Blockchain: Next Generation Supply Chain Security for Energy Infrastructure and NERC Critical Infrastructure Protection (CIP) Compliance

Michael Mylrea
Pacific Northwest National Laboratory
Richland, WA, 99354, USA

Sri Nikhil Gupta Gourisetti
Pacific Northwest National Laboratory
Richland, WA, 99354, USA

ABSTRACT

The U.S. power grid is a complex system of systems that requires a secure, reliable and trustworthy global supply chain. This is especially true for the grid's increasing number of networked energy delivery system (EDS) and industrial control systems (ICS) and associated vendors, distributers, integrators and end users. Grid modernization has increased the use of "smart" energy devices that network, digitize, automate and increasingly converge the cyber-physical energy supply chain. In this Energy Internet of Things (EIoT) environment there is an increasing number of both critical cyber assets as well as data speed and size requirements, creating new cyber supply chain security and NERC CIP compliance challenges for utilities, regulators and vendors. On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to address cyber security supply chain risk management for ICS hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations. In realization of these goals, improvements are needed in in the process and technology to better identify, monitor, audit, realize compliance goals and secure EIoT environments. This paper explores how blockchain technology presents a disruptive solution to facilitate NERC CIP compliance and increase the security of the BES supply chain through a cryptographically signed distributed ledger that provides increased data provenance, attribution 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

1. INTRODUCTION

The distributed *form* of a blockchain ledger complements the distributed *function* of a global energy infrastructure supply chain. The power grid weaves together cyber and physical cyber assets, information and operational technology, software and hardware, in a way that requires an improved chain of custody for monitoring, auditability and cyber security. Permissioned blockchain technology provides a consensus mechanism and trust anchor via a cryptographic hash that signs the who, what, when and where of the data in a block that becomes a widely witnessed, auditable and immutable event. This presents a number of potential opportunities to increase the cyber security of a supply chain that is increasingly distributed, data driven, global and vulnerable.

For one, blockchain facilitates the auditability of IoT environments: if you don't have an inventory of your critical cyber assets or ability to track who, what, when and where a critical cyber asset was developed, shipped and installed. Currently, these desperate data sets are often not tracked and monitored by utilities, creating an opportunity for malicious actors to exploit this knowledge gap in the chain of custody. Similarly, utilities often don't have visibility into the machine state integrity of field devices and other embedded systems. Thus, it becomes very challenging to detect, protect and respond to anomalies and cyber events. The following paper provides an overview of how blockchain technology can help improve the state of the art in responding to both of these challenges in realization of grid cyber and NERC CIP compliance goals.

Blockchain or distributed ledger technology (DLT) has many definitions. For this paper, blockchain is defined as a distributed database or digital ledger that records transactions of value using a cryptographic signature that is inherently resistant to modification [1]. Blockchain is a distributed database that maintains a continuously growing list of records, called blocks, secured from tampering and revision. Each block contains a timestamp and a link to a previous block [2]. Blockchain-based smart contracts can be executed without human interaction [3] and the data is more resistant to modification as the data that forms a block cannot be altered retroactively. Blockchain smart contracts are defined as technologies or applications that are executed on the participating nodes to maintain consensus of the result related to the exchange of value without intermediaries acting as arbiters of money and information [1]. With those fundamentals defined, blockchains can be classified as permissioned and permissionless. Further, there are several types of consensus mechanisms such as proof of work (PoW), proof of authority (PoA) [4, 5], etc. This paper primarily focuses on potential applications of permissioned proof of authority blockchain technology for secure supply chain and data management and facilitating NERC CIP 13 supply chain cyber security compliance requirements. Certainly, blockchain solution explored in this research provides increased security, data provenance, attribution and auditability that can help solve supply chain security and optimization challenges prevalent in other critical sectors [6–11]. The use of blockchain technology for supply chain management has been proposed for various sectors such as agri-food [12], pharmaceutical and other manufacturing [13 – 15] industries. Some of the blockchain based supply chain use-cases are:

1) *Agri-food use-case (using RFID) [12]:* In [12], the authors demonstrated blockchain and RFID based supply chain system to solve the challenges associated with traceability, inspection, safety status of food products. This is done by developing a transparent platform to: 1) have complete knowledge of the food product all the way from farm to the consumer; 2) be prepared in case of a safety accident that may lead to emergency measures. In this use-case, the participating actors may include the farm, plant or storage unit, warehouse center, sales market, transportation agency, regulatory agency, and customers. According to

[12], the products will be associated with RFID tags for data acquisition, circulation and sharing. This information will be visible to all authorized actors and can be updated throughout the food product's lifecycle in production phases, processing phase, warehousing phase, distribution phase, and sales phase. According to [12], such implementation will enable: 1) real-time tracking, monitoring and tracing of the product; 2) transparent information gathering, transmission and sharing of that information about the product across the authorized actors; 3) a platform for government department and third-party regulators to audit and check for safety requirements. In addition to the work detailed in [12], many industries [16] have already been implementing and testing the use of blockchain in food industry: [17 – 20] describes the use of blockchain supply chain to improve food safety and potentially prevent deaths; [21] highlights the use of blockchain in food safety to solve traceability challenges; [22, 23] not only highlights the use of blockchain supply chain and food safety but also details the associated challenges and security aspects; [24] articulates the use of blockchain supply chain for data visibility, process optimization, and for verified transparent trading; [25] takes a step further in agri-food supply chain use of blockchain: here, the authors talk about tracking the agricultural land, livestock wellness, and farming models as part of food safety models.

