2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics

Modeling the Energy Consumption of Blockchain Consensus Algorithms

Ryan Cole and Liang Cheng
Department of Computer Science and Engineering
Lehigh University
Bethlehem, PA 18015
Email: rbc218@lehigh.edu, cheng@lehigh.edu

***Abstract*—With the development of Internet of Things (IoT) and blockchain technologies, people find more and more blockchain applications in the IoT domain. While it is reasonable that IoT systems use hierarchical network structures, their sheer large scales may lead to hundreds or even thousands of non-leaf nodes, which may serve as full nodes when participating in IoT blockchains. From IoT blockchain design perspective, it is important to understand the scalability of the energy consumption feature of IoT blockchains. In our research we have collected real-world data that reflect the energy consumption features of several consensus algorithms of blockchain. In this work-in-progress paper, we report our results based on linear regression models. These models provide reference estimations of the energy consumption impact in designing blockchains for IoT systems.**

***Index Terms*—Blockchain, Consensus Algorithms, Internet of Things (IoT), Energy Consumption**

I. Introduction

Bitcoin [1], its variants [2], and blockchain-based systems [3] have gained a significant amount of attention. Distributed ledgers are implemented by those systems to record transaction information where distributed consensus mechanisms, such as PoW (i.e. Proof of Work in Bitcoin), PoS (Proof of Stake in Blackcoin [4]), and PoI (Proof of Importance in NEM [5]), are used for networked participants collectively agreeing on the contents of the distributed ledgers.

Generally blockchain mechanisms and distributed ledger technologies, such as Ripple [6], and Stellar [7], have been proposed to address the distributed consensus problem [8]. Each of these is designed to target a specific subset of the areas in which blockchains may be used, as opposed to the general-purpose use of older crytpocurrencies such as Bitcoin.

A. Blockchain for Internet of Things Applications

Modern Internet-of-Things (IoT) systems [9], such as interconnected transportation systems and smart communities [10] illustrated in Figure 1, generate a huge amount of data everyday. Data exchanges, sometimes monetized data transactions, among IoT systems enable services that could not be previously rendered by a single IoT system. These exchanges may be facilitated by a trusted intermediary or a central authority, and participating entities may raise cost, privacy, and security concerns. Due to blockchain's enabling

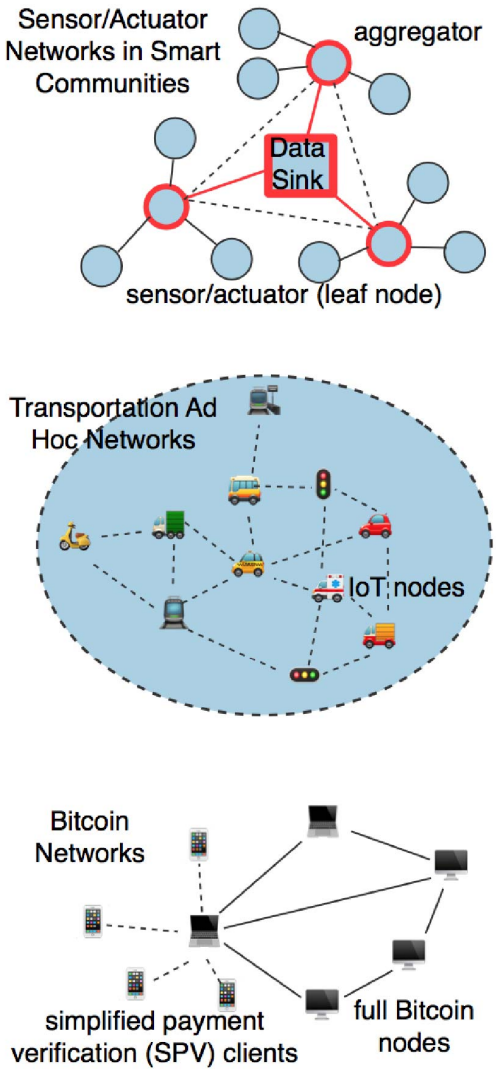

Fig. 1. IoT and Bitcoin System Architecture

978-1-5386-7975-3/18/$31.00 ©2018 IEEE
DOI 10.1109/Cybermatics_2018.2018.00282

capability of establishing distributed trust, IoT blockchains [11] have been proposed to address those concerns.

For example, IoT blockchains can track sensor data measurements and prevent modifications with other malicious data by taking advantage of the immutability characteristic of blockchain. Blockchains enable autonomy so that there is not a single point of failure in an IoT network and they provide a history of data exchanges and transactions which make troubleshooting easier.

B. Energy Consumption Issues of using Blockchain for IoT Applications

Yet despite the ever-present problem and study of energy usage by IoT nodes and networks [12], whether the use of blockchains for IoT systems and applications will make this problem even worse is still an open question rarely investigated. While it is reasonable that IoT systems use hierarchical network structures, their sheer large scales may lead to hundreds or even thousands of non-leaf nodes and/or ad hoc nodes as illustrated in Figure 1. Considering the similarities between the IoT network architecture and the blockchain system architecture, we may assume that these large number of non-leaf and/or ad hoc nodes serve as full nodes when participating in IoT blockchains. From IoT blockchain design perspective, it is important to understand the scalability of the energy consumption feature of IoT blockchains.

One of the most common criticisms of blockchain technologies, particularly PoW-based systems, is their unchecked energy consumption. Digiconomist [13] estimates that a single Bitcoin transaction uses over 800 kilowatt hour (kWh) of electricity. By comparison, the average United States household uses roughly 900kWh of electricity per month [14]. Different consensus mechanisms have been proposed to circumvent this issue, each with their own sets of advantage. The ultimate goal of this research is to answer the following question: Can we formulate the energy usage of different consensus protocols so that the energy impact of IoT blockchains can be estimated prior building the blockchains?

C. Contributions

In this paper, we describe approaches to modeling the energy consumption of both PoW and non-proof-of-work coins and associated consensus algorithms based on parameters including the size of the network, the number of messages sent per transaction, and the computing cost of such a consensus protocol. We have collected real-world data in our research that reflect the energy consumption features of several consensus algorithms of blockchain using their representative implementations such as Ethereum [16], Ripple, and Stellar systems. To the best of our knowledge, this is one of the first work directly addressing the above-mentioned research question.

In this work-in-progress paper, we report our preliminary results based on linear regression models. These models provide reference estimations of the energy consumption impact in designing blockchains for IoT systems. We future work includes using nonlinear models such as neural networks for more accurate prediction results and performing theoretical analysis for model generations.

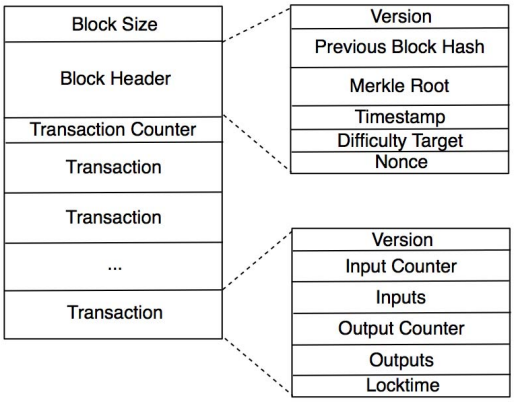

Fig. 2. Data Structure of a Block in Bitcoin Systems

The paper is organized as follows. Section II briefly describes the mechanisms and implementations of different consensus algorithms. Section III discusses the methods used to gather energy-consumption data for our modeling purpose. Section IV reports our work-in-progress results. Section V presents related work discussions. Finally, Section VI concludes the paper and discusses future work.

II. Consensus Algorithms in Blockchain Implementations

A. Proof of Work

Proof of Work is the original blockchain consensus algorithm. In Proof of Work, participants such as the full nodes shown in Figure 1 must solve a complex mathematical puzzle in order to be able to verify a group of transactions included in a block. In order to mine a block, a full-node miner must guess a nonce for the block. Each block includes the hash of the previous block, a set of transactions, a nonce and other information included in the block data structure depicted in Figure 2. In order to mine the block, the hash must have a certain prefix (e.g. 000) prescribed by the difficulty target. By modifying the nonce, the miner can change the hash. Miners increment the nonce and hash the block until the prefixes match. This requires a significant computational investment on the part of the miners. Once a block is mined the miner node will broadcast the block to the network for its validation by the rest of the network. The block will be added to the block chain when all participating nodes have agreed on its legitimacy. Note that Proof of Work favors liveness over safety and it requires enormous amounts of energy for consensus establishment.

B. Ripple Protocol Consensus Algorithm

The Ripple Protocol Consensus Algorithm, used by Ripple, is one solution to the Byzantine Generals Problem [17]. Ripple divides voting into rounds. Initially, each node collects all

transactions that it has seen that have not yet been applied and then publishes them in what is known as a "candidate set". Each node collects the candidate sets and votes on the validity of the transactions. All transactions that receive more than a certain percentage of "yes" votes proceed to the next round, if applicable. In the final round, at least 80% of the nodes must vote yes on each transaction for it to be verified. After this round, all transactions that have reached this threshold are added to the public ledger. Using multiple rounds with an increasing verification threshold can increase the verification speed and accuracy of the network. Latent nodes that may have been able to keep up in earlier rounds but not responsive in time later on will be removed from that round of consensus. This allows for faster decisions and prevents transactions from being discarded simply because there are too many slow nodes.

C. Stellar Consensus Protocol

The Stellar Consensus Protocol is a form of Federated Byzantine Agreement (FBA) [18], which is built on open membership and quorum slices. A quorum is a set of nodes sufficient to reach an agreement. FBA also utilizes quorum slices, which is a subset of a quorum that can convince another node of agreement. Each node decides upon a group of nodes that it trusts, which forms the node's quorum slice. There are two conditions for a node to accept a transaction: (i) the node must have never accepted a conflicting transaction, and (ii) a large enough portion of the node's quorum slice must also vote for or claim to accept the transaction. The protocol favors safety over liveness and by design any two quorums need to intersect and the intersection should not contain Byzantine nodes.

III. Data Collection for Energy-Consumption Modeling

A. Online Data Scraping

We scraped data on proof-of-work coins from cryptocurrency statistics available online [19], including Bitcoin, Ethereum, Litecoin, Monero, and Vertcoin. For each coin, we collected daily data on the number of transactions, the difficulty, hashrate, mining profitability, and price. The network hash rate reflects the processing power of the blockchain network. For example, if a network hash rate is 10 Th/s, it means that the network may make 10 trillion calculations per second.

One of the most often-cited sources for Bitcoin energy usage data is Digiconomist [13]. Using their formula, we estimated each coin's daily energy usage. Finally, we analyzed the data using regression techniques. The data sets have been divided into a training set for model fitting and a testing set for evaluations of the trained models.

B. Testbed Experiments

Two sets of experiments were performed using a testbed. One set of experiments was done using the Stellar Consensus Protocol (SCP). The other was conducted using the Ripple Protocol Consensus Algorithm (RPCA). A control experiment in which no consensus mechanism was run was also performed to determine the base energy consumption of every machine in the testbed.

The testbed consists of three worker nodes and a master/control node. Figure 3 illustrates a diagram of the testbed. Each worker node's energy consumption is instrumented by a monitoring device (Yokogawa power meter) throughout the experiments. The master/control node is in charge of starting experiments. An Ansible playbook [20] is used to set up and run each experiment from the master/control node where Ansible is a configuration management system for automating system configuration tasks for a network of computers. The master/control node also collects and stores each node's energy usage data from the monitoring device.

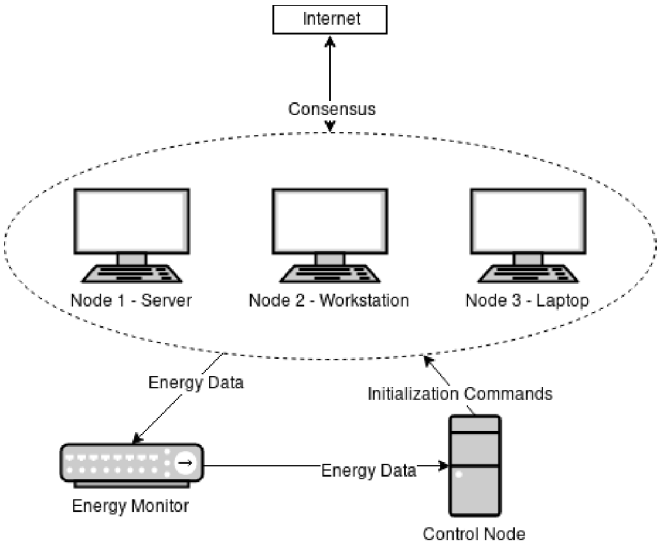

Fig. 3. Diagram of the Testbed for Data Collection

Aside from the consensus mechanism, each worker node also runs a packet sniffer to count the number of packets sent by the consensus mechanism during the time period of experiments. An observation is that verification on an individual node by either SCP or RPCA uses so little energy that the energy used in transmitting a packets between two nodes becomes relatively significant.

IV. Modeling Results

Generally speaking, the energy $\boldsymbol{e}$ required for one machine in a network to validate a transaction is the sum of the energy required for that node to validate the transaction locally, $\boldsymbol{v}$, and the energy used to send the packets required to communicate with other nodes $\boldsymbol{c}$. Thus an increase in local validation difficulty, such as through mining, or in the number of messages sent between nodes can greatly impact the energy consumption of a consensus protocol. The energy required for the entire network to validate a transaction is approximated as $\boldsymbol{e}$ multiplying the number of nodes $\boldsymbol{n}$ in the network.

A. Proof of Work

With any PoW consensus mechanism, the cost of validation on a single node becomes so high that the cost of sending messages between nodes is negligible. Still, the energy used by any given PoW cryptocurrency can vary drastically. For example, energy usage estimates for a single Bitcoin transaction recently vary from 200kWh to 950kWh; energy usage estimates for a single Ethereum transaction hover around 75kWh. This depends on the methods used to estimate the energy usage.

We modeled and predicted energy usage data for five different Proof of Work coins. In order to do this, we followed Digiconomist's process of predicting energy consumption. First, the total mining revenues for a given time period are predicted. In our case, these predictions were scraped from bitinfocharts. Then the portion of profits used to pay for electricity were estimated. For our purposes, as with Digiconomist, we assumed that 60% of mining revenue was spent on operational costs. Third, we determined how much miners spent per kilowatt hour on electricity. Based on global energy prices and distribution of miners, we estimated that miners spent $0.05/kwh on electricity. Finally, we converted these electricity cost estimates to energy consumption data.

We identified the most important indicators of energy usage for a transaction as the network hashrate $\boldsymbol{h}$, number of transactions in the last 24 hours $\boldsymbol{t}$, the average transaction fee $\boldsymbol{f}$, and the confirmation time of the network for a transaction $\boldsymbol{o}$. Using a LASSO (Least Absolute Shrinkage and Selection Operator) regression model [21] suitable for both linear and nonlinear system identification, we were able to produce a formula shown in Eq. (1) that estimates the energy usage of a cryptocurrency in kilowatt hours with 92% accuracy.

$$e = 8.987e^{-12}\boldsymbol{h} + 1.041e^{7}\boldsymbol{f} + 15.02\boldsymbol{t} + -1.375e^{4}\boldsymbol{o} \quad (1)$$

Note that data shuffling should be used to improve the modeling accuracy. Figure 4 shows a version of the regression test with only 57% accuracy using Ethereum data, in which the data is not shuffled before being split into testing and training data. Because the first two-thirds of the data, which changes significantly less than the last third, is used to predict energy consumption, minor changes in testing inputs cause the output to be significantly overestimated. When the data is shuffled, the model accuracy increases significantly. The accuracy, predicted by scikit-learn [22], is calculated as follows: "The [score] is defined as (1 - u/v), where u is the residual sum of squares ((y_true - y_pred) ** 2).sum() and v is the total sum of squares ((y_true - y_true.mean()) ** 2).sum(). The best possible score is 1.0 and it can be negative (because the model can be arbitrarily worse). A constant model that always predicts the expected value of y, disregarding the input features, would get a score of 0.0." [22]

B. Ripple Protocol Consensus Algorithm

Over the course of 10.5 thousand transactions, each test node consumed on average only 0.06kWh of electricity. This means that each transaction consumed $5.71e-6$ kWh, or 0.005 Watt hour (Wh). Throughout the course of these 10,500

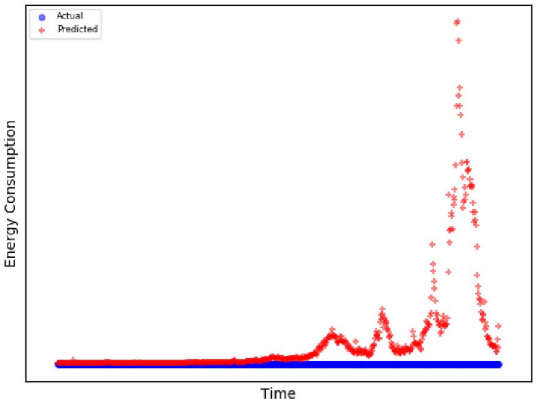

Fig. 4. Ethereum's Actual Energy Usage vs Predicted Energy Usage by LASSO Regression without Data Shuffling

transactions, each validator node sent approximately 15.5 million packets. This is roughly 1500 packets per transaction. This may seem high, but it is worth mentioning that a single message may be split into many packets. Estimates have placed the energy used to transfer data across the Internet at roughly 1.2mJ/packet. At this rate, the packets transmitted by a single node in the Ripple network use 1800 Joules or 0.5Wh per transaction. While tiny, this still plays a large part in the energy consumption of the network given that it is much greater than the energy required to validate a transaction locally. Therefore, the energy consumption of the Ripple network in kilowatt hours can be formulated as Eq. (2) based on the data collected from the testbed where $\boldsymbol{n}$ is the number of nodes on the network and $\boldsymbol{t}$ is the number of transactions for the period being measured.

$$\boldsymbol{e} = \boldsymbol{n} * \boldsymbol{t} * 5.05e-4 \quad (2)$$

As a point of reference, Visa uses approximately 200kWh of electricity to validate 100,000 transactions [13]. The size of the public Ripple network at the time of writing is 147 nodes and thus the energy consumption estimation is 147 * 100,000 * $5.05e-4$, i.e. 7,423.5kWh. Although this is significantly higher than the energy usage of the Visa network, which may be a cost of using the distributed consensus algorithm, it is in the orders of magnitude lower than the energy usage of Bitcoin.

C. Stellar Consensus Protocol

In the same time period in which the Ripple tests were run, 31,300 transactions were added to the Stellar network. During this period of time, each node consumed, on average, 0.02kWh of electricity. Therefore, each transaction consumed $1.91e-6$ kWh of electricity.

It is in the number of packets sent where the energy usage data for Stellar becomes interesting. Because each Stellar

node has a different quorum set, one would expect quorum sets of different sizes to transmit vastly different amounts of data. However, this did not seem to be the case. The first node we ran had a ten-node quorum. The second had a five-node quorum. Finally, the third node had a 10-node quorum in which nodes were nested such that the votes of certain nodes would be combined. These nodes sent 409,000, 368,000, and 406,000 messages respectively, and on average, each node sent 13.1, 11.8, and and 13.0 packets per transaction respectively. We had expected that a larger quorum would lead to a significant increase in the number of messages sent per transaction, but this was not the case.

The introduction of quorums into the Stellar Consensus Protocol likely explains the enormous difference in packets transmitted between SCP and RPCA. Using the formulas described above, a Stellar transactions uses roughly $4e-9$ kWh of electricity per node per transaction. A formula for the energy usage of the Stellar network in kilowatt hours can be formulated as shown in Eqs. (3)(4)(5) using the regression model based on the testbed data, where $\boldsymbol{v}$ is the amount of energy required to validate a transaction locally and $\boldsymbol{c}$ is the amount of energy used for communications between nodes:

$$\boldsymbol{e} = \boldsymbol{n} * \boldsymbol{t} * (\boldsymbol{v} + \boldsymbol{c}) \tag{3}$$

$$\boldsymbol{e} = \boldsymbol{n} * \boldsymbol{t} * (1.91e^{-6} + 4e^{-9}) \tag{4}$$

$$\boldsymbol{e} = \boldsymbol{n} * \boldsymbol{t} * 1.914e^{-6} \tag{5}$$

V. Related Work and Discussion

In a most recent work, Suankaewmanee et al. [15] studied the performance of a mobile commerce application using blockchain technology in terms of computation time, energy consumption, and memory utilization. Our work is new and different from the existing work in that our models are built upon real-world data and can be used to estimate the energy consumption of large blockchain systems before building them. This holds particular value for IoT blockchains, which may contain a large number of full nodes performing validation work.

Take, for example, a series of sensors such as surveillance cameras and IoT clusters placed in the city transportation systems and related data gathered from multiple organizations and crowdsensing [23] that can be used to determine weather and traffic patterns. This would allow city planners to predict road, bridge, and subway traffic and adjust traffic control signals during rush hours, help drivers and commuters avoid congested spots, and let people know when roads are cleared after snowstorms. However, in a large city such as New York this system would require tens of thousands of sensors and data from many different organizations and entities. Although hierarchical system architecture may be used to reduce the number of full nodes or validator nodes if IoT blockchains are used by this system, together these nodes can have a significant impact on the power requirements of such a system. The research presented in this paper can be used to help system designers understand the impact of such IoT blockchain projects before implementing them.

The variation in the number of packets sent based on Quorum size was touched upon when discussing Stellar, but similar principles can be applied to other blockchains. Nodes running validators for Ripple, for example, may need to send more messages as the size of the network grows.

Due to time and resource constraints, we were unable to test the energy usage of the consensus mechanisms with networks of different sizes. Because of this, we do not know the nature of the relationship between the number of nodes and either form of energy consumption (i.e. local or packet-dependent). We have assumed for the purposes of this paper that the relationship is linear but that assumption itself is worth testing in the future.

VI. Conclusion and Future Work

The salient features offered by IoT for the connected world and by blockchain for distributed trust in data exchanges are harbingers of more and more IoT blockchain projects. There are many blockchain consensus algorithms, each with its own set of strengths and weaknesses. However, there is lack of formal methods in comparing their energy consumption performance. If any blockchain is going to be used for real-world and large-scale IoT applications, this analysis should be done and our work here will encourage others to research further. Blockchain transactions will likely always consume more energy than credit card transactions, but trust is expensive and the trust that blockchain technologies can provide comes at the cost of energy rather than manpower.

In our research we have collected real-world data that reflect the energy consumption features of several consensus algorithms of blockchain, such as PoW, RPCA, and SCP, and modeled their energy consumption behaviors. In this work-in-progress paper, we report our preliminary results based on linear models using the LASSO regression model. These models provide reference estimations of the energy consumption impact in designing blockchains for IoT systems.

As a major barrier for large-scale IoT blockchains is the transaction time, future research could be conducted to find out how the size of blockchain networks impacts the transaction time and what trade-offs between the energy usage and the transaction time may be on large-scale blockchains.

Appendix
Table of Variables

Variable	Meaning
$\boldsymbol{c}$	Energy used to communicate between nodes
$\boldsymbol{e}$	Energy for a machine to validate a transaction
$\boldsymbol{f}$	Average transaction fee
$\boldsymbol{h}$	Network hashrate
$\boldsymbol{o}$	Average confirmation time for a transaction
$\boldsymbol{t}$	Number of transactions in the last 24 hours
$\boldsymbol{v}$	Energy to validate a transaction locally (Stellar)

REFERENCES

[1] S. Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System, 2008. http://bitcoin.org/bitcoin.pdf, accessed in May 2018.

[2] R. Farell. An Analysis of the Cryptocurrency Industry, *Wharton Research Scholars*, 2015. http://repository.upenn.edu/wharton_research_scholars/130, accessed in June 2018.

[3] X. Xu et al. A Taxonomy of Blockchain-Based Systems for Architecture Design, in *Proceedings of IEEE International Conference on Software Architecture* (ICSA), Gothenburg, Sweden, pp. 243-252, 2017.

[4] P. Vasin. BlackCoins Proof-of-Stake Protocol v2, 2014. https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf, accessed in June 2018.

[5] NEM Technical Reference, Version 1.2.1, February 23, 2018. https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf, accessed in June 2018.

[6] D. Schwartz, N. Youngs, and A. Brittos. The Ripple Protocol Consensus Algorithm, *Ripple Labs Inc.*, 2014.

[7] On Worldwide Consensus. *Medium, A Stellar Journey*, Apr. 8, 2015. URL: medium.com/a-stellar-journey/on-worldwide-consensus-359e9eb3e949, accessed in May 2018.

[8] M. Pease, R. Shostak, and L. Lamport. Reaching Agreement in the Presence of Faults, *Journal of Association for Computing Machinery*, Vol. 27, pp. 228-234, 1980.

[9] T. Qiu, N. Chen, K. Li, M. Atiquzzaman and W. Zhao. How Can Heterogeneous Internet of Things Build our Future: A Survey, *IEEE Communications Surveys & Tutorials*, February 2018.

[10] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi. Internet of Things for Smart Cities, in *IEEE Internet of Things Journal*, Vol. 1, No. 1, pp. 22-32, Feb. 2014.

[11] K. Christidis and M. Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things, *IEEE Access*, Vol. 4, pp. 22922303, 2016.

[12] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Whlisch. Information Centric Networking in the IoT: Experiments with NDN in the Eild, in *Proceedings of the 1st ACM Conference on Information-Centric Networking* (ACM-ICN '14), pp. 77-86, New York, NY, USA, 2014.

[13] https://digiconomist.net/bitcoin-energy-consumption, accessed in May 2018.

[14] U.S. Energy Information Administration. Frequently Asked Questions - How much electricity does an American home use? https://www.eia.gov/tools/faqs/faq.php?id=97&t=3, accessed in June 2018.

[15] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang and Z. Han. Performance Analysis and Application of Mobile Blockchain, in *International Conference on Computing, Networking and Communications (ICNC)*, Maui, Hawaii, USA, March 2018.

[16] V. Buterin. Ethereum: Platform Review - Opportunities and Challenges for Private and Consortium Blockchains, 2016. https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57506f387da24ff6bdecb3c1/1464889147417/Ethereum_Paper.pdf, accessed in June 2016.

[17] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem, *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, July 1982. URL: people.eecs.berkeley.edu/ luca/cs174/byzantine.pdf, accessed in May 2018.

[18] D. Mazires. The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus, Stellar Development Foundation, July 14, 2015.

[19] https://BitInfoCharts.com, accessed in May 2018.

[20] Red Hat, Inc. Working With Playbooks. URL: https://docs.ansible.com/ansible/2.5/user_guide/playbooks.html, accessed in June 2018.

[21] S. L. Kukreja, J. Lfberg, M. J. Brenner. A Least Absolute Shrinkage and Selection Operator (LASSO) for Nonlinear System Identification, *IFAC Proceedings Volumes for the 14th IFAC Symposium on System Identification*, Vol. 39, No. 1, pp. 814-819, Newcastle, Australia, 2006.

[22] scikit-learn developers. sklearn.linear_model.LinearRegression, Scikit-Learn. URL: scikit-learn.org/stable/modules/generated/sklearn.linear_model.LinearRegression.html, accessed in June 2018.

[23] H. Ma, D. Zhao and P. Yuan. Opportunities in Mobile Crowd Sensing, *IEEE Communications Magazine*, Vol. 52, No. 8, pp. 29-35, August 2014.