PNNL-27453

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Keyless Infrastructure Security Solution (KISS)

Technology Landscape Analysis Report

April 2018

ME Mylrea
SNG Gourisetti
H. Culley

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov


This document was printed on recycled paper.
(8/2010)

Acronyms and Abbreviations

BCC	Bitcoin Cash
BTC	Bitcoin
CIP	Critical Infrastructure Protection
DAO	Decentralized Autonomous Organization
DER	Distributed Energy Resource
DOE	Department of Energy
EDS	Energy Delivery System
ICO	Initial Coin Offering
IoT	Internet of Things
IT	Information Technology
KISS	Keyless Infrastructure Security Solution
KSI	Keyless Security Infrastructure
NERC	North American Electric Reliability Corporation
OE	Office of Energy
OT	Operations Technology
PoA	Proof of Authority
PoW	Proof of Work
SHA	Secure Hash Algorithm

Contents

Figures

Tables

1. Introduction

In realization of the U.S. Department of Energy Office of Electricity goals for the project "*Keyless Infrastructure Security Solution (KISS)*, the following landscape analysis explores blockchain or distributed ledger technologies application to securing electricity infrastructure and energy delivery systems. The exploration of how distributed ledger technologies can be used to increase the trustworthiness and integrity of the grid's edge is imperative to the economic, security and well-being of all modern societies that rely on electricity. Blockchain technology's ability to secure, track and optimize complex data transactions provides an exciting value proposition to securing and optimizing the U.S. power grid. Blockchain technology shows potential in securing energy delivery systems (EDS) operating at the grid's edge. This is important as EDS require unprecedented levels of security and trustworthiness to verify integrity of data and manage complex transactive and distributed Energy Resources (DERs) exchanges. Improving the ability to identify, control and secure grid-edge 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 following landscape analysis explores opportunities and challenges related to applying blockchain to grid cyber security. This is important as the U.S. power grid is a complex system of systems that requires more secure, reliable and trustworthy EDSs. Grid modernization has increased the speed and size of data sets exchanged on these systems (Gordes and Mylrea 2014). Exasperating the challenge is these systems are increasingly distributed creating new data fidelity and interoperability challenges for grid operators struggling to balance and incorporate DERs. Unlike public key infrastructure where there is a single authority that issues and revokes certs, blockchain keyless signature infrastructure being used in KISS applies an atomically verifiable cryptographic signature to help increase the trustworthiness of EDSs at the grid's edge. This feature is especially important at distribution level since EDSs and field devices have increasing operational and security requirements that are often diametrically opposed. For example, as data, speed and analytic requirements increase, security and functionality requirements increase. Further, as the grid's edge incorporate DERs and transacts in real time, availability is prioritized over the integrity and confidentially of that data.

Blockchain presents the prospect of solving some of these complex challenges related to grid security and modernization. However, many questions remain which require understanding the blockchain energy landscape, and validation and verification through additional research –goals of the KISS project. Realizing these goals is important as there are a number of theoretical blockchain applications to the energy sector, but few energy utilities have actually applied, implemented or even experimented with the underlying distributed ledger technology and consensus algorithms that enable blockchain to exchange data more efficiently and securely. To help fill these research gaps, the following landscape analysis explores:

1.) different blockchain technologies
2.) how blockchain is being applied to the energy sector
3.) how these technologies and applications apply to the Department of Energy (DOE) Office of Energy (OE) Cybersecurity for Energy Delivery Systems *Keyless Infrastructure Security Solution (KISS)* project: to develop a KISS to increase the trustworthiness, speed, integrity and resiliency of EDS responsible for transactive energy exchanges and integration of DERs.

1.1 Blockchain Definitions

Blockchain means different things to different people; therefore, it has many definitions. For the KISS DOE OE-sponsored project, we are defining blockchain as a distributed database or digital ledger that records transactions of value using a cryptographic signature that is inherently resistant to modification (Trottier 2013). 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 (Tapscott et al. 2016). Blockchain-based smart contracts can be executed without human interaction (Franco 2014) 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 (Tapscott et al. 2016).

Blockchain Keyless Signature Infrastructure (KSI) technology differs from proof or work blockchain based crypto currencies, such as Bitcoin and Ethereum. KSI is based around a concept of permission-based blockchain. It provides widely witnessed evidence on what can be considered the truth and does not rely on any single party. And, it does that while retaining complete confidentiality of the original data. Another unique characteristic that differentiates KSI blockchain from other distributed ledger solutions is its ability to scale to industrial applications to add one trillion data items to the blockchain every second, and to verify the data item from the blockchain within the next second. The ability to transact data at sub-second speeds is essential to handle the increasing data requirements of a modern power grid.

A number of other definitions are important to understand and consider. These changing definitions create a number of challenges from a policy perspective. (Walch 2017) notes: 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 times do not include an exchange of value and do not record anything publicly. Yet, Google defines (Jeffries 2018, Walch 2017) blockchain as "a digital ledger in which transactions made in Bitcoin or another cryptocurrency are recorded chronologically and publicly." Similarly, Investopedia's definition (Walch 2017) associates blockchain with decentralized ledgers of cryptocurrencies: "A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions."

