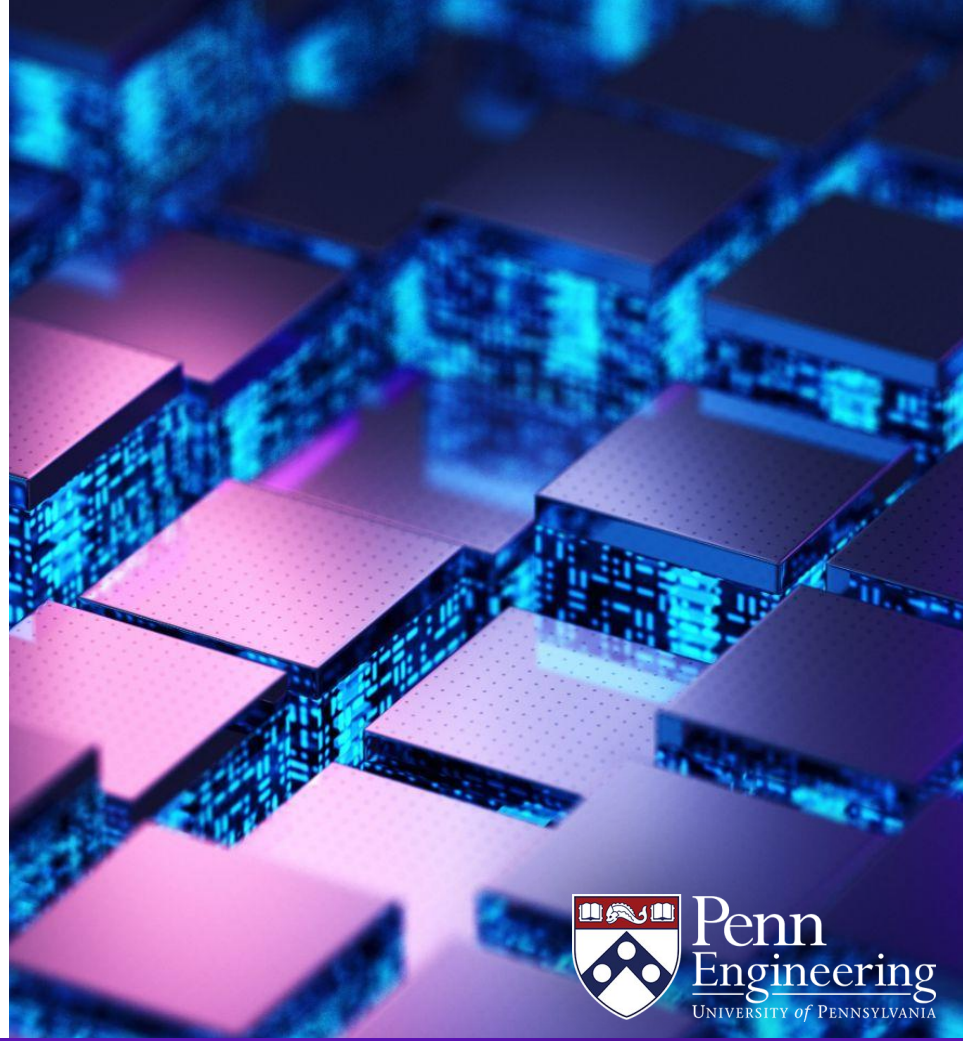
EAS 5830: BLOCKCHAINS

Monero

Professor Brett Hemenway Falk



Monero

- Launched in 2014
- Proof-of-Work blockchain
  - Uses RandomX for PoW
  - ASIC resistant
- 27th largest cryptocurrency
- Market cap $3 Billion (November 2023)
- Based on the CryptoNote protocol

