© SEP 2022 | IRE Journals | Volume 6 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV6I3-1714041

Blockchain-Assisted Secure Data Exchange Architectures for SCADA-Controlled Power Systems

MUJEEB A SHITTU[1], IBUKUN OLAOLUWA ADENIJI[2], HABEEB SHITTU[3], RUTH ADESOLA ELUMILADE[4], KAFAYAT OLOLADE LIADI[5], IFEANYI SIMON OPARA[6]

[1]Ikeja Electric, Lagos, Nigeria
[2]Electric Power Research Institute
[3]Moffatt Nichol, Savannah, GA, US
[4]University of Dundee, Dundee, United Kingdom
[5]Independent Researcher, Lagos, Nigeria
[6]IHS Towers, Enugu, Nigeria

Abstract- This study presents a comprehensive and critical examination of blockchain-assisted secure data exchange within SCADA-controlled power systems, motivated by the growing cybersecurity risks and trust deficits associated with increasingly digitalised and decentralised electricity infrastructures. The primary purpose of the study is to evaluate the extent to which blockchain technologies can enhance the security, integrity, and resilience of SCADA data exchange while remaining compatible with the stringent performance and safety requirements of power system operations. A structured review methodology was adopted to synthesise peer-reviewed literature from power system engineering, cybersecurity, distributed ledger technologies, and related cyber-physical system domains. The analysis systematically examined SCADA communication architectures, data exchange models, blockchain fundamentals, integration paradigms, consensus mechanisms, privacy and access control strategies, interoperability challenges, and empirical pilot implementations across both developed and developing contexts. The findings reveal that conventional SCADA architectures, largely built on centralised trust and legacy protocols, are increasingly inadequate for addressing modern threat landscapes and multi-stakeholder data sharing requirements. Blockchain-assisted architectures—particularly permissioned and hybrid on-chain/off-chain models—demonstrate strong potential to improve data integrity, auditability, non-repudiation, and cross-organisational trust without disrupting real-time control functions. However, the study also identifies persistent challenges related to scalability, interoperability, governance complexity, and human capacity, which constrain large-scale deployment. Empirical evidence from pilot projects further indicates that blockchain is most effective when applied selectively at supervisory and coordination layers rather than within time-critical control loops. The study concludes that blockchain-assisted secure data exchange represents a strategically valuable complement to existing SCADA security mechanisms rather than a standalone solution. It recommends future research on performance-optimised consensus protocols, standardised integration frameworks, and the convergence of blockchain with advanced analytics and artificial intelligence. Policy alignment, capacity development, and context-aware implementation strategies are also essential to support sustainable adoption, particularly in developing power system environments.

Keywords: SCADA Systems; Blockchain Technology; Secure Data Exchange; Power System Cybersecurity; Distributed Ledger Architectures; Smart Grids

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems form the operational backbone of modern power systems, enabling real-time monitoring, control, and coordination of geographically distributed assets across generation, transmission, and distribution domains. As electric power infrastructures evolve toward highly interconnected smart grids, SCADA platforms are increasingly integrated with advanced communication networks, intelligent electronic devices, and data-driven decision-support systems. While this transformation enhances efficiency, flexibility, and situational awareness, it also significantly expands the cyber-attack surface of power systems, exposing critical infrastructure to sophisticated threats that can compromise operational continuity, safety, and national security (Alcaraz & Zeadally, 2015; Humayed et al., 2017).

Traditional SCADA architectures were designed under assumptions of isolation, proprietary protocols, and trusted environments. However, contemporary power systems operate in open, heterogeneous, and often multi-stakeholder ecosystems where data must be exchanged across organizational and geographic boundaries. This shift has rendered conventional perimeter-based security mechanisms inadequate, as evidenced by the growing number of cyber incidents targeting energy infrastructures worldwide. Attacks such as data falsification, replay attacks, unauthorized command injection, and insider manipulation can disrupt grid stability, degrade equipment, and trigger cascading failures. Ensuring secure, trustworthy, and resilient data exchange within SCADA-controlled power systems has therefore become a pressing research and operational priority.

Blockchain technology has emerged as a promising paradigm for addressing trust, integrity, and transparency challenges in distributed systems. Characterised by decentralisation, cryptographic immutability, and consensus-driven validation, blockchain offers mechanisms for secure record-keeping and verifiable data sharing without reliance on a single trusted authority (Andoni et al., 2019). In the context of power systems, blockchain has been explored for applications such as peer-to-peer energy trading, distributed energy resource coordination, and secure metering. Its potential relevance to SCADA-controlled environments lies in its capacity to provide tamper-evident logging, decentralised authentication, and auditable data exchange across heterogeneous entities.

Insights from digital transformation in other critical sectors further reinforce the relevance of blockchain-assisted architectures. For instance, studies in healthcare systems highlight how strategic leadership and innovation are essential for deploying secure, technology-enabled platforms in complex, safety-critical environments (Gado et al., 2020). Similarly, the rapid expansion of telehealth services during and after the COVID-19 pandemic exposed the limitations of centralised data management and underscored the need for secure, interoperable, and resilient information exchange frameworks (Omotayo & Kuponiyi, 2020). Although these studies are situated outside the energy domain, they provide valuable analogies for SCADA systems, where data integrity, availability, and trust are equally mission-critical.

Emerging research on artificial intelligence-driven digital platforms in underserved regions also offers relevant perspectives. Frempong et al. (2020) demonstrate how decentralised and intelligent systems can enhance service delivery in environments characterised by limited infrastructure and high operational risk. These findings resonate with power systems in developing regions, including parts of Africa, where SCADA deployments must operate under constraints such as limited cybersecurity capacity, ageing infrastructure, and increasing integration of distributed energy resources. Blockchain-assisted data exchange architectures may offer a pathway to improving trust and resilience in such contexts by reducing dependence on centralised control points and enabling verifiable multi-party coordination.

From a technological standpoint, blockchain's suitability for SCADA environments is not without challenges. Power system operations impose stringent requirements on latency, determinism, and availability, which may conflict with the computational overhead and consensus delays associated with many blockchain platforms. Nevertheless, advances in permissioned blockchains, lightweight consensus mechanisms, and hybrid on-chain/off-chain architectures have opened new possibilities for aligning blockchain capabilities with industrial control system constraints (Shaik, Sadhu & Venkataramanan, 2019; Pop et al., 2018). These developments suggest that blockchain can complement, rather than replace, existing SCADA security mechanisms by providing an additional trust layer for data exchange and auditability.

The relevance of secure data exchange is further amplified by the growing interdependence between cyber and physical components in power systems. As cyber-physical systems, SCADA-controlled grids rely on timely and accurate data to maintain physical stability and safety. Compromised data integrity can therefore have immediate and tangible physical consequences. Research in cyber-physical system security consistently highlights the need for holistic approaches that integrate cybersecurity, system design, and governance considerations (Humayed et al., 2017). Blockchain-assisted architectures align with this perspective by embedding trust and verification mechanisms directly into the data exchange process.

In developing economies, including Nigeria and other African countries, the stakes are particularly high. Power systems in these regions often face reliability challenges, limited redundancy, and increasing exposure to cyber threats as digitalisation accelerates. Lessons from innovation-driven sectors such as healthcare supply chain management, where advanced technologies like nanomaterials and distributed tracking systems are leveraged to enhance reliability and transparency, illustrate the broader value of secure, technology-enabled coordination (Ike et al., 2020). Translating these principles to the energy sector underscores the potential of blockchain to support secure SCADA data exchange in resource-constrained settings.

The overarching aim of this review is to critically analyse blockchain-assisted secure data exchange architectures for SCADA-controlled power systems, with particular emphasis on their potential to enhance cybersecurity, trust, and operational resilience in increasingly digitalised power grids. As power system operations become more interconnected and data-driven, ensuring the integrity, authenticity, and availability of SCADA data has become essential for maintaining grid stability and preventing cyber-induced disruptions. This review seeks to clarify the role blockchain technologies can play in addressing these emerging challenges.

To realise this aim, the review is guided by several interrelated objectives. First, it aims to examine the inherent security weaknesses of conventional SCADA data exchange mechanisms, especially those arising from centralised trust models and legacy communication protocols. Second, it seeks to synthesise and evaluate existing blockchain-based approaches that have been proposed for securing SCADA data exchange, focusing on architectural design choices, trust management strategies, and data integrity mechanisms. Third, the review aims to assess the suitability of different blockchain deployment models—such as permissioned, consortium, and hybrid architectures—within the stringent real-time and reliability requirements of power system operations. Finally, it aims to identify unresolved technical, organisational, and regulatory challenges that may hinder large-scale adoption, thereby highlighting promising directions for future research.
The scope of this review is confined to SCADA-controlled power systems across generation, transmission, and distribution domains, with specific attention to secure data exchange rather than market-oriented or cryptocurrency-based applications. While insights from other critical sectors are used to enrich the discussion, the analysis remains firmly centred on power system cybersecurity. The review considers globally diverse literature, including perspectives relevant to developing regions, to ensure a comprehensive and context-aware assessment of blockchain-assisted SCADA security solutions.

1.1 SCADA Systems in Modern Power Grids

Supervisory Control and Data Acquisition (SCADA) systems are integral to the operation of modern power grids, providing real-time monitoring, control, and data acquisition across geographically dispersed assets. In contemporary electricity networks, SCADA platforms coordinate critical functions such as voltage regulation, fault detection, load balancing, and equipment diagnostics, thereby ensuring operational reliability and efficiency. As power grids transition from vertically integrated systems to decentralised and intelligent infrastructures, SCADA systems have evolved from isolated, proprietary platforms into complex cyber-physical systems tightly coupled with communication networks and digital control technologies (Gungor et al., 2011).

The integration of renewable energy sources, distributed energy resources, and advanced metering infrastructure has further expanded the functional scope of SCADA systems. Modern SCADA environments now support bidirectional data flows between field devices, control centres, and external stakeholders, enabling advanced automation and situational awareness. However, this increased connectivity also introduces dependencies on public and semi-public communication networks, fundamentally altering the risk profile of power system operations. Humayed et al. (2017) emphasise that SCADA-controlled power grids represent quintessential cyber-physical systems, where cyber-layer disruptions can directly propagate into physical failures with severe societal and economic consequences.

In developing regions, including parts of Africa, SCADA deployment plays a critical role in improving grid reliability and operational transparency. Studies from Nigeria demonstrate that SCADA-based monitoring has significantly enhanced fault response times and system visibility in power networks characterised by ageing infrastructure and limited redundancy (Eneh, Orah & Emeka, 2019). Nevertheless, these deployments often coexist with legacy components and constrained cybersecurity resources, amplifying the importance of secure and resilient data exchange. Consequently, understanding the evolving role of SCADA systems within modern power grids is essential for contextualising the need for advanced security mechanisms capable of supporting trustworthy and dependable grid operations.

1.2 Cybersecurity Threat Landscape in Power System Communications

The cybersecurity threat landscape confronting power system communications has expanded considerably with the digitalisation and interconnection of SCADA networks. Historically, SCADA systems relied on isolation and obscurity for protection, but modern deployments increasingly utilise standardised protocols and internet-enabled communication channels. This evolution has exposed power systems to a wide range of cyber threats, including data manipulation, denial-of-service attacks, malware infiltration, and unauthorised command execution. Such attacks can disrupt operational decision-making, damage physical assets, and, in extreme cases, trigger large-scale power outages (Alcaraz & Zeadally, 2015).
Industrial control system communications are particularly vulnerable due to protocol-level weaknesses and long equipment lifecycles. Many widely used SCADA protocols were not designed with robust security features such as encryption or authentication, making them susceptible to eavesdropping and spoofing attacks. Knowles et al. (2015) highlight that attackers increasingly exploit these weaknesses through advanced persistent threats and targeted intrusions, often remaining undetected for extended periods. The convergence of operational technology and information technology further complicates security management by blurring traditional organisational and technical boundaries.
In the African context, cybersecurity challenges are exacerbated by infrastructural constraints, skills shortages, and limited regulatory enforcement. Research focusing on Nigeria's smart grid initiatives reveals that inadequate cybersecurity frameworks and inconsistent security practices significantly increase exposure to cyber risks (Otuoze et al., 2019). As power utilities across the continent modernise their SCADA systems to support smart grid functionalities, the absence of secure and trusted data exchange mechanisms poses a substantial threat to grid resilience. Addressing this evolving threat landscape, therefore, requires security solutions that are not only technically robust but also adaptable to diverse operational and regional contexts.

1.3 Limitations of Traditional Security Mechanisms

Traditional security mechanisms employed in SCADA-controlled power systems are largely derived from conventional information technology security models. These mechanisms typically rely on perimeter defences such as firewalls, intrusion detection systems, and access control lists to protect centralised control architectures. While effective against certain classes of threats, such approaches exhibit fundamental limitations when applied to highly distributed and dynamic power system environments. Centralised trust models create single points of failure, making them attractive targets for sophisticated cyber attackers (Ten, Manimaran & Liu, 2010).

Another limitation lies in the reactive nature of many traditional security solutions. Signature-based intrusion detection and rule-based access controls are often unable to detect novel or stealthy attacks, particularly those exploiting zero-day vulnerabilities or insider privileges. Cherdantseva et al. (2016) argue that risk assessment and mitigation approaches for SCADA systems frequently fail to account for the complex interdependencies between cyber and physical components, resulting in incomplete threat coverage and residual vulnerabilities.

In developing regions, these limitations are further compounded by operational constraints. Studies of

Nigerian power utilities indicate that legacy systems, inconsistent security policies, and limited cybersecurity expertise undermine the effectiveness of traditional defence mechanisms (Haruna et al., 2022). Additionally, the increasing need for data sharing among utilities, regulators, and third-party service providers challenges the feasibility of strictly perimeter-based security. As power systems become more decentralised and collaborative, traditional security mechanisms struggle to provide scalable, transparent, and trustworthy data exchange. These shortcomings underscore the need for alternative security paradigms capable of supporting decentralised trust and verifiable data integrity in SCADA environments.

1.4 Motivation for Blockchain-Enabled Secure Data Exchange

The motivation for adopting blockchain-enabled secure data exchange in SCADA-controlled power systems stems from the inherent limitations of centralised security models and the growing need for distributed trust. Blockchain technology introduces a decentralised ledger architecture in which data records are cryptographically linked and validated through consensus mechanisms, ensuring immutability and traceability. These characteristics directly address critical SCADA security requirements such as data integrity, non-repudiation, and auditability (Andoni et al., 2019).

In power system communications, blockchain offers the potential to establish trusted data exchange among multiple stakeholders without reliance on a single authority. This is particularly relevant in modern grids that integrate independent power producers, distributed energy resources, and third-party service providers. Shaik, Sadhu,and Venkataramanan (2019) highlight that permissioned and lightweight blockchain frameworks can be adapted to resource-constrained environments, making them suitable for industrial and SCADA applications where latency and reliability are paramount.

Beyond technical advantages, blockchain-enabled architectures support institutional transparency and accountability in energy systems. Ahl et al. (2019) note that distributed ledger technologies can facilitate trustworthy coordination across organisational boundaries, an increasingly important requirement in decentralised power systems. For SCADA environments, blockchain can function as a secure middleware layer, complementing existing control mechanisms while enhancing trust in data exchange. This motivation underpins growing research interest in blockchain-assisted SCADA security as a pathway toward more resilient and trustworthy power system operations.

II. SCADA COMMUNICATION ARCHITECTURES AND DATA EXCHANGE MODELS

SCADA communication architectures define how data is generated, transmitted, processed, and acted upon within power system environments. At their core, these architectures comprise hierarchical layers that connect field devices, such as sensors and programmable logic controllers, to supervisory and control centres. Data exchange within these layers enables real-time monitoring of system states, execution of control commands, and long-term operational analysis. In modern power grids, SCADA communication has evolved beyond closed, proprietary networks into complex, heterogeneous ecosystems that integrate operational technology with information technology infrastructures (Gungor et al., 2011).

Traditional SCADA architectures are typically structured around a centralised control model, where data from remote terminal units and intelligent electronic devices is aggregated at a master station for analysis and decision-making. While this model simplifies coordination and oversight, it also concentrates trust and control within a limited set of components. As grid operations expand to include distributed generation, advanced metering infrastructure, and third-party service providers, the volume, velocity, and diversity of data exchanged through SCADA networks have increased substantially. Humayed et al. (2017) note that such cyber-physical integration amplifies the interdependencies between communication networks and physical power processes, making secure and reliable data exchange a critical requirement.

Contemporary SCADA data exchange models increasingly resemble distributed data pipelines rather than simple point-to-point communication channels. Concepts drawn from cloud-native data engineering, such as extract–load–transform workflows and automated data pipelines, are becoming relevant as utilities seek to integrate operational data with analytics and decision-support platforms. Akindemowo et al. (2021) demonstrate that automated data pipelines improve data consistency, timeliness, and scalability in complex digital environments. When applied conceptually to SCADA systems, similar pipeline-oriented models can enhance the management of telemetry, event logs, and control data, provided that security and latency constraints are adequately addressed.

The need for transparency and traceability in data exchange further influences SCADA communication design. Research on end-to-end visibility frameworks in global supply chains highlights the importance of maintaining trustworthy, auditable data flows across multiple organisational boundaries (Nnabueze et al., 2021; Moyo et al., 2021). Power systems increasingly share operational data with regulators, market operators, and external service providers, creating similar requirements for traceability and compliance. In centralised SCADA architectures, achieving such transparency often relies on post hoc logging mechanisms that are vulnerable to tampering and single points of failure.

From a cybersecurity perspective, the data exchange models underpinning SCADA communications remain a major source of vulnerability. Legacy protocols frequently lack encryption, authentication, and integrity verification, exposing data streams to interception and manipulation. Attack and defence modelling studies show that adversaries can exploit these weaknesses to inject false data or disrupt control signals, undermining grid stability (Ten, Manimaran & Liu, 2010). Alcaraz and Zeadally (2015) further emphasise that the interconnected nature of critical infrastructure communications magnifies the potential impact of such attacks, as compromised data can propagate rapidly across systems.

