Proof-of-Blackouts? How Proof-of-Work Cryptocurrencies Could Affect Power Grids

Johanna Ullrich[1,2] ✉, Nicholas Stifter[1,2], Aljosha Judmayer[1], Adrian Dabrowski[1], Edgar Weippl[1,2]

[1]SBA Research, Vienna, Austria
[2]Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI), Institute of Information Systems Engineering, TU Wien
Email: (firstletterfirstname)(lastname)@sba-research.org

Abstract. With respect to power consumption, cryptocurrencies have been discussed in a twofold way: First, the cost-benefit ratio of mining hardware in order to gain revenue from mining that exceeds investment and electricity costs. Second, the overall electric energy consumption of cryptocurrencies to estimate the environmental effects of Proof-of-Work. In this paper, we consider a complementary aspect: The stability of the power grids themselves. Power grids have to continuously maintain an equilibrium between power supply and consumption; extended periods of imbalance cause significant deviation of the utility frequency from its nominal value and destabilize the power grid, eventually leading to large-scale blackouts. Proof-of-Work cryptocurrencies are potential candidates for creating such imbalances as disturbances in mining can cause abrupt changes in power demand. The problem is amplified by the ongoing centralization of mining hardware in large mining pools. Therefore, we investigate power consumption characteristics of miners, consult mining pool data, and analyze the amount of total power consumption as well as its worldwide distribution of two major cryptocurrencies, namely *Bitcoin* and *Ethereum*. Thus, answering the question: *Are Proof-of-Work based cryptocurrencies a threat to reliable power grid operation?*

1 Introduction

Power grids must continuously keep an equilibrium between power consumption and supply. Power plant operators therefore have to follow the consumer demand, and adjust their supply in accordance. They rely on sophisticated prediction models, and the remaining gap between supply and consumption is closed by control reserve, i.e., power plants in standby. Whereas, a continuous imbalance in the power grid leads to the utility frequency drifting away from its nominal set point of 50 Hz or 60 Hz (depending on the country). If supply exceeds consumption, the frequency of the power grid increases; if supply fails to fulfill consumption, the frequency decreases. The system frequency is indeed an indicator of the power grid's state, and small fluctuations – a few hundred mH

– around the nominal value are normal. However, larger deviations – more than 0.5 Hz — trigger automatic emergency routines such as load shedding or power plant shutdowns. The operators' course of action relies on the assumption that power consumers behave independently of each other, and do not perform concerted actions. Recent work [1] has shown that coordinated control over devices is in fact able to cause load shedding, and large scale blackouts. Therein, the authors assume a botnet that allows an adversary to remotely and simultaneously increase the bots' power consumption. As electronic devices are orders of magnitude faster in modulating their power consumption than control reserve can be activated, the power grid frequency drifts away from its nominal value, finally triggering emergency routines. In addition to reaction speed, the total amount of control reserve, i.e., power plants, in standby is limited.

Proof-of-Work (PoW) cryptocurrencies such as Bitcoin and Ethereum draw substantial amounts of electric power as a consequence of their underlying consensus mechanism, referred to as Nakamoto consensus [2]. In principle, participation in this process is possible for anyone and is governed by economic factors, as prospective miners analyze the cost-benefit ratio of acquiring and providing computational resources to the network in exchange for cryptocurrency units[1]. Up until now, this fact has been discussed primarily in the context of sustainability and the potential ecological impact large scale cryptocurrency mining could entail [3–5]. Some estimates rank Bitcoin's overall electricity consumption comparable to that of medium-sized national states with the potential to grow even further in the future. In this paper, we discuss a complementary, yet unconsidered aspect of cryptocurrencies and power consumption. Specifically, we investigate whether PoW cryptocurrencies could represent a threat to reliable power grid operation that is comparable to the botnet described above. A closer look emphasizes that cryptocurrencies indeed have the potential to be harmful to reliable power grid operation for the following reasons:

– Hardware that is mining a particular cryptocurrency uses the same, or very similarly behaving, software on all nodes. Thus, their power consumption may not be independent of each other and therefore violating the grid operators' assumptions. A single disturbance in the software – may it be a consequence of an occasional error or a malicious action – impacts a large amount of miners at once. For example, a high number of all *Ethereum* nodes experienced an outage due to a software bug in September 2016[2]. If such an event impacts the nodes' power consumption, even minor changes add up to large overall power lifts for the power grid. For example, a Linux leap second bug caused an overall power increase by 1 MW in a single data centre in 2012[3].

[1] https://www.coinwarz.com/cryptocurrency
[2] https://blog.ethereum.org/2016/09/18/security-alert-geth-nodes-crash-due-memory-bug/
[3] http://www.h-online.com/open/news/item/Leap-second-bug-in-Linux-wastes-electricity-1631462.html

– Cryptocurrency nodes are electronic devices, and are thus able to modulate their power consumption in a fast way – typically below 100 ms – which is a few orders of magnitude faster than the reaction speed of the power grid.
– Miners – at least when operating in the same mining pool – share a communication infrastructure to coordinate their efforts. An error in this communication structure or its compromise by an adversary could allow for botnet-style control including manipulation of the participants' power consumption.
– Miners have vast computing power, and therefore draw high amounts of power from the grid. As long as it remains profitable their operators are economically motivated to bring more and more mining hardware into the cryptocurrency network, leading to increased power consumption at high growth rates – without actually improving capacity for the cryptocurrency. Beyond, this growth has been fueled by an ongoing cryptocurrency hype.

Summarizing, cryptocurrencies show potential to become troublemakers for power grids and their reliable operation. In addition to the overall power consumption, the miners' development over time and their geographical spread are of interest for an in-depth analysis. The paper at hand aims to contribute this missing information in order to shed light onto the issue whether cryptocurrencies are a threat to reliable power grid operation. In particular, we answer the following questions:

– How does power consumption of different cryptocurrencies and their mining pools behave over time? Further, how is power consumption geographically spread?
– Which scenarios, e.g., outage of a large number of miners, show potential to impact power grid reliability and which prerequisites have to be met for such an event to affect the power grid?
– Has power consumption of cryptocurrencies already surpassed the threshold of being critical for reliable power grid operation? Respectively, when does power consumption reach this critical threshold considering past growth of cryptocurrencies and their increased mining efficiency?

