Distributed Ledgers in IIoT

An Industrial Internet Consortium White Paper

2020-07-27

CONTENTS

We've all heard of volatile cryptocurrencies, such as Bitcoin and Ethereum, which rely on *distributed ledger technologies* (DLTs), such as blockchain, to function. But what about the impact of distributed ledgers in the Industrial Internet of Things (IIoT)? Industrial companies are using DLTs for everything from shipping-container tracking, vehicle identity and history, to energy trading and farm-to-store tracking—and succeeding because DLTs provide secure data sharing and trust.

Decision makers in IIoT companies need an overview of the use of DLTs today to understand their costs and benefits, and make good decisions on whether and how to incorporate DLT in their environments. This paper provides practical guidance on a variety of DLT use cases, architectures and the building blocks necessary for scalable industrial deployment, in the face of rapidly evolving technology. This paper investigates distributed ledger:

- characteristics,
- key drivers for implementation,
- current deployments,
- future opportunities,
- challenges,
- scale,
- security,
- trust,
- standards and
- practical guidance on how distributed ledgers may be deployed in IIoT systems.

We highlight several detailed use cases, explore security benefits and make deployment recommendations. A longer and more detailed distributed ledger architecture will be developed in a follow-up document.

WHAT IS A DISTRIBUTED LEDGER FOR IIOT?

A *distributed ledger* (also called a shared ledger) is a consensus of replicated, shared and synchronized data spread across multiple sites, countries or institutions. There is no central administrator and no centralized data storage. In the absence of a central authority, such as a bank, lawyer, realtor or government, trust must be provided through consensus mechanisms—collaborative methods of validating data before it is added to the system of record.

Distributed ledgers can comprise at least three layers. The bottom layer is the immutable ledger itself. The middle layer is the consensus algorithm that determines what can enter the lower ledger layer. The top layer of the architecture includes functionality such as smart contracts and smart grids.

DLTs are relevant to IIoT as they provide a safe, immutable distributed ledger to store sensor data and allow information to be verified without relying on a third-party authority. This reduces

mistakes and fraud, particularly along the IIoT supply chain. There are many IIoT use cases, several of which are outlined here.

Blockchain is one of the most popular and widely used types of DLT. A subset of the larger category of DLT, blockchain links transactions together into *blocks*, which are processed together and tracked using a cryptographic hash of the block's data.

A blockchain is a historical record of transactions, much like a database. A blockchain can contain financial and non-financial transactions, the details of which can be distributed across several systems in near-real-time over a peer-to-peer network. Blockchains come in both public/permissionless and private/permissioned variants. Permissionless networks rely on pseudo-anonymous identities and have a strong dependence on underlying game theory mechanics for the consensus mechanism, the process by which all participants agree on transaction history.

In private/permissioned networks, there is a strong dependence on identity of the participants on the network and the sophistication on role-based access controls for network participation and data access. Every participant helps determine the intrinsic *immutability* of all existing records using cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights. Blockchain has mechanisms to make it difficult to change historical records, but easy to detect when someone is trying to change them.

Directed acyclic graphs (DAGs) are a type of DLT that deliver properties similar to blockchain through different mechanisms. These technologies promise to deliver similar outcomes to blockchain, while using less computational effort. This class of technology differs from blockchain in that instead of requiring nodes in the network to validate all transactions from all nodes in the network, directed acyclic graphs nodes send transaction events only to nodes that are participating in a transaction. Nodes need not validate all transactions in a network at a given time, and blocks are no longer assembled or needed. Examples of DLT, without the use of blockchain, include Corda (*corda.net*), Hashgraph (*hedera.com*), OByte (*obyte.org*) and IoTA (*iota.org*).

A *smart contract* is a computer program that directly controls the transfer of digital currencies, assets or other information between parties under certain conditions. The contract is stored on the distributed ledger and whenever a transaction occurs that triggers a specific smart contract, it performs any necessary processing. Smart contracts are stored on the ledger because it is important for the contract to be readily available to the participants executing transactions.

