Crypto-control: Why Transactive Control Needs Blockchain

Ashley Pilipiszyn[1] and David P. Chassin[2]
DRAFT for 28 September 2017

Abstract

This white paper discusses the current status of transactive control technology and how blockchain technology can address some of the concerns about transactive energy more broadly. A summary of the requirements for so-called crypto-control systems is presented, and recommendations for research and development topics are discussed.

Introduction

Electricity generation, transmission and distribution infrastructure plays a key role in the vitality, productivity and efficiency of our global society. The importance of engineering a robust, integrated, and surplus maximizing electric system operation cannot be understated. Wholesale energy markets were promulgated more the thirty years ago to transform this critical infrastructure and make it more economically efficient and open to innovation. But in many ways, this transformation has failed to reach the retail level, both in distribution systems and within customer premises.

Transactive control was proposed as a mechanism to facilitate the extension of market-based paradigms to every part of our energy and power delivery infrastructure. Even before renewable intermittency, microgrids, electric vehicles, or electricity storage were envisioned as widespread threats and/or opportunities in the power grid, demand response was already considered the poster-child of a resource that, if broadly in play, could improve system reliability, reduce operating costs, and allow consumers to share in the economic surpluses arising from their demand volatility and their willingness to forgo or defer consumptions under certain conditions.

Meanwhile blockchain technology was developed independently to address the drawbacks of traditional financial arrangements when conducted online. Aside from direct barter, only two systems ever emerged to solve the trade coordination problems among a group of people: credit, which requires trust, and cash, which requires an initial allocation of currency to seed the system. The two systems are not equal: credit requires a third party who can guarantee that the funds used in one transaction don't get used in a second transaction before the first transaction is settled; cash offers privacy and anonymity, meaning nobody really knows who has how much cash and there's no need to involve a third party to complete the transaction. Bitcoin was among

[1] Ashley Pilipiszyn is a PhD student at the Université de Genève, in Geneva, Switzerland.
[2] David Chassin is a staff scientist at SLAC National Accelerator Laboratory in Menlo Park, California, which is operated for the US Department of Energy by Stanford University under Contract DE-AC06-76SF00515.

the most successful attempts to solve the problem of completing digital transactions without either cash or credit by using what is now known as "crypto-currency" technology built on a blockchain paradigm [1].

Bitcoin, the world's "first decentralized digital currency", was launched in 2009 and unlike traditional currencies, has no central monetary authority. Bitcoins operate on a peer-to-peer computer network comprised of its users' machines to generate them by solving difficult cryptographic problems, a process known as Bitcoin "mining". The entire network is used to monitor and verify both the creation of new Bitcoins through mining, and the transfer of Bitcoins between users. A log is collectively maintained of all transactions, with every new transaction broadcast across the Bitcoin network. All transactions are secured using public-key encryption, a technique that works by generating two mathematically related keys in such a way that the encrypting key cannot be used to decrypt a message and vice versa. This combination of components helps provide the transaction transparency and security needed for building and maintaining trust between transacting parties. As both energy companies and utilities find themselves in the midst of an energy transition characterized by distributed energy resources being traded in real-time among all actors for accurate load balancing, the application of crypto-currencies presents a unique opportunity for the future of transactive energy.

According to David Hardin, Chief Architect at the Smart Electric Power Alliance (SEPA), "Blockchains and executable contracts represent technology tools that could help enable transactive energy by supporting flexible and secure machine to machine transactions that are well-conceived, well-designed and well-integrated into grid operations and markets," [11]. For the power industry, possible blockchain solutions currently being explored include data logging, asset valuation, renewable energy certificates, bill payments via crypto-currency and conditional energy supply smart contracts. For example, Austria-based Grid Singularity has created a platform that allows for monitoring and sharing of power/energy data globally as well as storing immutable performance data for an asset on the blockchain [12]. In another example, SolarCoin (SLR) serves as a digital asset that rewards solar energy generation where PV-facility owners receive SolarCoins by generating solar electricity at the rate of 1SLR/MWh [13]. If these solutions prove secure and scalable, crypto-currencies and the underlying blockchain technology will have the capacity to maximize the potential of distributed generation and more efficiently manage less predictable and more volatile renewable power sources.

Transactive Control

The history of transactive control begins with Fred Schweppe's "homeostatic" system, in which autonomous loads could respond to either frequency or price signals [2]. According to this paradigm, distributed resources could provide useful responses to a power grid, either through frequency-based control analogous to ancillary services, or price-based control analogous to modern-day energy market participation. These capabilities complemented ideas proposed around the same time by Reid Smith, which he called "contract nets", in which scarce CPU resources were scheduled using an auction mechanism [3]. In 1995, Huberman and Clearwater successfully joined the two concepts in a commercial building control system that showed how such a system worked to satisfy local energy demands and operated economically efficiently [4].

A utility-scale implementation of a transactive system was first reported independently by both Kok's PowerMatcher system [5] and Hammerstrom's Olympic system [6], and subsequently scaled up in Widergren's Columbus system [7] and Melton's Pacific system [8]. Eventually Fuller provided a simple and clear definition of "transactive control" in [9]:

> *Utilizing a central control and distributed agent methodology [...] to act on behalf of consumers, sending information and automatically adjusting settings in response to a centralized signal.*

Since then transactive control has been taken up by many researchers and advocated by still more under the more general rubric of "transactive energy". But fundamentally the concept is the same as defined by Fuller.

Transactive control systems are generally characterized by the following essential elements:

(1) A market mechanism that simultaneously satisfies the physical and economic constraints of an engineering system, and
(2) Automation that allows consumers to delegate their price responsiveness to devices that act on their behalf in market-like mechanisms.

These are achieved by substituting price signals for the diverse control signals used in traditional system. Typically the clearing price is associated with the supply and demand power that corresponds to a dynamic econo-physical equilibrium. Although in the case of interconnections with multiple control areas, prices can also be associated with intertie flows, as reported by Behboodi [10]. Unlike Fuller's definition there is no absolute requirement for a central market or control system. It seems likely that if the developers of the original transactive control concept had thought it was possible, they most likely would have proposed and tested a completely distributed market design. In any case, regardless of the actual implementation, transactive control systems have the notable feature that they maximize global surplus and social welfare.

There are a number of important considerations that the extant implementations of transactive did not address fully or satisfactorily. Notable among these are

(1) **Cyber security**: As with many grid technologies, the security of the command and control infrastructure is often an afterthought, if thought of at all. This was certainly the case for early transactive control systems. For example, the Olympic and Columbus systems relied on secure sockets, encryption and certificates to secure communications.
(2) **Privacy**: In general, transactive systems protect the privacy of participants insofar as the bids and short term meter data are not shared with anyone but the utility. However, some will argue that even this data sharing presents potential legal and privacy problems because the utility may be compelled to disclose this information to authorities, tempted to sell the data for commercial gain, or may simply fail to adequately protect the data from hacking or accidental dissemination due to technical error, incompetence or

indifference. These concerns may reduce the willingness of consumers to enlist their resources and may increase the burden on utilities arising from regulatory oversight and consumer advocacy.

(3) **Single-point vulnerabilities**: The previous transactive control demonstrations relied on centralized clearing mechanisms. The central market is a single-point vulnerability subject to attack by hostile agents. As an element of critical infrastructure, this presents significant challenges for utilities because unlike much of their existing control infrastructure, transactive control infrastructure is inherently designed to operate in an environment where trust is largely absent.

(4) **Common-mode failures**: The previous transactive control demonstrations relied on large numbers of identical distributed agents implemented with identical algorithms and identical communications protocols. Homogeneous agents present a significant common-mode failure that was never adequately addressed except through heterogeneous implementations and diversity of coding methods. Without a concerted effort to secure against common-mode failures, the vulnerability to a significant fractions of the total resources that employ at least some common code elements remains very high.

(5) **Settlement and billing**: In previous implementations of transactive control systems, metering and billing were accomplished using the conventional utility infrastructure, despite the fact that these appeared quite ill-suited to the requirements for fast sampling, short delay, time-series measurements of both price and power at the device level.

Blockchain Technology

Blockchain is the technology at the heart of Bitcoin and other virtual currencies which serve as open, distributed ledgers that efficiently record transactions between parties in a verifiable and permanent way. Blockchain technology came into the fore with Bitcoin in 2009 when programmer Satoshi Nakomoto published a white paper, “Bitcoin: A Peer to Peer Electronic Cash System” [15]. In this paper, Nakomoto posits that the issue of double-spending for digital currency can be solved by utilizing a distributed database that enables one entity to confidently transact value directly with another entity without relying on a third-party to facilitate the transaction [17]. In less than a decade, this technology has evolved from underpinning Bitcoin transactions to being applied/explored in nearly every industry due to the following innovations:

(1) **Operate autonomously from crypto-currencies**: the realization that the underlying technology that operated Bitcoin could be separated from the currency and utilized for a variety of other use-cases such as medical records, academic credentials and voting.

(2) **Generate “smart contracts”**: Originally proposed by Nick Szabo in 1996, these computer protocols facilitate, verify, or enforce the negotiation of a contract [18]. Utilization of these smart contracts in blockchains began with the creation of second-generation blockchain technologies such as Ethereum, Namecoin and Ripple.

Micro-computer programs could be built directly into the blockchain that allowed more complex financial instruments to be represented, rather than only the cash-like tokens of Bitcoin. The ledger itself can also be programmed to trigger contingent transactions automatically.

(3) **Secure “proof of work”**: In order to prevent double-spending of one’s holdings on the Bitcoin blockchain, users detect tampering through hashes, long strings of numbers that serve both as proof of work, among other things. Generating just any hash for a set of transactions is trivial for a modern computer, so in order to turn the process into “work,” the Bitcoin network sets a certain level of “difficulty” and changes the cost (i.e., energy use) of finding a valid new block. The difficulty of the problem is adjusted so that a new block is “mined” - added to the blockchain by generating a valid hash - approximately every 10 minutes. Proof of work makes it extremely difficult to alter any aspect of the blockchain, since such an alteration would require re-mining all subsequent blocks.

(4) **Secure “proof of stake”**: While the purpose is the same as proof of work, the process of this algorithm is differentiated whereby the creator of the new block is chosen in a deterministic way, depending on its wealth, also defined as stake. As there is no block award like proof of work, the miners incur the transaction fees. The rationale behind moving away from proof of work and towards a proof of stake system is that proof of stake offers a less energy intensive and cheaper distributed form of consensus.

(5) **Enable blockchain scaling**: Currently every computer on the blockchain network processes every transaction, which is very inefficient. A scaled blockchain accelerates this process, without sacrificing security, by determining how many computers are necessary to properly validate each transaction and dividing up the work efficiently [20].

(6) **Multiple blockchains**: To date, there are three main categories of blockchains: public, private and federated. Public blockchains are based on proof of work or proof of stake consensus algorithms that are open source and without a central authority (i.e., permissionless). Examples of public blockchains include Bitcoin, Ethereum, Litecoin and Dodgecoin. Private blockchains are a way of exploiting blockchain technology by setting up groups and participants who can verify transactions internally. With private blockchains, write permissions are kept centralized to one organization and read permissions may be public or restricted to an arbitrary extent. Examples include IBM and Multichain. Finally, federated blockchains operate under the leadership of a group, are faster (higher scalability), and provide more transaction privacy. Unlike public blockchains, federated blockchains do not allow any person with access to the Internet to participate in the process of verifying transactions. Examples of federated blockchains are Energy Web Foundation, R3, and Corda [19].

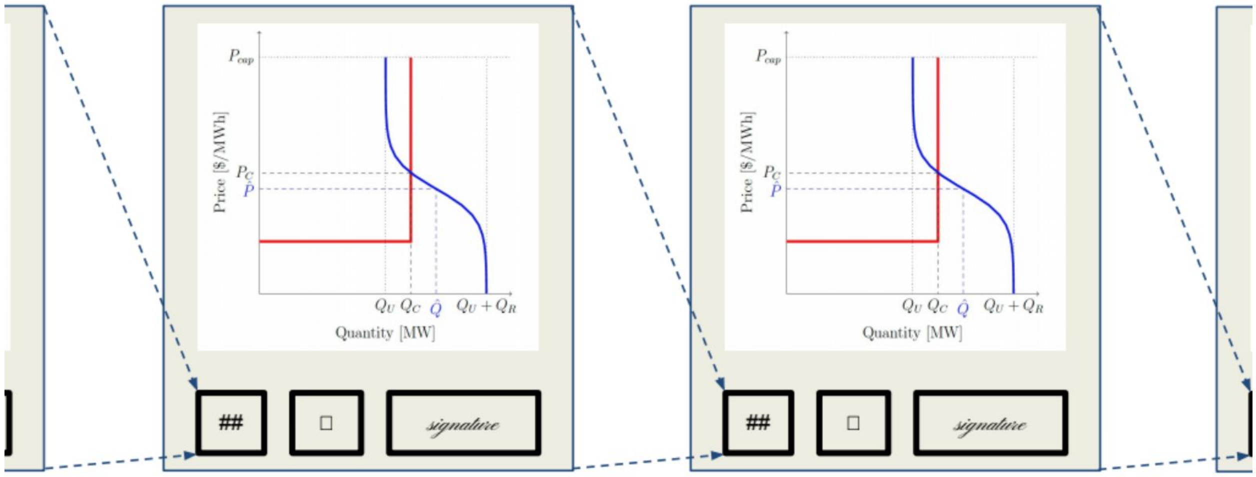

Figure 1: A transactive control blockchain with a link, timestamp, and signature.

Power Systems and Proof-of-Control

A relatively broad set of requirements for crypto-control of power systems should include at the very least the following capabilities.

(1) **Data acquisition, metrology and fast event detection**: Measurement is at the heart of all control systems, and trusted measurement in an untrusted environment is a critical barrier to successfully deploying distributed control systems. Blockchain technology offers the promise of trusted distributed data acquisition and event logging in an untrusted network environment. Furthermore, not all data is of equal value to participants. Therefore consumers of data should be able to place a "value" on the data they require so that good data is rewarded and bad data is penalized. These data transactions can and should be a matter of record in the transaction ledger.

(2) **Data transformation, filtering, and general calculations**: After data is acquired, it often must be transformed into useful information in a trusted manner. As with data acquisition, these valuable transformations should be a matter of record, the algorithms verifiable, rewarded and the outputs reproducible from the inputs by any component in the system.

(3) **Analytics and optimization**: The data and information that emerges from Capabilities (1) and (2) can be assembled and analyzed by more sophisticated tools to identify optimal configurations for system components. These analyses are just as important to record, reward, verify and reproduce as the more simple filtering processes in Capability (2).

(4) **Forecasting, bidding, and out-of-market trading**: As with Capability (3), forecasting, bidding and out-of-market trading are essential to overall functionality. In the case of forecasting, external data is used to drive a model that produces additional "virtual" data introduced into the control system. This data is analogous to Capability (1), except that the external data sources and models must be a matter of record, along with the data injected into the system. In the case of bidding, although the bidding strategies are private, the bids themselves are a matter of record. This is also true for out-of-market trades.

(5) **Schedule, dispatch, and regulation**: Core system functions such as scheduling, dispatch and regulation are typically the result of the implicit (or emergent) behavior of the transactive system itself and not performed explicitly by any centralized system. However, when performed centrally, these results are a matter of record as well.

(6) **Settlement and payments**: The system includes all reconciliation, settlement, and payment mechanisms necessary using heterogeneous multi-chain technology such as the Polkadot protocol [16].

(7) **Monitoring, oversight, and penalties**: Essential regulatory participant monitoring, system oversight, and penalty mechanisms are included in the record so that these operations are transparent, verifiable and reproducible. The procedures for detecting illegal activity and errors, adjudicated claims, and implementing mitigations must be designed into the blockchain mechanisms.

In all cases where software codes are being used to produce results, these codes sign their output in accordance with the usual protocols for public key cryptography. This assures consumers of the outputs that the results are authentic and eliminates the possibility of spoofed calculations adversely affecting system performance.

Scarcity is at the heart of all crypto-currency technologies. In the case of Bitcoin, mining operations establish a "proof-of-work" in the form of a "hash code" that is difficult to find but easy to verify. The search for these rare codes is costly because it requires specialized hardware, software, and most importantly energy to complete. Bitcoin uses the scarcity of these codes to limit the rate at which of valid blocks can be added to the blockchain. This both raises a financial barrier to fraud and rewards miners financially for finding the codes needed to create new blocks[1].

Scarcity is also inherent in an energy system, insofar as controllable resources are expensive to procure, maintain and operate and only useful for a limited time. It is likely that a scheme based

[1] Alternatives to proof-of-work have been proposed, such as proof-of-stake and proof-of-authority, but the details of these are not important in the context of this discussion--they all provide a similar inherent limit on who can create block or how many blocks can be created.

on *proof of control* may be an alternative to proof of work. But how proof of control is implemented is an open research problem. Notionally the approach may be understood as follows:

(1) Agent 1 send a proof-of-control challenge to Agent 2 to verify that Agent 2 can in fact control its load as claimed.
(2) Agent 2 sends a reply to Agent 1 with a random pattern, which it uses to alter its load momentarily.
(3) Agent 1 receives the reply and detects the magnitude of the load changes, and deduces the electrical "separation" between the load and the detector.

What has yet to be determined is precisely how controllability is monetized to support scarcity in the block creation process.

Distributed Market-Making

In power systems, markets are structured around system operators who have technical and financial jurisdiction over the pricing mechanism. The most important concept in energy markets is the *uniform price*, meaning that in general all consumers pay the same price for energy, and all producers are paid the same price. The only conditions under which a price difference between consumers and producers emerges are

(1) There is a tax or fee on consumption.
(2) There is a subsidy for production.
(3) There is an inefficiency in the market.
(4) There is a delivery constraint between producers and consumers.

Conditions (1) and (2) are matters of public policy, and (3) is matter of market design. However, condition (4) is arises from the physical limitations of the underlying network system: Consider a scenario where two control areas, Allston and Buckley are connected by a power line with limited capacity. If the total demand in Allston exceeds local supply plus the imports over the power line from Buckley, then the surplus maximizing outcome is a price that is higher in Allston than in Buckley. The magnitude of the price difference will depend on the mix of resources available and magnitude of the constraint. In wholesale energy markets these prices are called a *locational marginal price* or LMP. The separation of the single uniform price into two LMPs is obtained automatically by the market system.

In a distributed system, the existence and location of binding constraints that affect prices is not usually known a priori. Since each blockchain represents a single price/quantity pair discovered by the markets, any crypto-control implementation must be able to divide and merge blockchains to track the appearance and disappearance of constraints in the system. Blockchain division is accomplished by having multiple blocks refer back to the common antecedent block. Blockchain merging is accomplished by allowing all but one of merging blockchains to collapse to zero quantity. The mechanisms for managing constraints by dividing and merging market chains is the subject of the current research into distributed market-making using blockchains.

Utility Business Case

While at first glance, blockchain may seem to be a technological disruption that the power industry should avoid, it actually has the potential to be exactly what is required to keep up with evolving demand for electricity resource control in more minute quantities at higher frequencies. Currently, established utilities are best positioned to evaluate and test possible blockchain solutions and determine a strategic path forward for a decentralized energy future. One of the challenges in achieving this is having the appropriate tools for these utilities to “sandbox” possible scenarios, especially ones utilizing blockchain. To date, there are only a handful of resources available to model distributed energy systems, microgrids, etc. and even less available to model blockchain applications in the energy industry.

The business motive for utilities to support this technology is the recognition that managing network constraints generates revenue but only within a narrow optimal band of network capacity. On the one hand if network constraints are eliminated by “gold plating” the system, utility revenue declines because revenue-generating price differences disappear. On the other hand, if constraints are overly binding, revenues decline because power flows disappear. The business objective for the utility is to maximize revenue from use of the network, and this objective should correspond to the surplus maximizing capacity of the utilities infrastructure, assuming both supply and demand are sufficiently well engaged in the transactive energy trading mechanism.

From an engineering design and deployment perspective, transactive control systems challenge conventional power system simulation tools. This motivated the US Department of Energy to develop GridLAB-D, an agent-based simulation tool specifically designed to model and simulation smart grid technologies like transactive control. GridLAB-D has been available for more than 10 years, has been downloaded by tens of thousands of users, and is cited in more than 2,800 publications [14]. GridLAB-D enables researchers and utility engineers to study and deploy many important smart grid technologies, including transactive control systems.

Mainstream simulations of power systems do not yet implement models of blockchain technology. For agent-based simulations like GridLAB-D, this is be relatively simple to add, and provides the basis for modeling how crypto-control systems would behave, what kind of information could readily be discerned from the ledgers after prolonged operation, and provides the data needed to evaluate the business case for both microgrid operators and utilities who host microgrid systems. Development efforts are SLAC are currently underway to augment GridLAB-D to support microgrids and distributed ledgers. These capabilities will be further developed and integrated to enable the analysis required to estimate the value proposition for microgrids.

Path Forward

For key stakeholders in the energy industry to effectively transition to a decentralized energy system and determine the value-added from implementing crypto-control systems, it is critical to investigate the challenges and opportunities from a systems-level perspective.

The following research outline is proposed:

(1) Develop business/benefit cases for system operators, utilities, microgrids, and individual consumers.
(2) Develop simulation models to estimate cost and benefit of adopting crypto-control compared to traditional transactive control, blockchain only and business as usual.
(3) Design field demonstrations of a test case, e.g., utility and microgrid operation.
(4) Run field demonstration and compare performance with simulation models.
(5) Adjust and improve simulation models where deficiencies and errors are identified.
(6) Analyze, synthesize, and report results and release simulation tools to support widespread study and adoption of crypto-control concepts.

Conclusions

According to many experts in this space, the future of the energy industry will be characterized by four distinct stages: decentralization, decarbonization, digitalization and disruption. The use of crypto-control through the application of blockchain technology with transactive energy may facilitate the transition through these phases for key stakeholders. Thus utility companies, for example, may be able to provide tangible solutions that address long-term system security, revenue adequacy and energy efficiency concerns. One possible scenario in this context is where the utility would serve as a distributed service platform that would be compensated for coordinating a decentralized system built on efficient interactions between all participants in an untrusted environment. By utilizing the proof of control mechanism within this crypto-control framework, trust can be established between transacting entities. As a result, every electric vehicle, battery, solar panel, building controls system, or other connected smart asset on the grid could respond in real time to market conditions and real time prices.

In order for utility companies to fully exploit the opportunities made available from the use of blockchain in transactive energy, more robust modelling and simulation tools are required that can model the behavior of blockchain in various scenarios. Building upon the success of GridLAB-D in modelling transactive control, new features of this software are being explored to integrate the modelling of crypto-control on microgrids and distributed ledgers to better understand where value can be created for system participants. In conclusion, blockchain could facilitate the rapidly expanding ability of distributed assets on the power grid, to transact with the grid automatically, based on a network of hundreds or thousands of real-time geographically distributed prices. Furthermore, proof of control could facilitate and track automated power market transactions that need to occur without human intervention, thus support the emergence of a secure, distributed, autonomous system that can manage the demands of a 21st century grid.

References

[1] A. Narayanan, J. Bonneau, and E. Felten. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[2] F. C. Schweppe, R. D. Tabors, J. L. Kirtley, H. R. Outhred, F. H. Pickel, and A. J. Cox, “Homeostatic utility control,” IEEE Transactions on Power Apparatus and Systems, vol. PAS-99, pp. 1151-1163, May 1980.

[3] R. G. Smith, “The contract net protocol: High-level communication and control in a distributed problem solver,” IEEE Transactions on Computers, vol. 12, pp. 1104-1113, 1980.

[4] B. A. Huberman and S. H. Clearwater, “A multi-agent system for controlling building environments,” in ICMAS, pp. 171-176, 1995.

[5] J. K. Kok, C. J. Warmer, and I. Kamphuis, \PowerMatcher: multiagent control in the electricity infrastructure," in Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems, pp. 75{82, ACM, 2005.

[6] D. J. Hammerstrom, R. Ambrosio, T. A. Carlon, J. G. Desteese, R. Kajfasz, R. G. Pratt, and D. P. Chassin, “Pacific Northwest GridWise™ Testbed Demonstration Projects Part I: Olympic Peninsula Project," PNNL Report No. 17167, Pacific Northwest National Laboratory, October 2007.

[7] S. E. Widergren, M. C. Marinovici, J. C. Fuller, K. Subbarao, D. P. Chassin, and A. Somani, “Customer engagement in AEP gridSMART residential transactive system,” tech. rep., Pacific Northwest National Laboratory (PNNL), Richland, WA (US), 2014.

[8] R. B. Melton and D. J. Hammerstrom. "Transactive control: A technique for widespread coordination of responsive Smart Grid assets." *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*. IEEE, 2012.

[9] J. C. Fuller, K. E. Schneider, and D. P. Chassin, “Analysis of residential demand response and double-auction markets,” in 2011 IEEE Power and Energy Society General Meeting, IEEE, 2011.

[10] S. Behboodi, D. P. Chassin, N. Djilali, and C. Crawford, “Interconnection-wide hour-ahead schedule in the presence of intermittent renewables and demand response: A surplus maximizing approach," Applied Energy 189, 336-351, 2017.

[11] L. Barney, “What is blockchain’s role in transactive energy systems?,” Smart Grid Northwest. URL: http://smartgridnw.org/resources/blockchains-role-transactive-energy-systems/

[12] S. Ravens and R. Shandross, “Understanding peer-to-peer, blockchain, and transactive energy,” Navigant Research. URL: https://www.navigantresearch.com/blog/understanding-peer-to-peer-blockchain-and-transactive-energy

[13] SolarCoin (SLR) URL: https://solarcoin.org/

[14] Google Scholar: https://scholar.google.com/scholar?q=gridlab+d

[15] S. Nakomoto, “Bitcoin: A peer to peer electronic cash system.” 2008. URL: www.bitcoin.org

[16] Polkadot Protocol URL: https://polkadot.io/

[17] “Virtual currency: bits and bob,” The Economist. 2011. URL: https://www.economist.com/blogs/babbage/2011/06/virtual-currency

[18] N. Szabo, “Smart contracts: building blocks for digital markets,” URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[19] “Blockchains and distributed ledger technologies,” Blockchain Hub. URL: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

[20] V. Gupta, “A brief history of blockchain,” Harvard Business Review, 2017.