Due to the large number of available cryptocurrencies, we limit ourselves to the two currently most popular PoW cryptocurrencies by market capitalization and transaction volume, namely *Bitcoin* [6] and *Ethereum* [7]. With respect to the power grid, we investigate the impact on European power grids, among them the *Synchronous Grid of Continental Europe* (formerly UCTE grid) which is the largest power grid by total consumption. Beyond, European grids are considered to be among the most reliable networks.

The remainder of the paper is organized as follows: Section 2 provides a background on power grid operation and cryptocurrencies; Section 3 presents our threat scenario. Section 4 assesses power consumption models with respect to the quality of results. Then, Section 5 investigates cryptocurrencies' current power consumption for mining, while Section 6 investigates the geographic spread of miners by investigating the largest Ethereum mining pool as well as including

publicly available information for Bitcoin. Section 7 analyzes cryptocurrencies' impact on the power grid. Section 8 discusses our results, Section 9 presents related work, and Section 10 concludes.

2 Background

First, this section provides an overview on power grid operation before describing the technology behind cryptocurrencies.

Power Grids in Europe: Power grids have expanded from islands, e.g., a city, to national grids and finally international ones for reasons of higher reliability, as an outage of a single power plant is easier to handle by numerous other plants compensating for the loss. These grids are operated synchronously, i.e., the net sine is of the same frequency at the same angle; otherwise, short circuits would cause harm to the equipment. As electric power cannot be stored at large quantities, grid operators have to keep a balance between consumption and supply at all times. This is achieved in two steps: First, operators estimate power consumptions by means of load profiles. These are sophisticated models forcasting the consumption in dependence of time of the year, weekday, weather forecast and many more parameters. Second, fast power plants are run in stand-by mode to close the remaining gap between consumption and supply. This gap is measured by the network's frequency deviation from its nominal value (50 Hz in European networks). If consumption exceeds supply, turbines of power plants slow down leading to a lower frequency. If supply is higher than consumption, turbines accelerate and this increases frequency as well. Bearing in mind that *fast-reacting* power plants are still relatively slow in comparison to IT equipment [1]. While the latter are able to modulate their consumption within a range of multiple tens of milliseconds to seconds, gas turbines need tens of second for activation. Primary control, the fastest countermeasure reacting to imbalances, in the UCTE network is required to be fully activated within 30 s [8]. Secondary and tertiary control take even longer. Power operators aim to keep the frequency within a band around the nominal value, typically a few hundreds of mHz. Large deviations cause emergency routines [9]: (49.8 Hz) Alerting, Shedding of pumps, (49.0 Hz) load shedding of 10-15 % of total load, (48.7 Hz) load shedding of additional 10-15 %, (48.4 Hz) load shedding of further 15-25 % of load. At frequencies below 47.5 Hz and above 51.5 Hz all power plants are disconnected from the power grid in order to protect mechanical equipment like turbines and generators.

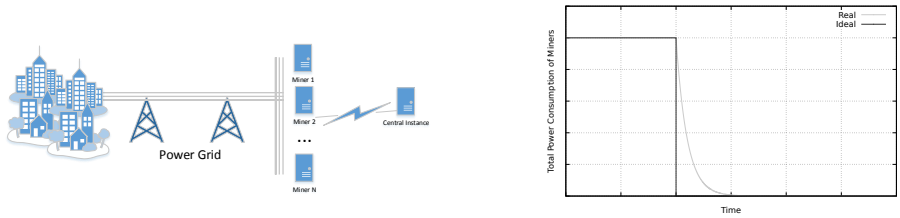
Cryptocurrency Mining: The cryptographic currency *Bitcoin* was inarguably the first successful *decentralized* implementation of an electronic payment system, as it does not have to rely on individual trusted parties to prevent the double spending problem [10]. To achieve resistance against *Sybil attacks* [11], but nevertheless allow for dynamic membership of (consensus) participants, Bitcoin requires some form of pricing mechanism ascribed to the creation of identities in the system. This is achieved through relying on a chained construction

of Proofs-of-Work, the latter of which traces its origins back to the works of *Dwork and Naor* [12] and *Back* [13]. In Bitcoin, *miners*[4] attempt to solve a cryptographic puzzle, namely a partial pre-image attack on the SHA-256 cryptographic hash function. As part of its input it takes a previous puzzle solution as well as a Merkle tree root of newly proposed transactions. Thereby, a cryptographically linked tree of puzzle solutions is formed, of which only the longest consecutive chain with the most cumulative difficulty of puzzles is considered to be the current valid state by honest participants. Under the assumption that the majority of computational power is controlled by honest participants, and that they will only append new solutions to the head of a valid (block)chain, it becomes exponentially difficult for an adversary to alter previous states by presenting a new, longer chain that is considered valid. This mechanism of reaching eventual agreement on a common prefix of chained puzzle solutions is referred to as Nakamoto consensus. The principles behind Nakamoto consensus form the basis for all decentralized PoW cryptocurrencies. Nakamoto consensus also relies on *game theoretic incentives*, whereby operators of mining hardware are rewarded in cryptocurrency units if their puzzle solution eventually ends up as part of the agreed upon valid blockchain. The operators can expect, on average, to successfully mine blocks that end up on the blockchain proportional to the amount of computational power they hold in relation to that of all participants Because mining is a random process with large variance, operators often form their mining hardware together in *mining pools* to benefit from more predictable payouts [14, 15]. Alternative cryptocurrencies often rely on a different Proof-of-Work function to Bitcoin, such as *Ethash* in the case of Ethereum [16]. When we refer to *hash rate* within the course of this paper, we imply the number of trials that are conducted for a given PoW function in an attempt to find a valid solution over a particular time frame.

3 Threat Model

Our threat scenario is depicted in Figure 1(a). We assume an amount of miners of the same cryptocurrency – may it be *Bitcoin* or *Ethereum* – mining the respective cryptocurrency. Each of these miners draws a modest amount of electricity from the power grid. However, in total, power consumption of individual miners add up to a large volume. If all (or a large number of) miners switch from mining to idling abruptly the total power consumption drops within seconds or less. Figure 1(b) depicts this effect from the power grid's perspective. While power consumption ideally would follow an inverse step function, it is likely that the real-world behavior is slightly smoother. The surplus of energy in the grid will lead to an increased frequency until the control reserves try to stabilize the system. However, due to generators' inertia, activation takes up to 30 seconds. If the miners' reduction in consumption is high enough the induced frequency shift

[4] We use the term *miners* as equivalent for mining hardware (and not the operators of this hardware).



(a) Scenario: In normal operation, miners draw high amounts of electric power from the grid.

(b) Qualitiative progression of totalled power consumption in presence of an incident.

Fig. 1: Threat model: An (occasional or malicious) incident leads to the outage of miners eventually causing totalled fluctuations on power consumption.

can (temporarily) exceed thresholds for emergency routines, eventually causing load shedding or shutdown of power plants.

In order to cause such an incident, the adversary requires the possibility of instantly forcing a high number of miners into idling. We therefore assume a central instance as depicted in Figure 1(a). This central instance is able to directly or indirectly influence miners which might appear artificial at first. However, in the past, cryptocurrencies have already experienced comparable situations, as emphasized in the following enumeration: (1) *Antbleed*[5] included a backdoor in the *Antminer* mining hardware that allowed the vendor to remotely shutdown devices. Its exploitation could have caused an estimated outage of up to 70 % of all mining equipment in the *Bitcoin* network. (2) In September 2016, *Ethereum* experienced an outage of lots of nodes due to a bug in the centrally maintained software[6]. The software as a central instance indirectly (and unintentionally) told the miners to stop mining by software malfunction, leading to a sharp decrease in hash rate of over 10 %. (3) Mining is typically performed in mining pools, i.e., miners jointly aim to create the next block in order to reduce variance and maximize revenue. Therefore, miners are connected to a central server or centrally managed infrastructure that forwards them their share of hashing puzzles. Malfunction or hostile takeover of the server and/or its communication – the de-facto standard is the *Stratum* protocol [17] – bears potential to take control over the hash rate of all miners in the pool. It has been already confirmed that fluctuations in consumption caused by botnets are able to trigger large frequency shifts and eventually load shedding and shutdown of power plants [1]. In this paper, we investigate whether *Bitcoin* or *Ethereum* is able to cause such large deviations threating reliable operation of the power grid.

[5] http://www.antbleed.com/
[6] https://blog.ethereum.org/2016/09/18/security-alert-geth-nodes-crash-due-memory-bug/

Model	Total Hash Rate	Power Consumption of Miners	Release Date of Miners	World Power Consumption	Mining Revenue	Acquisition Costs of Miners	Miner Lifetime	Ratio Electricity to Acquisition Costs	Electricity Price	Suitability of Model
O'Dwyer and Malone [3]	✓	✓								✓
Vranken [5]	✓	✓		✓	✓	✓			✓	✗
Deetman [18]	✓	✓	✓				✓			✓
The Vries [19]					✓			✓	✓	✗

Table 1: Usage of parameters in power consumption models: *Suitability* describes whether a model uses suitable parameters for estimation, see Table 2.

4 Assessment of Models for Power Consumption

In a first step, we need an estimation of the total power consumption of the respective cryptocurrencies. Multiple models – both from the world of academia as well as beyond – are available; however, they significantly differ with regard to their underlying assumptions, not to mention their final outcome on total power consumption. In addition, they mainly focus on Bitcoin. In the following paragraphs, we assess these models and their parameters with respect to the quality of the results. Finally, we decide for a model that is built upon within the remainder of this work.

- *O'Dwyer and Malone* [3] calculate an upper and lower bound for worldwide Bitcoin energy consumption based on the network's hash rate and consumption values of commodity hardware and specialized mining hardware. The authors did not aim to model the actual mix of mining hardware, and they could only conclude that the consumption lies between the calculated upper and lower bound.
- *Vranken* [5] calculated power consumption under the assumption that all Bitcoin mining is done on (i) CPUs, (ii) GPUs, (iii) FPGAs or (iv) ASICs before bounding power consumption by means of (a) the total world power production, (b) assuming that the total mining revenue is spent on electric power, and finally the (c) inclusion of acquisition costs. As *O'Dwyer and Malone*, there has been no effort to model the actual hardware mix of the mining network.
- *Deetman* [18] aimed to overcome the above drawback by modeling the hardware mix of the mining network in a more sophisticated way. First, the author inferred the decrease of power consumption per hashing operation over time based on mining hardware's specification and its release data. In

*P*arameter	*I*nformation Source	*S*uitable
Total Hash Rate	Based on Difficulty & Block Arrival Times	✓[a]
Power Consumption of Miners	Data sheets, Reviews	✓
Release Date of Miners	Data Sheets, Press Release	✓
World Power Consumption	Public Statistics	✓
Mining Revenue	Block Reward & Transaction Fees	✓
Acquisition Costs of Miners	Press Releases, Reviews	✗[b]
Miner Lifetime	General	●[c]
Ratio Electricity to Acquisition Costs	Based on Electricity Priceand Acquisition Costs	✗[d]
Electricity Price	Energy Providers	✗[e]

Table 2: Parameters with regards to suitability for power consumption modeling (✓Good, ●Intermediate, ✗Poor)

[a] Both, difficulty and block arrival time can be directly extracted from the blockchain.
[b] Acquisition costs including shipment vary depending on time and country.
[c] IT equipmentment is generally considered to have short life times of 12 to 18 months.
[d] Energy prices and acquisition costs vary significantly and so does their ratio.
[e] Energy prices are dependent on country and customer type (domestic, industrial).

a second step, the increase of hash rate per month has been attributed to newest hardware (that is then assumed to run three to five years before being removed from the mining network again), then, finally leading to the average power consumption of the respective hardware mix. By means of the hash rate, the total power consumption was calculated.

– *The Vries* [19] follows a financially-oriented approach assuming that a certain ratio of the network's mining revenue is spent on electricity (60 % with Bitcoin, 22 % with Ethereum). Assuming an average energy price (US$ 0.05 per kWh with Bitcoin, US$ 0.12 per kWh with Ethereum[7]), the total power consumption of the mining network is derived. The author claims that this model does not only include power consumption that is directly used for mining but also the power for additional needs, e.g., data center cooling.

Table 1 provides an overview of the parameters that are included into the calculation of each model. The parameters show diverse characteristics, e.g., with regard to fluctuations or validity of data sources, that influence the model's quality of prediction. Table 2 provides an assessment of the parameters included for power consumption estimation with respect to the source of information and their suitability. While some of them can be gained from (rather) authoritative sources like the blockchain directly, data sheets, reviews or press releases that are stable with respect to time and geographic location; others heavily fluctuate, in particular acquisition and electricity costs. Thus, we consider the first category as being suitable for power consumption estimation; the latter category as inappropriate – they would cause heavily fluctuating final results as well. In the last column, Table 1 highlights the models using only suitable parameters.

[7] According to the author, Ethereum is rather mined at residential homes; thus, residential rates apply.

From these models, *Deetman*'s appears most suitable for our purpose of estimating a mining network's total power consumption for the following reasons: (i) The included parameter values are based on confirmed sources, are neither heavily fluctuating nor geographically dependent.[8] (ii) A mix of mining hardware is considered; results are more practical than the calculation of lower and upper bounds as done by *O'Dwyer and Malone*'s model. (iii) The result includes the power consumption that is directly used for mining only. This matches our threat model in Section 3, i.e., the adversary is solely able to influence the mining hardware remotely, but not supporting measures such as cooling. (iv) The approach is universally applicable for all cryptocurrencies.

5 Total Power Consumption of Popular Mining Networks

After deciding for an appropriate model for power consumption, in this section, we describe our approach in detail and present the results for Bitcoin and Ethereum.

Methodology for Power Consumption Estimation: For estimating the total power consumption of a cryptocurrency, we performed the following steps:

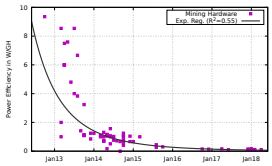
1. We collected the overall hash rates as well as power consumption for typical mining hardware of the respective currency from data sheets or reviews, and calculated the power consumption per computed hash (W/H). Current as well as outdated hardware has been included.
2. In addition, we collected the release dates of mining hardware from data sheets and press releases.
3. Assuming that power consumption per hash decreases over time due to better hardware, we performed a regression analysis to find a trend in miners' power efficiency based on the data that has been collected in step 1 and 2.
4. While the result of step 3 provides insight into the further development of miner efficiency, the hash rate of the entire cryptocurrency's mining process has to be calculated to obtain the overall network's power consumption. Following the algorithm of *Ozisik et al.* [20], we inferred the overall hash rate including the parameters *target (respectively difficulty)*, *time interval* between consecutive blocks and the observed *hash values*. These values have been gained directly from the respective public blockchain.
5. At a certain point in time, mining is not exclusively performed on newest hardware but also on older hardware; therefore, we aim to create a representative hardware mix. We assume that the increase in a cryptocurrency network's hash rate is caused by current hardware and that the hardware contributes hashes to the network for a fixed time period of six months

[8] The only arguable parameter is the hardware's total runtime. Therefore, we followed a twofold approach to test its plausibility: On the one hand, we collected typical runtimes in the community confirming our assumption. On the other hand, we argue that the range of plausible values does not change the result significantly.

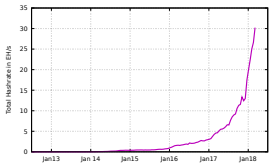
(Bitcoin) or 12 months (Ethereum). Instead of including power efficiency of individual miners into our calculation, we take the values from the regression analysis of step 3.

6. Finally, we infer the cryptocurrency's total power consumption for the hardware mix from step 5. We multiply the hash rates with the assigned power efficiency for every entry within the hardware mix.

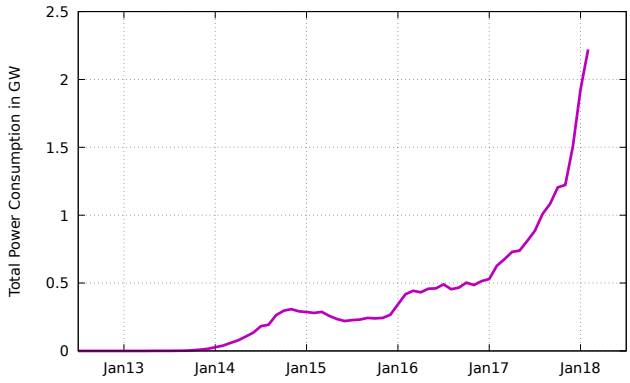
The gained results, as well as specifics, for Bitcoin and Ethereum are presented in the remainder of this section.



(a) Power efficiency of ASIC miners.



(b) Total hash rate.

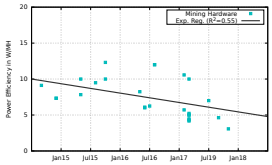


(c) Total power consumption.

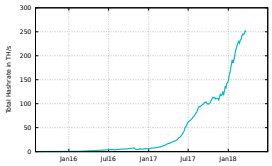
Fig. 2: Results for the Bitcoin network.

Total Power Consumption of Bitcoin: Collecting data for Bitcoin miners was based on a hardware list from the Bitcoin Wiki[9], we cross-checked the provided parameters for hash rate and power consumption and added release dates. However, we faced various difficulties: (a) Due to bankruptcies, companies producing hardware disappeared from the market and data sheets of their hardware is not available anymore (if ever present). In such cases, we relied on technical reviews on the respective hardware and blogs or forum posts of the active Bitcoin community. (b) Delivery dates were not met in multiple cases; shipment was delayed by multiple months and eventually the miners went online later than initially announced. Therefore, we verified the initial announcements from the hardware vendors with community posts. In case of delays, we included the actual shipping date into our calculation. (c) Some products have never been shipped at all, or we did not find any specification indicating their hash rate and/or power consumption. For these reasons, we excluded twelve miners from the original

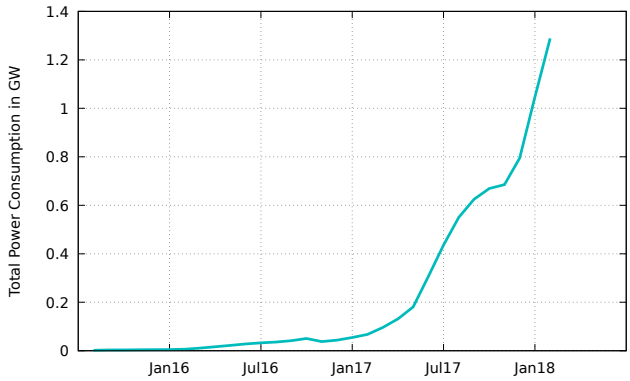
[9] https://en.bitcoin.it/wiki/Mining_hardware_comparison



(a) Power efficiency of GPUs.



(b) Total hash rate.



(c) Total power consumption.

Fig. 3: Results for the Ethereum network.

list containing 83 miners. As commodity hardware and field-programmable gate arrays (FPGAs) have become outdated for multiple years already, we focused on application-specific integrated circuit (ASIC) miners. The gained results for power efficiency, total hash rate and total power consumption are depicted in Figure 2: The power efficiency increased over time and as of February 2018, the mix of mining hardware requires 0.049 W/GH. The total hash rate of the Bitcoin network is estimated to be 30.2 EH/s and the total power consumption 2.2 GW.

Total Power Consumption of Ethereum: Ethereum is predominantly mined on (commodity) Graphics Processing Units (GPUs). Therefore, we collected data on GPU models commonly suggested for Ethereum mining. In comparison to Bitcoin mining, we were able to rely on specifications by the dominant players in the market, namely AMD Radeon and Nvidia GeForce. The results are depicted in Figure 3: The power efficiency increased over time and as of February 2018 is 5.2 W/MH. The total hash rate of the Ethereum network is estimated to be 253 TH/s and the total power consumption 1.3 GW. In comparison to Bitcoin, Ethereum mining hardware requires more power per hash. Thus, even though Ethereum's total hash rate is less than Bitcoin's, the power consumption has roughly the same magnitude. Beyond, linear regression provided best results for Ethereum while exponential for Bitcoin. Based on these facts, we believe that there is still room for improvement in further development of Ethereum mining hardware while efficiency gains for Bitcoin will be minimal in the future.

6 Geographic Spread of Miners

After calculating the total power usage of Bitcoin and Ethereum mining, we have to determine the share of consumption in distinct power grids. Therefore,

we analyze the biggest mining pools of both cryptocurrencies to infer the geographical spread of their miners. With respect to power grids, we focus on the following European systems as they are considered to be among the most reliable networks and rarely face blackouts: (A) The *Synchronous Grid of Continental Europe (UCTE grid)* spans 29 European and North African countries[10]. (B) *NORDEL* is a synchronous power grid comprising Denmark[11], Finland, Norway and Sweden. (C) Iceland, Ireland, and the United Kingdom each operate an island network of their own for geographic reasons. These individual synchronous grids are typically interconnected by DC lines; however, they are only able to provide a small ratio of the overall power consumption and cannot compensate major imbalances.

	Ethereum			*Bitcoin*		*Grid Characteristics*	
	ethermine	Lower Bound	Upper Bound	Lower Bound	Upper Bound	Total Load	Reference Incident
UCTE	22.1%[a]	79 MW	284 MW	56 MW	1194 MW	296.8 GW	3000 MW
NORDEL	1.41%	5 MW	18 MW	4 MW	68 MW	38.5 GW	600 MW
Iceland	0.18%	0.6 MW	2 MW	0.6 MW	9 MW	2.0 GW	90 MW
Ireland	0.09%	0.3 MW	1 MW	0.2 MW	4.3 MW	3.0 GW	160 MW
Great Britain	1.12%	4 MW	14 MW	2.8 MW	54 MW	34.7 GW	400-700 MW

Table 3: Power consumption of mining with regard to European power grids.

[a] From the overall *ethermine* hashrate measured from 2018-02-26 to 018-03-26

Due to the sources available to us, we had to follow two distinct approaches for Bitcoin and Ethereum to estimate the ratio per synchronous grid.

Geographic Spread of Ethereum Mining: For Ethereum, we could rely on regional data from the the biggest mining pool by mined blocks *ethermine*; the latter controls 27.9 % of the total Ethereum hashrate[12]. Having access to individual countries' hash rates allowed us to determine their share of the total hash rate; these numbers were then used to calculate power consumption for the different power grids. Finally, we calculated a lower and an upper bound for power consumption for the respective power networks; all results are presented in Table 3.

– The *lower bound* of power consumption is calculated under the assumption that just *ethermine* encompasses miners within Europe while the miners of other pools are outside of the continent, and represents a lower bound of power

[10] Country Codes (ISO 3166-2): AT, BA, BE, BG, CH, CZ, DE, DK, DZ, ES, FR, GR, HR, HU, IT, LU, MA, ME, MK, NL, PL, PT, RO, RS, SI, SK, TN, TR, EH

[11] Mainland Denmark is connected to UCTE, the islands to NORDEL. We split the power consumption according to the region's population. (54 % in the UCTE grid, 46 % in the NORDEL grid)

[12] https://etherscan.io/stat/miner?range=7&blocktype=blocks

consumption. This is insofar a lower bound to power consumption within these networks as we have ground truth from this pool.

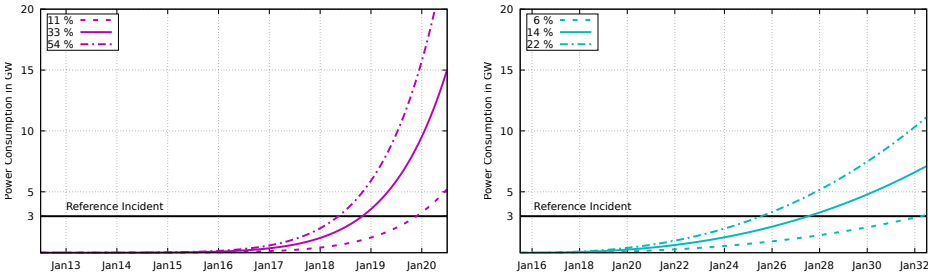
– For the *upper bound* of power consumption, we assume that all mining pools have an equal share of European miners as the investigated mining pool; this value represents insofar an upper bound as certain mining pools predominantly target miners outside Europe, e.g., by providing a homepage in Chinese only. Beyond, the investigated pool is considered to encompass more hash rate within Europe than others as the pool is run from a European country.

Geographic Spread of Bitcoin Mining: For Bitcoin mining, we were unable to obtain country specific information from a mining pool and had to rely on more coarse-grained, though publicly available information: *btc.com*, currently the largest pool mining 24.9 %[13] of all Bitcoin blocks, provides a list of successfully mined blocks and their origin at continent granularity; this way, we were able to calculate the share of blocks mined in Europe within this pool to be 7.4 % (March 2018). *slushpool.com*, third biggest pool controlling 11.7 % of Bitcoin's total hash rate, runs multiple, geographically spread *Stratum* servers and publishes the controlled hash rate per server. Individual miners connecting to a pool typically connect to the closest server to reduce network latency; this way, we are able to obtain a European share of 81 % within this mining pool. Taking these two results into account leads to a minimum power consumption of 251 MW within Europe; splitting this consumption among the power grids as Ethereum's consumption leads to a lower bound as presented in Table 3. The upper bound was calculated based on the following assumptions: (1) For the *btc.com* and *slushpool.com*, we included their share according the numbers above. (2) All pools with a Chinese-only homepage are assumed to control no miners in Europe, (3) the remainder pools are assumed to have the share of *slushpool.com* (as *ethermine* is considered to be an eurocentic pool for Ethereum, *slushpool.com* is for Bitcoin). The numbers for Bitcoin however might overestimate power consumption to a certain extent as the pools' definition of Europe may go beyond the countries in the UCTE, NORDEL, Icelandic, Irish and British grid.

7 Impacts on the Power Grid

We determined Bitcoin's total power consumption to be 2.2 GW. In European networks, 64 MW to 1329 MW are drawn. Ethereum's overall consumption is 1.3 GW of which 89 MW to 319 MW are drawn in Europe. The impact of an amount of power consumption is dependent on its share of the total power consumption and particularly the grid's reference incident. The latter indicates the power loss that the system is designed for, and its size is equivalent to the primary control, the fastest measure to stabilize a power grid. Consequently, imbalances can be compensated within a short period of time (on electrical engineering time frames). For example, the UCTE network maintains 3 GW in

[13] https://blockchain.info/pools



(a) Bitcoin ($R^2 = 0.88$). (b) Ethereum ($R^2 = 0.88$).

Fig. 4: Projection of future mining power consumption in the UCTE grid

stand-by for primary control which is fully activated within 30 seconds. Therefore, fast changes in power consumption of magnitude of the reference incidents are able to overpower the stand-by mechanisms and trigger emergency routines. Thus, we assume, the reference incident value to be an adequate threshold to determine the potential of a cryptocurrencies' power consumption to harm the power grid's operation. Therefore, Table 3 presents total power consumption alongside the reference incidents for European power grids.

In none of the power grids the consumption exceeds the reference incidents; nevertheless, upper bounds are in most cases only one order of magnitude below the threshold – two orders in the case of Ireland – and both cryptocurrencies grow exponentially at the moment. Therefore, we estimate power consumption's development in the future by performing exponential regression. Figure 4(a) shows power consumption in the UCTE network assuming a share of 11 % (lower bound, see Section 6), 54 % (upper bound) and 33 % (mean) of mining in Europe. Even in the best case, the reference incident of 3 GW[14] is reached by Bitcoin mining at the begin of 2020; in the worst case, in the middle of 2018. Results for Ethereum, see Figure 4(b), show that the reference incident will be exceeded in 7 to 14 years.

8 Discussion

Cryptocurrencies and their power consumption are either discussed with respect to hardware equipment's efficiency or the adverse impact on ecology due to high overall power consumption. In this paper, we emphasize that Proof-of-Work cryptocurrencies are in principle able to destabilize power grids. Cryptocurrency miners draw large amounts of power from the grid, despite all efforts to make them more efficient and high gains in their efficiency over the last years. Our

[14] Representing the amount of lost generation/load that can be handled by the power grid, reference incident values are hardly changed in practice despite increased energy consumption and increased network sizes.

analysis shows that cryptocurrency mining in both Bitcoin and Ethereum *currently does not represent an immediate danger to reliable power grid operation on the European continent.*

Our results show however that critical values to power grid operation lie just one or two orders of magnitude beyond the current consumption of Bitcoin or Ethereum and both grow at exponential rates. For example, the reference incident within the UCTE network is 3 GW [21], i.e., the respective power grid is planned to successfully compensate for a potential loss of this amount of power generation, which is roughly equivalent to two nuclear power plants. Assuming that current growth rates and the share of miners in the UCTE network are maintained, the level of the reference incident would be met within 0.5 to 2 years for Bitcoin and within 7 to 14 years for Ethereum. Then, the power grid's measures for frequency stabilization might not be sufficient any more in case of a sudden outage of all mining efforts in the respective cryptocurrency – may it be as a consequence of malfunction or due to malicious actions by an adversary.

In comparison to [1], our attack scenarios do not increase power consumption all of a sudden, but rather decrease it within seconds, which is more severe from the power operator's perspective as the blackout of November 2006 in Europe has shown [22]. The loss of electric load causes a shift towards higher frequencies, and wind turbines additionally increase the imbalance by stopping power input at frequencies beyond 50.2 Hz (Germany) or 50.3 Hz (Italy, Denmark) [23] destabilizing the power network even further. Despite the effort to change this behavior – a lesson learned from the 2006 blackout – it is rumored that roughly half of all turbines in Europe still follow legacy guidelines. In case of load loss, operators can only throttle power plants; this takes multiple tens of seconds for fast plants like gas turbines but hours or even days for base load plants (nuclear, coal, etc.). If the frequency reaches 51.5 Hz faster than operators are able to stabilize the network by throttling, all power plants perform a cumbersome and costly emergency shutdown. Beyond, our attack is easier to achieve than the previous approach as the tedious task of botnet creation is largely omitted. An adversary only has to compromise the communication and coordination infrastructure, smuggle malfunctionality into the software or exploit a backdoor. All three types of incidents have already been shown feasible or were actually observed in current cryptocurrency networks (c.f. Section 3). Certain protocols and software, e.g., Stratum, suffer from bad reputation with respect to security [17], and documentation as well as a planned security-by-design approach are generally lacking. Finally, we outline that our attack can also be combined with a botnet to form dynamic attacks and exploit resonance frequencies of the network, as presented in [1].

The consequences of such a described incident would be large-scale blackouts and the shutdown of power plants due to automatic emergency routines [9]. Besides the impact on the economy and the possible life-threating consequences through cease of medical care, water and other basic needs, large-scale blackouts entail a much greater challenge. Most plant types actually need electric energy to start up. Only very few power plants have black-start capabilities, i.e., a startup

procedure without external power. Afterwards, every other power plant has to be brought up by synchronizing into that grid, while simultaneously reconnecting an appropriate amount of household to keep an equilibrium of demand and production. After the 2003 Northeast blackout, it took two days to bring most households back on the grid; the remaining areas had to face up to two weeks without electrical power [24].

In recent time, cryptocurrencies – their value, as well as their mining operations – have experienced extraordinary growth and this trend is likely to continue in the near future, and possibly beyond. Thus, they will consume an increasing share of the produced electricity. In the course of this work, we focused on European power grids, namely the UCTE, the NORDEL as well as various island networks as they are considered to be among the most reliable systems. At the same time, miners are not predominantly present in these areas, but rather in other networks. Despite these considerations, the results show that cryptocurrencies might have a negative impact on reliable grid operation. Thus, any thresholds determined for that networks will likely be lower on other less robust grids with a higher mining ratio. For example, Venezuela, known for its continuous problems with power grid operation, has attributed blackouts purportedly to "illegal" Bitcoin mining[15].

Countermeasures: In conclusion, its worth to think about potential countermeasures such as the following:

– *Change of mining software behavior:* An approach that could readily help to mitigate the outlined attack is to update cryptocurrency mining software such that it takes the problem of sudden load swings into consideration. For instance, upon loss of connectivity or lack of work to be performed, mining software could continue the mining process for a randomized amount of time in order to reduce the overall power consumption more smoothly.

– *Further efficiency increase:* Mining hardware could be improved to reduce their power consumption per hash rate even further, and counteract the rising power consumption. Past growth rates however increased power consumption at higher rates than savings due to more efficiency. In addition, improvements in efficiency appear to be lower in the future as our trend analysis shows at least for Bitcoin, see Figure 2(a).

– *Replacement of Proof-of-Work:* There are currently several approaches to replace Proof-of-Work with alternative, less energy intensive mechanisms. Provably secure *Proof-of-Stake* designs have been proposed, where the required resource to be able to participate in mining are the cryptocurrency units themselves [25–27]. Furthermore, by relying on *trusted hardware*, systems employing Proof-of-Elapsed-Time (PoET) or Proof-of-Useful-Work (PoUW) can be realized [28]. Finally, alternative limited resources, such as disk space in the case of Proof-of-Space [29], may be utilized.

[15] http://www.dailymail.co.uk/news/article-5161765/Bitcoin-mining-causing-electricity-blackouts.html

– *Change of incentives:* Each mining operator aims to expand its mining capability as long as they expect a net profit in doing so. This increases the network's overall hash rate and power consumption; at the same time, the difficulty of the network is adjusted making Proof-of-Work harder to leave targeted block intervals unchanged. This implies that the cryptocurrency's throughput does not increase despite more effort (and power) spent on mining, i.e., it does not scale transaction numbers with the hash rate. Expanding the incentives in a way that rewards more resource efficient mining would not only reduce hash rate but also power consumption.

– *Regulation:* Power grids are critical infrastructure; nation states aim to protect their infrastructure and take actions usually by means of legislation, e.g., *Directive 2008/114/EC* by the European Union. In consequence, governments might regulate the use or mining of cryptocurrencies. For example, China has already banned Bitcoin trading[16], even though mining is still legal.

– *Purchase of surplus production:* Finally, there is also a benefit for power grid reliability with regard to cryptocurrencies. The latter could stabilize the power grid, and purchase a surplus of energy production in order to maintain the balance between supply and consumption. This typically happens in nights: Base load power stations, e.g., nuclear or coal power plants, suffer from slow dynamics and therefore operators prefer paying others to consume the power instead of reducing their plants' output. Killing two birds with a stone, miners would not only raise money through the mining reward and transaction fees but would also raise income through power consumption. However, mining equipment would not run 24/7 which impacts the return on investment.

– *Speed-up of power grid measures:* In future, primary control could improve responsiveness until full activation. As physical limits impose constraints on power plant turbines due to their mass; grid operators might have to find alternative ways for primary control, e.g., by using power from electric cars' batteries to stabilize the network.

9 Related Work

Large-scale power grid failures and destabilization incidents bringing grids to their limits are rare events in European power grids. Nevertheless, operators investigate and learn from these occurrences to be able to ensure more reliable operation in the future, e.g., the November 2006 blackout, which split the power grid into three synchronous zones due to cascading effects [22], a blackout in Turkey in 2015 [30], and inter-area oscillations [31]. Attacks against smart grids are outlined in *Mohsenian-Rad et al.* [32] and *Mishra et al.* [33], where an adversary manipulates messages, e.g., containing pricing information, causing *smart* behavior to indirectly affect the power grid, e.g., simultaneous charging of all electric vehicles. As of today, smart grid functionality is not yet widely deployed. Hence, the respective attack surface is low. On a smaller network scale

[16] http://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-cryptocurrency-trading-completely-ban

Xu et al. [34] investigate how power oversubscription in data centers could be used to conduct concerted attacks that lead to undesired power outages. Finally, the impact of dynamic load attacks on smart grid operation is outlined in *Amini et al.* [35], however the authors do not provide strategies how an adversary could gain such a high amount of controllable load. This problem is overcome in *Dabrowski et al.* [1], where it is shown that an adversary could form a botnet from commodity hardware as well as Internet-of-Thing devices to reach the necessary controllable load for a successful attack. In addition, it is highlighted that an adversary requires much lower amounts of controllable consumers than stated in [35]. In regard to power consumption cryptocurrencies are investigated in a twofold way: either for power efficiency of mining hardware or their total consumption's impact on the environment. *Wang and Liu* [36] consider the evolution of miners, including their power consumption and productivity. *O'Dwyer and Malone* [3] investigate the profitability of Bitcoin mining, including hardware characteristics as well as exchange rates, and bound the total power consumption of Bitcoin to 3 GW. Further publications that provide estimates on the total power consumption of Bitcoin are presented by *Vranken* [5], *Deetman* [18], and *The Vries* [19]. We asses their models in Section 4; our work is based on *Deetman*'s approach. Another estimation is published by *Orman* [37], however the numbers appear erroneous, e.g., a total Bitcoin hash rate of 1018 Hashes/s.

10 Conclusion

By now, power consumption with regard to cryptocurrencies such as *Bitcoin* and *Ethereum* has been considered in a twofold way. Either, mining operators have aimed to maximize revenue (and therefore invested in most efficient mining hardware), or ecologists criticize the cryptocurrencies' massive amount of power consumption and its adverse affects on the environment. In the course of this work, we broaden the discussion and investigate whether cryptocurrencies are able to destabilize power grid operation by suddenly reducing mining (and thus electric load). The latter might be achieved by the exploitation of a backdoor in a vast number of miners, by compromising the communication infrastructure or by malfunctionality of software required for mining – all events that have been shown possible or have actually happened in the past.

Indeed, we identified potential that such incidents might negatively impact power grid operation causing load shedding, the shutdown of power plants and eventually large-scale blackouts, if not now then possibly in the near future. Our results are based on European power grids, namely the UCTE, NORDEL and various island networks, that are considered to be among the most reliable. At the same time, these grids currently serve only a minor part of mining hardware. In the UCTE network, the biggest synchronous power grid by total load, we see power consumption of Bitcoin and Ethereum each reaching critical values within the next years, assuming further growth of cryptocurrencies. Whereas, some less stable grids are serving proportionally more mining facilities, and consequently face higher risks from such incidents. Concluding, the current gold rush-like hype

towards cryptocurrencies may not only impact finance but also the real, physical world. While we do not oppose cryptocurrencies in general, we view their ever increasing power consumption with a critical eye. In this respect it is essential to consider the possible consequences of uncontrolled growth and try to provide effective countermeasures that help to ensure the stable operation of power grids.

Acknowledgments

We thank Peter Pratscher operating ethermine and ethpool for providing valuable insight into hashrate population on a per country basis. This research was funded by Bridge Early Stage 846573 A2Bit and Bridge 1 858561 SESC (both FFG), the Christian Doppler Laboratory for *Security and Quality Improvement in the Production System Lifecycle (CDL-SQI)*, Institute of Information Systems Engineering, TU Wien and the Josef Ressel Centers project TARGET. The competence center SBA Research (SBA-K1) is funded within the framework of COMET Competence Centers for Excellent Technologies by BMVIT, BMDW, and the federal state of Vienna. The financial support by the Austrian Federal Ministry for Digital, Business and Enterprise and the National Foundation for Research, Technology and Development is gratefully acknowledged.

References

1. A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids," in *Annual Computer Security Applications Conference (ACSAC)*, 2017.
2. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *IEEE Symposium on Security and Privacy*, 2015.
3. K. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," *IET Irish Signals & Systems Conference*, 2014.
4. P. Fairley, "Blockchain world - feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," *IEEE Spectrum*, 2017.
5. H. Vranken, "Sustainability of bitcoin and blockchains," *Current Opinion in Environmental Sustainability*, 2017.
6. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
7. V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014.
8. ENTSO-E, *Continental Europe Operation Handbook*, 2004, ch. Appendix 1 - Load-Frequency Control and Performance.
9. Verband der Netzbetreiber (VDN), "Transmissioncode 2007 - netz- und systemregeln der deutschen bertragungsnetzbetreiber," 2007.
10. A. Narayanan and J. Clark, "Bitcoin's academic pedigree," 2017.
11. J. R. Douceur, "The sybil attack," in *International Workshop on Peer-to-Peer Systems*, 2002.
12. C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Annual International Cryptology Conference*, 1992.

13. A. Back *et al.*, "Hashcash-a denial of service counter-measure," 2002.
14. Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *International Conference on Autonomous Agents and Multiagent Systems*, 2015.
15. O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *International Conference on Financial Cryptography*, 2016.
16. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger eip-150 revision (759dccd - 2017-08-07)," 2017.
17. R. Recabarren and B. Carbunar, "Hardening stratum, the bitcoin pool mining protocol," in *Symposium on Privacy Enhancing Technologies (PETS)*, 2017.
18. S. Deetman. (2016) Bitcoin could consume as much electricity as denmark by 2020. [Online]. Available: https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
19. A. the Vries. (2014) Bitcoin energy consumption index. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption
20. A. P. Ozisik, G. Bissias, and B. N. Levine, "Estimation of miner hash rates and consensus on blockchains," 2018.
21. ENTSO-E, *Continental Europe Operation Handbook*, 2004, ch. Policy 1 - Load-Frequency Control and Performance.
22. Union for the Co-Ordination of Transmission of Electricity, "Final report: System disturbance on 4 november 2006," 2007.
23. J. von Appen, M. Braun, T. Stetz, K. Diwold, and D. Geibel, "Time in the sun: The challenge of high pv penetration in the german electric grid," *IEEE Power and Energy Magazine*, 2013.
24. U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada," 2004.
25. A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," 2016.
26. S. Micali, "Algorand: The efficient and democratic ledger," 2016.
27. I. Bentov, R. Pass, and E. Shi, "Snow white: Provably secure proofs of stake," 2016.
28. F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. van Renesse, "Rem: Resource-efficient mining for blockchains," 2017.
29. S. Park, K. Pietrzak, A. Kwon, J. Alwen, G. Fuchsbauer, and P. Gaži, "Spacemint: A cryptocurrency based on proofs of space," 2015.
30. ENTSO-E, "Report on blackout in tureky on 31st march 2015," 2015.
31. ——, "Analysis of ce inter-area osciallations of 19 and 24 february 2014," 2011.
32. R. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, 2011.
33. S. Mishra, X. Li, A. Kuhnle, M. T. Thai, and J. Seo, "Rate alteration attacks in smart grid," in *IEEE Conference on Computer Communications (INFOCOM)*, 2015.
34. Z. Xu, H. Wang, Z. Xu, and X. Wang, "Power attack: An increasing threat to data centers," in *Network and Distributed System Security Symposium (NDSS)*, 2014.
35. S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2015.
36. L. Wang and Y. Liu, "Exploring miner evolution in bitcoin network," in *Passive and Active Measurement*, 2015.
37. H. Orman, "The power (energy) of cryptography," *IEEE Internet Computing*, 2016.