Google Cloud

Secure blockchain transactions.

How Flashbots built verifiable ordering with Google Cloud's Confidential Computing.



October 2026



Executive summary

Flashbots, a leading Web3 research and development organization, is transforming how transactions are ordered and processed on blockchains. In adversarial blockchain environments, transaction ordering has emerged as a critical bottleneck, shaping execution quality, latency, and value distribution across systems that are designed to be open by default. Working closely with Google Cloud and leveraging Confidential Computing, powered by Intel®Trusted Domain Extensions (Intel® TDX) on C3 VMs, Flashbots creates blockbuilding infrastructure that makes ordering secure and efficient through verifiability. Through this collaboration, Flashbots is able to build market trust and enhance performance while scaling its ecosystem. The same verifiable execution foundation also creates a path toward provable execution quality, enabling participants to independently verify that routing and ordering decisions respected declared constraints and preferences. From block assembly to hosting sophisticated trading strategies inside hardware-backed Trusted Execution Environments (TEEs), Flashbots enables confidentiality, integrity, and auditability without sacrificing performance. This approach lays the foundation for transparent and efficient blockchain markets, while enabling a gradual path toward more secure and composable blockbuilding architectures over time.

Navigating the "dark forest" of blockchain transactions

Across public and permissionless blockchain protocols, transactions must navigate a "dark forest," an adversarial environment where bots and sophisticated actors compete to observe transactions and profit at their expense. This activity, known as Maximal Extractable Value (MEV), is a natural result of open interoperability. While some MEV improves market efficiency, predatory practices like "front-running" harm users and undermine the promise of blockchain fairness. As blockchains scale and interoperate with other execution domains, ordering becomes increasingly sensitive: it must remain fast, deterministic, and globally consistent, even as competing inputs and incentives interact across systems.

Flashbots bring transparency and structure to the "dark forest" of public blockchains, ensuring effective transaction execution, shielded from predatory behaviour. Achieving this demands new infrastructure, as traditional solutions rely on trusted intermediaries which imply risk of censorship, unfair advantage, and opaque execution — the very risks decentralized systems are built to mitigate.

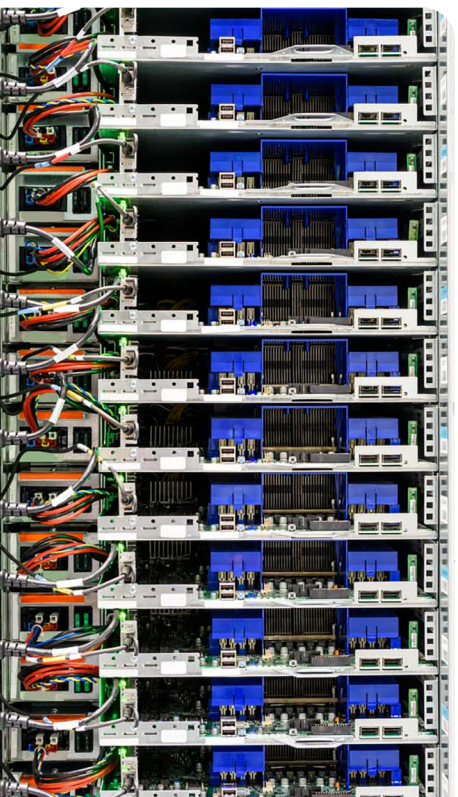


At the centre of this effort lies the problem of enabling efficient cooperation between market actors in the dark forest without requiring blind trust. Specifically, how to process and facilitate interaction over sensitive transaction data securely and verifiably, without imposing unacceptable overhead in a latency-critical setting. This challenge motivates Flashbots' focus on secure public cloud infrastructure as a core primitive in composable and verifiable "blockbuilding"—the process by which different users' activities are combined into the block that extends a blockchain.

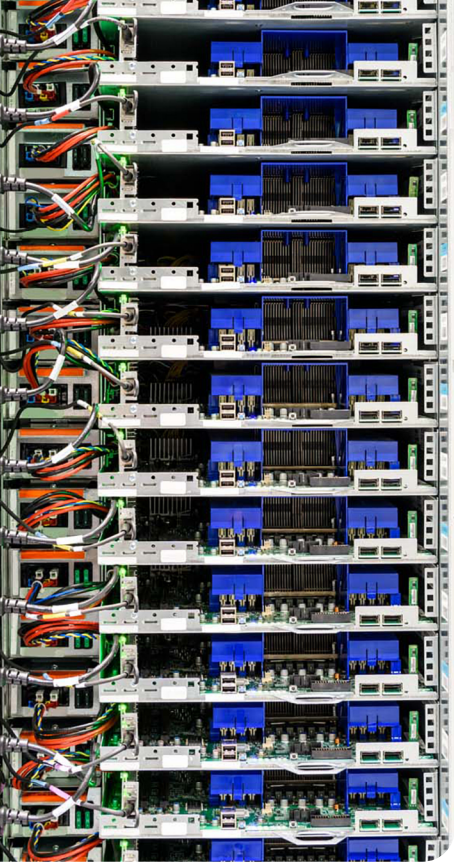
Google Confidential Computing powers verifiable ordering

Flashbots found a breakthrough in Google Cloud's Confidential Computing, specifically through the use of Trusted Execution Environments (TEEs) enabled by Intel TDX. TEEs protect data not only at rest and in transit, but also during execution, shielding code and data from privileged infrastructure actors such as the host operating system or hypervisor.

By running critical block assembly and ordering logic inside TEE-backed virtual machines, Flashbots provides auditable, hardware-enforced guarantees about confidentiality and integrity, even when execution depends on evaluating multiple private inputs and constraints under tight latency budgets. Sensitive transaction information and ordering preferences remain protected while blocks are being constructed, directly addressing the need for pre-trade privacy in permissionless, adversarial markets.



Equally important, TEEs enable remote attestation. This allows the system to cryptographically prove that specific code is running in a genuine, untampered execution environment. As a result, participants no longer need to rely solely on reputation or operator assurances, they can independently verify how ordering decisions were produced. This emphasis on reproducible and verifiable execution aligns closely with broader transparency efforts in cloud security and underpins Flashbots' goal of enabling blockbuilding systems that are private, performant, and auditable by design. This architecture enables a bring-your-own-constraints model, where execution can be verified against agreed-upon economic or policy rules, making deviations from those rules detectable without hard-coding trust in a single operator.



BuilderNet

Verifiable blockbuilding at ecosystem scale

Flashbots also developed and operate BuilderNet, a production blockbuilding network built on Google Cloud Confidential Computing. Since its launch, BuilderNet has demonstrated how Trusted Execution Environments can support large-scale transaction ordering on Ethereum while providing hardware-backed guarantees around confidentiality, integrity, and verifiable execution.

At various points since late 2024, BuilderNet has been responsible for building roughly 30% of Ethereum blocks, demonstrating that confidential computing can support production-scale ordering workloads without sacrificing performance.

By executing critical blockbuilding logic inside Intel TDX-backed confidential virtual machines, BuilderNet allows participants to independently verify the execution environment responsible for constructing blocks, reducing reliance on operator trust alone. By processing sensitive transaction-ordering workflows inside secure hardware running attested software binaries, BuilderNet provides end-to-end runtime privacy and verifiable execution while preserving the low-latency performance required by modern blockchain markets.

BuilderNet serves as a production example of how confidential computing can support real-world blockchain market infrastructure. The system demonstrates that multiple independent participants can cooperate around sensitive ordering and execution workflows while maintaining strong security boundaries, creating a foundation for increasingly open, transparent, and composable blockbuilding systems.

Enabling 200ms Flashblocks with Google Cloud

Flashbots co-designed the verifiable blockbuilding infrastructure that enabled Flashblocks on layer 2 blockchains.

For a major layer 2 blockchain, Flashbots builds Flashblocks inside Google Cloud C3 with Intel TDX Confidential VMs, enabling ~200ms preconfirmations while preserving verifiable ordering guarantees.

From a systems perspective, Flashblocks extend the blockbuilding auction to shorter time horizons: independent participants submit transactions and constraints under tighter latency budgets, and the system must resolve contention consistently without equivocation. By binding preconfirmation logic to attested execution, Flashblocks ensure that fast confirmations remain a property of execution, not trust, allowing rollups to safely push latency boundaries without sacrificing correctness or auditability.

> “Blockchains ultimately come down to how blocks are built. As blockbuilding becomes a global coordination problem, where economic, operational, and policy preferences all intersect, Flashbots’ role is to define the execution rules that make this coordination possible without centralization. What excites me about collaborating with a forward-looking partner like Google Cloud is the opportunity to ground these rules in reproducible, verifiable execution, drawing on our research into Data Center Execution Assurance to support institutional-scale activity moving onchain and accelerate a more transparent, agent-driven economy.”

Tina Zhen
Co-founder and steward

Flashbots

A strategic partnership for innovation

Flashbots' decision to work with Google Cloud was driven by several key factors



01

Deep Web3 understanding

The Google Cloud Web3 team brings a strong understanding of distributed systems, appreciation for a progressive decentralization ethos, demonstrated understanding of blockbuilding auction market structure, and the challenges of coordinating execution in open, interoperable environments.

02

Leading-edge technology

After extensive evaluation, Flashbots identified Intel TDX as a leading TEE architecture for performance-sensitive workloads. Google Cloud's rapid deployment of Intel TDX on C3 VMs and alignment with Intel's roadmap were decisive factors, particularly as Flashbots explores more composable execution models that depend on strong execution guarantees.

03

Breadth of engineering talent

Google Cloud's experience across open-source infrastructure, hardware security, and identity systems provides valuable insight as Flashbots scales blockbuilding and investigates future authentication and authorization workflows.

04

Collaborative development

Google Cloud worked closely with Flashbots from early stages, engaging deeply with technical requirements and long-term goals. This collaboration emphasized advancing verifiable execution and transparency, while remaining adaptable as architectures evolve.

Strengthening trust, operational security, and ecosystem participation

By adopting Confidential Computing, Flashbots is able to continue delivering on its mission and support the broader Web3 ecosystem:

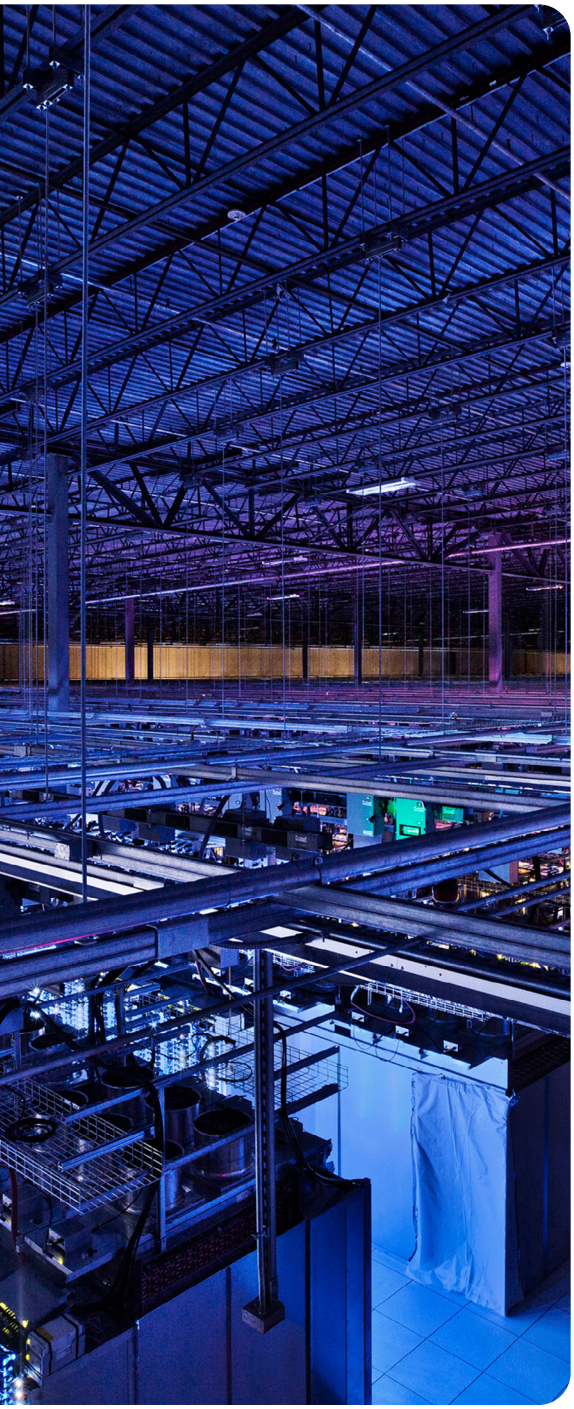
Stronger trust boundaries and verifiable execution:

Hardware-enforced isolation allows Flashbots to process sensitive ordering data with reduced reliance on infrastructure operators. Attested execution environments make it possible to verify how blocks are built, supporting secure, composable blockbuilding today while reducing centralization pressure over time.

Streamlined operational security

Isolating critical computations inside TEEs reduces the attack surface and simplifies security management for highly sensitive workloads.

> “Confidential Compute provides credible verification that allows us to create reproducible auction protocols on the blockchain and build market trust.”



Latency-sensitive confidential execution

Google Cloud C3 Confidential VMs with Intel TDX provide an attested execution environment for blockbuilding components in the Flashblocks path, supporting ~200ms preconfirmations while preserving confidentiality, integrity, and verifiable ordering.

Increased partner confidence and ecosystem participation

Hardware-backed privacy and attestation reports provide concrete guarantees to ecosystem participants, encouraging broader adoption and deeper cooperation among specialized actors.

Scalability across regions

Google Cloud's global availability of Intel TDX infrastructure enables Flashbots and its partners to deploy secure blockbuilding services wherever needed.

Improved user experience and new design possibilities

For end users, verifiable and confidential ordering contributes to more predictable transaction outcomes. For developers, TEEs provide a foundation for executing constrained logic over private data as blockbuilding becomes more secure and composable.



Looking ahead

Scaling verifiable infrastructure for programmable execution

Flashbots plans to continue working with Google Cloud to scale its confidential blockbuilding infrastructure across Layer 2 rollups and additional blockchain environments. As permissionless interoperability increases, the need for secure composition, verifiable execution, and application-specific constraints becomes more pronounced.

One emerging frontier is Application-Controlled Execution (ACE): a model in which applications express scoped execution constraints for their own transactions, such as atomicity, state bounds, or ordering within a defined execution envelope, while builders retain responsibility for global block construction and conflict resolution. In this model, Confidential Computing and attestation become the trust boundary that allows applications to rely on builder-enforced policy as a verifiable constraint, without requiring privileged control over the block. This approach provides the specialisation required to support heterogeneous forms of activity on shared infrastructure and provides the scaffolding for verifiable best execution and compliance. As applications, routers, and market participants express how their flow should be handled, Confidential Computing and attestation make it possible to verify that routing and ordering decisions honored those declared constraints, turning execution quality from an operator assurance into an independently verifiable property. As onchain execution becomes increasingly important for institutional-scale activity, the ability to demonstrate how execution decisions were made may become as important as the decisions themselves.

A second frontier is the evolution of blockbuilding markets themselves. Running strategy logic inside Trusted Execution Environments and extending auctions to shorter horizons through technologies such as Flashblocks changes who can compete and how execution quality is achieved. The same attested trust boundary can support privacy-preserving data clean rooms for emerging agentic systems and reinforcement-learning ("RL Gym") workflows, where NDAI-style information sharing and conditional-recall mechanisms allow participants to benchmark, train, and evaluate strategies over sensitive execution data without exposing proprietary models, user preferences, or raw orderflow.

This direction also raises the bar for infrastructure assurance. Flashbots' work is informed by ongoing research into Data Center Execution Assurance (DCEA) and broader proof-of-cloud approaches, which extend the logic of confidential-computing attestation beyond proving that specific code ran inside a Trusted Execution Environment, toward stronger evidence about the cloud platform and data-center environment in which execution occurred. For blockbuilding, this matters because independent participants need to verify not only ordering logic, but also the provenance of the infrastructure executing it.

Flashbots views Google Cloud as a key technology partner in building the secure, performant, and transparent foundation required for the next generation of decentralized and hybrid applications. The organizations will continue to collaborate to support secure innovation and verifiable execution at global scale.

Products used

Google Cloud C3 with Intel TDX Confidential VMs

Ready to build?

Get started with Confidential VMS

Explore Flashbots

Learn how Flashbots work

Secure your data

Discover Google Cloud Confidential Computing



Google Cloud