IBM's definition (Walch 2017) is "Blockchain technology is used in a peer-to-peer network of parties, who all participate in a given transaction. Because the ledger is distributed, everyone involved can see the 'world state' at any point in time and can monitor the progress of the transaction."

A very general way to delineate differences between different blockchains is proof-of-work versus proof-of-authority, public versus private blockchains. Not that these mechanisms are the only distinctions, but they make up a large percentage of various blockchain applications. A proof-of-work consensus mechanism underpins Bitcoin's blockchain, replacing the need for a central authority with a consensus algorithm to incentivize members of the network to trust transactions.

Arizona's Electronic Transactions Act was amended in 2017, and its definition (Walch 2017) is "'Blockchain technology' means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth." However, a number of events have proven that blockchains can be changed, from forks to cyber incidents.

In general, blockchains are immutable digital ledger systems that are implemented in a distributed way. Blockchains allow a community of users to record transactions in a public ledger (i.e., public to that community) in a way that the transactions cannot be changed once published. Although blockchain technology is often tied to cryptocurrencies, the technology can be used more broadly in a variety of applications. All the transactions over blockchain are cryptographically signed and they are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult (almost impossible) to modify. New blocks are replicated across all copies of the ledger within the network, and any conflicts are resolved automatically using established rules." (Yaga, et al. 2018)

2. Blockchain and Grid Modernization

Power utilities generally live in a world separate from their customers (Basden, et al. 2017). Although they may deal with you as a customer through customer service, they answer more to regulators and shareholders. State public utility commissions set the rates we pay for electricity. Most utilities are effective monopolies, with no competition, and sadly, regulation tends to incentivize inefficiency—the mandate is to keep the lights on, at all costs, not to provide power at the lowest possible price.

The electricity industry is due for a change, including greater customer empowerment through technology. Power prices have risen almost 50% in the last 15 years, even as the price of natural gas–which drives more generation than any other energy source–has fallen. Distributed generation plus the internet allows power to be produced and distributed more efficiently, and there is no reason customers should effectively pay for legacy grid investments that don't create new value to the end user. As a result, new blockchain energy startups – like Drift (Schiller 2017) aim to disrupt and improve the cost and value of service provided by traditional energy utilities by using distributed ledger technology to facilitate peer-to-peer energy sales.

Over time, technology may begin to undercut the current model, which effectively guarantees returns to companies. Solar panels and home storage systems allow homeowners to operate more independently of utilities, leading many utility companies to resist solar options. The accessibility of the internet allows for new forms of trading that are more "peer-to-peer" (supplier-to-customer) rather than "hub-and-spoke" (where utilities take up an enlarged role in the middle).

Residential consumers who have solar panels installed on their homes are already used to selling power back to the grid. When their home-based rooftop panels produce more electricity than is needed at any time, the residential customer can send energy to the wider network and gain a credit on their utility bill in return. That process is called net metering. In the future, the goal is to provide ways to sell power to other residential customers in addition to the utility companies. One way of accomplishing this goal is the use of the blockchain.

There has been a lot of interest in blockchain technology in the energy industry, with several early-stage projects already emerging. Drift has launched a blockchain-based utility in New York. LO3 Energy has launched a blockchain-based microgrid in Brooklyn. A large group of companies are involved with the Energy Web Foundation, a nonprofit group founded by the Rocky Mountain Institute and Grid Singularity, an Austrian blockchain developer focused on energy applications. Power Ledger has several blockchain pilot projects in Australia. In Austria, the country's largest utility conglomerate, Wien Energie, is taking part in a blockchain trial focused on energy trading with two other utilities. In Germany, the power company Innogy is running a pilot to see if blockchain technology can authenticate and manage the billing process for autonomous electric-vehicle charging stations.

With grid modernization comes a changing landscape:

1.) Consumers are new producers—new technologies are rapidly being adopted that allow prosumer (someone who is both a consumer and a producer of energy) to enter into the energy system.
2.) Costs of building on the model of the past are economically unviable; energy in our current structure is largely wasted—the United States economy is 86 percent energy inefficient, meaning most of our energy is consumed for "energy", the combined losses from transmission and distribution, combustion, and conversion to work. This means that only 14 percent of energy is consumed for useful work, or "exergy."
3.) Innovation is locked out—regulated electricity market players are not able to easily innovate to respond to the changing landscape.

The legacy grid model is not completely secure or practically scalable. Cyber-attacks are increasing, and the current system is not scalable to the developing world.

In general, blockchains are immutable digital ledger systems that are implemented in a distributed way—without a central repository—and many times without a central authority. Blockchains allow a community of users to record transactions in a public ledger (i.e., public to that community) in a way that the transactions cannot be changed once published. Beginning in 2008, the blockchain concept was innovatively combined with several other technologies and concepts to bring about the creation of modern cryptocurrencies—electronic money that is protected through cryptographic mechanisms. Bitcoin was the first such approach, but other successful e-commerce systems include Ethereum, Litecoin, and Ripple. Although blockchain technology is often tied to cryptocurrencies, the technology can be used more broadly in a variety of applications.

"Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across all copies of the ledger within the network, and any conflicts are resolved automatically using established rules." (Yaga, et al. 2018)

Blockchain and distributed ledger technology has a number of properties that facilitate more efficient and decentralized energy transactions.

