What about Security in DLT, blockchain and components like dApps, smart contracts, wallets, frameworks?

Security in DLT is different from implementing blockchain or smart contracts or the paper of Nakamoto or looking for bugs or errors or traditional pen tests. Its a different way of thinking. You need no experience inimplementing DLT or as an web developer. And e.g. you should accept, that smart contracts are implemented algorithms: Programs and software.

There are ony a few, security auditing DLT and blockchain, Ethereum, …including components like dApps, smart contracts, wallets, frameworks are special! You have to identify security bugs and errors: Vulnerabilities are the basis for attacks. You have to use several tools (not only one – they are overlapping in identifying vulnerabilities about 20% - but mostly they identify different vulnerabilities.

50% of the really critical vulnerabilities are identified by thinking to be an attacker. And: You really have to look tool-supported reviewing the implementation AND the executables. This requires much experience in crypto applications especially in source and byte code.

Smaller (only a few lines of code) applications and smart contracts you can check by formal verification. But this checks only the correctness of the code – to compare the implementation with the design. But what about the security of the design? And does the design fulfill the security requirements? You have to start at the beginning.

ISO-27034-based is a full security testing process with 5 methods - starting with 'security requirements analysis', 'threat modeling the security design', 'code reading / Static Source Analysis', 'Penetration Testing' and 'Fuzzing' the executables thus identifying known vulnerabilities and especially unknown Zero-Day-Vulnerabilities.If there are no longer vulnerabilities, no attack will be ever more successful because of missing an attack point and a attack surface.

Cryptography tools or suites are not an solution for security. The algorithms may be secure (but what about faster computers, quantum computing,…) – the implementation like every software may contain unpublished vulnerabilities and backdoors.

Not considering security will generate insecure blockchains, dApps, wallets etc.