Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security

Michael Mylrea, Sri Nikhil Gupta Gourisetti, *Member, IEEE*
Pacific Northwest National Laboratory
michael.mylrea@pnnl.gov, srinikhil.gourisetti@pnnl.gov

***Abstract*—Blockchain may help solve several complex problems related to securing the integrity and trustworthiness of rapid, distributed, complex energy transactions and data exchanges. In a move towards grid resilience, blockchain commoditizes trust and enables automated smart contracts to support auditable multiparty transactions based on predefined rules between distributed energy providers and customers. Blockchain based smart contracts also help remove the need to interact with third-parties, facilitating the adoption and monetization of distributed energy transactions and exchanges, both energy flows as well as financial transactions. This may help reduce transactive energy costs and increase the security and sustainability of distributed energy resource (DER) integration, helping to remove barriers to a more decentralized and resilient power grid. This paper explores the application of blockchain and smart contracts to improve smart grid cyber resiliency and secure transactive energy applications.**

***Keywords*— Blockchain; resilience; transactive energy; smart grid; cybersecurity; grid cybersecurity; cryptography; smart contracts**

I. Introduction

Blockchain is defined as a distributed data base or digital ledger that records transactions of value using a cryptographic signature that is inherently resistant to modification [1]. Applying blockchain based smart contracts [2 – 4] presents an opportunity to increase the speed, scale and security of transactive energy applications [5 – 7]. This provides a more resilient path for a decentralized modern grid [8, 9] and integration of internet connected Energy Internet of Things (E-IoT) and grid edge devices. These grid optimization and resilience improvements are essential operations and design criteria as we modernize our power grid. However, cybersecurity is often an afterthought as vendors and end users prioritize functionality and cost [10], leaving our power grid, the backbone of our economy, potentially vulnerable to a cyber-attack. This is especially true at the grid's edge which continues to increase the size and speed of data being collected and exchanged in absence of clear cybersecurity and IoT standards and regulation. As a result, the grid lacks the necessary defenses to prevent disruption and manipulation of DERs, grid edge devices and associated electricity infrastructure. Moreover, as the smart grid increases its connectivity and communications with buildings, cyber vulnerabilities will continue to extend behind the meter into "smart" building automation and control systems [11], which have a number of cybersecurity vulnerabilities.

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 [12]. Blockchain-based smart contracts can be executed without human interaction [13] and the data is more resistant to modification as the data in a block cannot be altered retroactively. Blockchain smart contracts are defined as technologies or applications that exchange value without intermediaries acting as arbiters of money and information. [1].

II. State of the Art

Applying blockchain based smart contracts to grid modernization, presents an opportunity to increase the speed, scale and security of a modern grid, where distributed energy resources and real time transactive energy applications require increase in speed, security and control of data. Blockchain provides a unique path for a more decentralized and resilient integration of Energy Internet of Things (E-IoT) and grid edge devices as proven in some recent use cases and studies [5, 6]. Improvements in grid resiliency are imperative in the operations and design criteria of energy delivery systems used to modernize how we exchange and consumer energy. Energy delivery systems operating at the grid's edge require unprecedented levels of security and trustworthiness to verify integrity of data and manage complex transactive and DER exchanges. However, grid edge devices lack visibility, control and security to conduct real time energy transactions with the required, speed, scale, control and security.

Blockchain based smart energy contracts can help fill these optimization and security gaps and improve the state of the art in grid resilience by providing an atomically verifiable cryptographic signed distributed ledger to increase the trustworthiness, integrity and resilience of energy delivery systems at the edge. Blockchain can be used to verify time, user, transaction data and protect this data with an immutable crypto signed ledger.

III. Goals and Benefits

A. Primary Goals and Engagements

The following conceptual paper outlines how to apply blockchain based smart contracts to increase speed, scale and security of exchanges of distributed energy resources. The paper begins with an overview of blockchain and smart contracts application to the energy arena. Then the paper

