

# Algorand's Layer-1

Intro to Algorand's Layer-1 Features

September 16, 2022

Joe Polny



# Performance

- ~4 second block time
- Instant finality
- 6,000 TPS
- .001 ALGO fee
- Low energy consumption



# Algorand Standard Assets (ASA)

- User-created tokens that are primitive to the blockchain
- Allows easy creation of tokens without smart contract risk
  - Supports fungible tokens and non-fungible tokens (NFTs)
- Features
  - Clawback: Allows a specified address to take back an asset
  - Freeze: Allows a specific address to freeze an asset
  - Metadata URL: Point to off-chain metadata for a token
  - Opt-in: Accounts must whitelist assets they wish to receive



# Smart Contracts

- Flat fee until congestion
- Turing complete
  - Hard-coded limitations to keep complexity in check
- Can read/write blockchain state and send transactions



# State Proofs

- Attest to state of the chain in a verifiable way
- Can be leveraged by other chains for interoperability
  - Bridge on another chain can verify Algorand state proof on-chain
- Provides quantum security of chain history



# Minimum balance requirement (MBR)

- Every account has a minimum balance
  - Starts at 0.1 ALGO
- Any transaction that would result in an account going under the MBR will fail
  - Exception is when an account makes an account to specifically close out the entire balance
- MBR is a way to rent space in the current state of the blockahin
  - Since ALGO is capped, the active state of the blockchain is also capped



# MBR Changes

Action	Effect	Effect on MBR
Asset opt-in	account can receive the asset	increased by 0.1 ALGO
Application opt-in	application can save state to the account	increased proportional to data saved locally (see formula <a href="#">here</a> )
Application creation	application is created	increased proportional to data saved globally (see formula <a href="#">here</a> )
Asset opt-out	account can no longer hold or receive asset	decreased by 0.1 ALGO
Application opt-out	account's local state for the given application is cleared	decreased by same amount as opt-in
Application delete	no one can interact with the app	decreased by same amount as creation



# Rekeying

- Allows a different private key to sign for a given address
- Once an account is rekeyed the original private key can no longer sign transactions
- Rekeying can be initiated with any regular transaction





# Atomic Transactions

- Algorand supports grouping 16 transactions together
  - If one transaction fails, they all fail
- Smart contracts can also send 16 transactions
  - Total of 256 atomic transactions
- Smart contracts can verify data of transactions in the same group

