Considering Blockchain In The Electricity Industry

By Mark Sundback, James Gatto, Kenneth Wiseman, Andrew Mina, William Rappolt and Mark Patrick

Law360, November 7, 2018, 1:51 PM EST

Blockchain technology and smart contracts have the potential to become major disrupters in the energy industry. For example, these technologies may accelerate the automation of some or all aspects of the electricity delivery transaction chain and allow for more decentralized, efficient electricity markets. Further, these technologies may allow end users (such as homeowners) to play a more active role in the electricity markets beyond simply relying on their local utility company to supply their electricity demand. Thus, blockchain technology could fundamentally change the way electricity is supplied and consumed in wholesale (i.e., the sale of electricity for resale) and retail (i.e., the sale of electricity to an end user) markets in the coming decade.

As these technologies advance and become more widespread (1) users of such technologies must be cognizant of the various regulatory requirements that could apply to them, (2) state and federal regulators need to update regulatory practices that are obsolete or impede the use of these technologies in the electricity industry and (3) traditional incumbent utilities should consider ways in which they can leverage these technologies.

The Technology

At its core, a blockchain is a distributed ledger for recording transaction data. A ledger is merely a list of transactions. Traditional paper-based ledgers include consecutive pages where each line records a transaction, and when the page is full, the process repeats on the next page. With many blockchains, each block is like a page. Transactions get verified and written into a block, and when the block is full, a new block is created. Unlike traditional ledgers, when a block is filled, the system creates a hash value, which is simply a random number generated by an algorithm based on the contents of the block. This hash value is then written as the first entry in the new block, thereby "chaining" together the blocks — hence the term "blockchain." If someone ever attempts to change an entry in a prior block, the hash value would no longer match what was written into the new block, and that attempt would be deemed invalid. In part, this is how an immutable record may be created using a blockchain.

There are three main types of blockchain platforms: public, private and consortium. Organizations may select among these platforms based on their specific needs. Public blockchains are a decentralized framework that allows anyone to add themselves to the network, read transactions, transfer assets and participate in the consensus process, typically without any special permission. Private blockchains are centralized frameworks that are permissioned, allowing only a preapproved set of members to read and send transactions, and participate in the consensus process. Consortium blockchains are a

hybrid of the public and private blockchain platforms. They leverage the decentralized nature of public blockchains and the permissioned capability of private blockchains. As with any consortium, the entire network, along with its validation rules and policies, can be defined and governed by members/nodes. They can control every aspect of the blockchain, including validation of transactions, addition of nodes, managing node privileges, smart contracts or deployment of chain codes.

An important feature of blockchain technology is smart contracts. Smart contracts (which are not necessarily legally binding contracts) are essentially self-executing code that implements the operational terms of an agreement between two or more parties. The code can exist across a distributed, decentralized, blockchain network. Using a scripting language or other techniques, a smart contract can include logic-based programs that run on top of a blockchain. A smart contract can receive data from various sources and programmatically implement a series of if-then rules that are performed at least in part by computers with little or no human interaction. Smart contracts may also provide for a built-in payment system (e.g., unique tokens or cryptocurrency). As applied to the electricity industry, smart contracts can form the foundation of electricity transactions by allowing for an automated system of selling and purchasing electricity between parties, provided certain conditions are met. For example, a smart contract can specify that an electricity transaction be executed only at a certain price or if certain other conditions are met. Further, smart contracts can provide for resource specific (e.g., only renewables) electricity transactions.

Blockchain and smart contracts offer several benefits in electricity markets, including: (1) automated and transparent processing of transactions; (2) easy specification and verification of electricity products bought and sold; and (3) a more decentralized approach to the sale and consumption of electricity. However, individuals and/or nonutility entities employing blockchain to execute electricity transactions must consider that the use of these technologies could expose them to state and federal regulatory oversight and ongoing regulatory requirements.

Regulatory Landscape

One of the most important areas to be explored as blockchain technologies become more widely adopted in the energy industry is how regulators will view and treat them. At present, most regulatory regimes have offered little, if any, guidance on the intersection between blockchain/smart contract technology and the electricity industry. Thus, there is significant regulatory uncertainty surrounding the use and application of blockchain technology to process energy transactions, which must be resolved as the use of blockchain becomes increasingly adopted in the electricity industry.

Electricity energy markets are overseen by a number of regulatory regimes, primarily state public utility commissions and the Federal Energy Regulatory Commission. State PUCs typically regulate, among other things, the siting of generation resources and retail sales of electricity in their respective states. FERC regulates wholesale sales of electricity in interstate commerce and the transmission of electricity. Additionally, FERC

oversees: (1) regional transmission organizations, or RTOs, and independent system operators, or ISOs, that operate organized wholesale electricity and electricity products markets and manage the interstate transmission grid in various regions of the U.S.; (2) utility accounting practices and conventions; (3) electric utility wholesale tariffs, including provisions governing the process by which billing disputes are resolved; (4) wholesale electric service agreements; (5) interconnection to the transmission grid; and (6) the treatment of utility FERC-jurisdictional costs (e.g., the expensing or capitalization of costs in a utility's cost of service used to set wholesale rates).

In addition to these two primary regulatory regimes, the North American Electric Reliability Corporation, the U.S. Department of Energy and the U.S. Commodity Futures Trading Commission, among others, also have oversight authority. NERC oversees the reliability of the North American electric grid in conjunction with FERC. DOE oversees various U.S. energy policies, including nuclear energy programs. CFTC regulates energy market transactions involving swaps, futures and market manipulation in futures markets.

Users of blockchain and smart contracts must understand the (sometimes overlapping) role each of these regimes plays and recognize that the use of these technologies may implicate a host of regulatory issues.

State Oversight: Retail Sales and Rates

At the state level, PUCs regulate retail sales of electricity, typically the siting of electricity generation sources and the operation of the distribution system. State PUCs may choose to regulate smart contracts and associated electricity sales to end users or aggregating entities under their authority to regulate the retail distribution and sale of electric energy. If a state PUC opts to assert such regulatory authority, individuals or entities may need approval from their respective PUCs prior to engaging in blockchain- or smart contract-facilitated electricity sales. In unbundled states (i.e., where each of generation, distribution and transmission is sold as a separate service), this may require obtaining a license to make retail sales. In bundled states, it could mean having a PUC-approved retail tariff. In addition to potentially needing prior regulatory approval simply to make sales of electricity, sellers of electricity may trigger stranded cost claims brought by local utility companies. Where the facilities of traditional public utilities — or load serving entities, or LSEs — become redundant due to the entry of new market competitors (in this case, users of smart contracts and blockchain), LSEs may bring claims seeking to assign the portion of the costs of those facilities that cannot be recouped because of the entry of the new market participant (i.e., the stranded costs) to either the new entrant or to the market generally.

Thus, any person or aggregator seeking to employ blockchain technology to make retail sales of electricity will need to have an understanding of the regulatory landscape in the state in which it intends to operate, and ideally each state PUC will provide guidance concerning the extent to, and manner in, which it intends to assert jurisdiction. Without understanding the scope of the regulatory jurisdiction over these technologies, users

could be potentially exposed to penalties imposed by a PUC, or run the risk that their upfront capital costs to employ blockchain technology would be unrecoverable if the PUC disallows such transactions. Further, without establishing guidance, blockchain users and traditional utilities will be left to operate in uncertain regulatory and commercial environments, which may discourage blockchain users from entering the market and impede LSEs' ability to efficiently operate and manage their utility systems.

Federal Oversight: Sales, Rates, Interconnection and Settlements

Wholesale sales in interstate commerce are subject to FERC jurisdiction. Thus, wholesale sales by any end user or entity using blockchain technology could invoke FERC oversight. Sellers could be required to obtain authority to make electricity sales at market- or cost-based rates, and to file associated tariffs with FERC. Where sellers make wholesale sales without FERC authorization, they could be subject to financial penalties. Further, the interconnection of smaller decentralized facilities to the transmission grid could be subject to FERC oversight. The process by which generators interconnect to the transmission grid can often be burdensome for the entity seeking interconnection; however, this process can be particularly onerous for smaller, less sophisticated sellers, who are likely to be first adopters of blockchain technology. Further, FERC jurisdiction could be invoked even where a blockchain user did not intend to supply electricity to the transmission grid.

Other issues may arise, as well, including those regarding rates, billing disputes, the potential for real time market manipulation, or manipulation in futures markets (which could invoke CFTC regulation). Further, FERC must consider whether existing transmission infrastructure is capable of handling increased transaction activity due to an increase in the number of blockchain/smart contract users potentially putting electricity onto the transmission grid.