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

978-1-5090-6055-9/17/$31.00 ©2017 IEEE

provides a brief analysis of cybersecurity vulnerabilities at the grid's edge. Next the paper provides an overview of two unique testbeds at Pacific Northwest National Lab (PNNL) and how they can be integrated to realize the following goals: 1) Reduce transaction costs in the energy sector and facilitate secure distributed energy exchange; 2) Launch a new energy focused blockchain platform; 3) Test different blockchain solutions on PNNL's Transactive Campus to investigate implementation issues and reduce cyber risks associated with broader adoption; 4) Validate and verify blockchain technology security applications to transactive energy at speed and scale; 5) Model various cyber-attack scenarios at the grid's edge to improve blockchain defenses and potential mitigations; 6) Investigate the communications between the blockchain ledger and control systems at local, system, and system of systems levels; 7) Explore various regulatory and standards models to facilitate the adoption and sustainability of decentralized security measures like blockchain; 8) Develop market standards that ensures interoperability, reduces costs and complexity, aligns currently dispersed blockchain initiatives, and facilities technology deploy through easy to implement applications; 9) Investigate cyber security affordances of blockchain; 10) Better understand how to implement protection measures using different blockchain solutions; and 11) Examine where blockchains fail to deliver and develop improvements.

B. Potential Benefits

Blockchain presents a number of potential security and optimization benefits in its application to electricity infrastructure. From a security perspective, it may enhance the trustworthiness and integrity of transactive energy data by supporting multifactor verification through a distributed ledger. Moreover, it can also provide autonomous detection of data anomalies and real-time response to unauthorized attempts to change critical EDS data, configurations, applications, and network appliance and sensor infrastructure. Additional potential blockchain benefits, may include, but are not limited to: 1) Enhances the trustworthiness and preserves the integrity of the data; 2) Supports multifactor verification through a distributed ledger; 3) Secures integrity of transaction data; 4) Reduces costs of energy exchanges by removing intermediaries; 5) Facilitates adoption and monetization of DER transactions: *All transactions would be executed in real time and settled on the basis on actual consumption*; 6) Blockchain based smart contracts can facilitate consumer level exchange of excess generation from DERs and EVs.; 7) Enabling consumers to also be producers could provide additional storage and help substation balancing from bulk energy systems; 8) Enables a more secure distributed escrow to maintain ordered time stamped data blocks that can't be modified retroactively; 9) Rapid detection of data anomalies may enhance the ability to detect and respond to cyber-attacks; 10) Helps align currently dispersed blockchain initiatives and facilitates technology deployment through easy to implement and secure applications; 11) Potentially helps reduce transaction costs in the energy sector; 12) Distribution system operators can leverage the blockchain to receive energy transaction data required to charge their network costs to consumers; 13) Transmission system operators would have reduced data requirements and constraints for clearing purposes.

Blockchain implementation and testing helps answer a number of key research questions in exploring blockchain grid applications: 1) How can blockchain smart contracts facilitate DER/DG prosumers that can sell to a consumer network based on the smart contract pricing? 2) How can blockchain help secure the grid's edge which is increasingly networked and digitized to Energy Internet of Things (EIoT) cyber-physical devices that are potentially vulnerable to cyber-attacks? 3) If blockchain can help cut out 3rd parties, who will be the winners and losers? 4) Does blockchain help move us toward a value of service business model, where demand response and time of use is the norm? 5) What are the potential security and privacy vulnerabilities of applying blockchain to electricity infrastructure? 6) Blockchain lacks standardization, regulations, legal settlement. What would sound sounds policy and regulation look like? How and by whom would they be enforced? 7) Are there any latency and interoperability issues introduced by blockchain that would be prohibitive? 8) How will blockchain change current The Payment Card Industry Data Security Standard (PCI DSS) cybersecurity regulations currently in place at the distribution level?

IV. SMART CONTRACT APPLICATION TO ENERGY ARENA

The following conceptual model highlights the application of blockchain technology to the smart grid to help reduce costs by cutting out 3rd parties and increasing the arbitrage opportunity for individuals to produce and sell energy to each other. Smart contracts facilitate peer-to-peer energy exchanges by enabling energy consumers and procures to sell to each other, instead of transacting through a multi-tiered system, in which distribution and transmission system operators, power producers, and suppliers transact on various levels. In April 2016, one of the first use cases was demonstrated where energy generated in a decentralized fashion was sold directly between neighbors in New York via a blockchain system, demonstrating that energy producers and energy consumers could execute energy supply contracts without involving a third-party intermediary; effectively increasing speed and reducing costs of the transaction [14]. In addition to potential cost savings, transaction data might be more secure through decentralized storage and multifactor verification of transactions in the blockchain distributed ledger [14]. Fig 1 highlights how blockchain reduces the need for 3rd parties to process transactions: Electricity is generated → Consumer buys the electricity → blockchain based meters update the blockchain, creating a unique timestamped block for verification in a distributed ledger: 1)At the distribution level, system operators can leverage the blockchain to receive energy transaction data to charge their network costs to consumers; 2) Reduces data requirements and increases speed of clearing transactions for transmission system operators as transactions could be executed and settled on the basis of actual consumption.

