on terms satisfactory to us, when we require it, our ability to continue to support the growth of our business and to respond to business challenges could be significantly impaired. If we are unsuccessful in raising capital when needed, you could lose your entire investment. Any issuance of equity will dilute the ownership stake of current equity investors.

General tax risks.

Items of income and loss will be determined by the Company's management in consultation with the Company's tax advisors. Adjustments, if any, resulting from any audit of the Company, should the Company ever be audited, might result in corresponding adjustments of Company items of income and loss reflected on your own tax returns. In addition, the Company's management has primary responsibility for Company level matters involving the Company's taxation, including the power to extend the statute of limitations for all persons holding an interest in the Company, including, without limitation, you, as to Company items of income and loss.

It may be difficult to enforce a U.S. judgment against us, our officers and directors, or to assert U.S. securities laws claims or serve process on our officers and directors.

We are incorporated in Switzerland. Most of our assets are located outside the United States. Therefore, it may be difficult to enforce a U.S. court judgment based upon the civil liability provisions of the U.S. federal securities laws against us or any of these persons in a U.S. or Swiss court, or to affect service of process upon these persons in the United States.

Additionally, it may be difficult for an investor, or any other person or entity, to assert U.S. securities law claims in original actions instituted in Switzerland. This is for two principal reasons: 1) because the Swiss courts may regard the U.S. law in question to be a penal, revenue or public law and therefore, under Switzerland, not capable of direct or indirect enforcement in the Swiss courts, or 2) because the Swiss court may stay the claim on the grounds Switzerland is not an appropriate forum. If U.S. law is found to be applicable to a claim which the Swiss court can and is prepared to hear, the content of applicable U.S. law must be proved as a fact by expert witnesses, which can be a time-consuming and costly process. If proceedings were to be brought in Switzerland, all procedural matters would be governed by Switzerland. There is little case law addressing the matters described above that would be binding case law in a Swiss court. As a result, an investor may lose its entire investment.

Jurisdiction and Enforcement Risk

The Company is incorporated in Switzerland and conducts the majority of its operations outside the United States. As a result, it may be difficult or impossible for investors to enforce U.S. legal rights or judgments against the Company, its officers, directors, or affiliates. Investors may have limited or no recourse in any jurisdiction and could lose their entire investment.

The Company's ability to succeed depends on the Company's ability to grow.

The introduction of new products and services and expansion of the Company's customer base will contribute significantly to the Company's operational results. The Company's future operational success will depend on a number of factors, including, but not limited to:

- The Company's ability to manage costs;
- The level of competition in the Company's industry;
- The Company's ability to provide efficient, timely and cost-effective products and services;
- The efficiency and effectiveness of the Company's sales and marketing efforts in signing up new customers, expanding business with existing customers, and building product, services and brand awareness;
- The level of consumer acceptance of the Company's products and services; and
- General economic conditions and consumer confidence.

The Company may not be successful in executing its growth strategy. Failure to successfully execute any material part of the Company's growth strategy would significantly impair the Company's future growth and its ability to attract and sustain investments in the Company's business.

RISK FACTORS RELATED TO THE SECURITIES BEING OFFERED

Risk of an illiquid market for Tokens.

There may never be any marketplace for Tokens. There are currently no exchanges upon which the Tokens would trade. If exchanges do develop, they will likely be relatively new and subject to poorly understood regulatory oversight. They may, therefore, be more exposed to fraud and failure than established, regulated exchanges for other products and have a negative impact on the Tokens. To the extent that any third party ascribes an external exchange value to Tokens (e.g., as denominated in a crypto or fiat currency), such value may be extremely volatile and diminish to zero. If (despite your representations to us to the contrary) you are holding Tokens as a form of investment on a speculative basis or otherwise, or for a financial purpose, with the expectation or desire that their inherent, intrinsic or cash-equivalent value may increase with time, you assume all risks associated with such speculation or actions, and any errors associated therewith, and accept that the Tokens are not offered by the Company or its affiliates on an investment basis.

Inability to fund development or maintenance.

The Company may not be able to fund development of the Tokens in the manner that it was intended.

Risk of uninsured losses.

Unlike bank accounts or accounts at some other financial institutions, the Tokens are uninsured unless you specifically obtain private insurance to insure them. Thus, in the event of loss or loss of utility value, there is no public insurer or private insurance arranged by us, to offer recourse to you.

Risk of lack of adoption or use of the Tokens.

While the Tokens should not be viewed as an investment, they may have value over time. That value may be limited or non-existent if the Tokens lack acceptance, use, and adoption on the Platform.

Risk of dissolution of the Tokens.

It is possible that, due to any number of reasons, including development issues with the Tokens, the failure of business relationships, lack of public interest, lack of funding, or competing intellectual property claims, the Platform and/or Tokens may no longer be viable as a business or otherwise and may dissolve or fail to maintain commercial or legal viability, or be abandoned. There is no assurance that you will receive any benefits through the Tokens.

Risk of malfunction in the Tokens.

It is possible that the Tokens or the Platform malfunctions in an unfavorable way, including one that results in the loss of the Tokens.

Tax risks relating to the Tokens.

The tax characterization of the Tokens is uncertain. You must seek your own tax advice in connection with acquisition, storage, transfer and use of the Tokens, which may result in adverse tax consequences to you, including, without limitation, withholding taxes, transfer taxes, value added taxes, income taxes, capital taxes and similar taxes, levies, duties or other charges and tax reporting requirements.

The Company may be required to register as a money services business or money transmitter and to comply with the requirements of the Bank Secrecy Act and applicable state requirements.

The Bank Secrecy Act, among other things, regulates the issuance, administration and exchange of "virtual currencies." Any entity performing any of those activities may be a money services business, required to

register with the United States Treasury Department, as well as state and foreign government administrative bodies, and to engage in continued practices of "know your customer" and anti-money laundering reporting. If the Company were to be subject to Bank Secrecy Act requirements, the Company is likely on a continuing basis to require recipients of Tokens to provide certain personal information as a condition of their receipt of Tokens. In some instances, the Company could be required to prohibit transactions, thereby interfering with the activity in any marketplace that may develop for the Tokens. Additionally, the Company may be required to issue suspicious activity reports upon detecting any "suspicious" transaction. Guidance on what constitutes a suspicious transaction is unclear, and failure to comply may result in severe civil and criminal penalties. Almost all states in the United States have some form of similar regulations, each of which may require obtaining a separate license, which can be an expensive and time consuming process. Compliance with the Bank Secrecy Act and any applicable state regulations would, if required, be a continuing, material expense, which if the Company cannot afford, would result in suspension of any marketplace that the Company develops that would in turn adversely affect demand for the Tokens.

A violation of privacy or data protection laws could have a material adverse effect on the Company's activities.

A wide variety of state, national and international laws and regulations apply to the collection, use, retention, protection, disclosure, transfer and other processing of data, including personal data. These data protection and privacy-related laws and regulations are varied, evolving, can be subject to significant change, may be augmented or replaced by new or additional laws and regulations and may result in ever increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. Foreign data protection, privacy and other laws and regulations are often more restrictive than those in the United States, such as the General Data Protection Regulations, effective in the European Union. Certain states in the United States have also introduced broad rules, which may or may not anticipate and be consistent with rules expected to be adopted by the U.S. federal government. The Company expects that the cost of compliance with these laws may be high in terms of both money and attention. The Company's failure to comply with all applicable privacy and data protection laws, regulations, standards and codes of conduct could result in enforcement actions against the Company, including fines, imprisonment of Company officials and public censure, claims for damages by affected individuals, demands that the Company modify or cease existing practices, damage to the Company's reputation and loss of goodwill, any of which could have a material adverse effect on the level of demand for Tokens.

Risk of litigation and/or third-party claims.

From time to time, third parties may assert claims against the Company, its developers, and/or its underlying technology. Regardless of the merit of any legal action or claim, any action that reduces confidence in the Company's long-term viability or the ability of individuals to hold and transfer Tokens may adversely affect the Platform. Additionally, a meritorious claim could prevent developers from accessing the most up-to-date protocol code or holding or transferring their Tokens.

Risk of alternative, unofficial platforms.

Following the issuance of the Tokens, it is possible that alternative applications or platforms could be established, which use the same or similar open-source code and protocol underlying the Tokens. The Tokens may have no intrinsic value with respect to such alternative applications. The Tokens may compete with these alternative, unofficial token-based applications, which could potentially negatively impact the Tokens.

Assertions by third parties of infringement or other violation by Us of their intellectual property rights could harm our ability to develop the Platform and the Token.

Third parties may in the future assert that we have infringed, misappropriated, or otherwise violated their copyrights, patents, and other intellectual property rights, and as we face increasing competition, the possibility of intellectual property infringement claims against us grows. Various laws and regulations govern the copyright and other intellectual property rights associated with the Platform. Existing laws and regulations are evolving and subject to different interpretations, and various legislative or regulatory bodies may expand current or enact new laws or regulations. We cannot assure you that we are not infringing or violating any third-party intellectual property rights, or that we will not do so in the future. In addition, internet and technology companies are frequently subject to litigation based on allegations of infringement, misappropriation, or other violations of intellectual property rights. Many companies in these industries, including many of our competitors, have substantially larger patent and intellectual property portfolios than we do, which could make us a target for litigation as we may not be able to assert counterclaims against parties that sue us for patent, or other intellectual property infringement. By their nature, media platforms feature content protected by intellectual property laws and may be fora for the publication of content that has infringed upon the intellectual property rights of others.

It is difficult to predict whether assertions of third-party intellectual property rights or any infringement or misappropriation claims arising from such assertions will substantially harm our business, operating results, and financial condition. If we are forced to defend against any infringement or misappropriation claims, whether they are with or without merit, are settled out of court, or are determined in our favor, we may be required to expend significant time and financial resources on the defense of such claims. Furthermore, an adverse outcome of a dispute may require us to pay significant damages, which may be even greater if we are found to have willfully infringed upon a party's intellectual property; cease exploiting copyrighted content that we have previously had the ability to exploit; cease using solutions that are alleged to infringe or misappropriate the intellectual property of others; expend additional development resources to redesign our solutions; enter into potentially unfavorable royalty or license agreements in order to obtain the right to use necessary technologies, content, or materials; indemnify our partners and other third parties; and/or take other actions that may have material effects on our business, operating results, and financial condition.

Token Integration risk and risk of insufficient interest in the platform.

There are no guarantees as to the timing of the Tokens being integrated into the Platform, which is dependent on many factors, including many outside the Company's control. Further, it is possible that there will be limited public interest in the Tokens or that public interest in the Platform may reduce over time. Such a lack of interest could negatively impact the Tokens and their functionality in the Platform.

Risk that the Tokens will not meet expectations.

Any expectations or assumptions regarding the form and functionality of the Tokens (including participant behavior) held by the Company or by you may not be met, for any number of reasons, including, without limitation, mistaken assumptions or analysis, a change in the design and implementation plans, and changes in the execution of the Tokens. Moreover, the Company may not be able to retain full and effective control over how other participants will use the Platform, what products or services will be offered through the Platform by third parties, or how third-party products and services will utilize Tokens (if at all). This could create the risk that the Tokens, as further developed and maintained, may not meet your expectations. Furthermore, despite our good faith efforts, it is still possible that the integration of the Tokens into the Platform will experience malfunctions or otherwise fail to be adequately maintained, which may negatively impact the Platform and Tokens, and the potential utility of the Tokens within the Platform.

Further innovations in the crypto asset industry may cause the tokens to lose value.

The development and acceptance of the cryptographic and algorithmic protocols governing the issuance of, and transactions in, crypto assets are subject to a variety of factors that are difficult to evaluate and predict. The use of crypto assets to, among other things, transact in goods and services is part of a new and rapidly

evolving commercial practice that employs digital assets based on a computer- generated mathematical and/or cryptographic protocol. The growth of this commercial practice in general, and the use of crypto assets in particular is subject to a high degree of uncertainty. Factors affecting further development of the crypto asset industry include, among other things, the continued worldwide adoption of crypto assets; governmental and quasi-governmental regulation of crypto assets and/or crypto asset exchanges; changing consumer demographics, tastes, and preferences; sustained development and maintenance of open-source software protocols; the popularity and availability of alternative and/or new payment services; and general economic conditions. If these factors negatively affect or impede the development of the crypto asset industry, the value of holding Tokens may also be negatively affected.

Risks associated with incomplete information regarding the Tokens.

You will not have full access to all the information relevant to the Company and the Tokens. The Company is not required to update you on the progress of the Tokens. You are responsible for making your own decision in respect of the acquisition of the Tokens. The Company does not provide you with any recommendation or advice in respect of the acquisition of the Tokens. You may not rely on the Company to provide you with complete or up-to-date information.

Purchasers will not be in any fiduciary, partnership, trustee, agency, or similar relationship with the Company or any of its Affiliates and will not be owed any fiduciary duty by the Company or any of its Affiliates.

The Purchasers have no direct management, equity, voting, or similar rights in the Company or any of its affiliates. However, without limitation to the above, the Company reserves all rights with respect to pursuing any form of decentralized governance should it so determine that doing so would be in the best interests of the holders of Tokens from time to time.

In order to seek compliance with (or to seek to mitigate the impact of) any laws, statutes, ordinances, rules, regulations, judgments, injunctions, orders, treaties, administrative acts or decrees of any nation or government, any state or other political subdivision thereof, any entity exercising legislative, judicial or administrative functions of or pertaining to government, including, without limitation, any government authority, agency, department, board, commission or instrumentality, and any court, tribunal or arbitrator(s) of competent jurisdiction, and any self-regulatory organization believed by the Company or its affiliates to apply to or affect the Company or its affiliates, the Tokens, the Company may in its sole and absolute discretion take such steps as it considers necessary or convenient to comply with such matters including, without limitation, the termination of the Tokens. In addition, the Company may take such steps as it considers necessary or convenient where it believes or suspects the Tokens may be used, trafficked, or applied in the attempted furtherance of money laundering, terrorist financing, tax evasion, or other unlawful activity or where it believes the Tokens are no longer viable.

Risks Associated with Potential Public Listings of Tokens Could Negatively Impact Their Price.

The Company may, in the future, list Tokens on digital asset trading platforms. Any such listing could negatively impact the price of Tokens, especially if there is significant selling activity on any such exchange. Lockups applicable to any securities purchased in this Offering may prevent participants in this Offering from selling their stake in Tokens while such Tokens remain subject to a lock-up.

RISK FACTORS RELATED TO TOKENS, CRYPTOCURRENCY, AND OTHER DIGITAL ASSETS

Risks associated with third party contractors.

Development of the Tokens may require third-party contractors with particular expertise in blockchain technology. The availability of such contractors is limited. There may not be sufficient (or any) such

contractors available on terms deemed acceptable by the Company. The costs associated with any such contractors may be significantly greater than currently estimated. Furthermore, the quality, reliability and timely delivery of services by such contractors may vary significantly.

Risk associated with licensed third-party technology.

The Tokens are created solely for purposes of operating and integrating with the Platform.

We may invest or spend the proceeds of this Offering in ways with which you may not agree or in ways which may not yield a return.

Our management will have broad discretion in determining how the proceeds of the sale of our Tokens will be used, and you will not have the opportunity, as part of your investment decision, to assess whether the proceeds are being used appropriately. Notwithstanding our current business plan, future events including, but not limited to, the problems, expenses, difficulties, complications and delays, as well as changes in the economic climate or changes in governmental regulations, may make the reallocation of funds necessary or desirable. Any such reallocation will be at the sole discretion of the Company. If we do not use the proceeds that we receive effectively, our business, financial condition, results of operations and prospects could be harmed. Further, the sale of Tokens will require intensive computing resources. The demand for these resources may exceed the Company's estimates. Ultimately, the Company's resources may prove inadequate to support the sale of our Tokens, which may affect the distribution and/or utility of the Tokens.

No guarantee that tokens will be released.

Many factors could influence the success of the Company and the Tokens, some of which are out of the Company's control, and there can be no guarantee that the Company will ultimately be successful in deploying and delivering the Tokens. The Company may change its plans for issuing the Tokens for a variety of reasons, including a change in business plan, technological challenges, lack of perceived demand, or other reasons. Finally, if the Company ceases operations, agrees to assign its assets and liabilities to a third party for the benefit of creditors in the case of insolvency, or engages in a liquidation or winding up, it may never issue the Tokens.

Risk of losing access to tokens due to wallet incompatibility.

Your cryptocurrency wallet must be compatible and possess technical infrastructure that is compatible with the receipt, storage, and transfer of the Tokens. Non-compatible wallet addresses will not be accepted, and any attempt to transfer Tokens to a non-compatible wallet address may result in the loss of such Tokens. In addition, your wallet address must not be associated with a third-party exchange or service that has custody over the private key. The Company reserves the right to prescribe additional conditions relating to specific wallet requirements at any time, acting in its sole discretion.

Risks associated with the overarching blockchain industry in which the Platform operates.

The growth of the blockchain industry in general, is subject to a high degree of uncertainty regarding consumer adoption and long-term development. The factors affecting the further development of the cryptocurrency and crypto assets industry, as well as blockchain networks, include without limitation, the worldwide growth in the adoption and use of digital assets and other blockchain technologies; governmental and quasi-governmental regulation of digital assets and their use, or restriction on or regulation of access to and operation of blockchain networks or similar systems; the maintenance and development of the open source software protocol of blockchain networks; changes in consumer demographics and public tastes and preferences; the availability and popularity of other forms or methods of buying and selling goods and services, or trading assets including new means of using government backed currencies or existing networks; the extent to which current interest in cryptocurrencies represents a speculative "bubble"; general economic conditions in the United States and the world; the regulatory environment relating to

cryptocurrencies and blockchains; and a decline in the popularity or acceptance of cryptocurrencies or other block- based tokens. The digital assets industries as a whole have been characterized by rapid changes and innovations and are constantly evolving. Although they have experienced significant growth in recent years, the slowing or stopping of the development, general acceptance and adoption, and usage of blockchain networks and blockchain assets may deter or delay the acceptance and adoption of the Tokens.

Risks associated with your credentials.

Any third party that gains access to or learns of your wallet login credentials or private keys may be able to dispose of your Tokens. To minimize this risk, you should guard against unauthorized access to your electronic devices. Best practices dictate that you safely store private keys in one or more backup locations geographically separated from the working location. In addition, you are responsible for giving us the correct wallet address to which to send your Tokens. If you give us the incorrect address to which to send your Tokens, we are not responsible for any loss of Tokens that may occur.

Purchasers are responsible for securing and maintaining their private keys and otherwise following cybersecurity best practices. Failure to do so may result in the loss of all the Purchaser's Tokens.

The Token balances are associated with the Purchasers' respective wallets with the Purchasers' respective token public keys, which in turn are associated with Purchasers' specific token private keys. Each Purchaser is responsible for knowing such Purchaser's private key and keeping it safe and a secret. A private key, or a combination of private keys, is necessary to control and use Tokens stored in a digital wallet or vault. The loss of one or more of a Purchaser's private keys associated with such Purchaser's digital wallet or vault storing the Tokens will result in the loss of the Purchasers' Tokens. The Company will never ask for Purchasers' private keys, and Purchasers should never share any private keys with anyone. Further, the Purchaser is responsible for becoming and staying educated on best practices for securely keeping private keys, protecting any relevant personally identifiable information, and on cybersecurity best practices more generally. Holders of crypto assets can be targeted by hackers in many ways which are out of our control. Holders' private keys can also be stolen. Any third party that gains access to one or more of Purchaser's private keys, including by gaining access to login credentials of a hosted wallet service used by the Purchaser, may be able to misappropriate Purchaser's Tokens. The Company has no control over such attacks and cannot stop hackers from stealing private keys of users. The Company will further accept no liability and will not reimburse the Purchaser for any theft of private keys or any malfunction of wallet software. As a result, any loss of the Purchaser's Tokens due to such theft or malfunction or unauthorized use of any private keys may be final and result in the complete loss of the Purchaser's Tokens purchased hereunder.

Risk of theft and hacking.

Smart contracts, software applications, and the Tokens may be exposed to attacks by hackers or other individuals, groups, organizations, or countries that interfere with the availability of the Tokens in any number of ways, including denial of service attacks, sybil attacks, spoofing, smurfing, malware attacks, or consensus-based attacks, or phishing, or other novel methods that may or may not be known. Any such successful attacks could result in theft or loss of Tokens, adversely impacting the ability to further derive any usage or functionality from Tokens. The Company must take appropriate steps to ensure the integrity of its smart contracts, systems, and other vectors of potential attack. You must take appropriate steps to satisfy yourself of the integrity and veracity of relevant websites, systems, and communications. Furthermore, because the Tokens employ open-source software, there is a risk that a third party or a member of the Company's team may intentionally or unintentionally introduce weaknesses or defects into the core infrastructure of the Token and negatively affect it.

You acknowledge, understand, and accept that if your private key or password gets lost or stolen, the Tokens associated with your wallet address may be unrecoverable and permanently lost. Additionally, any third

party that gains access to your private key, including by gaining access to the login credentials relating to your wallet, may be able to misappropriate your Tokens. Any errors or malfunctions caused by or otherwise related to the digital wallet or vault you choose to receive and store Tokens, including your own failure to properly maintain or use such digital wallet or vault, may also result in the loss of your Tokens, for which the Company shall have no liability.

Risk of mining attacks.

As with other cryptocurrencies, the blockchain used for the Smart Contract System is susceptible to mining attacks, including but not limited to double-spend attacks, majority mining power attacks, "selfish-mining" attacks, and rare condition attacks. Any successful attacks present a risk to the Smart Contract System, expected proper execution and sequencing of token transactions, and expected proper execution and sequencing of contract computations. The network of miners will ultimately be in control of the distribution of the Tokens via the Smart Contract System, and a majority of miners could agree at any point to make changes, updates, modifications to, or effect a deletion or destruction of the Smart Contract System, and that such a scenario could lead to the Tokens losing intrinsic value and/or functionality.

Risk of security weaknesses in the Tokens.

The Tokens consists, at least in part, of open-source software that may, in turn, be based on other open-source software. There is a risk that the Company or other third parties may intentionally or unintentionally introduce weaknesses or bugs into the core infrastructural elements of the Tokens to interfere with the use of or cause the loss of Tokens.

Risk of weaknesses or exploitable breakthroughs in the field of cryptography.

Advances in cryptography, or technical advances such as the development of quantum computing, could present risks to cryptocurrencies (like Tokens) by rendering ineffective the cryptographic consensus mechanism that underpins the Tokens, which could result in the theft, loss, or decreased utility of the Tokens. Smart contracts, blockchain application software, and blockchain platforms and protocols are still in an early development stage and relatively unproven. There is no warranty or assurance that the process for creating Tokens will be uninterrupted or error-free and there is an inherent risk that the software could contain defects, weaknesses, vulnerabilities, viruses, or bugs causing, inter alia, the complete loss of contributions and/or Tokens.

Technology relied upon by the Company for the design and maintenance of the Tokens, which is critical to the Token use case, may not function properly.

The technology relied upon by the Company for the design and periodic software updating and maintenance and functionality of the Tokens may not function properly, which would have a material impact on the Company's business, operations and financial conditions. Problems with the functionality of the software design of the Tokens would also have a direct, material adverse effect on the demand for Tokens.

Risk of incompatible wallet service.

The wallet or wallet service provider used to receive the Tokens must conform to the ERC20 token standard in order to be technically compatible with the Tokens. The failure to ensure such conformity may have the result that Purchaser will not gain access to his, her or its Tokens.

Tax risks relating to tokens, cryptocurrency, and other digital assets.

The regulatory regime governing blockchain technologies, cryptocurrencies, digital assets, digital exchanges and offerings of digital assets is uncertain, and new regulations or policies may materially adversely affect the development and the value of the Company's business.

Risk of unfavorable regulatory action in one or more jurisdictions.

Blockchain technologies and cryptographic tokens have been the subject of scrutiny by various regulatory bodies around the world. Blockchain technology allows new forms of interaction, and it is possible that certain jurisdictions will apply existing regulations on, or introduce new regulations addressing, blockchain technology-based applications, which regulations may be contrary to the current setup of the Tokens or their associated smart contract system and, therefore, may result in substantial modifications to the Tokens and such smart contract systems, including its termination and the loss of Tokens.

The regulatory status of cryptographic tokens and distributed ledger technology is unclear or unsettled in many jurisdictions. It is difficult to predict how or whether regulatory authorities may apply existing regulations with respect to such technology and its applications, including specifically (but without limitation to) the Platform and Tokens. It is likewise difficult to predict how or whether any legislative or regulatory authorities may implement changes to law and regulation affecting distributed ledger technology and its applications, including specifically (but without limitation to) the Tokens. Regulatory actions could negatively impact the Tokens in various ways, including, for purposes of illustration only, through a determination that Tokens are a regulated financial instrument that requires registration, licensing, recordkeeping, reporting, or restriction. The Company may cease operations in a jurisdiction if regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. The functioning of the Tokens could be impacted by any regulatory inquiries or actions, including restrictions on the use, sale, or possession of digital tokens like the Tokens, which restrictions could impede, limit, or end the development of the Tokens and increase legal costs.

The cryptocurrency exchange market, any token listing and trading market, initial coin offerings, and by extension the Tokens, are or may be subject to a variety of federal, state, and international laws and regulations, including those with respect to KYC/AML and customer due diligence procedures, privacy and data protection, consumer protection, data security, foreign exchange controls money transmission, and others. These laws and regulations, and the interpretation or application of these laws and regulations, could change. In addition, new laws or regulations affecting the Tokens could be enacted, which could impact the utility of the Tokens in the Platform. Additionally, users of the Platform are subject to or may be adversely affected by industry-specific laws and regulations or licensing requirements. If any of these parties fails to comply with any of these licensing requirements or other applicable laws or regulations, or if such laws and regulations or licensing requirements become more stringent or are otherwise expanded, it could adversely impact the Tokens, including the utility of Tokens with respect to the Platform, including any applications that are built in connection with the Platform.

The Company may need to obtain approvals from one or more governmental authorities and there is a risk that securing such approvals may delay or prevent the development of the Tokens and/or the Company's ability to issue the Tokens.

Long-term viability of crypto assets.

Crypto assets, including those like the Tokens, are a new and relatively untested product. There is considerable uncertainty about their long-term viability, which could be affected by a variety of factors, including many market-based factors such as economic growth, inflation, and others. In addition, the success of crypto assets (including the Tokens) will depend on the long-term utility and economic viability of blockchain and other new technologies related to crypto assets. Due in part to these uncertainties, the price of crypto assets are volatile and the Tokens may be hard to sell. Further, the value of Tokens may decrease over time, which may impact interest in, or the success of, the Platform. The Company does not control any of these factors, including the ability of the Tokens to maintain their value over time.

The further development and acceptance of blockchain networks, which are part of a new and rapidly changing industry, are subject to a variety of factors that are difficult to evaluate.

The growth of the blockchain industry in general, as well as the blockchain networks on which the Company's business and Tokens will rely, is subject to a high degree of uncertainty. The factors affecting the further development of blockchain networks and cryptocurrencies, include, without limitation:

- worldwide growth in the adoption and use of cryptocurrencies and other blockchain technologies;
- government and quasi-government regulation of cryptocurrencies and other blockchain assets and their use, or restrictions on or regulation of access to and operation of blockchain networks or similar systems;
- the maintenance and development of the open-source software protocol of cryptocurrency networks;
- changes in consumer demographics and public tastes and preferences;
- the availability and popularity of other forms or methods of buying and selling goods and services, or trading assets including new means of using government-backed currencies or existing networks;
- general economic conditions and the regulatory environment relating to cryptocurrencies; and
- a decline in the popularity or acceptance of cryptocurrencies or other blockchain-based tokens that would adversely affect the Company’s business and results of operations.

The cryptocurrency and blockchain industries as a whole have been characterized by rapid changes and innovations and are constantly evolving. Although they have experienced significant growth in recent years, the slowing or stopping of the development, general acceptance and adoption and usage of blockchain networks and blockchain assets may deter or delay the development of the Company’s business. Finally, the Company can give no assurance that technical advances, such as the development of quantum computing, will not present challenges to blockchain technology by rendering ineffective the cryptographic consensus mechanisms that underpin blockchain protocols.

Risk associated with underlying technology.

There can be no guarantee that the technology required for operation of the Platform will function as anticipated or function at all. This technology may malfunction because of internal problems or as a result of cyberattacks or security breaches or the Company might not be able to successfully develop the technology. Further, there may be no alternatives available if this technology does not work as anticipated. As a result, failure of this technology to work as intended may adversely affect the operation and growth of the Platform and may have a material adverse impact on Tokens.

Unanticipated risks.

Cryptographic tokens are a relatively new and comparatively untested technology. In addition to the risks discussed herein, there are risks that the Company cannot anticipate. Further risks may materialize as unanticipated combinations or variations of the discussed risks or the emergence of new risks.

RISK FACTORS RELATED TO A NETWORK

No guarantee on when or if the Token Integration Event will occur.

There are no guarantees as to the timing of the Token Integration Event or the release of the Tokens, each of which is dependent on many factors, including many outside the Company's control. If the Token Integration Event does not occur or for other reasons the Company does not issue the Tokens as planned, Purchasers will not receive some or all of their Tokens. The Company has sole discretion to determine when, or if, the Token Integration Event occurs.

Risk of Tokens being deemed a futures contract or swap.

Given the time period between the close of this Offering and delivery of the Tokens, there is a risk that any deferred delivery arrangement involving a commodity could be viewed as a futures contract or swap transaction under U.S. commodities laws. We believe that this risk is generally a latent one that is mitigated by the Company's obligation to deliver Tokens shortly after the Token Integration Event to Purchasers who represent and warrant that they are Platform users not purchasing with speculative intent and who are otherwise prohibited from transferring the Tokens before the Token is launched.

The value of the Tokens will be affected by the success of the platform.

Because the Tokens are intended for use on the Platform, a failure to maintain the Platform would negatively affect the value of the Tokens. There is no guarantee that the Network, including its use of the Tokens will develop as planned or become successful in the marketplace.

Risks associated with issuance of additional tokens.

Tokenholders may collectively determine it is in the best interest of the Network to adjust the supply of Tokens either upward or downward in the future. Further, if and when the Company enables staking, additional Tokens may be issued. If such events occur, the value of Tokens may be adversely impacted and a tokenholder's Token holding may also be diluted as a result.

RISK FACTORS RELATED TO A PROTOCOL

The Token Integration Event may not be adopted.

Insofar as the Protocol is not operated by the Company but by an independent community of participants around the world, the community may have discretion to adopt or not to adopt the Token Integration Event recommendation. Therefore, the Company cannot guarantee that a Token Integration Event will occur.

Risk of Protocol attacks and forks.

As with other blockchains, the Protocol could be susceptible to consensus-related attacks, including but not limited to double-spend attacks, majority validation power attacks, censorship attacks, byzantine behavior in the consensus algorithm or be subject to hard or soft forks. Any successful attack or fork presents a risk to the Protocol, the expected proper execution and sequencing of Token-transactions, the expected proper execution and sequencing of contract computations as well as the token balances in any investor's wallet.

Risk of mining attacks.

As with other cryptocurrencies, the blockchain used for the Smart Contract System is susceptible to mining attacks, including but not limited to double-spend attacks, majority mining power attacks, "selfish-mining" attacks, and rare condition attacks. Any successful attacks present a risk to the Smart Contract System, expected proper execution and sequencing of token transactions, and expected proper execution and sequencing of contract computations. The network of miners will ultimately be in control of the distribution of the Tokens via the Smart Contract System, and a majority of miners could agree at any point to make changes, updates, modifications to, or effect a deletion or destruction of the Smart Contract System, and that such a scenario could lead to the Tokens losing intrinsic value and/or functionality.

Risk associated with other applications.

The Protocol may give rise to other, alternative projects, promoted by unaffiliated third parties, under which Tokens will have no intrinsic value. This means that competitors may produce platforms that compete with our business model and project and may not accept our Tokens as payment for services within such platforms. Further, such platforms may become more popular and have greater success than our business model and project. In addition, the utility of Tokens depends on the success of our business model and project, if developed. Our business model and project may not be popular or widely used. In the long term,

our business model and project may fail to attract a critical mass of users. Our business model and project may be merged with other projects. Various circumstances, including technical advancement and competitors, may render our business model and project obsolete.

Risk of withdrawing partners.

The feasibility of the Protocol as a whole depends strongly on the collaboration of front-end providers and other crucial partners. There is no assurance that the Protocol as a whole will be successfully developed and deployed.

Risk of abandonment / lack of success.

The creation of the Protocol may be abandoned for a number of reasons including, but not limited to, lack of interest from the public, lack of funding, incapacitation of key developers and project members, force majeure (including pandemics) or lack of commercial success or prospects. There are no assurances, even if the Protocol was partially or fully developed and launched that any investors will receive any benefits through the Tokens held by it.

Tax risks related to the Protocol.

Regulation of digital assets, cryptocurrencies, blockchain technologies and cryptocurrency exchanges is currently undeveloped and likely to rapidly evolve as government agencies take greater interest in them. Regulation varies significantly among international, federal, state and local jurisdictions and is subject to significant uncertainty. Various legislative and executive bodies in the United States and in other countries may in the future adopt laws, regulations or guidance, or take other actions, which may directly or indirectly affect a digital asset network. Such authorities may also restrict the right to acquire, own, hold, sell, convert, trade or use digital assets, or to exchange digital assets for either fiat currency or other virtual currency, thus severely impacting the permissibility or use of the Tokens. Such regulatory changes may be contrary to the current setup of the Smart Contract System and may, inter alia, result in substantial modifications to the Smart Contract System and/or the Protocol, including its termination and the loss of Tokens for investors. Additionally, regulation of proposed activities of the Protocol is presently uncertain. It is not known what regulatory framework the proposed Protocol and associated activities will be subject to, the nature and obligations that will be imposed on the Company in order to comply with any such regulatory framework or when/if the Company will even be able to apply to be regulated, or successfully obtain the required licenses so that it may lawfully carry out its proposed business activities. The Company may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction.

RISK FACTORS RELATED TO LAYER 1 BLOCKCHAIN NETWORKS

Risks associated with the blockchain platforms.

Any malfunction, breakdown, abandonment, unintended function, unexpected functioning of, or attack on the platform upon which the Tokens are issued may have an adverse effect on the Tokens, including causing them to malfunction or function in an unexpected or unintended manner.

Proof-of-stake blockchains are a relatively recent innovation and have not been subject to as widespread use or adoption over as long of a period of time as traditional proof-of-work blockchains.

Certain digital assets, such as bitcoin, use a "proof-of-work" consensus algorithm. The genesis block on the Bitcoin blockchain was mined in 2009, and the Bitcoin blockchain has been in operation since then. Many newer blockchains enabling smart contract functionality, including the current Ethereum Network following the completion of the "Merge" in 2022, use a newer consensus algorithm known as "proof-of-

stake." While their proponents believe that they may have certain advantages, the "proof-of-stake" consensus mechanisms and governance systems underlying many newer blockchain protocols, including our Network, and its associated digital assets, such as the Tokens – have not been tested at scale over as long of a period of time or subject to as widespread use or adoption as, for example, the Bitcoin blockchain's proof-of-work consensus mechanism has. This could lead to these blockchains, and their associated digital assets, having undetected vulnerabilities, structural design flaws, suboptimal incentive structures for network participants (e.g., validators), technical disruptions, or a wide variety of other problems, any of which could cause these blockchains not to function as intended, lead to outright failure to function entirely causing a total outage or disruption of network activity, or to suffer other operational problems or reputational damage, leading to a loss of users or adoption or a loss in value of the associated digital assets, including the Tokens. Over the long term, there can be no assurance that the proof-of-stake blockchain on which our business model relies will achieve widespread scale or adoption or perform successfully; any failure to do so could negatively impact the value of the Tokens and our business.

Digital asset networks face significant scaling challenges and efforts to increase the volume and speed of transactions may not be successful.

Many digital asset networks, including our Network, face significant scaling challenges due to the fact that public blockchains generally face a tradeoff between security and scalability. One means through which public blockchains achieve security is decentralization, meaning that no intermediary is responsible for securing and maintaining these systems. For example, a greater degree of decentralization generally means a given digital asset network is less susceptible to manipulation or capture. Achieving decentralization may mean that every single node on a given digital asset network is responsible for securing the system by processing every transaction and every single full node is responsible for maintaining a copy of the entire state of the network. However, this may involve tradeoffs from an efficiency perspective, and impose constraints on throughput. A digital asset network may be limited in the number of transactions it can process by the fact that all validators participate in validating in each block and the capabilities of each single fully participating node. Many developers are actively researching and testing scalability solutions for public blockchains that do not necessarily result in lower levels of security or decentralization, such as off-chain payment channels. Off-chain payment channels would allow parties to transact without requiring the full processing power of a blockchain.

As corresponding increases in throughput lag behind growth in the use of digital asset networks, average fees and settlement times may increase considerably. Increased fees and decreased settlement speeds could preclude certain uses for our Network and could reduce demand for, and the price of, our Token, which could adversely impact its value.

There is no guarantee that any of the mechanisms in place or being explored for increasing the scale of settlement of our Network transactions will be effective, or how long these mechanisms will take to become effective, which could adversely impact the value of the Tokens.

The rapid development of other competing scalability solutions, such as those which would rely on handling the bulk of computational work relating to transactions or smart contracts and DApps outside of our Network, may cause alternatives to sharding to emerge. "Layer 2" is a collective term for solutions which are designed to help increase throughput and reduce transaction fees by handling or validating transactions off our Network (known as "**Layer 1**") and then attempting to take advantage of the perceived security and integrity advantages of our Layer 1 Network by uploading the transactions validated on the Layer 2 protocol back to the Layer 1 Network. The details of how this is done vary significantly between different Layer 2 technologies and implementations and could cause issues with our Network.

Many developers are actively researching and testing scalability solutions for public blockchains. However, there is no guarantee that any of the mechanisms in place or being explored for increasing speed and throughput of settlement of the Network transactions will be effective, which could cause the Network to not adequately resolve scaling challenges and adversely impact the adoption of Tokens and our Network and the value of the Tokens. There is no guarantee that any potential scaling solution, whether a change to our Layer 1 Network like sharding or the introduction of a Layer 2 solution like rollups, state channels or side chains, will achieve widespread adoption. It is possible that proposed changes to our Layer 1 Network could divide the community, potentially even causing a hard fork, or that the decentralized governance of our Network causes network participants to fail to coalesce overwhelmingly around any particular solution, causing our Network to suffer reduced adoption or causing users or validators to migrate to other blockchain networks. It is also possible that scaling solutions could fail to work as intended, could suffer from centralization concerns, or could introduce bugs, coding defects or flaws, security risks, or other problems that could cause them to suffer operational disruptions. Alternatively, if a widely-used Layer 2 network were to fail, it could reduce demand for Tokens because it would eliminate a source of demand for using Tokens to record transactions from the Layer 2 onto our Layer 1 Network. Any of the foregoing could adversely affect the price of Tokens.

The value of the Tokens relates directly to its price. The price of the Tokens may be highly volatile and subject to fluctuations due to a number of factors, including the successful development and acceptance of our Network.

Digital assets such as the Tokens were only introduced within the past 15 years, and the medium to long term value of the Tokens is subject to a number of factors over time relating to the capabilities and development of blockchain technologies, such as the recentness of their development, their dependence on the internet and other technologies, their dependence on the role played by users, developers validators and the potential for malicious activity. Our Token itself was only recently conceived and first sold. For example, the realization of one or more of the following risks could materially adversely affect the value of the Tokens: digital asset networks, and the software used to operate them are in the early stages of development. Given the recentness of the development of digital asset networks, digital assets may not function as intended and parties may be unwilling to use digital assets, which would dampen the growth, if any, of digital asset networks. Because the Token is a digital asset, the value of the Tokens is subject to a number of factors relating to the fundamental investment characteristics of digital assets, including the fact that digital assets are bearer instruments and loss, theft, compromise, or destruction of the associated private keys could result in permanent loss of the asset.

- An increase in the global Token supply or a decrease in global Token demand;
- Digital assets, including Tokens, are controllable only by the possessor of both the unique public key and private key or keys relating to our Network address, or "wallet", at which the digital asset is held. Private keys must be safeguarded and kept private in order to prevent a third party from accessing the digital asset held in such wallet. The loss, theft, compromise or destruction of a private key required to access a digital asset may be irreversible. If a private key is lost, stolen, destroyed or otherwise compromised and no backup of the private key is accessible, the owner would be unable to access the digital asset corresponding to that private key and the private key will not be capable of being restored by the digital asset network resulting in the total loss of the value of the digital asset linked to the private key;
- Forks in our Network, particularly where changes to our Network source code are either not well-received by key constituencies within our community or are not successfully executed or implemented and fail to achieve the functionality such changes were intended to bring about;

- Our Network's protocol is informally overseen by a collective of core developers who, along with members of our community, can introduce proposals for updating our Network. The core developers evolve over time, largely based on self-determined participation. A Network client ("**Network Client**") is a software application that implements our Network specification and communicates with our Network. A "node" is a computer or other device that has downloaded the Network Client and is connected to other computers also running the Network Client software, together forming our Network. To the extent that node operators update their individual Network Client to new specifications, our Network could be subject to changes that may adversely affect the value of the Tokens. In addition, if a digital asset network has high-profile contributors, a perception that such contributors will no longer contribute to the network could have an adverse effect on the market price of the related digital asset;

- Increased competition from other blockchain networks combining smart contracts, programmable scripting languages, and an associated runtime environment, with blockchain-based recordkeeping, particularly where such other blockchain networks are able to offer users access to a larger consumer user base, greater efficiency, reliability, or processing speed, or more economical transaction processing fees than our Network fees associated with processing a Token transaction and the speed at which Token transactions are settled;

- The ability for our Network to attract and retain validators to secure and confirm transactions accurately and efficiently;

- The acceptance of software patches or upgrades by some, but not all, nodes, users and validators in a digital asset network, such as our Network, could result in a "fork" in our Network, resulting in the operation of multiple separate networks;

- A lack of consensus or clarity on the governance of our Network, which may stymie our Network's utility and ability to grow and face challenges. In particular, it may be difficult to find solutions or martial sufficient effort to overcome any future problems on our Network, especially long-term problems;

- Digital asset validator operations have evolved from individual users to "professionalized" validating operations using proprietary hardware or sophisticated machines. If the profit margins of digital asset validating operations are not sufficiently high, including due to a decrease in transaction fees, validators are more likely to immediately sell tokens earned by validating, resulting in an increase in liquid supply of that digital asset, which would generally tend to reduce that digital asset's market price;

- To the extent that any validators cease to record transactions that do not include the payment of a transaction fee in solved blocks or do not record a transaction because the transaction fee is too low, such transactions will not be recorded on our Network blockchain until a block is validated by a validator who does not require the payment of transaction fees or is willing to accept a lower fee. Any widespread delays in the recording of transactions could result in a loss of confidence in a digital asset network;

- Software applications running on top of our Network (often referred to as "decentralized applications" or "DApps", whether or not decentralized in fact) and smart contract developers depend on being able to obtain Tokens to be able to run their programs and operate their businesses. In particular, decentralized applications and smart contracts require Tokens in order to pay the gas fees needed to power such applications and smart contracts and execute transactions. As such, they represent a significant source of demand for Tokens. Our Tokens' price volatility (particularly where the Token prices increase), or our Network's wider inability to meet the demands of

decentralized applications and smart contracts in terms of inexpensive, reliable, and prompt transaction execution (including during congested periods), or to solve its scaling challenges or increase its throughput, may discourage such decentralized application and smart contract developers from using our Network as the foundational infrastructure layer for building their applications and smart contracts. If decentralized application and smart contract developers abandon our blockchain for other blockchain or digital asset networks or protocols for whatever reason, the value of the Tokens could be negatively affected;

- In the past, bugs, defects and flaws in the source code for digital assets have been exposed and exploited, including flaws that may or have disrupted our Network, Network Clients, or DApp and smart contract operations or disabled related functionality for users, exposed users' personal information and/or resulted in the theft of users' digital assets. The cryptography underlying our Network or our Tokens as an asset could prove to be flawed or ineffective, or developments in mathematics and/or technology, including advances in digital computing, algebraic geometry and quantum computing, could result in such cryptography becoming ineffective. In any of these circumstances, a malicious actor may be able to compromise the security of our Network, which would adversely affect the value of the Tokens. Moreover, normal operations and functionality of our Network may be negatively affected Such losses of functionality could lead to our Network losing attractiveness to users, nodes, validators, or other stakeholders, thereby dampening demand for the Tokens. Even if another digital asset other than the Tokens were affected by similar circumstances, any reduction in confidence in the source code or cryptography underlying digital assets generally could negatively affect the demand for digital assets and therefore adversely affect the value of the Tokens.

Competition from central bank digital currencies and emerging payments initiatives involving financial institutions could adversely affect the value of the Tokens and other digital assets.

Central banks in various countries have introduced digital forms of legal tender ("**CBDCs**"). Whether or not they incorporate blockchain or similar technology, CBDCs, as legal tender in the issuing jurisdiction, could have an advantage in competing with, or replace, the Tokens and other cryptocurrencies as a medium of exchange or store of value. Central banks and other governmental entities have also announced cooperative initiatives and consortia with private sector entities, with the goal of leveraging blockchain and other technology to reduce friction in cross-border and interbank payments and settlement, and commercial banks and other financial institutions have also recently announced a number of initiatives of their own to incorporate new technologies, including blockchain and similar technologies, into their payments and settlement activities, which could compete with, or reduce the demand for, the Tokens. As a result of any of the foregoing factors, the value of the Tokens could decrease, which could adversely affect the value of an investment in the Tokens.

Mathematical or technological advances could undermine our Network's consensus mechanism.

Our Network relies on cryptographic algorithms for various operations, including address generation, transaction verification and smart contract execution. It is possible that mathematical or technological advances, such as the development of quantum computers with significantly more power than computers presently available, could undermine or vitiate the cryptographic consensus mechanism underpinning our Network. Quantum computing technology is an emerging phenomenon which, because it is still developing, makes it difficult to predict its ultimate effect on the future value of Tokens and other digital assets. However, recent announcements by computer technology companies have suggested that quantum computing technology may be advancing faster than previously anticipated. For example, in February 2025, Microsoft announced its Majorana 1 chip, which is claimed to have the potential to support a one-million-qubit quantum computer. If quantum computing technology is able to advance and significantly increase

its capacity relative to the capacity of today's leading quantum computers, it could potentially undermine the viability of many of the cryptographic algorithms used across the world's information technology infrastructure, including the cryptographic algorithms used for digital assets like the Tokens. If quantum computing is able to advance in that way, there is a risk that quantum computing could result in the cryptography underlying our Network becoming ineffective, which, if realized, could compromise the security of our Network, or allow a malicious actor to compromise the wallets holding Tokens owned on our Network, which would result in losses to Shareholders. While various actors in the our community are taking steps to enable the uses of cryptographic algorithms that would be resistant to advanced quantum computers, there is no guarantee that new quantum-proof architectures will be built and appropriate transitions will be implemented across the network at scale in a timely manner; any such changes could require the achievement of broad consensus within our Network community and a fork (or multiple forks), and there can be no assurance that such consensus would be achieved or the changes implemented successfully. If any of the foregoing were to occur, it could result in losses to Shareholders. Moreover, normal operations and functionality of our Network may be negatively affected. Such losses of functionality could lead to our Network losing attractiveness to users, nodes, validators, or other stakeholders, thereby dampening demand for the Tokens. Even if another digital asset other than the Tokens were affected by similar circumstances, any reduction in confidence in the source code or cryptography underlying digital assets generally could negatively affect the demand for digital assets and therefore adversely affect the value of the Tokens.

Smart contracts, including those relating to DeFi applications, are a new technology and their ongoing development and operation may result in problems, which could reduce the demand for the Tokens or cause a wider loss of confidence in our Network, either of which could have an adverse impact on the value of the Tokens.

Smart contracts are programs that run on our Network that execute automatically when certain conditions are met. Since smart contracts typically cannot be stopped or reversed, vulnerabilities in their programming can have damaging effects. For example, in June 2016, a vulnerability in the smart contracts underlying the DAO, a distributed autonomous organization for venture capital funding on the Ethereum Network, allowed an attack by a hacker to syphon approximately $60 million worth of ether from The DAO's accounts into a segregated account. In the aftermath of the theft, certain core developers and contributors pursued a "hard fork" of the Ethereum Network in order to erase any record of the theft. Despite these efforts, the price of ether reportedly dropped approximately 35% in the aftermath of the attack and subsequent hard fork. In addition, in July 2017, a vulnerability in a smart contract for a multi-signature wallet software developed by Parity led to a reportedly $30 million theft of ether, and in November 2017, a new vulnerability in Parity's wallet software reportedly led to roughly $160 million worth of ether being indefinitely frozen in an account. Furthermore, in April 2018, a batch overflow bug was found in many Ethereum-based ERC20-compatible smart contract tokens that allows hackers to create a large number of smart contract tokens, causing multiple crypto asset platforms worldwide to shut down ERC20-compatible token trading. Similarly, in March 2020, a design flaw in the MakerDAO smart contract caused forced liquidations of crypto assets at significantly discounted prices, resulting in millions of dollars of losses to users who had deposited crypto assets into the smart contract. In another example, in February 2022, a vulnerability in a smart contract for Wormhole, a bridge between the Ethereum Network and Solana Network led to a $320 million theft of ether. While persons associated with Solana Labs and/or the Solana Foundation are understood to have played a key role in bringing the network back online, the broader community also played a key role, as Solana validators coordinated to upgrade and restart the network. Other smart contracts, such as bridges between blockchain networks and decentralized finance ("**DeFi**") protocols have also been manipulated, exploited or used in ways that were not intended or envisioned by their creators such that attackers syphoned over $3.8 billion worth of digital assets from smart contracts in 2022. Problems

with the development, deployment, and operation of smart contracts may have an adverse effect on the value of the Tokens, just as they have for other digital assets like ether.

In some cases, smart contracts can be controlled by one or more "admin keys" or users with special privileges, or "super users". These users may have the ability to unilaterally make changes to the smart contract, enable or disable features on the smart contract, change how the smart contract receives external inputs and data, and make other changes to the smart contract. Furthermore, in some cases inadequate public information may be available information asymmetries may exist, even with respect to open-source smart contracts or applications; certain participants may have hidden informational or technological advantages, making for an uneven playing field. There may be opportunities for bad actors to perpetrate fraudulent schemes and engage in illicit activities and other misconduct, such as exit scams and rug pulls (orchestrated by developers and/or influencers who promote a smart contract or application and, ultimately, escape with the money at an agreed time), or Ponzi or similar fraud schemes.

Insofar as DeFi applications become deployed on our Network, smart contracts relating to DeFi applications may in the future constitute a significant source of demand for the Tokens. DeFi applications may achieve their investment purposes through self-executing smart contracts that may allow users to invest digital assets in a pool from which other users can borrow without requiring an intermediate party to facilitate these transactions. These investments may earn interest to the investor based on the rates at which borrowers repay the loan, and can generally be withdrawn by the investor. For smart contracts that hold a pool of digital asset reserves, smart contract super users or admin key holders may be able to extract funds from the pool, liquidate assets held in the pool, or take other actions that decrease the value of the digital assets held by the smart contract in reserves. Even for digital assets that have adopted a decentralized governance mechanism, such as smart contracts that are governed by the holders of a governance token, such governance tokens can be concentrated in the hands of a small group of core community members, who would be able to make similar changes unilaterally to the smart contract. If any such super user or group of core members unilaterally make adverse changes to a smart contract, the design, functionality, features and value of the smart contract, its related digital assets may be harmed. In addition, assets held by the smart contract in reserves may be stolen, misused, burnt, locked up or otherwise become unusable and irrecoverable. Super users can also become targets of hackers and malicious attackers. If an attacker is able to access or obtain the super user privileges of a smart contract, or if a smart contract's super users or core community members take actions that adversely affect the smart contract, users who transact with the smart contract may experience decreased functionality of the smart contract or may suffer a partial or total loss of any digital assets they have used to transact with the smart contract. Furthermore, the underlying smart contracts may be insecure, contain bugs or other vulnerabilities, or otherwise may not work as intended. Any of the foregoing could cause users of the DeFi application to be negatively affected, or could cause the DeFi application to be the subject of negative publicity. Because DeFi applications may be built on our Network and represent a significant source of demand for the Tokens, public confidence in our Network itself could be negatively affected, such sources of demand could diminish and the value of the Tokens could decrease. Similar risks apply to any smart contract or decentralized application, not just DeFi applications.

Digital assets may have concentrated ownership and large sales or distributions by holders of such digital assets, or any ability to participate in or otherwise influence a digital asset's underlying network, could have an adverse effect on the market price of such digital asset.

Ownership of our Tokens is presently concentrated to a limited number of wallets. Moreover, it is possible that other persons or entities control multiple wallets that collectively hold a significant number of Tokens, even if they individually only hold a small amount, and it is possible that some of these wallets are controlled by the same person or entity. As a result of this concentration of ownership, large sales or

distributions by such holders could have an adverse effect on the market price of the Tokens. Competition from other consortia or private blockchains could have a negative impact on the price of the Tokens and adversely affect an investment in them.

The price of Tokens may be affected due to stablecoins (including Tether and USDC), the activities of stablecoin issuers and their regulatory treatment.

The price of the Tokens may be exposed to risks that stablecoins pose for the market for our Tokens and other digital asset markets. Stablecoins are digital assets designed to have a stable value over time as compared to typically volatile digital assets, and are typically marketed as being pegged to a fiat currency, such as the U.S. dollar, at a certain value. Although the prices of stablecoins are intended to be stable, their market value may fluctuate. This volatility may, as it has for other tokens, impact the price of the Tokens. Stablecoins are a relatively new phenomenon, and it is impossible to know all of the risks that they could pose to participants in the Token market. In addition, some have argued that some stablecoins, particularly Tether, are improperly issued without sufficient backing in a way that, when the stablecoin is used to pay for Tokens, could cause artificial rather than genuine demand for the Tokens, artificially inflating the price of the Tokens, and also argue that those associated with certain stablecoins may be involved in laundering money. On February 17, 2021 the New York Attorney General entered into an agreement with Tether's operators, including Bitfinex, requiring them to cease any further trading activity with New York persons and pay $18.5 million in penalties for false and misleading statements made regarding the assets backing Tether. On October 15, 2021, the CFTC announced a settlement with Tether's operators, Tether Holdings Limited, Tether Operations Limited, Tether Limited, and Tether International Limited, in which they agreed to pay $42.5 million in fines to settle charges that, among others, Tether's claims that it maintained sufficient U.S. dollar reserves to back every Tether stablecoin in circulation with the "equivalent amount of corresponding fiat currency" held by Tether were untrue.

Bitfinex also agreed to pay the CFTC a $1.5 million fine to settle charges that Bitfinex offered off-exchange leveraged, margined, or financed transactions involving cryptocurrencies, including Solana, with U.S. customers who were not eligible contract participants and accepted funds (including in the form of Tether stablecoins) and orders in connection with such illegal off-exchange transactions, triggering an obligation to register with the CFTC, which the CFTC order asserts it violated. The CFTC previously fined Bitfinex in 2016 on similar charges.

USDC is a reserve-backed stablecoin issued by Circle Internet Financial that is commonly used as a method of payment in digital asset markets. While USDC is designed to maintain a stable value at 1U.S. dollar at all times, on March 10, 2023, the value of USDC fell below $1.00 for multiple days after Circle Internet Financial disclosed that US$3.3 billion of the USDC reserves were held at Silicon Valley Bank, which had entered FDIC receivership earlier that day. Stablecoins are reliant on the U.S. banking system and U.S. treasuries, and the failure of either to function normally could impede the function of stablecoins, and therefore could adversely affect the value of the Tokens.

Given the foundational role that stablecoins play in global digital asset markets, their fundamental liquidity can have a dramatic impact on the broader digital asset market, including the market for Tokens. Because a large portion of the digital asset market still depends on stablecoins such as Tether and USDC, there is a risk that a disorderly de-pegging or a run on Tether or USDC could lead to dramatic market volatility in digital assets more broadly. Volatility in stablecoins, operational issues with stablecoins (for example, technical issues that prevent settlement), concerns about the sufficiency of any reserves that support stablecoins or potential manipulative activity when unbacked stablecoins are used to pay for other digital assets (including Tokens), or regulatory concerns about stablecoin issuers or intermediaries, such as exchanges, that support stablecoins, or the removal or migration of prominent stablecoins away from our

Network, could impact individuals' willingness to trade on trading venues that rely on stablecoins, reduce liquidity in the Token market, and affect the value of the Tokens, and in turn impact an investment in the Tokens.

If the digital asset award or transaction fees for recording transactions on our Network are not sufficiently high to incentivize validators, or if certain jurisdictions continue to limit or otherwise regulate validating activities, validators may cease expanding validating power or demand high transaction fees, which could negatively impact the value of the Tokens.

If the digital asset awards for validating blocks or the transaction fees for recording transactions on our Network are not sufficiently high to incentivize validators, or if certain jurisdictions continue to limit or otherwise regulate validating activities, validators may cease expending validating power to validate blocks and confirmations of transactions on the our Network could be slowed. For example, the realization of one or more of the following risks could materially adversely affect the value of the Tokens:

- A reduction in the processing power expended by validators on our Network could increase the likelihood of a malicious actor or botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) obtaining control. Our Network could be vulnerable to attacks on transaction finality and consensus processes, which could adversely affect the value of the Tokens;

- Validators have historically accepted relatively low transaction confirmation fees on most digital asset networks. If validators demand higher transaction fees for recording transactions in our Network or a software upgrade automatically charges fees for all transactions on our Network, the cost of using Tokens may increase and the marketplace may be reluctant to accept Tokens as a means of payment. Alternatively, validators could collude in an anti-competitive manner to reject low transaction fees on our Network and force users to pay higher fees, thus reducing the attractiveness of our Network. Higher transaction confirmation fees resulting through collusion or otherwise may adversely affect the attractiveness of our Network and the value of the Tokens;

- To the extent that any validators cease to record transactions that do not include the payment of a transaction fee in blocks or do not record a transaction because the transaction fee is too low, such transactions will not be recorded on our Network blockchain until a block is validated by a validator who does not require the payment of transaction fees or is willing to accept a lower fee. Any widespread delays or disruptions in the recording of transactions could result in a loss of confidence in our Network and could prevent holders of our Tokens from completing transactions thereon;

- During the course of ordering transactions and validating blocks, validators may be able to prioritize certain transactions in return for increased transaction fees, an incentive system known as "Maximal Extractable Value" or MEV. For example, in blockchain networks that facilitate DeFi protocols in particular, such as our Network, users may attempt to gain an advantage over other users by increasing offered transaction fees. Certain software solutions, such as Flashbots, have been developed which facilitate validators in capturing MEV produced by these increased fees. The MEV incentive system may lead to an increase in transaction fees on our Network, which may diminish its use. Users or other stakeholders on our Network could also view the existence of MEV as unfair manipulation of decentralized digital asset networks, and refrain from using DeFi protocols or our Network generally. In addition, it's possible regulators or legislators could enact rules which restrict the use of MEV, which could diminish the popularity of our Network among users and validators. Any of these or other outcomes related to MEV may adversely affect the value of the Tokens.

Validators may suffer losses due to staking, or staking may prove unattractive to validators, which could make our Network less attractive.

Validation on our Network requires Tokens to be transferred into smart contracts on the underlying blockchain networks. If our Network source code or protocol fail to behave as expected, suffer cybersecurity attacks or hacks, experience security issues, or encounter other problems, such assets may be irretrievably lost. As part of the "activating" and "de-activating" or "cooling down" processes of staking, staked Tokens will be inaccessible for a variable period of time determined by a range of factors, resulting in potential inaccessibility during those periods. "Activation" is the funding of a validator to be included in the active set, thereby allowing the validator to participate in our Network's proof-of-stake consensus protocol. "De-activating" is the request to exit from the active set and no longer participate in our Network's proof-of-stake consensus protocol. As part of these "activating" and "de-activating" processes of staking on our Network, any staked Tokens will be inaccessible for a period of time. The duration of activating and exiting periods are dependent on a range of factors. However, depending on demand, un-staking can take between one to several epochs to complete.

Our Network requires the payment of base fees and the practice of paying prioritization fees is common, and such fees can become significant as the amount and complexity of the transaction grows, depending on the degree of network congestion and the price of the Tokens. Any cybersecurity attacks, security issues, hacks, penalties, slashing events, or other problems could damage validators' willingness to participate in validation, discourage existing and future validators from serving as such, and adversely impact our Network's adoption or the price of the Tokens. Any disruption of validation on our Network could interfere with network operations and cause our Network to be less attractive to users and application developers than competing blockchain networks, which could cause the price of the Tokens to decrease. The limited liquidity during the "activation" or "de-activation" processes could dissuade potential validators from participating, which could interfere with network operations or security and cause our Network to be less attractive to users and application developers than competing blockchain networks, which could cause the price of the Tokens to decrease.

Operational cost may exceed the award for validating transactions, and increased transaction fees may adversely affect the usage of our Network.

If transaction confirmation fees become too high, the marketplace may be reluctant to use our Network. This may result in decreased usage and limit expansion of our Network in the retail, commercial and payments space, adversely impacting investment in the Tokens. Conversely, if the reward for validators or the value of the transaction fees is insufficient to motivate validators, they may cease to validate transactions. Ultimately, if the awards of new costs of validating transactions grow disproportionately, validators may operate at a loss, transition to other networks, or cease operations altogether. Each of these outcomes could, in turn, slow transaction validation and usage, which could have a negative impact on our Network and could adversely affect the value of the Tokens.

Anonymity and illicit financing risk.

Although transaction details of peer-to-peer transactions are recorded on our Network, a buyer or seller of digital assets on a peer-to-peer basis directly on our Network may never know to whom the public key belongs or the true identity of the party with whom it is transacting. Public key addresses are randomized sequences of alphanumeric characters that, standing alone, do not provide sufficient information to identify users. In addition, certain technologies may obscure the origin or chain of custody of digital assets. The opaque nature of the market poses asset verification challenges for market participants, regulators and auditors and gives rise to an increased risk of manipulation and fraud, including the potential for Ponzi schemes, bucket shops and pump-and-dump schemes. Digital assets have in the past been used to facilitate

illicit activities. If a digital asset were used to facilitate illicit activities, businesses that facilitate transactions in such digital assets could be at increased risk of potential criminal or civil liability or lawsuits, or of having banking or other services cut off, and such digital asset could be removed from digital asset platforms. Any of the aforementioned occurrences could adversely affect the price of the relevant digital asset, the attractiveness of the respective blockchain network and an investment in the Tokens. If a holder of Tokens were to transact with a sanctioned entity, such Holder – or even the Company – could be at risk of potential criminal or civil lawsuits or liability.

If validators exit the Solana Network, it could increase the likelihood of a malicious actor obtaining control.

Validators exiting the network could make our Network more vulnerable to a malicious actor obtaining control of a large percentage of staked Tokens, which might enable them to manipulate our Network by censoring or manipulating specific transactions. If our Network suffers such an attack, the price of the Tokens could be negatively affected, and a loss of confidence in our Network could result. Any reduction in confidence in the transaction confirmation process or staking power of our Network may adversely affect an investment in the Tokens.

RISK FACTORS SPECIFIC TO THE COMPANY

We are not licensed to conduct a virtual currency business in New York and do not currently intend to become licensed in any other state. We have taken the position that New York's BitLicense regulatory framework does not apply to our offer and sale of the Tokens. It is possible, however, that the New York State Department of Financial Services could disagree with our position.

We are not licensed to conduct a virtual currency business in New York or any other state. We have, however, taken the position that the State of New York's BitLicense Regulatory Framework does not apply to the offering or operation of the Network or the offer and sale of the Tokens.

It is possible that the New York State Department of Financial Services could disagree with our position. If we were deemed to be conducting an unlicensed virtual currency business in New York, we could be subject to significant additional regulation and/or regulatory consequences and/or be required to no longer make the Network or the Tokens available in New York or to New York residents. Other states may take a similar position in the future. Any of these outcomes may negatively affect the Tokens, including its further development, or the value of the Tokens and/or could cause us to cease operations in New York or any other states requiring a license for our activity.

We are not licensed as a money transmitter under state law or registered as a money services business under federal law, and our business may be adversely affected if we are required to do so.

We believe that we are not a money transmitter under state law or a money services business under federal law in the United States when we offer the Platform to developers. Further, we do not generally or specifically target U.S. Persons (as defined under the Securities Act) or residents to be users of the Tokens. If we were deemed to be a money transmitter under state law and/or money services business under federal law, we would be subject to significant additional regulation and costs. This could lead to significant changes with respect to operations of the Platform, the Tokens, suspensions in the operation of the Platform, the Network, the Tokens or certain of its components, changes in how the Tokens are structured, changes in how they are issued and other regulatory or business consequences and would greatly increase our costs in creating and facilitating transactions of the Tokens. It could also lead to a decrease in value of Tokens. In addition, a regulator could take action against us if it views our activity regarding the Platform or the Tokens as a violation of existing law. Any of these outcomes would negatively affect the value of the Tokens and/or could cause the Company to cease operations in certain states or nationwide.

Operating history.

The Company has little operating history in the blockchain industry, which continues to be evolving and may not develop as expected. The Company's historical performance does not necessarily reflect future performance or the likelihood of the success of the Tokens. A significant amount of work was required in order to create the Tokens and implement the Token into the Platform and much of that work is reliant on the input or consent of other persons not under the control of the Company. Assessing the business and future prospects of the Company is challenging in light of the risks and difficulties the Company may encounter. These risks and difficulties include but are not limited to, their ability to:

- Navigate complex and evolving regulatory and competitive environments;
- obtain the requisite regulatory and other licenses in the relevant jurisdictions;
- obtain and retain customers;
- successfully develop, maintain, and update internal controls to manage compliance within an evolving and complex regulatory environment;
- effectively identify and react to market trends;
- be involved in the successful development and deployment of the Tokens;
- implement new products and services;
- successfully execute the Company's funding strategy;
- effectively compete with other companies;
- successfully navigate economic conditions and fluctuations in the market;
- effectively manage the growth of the business;
- continue to develop, maintain, and scale the Tokens;
- effectively use finite personnel and technology resources;
- effectively maintain and scale financial and risk management controls and procedures;
- maintain the security of technology infrastructure, and the confidentiality of the information provided and utilized therein; and
- attract, integrate, and retain qualified employees and contractors.

Misconduct and errors risks.

The Company is exposed to many types of operational risk, including the risk of misconduct and errors by our employees, former employees, and other third-party service providers, or by users and developers on the Platform, whom the Company does not control, could be in a position to handle large amounts of sensitive and potentially proprietary information, whose exposure could result in significant liability. It is not always possible to identify and deter misconduct by employees or third-party providers, and the Company cannot control developers or uses of the Platform. The precautions the Company takes to detect and prevent this activity, such as encryption of user data, may not be effective in controlling unknown or unmanaged risks or losses. Any of these occurrences could result in the Company's diminished ability to operate the business and develop the Platform, inability to attract future developers and users, regulatory intervention, and financial harm which could negatively impact the Company, the growth of the Company, and the value of Tokens.

Representation by legal counsel.

Certain counsel (the "***Law Firm***") represents the Company solely with respect to the specific matters pertaining to the preparation of this Memorandum. Other matters may exist that could have a bearing on the Company as to which the Law Firm has been neither retained nor consulted. The Law Firm does not undertake to monitor compliance by the Company and its affiliates with the guidelines and procedures set forth in this Memorandum, nor does the Law Firm monitor compliance by the Company and/or its affiliates with applicable laws, unless in each case the Law Firm has been specifically retained to do so. The Law Firm does not investigate or verify the accuracy and completeness of information set forth in this

Memorandum concerning the Company. Furthermore, the Law Firm is not providing any advice, representation, warranty, or other assurance of any kind as to any matter to any prospective investors of the Tokens. No separate counsel has been engaged by the Company to represent any investors with respect to a purchase of the Tokens.

The Company has the exclusive right, in its sole and absolute discretion, to address and remediate any of the operational, legal, or regulatory risks presented as of the date hereof or hereafter. In the exercise of such rights, it is possible that the Company may determine that the continued development of the Tokens is not feasible. Accordingly, there is a material risk that the Company and its affiliates may not successfully continue to develop, market, and operate the Tokens.

Violation of policies risks.

Any violation of Company policies and terms and conditions of use, including misuse of the Platform and Tokens, by users and tokenholders, may result in unforeseeable adverse impact to the Platform out of the Company's control, which may in turn potentially affect the value of Tokens.

Risk of competitors.

The Company believes that other organizations are or may be working to develop decentralized application systems for scalable and interoperable solutions for Web3 developers or other novel technologies that may be competitive with the technology of the Company. Some or all of these organizations that may have technology similar to the Company, may have substantially greater technological expertise, experience with blockchain technologies and/or financial resources than the Company has, and many of them may be attempting to patent technologies that may be competitive with or similar to the technology the Company has developed, or attempting to reverse engineer the Company's technology, which may be possible as a substantial portion of the software underlying the Platform is open source software that is generally available to the public.

Risk of underage users.

In certain jurisdictions, persons under the age of eighteen (18) have the ability to repudiate or disaffirm contracts entered into by those individuals, and some of the Platform users are likely to be under the age of eighteen. As a result, the Company may have difficulty enforcing the terms of service and other agreements entered into with such individuals that are under the age of eighteen in connection with the operation of the Company's business, the Platform, and the distribution of Tokens.

RISK FACTORS SPECIFIC TO THIS OFFERING

No specific use of proceeds.

At present, and other than as set out herein, no proceeds have been allocated for any particular purposes, and management expects to use the net proceeds from this offering for working capital and to promote the development, security, maintenance, and distribution of the Platform, regardless of whether all of the Tokens under this Offering are sold. Management may also use a portion of the net proceeds to acquire, license, and invest in complementary products, technologies, or businesses in the ordinary course of business. However, management will have broad discretion over the use of proceeds and reserves the right to change the use of proceeds on other than working capital and general corporate purposes should the circumstances change, or future research and development opportunities arise and could spend the proceeds from the offering in ways with which Purchasers may not agree with or that do not yield a favorable return, if at all. If management does not use the proceeds of this offering in ways that benefit the Tokens, the future value and utility of Purchasers' Tokens may be adversely affected.

Risks associated with the structure of Token Purchase Agreements.

An investment in a TPA involves a significant amount of risk and is suitable only for sophisticated Purchasers: (i) of substantial means who have no immediate need for liquidity in the amount invested; (ii) for whom such investment does not constitute a complete investment program; (iii) that fully understand, and are willing to assume and have the financial resources necessary to withstand, the risks involved in investing in a TPA; and (iv) that can bear the potential loss of all of their investment in a TPA. There is no assurance as to whether an investment in a TPA will be profitable. Any investment made in a TPA may result in a loss of all or part of a Purchaser's investment. The TPA or a portion thereof may be modified, waived, or amended without your consent consistent with its terms.

* * *

CERTAIN NOTICES

This Memorandum shall be maintained in strict confidence. Any reproduction or distribution of this Memorandum, in whole or in part, or the disclosure of its contents, without the prior written consent of the Company, other than to a recipient's legal, tax, or investment advisors, is prohibited.

This Memorandum has been prepared in connection with the Offering. Each Purchaser will be required to sign, execute, and deliver such documents as may be reasonably required by the Company to effect its purchase of Tokens.

This Memorandum contains a summary of the Offering, the Platform, the Tokens, and certain other documents referred to herein. However, the summaries in this Memorandum do not purport to be complete and are subject to and qualified in their entirety by reference to the actual text of the relevant Offering Documents, copies of which will be provided to each prospective investor on the Republic Platform. Each prospective investor should review the applicable Offering Documents, and such other documents for complete information concerning the rights, privileges, and obligations of Purchasers. If any of the terms, conditions, or other provisions of the Offering Documents or such other documents are inconsistent with or contrary to the descriptions or terms in this Memorandum, such other documents shall control. The Company reserves the right to modify the terms of the Offering and the Tokens described in this Memorandum are offered subject to the Company's ability to reject any commitment in whole or in part.

This Memorandum contains a summary of the material terms of the Tokens. The Tokens have not been and will not be registered under the Securities Act, as amended, the Securities Exchange Act of 1934, as amended (the "**Exchange Act**"), or any United States state securities laws or the laws of any foreign jurisdiction.

No person has been authorized to make any statements concerning the Company or the delivery of the Tokens discussed herein other than as set forth in this Memorandum or the Republic Platform, and any such statements, if made, must not be relied upon.

Prospective investors must make their own investigations and evaluations of the Platform and the Tokens that will be delivered pursuant thereto, including the merits and risks involved in a purchase therein. Prior to any purchase, the Company will give prospective investors the opportunity to ask questions of and receive answers and additional information from it concerning the terms and conditions of this Offering and other relevant matters to the extent the Company possesses the same or can acquire it without unreasonable effort or expense. Prospective investors should inform themselves as to the legal requirements applicable to them in respect of the acquisition, holding and disposition of the Tokens upon their delivery, and as to the income and other tax consequences to them of such acquisition, holding, and disposition.
By their participation in the Offering, Purchasers will be deemed to have agreed that their participation will constitute their representation, warranty, acknowledgment and agreement to all of the statements about Purchasers under the section titled "Notice to Purchasers." Potential Purchasers should carefully read that section of this Memorandum.

The Memorandum does not constitute an offer to sell, or a solicitation of an offer to buy, an interest in any jurisdiction in which it is unlawful to make such an offer or solicitation. Neither the United States Securities and Exchange Commission (the "**Commission**" or "**SEC**") nor any other U.S. federal, state, or foreign regulatory authority has approved of this Offering. Furthermore, the foregoing authorities have not confirmed the accuracy or determined the adequacy of this Memorandum, nor is it intended that the foregoing authorities will do so.

Prospective investors are not to construe this Memorandum as investment, legal, tax, regulatory, financial, accounting, or other advice, and this Memorandum is not intended to provide the sole basis for any evaluation of a purchase of an interest. Prior to purchasing the Tokens, a prospective investor should consult with its own legal, investment, tax, accounting, and other advisors to determine the potential benefits, burdens, and other consequences of such purchase.

* * *