


# Analyzing the Solo Mining Profitability of Zcash Cryptocurrency in the United States of America

Guilherme Albuquerque  [ Instituto Nutech de Pesquisa Aplicada em Ciência, Tecnologia e Inovação |

guilhermealbuquerque1@hotmail.com ]

Carlo Kleber da Silva Rodrigues  [ Universidade Federal do ABC | carlo.kleber@ufabc.edu.br ]

✉ Federal University of ABC - UFABC - Center for Mathematics, Computation and Cognition - CMCC - Avenida dos Estados, 5001, Santa Terezinha - Santo André, SP, 09210-580, Brazil.

Received: 23 June 2022 • Accepted: 03 October 2022 • Published: 17 February 2023

## Abstract

Zcash is a proof-of-work (PoW) cryptocurrency that has gained attention due to its promise of enhanced user privacy. Notwithstanding, Zcash's thorough acceptance notably depends on how profitable its *mining* process can be. To tackle this issue, we propose an analytical model to compute the *mining hashrate* under *solo mining* to achieve a liquid revenue equal to the minimum wage in the United States. In the sequence, we then estimate how profitable Zcash *solo mining* is based on that computed *mining hashrate*. Our proposed model spans crucial parameters of the whole *mining* process. In the experiments, we compare Zcash with the popular Bitcoin and also present a competitive analysis encompassing the ten top cryptocurrencies by market capitalization. Final results highlight that: (i) Zcash owns a value of  $h_{min}$  which is about eight orders of magnitude smaller than that of Bitcoin in all investigated scenarios, which refer to the ten least and most expensive american states in terms of electricity tariff; and (ii) Zcash is the second best cryptocurrency for *solo mining* among the aforementioned ten cryptocurrencies, being the only one whose protocol implements the concept of zero-knowledge proofs. Within this context, our key contribution is to provide the scientific literature with valuable insights to formally pave the way to develop practical analytical models for PoW-cryptocurrency systems, which may be chiefly valuable regarding competitive analyses in general.

**Keywords:** Zcash, Cryptocurrency, Bitcoin, Mining, Profitability, PoW

## 1 Introduction

All cryptocurrency's minting and trading activities are anonymously performed within a computer peer-to-peer (P2P) network, which is managed by a set of communication protocols under strong cryptography. As main feature, we highlight the non-dependency on centralized entities. This yields a rather sophisticated payment system which is much more resistant to banks' and governments' influences than those conventional ones [Quamara and Singh, 2022].

Under a technological view, the vital computational process of a proof-of-work (PoW) cryptocurrency system is block *mining* [Hong, 2022]. This process refers to building and validating data blocks formed by system users' transactions. In case this is executed by a single network peer, we have the *solo mining*. In case a group of network peers work together, we have the *pool mining*. The network peers, denoted as *miners*, are incentivized to participate by the prospect of acquiring a predetermined number of cryptocurrencies for every *mined* block, called the *mining* reward. In general, the more competing *miners* exist to *mine* blocks, the more difficult it becomes to receive rewards [Quamara and Singh, 2022; Li *et al.*, 2021].

The worldwide known Bitcoin PoW-cryptocurrency was proposed in the year 2008 [Nakamoto, 2008]. It has grown substantially since then, judging from its market capitalization which has already reached an expressive mark of about USD 352.29 billion [CoinMarketCap - Prices, 2022]. More-

over, it is recognized for its secure and profitable *mining* process. Other PoW cryptocurrencies have emerged based on Bitcoin's proposal over time. Among them, the Zcash cryptocurrency [Daira Hopwood, 2021; Ben Sasson *et al.*, 2014] has called attention due to its promise of being truly anonymous: unlike the Bitcoin's protocol, the Zcash's protocol retains no sensitive details of a system user's transactions, such as sender's and receiver's public keys besides the amount being transferred between accounts. As a result, Zcash can thus provide a kind of enhanced privacy to its users, especially compared to Bitcoin [Biryukov and Feher, 2019; Modesti *et al.*, 2021; Jawaheri *et al.*, 2020].

The Bitcoin and Zcash cryptocurrencies own quite similar *mining* processes, and their corresponding *miners* often deploy analogous hardware platforms. Notwithstanding, Zcash usually has less competing *miners* and grants smaller rewards to *miners* [Li *et al.*, 2021]. From this, we may then wonder whether Zcash's block *mining* is more profitable than Bitcoin's. Tackling this issue surely helps to predict how successful Zcash may still be in the upcoming future, since any PoW cryptocurrency's thorough acceptance depends a great deal on its *mining* profitability.

It is though worth noting that the computation of the aforementioned profitability is not an easy task. It depends on several pivotal parameters related to the entire *mining* process, such as hardware electrical power, electricity tariffs, expected rewards, and *mining hashrate*. Furthermore, as far as we are concerned, no closed-form solution to compute this

profitability has been presented in the literature up to the current moment.

The above is the motivation for this paper, whose main goal is to propose a generic analytical model under *solo mining* to compute the *mining hashrate* for a liquid revenue that equals the minimum wage in the United States of America (U.S.). The minimum wage underpins the ordinary citizen's purchasing power and, hence, constitutes a suitable baseline for our study. Besides, we also compare Zcash against the popular Bitcoin as for the aforementioned *mining hashrate*, and still carry out a competitive analysis against the top ten cryptocurrencies by market capitalization. The proposed model especially enables the following overall guidance: the computation of the *mining hashrate* provides evidence of how much computational effort is expended by *miners* and may be used to help estimate the *solo-mining* profitability.

It is important to outline that the main contribution of this paper is thus to provide the literature with valuable insights to formally pave the way for developing new analytical models to assess the profitability of *mining* processes, which may result very useful for conducting competitive analyses between PoW-cryptocurrency systems in general.

The remainder of this work is structured as follows. Section 2 briefly reviews essentialities concerning both Bitcoin and Zcash cryptocurrency systems. Related work is discussed in Section 3. In Section 4, we explain the proposed analytical modeling. Section 5 brings the experiments and discusses the obtained results from the comparison of Zcash with Bitcoin, besides the competitive analysis spanning the ten top cryptocurrencies by market capitalization. Finally, overall conclusions and directions for future work constitute Section 6.

## 2 Essentialities

### 2.1 The Bitcoin protocol

Bitcoin's architecture is based on a public-ledger philosophy. This means that all system users have access to all accounts' states, besides all transactions that occur, in a global-scale P2P network. Every time a transaction happens, the sender's and receiver's ledgers must be both updated, reflecting the current system state. The ledger is implemented through the concept of the Blockchain technology [Rodrigues, 2021; Sanka and Cheung, 2021], which is succinctly commented in the next subsection.

As already mentioned, each network peer is a *miner*, whose role is to *mine* blocks to receive rewards which, in this case, are measured in number of Bitcoins (BTCs). Moreover, as sequences of characters (i.e., public keys) are used instead of personal identification (ID number, address, phone number, etc.), a partial privacy is granted to its system users. By partial we mean it is possible to trace transactions to find out the real owners of the public keys through forensics [Yin *et al.*, 2019].

### 2.2 The Blockchain technology

Users' transactions are initially submitted to the P2P network. They are then grouped into blocks by *miners*. After being *mined*, each block is then propagated in the P2P network. When a *miner* receives a *mined* block, it verifies the block and adds it to the just previous *mined* block, creating a linked list of *mined* blocks. This list is denoted as Blockchain. Hence, besides denoting the distributed-ledger technology underpinning the Bitcoin cryptocurrency, the term Blockchain also refers to the ordered sequence of *mined* blocks, whose first block is called *genesis* block.

As a matter of fact, different blocks may possibly transit in the network at the same time. Additionally, different *miners* may successfully *mine* different blocks they believe to be the very next block of the Blockchain. As different parts of the network receive different pieces of information regarding the *mined* blocks, each *miner* creates its own version of what it assumes to be the right extension to the current Blockchain: the next block is always the *mined* block the *miner* has just received. This extension is called a *branch*.

Since different branches are very likely to be generated, it is assumed by design that only the longest *branch* will definitely merge with the current Blockchain at some time in the future. As a result, all other remaining shorter *branches* are forgotten (i.e., discarded), and so are their blocks and transactions within [Rodrigues, 2021; Sanka and Cheung, 2021].

### 2.3 The Zcash protocol

Zcash was launched in the year 2016, owning cryptocurrencies denoted as ZECs. It is based on Bitcoin's codebase, thereby sharing significant similarities on how the protocol overall operates [Li *et al.*, 2021]. Aside from protocol's specificity, the main difference is that transactions in Zcash may be performed in two distinct modes, *not shielded* and *shielded*, as briefly discussed in what follows.

*Not-shielded* transactions are the same as the ordinary Bitcoin's transactions, presenting no significant technical difference. By its turn, *shielded* transactions disclose neither sender's and receiver's public keys, nor the amount being transferred between users' accounts. Notwithstanding, this information may be disclosed if legally requested in the case of a formal audit. The protocol achieves that by utilizing the concept of zero-knowledge proofs, i.e., transactions may happen without any transiting of information regarding the involved parts themselves [Zhang *et al.*, 2020; Biryukov and Feher, 2019; Daira Hopwood, 2021].

### 2.4 Proof-of-Work

Proof-of-work (PoW) stands for a decentralized consensus mechanism that requires *miners* to expend effort solving an arbitrary hard mathematical puzzle. In practice, a *miner* must acquire a right to add a block to the Blockchain, i.e., the linked list [Yun *et al.*, 2019]. To have this right, the *miner* has to prove it has made a certain computational effort to solve the defined puzzle. The difference among the PoW-based cryptocurrency systems chiefly lies in the definition of this hard puzzle.

In the case of Bitcoin, block *mining* implies dealing with an equation based on the SHA-256 cryptographic hash function [Conti *et al.*, 2018; Bowden *et al.*, 2018]. By means of successive guesses (i.e., *nonces*), the *miner* attempts to find a four-byte number that, when set as the equation's input, will yield an outcome equal or smaller than a certain  $L$ , referred to as the *target*. A more common parameter is though the *difficulty*,  $D$ , which is inversely proportional to  $L$ . By design, the greater  $D$  is, the more difficult the puzzle becomes [Conti *et al.*, 2018; Bowden *et al.*, 2018]. The *nonce* which solves the problem is called *golden nonce*. Hence, the puzzle in Bitcoin stands for finding the *golden nonce*. Note this is a CPU-bound problem, i.e., the time to evaluate is mainly determined by the CPU's speed.

Concerning Zcash, the PoW relates to the Equihash algorithm. This algorithm is based on the well-known probability problem of finding two identical birthday dates within a group of randomly selected people [Ferdous *et al.*, 2021; Biryukov and Khovratovich, 2017]. More precisely, Zcash deploys a generalization form of this problem, whose goal is to find colliding hash values [Biryukov and Khovratovich, 2017; Ferdous *et al.*, 2021]. Its implementation is made in such a manner to create a memory-hard problem, i.e., it consumes significant amount of memory to be evaluated. The puzzle in Zcash is thus finding the adequate hash values.

### 3 Related Work

To the best of our knowledge, the formal analysis of cryptocurrency *mining* profitability based on analytical modeling is still an open issue in the scientific community, judging from the modest number of related researches which may be found in the literature. We conjecture this is mainly due to the dynamic scenario of cryptocurrencies and, consequently, the fast changes that occur [Rathore *et al.*, 2022]. Being aware of that, we herein discuss some of the most recent researches which somehow contribute to the overall purpose of this work.

Hacioglu *et al.* [2021] search to identify the best *mining* strategy to maximize profits. *Pool fee* (charged from each member *miner* to participate in the *pool* [Seth, 2021], electricity tariff, hardware rental, and hardware acquisition are several central parameters assessed in their study. The experiments reveal that strategies like *hosted mining* and *cloud mining* are promising alternatives to achieve attractive daily revenues. Furthermore, their analysis also outlines that Turkey is the top geographic location for *home mining*, i.e., owning the hardware platform and *mining* at home, among all european countries and the U.S.

Li *et al.* [2019] carry out experiments to estimate the global electricity demand of the Monero cryptocurrency's *mining* process. The results chiefly suggest that the *mining* activity may consume up to 645.0 GWh of electricity worldwide. Particularly, this figure stands for more than 19.12 thousand tons of carbon emission by China only (estimated between April and December in the year 2018). Their study also remarks on the surprising lack of academic work covering analyses of the *mining* process with respect to electricity consumption.

Grunspan and Pérez-Marco [2018] review the *selfish-mining* technique [Eyal and Sirer, 2018] to maximize profitability in the Bitcoin cryptocurrency system. In this case, a *pool* node  $p$  withholds its just *mined* block from propagating across the network while continuing to *mine* subsequent blocks. When node  $p$  finally releases all its *mined* blocks, other nodes are tricked into believing that node  $p$  has *mined* more blocks than they have during a certain time interval. This gives node  $p$  the right to claim a greater share of the total *pool* reward. Even though *selfish mining* is a preoccupation considering the *pool-mining* process, it has no impact on *solo mining*. This is because *solo-mining* nodes work independently from each other.

Davidson and Diamond [2020] look into a combined strategy to obtain more profits than is fairly due in the case of *pool mining*. This combined strategy exploits both (i) the vulnerabilities of the algorithms that adjust the *difficulty*  $D$  of the *mining* process, and (ii) the *selfish-mining* technique. Their work is more comprehensive than that of Grunspan and Pérez-Marco [2018], since the former spans the Litecoin, Bitcoin cash, Dash, Monero, and Zcash cryptocurrencies. Their results primarily show that Bitcoin is the least vulnerable, and that *miners* with modest *hashrates* may increase their profits up to 2.5 times, compared to those nodes acting honestly. Notwithstanding, the aforementioned strategy has no impact on *solo mining* for the same reason mentioned above for the work of Grunspan and Pérez-Marco [2018].

Salimitari *et al.* [2017] proposes a comprehensive analytical model to compute the profits a prospective *miner* may achieve within a Bitcoin *mining pool*. Their model encompasses several important parameters related to the *mining* process, such as electricity tariff, *pool-mining hashrate*, number of nodes, reward policy, and *pool fee*. From their model, it is possible to find out the most profitable *mining pool*. Our model mainly differs from theirs in that ours is devoted especially to *solo mining*.

To maximize profits in both *solo mining* and *pool mining*, Pathirana *et al.* [2020] analyze the impact of hardware platform efficiency, covering a broad range of platform types. More precisely, the authors are able to describe 119 Bitcoin *mining*-platform configurations based on 30 peer-reviewed publications (from the year 2013 to the year 2018). The results mainly reveal that platforms based on ASICs and FPGAs are more efficient than those based on CPUs and GPUs. Furthermore, they suggest that the most efficient platform is the one called BitmainAntminer S9, which is based on ASIC.

Much resembling the just previously cited work, Iyer and Dipakumar Pawar [2018] focus on analyzing prospective profits of the *mining* activity in function of the deployed hardware platform. Their work contributed to explaining some of the basic terminology commonly used in this context as well. The authors considered a plethora of cryptocurrencies (including Bitcoin) and hardware platforms based on GPUs and CPUs, excluding ASICs. Parameters such as *hashrates*, *pool* analytics, and electricity tariffs are used to build a quite robust financial report aimed to especially guide novice *miners* to start the *mining* activity.

From the researches discussed above, which are summarized in Table 1, we may note a promising revenue source sustained by the cryptocurrency *mining* activity. The cor-

responding results and findings derived in these researches are though chiefly focused on the *pool-mining* concept, besides being mostly based on measurements rather than on analytical modeling. Now, as a variety of new cryptocurrencies are very likely to be launched, it follows that new markets and technologies may come to exist, eventually shifting the academia and market's perspective towards more *solo mining*. Thereby, we conjecture that a practical analytical methodology to assess *solo-mining* profitability of new cryptocurrencies, like Zcash, is quite valuable and deserves to be pursued. This issue is therefore tackled in this research work.

## 4 Analytical Modeling

For PoW-cryptocurrency protocols, the average number of computations required to *mine* a block may be given by  $F \times D$  [Nakamoto, 2008; Daira Hopwood, 2021; Bowden *et al.*, 2018], where  $F$  is a fixed power-of-two factor, and  $D$  is the *difficulty* parameter (Subsection 2.4).

Let  $T_{MB}$  be the average time the *miner* spends to *mine* a block.  $T_{MB}$  depends on the *hasrate* parameter, which refers to a measure of how many computations can be performed per second by the *mining*-hardware platform. For most of the PoW-cryptocurrency systems, including Bitcoin, the *hasrate* is given in hashes per second (H/s). In the case of Zcash, the *hasrate* is though often given in solutions per second (Sol/s).

More precisely, Sol/s measures the rate at which Equi-hash solutions are found. Each one of these solutions is tested against the current *target*. Likewise, in Bitcoin each *nonce* variation is tested against the *target*, considering the SHA-256 cryptographic function. Hence, Sol/s and H/s in practice stand for the same logical procedure but applied to different systems, each of them sustained by a particular algorithm that defines the puzzle to be solved (i.e., Equi-hash and SHA-256, respectively).

Thus, there is no exact way to convert the Zcash *hasrate* to the Bitcoin *hasrate*, and vice versa. Nonetheless, computing each of these values separately and, thereafter, observing the relative difference may still result useful to bring initial clues with respect to how much computational effort is comparatively expended by the corresponding *miners*. Additionally, each computed *hasrate* may be used to help estimate the *solo-mining* profitability as shown in the mathematical derivations to follow. As a matter of fact, this overall understanding applies to all PoW cryptocurrencies.

With the above in mind and in order to facilitate our discussion, we henceforth assume the *hasrate* for any PoW cryptocurrency is computed in H/s, leaving it implicit that the resulting values are closely related to the deployed algorithm. Therefore,  $T_{MB}$  may be given in (1). Once the *hasrate* is computed in H/s, it follows that  $T_{MB}$  is given in seconds. Note we may manipulate (1) to obtain the necessary *hasrate*,  $h_{nec}$ , to *mine* a block within  $T_{MB}$  seconds, as shown in (2).

$$T_{MB} = \frac{F \times D}{\text{hasrate}} \quad (1)$$

$$h_{nec} = \frac{F \times D}{T_{MB}} \quad (2)$$

Let  $R_{rv}$  be a revenue per day, in USD/day, that equals the minimum wage in the U.S. Besides, let  $B_{rw}$  be the reward, in USD, for having *mined* a transaction block. It then follows that the maximum number of days to *mine* a block, given that a certain  $R_{rv}$  is granted, may be computed by means of (3).

$$\text{Max}_{days} = \frac{B_{rw}}{R_{rv}} \quad (3)$$

Now, let  $h_{min}$  be the average minimum *hasrate* to obtain a revenue per day that equals  $R_{rv}$ . Hence, we may compute  $h_{min}$  by means of (4), which is derived from (2) by setting  $T_{MB} = \text{Max}_{days}$  and since 1 day = 86400 s, where  $\text{Max}_{days}$  is given in (3).

$$h_{min} = \frac{F \times D}{86400 \times \text{Max}_{days}} = \frac{F \times D \times R_{rv}}{86400 \times B_{rw}} \quad (4)$$

The above computation of  $R_{rv}$  does not take into account the electricity cost. To add this cost, we proceed as follows. Let  $E_{kWh}$  be the electric energy, in kWh, consumed within a day time by the *mining* hardware to obtain  $R_{rv}$ . To compute  $E_{kWh}$ , we multiply the electric power of the *mining* hardware,  $P_{hw}$ , in watts, by the time during which *mining* is performed,  $T_m$ , in hours, and thereafter we divide the result by 1000, as shown in (5).

$$E_{kWh} = \frac{P_{hw} \times T_m}{1000} \quad (5)$$

See that the total cost,  $C_t$ , in USD, for having *mined* during  $T_m$  hours may be therefore obtained in (6), where  $t_{elt}$  stands for the electricity tariff, in USD/kWh, within the local geographic region. So, in order to compute  $h_{min}$  to obtain a liquid revenue of  $R_{rv}$ , we must still rewrite (4) as (7).

$$C_t = E_{kWh} \times t_{elt} \quad (6)$$

$$h_{min} = \frac{F \times D}{86400 \times \text{Max}_{days}} = \frac{F \times D \times (R_{rv} + C_t)}{86400 \times B_{rw}} \quad (7)$$

From the equations derived above, we may very practically analyze the *solo-mining* profitability under different aspects. For instance, we can evaluate the needed time length,  $L_{time}$ , in days, to make up for eventual capital expenditure,  $C_{exp}$ , in USD, due to *mining*-hardware acquisition by the part of the investor, as computed in (8). Finally, for ease of reference, we recap in Table 2 all parameters constituting the aforementioned equations.

$$L_{time} = \frac{C_{exp}}{R_{rv} - C_t} \quad (8)$$

## 5 Performance Evaluation

### 5.1 Parameter setup

This subsection presents the numerical values of the parameters just summarized in Table 2, mainly targeted at the Zcash

**Table 1.** Synthesis of related work.

Reference	Cryptocurrency	Main focus
Hacioglu <i>et al.</i> [2021]	Bitcoin	<i>Pool-mining</i> profitability
Li <i>et al.</i> [2019]	Monero	Environmental effects
Grunspan and Pérez-Marco [2018]	Bitcoin	<i>Selfish-mining</i> review
Davidson and Diamond [2020]	Bitcoin & others	<i>Selfish-mining</i> review
Salimitari <i>et al.</i> [2017]	Bitcoin	<i>Pool-mining</i> profitability
Pathirana <i>et al.</i> [2020]	Bitcoin	Hardware-platform technology
Iyer and Dipakumar Pawar [2018]	Bitcoin & others	Hardware-platform technology
This research	Zcash & others	<i>Solo-mining</i> profitability

**Table 2.** Parameter definition.

Parameter	Definition
$F$	Fixed power-of-two factor used to compute the average number of hashes necessary to <i>mine</i> a transaction block. Its numeric value is defined by the cryptocurrency protocol.
$D$	Variable <i>difficulty</i> . Like the factor $F$ , it is also used to compute the average number of hashes necessary to <i>mine</i> a transaction block. Its numeric value is defined by the cryptocurrency protocol.
$T_{MB}$	Average time the <i>miner</i> spends to <i>mine</i> a block, in seconds.
$h_{nec}$	Necessary <i>hashrate</i> to <i>mine</i> a block within $T_{MB}$ seconds, in H/s.
$R_{rv}$	Average revenue per day due to block <i>mining</i> , in USD/day. Its computation disregards the electricity cost.
$B_{rw}$	Corresponding reward for having <i>mined</i> a block, in cryptocurrencies or USD.
$Max_{days}$	Maximum number of days to <i>mine</i> a block, given that a certain $R_{rv}$ is granted.
$h_{min}$	Average minimum <i>hashrate</i> for a revenue per day that equals $R_{rv}$ , in H/s.
$E_{kWh}$	Electric energy consumed by the <i>mining</i> hardware to obtain $R_{rv}$ , in kWh.
$P_{hw}$	Electric power of the <i>mining</i> hardware, in watts.
$T_m$	Time interval during which <i>mining</i> is performed per day, in hours.
$C_t$	Total electricity cost for block <i>mining</i> during $T_m$ hours, in USD.
$t_{elt}$	Electricity tariff in the local region where <i>mining</i> is performed, in USD/kWh.
$C_{exp}$	Capital expenditure due to <i>mining</i> hardware acquisition by the investor, in USD.
$L_{time}$	Needed time length to make up for the capital expenditure, $C_{exp}$ , in days

and Bitcoin cryptocurrency systems. For ease of understanding, we opt to classify them in two different groups as detailed in what follows.

One group encompasses the parameters within Table 3. Their assigned values may vary according to the scenario being exploited in the experiments. In this case, they are directly computed from the equations derived in the last section. The other group's parameters are those given in Table 4. Their assigned values are fixed and determined by either cryptocurrency protocols or overall considerations related to the scenarios and/or time when these values were collected (in September 2022). The corresponding rationales for their values are succinctly informed in Table 5.

**Table 3.** Parameter value assigned by equation.

Parameter	Cryptocurrency	Equation
$T_{MB}$	Zcash & Bitcoin	(1)
$h_{nec}$	Zcash & Bitcoin	(2)
$Max_{days}$	Zcash & Bitcoin	(3)
$C_t$	Zcash & Bitcoin	(6)
$h_{min}$	Zcash & Bitcoin	(7)

## 5.2 Computing $h_{min}$ for Zcash and Bitcoin

This subsection aims to compute Zcash's  $h_{min}$  and compare against Bitcoin's. The computed results refer to the ten least and most expensive american states based on  $t_{elt}$ . Recall that  $h_{min}$  has been derived as a function of all other parameters within Table 3. Hence,  $h_{min}$  catches all influences impacting the *mining* profitability and, thereby, constitutes an ideal base performance metric for our study.

The computed results for  $h_{min}$  are presented in Table 6 (for the least expensive states), and in Table 7 (for the most expensive states). We may see that Zcash has a value of  $h_{min}$  that is about eight orders of magnitude smaller than that obtained for Bitcoin. Thereby, the computational effort expended by Bitcoin *miners* is expected to be much greater than that of Zcash *miners* to get the same value of revenue  $R_{rv}$ . In the next subsection, we broaden our discussion by focusing on the *solo-mining* profitability of Zcash by especially comparing it with that of other relevant cryptocurrencies.

## 5.3 Competitive Analysis

This subsection carries out a competitive analysis in terms of *solo-mining* profitability. To this end, we span the top ten

**Table 4.** Parameters with fixed values.

Parameter	Cryptocurrency	Numerical value
$F$	Zcash	$2^{13}$
$F$	Bitcoin	$2^{32}$
$D$	Zcash	77,182,937
$D$	Bitcoin	32,045,359,565,303
$R_{rv}$	Zcash & Bitcoin	58.0 USD/day
$B_{rw}$	Zcash	2.5 ZECs or USD 142.47
$B_{rw}$	Bitcoin	6.25 BTCs or USD 118,898.18.
$E_{kWh}$	Zcash & Bitcoin	11.2 kWh
$P_{hw}$	Zcash & Bitcoin	1400.0 W
$T_m$	Zcash & Bitcoin	8 hours
$t_{elt}$	Zcash & Bitcoin	Given in Table 6 and Table 7.

**Table 5.** Rationales for parameters.

Parameter	Rationale
$F$ and $D$	Their respective assigned values are by design determined in the respective cryptocurrency protocols (Nakamoto [2008]; Daira Hopwood [2021]; Bowden <i>et al.</i> [2018]).
$B_{rw}$	Its value in cryptocurrencies is halved by an event called <i>halving</i> at about every four years (Li <i>et al.</i> [2021]; Ghimire and Selvaraj [2018]). Currently, $B_{rw} = 6.25$ BTCs (Bitcoin system), and $B_{rw} = 3.13$ ZECs (Zcash system). Particularly, in Zcash, $B_{rw}$ is though split between its development fund (a 20% share), and <i>miners</i> (a 80% share) (Wikipedia [2022]). To focus on <i>mining</i> profitability, we then assume $B_{rw}$ to be 2.5 ZECs in our experiments.
$R_{rv}$ and $T_m$	For a work journey of eight hours per day, the minimum wage is currently 7.25 USD/hour or 58.0 USD/day in the U.S. (U.S. Department of Labor [2022]). Thereby, we set $R_{rv} = 58.0$ USD/day, and $T_m = 8$ hours. In Zcash, since $B_{rw} = 2.5$ ZECs, and a ZEC is currently quoted at USD 56.99, it follows that $B_{rw}$ equals USD 142.47. Likewise, in Bitcoin, since $B_{rw} = 6.25$ BTCs, and a BTC is currently quoted at USD 19,023.7, it follows that $B_{rw}$ equals USD 118,898.18 (CoinMarketCap - Prices [2022]).
$t_{elt}$ and $P_{hw}$	The value of $t_{elt}$ may vary from state to state in the U.S. For the experiments we carry out in this work, we consider the ten least and most expensive states referred to the year 2020 (U.S. Energy Information Administration [2021]). Additionally, for ease of comparison, we assume the deployment of a standard <i>mining</i> -hardware platform of $P_{hw} = 1400.0$ W in all investigated states in Subsection 5.2.

**Table 6.** Computation of  $h_{min}$  in the ten least expensive american states.

Rank	State	$t_{elt}$ (cents)	$h_{min}$ : Zcash	$h_{min}$ : Bitcoin	# Magnitude order
1st	Louisiana	7.51	3022.31 kH/s	788.34 TH/s	$\approx 8$
2nd	Oklahoma	7.63	3023.00 kH/s	788.52 TH/s	$\approx 8$
3rd	Idaho	7.99	3025.07 kH/s	789.06 TH/s	$\approx 8$
4th	Utah/Wyoming	8.27	3026.68 kH/s	789.48 TH/s	$\approx 8$
5th	Arkansas	8.32	3026.97 kH/s	789.56 TH/s	$\approx 8$
6th	Nevada/Washington	8.33	3027.03 kH/s	789.57 TH/s	$\approx 8$
7th	Texas	8.36	3027.20 kH/s	789.62 TH/s	$\approx 8$
8th	North Dakota	8.56	3028.35 kH/s	789.92 TH/s	$\approx 8$
9th	Kentucky	8.58	3028.47 kH/s	789.95 TH/s	$\approx 8$
10th	West Virginia	8.75	3029.44 kH/s	790.20 TH/s	$\approx 8$

**Table 7.** Computation of  $h_{min}$  in the ten most expensive american states.

Rank	State	$t_{elt}$ (cents)	$h_{min}$ : Zcash	$h_{min}$ : Bitcoin	# Magnitude order
1st	Hawaii	27.55	3137.60 kH/s	818.41 TH/s	$\approx 8$
2nd	Alaska	19.82	3093.13 kH/s	806.81 TH/s	$\approx 8$
3rd	Connecticut	19.13	3089.16 kH/s	805.78 TH/s	$\approx 8$
4th	Rhode Island	18.54	3085.76 kH/s	804.89 TH/s	$\approx 8$
5th	Massachusetts	18.19	3083.75 kH/s	804.37 TH/s	$\approx 8$
6th	California	18.00	3082.66 kH/s	804.07 TH/s	$\approx 8$
7th	New Hampshire	16.63	3074.78 kH/s	802.03 TH/s	$\approx 8$
8th	Vermont	16.33	3073.05 kH/s	801.58 TH/s	$\approx 8$
9th	New York	14.87	3064.65 kH/s	799.39 TH/s	$\approx 8$
10th	New jersey	13.63	3057.52 kH/s	797.52 TH/s	$\approx 8$

cryptocurrencies by market capitalization [CoinMarketCap - Tokens, 2022], within which Zcash and Bitcoin are included as shown in Table 8. This way, we are herein also able to demonstrate how our analytical modeling may be practically used for this kind of study.

In Table 9, we present the computed values of  $h_{min}$  for the above ten cryptocurrencies under the highest and lowest  $t_{elt}$ , corresponding to Hawaii and Louisiana states, respectively. Note that  $h_{min}$  varies from one cryptocurrency to another exclusively due to the values assigned to the parameters  $F$ ,  $D$ ,  $B_{rw}$ , and  $P_{hw}$  (please see Section 4). The values of  $F$  and  $D$  are given in Table 9, whereas the values of  $B_{rw}$  and  $P_{hw}$  may be consulted in Tables 8 and 10, respectively. So, based on Table 9, we can achieve the following observations.

- The computed values of  $h_{min}$  for the Zcash and Bitcoin cryptocurrencies differ a little from the corresponding ones in Tables 6 and 7. This is because we had previously assumed a common *mining*-hardware platform of  $P_{hw} = 1400.0$  W, as mentioned in Table 5. Now we opt to deploy a customized hardware specification for each of the cryptocurrencies in order to be more adherent to reality, as it may be seen in Table 10.
- For any of these ten cryptocurrencies, the relationship between its computed  $h_{min}$  and its market capitalization is rather complex. As a result, it becomes very unlikely to possibly derive a simple mathematical function to interrelate these two parameters. We conjecture this is because there are a number of stakeholders involved, e.g., *mining*-hardware manufacturers, cryptocurrency market, investors, among others. Besides, the influences coming from these stakeholders are known to change very dynamically in an unpredictable way, thereby impacting the investigated scenarios day after day.

Let us now look into the computed results shown in Table 11, Figure 1, and Figure 2. In the table, we see the value of  $C_{exp}$ , whereas in the figures we find the value of  $L_{time}$ . As it may be noted, these values refer to the cases of the highest and lowest  $t_{elt}$ . So, taking Zcash as a baseline, we point out what follows in terms of *solo-mining* profitability.

- Zcash notably outperforms Bitcoin. Its values of  $C_{exp}$  and  $L_{time}$  are about 50% smaller and shorter, respec-

tively, than those registered by Bitcoin under both the highest and lowest  $t_{elt}$ .

- Zcash outperforms eight out of the ten analyzed cryptocurrencies under both the highest and lowest  $t_{elt}$ . As a result, Zcash is the second-best cryptocurrency among the ten cryptocurrencies herein analyzed.
- Even though Kadena appears to be the first best cryptocurrency, we must outline that Zcash is the only one that may provide a differentiate enhanced privacy to its users due to deploying the concept of zero-knowledge proofs in its protocol [Biryukov and Feher, 2019; Daira Hopwood, 2021].

At last, before ending this subsection, it is worth recalling that our main contribution has been to yield analytical modeling to practically evaluate the *solo-mining* profitability of PoW cryptocurrencies. This implies that, even though the numerical results we have derived in this work apply specifically to the aforementioned current scenarios, which may change within a very short time period, our modeling still remains thoroughly valid.

For example, Bitcoin prices are currently down around 60% year to date, trading well off their all-time highs of around USD 69,000 in November 2021 [Curry and Powell, 2022]. That is, the numerical results we have derived in this research are certainly different from those that we would have derived in that time. Another example is the type of hardware equipment currently used for *mining*, i.e., those cryptocurrencies whose *mining* hardware is of ASIC type are likely to present smaller and shorter values of  $C_{exp}$  and  $L_{time}$ , respectively, than those deploying CPUs or GPUs instead. Hence, once hardware manufacturers start producing ASICs customized to Ravencoin and Monero cryptocurrencies, it is reasonable to wonder whether their corresponding values of  $C_{exp}$  and  $L_{elt}$  may then decrease, whereas their corresponding values of market capitalization may then increase. Notwithstanding, our analytical modeling will still remain valid no matter what changes eventually take place in the upcoming future.

## 6 Conclusions and future work

This paper analyzed the *solo-mining* profitability of the Zcash cryptocurrency in the United States. To this end, we

**Table 8.** Top 10 cryptocurrencies by market capitalization.

Rank	Cryptocurrency	Reference	$B_{rw}$ (USD)	Market Cap (USD Billion)
1st	Bitcoin	Nakamoto [2008]	118,898.18	352.29
2nd	Dogecoin	DOGECOIN [2022]	578	7.51
3rd	Ethereum Classic	Beck [2017]	101.696	3.77
4th	Litecoin	GRAYSCALE [2021]	668	3.62
5th	Monero	Alonso and Joancomartí [2018]	92.06	2.45
6th	BTC Cash	Frankenfield [2021]	692.06	2.10
7th	BTC SV	Jaid [2019]	314.61	0.908
8th	Zcash	Daira Hopwood [2021]	142.47	0.809
9th	Ravencoin	Fenton and Black [2018]	95.25	0.396
10th	Kadena	Martino and Popejoy [2019]	1.52	0.272

**Table 9.** Computation of  $h_{min}$  for the top 10 cryptocurrencies by market capitalization.

Cryptocurrency	$h_{min}$ : highest $t_{elt}$	$h_{min}$ : lowest $t_{elt}$	$F$	$D$
Bitcoin	865.95 TH/s	801.3 TH/s	$2^{32}$	32,045,359,565,303
Dogecoin	44.40 GH/s	40.84 GH/s	$2^{32}$	7,920,063.18
Ethereum Classic	18.75 GH/s	17.82 GH/s	$2^0$	2,648,407,829,100,655
Litecoin	61.68 GH/s	56.74 GH/s	$2^{25}$	1,627,796,063
Monero	258.1 MH/s	256.5 MH/s	$2^0$	350,968,626,999
BTC Cash	850.17 TH/s	786.699 TH/s	$2^{32}$	183,124,331,678
BTC SV	780.08 TH/s	721.840 TH/s	$2^{32}$	76,386,800,000
Zcash	3150.05 kH/s	3025.70 kH/s	$2^{13}$	77,182,937.11
Ravencoin	7.50 GH/s	7.47 GH/s	$2^{32}$	246,680.31
Kadena	140.52 TH/s	129.64 TH/s	$2^0$	285,972,059,450,921,700

**Table 10.** Customized *mining*-hardware equipment for the top 10 cryptocurrencies by market capitalization.

Cryptocurrency	Hardware type	$P_{hw}$ (W)	Hardware <i>hashrate</i>	Unit price (USD)
Bitcoin	Antminer S19 XP	3010	140 TH/s	10,920
Dogecoin	Antminer L7	3260	9.05 GH/s	13,999
Ethereum Classic	ETC Miner E9	1920	2.6 GH/s	9,999
Litecoin	Antminer L7	3260	9.05 GH/s	13,999
Monero	AMD EPYC 7742	225	2816 kH/s	8,500
BTC Cash	Antminer S19 XP	3010	140 TH/s	10,920
BTC SV	Antminer S19 XP	3010	140 TH/s	10,920
Zcash	Antminer Z15	1510	420 kH/s	4,299
Ravencoin	AMD RX 580 8 GB	130	13.45 MH/s	229.0
Kadena	KDA Miner KA3	3135	166 TH/s	≈ 37,500

**Table 11.** Capital expenditure under the highest and lowest  $t_{elt}$ .

Cryptocurrency	$C_{exp}$ (USD): highest $t_{elt}$	$C_{exp}$ (USD): lowest $t_{elt}$
Bitcoin	67,544	62,501
Dogecoin	68,680	63,173
Ethereum Classic	72,108	68,531
Litecoin	95,409	87,768
Monero	779,025	774,537
BTC Cash	66,313	61,362
BTC SV	60,846	56,269
Zcash	32,243	30,970
Ravencoin	127,795	127,184
Kadena	≈ 31,743	≈ 29,286



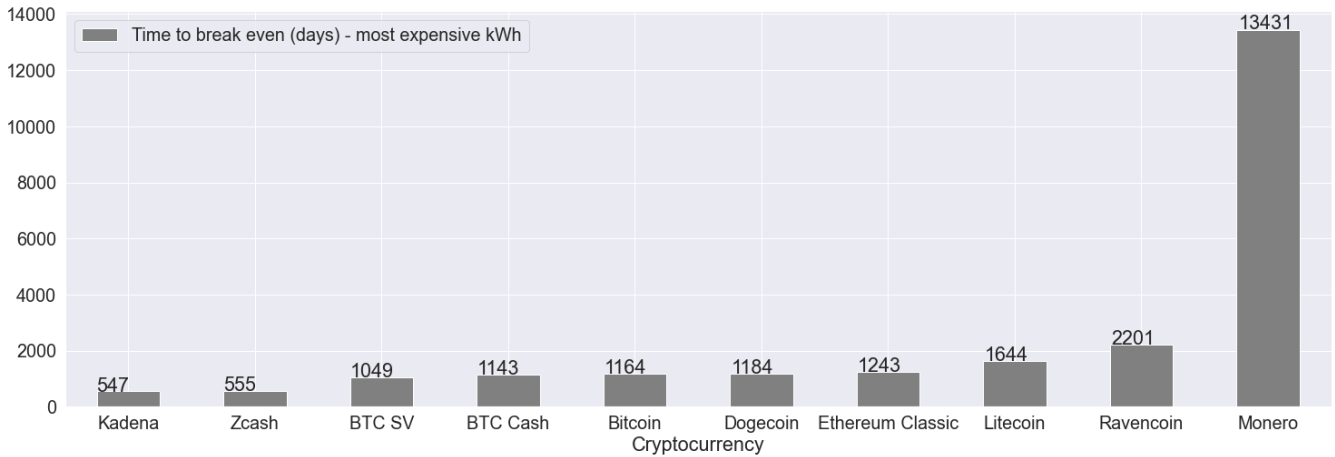


Figure 1. Profitability analysis: Time to make up ( $L_{time}$ ) for the capital expenditure ( $C_{exp}$ ), under the highest  $t_{elt}$ .

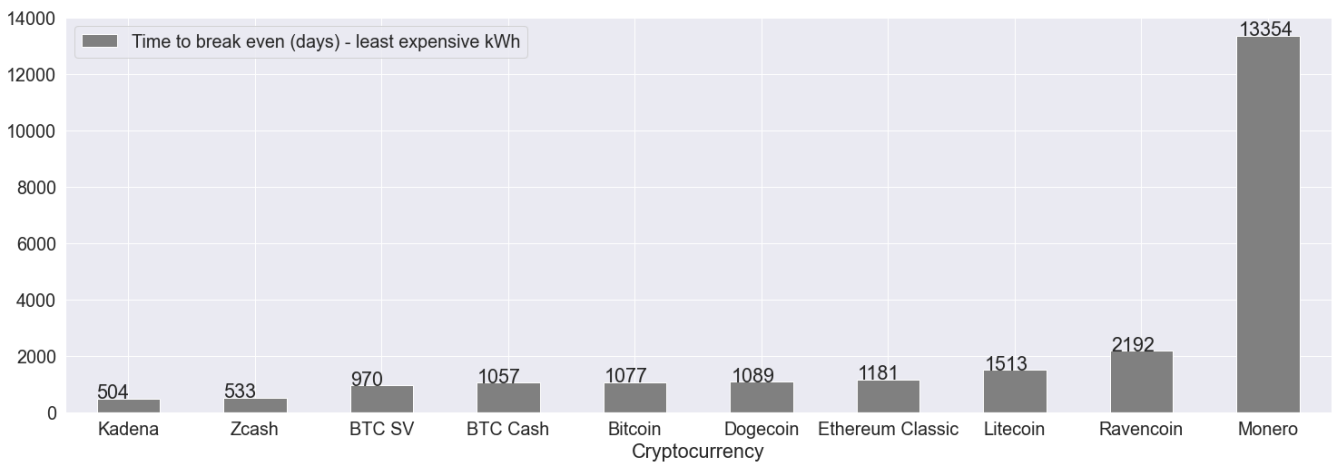


Figure 2. Profitability analysis: Time to make up ( $L_{time}$ ) for the capital expenditure ( $C_{exp}$ ), under the lowest  $t_{elt}$ .

proposed an analytical model to compute the *hasrate* of the *mining*-hardware platform to receive a liquid revenue equivalent to the minimum wage and, thereafter, the sequence, we estimated the *solo-mining* profitability based on that *hasrate*.

Among the major results achieved in experiments encompassing the ten most and least expensive american states in terms of electricity tariff, we may for instance highlight that Zcash outperformed the popular Bitcoin cryptocurrency, presenting an optimization of around 50% regarding both the capital expenditure for purchasing the *mining*-hardware platform and the *mining* time it takes to pay off this capital expenditure. Moreover, Zcash showed to be the second best alternative among the top ten cryptocurrencies by market capitalization, besides being the only one whose protocol deploys the concept of zero-knowledge proofs and, hence, that may provide a kind of enhanced privacy to its final users [Biryukov and Feher, 2019; Daira Hopwood, 2021].

In addition, it is worth mentioning that the analytical modeling and whole methodology used in our experiments can be adapted to evaluate the *solo-mining* profitability of any other PoW-cryptocurrency systems than those herein investigated. As its main contribution, our work thus provides the literature with valuable insights to formally pave the way to develop analytical models for PoW-cryptocurrency systems, which may be chiefly valuable regarding competitive analyses in general.

Notwithstanding, being aware of this research’s limitations, we especially consider these three forms to possibly enhance our analytical model: (i) taking cryptocurrency price as a variable rather than the value of fiat money to provide more stable outcomes in face of market fluctuations; (ii) including the probability that a mined block is not necessarily added to the final chain, what directly impacts the revenue achieved in the mining period; and (iii) making it time-dependent to best capture the overall dynamic behavior of the cryptocurrency systems, considering the variations and historical data in the values of electricity tariff, minimum wage, reward, cryptocurrency price, mining-hardware improvements, and mining difficulty.

Finally, as future work, we suggest these two possible directions: (i) proposing more altruistic and/or green alternatives to the PoW-based *mining* concept [Ren and Lucey, 2022]. For instance, rather than simply solving pure mathematical problems, one may use the equipment’s computational power to find solutions to concrete problems instead, like determining new prime numbers, identifying stable protein formulations for drug manufacturing, among others; and (ii) proposing mechanisms to accelerate branch convergence in the Blockchain, since long delays create resistance to cryptocurrency’s full adoption as a practical payment method [Wang *et al.*, 2021]. For example, we could randomly assume that one of the branches is the longest one

and, hence, consider all its transactions as valid. Notably, an economic fund should be created to cover eventual corrections in transactions. Under a practical view, this fund could be formed by a surplus fee charged over the value of the product associated with each transaction. This surplus would then cover service providers' losses due to eventually corrected transactions.

## Acknowledgment

### 7 Declarations

#### 7.1 Availability of data and materials

All obtained results have been computed directly from the mathematical equations presented in the manuscript.

#### 7.2 Competing interests

The authors declare that they have no competing interests

#### 7.3 Funding

The authors declare that they have received no funding.

#### 7.4 Authors' contributions

The authors have equally contributed to this work: Designed the solution; Designed the Experiments; Executed the experiments; Analysed the results; and wrote and revised the manuscript.

## References

- Alonso, K. M. and Joancomartí, J. H. (2018). Monero - Privacy in the Blockchain. Cryptology ePrint Archive, Paper 2018/535. Available at: <https://eprint.iacr.org/2018/535>.
- Beck, M. (2017). Into the Ether with Ethereum Classic. Online; accessed Sept. 22nd, 2022. Available at: <https://cryptoverze.com/ethereum-classic-whitepaper/>.
- Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474. DOI: 10.1109/SP.2014.36.
- Biryukov, A. and Feher, D. (2019). Privacy and Linkability of Mining in Zcash. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 118–123. DOI: 10.1109/CNS.2019.8802711.
- Biryukov, A. and Khovratovich, D. (2017). Equi-hash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. *Ledger*, 2:1–30. DOI: 10.14722/ndss.2016.23108.
- Bowden, R., Keeler, H. P., Krzesinski, A. E., and Taylor, P. G. (2018). Block arrivals in the Bitcoin blockchain. *CoRR*, abs/1801.07447. DOI: 10.48550/arXiv.1801.07447.
- CoinMarketCap - Prices (2022). Today's cryptocurrency prices by market cap. Online; accessed Sept. 22nd, 2022. Available at: <https://coinmarketcap.com>.
- CoinMarketCap - Tokens (2022). Top PoW Tokens by Market Capitalization. Online; accessed Sept 8th, 2022. Available at: <https://coinmarketcap.com/view/pow/>.
- Conti, M., Sandeep Kumar, E., Lal, C., and Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys Tutorials*, 20(4):3416–3452. DOI: 10.1109/COMST.2018.2842460.
- Curry, B. and Powell, F. (2022). Why Is Bitcoin Down Today? Online; accessed Sept 13rd, 2022. Available at: <https://www.forbes.com/advisor/investing/cryptocurrency/why-is-bitcoins-price-falling/>.
- Daira Hopwood, Sean Bowe, T. H. N. W. (2021). Zcash protocol specification. Online; accessed Nov. 13rd, 2021. Available at: <https://zips.z.cash/protocol/protocol.pdf>.
- Davidson, M. and Diamond, T. (2020). On the Profitability of Selfish Mining Against Multiple Difficulty Adjustment Algorithms. *IACR Cryptol. ePrint Arch.*, page 94. Available at: <https://eprint.iacr.org/2020/094>.
- DOGECOIN (2022). What is Dogecoin? - Such coin. Online; accessed Sept. 22nd, 2022. Available at: <https://whitepaper.io/document/672/dogecoin-whitepaper>.
- Eyal, I. and Sirer, E. G. (2018). Majority is Not Enough: Bitcoin Mining is Vulnerable. *Commun. ACM*, 61(7):95–102. DOI: 10.1145/3212998.
- Fenton, B. and Black, T. (2018). Ravencoin: A Peer to Peer Electronic System for the Creation and Transfer of Assets. Online; accessed Sept. 22nd, 2022. Available at: <https://ravencoin.org/assets/documents/Ravencoin.pdf>.
- Ferdous, M. S., Chowdhury, M. J. M., and Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, 182:103035. DOI: 10.1016/j.jnca.2021.103035.
- Frankenfield, J. (2021). What is Bitcoin Cash? Online; accessed Sept. 22nd, 2022; Available at: <https://www.investopedia.com/terms/b/bitcoin-cash.asp>.
- Ghimire, S. and Selvaraj, H. (2018). A Survey on Bitcoin Cryptocurrency and its Mining. In *2018 26th International Conference on Systems Engineering (ICSEng)*, pages 1–6. DOI: 10.1109/ICSENG.2018.8638208.
- GRAYSCALE (2021). An Introduction to Litecoin. Online; accessed Sept. 22nd, 2022. Available at: <https://mmarketcap.com/litecoin-whitepaper/>.
- Grunspan, C. and Pérez-Marco, R. (2018). On profitability of selfish mining. *CoRR*, abs/1805.08281. DOI: 10.48550/arXiv.1805.08281.
- Hacioglu, U., Chlyeh, D., Yilmaz, M. K., Tatoglu, E., and Delen, D. (2021). Crafting performance-based cryptocurrency mining strategies using a hybrid analytics approach. *Decision Support Systems*, 142(113473). DOI: 10.1016/j.dss.2020.113473.
- Hong, E. (2022). What Is Bitcoin Mining? . On-

- line; accessed Sept. 30th, 2022. Available at: <https://www.investopedia.com/tech/how-does-bitcoin-mining-work/>.
- Iyer, S. G. and Dipakumar Pawar, A. (2018). GPU and CPU Accelerated Mining of Cryptocurrencies and their Financial Analysis. In *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, pages 599–604. DOI: 10.1109/I-SMAC.2018.8653733.
- Jaid, S. (2019). Bitcoin SV (BSV) Whitepaper. Online; accessed Sept. 22nd, 2022. Available at: [https://coinnews.com/bitcoin-sv-whitepaper/#Bitcoin\\_SV\\_Whitepaper\\_PDF](https://coinnews.com/bitcoin-sv-whitepaper/#Bitcoin_SV_Whitepaper_PDF).
- Jawaheri, H. A., Sabah, M. A., Boshmaf, Y., and Erbad, A. (2020). De-anonymizing Tor hidden service users through Bitcoin transactions analysis. *Computers Security*, 89:101684. DOI: 10.1016/j.cose.2019.101684.
- Li, J., Li, N., Peng, J., Cui, H., and Wu, Z. (2019). Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy*, 168:160–168. DOI: 10.1016/j.energy.2018.11.046.
- Li, K., Liu, Y., Wan, H., and Huang, Y. (2021). A discrete-event simulation model for the bitcoin blockchain network with strategic miners and mining pool managers. *Computers & Operations Research*, 134:105365. DOI: 10.1016/j.cor.2021.105365.
- Martino, W. and Popejoy, S. (2019). The Kadana Public Blockchain. Online; accessed Sept. 22nd, 2022; Available at: <https://docs.kadena.io/basics/whitepapers/chainweb-layer-1>.
- Modesti, P., Shahandashti, S. F., McCorry, P., and Hao, F. (2021). Formal modelling and security analysis of Bitcoin's payment protocol. *Computers Security*, 107:102279. DOI: 10.1016/j.cose.2021.102279.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Online; Nov. 10th, 2021. Available at: <https://bitcoin.org/bitcoin.pdf>.
- Pathirana, A., Halgamuge, M., and Syed, A. (2020). Energy Efficient Bitcoin Mining to Maximize the Mining Profit: Using Data from 119 Bitcoin Mining Hardware Setups. *International Journal of Advances in Electronics and Computer Science*, 7(2):2394–2835. Available at: [http://www.ijae.in/journal/journal\\_file/journal\\_pdf/12-633-15871200397-14.pdf](http://www.ijae.in/journal/journal_file/journal_pdf/12-633-15871200397-14.pdf).
- Quamara, S. and Singh, A. K. (2022). A systematic survey on security concerns in cryptocurrencies: State-of-the-art and perspectives. *Computers Security*, 113:102548. DOI: 10.1016/j.cose.2021.102548.
- Rathore, R. K., Mishra, D., Mehra, P. S., Pal, O., Hashim, A. S., Shapi'i, A., Ciano, T., and Shutaywi, M. (2022). Real-world model for bitcoin price prediction. *Information Processing Management*, 59(4):102968. DOI: 10.1016/j.ipm.2022.102968.
- Ren, B. and Lucey, B. (2022). A clean, green haven? Examining the relationship between clean energy, clean and dirty cryptocurrencies. *Energy Economics*, 109:105951. DOI: 10.1016/j.eneco.2022.105951.
- Rodrigues, C. K. S. (2021). Analyzing Blockchain integrated architectures for effective handling of IoT-ecosystem transactions. *Computer Networks*, 201:108610. DOI: 10.1016/j.comnet.2021.108610.
- Salimitari, M., Chatterjee, M., Yuksel, M., and Pasiliao, E. (2017). Profit maximization for bitcoin pool mining: A prospect theoretic approach. In *2017 IEEE 3rd international conference on collaboration and internet computing (CIC)*, pages 267–274. IEEE. DOI: 10.1109/CIC.2017.00043.
- Sanka, A. I. and Cheung, R. C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications*, 195:103232. DOI: 10.1016/j.jnca.2021.103232.
- Seth, S. (2021). How Do Cryptocurrency Mining Pools Work? Online; May 8th, 2022. Available at: <https://shorturl.ae/8jsQU>.
- U.S. Department of Labor (2022). Minimum Wage. Online, May 20th, 2022. Available at: <https://www.dol.gov/agencies/whd/minimum-wage>.
- U.S. Energy Information Administration (2021). State electricity profiles, data for 2020. Online, Nov 18, 2021. Available at: <https://www.eia.gov/electricity/state/>.
- Wang, J., Wei, B., Zhang, J., Yu, X., and Sharma, P. K. (2021). An optimized transaction verification method for trustworthy blockchain-enabled IIoT. *Ad Hoc Networks*, 119:102526. DOI: 10.1016/j.adhoc.2021.102526.
- Wikipedia (2022). Zcash. Online; accessed Oct. 1st, 2022. Available at: <https://en.wikipedia.org/wiki/Zcash>.
- Yin, H. H. S., Langenheldt, K., Harlev, M., Mukkamala, R. R., and Vatrapu, R. (2019). Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain. *Journal of Management Information Systems*, 36(1):37–73. DOI: 10.1080/07421222.2018.1550550.
- Yun, J., Goh, Y., and Chung, J.-M. (2019). Analysis of Mining Performance Based on Mathematical Approach of PoW. In *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, pages 1–2. DOI: 10.23919/ELINFOCOM.2019.8706374.
- Zhang, Z., Li, W., Liu, H., and Liu, J. (2020). A Refined Analysis of Zcash Anonymity. *IEEE Access*, 8:31845–31853. DOI: 10.1109/ACCESS.2020.2973291.