2018 IEEE 38th International Conference on Distributed Computing Systems

Towards Realistic Energy Profiling of Blockchains for securing Internet of Things

Sriram Sankaran, Sonam Sanju, Krishnashree Achuthan
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Amritapuri, Kollam-690525
Email: srirams@am.amrita.edu

***Abstract*—Internet of Things (IoTs) offers a plethora of opportunities for remote monitoring and communication of everyday objects known as things with applications in numerous domains. The advent of blockchains can be a significant enabler for IoTs towards conducting and verifying transactions in a secure manner. However, applying blockchains to IoTs is challenging due to the resource constrained nature of the embedded devices coupled with significant delay incurred in processing and verifying transactions in the blockchain. Thus there exists a need for profiling the energy consumption of blockchains for securing IoTs and analyzing energy-performance trade-offs. Towards this goal, we profile the impact of workloads based on Smart Contracts and further quantify the power consumed by different operations performed by the devices on the Ethereum platform. In contrast to existing approaches that are focused on performance, we characterize performance and energy consumption for real workloads and analyse energy-performance trade-offs. Our proposed methodology is generic in that it can be applied to other platforms. The insights obtained from the study can be used to develop secure protocols for IoTs using blockchains.**

I. Introduction

The term Internet of Things refers to a network of tiny embedded devices interacting with everyday objects known as things with applications in numerous domains such as Smart home, Industrial Automation, Smart healthcare, Automotive, transportation etc. Typically, networks in IoTs are organized in a hierarchical manner where embedded devices communicate their observations to mobile gateways such as smartphones which in turn are connected to the Cloud servers for processing and analytics. IoTs are often application-driven which leads to numerous security challenges that need to be addressed before they are commercially deployed and widely accepted.

Blockchains are composed of a network of distributed computing nodes operating without a trusted third party and capable of transferring assets from one entity to another. While banking is one of the promising applications of blockchains for transferring digital currencies, there are numerous emerging domains such as Tracking, health care monitoring, automotive etc. where blockchains could be applicable. The heart of blockchains relies on an open and a distributed ledger where miners capable of validating the transactions receive rewards for expending their CPU cycles.

Applicability of blockchains to IoTs is challenging due to the following reasons. First sensors in IoT are resource constrained thus necessitating the need for lightweight solutions. Further interaction with the cloud servers emphasizes the need for an end-to-end approach for securing IoTs using blockchains. Finally, mining process is subject to significant delays due to massive amount of CPU cycles invested in validating transactions. Thus, analyzing energy and performance requirements when blockchains are applied to IoTs becomes necessary depending on the needs of applications.

In this work, we profile the energy impact of blockchains using real experimentation for Ethereum platform, since it is one of the widely used platforms. In particular, we set-up the Ethereum platform for IoTs that are composed of embedded devices such as Raspberry PIs and PCs. Further, we analyze the impact of workloads based on Smart contracts and estimate the power consumed by different operations on the platform. Our proposed methodology is generic in that it can be applied to other platforms for comparative analysis. Also, our analysis can be used to develop protocols for securing IoTs using blockchains.

II. Related Work

Nakomoto *et al.* [1] conceptualized the idea of Bitcoin and developed a practical system for transferring money among entities connected in a peer to peer manner. Based on this idea, several distributed computing platforms for blockchains such as Ethereum [2] and Hyperledger [3] used to power bitcoins were developed. One of the major differences between these platforms is the consensus protocol used by the computing nodes for reaching an agreement.

To ensure the feasibility of blockchains, performance analysis was carried out using different workloads and the impact of different parameters was investigated. Pongnumkul *et al.* [4] analyzed the performance of different workloads for Ethereum and Hyperledger platforms and showed a linear relationship between performance and application parameters. Similarly, Suankaewmanee *et al.* [5] analyzed the performance of mobile blockchains and developed a framework for efficient execution of mining on mobile devices.

