NSF Campus Cyberinfrastructure PI and
Cybersecurity Innovation for Cyberinfrastructure PI Workshop

Sep. 23-25, 2019 | Minneapolis, MN

NSF Program (either CC or CICI): CICI

Program Area: CyberInfra. **Award Number: 1547164**

PI: R. R. Brooks, Clemson
co-PIs: A. Skjellum, UTC

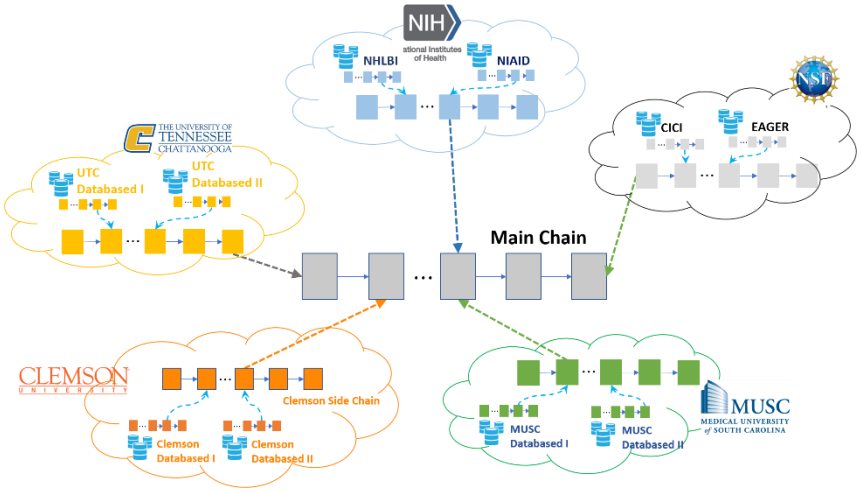
Project Title: CICI: Data Provenance: Collaborative Research: Provenance Assurance Using Currency Primitives

Richard R. Brooks
Professor ECE
Clemson University
rrb@g.clemson.edu

Anthony Skjellum
Professor and Director, SimCenter
Computer Science and Engineering
Tony-Skjellum@utc.edu

NSF Campus Cyberinfrastructure PI and
Cybersecurity Innovation for Cyberinfrastructure PI Workshop
Sep. 23-25, 2019 | Minneapolis, MN

CICI: Data Provenance: Collaborative Research: Provenance Assurance Using Currency Primitives



Broader Impact:

- *Collaboration with biomedical scientist from Medical University of South Carolina (MUSC).*
- *The winner of the White Board Challenge during the 2018 IEEE Blockchain for Clinical Trials Forum.*
- *Invited talk at 2018 IEEE Blockchain for Agriculture Forum.*
- *Invited talk at 2019 2nd IEEE International Conference on Blockchain*
- *The PI Richard serves as the recording secretary in the IEEE P2418.3 DLT for Agriculture Standards working Group.*

Challenges:

- *Efficient and secure symmetric key management has been a challenge. Thus, existing symmetric management systems are all centralized.*
- *Academic integrity in clinical studies is more complex than other areas because medical and national defense installations enforce data protection and privacy rules more vigorously than most universities.*

Deliverables:

- *System that uses a blockchain to manage symmetric keys establishment, distribution, and revocation*
- *Patent on "System and Method for Efficient Distributed Ledger Technology for Metadata Security "*
- *Patent on "Authorization of Data Access using Blockchain"*
- *Book chapter on Scrybe in the Springer book "Blockchain Cybersecurity, Trust, and Privacy"*

Metadata tag:

- *Journal paper to be submited: "A security analysis of Scrybe, a secure-provenance blockchain based on a lightweight consensus mechanism"*
- *Journal paper under review: "Scrybe: a secure audit trail for clinical trail data"*
- *Journal paper under preparation: "Symmetric key management using on-chain KEK"*
- *Looking for transition targets for the key management system, potential partner involves Google Trillian (https://github.com/google/trillian)*