- **100% up time:** Blockchain provides a reliable, fail-safe "logically centralized, physical 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. That being said, blockchain technology provides an atomically variable time stamped cryptographic signed electronic transaction that has proven very difficult to change.

- **Immutability:** It can lead to a number of challenges. Recently it was found that child pornography was saved in the Bitcoin blockchain (Suberg 2018). When illegal images or data are saved in the blockchain, it can prove very difficult to change. Another potential way to change the blockchain is to control or compromise 51% of the nodes needed to reach a consensus.

- **Big Data Management Blockchain:** It facilitates the distribution of prodigious data sets between organizations. Data can be synchronized and archived between multiple parties.

The KISS project leverages keyless signature infrastructure blockchain which is a permissioned proof-of-authority blockchain. One of the major advantages of permissioned proof of authority (PoA) blockchain is the authority node has complete control on the participating nodes and the type of transactions to be carried. In addition, the KSI blockchain does not publish any sensitive information on the blockchain which eliminates the privacy and security challenges that are associated with typical proof of work (PoW) blockchains.

3. Blockchains in Operation and Core Features

There are different types of blockchain consensus models and the well-known ones include PoW, proof of stake, PoA. In all those consensus models, some level of agreement is expected between the participating entities, otherwise known as "nodes". As shown in the below sections, each consensus model has unique features that are fit for specific purposes. Given the complexity and security associated with the grid systems, PNNL KISS research team has determined that PoA blockchains will provide such need security, privacy, confidentiality, and integrity.

Further, blockchains are categorized as permissioned vs permissionless blockchains. If any individual can read or write to a blockchain, it is considered permissionless. If only specific users can read or write to the blockchain, it is considered permissioned. Permissioned blockchains deviate from the original intention of the Bitcoin blockchain where everyone could read and write to the blockchain and the ledger was transparent. If multiple organizations would like to work together but do not fully trust each other, they can create a permissioned blockchain and record their transactions on a shared distributed ledger. These blockchains can be set up in a variety of ways. For example, they can be set up, so anyone can read them, but only selected members can record transactions on them or they can be set up, so anyone can record transaction on them, but only selected members can read the data. PoA blockchain architecture often resonates with the permissioned blockchain. In the EDS space, PoA permissioned blockchain gives visibility and authority to critical bodies such as DSO, utility. All blockchain nodes interact through smart contracts. A smart contract is a collection of data and code that is deployed to a blockchain. Transactions completed in the future can send data to a variety of public methods offered by a smart contract and the code that is on the blockchain is immutable. A smart contract can store information, perform calculations, and automatically send funds to other accounts.

Ledgers: A ledger is a collection of transactions and the blockchain ledger will be copied and distributed to every node within the system. New transactions would be submitted to a node, which then would alert the rest of the network that a new transaction has been submitted (this is a pending transaction and is not included in a block). After completing the system's required consensus method, the new block will be included and distributed throughout the system, and all ledgers will include the new transaction.

Blocks: A user may submit a candidate transaction to the ledger by sending the transaction to other nodes participating in the blockchain. These transactions are then disseminated to the other nodes in the network. These distributed transactions then wait in a queue, or transaction pool, until they are added to the blockchain by a mining node (a node that is part of a subset of nodes that maintain the blockchain by publishing new blocks); this occurs when the mining node publishes a block. The block contains a set of validated transactions. After it is created, each block is hashed, and therefore creates a digest that represents the block. A data structure known as a Merkle tree is utilized rather than storing the hash of each transaction within the block's header. A Merkle tree combines the hash values of data together until there is on root. The root is an efficient means for summarizing the transactions in a block and verifying the presence of a specific transaction within a block.

Proof of Work: In the proof of work model, a user is given the right to publish the next block by solving a computationally difficult puzzle. Solving the puzzle is the "proof" that they have performed work. Each

puzzle for a block is independent and requires the same amount of work. The proof of work model is designed for when there is little to no trust between users of the system. But many challenges remain. The KISS project avoided public PoW solutions for a number of 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 (Deetman 2016, Hern 2017, Power Compare 2017). Another challenge is that these nodes are widely witnessed and may lack the necessary privacy considerations. PNNL was able to leverage its Shodan research to identify additional information about where some of the more popular PoW blockchains are located. The below figure (Shodan LLC 2018) shows where some of the most popular public proofs of work nodes are and top organizations involved in those nodes. Through KISS, the nodes will be anonymized and can only be addressed through their secure hash value eliminating the well-known privacy concerns associated with typical PoW blockchains.

