Join Us!

IE ISSA

Dinner Meeting

Blockchain - What does it mean for Cybersecurity?

By:
Tej Aulakh - leading the source code analysis team as part of ethical hacking and security research group called Spirent SecurityLabs
&
Kurt Kumar - Blockchain Consulting Practice Lead

Blockchain enables consistent security approach of storing, sharing and distributing data and information by autonomously verifying the integrity of encrypted transactions and ability to manage a decentralized ledger of all transactions on the network.

Due to the decentralized networks, Blockchain does not have a centralized point of failure and is better able to withstand malicious attacks. DDOS attacks become moot because a blockchain distributed based approach to storing DNS entries will not likely fail under a high abnormal velocity of requests. Open ledger means that programs can check if a particular application or program is allowed to access a specific resource on the network and isolate it if rogue programs start sending spam requests or are under control of a BOT-Net. Each recipient application can check the immutable ledger before responding to request and thus prevent further damage.

Blockchain embodies on the implementation of a decentralized network that requires a complete shift on cybersecurity challenges such as transaction speed, the verification process, data privacy, and encryption along with possible integration and communication protocols with non-Blockchain related systems.