IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 7 June 2022, accepted 11 July 2022, date of publication 14 July 2022, date of current version 20 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3190891

SURVEY

A Survey on Technologies Which Make Bitcoin Greener or More Justified

HENRI T. HEINONEN[1], ALEXANDER SEMENOV[2], JARI VEIJALAINEN[1], AND TIMO HÄMÄLÄINEN[1], (Senior Member, IEEE)

[1]Faculty of Information Technology, University of Jyväskylä, FI-40014 Jyväskylä, Finland
[2]Department of Industrial and Systems Engineering, Herbert Wertheim College of Engineering, University of Florida, Shalimar, FL 32579, USA

Corresponding author: Henri T. Heinonen (henri.t.heinonen@student.jyu.fi)

ABSTRACT According to recent estimates, one bitcoin transaction consumes as much energy as 1.5 million Visa transactions. Why is bitcoin using so much energy? Most of the energy is used during the bitcoin mining process, which serves at least two significant purposes: a) distributing new cryptocurrency coins to the cryptoeconomy and b) securing the Bitcoin blockchain ledger. In reality, the comparison of bitcoin transactions to Visa transactions is not that simple. The amount of transactions in the Bitcoin network is not directly connected to the amount of bitcoin mining power nor the energy consumption of those mining devices; for example, it is possible to multiply the number of bitcoin transactions per second without increasing the mining power and the energy consumption. Bitcoin is not only ''digital money for hackers''. It has very promising future potential as a global reserve currency and a method to make the World Wide Web (WWW) immune to cyberattacks such as the Distributed Denial-of-Service attacks. This survey approached cryptocurrencies' various technological and environmental issues from many different perspectives. To make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified, what technological solutions do we have? We found that cryptocurrency mining might be cleaner than is generally expected. There is also a plan to make a vast renewable energy source available by combining Ocean Thermal Energy Conversion and Bitcoin mining. There are plans to use unconventional computing methods (quantum computing, reversible computing, ternary computing, optical computing, analog computing) to solve some of the issues regarding the vast energy consumption of conventional computing (including cryptocurrency mining). We think using spare computing cycles for grid computing efforts is justified. For example, there are billions of smartphones in the world. Many smartphones are being recharged every day. If this daily recharging period of twenty to sixty minutes would be used for grid computing, for example, finding new cures to cancer, it would probably be a significant breakthrough for medical research simulations. We call on the cryptocurrency communities to research and develop grid computing and unconventional computing methods for the most significant cryptocurrencies: bitcoin (BTC) and ether (ETH).

INDEX TERMS Blockchain, DLT, cryptocurrency, bitcoin, green technology, sustainability, unconventional computing, climate change.

I. INTRODUCTION

Blockchain is a distributed database that maintains a continuously growing list of records (blocks) linked to each other. Blockchain is a special case of the more general Distributed Ledger Technology (DLT). For example, IOTA (tangle), Hedera (hashgraph), and Corda are not blockchains but distributed ledgers. A blockchain database is secure by design, and once the block is recorded there, it cannot be modified retroactively in a way that other nodes would accept

The associate editor coordinating the review of this manuscript and approving it for publication was Thanh Ngoc Dinh.

the modification. Blockchain relies on a peer-to-peer (P2P) network without any central coordinating node; each node of the network may access the entire blockchain database. Decentralization and resistance to data modification sparked much interest in blockchain technology. The most popular applications are the cryptocurrencies such as Bitcoin or Monero; there, blockchain is used for storing currency transactions. Due to the decentralization of blockchain, there is no need for the intermediaries such as banks or other currency transaction regulating bodies. Transactions propagate through the P2P network, and all the nodes participating in the network may validate them. Blockchain is also suitable for recording medical data [1] or cadastre information [2]. Senator Rand Paul has said bitcoin could become the world's reserve currency [3]. Bitcoin and other blockchain technologies could make the World Wide Web resistant to Distributed Denial-of-Service attacks [4].

In the early years, Central Processing Units (CPUs) were used to secure blockchains. The downsides of the blockchain (and other DLT) technology include a heavy electricity usage and the short lifetime of the mining devices that secure the ledgers; there are now specialized devices to mine cryptocurrencies that have a short lifetime of just about 1.5 years (in the case of Bitcoin ASIC miners). After that, the devices become e-waste with no useful purpose.

There are many efforts to stop climate change and fix the environment. For example, Doughnut Economics explores the ways to achieve thriving humanity in the 21st century [5]. Many people raise many concerns over the environmental impacts of cryptocurrencies, and our survey is one of the first to summarize many helpful technologies to make cryptocurrencies sustainable. Our survey comprehensively summarizes green and justification technologies for the blockchain space.

In this survey, we approach the issues of cryptocurrencies from many different perspectives. We will give a short introduction to why bitcoin and other cryptocurrencies are using so much energy. In later sections, we will list many exciting technologies that could help make bitcoin and other cryptocurrencies greener and more justified.