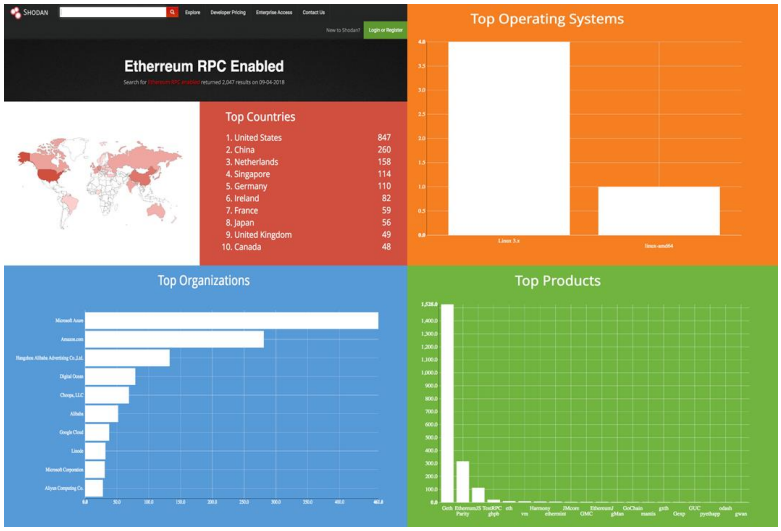

Figure 1. Exposure of widely witnessed PoW blockchain nodes and participants through Shodan

Proof of Stake: The proof of stake model is based on the idea that the more stake, the more likely it will want the system to succeed (and hence, the less likely it will want to undermine it). This model uses the amount of stake that a user has as the determining factor in new block creation. The system may use the stakes in a variety of ways, including multi-round voting, coin aging systems, and random selection of staked users. With this model, resource intensive computations are not needed, and therefore is less expensive in electricity, time, and processing power costs. In a multi-round voting (or Byzantine fault tolerance proof of stake [Bahsoun et al. 2015]) system, the blockchain selects several staked users to create proposed blocks and then allows the staked users to vote in multiple rounds. A new block is decided upon after multiple rounds. In the coin age proof of stake system, a user's staked cryptocurrency has an "age" property. Once a certain time has passed, the cryptocurrency can be spent, and a new block can be created; however, once it is spent, the age resets to zero and it cannot be used again until the required amount of time has passed. This system allows those with more stake to create more blocks, but without the fear of them dominating the system.

Proof of Authority: PoA blockchains have special nodes that act as trust anchors and that must agree. If they don't, consensus algorithms like voting are used. PoA works much more efficiently than PoW, but doesn't cover edge cases where trust anchors can vote for multiple different histories because there is no real cost for doing so. This works against ultimate consensus. Non-currency ledgers such as Hyperledger Fabric and GuardTime's Keyless Infrastructure System also use PoA. Now that several principle components of blockchain are defined, Table 4-1 provides a comparison of the technical aspects of various blockchains by vendor.

Table 1. Comparison of Technical Aspects of Blockchain

Topic	Bitcoin	HDAC	Ethereum	KSI	Hyperledger
Target Applications	Financial Transactions (Bitcoin script)	low cost automated transactions between IoT devices	Smart Contracts	Data and system Integrity, secure timestamping	Modular platform for business solutions with identity and smart contracts
		Public/Private Blockchain	Solidity, Serpent		
Smart Contract					
	NA	Yes	Yes	Yes	Yes
Consensus	Proof of Work (PoW)	ePoW; Trust-based	PoW	Proof of Authority (PoA)	PoA
Transaction Speed	7 tx/sec	~160 tx/sec (public)*	25 tx/sec	exabyte-scale/sec	Current: 1000tx/sec. Improvements coming for HLF V1.1
		~ 500tx/sec (per one private chain)			
Scalability	Limited by block size and creation frequency	Limited by block size and creation frequency	Limited by block size and creation frequency	Near-linear growth to the number of nodes.	
Block Time	10 minutes	3 minutes	12 seconds	1 second	
Finality	>= 1 hour (6 blocks)	>= 3 min	>= 3 min (12 blocks)	1 second	
Block Size	1MB	Dynamic (Max. 8 MB)	Dynamic	53 bytes	As per previous entry
Guaranteed download of complete history	Yes, from other nodes	Yes, from other nodes with access	Yes, from other nodes	No (dataset completeness not guaranteed, but any given entry can be validated)	
Extra Data	80 byte	Dynamic (Max. 4 Kb)	Dynamic 5 gas/byte[1]	Dynamic	
Topology	Public blockchain	Private/Public, Permissioned	Public, Permissionless	Private, permissioned	Permissioned
Privacy Model	None	Private blockchains	None	Hashing (data never leaves premises; only masked hashes do)	hashing, channels
Identity & Access Mgmt, authentication	PKI	Access rights administered on the blockchain	PKI	Hierarchical gateway-based	PKI
Programming	C++	C-like syntax	Solidity	C, Java SDK	Javascript, Java, Go
Deterministic transaction execution	Yes	Probably (using a virtual machine)	Yes	N/A	
Offline Verification	No	No	No	Yes - KSI calendar	
Post Quantum Security	No (but extendable in the future)	Unknown	Yes	Yes - since it is based only on hash functions	
Participation mechanism	Public	Public/permissioned	Public	Permissioned	Permissioned

[1] https://ethereum.stackexchange.com/questions/3/what-is-meant-by-the-term-gas

4. Potential Blockchain providers in the Energy Space

Some theoretical and applied Blockchain Applications in the energy space include (Gerber 2018):

