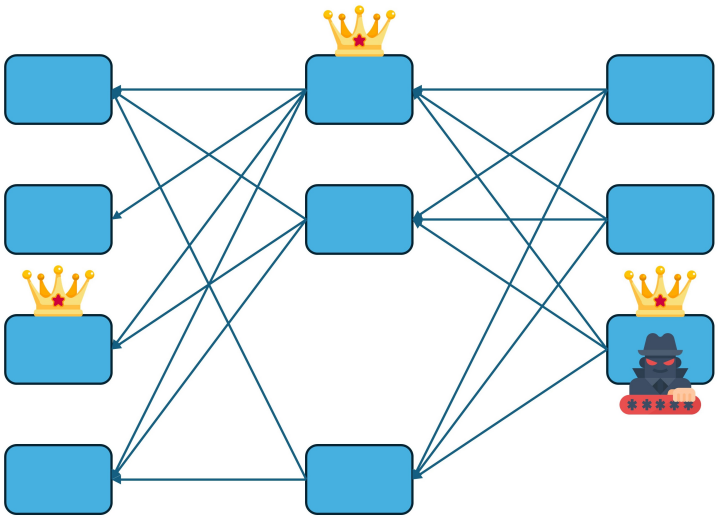
Security Analysis of DAG-Based Blockchains



DAG-based Byzantine Fault Tolerant (BFT) blockchains, such as Narwhal, Bullshark, and Shoal, represent a pioneering advancement in distributed ledger technology, offering a novel approach to achieving consensus among decentralized network participants. Unlike traditional blockchain architectures that rely on linear blockchains, DAG-based BFT blockchains utilize Directed Acyclic Graphs (DAGs) to structure transactions, enabling parallel processing and scalability while maintaining robust Byzantine fault tolerance. This paradigm shift allows for increased transaction throughput and reduced confirmation times.

Each blockchain protocol must satisfy two essential properties: safety and liveness, to be considered secure. However, there is a possibility that Byzantine validators/miners may target the safety and liveness of a blockchain protocol to compromise its security. Additionally, rational validators/miners may deviate from honest strategies to increase their payoff. In recent years, several attacks targeting the blockchain consensus layer, such as selfish mining in Bitcoin, as well as avalanche and balancing attacks in Ethereum, have been proposed.

The aim of this thesis is as follows: firstly, the student needs to review existing DAG-based BFT blockchains and the known attacks on blockchain protocols. Next, the student is expected to analyze the existing DAG-based BFT blockchains to identify potential security bottlenecks that malicious or rational validators may exploit within the blockchain network. For the implementation part, the student needs to implement the attack and assess its feasibility. Proposing a solution to mitigate the potential attack can be considered for bonus points.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Roozbeh Sarenche	roozbeh.sarenche@esat.kuleuven.be	office B01.13
	Varesh Mishra	varesh.mishra@esat.kuleuven.be	office B01.23
Nature of the work:	20% literature, 50% theoretical work, 30% implementation		
Number of students:	1		

 © 2026 – 2027 COSIC