ACADIAN

PERSPECTIVES

VIEWPOINTS FROM THE ACADIAN TEAM

PHILIP OWRUTSKY, PH.D., CFA
ASSISTANT VICE PRESIDENT, ASSOCIATE STRATEGIST

BITCOIN'S UNSUSTAINABLE SUSTAINABILITY PROBLEM

DECEMBER 2017

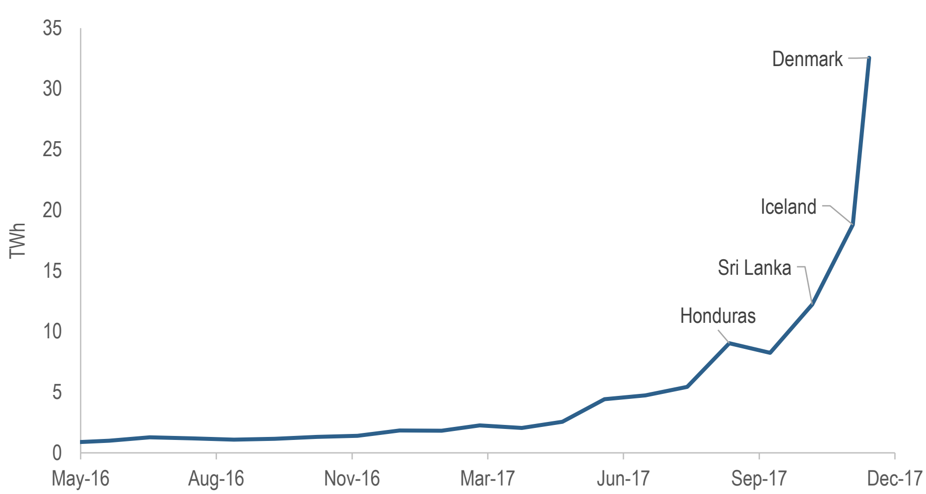
Bitcoin is an innovation that enables the exchange of digital currency anonymously, verifiably, and without a central clearinghouse. However, Bitcoin's popularization has come at an enormous economic and environmental cost, requiring greater ongoing electricity consumption than all of Denmark. This represents such a headwind to mass adoption that we are circumspect about the long-term viability of Bitcoin (at least in its current form) as a medium of exchange, despite the recent surge in its value and the intense attention that the instrument is receiving.

Bitcoin's sustainability problem derives from the decentralized public ledger—called the blockchain—that records Bitcoin transactions. For Bitcoin to be viable, there has to be some mechanism to ensure the validity of the ledger in the absence of a trusted, centralized custodian. Otherwise, there would be no way to guarantee that only the actual owner of a Bitcoin could spend it.

The key insight facilitating Bitcoin, is that counterfeit ledgers would be preventable if they were infeasibly expensive to create. To that end, Bitcoin requires the solution to a transaction dependent, complex cryptographic problem before transactions are added to the ledger. While *extremely* difficult to solve, the answers are easily verified and are included in the ledger of transactions.[1] Therefore, any potential falsified ledger would have to solve a large number of these cryptographic problems to avoid being easily identifiable as a fraud. This makes creating a fake ledger computationally intractable.

FIGURE 1

Bitcoin Energy Consumption Estimates (1TW = 16.7M 60W lightbulbs)



Source: Coindesk for historical price information. Electrical consumption of countries from the 2014 CIA Factbook. Energy estimates based on historical price and current mining difficulty. See appendix for supporting calculations.

BITCOIN DEMYSTIFIED

Bitcoin is a digital currency and payment system. Much like a traditional currency, a given Bitcoin (or portion of a Bitcoin) can only be in one place at a time. Bitcoins are held in digital wallets, ultimately represented by 1's and 0's in a public ledger. Using the Bitcoin protocol, these coins can be transferred electronically from a wallet you control to another of your choosing, in order to purchase goods or services.

The second component is a public ledger called the blockchain that contains a record of Bitcoin transactions. Through these records, the ledger tracks where each Bitcoin currently resides, which ensures that a Bitcoin cannot be double spent. The ledger itself is not centrally owned and updates are performed in a decentralized manner without dependence on a trusted agent.

Bitcoin transactions are not immediately entered into the blockchain ledger. Blockchain updates require solving a complex cryptography problem specific to the particular transactions. "Miners", a vague term that refers to individuals or institutions who contribute computation power to the Bitcoin network, find the solutions, and they're compensated in Bitcoin for doing so. While the problems are difficult, the solutions are easy to verify. Once solved, the block of transactions are added to the blockchain. This is why Bitcoin is a crypto-currency.

This solution is elegant. Simply declaring the most computationally complex blockchain to be the "real ledger" virtually eliminates the possibility of a counterfeit.[2] This is because an individual or small group seeking to create a fraudulent ledger can presumably bring to bear only a relatively small amount of computational power compared to the entire Bitcoin network. Paying individuals for contributing computation power to the genuine ledger (commonly called mining[3]) ensures that it always has more computational effort than any fraudulent ledger possibly could. This "proof-of-work" approach provides the required blockchain verification.

But computational power requires electricity, and in the context of Bitcoin, it turns out to be a truly staggering amount.[4] While it is difficult to generate a precise estimate of Bitcoin's power consumption and the associated environmental impact, the Appendix details several thoughtful estimations. The numbers are jarring. A reasonable estimate of Bitcoin's ongoing annualized electricity consumption is over 32 terrawatt-hours (TWh).[5] To put this into context:

- If Bitcoin were a country, its power consumption now would be on par with Denmark, ranking 59th in the world. A single bitcoin transaction could power an American home for about a week. Figure 1 shows the astronomical increase from Q3-Q4 2017.
- Bitcoin consumes the same amount of power as 2.8 million Americans, more than 3 times the energy used to manufacture all cars, light trucks, and sport utility vehicles in the U.S.[6]
- The true cost of a Bitcoin transaction is about $20, over and above any fees directly charged. That's over 1,000 times the cost of a credit card transaction using VISA.[7]

Our estimate of Bitcoin's carbon footprint is equally shocking. Bitcoin adds 16.3 million metric tons of carbon dioxide to the atmosphere annually, the equivalent of about 3.5 million cars.[8]

These figures are alarming, and because miners are compensated based on the price of Bitcoin, the environmental impact should increase as Bitcoin appreciates. This calls into question the sustainability of Bitcoin's "proof-of-work" based blockchain. It is our belief that in the near term Bitcoin will evolve its algorithm to increase transactional throughput in order to mitigate the cost per transaction. However, we expect this response will be insufficient and for Bitcoin-related electricity consumption to further increase.

As long as mining remains profitable, new entrants will be attracted to the space. Consequently, Bitcoin may need to change its core "proof-of-work" paradigm lest it be supplanted by a competing technology with less exorbitant resource requirements.

APPENDIX

ESTIMATING ELECTRICITY CONSUMPTION

A particularly conservative estimate of Bitcoin's electricity consumption, would 1) assume that all miners use the most power efficient device commercially available for mining, currently the AntMiner S9, which is an integrated circuit designed and optimized for Bitcoin Mining, and 2) exclude all power needed to cool hardware. AntMiner's manufacturer purports a 0.098 J/GigaHash (GH) efficiency. At Bitcoin's current difficulty, the hash rate is 11+ billion GH/s. At this rate, S9's use 0.0011 TW of power (11 billion * 0.098 / 10^12). Annualizing yields 9.8TWh (0.0011*24*365) of energy per year attributable to Bitcoin mining.

A more realistic estimate for power consumption derives from a model predicated on the assumption that Bitcoin production is determined in a context similar to a competitive market where miners create new Bitcoins as long as the marginal value of the cryptocurrency exceeds the marginal variable cost of production.[9] Those variable costs almost entirely reflect electricity. Currently a block is added to the blockchain every 10 minutes and rewards the miner with 12.5 Bitcoins for that interval or 1,800 Bitcoins a day. At a Bitcoin price of $17,348 (12-Dec-17), this represents $11.4B worth of mining rewards per year. We conservatively estimate that only 30% of this amount ($3.4B) is consumed by electricity costs.[10] Using the average price of U.S. electricity of 10.4 cents per kWh, this would translate to an estimate of 32.8 TWh of power consumption (3.4B/0.104).[11]

ESTIMATING CARBON DIOXIDE EMISSIONS

We base estimates of Bitcoin-related carbon dioxide (CO_2) emissions on the fraction of U.S. electricity production attributable to coal and other CO_2 emitting forms of energy generation. Since a large portion of mining occurs in developing countries, where coal is more prevalent than in the U.S., we believe this estimate is conservative.

According to the most recent U.S. Energy Information Administration report (for 2015[12]), the U.S generated just over 4,000TWh of energy and produced a little over 2 billion metric tons of CO_2 in the process. That equates to roughly 500,000 metric tons of CO_2 per TWh (2 billion/4000). Using the 32.8 TWh estimate of Bitcoin's electricity use, we conservatively attribute 16.3 million metric tons of carbon dioxide emissions to power consumption associated with Bitcoin transactions.

VISA

According to Visa's 10-K for FY 2017, the company processed over 111 billion transactions. They report network and processing expenses directly at $620 million or about ½ cent per transaction. Noting that a typical credit card transaction also requires interacting with the buyer and seller's bank, we conservatively multiply this by 3 for a per transaction cost of 1.67 cents.

Bitcoin is currently executing transactions at annualized rate of 133 million corresponding to nearly 250kWh (32.8TWh / 133mm) of electricity per transaction. Conservatively using China's cost of electricity of 8 cents per kWh, we find an electricity-only cost of $19.79.

The ratio in cost of a Bitcoin transaction to a Visa transaction is then $19.79/.0167 = 1183x.

ENDNOTES

1 On the desktop I'm writing this on, it would take over 100,000 years to solve just one of these problems. However, I can verify a solution in well under a second.

2 Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008

3 Most mining is now performed by specialized equipment for efficiency reasons, but anyone can mine using virtually any computer, which was fairly common several years ago.

4 Note: the computational complexity of elements in the ledger is routinely adjusted to account for improvements in technology or changes in the number of miners. This means that Moore's law should not be expected to reduce energy use.

5 See the appendix for assumptions and supporting calculations. Note that calculations are based on the current Bitcoin algorithm and volume of transactions, which will likely evolve over time.

6 United States Department of Energy/Energy Information Administration, First Use of Energy for All Purposes, (2014) Washington, D.C.

7 VISA information from the company's 2017 10-K. Supporting calculations in the appendix.

8 Based on a 2014 U.S. Environmental Protection Agency estimate that the typical passenger vehicle releases 4.7 metric tons annually. Office of Transportation and Air Quality. Publication EPA-420-F-14-040a. May 2014. 16.3 million metric tons of CO_2 then represents 3.5mm cars. To the extent that fuel efficiency has improved over time, this would be a conservative estimate of the current equivalent number of vehicles.

9 Hayes, Adam, "A cost of Production Model for Bitcoin," March 19, 2015.

10 Hayes suggests 60% is more accurate. This would yield an estimated 65.7TWh

11 Substantial mining is performed in developing nations with lower electricity costs.

12 United States Department of Energy/Energy Information Administration, Electric Power Annual, Table 9.1, (2017) Washington, D.C.

BIOGRAPHY

PHILIP OWRUTSKY, PH.D., CFA

ASSISTANT VICE PRESIDENT, ASSOCIATE STRATEGIST

Philip joined Acadian in 2016 as an associate strategist, aligned closely with Acadian's Global Client Group and Investment Teams. Prior to joining Acadian, Philip was an associate trader at Potamus Trading applying control theory principles to high frequency trading. Previously, he was a vice president at State Street Bank where he was responsible for developing and maintaining regulatory and economic capital models for the securities lending and stable value wrap business units. Philip has also independently consulted for several hedge funds including work on catastrophe bond valuations and trading commodities using machine learning methods.

Philip holds a Ph.D. in applied mathematics from Harvard University; an M.S. in engineering sciences and an M.A. in statistics also from Harvard; as well as a B.A. in mathematics and a B.S. in engineering physics from Cornell University. He is a CFA charterholder and a member of CFA Society Boston.

GENERAL LEGAL DISCLAIMER

Acadian provides this material as a general overview of the firm, our processes and our investment capabilities. It has been provided for informational purposes only. It does not constitute or form part of any offer to issue or sell, or any solicitation of any offer to subscribe or to purchase, shares, units or other interests in investments that may be referred to herein and must not be construed as investment or financial product advice. Acadian has not considered any reader's financial situation, objective or needs in providing the relevant information.

The value of investments may fall as well as rise and you may not get back your original investment. Past performance is not necessarily a guide to future performance or returns. Acadian has taken all reasonable care to ensure that the information contained in this material is accurate at the time of its distribution, no representation or warranty, express or implied, is made as to the accuracy, reliability or completeness of such information.

This material contains privileged and confidential information and is intended only for the recipient/s. Any distribution, reproduction or other use of this presentation by recipients is strictly prohibited. If you are not the intended recipient and this presentation has been sent or passed on to you in error, please contact us immediately. Confidentiality and privilege are not lost by this presentation having been sent or passed on to you in error.

Acadian's quantitative investment process is supported by extensive proprietary computer code. Acadian's researchers, software developers, and IT teams follow a structured design, development, testing, change control, and review processes during the development of its systems and the implementation within our investment process. These controls and their effectiveness are subject to regular internal reviews, at least annual independent review by our SOC1 auditor. However, despite these extensive controls it is possible that errors may occur in coding and within the investment process, as is the case with any complex software or data-driven model, and no guarantee or warranty can be provided that any quantitative investment model is completely free of errors. Any such errors could have a negative impact on investment results. We have in place control systems and processes which are intended to identify in a timely manner any such errors which would have a material impact on the investment process.

Acadian Asset Management LLC has wholly owned affiliates located in London, Singapore, Sydney, and Tokyo. Pursuant to the terms of service level agreements with each affiliate, employees of Acadian Asset Management LLC may provide certain services on behalf of each affiliate and employees of each affiliate may provide certain administrative services, including marketing and client service, on behalf of Acadian Asset Management LLC.

Acadian Asset Management LLC is registered as an investment adviser with the U.S. Securities and Exchange Commission. Registration of an investment adviser does not imply any level of skill or training.

Acadian Asset Management (Japan) is a Financial Instrument Operator (Discretionary Investment Management Business). Register Number Director-General Kanto Local Financial Bureau (Kinsho) Number 2814. Member of Japan Investment Advisers Association.

Acadian Asset Management (Singapore) Pte Ltd, (Registration Number: 199902125D) is licensed by the Monetary Authority of Singapore.

Acadian Asset Management (Australia) Limited (ABN 41 114 200 127) is the holder of Australian financial services license number 291872 ("AFSL"). Under the terms of its AFSL, Acadian Asset Management (Australia) Limited is limited to providing the financial services under its license to wholesale clients only. This marketing material is not to be provided to retail clients.

Acadian Asset Management (UK) Limited is authorized and regulated by the Financial Conduct Authority ('the FCA') and is a limited liability company incorporated in England and Wales with company number 05644066. Acadian Asset Management (UK) Limited will only make this material available to Professional Clients and Eligible Counterparties as defined by the FCA under the Markets in Financial Instruments Directive.

ACADIAN

BOSTON LONDON SINGAPORE TOKYO SYDNEY

ACADIAN-ASSET.COM