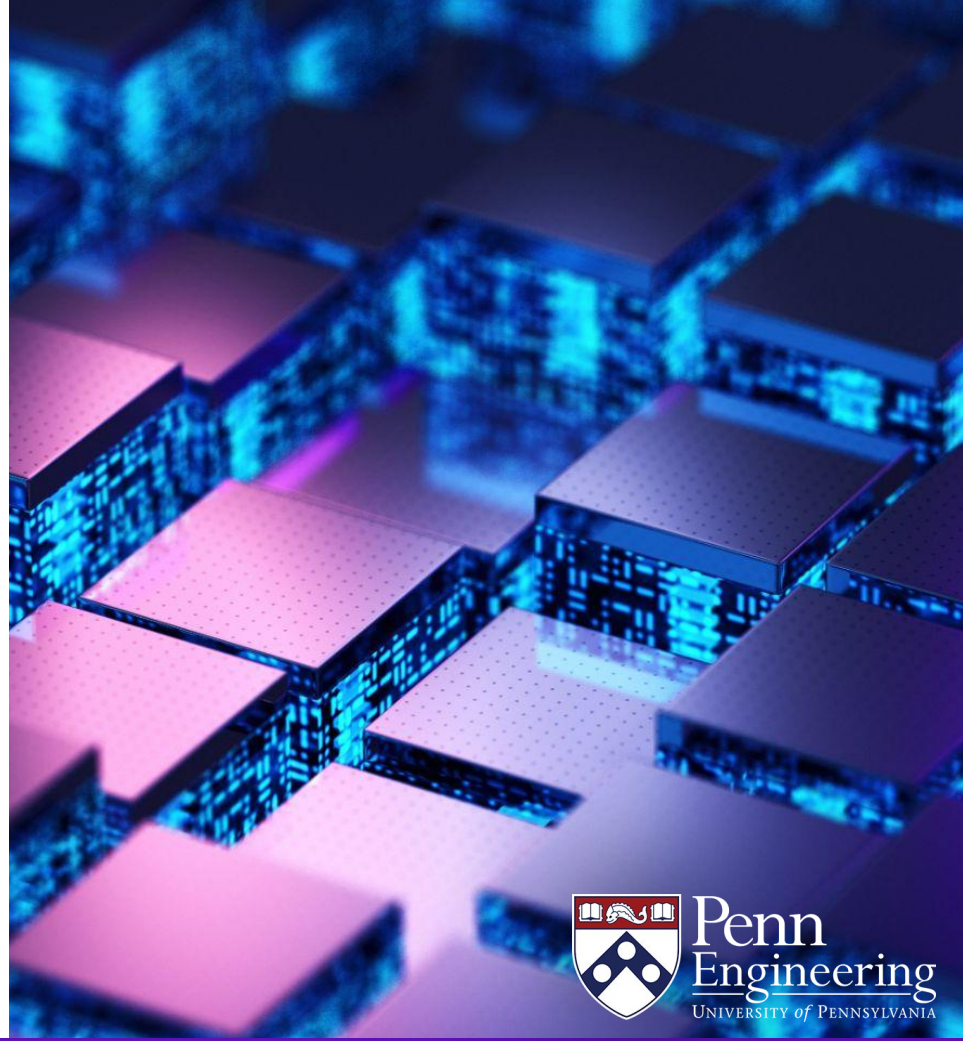
EAS 5830: BLOCKCHAINS

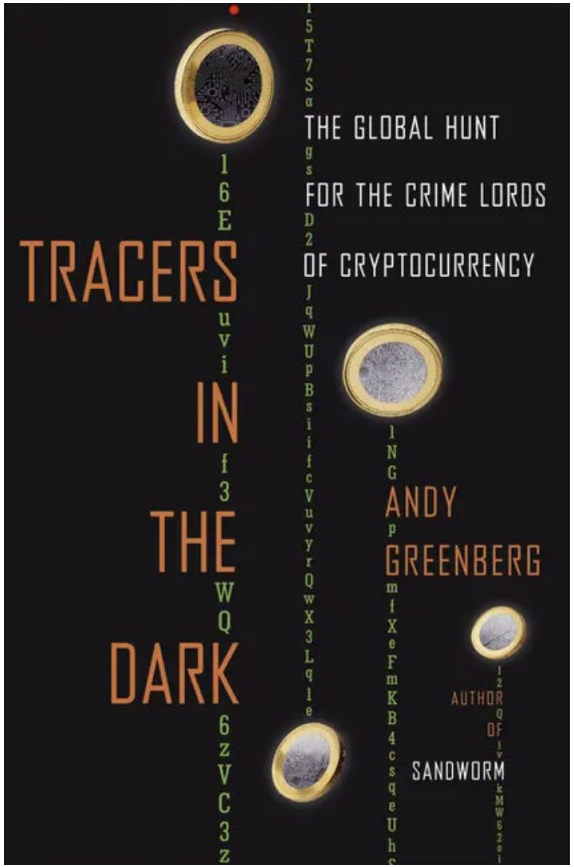
Privacy

Professor Brett Hemenway Falk



“Bitcoin is the opposite of untraceable…other cryptocurrencies too are completely traceable and had served as this kind of trap I began to see for people seeking Financial privacy”

Andy Greenberg


TRACERS
IN
THE
DARK
THE GLOBAL HUNT
FOR THE CRIME LORDS
OF CRYPTOCURRENCY
ANDY
GREENBERG
AUTHOR
OF
SANDWORM

"It became clear that not only was Bitcoin very traceable, but the cryptocurrency tracing had actually been used as this incredibly powerful law enforcement investigative technique in that this small group of detectives, who then become the subject of my book, had gone on this spree of cyber-criminal busts, tracing cryptocurrency to take down one massive criminal operation online after another"

Censorship resistance

Bitcoin was founded on the idea of censorship resistance

Not privacy

Public ledgers are not private

“The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method...”

-Satoshi Nakamoto

Maintaining Privacy in Bitcoin

"privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous."

(Public keys are pseudonyms)

(Recipients are hashes of public keys)

"a new key pair should be used for each transaction to keep them from being linked to a common owner."

-Satoshi Nakamoto

Pseudonymity

- All transactions are public
- Accounts have pseudonyms not names
- Users can have multiple accounts

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

University of California, San Diego George Mason University[†]

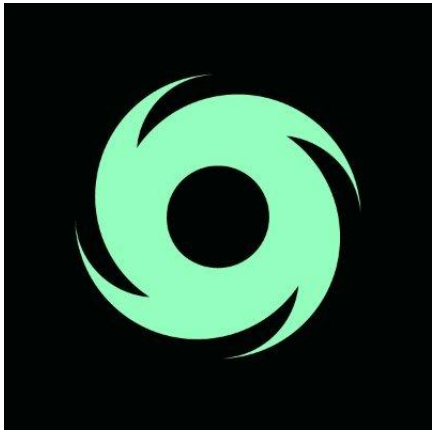

Chainalysis

VANITY FAIR

CRYPTO CRIME SEPTEMBER 2022 ISSUE

The Ballad of Razzlekhan and Dutch, Bitcoin's Bonnie and Clyde


ECKS



“Monero is a huge issue. People are out there talking about how they can trace Monero. They can’t. Not to a level where you can actually convict somebody in a criminal court without other evidence.”

Tigran Gambaryan

Former IRS CI Analyst