2) Manufacturing systems use-case (using RFID/QR/barcode) [14]: In [14], the authors demonstrated the use of blockchain in carboard manufacturing supply chain process. It was proposed that the product would be associated with a tag that contains a QR or RFID or barcode. Each tag associated with individual product represents a unique cryptographic identifier. The tag links the physical product to the virtual identity of the product on the network. Authorized actors such as registrars, standards organizations, certifiers, producers, manufacturers, distributors, retailers, waste management organizations, and consumers can register to be part of the blockchain network (upon authorization). Once registered, an actor can access the physical asset's virtual profile by scanning the tag. This way, current and past state of the product is visible to all actors and can be verified and validated throughout its manufacturing process.

It is evident from the above use-cases that blockchain technology has unique and much needed advantages that it can offer in supply chain space. Although blockchain supply chain has been explored in various manufacturing sectors, the technology has not been explored much in the energy or power grid space. Energy and grid space is rather a unique area where the utilities are required to be in compliance with various NERC requirements. Often, the systems and devices that the utilities need are manufactured based on the utility's requirements. Therefore, in case of grid supply chain use-case, the consumer may initiate the process rather than the manufacturer. This paper specifically explores various aspects of the use of blockchain technology coupled with scannable QR/barcode in energy supply chain management. Rest of the paper is organized as follows: Section – 2 introduces blockchain technology and NERC CIP 13; section – 3 highlights NERC CIP 13 requirements and blockchain controls that enforce the compliance; section – 4 details about the role of blockchain in supply chain management; section – 5 depicts an illustration about the use of PoA blockchains for supply chain management; section – 6 answers fundamental applicability questions about blockchain; section – 7 highlights some of the challenges; and section – 8 concludes the paper.

2. BLOCKCHAIN AND NERC CIP 13

A. NERC CIP 13 Supply Chain Security Background

Vendors of smart energy technology or ICS and EDS continue to prioritize functionality, interoperability, cost savings and analytic capability over security, which is often times an afterthought. Utilities have a return on revenue model that incentivizes them to buy energy delivery systems that are interoperable and reliable with their functional requirements of keeping the lights on, not securing the grid. As a result, grid cyber security is often an afterthought. The Federal Energy Regulatory Commission (FERC) approval of Order 829 on July 21, 2016 may help incentivize energy utilities and vendors to consider cyber security as part of their value propositions. The FERC order directed NERC to develop a Reliability Standard focused on supply chain security "for industrial control system (ICS) hardware, software, and computing and networking services associated with bulk electric system operations." This new standard creates a number of new supply chain and compliance challenges for electric utilities:

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

"Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle [11], as shown in Fig. 1."

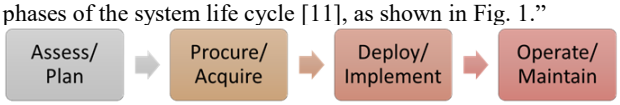

Fig. 1. Notional BES Cyber System Life Cycle [11]

FERC provided some flexibility around *how* related controls are implemented. The new order encourages utilities to draft cyber smart procurement language but does not hold utilities at fault for new ICS vulnerabilities. Procurement language puts more of the responsibility on the vendor to adopt basic software and hardware integrity criteria and controls. Procurement language also helps transfer risk from utilities to vendors.

3. BLOCKCHAIN COMPLIANCE MONITORING AND CYBER RESILIENCE

A blockchain based platform could help reduce the cost and increase the effectiveness of grid cyber security efforts through automating NERC CIP compliance process. The distributed ledger would cryptographically sign the who, what, when and where for critical cyber assets throughout their entire chain of custody, including monitoring the machine state integrity of deployed assets. Currently, the NERC CIP process is resource intensive, burdensome and often ineffective in securing the increasing number of networked field devices. Security controls – like white listing and laborious physical inventories and monitoring of critical cyber assets are challenging due in part to the increasing number of devices with connectivity. Not only is the attack surface increasing, but utilities can be fined up to $1 million dollars per day for NERC CIP noncompliance. Instead of periodic laborious compliance and security CIP assessments,

both regulators and utilities could use blockchain technology to facilitate monitoring and securing of complex energy IoT environments.

In realization of this goal, blockchain technology has several benefits that could improve supply chain cyber risk management and NERC CIP compliance:

1) Increased transparency and auditability of the system throughout the manufacturing, shipping, deployment and maintenance and retirement life cycle. The chain of custody and monitoring of field devices are provisioned and tracked in the blockchain through their entire life cycle;
2) Immutable archived records about the firmware, hardware, and software components of the system including the past and current patch management information can be widely witnessed through a cryptographic hash of their metadata captured in an immutable blockchain instead of a single server that can be manipulated or erased;
3) Expedites and enhances inter-vendor cooperative system development through increased visibility and accessibility of supply chain data;
4) Improved security of the supply chain process through increased trustworthiness and integrity of data through blockchain consensus mechanism which reduces reliance and can even replace need for intermediary trust mechanisms and brokers that are susceptible to manipulation and compromise;
5) Principle component traceability throughout the system lifecycle to incorporate efficient systems engineering processes;
6) Improved audibility and monitoring of critical cyber assets facilitates compliance and improves security of devices. The blockchain consensus algorithm could flag if a field device was not patched and may help deny a malicious change in the configuration of a field device by default.

