According to SANS, up to 80% of cyber breaches may involve supply chain compromise. Supply chain-based risks include counterfeit, malware-embedded or otherwise compromised hardware or software, whether used directly by a consumer or embedded into other devices. In fact, one of the largest Distributed Denial of Service attacks conducted to date was enabled by compromised software in video components which were embedded into other devices.

Participants in UCI’s Cybersecurity Policy & Research Institute (CPRI) have identified software and other supply chain security as a high-priority research issue. CPRI is working to establish a multidisciplinary effort into the potential uses of blockchain and related emerging technologies to better secure supply chains. Blockchain is a distributed virtual ledger technology offering transparency, immutability, authenticity and security.

Blockchains operate as an append-only data structure or a managed database, which is maintained by a decentralized collection of mutually distrusting computational nodes participating in a peer-to-peer network. Blockchain ledgers are updated as a result of recorded transactions, much like a personal bank account is updated through deposit, withdrawal, credit or debit transactions made by the account holder, through a third-party (the bank or transaction system processor), who may charge a fee for transactions.

Much like bank account transactions, blockchain update transactions are distributed over a network and are time-stamped, persistent, and verifiable. However, the peer-to-peer network of blockchain nodes is a decentralized autonomous authority without legal standing, compared to the centralized authority taken by a bank or credit/debit card transaction processor. Because blockchain databases are append-only -- they cannot be rewritten or ‘corrected’ later -- the peer verification system based on a consensus of multiple verification nodes mitigates against error while disallowing change to prior records. These characteristics have the potential to significantly improve supply-chain security.

CPRI has identified more than 15 UCI faculty affiliates for a blockchain research effort, each with research interests related to the potential for using blockchain and other emerging technologies to better secure software and other supply chains. Together, these faculty embody a truly multidisciplinary research effort, representing UCI’s Schools of Information and Computer Sciences, Engineering, Business, Humanities, Law, Physical Sciences, and Social Sciences.

We invite you to make a pledge today to support CPRI in its mission to find technological, legal and policy to combat cyber threats, while protecting and enhancing individual privacy and civil liberties.
Click [here](#) to download the Pledge form and join us in redefining the future of cybersecurity.