Regional studies underscore how these challenges manifest in practice. In Nigeria and other African countries, SCADA communication networks often operate alongside ageing infrastructure and inconsistent cybersecurity policies. Otuoze et al. (2019) observe that smart grid deployments in Nigeria face heightened risks due to limited security investment and skills shortages, making secure data exchange particularly difficult to sustain. These conditions highlight the need for architectures that embed trust and verification directly into the data exchange process, rather than relying solely on perimeter defences.

Emerging data-driven techniques also influence how SCADA data is processed and interpreted. The application of natural language processing and advanced analytics in research and operational contexts demonstrates how unstructured and semi-structured data can be transformed into actionable insights (Eboseremen et al., 2021). While SCADA data is primarily structured, the growing integration of alarms, maintenance reports, and operator logs introduces additional data types that must be securely exchanged and analysed. This trend further complicates communication architectures and increases the importance of robust data governance.

Blockchain-based approaches have been proposed as a means of enhancing SCADA data exchange by introducing decentralised trust and tamper-evident record keeping. Pop et al. (2018) show that blockchain can support scalable and tamper-resistant energy data registration, offering a foundation for secure data sharing across distributed entities. When integrated as a middleware layer, blockchain can complement existing SCADA communication protocols by providing immutable logs and verifiable data provenance without interfering with real-time control loops.

However, integrating blockchain into SCADA communication architectures requires careful consideration of performance and interoperability constraints. Consensus mechanisms and distributed ledger maintenance introduce computational and communication overheads that may conflict with the stringent latency requirements of power system control. Shaikand Venkataramanan (2019) argue that lightweight, permissioned blockchain frameworks are better suited to industrial environments, as they allow controlled participation and reduced consensus complexity. Such models align more closely with the operational realities of SCADA systems.

2.1 SCADA Network Layers and Communication Protocols

SCADA network architectures in power systems are typically organised into layered structures that reflect functional separation between physical processes, control logic, and supervisory operations. At the lowest layer, field devices such as sensors, actuators, and intelligent electronic devices interact directly with physical equipment, collecting measurements and executing control commands. These devices communicate with remote terminal units and programmable logic controllers, which aggregate data and perform local automation tasks. Above this layer, supervisory networks connect control centres where operators monitor system status, analyse data, and issue high-level commands (Stouffer et al., 2011).

Communication protocols play a central role in enabling data exchange across these layers. Legacy protocols such as Modbus, Profibus, and DNP3 were designed primarily for reliability and determinism rather than security. As a result, they often lack built-in mechanisms for authentication, encryption, and integrity protection. Cheminod et al. (2013) note that while these protocols remain widely deployed due to long equipment lifecycles, their inherent vulnerabilities pose significant risks when SCADA networks are connected to corporate or external networks. Newer standards, including IEC 61850 and secure variants of DNP3, aim to address some of these shortcomings but are not universally adopted.

The hierarchical nature of SCADA communication architectures historically supported a clear separation between operational technology and information technology domains. However, modern power systems increasingly blur this boundary as utilities integrate SCADA data with enterprise systems, analytics platforms, and cloud-based services. This convergence introduces additional communication layers, gateways, and interfaces that increase architectural complexity and expand the attack surface (Igure et al., 2006). Ensuring consistent and secure communication across heterogeneous protocols and network segments, therefore, remains a major challenge.

In developing regions such as Nigeria, SCADA network layers often coexist with ageing infrastructure and hybrid communication technologies, including radio, fibre, and cellular links. Ogundari et al. (2020) observe that inconsistent protocol implementation and limited security hardening are common in such environments, increasing susceptibility to interception and manipulation. These realities underscore the importance of understanding SCADA network layers and communication protocols as a foundation for designing secure and resilient data exchange architectures in power systems.

2.2 Data Types and Exchange Requirements

SCADA-controlled power systems generate and exchange diverse categories of data, each with distinct operational and security requirements. Real-time telemetry data, such as voltage, current, frequency, and breaker status, is continuously transmitted from field devices to control centres to support situational awareness and automated control. Control commands, which flow in the opposite direction, enable operators and automated systems to adjust system parameters, isolate faults, and restore service. In addition, event logs, alarms, and historical data are exchanged to support diagnostics, compliance, and long-term planning (Yan et al., 2012).

The exchange requirements associated with these data types are stringent. Telemetry and control data are highly time-sensitive, with latency and jitter directly affecting system stability. Even minor delays or inaccuracies can lead to inappropriate control actions or cascading failures. Cárdenas et al. (2008) emphasise that secure control in cyber-physical systems requires not only confidentiality and integrity but also availability and timeliness, distinguishing SCADA data exchange from conventional IT data transfers. Security mechanisms must therefore operate without introducing unacceptable delays or computational overhead.

From a cybersecurity perspective, different data types present varying risk profiles. Control commands are particularly critical, as unauthorised or manipulated commands can cause immediate physical damage.

Telemetry data, while often perceived as less sensitive, can be exploited for reconnaissance or false data injection attacks if integrity is compromised (Amin & Schwartz, 2013). Consequently, data exchange models must incorporate differentiated protection strategies aligned with the criticality and function of each data category.

In many developing power systems, data exchange requirements are further complicated by infrastructural and organisational constraints. Studies of Nigerian power utilities highlight challenges such as inconsistent data quality, fragmented data repositories, and limited real-time visibility (Okoye, Onuoha & Udemadu, 2022). These issues undermine effective decision-making and exacerbate the impact of security incidents. Addressing the diverse data types and exchange requirements within SCADA systems is therefore fundamental to designing architectures that support secure, reliable, and resilient power system operations.

2.3 Trust Models in SCADA-Based Power Systems

Trust models underpin how entities within SCADA-based power systems authenticate data sources, validate commands, and coordinate operational decisions. Traditionally, SCADA environments have relied on implicit trust assumptions, where devices and operators within a defined network perimeter are considered trustworthy by default. This model reflects the historical isolation of control networks but is increasingly incompatible with modern power systems characterised by interconnection, remote access, and third-party participation (Langner, 2011).

Centralised trust models concentrate authority within control centres or system operators, simplifying governance but creating single points of failure. High-profile cyber incidents demonstrate how compromised credentials or insider access can undermine such models, enabling attackers to bypass perimeter defences and manipulate trusted components. Fadok (2011) argues that these weaknesses reflect broader challenges in critical infrastructure governance, where trust is often assumed rather than continuously verified.

As power systems decentralise, alternative trust models are gaining attention. Distributed trust approaches seek to minimise reliance on any single authority by enabling multiple parties to validate data and actions. Blockchain technology has been proposed as one mechanism for implementing such models, leveraging cryptographic verification and consensus to establish trust among participants without requiring full mutual confidence (Kshetri, 2017). While not a panacea, these approaches align conceptually with the distributed nature of modern power grids.

In the Nigerian context, trust and governance issues are particularly salient due to regulatory fragmentation, legacy infrastructure, and evolving market structures. Digitalisation initiatives in Nigeria’s power sector often struggle with unclear trust boundaries and accountability mechanisms. These challenges highlight the need for explicit, technology-supported trust models that can adapt to multi-stakeholder SCADA environments. Understanding existing trust assumptions and their limitations is therefore essential for evaluating blockchain-assisted secure data exchange architectures.

2.4 Vulnerabilities in Existing Data Exchange Architectures

Existing SCADA data exchange architectures exhibit vulnerabilities that stem from both technical design choices and operational practices. Many architectures rely on legacy protocols and flat network structures that provide minimal segmentation and limited security controls. As a result, once an attacker gains access to a communication network, lateral movement and escalation are often possible with little resistance (Stamp & Young, 2003). These structural weaknesses undermine the confidentiality, integrity, and availability of SCADA data.

Protocol-specific vulnerabilities further exacerbate these risks. Studies of widely used SCADA protocols such as DNP3 reveal susceptibility to attacks, including spoofing, replay, and command injection due to inadequate authentication and integrity mechanisms (East et al., 2009). Even when security extensions are available, inconsistent implementation and backward compatibility requirements limit their effectiveness. Mo et al. (2012) demonstrate that false data injection attacks can remain stealthy while causing significant control errors, highlighting the difficulty of detecting sophisticated integrity breaches. Architectural vulnerabilities are also influenced by increasing system complexity. Integration with corporate IT networks, remote maintenance access, and third-party data sharing introduces additional interfaces and dependencies that are often insufficiently secured. In regions with limited cybersecurity maturity, these challenges are amplified. Salawu (2018) report that power system communication networks in parts of West Africa exhibit high exposure to cyber threats due to inadequate monitoring, weak access controls, and limited incident response capabilities.

Collectively, these vulnerabilities illustrate that existing SCADA data exchange architectures were not designed to withstand modern cyber threats. Their limitations underscore the need for fundamentally different approaches that embed security and trust into the data exchange process itself. This context provides a strong rationale for exploring blockchain-assisted architectures as a means of addressing persistent weaknesses in SCADA communication and data exchange models.

III. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY FOR INDUSTRIAL SYSTEMS

Blockchain technology represents a paradigm shift in how data is recorded, shared, and trusted within distributed systems. Originally conceptualised as the underlying architecture for digital currencies, blockchain has since evolved into a general-purpose technology with applications across diverse industrial domains. At its core, a blockchain is a distributed ledger maintained by a network of participants, where transactions are grouped into blocks, cryptographically linked, and validated through consensus mechanisms. This design eliminates reliance on a central authority while ensuring data immutability, transparency, and resistance to tampering (Nakamoto, 2008; Zheng et al., 2018).

For industrial systems, including energy, manufacturing, and supply chains, these foundational characteristics address long-standing challenges associated with data integrity, trust, and coordination across organisational boundaries. Industrial environments are typically characterised by heterogeneous stakeholders, legacy systems, and stringent reliability requirements. Traditional centralised databases often struggle to provide end-to-end visibility and verifiable audit trails in such contexts. Research on global supply chains demonstrates that blockchain-enabled visibility frameworks can significantly enhance transparency, compliance, and traceability by providing a single, shared source of truth accessible to authorised participants (Nnabueze et al., 2021). These principles are directly relevant to industrial control environments where trustworthy data exchange is critical.

Consensus mechanisms constitute a fundamental component of blockchain systems, determining how agreement is reached on the validity of transactions. While early blockchains relied on computationally intensive proof-of-work schemes, industrial applications increasingly favour alternative consensus models such as proof-of-authority and Byzantine fault-tolerant protocols. These approaches reduce latency and energy consumption while maintaining robustness against faults and malicious behaviour (Zheng et al., 2018). The adaptability of consensus mechanisms is particularly important for industrial systems, where real-time constraints and deterministic performance are paramount.

Smart contracts further extend blockchain functionality by enabling programmable logic to be executed automatically when predefined conditions are met. Christidis and Devetsikiotis (2016) highlight that smart contracts can support automation, access control, and policy enforcement in Internet of Things and industrial settings. In industrial systems, this capability allows operational rules, data-sharing agreements, and compliance requirements to be embedded directly into the data exchange infrastructure. Such automation reduces human intervention, minimizes errors, and enhances accountability.

The relevance of blockchain to energy and power systems has been reinforced by studies on renewable energy integration and infrastructure coordination. Yeboah and Ike (2020) emphasise that large-scale renewable projects require coordinated data sharing, transparent governance, and robust operational oversight. Blockchain's decentralised architecture aligns with these needs by facilitating secure coordination among distributed assets and stakeholders. Although originally examined in the context of renewable energy planning, these insights extend naturally to SCADA-controlled environments where distributed generation and grid-edge intelligence are becoming more prevalent.

Beyond technical considerations, effective deployment of blockchain in industrial systems depends on organisational readiness and human capacity. Workforce competence, leadership, and governance structures influence how new technologies are adopted and sustained. Also, reliability engineering and infrastructure resilience are closely linked to targeted training and leadership development. In blockchain-enabled industrial systems, such competencies are essential for managing cryptographic keys, configuring access policies, and responding to incidents, underscoring the socio-technical nature of blockchain adoption.

Interestingly, parallels can be drawn from blockchain-adjacent research in non-industrial domains. Studies in agriculture, such as Ofori et al. (2021), demonstrate how systematic, data-driven interventions improve transparency and outcomes in complex, resource-dependent systems. While the application domain differs, the underlying lesson—that structured data management and traceability enhance system performance—reinforces the rationale for blockchain adoption in industrial contexts. Blockchain provides a digital analogue to such systematic approaches by ensuring consistent, verifiable records across distributed operations.

A growing body of literature situates blockchain within broader industrial ecosystems that prioritise sustainability, accountability, and resilience. Saberi et al. (2019) show that blockchain supports sustainable supply chain management by enabling traceability and trust across lifecycle stages. These attributes are increasingly valued in industrial systems facing regulatory scrutiny and societal expectations for transparency. In power systems, similar pressures arise from the need to demonstrate operational integrity, regulatory compliance, and cybersecurity robustness.

From an African and developing-economy perspective, blockchain also holds promise for addressing governance and trust deficits. Abubakar et al. (2019) highlight how knowledge management and decision-making structures influence organisational performance in emerging economies. Blockchain's capacity to codify rules, decentralise trust, and provide immutable records can complement institutional reforms by reducing reliance on discretionary control and opaque processes.

IV. BLOCKCHAIN–SCADA INTEGRATION PARADIGMS

Blockchain–SCADA integration paradigms describe the architectural strategies through which distributed ledger technologies are embedded into supervisory control and data acquisition environments to enhance secure data exchange, trust, and system resilience. These paradigms are shaped by the inherent constraints of SCADA systems, including real-time performance requirements, legacy infrastructure, and safety-critical operations. Rather than replacing existing control mechanisms, blockchain is generally positioned as a complementary layer that augments data integrity, authentication, and auditability across power system communications (Mollah et al., 2019).

One dominant integration paradigm is the middleware-based approach, where blockchain functions as an intermediary layer between SCADA field devices and higher-level enterprise or analytics systems. In this model, real-time control loops remain isolated from blockchain operations to avoid latency penalties, while selected operational data, event logs, and configuration changes are recorded on the distributed ledger. This paradigm aligns with principles observed in risk-aware digital systems, where real-time monitoring is decoupled from analytical and compliance layers to preserve operational performance (Filani et al., 2022). For SCADA-controlled power systems, middleware-based integration enables tamper-evident logging and cross-organisational data sharing without disrupting time-critical control functions.

A second paradigm involves hybrid on-chain and off-chain architectures, which balance blockchain immutability with the scalability demands of industrial data. In this approach, only hashes or metadata of SCADA data are stored on-chain, while bulk data remains in traditional databases or data historians. This design reduces storage overhead and supports high-throughput data exchange while preserving data provenance and integrity verification. Similar architectural reasoning underpins agile multi-cloud portfolio management models, where distributed resources are coordinated through lightweight orchestration layers rather than fully centralised control (Akindemowo et al., 2022). For SCADA environments, hybrid architectures provide a practical pathway for incremental blockchain adoption.

Consortium and permissioned blockchain models represent another important integration paradigm. Unlike public blockchains, permissioned ledgers restrict participation to authenticated entities such as utilities, grid operators, regulators, and trusted service providers. This governance structure aligns with the regulated nature of power systems and supports deterministic consensus mechanisms with lower latency. Li et al. (2017) demonstrate that consortium blockchains can facilitate secure coordination in industrial Internet of Things environments, offering insights directly applicable to SCADA networks with multiple authorised stakeholders. Such models are particularly relevant in national or regional grids where trust relationships are formally defined.

From a governance and risk management perspective, blockchain–SCADA integration also intersects with threat intelligence and DevSecOps principles. Adebayo (2022) highlights the importance of embedding threat intelligence into system development and operations to proactively mitigate cyber risks. When applied to SCADA systems, blockchain can support this paradigm by providing immutable records of security events, configuration changes, and access attempts, thereby enhancing situational awareness and forensic capabilities. This integration supports a shift from reactive to proactive cybersecurity management in power system operations.

The data visualisation and decision-support paradigm further illustrates how blockchain-enabled SCADA data can enhance operational and policy decisions. Eboseremen et al. (2022) show that interactive and trustworthy data visualisations significantly improve decision-making in public policy contexts. In power systems, blockchain-backed data feeds can increase confidence in dashboards used by operators, regulators, and planners by ensuring that displayed information is verifiable and has not been manipulated. This paradigm underscores the socio-technical dimension of blockchain integration, where human trust in data is as critical as technical security.

Environmental and societal considerations also influence integration paradigms, particularly in developing regions. Studies on environmental risk assessment in Ghana illustrate how transparent and reliable data are essential for managing complex, high-impact systems (Agyemang et al., 2022). Although focused on environmental contamination, the underlying principle—that trustworthy data underpins effective risk management—applies equally to power system operations. Blockchain-assisted SCADA architectures can therefore support broader sustainability and accountability objectives by ensuring data integrity across environmental monitoring and energy infrastructure.

From a cyber-physical systems perspective, integration paradigms must respect the tight coupling between cyber actions and physical consequences. Sridhar et al. (2012) emphasise that security mechanisms in power grids must be designed with an understanding of physical system dynamics. Consequently, blockchain integration is typically limited to supervisory and coordination layers, avoiding direct insertion into fast control loops. This cautious integration paradigm reflects a recognition that blockchain's strengths lie in trust and auditability rather than real-time control.

In regions such as Nigeria, where digital infrastructure maturity varies, pragmatic integration paradigms are essential. Ogunleye and Adeyemo (2021) note that cybersecurity readiness in Nigeria's power sector is uneven, necessitating solutions that can coexist with legacy systems and constrained resources. Permissioned blockchain overlays and hybrid architectures offer feasible integration pathways that enhance security without requiring wholesale system replacement.

V. SECURE DATA EXCHANGE ARCHITECTURES USING BLOCKCHAIN

Secure data exchange architectures based on blockchain are designed to address persistent challenges of trust, integrity, and accountability in distributed and safety-critical systems such as SCADA-controlled power networks. These architectures leverage the decentralised and immutable nature of blockchain to ensure that operational data, control records, and system events are shared in a manner that is verifiable, tamper-resistant, and resilient to single points of failure. In contrast to conventional centralised databases, blockchain-based architectures embed trust directly into the data exchange mechanism, reducing reliance on implicit organisational or infrastructural assumptions (Mollah et al., 2019).

At the architectural level, blockchain-enabled secure data exchange typically adopts a layered approach in which the core SCADA control loops remain isolated from blockchain processes to preserve real-time performance. Data that is critical for auditability, coordination, and post-event analysis—such as state changes, alarms, access logs, and inter-organisational transactions—is selectively committed to the blockchain. This approach mirrors system-oriented frameworks observed in healthcare and service delivery, where complex journeys are mapped and secured through structured, end-to-end data flows rather than ad hoc exchanges (Gado et al., 2022). In power systems, such architectures enhance visibility across organisational boundaries while maintaining operational safety.

A defining feature of blockchain-based secure data exchange is cryptographic integrity assurance. Each transaction is digitally signed and linked to previous records, creating a chain of evidence that is computationally infeasible to alter retrospectively. This property is particularly valuable in SCADA environments, where disputes over data accuracy, responsibility, or timing can have regulatory and financial implications. Similar integrity requirements have been demonstrated in blockchain-based medical data preservation systems, where immutability and controlled access are essential for trust (Li et al., 2018). These principles translate directly to power system data exchange, where accurate historical records underpin system reliability and compliance.

Permissioned blockchain architectures are especially relevant for SCADA applications. In these architectures, participation is restricted to authenticated entities such as utilities, grid operators, regulators, and trusted service providers. Governance rules define who can write, read, or validate data, aligning technical controls with institutional responsibilities. Shaik, Sadhu, and Venkataramanan (2019) note that permissioned frameworks reduce consensus overhead and support predictable performance, making them suitable for industrial environments. Secure data exchange architectures for SCADA, therefore, often employ consortium blockchains that balance decentralisation with regulatory oversight.

Integration with advanced monitoring and analytics platforms further strengthens blockchain-enabled data exchange. AI-driven cybersecurity intelligence dashboards demonstrate how trusted data feeds enhance threat detection, forensic analysis, and situational awareness in regulated sectors (Bukhari et al., 2022). When blockchain-backed SCADA data is used as input to such dashboards, the reliability of analytical outputs improves, as decisions are based on data whose provenance and integrity can be verified. This integration supports proactive risk management rather than reactive incident response.

The role of visualisation and human decision-making is also central to secure data exchange architectures. Eboseremen et al. (2022) show that interactive and trustworthy data visualisations significantly improve policy and operational decisions. In power systems, blockchain-secured data streams can underpin operator dashboards and regulatory reports, increasing confidence in the information presented. This human-centric dimension underscores that secure data exchange is not solely a technical challenge but also a socio-technical one.

From a resilience perspective, blockchain-based architectures support distributed data availability, reducing the risk that data loss or compromise at a single node will disrupt system-wide operations. Network analytics research highlights how distributed visibility enhances the ability to anticipate and manage disruptions in complex systems (Nnabueze et al., 2022). Applied to SCADA-controlled power systems, blockchain can facilitate shared situational awareness during disturbances, enabling coordinated responses across organisational boundaries.

In developing regions, secure data exchange architectures must contend with uneven digital infrastructure and cybersecurity maturity. Studies of Nigeria's power sector reveal gaps in readiness that increase vulnerability to data compromise and operational disruption (Ogunleye & Adeyemo, 2021). Blockchain-based architectures offer a means of strengthening trust and accountability even in such contexts, provided they are deployed incrementally and aligned with local capacity constraints. Lessons from digital health frameworks aimed at marginalised communities further illustrate the importance of adaptable, inclusive architectures that prioritise secure access and data governance (Kuponiyi & Akomolafe, 2022).

Despite their promise, blockchain-enabled secure data exchange architectures also introduce challenges, including scalability limits, governance complexity, and integration overhead. Zheng et al. (2018) emphasise that careful architectural design is required to ensure that blockchain enhances rather than hinders system performance. In SCADA environments, this necessitates clear separation between real-time control and blockchain-based coordination layers.

VI. CONSENSUS MECHANISMS AND PERFORMANCE CONSTRAINTS

Consensus mechanisms are a foundational component of blockchain-based systems, as they define how distributed participants agree on the validity and ordering of transactions in the absence of a central authority. In the context of SCADA-controlled power systems, the choice of consensus mechanism has direct implications for performance, reliability, and operational safety. Unlike financial or purely informational systems, power system environments impose stringent constraints on latency, determinism, and availability, making consensus design a critical consideration for blockchain-assisted secure data exchange.

Traditional blockchain platforms rely on consensus mechanisms such as proof-of-work, which provide strong security guarantees but incur significant computational overhead and unpredictable confirmation delays. These characteristics are fundamentally misaligned with SCADA environments, where control decisions must be executed within strict time bounds. Survey studies on blockchain technologies consistently highlight that proof-of-work-based systems are unsuitable for industrial and cyber-physical applications due to their energy inefficiency and low throughput (Zheng et al., 2018). Consequently, industrial blockchain deployments increasingly favour alternative consensus models that prioritise performance and predictability.

Permissioned consensus mechanisms, including Byzantine fault-tolerant protocols, offer a more viable foundation for SCADA integration. Practical Byzantine Fault Tolerance (PBFT) enables a known set of authenticated nodes to reach agreement even in the presence of malicious actors, provided that a bounded fraction of participants is compromised (Castro & Liskov, 1999). This model aligns with regulated power system environments, where participating entities such as utilities, operators, and regulators are identifiable and governed by formal trust relationships. Ismail and Materwala (2019) observe that such consensus mechanisms achieve lower latency and higher throughput than public blockchain protocols, making them suitable for industrial use cases.

However, even lightweight consensus mechanisms introduce performance overhead that must be carefully managed in SCADA contexts. Blockchain operations such as transaction validation, block propagation, and ledger synchronisation consume network bandwidth and computational resources. In power systems, where communication networks may already be constrained, and field devices have limited processing capabilities, these overheads can impact system responsiveness. Insights from agile multi-cloud deployment models emphasise the importance of aligning system architecture with performance requirements to avoid bottlenecks and unintended dependencies (Akindemowo et al., 2022). Similar principles apply to blockchain–SCADA architectures, where consensus should be confined to supervisory or coordination layers rather than real-time control loops.

The performance implications of consensus mechanisms are not limited to latency alone. Scalability is a further constraint, particularly in large power systems with thousands of devices generating frequent data updates. High transaction volumes can overwhelm consensus processes, leading to congestion and delayed confirmation. Research on network analytics and disruption forecasting illustrates how system-wide visibility and coordination degrade when data flows exceed processing capacity (Nnabueze et al., 2022). In blockchain-assisted SCADA systems, selective data commitment strategies are therefore essential, ensuring that only critical events and summaries are subject to consensus while high-frequency telemetry remains off-chain.

Security-driven performance trade-offs also emerge when consensus mechanisms are integrated with broader cybersecurity frameworks. Adebayo (2022) highlights that threat intelligence and security monitoring systems must balance depth of analysis with operational efficiency. Blockchain-based consensus can enhance trust and forensic traceability, but excessive validation requirements may hinder timely response to incidents. Integrating blockchain outputs with real-time risk assessment dashboards, as demonstrated in regulated sectors, requires careful orchestration to ensure that security enhancements do not impede operational decision-making (Filani et al., 2022).

Human–system interaction further influences how consensus-related performance constraints are perceived and managed. Studies on interactive data visualisation show that timely and trustworthy information is essential for effective decision-making (Eboseremen et al., 2022). In SCADA environments, delays introduced by consensus processes can reduce operator confidence if system states appear outdated or inconsistent. Blockchain architectures must therefore be designed to support near-real-time visibility, even if full consensus finality is achieved asynchronously.

Broader system analogies from other domains also underscore the importance of performance-aware design. Digital twin frameworks in healthcare demonstrate that real-time data assimilation requires architectural separation between simulation, analytics, and operational control to maintain responsiveness (Omolayo et al., 2022). Similarly, blockchain consensus in power systems should support analytical and coordination functions without interfering with fast control actions. Environmental monitoring studies further reinforce that timely data processing is essential for managing complex risks, particularly in resource-constrained settings (Agyemang et al., 2022).

VII. PRIVACY, CONFIDENTIALITY, AND ACCESS CONTROL

Privacy, confidentiality, and access control are critical considerations in blockchain-assisted SCADA data exchange, particularly because power system data may reveal sensitive operational details with national security implications. While blockchain's transparency and immutability enhance trust, these same properties can conflict with confidentiality requirements if not carefully managed. In SCADA-controlled power systems, data such as network topology, load profiles, and control actions must be protected from unauthorised disclosure to prevent reconnaissance and targeted attacks.

Blockchain-based privacy preservation is typically achieved through cryptographic techniques and architectural design choices. Zyskind et al. (2015) demonstrate that decentralised access control mechanisms can be implemented on blockchain platforms by separating data storage from access permissions, allowing users to retain control over who can view or modify their data. Applied to SCADA systems, this approach enables sensitive operational data to remain off-chain or encrypted, while access policies and audit trails are recorded on-chain.

Fine-grained access control is essential in multi-stakeholder power system environments. Azaria et al. (2016) show that smart contracts can enforce role-based and attribute-based access policies, ensuring that only authorised entities can access specific data sets. In SCADA contexts, this supports differentiated access for operators, regulators, maintenance providers, and external auditors, reducing the risk of insider misuse while maintaining operational transparency.

From a scalability and performance perspective, privacy-enhancing mechanisms must not impose excessive overhead. Hou, Kang, and Guo (2020) emphasise that encryption and key management strategies must be carefully designed to support real-time data sharing in distributed systems. For power systems in developing regions such as Nigeria, where regulatory frameworks for data protection are evolving, blockchain-based access control can complement institutional safeguards by providing verifiable enforcement of privacy policies (Mbah, 2018). Overall, privacy-aware blockchain architectures enable secure SCADA data exchange while balancing transparency, confidentiality, and operational efficiency.

VIII. INTEROPERABILITY AND SCALABILITY CHALLENGES

Interoperability and scalability remain major obstacles to the widespread adoption of blockchain-assisted SCADA architectures. Power systems comprise heterogeneous devices, protocols, and legacy platforms that must coexist with emerging digital technologies. Integrating blockchain into this environment requires seamless interaction between distributed ledgers, SCADA communication protocols, and enterprise systems without disrupting operational continuity.

Interoperability challenges arise at both technical and organisational levels. Panarello et al. (2018) note that blockchain–Incompatible data models, communication standards, and middleware solutions hinder IoT integration. In SCADA environments, these issues are amplified by long equipment lifecycles and vendor-specific implementations. Achieving interoperability, therefore, demands standardised interfaces and abstraction layers that allow blockchain services to interact with diverse SCADA components.

Scalability is equally critical, as power systems generate large volumes of high-frequency data. Obaid et al. (2019) argue that interoperable blockchain systems must support horizontal scaling and cross-chain communication to avoid performance bottlenecks. For SCADA applications, this often necessitates hybrid architectures where only selected data is committed to the blockchain, while bulk telemetry is processed off-chain.

In developing regions, infrastructural and institutional factors further complicate interoperability. Studies on digital governance in Africa highlight fragmented systems and limited standardisation as persistent challenges (Ojo et al., 2019). Addressing interoperability and scalability in blockchain–SCADA systems, therefore, requires not only technical innovation but also coordinated policy and standards development to ensure sustainable integration across diverse power system contexts.

IX. CASE STUDIES AND EXPERIMENTAL IMPLEMENTATIONS

Empirical studies and pilot deployments have played a crucial role in demonstrating the practical feasibility and limitations of blockchain-assisted data exchange within power systems, particularly in contexts where decentralisation and multi-actor coordination are essential. Much of the existing empirical work has concentrated on microgrids and distributed energy systems, as these environments naturally embody the characteristics—such as peer-to-peer interaction, shared infrastructure, and distributed ownership—that blockchain technologies are designed to support. By examining such settings, researchers have been able to evaluate how blockchain can facilitate secure, transparent, and trustworthy data exchange under realistic operational conditions.

One of the most frequently cited empirical examples is the Brooklyn Microgrid project, which illustrates how blockchain can be used to support secure and transparent energy data sharing among prosumers in a local electricity network. In this case, blockchain technology was employed to record energy generation and consumption data and to support peer-to-peer energy transactions in a decentralised manner. The findings reported by Mengelkamp et al. (2018) demonstrate that blockchain-based coordination can enhance trust among participants by providing a shared, tamper-evident record of transactions. Although the primary focus of the Brooklyn Microgrid was market coordination rather than SCADA control, the project offers valuable insights into how distributed ledger technologies can support reliable data exchange across multiple autonomous actors, a requirement that is increasingly relevant for modern power systems.

Beyond microgrid-specific case studies, experimental platforms have explored the integration of permissioned blockchains with Internet of Things devices to emulate industrial and energy system environments. These platforms typically adopt consortium-based blockchain models, where participation is restricted to known and authenticated entities, thereby reflecting the governance structures common in power system operations. Chen et al. (2019) demonstrate that blockchain-based data trading and sharing frameworks can achieve acceptable performance when selective data sharing strategies are employed. By limiting on-chain data to critical events or summaries while keeping high-frequency measurements off-chain, these experimental systems are able to balance security and performance. Although such studies do not explicitly target SCADA-controlled power systems, they inform architectural decisions by illustrating how blockchain can coexist with resource-constrained devices and high-throughput data streams.

Survey-based and experimental analyses consistently reveal that most blockchain–smart grid initiatives remain at the prototype or pilot stage. Mollah et al. (2020) observe that while proof-of-concept implementations demonstrate technical feasibility, large-scale deployment is constrained by unresolved challenges related to scalability, interoperability, governance, and regulatory compliance. These limitations are particularly pronounced when blockchain solutions are extended beyond data logging or market coordination to more sensitive operational contexts such as SCADA data exchange. As a result, many experimental implementations deliberately avoid integrating blockchain into real-time control loops, instead focusing on supervisory, monitoring, or post-event analysis functions.

The geographic and institutional context in which pilot projects are deployed also has a significant influence on outcomes. In developing economies, empirical studies highlight both the potential benefits and the practical constraints of blockchain-based power system innovations. In Nigeria, for example, smart grid pilot projects illustrate how digital experimentation can improve visibility, accountability, and coordination within the power sector, while also exposing infrastructural and regulatory limitations (Ajewole et al., 2020). Limited communication infrastructure, skills gaps, and evolving regulatory frameworks can restrict the scale and sophistication of blockchain-enabled solutions. Nevertheless, these pilot initiatives provide important lessons on incremental adoption, demonstrating that blockchain-assisted data exchange can be introduced as an overlay to existing systems rather than as a disruptive replacement.

X. OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Interoperability and scalability remain major obstacles to the widespread adoption of blockchain-assisted SCADA architectures. Power systems comprise heterogeneous devices, protocols, and legacy platforms that must coexist with emerging digital technologies. Integrating blockchain into this environment requires seamless interaction between distributed ledgers, SCADA communication protocols, and enterprise systems without disrupting operational continuity.

Interoperability challenges arise at both technical and organisational levels. Panarello et al. (2018) note that blockchain–Incompatible data models, communication standards, and middleware solutions hinder IoT integration. In SCADA environments, these issues are amplified by long equipment lifecycles and vendor-specific implementations. Achieving interoperability, therefore, demands standardised interfaces and abstraction layers that allow blockchain services to interact with diverse SCADA components.

Scalability is equally critical, as power systems generate large volumes of high-frequency data. Obaid et al. (2019) argue that interoperable blockchain systems must support horizontal scaling and cross-chain communication to avoid performance bottlenecks. For SCADA applications, this often necessitates hybrid architectures where only selected data is committed to the blockchain, while bulk telemetry is processed off-chain.

In developing regions, infrastructural and institutional factors further complicate interoperability. Studies on digital governance in Africa highlight fragmented systems and limited standardisation as persistent challenges (Ojo et al., 2019). Addressing interoperability and scalability in blockchain–SCADA systems, therefore, requires not only technical innovation but also coordinated policy and standards development to ensure sustainable integration across diverse power system contexts.

CONCLUSION

This study has systematically addressed its stated aims by providing a comprehensive and critical examination of blockchain-assisted secure data exchange architectures for SCADA-controlled power systems. Through an extensive synthesis of interdisciplinary literature spanning power system engineering, cybersecurity, and distributed ledger technologies, the review has clarified how blockchain can be positioned as a complementary trust layer rather than a replacement for existing SCADA infrastructures. In doing so, it has met its objective of identifying the architectural, technical, and governance dimensions through which blockchain can mitigate long-standing vulnerabilities in SCADA data exchange.

Key findings from the study demonstrate that traditional SCADA communication architectures, while effective for deterministic control, are increasingly inadequate in addressing modern cybersecurity threats, inter-organisational data sharing requirements, and accountability demands. The review has shown that blockchain-enabled architectures offer tangible benefits in terms of data integrity, auditability, non-repudiation, and decentralised trust, particularly when implemented using permissioned and hybrid on-chain/off-chain models. These approaches align well with the performance and regulatory constraints of power systems, provided that blockchain operations are confined to supervisory, coordination, and auditing layers rather than real-time control loops. The analysis further reveals that consensus mechanisms, privacy-preserving techniques, and access control frameworks are decisive factors in determining the feasibility of blockchain–SCADA integration. Empirical evidence from pilot projects and experimental implementations underscores that context-aware design, selective data commitment, and robust governance structures are essential for operational viability, especially in developing regions where infrastructural and institutional constraints persist. The study also highlights that interoperability, scalability, and human capacity remain significant challenges that must be addressed to enable large-scale deployment.

Based on these findings, the study concludes that blockchain-assisted secure data exchange represents a promising yet nuanced pathway for enhancing the resilience and trustworthiness of SCADA-controlled power systems. It recommends future research to focus on standardisation efforts, performance-optimised consensus protocols, and the integration of blockchain with advanced analytics and artificial intelligence for predictive security and system optimisation. Additionally, policy-oriented research and capacity-building initiatives are recommended to support adoption in diverse regulatory and socio-economic contexts. Collectively, these recommendations position blockchain not as a panacea, but as a strategically valuable component of next-generation secure power system architectures.

REFERENCES

[1] Abubakar, A.M., Elrehail, H., Alatailat, M.A., and Elçi, A. (2019). Knowledge management, decision-making style, and organizational performance. Journal of innovation & knowledge, 4(2), pp.104-114. https://doi.org/10.1016/j.jik.2017.07.003

[2] Adebayo, A. (2022) ‘Leveraging threat intelligence in DevSecOps for enhanced banking security’, International Journal of Scientific Research and Modern Technology, 1, pp. 1–4.

[3] Agyemang, J., Gyimah, E., Ofori, P., Nimako, C. and Akoto, O. (2022) ‘Pollution and health risk implications of heavy metals in the surface soil of Asafo auto-mechanic workshop in Kumasi,

Ghana', Chemistry Africa, 5(1), pp. 189–199. Available at: https://doi.org/10.1007/s42250-021-00297-x

[4] Ahl, A., Yarime, M., Tanaka, K. and Sagawa, D. (2019). Review of blockchain-based distributed energy: Implications for institutional development. Renewable and Sustainable Energy Reviews, 107, pp.200-211. https://doi.org/10.1016/j.rser.2019.03.002

[5] Ajewole, T.O., Olabode, O.E., Babalola, O.S., and Omoigui, M.O. (2020). Use of experimental test systems in the application of electric microgrid technology across sub-Saharan Africa: A review. Scientific African, 8, p.e00435. https://doi.org/10.1016/j.sciaf.2020.e00435

[6] Akindemowo, A.O., Erigha, E.D., Obuse, E., Ajayi, J.O., Adebayo, A., Afuwape, A.A., and Adanyin, A. (2021). A Conceptual Framework for Automating Data Pipelines Using ELT Tools in Cloud-Native Environments. Journal of Frontiers in Multidisciplinary Research, 2(1), pp.440-452. https://doi.org/10.54660/.JFMR.2021.2.1.440-452

[7] Akindemowo, A.O., Erigha, E.D., Obuse, E., Ajayi, J.O., Soneye, O.M. and Adebayo, A. (2022) 'A conceptual model for agile portfolio management in multi-cloud deployment projects', International Journal of Computer Science and Mathematical Theory, 8(2), pp. 64–93.

[8] Alcaraz, C. and Zeadally, S. (2015) 'Critical infrastructure protection: Requirements and challenges for the 21st century', International Journal of Critical Infrastructure Protection, 8, pp. 53–66. Available at: https://doi.org/10.1016/j.ijcip.2014.12.002

[9] Amin, S., Schwartz, G.A., and Hussain, A. (2013). In the quest for benchmarking security risks to cyber-physical systems. IEEE Network, 27(1), pp.19-24. DOI: 10.1109/MNET.2013.6423187

[10] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., and Peacock, A. (2019) 'Blockchain technology in the energy sector: A systematic review of challenges and opportunities', Renewable and Sustainable Energy Reviews, 100, pp. 143–174. Available at: https://doi.org/10.1016/j.rser.2018.10.014

[11] Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. (2016) 'MedRec: Using blockchain for medical data access and permission management', IEEE Open & Big Data Conference, pp. 25–30. https://doi.org/10.1109/OBD.2016.11

[12] Bukhari, T.T., Moyo, T.M., Tafirenyika, S., Taiwo, A.E., Tuboalabo, A., and Ajayi, A.E. (2022). AI-Driven Cybersecurity Intelligence Dashboards for Threat Prevention and Forensics in Regulated Business Sectors. https://doi.org/10.54660/IJMER.2022.3.2.01

[13] Cardenas, A.A., Amin, S., and Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. In 2008 The 28th International Conference on Distributed Computing Systems Workshops (pp. 495-500). IEEE. DOI: 10.1109/ICDCS.Workshops.2008.40

[14] Castro, M. and Liskov, B., (1999). Practical Byzantine fault tolerance. In OsDI (Vol. 99, No. 1999, pp. 173-186).

[15] Cheminod, M., Durante, L. and Valenzano, A. (2013) 'Review of security issues in industrial networks', IEEE Transactions on Industrial Informatics, 9(1), pp. 277–293. https://doi.org/10.1109/TII.2012.2198666

[16] Chen, C., Wu, J., Lin, H., Chen, W., and Zheng, Z. (2019). A secure and efficient blockchain-based data trading approach for internet of Vehicles. IEEE Transactions on Vehicular Technology, 68(9), pp.9110-9121. DOI: 10.1109/TVT.2019.2927533

[17] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016) 'A review of cyber security risk assessment methods for SCADA systems', Computers & Security, 56, pp. 1–27. https://doi.org/10.1016/j.cose.2015.09.009

[18] Christidis, K. and Devetsikiotis, M. (2016) 'Blockchains and smart contracts for the Internet of Things', IEEE Access, 4, pp. 2292–2303. Available at: https://doi.org/10.1109/ACCESS.2016.2566339

[19] East, S., Butts, J., Papa, M., and Shenoi, S. (2009), March. A Taxonomy of Attacks on the DNP3 Protocol. In International Conference on Critical Infrastructure Protection (pp. 67-81).

Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-04798-5_5

[20] Eboseremen, B., Adebayo, A., Essien, I., Afuwape, A., Soneye, O., and Ofori, S. (2021) 'The role of natural language processing in data-driven research analysis', International Journal of Multidisciplinary Research and Growth Evaluation, 2(1), pp. 935–942.

[21] Eboseremen, B., Adebayo, A., Essien, I., Ofori, S. and Soneye, O. (2022) 'The impact of interactive data visualizations on public policy decision-making', International Journal of Multidisciplinary Research and Growth Evaluation, 3(1), pp. 1189–1203. https://doi.org/10.54660/.IJMRGE.2022.3.1.1189-1203

[22] Eneh, J.N., Orah, H.O., and Emeka, A.B. (2019), August. Improving the reliability and security of active distribution networks using SCADA systems. In 2019, IEEE PES/IAS PowerAfrica (pp. 110-115). IEEE. https://doi.org/10.1109/PowerAfrica.2019.8928647

[23] Fadok, D.S., (2011). Cyber War: The Next Threat to National Security and What to Do about It. https://www.jstor.org/stable/26270542

[24] Filani, O.M., Nnabueze, S.B., Ike, P.N. and Wedraogo, L. (2022) 'Real-time risk assessment dashboards using machine learning in hospital supply chain management systems', International Journal of Modern Engineering Research, 3(1), pp. 65–76. Available at: https://doi.org/10.54660/IJMER.2022.3.1.65-76

[25] Frempong, D., Ifenatuora, G.P. and Ofori, S.D. (2020) 'AI-powered chatbots for education delivery in remote and underserved regions', International Journal of Future Medical Research, 1(1), pp. 156–172. https://doi.org/10.54660/.IJFMR.2020.1.1.156-172

[26] Gado, P., Gbaraba, S.V., Adeleke, A.S., Anthony, P., Ezeh, F.E., Tafirenyika, S. and Moyo, T.M. (2020) 'Leadership and strategic innovation in healthcare: lessons for advancing access and equity', International Journal of Multidisciplinary Research and Growth Evaluation, 1(4), pp. 147–165.

[27] Gado, P., Gbaraba, S.V., Adeleke, A.S., Anthony, P., Ezeh, F.E., Moyo, T.M., and Tafirenyika, S. (2022) 'Streamlining patient journey mapping: a systems approach to improving treatment persistence', International Journal of Multidisciplinary Futuristic Development, 3(2), pp. 38–57. https://doi.org/10.54660/IJMFD.2022.3.2.38

[28] Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C. and Hancke, G.P. (2011) 'Smart grid technologies: Communication technologies and standards', IEEE Transactions on Industrial Informatics, 7(4), pp. 529–539. https://doi.org/10.1109/TII.2011.2166794

[29] Haruna, A., Mohammed, A.D., Abisoye, O.A., and Solomon, A.A. (2022). A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication.

[30] Hou, M., Kang, T., and Guo, L. (2020), March. A blockchain-based architecture for IoT data sharing systems. In 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 1-6). IEEE. https://doi.org/10.1109/PerComWorkshops48775.2020.9156107

[31] Humayed, A., Lin, J., Li, F. and Luo, B. (2017) 'Cyber-physical systems security—A survey', IEEE Internet of Things Journal, 4(6), pp. 1802–1831. Available at: https://doi.org/10.1109/JIOT.2017.2703172

[32] Igure, V.M., Laughter, S.A. and Williams, R.D. (2006) 'Security issues in SCADA networks', Computers & Security, 25(7), pp. 498–506. https://doi.org/10.1016/j.cose.2006.03.001

[33] Ike, P.N., Aifuwa, S.E., Nnabueze, S.B., Olatunde-Thorpe, J., Ogbuefi, E., Oshoba, T.O., and Akokodaripon, D. (2020) 'Utilizing nanomaterials in healthcare supply chain management for improved drug delivery systems', Medicine, 12, p. 13. Available at: https://doi.org/10.62225/2583049X.2024.4.4.5154

[34] Ismail, L. and Materwala, H., (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry, 11(10), p.1198. https://doi.org/10.3390/sym11101198

[35] Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015) 'A survey of cyber

security management in industrial control systems', International Journal of Critical Infrastructure Protection, 9, pp. 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

[36] Kshetri, N. (2017) 'Can blockchain strengthen the internet of things?', IT Professional, 19(4), pp. 68–72. https://doi.org/10.1109/MITP.2017.3051335

[37] Kuponiyi, A. and Akomolafe, O.O. (2022) 'A digital health framework for expanding access to preventive services in marginalized communities', International Journal of Advanced Multidisciplinary Research and Studies, 9(1).

[38] Langner, R. (2011) 'Stuxnet: Dissecting a cyberwarfare weapon', IEEE Security & Privacy, 9(3), pp. 49–51. https://doi.org/10.1109/MSP.2011.67

[39] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., and Liu, S. (2018). Blockchain-based data preservation system for medical data. Journal of Medical Systems, 42(8), p.141. https://doi.org/10.1007/s10916-018-0997-3

[40] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q. and Zhang, Y. (2017) 'Consortium blockchain for secure energy trading in industrial internet of things', IEEE Transactions on Industrial Informatics, 14(8), pp. 3690–3700. https://doi.org/10.1109/TII.2017.2786307

[41] Mbah, G.O., (2018). Advancing data protection in Nigeria: the need for comprehensive legislation. Int J Eng Technol Res Manag, 2(12), p.108.

[42] Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L. and Weinhardt, C. (2018) 'Designing microgrid energy markets: A case study: The Brooklyn Microgrid', Applied Energy, 210, pp. 870–880. https://doi.org/10.1016/j.apenergy.2017.06.054

[43] Mo, Y., Chabukswar, R. and Sinopoli, B. (2012) 'Detecting integrity attacks on SCADA systems', IEEE Transactions on Control Systems Technology, 22(4), pp. 1396–1407. https://doi.org/10.1109/TCST.2013.2280899

[44] Mollah, M.B., Zhao, J., Niyato, D., Lam, K.Y., Zhang, X., Ghias, A.M., Koh, L.H. and Yang, L., (2020). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things journal, 8(1), pp.18-43. DOI: 10.1109/JIOT.2020.2993601

[45] Mollah, M.B., Zhao, J., Niyato, D., Lam, K.Y., Zhang, X., Ghias, A.M., Koh, L.H. and Yang, L., (2020). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things journal, 8(1), pp.18-43. DOI: 10.1109/JIOT.2020.2993601

[46] Moyo, T.M., Taiwo, A.E., Ajayi, A.E., Tafirenyika, S., Tuboalabo, A. and Bukhari, T.T. (2021) 'Designing smart BI platforms for government healthcare funding transparency and operational performance improvement', International Journal of Multidisciplinary Engineering Research, 2(2), pp. 41–51. Available at: https://doi.org/10.54660/IJMER.2021.2.2.41-51

[47] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[48] Nnabueze, S.B., Ike, P.N., Olatunde-Thorpe, J., Aifuwa, S.E., Oshoba, T.O., Ogbuefi, E. and Akokodaripon, D. (2021) 'End-to-end visibility frameworks improving transparency, compliance, and traceability across complex global supply chain operations', International Journal of Multidisciplinary Finance and Development, 2(2), pp. 50–60. https://doi.org/10.54660/IJMFD.2021.2.2.50-60

[49] Nnabueze, S.B., Ike, P.N., Olatunde-Thorpe, J., Aifuwa, S.E., Oshoba, T.O., Ogbuefi, E. and Akokodaripon, D. (2022) 'Supply chain disruption forecasting using network analytics', International Journal of Futuristic Multidisciplinary Research, 3(2), pp. 193–203. https://doi.org/10.54660/.IJFMR.2022.3.2.193-203

[50] Obaid, Z.A., Cipcigan, L.M., Abrahim, L., and Muhssin, M.T. (2019). Frequency control of future power systems: reviewing and evaluating challenges and new control methods. Journal of Modern Power Systems and Clean Energy, 7(1), pp.9-25. DOI: 10.1007/s40565-018-0441-1

[51] Ofori, P., Asamoah, G., Amoah, B., Agyeman, K.O.A. and Yeboah, E. (2021) 'Combined application of poultry litter biochar and NPK fertilizer improves cabbage yield and soil chemical properties', Open Agriculture, 6(1), pp. 356–368.

[52] Ogundari, I., Otuyemi, F., Momodu, A., and Salu, L. (2020). Cybersecurity assessment of Nigeria's electric power infrastructure. African

Journal of Science Policy and Innovation Management, 1(2), pp.87-104. https://ajspim.oauife.edu.ng/index.php/ajspim/article/view/79

[53] Ogunleye, G.A. and Adeyemo, I.A. (2021). ‘Digital infrastructure and cybersecurity readiness in Nigeria’s power sector’, African Journal of Information and Communication, 27, pp. 1–18.

[54] Ojo, A., Janowski, T., and Estevez, E. (2019). ‘Digital government and interoperability in Africa’, Government Information Quarterly, 36(4), p. 101389.

[55] Okoye, N.J., Onuoha, O.C., and Udemadu, F.C. (2022). Influence Of Fraud And Corruption On Stock Value Traded InThe Capital Market: Nigeria Experience. European Journal of Economic and Financial Research, 6(4). https://oapub.org/soc/index.php/EJEFR/article/view/1390

[56] Omolayo, O., Aduloju, T.D., Okare, B.P., and Taiwo, A.E. (2022) ‘Digital twin frameworks for simulating multiscale patient physiology in precision oncology: A review of real-time data assimilation’, Predictive Tumor Modeling and Clinical Decision Interfaces.

[57] Otuoze, A.O., Mustafa, M.W., Ibrahim, O., Salisu, S., Mohammed, O.O., Oloyede, A.A., and Gaya, Z.S. (2019). Threats and Challenges of Smart Grids Deployments-A Developing Nationsâ€™ Perspective. ELEKTRIKA-Journal of Electrical Engineering, 18(2), pp.33-43.

[58] Panarello, A., Tapas, N., Merlino, G., Longo, F. and Puliafito, A. (2018) ‘Blockchain and IoT integration: A systematic survey’, Sensors, 18(8), p. 2575. https://doi.org/10.3390/s18082575

[59] Pop, C., Antal, M., Cioara, T., Anghel, I., Sera, D., Salomie, I., Raveduto, G., Ziu, D., Croce, V. and Bertoncini, M. (2019). Blockchain-based, scalable, and tamper-evident solution for registering energy data. Sensors, 19(14), p.3033. https://doi.org/10.3390/s19143033

[60] Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L. (2019) ‘Blockchain technology and its relationships to sustainable supply chain management’, International Journal of Production Research, 57(7), pp. 2117–2135. Available at: https://doi.org/10.1080/00207543.2018.1533261

[61] Salawu, A. ed. (2018). African language digital media and communication. London: Routledge.

[62] Shaik, M., Sadhu, A.K.R. and Venkataramanan, S., (2019). Unveiling the Achilles' Heel of Decentralized Identity: A Comprehensive Exploration of Scalability and Performance Bottlenecks in Blockchain-Based Identity Management Systems. 2019.

[63] Sridhar, S., Hahn, A. and Govindarasu, M. (2012) ‘Cyber–physical system security for the electric power grid’, Proceedings of the IEEE, 100(1), pp. 210–224. DOI: 10.1109/JPROC.2011.2165269

[64] Stamp, J., Dillinger, J., Young, W., and DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories.

[65] Stouffer, K., Falco, J., and Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), pp.16-16.

[66] Ten, C.W., Manimaran, G., and Liu, C.C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(4), pp.853-865. DOI: 10.1109/TSMCA.2010.2048028

[67] Yan, Y., Qian, Y., Sharif, H. and Tipper, D. (2012) ‘A survey on smart grid communication infrastructures: Motivations, requirements and challenges’, IEEE Communications Surveys & Tutorials, 15(1), pp. 5–20. https://doi.org/10.1109/SURV.2012.021312.00034

[68] Yeboah, B.K. and Ike, P.N. (2020). Programmatic strategy for renewable energy integration: Lessons from large-scale solar projects. International Journal of Multidisciplinary Research and Growth Evaluation, 1(3), pp.306-315. https://doi.org/10.54660/.IJMRGE.2020.1.3.306-315

[69] Zheng, Z., Xie, S., Dai, H.N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), pp.352-375. https://doi.org/10.1504/IJWGS.2018.095647

[70] Zyskind, G. and Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015, IEEE Security and Privacy Workshops (pp. 180-184). IEEE. DOI: 10.1109/SPW.2015.27