One thing that distinguishes Arbitrum from other Layer 2 technologies is its fast block time. Arbitrum One makes blocks every 250 milliseconds, and Orbit chains can be configured with block time as low as 100 milliseconds—if there are transactions arriving that quickly.

Let's unpack how Arbitrum does this—but first, let's review why it is important.

Why do we want fast block time?

The first advantage is obvious: faster blocks mean faster response time for users, which is great for user experience.

The second advantage of fast blocks is more subtle, but also quite important: it makes financial markets more efficient, and therefore attracts liquidity and leads to more market opportunities. Both theory and measurement (e.g., compare table 4A vs 4B in this Uniswap Labs paper) show that liquidity providers get better return on their investment when block times are fast, because less value is extracted by arbitragers. (tl;dr reason: Arbitragers exploit stale prices; faster blocks mean prices are less stale.) In a standard model known as "LVR with fees", arbitrage extraction scales with the square root of the block time. This predicts that Arbitrum's 250 millisecond block time leads to 65% lower arbitrage loss compared to a 2 second block time.

This pays off for users. Higher return for liquidity providers attracts more liquidity, and more liquidity means more and better trading opportunities for users. This is one big reason why Arbitrum One has more liquidity and more organic trading activity than any other L2, in DeFi applications like Uniswap.

How does Arbitrum provide fast block time?

So how does Arbitrum do it? There is an obvious answer and a less obvious one, which are both correct. Both tell part of the story.

The obvious answer is that the Arbitrum sequencer is designed and built with fast blocks in mind. This is reflected in many engineering decisions, large and small—and it's a credit to the Offchain Labs engineering team which built the current sequencer.

The less obvious answer is that the design reflects a subtle shift in mindset, from a "block building" model to a "sequencing" model.

Block building conventionally works like this: the system publishes a block; everyone sees the block; users submit transactions for the next block; incoming transactions accumulate in a mempool until some deadline is reached; the system builds the next block by selecting and arranging some transactions from the mempool; and the cycle repeats.

The block building model has it advantages, but it's not fast. You're not going to operate that cycle at anything like a 250 millisecond cadence at scale in the real world.

Sequencing thinks of the problem differently: pack the transactions into blocks as soon as they arrive, filtering out invalid ones. When the scheduled time for the next block is reached, publish the already-built block (unless it's empty) and start over. Don't stop and wait for anyone; and don't force transactions to sit around in a mempool awaiting a decision.

Sequencing is faster because it dispenses with the mempool, and it pipelines the process by sequencing each transaction immediately, and publishing each block as soon as it's ready.

Another advantage of the sequencing model is that by making this process part of the protocol, rather than externalizing it to outside parties as often happens with block building, sequencing better protects against front-running, sandwiching, and other exploiting block-building tricks.

Next steps for sequencing: MEV monetization and decentralization

There are two more steps on the road to sequencing nirvana: monetizing MEV and decentralizing the sequencing process.

Ethically monetizing MEV

Monetizing MEV is important, so the chain can capture more of the economic value it is creating, but we want to be sure to monetize in a way that doesn't undermine the advantages of fast sequencing. As an example, if we decided to auction block building rights, this would mean a switch back to block building mode, losing the speed advantage of sequencing—and opening the door to the high bidder exploiting users by front-running or sandwiching their transactions.

After a lot of study, the Offchain Labs team prefers the latest version of "timeboost": an express-lane auction approach to monetizing MEV. The idea is to retain the sequencing model, while creating an "express lane" for transactions. All transactions in the express lane would be sequenced immediately, while non-express lane transactions would be buffered (without leaking their contents) for 200 milliseconds before being sequenced. The right to use the express lane would be auctioned off for each period of (say) one minute.

The idea is that the party who buys express lane access would be able to get their transactions into the sequence ahead of everyone else (if they submit quickly), but they would not get to see what others had submitted. So that party can grab arbitrage and other non-exploitative MEV, but would still be prevented from sandwiching and similar exploits.

This approach maintains the fast response time advantage of fast sequencing, and protects economic efficiency by forcing arbitragers to act quickly so that prices don't get stale.

Timeboost is coming soon to the Arbitrum stack. Watch for news about this!

Decentralizing sequencing

The last piece is to decentralize the sequencing protocol—again, without giving up what is good about sequencing. And we're aiming for true decentralization, where no one party controls the contents of any block produced by the protocol.

In particular, we want to avoid a "rotating centralized" approach, in which a centralized party decides everything but different parties play that all-powerful role for different blocks. Such a strategy brings back many of the problems of block-building, including a slower timescale and the censorship and sandwiching problems.

So what we want is for sequencing to be done by a committee, with a guarantee that the rules for inclusion and ordering are followed as long as enough committee members are honest. This is the subject of an ongoing collaboration between Offchain Labs and Espresso Systems, to create a decentralized version of timeboost.

We'll be writing more about decentralized timeboost over the coming weeks and months. (This post is long enough already.)