Secure Hyperledger Implementation for Enhanced Logging and Decentralized Authentication at Taranis Energy Corp.

Elijah C Rodgers

Western Governors University

SECURE HYPERLEDGER IMPLEMENTATION FOR ENHANCED LOGGING AND DECENTRALIZED AUTHENTICATION AT TARANIS ENERGY CORP.

Table of Contents

A. Proposal Overview

A1. Problem Summary

Taranis Energy Corp. (TEC) is an energy provider with operations centered around multiple nuclear power plants located on the eastern coast of the United States. These power facilities collectively serve a customer base of over 27.5 million users. As a critical infrastructure provider, TEC places a paramount emphasis on cybersecurity. However, in recent years, budgetary constraints have had a notable impact on the company's security posture. The challenges arising from budget cuts have manifested in several ways. Aging servers, switches, and routers within TEC's network have been unable to receive automated patching due to a combination of secure and unsupported devices. Additionally, rising hardware costs have forced the abandonment of hardware lifecycle plans. Routine external audits, an essential aspect of security monitoring, were deferred, leading to unidentified gaps in the system. Furthermore, the IT teams at TEC have been stretched thin, struggling to address issues proactively. This situation has been exacerbated by staffing shortages in the industry, which were further complicated by the pandemic.

In early 2023, TEC faced a significant security breach within its supply chain, which was ultimately traced back to a third-party vendor collaborating with APT29. This vendor is suspected of implanting backdoors that granted unauthorized network access to the attacker. This breach allowed the attacker to intercept network traffic and extract a "golden ticket," providing nearly unrestricted access to TEC's network and the potential to disrupt its operations. This incident underscored vulnerabilities related to centralized authentication, fragmented security tools, decentralized logging practices, and continued third-party access, despite regulatory

requirements. The presence of poor security configurations and unsupported systems likely compounded these issues due to longstanding delays in remediation efforts.

To address these vulnerabilities and enhance its cybersecurity posture, TEC is implementing a private permissioned blockchain network. This network will consist of distributed validator nodes, forming a robust and decentralized platform for digital identity management, access control, and compliance via smart contracts. These smart contracts will be programmed to automate routine security checks that were previously delayed due to budget constraints, such as audits and patching of long-neglected assets. Moreover, penalty clauses within these smart contracts will incentivize vendors to adhere to security guidelines rigorously. The immutable ledger provided by blockchain technology will provide centralized logging that will record all changes and modifications, which can be attributed to individuals through smart contracts. By introducing transparency and immediacy to its security oversight, TEC aims to proactively fortify its cyber defenses, overcoming the limitations imposed by past financial constraints and workforce shortages.

A2. IT Solution

The recent cybersecurity breach at Taranis Energy Corp. (TEC) has shed light on critical vulnerabilities within the organization's security infrastructure. This breach, attributed to the advanced persistent threat (APT) group APT29, also known as Cozy Bear, demonstrated a high degree of sophistication and meticulous planning, highlighting the urgent need for remediation. Several weaknesses have been identified, including overreliance on centralized authentication via a single Active Directory server and the absence of automated security alerts. These vulnerabilities exposed TEC to potential threats and provided attackers with persistent access.

Furthermore, the lack of regular external security audits and internal security assessments left TEC ill-prepared to detect or respond effectively to such breaches.

In response to these pressing challenges, TEC has devised a comprehensive strategy to bolster its cybersecurity measures. The company plans to establish a private permissioned Ethereum network hosted on Microsoft Azure Kubernetes Service, capitalizing on the scalability, security features, and distributed consensus capabilities offered by Hyperledger Besu (Hyperledger, n.d.). To create a robust and resilient network infrastructure, approximately 30 Besu validator nodes will be deployed as Kubernetes pods behind Azure load balancers, spanning five regions. This distributed architecture ensures redundancy across regions, minimizing the risk of network disruptions due to outages or compromised instances. Key elements of the network's security framework will be defined through Solidity smart contracts. The Certificate Authority contract will employ Elliptic Curve Cryptography to generate and cryptographically sign X.509 certificates from a hardware security module-protected Besu private key (Berdy, 2021). These certificates will embed issuance data and public keys, permanently storing them on-chain for verification purposes. This approach eliminates single points of failure associated with using Active Directory, enhancing authentication security. Role-based access contracts will ensure that only approved systems have the necessary privileges, and access control contracts will reference these certificates to govern permissions based on differentiated roles and risk levels. To streamline security-related data management, log integration smart contracts will be employed to ingest security data streams into an immutable common format on the ledger. This will facilitate fast forensic indexing and querying, greatly aiding incident response and audits. The permanent audit trail established by these smart contracts will simplify forensics and provide auditors with independent verification of control measures.

Additionally, the transparency offered by smart contracts will extend to supply chain management. Procurement contracts utilizing Ethereum Request for Comment-721 (ERC-721) tokens will represent individual equipment and assets, each with a unique, untampered history (Entriken et al., 2018). These tokens will enforce programmable maintenance and equipment replacement agreements over their lifecycles, ensuring the integrity of the supply chain. (Know Your Customer) KYC smart contracts will be established to link third-party identity data to digital identities for tracing and auditing purposes (Kapsoulis, 2020). Furthermore, smart contracts will automate compliance tracking through procurement agreements and asset management, with non-compliance triggering immediate penalties to uphold regulatory requirements without delay. By recording all activities transparently on the blockchain, TEC will enable proactive monitoring and response capabilities. Policy violations will become instantly detectable and reversible through technical safeguards, strengthening the organization's overall cybersecurity posture.