PERMISSIONED VS PERMISSIONLESS DLTS

Most applications of industrial DLTs require a permissioned deployment as opposed to a public, permissionless option. Permissioned, or private, DLTs allow organizations to benefit from DLT without the reductions in throughput, scalability and security assurance negatives. This allows

the DLT system to scale with existing internal organizational processes and to limit power demands that are prevalent in a global, permissionless consensus model. Most DLTs are not strictly permissioned or permissionless. A DLT can be permissioned regarding access to its network, but permissionless in that any accepted network participant can propose a transaction. And the same DLT can again be permissioned in allowing users to develop applications on the DLT. As such, permissions can be set to varying degrees among the different levels of the DLT architecture.

USE CASES

Although IIoT distributed ledgers are in their infancy, there are trials and deployments today in certain industrial verticals. Depending upon the long-term success of the following real use cases, we could see a quicker uptake of blockchain.

MEDILEDGER NETWORK

Use Case: Pharmaceutical Supply Chain	
Industry Sector: Pharmaceuticals	**Industry Vertical:** Shipping
Use Case Description: This blockchain-based system allows pharma competitors to collaborate on a shared platform to raise drug safety, for instance, without sharing sensitive information. *MediLedger Network* is a consortium focused on pharma supply chains, which includes Gilead, Pfizer, Amgen, Genentech, AmerisourceBergen, and McKesson. *Chronicled* provides the underlying technology. The first solution in production from MediLedger is a product verification system that makes it easier to verify that a returned drug is authentic. When drugs reach their final destination, it's as if they arrive with a black box of data to assure not only authenticity but they have complied with business rules during their entire journey.	
Business Value: Supply Chain integrity	
Application: Supply Chain: Pharma Traceability	**DLT Type:** Blockchain
What challenge does this use case address? Tracking pharmaceuticals along the supply chain.	

ALIBABA FOOD TRACEABILITY

Use Case: Alibaba Food Traceability	
Industry Sector: Transportation	**Industry Vertical:** Shipping
Use Case Description: *Alibaba* is applying blockchain technology to enhance the traceability of food with a view of curbing counterfeits. In 2017, Alibaba partnered with postal services entity Australia Post and natural health firm Blackmores in using DLT to ensure that only genuine food products were shipped to China from Australia.	
Business Value: Supply Chain integrity	
Application: Supply Chain: Food Traceability	**DLT Type:** Blockchain
What challenge does this use case address? Tracking food along the supply chain.	

AMAZON MANAGED BLOCKCHAIN AND QUANTUM LEDGER DATABASE

Use Case: Amazon Managed Blockchain	
Industry Sector: Infrastructure	**Industry Vertical:** Cloud & Computing
Use Case Description: Amazon Web Service's (*AWS*) Blockchain service makes it cost-effective to create, manage and scale blockchain networks for multiple parties to transact in a decentralized manner. It supports Ethereum and Hyperledger Fabric. AWS's Quantum Ledger Database (QLDB) is a new class of database that provides a transparent, immutable and cryptographically verifiable ledger that customers can use to build applications that act as a system of record where multiple parties are transacting within a centralized and trusted entity. QLDB removes the need to build complex audit functionality into a relational database or rely on the ledger capabilities of a blockchain framework. Amazon Managed Blockchain makes it easy to replicate transactions to Amazon QLDB. This gives customers the ability to gain advanced insights on how to optimize the blockchain network by querying the change history of their network.	
Business Value: Managed Blockchain Service	
Application: All Industries	**DLT Type:** Blockchain, Ethereum and Hyperledger
What challenge does this use case address? Rather than developing and managing your own blockchain service, you use the cloud.	

WALMART FARM-TO-STORE

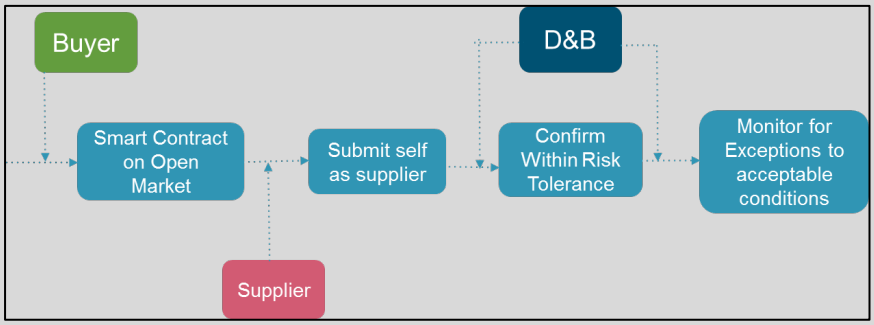
Use Case: Walmart/Sam's Club Farm to Store	
Industry Sector: Transportation	**Industry Vertical:** Shipping
Use Case Description: In the United States, Walmart and its *Sam's Club* division are using a farm-to-store DLT tracking system for some produce and expect to require their suppliers of leafy green vegetables to use blockchain tracking technology. The technology has reduced the amount of time it takes to trace the source of food from 7 days to 2.2 seconds. Unlike a public blockchain, Walmart's ledger system is designed for its supply chain partners only and is not yet a fully public database. Each entity that handles food along the chain of custody is represented by a section of the blockchain node. This makes for a much more efficient discovery process if there is contaminated produce in the supply.	
Business Value: Supply Chain integrity	
Application: Supply Chain: Food Traceability	**DLT Type:** Blockchain
What challenge does this use case address? Tracking food along the supply chain.	