Blockchain energy consumption is a primary concern preventing its widespread application; many authors proposed to make blockchain more green, that is, by reducing its energy consumption, such as Dubrovsky *et al.* [6] presenting a prototype of Photonic Miner, which is an application of modern analog and optical computing; or alternatively, to make energy consumption to serve more practical purposes, such as training deep learning models during mining [7], or ASIC-resistant puzzles [8], useful puzzles, non-outsourceable puzzles, and Proof-of-Stake and virtual mining. Because of our expertise in volunteer computing (mostly SETI@home and BOINC), we wanted to emphasize potential grid computing methods that could revolutionize cryptocurrency mining.

Yet another motivation are the recent letters [9], [10] to the Environmental Protection Agency (EPA). The letter from Congress of the United States to the EPA [9] claimed that people living near crypto mining facilities are suffering from the air, water, and noise pollution. They refer to the research [11], [12] by de Vries *et al.* They requested the EPA to evaluate the compatibility of cryptocurrency mining facilities with the Clean Air Act and the Clean Water Act.

The EPA also got a response letter from bitcoin miners [10] with some of the misperceptions (in the letter from Congress to the EPA) debunked. For example, bitcoin miners refer to the Bitcoin Mining Council's latest Q1 survey of miners. The miners surveyed use 64.6% sustainable energy (wind, solar, hydro, or nuclear), and according to conservative estimates about the energy mix, bitcoin mining globally might be using about 58.4% sustainable energy. They compare this figure to the default US energy mix at 21% sustainable [13]. These figures mean that bitcoin mining might be cleaner than usually expected.

II. MAKING BITCOIN GREEN AND JUSTIFIED

In this section, we compare our survey to other surveys, describe the basics of Proof-of-Work mining, introduce our categories of Green and Justified technologies, and give a short introduction to Grid computing.

A. COMPARISON TO OTHER SURVEYS

Unconventional computing is often overlooked, so we wanted to emphasize optical, ternary, and reversible computing methods. We think that no other survey on green blockchain technologies at the moment is focusing on these unconventional methods. Bada *et al.* [14] mention a comprehensive list of ''Proof-of-X'' consensus methods. Their paper discusses these methods mostly from the point of view of Green technologies. Tschorsch *et al.* [15] also present a long list of ''Proof-of-X'' methods. Their paper discusses many key ideas regarding blockchain technologies.

Our survey divides technologies into two categories: those that lower the blockchain infrastructure's energy consumption and those that add blockchain infrastructure's usefulness without lowering the energy consumption per se. Our survey has a novel way of categorizing technologies. We also discuss if it is plausible or not to use the technology in question to make the biggest cryptocurrency - bitcoin (BTC) - greener or more justified.

We also like to mention the concept from futures studies called the Kardashev scale [16]. This exciting method for categorizing technological civilizations based on their ability to access power and energy will be discussed in the subsection ''Renewable and Nuclear Energy''.

This survey does not cover all possible technologies related to blockchains and DLTs. Delegated Proof-of-Stake (DPoS), Proof-of-Luck (PoL), Proof-of-Activity (PoAC), Proof-of-Capacity (PoC), Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), Federated Byzantine Agreement (FBA), Delegated Byzantine Fault Tolerance (DBFT), Proof-of-Authority (PoA), Proof-of-Importance (PoI), Proof-of-Burn (PoB), Proof-of-Believability (PoBLV), Proof-of-Devotion (PoD), Proof-of-Reputation (PoR),

Proof-of-Weight (PoWe), Proof-of-Publication, Proof-of-Bandwidth, Proof-of-Download [17], Proof-of-Learning [18], Proof-of-Excellence, Proof-of-Vote [19] and possibly many other Proof-of-X schemes were left out from the current survey. Many of those listed technologies were covered by [14] and [15].

B. PROOF-OF-WORK MINING NEEDS LOTS OF ENERGY

Bitcoin was described in a white paper in 2008 [20], and the blockchain was started in early 2009. It was possible to run the whole Bitcoin infrastructure on a small set of home computers. The first block of the Bitcoin blockchain is called the Genesis Block, and it contains the following message ''The Times 03/Jan/2009 Chancellor on brink of second bailout for banks''. The message was one of the headlines from The Times magazine released on 3 Jan 2009, so the message proves that the first Bitcoin block was generated during or after 3 Jan 2009.

What are blocks? The Bitcoin blockchain's blocks have two parts:

- header with metadata including a hash pointer reference to the previous block, the Merkle tree root of transactions, and block creation time;
- list of new bitcoin transactions.

The Bitcoin blocks are like pages in a diary; the diary is blank at the beginning, and one usually appends new information to the diary, and erasing or modifying information from the diary written with a ballpoint pen is very difficult. It is also difficult or impossible to erase or modify information from the Bitcoin blockchain's blocks. Adding new information to the Bitcoin blockchain is appending new entries (blocks) to the ledger in a process called mining, which needs lots of energy.