A3. Implementation Plan

During the initial sprint, our main objective centers on gauging our existing cybersecurity maturity level to provide a point of reference for future evaluations and to lay the groundwork for a foundational network. We will use the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) as our yardstick for this assessment. Following the establishment of this baseline, we will execute the deployment of a robust node cluster on Kubernetes, distributed across Sites A, B, and C. This deployment will function as a distributed testnet, providing a solid foundation for our network infrastructure. Our Product Owners will then concentrate on prioritizing tasks that make certain of the basic functioning of our blockchain

network, specifically the signing and sharing of blocks between these nodes. Developers will configure cryptographic keys, while our DevOps engineers will be on hand to address any key or certificate-related issues that may arise. By the conclusion of Sprint 1, the three initial locations will be regularly communicating blocks, indicating the network's health. Our QA team will also conduct transaction load tests to demonstrate our capacity to handle future expansion. We will prepare our nodes for future coverage growth by scaling our infrastructure horizontally through Kubernetes integrations. Sprint 2 will see our experts designing data structures to capture security events in a reusable format. We will abstract log parsers from storage models through interfaces to maintain flexibility as our needs evolve. Our QA team will engage in unit testing of individual components and integration testing of full functionality to validate that events are accurately logged across all nodes. We will also ensure that user stories capture logging requirements to future-proof the solution. To mitigate risks of complex rules-breaking audit needs, our Developers will work collaboratively to ensure that underlying models support anticipated analytics. Sprint 3 will focus on building basic identity management. We will design an X.509 hierarchy with root/issuing authorities to provisionally authenticate users on the blockchain. Integration of key request/response APIs will expose issuance workflows, with testing concentrated on error handling to prevent tampering. A prototype ID portal will issue sample certificates linked to accounts during the Sprint Review. While this phase is simple, it will demonstrate that the concept works as we continue to build more mature identity solutions based on the foundational capabilities developed across previous sprints. Sprint 5 is dedicated to expanding our access governance capabilities. We will need to modify the smart contract's scheduling functions to automatically conduct periodic reviews of permissions and accounts. Developers will design algorithms to model various review types, from simple access

verifications to more in-depth audits. Stakeholder workshops will play a crucial role in debating policy options to ensure consistent governance as the ecosystem expands. Scenarios will refine rulesets, such as standardizing review cadences or escalating oversight for high-risk accounts. Implementation will involve integrating the scheduled audit capabilities directly into the smart contract logic through additional functions. Comprehensive testing, covering all review pathways and exception handling, will validate that the solution operates as intended over time. Sprint 6 will focus on addressing the compliance demands of partner networks joining our ecosystem. We will create a (Know Your Customer) KYC smart contract to securely intake and link third-party identity data for tracing (Kapsoulis, 2020). Systems integration will federate attributes from separate procurement systems comprehensively. Automated test suites will be used to cover edge cases, such as fault tolerance for document tampering, to ensure data integrity over time. A simulated partner enrollment portal will populate sample profiles onto the live contract for demonstration purposes. Procurement contract terms will be integrated with financial penalties as incentives through smart logic. Interviews will strike a balance between enforcement and flexibility, particularly in cases where requirements change. In the final sprint, Sprint 7, we will bring the full solution together through user acceptance testing. Cross-functional experts will rigorously exercise every capability from the ground up. Feedback will be processed into the backlog to resolve minor issues, ensuring that we deploy a fully vetted, production-ready solution.

B. Review of Other Works

B1. Review of work, B2. Relation to Project

The Use of Azure Kubernetes Service and Hyperledger Besu:

Microsoft's release of the Hyperledger Fabric (HLF) template for Azure Kubernetes Service (AKS) presents an appealing option with many benefits outlined in the Azure Blog post (Microsoft Azure, 2020). Deploying HLF on AKS removes the overhead of managing node infrastructure, allowing TEC's team to focus on the application layer. AKS delivers enterprise-grade security through role-based access controls and regular patching of the Kubernetes control plane. Its auto-scaling capability ensures optimal resource utilization. Furthermore, TEC is already well-versed in Microsoft technologies, reducing the learning curve. However, several limitations exist. Relying solely on Azure services keeps critical technology decisions in Microsoft's control. The multi-tenant nature of cloud infrastructure risks exposure from other tenants' activity. Moving entirely to a hosted model also increases operational costs versus a hybrid approach. Furthermore, it does little to address TEC's goal of decentralizing authentication and establishing an immutable ledger for auditing - the template deployment focuses more on consortium management workflows.

TEC thus elects to implement a hybrid model combining Azure services and an internal permissioned blockchain network. By deploying Hyperledger Besu on their existing AKS clusters, they gain infrastructure reliability without cloud vendor lock-in. Choosing Besu over Fabric enables the use of Ethereum standards for decentralized identities and transactions well-aligned with TEC's objectives. The modular architecture of Besu smart contracts separates concerns of identity, procurement automation, and auditing. Its native Solidity integration simplifies rules-based enforcement of security obligations. They are handling authentication

through distributed X.509 certificates that leverage established standards while preventing single points of failure.

Overall, the hybrid model balances cloud benefits, governance requirements, and technical preferences. It allows leveraging existing Azure investments and expertise while preserving control. The immutable transaction ledger and automated rules provide the transparency and assurance needed to strengthen third-party risk management. Further, the modular design proves highly adaptable to evolving needs.

The use of Decentralized Identity Management:

The paper proposed by Maram et al. (2021) presents an intriguing decentralized user identity management system. Similar to TEC, it aims to provide a secure and transparent method for user authentication that enhances accountability. Both approaches utilize a decentralized network of nodes to validate identities and transactions, as well as leverage existing online accounts to facilitate key recovery, improving usability. TEC's planned deployment of an Ethereum blockchain governed by smart contracts aligns well with the concepts proposed in the Maram et al. paper. Nevertheless, differences in scope and architecture exist. The paper solely concentrates on user identity management, whereas TEC encompasses broader goals related to supply chain management, auditing, and automation through smart contracts. Furthermore, the paper's identity system module and key recovery module are more loosely coupled independent components, whereas TEC envisions a more unified and standardized approach, making use of ERC standards.

Concerning decentralization and Sybil attack resistance, both the identity management system proposed by Maram et al. (2021) and TEC's blockchain network aims to leverage the properties of distributed consensus. The paper mentions utilizing a "decentralized set of nodes" to govern key recovery without relying on a centralized authority. Similarly, TEC intends to implement approximately 30 Besu validator nodes across multiple data centers. However, the paper is less explicit about the specific consensus protocol and how Sybil resistance is achieved. In contrast, TEC's use of QBFT through Istanbul hard forking provides well-defined mechanisms for reaching an agreement in a Byzantine fault-tolerant manner, potentially strengthening the proposed system against identity forgery attempts.

