Evaluating fair play in a $5 billion game:

How Monopoly GO! built player confidence through third-party validation

Monopoly GO! has been one of the most played & successful mobile games since its 2023 launch, generating $5 billion in revenue in slightly less than two years. In 2024, fairness concerns began to arise among users. Recognizing the potential for malicious players to deploy unauthorized cheating overlays that could manipulate dice roll outcomes, Monopoly GO! hired Trail of Bits to conduct an independent assessment of two design proposals for their pseudorandom number generation (PRNG) system. The evaluation addressed fairness concerns from users and identified the optimal architectural approach for hardening the system against cheating before implementation.

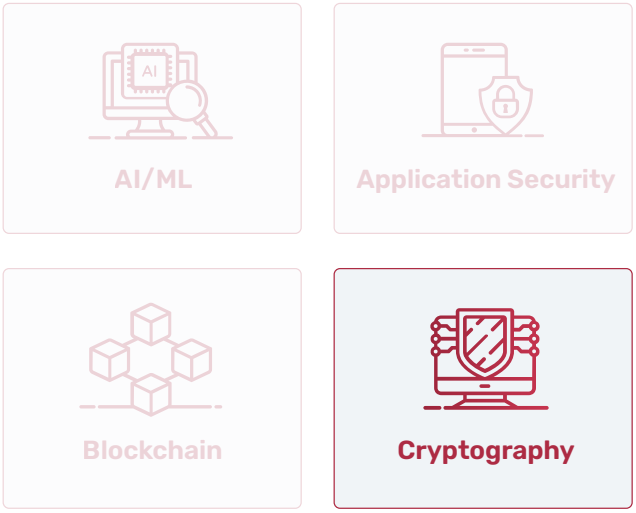
Assessment outcomes

One Trail of Bits consultant conducted a design assessment from December 11 to 26, 2024, analyzing the PRNG design, hardening techniques, and potential exploitation vectors.

The Design Assessment reviewed the integrity of two security properties:

1. The random number generator produces unbiased outcomes for all players.
2. The implemented countermeasures effectively prevent malicious actors from predicting or manipulating dice roll results through client-side interception techniques.

We found no evidence that the output of the PRNG is biased to reduce player rewards.

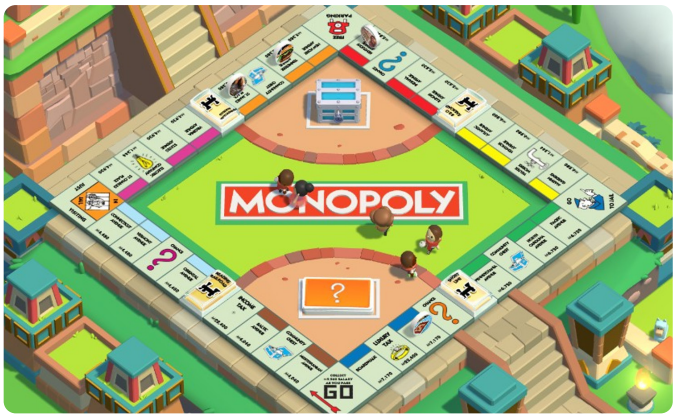


Looking forward

Monopoly GO! now has the security framework needed to stay ahead of evolving threats while maintaining complete transparency with players. This assessment provides the strategic foundation for continuous security improvements. The team can now make confident long-term commitments about fair gameplay while building lasting player trust through demonstrable security excellence.

> "Our vision is to stay ahead of emerging threats while being transparent and accountable to our community. We will continue to evolve our systems and work alongside security experts like Trail of Bits to ensure a safe, fair, and fun environment for all players."
>
> - Monopoly GO! Game Integrity Team

Evaluating fair play in a $5 billion game:
How Monopoly GO! built player confidence through third-party validation



> We strongly encourage other developers to take a proactive approach to auditing randomness systems. In today's environment, trust in outcomes is critical to player retention and brand reputation."
>
> - Monopoly GO! Game Integrity Team

Advice to game developers

- Ensuring the security, safety, and integrity of your game requires proactive investment in security-focused design and architecture
- Engaging experts like Trail of Bits to assess your system's design will identify and remediate entire classes of vulnerabilities, such as randomness manipulation, before launch
- Proactive security measures like these design assessments will ultimately build trust with your players and result in a better gaming experience and a stronger community

Learn more about cryptographic design assessments

> Trail of Bits brought their world-class cryptographic expertise to help us evaluate the design and implementation of our RNG hardening techniques."
>
> - Monopoly GO! Game Integrity Team

BLOGS:

- Best practices for key derivation
- State of the Art Proof-of-Work: RandomX
- Cryptographic design review of Ockam

PUBLIC REPORTS:

- Monopoly GO! Letter of Attestation
- Discord Design Assessment
- Ockam Design Assessment
- RandomX Design Assessment

ABOUT TRAIL OF BITS

Trail of Bits brings specialized cryptographic expertise that combines Ph.D.-level theoretical knowledge with practical security engineering experience. This unique capability was essential for evaluating the theoretical and practical nuances ofMonopoly GO!'s Cryptography

www.trailofbits.com AI/ML | Application Security | Blockchain | Cryptography | Research & Engineering