FIN593 Blockchain Security and Privacy

Level: 5
Credit Units: 2.5 Credit Units
Language: CHINESE
Presentation Pattern: EVERY JULY

Synopsis:

FIN593 Blockchain Security and Privacy focuses on information security and cryptography techniques underlying fintech and blockchain technology. The course analyses different security concepts and examines how cryptographic techniques are used to realise different security objectives. It then looks at how the properties of secure cryptographic function techniques can be used to protect data integrity, authentication and user privacy in blockchain and fintech applications, and evaluates the feasibility of the protocol design. It also discusses data integrity and confidentiality protection techniques, public-key infrastructure, peer-to-peer security, and network security, access control models and advanced cryptographic techniques to provide user privacy. Students will learn how to use open source security software such as Cryptool, GNU Privacy Guard, and the Python package for cryptography at an advanced level.

Topics:

- Security objectives, threat and defense in a blockchain system
- Hash function
- Digital signature
- Peer-to-peer and network security: attacks and defense
- User privacy and identity
- Data privacy on a blockchain
- Zero-knowledge proofs
- Secure multi-party computing

Learning Outcome:

- Appraise security objectives, threat models and the defense mechanism in a blockchain system
- Assess how cryptographic techniques are used to make blockchain works as a secure distributed ledger technology
- Appraise peer-to-peer and network security and relate it to blockchain applications
- Evaluate the need of user privacy and criticise how user privacy is provided in existing blockchain and fintech applications
- Design solutions to address design flaw(s) in cryptographic protocols
- Construct applications based on existing open-source software to simulate blockchain applications

Assessment Strategies (Evening Class):

Components	Description	Weightage Allocation (%)
Overall Continuous Assessment	PARTICIPATION 1	10
	GROUP BASED ASSIGNMENT 1	40
Overall Examinable		

Overall Examinable Components	ECA	50
Total		**100**