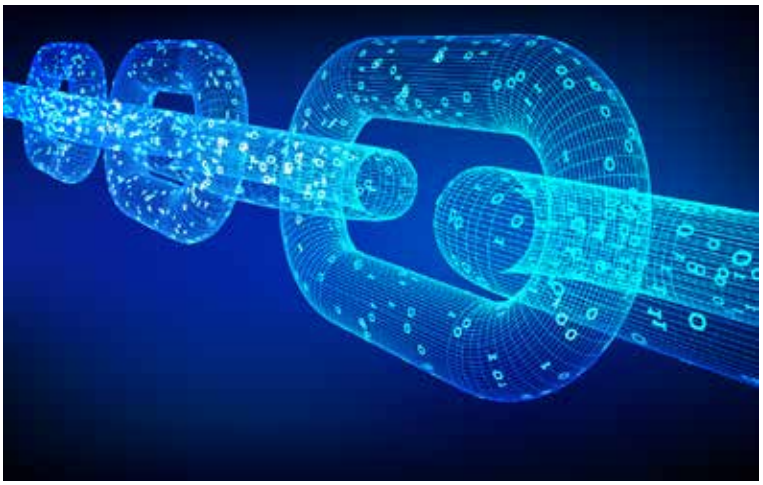
MULTOS Blockchain

Technology for Trusted Services

The Vision & Issue

Blockchain technology is receiving an increasing focus from a wide range of business sectors today, and promises to add trust to information exchanged within decentralized systems. As devices become ever more connected and autonomy is more heavily relied upon, it is clear that blockchain enabled services gain adoption in the coming months and years.

Distribution Ledger Technology utilizing blockchains do have some inherent resistance to attacks but are not immune, and are subject to security issues that centralized data bases are not. One of the most likely vulnerabilities originates outside the blockchain at the endpoints.



Endpoint vulnerabilities reflect on the security of blockchain technology particularly the credentials that are required to access a shared distributed ledger which can be exposed by security weaknesses at the endpoints.

Access to a blockchain requires both a public and a private key. Since it is essentially impossible to access data within a blockchain without the right combination of public and private keys, this represents the strength - and the weakness - of blockchain technology.

MULTOS Blockchain Security

Since hackers know there is no use in trying to guess anyone's keys, they focus a great deal of their time on stealing them. Anytime blockchain keys are entered, displayed, or stored unencrypted, the prying eyes of hackers can capture them.

The secure and trusted MULTOS OS within its hardened, tamper resistant IC is a robust solution for storing endpoint digital credentials.

Protected from hackers, a device may process cryptographic functions ensuring blockchain data and entries are genuine.