State of the Art Analysis

Overview of DLT

Distributed ledger technology (DLT) is a type of database that has the following notable features:

- Distributed participation
- Decentralization
- Distributed Consensus
- Public-Private key cryptography

In distributed databases, every network participant shares an exact replica of the network's transaction history. The information is updated to all nodes (computers of network participants) in near-real time. All parties see and share the same information.

Decentralization is important because the information stored on a blockchain is not controlled or harvested by any single party. Therefore, there is no single point of failure. If a node fails or is compromised, the network carries-on undisturbed by the remaining network participants.

The information in a blockchain is shared and can be simply verified by reconciling one version of the database to another hosted on a separate node. Simultaneously, every party controls the information, yet no one party controls said information.

Consensus in blockchain networks can take many forms including; Proof of Work, Proof of Stake, Proof of Authority, practical Byzantine Fault Tolerance, Single Authority, etc. Regardless of the type, each form of consensus ensures that transactional accuracy within the network is agreeable among network participants with varying degrees of assurance depending on methodology. This contrasts with traditional databases; whereby inputted information is assumed accurate until subsequently reviewed.

Public-private key cryptography allows participants to transact pseudonymously. Public keys are a user's address on a blockchain network. Public keys are long strings of randomly generated numbers and letters. Transactions are sent to and from public keys. Private keys act as the passwords to public keys, allowing users to access their digital assets. Public-private key cryptography provides security to parties transacting on blockchain networks.

Blockchain and IoT

The internet of things (IoT) is a technological phenomenon whereby devices, machines, objects or even people are connected to the internet via unique identifiers (UIDs). These connected devices can automatically communicate with each other over the internet, without the need for human, manual interaction. In the context of enterprise, IoT has significant implications when it comes to transparently tracking, and tracing voluminous or complex interactions between automated processes.

Blockchain is the underlay that records all transactional data in an immutable, auditable distributed ledger. Data is accessible by any stake-holding party whose connected device is part of the value chain. Without DLT, the data from all IoT interactions would be recorded and siloed by the party hosting each connected device. In the world of highly integrated supply chains, where stakeholders are numerous, sharing of complete data is paramount.

Currently lacking in the blockchain, IoT space is tamper-proof digital replication of physical assets. Inherent in providing digital identifiers to physical assets, there are significant threats to accuracy. QR codes or other such identifiers can be replicated and applied to multiple physical assets, they can be rendered unreadable from wear and tear, they can be lost, they can be replaced with fraudulent identifiers, etc.

However, technology exists that when integrated with blockchain and IoT, users can ensure accuracy in physical-digital pairings. It works as follows; in a designated area on any physical asset, users can take a picture on their smart phones, and by analyzing the microscopic features of the asset, a unique hash will be generated. Every good, regardless of wear/tear or homogeneity among similar products, has unique features that yield unique hashes. Once produced, these hashes are tamper-proof, and ensure complete accuracy in every physical-digital pairing documented on a blockchain.