DUN & BRADSTREET BUSINESS IDENTITY

Use Case: Dun & Bradstreet Business Identity

Industry Sector: Finance & Banking	**Industry Vertical:** Investment

Use Case Description: *Dun & Bradstreet* provides a continuously updated view of each participant to a transaction. They provide an Oracle, which is a trusted source of data that is not part of the blockchain, which lives as a node with signature authority on your network. They monitor events and handle API calls so data is requested at the smart contract level. This provides a trusted source of multi-sourced identity validation information. Immediate counterparty profiling prevents pushing high-risk transactions into flight and provides better insight into potential risk, fraud and compliance issues.



Business Value: Transaction integrity

Application: Identity validation for transactions	**DLT Type:** Blockchain

What challenge does this use case address? Validating all parties to a transaction.

EVERLEDGER DIAMONDS

Use Case: Everledger Diamonds	
Industry Sector: Mining & Metals	**Industry Vertical:** Diamonds
Use Case Description: Counterfeiters flood the market with convincing fake diamonds. It can be a challenge to ensure you're buying an authentic diamond. A London-based company, *Everledger*, has placed more than 1.6 million diamonds on a blockchain. Entries on the digital record include dozens of attributes for each diamond, including the color, carat and certificate number, which can be inscribed by laser on the crown or girdle of the stone. They create a *digital twin* of the object on the blockchain. The technology has enabled diamond suppliers and intermediaries (e.g., border agents) to replace a paper certification process with a blockchain ledger. The process involves using computer scanning tools to access a digital vault and to determine the provenance of any diamond.	
Business Value: Supply Chain integrity	
Application: Track and Trace	**DLT Type:** Blockchain
What challenge does this use case address? Tracking diamonds along the supply chain.	

WIEN ENERGIE

Use Case: Wien Energie	
Industry Sector: Energy & Utilities	**Industry Vertical:** Electric
Use Case Description: Austrian utility, *Wien Energie*, experimented with blockchain applications in commodity trading and plans to market end-customer products (green electricity provision, electric car charging and land registry services) in a new central Viennese urban development. The energy industry must handle increasingly complex transactions between big and small producers and consumers, and corporate entities, as more decentralized renewable energy volumes arrive. Energy companies are working to consolidate back-office processes, cut down risk, protect against cyber threats and thus save costs in the long run and looking to distributed ledgers to help.	
Business Value: Secure Energy Trading Platform	
Application: Product Traceability	**DLT Type:** Blockchain
What challenge does this use case address? Increased difficulties with energy trading.	

SKYCELL SMART CONTAINERS

Use Case: SkyCell Smart Containers	
Industry Sector: Transportation & Logistics	**Industry Vertical:** Freight Management
Use Case Description: *SkyCell* containers are equipped with IoT sensors that connect to a data cloud. They can remotely monitor and intervene on every container to ensure quality standards. Their monitoring software is based on blockchain technology. Containers are cleared for use when their software indicates it is in perfect condition. Real-time monitoring service allows them to intervene immediately when deviations occur in the supply chain. For instance, biopharmaceuticals are exceptionally sensitive to changes in pH, temperature and environmental contaminants. Even slight changes can alter the chemistry of the protein under production, rendering it ineffective or even dangerous. Because biopharmaceutical production costs are much higher than for traditional drugs, supply chain waste and loss is costlier, and companies have a strong incentive to minimize it. SkyCell's air freight containers are equipped with a plethora of sensors that monitor temperature, humidity and geolocation. The SkyCell cloud platform records documentation like bills of lading and customs forms for each container on a blockchain-like ledger, providing a level of supply chain visibility and security that complements the container's temperature security.	
Business Value: Supply chain integrity	
Application: Product Traceability	**DLT Type:** Blockchain
What challenge does this use case address? Lack of visibility and security of products in shipping containers.	

MAERSK'S & IBM'S GLOBAL TRADE PLATFORM

Use Case: Maersk's and IBM's Global Trade Platform	
Industry Sector: Transportation	**Industry Vertical:** Shipping
Use Case Description: *Maersk*'s and *IBM*'s goal is to reduce the cost of global shipping, improve visibility across supply chains and eliminate inefficiencies stemming from paper-based processes. They built the TradeLens solution from scratch on blockchain technology and made it open to all supply chain participants. It brings together all parties in the supply chain—including shippers/BCOs, freight forwarders, inland transportation, ports and terminals, ocean carriers, customs and other government authorities as well as others—on to a blockchain-based platform with a secure permission and identity framework. It provides for secure sharing of instantaneous, actionable supply chain information and visibility across all parties to a trade—encompassing shipping milestones, cargo details, trade documents, the structured data embedded in trade documents, customs filings and IoT data from sensor readings.	
Business Value: Secure Supply Chain	
Application: Supply Chain	**DLT Type:** Blockchain
What challenge does this use case address? Shipment tracking inefficiencies. Reduce and improve current inefficiencies.	

END-TO-END DELOITTE SUPPLY CHAIN WITH INTEGRATED IOT AND ERP

Use Case: Optimizing Supply-Chain Traceability and Transparency with AWS IoT and Amazon Blockchain service	
Industry Sector: Supply Chain	**Industry Vertical**: Automotive
Use Case Description: Lack of transaction and inventory visibility continues to be a significant challenge. Companies today are asked to ensure that their supply chain operations can withstand disruptions caused by geopolitical events, climate-related disasters, public health crises and more. Investments made to avoid supply chain disruptions from customer demand, materials supply and logistics services fail when they rely on outdated or rigid systems and strategies that cannot provide a complete view across the end-to-end dependencies both inside and outside of the enterprise. IoT-Enabled Blockchain solutions powered by AWS provide the traceability needed to track product quality, store SAP supply-chain events data with a tamper-proof solution, sustain product lifecycle information as a single source of truth inside a distributed ledger and create an efficient communication mechanism to share information between supply chain participants. Enhancement via secure voice-enabled applications further increase convenience and flexibility. The solutions provide end-to-end visibility of product quality, ownership and stated change information, thereby enforcing transparency and trust throughout the supply chain.	
Business Value: Secure Supply Chain	
Application: Product Traceability	**DLT Type:** Blockchain
What challenge does this use case address? Real-time IoT telemetry and ERP reporting.	

BOSCH & TÜV ODOMETER

Use Case: Bosch & TÜV Automobile Odometer Integrity	
Industry Sector: Transportation	**Industry Vertical:** Automotive
Use Case Description: Prevent odometer fraud by using a certificate, connected to a blockchain, which ensures a car's mileage data is correct. *Bosch* and *TÜV* installed a connectivity device in the car to read its mileage data. Using the device, they then transmitted the data to a backend which is connected to a blockchain. They also developed an app for consumers that enables them to view the mileage history of their car. Users can access an online service to get a digital certificate indicating whether the mileage has been manipulated or not. By using this live service, consumers can easily create a digital certificate for their cars and even share the information with other entities in order to create trust in the specific car data. The companies are collaborating with an original equipment manufacturer and have a fleet of about 100 cars in Germany and Switzerland that is connected to the blockchain.	
Business Value: Secure Supply Chain	
Application: Product Traceability	**DLT Type:** Blockchain
What challenge does this use case address? Automobile odometer fraud.	

BLOCKCHAIN SCALABILITY & SECURITY

While blockchain technology has great potential for disrupting and improving enormous industries, it must be able to scale to meet the requirements of a variety of industrial applications. Due to the decentralized nature of blockchain operations, scaling a blockchain-based application poses significant challenges in practice.

The *scalability trilemma* posits that blockchains can generally have only two of the following three properties: decentralization, security and scalability.

1. Decentralization can be quantified by the number of block producers,
2. Security, which is the most important aspect for a blockchain network with mutually untrusted participants, refers to the cost for adversaries launching an attack that alters transaction ordering,
3. Scalability depends on the number of transactions per unit time that a blockchain network can process.

Balancing decentralization, security and scalability is a complex issue and multiple technologies have been developed to address the scalability challenges specifically, as detailed below.

Hardware-layer solutions: For those blockchain platforms in which a small group of nodes is responsible for producing blocks (i.e., permissioned blockchains), the transaction throughput of

the system can be significantly improved using high-end machines for accelerating blockchain operations, such as transaction validations and signature verifications.

Data-layer solutions: The transaction throughput can be boosted by increasing the block size and reducing the interval at which blocks are created. One can also compress the information in the block using signature aggregation techniques and alternative data structures (e.g., *Sparse Merkle Trees (nakamoto.com/merkle-trees/)*). Conventional database scaling technology, such as sharding, is also applicable to blockchain by dividing the blockchain state into small shards that run parallel to one another. Each shard is responsible for processing transactions within the group, thereby increasing the overall throughput.

Network-layer solutions: Most blockchain protocols rely on a trustless peer-to-peer network model, in which information must be propagated to and validated at every hop in the network. Although there are physical limitations to network latency and transmission capacity, optimizing network bandwidth usage and increasing connectivity among blockchain nodes can improve the transaction throughput to some extent.

Consensus-layer solutions: The performance of consensus algorithms has a significant effect on the throughput of blockchain platforms. Multiple high-performance consensus mechanisms have been developed to allow for greater scalability. Examples include *delegated proof-of-stake* and *practical Byzantine fault tolerance (http://nakamotoinstitute.org/static/docs/on-stake-and-consensus.pdf)*. Other forms of distributed ledgers, such as those built upon DAGs, may scale with high throughput capabilities.

OFF-CHAIN SOLUTIONS

Various efforts have been made to move scalability solutions to a second layer where transactions are off-loaded from the main blockchain to reduce network traffic. The off-chain solutions are usually in the form of state channels, side chains and *trusted execution environments* (TEEs).

State channels: State channels enable two parties to establish a private communication channel so that transaction processing and state updates can be outsourced to them. With state channels, users reduce their on-chain operations by transacting with one another directly off-chain of the blockchain. A smart contract, for instance, is deployed to lock parts of the blockchain state, followed by the continuous off-chain transactions and state updates between two parties. Finally, both parties submit the state back to the blockchain.

Side chains: Side chains are separate blockchains that are compatible with the main blockchain and linked to it via a two-way peg mechanism. The two-way peg facilitates interchangeability of assets between the main blockchain and side chains. In this layered architecture, the main blockchain is responsible for resolving disputes and ensuring overall system security, while side chains operate more efficiently.

TEEs: A hardware-based TEE (e.g., Intel SGX (*https://software.intel.com/en-us/sgx*)) solution is able to guarantee an off-chain trusted execution via a hardware-based digital signature. An off-chain execution signature (an *execution attestation*) signed by a private key protected by a secured TEE can be then verified by blockchain based on-chain network to prove the correctness of the off-chain execution.

Scalability: Scalability is the capacity of the blockchain network to improve performance (e.g., throughput and latency) as the number of users and the complexity of Decentralized Applications (*DApps*) increase, without making a difference to the user experience and security. The network architecture must be able to adapt to new demands as adoption increases, not the other way around. With decentralized cloud computing backed by TEE, the blockchain on-chain network can offload intensive workloads to off-chain without compromising user experience and security.

Privacy preserving: The core of blockchain is decentralization and sensitive data can be used with applications on decentralized nodes and can be easily inspected and tampered with by super-privileged administrators of any decentralized node. A hardware-based TEE solution is so far the only scalable solution to preserve the privacy of the data in decentralized networks. With TEE, data is strictly encrypted before sending to decentralized networks and then the decryption only happens inside a hardware secured enclave. The decrypted secrets can never be disclosed to anyone including the owner of the node that hosts the data storage and applications execution. TEE can be widely used in different blockchain-based use cases, such as multi-party computing and dataset monetizing without losing data privacy and ownership.

OPEN SOURCE & STANDARDS

There are several open-source and standards-based communities for developing architectures around distributed ledgers. It will be important to follow, and contribute to, these initiatives which are relevant to Industrial distributed ledger (*IDL*) interoperability.

OMG Finance Domain Task Force DLWG: The OMG DLT Working Group (*omg.org*) was superseded by the creation of a Blockchain PSIG in December 2018. The new Blockchain PSIG takes on the activities of the earlier FDTF DLT WG including the ongoing proof of concept activity for semantics and FIBO usage.

IEEE P2418: IEEE recognizes the vital role standards will play in the development and adoption of blockchain technologies. IEEE Standards Association, a globally recognized standards-setting body within IEEE, has been actively pursuing blockchain standardization efforts through activities in multiple industry sectors, including the launch of the world's first Advancing HealthTech for Humanity™ virtual workshop (*https://blockchain.ieee.org/standards/virtual-blockchain-2016/about*).

ISO TC 307: The International Organization for Standardization (*iso.org*) is an independent, non-governmental international organization with a membership of 164 national standards bodies. In

ISO Technical Committee (TC) 307 they have created: blockchain and DLTs–use cases, terminology, privacy and personally identifiable information protection considerations, security risks, threats and vulnerabilities, overview of identity management using blockchain and DLTs, reference architecture, taxonomy and ontology, legally binding smart contracts, security management of digital asset custodians and guidelines for governance.

ITU FG DLT: International Telecommunication Union (*itu.int*) is a specialized agency of the United Nations that is responsible for issues that concern information and communication technologies. The Focus Group on Application of Distributed Ledger Technology was formed to identify and analyze DLT-based applications and services; to draw up best practices and guidance which support the implementation of those applications and services on a global scale; and to propose a way forward for related standardization work in ITU-T Study Groups.

Hyperledger is a multi-project open source collaborative effort hosted by The Linux Foundation (*hyperledger.org*), which was created to advance cross-industry blockchain technologies.

Interledger (*interledger.org*) is an open protocol suite for sending payments across different ledgers. Like the internet, connectors route packets of money across independent networks. The open architecture and minimal protocol enable interoperability for any value transfer system. Interledger is not tied to a single company, blockchain or currency.

ETSI Permissioned Distributed Ledger: ETSI's *Industry Specification Group Permissioned Distributed Ledger* (*https://www.etsi.org/committee/1467-pdl*) analyzes and provides the foundations for the operation of permissioned distributed ledgers, with the ultimate purpose of creating an open ecosystem of industrial solutions to be deployed by different sectors, fostering the application of these technologies, and therefore contributing to consolidate the trust and dependability on information technologies supported by global, open telecommunications networks.

NIST Blockchain: Engineers at the National Institute of Standards and Technology (*nist.gov*) needed a way to secure smart manufacturing systems using the digital thread, so they turned to blockchain. According to a NIST report, blockchain provides tamper-proof transmission of manufacturing data and traceability of that data to all participants in the production process.

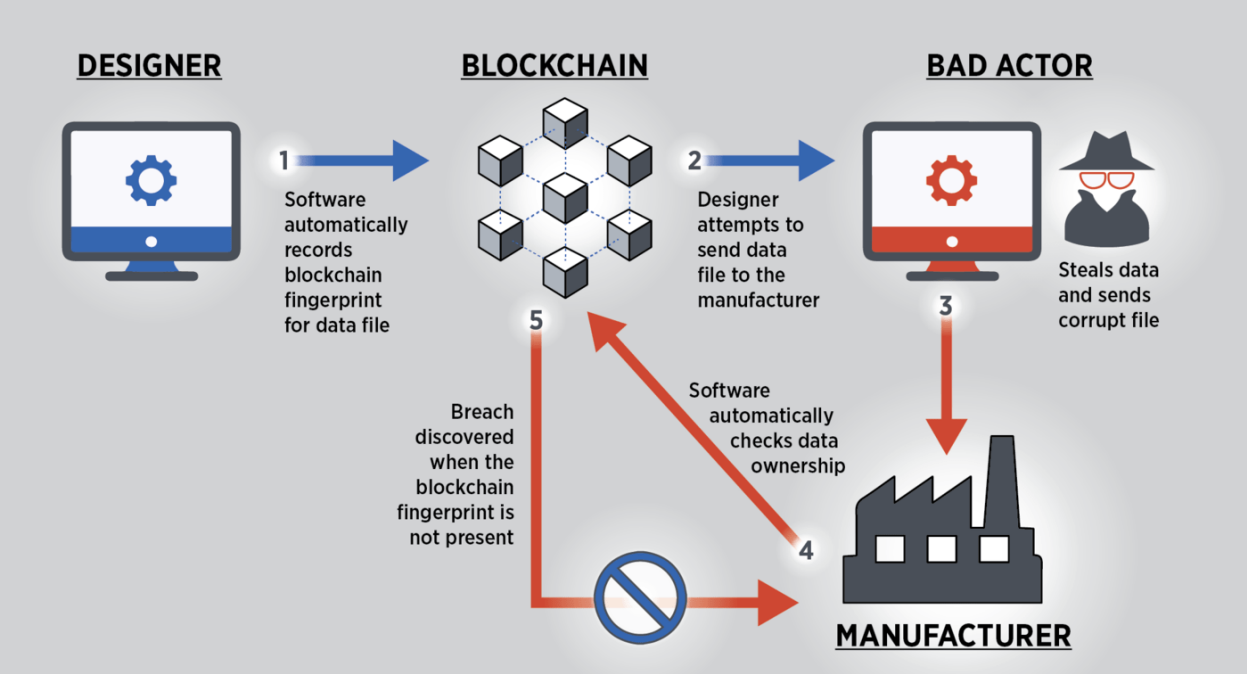


Figure: Blockchain Identity Verification

Credit: N. Hanacek/NIST

Enterprise Ethereum Alliance (*https://entethalliance.org/*) is a member-led industry organization whose objective is to drive the use of Ethereum blockchain technology as an open-standard to empower all enterprises.

CORDA: Built specifically for businesses, Corda (*corda.net*) is an open source distributed ledger platform that allows developers to freely build applications, or CorDapps, on top of Corda. Corda benefits from a large community of developers and ecosystem participants.

CHALLENGES

There are challenges to be aware of when considering the deployment of an IIoT distributed ledger solution.

Interoperability: Although standards and open source bodies are working on interoperability, there is little interoperability between DLT/blockchains ledgers today. If one plant or factory uses one type of distributed ledger and another factory uses another, there is currently no interoperability solution between the two.

Distributed *key management:* Key management, at scale, including provisioning and rekeying, is hard to implement successfully. Blockchain makes implementation of a key management program more difficult.

Data privacy: Data is immutable and encrypted on a ledger forever. Even though encryption is being used and not realistically comprisable today, it could be exposed in the future, perhaps using quantum computing. Hackers are always chasing new algorithms.

Scalability: As the number of transactions grow, so too does the ledger's size, resulting in more data being processed and stored on each node. Deploying additional nodes may make the problem worse because more time is needed for verification. Because each node must process every transaction, it's inevitable that users will be confronted with performance and reliability issues as latency increases, throughput decreases and storage costs rise.

Garbage in, garbage out: As with any other technology, there is no guarantee that the data being input into a distributed ledger is valid to begin with. This is where the previously described off-chain trust systems exist. Trusted third-party solutions, such as Dun and Bradstreet's Oracle solution, are available to help ensure the integrity of the data input into a DLT.

CONCLUSION

Distributed ledgers are a nascent technology, there are very few wide-scale, production-grade distributed ledgers in use today; however, they are already being used in some IoT environments. To remain competitive, to prevent fraud and to add simplicity to existing ledgers, distributed ledgers have a current and future place in IIoT. There are weaknesses with DLT, as there are with all technologies; as such, due diligence in testing must be maintained. Permissioned IDLs appear to currently be the most successfully deployed solution today, particularly with the supply chain use case.

AUTHORS AND LEGAL NOTICE

This document is a work product of the Industrial Internet Consortium's Industrial Distributed Ledger Task Group, chaired by Mike McBride (Futurewei), Anoop Nannra (Trusted IoT Alliance) and Xinxin Fan (IoTeX).

Authors: Mike McBride (Futurewei), Pieter van Schalkwyk (XMPro), Bassam Zarkout (IGnPower), Lei Zhang (iExec), Xinxin Fan (IoTeX), Alex Ferraro (PwC) and Anoop Nannra (Trusted IoT Alliance).

Technical Editor: Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors, Editors and Contributors into an integrated document.

& Notices, as posted at *http://www.iiconsortium.org/legal/index.htm#use_info*. If you do not accept these Terms, you are not permitted to use the document.