

January 21, 2021

Felice Manganiello, PhD

School of Mathematical
and Statistical
Sciences

College of SCIENCE

Clemson University
220 Parkway Dr.
O-110 Martin Hall
Clemson, SC
29634-0975

P 864-656-1657
F 864-656-5230
manganm@clemson.edu

Dear selection committee,

I would like to nominate Sam Smith for an award.

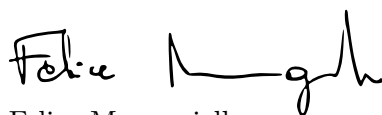
Sam is taking a CI with me in collaboration with Dr. Goodell from Insight
Decentralizes Consensus on a project for the Monero Research Lab. We both are
really impressed by his skills and independence in research.

Sam is the only undergraduate student in my graduate cryptography class. Al-
though it is too early to talk about his performance, I believe he will at the level
of our graduate students in this class. Moreover, Sam already has taken other
graduate classes with excellent results.

The following you can find the recommendation letter of Dr. Goodell.

Please contact me if you need further information.

Best regards,



Felice Manganiello
Associate Professor

To Whom It May Concern,

My name is Dr. Brandon Goodell. I received my Ph.D. in Mathematical Sciences from Clemson University in 2017. Since, I've worked in financial technology, applied cryptography, and cryptocurrencies. It has come to my attention that Samuel Smith, an undergraduate student with whom I am working via the Clemson Creative Inquiry program, is up for an award. This letter is in support of Sam.

Sam is working on a *crime-fighting* project for the Monero Research Lab (MRL). MRL is one of several workgroups of the Monero Project, an open-source cryptocurrency with an emphasis on privacy and maintained by volunteers (such as myself). Monero has a market cap exceeding \$2.5B USD, but has a bad reputation for being associated with criminal activity. Recently, the Internal Revenue Service offered a bounty of up to \$625,000 for tools that can trace transactions through the Monero ledger. Sam's project (once completed) may qualify.

Sam and I are employing some simple, well-known, and well-studied algorithms to trace transactions, boosting performance with open source intelligence such as from social media, stochastically generating simulated ledgers, and assessing the quality of the tracing algorithm by comparing with the simulated ground-truth. His work is usable by law enforcement to retroactively trace transactions and "follow the money" during an investigation into a sequence of ledger transactions. His work is usable to determine the effectiveness of these ledger forensics methods, providing tools to prevent situations akin to racial profiling where some demographics are unfairly and disproportionately investigated for innocuous behavior. On the flip side, his work can be used to inform parameter selection in the design of new cryptographic protocols, leading to improved security for users of 21st century financial technology.

I've thrust Sam into some of the most annoying problems revolving around traceability in transaction graphs, with an incomplete codebase for generating simulations, and with loose, vague descriptions of already hard-to-describe problems. Sam has performed admirably. His work has included debugging simulations, familiarizing himself with graph theory and several important graph-theoretic algorithms, and writing the core functionality of the open source intelligence component of the project. A great deal of work remains, but we will be able to gather data soon. We plan to publish a series of peer-reviewed papers on the topic.

Sam's project is wildly difficult, has real money on the line as a topic of study, has concrete financial incentives provided by the Internal Revenue Service, but is likely to have practical consequences in the criminal justice system. In short, Samuel Smith absolutely deserves the award.

Thank you for your consideration,

Dr. Brandon Goodell
Senior Cryptographer and Resident
Insight Decentralized Consensus