

Nomination Statement

The Poorest Man in Babylon: A Longitudinal Study of Cryptocurrency Investment Scams

The Poorest Man in Babylon, published in WWW 2025, makes a foundational contribution at the intersection of cybercrime measurement, scalable detection, and practical defense. The paper introduces Crimson, a novel end-to-end system for detecting cryptocurrency investment scam websites in near real time as they emerge, without relying on social-media discovery or manual engagement with scammers. Methodologically, this is a significant advance: the system combines certificate-transparency monitoring, domain and content filtering, OCR-based extraction, LLM-assisted classification, and authenticated crawling to study a threat class that has previously been difficult to measure systematically.

The paper's scientific value is amplified by its breadth, rigor, and empirical depth. Over the first eight months of 2024, Crimson processed roughly 6 billion domain names and identified 43,572 unique cryptocurrency investment scam websites. The authors move beyond detection to provide a multidimensional analysis of scam infrastructure, clustering sites by hosting, design, JavaScript reuse, and embedded indicators of compromise. This reveals structural regularities across the ecosystem, including a heavy concentration of infrastructure, extensive template reuse, and meaningful opportunities for hosting-provider and platform intervention. The study also shows that nearly half of the detected scam sites remained active at the end of the observation period, highlighting the persistence of this threat and the inadequacy of current mitigation practices.

Equally important, the paper connects technical detection to real-world harm. By extracting scammer-controlled wallet addresses from a subset of sites and analyzing blockchain transactions, the authors estimate a conservative lower bound of \$2.04 million in victim losses. The paper also evaluates widely used blocklists and finds that most of the detected scam sites were absent from them, demonstrating a clear and actionable gap in today's protective ecosystem. The result is not only a strong measurement paper but also one with immediate operational relevance and broad defensive implications.

This work exemplifies the cybersecurity science the competition seeks to honor: it precisely defines a pressing threat, builds a principled and scalable methodology to study it, produces new empirical knowledge about adversary behavior, quantifies real-world harm, and yields insights that can directly improve defenses. For its novelty, rigor, scale, and practical impact, this paper is highly deserving of the award.