# Bitcoin/Blockchain: threat analysis, mitigation, and applications

**Jiangshan Yu**

CritiX Lab (Critical and Extreme Security and Dependability)
Interdisciplinary Centre for Security, Reliability and Trust - University of Luxembourg

PEARL Grant FNR/P14/8149128 – Paulo Esteves-Veríssimo

Jiangshan.yu@uni.lu
jiangshanyu.com

# I'm new to CritiX

**My background:**

- **Ph.D in Cyber Security** (2012-2016). University of Birmingham, UK.
- **M.Phil in Cryptography** (2011-2012). University of Wollongong, Australia.
- **M.Sc. in Info. Security** (2010-2011). University of Wollongong, Australia.
- **B.Eng. in Computer Science** (2005-2009). Northeast Agricultural University, China.

# I'm new to CritiX

**My background (cont.):**

- RA at CritiX, SnT, University of Luxembourg. (Dec. 2016-)
- Honorary research fellow, University of Birmingham, UK. (Oct. 2016-)
- Director, CloudTomo Ltd, (Uni spin-out company), UK. (Nov. 2014-)

# Previously:

securityandtrust.lu

**Past research interests:**

Design and analysis of cryptographic protocols

- Key management (e.g. X.509 PKI)
- Secure authentication (e.g. SSO)
- Post compromise security
  (e.g. Device compromise detection)
- Public-ledger-based application
  (e.g. systems with verifiable transparency)

# Previously:

securityandtrust.lu

CRITIX

**Highlights of past research impact:**

- Ledger-based secure messaging application (2014)
  - InnovateUK funded the feasibility study (GBP 33k)
  - Both German gov and US/UK defence supplier (L3-TRL) have been interested in adapting it
- Key management (2016)
  - Huawei SoC secure boot solution

# Now and Future

securityandtrust.lu

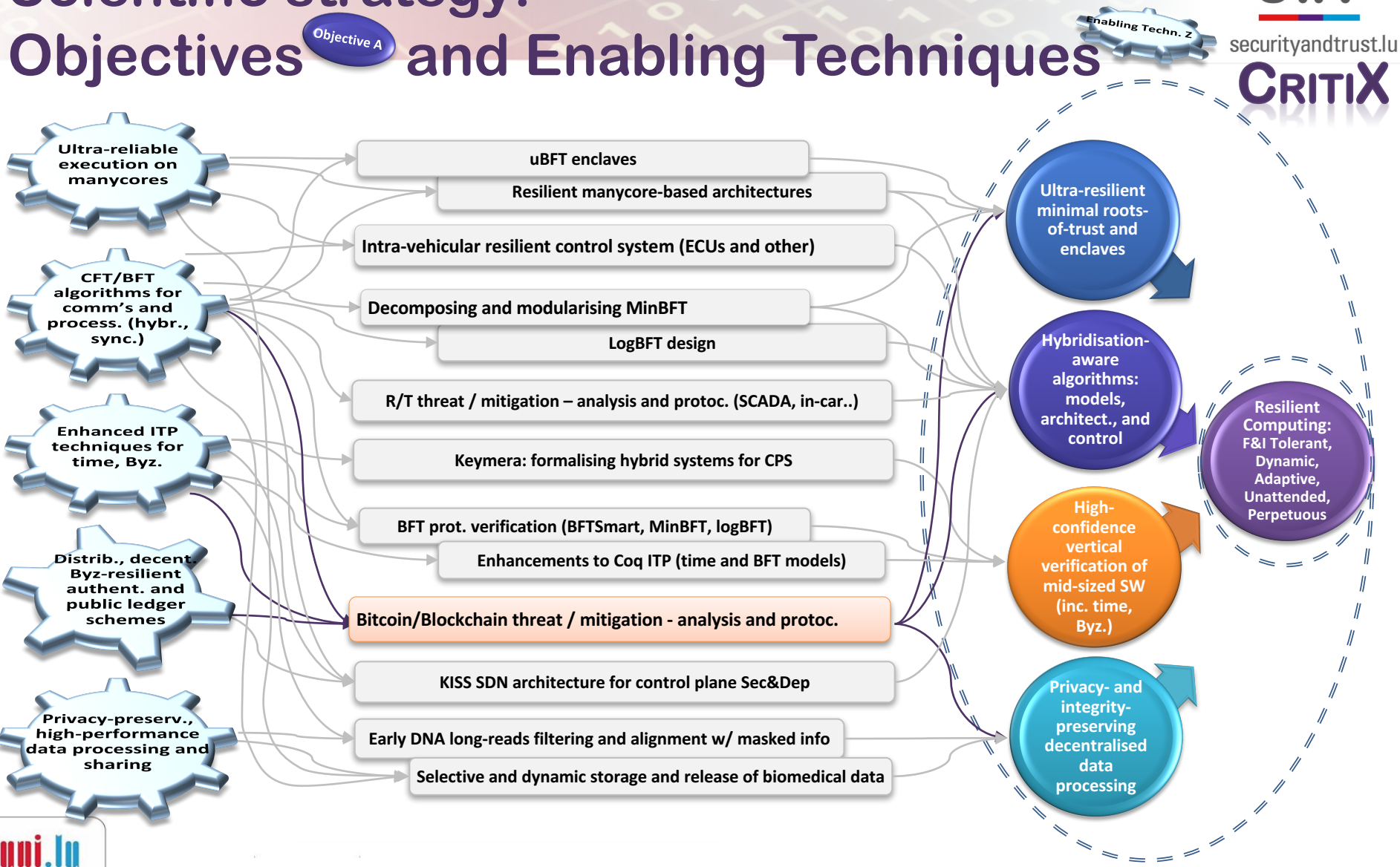
CritiX

**Research plan in CritiX:**

Blockchain application and threat analysis

uni.lu UNIVERSITÉ DU LUXEMBOURG

# Scientific strategy: Objectives and Enabling Techniques



# Now:

securityandtrust.lu

**Current research:**

- Bitcoin analysis and improvement
  - Analyse and eliminate rational attackers (Selfish mining attack needs >25% computing power rather than >50%)
  - Improving the blockchain proof-of-work mechanism by using different concepts (e.g. reputation based system, trusted hardware)

# Future:

securityandtrust.lu

**Future research:**

- Adapting Byzantine fault tolerance techniques and hybrid models in Blockchain consensus
  - Use trusted computing where we can
  - Use efficient protocols in normal cases
  - Switch to more robust (expensive) protocols when attacks detected

# Future:

securityandtrust.lu

**Future research:**

- Ensure transparency and authenticity in critical infrastructures, such as
  - home automation
  - automated vehicle communication
  - smart contract
  - software defined networking