Blockchains in Industrial Automation Applications

Jay Bayne, PhD
jbayne@stratum4.org

Abstract

Blockchain technology has a significant potential role to play in the automation of industrial processes. In addition to its role in implementing cryptocurrencies (e.g., Bitcoin) and smart digital contracts, blockchains support the operation of *decentralized industrial organizations* (DIO)[1], establishing economic value derived from advanced industrial automation (IA) applications—often in the context of emerging Cyber-Physical (CPS)[2] and Industrial Internet of Things (IIoT)[3] systems.

Blockchains are immutable distributed ledgers[4]. Used in industrial automation systems, they can store sequences of cryptographically secure measurements of the evolving states and behaviors of physical and synthetic[5] processes. Viewed as a multi-agent agreement protocol, blockchains solve a challenging problem in guaranteeing, without need of a central authority, by providing consensus among collaborating DIO on the performance of processes resulting from sequences of control transactions.

IA systems are *cybernetic* [6] to the degree they implement, with predictable performance, the regulatory and supervisory feedback control of *value production* processes. To achieve this end, cybernetic IA systems are *intelligent*, maintaining situational awareness and exhibiting reflexive, cognitive, and adaptive behavior. As such, they are increasingly dependent on advanced computational science and *artificial intelligence* (AI) techniques, able to recognize and respond to processes that evolve over time at various rates in discrete or continuous steps. In addition, IA/AI strategies are typically constrained by critical timeliness properties (e.g., task completion times) and regulatory requirements (e.g., safety and security). Further, they are subject to enterprise operational protocols (e.g., information security, supply chains, and resource planning).

Developing effective automated monitoring and control services in DIO systems presents significant policy and engineering challenges—especially in process industries with regulated supply chains (e.g., pharmaceuticals, healthcare, energy, transportation and communications.) In this context, intelligent automation requires agile and transparent (i.e., auditable) governance services that adheres to control strategies that are efficient and accurate in maintaining *situational awareness*, performing adaptive *planning,* and providing predictable performance when plans are in *execution*.

In computational terms, intelligent automation services are provided by (instantiated in) *cyberspatial objects* (CSO) delivering services located by their respective *cyberspatial coordinates*[7]. CSO are responsible for

[1] A concept derived from Decentralized Autonomous Organizations (DAO), https://en.wikipedia.org/wiki/Decentralized_autonomous_organization
[2] *A* transdisciplinary approach to regulating behaviors in dynamic socio-technical systems.
[3] https://en.wikipedia.org/wiki/Internet_of_things
[4] See Harvard Business Review, https://hbr.org/2017/01/the-truth-about-blockchain
[5] Objects are *synthetic* if man-made, versus made naturally or organically.
[6] http://cyberphysicalsystems.org/
[7] *Cyberspace* is an abstract four-dimensional space with infospatial, geospatial, sociospatial and temporal coordinates.

monitoring and controlling the behavior of one or more value production processes whose states are at least partially observable and controllable.

In our view, Figure 1 diagrams a CSO's internal stream processing pipeline showing its input and output data streams and its three computational stages. Each stage operates continuously and in parallel. Real-time situational awareness of regulated a value production process is maintained by a *Situation Assessment Service* (SAS) that performs data acquisition, filtering, identification (e.g., pattern recognition and event detection), analysis, archiving and learning. *Plan Generation Service* (PGS) is responsible for planning of responses to unfolding situations, including checks for policy compliance (e.g., adherence to "rules of engagement") and protocols for coordinated sharing of reusable assets. And the *Plan Execution Service* (PES) provides authorization, execution, and performance assessment of all controlled processes as they move from their trajectories from their present to next states.

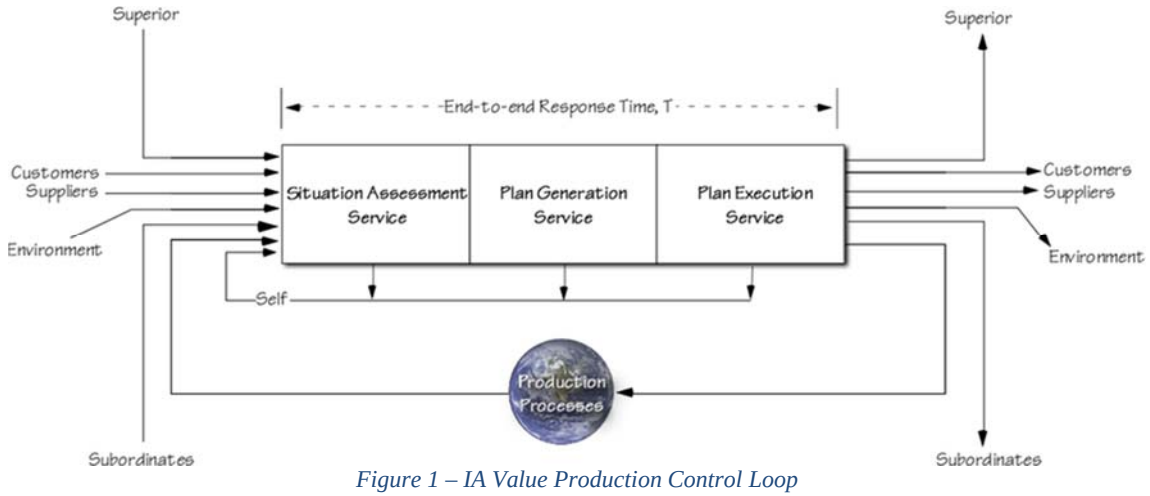

Figure 1 – IA Value Production Control Loop

Data streams inbound to a SAS stage carry commands and status from the CSO's superiors, subordinates, supply chain customers (consumers) and suppliers (producers), its own operating environment, including the status of its internal SAS, PGS and PES applications. Output data streams carry demands of and results for a CSO's superiors, subordinates, consumers, producers, and where meaningful, adjustments to its operating environment. CSO bandwidth (i.e., input-output throughput) must be maintained at a level sufficient to maintain effective process control[8].

Natural and synthetic processes that are candidates for intelligent automation exist at all organizational levels of an industrial enterprise (Table 1). Each level defines an *accountability domain*, with each domain typically supervised by one or more human or automated management agents.

Table 1 – Typical IA Accountability Levels

Level	Enterprise Levels of Accountability
4	Enterprise systems: strategy, policy, capital assets
3	Business unit: P&L & personnel systems
2	Factory systems: production lines & supply chains
1	Cell systems: manufacturing processes
0	IoT devices: processes, sensors & actuators

[8] Generally, at least twice the fundamental frequency (aka, Nyquist Rate) of the process under control.

Industrial enterprises are governed by both human and synthetic agents, at both supervisory and regulatory levels. The behavior of these agents may be formal (prescribed, algorithmic) or ad hoc (heuristic, intuitive). If formal, historical precedents provided by organizational designs[9] prescribe, through operating policies, the social roles for dealing with complexity (e.g., faults) in areas such as production, trade, accounting, human resource and law (policy) enforcement.

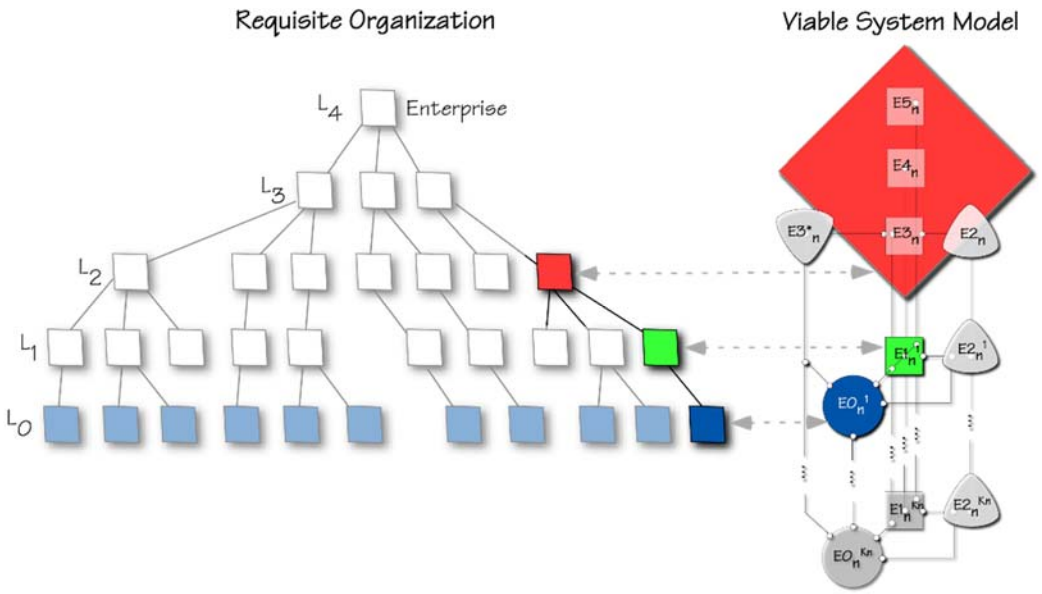

Figure 2 – Nested Enterprise Governance System

Figure 2 introduces a *Viable System Model*[10] (VSM) that exemplifies a governance structure compatible with automation strategies employing blockchain technology. The VSM architecture (its structure, function and performance) provides a computational framework focused on establishing and maintaining dynamic equilibrium (homeostasis) by balancing the global demands for optimal group-level performance against the typically conflicting demands for optimal performance of individual subordinate processes.

Depending on the complexity of an enterprise and its processes, a given governance function may be the responsibility of a single agent or a team of agents. For a single unit of organization (e.g., a jet fighter), all functions may fall to a single agent (the pilot) aided by automated subsystems. For a complex DIO (e.g., a regional emergency management system), each function may comprise groups of collaborating human and automated agents from multiple organizations (e.g., fire, police, healthcare).

Table 2 - Management Agents

Label	Agent Functions
E5	Executive: highest level of authority, accountability
E4	Navigator: situation assessment, adaptation and forward planning => (SAS, PGS)
E3	Operator: coordinated plan execution => (PES)
E3*	Auditor: independent performance measurement and assessment
E2	Coordinator: asset management, scheduling and synchronization

[9] See https://en.wikipedia.org/wiki/Requisite_organization
[10] See https://en.wikipedia.org/wiki/Management_cybernetics

E1	Director: individual process supervision and performance assessment
E0	Controller: direct process regulatory control

The DIO VSM model recognizes seven distinct governance roles, each responsible for a given administrative domain. As noted by indices in Figure 2, an enterprise may comprise potentially many (1..n) supervisory organizational units, with each in turn comprising potentially many (1..K_n) subordinate regulatory value production domains.

Figure 2 shows communication paths interconnecting governance functions listed in Table 2. The central vertical axis ("spine") represents the VSM's operational chain of command. It directly connects the E3 Operator (e.g., chief operating officer) with its subordinate E1 Process Directors (e.g., factory managers). The command axis provides the path for issuing coordinated PGS "tasking orders" governing overall value production, subsequently returning operational status reports. The set of PGS tasking orders is produced jointly by the E5-E4-E3 triumvirate, as authorized by E5, planned by E4, and executed by E3 and its subordinates.

The E3-E2 loop provides the E3 Operator with the ability to observe the concurrent behaviors of multiple E1 processes, synchronizing timing and access to shared resources and handling exceptions (e.g., "faults") in encapsulated E0 processes. This E2 loop also allows individual E1 Directors to observe and self-regulate their operations in concert with their E1 peers. Each E0 agent is an endpoint in a horizontal supply chain, while each corresponding E1 agent is an endpoint along a vertical command chain. In addition to the independent reporting E3 receives from its E1 Directors, the E3-E3* Audit loop provides the Operator with an assessment of E0 performance.

A key feature of this cybernetic model is its recursive (nested, fractal, scalable, reusable) nature. As indicated in Figures 2 and 3, each E1 at level "n" is the E5-E4-E3 triumvirate at the next lower level (n-1).

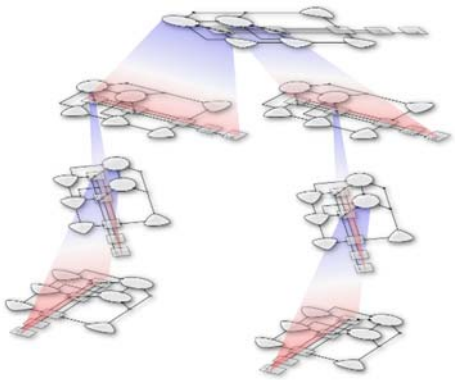

Figure 3 - Fractal Nature of Governance

In this DIO model a blockchain provides a continuously growing immutable list of records ("blocks") documenting inter- and intra-CSO request-response transactions that are linked and secured using cryptographic signatures (Figure 4). In general, each block contains a *hash pointer* to a preceding block, a transaction timestamp, a cryptographic initialization vector (aka "nonce") and either the transaction data or its associated metadata. By this design, blockchains are resilient, inherently resistant to modification of either the transaction timestamp or data.

In industrial settings, blockchains are typically implemented in closed (i.e., *permissioned*) networks among collaborating CSO nodes that adhere to a *consensus protocol*[11] for validating new blocks. Once a block is recorded on the chain, data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, requiring collusion among the networked majority.

Industrial organizations (e.g., their factories) are required to coordinate sets of production *areas*, each comprising production *cells*. Figure 4 idealizes a production area network, highlighting a factory's n^{th} area supervisory

[11] Ex, Proof of Work (PoW), Proof of Stake (PoS), etc.

control system and its K_n cell control loops. The cell designated $E1^1$-$E0^1$ is responsible for regulatory control of process P^1. In Figure 4, three primary activities are apparent: E3 governance of subordinate E1 directors, E1's supervisory control of its subordinate E0 cells, and E2 synchronization of concurrent E1-E0 behaviors.

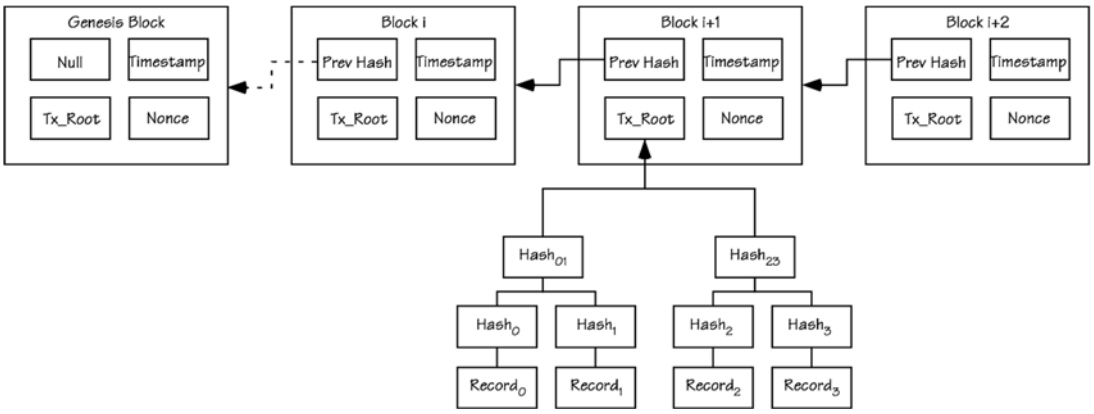

Figure 2 - Blockchain Structure

Timing of cell control loops, and therefore their stability, typically depend on the rates of the processes under their control and the rate at which supervisory controls (e.g., production task schedules) are issued by E3. Whether control interventions are synchronous or asynchronous, their issuance and subsequent completion define evolutionary *epochs*.

At any given time, the state of an E1 production cell is defined by a record of its inputs, outputs, process state, and side-effects (e.g., faults). During each epoch, E1 performance is recorded in blocks attached to (published by) the encapsulating E3 area blockchain and allied E1 blockchains (e.g., via *smart contracts*) associated with supply chains in which E1-E3 participates.

In summary, use of blockchains in industrial automation applications promises to significantly enhance automation infrastructure by providing security, fault tolerance and distributed agreement through immutable records of the evolving states and behaviors of distributed value production processes. Blockchain records guarantee coherence in supervisory and regulatory control regimes by maintaining causal relationships and ensuring traceability of economic benefits without need for a central authority.

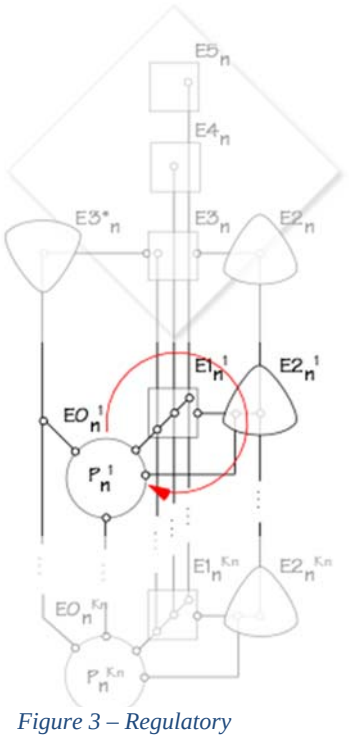

Figure 3 – Regulatory Loop

The computational science and engineering disciplines behind CPS, IoT and blockchain-based automation systems, including their use of advanced AI techniques, are witnessing accelerated global acceptance and development. In support of economic development through digital innovation, they are the focus of public and private funded research programs, are discussed in published conference and journal papers, and are receiving significant commercial attention in products and services offered by industrial enterprises. Questions and comments are encouraged and may be addressed to the author via email.