13th Annual Conference – Oct. 4ᵗʰ, 2021

Presentation Title	Formal Verification of Smart Contracts
Speaker	Souhail Mssassi He has 8+ years experience in cybersecurity in offensive Security specialized in application security, cryptography and security of decentralized applications. He is Also a Speaker and we presented Security lectures in schools as well as universities in Morocco. In parallel, he also does research in the field of security lately in Formal Verification
Abstract	A smart contract is written in a programming language (commonly Solidity) and then translated into bytecodes. Once a smart contract is reduced to bytecodes, it can be deployed on the blockchain as a contract account at some address. Once deployed no one can change it or apply a patch to it. We should have great confidence that the contract will behave correctly no matter what. Formal verification is essentially concerned with identifying the correctness of hardware and software design operation. Because verification uses formal mathematical proofs, a suitable mathematical model of the design must be created.