Statement of Paul Skare
Chief Cyber Security Program Manager
Pacific Northwest National Laboratory

Before the
United States Senate
Committee on Energy and Natural Resources

August 21, 2018

Good morning. Thank you, Chairman Murkowski, Ranking Member Cantwell, and Members of the committee. I appreciate the opportunity to appear before you today to discuss blockchain as it relates to U.S. electric infrastructure issues and opportunities.

My name is Paul Skare, and I lead the Grid Cybersecurity Research Program at the Pacific Northwest National Laboratory (PNNL), a Department of Energy (DOE) National Laboratory located in Richland, Washington. I also support the Security and Resilience team in DOE's Grid Modernization Laboratory Consortium, a team of 14 National Labs that, along with industry and university partners, supports the Department's Grid Modernization Initiative. The consortium members include PNNL, the National Renewable Energy Laboratory, Argonne National Laboratory, Brookhaven National Laboratory, Idaho National Laboratory, Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, the National Accelerator Laboratory at Stanford, National Energy Technology Laboratory, Oak Ridge National Laboratory, Sandia National Laboratories, and Savannah River National Laboratory. I have worked in the power industry for 38 years, starting at Northern States Power in Minneapolis, MN, Siemens Energy in Minnetonka, MN, and. I started working on cybersecurity for the grid 20 years ago. Today I will address these points:

1. Blockchain technology can be thought of as an electronic general ledger, securely capturing transactions without the need for a centralized authority, and cryptocurrency is *just one application* that uses this technology.
2. Cryptocurrency mining is having localized impacts on the U.S. power grid. However, most of our understanding remains anecdotal, and it is unclear what the long-term impacts will be as cryptocurrency prices fluctuate.
3. Grid cybersecurity is a multi-faceted issue with threats coming from many different directions, and blockchain is just one tool that PNNL and others are exploring that can help secure the grid. *But there is no silver bullet to securing our power grid and other critical infrastructure.*

Background

For more than two decades, PNNL has supported power system reliability, resilience and innovation for the State of Washington, the Pacific Northwest, and the nation. Over this period, the laboratory has:

1. Helped the North American Electric Reliability Corporation (NERC) and DOE design and implement the series of national grid cyber exercises known as *GridEx* which linked industry with government and law enforcement agencies and allows participants to practice their incident response plans. *GridEx III* engaged over 400 organizations and 4000+ participants in scenarios designed and operated with support from PNNL.

2. PNNL helped DOE develop the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). This allows for utilities to assess their business practices supporting cybersecurity and learn where their business could invest more to meet their business's goals for cyber. Cybersecurity insurance companies have used this to influence the rates for insurance. PNNL has expanded on ES-C2M2 to create models for Buildings, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Secure Design and Development Principles.

3. Led DOE-industry collaborations in developing and deploying synchrophasor technology to help avoid blackouts. Phasor measurement unit networks are designed to enhance situational awareness of wide area systems. This new grid tool has demonstrated value by detecting impending system control and equipment faults for system operators, thus avoiding major outages.

4. Led a public-private collaboration with utilities and vendors to develop and demonstrate transactive control concepts on the Olympic Peninsula in Washington and for the Pacific Northwest Smart Grid Demonstration project—the largest of its kind—to validate smart grid benefits and new control approaches that engage demand and distributed resources at scale.

5. Delivered the first applications of high performance computing to grid tools such as interconnection-scale contingency analysis, reducing run times from days to under two minutes. PNNL also applied high performance computing and phasor measurement unit data to deliver the first real-time dynamic state estimation to open the door to the future world of predictive grid tools. This parallelized state estimator tool enabled PNNL to deliver assessments of system risk at the interconnection scale (the Western Interconnection) in less than 2 minutes versus the traditional 24 hours.

These examples illustrate the high return on investment possible by utilities and National Labs across the country when combining advanced electric infrastructure technology innovation with public-private validation and deployment.

