Abstract Submitted
for the EGLSF21 Meeting of
The American Physical Society

Is Quantum Money a Waste of Time? CHRISTIAN QUERREY, NOAH LINDSELL, Case Western Reserve University — Since Weisner's proposal in 1983, the idea of quantum money has received little attention. However, new advancements and research in digital currencies, quantum communication, and quantum cryptography present attractive avenues which warrant revisiting the idea quantum money. Current cryptographic currencies solve the double-spending problem often by integrating a blockchain which is backed by hard-to-solve cryptographic hash functions. The study of Quantum Information presents many concepts such as quantum teleportation, quantum digital signatures, and quantum secret sharing which make its application to such problems extremely attractive and a rich source of scientific research. In this study, we ask ourselves the question, "Is Quantum Money a waste of time?" We first discuss the vulnerabilities and inefficiencies of present digital currency schemes. We then proceed to a thorough literature review and categorization of research regarding quantum money since Weisner's proposal, discussing the improvements each scheme proposes, and classifying the methods used to do so. Finally, we motivate our own proposals to incorporate quantum technology into cryptocurrency.

Christian Querrey
Case Western Reserve University

Date submitted: 29 Oct 2021 Electronic form version 1.4