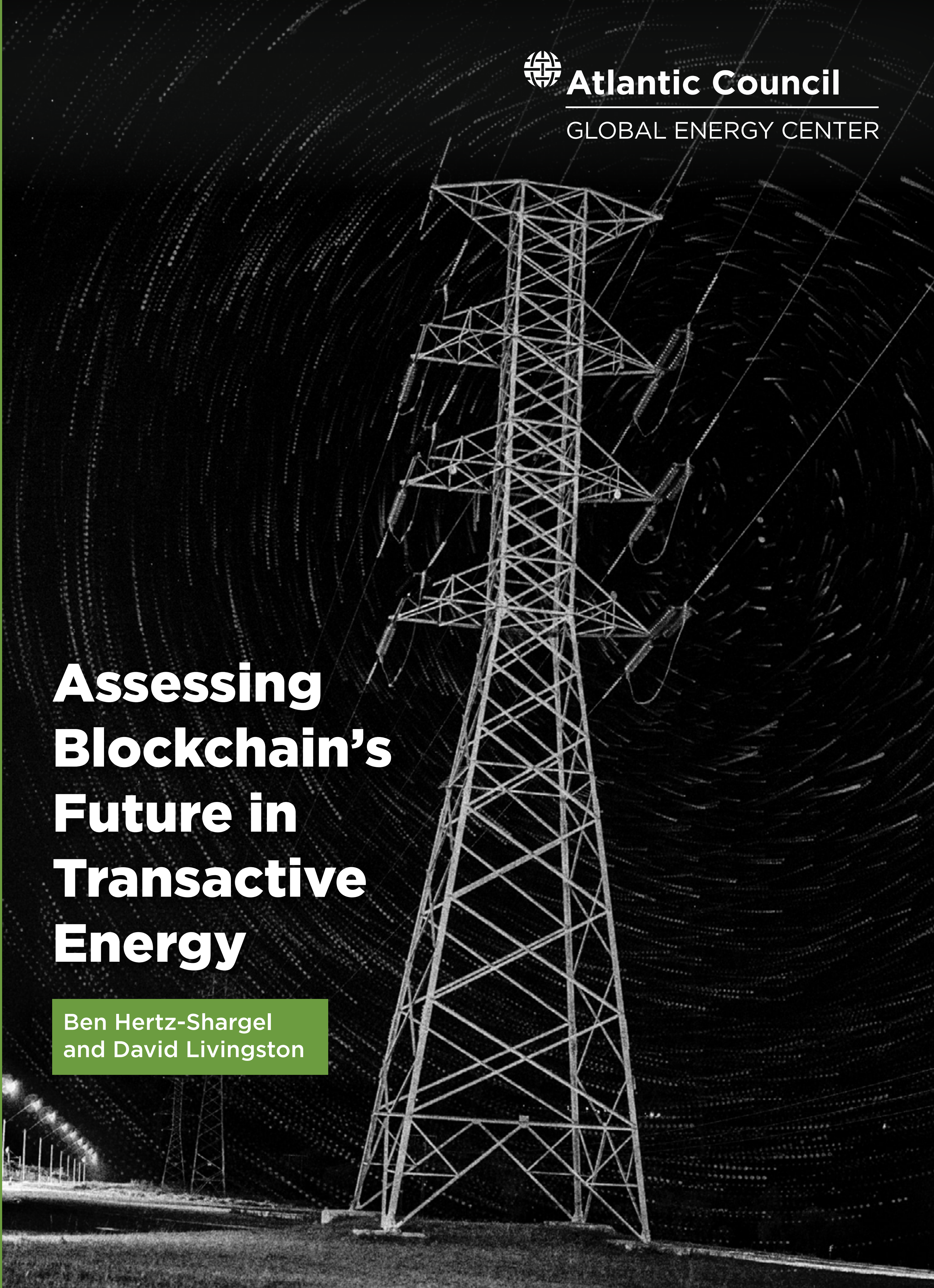
Atlantic Council
GLOBAL ENERGY CENTER



Assessing Blockchain's Future in Transactive Energy

Ben Hertz-Shargel
and David Livingston

Assessing Blockchain's Future in Transactive Energy

Ben Hertz-Shargel and David Livingston

ISBN-13: 978-1-61977-599-2

Cover: Transmitter tower outside Araçatuba, Brazil. Source: Rodolfo Marques on Unsplash

Atlantic Council
1030 15th Street, NW
12th Floor
Washington, DC 20005

Website: www.atlanticcouncil.org

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The electric power system is undergoing a rapid transition toward decarbonization and decentralization. The legacy model of one-way power flow from large, primarily fossil-based generators to consumers on the distribution grid is being upended, driven by the plummeting costs of distributed renewables, battery storage, and smart energy technologies. Residential and commercial utility customers, once simply consumers of electricity, are deploying these distributed energy resources (DERs) at scale alongside project developers, becoming producers themselves in a new, increasingly decentralized power system.

These changes pose a threat not only to the business models of utilities and conventional generators, but to the stability of energy markets and the electric grid itself. At the same time, they offer an opportunity: the flexibility of these new resources and technologies, their low carbon footprint, and their proximity to consumer loads could permanently reduce electricity and infrastructure costs while enabling the power sector to meet ambitious decarbonization targets. In order for this opportunity to be realized, however, legacy retail energy markets must be reformed to allow all distributed resource owners to participate and provide value, regardless of asset size and customer classification. These new markets must achieve for distribution systems what wholesale markets have for transmission systems, which is to align energy prices with real-time grid conditions such that efficient grid balancing occurs as a byproduct of market transactions. In other words, reformed market frameworks are needed to ensure these plentiful distributed resources work together as a symphony, rather than a cacophony, on the 21st century grid.

Blockchain, a technology that allows a network of mistrusting parties to securely transact with each other, has been proposed as a platform to host such transactive energy markets. Blockchain has the capability to bypass existing markets as well as the authority of electric utilities, offering residential and commercial actors a digital platform to directly buy and sell energy with each other, as well as with the utility. It also shares the power sector's growing ethos of decentralization and democratization, suggesting that it might be the means to transactive energy's end.

This report assesses the suitability of blockchain for this purpose, as a platform for transactive energy. It performs a first principles analysis of blockchain's technical attributes in order to align them with the expected needs of a transactive market, regardless of its precise design. Its principal conclusion is that blockchain is not currently well suited for this task, or indeed for hosting any of the primary functions of a real-time energy market, including energy data transmission, financial bids, trades, settlement, price formation, and grid service provision to the utility. While blockchain has many other potential energy-relevant applications for which it may be a far more logical and valuable tool, this does not currently extend to serving as the key platform for transactive energy markets.

This conclusion results from the identification of a fundamental tradeoff, in which blockchain's disintermediation of a central authority is achieved at the expense of six costs: (1) Efficiency, (2) Scalability, (3) Certainty, (4) Reversibility, (5) Privacy, and (6) Governance. The upside of this blockchain tradeoff has questionable value, and viability, in the context of transactive energy as there exist natural central authorities: public utility commissions, which have statutory authority over retail energy, and the electric utilities they oversee, which are tasked with ensuring the safe, reliable, and efficient operation of the electric distribution system.

At the same time, the costs of blockchain in this particular application are steep. The duplication of data hosting and processing across every node in the blockchain network dramatically limits both capital efficiency and scalability to real-world data and transaction volumes. The consensus methods by which blockchain nodes agree upon the shared transaction ledger rely upon economic incentives for—and the rationality of—its participants, posing risks to settlement finality and the security of the network in the face of hostile state actors. Perhaps most problematic, blockchain faces the opposing obligations of keeping mission-critical electrical and financial data confidential, while making it visible to its fleet of validator servers, which operate outside of a corporate firewall. Moving this confidential data off-chain would eliminate the issue, but significantly reduce blockchain's role in primary transactive

Source: Clint Adair on Unsplash

market functions. Cryptographic techniques to allow blockchain to meet these opposing obligations exist, but are in an early stage of research and development. They and their present limitations are discussed in detail in the appendix.

The report makes several policy recommendations, which aim to encourage and focus the development of transactive energy platforms—blockchain-based or not—that are capable of inverting the six costs, meeting specific criteria in these key performance areas for transactive energy. The recommendations include direct financial incentives, such as agency funding and prize-based awards, as well as indirect incentives that clarify the regulatory and commercial landscape for these platforms. They also include the formation of working groups and regulatory proceedings to study the value of transactive energy in light of state-specific policy objectives, such as distribution infrastructure deferral, grid resilience, renewable portfolio standards, and retail market animation, resulting in concrete policy and budgetary roadmaps toward the transactive systems that best meet those objectives.

Importantly, the report assesses blockchain's suitability as the platform for a real-time transactive energy market. It does not speak to the selective application of blockchain to energy applications in which the six costs have minimal impact, such as those involving less frequent transactions and non-confidential data. Renewable energy credit tracking and energy asset onboarding are two such examples. In sum, this report finds that blockchain should neither be dismissed outright, nor be viewed as a comprehensively disruptive technology or panacea for all energy challenges. Instead, it will likely continue to evolve as an increasingly useful tool for specific applications, building upon (rather than replacing) legacy systems to bring improvements to the function of energy markets as they become increasingly distributed and transactive in the years to come.

1. INTRODUCTION

A pair of technological disruptions are underway today that seem, in the minds of many, destined to join forces to transform the way that electricity is bought, sold, and valued.

The first is occurring in the power sector, where distributed energy resources (DERs) such as solar photovoltaics (PV) are threatening both the operations and the traditional business model of electric utilities. DERs today reduce the revenue that utilities earn from selling power while complicating the power flow on their networks, at times elevating voltages and even reversing the intended flow of electrical current. Many outside of the utility sector are sanguine about this upheaval, seeing it as inevitable growing pains as the industry both decarbonizes and modernizes to accommodate more dynamic and consumer-focused technologies.[1] The most ambitious possible outcome of this transformation is known as transactive energy, or what McKinsey & Company calls "energy eBay."[2] In short, it comprises a reimagining of the power sector in which end customers become both producers and consumers of energy, empowered to transact with each other as well as with the utility to maximize profit while helping balance the grid. To what extent this vision will become a reality is much debated, but the increasing capabilities and connectivity of consumer hardware such as smart solar inverters, stationary batteries, and electric vehicle infrastructure suggest the building blocks are there.[3]

The second disruption is blockchain, a technology that originated in the financial sector as a means of disintermediating banks from financial transactions.[4] Blockchain enables a set of participants, whether individuals or organizations, to safely transact with each other without investing trust in a central governing authority, such as a financial institution (e.g., Visa or a bank) or platform provider. It achieves this by distributing the storage and validation of a shared transaction ledger to all (or a subset of) participants and using sophisticated consensus mechanisms to ensure that they reach honest agreement on updates to the ledger.

The possibility to leverage this technology at the seams of joint ventures and global supply chains has caught widespread imagination, rocketing the idea to the forefront of media and technology innovation. To date, more than one hundred blockchain use cases are being worked on, and the technology has been promoted in industries as diverse as media, disease control, and fishing.[5] The energy sector is no exception, with incumbent utilities and energy firms as well as disruptive startups pursuing blockchain ventures, ranging in scope from green attribute certificate tracking, to financial settlement for grid services, to transactive energy writ large.[6] The degree to which blockchain shares the transactive energy ethos of democratization and decentralization is unmistakable, suggesting that blockchain might be the means to transactive energy's

[1] Todd Glass and Heather Curlee, "Use It or Lose It: The Once-in-a-Generation Opportunity to Change the US Electric Grid." Utility Dive, April 29, 2019, https://www.utilitydive.com/news/use-it-or-lose-it-the-once-in-a-generation-opportunity-to-change-the-us-el/553569/.

[2] Matt Rogers and Kimberly Henderson, "How Blockchain Can Help the Utility Industry Develop Clean Power," McKinsey & Company, April 10, 2019, https://www.mckinsey.com/business-functions/sustainability/our-insights/sustainability-blog/how-blockchain-can-help-the-utility-industry-develop-clean-power.

[3] Josue Campos do Prado, Wei Qiao, Liyan Qu, and Julio Romero Agüero, "The Next-Generation Retail Electricity Market in the Context of Distributed Energy Resources: Vision and Integrating Framework," *Energies* 12, no. 3 (2019): 491; Michael Giberson and Lynne Kiesling, "The Need for Electricity Retail Market Reforms," *Regulation* 40 (2017): 34, https://object.cato.org/sites/cato.org/files/serials/files/regulation/2017/9/regulation-v40n3-4.pdf.

[4] Disintermediation in this paper means obviating a central authority (for example, a bank or platform provider) by enabling the network of participants to themselves validate, record, and secure their transactions.

[5] Matt Higginson, Marie-Claude Nadeau, and Kausik Rajgopal, "Blockchain's Occam Problem," McKinsey & Company, January 2019, https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem; World Economic Forum, *Building Block(chain)s for a Better Planet* (September 2018), http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf.

[6] David Livingston, Varun Sivaram, Madison Freeman, and Maximilian Fiege, *Applying Blockchain Technology to Electric Power Systems*, Council on Foreign Relations, July 2018, https://cfrd8-files.cfr.org/sites/default/files/report_pdf/Discussion_Paper_Livingston_et_al_Blockchain_OR_0.pdf; Kevin Stevens, "Why Blockchain Will Power the New Energy Network," Utility Dive, October 23, 2018, https://www.utilitydive.com/news/why-blockchain-will-power-the-new-energy-network/540226/; Jason Deign, "4 Energy Blockchain Companies You Should Watch in 2019," Greentech Media, January 3, 2019, https://www.greentechmedia.com/articles/read/4-energy-blockchain-companies-you-should-watch-in-2019#gs.7qce2c; Charlie Burton, "In 2019, a New Blockchain Will Fix How We Buy and Sell Green Energy," Wired, December 13, 2018, https://www.wired.co.uk/article/energy-web-foundation-blockchain; Tohoku Electric Power Co., Inc., Toshiba Energy Systems & Solutions Corporation, "Joint Research Agreement for P2P Energy Trading between Individuals Using Distributed Energy Resources," press release, April 26, 2019, Toshiba-energy, https://www.toshiba-energy.com/en/info/info2019_0426.htm?from=RSS_PRESS&uid=20190426-6075e.

end. Government has taken notice, with dockets introduced in public utility commissions, multiple US Department of Energy grants focused on blockchain, congressional hearings, and even the formation of a Congressional Blockchain Caucus, which has shown interest in blockchain's relevance for the energy sector.[7]

Despite the breathless proclamations emanating from industry, criticism has surfaced as well, marking blockchain's initial, and expected, evolution along the hype cycle of emerging technologies. Most prominent have been cries over the lack of sustainability of blockchain's "proof of work" consensus method, which demands vast amounts of computation—and therefore energy use—to guard against malfeasance in the network, as well as over the instability of cryptocurrencies.[8] As second-generation blockchains have begun to move away from proof of work, more nuanced criticism has taken aim at blockchain's suitability for broader applications, questioning its scalability, cost-effectiveness, potential lack of data privacy, and cybersecurity.[9]

These analyses have implications for blockchain's application to energy, but they offer limited insight because they do not take into account the unique economic, technical, and regulatory concerns of the industry. Conversely, appraisals of blockchain from within the energy industry have not viewed the technology with a sufficiently technical lens, raising questions but few answers as to its applicability, and in some cases underestimating—or misunderstanding—its limitations.[10] Common examples are claims that, as a distributed ledger technology, blockchain makes it faster or easier for distributed resources to submit transactions to the network than traditional centralized platforms, or that blockchain relates to the distributed control often proposed for smart grids.

In fact, blockchains today can support an order of magnitude fewer transactions than other modern platforms, and their distributed ledger control has little relation or contribution to the kind of intelligent grid and energy market management required for transactive energy. Blockchain, though offering a number of significant benefits, is not a panacea. A more detailed understanding of its strengths and limitations in particular use cases—for the purposes of this paper, as a transactive energy platform—can help guide its evolution as it matures and gains greater exposure in real-world, commercial applications. What energy regulators, executives, and investors need is a careful, first principles analysis of blockchain that scrutinizes its benefits and costs against specific needs of the energy industry, in order to evaluate its potential as a platform architecture.

This paper seeks to perform such an analysis.

[7] "Commissioner Tobin Opens Docket to Examine Blockchain Technology," Arizona Corporation Commission, July 16, 2018 https://www.azcc.gov/news/2018/07/16/commissioner-tobin-opens-docket-to-examine-blockchain-technology; Robert Walton, "Nevada Considers Blockchain to Track Renewable Credits," Utility Dive, October 15, 2018, https://www.utilitydive.com/news/nevada-considers-blockchain-to-track-renewable-credits/539597/; Full Committee Hearing: Energy Efficiency of Blockchain and Similar Technologies, Senate Committee on Energy and Natural Resources, 115th Cong. (August 21, 2018).

[8] Nathaniel Popper, "There Is Nothing Virtual about Bitcoin's Energy Appetite," *New York Times*, January 21, 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html; G.F. "Why Bitcoin Uses so Much Energy," *Economist*, https://amp.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy; Bank for International Settlements, *Annual Economic Report 2018* (June 2018), 91-114, https://www.bis.org/publ/arpdf/ar2018e.pdf.

[9] Mike Orcutt, "Ethereum's Smart Contracts Are Full of Holes," *MIT Technology Review*, March 6, 2018, https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/; Jason Bloomberg, "Don't Let Blockchain Cost Savings Hype Fool You," *Forbes*, February 24, 2018, https://www.forbes.com/sites/jasonbloomberg/2018/02/24/dont-let-blockchain-cost-savings-hype-fool-you/#56c633405811.

[10] Benjamin L. Gerber, "Don't Believe All the Blockchain Hype," Utility Dive, November 9, 2018, https://www.utilitydive.com/news/dont-believe-all-the-blockchain-hype/541303/; World Economic Forum, *Building Block(chain)s for a Better Planet*; World Energy Council, *World Energy Insights Brief 2018-Blockchain Anthology of Interviews* (October 2018); Merlinda Andoni, Valentin Robu, David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter Mccallum, and Andrew Peacock, "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities," *Renewable and Sustainable Energy Reviews* 100 (2019): 143-74, doi:10.1016/j.rser.2018.10.014.

It begins with a review of retail energy today, its limitations, and the opportunities for a future, more efficient, transactive grid. Common designs for a transactive energy market are outlined, along with their core economic and technical challenges. Blockchain's architecture and key attributes are then presented, followed by its prototypical approach to transactive energy, illustrating the value chain from power generation to tokenization, to downstream market transactions.

The paper then turns to evaluating blockchain's suitability as a transactive energy market platform, aligning its properties with the needs of transactive energy and contrasting with traditional platform architectures. Rather than paint a straw man perspective of first-iteration blockchain systems that would inevitably be easy to critique, the analysis takes account of advances in blockchain consensus, on- and off-chain scaling, governance models, privacy enhancements, and other extant and prospective innovations.

The evaluation finds that blockchain offers what is termed a blockchain tradeoff for applications, in which disintermediation of a central platform authority is achieved at the expense of six costs: efficiency, scalability, certainty, reversibility, privacy, and governance. The paper characterizes these costs in detail, as well as the innovations that blockchain developers have proposed to remedy them. It argues that the blockchain tradeoff is difficult to justify for some—though not necessarily all—aspects of transactive energy, since decentralization of authority has questionable value (and viability) in the retail energy sector and the costs of achieving it are high, so far. Moreover, microtransactions, smart contracts, and support for third-party application development, often leaned on as selling points of blockchain, may in fact be better supported by traditional platform architectures. This raises, though not insurmountably, the burden of proof for blockchain's value proposition, which must demonstrate not only viability, but its superiority to proven platform alternatives.

Next, the paper focuses on a core challenge in transactive energy: how to couple the constantly evolving physical state of the electrical grid to transactive market prices, such that social welfare (gross energy consumption value minus production costs) is maximized subject to grid stability. This is a hard problem at the intersection of mathematics, economics, and electrical engineering, to which blockchain—unlike other proposed decentralized architectures—does not yet contribute to solving.[11] Even if blockchain does play a role in a future transactive energy market, therefore, it is so far unprepared to play a leading role.

The paper concludes by synthesizing the foregoing takeaways into insights and recommendations for policymakers, insofar as they have the capacity to direct further blockchain innovation in the direction of the most appropriate use cases. Innovation does not occur in a policy vacuum, and so there still exist opportunities to shape blockchain development to address sensible applications.

[11] Matt Kraning, Eric Chu, Javad Lavaei, and Stephen Boyd, "Dynamic Network Energy Management via Proximal Message Passing," *Foundations and Trends® in Optimization* 1, no. 2 (2013): 70-122, doi:10.1561/2400000002; Elli Ntakou and Michael Caramanis, "Distribution Network Electricity Market Clearing: Parallelized PMP Algorithms with Minimal Coordination" (paper presented at the 53rd IEEE Conference on Decision and Control, Los Angeles, 2014), doi:10.1109/cdc.2014.7039642; Hyojong Lee, Shwetha Niddodi, Anurag Srivastava, and David Bakken, "Decentralized Voltage Stability Monitoring and Control in the Smart Grid Using Distributed Computing Architecture" (paper presented at the 2016 IEEE Industry Applications Society Annual Meeting, Portland, Oregon, 2016), doi:10.1109/ias.2016.7731871.

2. TOWARD A TRANSACTIVE GRID

Retail Energy Today

Retail energy features prominently among industries that proponents of blockchain claim the technology is poised to disrupt. Indeed, there is little question that retail energy is poised for disruption. More than twenty years after the first electric monopolies were broken up and competition was introduced in the 1990s, many vestiges of the industry's origin exist today. Regulated markets, often in lower population density regions, remain monopolies, with single utilities owning the generation, transmission, distribution, and retail sale of bulk power, and earning a fixed rate of return on energy sales and capital investments. In unregulated markets, companies are restricted to owning only a single part of this value chain, or to owning the distribution and retail sale of bulk power in the case some distribution utilities. Those providing transmission or distribution are regulated by state public utility commissions, similar to regulated markets, while generators and retailers must compete for market share under lighter regulation. In the unregulated setting, energy retailers purchase bulk power, typically through long-term power purchase agreements or real-time wholesale markets, which they then resell to end customers. Wholesale markets optimize the procurement of energy and future capacity, as well as ancillary services—advanced power control necessary to stabilize the grid—and determine the prices paid at each moment and location on the transmission grid.

Retail markets today shield mass market customers from the complexity and risks of wholesale markets. Customers are charged for their use of the grid according to simple monthly rates, whose components can include a fixed charge; a tiered charge based on total kilowatt-hours (kWh) of energy consumed; a demand charge, based on the highest single hour of consumption (primarily for large commercial customers); and a delivery charge levied by the distribution operator. Only in the last several years have utilities begun rolling out time-of-use (TOU) rates, which charge more during the late afternoon and early evening when demand tends to peak, coarsely aligning end user costs with expected wholesale and delivery costs.

Silicon Valley Power. Source: American Public Power Association on Unsplash

While retail customers have benefited from the simplicity and affordability of these rates, they appear increasingly outdated and restrictive in the context of the "modern" grid.[12] DERs such as residential and commercial solar, smart thermostats and water heaters, stationary batteries, and electric vehicles have enjoyed tremendous growth, but current rate structures leave customers limited opportunity to monetize them, for instance by reducing power consumption when it is most expensive. At the same time, wholesale markets are largely inaccessible to residential and small commercial customers, as burdensome requirements on resource size, power metering, year-round availability, and real-time data communication and control present formidable barriers to entry.[13]

There are even more fundamental problems with existing rates from the perspective of an electric utility. In the absence of meaningful incentives, customers consume—and their DERs produce—power irrespective of grid conditions, leading to inefficient behavior at multiple grid scales. At the edge of the grid, excess daytime solar production leads to elevated voltages and reverse power flows, while in the evening excess power demand leads to under-voltage conditions and the risk of transformer overload. Higher up in the distribution network, operators see congestion due to wasteful reactive power demand—the component of electrical power that is required by air conditioners, motors, and other inductive loads but is lost as heat, rather than converted to useful work. At the global network level,

[12] Giberson and Kiesling, "The Need for Electricity Retail Market Reforms."

[13] PJM, *PJM Manual 18: PJM Capacity Market* (January 2019), https://www.pjm.com/-/media/documents/manuals/m18.ashx.

system operators dispatch (often inefficient) fossil generators at breakneck speed to adjust to dips in intermittent renewable production and the load ramps leading up to the evening peak, at times offsetting much of the environmental contributions of the renewables.[14]

No retail price signals exist today at scale to alert customers of these phenomena as they occur, incentivizing them to modify their behavior to help alleviate the problem. Instead, utilities shoulder the full burden of grid balancing, relying on dedicated infrastructure and reserve capacity contracts, costly investments with low utilization factors. In a vicious cycle, the lack of market access or incentives for grid-responsive behavior inhibit customer adoption of more efficient technologies, which results in a loss for customers, the grid, and public policy goals such as decarbonization.[15]

Transactive Energy

Transactive energy is a model for the grid that inverts the present one by decentralizing not only the production of energy, but the complex balancing of the grid itself. In this model, customers and their energy assets are empowered to transact with each other and the distribution utility according to real-time, local prices for energy products such as real power, reactive power, and grid support services.[16] Importantly, these prices are based on local grid needs as well as participant supply and demand, acknowledging the physical limitations of the network.[17] Coupling economic value with physical stability ensures customer capital—DERs and site loads—will act as first responders in grid balancing, depending on leaner, more expensive utility infrastructure only as a backstop.[18] It will also, according to transactive energy proponents, drive greater technological and financial innovation, as the vast pool of revenue for grid management is opened up from large operators to all customers, whose earnings are limited only by the tools and business practices they use to manage their energy.[19]

How these new transactive energy markets will work, what entity will host them, and how exactly they will couple physical stability with economic value are subjects of ongoing research and debate.[20] Bilateral trading is a possibility, either peer-to-peer or through a central exchange, but it is not clear how such bilateral trading could take account of the overall state of the electric grid in determining prices, which is essential for delivering system-optimal, rather than simply bilaterally optimal, pricing. Bilateral energy markets have proven inferior to centralized clearing markets for energy, historically.[21]

Moreover, the physical characteristics of medium- and low-voltage distribution networks—upon which a transactive market would be built—necessitate a full optimal power flow (OPF) calculation in order to produce locational marginal prices: the most economically efficient for electricity markets.[22] This calculation, performed routinely by wholesale market operators for the high-voltage transmission system, is the basis of a centrally-cleared market, further suggesting this market design would be most optimal for a transactive system. It was the design chosen in several of the most prominent transactive energy pilots to date, including the Olympic Peninsula Demonstration project in Washington State and the AEP gridSMART® demonstration in Ohio.[23]

[14] Union of Concerned Scientists, *Turning Down the Gas in California: The Role of Natural Gas in the State's Clean Electricity Future* (August 2018).

[15] MIT Energy Initiative, *Utility of the Future: An MIT Energy Initiative response to an industry in transition*, 2016, http://energy.mit.edu/research/utility-future-study/.

[16] GridWise Architecture Council, *GridWise Transactive Energy Framework Version 1.0* (January 2015), https://www.gridwiseac.org/pdfs/te_framework_report_pnnl-22946.pdf.

[17] Smart Electric Power Alliance, *Transactive Energy: Real-World Applications for the Modern Grid* (April 2019), https://sepapower.org/resource/transactive-energy-real-world-applications-for-the-grid/; "Transactive Energy: An Overview," NIST, April 19, 2017, https://www.nist.gov/engineering-laboratory/smart-grid/transactive-energy-overview.

[18] GridWise Architecture Council, *GridWise Decision-Maker's Transactive Energy Checklist* (December 2016), https://www.gridwiseac.org/pdfs/gwac_te_checklist_dec2016_pnnl_25658.pdf.

[19] do Prado, Campos, Qiao, Qu, and Agüero, "The Next-Generation Retail Electricity Market."

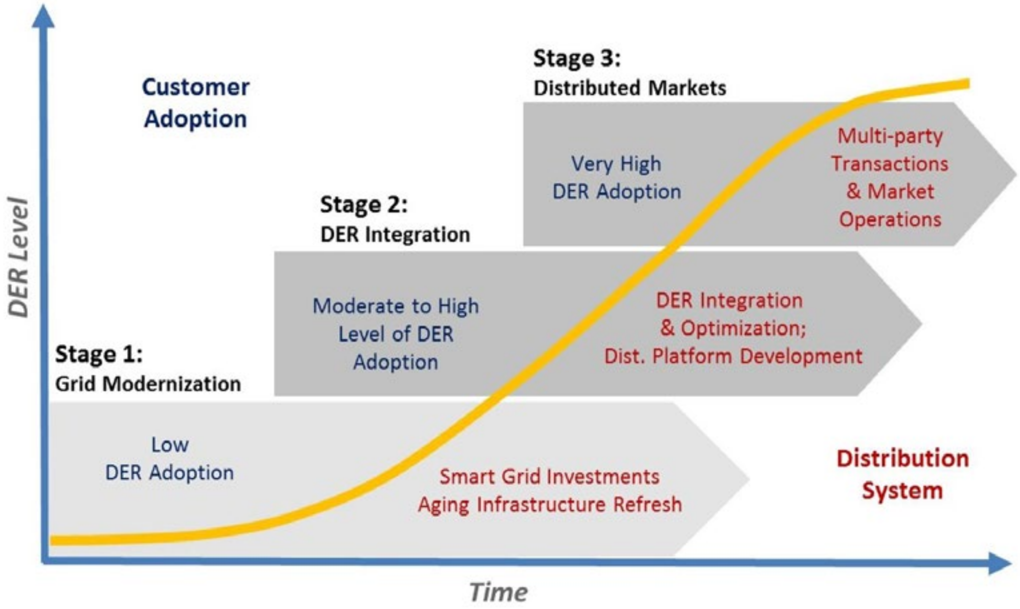
[20] NIST, "Transactive Energy: An Overview," April 19, 2017, https://www.nist.gov/engineering-laboratory/smart-grid/transactive-energy-overview.

[21] Erin T. Mansur and Matthew White, "Market organization and efficiency in electricity markets," unpublished results (2012).

[22] MIT Energy Initiative, *Utility of the Future: An MIT Energy Initiative response to an industry in transition* (2016); International Energy Agency, *Tackling Investment Challenges in Power Generation in IEA Countries: Energy Market Experience* (2007), http://www.iea.org/publications/freepublications/publication/tackling_investment.pdf; Hogan, William W., and Susan L. Pope. "Priorities for the evolution of an energy-only market design in ERCOT," FTI Consulting (2017), https://hepg.hks.harvard.edu/files/hepg/files/hogan_pope_ercot_050917.pdf

[23] Jianming Lian, Zhang, Wei, Sun, Y., Marinovici, Laurentiu D., Kalsi, Karanjit, and Widergren, Steven E. Wed, "Transactive System: Part I: Theoretical Underpinnings of Payoff Functions, Control Decisions, Information Privacy, and Solution Concepts," United States, doi:10.2172/1422302. https://www.osti.gov/servlets/purl/1422302.

Figure 1: Distribution System Evolution



Displayed is a three-stage evolutionary framework for the distribution system driven by its aggregate growth of DERs. The stages are related to the required distribution system changes and potential for DER service transactions at certain thresholds of DER adoption, as experienced in the US and globally to date.

Source: De Martini, P., L. Kristov, and L. Schwartz (subsidiary author/ technical editor). 2015. *Distribution Systems in a High Distributed Energy Resources Future*. Future Electric Utility Regulation series. Berkeley Lab.

In light of the foregoing considerations, significant research has been devoted to developing a two-sided clearing market similar to wholesale markets but tailored to the distribution system.[24] In this setup, a market engine solves an optimal power flow problem on a recurring basis, which maximizes participant value while meeting distribution system constraints, such as current limits on transformers. Outputs of the process include local prices for energy and reserve products, as well as an optimal power schedule for the network. This real-time market could optionally be preceded by a forward market, in which cleared demand bids and supply offers would financially commit participants to grid balancing behavior, as they do in wholesale markets today. Such obligations would settle according to real-time market prices, based on measurably delivered or consumed energy.

Transactive markets would be administered by a distribution system operator (DSO), analogous to the independent system operators (ISO) that run today's wholesale markets, which could be a utility, another entity, or a consortium.[25] How the DSO interacts with the ISO, and to what degree it relies on price signals versus active control over DERs in order to maintain distribution stability, remain important questions of grid architecture.[26]

Transactive energy markets will require vastly more data than is involved in distribution operations management today. This includes utility equipment and sensor data throughout the grid, as well as customer financial and electrical data at its edges, likely gathered at a fifteen-minute or five-minute time resolution (consistent with the granularity of wholesale prices today).[27] Capturing

[24] Linquan Bai, Jianhui Wang, Chengshan Wang, Chen Chen, and Fangxing Li, "Distribution Locational Marginal Pricing (DLMP) for Congestion Management and Voltage Support," *IEEE Transactions on Power Systems* 33, no. 4 (2018), doi: 10.1109/ TPWRS.2017.2767632; Sina Parhizi, Amin Khodaei, and Shay Bahramirad, "Distribution Market Clearing and Settlement," in 2016 I*EEE Power and Energy Society General Meeting (PESGM)* (IEEE, 2016), 1-5; Elli Ntakou and Michael Caramanis, "Distribution Network Electricity Market Clearing: Parallelized PMP Algorithms with Minimal Coordination," in *53rd IEEE Conference on Decision and Control* (IEEE, 2014) 1687-1694, https://ieeexplore.ieee.org/document/7039642; Tabors, Parker, Centolella, and Caramanis, *Developing Competitive Electricity Markets.*

[25] Sander Van Ginkel, "Role of Distribution System Operators in the New Energy System," Accenture, June 19, 2017, https://www.accenture.com/us-en/blogs/blogs-distinctive-role-distribution-system-operators; IRENA, *Future Role of Distribution System Operators: Innovation Landscape Brief* (2019), https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Feb/IRENA_Landscape_Future_DSOs_2019.pdf?la=en&hash=EDEBEDD537DE4ED1D716F4342F2D55D890EA5B9A.

[26] Lorenzo Kristov, Paul De Martini, and Jeffrey D. Taft, "A Tale of Two Visions: Designing a Decentralized Transactive Electric System," *IEEE Power and Energy Magazine* 14, no. 3 (January 15, 2016): 63-69, doi:10.1109/mpe.2016.2524964.

[27] U.S. Federal Agency Regulatory Commission, 18 CFR Part 35, Docket No. RM15-24-000; Order No. 825, Settlement Intervals and Shortage Pricing in Markets Operated by Regional Transmission Organizations and Independent System Operators (June 6, 2016), https://www.ferc.gov/whats-new/comm-meet/2016/061616/E-2.pdf.

this data reliably, efficiently, privately, and securely, while making it available to public markets and the distribution utility in real-time will be an enormous challenge for the hosting platform. Beyond data management, the hosting platform will also be responsible for supporting a range of transactions, from bids and offers for market products to market clearing and settlement activity, the latter made complex by the involvement of utility data. These transactions must be processed at scale, with strict latency, finality, and privacy requirements.

In light of these requirements, some blockchain proponents consider it unrealistic for the technology to host transactive energy markets. According to this view, blockchain is positioned to play a focused role, such as enabling energy asset registration and data access, working alongside more real-time communication, control, and grid-aware technologies to meet the needs of transactive energy. This view is credible, and has been explored elsewhere, but is not investigated in this report.[28]

Other blockchain proponents see the technology more expansively, as the natural platform for hosting transactive energy markets.[29] The decentralized control fundamental to transactive energy is analogous to the decentralized consensus of blockchain, and both share the aim of opening and democratizing markets. Moreover, blockchain has established itself as a secure platform for automating multilateral transactions, including complex contracts and financial instruments. Recent innovations enable blockchains to go further, interacting with external systems and, therefore, the physical world, allowing transactions to trigger—and be triggered by—real world events, such as electric meter reads and the initiation of electric vehicle charging.[30]

Business models and frameworks for blockchain's role in transactive energy vary. Startup Grid+ aims to be a reimagined energy retailer, exposing customers to wholesale prices and providing them the tools to manage their energy consumption and generation effectively; Lithuania-based WePower uses blockchain to crowdfund renewable project finance, in which only forward contracts for energy are transacted; and Electron, a United Kingdom (UK)-based entrant, has created an energy asset registration system, and has begun to develop a more ambitious energy trading platform for balancing electricity markets.[31] The companies whose blockchain approaches are profiled below share Electron's expansive vision for blockchain as the platform underlying the full gamut of energy transactions: consumption and production metering and accounting; energy market bids, trades, price formation and settlement; and grid service provision to the utility. As the use case underlying claims of industry disruption, it is this final, ambitious potential role for blockchain that is evaluated in this report. The findings should thus not be seen as critical against many other intermediate applications of blockchain, or applications in other promising areas that could aid the energy transition.

There may indeed be such a role for blockchains in transactive energy markets of the future. However, this report finds that there are characteristics of blockchains that may prevent them from serving as platforms that can achieve the speed, scale, and security necessary to realize the transactive energy vision. To facilitate a fair and informed assessment, it is important first to understand the basic design of blockchains and the tradeoffs implied by their current design features. While some of these tradeoffs are likely to evolve (or to be eliminated entirely in accordance with computer science advancements), others regard intrinsic structural features that are likely to persist into the future. All these tradeoffs are explored in detail in the sections that follow.

[28] World Economic Forum, *Building Block(chain)s for a Better Planet* (September 2018), http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf; Philipp Richard, Sara Mamel, and Lukas Vogel, *Blockchain in the Integrated Energy Transition* (Dena, February, 2019), https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2019/dena-Studie_Blockchain_Integrierte_Energiewende_EN2.pdf.

[29] Lawrence Orsini and Bill Collins, *Exergy: Electric Power Technical Whitepaper* (L03 Energy, December 14, 2017); "Welcome to the Future of Energy," Grid+; Power Ledger, *Power Ledger White Paper*; Avangrid, Con Edison, National Grid, New York Power Authority, and Indigo Advisory Group, "New York Utilities: We Believe Blockchain Is 'Transformative,'" Greentech Media, July 19, 2018, https://www.greentechmedia.com/articles/read/utilities-and-blockchain; Jeff St. John, "Ameren and Opus One to Test Blockchain-Enabled Microgrid Energy Trading," Greentech Media, April 2, 2019, https://www.greentechmedia.com/articles/read/ameren-and-opus-one-to-test-blockchain-enabled-microgrid-energy-trading.

[30] Julian Spector, "Blockchain-Enabled Electric Car Charging Comes to California," Greentech Media, August 2, 2017, https://www.greentechmedia.com/articles/read/blockchain-enabled-electric-car-charging-california#gs.nx7447.

[31] Electron, "Electron Wins Government Award to Advance Blockchain in Balancing Electricity Markets," Finextra, September 27, 2017, https://www.finextra.com/pressarticle/70874/electron-wins-uk-government-award-to-advance-blockchain-in-balancing-electricity-markets; Kelvin Ross, "Blockchain Firm Electron in Korean Energy Project," Power Engineering International, October 17, 2018, https://www.powerengineeringint.com/articles/2018/10/blockchain-firm-electron-in-korean-energy-project.html; WePower, "WePower Whitepaper Version 2" (February 27, 2019), https://wepower.network/media/WhitePaper-WePower_v_2.pdf.

3. APPLYING BLOCKCHAIN TO TRANSACTIVE ENERGY

ARCHITECTURE

A Unified Definition

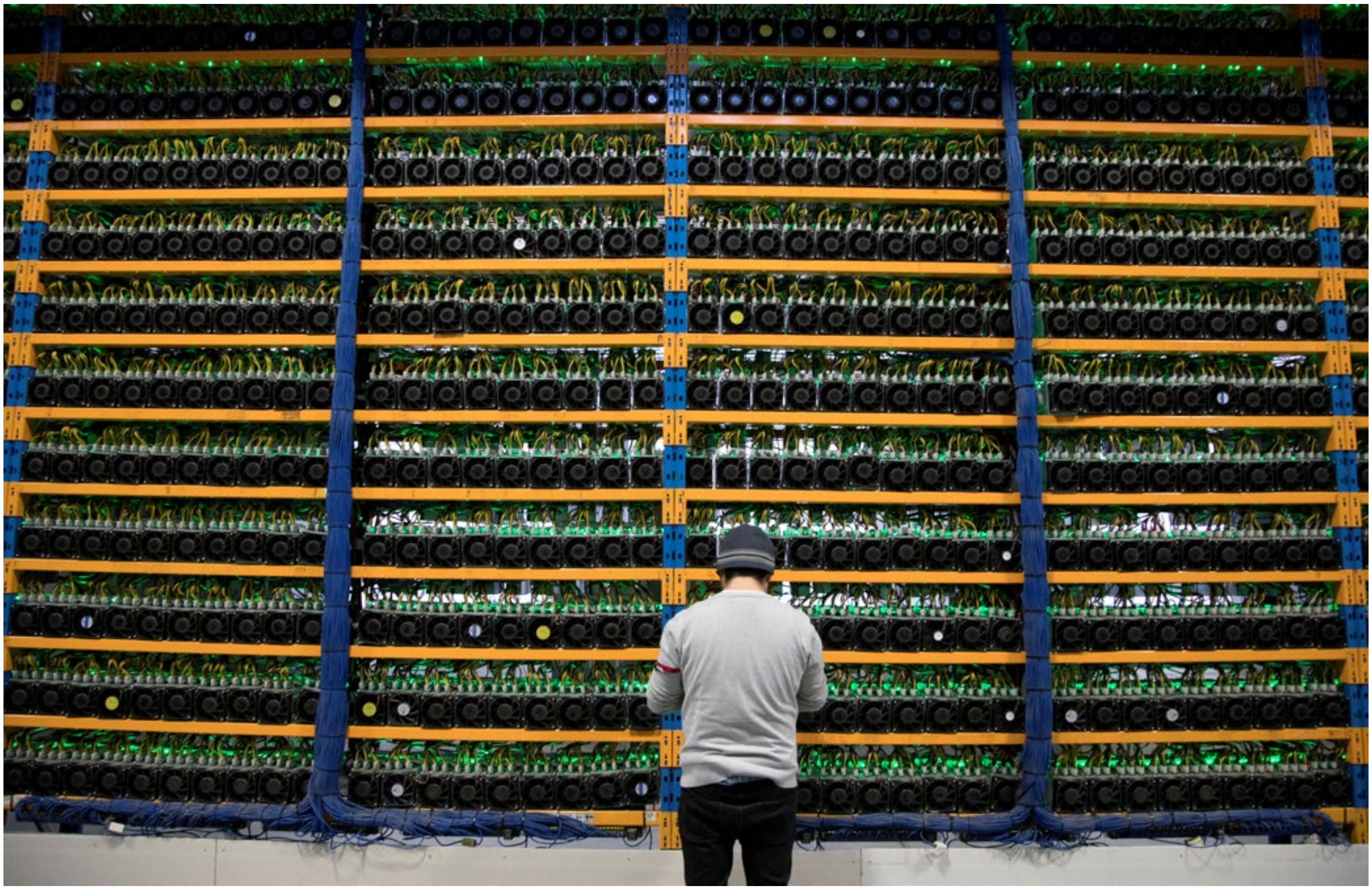
A wide range of technologies self-identify as blockchains today, making a unified definition difficult. The public blockchains that host cryptocurrencies, for example, differ from the Hyperledger family of blockchains developed by IBM, the Linux Foundation, and others to support private commercial applications. Despite their differences, however, these technologies share several key elements which constitute a working definition.

First, all blockchains involve computational nodes, commonly referred to as peers, operated by participants, each of which owns a copy of a shared transaction ledger. Blockchains are broadly categorized as permissioned or permissionless based on whether these peers are on equal footing, particularly with regard to their involvement in reading from, writing to, and validating the ledger. Permissionless, also known as public, blockchains such as Bitcoin and Ethereum grant all peers equal rights to perform all of these tasks. Permissioned, also known as private, blockchains limit the data access or validation privileges of peer nodes based on participant identity or role.

Transactions and Smart Contracts

Blockchain transactions most commonly represent the transfer of a digital token or currency from one set of participants to another. Transactions must be cryptographically signed by any blockchain account that is party to them, which requires access to that

An Electrify SG engineer shows how a PowerPod is installed to record data of photovoltaic solar panels on a rooftop in Singapore, December 18, 2017. Electrify is a Singaporean company that has launched a blockchain-based exchange. Picture taken December 18, 2017. REUTERS/Edgar Su



A worker checks the fans on miners, at the cryptocurrency farming operation, Bitfarms, in Farnham, Quebec, Canada, February 2, 2018. Picture taken February 2, 2018. REUTERS/Christinne Muschi

account's secret key, and therefore cannot be faked or repudiated.[32] Once submitted to the network, transactions are grouped into blocks in order to be validated and added to the ledger; each block contains a cryptographic reference to the one that came before, resulting in the eponymous blockchain.

Beyond simple token transfers, transactions can also trigger what are known as smart contracts: collections of software functions that maintain internal data about participants and their devices. A smart contract might store the number of kilowatt hours (kWh) of energy produced by a solar array, for instance, and expose one function for a smart meter to increment the value and another for the utility to read the value. Typically, smart contracts are stored on the blockchain itself, inside special types of transactions, making them inspectable by participants and immutable. Despite their name, smart contracts carry no intrinsic legal meaning and can be thought of simply as blockchain-specific computer programs.

Peer Consensus

Peer nodes in a blockchain network operate freely and independently of each other. As they receive transaction blocks proposed by other peers, and new transactions submitted by participants, not yet added to a block, they share them with other peers in order to ensure that all are working with the same information. Owing to the latencies in their communication, peers' versions of the shared ledger may disagree from moment to moment. These differences are reconciled through a consensus protocol, designed to overcome mistakes, honest disagreements, and intentional manipulation. The consensus protocol determines at any given time which node is able to add the next block to the chain, and which peers are assigned to validate that block. The former is called mining, or forging, the block, and can earn the owner of the peer a mining reward, in addition to transaction fees offered by each transaction included in the block. These rewards are paid in cryptocurrency automatically by the blockchain software.

[32] D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, and Shu-Jen Chang, *Introduction to Public Key Technology and the Federal PKI Infrastructure* (National Institute of Standards and Technology, February 26, 2001).

In the original proof of work (PoW) protocol, utilized today by the two largest public blockchains, Bitcoin and Ethereum, any peer is permitted to mine a block at any time, provided it solves a cryptographic math problem based on that block. The term "mining," in fact, derives from the lengthy, repetitive calculations required by design to solve this problem. Each peer is racing against the others to achieve this first, because the protocol specifies that longer chains are "more valid" than shorter ones, and only the first peer to add a valid block can be confident that their extended version of the blockchain will be accepted by a majority of the others. All peers participating in the mining process are implicitly validators, accepting this role out of the self-interest of knowing that proper validation is the surest guarantee that their own mining efforts will be rewarded through cryptocurrency.

The enormous energy consumption and associated carbon emissions required for PoW (due to the electricity needed to power the underlying computational activity) have been well documented.[33] Less energy-intensive consensus alternatives include proof of stake (PoS) and proof of authority (PoA), in which peers must stake some portion of their cryptocurrency wealth or their network reputation, respectively, in order to forge a block, and lose that collateral if the blocks they propose are not accepted. A notable property that these alternatives share with PoW is a reliance on both the economic incentives offered to validators for honest work and the self-interest of the validators in pursuing those incentives. If a majority of peers fail to follow these incentives for any reason, even briefly, all assurances of ledger integrity are lost.

An example is what is known as a 51% attack, in which one or more validators representing a majority of the computing power in the network (or stake, depending on the consensus method) collude to hijack the blockchain.[34] The conspirators spend all of their wealth on the main blockchain in order to purchase physical goods or services, and then use their validation influence to promote an alternative chain in which the transactions never took place. Renting the resources necessary to carry out a 51% attack on a major PoW blockchain is expensive, but not prohibitive—certainly for state actors—and the cost threshold is lower for blockchains with fewer nodes and less computing power involved.[35]

The Blockchain Ledger and Distribution of Authority

Two other defining properties of blockchain are the immutability of the transaction ledger and its transparency for validators. Immutability is crucial not only for efficient validation and consensus, but for ensuring that the state of the ledger remains well-defined, as a change to historical state—such as an account balance—could render future transactions invalid. Transparency is a precondition for validation itself since unless a peer can inspect a transaction and its effect on the ledger, it cannot validate it.

From the perspective of blockchain's design principles, these properties serve a unifying purpose: They distribute the responsibilities of managing a transaction network from a single authority, such as a financial institution or commercial platform provider, to many. These responsibilities include the hosting of data, the computation necessary to process transactions and run applications (smart contracts), and the hosting of staked collateral, all of which are performed by peers. The responsibility of transaction validation is distributed over the potentially smaller set of validator nodes. The costs associated with these shared activities are similarly distributed across the network, borne by all participants as transaction costs.

The Blockchain Approach

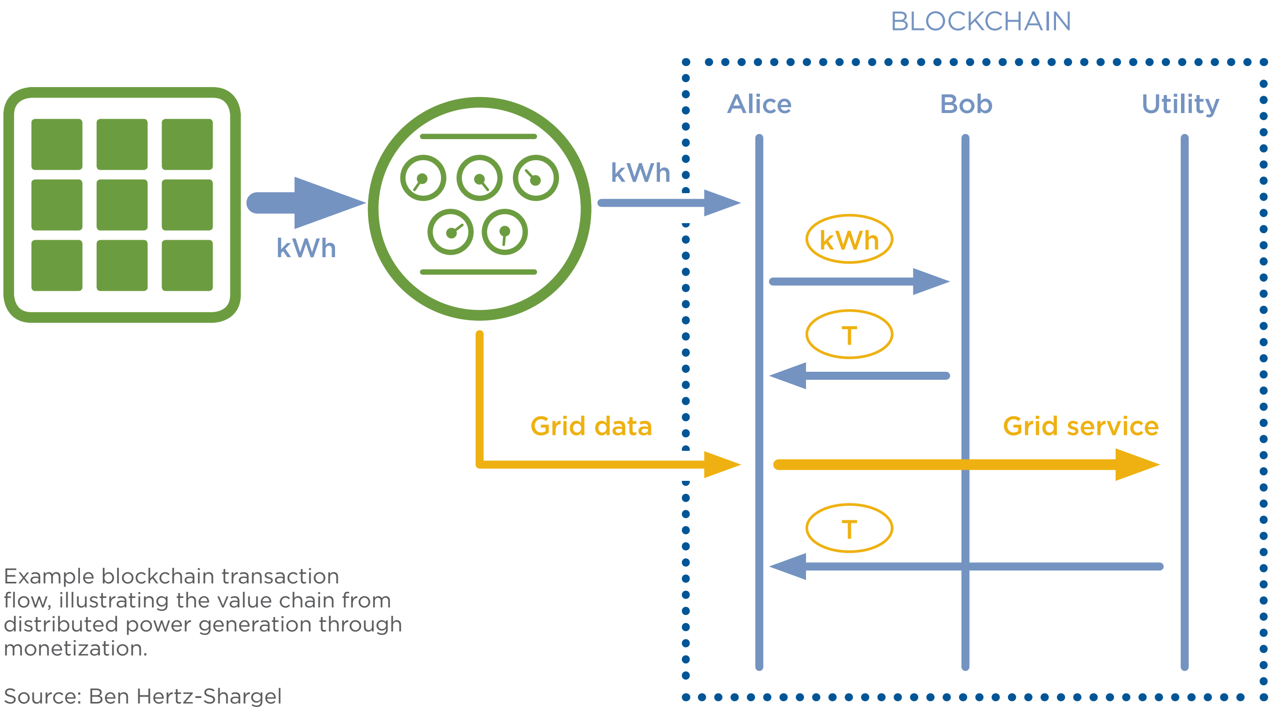
To illustrate how blockchain supports the energy value chain from point of production to downstream transactions, a prototypical flow diagram is presented below. In the example, Alice is a producer, who seeks to monetize her investment in a rooftop solar array. This must be achieved on a daily basis, with minimal involvement from Alice, as few energy futurists consider it realistic for customers to micromanage their energy asset investments, whether it is to day trade energy or negotiate grid services to a utility. It would be a smart software agent, such as an artificial intelligence (AI)-enabled digital assistant, that is managing such transactions, seeking only high-level guidance and permissions from the customer. As an example, the agent may forecast energy usage in the home to procure day-ahead energy and adjust to real-time deviations from the forecast with procurements from the real-time market. Forecasted excess capacity could be bid into a reserve

[33] Max J. Krause and Thabet Tolaymat, "Quantification of Energy and Carbon Costs for Mining Cryptocurrencies," *Nature Sustainability* 1, no. 11 (2018): 711.

[34] Mike Orcutt, "Once Hailed as Unhackable, Blockchains Are Now Getting Hacked," *MIT Technology Review*, February 19, 2019, https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

[35] "PoW 51% Attack Cost," Crypto51, https://www.crypto51.app/.

Figure 2: Example Blockchain Transaction Flow and Value Chain



Example blockchain transaction flow, illustrating the value chain from distributed power generation through monetization.

Source: Ben Hertz-Shargel

market, earning additional revenue while providing much-needed flexible capacity to the market.

Alice begins by purchasing what are known as utility tokens from the blockchain network—tokens required by the blockchain provider for platform access, as a means of charging economic rent. PowerLedger, an Australian blockchain energy startup, requires customers or their retail energy provider to purchase the company's POWR tokens, which are then escrowed in exchange for Sparkz tokens, which can be used to transact.[36] LO3 Energy, a Brooklyn-based startup, requires participants to purchase their XRG tokens and then stake them to a blockchain account or smart meter in order to participate.[37] The more XRG a producer stakes to their meter, the greater their revenue potential, and the more a DSO stakes to customer devices, the more data they will be able to access.

When Alice's PV array produces power, it is measured and recorded by a smart meter (or a smart inverter directly integrated with the array).[38] A software client on the smart meter, known as a blockchain oracle, connects to the blockchain over the internet or a home area network and submits a transaction, registering the meter read. When validated and performed by the blockchain, the transaction invokes a function on a smart contract, passing the oracle's identity, the kWh value, and any other attributes of the solar production as inputs. The oracle is thus a critical part of the digital-physical interface: no matter how sophisticated the blockchain design may be, it means nothing if the physical information (such as meter reads) passed to it by the oracle is not accurate in the first place.

After validating the identity of the oracle—the only external software permitted to invoke it—the smart contract function credits Alice's blockchain account for the production. That involves either minting tokens denominating energy and its attributes, such as generator type and carbon footprint, or transferring cryptocurrency equal to their local market value. Most presumptive blockchain platforms use their own cryptocurrencies: PowerLedger offers Sparkz, which is

[36] "Power Ledger White Paper," Power Ledger, 2018, https://cdn2.hubspot.net/hubfs/4519667/Documents%20/Power%20Ledger%20Whitepaper.pdf.

[37] Lawrence Orsini and Bill Collins, "Exergy: Electric Power Technical Whitepaper" (LO3 Energy, November 17, 2017), Exergy, https://exergy.energy/wp-content/uploads/2017/11/Exergy-Whitepaper-v6.pdf.

[38] Smart meters deployed today only capture whole site load at the point of interconnection, net of any local energy storage or generation, so this type of envisioned submetering requires novel capabilities.

pegged to local fiat currency, and Grid+ offers BOLT, an aspiring stable currency pegged specifically to the US dollar. By contrast, the Energy Web Chain, a blockchain developed by the Energy Web Foundation (EWF)—a nonprofit consortium founded by Rocky Mountain Institute and startup Grid Singularity—imposes its own utility token but allows application developers to use their own energy and cryptocurrency tokens for transactions.

Assuming Alice is credited with tokenized energy production, she (or her software agent) is free to monetize it in the transactive market. For instance, her agent may sell the energy or its attributes (for example, credits for being low carbon) to Bob's agent in exchange for cryptocurrency. The agent may also sell more complex energy products and services, such as day-ahead energy forward contracts or real-time voltage support, to the utility. Verification of energy services may require additional technical data, such as voltage and power quality, which would be captured by her smart meter. This data could be tokenized along with her energy, which is LO3's approach, or automatically sent to the smart contract governing the service. Compensation would follow only if the physical data is consistent with the service performance requirements, according to the smart contract's measurement and verification rules.

Notably, blockchain solutions for transactive energy do not need to address an entire electric distribution system. Privacy-preserving Energy Transactions, or PETra, for example, is a decentralized control framework for transactive energy on microgrids, developed by Vanderbilt University and Siemens.[39] Microgrids are self-managing subsections of a distribution system that can operate synchronously with the wider electric power system, or disconnected, as an independent island. PETra uses a private Ethereum blockchain, consisting of a microgrid operator node, prosumers nodes representing participating households, and miners. A smart contract broadcasts bids and offers for energy from prosumers, enabling them to bilaterally transact. The model does not achieve physical-to-economic coupling, however, as the operator node can only control the energy and financial assets in participants' accounts. This permits some basic account oversight, but does not meaningfully address system stability or data privacy requirements. Nevertheless, it represents an early, microgrid-targeted solution.

ENERGY DATA ON BLOCKCHAINS

There are several options for representing energy data on a blockchain. The first is tokenization: A unique digital token is minted for each unit of energy produced, which is credited to the producer's blockchain account and from that point on available to buy or sell. The token may include attributes of the energy, such as the generation type, carbon emissions, and power quality, or those attributes may be individually tokenized themselves (the latter is the practice with renewable energy credits today, which are unbundled from the energy commodity). Each type of token would be implemented by a smart contract, which manages token creation, ownership, transfer, and potentially retirement.

Alternatively, energy data may live on the blockchain, but not as a token: It would be maintained either in the state of a smart contract or in the body of a submitted transaction. In either case, the data would be stored and validated by the blockchain but would not exist in a tradeable form. Finally, energy data could be hosted off-chain, in an external database, with only a small, cryptographic hash of the data stored on the blockchain. This hash would enable validation of the externally hosted data without incurring blockchain storage cost and latency but would not enable blockchain-based transactive energy applications to leverage the underlying data.

All of these methods incur ongoing transaction costs, as the submission of data and its access via smart contract are performed through blockchain transactions. Notably, however, the off-chain approach can significantly reduce transaction costs, if hashes of entire datasets are submitted, rather than hashes of individual data.

[39] Karla Kvaternik, Aron Laszka, Michael Walker, Douglas Schmidt, Monika Sturm, Martin lehofer, and Abhishek Dubey, *Privacy-Preserving Platform for Transactive Energy Systems* (January 30, 2017), https://arxiv.org/pdf/1709.09597.pdf.

4. THE BLOCKCHAIN TRADEOFF

The defining features of blockchain discussed above, and the unifying purpose they serve, are the basis on which one must evaluate whether blockchain is appropriate for any given application. In the context of transactive energy, these features amount to what is termed here the blockchain tradeoff, in which the disintermediation of a central authority from a transaction platform—the fundamental goal of blockchain—is achieved at the expense of six costs, which arise from its defining features. These costs are efficiency, scalability, certainty, reversibility, privacy, and governance, and are summarized later in Table 1.

The degree of each cost varies by blockchain implementation, but never vanishes. For some costs, further innovation may nearly eliminate them entirely, such as if ubiquitous energy-efficient computing is realized in the future and renders concerns about blockchain's energy use moot. For other costs, the tradeoffs are more structural and are unlikely to be mitigated with further innovation.

The central question in evaluating blockchain as a platform for transactive energy is whether the blockchain tradeoff is justified. That is, is the disintermediation of a central authority from the transactive energy network worth the costs that blockchain incurs? Evaluating each side of the tradeoff, it is difficult to conclude in the affirmative. This should not be construed as an implicit endorsement of alternative models to blockchain, however, such as centralized cloud hosting, many of which will surely also need to improve significantly if they are to prove satisfactory as platforms for transactive energy.

ASSESSING THE UPSIDE: DISINTERMEDIATION

Disintermediation of a central authority has significant value in contexts in which no such natural authority exists. Examples include joint ventures and supply chains, in which the entities involved are mutually mistrusting and might be unwilling to trust—or to pay—a neutral third party. This disintermediation has questionable value in the context of transactive energy, however, as there exist two undisputed and aligned authorities in power distribution: state regulators and the utilities they oversee. Regulators have clear statutory authority, including the responsibility to see that public policy goals pertaining to energy—such as affordability, reliability, or environmental impact—are met. Utilities are required to operate and maintain the grid, to ensure reliable power delivery and receipt (in the case of distributed generation), and to ensure public safety. It is difficult to assert that customers can rely on utilities for the power running through their wires but not the metering of that power, or billing based on it—particularly when there is a century of precedent for it. It therefore seems highly plausible that the utility or another entity designated by state regulators could act as the sole authority for a future transactive energy platform, possibly contracting out implementation or management but maintaining oversight and control.[40] Notably, all three energy restructuring models put forward by the MIT Energy Initiative in its landmark *Utility of the Future* report feature a centralized market operated by a DSO, recognizing the crucial role this central authority plays in maximizing social welfare.[41]

Despite their clear, central role in retail energy, however, utilities have a public relations problem. Accenture has found that upwards of 76 percent of consumers do not trust their local utility, a finding that weighs on utilities' prospects in a transactive energy future.[42] This sentiment is shared across other sectors as well, in particular toward organizations that have fallen victim to large-scale data breaches.[43] Blockchain offers a dramatic departure from the traditional, centrally managed data model: Rather than entrusting confidential data to individual institutions and relying on their cyber and ethical diligence, data is widely

[40] Richard Tabors, Geoffrey Parker, Paul Centolella, and Michael Caramanis, *White Paper on Developing Competitive Electricity Markets and Pricing Structures* (Tabors Caramanis Rudkevich, April 2016), http://www.bu.edu/pcms/caramanis/NYPSC%20TCR%20WhitepaperApril2016.pdf.

[41] MIT Energy Initiative, *Utility of the Future: An MIT Energy Initiative response to an industry in transition* (2016).

[42] Katherine Tweed, "Survey: 76% of Consumers Don't Trust Their Utility," Greentech Media, July 8, 2013, https://www.greentechmedia.com/articles/read/consumer-trust-in-utilities-continues-to-nosedive.

[43] Céline Fenech, Lisa Hamilton, Simon Borwick, and Ben Perkins, *The Deloitte Consumer Review. Consumer Data under Attack: The Growing Threat of Cyber Crime* (Deloitte, 2015), https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf.

distributed but encrypted. This model relies heavily on publicly validated cybersecurity techniques, trusting them to hide from hackers' data that is in plain sight.

If the transactive market is chosen to be a clearing market, rather than a bilateral one, an argument can be made that a conflict of interest arises for a central DSO. By manipulating prices, such as reporting higher prices for consumption than for generation, market value is created that is not retained by consumers or suppliers, and which could instead become monopoly rent captured by the authority.[44] Conflict of interest concerns such as this can be addressed, however, by regulators prohibiting the DSO from receiving revenue from the market. For instance, surplus payments could be distributed among participants according to a fairness rule. This is a widespread practice in wholesale markets today, with excess revenue (or shortfall) during an interval allocated to participants pro rata based on the size of their obligations, and financial penalties assessed to underperforming resources allocated to resources that overperformed.[45]

While the upside of the blockchain tradeoff is questionable, the impact of its costs is considerable.

WEIGHING THE DOWNSIDE: THE SIX COSTS OF BLOCKCHAIN

Efficiency

Unlike traditional distributed systems, whose resources work cooperatively to solve problems by strategically sharing data and computation to improve the rate of transaction processing, blockchain peer nodes cannot trust each other, and they therefore cannot work together beyond reaching consensus on ledger state.[46] Instead of parallelism, which is the hallmark of distributed systems, what arises is duplication, as the vast network of peers simply replicate each other's data and computation in order to catch fraud. In particular, each peer holds the entire transaction ledger—which, for Ethereum, exceeded 100 gigabytes (GB) in mid-2018—and performs every transaction, including evaluating every line of every invoked smart contract function.[47] In fact, smart contracts and the software libraries they use must be implemented with extra care to make sure that every peer agrees precisely on their outcome, and execute slower and at more complex cybersecurity risk than traditional software code.[48] This amounts to a significant resource inefficiency issue, as a million computers do the work of one. Notably, it is independent of and in addition to the inefficiency of PoW block mining, which pertains specifically to that consensus method.

Replication has important uses in database systems, where it can eliminate single points of failure and reduce bottlenecks in reading and writing data. The extreme degree of replication in blockchain cannot be justified from a resource efficiency or resiliency perspective, however. In light of this, researchers are investigating whether a technique known as sharding can be imported from the field of database systems.[49] In a sharded blockchain, nodes would be responsible for only a portion of the overall data, requiring a new distributed form of consensus and a mechanism for deciding which nodes act to verify which data. Even if such an approach proves possible, however, it is unlikely to resolve the resource inefficiency inherent to blockchain fully: the lack of trust between peers necessarily creates friction in the network, including pervasive validation and replication of transactions.

Scalability

Platform scalability is of the utmost importance to transactive energy, which involves a tremendous amount of data, from meter readings to bids and trades. Consider a network with a million meters, representing a mid-sized metropolitan area. Assuming that all metered site data, including power and voltage, can be bundled into a single blockchain transaction, and that such readings are submitted every fifteen minutes—adequate

[44] Eric Munsing, Jonathan Mather, and Scott Moura, "Blockchains for Decentralized Optimization of Energy Resources in Microgrid Networks," 2017 *IEEE Conference on Control Technology and Applications (CCTA)* (2017), doi:10.1109/ccta.2017.8062773.

[45] ISO New England, ISO *New England Manual for Market Rule 1 Accounting Manual M-28* (March 1, 2017), https://www.iso-ne.com/static-assets/documents/2017/03/m28_market-rule-1-accounting_rev60_20170301.pdf; PJM Interconnection, L.L.C., *Amended and Restated Operating Agreement of PJM Interconnection, L.L.C.* (July 14, 2011), https://www.pjm.com/directory/merged-tariffs/oa.pdf; PJM, *Open Access Transmission Tariff, Attachment DD Reliability Pricing Model* (September 17, 2010).

[46] In proof of stake or authority systems, peer nodes may *temporarily* trust one another in the interest of expediting block validation. However, this is best characterized as an impermanent contingent trust-but-verify system rather than a permanent system of nodes that trust one another by design.

[47] "Ethereum Chain Data Size Growth," Etherscan, https://etherscan.io/chart2/chaindatasizefast.

[48] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor, "Making Smart Contracts Smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), 254-269.

[49] Lucas Mearian, "Sharding: What It Is and Why Many Blockchain Protocols Rely on It," *Computerworld*, January 28, 2019, https://www.computerworld.com/article/3336187/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html.

but conservative for a real-time market—the network would generate over 1,100 transactions per second. This number is termed the network's transaction rate.

A blockchain's transaction rate is the product of its block size (in megabytes) and block rate—the number of blocks mined, on average, per second.[50] Blocks must be shared rapidly between peers for consensus to take place, but peers are constrained by their internet bandwidth. Elevated transaction volumes can delay consensus, and therefore settlement, in the blockchain, since there is more data that must be shared and processed throughout the network per unit time. They also progressively knock peers out of the consensus process that are unable to handle the data volume.

Blockchains maintain strict limits on block size and block rate to mitigate these issues. As a result, Bitcoin is limited to processing around five transactions per second, and Ethereum twenty per second, two orders of magnitude less than what was required for the example transactive network above. Visa's transaction rate is typically quoted as around two thousand per second on average and fifty-six thousand per second as a maximum during peak periods.[51] Google handles at least forty thousand search queries alone in this time, not counting email, text, and file transfer transactions, a testament of what is possible with traditional transaction systems.[52]

Scalability affects permissioned blockchains as well as permissionless ones. The transaction processing speed of the network is proportional not to the number of validators in the network, but to the typical speed of a single validator. Some permissioned chains support private subnetworks of peers, such as Hyperledger Fabric's channels, whose transactions are maintained and therefore validated independently of each other's. This can increase transaction rates to a degree, but it is limited by the number of subnetworks, their exclusivity, and the size of the largest subnetwork—which is itself, of course, just a smaller blockchain, and therefore faces the same scalability challenge. Even under optimal tuning, Hyperledger Fabric can handle an order of magnitude fewer transactions than what is required by the example network above.[53]

While already a formidable challenge, the estimated requirement of 1,100 transactions per second does not include the bids, trades, settlement, and other market activity that accompany the raw energy data. These additional transactions magnify the transaction processing requirements of the platform, widening the gap with blockchain's capabilities. Owing to their likely smart contract complexity, scalability with respect to these transaction types must account for their computational requirements as well as their sheer number.[54]

Blockchain's scalability challenge has a data storage dimension as well. Peer nodes must hold a copy of the entire transaction ledger, so the greater the ledger grows, the fewer nodes are capable of being peers. As of early 2019, for example, Bitcoin had reached 210 GB, growing at a steady rate of 50 GB per year, and Ethereum had reached 130 GB, at an even steeper rate of 90 GB per year, both consolidating control of the network among only the participants with the greatest resources.[55] In the case of transactive energy, storing all historical energy readings for all customers on the blockchain would be prohibitive. Using an optimistic estimate of 100 bytes per transaction (a lower bound for Ethereum), the example network above would produce 10 gigabytes of data per day, or over 3 terabytes per year, quickly swamping all nonspecialized hardware.

Given widespread concern over scalability in the blockchain community, multiple remedies have been proposed. The most popular is to move calculations off-chain, reducing computational demand on the network. Developers of some of the most fundamental blockchain technologies have concluded that blockchain applications should perform as much business logic

[50] Kai Krämer and Sam Hartnett, "When It Comes to Throughput, Transactions Per Second Is the Wrong Blockchain Metric–Energy Web Foundation," Energy Web Foundation, May 10, 2018, https://energyweb.org/2018/05/10/when-it-comes-to-throughput-transactions-per-second-is-the-wrong-blockchain-metric/.

[51] Manny Trillo, "Stress Test Prepares VisaNet for the Most Wonderful Time of the Year," Visas Blog Visa Viewpoints RSS, October 10, 2013, https://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html; *Visa Inc. at a Glance*, PDF, Visa, https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.

[52] "Google Search Statistics," Google Search Statistics—Internet Live Stats, http://www.internetlivestats.com/google-search-statistics/.

[53] Parth Thakkar, Senthil Nathan, and Balaji Viswanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)* (May 29, 2018), doi:10.1109/mascots.2018.00034.

[54] Krämer and Hartnett, "When It Comes to Throughput, Transactions Per Second Is the Wrong Blockchain Metric–Energy Web Foundation."

[55] "Blockchain Size," Blockchain, https://www.blockchain.com/charts/blocks-size; "Ethereum Chain Data Size Growth."

as possible outside of the blockchain, submitting only those transactions for which consensus is necessary.[56] Power congestion and peer-to-peer trading use cases proposed in a recent study by the German Energy Agency (dena) suggest this approach as well.[57]

Blockchain, in other words, should play only a fiduciary role. A technology that seeks to systematize this is Raiden, a software layer added to Ethereum that allows participants to transact indefinitely off-chain, on private, so-called state channels, affording each participant the opportunity to submit the net balance of the transactions for settlement at any time. Grid+, a US-based transactive energy startup, uses Raiden channels for real-time energy payments, for example, avoiding sending every transaction to the blockchain.

Reliance on off-chain computation has two important implications, though. The first is that the role of smart contracts is proportionately reduced, from the engine of complex applications to the more mundane transaction contracts their name suggests. The second is that another, non-blockchain platform is required to host the majority of the data and computation involved in the application. When a market relies on access to real-time data, as is the case in transactive energy, it must obtain it from the second platform, not the blockchain.[58] Both of these implications undermine the original proposition of blockchain as the primary application platform, though they do not rule out a more circumscribed role in the right contexts.

An alternative to off-chain remedies are on-chain ones, in which intensive calculations are exported to external parachains, whose results can be imported back.[59] Technologies such as Polkadot and Ethereum Plasma offer global consensus methods between blockchains, enabling transactions—and therefore computational loads—to be shared between them. As subnetworks of a wider blockchain inter-network, parachains are similar to channels in Hyperledger Fabric, however, and their scalability benefits face similar limitations.

Both on- and off-chain scaling technologies are in their early stages of development—indeed, just as is transactive energy as a concept. Nonetheless, for a scalable transactive market to be successful with so many moving parts and simultaneous evolutions from the current system, these technologies are tenuous anchors on which to hang its success. Even if one approach does prove itself viable, it can only reduce—not eliminate—the resource inefficiency of blockchain, which, as has been demonstrated, relies on data and calculation replication by design. Traditional distributed architectures, in which computing nodes work cooperatively, rather than duplicatively, are more scalable in terms of both data storage and throughput. By the same token, they are also more cost effective from a resource capital perspective.

Certainty

Fundamental to blockchain is that the validity of the transaction ledger is defined by group consensus—something to be voted on, either explicitly or implicitly. While blockchain provides detailed cryptographic methods for an honest peer to determine validity, there is no guarantee that nodes will use it, and not judge transactions based on malicious motivations. Indeed, blockchain consensus methods use combinations of punitive and reward incentives to encourage validators to act honestly, relying on participants' economic self-interest in pursuing these incentives and rationality in following the rules successfully. For example, PoS and PoA rely on participants' concern for the wealth or validator reputation they have staked over ulterior motivations they may have. This basic uncertainty in whether the rules of the network will be followed, or if they will be subverted from time to time by the actions or one or more participants, is a risk that blockchain adds to an application. Public utility commissions may not accept such risk in retail energy payments, or the diffusion of responsibility in transaction processing, requiring instead a single, regulated entity to be legally accountable.

Malicious subversion or manipulation of consensus processes has been rare in the most common of blockchains in use today. Indeed, this is due in no small part to the intrinsic economics of blockchains, in which the selfishness of individual nodes provides the collective computing power needed to run the system

[56] "Account Types, Gas, and Transactions," Ethereum Homestead, https://ethereum-homestead.readthedocs.io/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html; Guy Zyskind, Oz Nathan, and Alex "Sandy" Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," *New Solutions for Cybersecurity* (2015), doi:10.7551/mitpress/11636.003.0018.

[57] Philipp Richard, Sara Mamel, and Lukas Vogel, *Blockchain in the Integrated Energy Transition* (Dena, February 2019), https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2019/dena-Studie_Blockchain_Integrierte_Energiewende_EN2.pdf.

[58] *A Privacy Preserving Virtual Machine Powering Zero-Knowledge Financial Applications* (Ren, 2019), https://renproject.io/litepaper.pdf.

[59] Gavin Wood, Polkadot: Vision for a Heterogeneous Multi-Chain Framework (Polkadot, 2016), https://polkadot.network/PolkaDotPaper.pdf.

and should, in theory, disincentivize manipulation by any single node. However, one under-addressed aspect of blockchain security relates to participants with malicious intent that do not behave as rational economic actors. Consider hostile state or nonstate entities with a goal not of maximizing gains (via the acquisition of cryptocurrency or some other asset), but instead of maximizing damage or destabilization, as is common in cyber attacks (including those on power grids) to date.[60] In this case, attacks that theoretically should not be viable in blockchain systems (because the costs of the attacks exceed the prospective gains) indeed must be considered and prepared for.

Even absent bad behavior, the consensus process itself introduces uncertainty into the state of the ledger. The reason is that consensus plays out over time, as peers share newly forged transaction blocks and must at times decide between competing ones, each offering an alternative update to the ledger. Querying the ledger copy held by a single peer is akin to querying a secondary database in a modern database system—an internal, auxiliary database that is not guaranteed to return the official result of the primary one. Indeed, the documentation for HyperLedger Fabric recommends that applications issue a blockchain query, such as the balance in an account, to more than one peer, given the possibility that results from individual queries may disagree or be out of date.[61]

This type of uncertainty is problematic insofar as, for example, it interacts with established notions of legal settlement finality, a statutory and contractual concept. The Bank for International Settlements notes that, "In traditional systems, settlement finality is a clear and well-defined point in time, backed by a strong legal basis."[62] It is the point at which a transaction becomes, in legal and not just operational terms, "unconditional and irrevocable."[63] While such finality can exist for interbank transfers, checks, wire transfers, and a litany of other extant transaction types, certain blockchain designs may not achieve the same level of finality for legal purposes. For example, if the ledger of a blockchain could ultimately be reversed or revised (regardless of justification) through the relevant consensus process, then some argue that its transactions can achieve at best "probabilistic" settlement, but not "finality" in the legal sense of the term.[64] Retail energy transactions today take place on traditional payment channels; if they are migrated to a blockchain-based system, this ambiguity regarding settlement finality may become a concern.

Efforts are underway to address this challenge. The Dfinity blockchain project, for example, claims to have developed a state-of-the-art consensus mechanism that produces a block every "few seconds" and achieves transaction finality after only two blocks.[65] This would imply an impressive time window of four-plus seconds for finality, though the underlying paper explaining the mechanism leaves out certain key details, including empirical work to substantiate the conceptual claims and quantification of the block size and network latency underlying them. While the improvement may very well prove valid, it will—as with any similar system—take time for new innovative mechanisms to be validated and to prove themselves against exploits. Suffice it to say, however, that the choice of consensus protocol will have significant implications for the timing and degree of certainty of blockchain finality.

Reversibility

The immutability of blockchain's ledger is crucial for the degree of finality that the platform is able to achieve. It also provides a critical shortcut to the validation process: under the assumption that existing blocks cannot change, the existing transaction history can be checked quickly through cryptographic methods, a property that makes blockchain's frequent self-

[60] *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case* (E-ISAC and SANS, March 18, 2016), https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf; Andy Greenberg, "The Highly Dangerous 'Triton' Hackers Have Probed the US Grid," *Wired*, June 1, 2019, https://www.wired.com/story/triton-hackers-scan-us-power-grid/.

[61] Addressing the question of how to guarantee correctness of a ledger query, the Hyperledger Fabric documentation advises, "The client can query multiple peers, compare their block heights, compare their query results, and favor the peers at the higher block heights." In effect, users must sample peer responses to achieve high confidence of correctness, with certainty not guaranteed even if every single peer is queried. See "Frequently Asked Questions," Hyperledger Fabric, 2019, https://hyperledger-fabric.readthedocs.io/en/release-1.4/Fabric-FAQ.html.

[62] *Distributed Ledger Technology in Payment, Clearing and Settlement* (Bank for International Settlements, February 2017), https://www.bis.org/cpmi/publ/d157.pdf.

[63] *Principles for Financial Market Infrastructures* (Bank for International Settlements and International Organization of Securities Commissions, April 2012), https://www.bis.org/cpmi/publ/d101a.pdf.

[64] Nancy Liao, "On Settlement Finality and Distributed Ledger Technology," *Notice & Comment*, Davis Polk & Wardwell LLP, June 9, 2017, http://yalejreg.com/nc/on-settlement-finality-and-distributed-ledger-technology-by-nancy-liao/.

[65] Timo Hanke, Mahnush Movahedi, and Dominic Williams, *DFINITY Technology Overview Series, Consensus System* (2018), https://arxiv.org/pdf/1805.04548v1.pdf.

```
nt( "\n\n Characters in array:" )        acter_array,
                                          number_of_charac
( int character_index = 0 ;
      character_index < number_of_characters ;
      character_index ++ )
{
   System.out.print( "  " + character_array[ charac
}
}
static void print_array( char[] character_array )
{
   System.out.print( "\n\n Characters in array:" ) ;
   for ( int character_index = 0 ;
         character_index < charact
         character_index ++ )
   {
      System.out.print(
   }
}
```

Source: methodshop.com on Flickr

examination feasible, without which even today's modest transaction throughput would not be possible.

But immutability is a double-edged sword, bringing with it amplified consequences of faulty and fraudulent transactions. All such transactions must be reversible in order for the platform to be viable for real-world applications. This concern is most salient at the physical/digital interface, where messy real-world data from devices such as sensors, location trackers, and meters enters the blockchain, but it also applies at the interface with enterprise data platforms, which routinely revise data, with settlement implications.[66]

This matters greatly for energy. A transactive energy future is likely to be a highly automated one. Smart software agents, smart appliances, and third-party energy service providers and aggregators would be responsible for managing residential and commercial energy use in concert with real-time product and service markets.[67] Direct human management would be impractical and, perhaps more importantly, ineffective. All software has bugs, however, and all hardware is susceptible to failure, realities that do not escape intelligent energy management software or the smart devices it depends upon. The result is that participants in a transactive energy network would be exposed to significant risk of bug-induced market transactions, faulty meter reads, or device malfunction, none of which could be directly undone on a blockchain platform. Indeed, as discussed previously, smart contract involvement could trigger knock-on effects that are difficult, if not impossible to unwind. The risks are not only financial, pertaining to the home or business owner, but reputational for the platform, should participants suffer losses and lose confidence in it.

Many transaction platforms today share blockchain's ledger immutability but manage to solve this reversibility problem. Credit card companies and retail banks, for instance, issue corrective transactions to credit an account rather than remove an offending charge. Blockchain platforms can take this tack as well, but it would not be as straightforward. Even a simple

[66] David Livingston, Varun Sivaram, Madison Freeman, and Maximilian Fiege, *Applying Blockchain Technology to Electric Power Systems*, Council on Foreign Relations, July 2018, https://cfrd8-files.cfr.org/sites/default/files/report_pdf/Discussion_Paper_Livingston_et_al_Blockchain_OR_0.pdf; Kevin Stevens, "Why Blockchain Will Power the New Energy Network," Utility Dive, October 23, 2018, https://www.utilitydive.com/news/why-blockchain-will-power-the-new-energy-network/540226/.

[67] do Prado, Qiao, Qu, and Agüero, "The Next-Generation Retail Electricity Market"; *Transactive Energy: Real-World Applications for the Modern Grid* (Smart Electric Power Alliance, April 2019).

token transfer may not be easy to reverse if it causes the sender's balance to fall below a threshold, triggering a smart contract that registers a default or invalidates a prior purchase of goods.

Indeed, smart contracts can cause a cascade of effects that render the consequences of a transaction more complex and widespread than that of a simple balance transfer. Interdependencies between smart contracts and the arbitrary complexity of their internal state, moreover, make those effects harder to unwind. Each smart contract must be designed with its own unwind mechanisms—modifying internal state as appropriate—which must work in concert with those of others to ensure a mutually consistent and correct ledger state after a roll-back. Such coordination is possible, but it would be challenging under a platform model that supports independently developed third party applications.

Transactions are not the only elements in a blockchain that require correction. Smart contracts themselves may contain software bugs or security vulnerabilities, which are discovered only after they are deployed on a blockchain. Indeed, due to the unique manner in which blockchain peers execute software code, often on unsecure machines, smart contracts operate with novel cybersecurity and correctness risks compared to traditional transaction software.[68] For blockchains such as Ethereum, in which smart contracts themselves are submitted in transactions, immutability means that contracts cannot be patched (retroactively addressed) like traditional software even after defects or vulnerabilities are found.[69]

Privacy

THE TRANSPARENT PRIVACY PROBLEM

The Need for Market Data Access

Nearly all blockchain consensus protocols require a significant degree of transparency for ledger contents, implying a potential trade-off with privacy. If a validator node cannot track the balance in an account or the internal state of a smart contract, it cannot verify whether the account is overspent or how the smart contract should behave when invoked. The degree of data access possessed by individual participants varies from permissionless blockchains, such as Ethereum, where all participants can see all data, to permissioned blockchains, where only validators have this level of access, and others are restricted by organization or role.

In the case of transactive energy, it is critical that customer energy data be accessible by the market, both for settlement of trades and local determination of price. For example, the market must know about elevated voltage at a meter in order to reduce the price of both real power—disincentivizing distributed generation, which exacerbates such conditions—and reactive power, which is critical for maintaining stable grid voltage. It must also have access to production and consumption data in order to settle obligations. The distribution utility must have access to energy data as well, in order to track the physical state of the network and ensure stability.

The Need for Energy Data Confidentiality

To skeptics of centralized control of data, blockchain's transparency is a welcome alternative to the information asymmetry between traditional platform authorities and their participants.[70] For many applications, however, including transactive energy, it could be deeply problematic. The Energy Web Foundation's D3A transactive energy model, for example, identifies the seeming paradoxical challenge of broadcasting market information to participants while shielding the sensitive information it derives from transparent privacy.[71]

The risks posed by data visibility are not always evident. For example, the price at which one bids in an energy market, or the hourly energy consumption of a home, may appear innocuous. But advances in energy disaggregation—a field of machine learning—can yield invasive insights into the behavior of the occupants, including when they are home, wake up and go to sleep, and are eating or exercising, by detecting lighting and appliance use.[72] Even more consequential, visibility of certain types of data, such as financial and electrical power system data, pose security risks to institutions,

[68] Luu, Chu, Olickel, Saxena, and Hobor, "Making Smart Contracts Smarter," 254-269.

[69] Ibid.

[70] *Building Block(chain)s for a Better Planet* (September 2018), World Economic Forum, http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf.

[71] Peter Bronski, Jon Creyts, Sheila Gao, Sarah Hambridge, Sam Hartnett, Ewald Hesse, Jesse Morris, Rushad Nanavatty, and Neil Pennington, *The Decentralized Autonomous Area Agent (D3A) Market Model* (Energy Web Foundation, 2018), https://energyweb.org/wp-content/uploads/2018/04/EWF-D3A-ConceptBrief-FINAL201804.pdf.

[72] K. Carrie Armel, Abhay Gupta, Gireesh Shrimali, and Adrian Albert, "Is Disaggregation the Holy Grail of Energy Efficiency? The Case of Electricity," *Energy Policy* 52 (2013): 213-34, doi:10.1016/j.enpol.2012.08.062.

governments, and physical infrastructure.[73] Storing sensitive grid data publicly is a clear impossibility: the ambitions of US adversaries to identify and exploit vulnerabilities in its power distribution networks are well known.[74] Energy data must therefore be encrypted on the blockchain, but in such a way that it can be validated by the network and visible to the market. The EWF raises the question in its white paper on the energy web chain of whether blockchain is appropriate at all in such circumstances, when privacy is required beyond a small group of transactors.[75]

Blockchain Anonymity Is Not Sufficient

One of the attractive attributes of blockchain networks is that participants are afforded considerable anonymity. Rather than personal information, participants are identified via random cryptographic address. This anonymity has its limits, however, as there is nothing to prevent the reverse-engineering of identities from transaction data, a fact with important (positive) implications for anti-money laundering efforts. The concern becomes more acute with applications such as transactive energy, in which data must be tied to a small geographic area, such as a microgrid or distribution feeder. Put simply, the anonymity of cryptographic addresses is insufficient when rigorous data privacy is required.

If energy data is stored exclusively off the blockchain, then market price formation and settlement must occur off-chain as well, significantly reducing blockchain's role in the transactive marketplace. Assuming, to the contrary, that such data is stored on the blockchain—likely in addition to off-chain utility storage—one runs headlong into the transparent privacy problem.

CRYPTOGRAPHIC TECHNIQUES TO SOLVE TRANSPARENT PRIVACY

In spite of its apparent intractability, three techniques to solve transparent privacy exist and are under development. Each aims to provide validators the tools they need to verify transactions, including smart contract invocations, while shielding the details of the transaction themselves, including the identities of the parties involved. They take subtly different tacks: zero-knowledge proofs allow transacting parties to cryptographically prove to validators that they carried out a smart contract correctly, without revealing any of its inputs or outputs; multi-party computation (MPC) allows a network of untrusted computers to collectively carry out smart contracts, using only cryptographic references to the data; and secure hardware enclaves, built within specialized computer processors, offer an isolated environment for an untrusted computer to operate on private data, to which not even the computer's operating system has access.

Details of these techniques, examples of their usage in blockchains today, and analyses of their strengths and weaknesses are discussed in the appendix. Zero-knowledge proofs and MPC enjoy significant privacy guarantees but are presently very limited in regard to the complexity of the applications they can shield and the computational overhead they impose. Significant theoretical developments would be required to overcome these limitations, followed by engineering and commercial development to make them viable for real-world applications, rendering these techniques a research direction for blockchain rather than a near-term solution. Secure enclaves have the opposite profile: they are commercialized today, by such major chip developers as Intel and ARM, but insufficient security guarantees have exposed high-profile vulnerabilities, raising questions as to their fitness for hosting the sensitive energy and financial data required for transactive energy. Secure enclaves are also inferior to the foregoing techniques in the sense that the sensitive data is actually decrypted within the enclave, presenting a theft opportunity to a malicious third party, whereas under normal operation of zero-knowledge proof systems and MPC no data is ever decrypted.

LEVERAGING THESE APPROACHES FOR TRANSACTIVE ENERGY

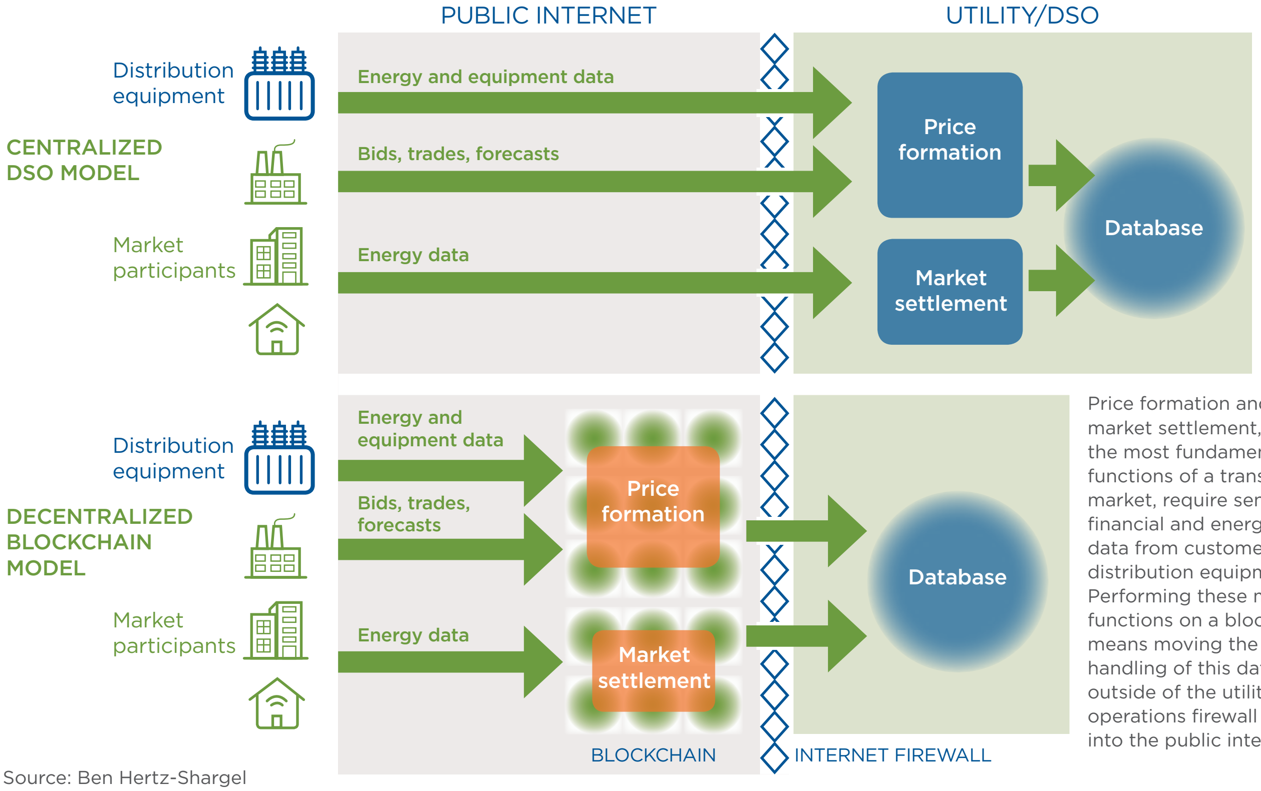
Despite their present limitations, these three cryptographic techniques offer blockchain a way forward to achieve transparent privacy in transactive energy applications. For the basic requirement of validating transactions encrypted on the blockchain, two approaches present themselves. The first is for oracles, perhaps embedded in smart meters, to submit encrypted data such that it can be decrypted by validators only within secure hardware enclaves.

[73] Richard J. Campbell, *Electric Grid Cybersecurity,* R45312 (Congressional Research Service, September 4, 2018).

[74] Lily Hay Newman, "Russian Hackers Are Still Probing the US Power Grid," *Wired*, November 30, 2018, https://www.wired.com/story/russian-hackers-us-power-grid-attacks/.

[75] *The Energy Web Chain: Accelerating the Energy Transition with an Open-Source, Decentralized Blockchain Platform* (Energy Web Foundation, October 2018), https://energyweb.org/wp-content/uploads/2018/10/EWF-Paper-TheEnergyWebChain-v1-201810-FINAL.pdf.

Figure 3: Confidential Data Management Under Blockchain and a Centralized Authority



Price formation and market settlement, the most fundamental functions of a transactive market, require sensitive financial and energy data from customers and distribution equipment. Performing these market functions on a blockchain means moving the secure handling of this data outside of the utility/DSO operations firewall and into the public internet.

Source: Ben Hertz-Shargel

This would enable validators to perform their jobs nearly identically as they do on public blockchains today, but without visibility into third-party energy or financial data. The downside of this approach is the number of peer nodes that must be provided access through enclaves, which collectively present a broad, open surface for cyberattack, as well as its reliance on secure enclaves themselves, which have thus far proven themselves insecure.

The second approach to validation is for oracles to submit an encrypted blockchain transaction as well as a zero-knowledge proof of its correctness, which could be publicly checked by validators. This approach enjoys what are likely to be stronger security guarantees from zero-knowledge proofs compared to secure enclaves, and it avoids data decryption altogether.

In short, blockchain consensus may indeed be able to accommodate encrypted energy data. Leveraging that data for transactive market processes is more problematic, however. The case of a centralized market, rather than a bilateral one, is considered here because of the considerations put forward earlier in the report: it is both the closest analog of wholesale markets today and the market design that can most clearly support the integration of grid state into price formation. It is more speculative whether a bilateral market, exchange-hosted or peer-to-peer, could similarly combine grid state with customer supply and demand in price formation, and what additional assumptions would be required to enable this.

For a centralized market to be run on-chain, via smart contracts, it must operate on encrypted customer energy and financial data, as well as sensitive grid state data, without publicizing it. MPC is a candidate approach for this, but its computational runtime and limited expressiveness rule it out in practice, at least at present. Secure enclaves appear to be the only alternative, but the prospect of a network of third party-owned computers decrypting a market's worth of sensitive energy and financial data outside of an enterprise firewall would unlikely be acceptable to regulators or other stakeholders.

One therefore reaches the conclusion that a centralized market with encrypted data must be run off-chain.

The DSO operating such a market could avail itself of much more powerful and convenient computation tools than are possible on a blockchain, while still leveraging blockchain as a ledger of public record. Market processes such as security-constrained economic pricing runs, where locational prices and energy awards are determined, would operate on sensitive grid and customer data (obtained from the blockchain or a separate source) and submit their results to a blockchain. These transactional results would be encrypted to ensure financial privacy and validated using one of the techniques discussed above. Settlement would occur as the fulfillment of these transactions, in which customer energy data, such as power consumption and voltage readings, are evaluated against market or bilateral obligations, with customers charged or compensated for the difference based on locational price.

Crucially, however, while it is feasible for the DSO to submit zero-knowledge proofs as to the correctness of market transactions—for instance, that token inputs sum to outputs—it is highly unlikely that the DSO could submit a zero-knowledge proof of the market process that produced those transactions. The reason is that distribution market algorithms are likely to be even more computationally intensive than wholesale market algorithms, already massive mathematical optimizations over millions of physical and financial variables and would need to be performed at the same five- or fifteen-minute frequency. Generating a zero-knowledge proof of the distribution market algorithm in that time frame—which takes longer than the algorithm itself, even before accounting for the fact that every single intermediate variable must be retained—is very likely intractable.[76]

An off-chain DSO market that submits proofs of transaction correctness but not market processes themselves cannot be said to derive much benefit from the blockchain. On one hand, the determination of wealth transfer is happening through the market process, which is opaque to the blockchain. Validating the resulting transactions alone is akin to a casino-monitoring card players but not the dealer. On the other hand, the DSO would be a tightly state-regulated entity, either with nonprofit status such as today's wholesale ISOs and RTOs or constituted so as to be financially ambivalent as to market outcomes. Even if zero-knowledge proofs of DSO market processes were technologically attainable, the research and development cost to achieve them would far outweigh the marginal public benefit of validating every digital step of such an entity. Basic transparency requirements, business controls, and oversight would likely suffice, justified by the behavior thus far of the ISOs and RTOs.

Governance

The one time a blockchain can be modified is during a fork, which raises a governance problem with implications for energy applications. Blockchain forks are categorized as either hard or soft. Soft forks are software upgrades that are backwards compatible, in the sense that even peers that have not upgraded will recognize blocks produced by those that have as being valid. An example is reducing the maximum allowed block size, which keeps the set of admissible blocks within the set accepted by non-upgraded peers. Hard forks, conversely, are not backward compatible. Peers that have upgraded and those that have not will disagree over which blocks are valid, leading them to recognize different blockchains moving forward.

Historically, blockchain forks have been proposed and marketed by the community developing the software, and are adopted based on stakeholder majority, since that majority determines consensus. Several recent blockchains, such as Tezos and Decred, have attempted to systematize this ad hoc process, with the aim of promoting more ordered governance and reducing contentious outcomes.[77] Retail energy markets are governed by state regulators, however, not the blockchain community. It stands to reason then that regulators should be the sole arbiters of transactive platform forks, established through the same public proceedings that govern rulemaking today. It is not clear how this policy could be enforced, however, unless a majority of stake in the network is retained by state-aligned central authorities, violating a basic blockchain tenet.

By contrast, it is possible that blockchain's distribution of authority across the network could be problematic for transactive energy, both from an operational and a regulatory perspective. Recall that under the assumed model, validator consensus determines the transaction settlement as well as the system of record for energy production and consumption. This raises the question of whether a utility and DSO—if independent—can ensure reliable service and public safety at minimal cost if they do not have full determination over the validity

[76] See appendix.

[77] Cade Metz, "A Plan to Save Blockchain Democracy from Bitcoin's Civil War," *Wired*, March 29, 2017, https://www.wired.com/2017/03/plan-save-blockchain-democracy-bitcoins-civil-war/; Jacques Y, "Apples to Apples, Decred Is 20x More Expensive to Attack than Bitcoin," CryptoCanucks, November 29, 2018, https://cryptocanucks.com/apples-to-apples-decred-is-20x-more-expensive-to-attack-than-bitcoin/.

of energy transactions or even what activity took place. For example, if blockchain consensus rejects a customer meter reading, whether submitted as a well-formed and signed transaction or not, how should the utility interpret this? Should it accept the votes of the third-party validator nodes over the hardware that generated the reading? This situation may not be frequent, but it highlights the systemic change blockchain would introduce to electric grid operations, in which the votes of network participants, not utility hardware, provide the system of record of energy consumption and production.

Numerous questions follow. Are blockchain nodes operated by retail customers entitled to invalidate transactions related to other customers, or to the utility? In a permissioned network governed by organizations such as retail energy providers (REPs) and energy service providers, perhaps by PoA, should these organizations be permitted to resolve their own disputes through their validator nodes, rather than courts and regulators? Practically speaking, how would these authorities involve themselves in automated, distributed processes in the first place? Finally, consensus protocols typically treat validators as equals, but equating utilities, REPs, application developers, and individual customers may be problematic. If authority is distributed among these and other network participants, how should it be allocated, and on what basis? As an example, EWF's Energy Web blockchain would be governed solely by blockchain application developers, granting this group only the power of dispute resolution and the determination of ground truth. Validator votes would be allocated in proportion to application usage, a mechanism outside of regulator control which EWF acknowledges may be too simplistic to ensure balanced governance.[78]

One uncertainty to be further resolved—though not central to the tradeoffs that form the focus of this paper—is the evolving regulatory approach of financial regulators with regard to the determination of whether tokens and similar digital assets constitute financial securities and are thus exposed to relevant regulation. While the US Securities and Exchange Commission (SEC) recently issued guidance on this question, the guidance provides an analytical framework but not a conclusory test.[79] With other important jurisdictions at similar points of evaluation of the treatment of digital assets on blockchains, final resolution of key questions in this domain remains elusive.

WEIGHING THE TRADEOFF

These are the costs that blockchain incurs to secure transactions absent a central authority. Individually, they may be tolerable for an application: a future sharding technology may reduce resource inefficiency, an off-chain state channel solution might improve scalability, and role-based data access in a permissioned blockchain may be sufficient to allay privacy concerns. Ultimately, however, the application sponsor must weigh the sum of these costs and the challenges they add to implementation against the value added by the disintermediation of a central authority to determine if blockchain is the right tool for the problem. It is for this reason that many projects underway today are very intentionally designed to keep sensitive data, such as energy consumption, and significant computation loads off-chain.

Many of the foregoing costs incurred by the blockchain tradeoff are reduced as the blockchain platform architecture centers more authority in fewer entities, which can utilize system resources more efficiently, shield and manage data more flexibly, and act in line with retail market regulators. Such an architecture would represent a compromise between blockchain and traditional centralized architectures today. Alternatively, the decentralized character of blockchain could be retained by limiting its scope to application areas in which the six costs have minimum impact, for instance in light of infrequent transactions and nonconfidential data. This would represent a selective, rather than comprehensive, role for blockchain technology in the power sector, recognizing that blockchain is but one tool in the toolbox toward a more transactive and modern grid, rather than a silver bullet for all circumstances.

COMPARING OTHER BENEFITS OF BLOCKCHAIN TO TRADITIONAL APPROACHES

While the core tradeoff offered by blockchain has questionable value to transactive energy, it has other compelling attributes, ranging from the elimination of platform intermediaries to a simple third-party development model. Often touted as game-changing for applications, the reality of these attributes is often more nuanced, including their uniqueness to blockchain.

Perhaps most closely associated with blockchain are

[78] *The Energy Web Chain: Accelerating the Energy Transition with an Open-Source, Decentralized Blockchain Platform* (Energy Web Foundation, October 2018).

[79] "Framework for 'Investment Contract' Analysis of Digital Assets," US Securities and Exchange Commission, April 3, 2019, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

Table 1: The Six Costs of Blockchain

COST	DESCRIPTION	TRANSACTIVE ENERGY PAIN POINT	MITIGATION
Efficiency	Duplication of data storage and processing, such that an entire network of computers does the work of one.	Increased capital costs, through under-use of machines hosting the transactive network.	A structural feature of the technology, so difficult to address. Speculative techniques to divide, or shard, the ledger have been proposed.
Scalability	Blockchains support a fraction of transaction volume of modern platforms and increasingly require specialized computing resources.	Support for a realistically sized transactive network and realistic transaction rates.	Techniques exist that can move data and computation off-chain, but this reduces on-chain data access and smart contract functionality.
Certainty	Consensus protocols rely on rational economic behavior, can take long to complete, and may not meet legal settlement criteria.	Transactions are likely to occur at a 15-minute frequency or higher, so they must be settled quickly and with legally enforceable finality.	Early cryptographic research suggests techniques to quicken and strengthen finality, but 51% attacks remain a major risk.
Reversibility	Blockchain's immutability makes it difficult to unwind complex smart contract transactions, and software bugs cannot be patched.	Transactive markets will be viable only if routine incorrect and fraudulent transactions can be unwound, and software bugs fixed.	Little attention or efforts have been devoted to this issue.
Privacy	Participants and utilities require data privacy while peers require data access to validate the ledger.	Financial transactions, market bids, energy consumption data, and other confidential data must be hosted by the market platform.	Cryptographic approaches exist but require significant theoretical advancement to meet transactive energy's needs.
Governance	Blockchain's governance is inherently distributed, posing both policy and enforcement challenges to regulators.	Distributed governance is at odds with the statutory authority of state regulators over retail energy markets and their rulemaking process.	A novel paradigm that marries blockchain's distributed consensus with centralized, state-level governance is required.

its transaction integrity guarantees. Energy market participants can be confident that smart contracts will charge them fairly for energy consumed and compensate them fairly for DER energy produced. Customers already enjoy strong guarantees from traditional transaction networks, however, such as online brokerages and marketplaces, which often guarantee deposits and absorb fraud liability. Both blockchain and traditional networks, however, share the risk originating from the smart meters, electric vehicle chargers, and other devices that submit transactions to them on customers' behalf, which could be compromised. Cyberattacks targeting internet-of-things (IoT) devices became a widespread concern with the Mirai botnet attack in 2016 and remain one today, with vulnerabilities being discovered in each generation of hardware.[80] Blockchain offers no protection or guarantees at the physical-digital interface, relying on the trustworthiness of oracle hardware and software. As has been noted, it is at a distinct disadvantage with such vulnerabilities as it may not be able to unwind the consequences of fraudulent transactions made during an attack. The concentration of risk at the physical edge of a blockchain network warrants close regulation and a certification regime of oracle devices, which prompts the question of why the entity(ies) entrusted with certification—and therefore ultimately the security of the network—cannot be entrusted with the management of the network itself.

Once submitted to the network, blockchain's integrity guarantees for transactions are strong enough that they do not require audit verification. In fact, blockchain is often credited with eliminating transaction costs to

[80] Josh Fruhlinger, "The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet," CSO Online, March 9, 2018, https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html; Lindsey O'Donnell, "Security Glitch in IoT Camera Enabled Remote Monitoring," *Threatpost*, July 27, 2018, https://threatpost.com/security-glitch-in-iot-camera-enabled-remote-monitoring/134504/; Newman, "Russian Hackers Are Still Probing the US Power Grid."

middlemen such as platform providers and brokers, as well as auditors, reducing market frictions and increasing efficiency. The accuracy of this claim comes down to semantics, however. The transaction fees normally collected by a central platform provider are instead collected by the validator nodes who process the transactions and who, collectively, do act as platform providers for other users. Such fees are subject to raw supply and demand on permissionless blockchains, and have demonstrated not only severe volatility but growth that has called into question the feasibility of blockchain for microtransactions—a key requirement for transactive energy.[81] There is no indication that blockchain fees for retail energy transactions, whether on permissioned or permissionless platforms, would be less expensive or variable than those collected by a centralized energy platform provider. A central provider might additionally be more capable of managing transactions according to regulator policy goals, such as reduced fees for low income residents.

Regarding brokers, they may have as robust a roll to play in a blockchain-based market as in traditional markets today. Smart contracts offer the automation necessary to match buyers with sellers and arrange multi-stage and multi-party transactions, but such contracts would be complex, enterprise-grade distributed applications. It is possible that, based on the nature of the energy market, versions of such applications will be embedded into the platform and provided for free, but it is equally possible that a market for paid versions will develop, offering superior features and performance in exchange for a fee. Notably, freeware does not dominate any of today's major online broker marketplaces, with developers unwilling or unable to compete with for-profit applications developers such as Kayak, E-Trade, and StubHub. Whether they capture revenue on the buy or sell side, brokers have a role to play in any sizable market.

The openness of blockchain to third-party application developers seeking to build on the underlying transaction platform is a central aspect of the technology. The flexibility of smart contracts, paired with secure, real-time and historical access to an entire corpus of microtransactions has the potential to foster energy service and financial innovation. Importantly, though, peer-to-peer transactions, smart contracts, and third-party applications can still be supported if validation by consensus is eliminated. These features are independent of the underlying platform architecture, including its degree of centralization, and do not constitute a reason to prefer blockchain. The iOS and Android mobile platforms, for example, support third-party applications that let customers instantly transact with text, photos, videos, and money via the data, hardware, and application programming interfaces (APIs) they expose. Facebook, Samsung SmartThings, and Apple HomeKit are other examples, offering application developers access to social media and smart home data and transactions. Recalling that smart contracts are just software libraries with internal state data, written in a general-purpose programming language, they represent just one kind of third-party application possible on traditional platform architectures.

The only defect of the foregoing models with respect to transactive energy is that the central platform authority is a commercial entity, the type blockchain justifiably seeks to disintermediate. They represent viable alternatives to blockchain if the authority is instead a state regulated entity, with platform implementation only contracted out to commercial vendors. It remains to be seen, however, whether a business model can be established that incentivizes implementor innovation comparable to the example platforms while extracting minimal value from the network.

A final attribute of blockchain worth careful consideration is its claimed facility for microtransactions. Some of the most breathless testaments to the technology imply that it is capable of ingesting transactions at a speed and scale that enables entirely new distributed applications. Evaluations of blockchain's scalability and resource efficiency, however, suggest it is in fact uniquely unsuited to microtransaction-based applications, or at least is less suited than modern client-server architectures. Google is able to instantly respond to the forty thousand search requests it gets on average per second, in addition to comparable numbers of emails, text messages, and file downloads, because such transactions do not need to be processed by every server in its data centers. Numerous mobile, social, and IoT platforms today process high volumes of data transactions across vast numbers of devices, leveraging the same type of massively parallel architecture. Blockchain's trust-by-replication model is manifestly less scalable and efficient, and therefore at a disadvantage for microtransaction applications such as transactive energy.

[81] Paul De Martini and Lorenzo Kristov, *Distribution Systems in a High Distributed Energy Resources Future* (Future Electric Utility Regulation, October 2015), https://emp.lbl.gov/sites/default/files/lbnl-1003797.pdf.

Lafayette Public Power Authority. Source: American Public Power Association on Unsplash

A DIFFERENT CONSENSUS FOR TRANSACTIVE ENERGY?

Blockchain is a model for decentralized control of a transaction ledger. What is considered decentralized is the determination of the history and present state of the ledger, achieved through participant consensus. This type of control is sometimes conflated with the decentralized control required in applications such as transactive energy, in which the energy consumption and production behavior of individual participants must be coordinated so as to collectively balance the electric grid. Blockchain's decentralized ledger control, in fact, has no direct relation or contribution to the kind of intelligent grid and energy market management required for transactive energy, which may ultimately limit its usefulness as a platform.

Decentralized control models do exist for transactive energy, which are fundamentally different from blockchain in that participant computational nodes work cooperatively, not duplicatively, enabling not only power flow optimization but customer privacy. One prominent example is proximal message passing, a mathematical model for grid management developed in the academic machine learning community.[82] The model does not prescribe the operation of a transactive market, but rather accepts a complete specification of an electric grid network, complete with customer and utility assets, as well as objectives and limitations for those assets, and optimizes power flow across the network to collectively maximize the objectives. Time- and location-specific shadow prices for power and other constrained quantities emerges from the optimization as it does in the optimization performed by wholesale

[82] Matt Kraning, Eric Chu, Javad Lavaei, and Stephen Boyd, "Dynamic Network Energy Management via Proximal Message Passing," *Foundations and Trends® in Optimization* 1, no. 2 (2013): 70-122, doi:10.1561/2400000002; Elli Ntakou and Michael Caramanis, "Distribution Network Electricity Market Clearing: Parallelized PMP Algorithms with Minimal Coordination," in *53rd IEEE Conference on Decision and Control* (2014), doi:10.1109/cdc.2014.7039642.

markets, offering potential real-time prices to expose to participants. What is significant about the optimization, beyond the fact that it achieves the core economic-to-physical coupling required for transactive energy, is that it does not need to be performed centrally, but can instead be distributed: each node performs a private optimization based on its personal objectives and the results of optimizations performed by its neighbors on the grid. In this way, a global solution can be found without any customer knowing the behavior or objectives of any other customer. Mathematically, this is known as a consensus method (not to be confused with blockchain's validation consensus), because the global solution emerges from the mathematical negotiation of neighboring nodes of their shared conditions, such as the voltage and current on a distribution feeder.

Proximal message passing addresses the key distributed control problem for transactive energy, and yet it is independent of the degree of centralization of the underlying transactive platform. It could be implemented in a client-server architecture, for instance, in which software clients, embedded within smart meters and other grid assets, perform the local optimizations and communicate the results to a central utility server. The server would share the results between neighboring nodes, ensuring privacy not only for customer data but sensitive distribution equipment data, which should only be seen by the utility. It could also be implemented in a decentralized architecture, in which neighboring clients communicate in direct, peer-to-peer fashion over a secure network, such as the utility's field area network.

While blockchain's distributed consensus does not contribute to the decentralized control of a transactive grid, it is not incompatible with it either. Decentralized models have been developed for blockchain as well, seeking to increase the transparency of the power flow optimization process. In one example, participants optimize their local objective off-chain, sharing the result with a central smart contract which acts as a data aggregator.[83] The aggregator performs a global update, passing local values back to participants for further optimization, a process that continues until convergence. This example, however, showcases some of the challenges introduced by blockchain. Using a smart contract as the data aggregator means the grid state is publicly visible to all peers, including sensitive distribution equipment data—a network vulnerability. Moreover, solving the simplified power flow optimization for a small test network of fifty-five nodes on a dedicated Ethereum blockchain took three minutes for the study authors, performance that would be far from adequate in the face of realistic power flow formulations and network sizes, and is not competitive with centralized techniques.[84] These are reminders that blockchain decentralized control applications are subject to the same blockchain tradeoff as other applications.

No academic consensus exists today that control of distributed resources in a smart grid should be decentralized in the first place. Decentralization has the potential to offer significant benefits, including resilience to node failure, simplicity of operation, and scalability. But initial studies have suggested that optimal approaches may have both centralized and decentralized elements, and given the successful track record of centralized approaches in wholesale markets, significant effort has gone into extending these techniques to distribution markets.[85] Centralized approaches inherently rely on less network communication, a significant source of latency, and can leverage economies of scale in data processing with specialized hardware and computer code. Decentralized approaches would rely on remotely deployed utility hardware or, more fraught, consumer hardware, which may be less reliable, manageable, secure, and consistently network-connected. The prospect of migrating critical utility systems to customer hardware communicating over a local broadband connection may give pause to many utilities. Nevertheless, intermediate solutions exist, which are neither fully centralized or decentralized, organizing the grid into hierarchical layers that interact only with the neighboring layers above and below.[86] These approaches would reduce reliance on customer hardware but require highly specialized control software.

[83] Munsing, Mather, and Moura. "Blockchains for Decentralized Optimization of Energy Resources in Microgrid Networks."

[84] Ibid.

[85] Ntakou and Caramanis, "Distribution Network Electricity Market Clearing: Parallelized PMP Algorithms with Minimal Coordination."

[86] Kristov, Martini, and Taft, "Designing a Decentralized Transactive Electric System."

5. POLICY RECOMMENDATIONS

The appraisal of blockchain's current trade-offs in transactive energy applications is meant to serve not as an indictment, but instead as a focusing mechanism. It is intended to draw the attention of interested stakeholders, including policymakers and regulators, to the areas where blockchains will need further innovation and refinement in order to be fit for purpose in a transactive energy future, and to point out those dimensions in which blockchain is unlikely to evolve to such a place at all due to fundamental design. These fitness determinations are likely to be application-specific, based on scalability, privacy, and other needs. When armed with a sound and dispassionate analysis of these trade-offs, decision-makers in the energy sector will then be well-suited to determine where, how, and when to deploy blockchains for transactive energy applications, and where other approaches may be preferable.

For a technology area that is still very much in its infancy, it can be difficult to make the case for a significant or muscular role for policy in various applications of blockchain to transactive energy. There is rightly an aversion to overburdening under-resourced start-ups and programmers while their products and services are still very much a work-in-progress, or to targeting with policy certain technologies that may evolve significantly in how they interact with firms, consumers, and markets. In other words, there is a strong case for allowing "regulatory sandboxes" that would enable technology demonstration at manageable scales.[87]

Nonetheless, there is still a case for certain policy tools—including government-directed research funding and standards development processes—to encourage the development of platforms for transactive energy that build technical solutions to the challenges identified in this paper. Such approaches need not exclude blockchains, but nor should they focus exclusively on them. Indeed, though technology agnosticism is not always a defensible public policy approach when it comes to capital-intensive technologies or markets with high barriers to entry, it is arguably the perfect approach when it comes to the digital platforms being developed to facilitate transactive energy markets.

This could be done through incentives that are direct, such as funding from the Department of Energy's Advanced Research Projects Agency-Energy (ARPA-E) innovation program, or that are indirect, such as the promulgation of new market rules and standards. As an example of the latter, the Federal Energy Regulatory Commission (FERC) could establish rules for transactive energy markets as they have for wholesale markets, providing clarity on thorny issues involving market design, participation, and price formation, thereby offering commercial certainty for eligible participants. The National Institute of Standards and Technology (NIST), moreover, could establish technological standards that help the market determine which platform technologies are most credible, secure, and cost-effective, and therefore worthy of investment.

Regardless of which policy mechanism is used to generate these incentives, it is advisable that transactive energy platforms, whether blockchain-based or not, are designed to achieve maximal scope for transactive energy applications, while overcoming or minimizing the six costs identified in the blockchain tradeoff. One could imagine that under a prize-based system (for example, an Xprize for transactive energy systems), requirements could include:

- **Scalability:** Support a transaction volume on the order of one meter read and one market transaction per customer (meter) per every five minutes, assuming a moderately sized distribution network with a given number of participants. This requirement could be strengthened to support more computationally intensive transactions and infrequent peak transaction volumes.

[87] Livingston, David, Varun Sivaram, Madison Freeman, and Maximilian Fiege, *Applying Blockchain Technology to Electric Power Systems*, Council on Foreign Relations, July 2018, https://cfrd8-files.cfr.org/sites/default/files/report_pdf/Discussion_Paper_Livingston_et_al_Blockchain_OR_0.pdf.

- **Efficiency:** Prove the ability to meet the aforementioned scalability benchmark at minimum capital cost per transaction per unit time, accounted for across the network. While capital cost will have a different structure and set of dynamics depending on the technology employed (for example, blockchain vs. more traditional platforms), a comparison across platforms should nonetheless be possible.

- **Reversibility:** Provide for unwinding faulty or fraudulent transactions and their consequences, such as due to meter defect or fraud, and prove the ability to similarly unwind any relevant cascade of smart contracts triggered in the interim. Where third-party applications (including smart contracts for blockchain) interact with the platform, this would require an operations/governance model that ensures unwinding support regardless of how the app ecosystem evolves. Moreover, this should be guaranteed without compromising the integrity of the aforementioned finality features of the platform.

- **Privacy:** Demonstrate that confidential data that is necessary for transactive energy, such as metered energy data, market bids, and financial transactions, can be both validated and available to the market while remaining private and secure.

- **Governance:** Identify the appropriate level of power over key governance functions (verifying transactions, changing market rules, so on) for each participant in a given market. For actors that might play a role in an underlying platform but who play no formal role in the underlying market (for example, miners that lend their computing power to a public blockchain but are not actually participants in the underlying energy market that it is serving), establish a clear set of criteria for justifying inclusion/exclusion.

Regardless of the degree to which a future transactive energy system relies on a blockchain platform, if at all, there are a number of key steps that policymakers can take to help facilitate transactive energy systems that benefit the grid and society as a whole. While such measures would in most cases also help pave the path for a quicker road to impact for blockchains if they are able to meet the requirements noted above, these measures would confer broad benefits even in the absence of significant uptake of blockchains in transactive energy. Such measures could include:

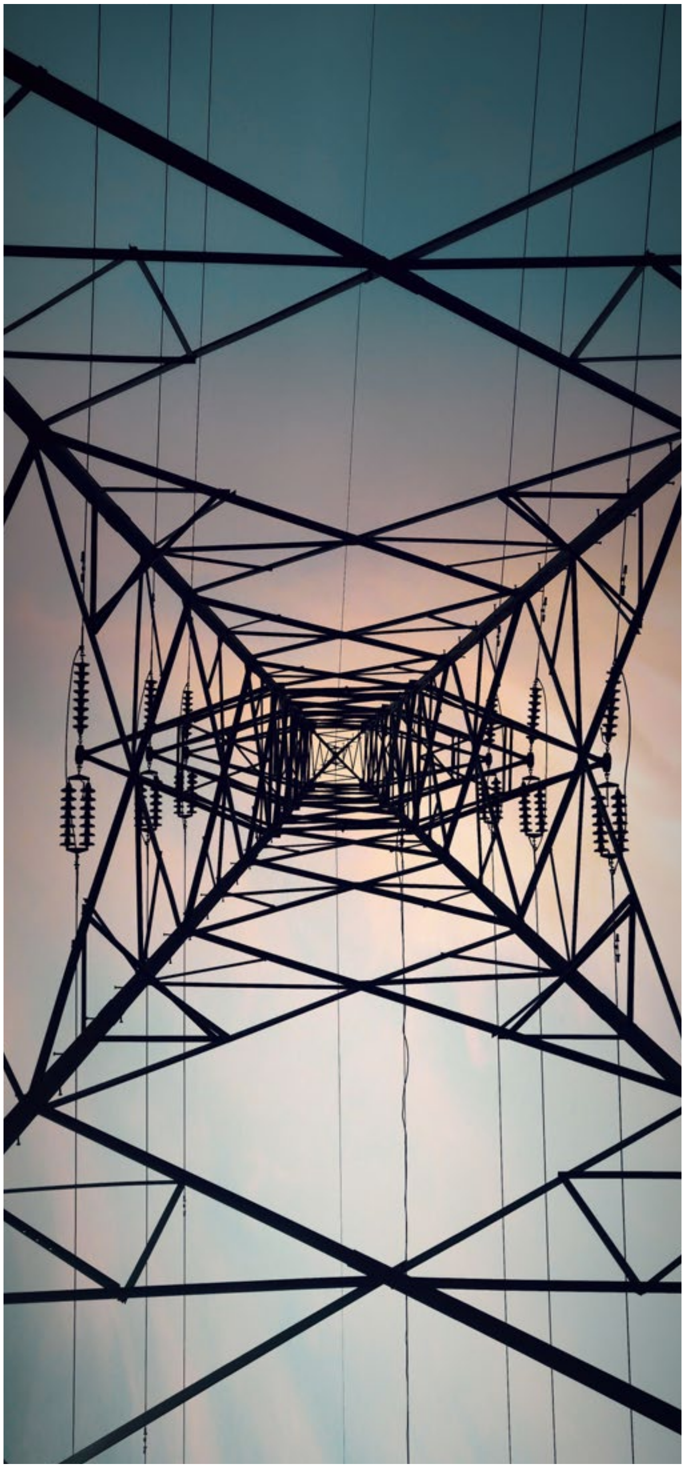
- Clarify the jurisdictional issues involved in transactive energy markets, particularly the role that FERC and state public utility commissions play in regulating these markets, and how such regulation will interact. For example, demand response—a key element of transactive energy—implicates both retail and wholesale energy markets, which can lead to regulatory ambiguity.

- At the state level, form working groups to study the value that a transactive energy system would provide across a variety of policy objectives, such as distribution infrastructure deferral, grid resilience, renewable portfolio standards, and retail market animation. Issues could include, among others, the appropriate scope and design of the transactive market (for example, bilateral, exchange-traded, or a one- or two-sided centrally cleared market, and the energy products involved); the role and identity of a DSO, if any, to manage the system; the range of minimal and permitted rate offerings to retail customers (including, possibly, a variant of today's simplistic rates) and the appropriate scope of regulation; and how to value energy resources at the grid edge.

- These working groups should be led by commission staff and solicit the input of various stakeholders, particularly utilities, with the aim of arriving at a clear articulation of transactive energy's benefits and costs vis-à-vis each state goal. Materials should be captured in a dedicated regulatory docket, following the example of Arizona.[88]

- If the findings of such a benefit-cost analysis are favorable, it should be followed by a formal regulatory proceeding, enabling the commission to take the reins and guide further exploration toward concrete proposals. This exploration should center on what the parameters of an optimally tailored transactive energy system would be, from

[88] "Commissioner Tobin Opens Docket to Examine Blockchain Technology," Arizona Corporation Commission, July 16, 2018.



Transmission tower. Source: sraone on Unsplash.

a feasibility and timeline perspective as well as the foregoing policy perspective.

- The outcome of a regulatory proceeding should include a published policy, technology, and budgetary roadmap for the evolution of the current state energy system to the envisioned transactive one. Such a roadmap should have clear stages, with an accompanying timeline, and be used to procure the necessary equipment and services from the private sector and measure performance. Examples of this include New York State's "Reforming the Energy Vision" (REV) process, which has sought to proactively anticipate and build out the regulatory underpinnings of a more transactive energy system.

- Set ambitious decarbonization goals whose success depends on a leaner, more efficient use of the electric power system. This could include clean energy standard targets, a price on carbon, and peak demand reduction targets for specific sectors. These goals must be backed up with state subsidies for equipment and services that support their achievement, and mandatory preference for non-wire alternatives (NWA) to grid infrastructure projects for regulated utilities or utility commissions issuing requests for proposals (RFPs).

- Use state and federal agencies (for example, state green banks) to fund proven transactive platform technologies that have the capability to scale. Leverage state regulatory sandboxes to test and help finetune their development in realistic distribution grid environments.

- Complete the roll-out of advanced metering infrastructure (AMI) within the United States, which presently is close to halfway complete.[89] The sub-hourly power and voltage measurements of advanced meters would be required to settle the real-time prices of a transactive market. These meters should have their home area network (HAN) radios activated, so that readings are available in real-time to smart devices in the home, rather than queried with significant delay from the utility.

[89] "Annual Electric Power Industry Report, Form EIA-861 detailed data files," US Energy Information Administration, July 31, 2019, https://www.eia.gov/electricity/data/eia861/.

6. CONCLUSION

There are compelling reasons for energy markets, and their governance, to move in the direction of a more transactive energy system. The growth of distributed energy resources at the grid's edge, the new opportunities for demand management afforded by digital technologies, and the imperative of keeping system costs as low as possible while accommodating these trends all augur for a much more transactive energy market. While some would propose blockchain as the first choice platform for such a market, a closer investigation reveals that blockchains may not serve as the primary solution for many transactive energy applications. In fact, blockchains may have limitations or even structural features that would prevent them from serving as the sole technology underpinning transactive energy systems.

Blockchains are novel, significant, and perhaps even transformational financial tools, and they have particular value in situations where multiple mistrusting parties are involved (such as in managing supply chains or joint ventures or land registries). The question is whether the electric grid, and the various technical, privacy, and security considerations needed to manage it effectively, constitute such a situation.

Blockchains are technologies still in their infancy, and they are poised to evolve and advance significantly in coming years, particularly in those contexts where their characteristics are well-suited to address extant needs or shortcomings. In assessing the role for blockchains in transactive energy applications, the matter at hand is not to embrace nor indict blockchain technologies in a vacuum, but instead to judge their fitness for purpose in supporting the key functions of a twenty-first-century transactive energy grid.

Blockchain's future as the architecture of a transactive energy grid may yet come to pass, but at present many of its key characteristics seem at odds with the specific, defining needs of such a future grid. Indeed, in ten years' time, when assessing the state of transactive energy, the best possible sign of the maturation of blockchains might be that they are serving various transactive energy applications without the word blockchain being mentioned at all. In November 1984, Harper's Magazine published a thoughtful article on a similar, attention-grabbing innovation in date management, titled "A Spreadsheet Way of Knowledge."[90] A few decades later, the spreadsheet has become an indispensable tool, but is never referenced by name when utilities adjust their rates, when chief executive officers (CEOs) set forth new strategies, or when the Organization for Petroleum Exporting Countries (OPEC) decides to cut or increase its oil production. The spreadsheet's ubiquity in business increased in perhaps some rough reverse correlation to popular fascination with it, and so might blockchain hope that its hype will over time lead to sensible and sustainable applications within the energy sector.

When it comes to transactive energy, it looks unlikely that blockchain will serve as an all-encompassing platform anytime soon, though continued consideration of its particular strengths and weaknesses in various contexts is merited. Blockchain as a technology solves an incredibly hard problem, allowing mistrusting parties to transact with each other, and in the process unlocks new possibilities and value. Hard problems, however, are rarely solved without a comparable cost. In the case of blockchain, that cost involves massive duplication and, in many cases, a large "brake" on the process (via consensus). The costs may well be worth it when disintermediation is at a premium, but it is doubtful that this would be the case in a future transactive distribution market, where in fact performance, security, and cost-effectiveness are most critical, rather than dis-intermediation. The tool of blockchain is a powerful one, and may very well unlock significant value in other areas of the energy sector. But even the most disruptive of tools still require discretion in their application.

[90] Steven Levy, "A Spreadsheet Way of Knowledge," *Wired*, October 17, 2017, https://www.wired.com/2014/10/a-spreadsheet-way-of-knowledge/.

APPENDIX: CRYPTOGRAPHIC APPROACHES TO THE TRANSPARENT PRIVACY PROBLEM

Transparent privacy is a vexing challenge for blockchain. Most real-world applications, including transactive energy, involve confidential transaction data, and yet third-party validator nodes require access to this data, at least to the extent that they can verify transaction correctness. These opposing needs arise from blockchain's ambition to hide confidential data in plain sight, outside of a corporate firewall. The three most prominently proposed techniques for addressing transparent privacy are zero-knowledge proofs, multi-party computation, and secure hardware enclaves. Understanding the capabilities and limitations of these techniques is crucial for assessing the degree to which blockchain can be trusted with confidential data in a transactive energy system and other critical applications.

All three techniques are early stage and have not been attempted in energy-related applications. In order to evaluate their potential for transactive energy, therefore, one is restricted to the handful of present-day blockchain projects to which they have been applied. Zero-knowledge proofs, for example, are the basis of Zcash, a cryptocurrency blockchain that supports private transactions. The details of these transactions are fully encrypted on the blockchain, shielded from public inspection, but the transactions themselves can nevertheless be validated by the network, ensuring for instance that the sender has the required balance of unspent tokens and that the sum of the input notes equals the sum of the output notes. The specific type of zero-knowledge proofs used by Zcash, and anticipated for other blockchains, such as Ethereum, is called a zero-knowledge succinct noninteractive argument of knowledge, or zk-SNARK. The noninteractive aspect is crucial: It means that transactors can simply publish a single proof to be evaluated independently by all network validators, rather than be interrogated by each validator in turn, a requirement of other protocols.

Zk-SNARKs require an elaborate, trusted setup procedure for each confidential algorithm they are to certify, such as Zcash transactions. One or more parties must come together to jointly create cryptographic secrets, which are used to generate a public proving key and validating key for the network. These keys are used going forward by participants to produce and to verify zero-knowledge proofs, certifying invocation of the algorithm on confidential data. It is critical that at least one participant destroy their share of the cryptographic setup secrets in order for the network to be secure, however. The reason is that these secrets, referred to as toxic waste, could be used to generate false proofs, validating malicious transactions such as token counterfeit.

The trusted setup phase can be thought of as concentrating the vulnerability of the algorithm at the moment of its creation. Zcash founders meticulously documented the creation, use, and then destruction of its cryptographic secrets, concluding with the spectacular destruction of the computer hardware involved. In order for zk-SNARKs to become a practical solution for smart contracts and other distributed applications in blockchains, researchers must devise a way to significantly automate this setup phase, without diminishing participants' confidence in the network. This could be thought of as somewhat akin, in a stylized way, to similar issues in the international governance regime created around nuclear nonproliferation.

To address some of these residual privacy concerns, researchers are pursuing alternative zero-knowledge proofs that do not rely on a trusted setup phase, surrendering zk-SNARK's convenient noninteractive property, fast validation time, or general flexibility in order to jettison this requirement.[91] Researchers at Stanford University and Visa, for example, have proposed Zether, a confidential transaction payment method that operates as a smart contract within public blockchains, such as Ethereum.[92] No trusted setup is required, but its functionality is limited to token transfers, rather than arbitrary business logic, and its zero-knowledge proofs involve a multistep interaction between transaction prover and verifier.

A second challenge facing zk-SNARKs is their computational burden. State-of-the-art proof generation techniques require between one and four times the amount of computation involved in the underlying algorithm being shielded.[93] This is not an issue for simple applications like Zcash token transfers, but becomes problematic for more complex and real-time applications, such as those involving electric grid management or market operations. Exacerbating the issue is that the input to the proof generation procedure is the value of every single variable computed in the course of the private algorithm. Modern software execution environments achieve much of their efficiency by intelligently discarding intermediate data once its purpose is served, which implies that private algorithms must be run in special-purpose environments burdened by full auditing, incurring what could be significantly greater runtime.[94] On the other hand, many more computational reduction efforts, including Bulletproofs, used by Monero as well as Zether, and Aztec Protocol, are being developed.[95] Zether is estimated by its creators to cost the equivalent of around $1.51 per transaction as of early 2019, but this could potentially be ameliorated through small changes to the Ethereum network in which it is traded.[96]

Multi-party computation (MPC) is another approach to transparent privacy that faces computational cost challenges. In MPC, a network of untrusted computers collectively perform computations on sensitive data without having direct access to it: each node receives a unique cryptographic reference to each secret value, which the node can operate on as if they were the values themselves, and which collectively serve as decoding keys to obtain the result.[97] The trick is the transformation from data to reference, which is known in mathematics as a homomorphism: Operations on the reference have the same effect as operations on the data itself, so when the reference is transformed back into data, the result is the same as if the transformation never took place. The MPC nodes work only with the reference data, and therefore perform the desired computation without ever seeing the data underlying it. Multiple nodes are involved in order to protect against errors or manipulation; as with blockchain consensus, a critical number of nodes must collude in order to break the system.

The computational challenges of MPC begin with its expressiveness: the only operations that are supported are the addition and multiplication of cryptographic

[91] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," in *2018 IEEE Symposium on Security and Privacy (SP)* (IEEE, 2018), 315-334.

[92] Benedikt Bünz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh, *Zether: Towards Privacy in a Smart Contract World* (Stanford, February 20, 2019), https://eprint.iacr.org/2019/191.pdf.

[93] B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly Practical Verifiable Computation," *2013 IEEE Symposium on Security and Privacy*, doi:10.1109/sp.2013.47; Jens Groth, "On the Size of Pairing-Based Non-interactive Arguments," *Advances in Cryptology—EUROCRYPT 2016 Lecture Notes in Computer Science* (2016), 305-26, doi:10.1007/978-3-662-49896-5_11.

[94] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza, "SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge," in *Advances in Cryptology—CRYPTO 2013 Lecture Notes in Computer Science* (2013), 90-108, doi:10.1007/978-3-642-40084-1_6.

[95] Lucas Nuzzi, "Monero Becomes Bulletproof," DigitalAssetResearch, October 18, 2018, https://medium.com/digitalassetresearch/monero-becomes-bulletproof-f98c6408babf; "AZTEC Protocol," AZTEC Protocol, https://www.aztecprotocol.com/.

[96] Bünz, Agrawal, Zamani, and Boneh, *Zether: Towards Privacy in a Smart Contract World.*

[97] Adi Shamir, "How to Share a Secret," Communications of the ACM 22, no. 11 (1979): 612-613.

references.[98] Zero-knowledge proofs share this limitation, and while these operations do in theory allow for universal computation, in the case of MPC the multiplication of two references—representing, say, energy and price—requires communication between nodes. In comparison, today's high-performance software is tailored meticulously to the underlying hardware, leveraging calculation rates on the order of billions of floating point operations per second (flops) for graphical processing units, the hardware of choice for large-scale computing.[99] Network communication latency is an eternity compared to such optimized numerical operations, and inserting it between every multiplication would effectively ground applications to a halt.

A second computational cost challenge for MPC arises from conditional logic, the if-then-else statements pervasive at all levels of software. Without knowledge of the underlying values, it is impossible for MPC nodes to evaluate questions as simple as whether one number is greater than another, whose result nevertheless governs the remainder of the computation. Nodes must therefore travel every conditional path, computing every possible sequence of operations, whose number grows exponentially with the number of conditionals—an impossibility in real-world applications.[100]

Despite its practical challenges, MPC is the aspiration of Enigma, a blockchain startup aiming to support self-described secret contracts on public blockchains.[101] In the Enigma model, the blockchain manages data access permission and public data, including nonsensitive references to secret data (distinct from the cryptographic references), while the Enigma network is responsible for calculations involving sensitive data.

While Enigma and the cryptography research community work to advance MPC, Enigma has replaced it with a technology that exists today: secure hardware enclaves. Secure enclaves encrypt both computer code and the data it operates on, shielding them from even the computer's operating system. They offer confidential computing as well as an attestation that the result was produced, as intended, by the enclave, and not a rogue third party. Enigma nodes are required to use Intel chips supporting Software Guard Extensions (SGX), Intel's implementation of the technology.

Competing secure enclave implementations exist, such as ARM's TrustZone and Secure Encrypted Virtualization—an enclave for cloud computing—as well as Keystone, an open- source enclave.[102] A sequence of high-profile exploits have called the enclave approach to transparent privacy into question, however, revealing that even these carefully protected data environments remain vulnerable.[103] Closed source implementations such as SGX and TrustZone also arguably defeat the purpose of blockchain, putting network security in the hands of a single corporate entity, such as Intel.

[98] Michael Ben-Or, Avi Wigderson, and Shafi Goldwasser, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation," in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing—STOC 88* (May 2-4, 1988), 1–10, https://doi.org/10.1145/62212.62213.

[99] Alberto Cano, "A Survey on Graphic Processing Unit Computing for Large-Scale Data Mining," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 8 no. 1 (February 2017), https://doi.org/10.1002/widm.1232.

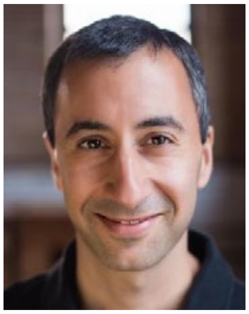
[100] Zyskind, Nathan, and Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy."

[101] Ibid; "Expanding Enigma's Roadmap: Towards a Privacy Layer for the Decentralized Web," Enigma, September 20, 2018, https://blog.enigma.co/expanding-enigmas-roadmap-towards-a-privacy-layer-for-the-decentralized-web-f1d6b7908251.

[102] "Keystone," Keystone Project, https://keystone-enclave.org/.

[103] Lily Hay Newman, "Critical Flaw Undermines Intel CPUs' Most Secure Element," *Wired*, August 20, 2018, https://www.wired.com/story/foreshadow-intel-secure-enclave-vulnerability/; Richard Chirgwin, "Boffins Show Intel's SGX Can Leak Crypto Keys," *Register*, April 16, 2017, https://www.theregister.co.uk/2017/03/07/eggheads_slip_a_note_under_intels_door_sgx_can_leak_crypto_keys/; Richard Chirgwin, "Foreshadow and Intel SGX Software Attestation: 'The Whole Trust Model Collapses,'" *Register*, August 15, 2018, https://www.theregister.co.uk/2018/08/15/foreshadow_sgx_software_attestations_collateral_damage/; Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado, *Inferring Fine-Grained Control Flow Inside SGX Enclaves with Branch Shadowing* (November 21, 2016); Mohit Kumar, "Researchers Defeat AMD's SEV Virtual Machine Encryption," *Hacker News*, May 28, 2018, https://thehackernews.com/2018/05/amd-sev-encryption.html.

ABOUT THE AUTHORS



Ben Hertz-Shargel is vice president, advanced grid services and analytics at EnergyHub, the distributed energy resource (DER) management platform for utilities. He is responsible for advanced grid services as well as analytics within the company's Mercury DERMS platform.

Hertz-Shargel is an expert on the intersection between advanced energy technology and energy markets, contributing most recently to the book *Digital Decarbonization* published by the Council on Foreign Relations. He came to EnergyHub from ThinkEco, where he was vice president, technology, and prior to that was a member of the Quantitative Strategies group at Credit Suisse.

He holds a BA in Computer Science from Northwestern, an MS in Mathematics from the Courant Institute at NYU, and a PhD in Mathematics from UCLA.

David Livingston is deputy director for climate and advanced energy, in the Atlantic Council's Global Energy Center.

He is also a fellow of the Initiative for Sustainable Energy Policy at Johns Hopkins University, and of the Payne Institute at the Colorado School of Mines. He also teaches a course on energy for the University of Southern California (USC) program in Washington, DC, and serves as a strategist for the Obama Foundation Scholars program.

Previously, Livingston served as a fellow at the Carnegie Endowment for International Peace, and as the inaugural Robert S. Strauss fellow for geoeconomics at the Office of the US Trade Representative, where he concluded as acting assistant US trade representative for congressional affairs.

He also has worked at the World Trade Organization in Geneva and at the United Nations Industrial Development Organization (UNIDO) in Vienna. Earlier in his career, Livingston was selected as a Future Energy Leader by the World Energy Council, and is an alumnus of the Atlantik Brücke Young Leaders Program. He earned a BA with highest honors from the University of Southern California in Los Angeles, and an MSc with distinction from the University of Oxford in the United Kingdom.

ACKNOWLEDGMENTS

The Atlantic Council Global Energy Center is grateful for the support of the MacArthur Foundation that made this publication possible.

The authors are grateful to the Atlantic Council staff that played key roles in the publication of this paper, including Randolph Bell, Kevin Fry, Jennifer T. Gordon, and Becca Hunziker. In addition, the authors thank the multiple individuals outside of the Council who dedicated significant time to reading various drafts of the paper, including Peter Bronski, Kristen Brown, Doug Miller, Jesse Morris, and Ashley Pilipiszyn.

Their feedback helped strengthen the paper significantly, and greatly enriched the process of researching, writing, and editing. Any errors herein remain the sole responsibility of the authors.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org