Blockchain: a new technology with many potential applications

Blockchain is most widely known as a technology that cryptocurrencies – Bitcoin being the most famous – use to secure digital transactions. The underlying blockchain technology, invented in 2008 as part of the Bitcoin cryptocurrency, consists of a database distributed across all computers in the blockchain network that maintains a continuously growing list of records – called blocks – that are protected from tampering and revision. Each block contains a timestamp

and a link to a previous block. The use of blockchain allows users to exchange value without intermediaries acting as arbiters of money and information, as the blockchain serves as a general ledger for transactions whose authenticity is established by the network itself.

Cryptocurrencies are an example of the 'public' use of blockchain (sometimes referred to as 'permissionless' or 'open'), meaning anyone connected to the network can access the blockchain without restriction. This makes the transactions transparent and permanent. In these public blockchains, volunteers must solve complex digital 'proof of work' puzzles to make new entries in the blockchain without any other access control or identity verification. Solving these complex puzzles to verify the new block entries produces cryptocurrency as the reward for supplying computer calculations. This is known as 'mining' and is the source of unexpected energy usage electric utilities (especially those with lower energy prices) are facing today.

For other use cases beyond cryptocurrencies, 'private' blockchain is often used –also sometimes called 'permissioned', 'consortium', or 'hybrid' blockchain. This form does not allow public access to the blockchain, so mining is not necessary for access control and verifying blocks.

The key to the security of the blockchain transaction is the distributed, so called 'Byzantine' fault tolerant architecture used to validate each transaction. In this scheme, numerous computers (nodes in the blockchain network) are evaluating each transaction in parallel, independently looking at each transaction, and then comparing results with the other nodes. These blocks cannot be altered without altering all the blocks AND having a consensus of the nodes. In addition, access to the blockchain uses public-key cryptography to identify an address on the blockchain. This can be thought of as 'secure by design' in our current technology. It is fair to note here that there are no 100% secure systems or solutions. Please refer to a paper I cowrote with others on the application of Byzantine Architectures to secure control systems, 'Survivable SCADA Via Intrusion-Tolerant Replication' (IEEE TRANSACTIONS ON SMART GRID, VOL. 5, NO. 1, JANUARY 2014).

Cryptocurrency mining is straining localized parts of the US power grid

The energy used in cryptocurrency mining has been compared to the total energy usage of some states and some countries. From an electric utility's perspective, this can appear as an unexpected energy load on their distribution grid. A qualitative analysis shows that this strain is typically appearing in areas with low energy costs and low fixed costs (such as rent).

Cryptocurrency miners must complete increasingly complex calculations, requiring increasing amounts of computing power and therefore energy, to capture returns in the form of cryptocurrency. Thus, the practice is most profitable wherever electricity prices are low, such as the Columbia River Basin in Eastern Washington. When large mining operations move into a particular location, the increase in load can cause the utility to increase its generation, buy power from others, or experience overloaded distribution circuits which could lead to localized power outages. A number of cities have placed moratoriums on new high-density load hookups to give staff time to develop a plan for dealing with the demand for electricity from digital currency miners (https://news.bitcoin.com/washington-utility-increases-security-amid-crypto-mining-moratorium/). While there has been no shortage of popular press coverage of the scale and

impact of the growing cryptocurrency mining community on the US power grid, I am not aware of any quantitative studies of cryptocurrency mining impacts.

Today, what we know comes from press stories and anecdotal evidence is that some utilities have knocked on doors to investigate unexpected loads and found rows of computer racks doing cryptocurrency mining in both residential and commercial areas. This year, Bitcoin alone has dropped more than 50% in value, and it is unclear how mining operations will respond to the fluctuating prices. Understanding the elasticity of demand for cryptocurrency is necessary to understand any potential long-term impacts on the US power grid.

Grid cybersecurity and how blockchain fits into the landscape

The U.S. power grid is rapidly changing from an earlier, simpler era with large generation stations and passive energy loads to a much more dynamic grid with growing distributed energy generation resources and much more active, connected, "smart" loads. With the increase in renewables on the grid, and the retirement of some older larger generators, generator inertia - which is crucial to the reliable operation of an AC power system – is strained. In addition, availability of black start generation – needed to restart generators after an outage – is also strained at some locations.