- **EV Charging:** Use blockchain to record the energy consumed by the EV. This amount in kWh is subtracted from the smart meter read or billing to determinate data for the prosumer.
- **Mandate Management:** In a market with a central register of meter reads, only contract parties are allowed access to a given customer meter data.
- **Asset Lifecycle Management:** Use blockchain to manage end-to-end lifecycle of assets' parts and/or components (construction, operations, maintenance, disposal).
- **DER Transaction Processing:** Use blockchain to process any transaction involving a DER asset, e.g. storage, solar PV, EV, micro combined heat and power (micro-CHP).
- **Nuclear Decommissioning:** Use blockchain to control end-to-end nuclear decommissioning process for all parts and/or components along the asset lifecycle.
- **P2P Trading of Distributed Energy:** Use blockchain to implement multi-sided platform for direct trading of distributed energy generation.
- **Energy Trade Settlement:** Use blockchain to settle trades at energy exchanges (e.g. EEX; owned by Deutsche Boerse), OTC/extra-exchange trades, or for direct agreements/trades between market participants.
- **Energy Coin:** Use blockchain to prove authenticity of energy origin
- **Supplier Switching:** Supplier switching within 24h, as mandated by Office of Gas and Electricity Markets (ofgem).
- **Emission Certificates:** Use blockchain to generate, own, trade emission certificates related to energy generation.
- **Compliance Internal Ledger:** Use blockchain for improved bookkeeping, data mining, and records verification to reduce the effort spent on reconciling information among various computer systems; various applications.
- **Shared Ledger of Reference Data:** Use blockchain to provide reference data that is relevant to a number of market participants in real time and with full accuracy (single version of the truth); various applications are possible.
- **Energy Delivery Settlement:** 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.
- **Virtual Metering:** Use blockchain to augment smart meter for recoding energy use of appliances (EV, Heating).
- **Energy Trading:** Trade secondary reserve power.

Beyond cybersecurity, blockhain shows potential to simplify today's multi-tiered energy sector in which power producers, transmission system operators, distribution system operators and suppliers transact on various levels by directly linking producers with consumers. To address some of the above application requirements, there have been multiple blokchain vendors investing and investigating the applications in energy/grid space. The companies that has been making progress in the energy space include:

LO3 Energy: LO3 Exergy (Morris 2017, Exergy 2017) is a startup company focused on building blockchain-backed "smart grids" for local energy trading. LO3 created Exergy – a multi-layered blockchain to tackle the transformation of traditional energy market to prosumer-based market.

WePower: WePower (WePower 2017, Schiller 2017) is a European startup company that was established to change the way energy is developed and distributed. WePower proposes to bring together producers of renewable energy, including solar, wind, and hydro plants, as well as to sign up investors who pay upfront

for the right to consume electricity generated by those plants. To accomplish this, it has created its own cryptocurrency—a token called WPR. Each token represents one kilowatt-hour of power produced and the tokens are tradable on the platform. Using this method, producers can sell energy upfront in the form of a token rather than taking on debt.

Drift: Drift (Schiller 2017) is a startup utility from Seattle that is launching a method of lowering energy cost in New York. This initial launch links up independent upstate power producers with residents in New York; it aims to cut out the center of the supply chain, including unnecessary middlemen and outdated software. Drift customers are able to choose whether they would like to prioritize clean power or cheap power using a web-based dashboard.

Rocky Mountain Institute Energy Web Foundation (EWF): A host of companies has joined forces to support the Energy Web Foundation (EWF) (Morris 2017, Zeranski 2017) a non-profit organization whose mission is to accelerate the commercial deployment of blockchain technology in the energy sector. EWF's current test network is a proof-of-concept for the new consensus algorithm. It is called "Kovan" and is able to perform up to 1,000 transactions per second. The KISS team would like to highlight that this is another effort the team has been investigating to find its relevance in energy space. Although these investigations are not part of this particular project, the team may discover aspects that might be relevant to KISS project.

Power Ledger: The Power Ledger (Power Ledger 2017) Platform (Platform) is a transparent and interoperable energy trading platform that supports a growing suite of energy applications with the use of an exchangeable frictionless energy trading token, Sparkz. Energy trading applications have already been proven and are deployed in energy markets and communities in Europe, Australia, and Asia.

Hyperledger: Hyperledger is a group of projects that aim to create enterprise grade, open source distributed ledgers (Hyperledger Projects 2018). This project is supported and hosted by the Linux Foundation, but each project was contributed to and developed by different sources. Some of the projects that evolved from Hyperledger to solve specific problems include Hyperledger (Fabric, Sawtooth, Iroha, Burrow, Indy).

Guardtime's KSI: Blockchain KSI differs from proof of work blockchain based crypto currencies, such as Bitcoin and Ethereum. This a permissioned proof-of-authority blockchain with unique features such as storing the hash of data on the blockchain instead of the data itself. Such niche features imply a tremendous increase in speed of executing smart contracts over KSI blockchain.

5. Guardtime's KSI Overview

Blockchain KSI differs from proof of work blockchain based crypto currencies, such as Bitcoin and Ethereum. KSI is based around a concept of permission-based blockchain. Blockchain KSI provides widely witnessed evidence on what can be considered the truth and does not rely on any single party. KSI performs the validation while retaining complete confidentiality of the original data. Another unique characteristic that differentiates KSI blockchain from other distributed ledger solutions is its ability to scale to industrial applications to add one trillion data items to the blockchain every second and to verify the data item from the blockchain within the next second. The ability to transact data at sub-second speeds is essential to handle the increasing data requirements of a modern power grid.

