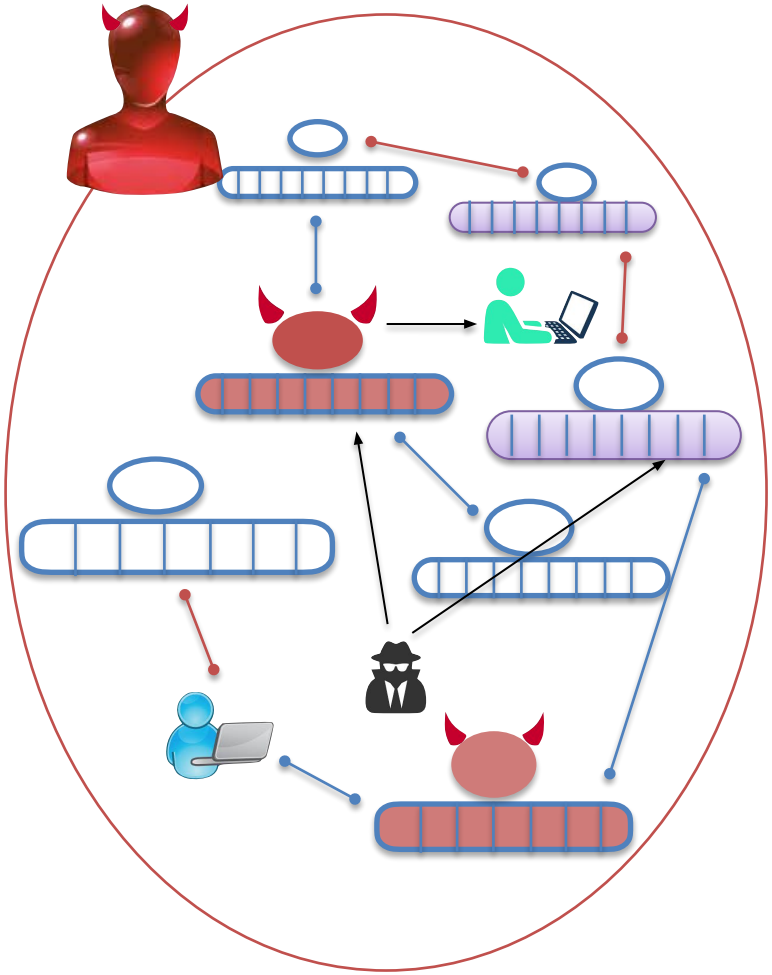
SaTC: CORE: Small: A Broad Treatment of Privacy in Blockchains

Challenge:

- Formalize privacy properties in blockchain.
- Provide constructions that achieve desired level of privacy in presence of powerful network attacks

Solutions:

- Identified shortcomings of previous approaches; provided composable definitions.
- Designed new crypto primitives that leverage/are compatible with the blockchain setting.
- Applied techniques from differential privacy for efficient private large-scale mixing of blockchain transactions.



An ecosystem of interacting Blockchains in the presence of privacy adversaries

Scientific Impact:

- Our attacks raise awareness of the challenges of designing privacy-preserving schemes in the blockchain setting.
- They can pave the way to new approaches for developing privacy-preserving solutions for blockchain

Broader Impact:

- Awareness of the inherent attacks is key when developing real world applications.
- Some of our designs can be efficiently implemented in certain settings (such as blockchain governance).
- Our findings are incorporated in our crypto/security classes. Both PIs participate often to specialized panels and raise awareness of such issues

Project info: 1718074, NCSU/GMU,
PI A. Scafuro ascafur@ncsu.edu
Co-PI F. Baldimtsi foteini@gmu.edu

NC STATE UNIVERSITY

GEORGE MASON UNIVERSITY