Loopring 3.6 vs 3.1

	3.1	3.6	STATUS
Circuits & Blocks	3.1 has a few block types, each can only batch-process a particular type of onchain/offchain requests, such as deposits, trades. The benefit of such a design is the provers are most cost-effective; the downside is that users have to wait longer and there are more small blocks when the number of user requests are big enough.	3.6 only has one single block type. In each block, we can put all kinds of user requests. The prover is less efficient and will cost more, but because we can create a lot of big blocks, the on-chain cost per request will become smaller. Most importantly, user’s wait time will be much smaller so the experience should be improved.	Completed
Increased Capacity	3.1 supports 1204 tokens, and 2^20 users	3.5 supports 4096 tokens. The initial account capacity will be 2^24, and the operator can increase the capacity on demand. Each time, the account capacity will be increased by 4x. The account capacity’s upper-bound is 2^32.	In Progress
Agents	NA	The exchange admin can add some functionalities by whitelisting some smart contract addresses as “agents”; users can also authorize other address as their agents to perform actions that would otherwise request the user’s ECDSA signatures. The FastWithdrawal feature is implemented using the Agent design.	Completed
Fast Withdrawal	NA	The operator can work with liquidity providers to set up a fund to accelerate withdrawals. Fast withdrawal may or may not be visible to the users, therefore, any normal withdrawals can become fast withdrawals if the operator decides to speed them up.	In Progress
Offchain Request Authorization	3.1 requires all offchain requests to be signed by the account’s EdDSA private key.	3.6 supports 3 different authorization: - EdDSA signature (as in 3.1, this is checked in the circuits and is not part of the rollup data) - ECDSA signature (checked onchain, signatures will be part of the request’s auxiliary data) - Onchain approval hash (the request doesn't’ have any signatures, but its EIP712 hash can be found onchain).	Completed
Conditional Transfers	NA	Built on top of Agent and onchain approval hash, user can request layer2 transfers with a required condition onchain.	Completed

	3.1	3.6	STATUS
Open Transfers and Dual Authoring	NA	3.6 allows layer-2 transfers no to have any recipient. But to prevent the relayer from stealing the fund, we bring back Dual Authoring back from our Loopring 2.0.	Completed
Order Matching Protection	NA	3.6 allows orders to specify a bloom filter so they can only be matched with orders from a selected group of owners. This is mostly designed for trust-less OTC/peer-to-peer settlements. Orders in these trades cannot be freely re-matched with orders created by the relayer.	In Progress
Paralleled Transfers	3.1 requires transfers to have an increasing nonce (but not strictly +1). If a transfers is finalized in a block, other transfers with smaller nonces will become invalid.	3.6 allows 2^14 concurrent transfers to be processed out of order. But if the transfer with id= X + 2^14*m is processed, all transfers with id= X + 2^14*n where n < m will become invalid. Behind the scene, we use the same slots and id space for both orders and transfers.	In Progress
Implicit Account Creation	3.1 requires the receipt of tokens on layer-2 must have created an account.	3.2 will create an account automatically (without EdDSA pub-key) for the recipient if there is no account associated with the recipient address yet. This enables users to transfer/deposit to any addresses.	Completed
Onchain Fee Withdrawal	The operator will have to withdraw the onchain request processing fees for each block. This is tedious.	The onchain processing fees are automatically paid out to the operator when the block is submitted.	Completed
Token Registrations	Each token registration will cost some LRC tokens, WETH is registered automatically.	Token registration is free. No automatic WETH registration.	Completed
Forced Deposits	Deposits are put into a queue and must be processed in the exact order. All deposits need to be processed within a window.	Deposit processing is optional. If after some time a deposit is not processed, the owner can withdraw these tokens back to their wallet.	Completed
Onchain Withdrawals	Similar with deposits, onchain withdrawals are also put into a queue for sequential processing. Onchain withdrawals are also forced.	Named to “Forced Withdrawals” as all onchain withdrawal quests must be processed within a time window. The difference is that in 3.6, forced withdrawals doesn’t specify the amount, all layer-2 balance for the token will be withdrawn.	Completed
Deposit/Withdraw to Any Address	Can only deposit and withdraw to the owner address	Users can deposit and withdraw to any addresses.	Completed

	3.1	3.6	STATUS
Maintenance Mode	The operator can buy time by spending LRC to put the DEX into a Maintenance Mode. In such mode, user deposits and withdrawals are temporarily disabled.	As deposit processing is now optional, the Maintenance Mode is removed.	Completed
Shutdown Mode	The operator need to send back all tokens to the users to bring the DEX into its very initial state (empty Merkle tree) before the operator can withdraw staking.	The operator only promises to keep processing requests for another time window before he can claim his staking.	Completed
Account Ownership Transfers	NA	Account owner can transfers his ownership of the layer-2 account to another address. This also means 3.6 supports one Ethereum address to have multiple layer-2 accounts.	Completed
Stateless Layer2 Wallet	NA	Support social recovery of account ownership and account inheritance using Stateless Wallet.	Completed
Receipts	NA	The operator can generate and share a signed receipt for offchain requests. 3.6 will allow people to challenge the operator with such signed receipts (and a challenge fee) and wait for the operator to prove the onchain inclusion of the receipt's corresponding requests. This is designed to offer merchant assurance of payments.	
Query Protocol Fee Withdrawal Timestamp	NA	Available now. LRC staking contract can withdraw protocol fees for users dynamically.	Completed
Flexible Withdrawal Distribution	3.1 has a universal gas limit for distributing ERC20 tokens to the users after successful withdrawals. This causes some token distribution to fail as many ERC20 transfers cost way more than this gas limit.	3.6 allows user to specify now much gas the operator should offer for each request (if the operator doesn't agree, the request will be rejected). The operator can offer a higher gas limit than what the user specifies.	Completed
Offchain Request Expiry	NA	Allows all types of offchain requests to have a validUntil field.	In Progress