Smart contracts execute and record transaction in the blockchain load ledger through blockchain enabled advanced metering infrastructure (AMI). Blockchain based smart contracts can facilitate consumer level exchange of excess generation from DERs, EVs, etc. This could 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. This highlights the disruptive potential for blockchain on energy markets through the introduction of a more autonomous and decentralized transaction model. This peer to peer system may reduce or even replace the need for a meter operator if the meter blockchain is shared with the distribution system operator.

New blockchain opportunities, however, are also accompanied by new challenges. For one, blockchain policies

and regulations need to be in place to help determine licensing and other key roles for energy companies. For example, there still needs to be schedule and forecast submitted to the transmission system operator. Another challenge is incorporating individual blockchain consumers into a balancing group and having them comply with market reliability and requirements and submit accurate demand forecasts to the network operator. Managing a balancing group is not a trivial task and could potentially increase costs of managing the blockchain [15]. To avoid costly disruptions, blockchain autonomous data exchanges, such as demand forecasts from the consumer to the network operator will need to be stress tested for security and reliability before deployed at scale.

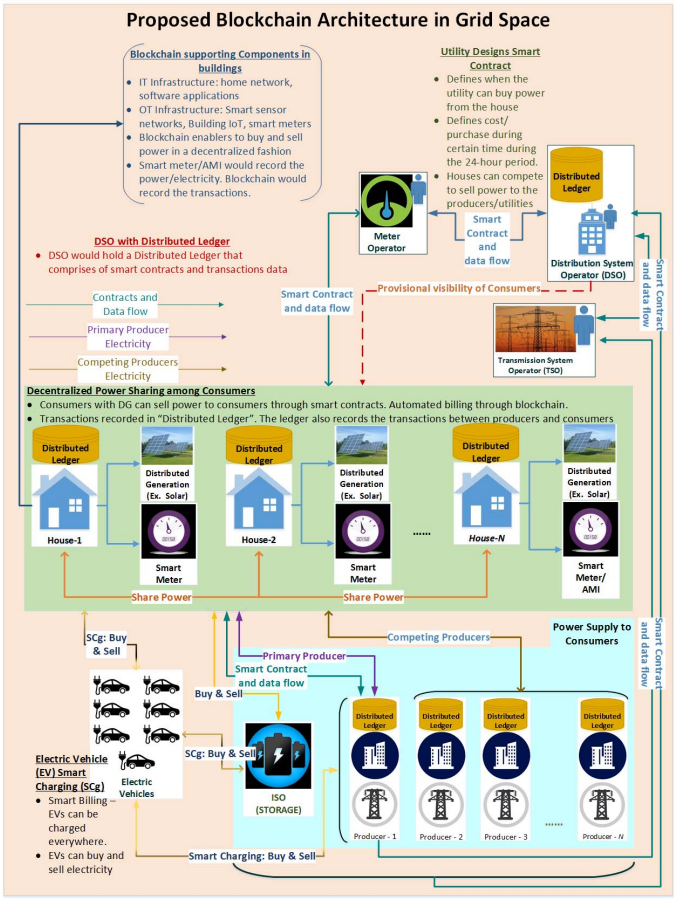

Fig. 1. Blockchain Application to the Electricity Infrastructure [15]

V. Blockchain Cybersecurity

A. *Collaborative testing of Blockchain in Grid Space*

Blockchain provides a unique way to distribute trust that has a clear cybersecurity value proposition. 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, such as keyless signature infrastructure (KSI), may increase reliability of authentication and encryption without the laborious, cost prohibitive deployment of keys. Blockchain applications also increase the trustworthiness and data provenance with "immutable properties that can be distributed and validated independently by any entity across boundaries or authority enclaves" [16]. Moreover, blockchain applications can help secure communications from industrial control systems and other operational technology (OT) protocols (Modbus, DNP3, BACnet, etc.) 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 the signature.