Why is bitcoin using so much energy? Most of the energy is used during the bitcoin mining process (called the Proof-of-Work or PoW), which serves at least two different major purposes:

- it distributes new cryptocurrency coins to cryptoeconomy; and
- it secures the Bitcoin blockchain ledger.

The bitcoin PoW mining algorithm is actually very simple in pseudo-code [21], [22]:

```
nonce=MIN
while(nonce<MAX):
  if sha256(sha256(block+nonce))<target:
    return nonce
  nonce+=1
```

The problem is that `target` tends to be a small number, so the SHA256d hash of `block+nonce` also needs to be a tiny number. One needs to try a considerable number of nonces to find a hash that is small enough eventually. This process of trying very many nonces is what consumes electrical energy.

In the late 2010s, bitcoin's colossal energy consumption became a major news topic. There was even a prediction in 2017 that bitcoin would consume all of the world's energy in 2020 [23]. This prediction was nowhere near becoming a reality because of the limitations of electricity grids, strict electricity regulations, the profitability of bitcoin mining, the lack of bitcoin mining devices, and many other reasons. In 2018, Mora *et al.* [24] claimed that bitcoin emissions could push global warming above two centigrades. The analysis and results of the paper by Mora *et al.* have been debunked at least by Houy [25], Masanet *et al.* [26], and Dittmar *et al.* [27]. According to Houy, rational mining limits Bitcoin emissions, and the average of a list of 62 ASIC miners used by Mora *et al.* in their analysis is not realistic; a rational miner would have turned off 14 of those 62 miners for most of the time. Masanet *et al.* remind us that poorly constructed future IT energy usage scenarios can spread misinformation and lead to ill-informed decisions. They give the five most important issues regarding the critical flaws in the design and execution of the research by Mora *et al.* Also, Dittmar *et al.* note that the electricity demand scenarios by Mora *et al.* seem unlikely.

De Vries [28] estimated in 2018 that the Bitmain company, with a claimed market share of 70%, could produce up to 6.5 million bitcoin mining machines (Antminer S9) in 2018. The machines would have a combined electrical power need of 8.92 GW. Table 1 shows the annual electricity consumption of Bitcoin in 2018 and 2021 and the annual electricity consumption of Ethereum in 2022. In 2019, the average power need of the whole world was 18.44 TW or 0.73 on Carl Sagan's interpolated Kardashev scale [29]. Table 1 shows the annual total energy consumption of the world in 2019 and 2020. In 2020, possibly due to the lockdowns caused by COVID-19, the annual total energy consumption of the world was lower than in 2019.

Bitcoin (BTC) and ether (ETH) are the most popular cryptocurrencies in 2022. Table 1 shows bitcoin, ether, and Visa ''transaction'' energy consumptions in kilowatt-hours in April 2022. We use the quotation marks with the transaction word (''transaction'') to inform the reader of the fact that it is somewhat misleading [30] to compute the transaction energy consumptions by taking the whole network's energy consumption in a period and dividing it by the number of transactions in a said period. In reality, bitcoin and ether transactions are not directly connected to the power needs of mining machines. According to Cambridge Centre for Alternative Finance [31], adding (or removing[1]) mining devices and thus increasing (or decreasing) electricity consumption does not have an impact on the number of processed transactions (transaction throughput). They note that a single transaction can contain hidden semantics like hundreds of payments or settlements (opening and closing transactions of micropayment channels) of Layer 2 payment solutions like

[1]Note by the corresponding author of this survey.

TABLE 1. Various energy consumptions in kilowatt-hours.

ID #	Characteristic	Energy consumption in kWh	Reference(s)
0	One Visa "transaction" (around April 27, 2022)	∼0.0014863	[32], [33]
1	*One ETH "transaction" (around April 27, 2022)*	∼238.22	[33]
2	*One BTC "transaction" (around April 27, 2022)*	∼2,188.59	[32]
3	The annual total energy consumption of a Type 0 civilization	8,760,000.00	[29]
4	The annual global electricity consumption of Facebook (2019)	∼5,140,000,000.00	[34]
5	The annual electricity consumption of Google (Alphabet) (2019)	∼12,700,000,000.00	[35]
6	*The annual electricity consumption of Bitcoin (November 2018)*	∼45,800,000,000.00	[36]
7	Tsar Bomba's yield (58 Mt TNT or 242.672 PJ)	∼67,410,000,000.00	[37], [38]
8	The annual electricity consumption of PC gaming (2012)	∼75,000,000,000.00	[39]
9	The annual electricity consumption of Finland (2019)	∼86,100,000,000.00	[40]
10	*The annual electricity consumption of Ethereum (21 April 2022)*	∼105,630,000,000.00	[41]
11	*The annual electricity consumption of Bitcoin (May 2021)*	∼113,890,000,000.00	[42]
12	The annual total energy consumption of the gold industry (May 2021)	∼240,610,000,000.00	[42]
13	The annual total energy consumption of the banking industry (May 2021)	∼263,720,000,000.00	[42]
14	The annual total energy consumption of Finland (2019)	∼378,000,000,000.00	[43]
15	An unmanned probe to reach Alpha Centauri in 71 years (with deceleration at the destination)	∼2,778,000,000,000.00	[44], [45]
16	The annual total energy consumption of the world (2020)	∼154,750,000,000,000.00	[46]
17	The annual total energy consumption of the world (2019)	∼161,530,000,000,000.00	[29], [46]
18	The annual total energy consumption of a Type I civilization	87,600,000,000,000,000.00	[29]