Privacy

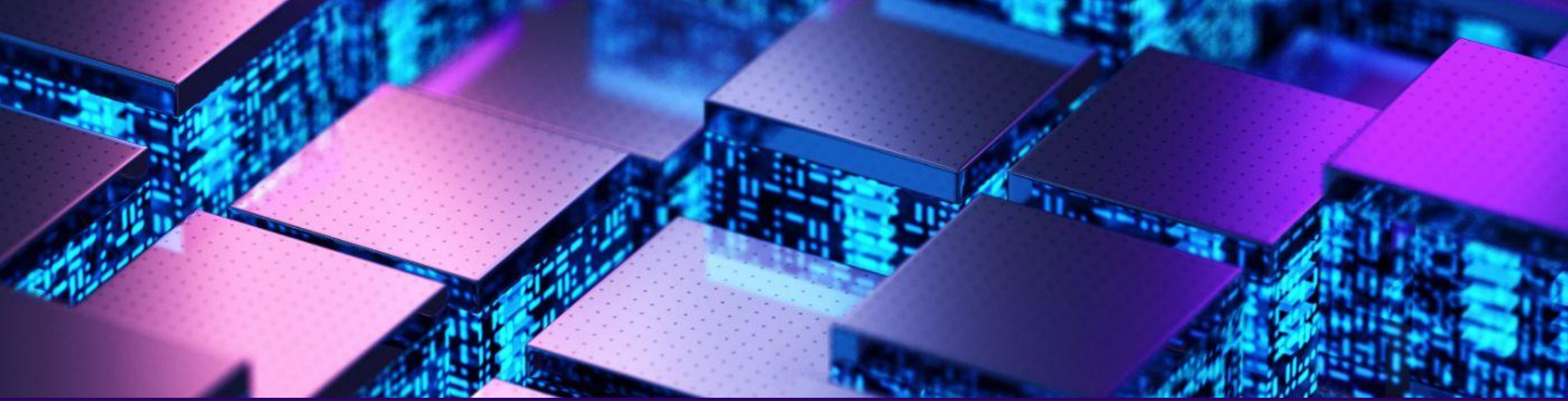
- Sender Privacy
  - Ring Signatures
- Receiver Privacy
  - Stealth Addresses
- Value privacy
  - Ring confidential transactions

CRYPTOCURRENCY CURRENTS —

Monero emerges as crypto of choice for cybercriminals

Untraceable "privacy coin" is rising in popularity among ransomware gangs.