In addition to performance, scalability [6] and security of blockchains have been analyzed for different environments such as healthcare [7] and IoTs [8] [9] [10]. Also security of blockchains have been analysed [11]. Zyskin *et al.* [7] developed an approach for securing healthcare records using

2575-8411/18/$31.00 ©2018 IEEE
DOI 10.1109/ICDCS.2018.00148

a combination of blockchains and attribute-based encryption. Dorri *et al.* [8] [10] proposed a lightweight approach for securing smart home based IoTs using symmetric key based primitives.

While there exist approaches for performance analysis and security, little has been done to analyze the energy impact of blockchains, which could be one of the limiting factors to adoption of blockchains in critical applications. Dwyer *et al.* [12] measured and analyzed the energy footprint of bitcoins. Kreku *et al.* [13] analyzed the efficiency of blockchains for IoTs using simulations. Our earlier work [14] modeled core-level power consumption as a function of the activity of individual cores using linear regression. In contrast to existing approaches, we characterize the energy and performance impact of blockchains for IoTs using real benchmarks and analyze the energy-performance trade-offs.

III. Background

Blockchains are de-centralized networks of computing entities [15] that power bitcoins [1] for performing transactions across computing entities through digital currencies. These networks operate without the need for trusted intermediaries thus preventing single form of failure. Ethereum [2] and Hyperledger [3] are two of the most prominent platforms for blockchains. While the underlying technology is common in both the platforms, these differ in terms of consensus protocols which have implications on overall system performance.

In a blockchain, each transaction is digitally signed by the computing entities using the Elliptic Curve Digital Signature Algorithm (ECDSA), since it provides non-repudiation. Further, miners validate transactions and preserve the integrity of the transactions by applying a hash and appending the latest block to the previous one, thus preventing data tampering. In addition, blockchains provide an ability to audit transactions in a secure manner. There can be an arbitrary number of transactions in each block. Finally, these blocks need to be replicated across the nodes in the blockchain so as to preserve consistency.

In Ethereum, consensus is based on choosing the block with the highest total difficulty. Difficulty is a measure of work required to find a hash with a unique number of leading zeros. Ethereum uses Proof of Work [11] for consensus which involves finding a nonce input to the algorithm, so that the result is below a certain threshold depending on the difficulty. The difficulty is dynamically adjusted so that, on an average, a block is produced by the network every 12 seconds.

It is necessary to understand the notion of gas and gas limit in Ethereum. Gas is a limited resource consumed by transactions which are executed by miners. The maximum gas per block is decided by miner's vote which imposes a global rate limit called gas limit on the transactions. Gas limit acts as a safety mechanism to protect the node from depleting their resources which may be caused due to intentional or unintentional errors.

The use of blockchains raises privacy concerns since the transactions performed in the blockchain are typically visible to computing entities. Further, miners need to be trusted since they validate each of the transactions and add them to the blockchain. Finally, blockchains consume significant amount of energy due to the compute-intensive operations such as mining performed by the entities. These concerns can be alleviated by the use of private blockchains where computing requirements are limited to a certain set of nodes in the blockchain thus resulting in improved privacy, trust and energy efficiency.

IV. Experimental Set-up

In this section, we discuss the experimental set-up for Ethereum blockchain platform along with the tools used for power measurement and benchmarks for evaluation. Figure 1 contains a pictorial description of the experimental set-up used to profile the energy consumption of blockchains.

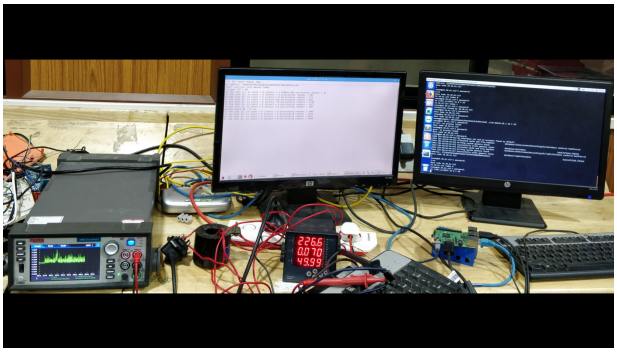

Fig. 1: Experiment Set-up

***Infrastructure*:**

Our infrastructure is composed of Raspberry PI devices acting as clients sending requests to high-end servers for initiating transactions to other clients. Raspberry PI devices contain ARM Cortex-A7 processor with 1 GB RAM and 16 GB SD card and run the Raspbian Jessie Lite operating system. We deploy the Go Version of the Ethereum platform, geth [16] on the Raspberry PIs which are referred as Blockchain nodes.

The experiments were run on a maximum of 6-node cluster. We start with deploying a single node that acts as a client initiating transactions and gradually scale the number of nodes. Once clients initiate a transaction, server performs the compute-intensive task of mining for validating the transaction. Since raspberry PI clients cannot run mining on their own devices due to resource constraints, our set-up involves servers. Upon successful verification, server broadcasts the transaction to other clients which in turn will be logged for data consistency. We chose this architecture such that in the future computation could be offloaded to the IoTs depending on the need of applications.

***Power Measurement*:**

We use the Keithley's series 2461 Source Measure Unit (SMU) [17] for measuring the power consumption of the Raspberry PI boards. SMU integrates both source and measurement circuitry in a single unit thus facilitating a quick and accurate

TABLE I: Blockbench Benchmarks

Benchmark	Description
YCSB	Functions as a Key-Value Storage used for evaluating NoSQL databases Workloads used: 1. Workload A: Update heavy workload Example: Session store recording recent actions 2. Workload B: Read mostly workload Example: Photo tagging
SmallBank	Simulates basic operations on bank accounts such as transferring money from one account to another

measurement of power consumption. Raspberry PI devices are connected to the SMU which logs the power consumed by the devices at distinct time intervals. When the client initiates a transaction, SMU displays the real-time estimate of power consumption for varying system parameters.

In our analysis, we account for power consumed by the operations performed by the Raspberry PI clients and high-end servers. From a client perspective, we analyze the energy consumed for varying parameters such as transaction rates, difficulty, gas limit etc. On the server-side, energy is analyzed when compute-intensive task of mining is performed to validate transactions. Since performance is also a major concern, we estimate performance such as throughput, latency and execution time and analyze energy-performance trade-offs.

***Benchmark Applications*:**

We evaluate our blockchain system using Blockbench benchmark suite [18]. Blockbench is an evaluation framework for analyzing private blockchain platforms. One of the main advantages of Blockbench is that it can be integrated into blockchain platforms through simple APIs and performance of the platform can be measured using the various applications which reflect the operations typically performed on the blockchain.

We integrate Blockbench with the Ethereum platform using the APIs for energy analysis. The core component of blockbench is the Driver that takes as input a workload, user-defined configuration and executes them on the blockchain and outputs running statistics. We implemented the smart contracts for the Blockbench workloads described in Table I for analyzing the energy impact of blockchains on IoTs. Similarly other applications can be profiled and their impact analyzed.

V. Energy and Performance Analysis

In this section, we provide an analysis of energy consumption and performance incurred as a result of operations performed by the clients and servers in the Ethereum platform. Our experiments consist of IoT clients initiating transactions for other clients through a server which mines the transactions and adds them to the blockchain. Our metrics for evaluation are the following.

Throughput: It is measured as the number of successful transactions per second. Throughput T is estimated using the following equation

$$T = N_{transactions}/T_{time} \tag{1}$$

where $N_{transactions}$ and T_{time} refer to number of transactions and unit time respectively.

Latency: It is denoted as the response time per transaction. Latency L is estimated using the following equation

$$Latency = T_{response}/N_{transactions} \tag{2}$$

where $T_{response}$ and $N_{transactions}$ refer to the sum of response time of all transactions per unit time and number of transactions respectively.

Average Power: It is measured as the power consumed per unit time. Average Power $P_{average}$ is estimated using the following equation

$$P_{average} = P_{total}/T_{time} \tag{3}$$

where P_{total} and T_{time} refer to total power consumption and unit time respectively.

A. Power consumption of IoT

In this subsection, we analyze the power consumed by IoT clients. In particular, when IoT clients initiate the transactions, sourcemeter connected to the clients facilitates the power traces to be observed for a period of time. Figure 2 contains the results for power consumed by IoT for static workloads. In our experiments, transaction rate was set to 16 transactions/sec, difficulty level to 2097151 and gas limit of 8000K.

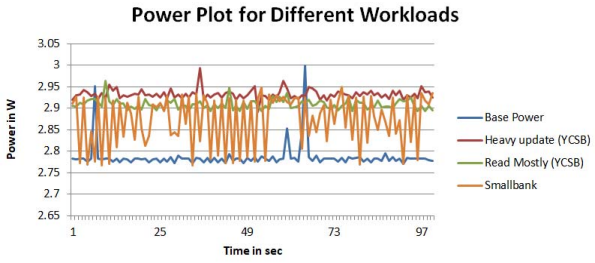

Fig. 2: Power Consumption of IoT

The results indicate that devices incur a certain amount of base power. In addition, each of the workloads has a corresponding impact on the power consumption. In particular, Heavy Update workload from YCSB consumes the most amount of power followed by Read Mostly since Heavy Update requires 50% of transactions to be updated on the blockchain while Read Mostly requires only 5% to be updated. We also observe the fluctuating power consumption of Smallbank due to variable number of transactions.

B. Performance of IoT

In this subsection, we estimate throughput and latency for varying number of parameters such as Transaction rates, difficulty levels, gas rates etc for numerous workloads. In addition, we also analyze the impact of scaling on performance for the workloads.

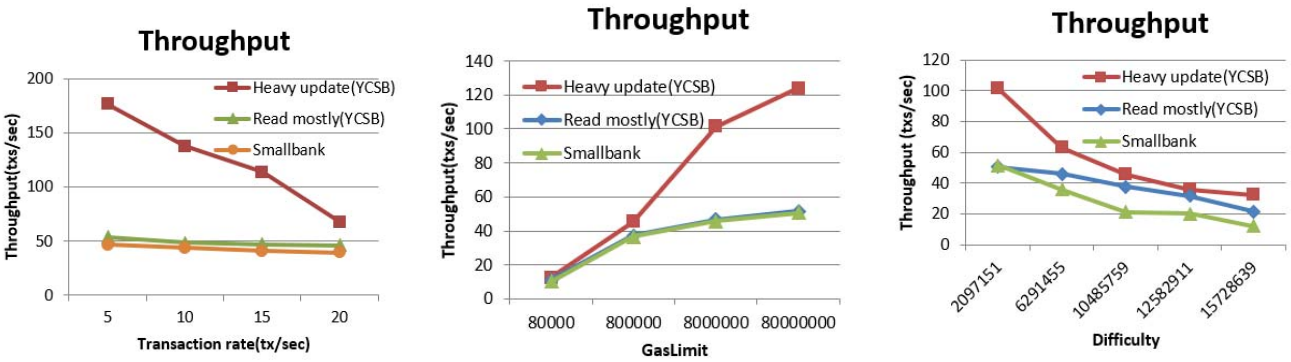

Fig. 3: Throughput

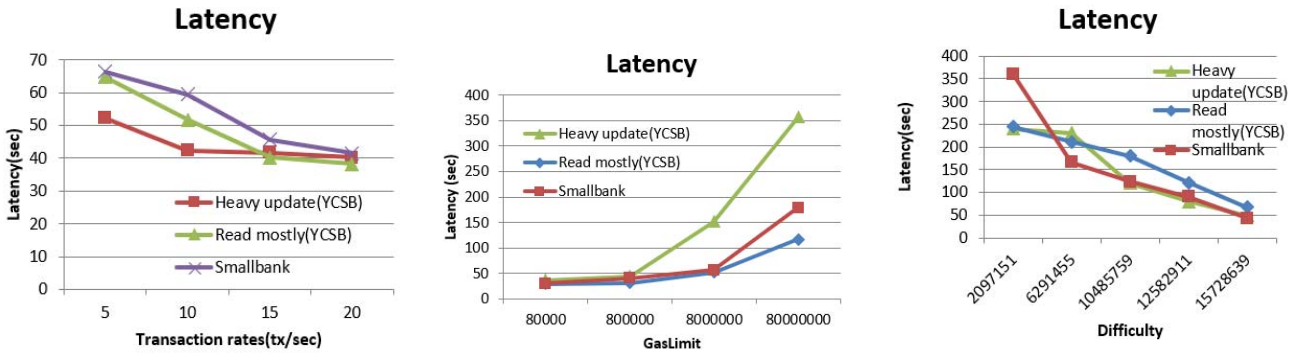

Fig. 4: Latency

Figure 3 contains the results for throughput. The results indicate that as transaction rate increases, throughput decreases since increasing number of transactions need to be processed. Also with increase in difficulty, throughput decreases since mining rate decreases [11]. However, when the gas limit increases, throughput increases since there exists more capacity for processing transactions.

Figure 4 contains the results for latency. Latency increases with increase in gas limit since there exists more capacity for processing transactions. However, increase in difficulty results in decrease in latency since mining rate decreases and that there exists lesser number of blocks for mining. Similarly, latency decreases with increase in transaction rates since there exists lesser number of transactions available for validation.

1) Impact of Scaling: We scale the number of nodes and analyze its impact on performance. In particular, we increase the number of IoT clients initiating transactions to other clients via a server and measure throughput and latency for different workloads. Figures 6 and 7 contain the results for Throughput and latency respectively for minimum and maximum number of nodes.

The results indicate that as we scale the number of nodes, server receives increasing amount of requests to validate the transactions and add them to the ledger. This causes the throughput to decrease and latency to increase when the number of nodes are increased. In particular, the rate at which throughput decreases is significant for Heavy update workload part of YCSB compared to others due to the overhead involved in updating the transactions on the blockchain.

C. Power consumption of Mining

In this subsection, we analyze the power consumed due to mining for varying parameters such as transaction rates, gas limit, difficulty etc. The process of mining is claimed to be resource-intensive [19] [12] due to significant amount of computational time invested by the miners for validating transactions and adding them to the blockchain. We are not aware of any work that characterizes power consumed due to mining for varying parameters.

Figure 5 contains the results for mining power for varying number of transaction rates, gas limit, difficulty etc. The results indicate that as transaction rates and gas limits increase, number of transactions processed consequently increases for each of the workloads. In contrast, mining power decreases with increase in difficulty since difficulty is inversely proportional to mining rate [11]. Increasing number of nodes does not affect the mining power due to the sequential nature of the nodes.

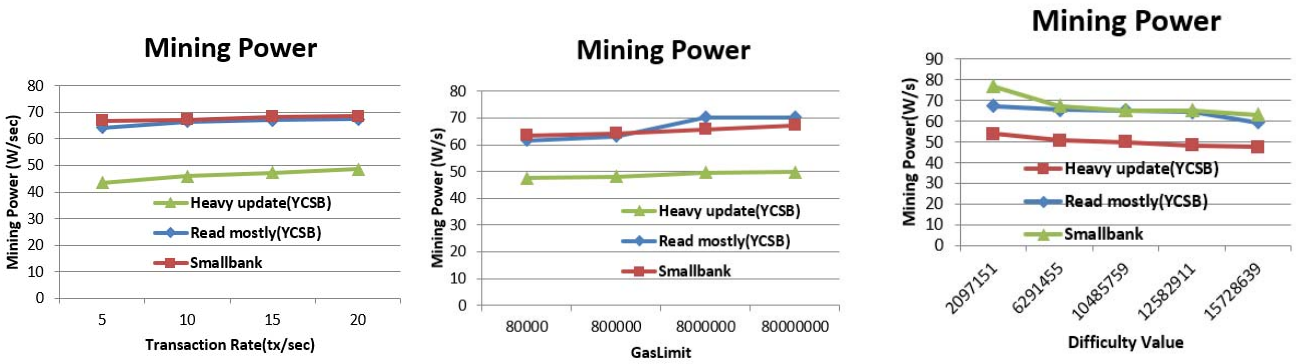

Fig. 5: Mining Power

TABLE II: Percentage increase in Mining Power

	Heavy update (YCSB)		Read Mostly (YCSB)		Smallbank	
Difficulty	**Mining Power (Watt/sec)**	**Percentage Increase**	**Mining Power (Watt/sec)**	**Percentage Increase**	**Mining Power (in Watt)**	**Percentage Increase**
2097151	53.8497	201.84	67.27	252.17	76.68	287.42
6291455	50.8	190.4	65.46	245.36	67.19	251.86
10485759	49.87	186.92	65.15	244.2	65.22	244.47
12582911	48.341	181.19	64.39	241.36	65.176	244.29
15728639	47.62	178.49	59.45	222.85	63.004	236.15
GasLimit						
80000	47.62	178.49	61.63	231	63.51	238.05
800000	48.08	180.21	63.25	237.07	64.32	241.08
8000000	49.65	186.09	70.26	263.35	65.73	246.37
80000000	49.74	186.43	70.39	263.86	67.35	252.47
Threads						
1	43.227	162.02	62.87	235.68	64.83	243.01
4	44.864	168.16	66.29	248.5	65.3	244.78
8	47.62	178.49	66.76	250.24	65.94	247.16
16	48.314	181.09	66.93	250.88	67.196	251.86
32	48.484	181.72	67.027	252.17	69.46	260.35
Transaction Rate						
5	43.4	162.67	64.1	240.26	66.74	250.16
10	45.98	172.34	66.42	248.96	67.19	251.86
15	47.162	176.77	67.03	251.25	68.39	256.36
20	48.63	182.27	67.27	252.17	68.57	257.03

To determine the percentage increase in mining power for various workloads, we analyze mining power with respect to the base power, P_{base}, which is the power consumed by the platform. We observe the base power, P_{base} to be 26.68W. Thus, percentage increase in mining power can be computed using the following equation.

$$P_{change} = ((P_{mine} - P_{base}) * 100)/P_{base} \quad (4)$$

Table II contains the results for percentage increase in mining power with respect to base power for varying parameters. The results indicate that mining consumes upto thrice as much of base power and that it can be attributed to the proof-of-work consensus protocol used by Ethereum platform. Thus mechanisms for energy efficient mining are necessary to minimize the energy consumed by mining.

VI. Discussion

Comparative Analysis: Although, we have focused on the energy analysis of Ethereum platform, our proposed methodology can be applied to other platforms such as Hyperledger, Ripple etc. for comparative analysis. One of the main differences between these platforms is the consensus protocol which may have a significant factor on energy consumption. For instance, Ethereum uses Proof of Work (PoW) consensus which consumes significant CPU cycles compared to Hyperledger. Although our analysis of power consumption is limited to execution layer, we plan to investigate the impact of consensus layer as part of future work.

Secure Protocols: Our analysis can be used to develop protocols for secure end-to-end communication for IoTs using blockchains. Towards this goal, devices in the IoTs must register securely in the blockchain so as to bootstrap secure communications. Although blockchain platforms provide solutions for preserving integrity and non-repudiation, they need to interface with IoTs from different manufacturers. Further, proposed security solutions need to be platform independent in that it can be applied to any platform. Finally, energy-performance-

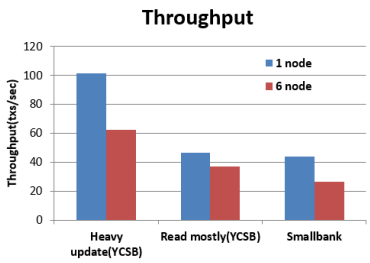

Fig. 6: Throughput

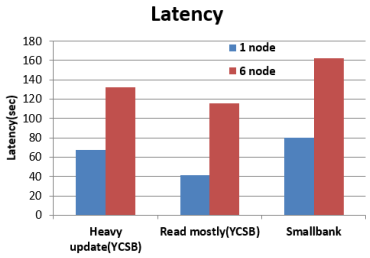

Fig. 7: Latency

security trade-offs of protocols need to be analyzed for varying platforms.

Impact of Scaling: Although our analysis of scaling is limited to a few nodes, scaling to a realistic environment requires a massive number of nodes which we plan to investigate as part of future work. Since compute-intensive task of mining may be resource consuming for IoTs, we can delegate the task of mining to edge nodes [20] or high-end servers for validating transactions initiated by IoTs. Further these servers need to be placed closer to devices depending on the needs of applications so as to incur lesser delay in responding to transactions from IoTs. Finally, servers can distribute the load evenly among servers so as to maximize performance.

VII. Conclusion

In this work, we have profiled the energy consumed by Ethereum blockchain platform using real experimentation and analyzed energy-performance trade-offs. In particular, we construct a blockchain network composed of Raspberry PIs and PCs and connect them to a sourcemeter for measuring the power consumed by different operations in the Ethereum platform. Our analysis reveals that the power consumption depends on the needs of the applications and that mining power is significant compared to other operations in the blockchain. Our proposed methodology is generic in that it can be used to perform a comparative analysis of energy consumed by different platforms. The results from the study can be used to develop secure and lightweight protocols for IoTs using blockchains.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] "Ethereum Project," https://www.ethereum.org/.
[3] "Hyperledger," https://www.hyperledger.org/.
[4] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, July 2017, pp. 1–6.
[5] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, "Performance analysis and application of mobile blockchain," *arXiv preprint arXiv:1712.03659*, 2017.
[6] B. Alangot, M. Suresh, A. S Raj, R. K Pathinarupothi, and K. Achuthan, "Reliable collective cosigning to scale blockchain with strong consistency," in *Proceedings of the Network and Distributed System Security Symposium (DISS'18). NDSS*, 2018.
[7] G. Zyskind, O. Nathan, and A. . Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, May 2015, pp. 180–184.
[8] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, March 2017, pp. 618–623.
[9] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler, and R. A. Popa, "Wave: A decentralized authorization system for iot via blockchain smart contracts," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2017-234, Dec 2017. [Online]. Available: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-234.html
[10] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, April 2017, pp. 173–178.
[11] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 3–16. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978341
[12] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, June 2014, pp. 280–285.
[13] J. Kreku, V. A. Vallivaara, K. Halunen, and J. Suomalainen, "Evaluating the efficiency of blockchains in iot with simulations," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, IoTBDS 2017, Porto, Portugal, April 24-26, 2017*, M. Ramachandran, V. M. Muñoz, V. Kantere, G. Wills, R. J. Walters, and V. Chang, Eds. SciTePress, 2017, pp. 216–223. [Online]. Available: https://doi.org/10.5220/0006240502160223
[14] S. Sankaran, "Predictive modeling based power estimation for embedded multicore systems," in *Proceedings of the ACM International Conference on Computing Frontiers*, ser. CF '16. New York, NY, USA: ACM, 2016, pp. 370–375. [Online]. Available: http://doi.acm.org/10.1145/2903150.2911714
[15] M. E. Peck, "Blockchains: How they work and why they'll change the world," *IEEE Spectrum*, vol. 54, no. 10, pp. 26–35, October 2017.
[16] "Ethereum geth version 1.7.2," https://github.com/ethereum/go-ethereum/wiki/Building-Ethereum.
[17] "Keithley 2400 sourcemeter," *http://www.tek.com/keithley-source-measure-units/keithley-smu-2400-series-sourcemeter*.
[18] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*. ACM, 2017, pp. 1085–1100.
[19] P. Fairley, "The Ridiculous Amount of Energy It Takes to Run Bitcoin ," https://spectrum.ieee.org/energy/policy/the-ridiculous-amount-of-energy-it-takes-to-run-bitcoin, 2017, [Online; accessed 28-December-2017].
[20] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing: Challenges and applications," *arXiv preprint arXiv:1711.05938*, 2017.