the Lightning Network or represent timestamped data points (for example, https://opentimestamps.org/).

If we continue using the misleading metric of energy per transaction, we can see that ten ether ''transactions'' is equal to about one bitcoin ''transaction'', but still, about 160,000 Visa ''transactions'' can be done with the same energy as only one ether ''transaction''. Figure 1 shows energy consumptions of the activities listed in Table 1.

Alden [47] says that Bitcoin's energy usage is not a problem because the energy used for mining is less than 0.1% of the world's energy consumption and because a sizable portion of the energy used for mining would be otherwise stranded and wasted.

The annual electricity consumption of Bitcoin in November 2018 was 45.8 TWh and the annual carbon emissions were between 22.0 and 22.9 $MtCO_2$ [36]. For comparison, the total electricity usage in Finland was 86.1 TWh in 2019 [40], the total energy consumption in Finland was 1362 PJ or 378 TWh [43] in 2019, and the total emissions of carbon dioxide (CO2 eq.) in Finland was 48.3 million tonnes in 2020 [48].

However, another problem with Bitcoin is the low throughput of the network on Layer 1: only about seven bitcoin transactions per second were possible globally before the SegWit and the Lightning Network updates. Only about 1 megabyte of information can be recorded on a Bitcoin block, and there are only about six blocks per hour. There are Layer 1 solutions to this; one of the solutions is used in the blockchain called Bitcoin Satoshi's Vision (BSV), a hard fork of Bitcoin Cash (BCH). Bitcoin Cash is a hard fork of Bitcoin (BTC). They all have a shared history - thousands of blocks since the Bitcoin Genesis block is identical to these three blockchains! After the hard fork, the chains separated into different branches. Hard forks can happen when there is a significant change in consensus rules that are incompatible with the old clients. For example, decreasing the block size is compatible with the old clients, so it can be considered a soft fork; increasing the block size is not compatible with the old clients, so it can be considered a hard fork. Bitcoin Cash is a hard fork caused by increasing the maximum block size. Bitcoin SV is a hard fork of Bitcoin Cash caused by implementing even a bigger block cap size. Bitcoin SV is reported to have a throughput of 9,000 transactions per second [49]. The hash rate of Bitcoin SV is still considerably lower than that of Bitcoin's, which means that high throughputs and low energy consumptions are possible with Bitcoin-like technology.

There are also Layer 2 solutions to the low throughput problem of Bitcoin. The Lightning Network is a Layer 2 solution, and it will be discussed later in this survey paper.

C. TWO DIFFERENT TECHNOLOGY CATEGORIES: GREEN AND JUSTIFIED

Usually, the arguments [50] on cleaning cryptocurrencies suggest banning the bitcoin cryptocurrency, cleaning Bitcoin's energy supply, or changing Bitcoin's consensus method from Proof-of-Work (PoW) to Proof-of-Stake (PoS). One does not usually differentiate what is meant by ''banning the bitcoin''. There are several forms of banning the bitcoin, including:

- one does not allow bitcoin to be used at all in the economy, and mining is prohibited in a certain jurisdiction;
- bitcoin is allowed to be used in an economy, i.e., financial transactions are allowed, but mining is prohibited in a jurisdiction;
- bitcoin mining is allowed in the jurisdiction, but its use to convey financial transactions is prohibited.

For example, the European Securities and Markets Authority vice-chair proposed the EU ban the PoW mining, but the proposal did not go through the EU committee [51].