HANNAH MURPHY, FINANCIAL TIMES - 6/22/2021, 9:35 AM



Ring Signatures

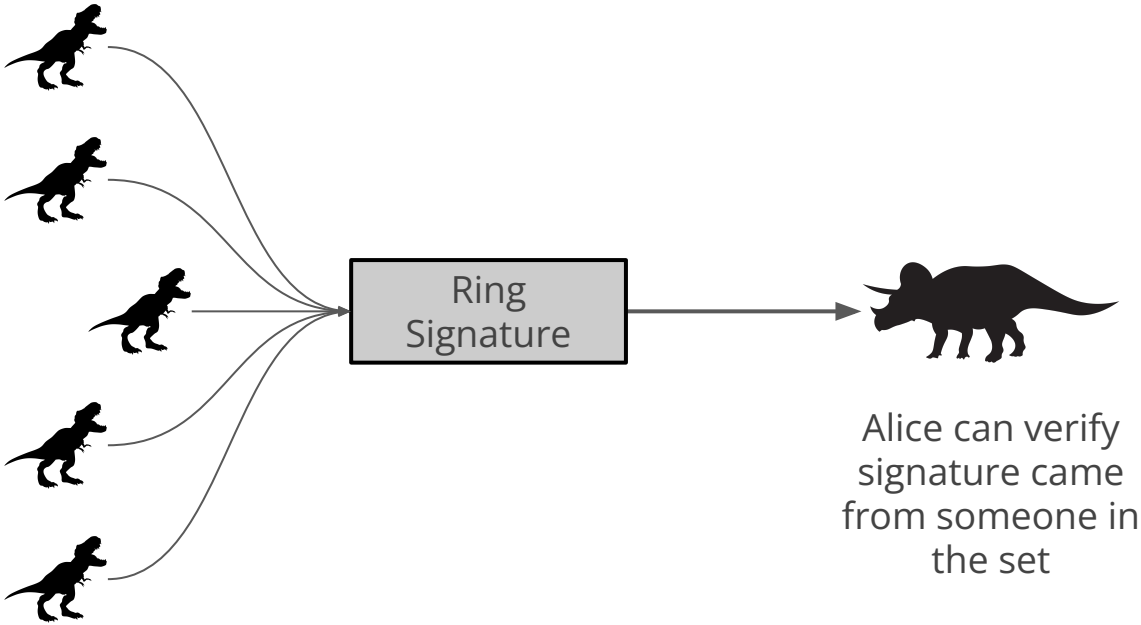
Ring signatures

- How to leak a secret (2001)
- A cabinet member, Bob, wishes to leak a juicy fact to a journalist
- Journalist wants to know the information came from a cabinet member
- Bob wants his identity to remain hidden