Blockchain technology shows potential in securing energy delivery systems (EDS) that have transactional attributes. This is important as these control systems require unprecedented levels of security and trustworthiness to verify integrity of data and manage complex demand response and market system exchanges. Improving the ability to identify, control, and secure grid devices with blockchain technology may increase the security and trustworthiness of real-time energy transactions without adding prohibitive costs, latency, interoperability or scale issues. The wide range of potential applications of blockchain to EDS has made the technology a priority for DOE.

In fact, blockchain and other distributed ledger technologies have many properties that make them well suited to facilitate more efficient and decentralized energy transactions, but these properties also come with some potential challenges:

- Distributed consensus mechanism: This supports decentralization of authority from single points of failure or compromise. This is a great advantage, but the challenge associated with purely distributed proof of work type consensus model is its vulnerability towards a 51% attack of the nodes. In such an attack, enough nodes can be compromised to approve a transaction. Such situations could be avoided by using permissioned type consensus model. In permissioned consensus models, privacy controls can also be implemented and customized as per the need of the application.
- 100% up time: Blockchain provides a reliable, fail-safe logically centralized, physically distributed persistence mechanism. Bitcoin failures were focused on the application layer where there has been theft and loss of Bitcoins when users lose their private key required for signing a transaction or data content.
- Strong immutability: Even blockchain technology has proven nothing is immutable, with examples of mutations such as forks and or blockchain hacks that required rolling back

the blockchain. Blockchain technology does provide an atomically variable time stamped cryptographic signed electronic transaction that has proven to be very difficult to change.

- Immutability challenges: Immutability can lead to a number of challenges. Recently it was found that illegal images were saved in the Bitcoin blockchain. When undesired data are saved in the blockchain, it can prove very difficult to change. As discussed above, another way to change the blockchain is to control or compromise 51% of the nodes needed to reach a consensus.
- Big data management blockchain: Blockchain facilitates the distribution of prodigious data sets between organizations. Data can be synchronized and archived between multiple parties. The challenge here is at some point the blockchain might be overwhelmed by the amount of data being stored. It is important to address this by ensuring data is stored in efficient formats that minimize overall data volumes stored in the blockchain.
- Endpoint Security: No matter how secure the blockchain aspects of a solution are, the endpoints – parts of the solution on either end of the blockchain technology – remain as open to vulnerabilities as any other software.

PNNL is leading the way in Advanced Grid Cyber Security Approaches and new Technologies

PNNL is a leader in developing the foundational understanding and technologies for security of our power grid. We take a broad approach to this critical national need – from stewarding operational capabilities like the cyber threat monitoring program called CRISP to developing entirely new technologies that keep our defenses at the forefront.

CRISP – the Cybersecurity Risk Information Sharing Program – uses data shared by utilities to perform an intelligence-informed analysis that identifies threats that neither utilities alone, nor private cybersecurity firms, can identify. CRISP provides a strong complement to what utilities and private cybersecurity firms provide. Utility participation in CRISP will soon provide complete coverage of the continental United States. This program is able to identify traffic from malware that uses blockchain technology.

PNNL was recently awarded a project by the DOE Office of Cybersecurity, Energy Security, and Emergency Response's (CESER) Electricity's Cybersecurity for Energy Delivery Systems (CEDS) program (formerly part of the Office of Electricity Delivery and Energy Reliability) to evaluate uses of blockchain in the electric grid. In this program, we are applying private blockchain solutions – so one that does not require the energy intensive mining process – to a variety of use cases in the power grid.

By using a private blockchain, this approach has the potential for power system applications to add items at scale to the blockchain every second, and to verify data from the blockchain within the next second. This quick updating ability is *essential* to handle the increasing data requirements of the modern power grid.