KSI has been in production use since 2007, is employed by a number of world's governments—i.e., Estonia and Defense contractors in the United States—and is beginning to see adoption in the private

sector for application of their systems and networks. Blockchain KSI may also help realize a number of cybersecurity and compliance goals for the energy sector, such as:

- **Smart contracts:** Smart contracts execute and record transaction 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 is a possible option to fill various 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 security of EDSs at the edge. Blockchain can be used to verify time, user, and transaction data and protect this data with an immutable crypto signed distributed ledger.

- **Blockchain KSI**: It 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, where it is transactions related data or system-to-system data—two major challenges that currently threaten the security of electricity infrastructure. Implementations of blockchain integrity mechanisms, such as KSI, may increase reliability of authentication and encryption without the laborious, cost prohibitive deployment of keys. Blockchain applications may 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” (Guardtime 2017). Moreover, blockchain applications can help secure communications from industrial control systems and other operational technology 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 signature.

6. Why Guardtime KSI?

Guardtime's Keyless Signature Infrastructure (KSI) does not store arbitrary data on the chain, not even links. All that can ever be stored on the blockchain are values of verifiers which are hashes of content arranged in a Merkle tree and time stamped. These hashes can be certified without having an entire copy of the blockchain locally. Thus, no-one can place or link data on the blockchain. They may use the chain to irrevocably attest that they have data of any kind, size, or content, but they cannot store any arbitrary content on the chain.

Total control of what goes on the blockchain produces two other benefits: (1) KSI blockchains grow more slowly than other blockchains and have an upper bound on their rate of growth, and (2) KSI blocks may be highly organized and optimized for rapid search and processing.

The organization of KSI blockchains makes their transaction performance superior to other blockchains and comparable to a centralized database. While the blocks on most blockchains have highly variable content, KSI blocks consist of Merkle trees of hashes. A Merkle tree is a binary tree where the data in the leaves is hashes of data to be verified and each fork is made from the hash of the concatenation of its two child nodes. Nodes are combined in this way until there is a single root value whose hash is completely determined by the hashes of all the data in the leaves. No data in the tree may change without invalidating

the root and every fork leading to the modified data. This makes it possible to (1) assure validity of a large number of transactions and (2) if a change is introduced, identify exactly where it was made. Another benefit of the Merkle tree structure is that to verify the hash of a single leaf node, only the hashes that participate in its contribution to the root value need to be compared to verify it. The number of hashing operations needed to verify authenticity is only$[2\log_2(n)+1)]$ as opposed to [n-1], where n is the number of transactions in the block. Since hashing operations are computationally expensive this is a substantial savings. And since the number of hashes grows much more slowly, it is easy to abstract the relevant hashes from the tree and preserve them as the "signature" of the item without needing any keying infrastructure. KSI can be seen more as a chain of highly organized binary trees, a tree-chain, than as a chain of opaque blocks.

Without signatures the root of trust in the KSI system is in the gateway aggregator nodes. In KSI, contributors of hashes send in hashes of data along with a hash-based message authentication code (HMAC, a cryptographic hashing operation that uses a secret key to verify authenticity of the message source). Decentralized public key cryptography allows users and infrastructure nodes to select a large number as private key and to generate a public key from this. No central trust is needed to do this. HMACs are signed by this private key, and the system believes that the content given to it is accurate because the HMAC is a signed hash, and it can only be reproduced by someone who has the private key of the sender. However, the user must trust the KSI gateway to properly authenticate its hashes and form the Merkle tree. This is solved by two means: first, the gateway is generally privately owned by a trusted partner, and second, there is no real motivation for it to behave badly except simply to deny service.

Since KSI stores no data, the data may be stored anywhere. When it is attested by the KSI system the sender receives a signature back from the data that shows its authenticity. Anyone having the original data and this signature can independently verify that the data was created authentically and at the time claimed. The result is a system that establishes trust with only a bare minimum infrastructure and no requirement for trust in any entity.

7. KISS Project Overview

The project plans to develop a Keyless Infrastructure Security Solution (KISS) to increase the trustworthiness, speed, integrity and resiliency of EDS responsible for transactive energy exchanges and integration of DERs. KISS will develop the first blockchain Keyless Signature Infrastructure (KSI) prototype to continuously monitor and autonomously verify energy exchanges. KSI will also enhance the existing cyber security integrity features in the overall VOLTTRON platform by providing integrity violation and tamper detection capabilities for application, configuration, and endpoint telemetry services. KISS team will also develop a VOLTTRON and EDS plug-in for blockchain based KSI smart contracts. These smart contracts will maintain ordered time stamped data blocks via the KSI blockchain and use of Keyless Signature XML dockets and validate and verify that KISS can validate transaction data and rapidly detect data anomalies and ensuring that the smart contracts can’t be modified retroactively. Some of the near-term to long-term goals of KISS are to:

1.) Examine the role of blockchain to secure and optimize complex grid edge transactions
2.) Investigate grid-cybersecurity applications for blockchain
3.) Design specifications and architectural requirements to develop blockchain plug-in driver/agent VOLTTRON platform to improve trustworthiness and integrity of transaction
    a. Engage utility partners, industry partners, and blockchain providers to gear towards the development of the blockchain plug-in driver for VOLTTRON platform

b. Test the VOLTTRON blockchain agent through testbed deployment and explore field deployment strategies

4.) Design the framework to develop smart contracts and blockchain based exchanges (commands, data, etc.) between the connected systems.
    a. Ensure device-device communication and data integrity with cybersecure command transfer and execution.
    b. Test, validate, and verify the associated automated and validated path management and supply-chain management
    c. Ensure the interoperability of the developed KISS agent to cohesively work with INGRESS technology developed by PNNL and UTRC as part of an ongoing DOE CEDS industry project. This may answer the important question: "What is a valid command?"

