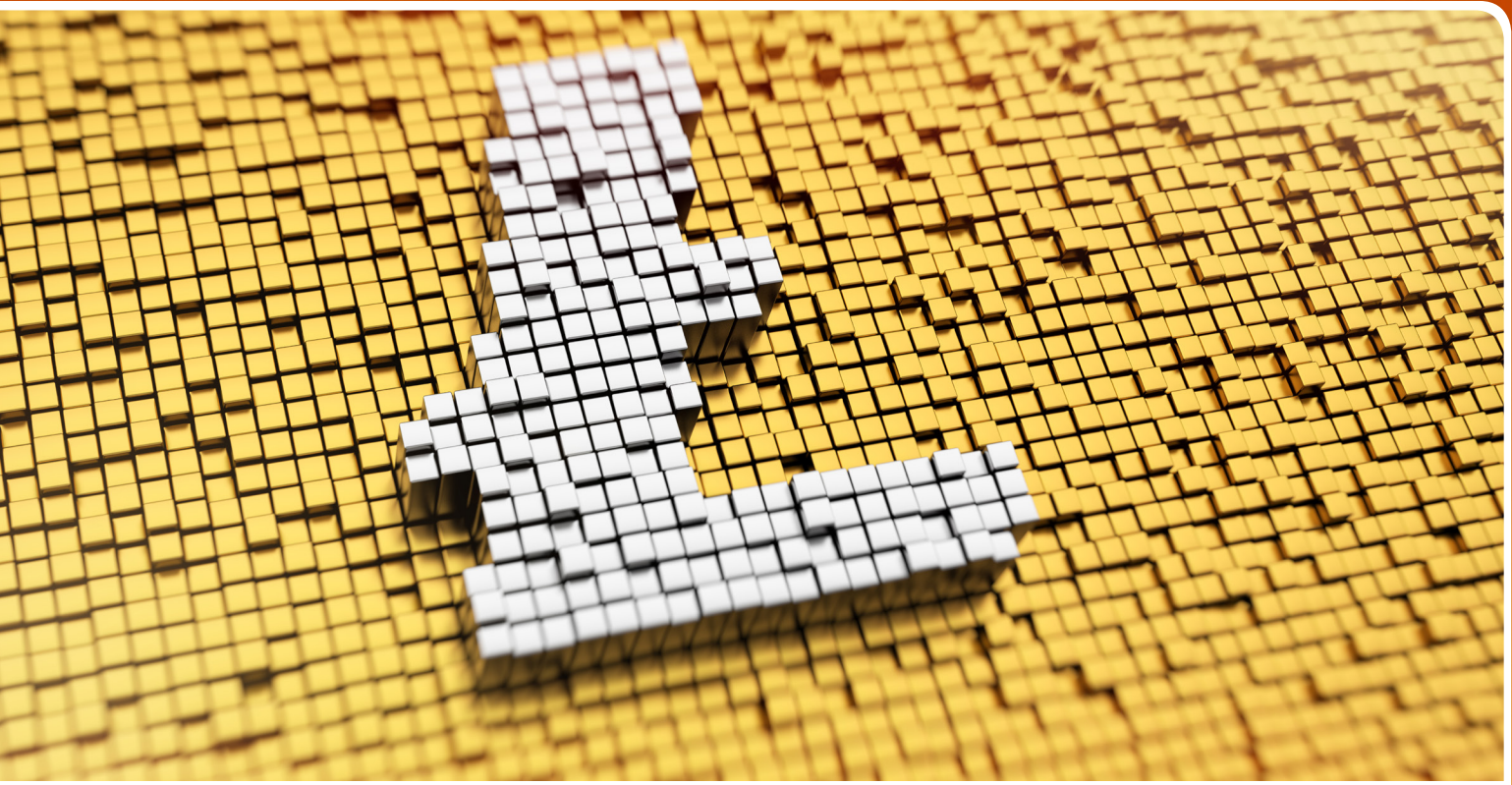
Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*



Digital Currency Graph Forensics

Initially, financial systems maturation occurred through the digitization of banking and credit networks. More recently, it has changed through the rise of digital currencies and crypto-currencies (CCs), the most prominent of which is Bitcoin. The introduction of this new currency as well as the development of new information technologies, has opened a door to opportunities to defraud the system. Scientists at Pacific Northwest National Laboratory (PNNL) have been working on ways to deter these efforts.

Challenge

CCs are often described as a collection of concepts and technologies that form the basis of a digital money ecosystem, or more broadly, a global-scale, decentralized leger system. Units of currency are used to store and transmit value among participants in a distributed, publically available, peer-to-peer network. The mechanism of the cryptographic "block chain" allows encoding of the Bitcoin transaction network in a public, but pseudonymous, fashion.

CC users communicate with each other using a cryptographic protocol primarily via the Internet, although other transport networks can also be used. Users can transfer CCs over the network to do nearly any transaction that can be completed with conventional currencies, such as buy and sell goods, send money to people or organizations, or extend credit. They can be purchased, sold, and exchanged for other currencies at specialized currency exchanges, and since values can fluctuate relative to fiat currencies, they can also be a vehicle for speculation.

The attraction of digital currencies to criminals, and in particular the ability to engage in activities such as tax evasion, trafficking of illicit goods, and money laundering, engender severe technical risks and challenges to technologists, analysts, law enforcement, and policy makers.

Approach

PNNL research is finding ways to identify patterns of anomalous behavior in the publicly available information derived from these large anonymous, distributed cryptographic data networks. This research requires novel technological developments around graph data management, graph pattern mining, and graph data modeling.

Data scientists at PNNL are examining the "public block chain" of CC transactions in an attempt to identify significant patterns, including those that appear to match known patterns of illicit activity. Beyond identifying individual CCs, researchers are exploring ways to link multiple financial networks through their exchanges, services that link to a traditional financial network, or other CCs. This will support the identification of broader patterns that may include the existence of more sophisticated laundering mechanisms and cross currency movement. In addition, forensics intends to characterize the relative strengths and weaknesses of various privacy technologies including block-chain schemes. The block-chain approach's effectiveness will be compared to other techniques including differential privacy and homomorphic encryption.

Impact

Digital Currency Graph Forensics will be able to augment the national security community's ability to identify threat finance activities by providing a foundational computational capability for global-scale, decentralized leger systems. This science also intends to offer data-protection recommendations to the PNNL Data Stewardship Board and improve involvement in the larger privacy research community.

Digital Currency Graph Forensics Capabilities

- Novel formal, mathematical, and computational mechanisms and methodologies to represent and analyze transaction graphs as directed hypergraphs
- Ability to model and identify patterns of behavior in distributed cryptographically assured transaction networks beyond CCs
- Mathematical and comparative understanding of privacy approaches

About PNNL

Interdisciplinary teams at PNNL address many of America's most pressing issues in energy, the environment and national security through advances in basic and applied science. Founded in 1965, PNNL employs 4,400 staff and has an annual budget of nearly $1 billion. It is managed by Battelle for the U.S. Department of Energy's Office of Science.

For more information, please contact:

Cliff Joslyn
Scientist
(206) 528-3042
cliff.joslyn@pnnl.gov

Curtis West
Engineer
(206) 528-3406
curtis.west@pnnl.gov

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

U.S. DEPARTMENT OF ENERGY