Guardtime, one of the largest blockchain providers by revenue, leverages a keyless signature infrastructure to provide a highly redundant, distributed, and secure distributed platform, allowing users to access and participate in the cryptographic signing of events [14]. This approach complements various energy use cases in that it can leverage existing energy infrastructure and cloud platforms to secure and enable the backend of various cloud-based energy-management solutions for buildings and facilities. Combining cryptographic signing events and distributed infrastructure may help increase fidelity of data, competition and real-time energy exchange for micro grids and building to building energy generation and sale.

Increased data fidelity afforded by blockchain could also help detect targeted cyber-attacks and increase resiliency of DER grid integration. Current techniques used in energy distribution and buildings-to-grid connections are vulnerable to cyber-attacks [10]. The integration of DERs without appropriate cybersecurity measures including trustworthy communications and monitoring could potentially destabilize the power grid and create outages and reliability problems for customers. These vulnerabilities can be exploited by an adversary to execute attacks without being detected due in part to the lack of encryption and authentication of DERs. There are number of potential attack scenarios worthy of additional blockchain mitigation research. Currently, attackers may be able to tamper with DER data sent to the energy management system exploiting unsecured communications to compromise the input-output signals of the DER or the DER control algorithm. Blockchain could help mitigate this type of attack as the ledger would record the energy transaction time and use data as registered in block. This provides a means of verifying what data is valid and what data is invalid, enabling the blockchain platform to quarantine data, drop malicious commands not contained in the smart contract and return to a steady state.

The impact of an attack depends on the number of devices compromised, the location of the devices (e.g., close to the substation or away from the substation), the condition, configuration and characteristics of the distribution feeder as well as the type of the attack. All different parameters that can be explored in PNNL's Buildings-to-Grid (B2G) Cybersecurity Testbed infrastructure. Certainly, additional research and development of blockchain security applications are needed to securely deploy DERs at scale and execute transactions at speed. In addition, policies and standards are needed to facilitate the deployment of blockchain into the power grid.

Blockchain is being adopted by a large number of energy utilities in Europe [17, 18] and its value to the energy sector is proven. Yet, many questions remain. As a result, technical risks to realize projects goals include: inability to transact energy securely at speed and scale. In addition, the lack of standardization and regulation around blockchain technology create various interoperability, legal and security challenges.

B. *Key Blockchain Cybersecurity Questions in Grid Space*

Blockchain based smart contracts improve the state of the art of both grid modernization and security by increasing trustworthiness and efficiency of electricity infrastructure. Blockchain is based on a proven cryptograph signature that

prevents manipulation of energy transactions and configurations of energy delivery systems. Due to its distributed nature, instantaneous recording, and cryptographic signatures, blockchain may be more resistant to tampering than centralized systems currently deployed in the power grid. Smart contracts also remove the need for 3rd parties to verify and enforce contracts, enabling secure real time transactive energy applications to function with speed, security and controllability of data. This section explores some of the key cybersecurity questions associated with blockchain:

1. How does Blockchain help prevent adversaries from "hijacking" a transactive retail market, and posting their own fake market signals?

Blockchain security solution does not guarantee 100% security or prevention of attacks. Instead it improves security through authentication, encryption and ability to verify integrity of the data. Thus, blockchain shows promise to facilitate secure data exchange at the Grid's edge and other infrastructures with embedded systems that are increasingly interconnected, including cloud based platforms and transactive energy which requires dynamic and highly scalable event driven architectures. In exploring this question and others it is also important to distinguish between blockchain keyless signature infrastructure solutions, such as Guardtime's Blockchain, which is permission based and cryptocurrency blockchain deployments – like Bitcoin, which is proof of work based. Permission based solutions require signing entities to authenticate to the infrastructure before signing using the block [16].

Security feature 1: Guardtime's KSI provides a distributed ledger that records all transactions in a way where the data receives: a. immutable data authenticity, verification of signing entity and signing time. The first security layer is Blockchain KSI cryptographic technology – the atomic outputs of participation are also called KSI Signatures.

- Assigns a data signer, authenticity of the data, and time of signing to a data asset in the transactive retail market.
- This is represented by including the hash of the data in the signature. The data format being signed can be anything in a digital format [16].

Security feature 2: The second security layer of the Blockchain KSI is the stack. This provides a highly redundant, distributed, and secure platform for which entities can leverage to access and participate in the cryptographic signing events.

- This stack can be distributed to individual customer premise, or leveraged in a managed service or cloud approach depending on customer requirements and use case.
- Because of the combination of both the cryptographic signing events and this distributed infrastructure, multiple customers can leverage the same widely witnessed KSI Blockchain with no overlap in infrastructure if needed, while still having the ability to cryptographically verify the other entities data when needed, creating a true cross boundary trust mechanism [16, 19].