5.) Investigate and design the framework through a technical paper to develop smart contract between an energy producer and a consumer that autonomously and securely regulates both supply and payment.
    a. Engage utility partners, industry partners, and blockchain providers to gear towards the development of the smart contracts for this application (example: prosumer based, DER engaged transactive platform)
    b. Develop the architecture and methodology through a technical paper for the transactive application to be able to execute the smart contracts across the systems in testbed to explore field execution strategies

Advantages of Guardtime KSI specific to KISS:

- tested supply chain security mechanisms for large data sets and IoT envrionments that challenge traditional security paradigms around inventory
- ability to perform patch, configuration and identify management security
- atomically verified meta-data can be crytographically hashed to secure and preserve privacy
- provides sound alternative to limitations and vunerabliities around PKI
    - (for example: Guardtime's KSI that enables "trust" between different systems without the need of key exchange)
- data integrity and system to system secure command/data exchange
- support multifactor verification through a distributed ledger
- reduce costs of energy exchanges with an ability to perform real-time transactions/exchages
- ensure peer-to-peer consumer level exchange
- enable consumers to also produce, prosumers
- enables a more secure distributed escrow to maintain ordered time stamped data blocks that can't be modified retroactively
- rapid detection of data anomalies may enhance the ability to detect and respond to cyber-attacks
- perform verification without a trusted third party
- establish a pipeline for the distribution system operators to receive energy transaction data to be able to adjust the customer costs/bill.
- **Interoperability advantages of blockchain technology:** Provides a public multicast communication platform where a sender can reach a large audience that can both read/write to blockchain.

8. Blockchain Deployment to Realize NERC CIP Requirements

In Version 5 of the Critical Infrastructure Protection (CIP) Reliability Standards (CIP Version 5 Standards), the existing versions of CIP-002 through CIP-009 have been significantly revised, and two

new standards, CIP-010 and CIP-011, have been added. These complex standards and accompanying "Guidelines and Technical Basis" now stand at over 300 pages. This revised standard uses a new term to define the assets subject to CIP protections – "BES Cyber System". NERC defines "BES Cyber System" as "one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity". NERC defines "BES Cyber Asset" as follows: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.

In particular KISS blockchain is potentially suited to meet CIP Standards 10 and 11 which pertain to CIP-010-1 – Cyber Security – Configuration Change Management and Vulnerability Assessments and CIP-011-1 – Cyber Security – Information Protection respectively. With KISS, one may control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources with the portability of KISS signatures and integrity evidence.

Through KISS, the organizations may be able to employ protections that manage risk in their software supply chains and continuous delivery systems (Secure Development Operations) for components or subcomponent products and services. KISS affords real-time quality control and tamper detection (manipulation) of baseline changes in software such as source code, compiled binaries, and/or firmware, which can be verified in real-time for audit/investigative/configuration/ control actions.

KISS could potentially be readily integrated into common application and source software development operations and continuous delivery platforms like Puppet and OpsCode Chef[1], as well as developer management tools such as Git, Subversion, Mercurial, etc. KISS may further allow organizations to independently detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions.

By signing critical software functions, configuration files, and software with KISS, counterfeit/malicious components may be quickly compared against known good states and validated in real-time without the reliance on a trust anchor, especially in automated and abstracted management environments.

The impact of using KISS in this manner could ensure that users (power grid utilities) of this technology can strengthen their transactive system, detect vulnerabilities through rigorous test and evaluation capabilities while observing the transactions/data, including developmental, acceptance, and operational testing. By signing critical functions and using KISS related products like Overwatch, counterfeit and malicious components may be compared/contrasted against approved release states and validated independently in real-time in coordination with governance policy rules. Such ability to provide log file integrity and change detection is second to none. Below subsections are tailored to detail certain security features that are beneficial to realize secure transactive system/environment.

9. Conclusion: Blockchain Limitations and Misconceptions

It is important to understand the misconceptions and limitations (Narayanan 2015, Greenspan 2017, Coinfox 2016) that surround the blockchain technology. A major misconception of the blockchain is that "all" blockchains are trustless environments. This misconception stems from people hearing that there is no trusted third party. Although there is not a trusted third party that certifies transactions in

[1] https://www.upguard.com/articles/puppet-vs.-chef-revisited

permissionless systems, there is still a requirement of a lot of trust needed to work within a blockchain system – there is trust in the cryptographic technologies utilized, there is trust that nodes are accepting and processing transactions fairly, and there is trust in the developers of the software.

