REFLEXIVITY RESEARCH

reflexivityresearch.com

FAIR

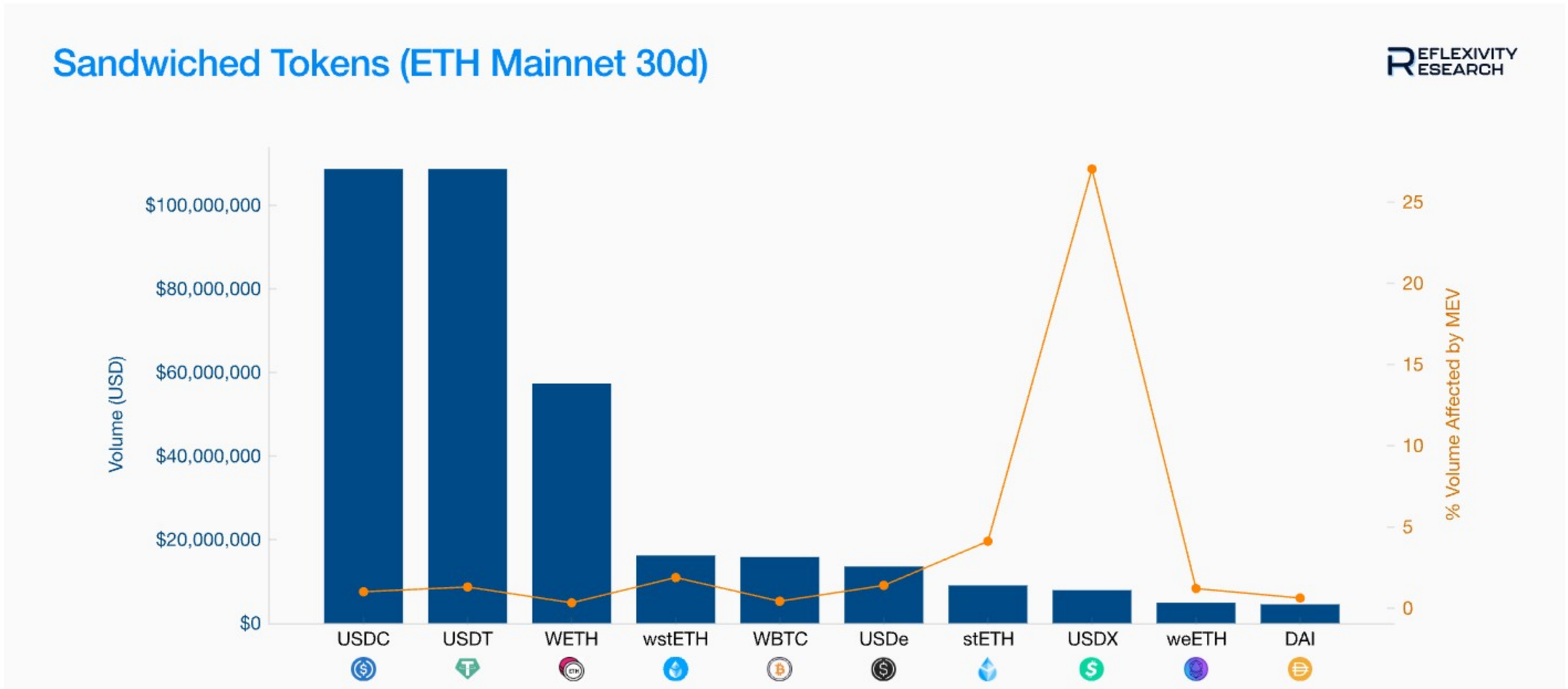
A New Era of Fairness in Crypto

FAIR

FAIR

Introduction to MEV

Maximal Extractable Value (MEV) refers to the excess profit that blockchain insiders (miners, validators, or even bots) can capture by manipulating the ordering, inclusion, or censorship of transactions in a block. In practice, MEV manifests through tactics like **front-running** and **sandwich attacks**, where automated bots exploit knowledge of pending transactions in the public mempool. For example, bots may detect a large decentralized exchange trade and **insert their own transactions before and after** the victim's trade (a sandwich attack), profiting from price changes at the expense of the user. Such manipulation has caused significant losses, with **users having lost nearly $2 billion to MEV since 2020**. MEV has thus been described as an "invisible tax" on crypto users, siphoning value from everyday traders into the pockets of a few savvy actors. Take the below illustration as an example, which highlights the percentage of volume affected by sandwich attacks on the Ethereum mainnet for the last month:



This is more than just an economic nuisance; **MEV undermines the core principles of blockchain fairness and decentralization**. By exploiting transaction visibility, MEV extractors gain an unfair advantage, recreating the power imbalances that blockchains were meant to eliminate. **Ordinary users suffer worse trade prices (higher slippage) and unpredictable outcomes due to these exploits**. In fact, on chains like Ethereum and Solana every trade can incur a hidden MEV cost, essentially a transaction tax on users. Industry responses so far have been imperfect, **often monetizing MEV instead of truly fixing it**. With onchain volume poised to **increase exponentially** (e.g., through rising stablecoin use and autonomous AI trading agents), leaving MEV unchecked could snowball into a **$100 billion+ extraction problem** in the coming years. In summary, MEV represents a pressing challenge: it erodes user trust, creates unfair markets, and, if not mitigated at the protocol level, will continue to worsen as Web3 adoption grows.

FAIR Overview: A Blockchain Built for Fairness

FAIR is a next-generation Layer-1 blockchain designed from the ground up to **eliminate MEV at the consensus level**. Developed by the SKALE Labs team, FAIR's mission is to embed fairness and privacy into the base protocol of a blockchain without sacrificing performance or compatibility. In the evolution of blockchains, if Bitcoin brought security,Ethereum brought programmability, and Solana brought performance, FAIR's contribution is **provable fairness and MEV-resistance**.

At its core, FAIR is the f**irst Layer-1 chain to implement BITE (Blockchain Integrated Threshold Encryption) Protocol** natively. This means that every transaction on FAIR is handled in encrypted form until after the network reaches consensus, **making front-running or sandwich attacks impossible** on this chain.

This breakthrough enables entirely new DeFi primitives like sealed-bid auctions, encrypted order books, and truly private algorithmic trading - use cases that were previously impossible to achieve in a decentralized system. FAIR unlocks a new era of onchain finance where privacy, fairness, and automation can finally coexist.

By stopping MEV at the consensus layer, FAIR establishes a new standard for securely processing decentralized transactions. For users, what-you-see-is-what-you-get, i.e, you no longer have to fear hidden bots exploiting your trades or miners extracting value, because the blockchain itself guarantees fair ordering.

FAIR's origins lie in the SKALE ecosystem's recognition that one size does not fit all for blockchain needs. SKALE has been operating a network of high-performance, gasless chains for specific dApps, but **FAIR was introduced as a permissionless, MEV-resistant L1 to complement these chains**. FAIR compliments the existing SKALE ecosystem of chains, but runs as an independent Layer-1 with its own token and fee market.

The relationship is synergistic: **SKALE's existing dApps** can tap into FAIR's deep liquidity and fair execution, and in turn, FAIR benefits from an immediate developer and user base. In effect, SKALE will continue to provide scalable, gas free, user-friendly app-specific chains, while FAIR acts as the **home for DeFi & liquidity for the whole ecosystem. To give back even further to the SKALE community, a large percentage of FAIR's native token will be allocated for airdrops to SKL holders**. FAIR also features a **hyper-optimized EVM execution environment** to maximize performance for complex DeFi and AI use cases. **FAIR EVM** is a custom high-performance implementation in C++ that supports asynchronous, parallel transaction execution with instant finality. This makes FAIR not only fair, but extremely fast and scalable. Combined with onchain privacy features (described below), FAIR is positioned as an ideal platform for the next generation of DeFi and AI-driven applications. In short, FAIR's purpose is to be a **provably fair and private smart contract platform** that resolves MEV, empowers advanced use cases, and works in tandem with SKALE's existing infrastructure to drive Web3 forward.

BITE Protocol Explained: Consensus-Level MEV Resistance

The technological breakthrough enabling FAIR's MEV resistance is **BITE Protocol**, which stands for *Blockchain Integrated Threshold Encryption*. Unlike stopgap MEV solutions that add external relays or partial privacy, BITE is built **into the consensus layer** of the blockchain. It **doesn't just minimize MEV, it removes the root cause** by ensuring transaction details are encrypted until a block is finalized. In essence, BITE makes every transaction like a **sealed envelope**: you sign your transaction, and it gets sealed (encrypted) before it ever reaches the mempool, **so no validator or bot can peek at the contents**. Only after the block is agreed upon do a group of network nodes collectively decrypt the envelope and execute the transaction. With **no visibility, there is no opportunity for MEV** i.e, frontrunning and other attacks become structurally impossible on a BITE-enabled chain.

How does BITE work under the hood?

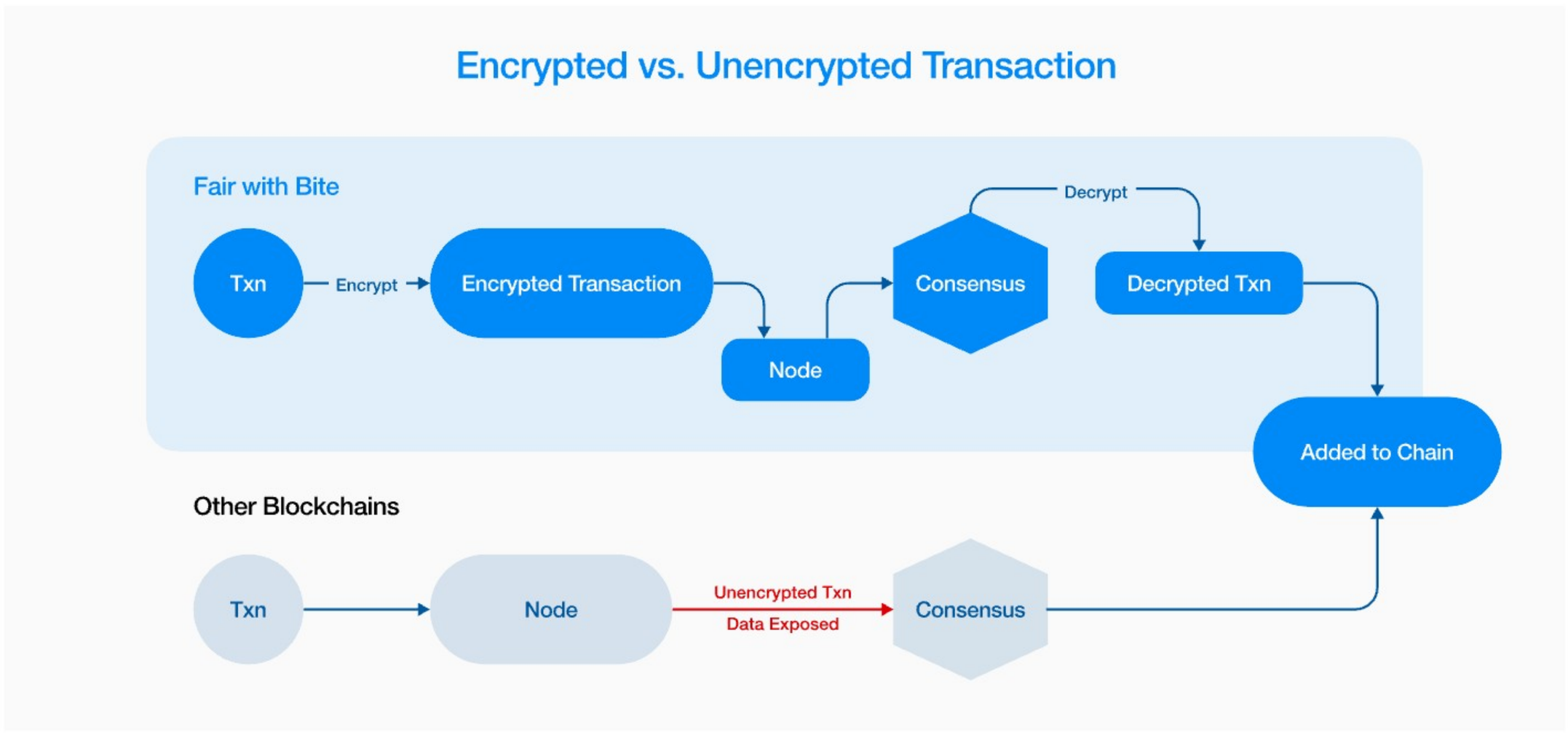
Seal – Your wallet encrypts the transaction's data + destination address with the committee's public key.
Blind Ordering – Validators see only an encrypted transaction; they finalise block order without knowing the transaction's details.

Decryption by Committee – After finality, ≥ 2/3 of the committee combine their key-shares (e.g. 67 / 100) to decrypt; no single node can peek.

Execute – Once decrypted, transactions are executed transparently within the EVM. The process then repeats for the next block.

Because **transaction details remain encrypted and hidden until after the block order is finalized**, frontrunning, sandwich attacks, and mempool other forms of manipulation and MEV are effectively impossible.

This can be more simply visualized in the illustration below:



Security model
BITE marries **threshold cryptography** with **TrustedExecutionEnvironments (TEE)**

- A super-majority of validators (≥ 2⁄3) holds key-shares; no single node can decrypt.
- Decryption shares are generated **inside SGX enclaves**, so private keys and plaintext never touch untrusted memory.
- Result: transaction privacy and MEV resistance hold as long as the committee's honest majority assumption does.

BITE is undergoing the below phases of its roadmap

Four Phase Roadmap

Phase	What it adds	Example use-cases
1. Encrypted transactions	Data + destination encrypted until block finality → no frontrunning/sandwiching/ censorship.	Fair DEX trades, sealed-bid auctions, cheat-proof games.
2. Encrypted contract state	Contracts can store data encrypted and request decrypt in the next block.	Sealed-bid auctions, time-locked wills, conditional triggers.
3. Threshold re-encryption	Contract can re-encrypt ciphertext to another user/group key without revealing plaintext.	Private social posts, subscription content, confidential DAO votes.
4. TFHE onchain	Basic maths on ciphertexts inside Solidity: plaintext never revealed.	Fully private DeFi, encrypted on-chain banking. zero-knowledge credit scoring.

Together these stages turn FAIR into a **privacy-preserving, MEV-proof smart-contract platform**, evolving from hidden trades (Phase 1) to full confidential computing (Phase 4).

Across these four phases, BITE gradually transforms what blockchains can do. It **bridges the gap between Web2 and Web3 privacy** by enabling use cases like **sealed auctions, private messaging, confidential trading, encrypted gaming, private DAOs, and fully onchain banking**, all on a decentralized network.

In summary, BITE Protocol provides FAIR with *consensus-level MEV resistance from day one* and a clear path to unmatched privacy features through threshold encryption, re-encryption, and homomorphic encryption at scale.

Who Benefits and How - Built for the Future of DeFi and AI

A blockchain that is **provably fair and private** at the base layer has wide-ranging benefits for many stakeholders in the crypto ecosystem:

FAIR's proof-of-encryption model delivers three immediate wins.

First, everyday traders simply keep more money: with a sealed mempool, bots cannot front-run, sandwich, or skim the hidden "MEV tax," so swaps execute at the price users expect, and limit orders finally become safe.

Second, DeFi venues (especially on-chain central-limit-order-books) can match the fairness of CeFi while adding confidentiality: orders remain invisible until block finality (Phase 1), and forthcoming phases enable sealed bids and private order-books, eliminating manipulative re-ordering and letting liquidity stay onchain.

Third, autonomous AI agents and quantitative traders gain a high-speed, private execution environment: FAIR's parallel C++ EVM lets bots rebalance or arbitrage at scale without revealing strategies or being copied, because no observer can see transaction details before they're locked in the chain. In short, FAIR cuts hidden costs for users, makes DeFi markets provably fair, and gives onchain AI a secure, MEV-proof home.

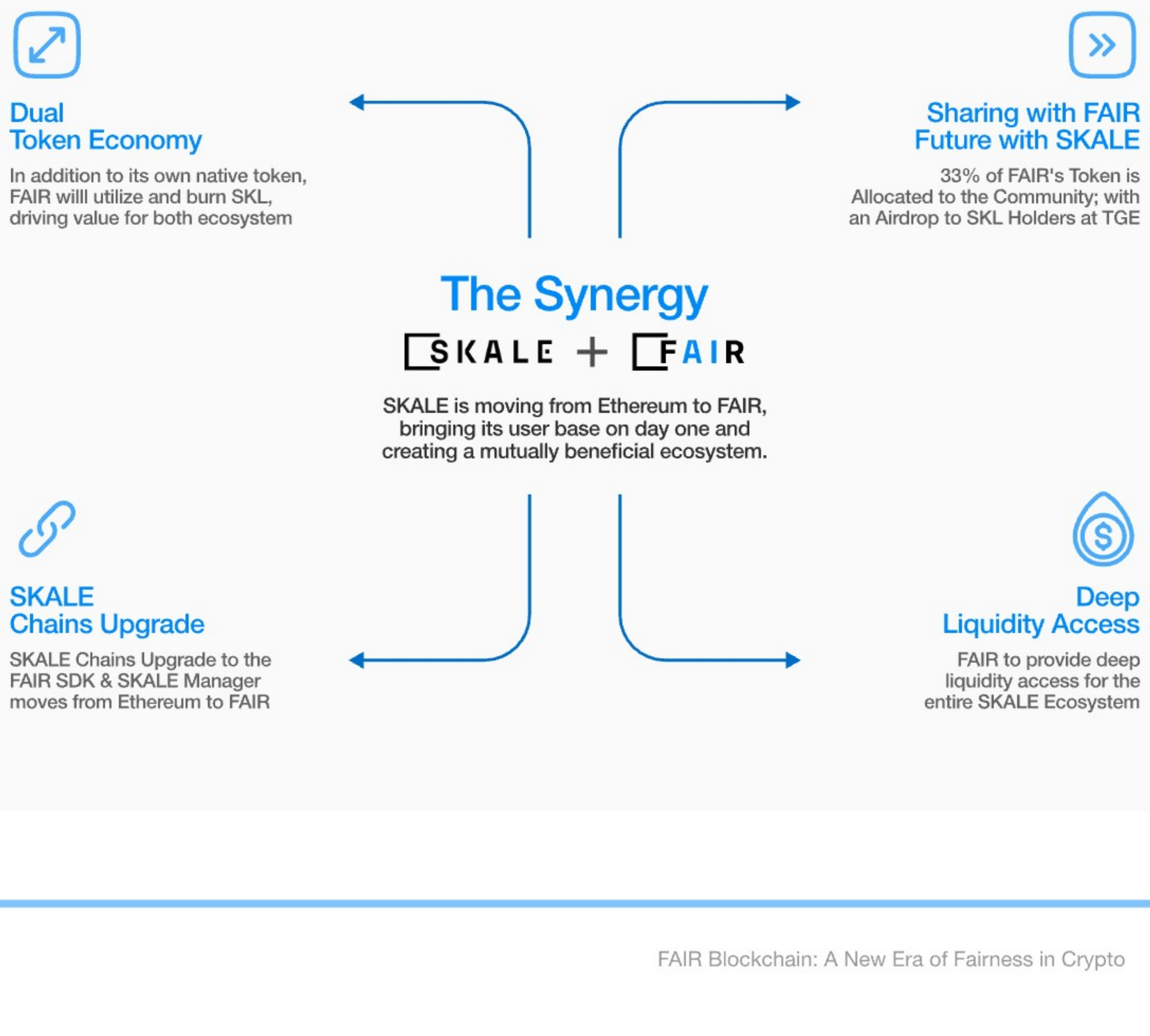
Competitor Landscape: MEV Mitigations vs. BITE's Approach

The crypto industry is well aware of the MEV problem, and several stopgap solutions have emerged. The most prominent are **private mempools and relay services**. For example, Flashbots on Ethereum pioneered an off chain "dark pool" where users can send transactions that won't be seen by the public mempool, thus avoiding frontrunning. While this and similar services (Eden Network, BloXroute's Flashbots alternatives, etc.) have provided some relief, they come with significant drawbacks. **Private mempool solutions are typically centralized services and opt-in only**. Users or dApps must trust a third-party relay to handle their transactions, and those not explicitly opting in remain vulnerable. Moreover, these systems often just shift who captures MEV (from independent bots to miners/validators via auctions) rather than eliminating it, the **extraction still occurs**, albeit in a perhaps more orderly fashion. As a result, the fundamental unfairness and inefficiency of MEV persist as an "accepted" cost on most chains. In short, earlier solutions **treat the symptoms** of MEV but not the cause: the fact that transactions are exposed in plaintext before finalization.

BITE and FAIR's approach is markedly different. **Instead of a band-aid, it's a cure**: by design, the blockchain never exposes transaction content prematurely. This means **MEV protection is automatic and universal** for all users, not just those who know to use a special service. There's no need for users to trust a separate relay or pay kickbacks to miners; the consensus protocol itself guarantees fairness. This "first principles" solution closes the gaps that other approaches leave open. For example, even with Flashbots, a user might accidentally broadcast a transaction to the public mempool, or the relay itself could be exploited or censored (and it introduces centralization). With FAIR's onchain encryption, by contrast, every transaction from every user is protected by providing **gapless MEV resistance at the protocol level**.

It's worth noting that some upcoming projects and research are also exploring MEV-resistant designs (such as proposer/builder separation in Ethereum, or alternate fair ordering protocols). However, **FAIR is the first L1 to implement a provably secure, cryptographic solution to MEV**. By integrating threshold encryption in a decentralized way, FAIR avoids reliance on any single party and maintains decentralization. The SKALE team leveraged their unique expertise, SKALE's network already supported distributed key generation and threshold signatures in production, to build something that wasn't readily achievable on other chains without a hard fork. In summary, while others in the industry have attempted to mitigate MEV through off-chain agreements or minor tweaks, **FAIR's BITE protocol offers a holistic fix. It directly addresses the root cause (mempool transparency) within the consensus mechanism**, delivering an unmatched level of fairness. This differentiator puts FAIR in a league of its own: as one report aptly put it, **FAIR is "the first un-MEV-able blockchain."**

FAIR and SKALE Synergy: Economic Model & Adoption



Dual-token model (NOTE: Tokenomics are still in progress and subject to passing DAO votes)

- **Two tokens, two jobs.**
  FAIR pays gas, secures staking, and runs governance on the new Layer-1.
  SKL is the “fuel” you can **burn** to access cetain features of FAIR.

- Every **burn** is permanent, so SKL supply falls as FAIR activity rises.

- **Day-one airdrop.**
  A portion of FAIR’s genesis supply (part of a 33 % community pool) is earmarked for an airdrop to SKL holders at TGE, subject to DAO approval and lock-ups. That gives the existing SKALE community direct stake in FAIR from the start.

Bootstrapping & tech fit

Day-one validator set. Top SKALE operators like Chorus One, Figment, and Blockdaemon will validate FAIR on launch, bringing proven uptime and credibility.

Good-bye Ethereum admin fees. SKALE Manager, the smart contracts that run the SKALE Network, will migrate from Ethereum to FAIR, cutting operational additional value leaks towards Ethereum.

Bottom line: FAIR drives demand for SKL through mandatory burns, rewards SKL holders with an airdrop, and lets every SKALE dApp tap fair, liquid markets without leaving the ecosystem, all while shrinking external costs.

*It’s important to note that details on timing, eligibility, lock periods, and distribution mechanics are subject to change and will be announced closer to mainnet launch. This airdrop is also contingent on a successful mainnet launch and onchain governance approval from the respective DAOs.

In practical terms, the **rollout is planned in three key phases:**

Phase	Key activities	Resulting outcome
1. Launch FAIR Mainnet	• Deploy FAIR blockchain with BITE Phase 1 active • Bring online a decentralised validator set (incl. leading SKALE validators) • Distribute FAIR tokens, allocating a portion to SKL holders and other stakeholders	Establishes the MEV-resistant Layer 1 and opens FAIR for dApp deployment
2. Integrate FAIR SDK into SKALE chains	• Upgrade existing SKALE chains and tooling to embed FAIR features • Enable encrypted transactions on gas-free SKALE via the FAIR SDK • Provide seamless routing of suitable transactions to FAIR and shared liquidity/services	Makes SKALE "FAIR-aware," extending BITE's benefits and linking ecosystems
3. Migrate SKALE Manager to FAIR	• Shift SKALE's administrative/orchestration contracts from Ethereum to FAIR • Redirect functions such as chain creation, staking and governance to FAIR, with associated SKL burning	Establishes the MEV-resistant Layer 1 and opens FAIR for dApp deployment

Through these steps, **FAIR adds substantial utility to SKALE**. SKALE dApps gain access to a **fair, liquid financial layer** with deep liquidity and MEV-free execution. SKL token holders benefit from new use cases and burn mechanisms, potentially increasing the value of SKL as network usage grows. Meanwhile, FAIR benefits from instant network effects, hundreds of dApps, and a plethora of users from SKALE can become FAIR users without friction. This kind of synergy between a scaling solution and a robust L1 is quite unique in the blockchain space.

Conclusion: What to Expect Next

FAIR is more than the next Layer-1; it is the first purpose-built home for **provably fair, privacy-preserving finance**. By encrypting every transaction until after finality with the BITE Protocol, the chain removes the structural advantage MEV bots and insiders have enjoyed since DeFi's birth. The result is a market where **price quotes hold, strategies remain private, and value accrues to users instead of extractors.**

What DeFi Looks Like on FAIR

Today on most chains	Tomorrow on FAIR
Slippage and hidden "MEV tax" on every swap	**Sandwich-free swaps** that fill at the price you sign
Public mempools that broadcast new-token launches to snipers	**Sniper-proof launchpads** where allocations stay secret until the block is sealed
Sealed-bid auctions only possible off-chain or behind a gate	**Fully on-chain sealed auctions** where bids are revealed simultaneously and immutably
Limit orders and index rebalancing restricted by frontrunners	**MEV-protected CLOBs, limit orders and automated indices** that can finally live on-chain
Liquidity fragmented across roll-ups and sidechains	A single, **high-performance EVM** backed by SKALE's user base and liquidity flows

For builders, this means launching dApps that were previously impractical: private derivatives venues, AI-driven market-making bots whose code is never copied, and consumer-grade wallets where users simply swap without thinking about slippage settings. For everyday users, it means **lower costs, predictable execution and true ownership of trading intent**.

Why It Matters

- **Fair pricing** – no more invisible tax siphoned to unseen actors.
- **True privacy** – strategies, bids and wallet activity stay confidential until they are irreversible.
- **Level playing-field liquidity** – institutions, AI agents and retail trade on equal terms.
- **Composability without compromise** – the familiar EVM tool-chain, now protected at consensus.

You are now able to sign up for the waiting list at fairchain.ai and be first to deploy (or simply trade) in a world without MEV.

REFLEXIVITY RESEARCH

“

Our mission is to bridge traditional finance into digital assets through our crypto native research.