We think that there are two main ways to make cryptocurrencies survive in the world of climate change and green politics. The securing process of the blockchain could

1) use less energy, so the blockchain's contribution to the climate change would be reduced;

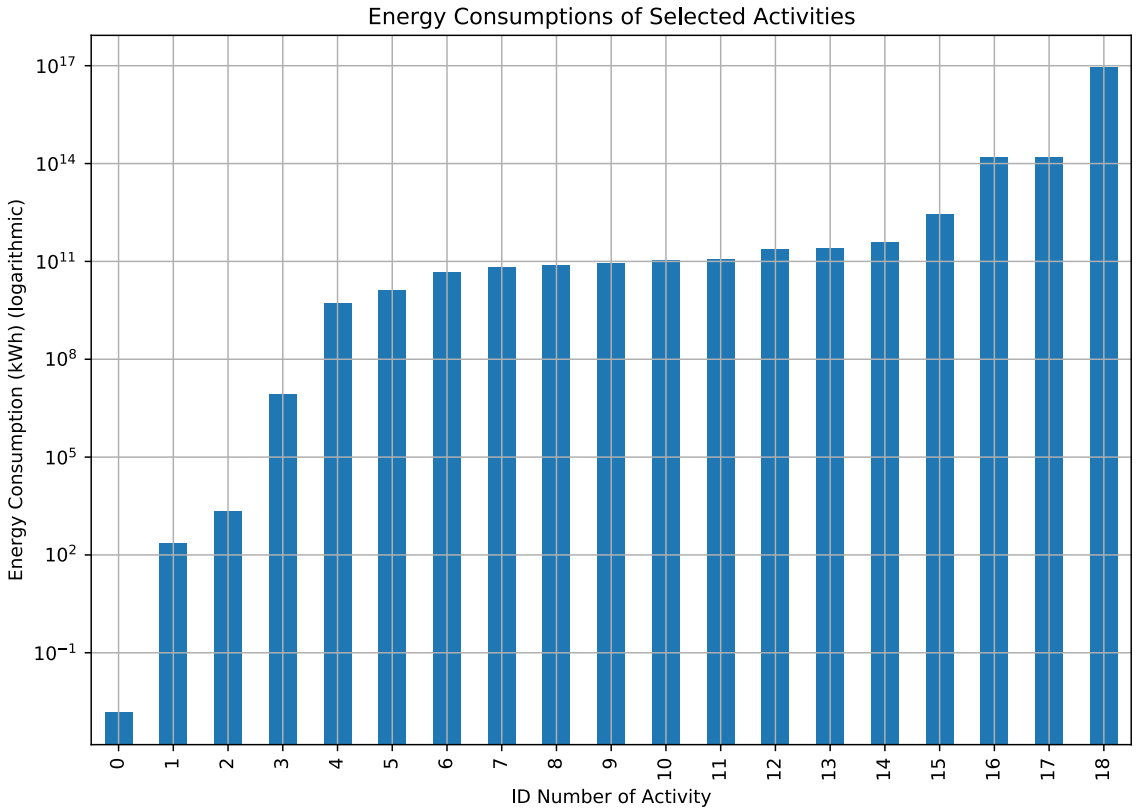

FIGURE 1. Energy consumptions of selected activities in kWh. See Table 1 for explanations to the ID numbers of selected activities.

TABLE 2. Global average virtual water content of selected products, per unit of product [52] and per gram of product.

Product	Virtual water content (litres)	Virtual water content (litres per gram)
1 tomato (70 g)	13	0.186
1 microchip (2 g)	32	16
1 slice of bread (30 g)	40	1.333
1 cotton T-shirt (250 g)	2000	8
1 hamburger (150 g)	2400	16

2) do something valuable (besides securing the blockchain) to make that process more justified.

We call the technologies fitting the description of the first list item the Green Technologies, and the technologies fitting the description of the second list item the Justification Technologies. In short, an example of a Green Technology would be a consensus process that secures the blockchain but does not use massive amounts of energy, even for a blockchain like Bitcoin. What if there is an optical computing method or a reversible computing method to calculate hashes? An example of a Justification Technology would be something that adds additional value to the consensus process without reducing energy consumption. What if the hashes generated in bitcoin mining could be recycled to seed PseudoRandom Number Generators? What if bitcoin mining could simulate new drug molecules for curing cancer?

D. GRID COMPUTING

The Justification Technology is related to volunteering computing [53] or grid computing platforms like GIMPS, distributed.net, SETI@home, Berkeley Open Infrastructure for Network Computing (BOINC), and Folding@home. In 1996, Great Internet Mersenne Prime Search (GIMPS) popularized volunteer computing, followed by distributed.net in 1997. There was a screensaver for volunteer computing called SETI@home in 1999 and the early 2000s before switching to the BOINC platform. SETI@home was invented to use the otherwise wasted spare CPU cycles of home computers when they were left idle with power on. Folding@home was introduced in 2000 and it eventually became one of the most powerful computing systems in the world; it reached 2.43 exaFLOPS (2.43 Eflops/s) in April 12, 2020 [54].

The CPU load of the computer running the grid software like SETI@home was usually around 100% depending on the software settings making the energy consumption also higher than in computers that were left to idle with power on. What is usually not considered is that developing and manufacturing a computer with a processor, mass storage, a Random Access Memory (RAM), a motherboard, a graphics card, and other electronics connected to the computer is also very resource-consuming. What if the computer is never used for anything (scientifically) useful? What if the computer is never even turned on? That computer is never wasting any electrical

energy from the wall socket, but still, vast amounts of energy and other resources were wasted during the manufacturing of the computer's microchips. Hoekstra *et al.* [52] claim that a 2-gram microchip has a virtual water content of 32 liters. For comparison, a 70-gram tomato has a virtual water content of 13 liters, and a 250-gram cotton T-shirt has a virtual water content of 2000 liters. Table 2 shows the virtual water content of selected products per unit of product and gram of product. According to Williams [55], secondary inputs of fossil fuels for manufacturing a microchip are 600 times the weight of the chip. This factor is around 1 or 2 for a car or refrigerator for comparison. We use the term ''manufacturing debt'' to describe the burden of manufacturing chips.

To counterbalance the wasteful manufacturing processes of electronics and wasteful idling of CPUs, one can donate spare computing cycles to scientific grid platforms like BOINC and Folding@home. These platforms then send workunits (analyzable data) to the computer to find new medicines for diseases like COVID-19, Alzheimer's, cancer, Huntington's, and Parkinson's. They can also send workunits to analyze radio telescope data to find evidence of extra-terrestrial intelligence or to simulate molecular interactions for material science research.

III. REVIEW OF GREEN TECHNOLOGIES

In this section we review the following technologies: Proof-of-Stake, The Lightning Network, Optical Computing, Reversible Computing, Ternary Computing, SolarCoin, Proof-of-Elapsed-Time, Renewable and Nuclear Energy, and Application-Specific Integrated Circuits.

A. PROOF-OF-STAKE

The second-largest cryptocurrency at the moment is ether (ETH), using the Ethereum blockchain [56] and a PoW consensus method. The mining of Ethereum's PoW is mostly done using Graphics Processing Units (GPUs) because it is challenging to develop Application-Specific Integrated Circuits (ASICs). The situation is not identical to Bitcoin's PoW because it was relatively easy to develop ASICs for Bitcoin mining [57]. As of April 21, 2022, Ethereum is using 105.63 TWh of electrical energy annually (comparable to the power consumption of Kazakhstan), and the carbon footprint is 58.91 Mt CO2 annually (comparable to the carbon footprint of Libya) [41]. The ASIC mining devices of Bitcoin have a service life of only about 1.5 years [58], and after that, they serve no practical purpose anymore because they can only calculate SHA256d hashes. Bitcoin mining generates 30.7 metric kilotons of e-waste annually, per May 2021 [11]. The numbers above give a strong incentive to develop environmentally friendly methods to achieve consensus in cryptoeconomies like Ethereum and Bitcoin. In 2022, Ethereum is switching from PoW to PoS. The first blockchain network to use PoS was probably Peercoin (or sometimes called ''PPCoin'') described in a whitepaper [59] in 2012. The native cryptocurrency, or coin, of the Peercoin blockchain, is peercoin (PPC).

BitFury Group has examined, in 2015, the pros and cons of PoW and PoS [60]. They use the term ''block mining'' to call the process of solving a computational challenge by a PoW protocol and the term ''block minting'' to call the process of solving a computational challenge by a PoS protocol. They list three important cryptocurrencies using the Hybrid PoW / PoS consensus method: Peercoin (PPCoin), Blackcoin, and Novacoin. They mention that the Nxt cryptocurrency uses the PoS consensus method alone, that BitShares uses Delegated Proof-of-Stake, and that Ethereum will use Delegated Proof-of-Stake in the future. The ''Nothing at Stake Problem'' is mentioned as a potential problem, which allows minting blocks on different branches after forking of the blockchain has happened.

How does a PoS system work? Tschorsch *et al.* [15] mention the concept of ''coin-age'', which is defined as the amount of currency multiplied by the holding period. If Alice sends ten coins to Bob, and Bob holds these coins for two weeks, the coin-age is 140 coin-days. Bob will destroy the accumulated coin-age by spending the ten coins. The coin-age is used to calculate the block reward in PoS. Minting a PoS block needs a hash value below or equal to a target value (similar to PoW mining). PoS (in contrast to PoW) has individual difficulty, which is inversely proportional to the coin-age. The PoS minters cannot use computational power to solve the puzzle faster than others because there is no nonce to modify. Every time the timestamp changes, the minters have a new chance to find the correct solution. After finding the correct solution, the minter broadcasts the block, including the coinstake transaction, rewarding the block minter.

For becoming a PoS validator (similar to being a PoW miner) in Ethereum, one needs to stake 32 ethers [61], which are worth almost 90,000 euros as of April 22, 2022. Because many people do not have such funds available, staking services (similar to PoW mining pools) allow users to serve as validators jointly. The more ethers one stakes (similar to having more mining power in PoW consensus), the greater the chance to win the lottery game of consensus forming.

The change from PoW to PoS should reduce Ethereum's energy consumption by 99% and allow 100,000 transactions per second [61]. From Table 1 we can assume that PoS version of Ethereum ''transaction'' (1% of PoW energy consumption after the 99% reduction) would consume about 2 kilowatt-hours. One PoS Ethereum ''transaction'' would consume as much as about 1600 Visa ''transactions''.

B. THE LIGHTNING NETWORK

The regular bitcoin payments operate on Layer 1. They were limited to around seven transactions per second globally before the SegWit update because the Bitcoin blocks are limited to about one megabyte of size, and mathematics guarantees that about 10 minutes pass between two blocks in general. On average, there are about six new Bitcoin blocks per hour. A common misconception links the Bitcoin network's throughput (transactions/s, or tx/s for short) and the Bitcoin network's energy consumption together. In reality, the

throughput is not directly connected to the amount of bitcoin mining power nor the energy consumption of those mining devices. It is possible to increase the number of bitcoin transactions per second without increasing the mining power and energy consumption.

The Lightning Network (a Layer 2 solution) is one possible method to have a considerable number (thousands) of bitcoin transactions per second. Litecoin was the first blockchain to test the Lightning Network. There is also a similar network for fast, cheap, scalable, and privacy-preserving payments (ERC-20-compliant token transfers) for Ethereum - the Raiden Network. The main idea is to open a micropayments channel, have almost unlimited transactions off-chain, and then close the micropayments channel. Only the transactions involved with the opening and closing of the micropayments channel will be recorded on-chain. Poon *et al.* [62] claim in the Lightning Network paper that 7 billion people making two transactions a day on Layer 1 would require 24-gigabyte blocks every ten minutes. However, seven billion people making two transactions a year (opening and closing the micropayment channels) on Layer 2 (the Lightning Network) would allow unlimited transactions inside the channel and require only 133-megabyte blocks every ten minutes.

C. OPTICAL COMPUTING

Optical computing means using light waves for processing, storage, and communication. Using conversion from photons to electrons would make the system slower and bulkier thus an efficient optical computing system needs three things:

- optical processor;
- optical data transfer; and
- optical storage.

Optical computing is still not widely used, so it is categorized as a form of unconventional computing in Table 3. Still, optical technologies are used for data transmission applications such as optical digital audio (TOSLINK) and fiber-optic communications (some versions of Ethernet). In everyday applications, optical technologies are used in cameras, displays, remote controls, optical mouses, and optical/magneto-optical discs (Laserdisc, CD, MiniDisc, DVD, HD-DVD, Blu-ray, and Ultra HD Blu-ray).

Sawchuck *et al.* [63] define optical computing as ''the use of optical systems to perform numerical computations on one-dimensional or multidimensional data that are generally not images''. They mention that optical signals can interact on time scales smaller than a picosecond (10^{-12} s) via an intermediary medium making high throughputs possible.

1) OPTICAL PROOF-OF-WORK

The motto for Bitcoin's PoW consensus method was ''one CPU, one vote,'' but today, the Bitcoin blockchain is secured by a small number of corporate organizations using ASIC machines, and the mining energy is coming from places with cheap electricity [64]. The ongoing discussion on climate change has also put some pressure on introducing greener cryptocurrencies. For example, Hal Finney, who was a Bitcoin pioneer, thought about ways to reduce carbon dioxide emissions of Bitcoin already in 2009 [50].

Optical Proof-of-Work (oPoW) is a PoW paradigm to decouple Bitcoin mining from energy. Dubrovsky *et al.* [6] present their oPoW Silicon Photonic Miner Prototype as a new application of modern analog computing and optical computing. It should make it possible to mine bitcoin even in areas with high electricity costs. oPoW should shift the operating expenses (OPEX) of electricity to hardware's capital expenses (CAPEX). The new consensus method is computable with photonic processors, but it should also be hardware-compatible with GPUs, Field-Programmable Gate Arrays (FPGAs), and ASICs, making it possible to use both

TABLE 3. Different forms of computing.

Different forms of computing		
Category	Explanation	Example
digital	Conventional computing, where information is discret.	Almost all of the computers of today.
analog	Unconventional computing, where information is continuous.	TDC Mark III.
binary	Conventional digital computing, which uses 2-valued logic.	Almost all of the computers of today.
ternary	Unconventional digital computing, which uses 3-valued logic.	Setun.
decimal	Unconventional digital computing, which uses 10-valued logic.	ENIAC.
irreversible	Conventional computing, which erases information and where going back to the previous state of the calculation is generally not possible.	Almost all of the computing in the past and nowadays.
reversible	Unconventional computing, which does not erase information and where going back to the previous state of the calculation is possible.	Mostly theoretical at the moment.
electrical	Conventional computing, which is controlled by electrical circuits.	Almost all of the computers of today.
mechanical	Unconventional computing, which is controlled mechanically.	Antikythera mechanism.
DNA	Unconventional computing, where the huge parallelization of the deoxyribonucleic acid is being used.	Mostly theoretical at the moment.
optical	Unconventional computing, where computations, data transfer and storage are done using optical methods.	Mostly theoretical at the moment.
classical	Conventional computing, where classical physics is used to process information.	Almost all of the computing in the past and nowadays.
quantum	Unconventional computing, where quantum physics phenomena are being used to process quantum information.	IBM Q 5 Tenerife.

optical and electrical (non-optical) computing methods for mining. A high-CAPEX PoW should also have the benefit of making the hash rate resilient to price fluctuations because it is not expensive to keep low-OPEX hardware online even during a period of low mining rewards [64].