- *The challenges with trust are eliminated in permissioned blockchains such as Guardtime KSI. Therefore, PNNL KISS team decided to use Guardtime's KSI to enforce such overarching authority to eliminate sole trust-based dependency of the nodes.*

A limitation of the permissionless blockchain system where the users are pseudonymous is that although the system can enforce transaction specifications and rules, it is not able to enforce a code of conduct. These systems must provide an incentive to motivate users to act fairly, but some users may choose to act in a malicious manner if that provides them with greater incentives.

- *This limitation is addressed by permissioned PoA blockchains. Following such architecture, in KISS, all users are visible to the overarching authority and only permissioned users can participate in exchanges that are bound by set-rules. The smart contracts will be executed by completely relying on the set-rules. Any malicious user attempts will be discarded, and the malicious user will be penalized.*

Another limitation of the system stems from the fact that blockchains are not centralized. Therefore, there is not one central place for user key management. Users need to manage their own private keys, and if they lose that private key, everything associated with it is lost. There is not a "recover my account" or "forgot my password" capability on blockchains. Also, blockchain technology utilizes a public/private key structure, but since a user can have multiple private keys and a public key can create multiple addresses, identity is not always clear.

- *The keyless management is one of the major advantages with using Guardtime KSI technology. In addition to the above challenge with PKI, EDS are not designed to perform key (and certificate) exchanges. Therefore, KISS will use the KSI technology instead of PKI.*

Blockchain systems consume a lot of resources. Since every transaction is verified and the blockchain must be kept in sync amongst all users, the consumption of electricity and processing time is great.

- *This requirement is again true in PoW blockchains that rely on mining. In KISS, there is neither mining nor cryptocurrency involved. Besides, unlike any typical blockchain technology where the data and smart contracts are stored on the blockchains, KISS will only store the hash of the data. Therefore, irrespective of the size of the data, the size of hash value is always constant. This reduces the amount of information stored on the blockchain by an inestimably massive percentage (as the percentage may differ based on the blockchain KSI is compared against).*

10. References

Bahsoun J.P, Guerraoui R, and Shoker A. 2015. Making BFT Protocols Really Adaptive. 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, pp. 904-913, 2015.

Basden J, Cottrell M. 2017. How Utilities Are Using Blockchain to Modernize the Grid. HBS Review

Coinfox. 2016. Bitcoin blockchain size reaches 100 GB. Coinfox.

Deetman S. 2016. Bitcoin Could Consume as Much Electricity as Denmark by 2020. Motherboard.

Exergy. 2017. Exergy Token: The First Marketplace for the New Energy Consumer.

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

Gerber N. Accessed: 2018. "Blockchains in Energy and Utilities: Industry-specific discussion"

Gordes J. N, Mylrea M. 2014. A new security paradigm is needed to protect critical US energy infrastructure from cyberwarfare. Foreign Policy Journal

Greenspan G. 2017. The Blockchain Immutability Myth. MultiChain.

Guardtime. 2017. Keyless Signature Infrastructure (KSI) Overview

Hern A. 2017. Bitcoin mining consumes more electricity a year than Ireland. The Guardian.

Jeffries A. 2018. Blockchain' is meaningless 'You keep using that word. I do not think it means what you think it means'. The Verge.

Morris D. 2017. Siemens to Invest in Blockchain-Based Smart Grid Builder LO3.

Morris J. 2017. Blockchain in Energy: Powered by EWF

Mylrea M. 2017. Keynote Presentation: Blockchain Cybersecurity for Critical Infrastructure. Security IOT World. San Diego California.

Mylrea M. 2018. Blockchain West. Blockchain: Next Generation Supply Chain Security and Identify Management. San Francisco.

Mylrea M. 2018. Blockchain Cyber Security for Critical Infrastructure. Artificial Intelligence Conference, Stanford University.

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

Mylrea M, Gourisetti S. 2016. Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security. Resilience Week, Colorado.

Mylrea M, Gourisetti S. 2017. Keyless Signature Blockchain Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure. IEEE/PES Transmission and Distribution Conference and Exposition.

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

Narayanan A. 2015. Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day. MultiChain.

Power Compare. Accessed: 2018. Available at: https://powercompare.co.uk/bitcoin/

Power Ledger. Accessed: 2017. Power Ledger Whitepaper

Schiller B. 2017. This Blockchain-Based Energy Platform is Building a Peer-to-Peer Grid.

Schiller B. 2017. Drift is an Entirely new type of Power Utility that lets you take Control of your Electricity Bill.

Shodan LLC. Accessed: 2018. Shodan.io

Suberg W. 2018. German Researchers: Child Abuse Content Found on Bitcoin Blockchain, Users must be Protected.

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

Trottier L. 2013. Original-bitcoin. Available on Github

Walch A. 2017. The Path of the Blockchain Lexicon (and the Law) 36 Review of Banking & Financial Law 713. St. Mary's University School of Law, University College London

WePower. 2017. We Power Green Energy Network: Energy Trading Platform Powered by Blockchain Technology

Zeranski T. 2017. Energy Companies join forces with Rocky Mountain Institute and Grid Singularity to launch Global Blockchain Initiative for Energy

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov