Real-time Programmability over BlockDAGs

Litepaper v1

Igra Labs

Abstract

We present igra, a decentralized EVM-compatible programmability layer designed to work atop the Kaspa network. igra leverages Kaspa's security and throughput to the fullest extent, providing high volumes and internet-fast finality with proof-of-work security guarantees. To maintain decentralization, igra proposes a tandem of economic incentives with novel data-availability solutions tailored for Kaspa's unique consensus mechanism.

igra is a *based* rollup system (see [Dra23]): users interact with the programmability layer by posting transactions to the *base* layer. The based architecture sequences user transactions in the order determined in the base layer consensus, providing two incredible benefits: igra inherits Kaspa's exceptional security, scalability, and performance, while sharing its revenue with the base layer rather than being parasitic.

The igra design furnishes novel resolutions for trust bottlenecks. To enable many independent sources of truth, we introduce *accepted transaction archival nodes* (ATANs): a modular design for data storage that minimizes the subset of data that requires a trusted Kaspa node for validation. The ATAN design is highly modular and of independent interest to any network facing data availability requirements. We propose that igra achieves node decentralization by an ATAN-based network with economic incentives for node operators (in the form of a stakeable coin).

Finally, we propose three bridging models, one interim, and the other two based on the future roadmap of the base layer: ZK based bridging if ZK opcodes are ever implemented, and MPC based bridging in case they are not.

1 Introduction

Kaspa (Aramaic: כַּסְפָּא, silver) is the fastest and most capacious proof-of-work sequencer in the world. By design choice, the only on-chain utility provided by Kaspa is an implementation of the UTXO model with arbitrary payloads (with plans to add ZK opcodes and subnetwork support), delegating more complex functionalities to higher layers.

igra (Aramaic: אִירָא, roof) is a general-purpose programmability layer that can platform arbitrary smart contracts. igra employs a *based rollup* architecture [Dra23], where *sequencing* is delegated to the *base layer*.

igra is a programmability layer sequenced on Kaspa, offering users the fastest and most performant decentralized execution stack to date, which relies on proof-of-work secure sequencing.