Accountability is another shared key goal. The paper outlines the generation of "accountability claims" to track actions correlated with identities (Maram et al., 2021). Although implementation details are not specified, this aligns with TEC's objective of creating an immutable centralized log of all authenticated interactions stored on-chain.

Regarding compatibility with legacy systems, the identity management system focuses on facilitating key recovery through existing online accounts. TEC faces additional complexities related to integrating a blockchain network into existing infrastructure, processes, and vendor relationships. The techniques described for leveraging external logins in the paper could potentially inform TEC's vendor onboarding strategies through standards like ERC-725 (Vogelsteller, 2017).

Incorporating Digital Identities and Addressing Multi-Factor Authentication using Blockchain:

This paper delves into two essential cryptographic components - fuzzy extractors and secure sketches (Dodis, Ostrovsky, Reyzin, & Smith, 2008). Fuzzy extractors are instrumental in extracting nearly uniform randomness from error-prone inputs like biometrics, demonstrating tolerance for irregularities. On the other hand, secure sketches contribute to the consistent recreation of such inputs.

These concepts hold significant relevance to the current challenges TEC faces in authenticating endpoints and vendors, given the inherent variability in biometrics and hardware. As TEC proposes a blockchain-based digital identity system, that pairs biometrics with on-chain credentials, the principles discussed in this paper could play a crucial role.

Specifically, secure sketches could be used to recreate biometrics reliably for accessing credentialed private keys. Meanwhile, fuzzy extractors could draw uniform randomness from the biometrics to digitally sign transactions. The paper sets forth constructions for these components under varying "closeness" measures, including Hamming distance, which are essential for calculating biometric variances like fingerprints and facial features (Dodis et al., 2008). This suggests that these techniques could be smoothly incorporated into TEC's decentralized identity management objectives via standards-compliant smart contracts.

The paper presents invaluable cryptographic elements that can address TEC's key challenges - the authentication of unpredictable biometric inputs. The integration of these components as reusable elements in TEC's blockchain design could fortify identity management by employing

industry-leading secure techniques for handling "noisy" real-world attributes (Dodis et al., 2008). This also future-proofs the solution in line with the ongoing advancements in biometrics. Furthermore, these components could also be used for other error-prone data types, such as hardware IDs, which are vital for improving supply chain security.

The Use Case of Blockchain for Secure Supply Chain Management:

The article proposes several persuasive use cases that inspired the design of TEC's IT Solution (Chawre, n.d.). First, TEC harnesses smart contracts and decentralized ledger technology for comprehensive traceability throughout its operations. This practice reflects the article's portrayal of precise goods tracking and enhanced accountability (Chawre, n.d.). By permanently recording every transaction, document, and activity associated with equipment, assets, and third parties, TEC achieves unambiguous visibility of each item's lifecycle. Second, TEC's network promotes transparency among stakeholders, countering traditional supply chain hurdles like lack of visibility and trust (Chawre, n.d.). The ledger, acting as a "single source of truth," enables all approved parties to validate information swiftly. Third, TEC utilizes smart contracts to streamline processes and meet agreements, mirroring the article's emphasis on smart contracts simplifying supply chain operations through automatic execution (Chawre, n.d.). This matches TEC's plan to automate payments and certificate verification within its network architecture. Lastly, TEC plans to integrate real-time inventory and asset data on its ledger to enhance compliance and inventory management, echoing the capabilities underscored in the article, such as accurate monitoring, error minimization, and decision-making optimization (Chawre, n.d.).

C. Project Rationale

The recent cyberattack targeting TEC has exposed critical vulnerabilities within the organization's infrastructure and emphasized the pressing need to fortify security defenses against ever-evolving threats that specifically target essential infrastructure. This intrusion, which involved compromising Active Directory and exploiting vendor backdoors, showcased the attackers' sophisticated techniques for infiltrating networks and nearly disrupted vital operations. Unfortunately, this breach occurred at a challenging time when funding constraints had hindered routine security upgrades. The presence of outdated systems and a reactive security approach left vulnerabilities that determined adversaries could easily exploit.

The evolving threat landscape, characterized by the proliferation of ransomware attacks and incidents like the Colonial Pipeline attack, underscores the fact that nation-state and ransomware actors are increasingly targeting critical infrastructure. (Cybersecurity and Infrastructure Security Agency, 2021) As geopolitical tensions escalate, organizations like TEC face a heightened risk. TEC plays a pivotal role in the lives of millions who depend on its power supply, making any disruption a potential threat to public safety and national security. To avert catastrophic consequences, TEC must adopt a proactive and resilient security model that aligns with the dynamics of today's threat landscape.

While cost considerations are valid, blockchain technology offers a future-proof solution for TEC's security infrastructure, thanks to its flexible and modular design. The traditional approach of centrally managed, manual systems is no longer adequate to counter the agile threats that target single points of failure as witnessed in the attack by APT29. With blockchain, smart contracts facilitate continuous innovation, allowing for easy updates as better solutions emerge.

Instead of relying on aging systems with inherent fragility, the network can seamlessly scale to integrate new sites, partners, and data sources. Expanding the grid becomes a straightforward process through the addition of new nodes. Most importantly, blockchain establishes cyber resilience as threats evolve rapidly. TEC can proactively embrace upgrades through well-tested network changes, as opposed to reacting to vulnerabilities or attacks with haphazard patches.

TEC recognizes that cyberattacks frequently hinder innovation within critical infrastructure sectors. However, their permissioned blockchain network architecture establishes advanced security from the ground up that seeks to change how innovation occurs in critical infrastructure. By design, the regulated utility industry demands rigorous compliance that blockchain excels at ensuring through features like programmable smart contracts and transparent auditing capabilities. TEC plans regular assessments of their technical framework to guarantee ongoing risk mitigation efforts remain ahead of emerging cyber threats targeting national utilities. This proactive approach to security will bolster customer confidence in service continuity.

Additionally, TEC is positioned to become an early blockchain leader and plans to actively share their research experience and production findings. Collaborating openly with other utilities exploring this technology, TEC can inspire further pilot deployments across the sector. Over time, a cooperative community blockchain network could form between utilities seeking interoperability while retaining proprietary node identities on an immutable shared ledger for traceability. TEC also recognizes that cultivating strategic academic relationships helps shape future talent needs. By informing university curricula of competencies required for next-generation energy delivery, TEC can develop a pipeline of qualified professionals ready to advance the company’s technical strategy.

Overall, TEC's open and pioneering application of blockchain establishes a model of security, compliance, and innovation that distinctly elevates its brand reputation. If successful, this long-term initiative is poised to deepen valuable partnerships, attract high-caliber talent, and ultimately drive business advantages through differentiated delivery of safe, reliable utility services powered by responsible technology leadership. Given the widespread reliance on its services, TEC has a duty to adopt fortified security measures commensurate with its significant responsibility to the public. This project represents a proactive and vital step towards fulfilling that imperative.

D. Current Project Environment

Taranis Energy Corp. is a privately owned nuclear company that serves over 27.5 million residential and commercial customers by providing power through pressurized water nuclear reactors. Historically, the company has placed a strong emphasis on physical security, with a focus on perimeter defenses and access control. This includes the deployment of three armed security checkpoints equipped with Igos RT2000 smart card readers featuring biometric fingerprint scanners, coupled with digital photo ID validation. Furthermore, the organization maintains a robust network of over 300 Axis camera systems for continuous monitoring of sensitive areas, overseen by a central command center powered by four Dell Precision 7920 tower workstations running Genetec Security Center 5.8.

In terms of network infrastructure, TEC employs a strategy of segregation, utilizing a combination of hardware and software segmentation at each of its facilities. The operational technology network operates on an ABB AC800M distributed control system, running VxWorks, and includes over 100 Allen-Bradley CompactLogix PLCs, along with Motorola RB5000 radios.

This network is isolated from other segments through Cisco Catalyst 3850 switches and is safeguarded from external threats by a dual-homed Check Point GAiA firewall appliance operating in routed mode.

On the information technology side, TEC's network supports 3500 clients using either Windows Server 2012 R2 or Ubuntu 16.04 LTS. It grants access to corporate applications, such as the Oracle e-Business Suite R12 human resources and finance database. User authentication is handled by Active Directory Domain Services, hosted on a cluster of Dell PowerEdge R740XD servers, with multi-factor verification enforced for the domain admin group through RADIUS integration with SecurID tokens. Additionally, a guest-wireless network is available for visitors, securely separated from the IT subnet through the use of Cisco ASA 5520-X next-generation firewalls.

The organization relies on centralized monitoring and threat hunting, facilitated by Splunk Enterprise 7.2.3, which sources logs from all devices and captures additional network metadata from Bro IDS sensors distributed throughout the environment. Automated incident response capabilities have been implemented using playbooks through Demisto's SOAR platform, orchestrating actions with tools such as Phantom, McAfee, and Qualys.

The most recent significant infrastructure update occurred in 2017, focusing primarily on patching vulnerabilities exploited by WannaCry (WannaCry ransomware attack, 2017. Legacy systems like Windows Server 2008 and Windows 7 endpoints, which were no longer receiving support patches, were upgraded or replaced with Ubuntu workstations where feasible. This transition required significant unplanned expenditure, diverting approximately $500,000 from the upcoming fiscal year IT replacement cycle. Challenges remained, including unsupported

operating systems, insufficient device hardening configurations, and budget limitations, which hindered further progress. Annual IT spending had decreased by 15% year-over-year due to rising hardware costs and reduced fee revenue during COVID-19 shutdowns (Gartner, 2020).

Furthermore, supply chain issues in 2021 led to a 20-30% increase in server costs, prompting the abandonment of the five-year hardware lifecycle plan (Global Chip Shortage, 2023). Only failed equipment received a replacement, often with used components to minimize expenses. This resulted in a mix of unsupported and secure devices within the infrastructure. Additionally, TEC decided to deploy some workloads to Microsoft Azure for improved scalability and management. This included hosting some internal tools and documentation portals on an AKS cluster. Routine external audits were deferred, leaving unidentified security gaps. Staffing shortages, exacerbated by the "Great Resignation," constrained overworked IT teams, hindering their ability to address issues proactively (Lee et al., 2023). This delayed response effectively made TEC a more attractive target for motivated attackers. Despite strong leadership support for robust security measures, budget constraints hindered IT's ability to implement gold standard practices.

In early 2023, TEC detected anomalous SSH and RDP login attempts targeting Industrial Control System (ICS) servers within the OT zone of its largest facility. Network traffic analysis indicated the use of encryption, fast flux DNS, and multi-staged commands resembling tactics employed by APT29 (MITRE, 2023). Forensic analysis, following isolation of the affected hosts in a honeypot environment, identified a bash script scheduled as a cron job to execute after a vendor's support contract had expired. The script exploited existing vendor-installed remote access trojans, escalating privileges and laterally moving through the network using an extracted Active Directory golden ticket crafted from the stolen NTLM hash of the Kerberos Ticket Granting

Service (Netwrix, 2020). This allowed unauthenticated domain access, with the script designed to encrypt industrial process controllers and SCADA histories using the vendor account's elevated privileges, disrupting critical operations. The attack featured resilient payloads and redundant Command & Control beacons aimed at impeding remediation, along with deception techniques like token dropping and lateral movement in an attempt to frame the new vendor. However, YARA rules and kernel object auditing linked tools and folded time stamps to the initial intrusion vector (Arntz, 2017). With a power cycle and the script deleted from infected systems, the attack was contained, but it raised concerns regarding supply chain compromise and risks associated with continued third-party access. The vendor's level of involvement remains unclear.

In response to these cybersecurity challenges, TEC has decided to take proactive measures to enhance its security posture (National Infrastructure Advisory Council, 2017). The organization will adopt a decentralized authentication approach, establish an automatically updated immutable centralized log, and enforce more stringent rules through automation. To achieve this, TEC will deploy a permissioned Ethereum blockchain on Azure Kubernetes Service (AKS), using Hyperledger Besu, an Ethereum client optimized for enterprise applications. Approximately 30 validator nodes running Besu will form the initial network across five geographically dispersed data centers, enhancing resilience against threats such as outages or compromised nodes. The Quorum Byzantine Fault Tolerance (QBFT) consensus mechanism will validate transactions, providing robustness against malicious nodes or outages (Hyperledger, n.d.). Besu supports QBFT through an Istanbul hard fork integrated with Tessera for private transactions on designated channels. Solidity smart contracts, compliant with ERC-20 standards, will establish a

standardized API for token interactions, including transfers and approvals (Ethereum Foundation, n.d.).

TEC will implement a Certificate Authority (CA) hosted on AKS to issue X.509 certificates to participating nodes and endpoints. The CA will manage the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP), regulating node and device identities on the network. Over time, an event stream will index Transactions Per Second (TPS), providing a tamper-proof record of all authenticated interactions for auditing purposes. Additional smart contracts will automate procurement, leveraging ERC-725 digital identity standards for traceable vendor onboarding (Lundkvist et al., 2018). Supply chain Know Your Customer (KYC) processes, facilitated through the decentralized identity provider, uPort, will bind government IDs to on-chain identities, addressing vulnerabilities associated with third-party access. Security standards defined in procurement smart contracts, such as regular penetration tests or log integrity checks, will be executed through native Solidity functions to overcome budget and staffing constraints. Smart contract timers will trigger automatic payments or penalty deductions for non-compliance. All contract events and state changes will be permanently stored on-chain, providing transparency while reducing the risk of manipulated audits or unfulfilled obligations through rule-based enforcement (Buterin et al., 2014).

E. Methodology

This blockchain project aims to revolutionize core security, identity, and supply chain operations within a regional network that provides critical services. The inherent complexity of the project, coupled with its interdependencies, makes it crucial to proceed with precision from the outset. Traditional waterfall approaches, due to their inherent rigidity and inability to

accommodate evolving needs, carry unacceptable risks in such a dynamic landscape (Boehm, 1988). Given that blockchain technology remains in its early stages, our understanding and requirements may evolve as we progress. A more flexible and adaptive approach is needed, and Scrum's iterative methodology is the ideal choice for establishing a solid foundation in the face of uncertainties (Schwaber & Beedle, 2002).

Breaking the work into short, manageable cycles through Scrum will allow us to start delivering capabilities swiftly, validating assumptions, and maintaining a solution grounded in practical realities (Cohn, 2009). Sprint 1 will focus on measuring a baseline and establishing the fundamental distributed ledger infrastructure. Deploying the initial node cluster early on will enable us to test basic on-chain operations and proactively address configuration challenges. This early identification and resolution of issues will pave the way for subsequent sprints to seamlessly extend the network's coverage. In parallel, sprint planning will prepare for future development by capturing diverse logs and access scenarios, ensuring our data models remain adaptable to unpredictable use cases. Early inspection and reviews will expose flaws before deep investments are made, providing stakeholders with confidence that the project is on the right track.

Agility is a core tenet of Scrum, recognizing that plans may need to change as knowledge accumulates during development (Sutherland & Schwaber, 2020). For example, configuring cryptographic keys during the initial node deployment may present unforeseen challenges that could potentially slow down the process. Scrum's inspect-and-adapt cycles empower us to identify and address these issues promptly (Kniberg & Skarin, 2010). If key configuration becomes a challenge in Sprint 1, a solution can be prioritized, allowing subsequent sprints to

adhere to the planned schedule. Transparent progress updates provided by Scrum will facilitate stakeholder support in overcoming emerging obstacles. The framework's flexibility to move tasks between sprints ensures that goals can remain attainable as our understanding deepens. It allows us to adapt to unforeseen complexities as they arise, ensuring that we build the right solutions. In the event of complications, such as unexpected key issues, Scrum provides an environment where changes can be addressed, tested, and incorporated without disrupting the overall timeline. This approach positions the project well to achieve milestones despite the inevitable uncertainties associated with cutting-edge technologies.

At the end of each sprint, which occurs every 30 days, Scrum ceremonies will ensure that the team continuously delivers valuable working functionality (Cohn, 2009). During the Sprint Review meeting, the team will showcase what has been completed during that increment. Instead of presenting slides, live demonstrations of the blockchain network and smart contracts in action will be conducted. For example, the first Sprint Review after Sprint 1 will feature live demonstrations of secure transactions being logged across distributed nodes, confirming the foundational infrastructure's performance. As subsequent sprints introduce features such as identities and access controls, more advanced and integrated demonstrations will prove the capabilities. These tangible working demos will verify that technical achievements align with evolving objectives and educate stakeholders on blockchain intricacies (Daley, 2018).

Most importantly, the frequent Sprint Reviews will confirm that the project is delivering incremental value. By showcasing returns every 30 days, we will justify the allocation of resources to complete the project's vision. Stakeholders attending Scrum events will gain assurance that the project will achieve a return on investment as capabilities mature sprint by

sprint. Through the successful deployment of refined functionality each cycle, the team will build confidence in its ability to address the right problems. With this continuous delivery approach, Scrum is well-suited to generate ongoing value from this blockchain project as requirements emerge and evolve.

F. Project Goals, Objectives, and Deliverables

F1. Goals, Objectives, and Deliverables Table

#	Goal	Supporting objectives	Deliverables enabling the project objectives
1	Decentralize Security Systems	Migrate monitoring to the blockchain network	Besu/Hyperledger nodes deployed across sites
			Solidity smart contract for security event logging
			Dashboard for real-time decentralized monitoring
2	Improve Access Control	Enhance identity management	X.509 digital certificate authority
		Automate access reviews	Smart contracts for access approvals/revocations
			Scheduled access reviews on blockchain

3	Improve Supply Chain Security	Onboard vendors digitally	KYC smart contract for digital identities
			Procurement contract for requirements
		Enforce compliance policies	Contract penalties for non-compliance
4	Improve Incident Response and Digital Forensics	Attribute actions on the network	Immutable transaction log on blockchain
			Smart contract for response workflow integration
			KYC and CA tracing events to digital identities through smart contracts

F2. Goals, Objectives, and Deliverables Descriptions

Goal 1: Decentralize Security Systems: The primary objective of Goal 1 is to harness blockchain technology to enhance security monitoring across the organization's distributed infrastructure and set the stage for achieving subsequent goals. Currently, individual sites operate separate, isolated security analytics tools that generate logs and alerts, which poses challenges in obtaining a comprehensive view of risks and attacks spanning multiple networks.