Use cases for this project:

- Supply Chain ‘chain of custody’ – the ability to trace products and components from origin to destination – this will allow utilities to see and track the source of all the components in a system, allowing for better understanding of risks due to potential vulnerabilities and patches.
- Device Integrity – verification of control signals
- Enhanced cybersecurity controls – trusted zone of nodes using verifiable digital signatures and signed messaging
- Patch Management – allows an asset owner to track and trace a patch from the vendor to their system.
- Supply and Demand transactions between microgrids

PNNL’s current program only scratches the surface of where we see potential for blockchain applications on the grid. We see many other potential use cases, including:

- EV Charging: Use blockchain to enable EV charging and billing interactions with the EV owner. This amount in kWh is subtracted from the smart meter read or billing to determine data for the prosumer (Prosumers are amateur advocates for products – in this case these are people who both produce and consume energy).
- Meter Data Access Management: Use blockchain technology to work with a central meter management system to allow consumers to manage who is allowed access to their meter data.
- Asset Lifecycle Management: Use blockchain to manage beginning-to-end lifecycle of assets' parts and/or components (construction, operations, maintenance, disposal). This can also include the chain of custody for the supply chain.
- Distributed Energy Resources (DER) Transaction Processing: Use blockchain to process any transaction involving a DER asset, e.g., storage, solar photovoltaic (PV), EV, micro-combined heat and power (micro-CHP).
- Peer to Peer Trading of Distributed Energy: Use blockchain for bilateral trading of distributed energy generation (similar to the Brooklyn Microgrid project).
- Markets, Energy Trade Settlement: Use blockchain to support electronic trades at energy exchanges or for direct agreements/trades between market participants.
- Supplier Switching: Use blockchain technology to track supplier switching.
- Emission Certificates: Use blockchain to generate, own, and trade emission certificates related to energy generation.
- Energy Supply Chain: Supply chain reconciliation (energy delivered, technical/non-technical losses, consumption, etc.) spanning all measurement points all the way through from generation to consumption for commercial settlement.
- Blockchain based Metering: Use blockchain to augment smart meter for recoding energy use of appliances (EV, heating).

In addition to our program evaluating blockchain for grid cybersecurity, we are also completing many other projects for the CEDS program, including:

- MEEDS – the Mitigation of External-exposure of Energy Delivery Systems –This project works with an existing cybersecurity search engine tool called Shodan to support a private review of control systems connected to the internet for a particular utility without publishing results publicly.
- SSASS-E – Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems - This project supports continuous scanning of control systems without negatively impacting the performance of the control systems and devices.

On the technology front, PNNL has begun a new program with Lab Directed Research and Development funding, called Proactive Adaptive Cybersecurity For Control, or PACiFiC, which includes two focus areas:

1. Deception:
   Adaptive Cybersecurity Controls are being explored from many perspectives. Traditional approaches have put us in an asymmetric disadvantage against our adversaries in defending our systems. Adaptive Cybersecurity Controls can be a way to provide a more level playing field by adjusting control system environments on the fly to confuse, obfuscate, and mislead adversaries as they work their way through a system, increasing the effort and knowledge needed to get through the defenses, while also giving a better chance for detection solutions to be effective.

2. Secure Design and Development Principles:
   While there are many documented methods to secure operation systems, there are no documented ways for a vendor to create a secure product that they can control and implement. This body of work provides a set of over 600 best practices that encompasses the entire product lifecycle.

Conclusion

Industry and DOE have partnered over the past several years to significantly advance our grid cyber technologies, and new projects are breaking new ground in leading edge technology such as blockchain. To see some potential of blockchain, look at Estonia – the first country to face a nationwide cyber-attack. As a result, ongoing investments have led to public services being digitized and accessed via secure digital identities provided to every citizen and resident. Integrated into the digital services is blockchain technology.

In parallel to "better securing" the grid, we need to leverage these same foundational science and technology tools of high-performance computation, analytics, deep learning and control theory to develop more resilient system designs for networks, data and grid control systems. These will enable the system to better resist inevitable attacks, better defend and ultimately recover quickly.