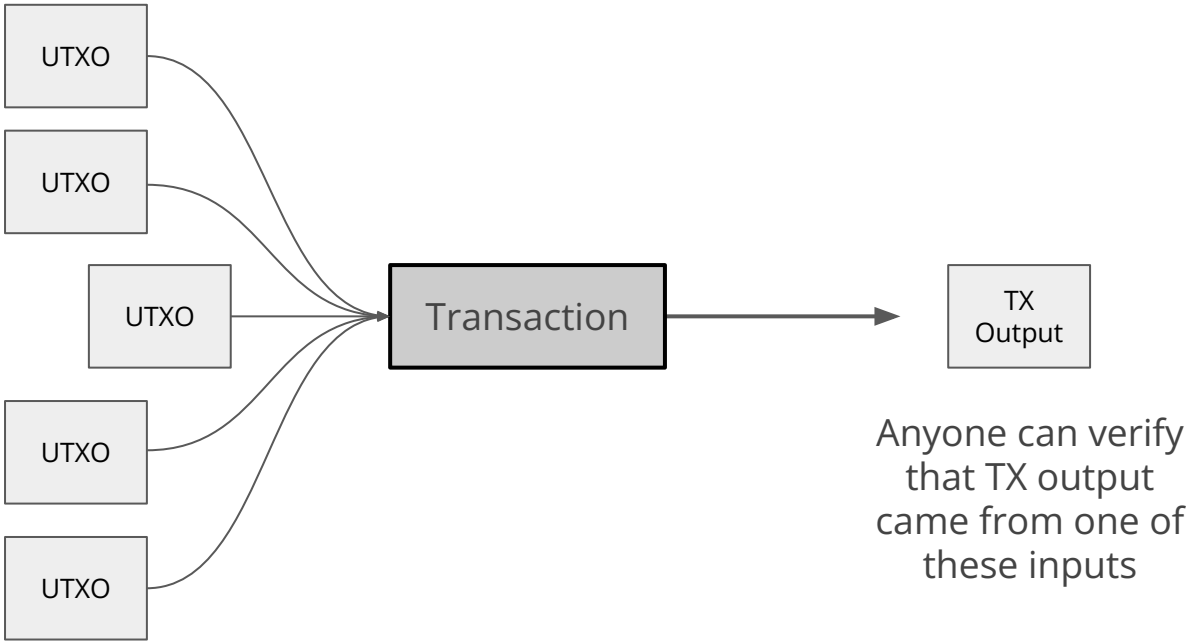
Regular signatures

Alice can verify signature came from Bob

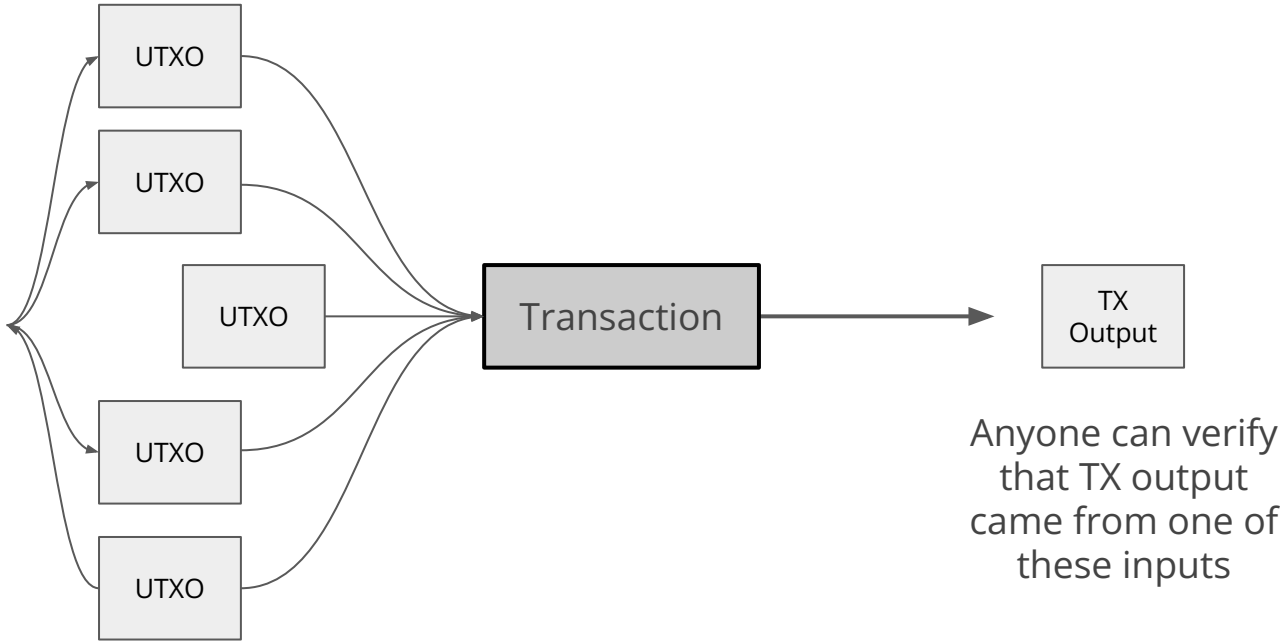
Ring signatures



Ring signatures

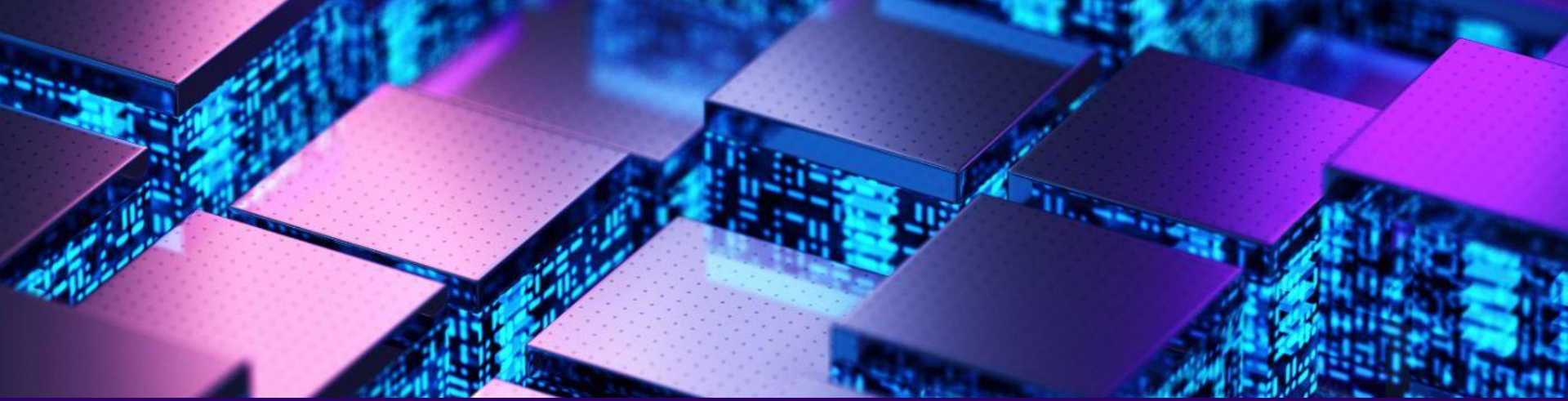


Ring signatures



Other inputs are called “mixins”

Anyone can verify that TX output came from one of these inputs



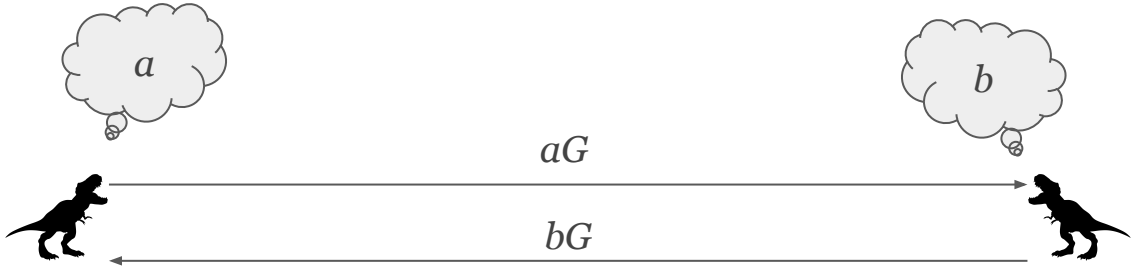
Stealth Addresses

Receiver privacy

- Stealth addresses
- Sender can re-randomize receiver’s address
- Receiver scans through transactions to find re-randomized addresses

Diffie-Hellman Key Exchange

EC-DL problem:
Given aG it's hard to find a



Alice computes $a(bG)$

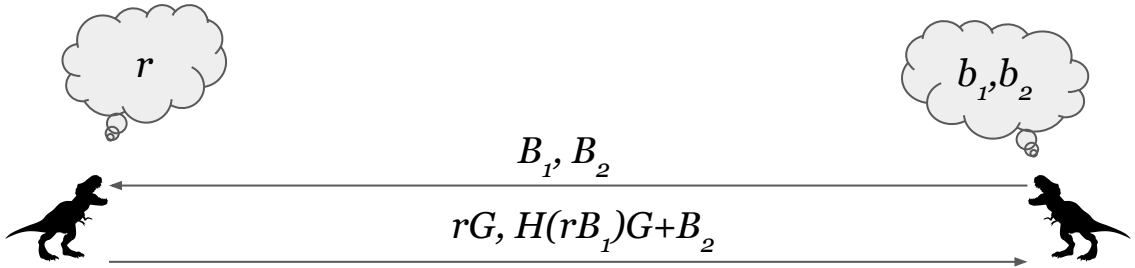
Bob computes $b(aG)$

$H(abG) = H(baG)$ is a 256-bit integer that can be used as a private key

Stealth addresses

- Recipient, Bob, has two keys b_1, b_2
- Use the first for a DH key exchange to derive a one-time key, k
- Stealth key is $k + b_2$

Stealth addresses



Alice sends Bob:

$R = rG$ (for DH key exchange)

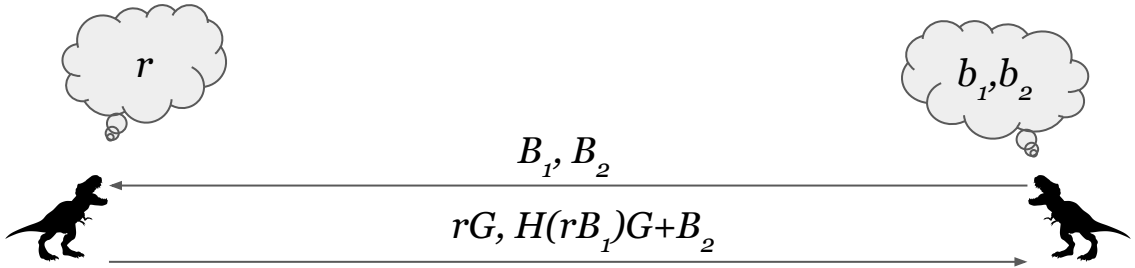
$PK = H(rB_1)G + B_2$

Bob has two public keys:

$B_1 = b_1G$ (for DH key exchange)

$B_2 = b_2G$

Stealth addresses



Alice sends Bob:

$R = rG$ (for DH key exchange)

$PK = H(rB_1)G + B_2$

DH key is: $k = H(rB_1)$

One-time "Stealth" PK is:

$PK = kG + B_2$

Bob knows SK:

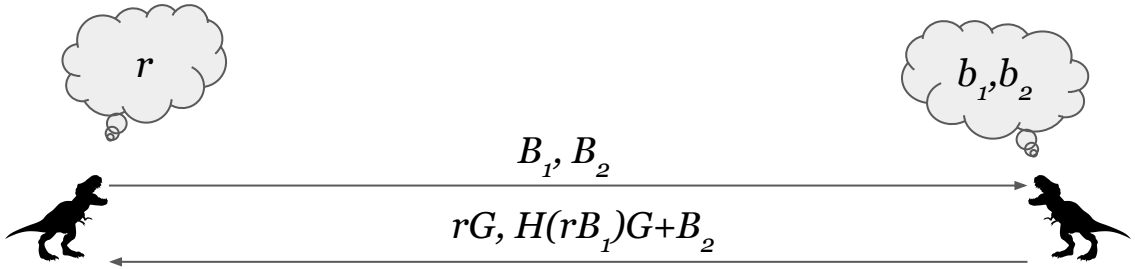
$H(b_1R) + b_2 = k + b_2$

Bob has two public keys:

$B_1 = b_1G$ (for DH key exchange)

$B_2 = b_2G$

Stealth addresses



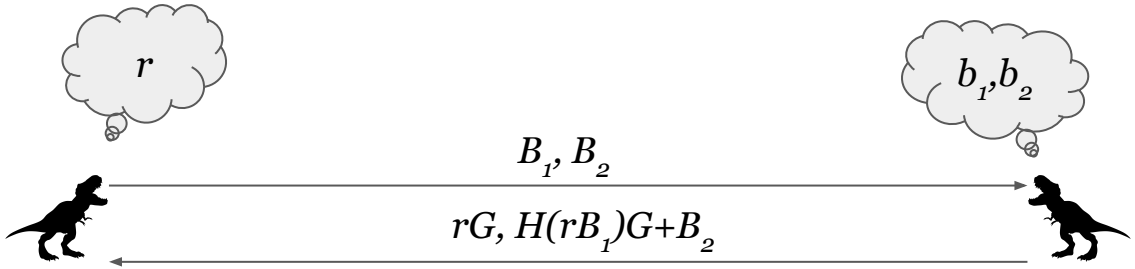
Alice sends to
$PK = H(rB_1)G + B_2$
Also includes $R = rG$

Transaction includes:
(R, PK)

Bob checks:
$H(b_1R)G + B_2 = PK$
For **all** transactions to see if he is the recipient

Bob has two public keys:
$B_1 = b_1G$
$B_2 = b_2G$

Stealth addresses



Alice sends to
$PK = H(rB_1)G + B_2$
Also includes $R = rG$

For every transaction recipient (R, PK):

Bob checks:
$H(b_1R)G + B_2 = PK$

If so, Bob knows SK
$H(b_1R) + b_2 = H(b_1rG) + b_2$

Bob has two public keys:
$B_1 = b_1G$
$B_2 = b_2G$

Privacy

- Ring signatures
  - True input is masked with a small set of “mixins”
- Stealth addresses
  - Every transaction is sent to a new address
- Ring confidential transactions
  - Hides amount
- Transaction *times* are not hidden

“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