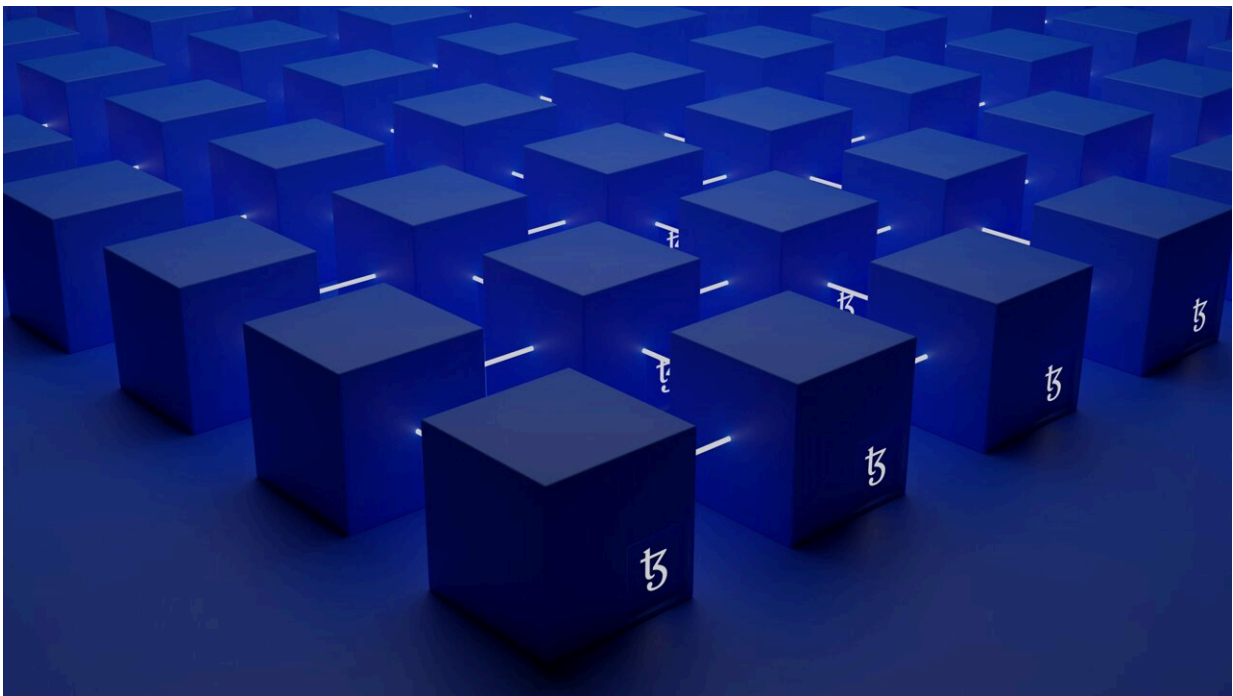# Researchers work to avoid future FTX debacles

January 10 2023, by Katie Malatino

Credit: Unsplash/CC0 Public Domain

The Center for Research toward Advancing Financial Technologies (CRAFT), a collaboration between Rensselaer Polytechnic Institute and Stevens Institute of Technology, is dedicated to advancing blockchain technology so that scams along the lines of FTX's can be avoided. CRAFT researchers from Rensselaer recently presented their findings on blockchain interoperability and cryptocurrency scam detection at the

[2022 IEEE International Conference on Big Data](link).

"The FTX debacle is just one instance of the range of challenges faced by a fragmented blockchain ecosystem that is unlikely to ever become completely decentralized," said Aparna Gupta, CRAFT co-director and site director and Rensselaer professor of quantitative finance. "From Central Bank Digital Currencies (CBDCs) to transactions in a vast range of other digitized assets, sound blockchain interoperability is key to resilience."

Oshani Seneviratne, assistant professor of computer science and associate director of the Tetherless World Constellation at Rensselaer, along with Gupta and doctoral student Inwon Kang [researched different ways to achieve blockchain interoperability](link).

Now, customers largely choose among technologies, rather than benefit from being able to transmit tokens or execute smart contracts among platforms. With blockchain interoperability, transfers can be made among different blockchains without sacrificing performance or security.

The team found that three broad integration modes were common throughout: decentralized relays, hub and spoke, and decentralized oracles. In decentralized relay architecture, networks communicate through gateways that offer read and write access. With the hub and spoke architecture, both the hub and spoke are different blockchains that sync with the target chains. With decentralized relay, blockchains are connected with software rather than additional blockchains.

The researchers found that all of the modes have strengths and weaknesses and, although it is too early to decisively categorize one as superior, it is important for both users and developers to prioritize interoperability moving forward.

"It could be argued that FTX's collapse would not have happened if it had embraced the principles that blockchain and cryptocurrencies were founded on, namely decentralization and transparency," Seneviratne said.

"However, exchanges such as FTX exist due to problems with asset custodianship, as novice crypto users can lose access to their assets in various decentralized systems if they lose their private keys. Therefore, as cryptocurrencies become more mainstream, and since there is no single, dominant blockchain, we need robust interoperability solutions that will provide stability in the absence of complete decentralization."

Seneviratne and her undergraduate research student Jared Gridley also developed a model to predict cryptocurrency scams. Using graph mining techniques, they collected essential information on transactions. Then, the team applied Benford's Law to extract distributional information on the unique, random sets of numbers and letters that are applied to each transaction.

Benford's law is a natural phenomenon that maps the occurrence of first and second digits in many naturally occurring numerical sets. Simply put, according to Benford's Law, the number one ("1") will be the leading digit 30.1% of the time, number two ("2") will be the leading digit 17.6% of the time, and each subsequent number will be the leading digit with decreasing frequency in a power law distribution. Any naturally occurring numerical dataset that deviates from this pattern typically has made-up data characteristic of scams, frauds, and attacks.

The team applied this methodology to Ethereum transaction data and reported scam data from Etherscan. Their labeled dataset consisted of thousands of suspected Ethereum scam addresses with approximately 2.6 million transactions. To get the features to train the model classifiers, the team extracted the transaction graph for each address and then generated

a statistical representation of the [transaction](#) graph. They examined various features such as the number of transactions, unique addresses, values for gas limits, and value transferred.

Each feature was broken down between incoming and outgoing, and to measure the fit of these features with Benford's Law, the team separated the addresses by the scam and non-scam labels and used two statistical tests. They found that the scam addresses had a clear divergence, while non-scam transactions followed Benford's law more closely.

"These findings are significant because it is one of the first uses of Benford's Law to predict scams in cryptocurrencies," Seneviratne said. "Further, Benford's Law has been admitted as evidence in court, making it a valuable tool in legal proceedings."

Seneviratne notes that the research was well-received at the IEEE conference and was a great achievement for Gridley as an undergraduate.

Provided by Rensselaer Polytechnic Institute