Additionally, FERC could regulate blockchain usage on a broader scale in the ISO/RTO electricity and transmission markets. FERC regulates ISOs and RTOs, which operate markets for services that may include, for instance, different types of electricity products, such as day-ahead energy, real-time energy, ancillary services and financial transmission rights. ISOs and RTOs could use blockchain technology to provide a transparent and efficient means of settling and reporting wholesale electric transactions, as settlements are typically made by the RTO/ISO. For example, some RTO/ISOs make daily settlements seven calendar days after each operating day using operational and market participant submitted data. Market participants typically use a shadow settlement system to evaluate and confirm their transactions with the settlement information provided by ISOs/RTOs. Both processes are time and resource intensive. Blockchain could help streamline these processes, including by allowing ISOs/RTOs and market participants to avoid administrative and working capital costs associated with the settlement process. In addition, data would be available in a more timely fashion and could be more easily utilized by FERC, market monitors and market participants. However, deployment of blockchain by ISOs and RTOs will invariably invoke scrutiny by FERC and potentially NERC.

Reliability Considerations

The use of blockchain technology has the potential to compromise the reliability of distribution and transmission systems. As blockchain technology facilitates an increasing number of electricity transactions occurring on distribution and transmission systems, there is a risk that, without regulatory oversight, regulators, LSEs and ISOs/RTOs may lack a complete understanding of (1) what is occurring on those systems at any given time and (2) whether those systems can handle increased traffic during times of peak demand. This could result in distribution and transmission facilities becoming overloaded with power, potentially causing outages, blackouts and other reliability issues. Thus, to maintain safe and reliable operations, it is imperative that owners and operators of distribution and transmission facilities, as well as regulators, be able to adequately monitor blockchain transactions.

Security Considerations

There have been several high-profile cybersecurity attacks on local utility companies in recent months. Systems using blockchain technology and smart contracts may be equally susceptible to such cyberattacks, which can pose security risks to distribution and transmission systems. Thus, data protection and grid security are serious concerns and must be adequately considered.

While blockchain technology may have its own built-in security protocols, systems using such technologies are not immune from attack. As blockchain technology facilitates a more decentralized approach to the sale and purchase of electricity, blockchain users, who may be less sophisticated than utility companies and thus may not have the necessary security measures in place, are particularly at risk of cybersecurity hacks. Regulators should consider and implement policies and other measures aimed at protecting the grid and individual users from cybersecurity attacks, including establishing a minimum security “floor” to which all users would be subject.

What All of This Means for Non-Utility End Users

While blockchain/smart contract technologies may result in an exciting new advancement in the way electricity is purchased and sold, potentially exposing blockchain and smart contract users to regulatory oversight at the state and federal levels may have a chilling effect. The use of such technologies could implicate oversight by both state and federal regulators. This may create a complex web of regulatory and bureaucratic burdens that ultimately may inhibit or preclude the deployment and adoption of blockchain on a broader scale. For example, homeowners may forego using blockchain to engage in electricity transactions if they are required to become authorized electricity providers or potentially become subject to other various state and federal rules. Further, blockchain and smart contract users could be subject to additional fees for using a distribution or transmission system to make electricity sales or purchases. However, it is unclear what ratemaking mechanisms electric market

regulators will establish. This lack of clarity and regulatory guidance could result in end users and non-utility entities choosing to continue to rely on their local utility companies for their electricity needs rather than engaging in decentralized blockchain electricity transactions.

What All of This Means for Utilities

Utilities should consider that decentralized microgrids using blockchain technology could pose a threat to their traditional business model, including that such technologies could lead to the replacement of some or all of their generation, transmission and/or distribution facilities. As blockchain technologies advance and make it easier for individuals to engage in decentralized electricity transactions, merchant generators, LSEs and other utilities could become obsolete or lose significant market shares. For example, a neighborhood microgrid could come to rely on traditional generation less and less as blockchain technology advances, especially given the increasing proliferation of electric storage facilities and rooftop solar, which can be installed to serve a microgrid system. Utilities must carefully and comprehensively assess their ability to continue to play a competitive role in electricity markets in light of these emerging technological advancements. Just as we have seen in other industries (e.g., the creation and proliferation of ride hailing companies, and the negative impact they have had on taxicab companies), traditional utilities face the risk of losing significant market shares to technologies that are more decentralized with lower fixed costs if they fail to find ways of adopting and implementing such technologies to provide competitive electricity products in a new paradigm. On the other hand, utilities could integrate blockchain technology and smart contracts into their systems in order to enhance operational efficiency, customer satisfaction and competitive rates by, for example, further automating electricity transactions using utilities' existing infrastructure, increasing data transparency and providing consumers with an increased role in the management of their power needs.