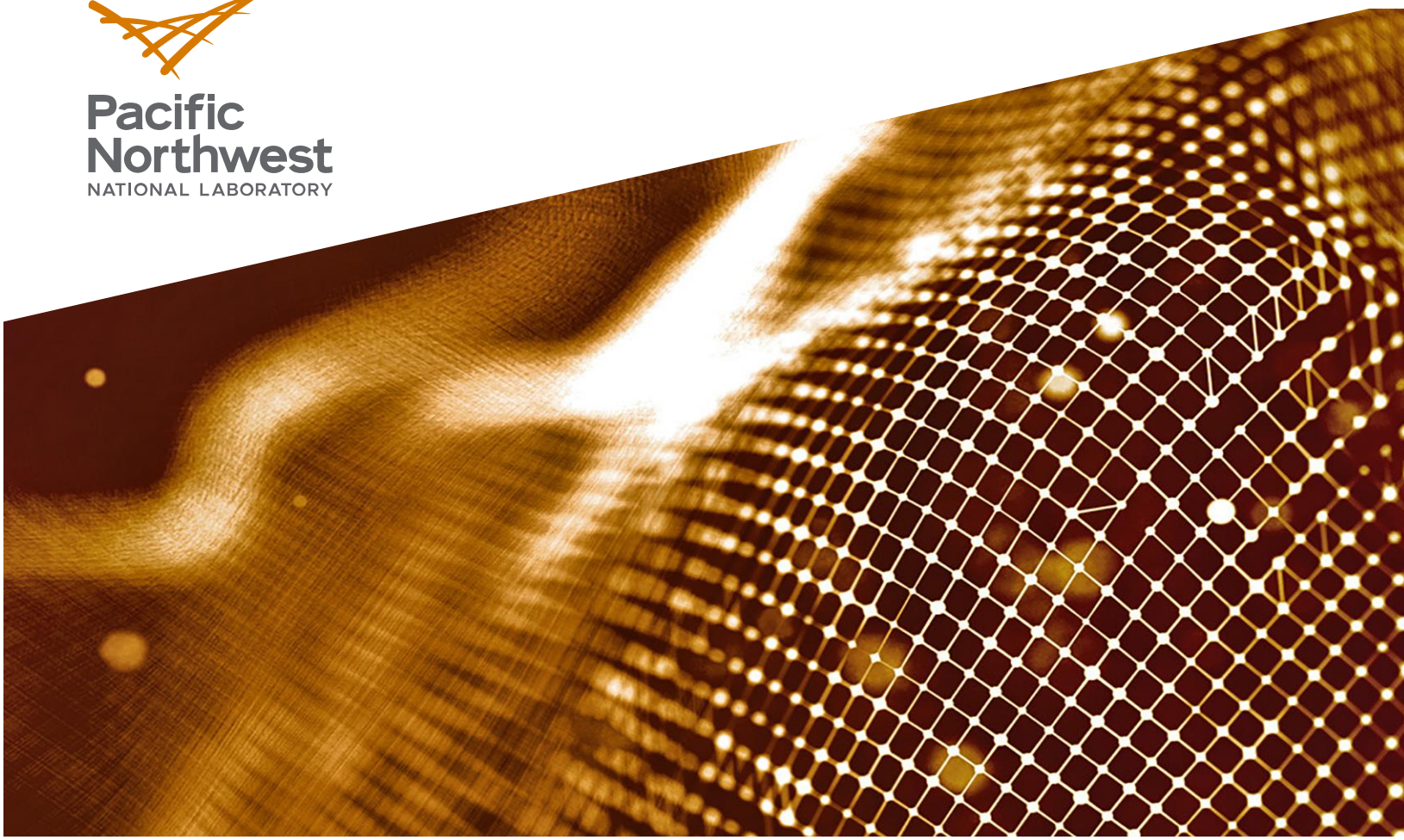
Pacific Northwest
NATIONAL LABORATORY



PNNL-32289

Blockchain for Fault-Tolerant Grid Operations

December 2021

Bishnu Bhattarai, David J Sebastian Cardenas, Fernando Bereta dos Reis, Monish Mukherjee, Sri Nikhil Gupta Gourisetti

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-32289

Blockchain for Fault-Tolerant Grid Operations

December 2021

Bishnu Bhattarai, David J Sebastian Cardenas, Fernando Bereta dos Reis, Monish Mukherjee, Sri Nikhil Gupta Gourisetti

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

Distribution systems are more likely to have faults in comparison to transmission and generation systems. Most distribution systems have a radial design. The radial design results in the disconnection of customers for any given component failure. To maintain and improve the distribution system's fault tolerance for a grid with high penetration of distributed energy resources novel solutions are required. Blockchain can add value to improve fault-tolerant grid operations. That can be achieved using blockchain's core features of distributed consensus-based decision-making process and immutability. In the process of preparing for an event or system restoration, there is a need for reliable data and system situational awareness. The system situational awareness enables accurate planning for possible scenarios and system restoration after an event, an area where blockchain's distributed architecture can help. The value of blockchain for a fault-tolerant grid operation is elaborated with three use cases: 1) data configuration; 2) topology identification; and 3) fault location, isolation, and service restoration. The proposed use cases demonstrate the use of blockchain smart contracts to support a distributed implementation of fault-tolerant algorithms. Blockchain's immutable distributed ledger and execution capabilities can increase situational awareness during an event and facilitate improved fault tolerance of the overall system through consensus mechanisms that are integrated into Blockchain technology. Fault-handling algorithms such as fault location, isolation, and service restoration are highly dependent on the system situational awareness. The use cases demonstrate how blockchain-based architecture can facilitate addressing the existing limitations of present implementations.

Acknowledgments

This project was supported by the Department of Energy, Office of Electricity, Advanced Grid Research and Development Program. The authors would like to thank Chris Irwin and Ryan Knapp for their support of this study.

Acronyms and Abbreviations

DER	distributed energy resource
DMS	distribution management system
DSO	distribution system operator
FLISR	fault location, isolation, and service restoration
IoT	Internet of Things
OMS	outage management system
SCADA	supervisory control and data acquisition

Contents

Figures

Tables

1.0 Introduction

The power distribution system is a critical segment of the overall power delivery system that has direct impact on customers. Unlike the transmission system which is typically planned for N-1 or N-2 contingencies (systems capable of handling failure of one or two simultaneous components), the distribution system has limited contingency capabilities due to its radial nature. Thus, there is a larger likelihood a failure on any single piece of equipment will lead to customer disconnection when compared to a single failure occurring in the transmission system. Since the majority of distribution systems are conventionally designed with a radial structure, the failure of a single component in such segments often results in the loss of power to downstream customers. More importantly, distribution systems have the highest concentration of faults compared to the transmission and generation systems.

The increased penetration of distributed energy resources (DERs) can add additional challenges to utilities as the conventional protection system designed for the distribution system may not work due to grid changes that will impact the traditional unidirectional power flow. For instance, most of the existing protection systems are designed based on radial network topology with unidirectional power flow, which is not always the case with high penetration of DERs. In addition, the fault current contributions from such large numbers of DERs can result in lower overall fault current on the feeder impacting overcurrent protection schemes and the ability to identify and isolate faults.

Electric utilities currently design their protection system such that a protective device closest to the fault location in a distribution system provides the first line of defense (primary protection) against the fault. In case the primary protection fails to respond to the fault, backup protection, the next nearest protective device from the fault location, responds. In both cases, the protective devices are preconfigured with proper settings, so they respond locally to fault conditions based on the preset protection settings. Since the increased penetration of DERs leads to increased system dynamics (e.g., variability in the state of DERs such as photovoltaics and batteries results in increased dynamics in the distribution system), protective settings need to be updated to reflect both the operational as well as topological changes in the distribution system.

Currently, utilities receive information from supervisory control and data acquisition (SCADA) to the centralized control center and the distribution management system (DMS) makes a sequence of decisions for locating faults (using SCADA measurements and an operational grid model), isolates faults via switching commands, and restores the system. The existing centralized implementation of SCADA and DMS for fault location, isolation, and service restoration (FLISR) or centralized FLISR implementation leads to a single point of failure for data-driven faults or loss of communication. Therefore, there is a strong need for an innovative solution to prevent and ride through the faults in a distributed manner. Blockchain is one of the technologies that can add value to maintain fault-tolerant grid operations via its core features: a distributed consensus-based decision-making process and immutability.

1.1 Study Objectives

The overall goal of this study is to identify the role blockchain can play in ensuring improved fault-tolerant grid operations. The specific study objectives include:

- Catalog existing and emerging fault and failure modes in the distribution system

- Determine the functional requirements to maintain fault-tolerant distribution system operations
- Identify the blockchain value proposition in maintaining fault-tolerant distribution system operations
- Prepare a roadmap for blockchain application in fault-tolerant grid operations.

1.2 Study Approach

This section describes the overall study process and structure as well as the breadth of investigation of blockchain for fault-tolerant distribution system operations. As shown in Figure 1, the study has three major phases. The first phase is focused on understanding and capturing (a) different types of fault and failure modes in the distribution system, (b) existing utility practices in terms of handling such faults and failures modes, and (c) potential room for improvement. The first phase starts with the literature review to categorize existing and emerging distribution system faults and ends with a set of potential areas for improvement.

The second phase is focused mostly on the functional requirements to mitigate and tolerate common distribution system faults and failures. Since every fault and failure mode brings unique issues and challenges, identifying the functional requirements to address such faults will help to generalize the solution approach.

The last phase is primarily focused on identifying the value proposition blockchain brings to fault-tolerant grid operations. This section ends with three proposed use cases where blockchain can add value in terms of maintaining the fault-tolerant grid operations.

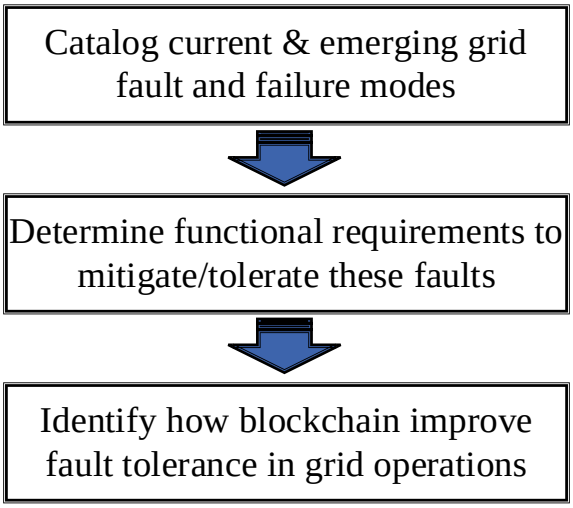


Figure 1. Overall study approach.

1.3 Report Structure

The remainder of the report is structured as follows. Section 2.0 presents an overview of the distribution system operation under existing and emerging grid fault and failure modes. This chapter will also provide functional requirements for the system operator to achieve fault-tolerant grid operations. Section 3.0 presents the application of blockchain in distribution system operations. While this chapter provides an overview of the blockchain for distribution system

operations, it also focuses on how blockchain functionally helps distribution system operations under fault conditions. Section 4.0 provides the overall solution space for the application of blockchain in distribution system operations and detailed specific use cases where blockchain adds value in terms of making the distribution system operation fault-tolerant. Finally, Section 5.0 presents conclusions and future work.

2.0 Distribution System Operation Under Existing and Emerging Grid Faults

The power distribution system acts as the final stage of the delivery of electric power to millions of customers (residential, commercial, and industrial). In contrast to their transmission counterparts, distribution networks are designed with radial structures with branches and tapped laterals to facilitate electricity delivery to end users. These radial distribution networks, dispersing over vast rural and urban areas, are vulnerable to different types of faults initiated by sources such as adverse weather conditions, natural disasters, vegetation growth, equipment failure, and even malicious attacks.[1] These faults and outages affect the quality of electricity delivered to the customers in terms of service continuity and disturbance propagation. Power distribution systems have the highest concentration of faults and are often characterized by the largest number of faults among the generation, transmission, and distribution systems. Almost, 80% of all customer interruptions are caused by faults and outages in distribution networks.[2]

Moreover, the existing distribution systems are often not designed to handle N-1 or N-2 contingency scenarios. Therefore, any fault or failure of a single component in a radial segment often results in the loss of power to the downstream customers. As quality of service has emerged as an important criterion for customers, improving quality indices continues to be a significant driver in order to be competitive in the existing electric open market and avoid regulator-imposed penalties. Furthermore, maintaining more stringent regulatory mandates, supporting customer needs for high-availability power, and remaining relevant in an increasingly competitive electric service provider market is also driving utilities to look for improved reliability.

With the increased penetrations of utility-owned and nonutility-owned DERs in the distribution system, the number of faults could potentially increase or remain at the same level due to significantly larger numbers of connected devices managed by independent entities and as the mechanism to handle faults becomes more complex. Furthermore, the overall observability and substation-level situational awareness mechanisms may need to be augmented to accommodate such complex multi-owner ecosystem. This is because most of the existing protection systems in distribution systems are designed based on radial network topology and unidirectional power flow assumptions, which are not always valid when the penetration of the DERs increases. In addition, the fault current contributions from such large numbers of DERs impose challenges for the utilities to identify and isolate the faults. Therefore, understanding the spectrum of existing and emerging distribution system faults is very important to ensure fault-tolerant operations of the feeder. This section presents an overview of distribution system fault types, causes of those faults, and the functional requirements for the distribution system operators to prevent or ride through those faults.

2.1 Existing and Emerging Distribution System Faults

While a major share of customer interruptions (~80%) are caused by faults and outages in distribution networks, the nature of faults and their cause can vary significantly from one region to others and from one climate zone to another climate zone. Figure 2 presents a breakdown of various causes to distribution system faults based on feeder-level data captured through ~300 outage events recorded by five utilities in the United States.

[1] Bompard, Ettore, et al. "Classification and trend analysis of threats origins to the security of power systems." International Journal of Electrical Power & Energy Systems 50 (2013): 50-64.
[2] Gonen, Turan. Electric power distribution engineering. CRC press, 2015.

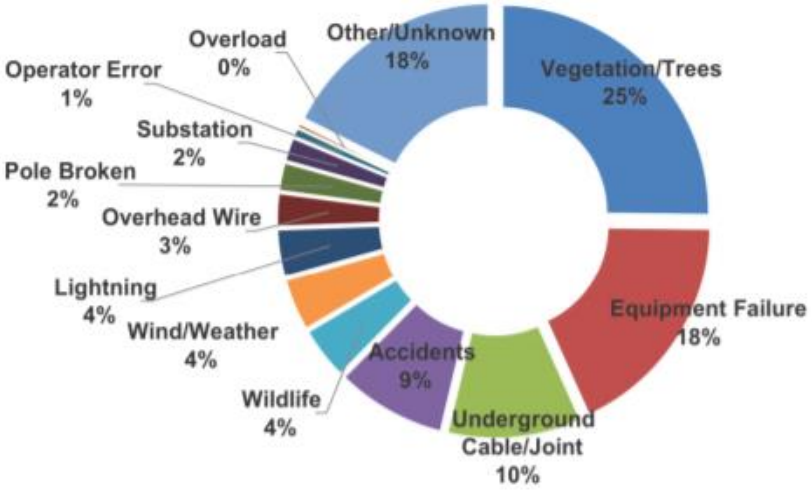


Figure 2. Cause of distribution system faults[3].

Figure 2 presents a statistical analysis of the distribution system events that lead to service disconnections. Interpreting the statistical analysis, system operations are often directly related to the events (e.g., lack of preventive maintenance and vegetation control). These faults can be broadly categorized by one or a combination of the following based on their cause of origin:

Natural causes: Faults due to physical damage of grid infrastructure due to natural events.

Technical and operational errors: Faults due to operational malfunctioning of equipment, monitoring/control system, or human error.

Attacks: Damage to supporting infrastructure due to malicious attack on the physical or the cyber system.

Table 1 presents example distribution system faults along with possible outcomes classified according to their cause.[3]

[3] "Fault location, isolation, and service restoration technologies reduce outage impact and duration smart grid investment grant program," tech. rep., Electricity Delivery & Energy Reliability, U.S. Department of Energy, Dec 2014

Table 1. Categorizing distribution system faults based on causes.

Causes	Examples	Possible Impacts
Natural Causes	Earthquake	Severe damage to equipment/installations (lines, outdoor substations, power units, etc.) and control centers.
	Heat/cold wave	Adverse operating conditions for equipment and maintaining power balance due by decreased generation or increased demand.
	Wildfire	Damage to power systems equipment/installations (lines, substations, power plants, power units, communication sites) and control centers.
	Cyclone/ thunderstorm	Severe damage to overhead lines, outdoor substations, power plants, power units, and communication sites.
Technical and Operational Errors	Design error	Errors in the stages of system planning or decision-making systems leading to overloading of transformers, line overloads, and faults.
	Operational mistake	Human error in executions or commands during real-time operation leading to cascading outages and blackouts.
	Technical failure	Equipment breakdown due to internal factors leading to loss of system functionality and unexpected faults leading to customer outages.
	Human/animal interference	External intervention causing electrical arc ignition or short circuit leading to equipment breakdown, tripping, and accidental outages.
Attacks	Sabotage	Intentional physical damage to equipment, such as the sniper attack in April of 2013 on the Metcalf substation in southern California.[4]
	Theft	Theft of equipmen such as transformers and copper or metal items from overhead lines leading to loss of system functionality.
	Insider threat	Insider with access, exploiting the vulnerabilities of the system to trigger outages or cause grid deadlocks.
	War act	A military attack on the system to completely disable its functionality.
	Malware	Software designed to disrupt operation, gather information, or gain unauthorized access leading to prolonged outages or blackouts.
	Hacking	Hacking into cyber system to control power system with the intention of destroying the desired state causing a loss of system functionality.

Most behind-the-meter DERs are not visible to operators and many operators have reported reduced visibility with the proliferation of DERs[5]. However, the combination of DERs and the Internet of Things (IoT)-enabled devices with appropriate secure communications, along with the rollout of smart metering, offers the promise of increased observability, visibility, and controllability of distribution systems. However, DERs also introduce new vulnerabilities to the system, which may lead to an increased number of emerging data-driven faults in the future power distribution system. Those data-driven faults often include any malicious attempt to incorrectly operate monitoring, control, or even trigger traditional protection systems, leading to outages. These DERs and IoT devices are often less secure, making them easy access points

[4] Smith, R. "Assault on California power station raises alarm on potential for terrorism. Wall Street J." (2014).
[5] Smith, Jeff, et al. "It's all in the plans: Maximizing the benefits and minimizing the impacts of DERs in an integrated grid." IEEE Power and Energy Magazine 13.2 (2015): 20-29.

for adversaries to design coordinated attacks. The majority of the conventional fault-handling techniques were not designed to effectively handle such data-driven faults. While the frequency of such data-driven and natural disaster faults is low, their impact can be significant. Figure 3 illustrates the degree of damage due to different types of faults.

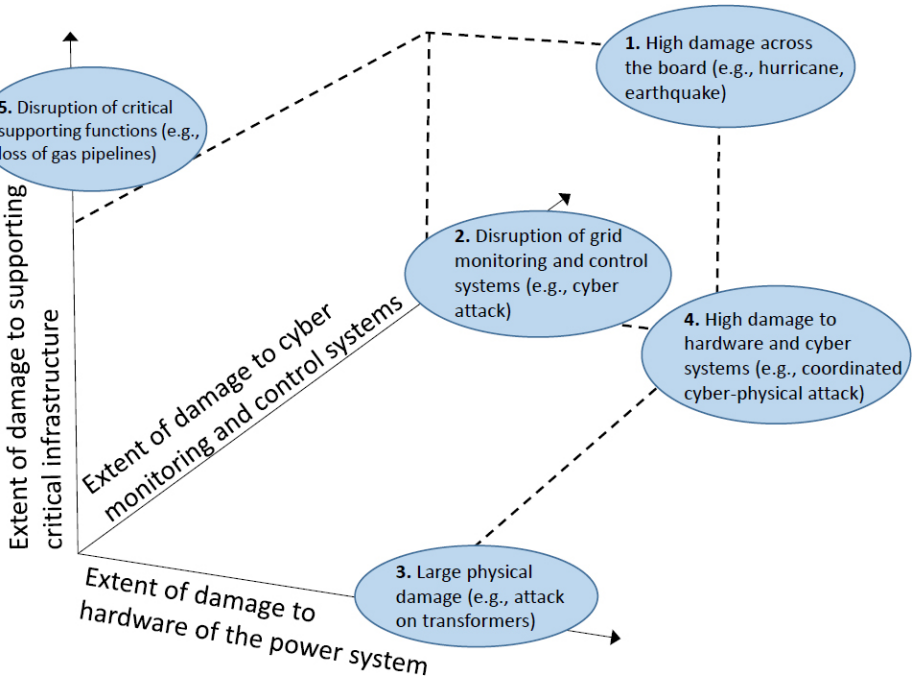


Figure 3. Degree of damage due to different grid faults.[6]

2.2 Functional Requirements to Mitigate and Tolerate Faults

This section identifies how utilities currently deal with fault conditions and presents insights in terms of what is needed to make the power distribution system fault-tolerant to both existing and emerging faults. Traditionally, an outage management system (OMS) is employed by the utility that works in conjugation with multiple other subsystems belonging to the DMS to facilitate with operations and control decisions during outages. Figure 4 shows the architecture of a typical OMS, along with interconnection of different levels of distribution automation connected to it. During a fault event, the OMS collects measurements from SCADA and the advanced metering infrastructure, along with outage reports from the customer information system and the interactive voice response system.

[6] Academies of Sciences, Engineering, and Medicine 2017. Enhancing the Resilience of the Nation's Electricity System. Washington, DC: The National Academies Press. https://doi.org/10.17226/24836

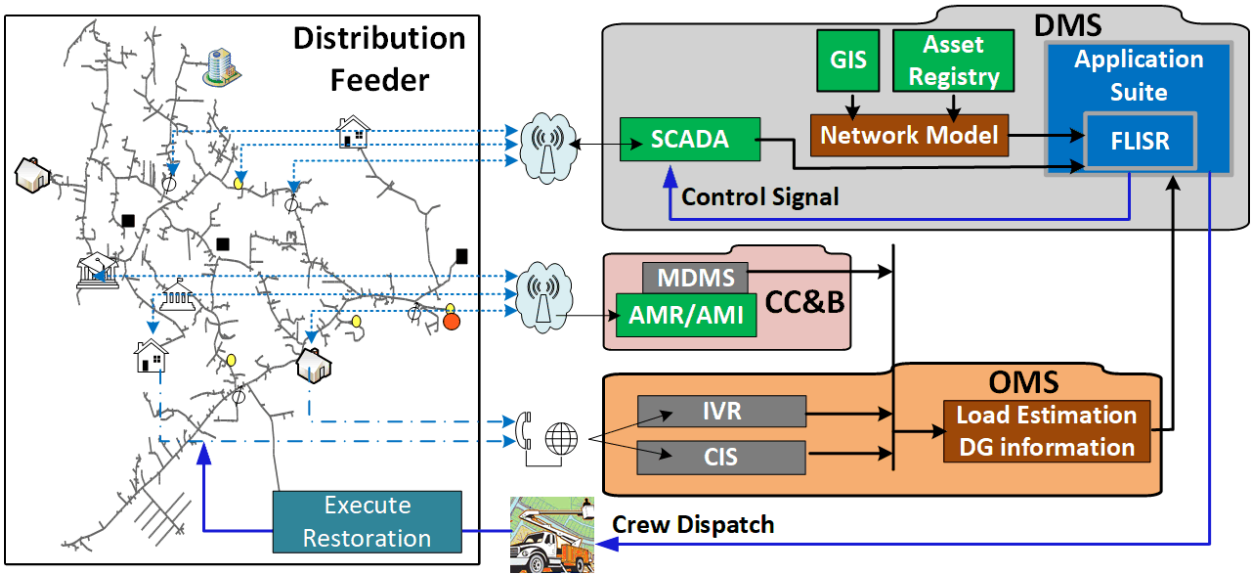


Figure 4. Architecture of a typical OMS along with the information flow.

FLISR systems involve coordinated operation of automated feeder switches and reclosers, communication networks, DMS, OMS, and SCADA to automate power restoration during faults, reducing both the impact and length of power interruptions. Figure 5 illustrates the sequential operations of FLISR systems, starting with locating the fault based on sensor measurements, isolating the faulted sections through appropriate switching operations, and finally re-energizing non-faulted portion(s) of the feeder to restore customer service. Although automated recovery systems facilitate faster recovery and service restoration, they are also prime targets for malicious attacks. For example, coordinated attacks or data manipulation over the measurements can trigger the operation of such self-healing systems to operate under normal conditions, leading to outages and thereby customer interruptions.

Future faults in the power distribution system may arise due to the lack of data/system integrity on monitoring and control because future power distribution will have an increased number of active players and increased interactions among them. Both the increased number of players and interactions lead to data and system integrity issues. Therefore, the functional requirements for fault-tolerant grid operations include:

- Secure handshaking of data
- Ensuring data integrity
- Ensuring system integrity
- Data security and privacy preservation.

Blockchain is one of the technologies that can add value to maintain fault-tolerant grid operations, especially for data-driven faults where data or system integrity is at risk. Blockchain increases trust in the data being shared and provides situational awareness to support the distributed decision making. Improved situational awareness can be achieved by providing information on neighboring substations and feeders that are in the given blockchain network and reduces the number of unknown parameters for FLISR decision making. Moreover, the blockchain helps to detect induced and data-driven faults.

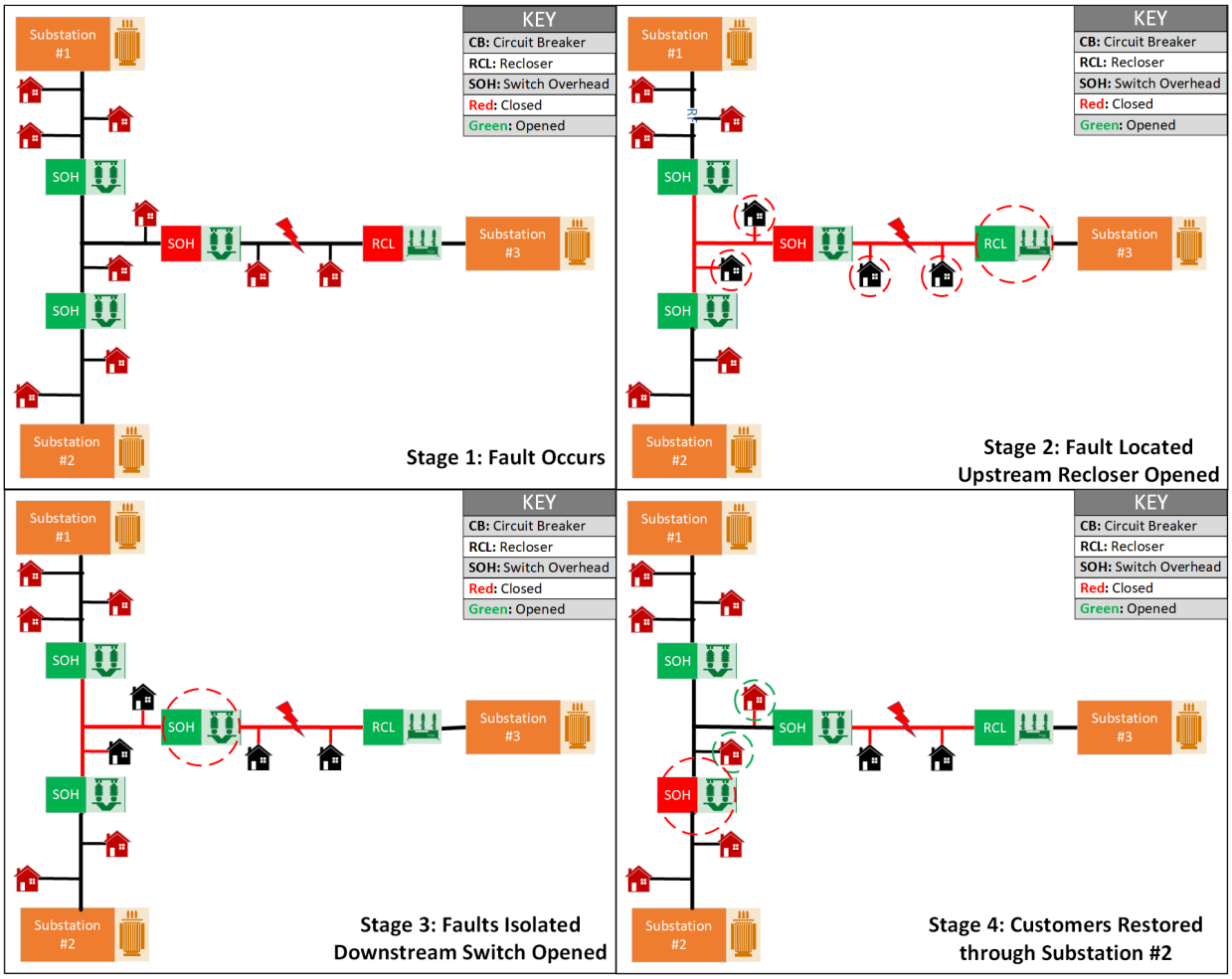


Figure 5. Illustration of how faults are currently handled by utilities.

3.0 Blockchain Applications in Distribution System Operations

Over the last decade, blockchain has emerged as a novel technology that can be used to address some of the existing challenges faced by the electricity industry. Specifically, blockchain has been identified as a technology that could enable grid decentralization and empower decarbonization and democratization.[7]

At its core, blockchain integrates a wide set of technical constructs that work together to host a distributed world state. These constructs can be briefly summarized as follows:

A hash-based linked list (immutable ledger): An immutable ledger is a construct that is based on a linked list structure that operates over a series of data blocks. The ledger contains the entire recorded history and is immutable in nature due to the underlying cryptographic hashing mechanism, strict inability to edit past records (at least within the global view, since local states can be modified), and its distributed storage. Traditional pointer references are replaced with cryptographically secure hashes that mathematically link the current data block to the preceding data block. In addition, each block contains a signature field that ensures both the link and data contents of the block remain secured. This component is often referred to as the immutable ledger and is the basis of the name blockchain, as blocks become effectively tied to each other; this chaining provides the system with strong immutability properties that make blockchain ideal for storing critical data.

Consensus mechanisms: This construct enables participants to "agree" on operations that lead to block creation and their ultimate order. The consensus mechanism is usually tied to a blockchain implementation, but can be selected by end-user needs. Broadly speaking, users must choose between fully open, decentralized solutions or permission-based solutions, each with their own set of benefits and drawbacks. Within the field of power systems, permissioned blockchain implementations seem to have become the preferred option due to their high computational efficiency and ability to tie participants' digital identities to physical service addresses.

Credential management: Ledgers rely on cryptographically secure functions to achieve data immutability. In many blockchain implementations, these functions are further leveraged to provide additional security properties such as nonrepudiation by appending the digital fingerprint of the entity that originally submitted a new block request, as well as being capable of tracking the endorsement process that leads to a specific block's commitment into the ledger. The exact capabilities that are available to the end user are determined by the type of blockchain implementation, but may incorporate features such as identity registration, renovation, and revocation, either as a self-managed process, via a centralized entity, or using an external service provider.

Distributed system architecture: Blockchain relies on well-known distributed system architectures to ensure that agents can communicate across the network and that consensus will be eventually reached (subject to the CAP theorem[8]). Different voting and data ordering algorithms are used to ensure data consistency.

[7] Hertz-Shargel, Ben. "Assessing Blockchain's Future in Transactive Energy." (2019).

[8] The CAP theorem states that a distributed system can only guarantee two out of three desired traits of distributed systems. Namely: a) Consistency (the systems agree on the data being stored), b) Availability (all requests receive an appropriate response); c) Partition tolerance (the system continues to operate when the set of participating agents breaks).

State replication: Although blockchain is often associated with ledger technology, the underlying distributed systems and consensus constructs are broad enough to be used as a generic state replication platform, which enables the implementation of complex state machines with varying levels of complexity. These are often referred to as smart contracts and enable end users to execute complex logic actions across multiple nodes in a highly replicable manner, eliminating the risk of common points of failures.

3.1 Blockchain Features

Due to its underlying structure, blockchain technology natively provides three core features: 1) an immutable, decentralized, and distributed ledger; 2) a distributed, consensus-based agreement process; and 3) a distributed state replication engine (for data and application logic). These features, along with potential uses within the energy space, will be explored in more detail in the following subsections.

3.1.1 Immutable, Decentralized, and Distributed Ledger

This feature represents one of the most widely known features of blockchain. The in-depth technical review of the inner workings of this system are outside the scope of this report but can be found in Yaga et al.[9] These features can be leveraged to solve a variety of problems including:

- Secure asset tracking across their operational lifecycle (supply chain applications)
- Secure data storage across a distributed network (with open/closed registration systems)
- Secure third-party or decentralized attestation services, which can be done by tying data with event/time ordering.

3.1.2 Distributed Consensus-Based Agreement Process

Due to its construction, blockchain technology can leverage a diverse set of consensus mechanisms such as proof-of-work, proof-of-stake, and proof-of-authority, among others, to ensure that the data stored on the ledger accurately represent the intended system state. These mechanisms can be tailored to satisfy a wide variety of end-user requirements which may include (a) types of participants (known identities vs. public systems), (b) number of participants (c) transaction speed requirements, and (d) the amount of data and transactions that must be processed. In addition, there may be a need for ordering the received events themselves, either in their totality or partially (within certain time bounds). Total ordering may be relevant to use cases where events depend on a sequence and are together (such as financial transactions), while partial ordering may be suitable for applications that do not care about the exact order, but need to ensure that data are properly protected (such as capturing measurement data).

3.1.3 Distributed State Replication Engine

A key feature of modern blockchain implementations is their ability to not only replicate data, but also provide logical states that can be used to run distributed applications. Depending on the class of automaton (e.g., the level of computational complexity that can be handled) that is

[9] Yaga, Dylan, et al. NISTIR 8202 Blockchain Technology Overview. NIST. Internal Report 8202, 66 pages (October 2018). https://doi. org/10.6028/NIST. IR. 8202, 2018.

provided by the underlying implementation, a diverse set of applications can be deployed (through smart contract solutions). Possible examples include (in order of complexity):

On-demand data storage and transformation agents: Common applications may include data aggregators and event taggers; relatively simple *if then else* clauses are likely to be sufficient.

Automated, periodic data storage and transformation agents: These types of applications may necessitate more advanced control structures such as loop and stack mechanisms to perform periodic actions.

Self-supervisory/contract-enforcing agents: These applications are required to make complex decisions, such as automated billing, market clearance, and attestation services. These applications may require complete Turing abilities.

Fully decentralized grid applications: These applications have complex behaviors (such as power flow calculations); they may need to access data not available in the blockchain or external services to complete their tasks. Note that certain operations, which are not deterministic (such as truly random functions; which rely on observing unpredictable, external information) cannot be solved by present-generation smart contract solutions.

3.2 Application of Blockchain in Grid Operations

Blockchain has the capability to support a wide array of energy applications. This section focuses on presenting potential applications towards distribution system operations. The presented examples represent high-level overviews that are intended to be illustrative and may require substantial amount of refinement and maturity before any deployment.

Providing attestation services to existent data collection processes: Data collection in distribution systems is an everyday task that utilities across the world perform. This process occurs using a mixture of dedicated equipment (e.g., advanced metering infrastructure) and highly specialized network protocols (DNP3, 802.11, 802.15.4, etc.) that give visibility to distribution system operators (DSOs). Although the collected data are secured in transit, blockchain could be leveraged to provide third-party attestation services that can increase the overall level of trust. In addition, the ledger could be used to store periodic, aggregated records that can be used to verify the integrity and authenticity of data for future reference (e.g., for reliability analysis).

Providing decentralized computational capabilities to distribution systems: Present-generation distribution systems rely on centralized services to perform their duties. Although this approach remains valid and has been optimized across the years, the benefits of decentralization cannot be ignored. Potential applications include having decentralized billing (both long-term storage and price calculation), decentralized asset management (equipment tracking), and non-real-time activities (such as customer disconnections, repair orders).

Provide support for resilient, fault-tolerant operations: Due to its unique features, blockchain technology can be leveraged as an architectural block for building robust, decentralized systems that can continue to operate under abnormal or stressful conditions. These conditions could arise during a variety of operational scenarios, including cyberattacks, weather disruptions, natural disasters, or any event that compromises or diminishes the availability of traditional resources (which are often managed in a centralized manner). Therefore, blockchain can be used to deploy solutions that offer dynamically managed “survivability” modes that can stabilize a system to a known minimal operational state. Once this state is reached, more traditional techniques could be used to accomplish a full-service restoration.

4.0 Blockchain Application in Fault-Tolerant Grid Operations

This section provides potential value propositions that blockchain can bring for fault-tolerant grid operations. Generally, blockchain adds value in response to data-driven faults that arise from data or system integrity issues. Therefore, there are a number of blockchain features that can potentially help to provide fault-tolerant operations against data-driven faults for DSOs. For instance, the distributed consensus feature of blockchain provides a mechanism to detect and mitigate data-driven/induced faults, as well as intentional and inadvertent bad data configurations, which if untreated can maloperate the protection system and eventually lead to outages. Similarly, the distributed decision-making aspects of blockchain technology provide a mechanism to minimize the impacts by localizing the data-driven faults to a small area. Moreover, the immutability feature of the blockchain provides an effective post-mortem mechanism to identify the cause of faults and detect bad data, and hence helps DSOs to develop proper mechanisms to detect those faults, make financial settlements (if any), and set the overall data configuration settings.

DSOs design their protection system to detect faults and isolate them. The restoration system restores the system after faults to maximize the loads being served. The first-level reaction to the distribution system faults is very simple where protective devices such as fuses, reclosers, and relays respond to preset protection settings. These devices are coordinated using the settings to provide backup protection in case the first line of protection devices fails to operate as expected. While the first level of protection is decentralized and works autonomously based on the circuit configurations, several changes might occur in the system operations (e.g., topology changes, changes in power flow directions) that warrant updating the protective settings to make sure that the system responds properly to the faults. Furthermore, reconfigurations occur relatively fast, which may mean power flow changes fast (especially with DERs on the system). Changing these settings with new configurations needs to be done fast; therefore, distributed approaches for communicating and solving locally may be required to avoid delays associated with a centralized system needing to solve optimizations. Blockchain is a distributed technology that can be an instrumental tool in identifying the provenance of such system changes proactively and the DSOs can use that information to make the necessary updates in the protection settings including rapid system reconfigurations.

The features provided by blockchain technology can be thought as an extension to more traditional distributed computing techniques, but with much stronger data immutability properties. This can be ideal for distribution systems that have an always-evolving architecture, but require stringent cybersecurity requirements. Blockchain has the potential to help improve fault-tolerant operations of the distribution system by:

- Using blockchain smart contracts to support distributed implementations of fault-handling algorithms
- Leveraging distributed consensus mechanisms and blockchain's ability to facilitate trust between untrusted entities and act as a trust anchor to increase the trust in the data being shared (all participant systems will have higher confidence in data quality/integrity)
- Using blockchain's immutable distributed ledger to support increasing situational awareness and facilitate improved fault tolerance of the overall system through integrating consensus mechanisms to the fault-handling algorithms.

- Using the inherent and peripherally configurable platform features for improved security of the data involved to address fault-tolerant operations, for instance:
    - Data integrity by using cryptographic hashing
    - Confidentiality by enforcing access controls and incorporating peripheral security controls for increased security through encryption
    - Data access control by using an immutable ledger with transactional records
    - Logic process automation by using smart contracts or platform-level enforcement of governance and rules and fault-tolerant operations by using a consensus mechanism.

A generic example of how blockchain technology can help a utility is presented in Figure 6. In this case, smart contracts, which are logical pieces of code that are run on top of blockchain services, can be used to make distributed decisions using a variety of data sources that are collected across multiple, independent organizational units. This naturally creates a highly resilient environment that can be leveraged by industry to help address some of the upcoming grid challenges, such as high renewable penetration, self-healing microgrids, and increasing grid reliability under abnormal or extenuating conditions.

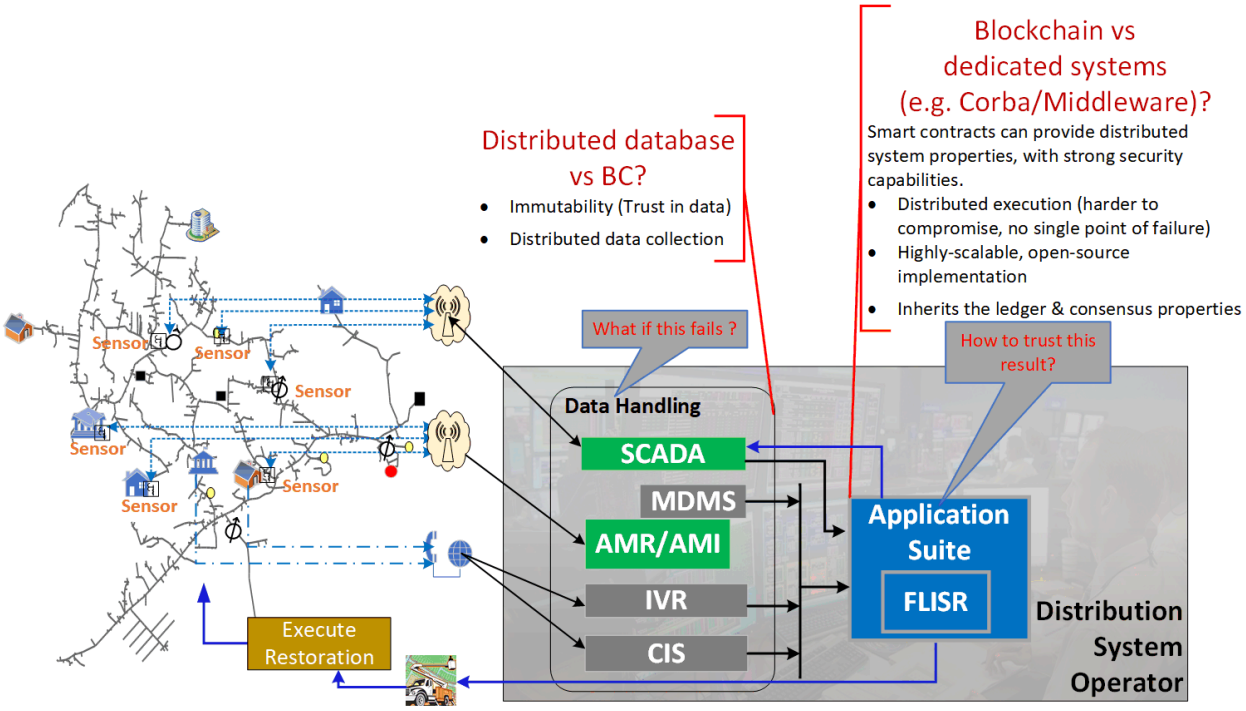


Figure 6. Potential for distributed applications using blockchain technology constructs.

Based on the existing literature review, discussions with subject matter experts, and the pathways utilities and industry are taking in terms of operations, the research team identified three key use cases where blockchain can provide significant support. The following are the three core applications where blockchain has the highest value proposition in terms of maintaining fault-tolerant grid operations.

4.1 Use Case 1: Blockchain for Data Configuration

Planning and performing actions in a system are dependent on knowledge of the system itself. Accurate knowledge and system visibility are imperative in decision making especially during fault conditions. The understanding of a given power system comes from reducing the number of system unknowns by increasing the situational awareness of the system, e.g., through inclusion of component-level measurements, and accurate system parameters. These measurements can provide information on the state of a system including component level information. This use case focuses on data configuration for consistent visibility at the individual component-level of the system. Blockchain based architectures can support consistency in the data configurations which would facilitate in identifying the system topology (presented as Use Case 2) and provide the system information required for implementing fault-handling algorithms like FLISR (discussed in Use Case 3). For example, let us assume that the state of a recloser is known from the measurement of the equipment and that information is incorrect. Considering all the measurements available and the system knowledge is up to date the inconsistency of the recloser state could be fixed. Furthermore, fault-handling algorithms such as FLISR require the knowledge of the components' states to operate in a manner that reduces the impacts of failures and systems faults. Thus, Use Case 3 presents the distributed implementation of FLISR that is dependent of Use Case 1, and 2.

The data configuration of equipment connected to the system is crucial to maintain communication to the devices and the required intercommunication of devices (e.g., communication-dependent protection). Updated system knowledge is key for preventing undesired protection actions, proper power system operation, and timely recovery from an event. Furthermore, blockchain-based architecture will not only help with maintaining the validity of configuration as the system changes, but also provide distributed real-time access to peripheral information such as new devices being added or connected to a particular device, etc. Since such information can be provided through blockchain's immutable ledger and the data entered into the ledger are verified and validated through distributed consensus, blockchain can help provide fault-tolerant measures of sharing the system and network level information.

Currently, utilities set up the data configuration with installation of the equipment from vendors. The equipment configuration is updated as changes occur to the system (e.g., the addition of new devices and system expansion). The performance of the updates involves risks on data configurations that can potentially lead to unintended responses from the protective devices. Data configuration issues become even more important with organizational boundaries (e.g., having different utility ownership connections and nonutility DER connections) because accurately capturing data and segmenting them is difficult with those boundaries. Blockchain can assist with (a) updating the configurations and maintaining up to date configuration information while facilitating distributed consensus for verification and validation of the data entries, (b) ensuring accountability about the bad configuration, and (c) increasing situational awareness.

4.2 Use Case 2: Blockchain for Topology Identification

The application of blockchain to help identify correct system topology is critical to ensure proper operation of fault-handling algorithms such as FLISR (to be presented in Use Case 3). Identifying system topology is dependent on proper system data configuration (i.e., as presented in Use Case 1). The system topology also impacts the protection system. Protective

devices respond to fault conditions based on preset settings and are coordinated to provide backup protection. The configuration of the settings is dependent on the understanding of how the system will behave under faults. Thus, a change in system topology may require the protection settings to be updated. The system topology can change frequently. If the changed in system topology is not updated properly in the utility operational models, the settings designed for a given topology may malfunction. The malfunction of the protection system will result from the following:

- The protective device does not respond to faults. Lack of sensitivity of the protection device can occur for either primary or backup protection. This problem can lead to equipment damage or larger outages by forcing other backup protective devices to respond to the fault.

- Protective devices respond to normal operating conditions due to lower settings that can lead to undesired and unnecessary outages.

- Protective devices respond to faults without coordination. Lack of coordination will make the backup protection device operate to a fault without giving sufficient time for the primary protection to operate, thus increasing the outage impact.

Utilities update the protection settings of devices based on information about the system topology. The system topology is changed by maintenance workers or automatically if operators are reconfiguring the system. Knowing the accurate and trusted system topology is a key to prevent malfunction of the protection system (assuming protection devices do not fail to operate in accordance with their settings). Also, the accurate system topology is a key for the FLISR operation. Blockchain can provide situational awareness and consensus among the protective devices to (a) obtain accurate system topology, (b) perform trusted changes in system topology, and (c) maintain data configuration up to date.

4.3 Use Case 3: Blockchain for Distributed FLISR

As described in Section 2.0, FLISR is one of the commonly used technologies by DSOs for locating, detecting, and responding to distribution system faults. Currently, protective devices are configured to respond to faults with local measured information such as measured fault current. In addition to the response from the local protective devices, utilities receive information from SCADA to a centralized control center or DMS. Based on the received information, a sequence of decisions for FLISR is performed in a centralized manner using SCADA measurements and an operational grid model. The problem with the existing centralized FLISR implementation is a single point of failure for data-driven faults or loss of communication.

While the existing implementation of FLISR is mostly centralized, there are a few organizations, such as Avista™ and Schweitzer Engineering Laboratories™, that are taking initiatives toward distributed implementation. Blockchain can be one of the technologies that support the distributed implementation of FLISR and help decision making via distributed consensus mechanisms. Looking forward in terms of distribution system operations, a distributed implementation of FLISR is one of the core use cases for the blockchain.

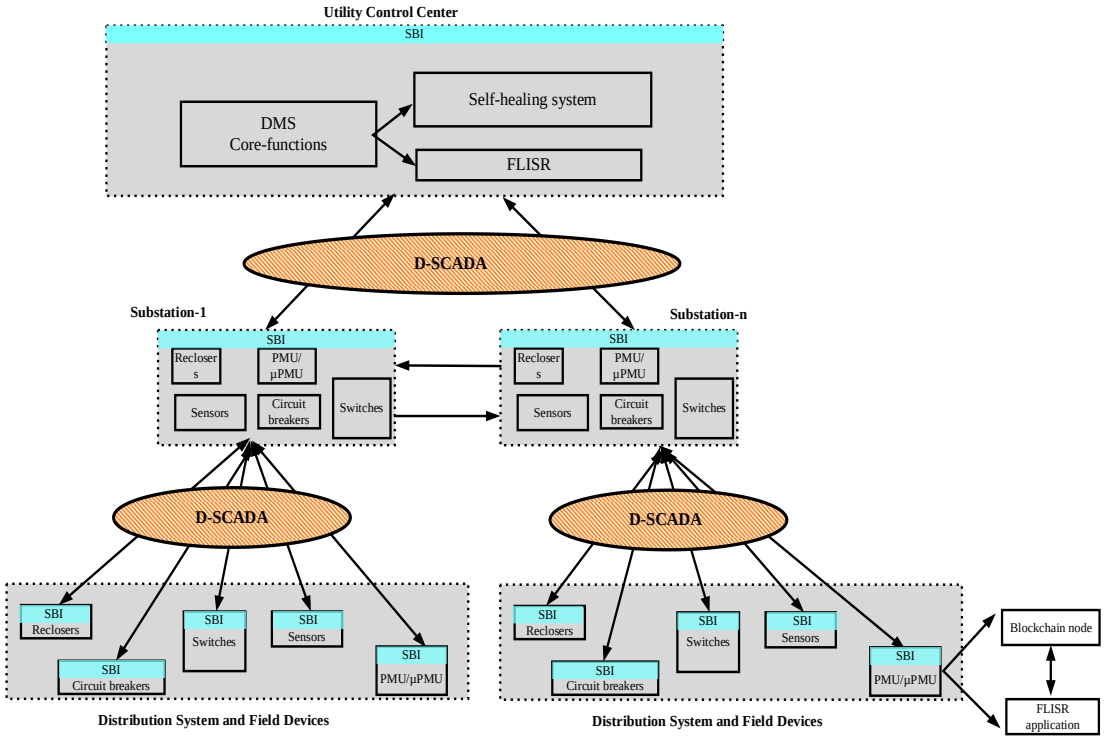


Figure 7. Centralized FLISR implementation.

Distributed implementations for handling faults, such as S&C™ Electric Company IntelliRupter technology, can address the single point of failure of existing centralized implementations. However, these distributed implementations are highly dependent on point-to-point communication between the decision-making nodes and protective devices. The point-to-point communication link makes the system susceptible to data-driven attacks.

Blockchain can reduce the vulnerabilities of data-driven attacks by helping in the detection of induced/data-driven faults. Thus, improving the system situational awareness as presented in Use Case 1, and 2. With the validated and distributed approaches in Use Case 1, and 2 provide the system information for the distributed FLISR implementation. Thus, having an improved situational awareness, and reducing the vulnerability of communication link failures. Local situational awareness is improved through a blockchain network sharing information across neighboring substations/feeders. This enables distributed observability and control at the substation and feeder level, offering faster response to faults and greater resiliency. The blockchain-enabled distributed FLISR in a scenario of communication link failures can still perform decisions with the available information. For example, assuming a communication link failure between substation and control center, a distributed FLISR at the substation can still perform decisions with information received from neighboring substations.

In the future with the increased penetration of DERs, the FLISR implementation capabilities for system restoration will be improved by the use of such resources. DERs can be engaged to increase the area to reconnect after a fault event, thus improving reliability. Not all DERs will be owned by utilities. Multi-ownerships of DERs will bring increased operational boundaries for the utilities. The increased operational boundaries will bring more value to blockchain to promote trust, distributed decision making, and increased situational awareness. The importance of situational awareness is presented in Use Case 1, and 2.

5.0 Conclusions and Future Work

The power distribution system is the final stage of the electric power delivery to millions of customers and is a critical segment of the modern-day electricity infrastructure. However, distribution systems are prone to faults because of their complex topology, more vulnerable to natural and man-made threats (i.e., given its reduced clearance from threats), and the vast diversity of connected devices. Existing studies indicate that almost 80% of all customer interruptions are caused by faults and outages in distribution networks. Furthermore, the proliferation of DERs is introducing new complexities and vulnerabilities that the traditional fault management systems are not equipped to handle. In this regard, blockchain is one of the emerging technologies that has potential to add value to maintain fault-tolerant grid operations, especially where data or system integrity is at risk. This is due to the Blockchain core features of distributed consensus-based decision-making process, and immutability.

Blockchain can facilitate distributed implementation of FLISR or other fault-handling algorithms to avoid the single point of failures experienced with the most existing utility fault-handling frameworks. Furthermore, it increases the trust in the data being shared (the receiver will have higher confidence in data quality/integrity) and provide increased situational awareness through a distributed consensus mechanism. The following points provide specific benefits that blockchain brings in terms of fault-tolerant grid operations:

- Provides a decentralized platform to support a FLISR implementation.
- Helps to detect induced/data-driven faults.
- Improves situational awareness by providing information of neighboring substations/feeders that are in the given blockchain network and reduces the number of unknown parameters for FLISR decision making.
- Enables information validation among substations via consensus, enabling FLISR schemes to continue to operate in cases where communications to a centralized control center have been severed.

In case of communication link failures (e.g., communication between substation and control center), the blockchain-enabled FLISR distributed at the substation can still make decisions with information received from neighboring substations. For instance, even if there is a communication link failure between the control center and Substation A, the substation can potentially receive information through the blockchain network (e.g., Substation A information can be validated by consensus with other substations excluding the control center). Some future schemes, such as those modeled by OpenFMB, could enable sharing of information across substations to support local FLISR decisions. However, the challenges pertaining to data integrity and risk from single point of failure continues to persist and is an area where blockchain has the potential to augment and improve the process.

Future work would focus on designing simulation-based experiments to demonstrate blockchain's ability to assist with fault-tolerant grid operations under high penetration of DERs (with a mix of utility-owned and nonutility-owned assets). The three use cases identified through this report would be used as applications for comparison against traditional centralized response systems to articulate blockchain's value proposition. This will further facilitate evaluating the feasibility blockchain-based coordination applications between disparate entities.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov