Introducing Shutter — Combating Front Running and Malicious MEV Using Threshold Cryptography

Shutter Network Mar 26, 2021 4 min read



Maximal Extractable Value (MEV) and front running are widely recognized to be among the final unsolved fundamental issues in the blockchain space. There are now

Archived copy · cryp2nova.com

hundreds of millions of dollars of documented MEV, most of which is tremendously harmful for users and traders. This problem will inevitably become more devastating over time and eventually could even pose a fatal obstacle on our community's path to mainstream adoption.

We would like to introduce Shutter, an open-source project that aims to prevent front running on Ethereum by using a threshold cryptography-based Distributed Key Generation (DKG) protocol. Its first instantiation will be a simple drop-in solution for smart contracts. A testnet version of this system will be released on Goerli shortly.

MEV and Front Running

The term MEV was coined by Phil Daian et al. and describes revenue that block producers can extract by selecting, injecting, ordering, and censoring transactions. The MEV extracted in 2020 alone was worth more than $314M — and that is only a lower bound. Oftentimes, the MEV is not captured by the block producers themselves, but rather by independent entities using sophisticated bots.

An important subset of MEV is the revenue extracted by so-called front running — an attack that is illegal in traditional markets, but uncontrolled in the crypto space. A front runner watches the network for transactions that are worth targeting. As soon as they find one, they send their own transaction, trying to get included in the chain beforehand. They achieve this by paying a higher gas price, operating world-spanning network infrastructure, being a block producer themselves, or paying one via a back channel.

The most frequent victims of front running attacks are traders on decentralized exchanges. Front running makes them suffer from worse prices instead of being fairly rewarded for the information they provide to the market. On the other side, front runners siphon off profits from their victims in a nearly risk-free fashion without contributing anything useful to the system. A simple example of this are arbitrage transactions benefitting from the price difference of the same asset on two different DEX’s. Front runners regularly copy these kinds of transactions from other market participants and execute them earlier, reaping the rewards, whereas the original trader comes away empty-handed.

Archived copy · cryp2nova.com

Besides exchanges, many other applications can be affected as well, including bounty distributions and auctions. Importantly, because they rely on voting, governance systems, which represent a large and fast-growing field within Ethereum, are prone to front running and could face significant challenges without a system that protects against these types of attacks.

In traditional finance, front running can be curbed (somewhat) via regulation or oversight by various trusted intermediaries and operators. In permissionless, decentralized systems this is not the case, so it might be a strategic blocker to mainstream crypto adoption.

The Solution

A system that solves front running on Ethereum should meet the following requirements:

- It must be **decentralized**. Ignoring this property would make the whole point of using blockchains meaningless.
- It must be **efficient**. The solution should be gas-efficient in order to keep transaction fees low.
- It must **not require base protocol changes**. Ideally, front running should be prevented at the base layer. However, such a protocol change would take a long time to implement. As a community, we don't want to wait for too long.

Shutter is designed to be such a solution — decentralized, efficient, and practical. Projects can adapt their existing smart contracts with little effort and without waiting for an Ethereum protocol update.

Shutter allows users to send encrypted transactions in a way that protects them from front runners on their path through the dark forest (the metaphorical hunting ground of front runners that each transaction must cross). For example, a trader could use Shutter to make their order opaque to front runners, which means attackers can neither determine if it is a buy or a sell order, nor which tokens are being exchanged, or at

Archived copy · cryp2nova.com

which price. The system will only decrypt and execute a transaction after it has left the dark forest and is included in a block.

Simplified illustration of transaction execution in Shutter

The keys for encryption and decryption are provided by a group of special nodes called Keypers. Keypers regularly produce encryption keys by running a Distributed Key Generation (DKG) protocol. Later, they publish the corresponding decryption key. The protocol uses threshold cryptography — a technique enabling a group of key holders to provide a cryptographic lock that can only be opened if at least a certain number of the members collaborate. This ensures that neither a single party, nor a colluding minority of Keypers, can decrypt anything early or sabotage the protocol to stop it from executing transactions. As long as a certain number of Keypers (the "threshold") is well-behaved, the protocol functions properly.

Next Steps

Archived copy · cryp2nova.com

The Shutter software is currently going through some tests and getting ready for the first testnet release. In a future blog post we will tell you about the project in more detail. To stay up to date, please follow us on X-Twitter and join the Discord server! You are welcome to share your feedback or reach out to us via DM on X.

We have been working on Shutter for a long time and would like to thank those who have provided invaluable external contributions and feedback, especially Stefan George, Martin Köppelmann, Prof. Sebastian Faust, Prof. Stefan Dziembowski, William George, and Patrick McCorry.

Share this article:

NEWER POST

Shutter Alpha Released on the Testnet!

CRYP2NOVA

You might also like

Archived copy · cryp2nova.com

Shutter Joins the Encrypt the Mempool! Coalition



Hegotá Update: EIP-8105 Team Giving Full Support to LUCID EIP

Archived copy · cryp2nova.com

Hegotá Should Complete the Holy Trinity of Censorship Resistance



How to Protect Yourself Against Malicious MEV in 2026

Archived copy · cryp2nova.com

Subscribe to Shutter Blog newsletter and stay updated.

Don't miss anything. Get all the latest posts delivered straight to your inbox. It's free!

Your name

Your email address

Subscribe

CRYP2NOVA

Shutter Blog

The Future of Fair and Secure Blockchain Starts Here

Features

Contact

Home

Archived copy · cryp2nova.com

© Shutter Blog 2026. Published with Ghost and Porto

↑ Back to top

Archived copy · cryp2nova.com