Objective 1.a: To transition security event collection, log aggregation, and alerting to a decentralized blockchain network, offering several advantages over the current siloed approach (Xu et al., 2022).:

- **Redundancy and Resilience:** By distributing monitoring data across validator nodes in various regions, the system gains redundancy and resilience, eliminating the risk of a single point of failure.
- **Transparency and Auditing:** All security events and alerts will be cryptographically signed and immutably stored in the blockchain transaction log, facilitating traceability and providing a non-repudiable record for audits and future investigations.
- **Standardized Logging:** Utilizing a smart contract schema will ensure consistent formatting of events, simplifying correlation across diverse tools and vendors.

Deliverable 1.a.i: This involves deploying Hyperledger Besu nodes on Kubernetes infrastructure. Approximately 30 nodes across 5 regions will establish the initial decentralized monitoring network, a task that can be efficiently accomplished using AKS.

Deliverable 1.a.ii: The creation of a Solidity smart contract to define the schema and storage for all security events and logs will ensure the establishment of a tamper-proof "ledger of truth" for incident tracking and management (Buterin, 2014)

Deliverable 1.a.iii: This will provide a dashboard interface for relevant teams to gain unified, real-time visibility into risks and threats, enabling early detection of broader compromises or attacks.

Goal 2: Improve Access Control: The primary objective of Goal 2 is to enhance access control management across the organization's systems, streamlining the currently dispersed and manual processes, which can lead to issues such as excessive or inappropriate entitlements over time (Zyskind et al., 2015.)

Objective 2.a: To enhance identity management practices through digitization and authentication standards, beginning with the fundamental step of knowing exactly who is accessing protected resources.

Deliverable 2.a.i: This involves deploying a Certificate Authority (CA) capable of issuing identity credentials in the form of X.509 digital certificates, binding users' real-world credentials to their network accounts, and establishing a chain of trust.

Objective 2.b: To automate manual access review tasks through the use of smart contracts, which can encode business logic and workflows.

Deliverable 2.b.i: Developing smart contracts that define access permissions and approval/revocation processes for accounts, ensuring programmatic reviews to maintain consistency.

Deliverable 2.b.ii: Scheduling regular reviews of all assigned entitlements through the smart contract to prevent unnecessary persistent access, addressing lapses that may occur in manual reviews.

Goal 3: Strengthen Supply Chain Security: The primary objective of Goal 3 is to enhance security within the supply chain by digitizing vendors and enforcing compliance, replacing the current paper-based onboarding process and annual audits.

Objective 3.a: To transition suppliers, partners, and other third parties to have digital profiles on the network through a KYC (Know Your Customer) process.

Deliverable 3.a.i: Supporting this objective with a smart contract to house digital identity schemas and capture government IDs for correlation, ensuring digital attestation of real-world credentials.

Deliverable 3.a.ii: Expanding the procurement smart contract schema to outline requirements such as security best practices, patching schedules, and data protection controls for outside companies to follow.

Objective 3.b: To automate the verification of third parties' ongoing compliance through compliance audits.

Deliverable 3.b.i: This involves programming penalties directly into the procurement contract, which are automatically enforced if periodic attestations or checks find deviations from agreed terms, acting as a deterrent to non-compliance without requiring costly legal action.

Goal 4: Improve Incident Response and Digital Forensics: The primary objective of Goal 4 is to enhance the organization's incident response capabilities and digital forensics investigations,

addressing the current challenges in attributing suspicious activity to actors and reconstructing event timelines.

Objective 4.a: To leverage blockchain's ability to definitively trace witnessed actions or transactions back to the accountable participant through their digital identity.

Deliverable 4.a.i: Creating the immutable transaction log on the network where all activity, including log collection, smart contract executions, and identity attestations, will be permanently stored (Nakamoto, 2008)

Deliverable 4.a.ii: Developing smart contracts that can automate common steps in incident response, such as isolating impacted hosts and orchestrating evidence gathering from various systems, ensuring consistency.

Deliverable 4.a.iii: Building on the identity layer established in Goal 3, this will allow any events in the blockchain to be undeniably linked to the real individuals or groups responsible through their authenticated digital profiles, providing a "single version of truth" for investigators during and after an incident, with legally defensible attribution and timelines.

G. Project Timeline with Milestones

Sprint 1 (December 18, 2023 - January 10, 2024): The initial priority will be establishing a baseline and deploying a functional distributed blockchain platform to serve as the technological backbone enabling future capabilities. During this sprint, nodes will be initiated at three sites to ensure that the project stays within scope. The Besu clients will run on Kubernetes, allowing for

horizontal scaling. Regular commits will integrate changes from the Product Backlog. At the Sprint Review on January 10, 2024, live demos will showcase transactions stored on-chain across multiple locations, validating basic distributed operations. By the end of this sprint, the initial sites will have the capability to sign and share blocks, indicating network health.

Sprint 2 (January 10-24, 2024): This sprint shifts focus to the Smart Contract developer, who will be working with Solidity. Their task is to design data structures and functions for logging security events in a consistent format. Unit and integration tests will be conducted to ensure that events are properly saved to storage. A significant concern is the risk of complex logging rules breaking future auditing needs. User stories will capture diverse formats to future-proof the model, and development pairs will ensure flexibility through abstraction. By the Review on January 24, 2024, the smart contract should be capable of ingesting sample logs replayed from the production system, with verification by the Product Owner.

Sprint 3 (January 24 - February 14, 2024): The focus of this sprint is on basic authentication capabilities. The team will design an X.509 PKI root certificate and an issuance workflow. The integration will expose the API for generating signing requests. The Review on February 14, 2024, will include a prototype ID portal demo that issues certificates for users to claim their blockchain accounts.

Sprint 4 (February 14-27, 2024): In this sprint, the focus will shift to developing the smart contract logic. The contract will define the structure and permission levels across many accounts and systems. Rigorous Unit and Integration testing will cover edge cases. By the Review on February 27, 2024, the contract should be able to view, grant, and revoke access dynamically,

with transactions simulated on the live network, paving the way for rollout after successful security audits.

Sprint 5 (February 27 - March 20, 2024): This sprint expands the contract's schedule function to include periodic reviews. Governance processes will be debated and modeled computationally for consistency. The Review on March 20, 2024, will showcase contract-triggered reviews running as intended, ensuring that access lists remain current automatically over time.

Sprints 6 and 7: With the foundations of distributed logging and access controls established, the focus will shift to partners and compliance in these sprints.

Sprint 6 (March 20 - April 15, 2024): This sprint will center on capturing digital profiles for third parties. The KYC smart contract schemas will integrate IDs and attributes across procured systems. Automated testing will stress data integrity, including edge cases like document tampering. By the Review on April 15, 2024, a prototype intake portal will populate sample partner profiles into the live contract for tracing. Additionally, during Sprint 6, the procurement smart contract will be updated to include financial penalties for non-compliance, with stakeholder interviews to ensure fair enforcement of agreed-upon requirements.

Sprint 7 (April 15 - May 14, 2024): This sprint will focus on User Acceptance Testing (UAT) across the fully integrated solution. Business and security experts will methodically test every capability, from event logging to identity issuance to compliance attestations. Feedback will identify minor bugs but validate technical success in meeting project goals. The leadership team will sign off on deployment readiness. The next steps will involve the development of a

production rollout plan, change management preparation, and the transition to operations support.

Milestone or deliverable	Duration	Projected start date	Anticipated end date
Deploy initial Besu nodes	80 hours	December 18, 2023	January 10, 2024
Create a digital certificate authority	96 hours	January 10, 2024	January 24, 2024
Develop security event logging smart contract	120 hours	January 24, 2024	February 14, 2024
Build digital identity KYC smart contract	128 hours	February 1, 2024	February 27, 2024
Initial monitoring dashboard	160 hours	February 14, 2024	March 25, 2024
Access approvals smart contract	112 hours	February 27, 2024	March 20, 2024
Add the final two blockchain nodes	64 hours	March 25, 2024	April 8, 2024
Access reviews schedule integration	96 hours	March 20, 2024	April 15, 2024
Procurement contract	80 hours	April 8, 2024	April 29, 2024

requirements			
Compliance penalty programming	128 hours	April 15, 2024	May 14, 2024
User acceptance testing	240 hours	May 14, 2024	June 26, 2024
Pilot digital processes and integrate full workflow through training	160 hours	June 26, 2024	August 9, 2024
Official project completion	1464 hours	August 9, 2024	August 9, 2024

H. Outcome

The primary objective of this initiative is to revolutionize the collection, aggregation, and analysis of security event data across Taranis Energy Corp's distributed environment by decentralizing the security systems. Currently, relying on localized and disconnected security tools in each facility creates vulnerabilities that attackers could exploit. By centralizing logging on an immutable shared ledger, teams gain a comprehensive view of threats that may span multiple locations (NIST, 2018). The Besu nodes forming the backbone of the new blockchain infrastructure will operate as Kubernetes pods distributed behind Azure load balancers across five regions, ensuring redundancy in the face of localized outages or attacks. Successful node connections and block sharing signal the network's resilience, ensuring continuity even if one site encounters issues or falls under malicious control. Once logging smart contracts establish a standardized format for log ingestion, security events will be consistently parsed and

permanently recorded in the blockchain through cryptographic signatures. This creates an indisputable audit trail independent of internal systems. Immutable data storage prevents tampering and establishes a clear chain of custody for forensic investigations.

Another pivotal objective centers around enhancing the management of identities and privileged access across Taranis' intricate environment. Presently, spreadsheets and manual reviews can lead to gaps and potential errors or excessive permissions over time. Smart contracts, programmed with business logic, will create structured digital profiles, delineating differentiated roles through certificates issued by the deployed Certificate Authority (Ripple, 2014). Account privileges will be rule-driven and transparently governed. Scheduled reviews encoded in the contract will ensure assignments remain optimized as needs evolve, replacing fallible human memory. This introduces consistency and accountability absent in previous processes. Contract events permanently recorded on the blockchain serve as irrefutable evidence certifying that controls functioned as intended, bolstering compliance postures.

A final crucial objective is to enhance third-party security by transitioning from opaque paper-based onboarding and audits to digital, rule-enforced standards. Historically, breaches have occurred when compromised outsiders move laterally within the system. Through self-sovereign identity techniques, procurement smart contracts will establish vetted counterparty profiles linked to government IDs and attributed to real entities (Hori, 2022). Enforcing contractual terms like scheduled assessments or maintenance through technical penalties prevents complacency from jeopardizing critical industrial functions. With all activity, including attestations, immutably logged on-chain, excuses for noncompliance become implausible. Transparency across buying consortiums using shared ledgers fosters collective security driven by aligned

incentives for streamlined compliance. Overall, digitization and standardization aim to reduce vulnerability surfaces exploited by sophisticated adversaries.

Before initiating development in Sprint 1, a CSF self-assessment will establish baseline maturity scores (Verve Industrial, 2018). Using the Framework's Profiles, the current status across all Functions and Categories will be documented – supported by evidence from audits, policies, and operational testing. Key focus areas leveraging the Framework's Profile mapping include: asset management under Identify (ID.AM); access control and awareness/training within Protect (PR.AC, PR.AT); anomaly/event detection in Detect (DE.AE); response planning and communications in Respond (RS.RP, RS.CO); and recovery/improvements under Recover (RC.IM). This establishes quantifiable starting points and identifies areas of highest/lowest scores to prioritize improvements through subsequent Sprints. Stakeholder workshops will validate accuracy and prioritization.

Following User Acceptance Testing in Sprint 7, a follow-up CSF assessment will evaluate maturity growth. Demonstrations, leveraging deployments from Sprints, are expected to substantiate enhancements across:

- Identity/access management through decentralized authorization models, standardized credentialing schemes, and automated reviews (PR.AC, ID.AM).
- Visibility and analytics utilizing blockchain event consolidation, alert correlation, and forensic tracing (DE.AE, RS.AN).
- Continuity/resilience from distributed logging infrastructure and smart rules governing accountability (RC.RP, ID.BE).

Metrics around improved detection coverage, reduced dwell times, and enforced third-party diligence will serve as evidence of enhanced capabilities. Interviews/workshops will validate operations meeting strategic goals. A Program Management Review comparing baseline/final Profiles will confirm target Category enhancements. With leadership endorsement of maturity elevations directly addressing priorities, the blockchain initiative will achieve its objectives and progress toward productionization. This final technical assessment, leveraging NIST's Framework guidelines, will objectively signify that project completion milestones have been met.

I. References

Arntz, P. (2017). Explained: YARA rules. Malwarebytes. [Website] https://www.malwarebytes.com/blog/news/2017/09/explained-yara-rules

Berdy, N. (2021, March 17). The layman's guide to X.509 certificate jargon. Microsoft Tech Community. [Website] https://techcommunity.microsoft.com/t5/internet-of-things-blog/the-layman-s-guide-to-x-509-certificate-jargon/ba-p/2203540

Boehm, B. W. (1988). A spiral model of software development and enhancement. Computer, 21(5), 61-72. https://doi.org/10.1109/2.59

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. [Website] https://github.com/ethereum/wiki/wiki/White-Paper

Chawre, H. (n.d.). Blockchain for supply chains [Web page]. Turing.com. https://www.turing.com/resources/blockchain-for-supply-chains

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Cohn, M. (2009). Succeeding with agile: Software development using Scrum. Addison-Wesley Professional.

Cybersecurity and Infrastructure Security Agency. (2021, May 11). Attack on Colonial Pipeline: What we've learned, what we've done over the past two years. [Website] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Daley, B. (2018). The daily scrum in blockchain. Medium. [Website] https://medium.com/@brucedaley/the-daily-scrum-in-blockchain-df5ddf2f2996

Dodis, Y., Ostrovsky, R., Reyzin, L., & Smith, A. (2008). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Scientific Computing. [Journal] https://epubs.siam.org/doi/abs/10.1137/060651380

Entriken, W., Shirley, D., Evans, J., & Sachs, N. (2018). ERC-721 non-fungible token standard. Ethereum Improvement Proposals. [Website] https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

Ethereum Foundation. (n.d.). ERC-20 token standard. [Website] https://eips.ethereum.org/EIPS/eip-20

Gartner. (2020). Gartner says global IT spending to decline 8% in 2020 due to the impact of COVID-19 [Press release]. [Website] https://www.gartner.com/en/newsroom/press-

releases/2020-05-13-gartner-says-global-it-spending-to-decline-8-percent-in-2020-due-to-impact-of-covid19

Global Chip Shortage. (2023, April). In Wikipedia. [Web page] https://en.wikipedia.org/wiki/2020%E2%80%932023_global_chip_shortage

Hori, M. (2022). Self-sovereign identity for procurement. In Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE.

Hostage, C., & Broadwell, P. M. (2015). Resilient command and control: Surviving a cyber attack on critical infrastructure [White paper]. MITRE Corporation.

Hyperledger. (n.d.). Besu - Hyperledger. [Website] https://www.hyperledger.org/projects/besu

Hyperledger. (n.d.). QBFT consensus protocol [Documentation]. [Website] https://besu.hyperledger.org/23.4.0/private-networks/how-to/configure/consensus/qbft

Kapsoulis, N., Psychas, A., Palaiokrassas, G., Marinakis, A., Litke, A., & Varvarigou, T. (2020). Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. Future Internet, 12(2), 41. https://www.mdpi.com/1999-5903/12/2/41

Lee, D., Park, J., & Shin, Y. (2023). Where Are the Workers? From Great Resignation to Quiet Quitting. National Bureau of Economic Research. [Website] https://www.nber.org/papers/w30833

Lundkvist, F., Heck, J., Torstensson, J., Mitton, Z., & Sena, M. (n.d.). C-725 Alliance Identity Standard Proposal v2 [EIP Draft]. [Website] https://github.com/ethereum/EIPs/issues/725

Maram, D., Harjasleen, M., Zhang, F., Jean-Louis, N., Frolov, A., Kell, T., Lobban, T., Moy, C., Juels, A., & Miller, A. (2021). CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability. IEEE Symposium on Security. [Journal] https://ieeexplore.ieee.org/abstract/document/9519473

Microsoft. (2020). Hyperledger Fabric on Azure Kubernetes Service Marketplace template [Blog post]. Azure Blog. [Website] https://azure.microsoft.com/en-us/blog/hyperledger-fabric-on-azure-kubernetes-service-marketplace-template/#:~:text=We%20are%20sharing%20the%20release%20of%20a%20new,solution%20template%20by%20providing%20few%20basic%20input%20parameters

MITRE. (2023). APT29. [Website] https://attack.mitre.org/groups/G0016/

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. [Website] https://bitcoin.org/bitcoin.pdf

NIST. (2018). Blockchain technology overview. National Institute of Standards and Technology.

National Infrastructure Advisory Council. (2017). Securing cyber assets: Addressing urgent cyber threats to critical infrastructure [PDF file]. Cybersecurity and Infrastructure Security Agency. [PDF] https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

Ripple. (2014). The Ripple protocol consensus algorithm. Ripple Labs Inc.

Schwaber, K., & Beedle, M. (2002). Agile software development with Scrum. Prentice Hall.

Sutherland, J., & Schwaber, K. (2020). The Scrum guide: The definitive guide to Scrum: The rules of the game. [Website] https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf

Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

Verve Industrial. (2018). Cybersecurity framework self-assessment tool. Verve Industrial Protection. [Website] https://verveindustrial.com/solutions/by-standard/nist-csf-maturity/

Vogelsteller, F. (2017). ERC: Claim Holder #735. [Website] https://ethereum.org/en/developers/docs/standards/tokens/erc-735/

WannaCry ransomware attack. (2017, May 12). In Wikipedia. [Web page] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, B., & Chen, S. (2016). The blockchain as a software connector. In 13th Working IEEE/IFIP Conference on Software Architecture (WICSA) (pp. 182-191). IEEE.

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE