Blockchain for Supply Chain Cybersecurity, Optimization and Compliance

Michael Mylrea, Sri Nikhil Gupta Gourisetti
Pacific Northwest National Laboratory
{michael.mylrea, srinikhil.gourisetti}@pnnl.gov

***Abstract*— The U.S. power grid is a complex system of systems that requires a trustworthy, reliable, and secure global supply chain. A formidable challenge considering the increasing number of networked industrial control systems (ICS) and energy delivery systems (EDS) and growing number of intermediary distributors, vendors and integrators involved. Grid modernization has increased the use of "smart" energy devices that automate, digitize, network, and bring together the cyber-physical energy supply chain. In the current Energy Internet of Things (EIoT) environment, the growth of data speed and size requirements as well as the number of critical cyber assets has generated new North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance requirements and cyber supply chain security challenges for vendors, regulators, and utilities. The issuance of Order No. 829 by the Federal Energy Regulatory Commission (FERC) instructed the North American Electric Reliability Corporation (NERC) to confront cybersecurity supply chain risk management for ICS software and hardware, as well as the networking and computing services associated with Bulk Electric System (BES) operations. To meet these goals, current technology and processes must be improved to better identify, monitor, and audit vulnerable EIoT environments. This paper examines how blockchain technology can enable NERC CIP compliance as well as aid in the security of the BES supply chain through an immutable cryptographically signed distributed ledger that allows for improved data security, provenance and auditability.**

Keywords— ***Blockchain, NERC CIP, cybersecurity, supply chain, cryptography, internet of things, data provenance, data management, electricity infrastructure, industrial control systems, IoT, cyber-physical security***

I. INTRODUCTION

The U.S. power grid weaves together cyber and physical, OT and IT, devices and networks creating a complex interconnected system of systems. This complexity requires a strong chain of custody for auditing, monitoring, and cybersecurity. Permissioned blockchain technology provides many potential opportunities to enhance the cybersecurity of a supply chain through the use of a decentralized cryptographically signed trust anchor. For example, blockchain distributed ledger technology can improve the auditing of Internet of Things environments. Often, utilities do not have an inventory of their most critical cyber assets, or the ability to track when, where, who, and what software and hardware was developed, shipped, and installed, leaving the systems vulnerable to malicious cyber actors. The use of blockchain provides a means for auditing and tracking the who, what, when, and where of the software and hardware supply chain as well as the data being exchanged in associated transactions.

Blockchain (or distributed ledger technology) has a wide variety of definitions, but for this case, we will define it as a digital ledger or distributed database that records transactions of value using a cryptographic hash function that is inherently resistant to modification [1]. Blockchain maintains a constantly growing list of records (or blocks) that is secured from modification or tampering. Blocks contain a link to the previous block, as well as a timestamp [2]. Blockchain based smart contracts can be implemented without human interaction [3] and the data is not easily modified. Smart contract is digital code which is executed over the blockchain over different nodes to maintain the consensus of the result of the contract. These digital codes are triggered automatically on the ledger based on the conditions specified and the result is stored on the immutable ledger for auditing purposes. Such blockchain smart contract execution is related to exchange of value, without the need for third party intermediaries to exchange value [1]. Blockchains are often classified as either permissioned or permissionless; there are also several types of consensus mechanisms (e.g., proof of work, proof of authority) [4, 5].

This paper provides a summary of the ways blockchain technology can improve the functionality and security of the grid as well as how the technology can facilitate NERC CIP compliance requirements. The blockchain solution explored in this research provides increased security, data provenance, attribution, and auditability to help improve supply chain security and solve related challenges such as: software, patch, and hardware security and optimization challenges prevalent in other critical infrastructure sectors [6 – 11]. The paper is organized as follows: Section II provides an overview of proof of authority (PoA) blockchains, Section III provides a brief introduction to NERC CIP-010, Section IV walks through the use of blockchain for software supply chain management, patch management, and configuration management, Section V highlights some of the potential challenges, and Section VI provides some concluding remarks.

II. OVERVIEW OF PERMISSIONED POA BLOCKCHAIN

Blockchain technology varies greatly in its costs, functional requirements, transaction times, security properties, and consensus algorithms that verify and validate. It is important to understand these differences when applying blockchain to help realize cybersecurity goals. Permissioned proof of authority (PoA) blockchain does not rely on a single party and provides widely witnessed evidence to what can be considered the truth. It can perform validation of data while retaining confidentiality from the outside network (only permissioned nodes can see,

This study was conducted at the Pacific Northwest National Laboratory, which is operated for the U. S. Department of Energy by Battelle Memorial Institute under Contract DE-AC05-75RL01830.

communicate or validate transactions). Proof of authority blockchains can also scale to industrial applications at high speeds. Availability and functionality of scale without prohibitive latency is essential for use in the power grid and other critical processes performed by operational technology such as industrial control and energy delivery systems.

Permissioned PoA blockchains have been around for over a decade and are seeing an increase in industry adoption. Moreover, this technology may help automate and improve cybersecurity and facilitate NERC CIP compliance for utilities.

Smart contracts allow for the execution of digital code which results in various transactions within defined perimeters. These executions of complex transactions take place over the blockchain and are recorded over the distributed ledger. Smart contracts could also help automate supply chain security through dynamic patch management alerts and updates, roles-based access controls and baselining and monitoring machine state integrity. Once the smart contracts are initialized on the blockchain, it gets an address associated with it. That address can be used to interact with the smart contract. That smart contract is present in the form of Bytecode on the blockchain. Blockchain provides an atomically verifiable cryptographic signed distributed ledger, which provides a unique way of distributing trust. Instead of storing supply chain data such as inventory of critical hardware or time, date of patch for critical software, critical supply chain data is stored in the distributed escrow of the blockchain, which maintains time stamped data blocks that cannot be modified retroactively, which increases the trustworthiness and integrity of the data. Several proof of authority blockchain technologies enable secure communications from operational technology protocols and industrial control systems by including an advanced cryptographic signature that assigns the time of signing and data signer to a data asset, as well as authentication.

III. Blockchain and NERC CIP-010.1

Vendors of smart energy technology, energy delivery systems (EDS) and industrial control systems (ICS) continue to prioritize cost savings, functionality, analytic capability, and interoperability over security. Energy utilities use a cost of service return on revenue model, which gives them an incentive to buy energy delivery systems that are reliable and interoperable, not necessarily secure. Therefore, cybersecurity of the grid is often an afterthought. The Federal Energy Regulatory Commission (FERC) approved Order 829 on July 21, 2016, which may encourage energy vendors and utilities to include cybersecurity as part of their design criteria. The order instructed NERC to develop a Reliability Standard directed to supply chain security "for industrial control system (ICS) hardware, software, and computing and networking services associated with bulk electric system operations."

FERC allowed for some flexibility around the implementation of related controls. Utilities are encouraged to prepare cyber smart procurement language, but they are not considered at fault for any new ICS vulnerabilities. The procurement language transfers much of the risk from the utilities to the vendors. It also places some of the responsibility on the vendor to adopt basic hardware and software integrity controls and criteria.

IV. Software, Patch and Configuration Management using Blockchain Technology

A blockchain based platform may help reduce cost and increase of effectiveness of grid cybersecurity efforts through the automation of the NERC CIP compliance process. The distributed ledger technology would cryptographically sign the, who, when, where, and what for all critical cyber assets, both hardware and software, throughout the chain of custody. Currently, the NERC CIP process is burdensome and resource intensive, especially for small utilities that don't have the necessary expertise to realize their compliance goals. Many people complain that the process is ineffective in assuring the growing number of networked field devices are secure. Blockchain technology could revolutionize how utilities and regulators monitor, secure and realize compliance requirements for complex energy Internet of Things environments. To fulfill this goal, blockchain provides the following:

1. An increase in transparency of a systems machine state integrity and the ability to audit the system and network throughout the entire lifecycle
2. Software, hardware, and firmware records that are archived and tracked in an immutable distributed ledger
3. Increased accessibility and visibility of supply chain data that enhances and expedites inter-vendor cooperation
4. Component traceability throughout the entire lifecycle of the system to assure efficient and secure processes
5. Improved monitoring of critical cyber assets, both hardware and software, which facilitates auditing, security and compliance.

A. Blockchain based software supply chain management

The software development process for new products or for upgrading process of existing products often involves multiple global teams working in tandem, external consultants, third-party open source libraries, and many other disparate pieces that are different to track. The process of integrating various modules through a secure, verifiable, and accountable practice may be simplified by dividing the method into three phases:

1. Software module processing: During the development phase, various software modules from the development teams, open-source libraries, and other sources may be used. If every module development team is registered to the blockchain, the state of each module when being assembled is stored on the blockchain which will prove its provenance. Any state changes on the modules are recorded on the blockchain in the form of a transaction which is linked to the previous state of the product. Upon achieving the final module (sub-product), it can be validated at any point in the future by registering with the blockchain and accessing the module's virtual profile. Throughout the development process 1) all the different steps including addition of new modules (hardware/software) become a part of individual transactions which become an immutable part of the blockchain linked to each other based on their transaction ID, 2) rules can be integrated into the smart contract to perform periodic validation processes and generate

alerts upon identifying any malicious unsigned code (software module) or if a signature from an unknown source is detected, and 3) software going further can be remediated due to the immutable nature of the blockchain and the associated smart contract can be triggered to roll the software back to a known good (verified, validated, and tested) state for the users.

2. Software combination and integration: Approved third-party libraries and modules developed by individual teams can be combined together as part of different transactions suggesting that every step of development and integration gets added to the ledger and are linked to each other by the previous transaction ID, hence forming a chain of linked transactions before the final desired software product is created. To ensure the integrity of the software in a collaborative but potentially trustless environment, the modules can be cryptographically signed and transferred for aggregation. Therefore, throughout the software development process, all modules can be signed to create individual provenance components—all associate with the software's virtual profile registered with the blockchain. At the aggregation end, the module is verified by backtracking the various linked transactions from the end to the very beginning of the provenance of different steps involved using the transaction ID. Upon integration of all the modules, the software package or product is cryptographically signed and registered with the blockchain.

3. Software transfer: Upon verified integration, the software can be released to the user and/or consumer space. As long as the user is a permitted node on the blockchain, at any time in the future, every module that is part of the software can be verified and validated. The associated development history of the software may include individual authors of the modules, and an entire history of the code versioning, integration, and testing processes. Therefore, the software buyer can validate the software modules prior to integration.

Although the above depicted process is very simplified, the underlying principles can be adopted towards software development processes irrespective of the number of steps and processes involved. The goal of the above illustration was to introduce and depict the secure process of software development using blockchain technology.

B. Blockchain based patch management

Most large organizations and facilities, such as energy utilities, consist of a multitude of devices. In the energy facilities, these devices often include both information technology (IT) and operational technology (OT) devices, such as supervisory control and data acquisition (SCADA), human machine interfaces (HMI), and remote terminal units (RTU). Due to a high emphasis on availability – the requirement to keep the facility operational with very minimal to no downtime – cyber secure patch management is an afterthought. As much as possible, the systems are either patched manually or through a third-party vendor, which can not only expose them to potential cyber threats but may also disrupt the operational environment. The traceability, transparency, and accountability features of blockchain technology could mitigate some of the challenges associated with patching critical IT and OT systems.

Since cryptographic hashing is one of the key attributes of blockchain that allows data-centric security, ensuring the legitimacy, security, and potential compatibility of a patch can be achieved through blockchain. To illustrate this, assume that an asset vendor and asset owner are nodes of a blockchain. The patch generated by the vendor can be tagged by the asset vendor along with its release. The asset owner can track and verify the patch based on its history associated with the tag in real-time. Upon verification, the asset owner can install the patch in the test environment, update the tag with any findings, and identify any issues with the patch. This information can be seen by other nodes on the blockchain, including the asset vendor. Upon obtaining a final stable patch, the asset owner can install the patch in the production environment.

To take the above description to another level, the patch management process may also be automated using blockchain. In such a scenario, an individual device can be configured to update a blockchain node and a smart contract can be developed to execute upon identifying a new patch or its tag on the blockchain. In this scenario, the asset's smart contract will be executed to obtain the patch from a secure location; this will be recorded in the blockchain's immutable ledger. Upon unit testing and installation, another update is pushed to the asset's tag. Throughout the patch lifecycle—from its release to the point where all assets are patched—the entire process can be tracked through its tag in the blockchain and can be traced back to any point in its history. Fig.1. depicts the blockchain based patch management process.

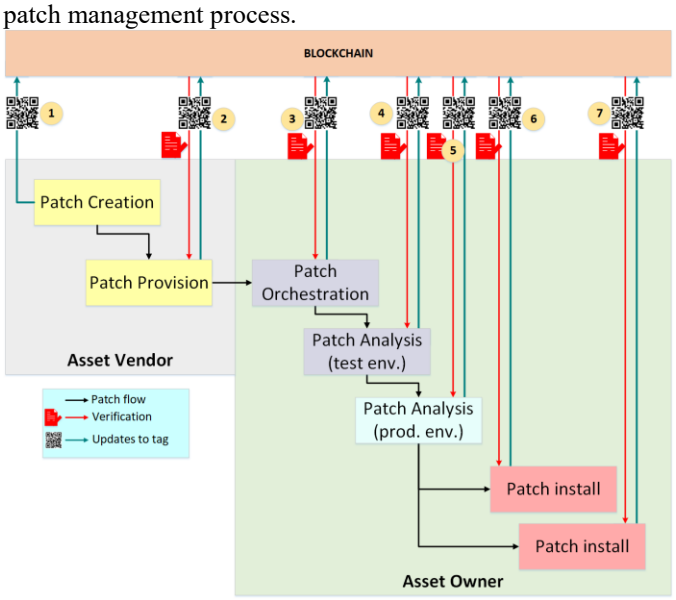

Fig. 1. Illustrative work-flow of blockchain based patch management

The below sequence of steps will walk through the illustration shown in Fig.1:

Step-1: The asset vendor begins the process of patch creation. Along with the initiation of the process, the vendor also creates a unique identifier (such as a QR code) and registers the cryptographically signed unique identifier with the blockchain. Therefore, a cryptographic link is established between the QR code and the patch. The QR code stays as a constant tag through the patch's life cycle and by scanning it, the asset vendor and asset owners can be connected to the virtual profile

associated with the tag. The virtual profile holds the entire history associated with the patch development, testing, analysis, and integration processes. All the updates and development done towards patch creation are pushed to the virtual profile associated with the QR code.

Step-2: Irrespective of whether the patch is developed under a single facility or is being developed in a multi-partner collaborative environment, there is always a possibility for the patch to be corrupted by an attacker. Therefore, during the patch provision or release phase, the vendor's release team will first verify the integrity of the patch (purple arrows in Fig.1). Upon verification, validation, and testing, the patch is released to the asset owner space.

Step-3: Patch processes may vary in an asset owner's space. For the sake of this illustration, it is assumed that the asset owner performs patch orchestration initially. During this step, the asset owner may perform some patch automation and coordination services that may not be common across various asset owners. The vendor first verifies the patch based on the history recorded in its virtual profile. Since the asset owner is another permitted node in the blockchain, the owner will be able to scan the QR code and retrieve the immutable virtual profile. Upon verification, patch orchestration is performed, and the asset owner updates the virtual profile with findings, the current state, and any other relevant information.

Step-4: The patch is then verified and installed in a test environment. This may be done manually by a tester team or possibly can be automated. Under automation, a smart contract can be executed upon the availability of a new software/patch item on the blockchain. The smart contract would initiate the verification procedures. Upon verification, it will invoke a system level application that can take the patch and install it in the test environment. Upon validating the patch in the test environment, another native application will combine all of the findings and analysis reports. This new data will be transferred to the patch's virtual profile through another smart contract. If the validation fails, the asset vendor will be able to immediately know the details of the failure through the virtual profile. Therefore, since the asset vendor and owner are active blockchain nodes, securing and updating the patch can be potentially performed in an autonomous fashion.

Step-5: This step is very similar to step-4 but is performed in the production environment. Through the validation processes, if any associated systems are observed to be impacted, the patching process is halted and reverted to the previous stable version. This information is sent to the virtual profile, which can be used by the vendor to design a fix.

Step-6: Finally, the patch is pushed to all relevant systems. Upon any hurdles, the virtual profile is updated, and the vendor is notified immediately.

This novel blockchain based patch management solution has not been designed or tested in a production environment. Due to its potential to facilitate a cybersecure patch testing and installation process with no intervention of third-party personnel, blockchain based patch management shows tremendous promise especially in a converged IT/OT environment. Some of the advantages for the proposed process include the following:

1. Patch does not change as it moves throughout the process.
2. Patch can be verified at each step, providing transparency.
3. Patch can be validated at each step. Therefore, anything anomalous during transit or at rest should be detected.
4. Patching process could potentially be automated to some degree with a smart contract. This could be facilitated by vendor testing of the patch on systems in a controlled environment. The challenge being systems and network configurations in energy utilities are not uniform

C. Blockchain based configuration management

It is challenging to identify and protect critical cyber assets (e.g., EDS, IoT, ICS) when network-enabled field devices and other smart technologies are not inventoried and monitored or are deployed without basic security or operation controls in place. If a malicious adversary understands an organization's networks and systems better than those protecting it, the risk that the system will be compromised is increased. Distributed ledger technology enables organizations to more effectively conduct inventories and oversee critical cyber assets in complex supply chains that are found in the utilities' infrastructure, as well as other critical infrastructures that are becoming more vulnerable to cyber-physical threats.

Blockchain can help increase the auditability of critical systems, allowing for data integrity in complex supply chains and cyber risk management efforts. This is essential for IoT environments found in critical infrastructures such as the electricity grid. Automating these functions can significantly enhance cyber risk management for the power infrastructure.

The core of NERC CIP-010 has three configuration management and vulnerability assessment requirements (denoted as R1, R2, and R3) that are associated with their respective measures (M1, M2, and M3). Fig. 2–11 depict those requirements and how the application of blockchain technology facilitates the implementation and compliance of these controls.

NERC CIP-010 requires documented proof to show that the cyber assets baseline configurations are modeled, and periodic vulnerability assessments are performed. The documentation shall include evidence of the cyber assets baselining, a list of cyber controls, differences between test and production environments, vulnerability assessments tools, findings of those assessments, and other relevant information. The documented information may be used during the auditing process. In the current state, there is often minimal documentation that provides all the details related to baseline configuration management and vulnerability assessments. Therefore, checks for compliance can lead to subjective decisions based on available information. Blockchain technology can facilitate the implementation of the compliance process requirements (left column in Fig. 2–11) with blockchain controls (right column in Fig. 2–11) to ensure NERC compliance.

As shown in Fig. 2, the first requirement, R1, focuses on the configuration change management process by the responsible entity. As per NERC CIP-010 documentation, a responsible entity may be defined as the entity that owns the control system (example: a utility that owns the control systems). The R1 requirement is further divided into five segments:

R1.1. Develop baseline configuration that includes critical elements listed in Fig. 2.

R1.2. Authorize and document changes that deviate from the existing baseline configuration.

R.1.3. For a change that deviates from the existing baseline configuration, update the baseline configuration under a defined period of time.

R1.4. Perform needed tests in the test environment and document the results for a change that deviates from the existing baseline configuration.

R1.5. Perform needed tests in the production environment and document the results for a change that deviates from the existing baseline configuration.

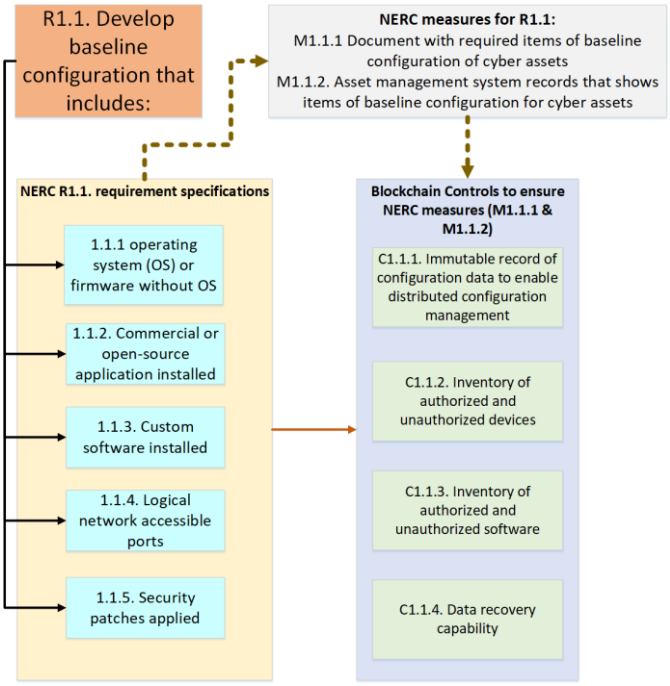

Fig. 2. Blockchain technology for configuration management (R1.1)

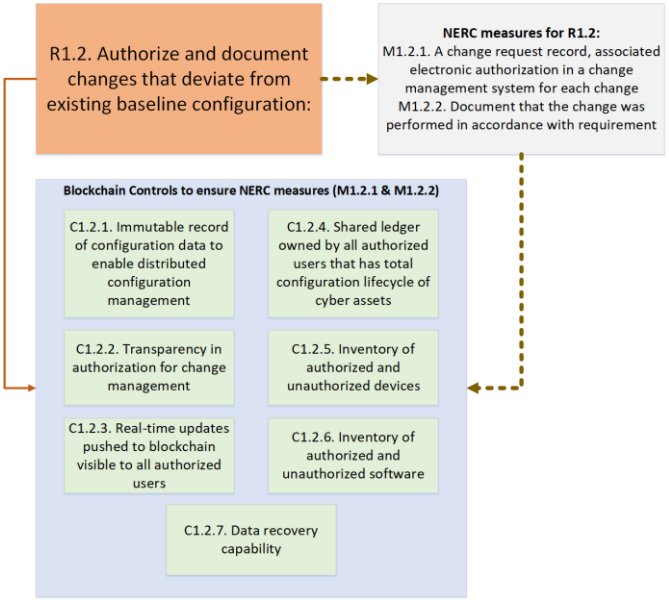

Fig. 3. Blockchain technology for of configuration management (R1.2)

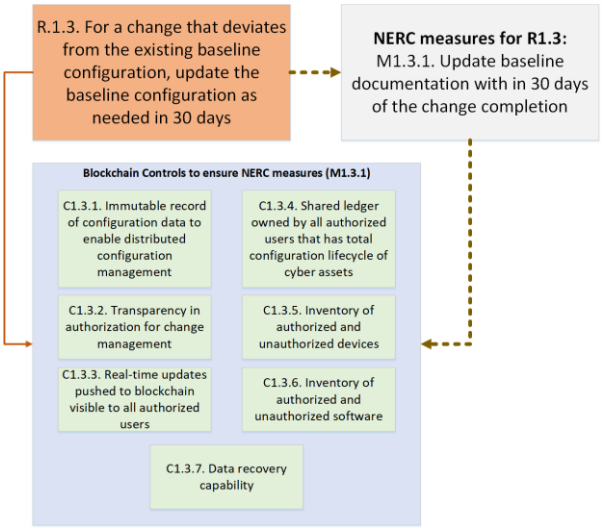

Fig. 4. Blockchain technology for configuration management (R1.3)

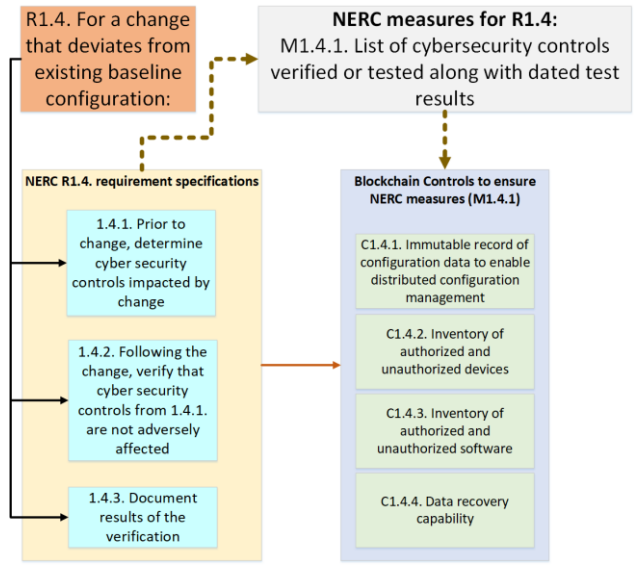

Fig. 5. Blockchain technology for configuration management (R1.4)

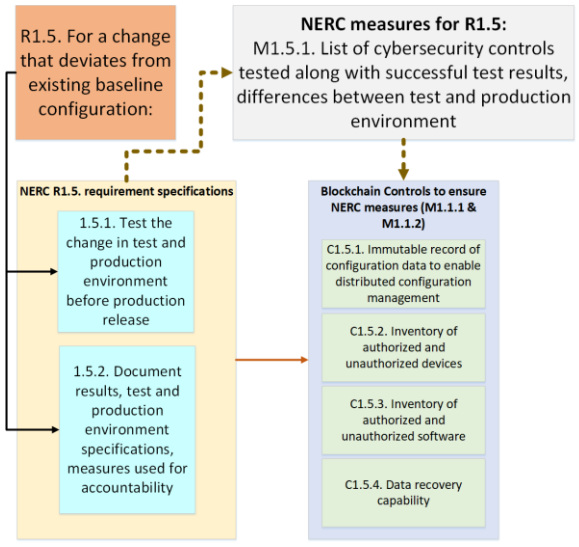

Fig. 6. Blockchain technology for configuration management (R1.5)

As per NERC CIP 10, the configuration management should consider the above factors to enforce measures M1.1.1, M1.1.2, M1.2.1, M1.2.2, M1.3.1, M1.4.1, and M1.5.1. Those measures focus on the documentation of findings.

The second requirement, R2, focuses on implementing the configuration monitoring that is developed by meeting the R1 requirement. Core aspects of the R2 include the following:

R2.1. Complete periodic monitoring of changes to baseline configuration. Document & investigate unauthorized changes.

Measure M2.1.1 is met when the responsible entity can show the documentation of identified anomalies. Fig. 7 shows how the associated blockchain controls can facilitate R2.

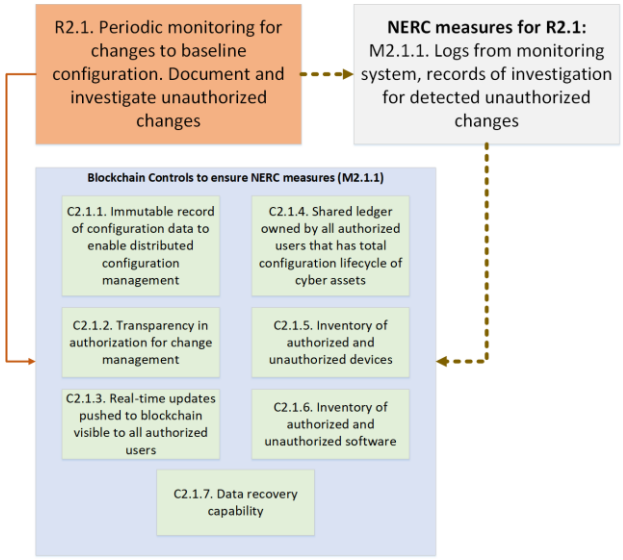

Fig. 7. Blockchain technology for monitoring configuration changes (R2.1)

The final requirement, R3, is to perform vulnerability assessments (see Fig. 8–11). This is further divided as the following sub-requirements:

R3.1. Conduct periodic vulnerability assessments.

R3.2. Determine parameters related to performing vulnerability assessments in test and production environments.

R3.3. Perform active vulnerability assessments on new cyber assets before connecting in the production environment and model baseline configuration.

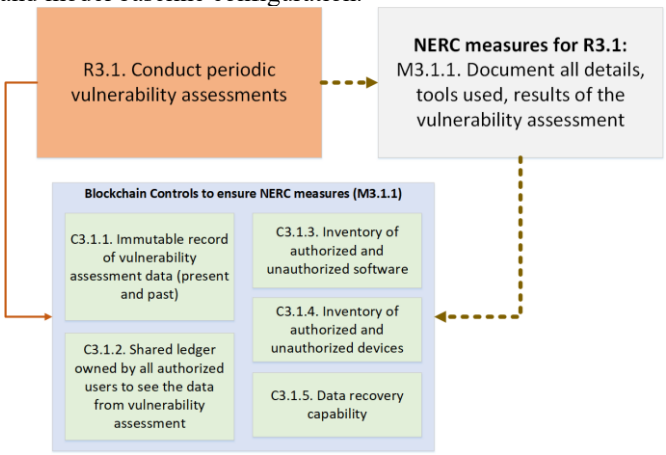

Fig. 8. Blockchain technology for conducting periodic vulnerability (R3.1)

R3.4. Develop a time-boxed action plan to mitigate vulnerabilities discovered in active vulnerability assessments.

The measures M3.1.1, M3.2.1, M3.3.1, and M3.4.1 will determine the level of R3 compliance.

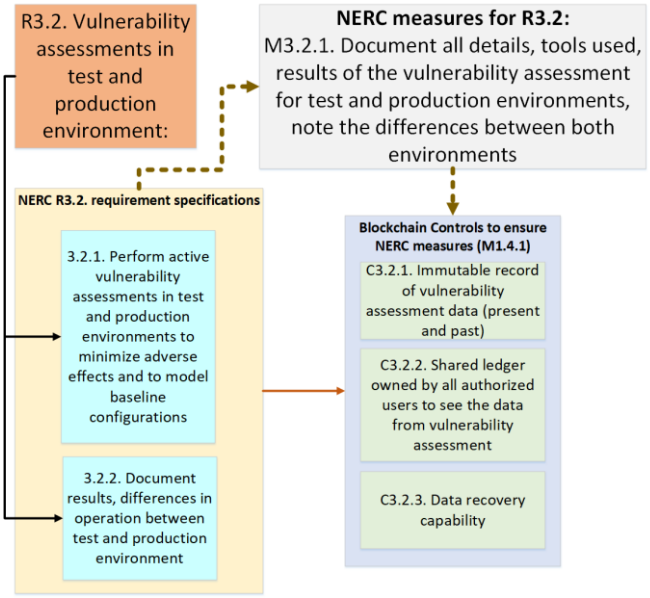

Fig. 9. Blockchain technology for conducting vulnerability assessments in test and production environments (R3.2)

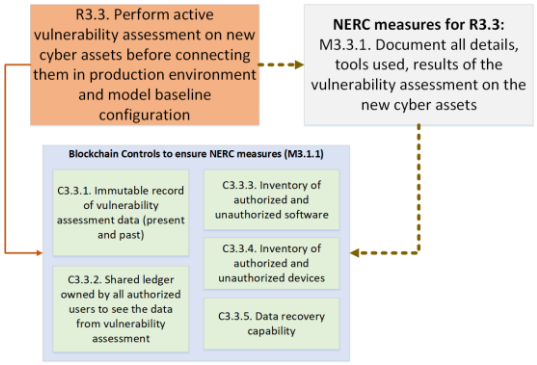

Fig. 10. Blockchain technology for conducting vulnerability assessments on new cyber assets (R3.3)

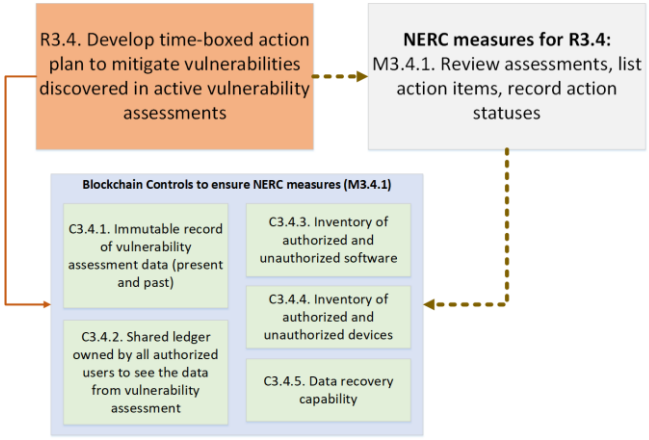

Fig. 11. Blockchain technology for developing time-bozed action plan to mitigate vulnerabilities (R3.4)

Fig. 2 – 11 depict four to seven different blockchain controls that may be leveraged to address various aspects of R1, R2, and R3 to ultimately satisfy their respective measures. Below are the seven controls that can be facilitated through blockchain technology:

1. Immutable record of configuration data to enable distributed configuration management
2. Inventory of authorized and unauthorized devices
3. Inventory of authorized and unauthorized software
4. Data recovery capability
5. Transparency in authorization for change management
6. Shared ledger owned by all authorized users that has total configuration lifecycle of cyber assets
7. Real-time updates pushed to blockchain visible to all authorized users

The blockchain or distributed ledger consensus algorithm is updated as the responsible entity makes progress toward helping to automate and better track the above processes to meet requirements R1, R2, and R3. The responsible entity can simply access the blockchain to track and enforce the measure. Similarly, the NERC auditing process can leverage the blockchain's distributed ledger technology to retrieve all required information to check for compliance.

V. Blockchain Business and Implementation Challenges

Blockchain provides the prospect of increased security and optimization for energy utilities but is not a panacea. Before applying blockchain technology to secure electricity infrastructure, it is important to understand the implications. The application of the wrong blockchain solution can create more problems and costs than solutions. Blockchain solutions must be economical, energy efficient, and interoperable when they are tracking and securing large data sets. When considering requirements for grid cyber use cases, functionality, scalability, speed, cost, and cyber resilience are important factors.

This article highlighted a number of blockchain supply chain security benefits among others [12]. However, many challenges remain in the application of a distributed ledger system to secure and optimize electricity infrastructure. Authors of this paper are currently exploring an applied use case of this concept to validate and verify the opportunities and challenges of blockchain for electricity infrastructure optimization and security.

One of the challenges highlighted by this research is that blockchain technology is new and there are many different definitions for blockchain. This creates a number of challenges for researchers, regulators and policy makers working to establish applications and governance for blockchain technology.

There are also significant knowledge gaps related to functionality, cost, security, and energy efficiency, especially when evaluating public proof of work blockchain solutions. There can be an excessive amount of energy required to solve proof of work consensus algorithm and there are a number of privacy concerns with public blockchain solutions. Some proof of work servers are located in areas that have had issues with intellectual property theft and suffer from rampant economic espionage. Proof of work systems can also require complex puzzle-solving algorithms [13, 14] as part of the consensus process, which can lead to prohibitive latency and costs for various time sensitive transactions.

Another challenge is that non-functional and functional requirements, as well as the technology stack, are often changing in order to integrate the blockchain technology and to be sure that system manufacturing is tracked throughout the entire development lifecycle. In addition, when there are different vendors involved using different blockchain technology that can create various interoperability issues. This can be solved, in part, by using an intermediate node between various blockchains and data bases.

VI. Conclusion

Grid modernization has increased the deployment of smart internet connected energy technology that is potentially vulnerable to cyber threats. Securing these devices and realizing new NERC CIP compliance requirements continues to challenge energy utilities, especially organizations that lack the necessary resources. Innovative solutions are needed in response to these complex and evolving cyber challenges. This paper explored various opportunities and challenges in applying blockchain distributed ledger technology to optimize and secure the complex software and hardware supply chain that makes up modern energy utilities.

Acknowledgement

The authors would like to acknowledge Scott Mix for his contribution towards the paper through a one-on-one interview on NER CIP-010 standard.

References

[1] A. Tapscott, "The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World," Portfolio, 2016

[2] L. Trottier, "original-bitcoin," 2013, Github

[3] P. Franco, "Understanding Bitcoin: Cryptography, Engineering and Economics," John Wiley & Sons, 2014.

[4] POA Network, "Proof of Authority: consensus model with Identity of Stake," Medium, 2017

[5] A. Walch, "The Path of the Blockchain Lexicon (and the Law) 36 Review of Banking & Financial Law 713," University College London, 2017

[6] M. Mylrea, "Blockchain Cybersecurity for Critical Infrastructure," Artificial Intelligence Conference, Stanford University, 2018

[7] M. Mylrea, S. Gourisetti, "Blockchain: A Path to Grid Modernization and Cyber Resiliency," IEEE North American Power Symposium, WV, 2016

[8] M. Mylrea, et al, Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security, Resilience Week, 2016

[9] M. Mylrea, S. Gourisetti, R. Bishop, M. Johnson, "Keyless Signature Blockchain Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure," IEEE PES T & D. Conference & Exposition, 2017

[10] M. Mylrea, S. Gourisetti, "Leveraging AI and Machine Learning to Secure Smart Buildings," AAAI, Stanford University, Springer, 2017

[11] NERC CIP., "CIP-010-1 – Cyber Security – Configuration Change Management and Vulnerability Assessments," Retreived on March 1'18.

[12] A. Pradhan, et al, "Supply Chains Are Racing to Understand Blockchain – What Chief Supply Chain Officers Need to Know," Gartner, 2017

[13] S. Deetman, "Bitcoin Could Consume as Much Electricity as Denmark by 2020," Motherboard, 2016

[14] A. Hern, "Bitcoin mining consumes more electricity a year than Ireland," The Guardian, 2017