The blockchain architecture helps ensure the data integrity throughout the chain of custody by verifying the identity of the sender and signer and alerting if the data have been manipulated. A cryptographically signed hash of the data is captured as a block in the chain and a regulator returns a signature token to the sender at each route along the supply chain (e.g., vendor, supply, customer). In the context of NERC CIP compliance, the hash would be sent to the regulator along with chain-of-custody data and device logs, which could potentially help verify everything from machine state integrity to software version and patch information using the hash calendar on the blockchain. Sending the logs and machine state separately helps increase the availability and security of the data.

The blockchain architecture produces a Merkle tree with the root hashes and the hash calendar is published in the blockchain. Because of the blockchain includes a hash of the metadata, the calendar helps preserve the privacy of the data. The blockchain uses the hash instead of actual data, the signature token, which consists of the data to reconstruct the path from its hashed value to the top of the tree. All that information is required by the client to verify the validity of the signed data. This helps in verifying the existence of the client's hash in the tree. For example, in **Error! Reference source not found.**2, the left side shows the construction of a Merkle tree and the right side is verification of the presence of *y* in the tree. Here, x_1 through x_4 are different hashes that get concatenated to obtain higher level nodes x_{12} and x_{34}. The nodes are further concatenated to yield the root node of the tree, x_{top}. Now, to verify if y exists in the tree (in place of x_2), x_1 and y are concatenated to obtain a node $y_2 = h(x_1 \mid y)$. Then, this node is concatenated with x_{34} to obtain $y_3 = h(y_2 \mid x_{34})$. If $y_3 = x_{top}$, then y exists in the tree [16].

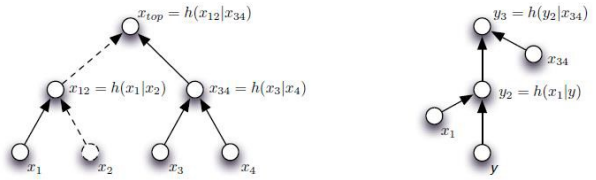

Fig. 2. Computation of Hash Tree Consensus Algorithm and Verification of a Hashed Node [16]

A. Relationship of NERC CIP 13 Requirements, Measures with Blockchain Controls

Identifying and protecting critical cyber assets (e.g. EDS, IoT, ICS) is incredibly challenging as networked enabled field devices and other smart technology are deployed without basic security design or deployment controls in place. If a malicious adversary knows a utilities systems and networks better than the people protecting it, there is an increased risk that these systems will be compromised. Distributed ledger technology provides a better way to conduct inventory and monitor critical cyber assets in complex supply chains found in electricity infrastructure sector and other critical infrastructures that are increasingly networked, digitized and vulnerable to evolving supply chain and other cyber-physical threats.

Blockchain adds auditability, non-repudiation and data integrity to complex supply chains and cyber risk management efforts. This is very much needed for IoT environments found in critical infrastructures, such as the power grid. Automating these functions through monitoring integrity of field devices can improve the state of the art and significantly improve cyber risk management for electricity infrastructure.

The core of NERC CIP 13 has three supply chain security requirements (denoted as R1, R2, R3) that are associated with their respective measures (M1, M2, and M3). Fig. 3 – 5 depict those NERC CIP requirements and how application of blockchain technology facilitates implementation of these controls and compliance.

NERC CIP 13 requires a documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: "One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)." A plan also must include one or more process used in procuring BES Cyber Systems found in 1.2.1 – 1.2.6 in Fig. 2. Blockchain technology can facilitate the implementation of the compliance process requirements (left column in Fig. 3 – 5) with blockchain controls (right column in Fig. 3 – 5) to ensure NERC compliance.

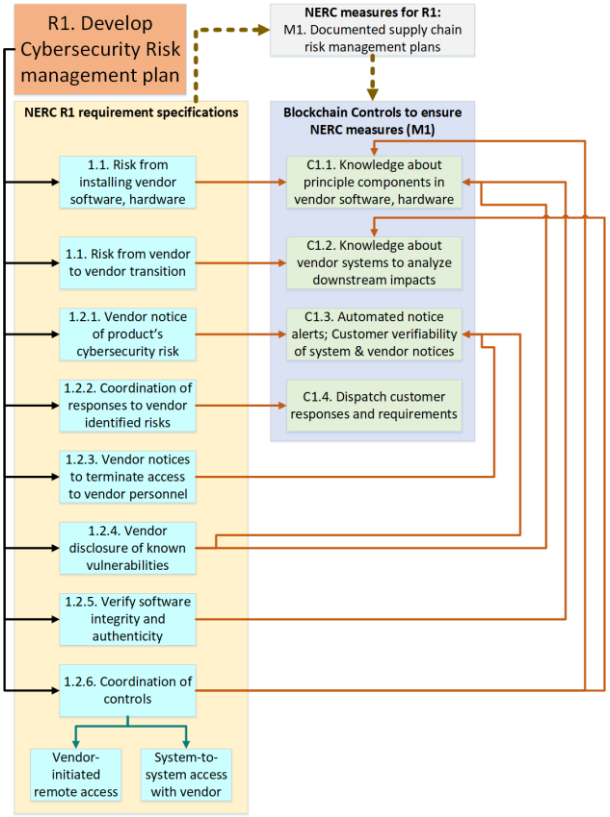

Fig. 3. Blockchain technology for monitoring and enforcement of cybersecurity risk management plan in compliance of NERC CIP 13

As shown in Fig. 3, the first requirement R1 mainly focuses on developing cybersecurity risk management plan by the responsible entity. As per NERC CIP 13 documentation, a responsible entity may be otherwise defined as the entity that owns the control system (example: a utility that owns the control systems). The requirement R1 focuses on identifying risks associated with the newly purchased control system, risk imposed by the control system on other processes due to its installation, vendor responsibilities in transparent articulation of risks associated with the newly purchased system, and finally coordination of access controls as needed.

As per NERC CIP 13 requirement, the risk management plan should consider all the above factors to enforce the measure M1 which is to document the risk management plan. Fig. 3 depicts four different blockchain controls that may be leveraged to address various aspects of R1 to ultimately satisfy M1. The second requirement R2 focuses on implementing the risk management plan that is developed by meeting R1 requirement. Measure M2 is met when the responsible entity can demonstrate the implementation of the newly developed of supply chain cybersecurity risk management plans. Fig. 4 shows how the associated blockchain controls that can facilitate requirement R2. The final requirement R3 is to gain CIP senior manager approval. The blockchain or distributed ledger consensus algorithm is updated as the responsible entity makes progress helping to automate and better track the above processes to meet requirements R1 and R2. The responsible entity can access the blockchain to enforce measure M3. This relationship flow and associated blockchain controls are shown in Fig. 5.

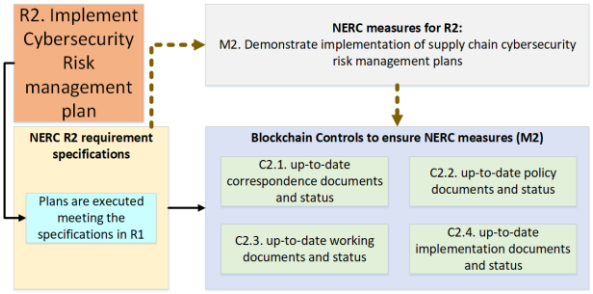

Fig. 4. Implementation of cybersecurity risk management plan through Blockchain following NERC CIP 13

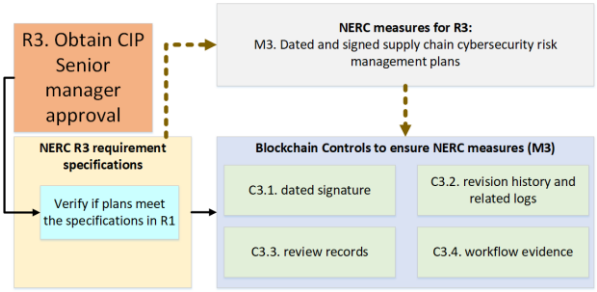

Fig. 5. Approvals of cybersecurity risk management plan through Blockchain following NERC CIP 13

B. Relationship of NERC CIP 13 Compliance Specifications with Blockchain Controls

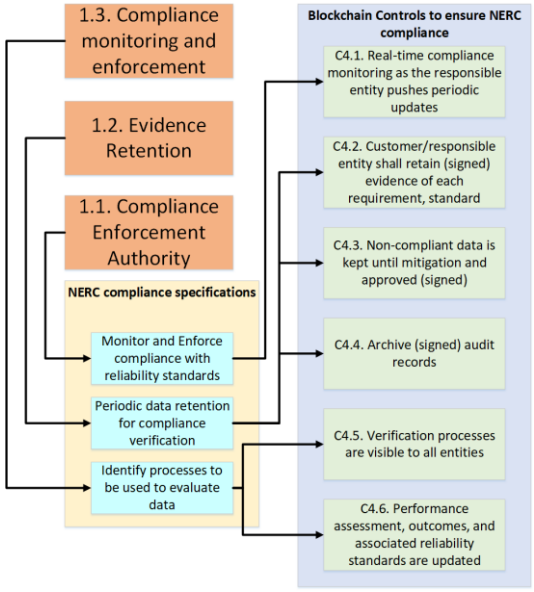

Fig. 6. Relationship of NERC CIP 13 Compliance Specifications with Blockchain Controls

Fig. 6 highlights three additional NERC CIP 13 requirements: compliance enforcement authority, evidence retention, and compliance monitoring and enforcement. Fig. 6 shows the specifications associated with above compliance items and how blockchain can facilitate and improve the compliance process.

4. BLOCKCHAIN FOR SUPPLY CHAIN SECURITY

A. Blockchain and Supply Chain Security

Although the core functionalities of various blockchain solutions share some commonalities, their design, function and

implementation often vary. This section depicts the high-level flow and overview of blockchain based supply chain management. As shown in Fig. 7, the customer (responsible entity) may initiate a control system order. Following the NERC CIP 13 standard, the customer documents the "must haves", system requirements and specifications. This information is pushed to the blockchain and is picked by a vendor and manufacturer (based on the event specified in the smart contract). The vendor begins the manufacturing process by updating all the information about the principle components that may go into the final product under a scannable barcode. This information is sent to the blockchain. After a complete assembly, the customer receives the product and the transaction is complete. The customer can simply scan the barcode to verify and validate the chain of custody through the associated hash value. As a result, the customer gains increased awareness of its chain of custody of critical cyber assets, enabling improved monitoring throughout the supply chain.

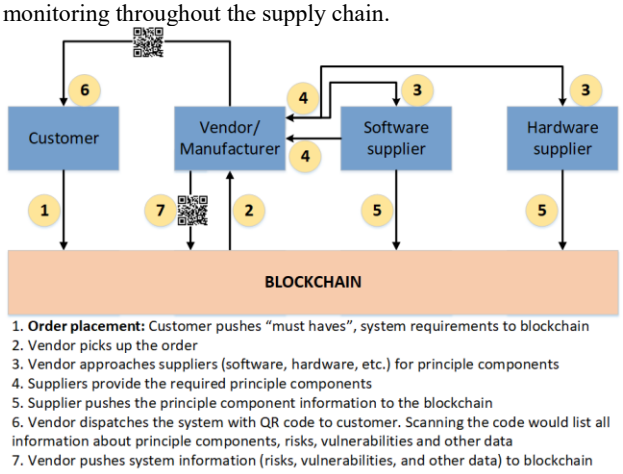

Fig. 7. Illustration of Blockchain for Supply Chain

B. *Use of Blockchain for NERC Auditing Purposes*

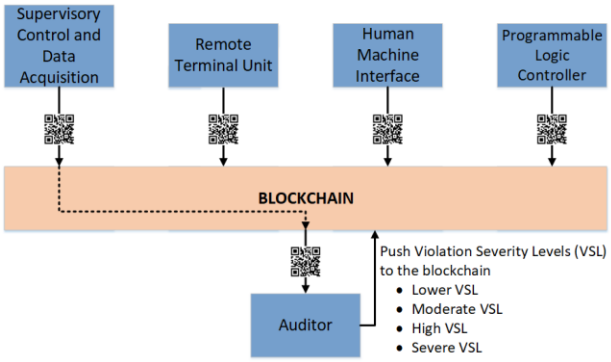

Fig. 8. Illustration of Blockchain for Auditing

Upon installation in the customer environment, as shown in Fig. 8, the compliance auditor can retrieve the information from the blockchain to determine the configuration, controls and any potential associated compliance Violation Severity Levels (VSL). These scores for each system are pushed back to the blockchain by updating it on the associated barcode. Blockchain technology facilitates a more efficient, autonomous, immutable, and trustworthy supply chain and auditing process significantly improves the current security, auditing and NERC CIP compliance process.

5. PERMISSIONED POA BLOCKCHAINS FOR SUPPLY CHAIN SECURITY

A. *Overview of Permissioned PoA Blockchain*

Blockchain technology has a lot of variation in its security properties, functional requirements, costs, transaction times as well as the consensus algorithms that validate, verify and sign data to the block. It is imperative to understand these differences when applying blockchain to facilitate NERC CIP compliance and grid cybersecurity goals. Permissioned proof of authority (PoA) blockchain differs from proof of work blockchain based crypto currencies, such as Bitcoin and Ethereum. PoA blockchain provides widely witnessed evidence on what can be considered the truth and does not rely on any single party. PoA blockchain performs the validation while retaining confidentiality of the original data. Another unique characteristic that differentiates some permissioned PoA blockchains from other distributed ledger solutions is their ability to scale to industrial applications to add and verify prodigious data sets to the blockchain at second and sub-second speeds. The ability to transact at speed, scale and with increased security are essential requirements for the power grid.

Permissioned PoA Blockchains has been in production for over a decade and are beginning to see increased industry adoption. Permissioned PoA blockchain helps realize several power grid cybersecurity goals, supply chain and compliance goals.

Smart contracts: Smart contracts execute and record transactions in the blockchain load ledger through blockchain enabled advanced metering infrastructure. Blockchain-based smart contracts may help facilitate consumer level exchange of generation from DER to provide additional storage and help substation load balancing from bulk energy systems. Moreover, smart contract data is secured in part through decentralized storage of all transactions of energy flows and business activities.

Secure Data Storage in Cryptographically Signed Distributed Ledger: Blockchain helps realize various optimization and security gaps and can improve the state of the art in grid resilience by providing an atomically verifiable cryptographic signed distributed ledger to increase the trustworthiness, integrity and security of EDSs at the grid's edge. Blockchain can be used to verify time, user, and transaction data and protect this data with an immutable crypto signed distributed ledger.

Blockchain PoA: PoA distributed ledger technology provides a unique way to distribute trust that has a clear cybersecurity value proposition for electricity infrastructure. Some cybersecurity advantages include, enabling a distributed escrow to maintain ordered time stamped data blocks that cannot be modified retroactively. This helps to enhance the trustworthiness and preserve the integrity of the data—two major challenges that currently threaten the security of electricity infrastructure. Implementations of blockchain integrity mechanisms may increase reliability of authentication and encryption without the laborious, cost prohibitive deployment of keys. Various blockchain PoA technologies and applications can help secure communications from industrial control systems and other operational technology protocols by including an advanced crypto signature that assigns a data signer, authenticity of the data, and time of signing to a data asset. This signature is represented by including the hash of the data in signature.

B. *Permissioned PoA Blockchain for Energy Supply Chain Management*

One of the core components of permissioned PoA blockchains are their unique (proprietary style) transfer and data exchange. Since these data clusters vary for different permissioned PoA blockchain vendor, the authors of this paper will address them as "signed data cluster". Through signed data clusters and by leveraging the ability to sign the data that provides cross-boundary truth, the truth associated with a supply chain can be independently verified [9]. The signed data clusters are designed to store both the history of the asset and product (the who, what, where and when) and the proof of registration that shows its association with the Blockchain. Therefore, the consumers can validate the authenticity of the asset and product, know the associated suppliers during the manufacturing process, risks and known vulnerabilities of the product by accessing the portable, single, and independently verifiable signed data clusters.

Therefore, using the signed data clusters, the customer, manufacturer, associated suppliers, and other participating entities can independently verify the critical cyber assets and the associated signed data cluster by trusting only the cryptographic immutability of the unique signatures associated with the signed data cluster. Note that in this particular use-case, the signed data cluster is ever-evolving and the final signed data cluster (when the customer receives the final product) may encapsulate several previous signed data clusters. With this construct, the truth resides within the blockchain, providing a cross-boundary truth mechanism.

C. *Illustration of Physical Supply Chain using permissioned PoA Blockchain*

The scenario listed below is divided into two phases: 1) Phase-1 focuses on the flow of data and information from the customer to the manufacturer and to the suppliers of principle components as shown in Fig. 9; 2) Phase-2 focuses on the flow of data and information from the suppliers to manufacturer and finally to the customer as shown in Fig. 10. Below steps details the intermediate steps spread across those two phases:

1. In step-1 (under phase-1), the customer would articulate the required product, requirements and specification following the NERC CIP 13 guidelines. At this step, the customer will register a unique identifier in the blockchain. This unique identifier could be a self-generated QR code that is made of hashed meta data that cryptographically signed and stored in the blockchain. Each QR code is unique and is associated with a desired product. By this process, a cryptographic link is established between the self-generated QR code of the required product and the unique cryptographic signature. The customer would generate a signed data cluster that encompasses all the information requirements and specifications that provide unique identifier, contextual base information. Such information includes expected receiver, location, time, and any attribute or context that is worth associating with the desired product. The data is immutably bound along with the identity of the entity that created the signed data cluster and registered the physical component. Finally, the signed data cluster will be signed with a unique signature that will be published in an immutable signed ledger. Throughout the manufacturing cycle and post-deployment phase, all entities such as the customer, manufacturer, suppliers, and auditors can simply scan the QR code to get product life-cycle information.
2. In step-2 (under phase-1), the signed data cluster is sent to the manufacturer. Because of the immutability and portability associated with the signed data clusters and because the signed data clusters are signed by unique signatures, any attempts to tamper or alter can be detected. This enables a more secure and agile exchange and distribution of critical cyber assets. Finally, the signed data cluster sent by the customer is received by the manufacturer. The manufacturer would initiate the product development process and appends the information to the customer-generated barcode. Then, the manufacturer identifies suppliers to loop-in for firmware, software, and other principle components requirements. The manufacturer then sends the updates signed data cluster to suppliers and associated with the same QR.

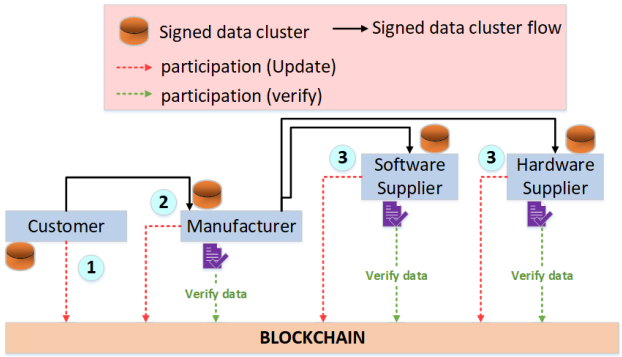

Fig. 9. Phase-1 illustration of permissioned PoA blockchains for Supply Chain

3. In step-3 (under phase-1), the suppliers received the known registered assets represented by signed data clusters. Suppliers would use this information to verify the crucial cyber assets (e.g. ICS, EDS, etc.) received from the prime manufacturer. After validating and interrogating the signed data cluster for policy input with complete trust, the suppliers need not login to any third-party or enterprise service to see any attributes of the signed data cluster. Note that some of the attributes were set by the customer and may have been updated by the prime manufacturer. Therefore, the suppliers can perform independent verification for authenticity and accuracy using the information within the signed data cluster. Once the suppliers verify the unique signature associated with the signed data cluster, the information associated with the "QR code (see step-1) and its attributes is leveraged. Then, the suppliers will create a new event to incorporate the received signed data cluster and signs this new signed data cluster with new unique signature with the updated information and the previous signed data clusters. This is a state of "cluster-of-clusters" or "nested clusters" where the new signed data cluster contains additional information and encapsulates the previous signed data clusters. At this point, if any permitted entity attempts to verify the signed data cluster, it will clearly show the change of ownership as each supplier is individually credentialed with respect to the blockchain.
4. In step-4 (under phase-2), the new signed data cluster along with associated assembled systems are sent back from the suppliers to the prime manufacturer. The manufacturer integrates the newly received systems and integrates them in the product development process. In this

process, the manufacturer updates the signed data cluster (i.e., create a new signed data cluster) with all previous signed data clusters as part of it and finally, signs it with a new unique signature (same process as in Step-3).

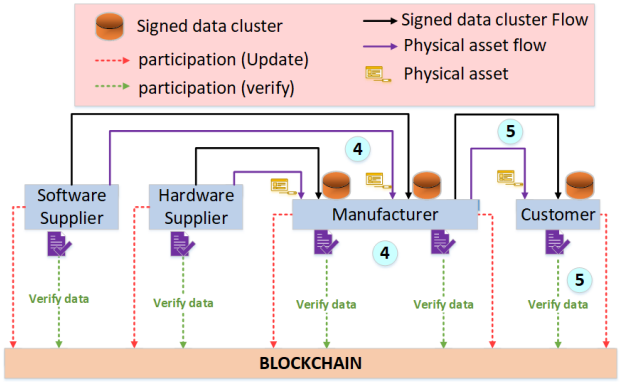

Fig. 10. Phase-2 illustration of permissioned PoA blockchains for Supply Chain

5. In Step-5 (under phase-2), final steps of order processing are performed, signed data cluster is updated with all the information associated with the physical asset/product. The signed data cluster would contain information per NERC CIP 13 requirements. Finally, the product is sent back to the customer. The customer, at any given time, can independently verify the information associated with the product and its authenticity all the way to the principle component level through signed data clusters. The customer may choose to create a new signed data cluster that holds all the previous signed data clusters with other information such as downstream connections, etc. This signed data cluster can be used by NERC for auditing purposes and standard compliance checks.

6. WHEN TO USE BLOCKCHAIN TO SECURE YOUR ENERGY SUPPLY CHAIN

Before optimizing or securing electricity infrastructure with blockchain technology, it is important to determine what technology is going to be applied and what problem will be solved. A number of blockchain solutions create more problems than solutions, expand security gaps more than mitigate them, increase costs rather than efficiencies, increase latency rather than optimized and increase energy use rather than reduce it. Blockchain solutions that help track and secure large data sets also need to be energy efficiency, economic and interoperable.

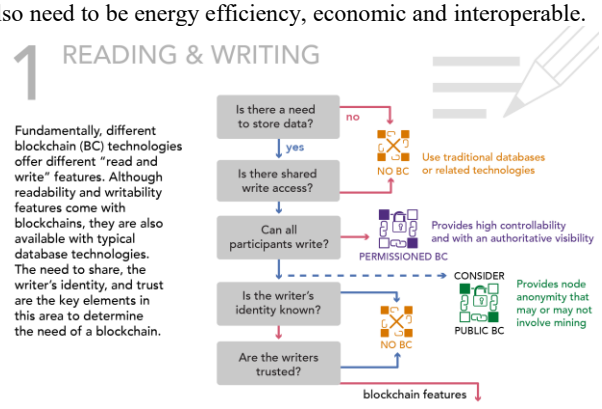

Fig. 11. Energy Blockchain Roadmap: Part-1: Reading and Writing

Cost, functionality, scalability and cyber resilience were all important factors in considering the functional requirements for grid cyber use cases being explored by researchers at PNNL. The road map shown in Fig. 11 – 13 was developed to help end users determine when to use blockchain to increase the cyber security of electricity infrastructure.

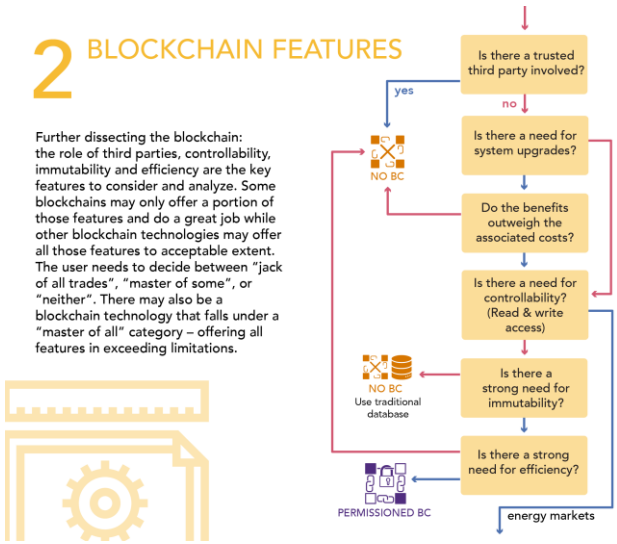

Fig. 12. Energy Blockchain Roadmap: Part-2: Blockchain Features

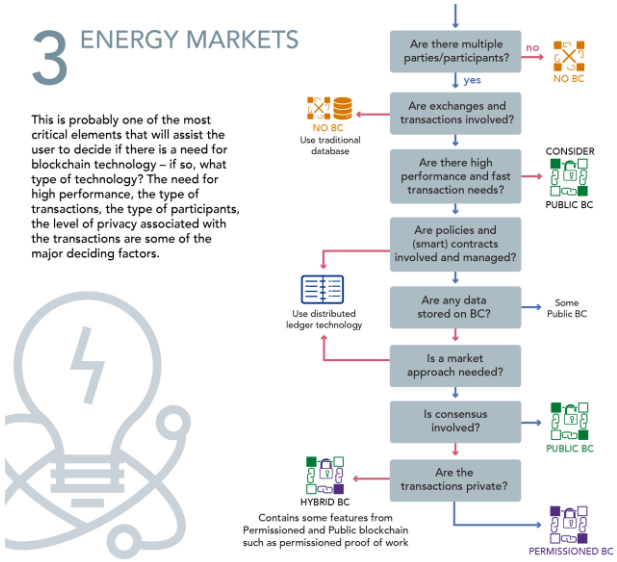

Fig. 13. Energy Blockchain Roadmap: Part-3: Energy Markets

7. POTENTIAL BLOCKCHAIN BUSINESS AND IMPLEMENTATION CHALLENGES

Blockchain shows great promise in the energy supply chain security and management [27]. Additional study, validation and verification of blockchain's application to grid cyber security challenges is needed as number challenges remain with applying distributed ledger technology to secure and optimize complex systems.

One challenge is that Blockchain technology – like its application to the energy space - is at a nascent stage. Evolving blockchain definitions create several challenges from a policy perspective. It is noted that [5] the "rapidly shifting, contested

vocabulary poses for regulators seeking to understand, govern, and potentially use blockchain technology, and offer suggestions for how to fight through the haze of unclear language." One of the general misconceptions around blockchain definitions is caused from the assumption that blockchain equals Bitcoin. While blockchains include cryptocurrencies and transactions recorded publicly, private or permissioned blockchains often do not include an exchange of value and do not record anything publicly. Yet, Google defines [5] blockchain as "a digital ledger in which transactions made in Bitcoin or another cryptocurrency are recorded chronologically and publicly." Similarly, Investopedia's definition [5] associates blockchain with decentralized ledgers of cryptocurrencies: "A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions." [5]

Definitions are evolving, contradicting and differ greatly among sector, application, functional requirements and the technology stack that they are deployed. Proof of work, proof of authority, zero proof and proof of burn are just some of the different descriptions of the consensus algorithms that establish the trust mechanisms to secure data the distributed ledger. This will continue to challenge regulators seeking to establish policies and regulations for blockchain's application to the energy sector.

Public proof of work blockchain solutions also have several gaps related to security, functionality, cost and energy efficiency. A major pitfall is that there is an excessive use of energy in solving the puzzles [28, 29]. Another challenge is that these nodes are widely witnessed and may lack the necessary privacy considerations. PoW servers are located in some countries that have been accused of economic espionage and theft of intellectual property Finally, PoW consensus algorithms can add prohibitive latency issues to times sensitive transactions.

Another challenge is the change in functional and non-functional requirements and technology stack which is needed to integrate the blockchain technology and to ensure that system manufacturing is tracked throughout the development lifecycle. Some related challenges for implementing blockchain to facilitate supply chain security include:

1) Multiple vendors are involved in product and systems development as well as the chain of custody. Vendors have different levels of resources, unique constraints and other considerations to keep in mind;
2) Vendors might be using different blockchain technology that are not interoperable with each other or with the data being tracked. An intermediate node between different blockchain and data bases can facilitate functionality in a single overall common blockchain;
3) Integrating different data sets for business ecosystems and supply chain functional and non-functional requirements into a blockchain across different data boundaries.

8. CONCLUSION

As grid modernization continues to expand the attack surface of the energy supply chain, new innovative solutions are needed to mitigate a complex and evolving cyber-physical threat. This paper examined how blockchain technology can help facilitate supply chain security and associated NERC CIP compliance requirements for securing critical energy infrastructure from evolving cyber threats and vulnerabilities through a cryptographic signed distributed ledger that provides data provenance, attribution and auditability. In realizing these security goals and NERC CIP 13 requirements, blockchain provides a number of clear opportunities, challenges and benefits worthy of future research and application to securing a rapidly evolving electricity infrastructure and its array of vulnerable energy control systems and internet of things.

6. REFERENCES

[1] Tapscott, 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 A, **The Path of the Blockchain Lexicon (and the Law) 36 Review of Banking & Financial Law 713,** University College London, 2017

[6] M. Mylrea, **Blockchain Cyber Security 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, S. Gourisetti, **Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security,** Resilience Week, Colorado, 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 Transmission & Distri. 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, **Cyber Security Supply Chain Risk Management Plans: Implementation Guidance for CIP-013-1.** Retreived on March 1, 2018 at CIP-013-1 – Cyber Security - Supply Chain Risk - NERC

[12] F. Tian, **An agri-food supply chain traceability system for China based on RFID & blockchain technology,** 13th international conference on service systems and service management, 2016

[13] H. Kim, M. Laskowski, **Toward an ontology-driven blockchain design for supply-chain provenance**, Intelligent Systems in Accounting, Finance and Management, 2018

[14] S. Abeyratne, R. Monfared, **Blockchain ready manufacturing supply chain using distributed ledger**, International journal of research in engineering and technology, 2016

[15] S. Apte, N. Petrovsky, **Will blockchain technology tevolutionize excipient supply chain management?** Journal of Excipients and Food Chemicals, 2016

[16] J. Wong, **WALMART: The world's biggest retailer wants to bring blockchains to the food bushess**. Accessed 2018.

[17] M. Unuvar, **Blockchain and food safety at the CGF Global Summit**, 2017

[18] B. McDermott, **Improving confidence in food safety with IBM Blockchain**. 2017

[19] D. Pyrzenski, **I'll only eat blockchain cereal with a food safety label on the box**, 2017

[20] D. Detwiler, **One nation's move to increase food safety with blockchain**, 2018

[21] S. Ramamurthy, **Leveraging blockchain to improve food supply chain traceability**, 2016

[22] S. Dudley, **Security, food safety and cognitive with blockchain**, 2016

[23] M. Unuvar, **The food industry gets an upgrade with blockchain**, 2017

[24] E. Lowry, **Top learnings about blocklchain for supply chain at Distributed: Trade**, 2017

[25] H. Chantz, **Weather, wither, whether: How blockchain enables precision agriculture**,2018

[26] A. Buldas, A. Kroonma, R. Laanoja, **Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees**, Secure IT systems: 18th Nordic Conference, 2013

[27] A. Pradhan, A. Stevens, J. Johnson, **Supply Chains Are Racing to Understand Blockchain – What Chief Supply Chain Officers Need to Know**, Gartner, 2017

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

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