The DOE investments in fundamental science, applied technology and public/private partnerships in grid cybersecurity are essential elements of an effective, integrated national cyber readiness strategy for the U.S. electric power system and its related infrastructures. Securing our electric grid is a long-term endeavor that will require a range of strategies and new technologies;

there is no one silver bullet. Blockchain is just one of a set of tools we must develop as we work to accomplish the goal of securing our energy systems.

I appreciate the opportunity to discuss this important issue with you today, and I am happy to answer your questions.

Thank you.

CEDS-Supported Projects in Washington State (Active)

Prime Performer	Project Title
Pacific Northwest National Laboratory (PNNL)	Automated, Disruption-Tolerant Key Management System
Pacific Northwest National Laboratory (PNNL)	Enabling Situation Assessment/Awareness for Utility Operators and Cybersecurity Professionals
Pacific Northwest National Laboratory (PNNL)	Universal Utility Data Exchange (UUDEX)
Pacific Northwest National Laboratory (PNNL)	Keyless Infrastructure Security Solution (KISS)
Pacific Northwest National Laboratory (PNNL)	Software Defined Networking for Energy Delivery Systems (SDN4EDS)
Pacific Northwest National Laboratory (PNNL)	Research Exploring Malware in Energy DeliverY Systems (REMEDYS)
Pacific Northwest National Laboratory (PNNL)	Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems (SSASS-E)
Pacific Northwest National Laboratory (PNNL)	Mitigation of External-exposure of Energy Delivery System Equipment (MEEDS)
Schweitzer Engineering Laboratories, Inc.	Secure Software Defined Radio
Schweitzer Engineering Laboratories, Inc.	The Alliance Project
Schweitzer Engineering Laboratories, Inc.	Tempus Project Time Synchronization Platform for GPS Spoofing
Schweitzer Engineering Laboratories, Inc.	Chess Master Project

1. Pacific Northwest National Laboratory (PNNL): Automated, Disruption-Tolerant Key Management System

Partners: Arizona Public Service (APS), Lawrence Berkeley National Laboratory (LBNL)

Project Description: The project is working to design a standards compliant and interoperable system, implement a prototype key management and field device services, and evaluate and compare the performance and effectiveness of the prototype against existing key management systems for the energy sector. This effort is improving security and the efficiency of operations by providing a new key management architecture suited to the unique requirements of EDS.

2. Pacific Northwest National Laboratory (PNNL): Enabling Situation Assessment/Awareness for Utility Operators and Cybersecurity Professionals

Partners: Idaho National Laboratory (INL), GE (Alstom Grid), Peak RC, Total Reliability Solutions, WAPA

Project Description: Utility operators are bombarded with data from differing sources and systems and struggle to derive meaning from the data. To enable operators to make informed decisions in the finite amount of time available, operators need a cognitive system that displays the associated data to enhance situational awareness. This project will develop visualizations that power system operators and/or cybersecurity professionals can use to make fast, accurate assessments of situation, enabling them to maintain situation awareness during unfolding events.

3. Pacific Northwest National Laboratory (PNNL): Universal Utility Data Exchange (UUDEX)

Partners: MITRE, OATI

Project Description: The project team will develop a secure and flexible data-exchange approach to replacing key communication between control centers, including Inter-Control Center Communications Protocol (ICCP) data exchanges, threat information, synchrophasor, Reliability Coordinator Communications Information System (RCIS), and incident information. ICCP will be replaced with a modern model-driven data-exchange architecture and protocols, taking advantage of current methods of data transport and configuration.

4. Pacific Northwest National Laboratory (PNNL): Keyless Infrastructure Security Solution (KISS)

Partners: Avista, Cisco, Guardtime, Rocky Mountain Institute, TVA (Utility Advisor), Washington State University, OATI

Project Description: The project team will develop a Keyless Infrastructure Security Solution (KISS) to increase the trustworthiness, speed, integrity, and resiliency of EDSs responsible for complex grid-edge energy exchanges and integration of distributed energy resources, by developing a prototype of a secure and trustworthy blockchain energy platform.

5. Pacific Northwest National Laboratory (PNNL): Software Defined Networking for Energy Delivery Systems (SDN4EDS)

Partners: AECOM, CAISO, Dispersive Technologies, Juniper Networks, National Renewable Energy Laboratory (NREL), Sandia National Laboratory (SNL), Schweitzer Engineering Laboratories, Inc. (SEL), Southern California Edison (SCE)

Project Description: The project team plans increase the adoption of SDN technologies and improve security for local area networks (LANs) and wide area networks (WANs) components in the energy sector.

6. Pacific Northwest National Laboratory (PNNL): Research Exploring Malware in Energy DeliverY Systems (REMEDYS)

Partners: ORNL, MIT, ANG Consulting, James P. Fama, Nevermore Security

Project Description: The project team will develop, evaluate, and refine organizational structures that could be used to coordinate the nation's multiple energy sector stakeholders in the rapid research, development, and distribution of mitigations that reduce the risk of an imminent or emerging malware cyber-attack that might otherwise disrupt energy delivery.

7. Pacific Northwest National Laboratory (PNNL): Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems (SSASS-E)

Partners: Chelan County PUD, National Rural Electric Cooperative (NRECA), Tenable Security, University of Illinois at Urbana-Champaign (UIUC)

Project Description: The project team will develop, validate, and verify innovative safe scanning methodology, models, and architectures, and produce a prototype to transform Tenable's IT/OT platform, the most widely deployed vulnerability scanner in the IT space, to secure operational technology (OT) installed in critical energy infrastructure.

8. Pacific Northwest National Laboratory (PNNL): Mitigation of External-exposure of Energy Delivery System Equipment (MEEDS)

Partners: Shodan, LLC, National Rural Electric Coop, Tenable, Chelan PUD

Project Description: MEEDS is a user-friendly web application for utilities built upon the existing Shodan technology for performing continuous monitoring of utilities' internal networks to detect and identify any EDS equipment that may be inadvertently exposed to the internet.

9. Schweitzer Engineering Laboratories (SEL): Secure Software Defined Radio

Partners: Pacific Northwest National Laboratory (PNNL), San Diego Gas & Electric (SDG&E)

Project Description: The Secure Software-Defined Radio Project (SEL-3070) is developing a flexible platform for secure wireless communications to utility distribution automation devices, providing capabilities not offered in cellular, narrow-band licensed, or other unlicensed-band radios.

10. Schweitzer Engineering Laboratories (SEL): The Alliance Project

Partners: Sandia National Laboratory (SNL), Tennessee Valley Authority (TVA)

Project Description: The Alliance project is developing a proximity card reader and controller that allows physical and cybersecurity access to be monitored, tracked, and controlled using a single system. The reader and controller consist of four easy-to-deploy components: an access terminal, an access control processor, enhanced firmware for the SEL-3620 and SEL-3622 security gateways, and a card enrollment solution.

11. Schweitzer Engineering Laboratories (SEL): Tempus Project Time Synchronization Platform for GPS Spoofing

Partners: San Diego Gas & Electric (SDG&E), Southwestern Research Institute (SwRI)

Project Description: SEL will research, develop and demonstrate the capabilities of a secure, modular, and customizable time synchronization platform that provides layers of protection from GPS spoofing attacks. The project will include the development of innovative algorithms and electronics that detect GPS signal manipulation for critical applications that use timing signals in the energy sector.

12. Schweitzer Engineering Laboratories (SEL): Chess Master Project

Partners: Ameren Energy Resources, Sempra, Veracity Security Intelligence

Project Description: This project will provide system operators with a global view of their operational network, enabling them to set and view field network security policy and validate operational adherence to those policies. The Chess Master team will build on the successful commercial release of utility rated software defined network (SDN) technology under the previous CEDS project, Watchdog.