praetorian

DATA SHEET

Smart Contracts

KEY BENEFITS

- **Identify** vulnerabilities in smart contracts and surrounding infrastructure
- **Defend** blockchain-based platforms and assets against real-world attacks
- **Assure** your stakeholders that remediations are effective

WHY PRAETORIAN

At Praetorian, we understand that discerning organizations are looking for a cybersecurity partner in today's connected world. Our clients gain maximum benefit from our tailored approach to each engagement, our deep technical expertise, and our focus on providing the best possible client experience. You can rely on us to ask deep questions, work closely with your teams, and provide direct, clear feedback on what we find. Our team keeps your bigger picture in mind in order to help your company understand both the ground truth about your security program and its implications for your company's future.

CAPABILITIES OVERVIEW

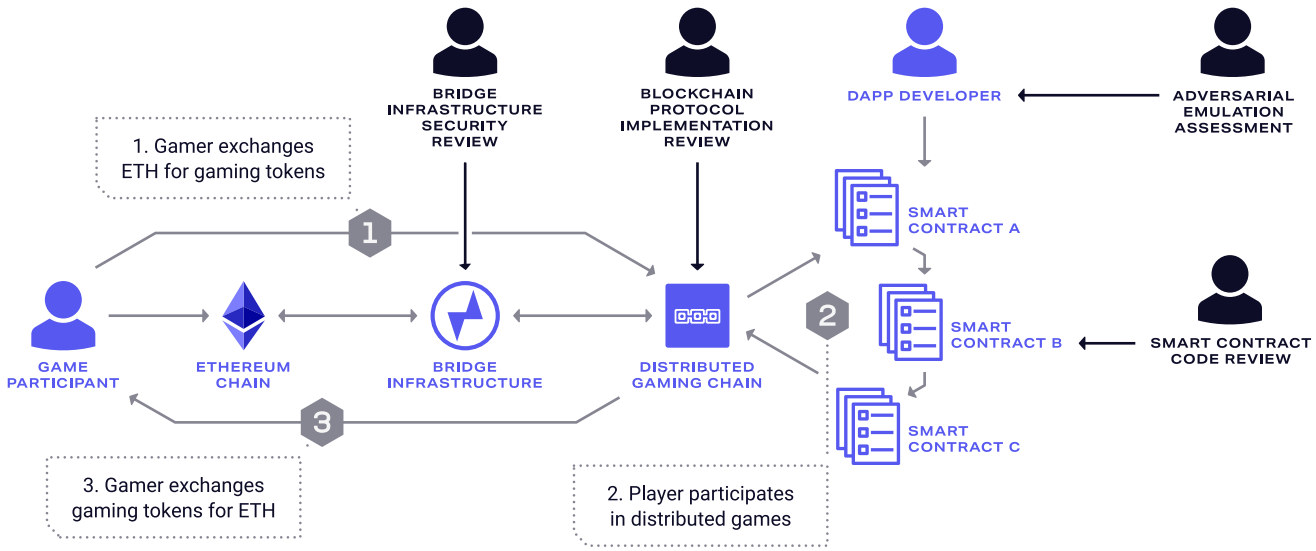
Praetorian takes a multi-layered approach to Web3 security. The core component is a methodical review of the smart contracts' source code. Our engineers possess the necessary expertise to comprehensively identify vulnerabilities in domain-specific languages such as Solidity and Vyper. A thorough code review that combines manual and automated techniques can surface vulnerabilities related to reentrancy, price manipulation, paths to unprotected token and value transfers, and authorization issues. During this step, we also

- Assess the resilience of a client's smart contracts against transaction ordering attacks from often unexpected threat actors such as MEV bots or malicious miners/validators. These attackers will front-run externally profitable transactions and manipulate block properties such as the block timestamp in order to influence the conditions of a transaction in their favor (e.g. lottery/random value manipulation).
- Web3 also poses unique concerns related to denial of service. In many cases, Web3 denial of service attacks result in a weakening of the system's security guarantees or may cause permanent and direct loss of value. For example, our engineers can locate unbounded loops and other anti-patterns that could allow an attacker to manipulate the cost of executing a contract or prevent execution of a contract altogether.

Additionally, Praetorian evaluates the security of the infrastructure and technical protocol implementation used by the underlying blockchain. This includes confirming that sufficient protections are in place against threats such as validator takeover, 51% attacks, and vulnerabilities involving bridges and RPC nodes. Finally, and when applicable, Praetorian also undertakes a thorough review of traditional frontend and backend application vulnerabilities that might represent an attacker's path of least resistance.

Throughout a smart contract engagement, Praetorian's domain experts use industry-standard static analysis tools in conjunction with their thorough manual source code review. After identifying one or more potential vulnerabilities, Praetorian will simulate attacks in a local fork/simulated environment to determine the real-world impact without disrupting the customer's business operations.

WORKFLOW



WHO NEEDS THIS SERVICE

- Developers of decentralized applications looking to provide assurance to their internal or external stakeholders.
- Counterparties seeking an independent risk assessment before executing a transaction via smart contract.
- Businesses who are just starting out in the decentralized space and want additional clarity about where the risks really are.

DELIVERABLES

Executive Summary

Concise explanation of engagement goals, significant findings, business impacts, and strategic recommendations

Engagement Outbrief Presentation

Similar to the executive summary, presented to the audience of your choosing

Technical Findings Report

Full descriptions of vulnerabilities, each including a severity rating, instructions to reproduce, and recommendations to mitigate

Praetorian Security, Inc.
6001 W Parmer Ln, Ste 370, PMB 2923
Austin, TX 78727 USA
info@praetorian.com

To learn more about Praetorian, visit: www.praetorian.com

ABOUT PRAETORIAN

Praetorian is an offensive security engineering company whose mission is to make the digital world safer and more secure. Through expertise and engineering, Praetorian helps today's leading organizations solve complex cybersecurity problems across critical enterprise assets and product portfolios.