2. How does BC prevent hackers from getting in to the consumer's behind-the-meter systems, either at the device/IOT level, or the supervisory Hybrid Energy Manager (HEM)/Building Management Systems (BMS) level?

Blockchain may not prevent access to behind the meter systems. However, blockchain reduces and/or removes need for third party to clear transactions. And by doing so, it potentially helps reduce the attack landscape by reducing number of nodes susceptible of attack. But, its security value is more about the securing or protecting integrity once an attacker is already in a system. Blockchain can help detect manipulation of configurations or critical systems are changed or the terms of smart contract are manipulated. It can also isolate or drop malicious actors or at least provide forensic evidence of tampering sufficient for settlement or to reconfigure to baselines.

3. How does BC Identify DER devices and nodes unambiguously and prevent spoofing?

Blockchain's two security layers provide distributed data validation to previously segregated architectures. Where before, entities required to be part of a trusted community, such as an authorized member of a Public Key Infrastructure or Active Directory Domain, KSI provides a distributed, widely witnessed trust anchor backed by Blockchain technology. This provides the ability for a verifying entity to verify who signed the data, what the data should be, and what time the data was signed without explicitly [16].

VI. PNNL Blockchain Application to Energy Arena

A. Exploring Blockchain Smart Contracts & Cybersecurity in PNNL's Buildings-to-Grid (B2G) Cyberseurity Testbed

Exploring blockchain cyber threats, vulnerabilities and mitigations in the context of securing the grids edge and providing more secure transactive energy solutions would provide a significant contribution to grid cybersecurity and resilience research. This research leverages PNNL's buildings-to-grid cybersecurity testbed (Fig 2) to validate and verify the application of blockchain technology to securing distributed energy exchange at both speed and scale.

PNNL's B2G Cyber Testbed provides the capability to model and simulate energy delivery systems from the distribution substation all the way to the end consumer. In addition to capturing the physical system details, the model also captures the overlaying cyber control system, wherein industry-grade hardware and communication protocols are used to closely mimic real-world control hierarchies. Of specific interest to this proposed effort is the OT/IT communications between the blockchain ledger and control systems at three levels: 1) Local level—local and supervisory building automation system (BAS) controllers, 2) System level—control at the BEMS level, and 3) System of systems level—control at the distribution control center. Fig 3 shows high-level rendering of buildings-to-grid cybersecurity testbed, highlighting its integration with infrastructure supporting PNNL's transactive campus.

B. Combining PNNL's B2G Testbed And Connected Campus To Improve Blockchain Transactive Energy Solutions

If PNNL's Buildings-to-Grid Cybersecurity Testbed can simulate various cyber-attack scenarios, threats, vulnerabilities and blockchain mitigations, PNNL's Connected Campus provides the necessary speed and scale to validate and verify blockchains application at the cyber energy nexus. Combing these two unique testbeds may help improve the state of the art

in blockchain application to provide security, speed and scale to transactive energy.

The connected campus is an integrated feature of the B2G Cyber Testbed. Originally, PNNL, Washington State University, and the University of Washington built of their Pacific Northwest Smart Grid Demonstration Project. This was the first-time researchers could test the use of transactive control of building loads at this scale, involving multiple buildings and devices. The transactive concept combines financial signals and dynamic control techniques to shift the timing and quantity of energy usage in devices and buildings resulting in greater efficiency and reduced energy costs, while also providing significant flexibility for the power grid [20].

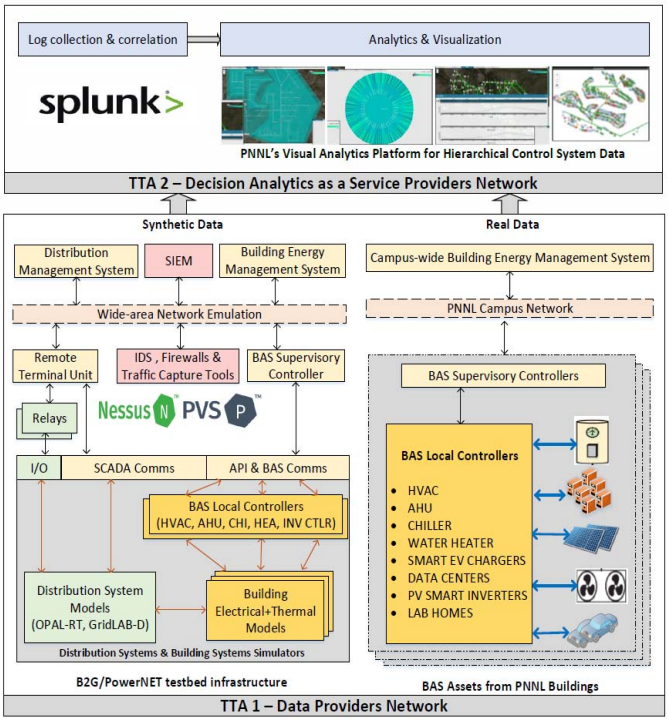

Fig. 2. PNNL's Buildings-to-Grid (B2G) Cyberseurity Testbed [21]

C. PNNL Transactive Campus

Transactive energy is defined as a system of economic and control mechanisms that allows the dynamic balance of supply and demand across the entire electrical infrastructure using value as a key operational parameter [21, 22]. PNNL has been the leading national lab in the clean energy and transactive campus (CETC) research efforts focused on buildings to grid DER integration and optimization [23]. While these efforts help enables agreed upon actions for each responsive building or energy resource within each campus, without human interaction. PNNL's transactive campus included active and passive automation and diagnostic systems in more than 10 PNNL buildings to find operational issues, to manage building loads. Blockchain provides the operators with increased visibility and control of building load transactions, price signals, control commands, and other information exchanged that is logged into blockchain's ledger, improving: 1) controllability with security; 2) trusted transactions through smart contracts; 3) data integrity and visibility through ledgers.

PNNL has designed the transactive energy architecture to manage devices, data, and decision-making in a connected buildings environment. Through those intelligent controls, the buildings are already enabled to communicate and to adjust energy loads [24]. Such connected transactive campus offers a realistic testbed to perform blockchain framework testing: 1) To implement the blockchain as an overlaying security architecture across those various connected buildings in PNNL; 2) To set up smart contracts to define energy exchange and consumption, load management, and building-to-building transactions; 3) To enable end-point cyber security in realizing those optimized energy management controls.

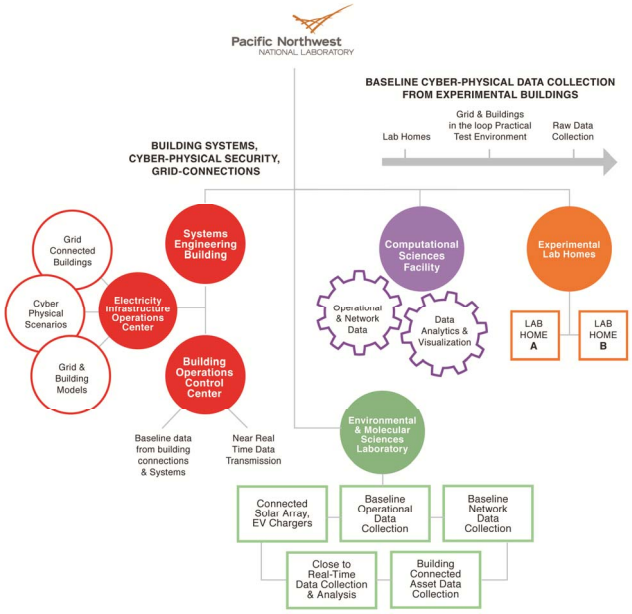

Fig. 3. PNNL B2G Cybersecurity Integration + Transactive Campus [18]

The blockchain based transactive energy testbed may provide a path for a more secure and efficient transactive campus with the ability to exchange information and operate loads more effectively, efficiently and securely. This unique infrastructure and integrated testbed also presents a unique environment to explore a number of timely research questions related to blockchain application to electricity infrastructure and grid modernization. These questions include, but are not limited to: 1) How can blockchain smart contracts facilitate DER/DG prosumers that can sell to a consumer network based on the smart contract pricing? 2) How can blockchain help secure the grid's edge which is increasingly networked and digitized to EioT cyber-physical devices that are potentially vulnerable to cyber-attacks? 3) If blockchain can help cut out 3rd parties, who will be the winners and losers? 4) What are the potential security and privacy vulnerabilities of applying blockchain to the grid? 5) What should Blockchain best practices, policies, standardization, and regulations look like?

CONCLUSION

Currently, the power grid lacks the necessary security and resilience to prevent cyber-attacks on DERs, grid edge devices and associated electricity infrastructure. Cyber vulnerabilities and interoperability challenges also extend behind the meter into building automation and controls systems. Applying blockchain could help increase fidelity and security of buildings to grid communications. Moreover, multiple customers can leverage the same widely witnessed blockchain to cryptographically verify the other entities data when needed, creating a distributed trust mechanism.

Blockchain may also help solve several optimization and reliability challenges that have been ushered in with grid modernization. Currently, time-lags for payment and uncollected bills leaves value on the table and the real cost associated with the energy value chain is not captured.

Blockchain can record real time net loads and smart contracts execute customers distributed generated sales and purchases. Currently, grid operators lack visibility and control of real-time power flows and injections from DERs and distributed generation customers. Blockchain can help optimize network data and record residual energy at the substation level. Increasing the fidelity and control of utility data will also help settle with bulk systems as well as negotiate future contracts.

To improve blockchain technology applications to modernizing and securing the grid, it is important to simulate applications in a realistic environment to improve the state of the art at both speed and scale. While no testbed is identical to the power grid's complex system of systems, PNNL's B2G testbed and integrated Transactive Campus provide a unique combination of live telemetry and real-time data to simulate the power grid and improve the state of the art of blockchain security technology to create a more resilient grid.

REFERENCES

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

[2] V. Buterin, "A next-generation smart contract and decentralized application platform." *white paper*, 2014.

[3] K. Delmolino, K, et al., "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab", *Intl. Conf. on Financial Cryptography and Data Security*, Springer, pp. 79-94, 2016.

[4] A. Kosba, et al., "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *IEEE Symposium on Security and Privacy*, USA, pp. 839-858, 2016.

[5] K. Christidis, M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, no. , pp. 2292-2303, 2016

[6] E. Munsing, J. Mather, S. Moura, "Blockchains for Decentralized Optimization of Energy Resources in Microgrid Networks", UC Berkeley: Energy, Controls, and Applications Lab, USA, 2017.

[7] S. Chen, C. Liu, "From demand response to transactive energy: state of the art", Journal of Modern Power Systems and Clean Energy, Springer, vol. 5, no. 1, pp. 10–19, 2017.

[8] S. McNeil, "Privacy and the modern grid." *Harv. JL & Tech.* 25, 2011.

[9] Y. Huang, et al., "SmartGRID: A Fully Decentralized Grid Scheduling Framework Supported by Swarm Intelligence", *Intl. Conference on Grid and Cooperative Computing*, Shenzhen, pp. 160-168, 2008

[10] M. Mylrea, "Smart Energy-Internet-Of-Things Opportunities Require Smart Treatment Of Legal, Privacy And Cybersecurity Challenges", Jour. of World Energy Law and Business, vol.10,no.2,pp.147–158, 2017

[11] M. Mylrea, "Cyber Security and Optimization in Smart Autonomous Buildings", Stanford University, AAAI Symposium, 2016

[12] L. Trottier, "original-bitcoin", 2013, [Online]. Available on Github

[13] P. Franco, "Understanding Bitcoin: Cryptography, Engineering and Economics", John Wiley & Sons. p. 9, 2014

[14] PWC Global Power and Utilities, "Blockchain opportunity for energy producers and consumers", 2017

[15] M. Mylrea, S. Gourisetti, "Leveraging AI and Machine Learning to Secure Smart Buildings", AAAI, Stanford University, Springer (review).

[16] Guardtime, "Keyless Signature Infrastructure (KSI) Overview", 2017.

[17] Coinfox, "European utilities to test blockchain-based energy trading", 2017

[18] Engerati, "Blockchain Europe: Utilities pilot peer-to-peer energy trading", 2017

[19] Mike Gault, "Blockchain Security Implications for the Industrial Internet", CIOReview: IoT Technology magazine, July 1, 2017

[20] PNNL, "Connected Campuses to Test Transactive Energy", 2015

[21] S. Sridhar, M. Mylrea, A. Ashok, S. Gourisetti, S. Pal, "Testbed Environment for Buildings-to-Grid Resilience R&D", Resilience Week, 2017 (forthcoming).

[22] GWAC, "GridWise Transactive Energy Framework", Jan. 2015

[23] Dennis Stiles, "Clean Energy & Transactive Campus Project", 2016

[24] GMLC, "Clean Energy and Transactive Campus", 2016