FAIR: Encrypted Blockchain Platform

A Fair, Private, and Agentic Layer 1 Blockchain

The FAIR Research Team

Version 1.0

Abstract. Bitcoin proved digital money. Ethereum unlocked programmable finance. FAIR introduces the next evolutionary leap forward: a Layer 1 blockchain built on Proof of Encryption (PoE). Proof of Encryption is a consensus-level innovation that enables fully encrypted transactions and privacy-preserving smart contracts. By integrating PoE directly into the consensus mechanism, FAIR eliminates Maximal Extractable Value (MEV) at its root, secures user and protocol-level privacy, and supports persistent autonomous AI agents. FAIR's architecture merges EVM Proof of Stake and PoE to unlock trillions in latent capital, by enabling a new era of onchain finance, advanced defi strategies, agentic applications and encrypted enterprise coordination.

1. Introduction

Blockchain technology has advanced in waves. Bitcoin established a decentralized monetary system, unlocking the idea of trustless value transfer. Ethereum built upon that foundation with programmable smart contracts, enabling the first generation of onchain applications. However, as more capital, complexity, and automation have moved into blockchain ecosystems, foundational flaws surfaced. The most critical are MEV (Maximal Extractable Value), lack of privacy, and fragile execution environments. These structural problems have left trillions in potential capital trapped offchain and prevent blockchains from absorbing the next wave of economic activity.

These flaws are not minor. MEV creates systematic inequity, allowing searchers to extract value by reordering or sandwiching transactions. This breaks fair markets and destroys trust. MEV exploitation has become a significant source of friction in blockchain ecosystems with malicious actors profiting at the expense of regular users, siphoning over 1 billion USD annually [1].

The absence of privacy makes sophisticated strategies impossible to protect, while AI agents and enterprises are rendered nonviable in an environment where visibility equals vulnerability. Existing networks bolt on privacy as an afterthought or treat MEV as inevitable, which compromises decentralization and limits innovation.

FAIR takes a different approach.

FAIR is an EVM Layer 1 blockchain that introduces **Proof of Encryption (PoE)**: a novel consensus primitive where transactions are encrypted before consensus and decrypted only after finalization. This ensures that no participant—validator, searcher, or bot—can view or exploit transaction content before it is immutably committed. It is the first protocol to offer **MEV resistance, programmable privacy, and agent-native execution as defaults.**

PoE is powered by BITE (Blockchain Integrated Threshold Encryption)—FAIR's protocol-level system for embedding privacy and fairness into consensus. BITE enables threshold encryption, re-encryption, and confidential computation as native capabilities of the chain.

By embedding these primitives directly into its core consensus layer, FAIR creates a secure, programmable environment where **autonomous agents, private financial strategies, and enterprise-grade workflows can thrive**. FAIR is a new substrate for encrypted, agentic coordination where privacy, fairness, and automation are not trade-offs but primitives.

In the sections that follow, we describe how FAIR is architected, what it unlocks, and how it launches. From DeFi to AI to enterprise, FAIR unlocks use cases that previous chains could not support and creates an execution environment built for the next trillion dollars of onchain activity.

2. FAIR Blockchain Design

2.1. High Level Architecture

FAIR is a sovereign Layer-1 blockchain network designed to deliver a high-performant and censorship-resistant execution environment. The network is secured by a permissionless validator set, denoted by V, from which a subset of nodes are selected to form a committee $C \subseteq V$. This committee is responsible for receiving transactions, running consensus, and producing blocks. The protocol is fully EVM-compatible and has fully programmable smart contract support. While maintaining interoperability within existing Ethereum tooling and developer workflows.

Each FAIR validator node utilizes a Trusted Execution Environment (TEE) – currently Intel® SGX – that is leveraged to securely perform threshold cryptographic operations including signature aggregation and threshold decryption. FAIR utilizes a Byzantine Fault Tolerant (BFT) protocol (detailed in Section 2.3) that is designed to provide deterministic finality and high transaction throughput in a fully asynchronous manner. The system is governed in an autonomous manner through a set of smart contracts deployed directly on FAIR itself known as FAIR Manager which contains the following modules: Staking, Committee, and Distributed Key Generation (DKG).

2.2. Committee

2.2.1. Committee Design

FAIR employs a rotating *committee-based* architecture to scale consensus and threshold cryptographic operations. Let V denote the full FAIR validator set. At any time, a subset $C \subseteq V$ is selected to serve as the *active committee*, responsible for ordering blocks and executing protocol operations on behalf of itself. Once blocks are produced and finalized by C , the remainder of validators in V *synchronize* to the finalized chain state.

FAIR uses threshold cryptography in the form of BLS threshold signatures to ensure that the committee cannot execute unless a sufficient number of members come to consensus. This provides mathematically proven safety guarantees at any given block with any given committee.

To be eligible for inclusion in C, each node must:

- be formally registered with FAIR Manager,
- have some delegated stake, and
- be deemed healthy according to the onchain liveliness protocol

Only validators who meet these constraints will be eligible for selection into a committee. At launch, the research team proposes a committee size of $|C| = 22$ with a threshold of $t = 15$, meaning at least 15 out of the 22 committee members must agree to execute an action on behalf of the supermajority, formerly denoted as C.

2.2.2. Committee Rotation

To ensure sufficient decentralization, prevent collusion, and enable broader validator participation over time, FAIR performs rotations of the active committee C.

Committee rotation is orchestrated by onchain logic managed through FAIR Manager. The selection of committee members takes into account multiple criteria:

- The node's percentage of total stake,
- The operational health and performance metrics of the node, and
- Randomness derived from the native onchain random number generator to ensure unpredictability.

To facilitate smooth transitions, a new committee is elected midway through the active epoch of the current committee. This timing provides sufficient opportunity to execute the Distributed Key Generation (DKG) protocol onchain, allowing the network to securely generate fresh threshold key shares and prepare for seamless handover.

Notably, FAIR is the first public blockchain to implement live committee rotations secured by BLS threshold encryption with zero-downtime transitions and no loss of data or disruption to consensus.

2.2.3. Committee Lifecycle

Each committee in FAIR progresses through a well-defined lifecycle consisting of three stages — Next, Active, and Previous — allowing for seamless and secure transitions of authority across epochs.

- Next Committee: This is the incoming committee that has been pre-selected by FAIR Manager based on current eligibility requirements (stake, health, registration). While in this stage, the committee prepares to assume responsibility at the next rotation point by undergoing a round of distributed key generation (DKG) and generating a common public BLS key and private key shares stored securely in each node's TEE. At this time it continues to synchronize state, but does not yet participate in block production.

- Active Committee: This is the committee currently responsible for producing blocks, signing messages, decrypting transactions, and executing transactions in the EVM on behalf of the validator set. The Active committee operates under a cryptographic threshold (e.g., 15 of 22 signatures) and has authority for the duration of a single epoch.

- Previous Committee: Once the rotation occurs, the former Active committee becomes Previous. It no longer has protocol authority but remains responsible for attesting that the hand-off to the new Active committee was completed correctly. Members of the Previous committee continue to monitor the chain and can be held accountable for misbehavior discovered post‑rotation

  By maintaining these three overlapping stages, FAIR ensures clean key handover, eliminates gaps in execution, and supports uninterrupted finality across committee transitions.

2.3. Consensus

FAIR builds on top of SKALE Consensus [2] – the world's first production Asynchronous Binary Byzantine Agreement (ABBA) protocol – while introducing additional steps within consensus to enable Proof of Encryption. Inheriting SKALE's leaderless and asynchronous design, FAIR provides fault tolerance and scalability through a Byzantine Fault Tolerant (BFT) architecture without sacrificing performance or finality.

FAIR leverages Boneh-Lynn-Shacham (BLS) threshold signatures, where BLS private key shares are assigned through a Joint-Feldman Distributed Key Generation (DKG) protocol executed directly on FAIR. The protocol guarantees data availability through a supermajority signature mechanism, whereby encrypted block proposals are validated and committed only after receiving signatures from more than two-thirds of participating nodes. By combining these privacy features with SKALE's high-throughput Ethereum Virtual Machine (EVM) and modular shard architecture, FAIR achieves scalable, secure, and confidential transaction processing — making it an ideal platform for privacy-sensitive decentralized applications.

2.3.1. Node Committees

Nodes participating in a FAIR consensus committee share a common threshold encryption (TE) public key and possess a set of TE private key shares. The size of the FAIR committee is typically $3t + 1$, where t is an integer.

A user can encrypt plaintext P using the TE public key. To decrypt the resulting ciphertext C, a threshold decryption protocol must be executed by a supermajority of $2t$+1 nodes. During the protocol, each node uses its private key share to generate a decryption share, which it then broadcasts to its peers. A total of $2t$+1 decryption shares are required to reconstruct the original plaintext P. For example, if the committee size is 100, at least 67 nodes must cooperate to recover P.

2.3.2. Encrypted Transaction Lifecycle

The transaction lifecycle of a blockchain implementing Proof of Encryption must defer from the traditional flow. FAIR implements Proof of Encryption in the form of BITE protocol (see Section 3.2), however, the lifecycle of such a transaction would still follow the same steps.

Note in the diagram below, the transaction includes all of the core steps required for interaction with a smart contract supported blockchain today, in addition to two key steps: Encryption & Decryption phases.

Traditionally, the flow of a transaction looks like such:

1. User creates transaction
2. User signs transaction with a wallet (or private key)
3. Transaction is submitted to the blockchain
4. Transaction is added to the memory pool (mempool) or it's pending queue equivalent
5. The transaction is included in a block proposal
6. Block proposal is finalized and then committed to the chain
7. The transaction is executed by the EVM

On FAIR, additional steps are slotted in after the first and sixth steps where the transaction (tx) tx.*data* and the tx.*to* fields are encrypted using the Threshold Encryption (TE) public key and then the consensus committee decrypts tx.data and tx.data respectively.

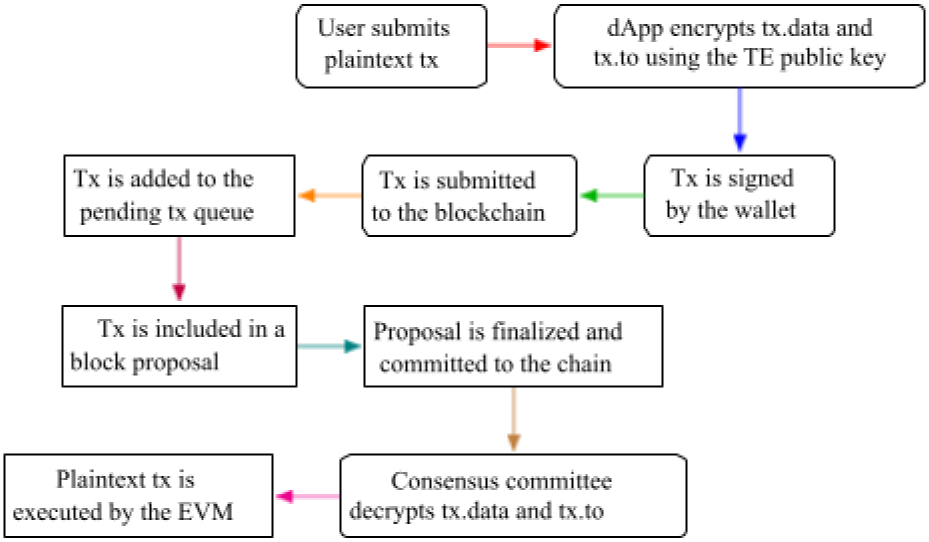
User submits plaintext tx
dApp encrypts tx.data and tx.to using the TE public key
Tx is signed by the wallet
Tx is submitted to the blockchain
Tx is added to the pending tx queue
Tx is included in a block proposal
Proposal is finalized and committed to the chain
Consensus committee decrypts tx.data and tx.to
Plaintext tx is executed by the EVM

Fig. 1. Encrypted transaction lifecycle in a BITE blockchain.

This design – unlike offchain ZK and L2 privacy solutions – operates natively within consensus negating the need for application level batching, custom sequencers, or fragile offchain logic.

2.3.3. Finality

The asynchronous and leaderless consensus within FAIR makes it the only permissionless Layer-1 EVM blockchain offering guaranteed single-slot — one-block — finality.

Single-slot finality is further defined as *instant finality*, where a transaction is considered irreversible and permanently committed to the ledger immediately after its inclusion in a block.

This architectural advantage introduces a set of guarantees unique to FAIR:

- Permanent Trust – With immediate settlement on FAIR, users and applications face zero risk of rollbacks or chain reorganizations. Finalized transactions are irreversible.

- Simplified UX & DX – dApps and users no longer need to wait *N* blocks for finality. CEXs and wallets can confidently settle within 1 block (which averages ~1 second).

- Financial Safety – The elimination of reorg risk enables high-frequency and high-value trading directly on an EVM blockchain layer with true instant settlement.

- Enhancing Layer 2s: FAIR by default improves guarantees for SKALE Chains and Layer 2 Rollups by offering instant cross-chain execution and settlement for sChains and rollups at a fraction of the price making FAIR the default best solution for application and ecosystem specific blockchains

- Cross Chain Composability – Bridging, intents, and messaging protocols rely on deterministic settlement. With single-slot finality, FAIR is the only EVM Layer-1 capable of enabling *block-n+1* settlement on external chains while preserving full state guarantees.

Once a node creates a block proposal, it shares this proposal with the network through a robust data availability process. This ensures that a supermajority of nodes (more than two-thirds) receive and verify the full block data before moving forward.

The process works as follows:

- The proposing node sends the block and transaction references to its peers.
- Peers reconstruct the block by matching the transactions they already have or requesting missing ones from the proposer.
- Each peer then confirms receipt by sending back a partial signature.
- When the proposer collects enough partial signatures from the supermajority, it combines them into a single proof that the block data is widely available.
- This proof is broadcast to all nodes, and subsequent votes on the block require this proof to be considered valid.

This protocol, backed by cryptographic key shares distributed among nodes, guarantees that any block finalized by consensus is fully available to the honest network participants — a cornerstone of FAIR’s instant, single-slot finality.

2.4. FAIR EVM

2.4.1. Hyper-Advanced C++ EVM

FAIR operates a high-performance Ethereum Virtual Machine (EVM) implemented in C++ – a low-level, highly performant programming language widely used in performance sensitive and distributed applications – to circumvent traditional limitations found commonly within the official Go Ethereum client (Geth) and associated forks.

2.4.2. Random Number Generation (RNG)

FAIR implements native, verifiable randomness as a fundamental protocol feature, ensuring secure and unbiased entropy generation. The randomness is collaboratively produced by the chain's active validator committee using a threshold BLS signature scheme.

During each epoch, a supermajority of validator nodes signs the block data, and the aggregated threshold signature is hashed to generate a secure, unpredictable random number. This random output is seamlessly exposed to smart contracts within the EVM through a precompiled contract interface, enabling deterministic, gas-efficient access to provable randomness.

By embedding randomness generation directly within the leaderless consensus layer, FAIR guarantees tamper-resistant and unbiased entropy, eliminating reliance on external oracles or vulnerable block hash sources.

This robust randomness powers critical decentralized applications, including validator rotation, leader election, onchain gaming, and lotteries, fostering trust and reliability in the ecosystem.

3. Proof of Encryption

3.1. Introduction to PoE

Proof of Encryption (PoE) is a foundational security protocol that guarantees the confidentiality and integrity of every transaction from initiation to final consensus within the FAIR blockchain. Unlike traditional blockchain systems where transaction data is often visible or partially exposed during propagation and validation, PoE enforces **full end-to-end encryption** throughout the entire transaction lifecycle.

This means that transaction details remain **cryptographically sealed and inaccessible** to any party—including validators, network nodes, or potential adversaries—until after the transaction has been irreversibly committed by the consensus mechanism. By doing so, PoE eliminates the risk of **premature parsing, front-running, manipulation, or data leakage** that could otherwise compromise user privacy or network fairness.

FAIR also utilizes threshold encryption to ensure that transaction decryption is only possible when a supermajority of the active committee collaborates. Specifically, once the block proposer collects more than two-thirds (>⅔) of the necessary decryption shares from committee members, the encrypted transaction can be securely decrypted.

3.2. BITE Protocol

FAIR implements Proof of Encryption through BITE protocol. With the provably secure consensus of FAIR being built on seven (7) years of research and production operation of SKALE Consensus; BITE's primary function is to enable the EVM and Solidity to handle threshold-encrypted user transactions and data.

The core objective of BITE is the same as Proof of Encryption: eliminate all MEV and bring the world onchain by enabling the capabilities that traditional web2 applications have.

BITE development has been segmented into four (4) phases: Threshold decryption during consensus, threshold decryption on smart contract data, threshold re-encryption, and threshold fully homomorphic encryption within smart contracts. The following sections 3.2.1-3.2.4 walk through each of these phases at a high level and provide some examples.

3.2.1. BITE Phase I

FAIR introduces encrypted transaction handling directly into the consensus process. Using a threshold decryption scheme, transactions remain fully encrypted — including transaction data and recipient addresses — until a supermajority of validators reaches agreement. Once consensus is secured, transactions are decrypted *just-in-time (JIT)* for execution in the EVM. This eliminates all front-running and MEV vectors while preserving single-slot finality and throughput.

- MEV-Proof Transactions: Prevents preview and extraction by validators or sequencers
- One-Round Encrypted Consensus: No additional consensus rounds or latency penalties
- Unlocks: Private DeFi, shielded prediction markets, and concurrent transaction flows. Encrypted CLOB or TWAP order execution

3.2.2. BITE Phase II

Phase 2 extends FAIR's encryption model to onchain data at rest. Smart contracts can now store encrypted state, which is selectively decrypted via a callback in block *N+1* using threshold decryption. This enables contracts to operate on sensitive information without revealing it publicly, while still enabling verifiable execution. Privacy becomes intrinsic to application logic — not an add-on.

- Encrypted Triggers: Capability to execute arbitrary private logic on any trigger. (i.e. if Bitcoin hits X, execute order(s))
- Privacy-Native Contract Logic: Enables sealed bids and deferred reveals
- Unlocks: Confidential compute, onchain gaming logic privacy, sealed-action workflows

3.2.3. BITE Phase III

With re-encryption, FAIR enables secure transfer of encrypted data between users and smart contracts. Encrypted outputs can be re-encrypted to a user's public key (or group key) without ever decrypting onchain, granting selective access while preserving privacy. This creates a powerful primitive for private coordination, access control, and data mobility across decentralized systems.

- Fine-Grained Encrypted Access Control: Re-encrypt results to specific users/groups
- Trustless Confidential Coordination: Enables private DAOs and encrypted escrows
- Unlocks: Secure data sharing, dispute resolution, enterprise workflows, private governance

3.2.4. BITE Phase IV

Phase 4 culminates in executing mathematical operations directly over encrypted values — enabling smart contracts to compute on data that no validator, user, or contract can read. Utilizing homomorphic encryption and ZK-like techniques, FAIR unlocks *verifiable privacy-preserving computation* entirely on chain and at scale.

- Private Compute on Encrypted Inputs: No decryption required for execution

- Confidential Logic + Confidential Data: Unlocks fully private program states
- Unlocks: Confidential tokens, onchain banking, private voting for DAOs and governments

3.3. Native MEV Resistance

BITE achieves provable MEV-resistance by encrypting the *destination address* and *data field* of transactions prior to their submission to the blockchain.

When a user submits a transaction, the payload is encrypted using the threshold encryption algorithm native to FAIR consensus. This encryption is performed directly on top of the existing Ethereum transaction format and is designed to be transparent to wallets, RPC infrastructure, and existing client software — no changes to the standard developer/user tooling are required.

In Ethereum, the destination address identifies the smart contract that will be invoked, while the data field specifies the function parameters — such as the selector, price, amount, and asset pair. These values are exactly what MEV actors analyze in order to front-run or censor transactions. BITE prevents such extraction by concealing them until **after** the encrypted transaction has been finalized onchain. As a result, MEV searchers are unable to distinguish or prioritize transactions based on their economic content. The transaction remains fully opaque until it is too late for an attacker to reorder it.

The core innovation of BITE lies in its **two-phase execution model**:

1. **Inclusion Phase** — encrypted transactions are verified and finalized onchain.

2. **Execution Phase** — immediately after block finality is reached, but prior to EVM execution, the FAIR validator committee runs a threshold decryption protocol and reveals the plaintext destination and calldata. At this point, the decrypted transaction is executed by the unmodified EVM.

Because inclusion happens *before* decryption, the blockchain achieves **commit-then-reveal** semantics, which provably eliminates frontrunning and censorship based on transaction content — unless more than two-thirds of the validator committee becomes malicious (e.g., >67 for a 100-member committee).

Importantly, other transaction fields such as the sender address, nonce, gas limit, and gas price remain unencrypted, preserving full compatibility with the Ethereum transaction lifecycle and tooling. Once decrypted, the transaction is processed by the EVM exactly as if it had been submitted in plaintext, requiring **no changes** to existing smart contracts.

This construction is made possible only because FAIR consensus natively supports **threshold encryption**, with fresh public/private keys generated at the start of each epoch through an **onchain Distributed Key Generation (DKG) protocol**. Each epoch, a new committee is randomly selected from the permissionless validator set to participate in encryption and decryption duties. SKALE first pioneered the use of DKG within a production blockchain, and FAIR remains the only production Layer-1 to couple DKG, threshold BLS signatures, and encrypted mempool-less execution — making BITE's MEV-free property uniquely difficult to replicate on other blockchains.

3.4. Censorship Resistance

Transactions making use of BITE Protocol are automatically provided with censorship resistance at the blockchain level since the destination address – i.e. the transaction *to* field – is encrypted to ensure that routine or consistent transactions with similar data and gas are not traceable.

4. FAIR Use Cases

FAIR unlocks application classes that were previously impossible or too risky to deploy on public blockchains. By eliminating MEV at the consensus layer, embedding programmable privacy, and enabling native AI agents, FAIR becomes the foundation for a new wave of encrypted, automated, and fair coordination across sectors.

4.1 MEV-Free Financial Coordination

DeFi is broken by design with visible mempools, frontrunning, and strategy leakage are the norm. FAIR fixes this at the base layer:

- **Encrypted Limit Orders & TWAPs**: Traders can express intent without revealing size or direction.
- **Structured Vaults & Index Products**: Native vaults manage portfolio rebalancing, yield harvesting, and DCA without leaking logic.
- **Confidential Tokens & onchain Banking**: TFHE-wrapped ERC-20s enable fully private balances, payments, lending, and staking.

Unlocked by BITE Phases 1–4.

4.2. Agentic AI Infrastructure

FAIR is AI-native. Agents can persist, execute, and coordinate securely onchain, enabling:

- **Autonomous Trading Agents**: Agents rebalance, farm, and execute strategies in encrypted environments.
- **Self-Defending Contracts**: Embedded LLMs review contracts pre-deploy and simulate transactions in real-time to prevent exploits.
- **Collaborative AI Systems**: Multi-agent protocols can coordinate capital or behavior without leaking internal logic.

Enabled via Trusted Execution Environments and onchain agent runtime.

4.3. Encrypted Enterprise Coordination

Enterprises have historically been unable to operate on public blockchains due to three constraints: visible logic, lack of compliant privacy controls, and an inability to automate complex workflows securely. FAIR removes all three.

- **Encrypted Compliance & Access Control**: KYC, AML, and identity gates can now run onchain without exposing sensitive data. Through threshold re-encryption, permissions and audit trails can be enforced privately and dynamically. To support institutional compliance requirements, FAIR enables opt-in transparency via view-only keys. Enterprises can generate cryptographic attestations of transaction history or contract behavior without revealing full execution logic. This strikes a balance between regulatory visibility and operational confidentiality.
- **Secure Workflow Automation (Payroll, Escrow, Procurement):** Internal processes (payroll disbursements, procurement approvals, cross-departmental funds transfers) can now run as encrypted smart contract flows. Logic is kept private, data is shielded, and execution is verifiable.
- **Confidential Licensing, Copyright, and IP Controls:** Software licenses, digital rights, and subscription access can be distributed via smart contracts that enforce logic without disclosing it. Encryption ensures terms and usage cannot be spoofed, copied, or exploited.
- **Encrypted Supply Chains & Logistics:** Origin metadata, quality certificates, or routing instructions can be encoded onchain, and selectively revealed via re-encryption. This creates trusted but private coordination across manufacturers, suppliers, and vendors.

Powered by BITE Phases 2–3.

5. Conclusion

The blockchain industry is at a turning point. MEV, transparency-as-liability, and execution asymmetries are no longer acceptable trade-offs. For the next trillion dollars of capital, AI apps, and coordination to move onchain, the foundational substrate must change.

FAIR enables that movement.

By embedding Proof of Encryption directly into consensus, FAIR eliminates MEV at its root, enables composable privacy, and creates an execution layer where autonomous agents and enterprises can operate securely. It unlocks sophisticated financial strategies, native AI automation, and encrypted real-world workflows all in a developer-friendly, Ethereum-compatible environment. FAIR tracks net protocol revenue, fee burn, and trader win-rate as not just latent TVL. This ensures alignment with actual user value and market traction

The next generation of blockchains are private, autonomous, and **FAIR**.

References

1. **Galaxy Digital Research Team, A Perspective on Maximal Extractable Value.** https://www.galaxy.com/insights/perspectives/distribution-of-mev-surplus/

2. **SKALE Labs, SKALE Provably Secure Consensus Spec.** https://github.com/skalenetwork/skale-consensus/blob/develop/docs/consensus-spec.md/

3. **BITE Research Team, BITE Whitepaper**

   https://cdn.prod.website-files.com/625c39b93541414104a1d654/6826797bf4b6c19e48a1591c_1a7a26363c6683b20a686da37f7bdd64_BITEWhitePaper.pdf

This document is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in the N.O.D.E. Foundation, SKALE Labs, Inc. or any related or associated company. Any such offer or solicitation would only be made by a confidential offering memorandum and in accordance with applicable securities and other laws. SKALE Labs may make changes to this White Paper at any time. Please visit www.SKALE.space for the most recent version.