White paper

Blockchain security features 101 for Supply Chain

VARA Technology

A VARA Perspective

INTRODUCTION

Supply chain involves multiple collaborating entities with different security policies, mutually incompatible commitments and expectations from the system.

Anonymity

Conventionally anonymity systems relied on third parties to resolve temporary identities from fixed credentials linked to a long term stable identity. The Blockchain advantage is that identity resolution can be done locally without entering into a compulsive trust relationships with remote entities, with no control over them.

Fault Tolerance

The resilience stems from the participative nature of the system; incompetence and/or malice can be detected and prevented as and when they happen. Blockchain will reside more at the back end rather than facing the user. Furthermore the ability to prevent unauthorized modification (tampering) of information as well as code coupled with the participative nature of the system reinforces the fault tolerance capability of the patform.
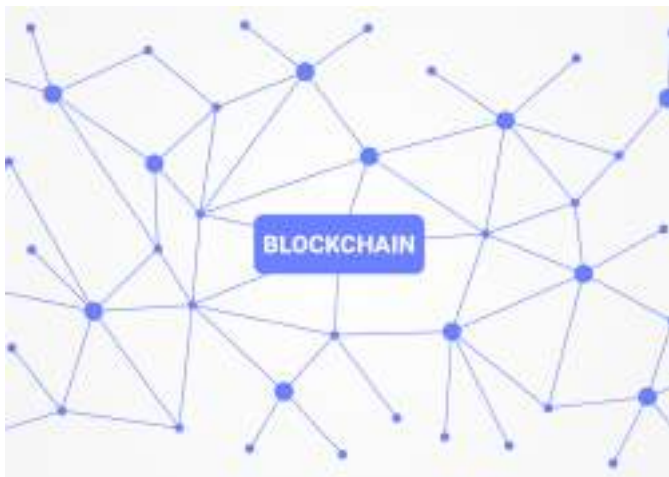
Trustless

Trust is a measure of risk; it is often a substitute for knowledge we do not have about remote entities who can potentially harm us. The fact we can independently verify the fate of each and every transaction eliminates the need to trust remote entities. Moreover compared to the opacity that existed in traditional systems a blockchain platform enables transparency. However information which needs to be protected can be done to protect competitive advantage and trade secrets without affecting the transparency of the process.

A typical supply chain may involve hundreds or thousands of business transactions every day. These transactions generally take place in a bilateral manner – for instance, between a supplier and a manufacturer or between a retailer and a logistics service provider – and are stored in each of the supply-chain actor's own ledgers. As a product travels from its origin to its destination in a supply chain, there may be many organizations involved. Each holds its own version of "truth" about the product's digital journey. The multiple ledgers (hence the multiple "truths") often lead to error, fraud, delays and inefficiency.

Blockchain can reduce those complex bilateral communications and informational linkages and leakages by providing a single, shared, tamper-evident ledger that records the transactions as they occur. Transactions in a blockchain are confirmed by all participants via a consensus mechanism. Once validated and recorded in a blockchain, a transaction becomes permanent. No single participant, even a system administrator, is able to delete or change a transaction unilaterally. Therefore, blockchain enables supply-chain actors to share control over access to –and evolution of – the data.