Sundial Whitepaper

Working Draft - March 19th, 2025

In collaboration with the Midgard tech stack, Sundial is the first optimistic rollup network on Cardano. It offloads transaction processing from Layer 1 (L1) to Layer 2 (L2) while maintaining L1's security and decentralization properties for those transactions. As a result, it can handle a significantly higher volume of transactions without compromising on security. This whitepaper outlines the interactions between L1 and L2, as well as going into detail about Sundial's specific target market fit: being a hybrid L2 for other UTxO chains, including Bitcoin, and scaling new and novel use cases as a "super" UTxO chain.

The optimistic rollup model implemented in Sundial represents a significant advancement in the scalability and security of general-purpose Layer 2 solutions on Cardano. Below are detailed economic incentives that ensure the protocol's integrity and efficiency.

Operators guarantee the validity of their committed blocks by posting bonds, which are slashable if the blocks are proven invalid. Members of the public are incentivized to watch the operators' blocks, and they are rewarded with a portion of the slashed bonds when their fraud proofs prevent invalid blocks from merging into Sundial's confirmed state. Sundial's architecture leverages a family of smart contracts on Cardano's L1 to manage state transitions and enforce the security of the L2 operations. Key components include a robust operator management system, efficient storage for transaction blocks committed from the L2, and a comprehensive mechanism for submitting and validating fraud proofs. Overall, Sundial's design aims to provide a scalable and secure solution for the growing needs of the Cardano ecosystem and beyond.

Technical Overview:

Sundial is a Layer 2 (L2) scaling solution for the Cardano blockchain. It employs optimistic rollup technology to enhance Cardano's capacity to process transactions and host more complex applications, delivering a richer user experience at a more competitive cost. As Cardano continues to grow in usage and demand, scaling solutions like Sundial are critical for maintaining high performance and low transaction costs.

Optimistic rollups process blocks of transactions off-chain and commit those blocks' headers onchain to the L1 ledger. Each block is committed by a Sundial operator who guarantees the block's validity. The block then waits in a queue for at least a fixed duration to be merged into the confirmed state of the optimistic rollup on L1. The operator must collateralize their guarantee with a bond deposit and publish the full contents of the block on the publicly accessible data availability (DA) layer. While a committed block is queued, anyone can inspect its contents on the data availability layer and ascertain whether it is valid. If someone detects that the block is invalid, they can submit a fraud proof to prevent it from being merged into the confirmed state, slash the operator's bond, and receive a portion of the forfeited bond as a reward. Thus, an optimistic rollup can process a large number of transactions offchain while maintaining security and finality properties that are similar to transactions processed directly onchain, as long as:

- The bond requirement for the rollup's operators is large enough to discourage fraud.
- The reward for preventing an invalid block from merging is large enough to encourage public vigilance in watching the operators.
- The waiting period for committed blocks is long enough to allow the watchers to detect and prove fraud before those blocks are merged.
- The data availability layer is accessible by anyone who wishes to inspect the rollup blocks at any time that they wish to do so.

Whenever the latter three security parameter values are calibrated to provide a high probability of invalid blocks being detected and disqualified, the bond requirement is a strong deterrent against operators attempting fraud. An operator cannot dismiss the forfeited bond as merely a "cost of doing business" paid to obtain potentially larger revenues from fraud. Whenever an invalid block is disqualified, it does not affect the confirmed state, so there are no revenues from that fraud to offset the operator's forfeited bond.

The main design goal of Sundial is to streamline the processes by which blocks are committed/merged, fraud is detected, and fraud proofs are verified onchain. Advancing this goal allows the security parameters to be calibrated to achieve a better balance between security, transaction throughput, confirmation time, and community participation in committing blocks and detecting fraud.

Scalability and efficiency

By processing transactions off-chain and only validating them on-chain when fraud proofs challenge them, Sundial significantly increases throughput and reduces costs for Cardano transactions. Its rollup blocks use sparse Merkle trees and compact state representations to enhance the protocol's efficiency further, enabling it to handle a large volume of transactions without overburdening the L1.

The deterministic nature of Cardano transactions allows Sundial fraud proofs to pinpoint the specific site of a transaction that violated Sundial's ledger rules, without having to look at any other parts of that transaction, any other unrelated transactions within the block, or any other blocks. This keeps fraud proofs and their onchain validation procedures small and efficient, which reduces the time and cost needed to submit fraud proofs when invalid blocks are detected, which makes it feasible for a wider group of people to police Sundial's blocks. In this way, Sundial significantly reduces fraud proof size relative to optimistic rollups used in Ethereum and other account-based blockchain ecosystems, where a much larger part of the global blockchain state needs to be inspected when constructing and verifying a fraud proof.

Censorship resistance and fallback mechanisms

On its own, the optimistic rollup mechanism described above ensures a high-level of assurance for the validity of block headers committed to the state queue and merged to Sundial's confirmed state. However, it does not prevent operators from censoring users' deposits, withdrawals, and L2 transactions. Consequently, Sundial's consensus protocol includes additional smart contract mechanisms to provide censorship resistance for these events. Sundial deposits and withdrawals are initiated via L1 smart contracts that assign definite inclusion times to them. An operator block is invalid if it contains these inclusion

times in its event interval but fails to include the associated deposit or withdrawal events. This ensures that if operators continue committing blocks to Sundial's state queue, then they cannot ignore deposit and withdrawal events. Sundial L2 transaction requests are typically submitted to operators via a publicly accessible API, and they can be ignored by operators. However, any user can escalate his L2 transaction request by posting a transaction order on L1. Similar to Sundial deposits and withdrawals, an L1 transaction order is assigned an inclusion time that guarantees its inclusion in a subsequent valid block. If Sundial operators stop committing blocks at all to the state queue, then the inclusion times on their own cannot guarantee that deposits, withdrawals, and L2 transactions will be processed in a timely manner. However, for this extreme case, Sundial's consensus protocol includes the escape hatch mechanism, which allows a special non-optimistic block to be appended to the state queue by a non-operator. This block can include any deposits, withdrawals, and L2 transactions that are verified on L1 to comply with Sundial's ledger rules. This ensures that user funds cannot be stranded on Sundial even if its operators entirely stop committing blocks.

Sundial Use Cases

The UTxO model, used by Bitcoin, Dogecoin, Litecoin, and other major blockchains, lacks native smart contract capabilities. As a result, trillions of dollars in hard assets remain idle, unable to generate yield or utility. Previous attempts at Bitcoin Layer-2 solutions, primarily using Ethereum Virtual Machine (EVM) architectures, have faced security vulnerabilities, technical limitations, and adoption challenges.

Sundial's primary use case—beyond scaling Cardano—is to seamlessly merge Bitcoin's vast liquidity with Cardano's advanced eUTxO smart contracts, enabling next-generation decentralized finance (DeFi). As the first sophisticated Layer-2 on Cardano, Sundial is purpose-built for scalability, reduced transaction costs, and institutional-grade security.

Key Innovations

Sundial introduces groundbreaking features to unlock new capabilities for UTxO-based blockchains:

- Babel Fees – Enables users to pay transaction fees with any token, enhancing DeFi accessibility and usability.
- ZK Bridge – A fully trustless rollup bridge secured by zero-knowledge proofs, ensuring seamless interoperability with metaprotocols.
- Native UTxO Security – Eliminates vulnerabilities common in other blockchain ecosystems:
    - No wallet drainers
    - No smart contract exploits
    - No failed transactions
    - No network outages
- Cardano Ecosystem Integration – Partners with leading DeFi and gaming protocols on Cardano to drive adoption and utility.

Core Benefits

By integrating with Cardano Layer-1 and other UTxO chains, Sundial becomes a hybrid Layer-2 solution, delivering:

- Trustless UTxO Interoperability – Seamlessly connects Bitcoin, Cardano, and other UTxO-based assets.
- Trading – Enables low-cost, high-speed on-chain and cross-chain asset exchanges.
- Lending & Borrowing – Allows BTC, ADA, LTC, and other assets to be used as collateral in DeFi.
- Staking & Yield Generation – Implements secure and sustainable on-chain rewards mechanisms.
- DeFi & Web3 Integration – Positions BTC as a foundational asset for decentralized applications in finance, culture, and entertainment, leveraging Cardano's existing ecosystem.
- Institutional-Grade Compliance – Implements advanced compliance, reporting, and risk management tools to support institutional participation.

Sundial redefines the potential of UTxO assets, bridging the gap between Bitcoin and smart contract-driven DeFi, unlocking liquidity, and expanding the possibilities of blockchain finance.

Conclusion

Sundial is the first optimistic rollup on Cardano, designed to scale transactions while preserving Layer 1 security and decentralization. By serving as a hybrid Layer-2 for Bitcoin and other UTxO chains, Sundial creates a "super" UTxO network, unlocking novel use cases and seamless interoperability. With Bitcoin's market capitalization projected to reach $10 trillion by 2030, the need for scalable DeFi solutions is greater than ever. While the EVM ecosystem thrives on cross-chain connectivity, UTxO networks—despite being eight times larger—remain isolated. Sundial bridges this gap, enabling trustless asset movement, institutional-grade security, and the full integration of Bitcoin into decentralized finance. Positioned as a critical infrastructure layer in the evolving financial landscape, Sundial is set to redefine blockchain scalability and utility.