Sawchuck *et al.* [63] predicted, in 1984, that optical systems might be cheaper than equivalent non-optical systems for specific signal processing applications. Interestingly, the developers of oPoW claimed, in 2021, that the silicon photonics used in oPoW are cheaper to develop because they use the older fabrication nodes (90 nm) than the state-of-the-art non-optical computing systems (5 nm) [64].

D. REVERSIBLE COMPUTING

When one calculates something with a regular computer, one asks the computer a question. For example, one is asking the computer "What is $2 + 2$?", and the computer answers "4". From the answer, it is not so easy to form the original question; the question could have been "What is $-6 + 10$?" or "What is $20 - 1 - 19 + 4$?" The information of the original question has been erased. Nevertheless, the information has not disappeared from the universe because there is the law of conservation of information. Erasing even one bit of information generates waste heat because of the laws of thermodynamics [65].

The conventional computing of today is irreversible, meaning that information is erased and vast amounts of waste heat are generated during computations. The computation process can be reversed in time in reversible computing to reaccess the previous states. Frank [66] states that reversible computing preserves signal energies and reuses them. The more popular method of unconventional computing - quantum computing - might only give some speedups on a few specialized applications, but reversible computing might achieve greater energy efficiency and functional performance for all digital computing applications. Reversible computing could be from 1000 to 100,000 times as cost-effective as irreversible computing in the 2050s [67].

Landauer [68] formulated

$$E = k_{\mathrm{B}} T \ln(2), \tag{1}$$

which states that E is the heat dissipated by a logically irreversible gate to its environment, k_{B} is the Boltzmann constant, T is the temperature of the environment in kelvins, and ln(2) is the natural logarithm of 2. At room temperature (293.15 K), erasing one bit of information generates about $2.805 \cdot 10^{-21}$ joules of heat [69].

Making gates logically reversible is probably not enough to achieve energy savings. The gates must also be physically reversible, which they are not in a traditional CMOS design. The charging and discharging of circuit elements must be adiabatic. The rules [69] to achieve this are

1) Do not turn on a switch if there is a significant voltage difference between the channel terminals.
2) Do not turn off a switch if there is a significant electrical current flowing through the channel of the switch.

Probably one of the earliest attempts to use reversible logic for developing secure cryptosystems was the research by Thapliyal *et al.* [70] in 2006. They present reversible designs of adders and Montgomery multipliers for a prototype of a reversible ALU for a cryptoprocessor. The motivation for this is the Differential Power Analysis (DPA), where attackers could break encryptions by measuring the energy consumed, Equation (1), in an irreversible digital circuit.

Heinonen *et al.* [71] suggested using reversible computing in bitcoin mining, but it is not known how much additional energy efficiency it would give (if any) when compared to the irreversible ASIC bitcoin mining. The paper showed that the number of bits generated by a regular ASIC miner is so high that any cloud-based scratch memory (used in reversible computing) is out of the question with any realistic Internet connection bandwidths of today (for example, 1 Gbit/s). There are also no practical reversible computing architectures when writing this. The suggestion to use reversible computing for bitcoin mining was made to motivate bitcoin ASIC developers to jump-start the development of reversible computing chips. Reversible computing might be the only way to keep increasing the computing power in the future after the conventional computing methods of today have reached their limits.

E. TERNARY COMPUTING

Digital computing is almost always using the binary base of two digits: 0 and 1. The binary base is not the only possible method for digital systems. For example, the ternary (trinary) system is based on three digits. The following list of trinary digit mappings is from Connelly's thesis [72]:

- unbalanced trinary: {0, 1, 2};
- fractional unbalanced trinary: {0, 1/2, 2};
- balanced trinary: {−1, 0, 1};
- unknown state logic: {F, ?, T};
- trinary coded binary: {T, F, T}.

In the previous list, "T" means True, "F" means False, and "?" means unknown (both T and F at the same time).

According to the IOTA Beginners Guide [73], ternary systems used for complex logic circuits within a CPU will lead to energy savings and also to space savings due to the smaller design of the microcontroller. Ternary systems have not been used because there is a lack of mass-market support. What other reasons could there be to change from binary logic to ternary logic? The ternary logic could [72], [74]–[79]

- reduce the required interconnections for logic functions;
- reduce the chip area;
- allow more information transformation over a line;
- reduce the memory requirements for data;
- allow higher speeds for serial operations.

The Ternary Manifesto by Douglas W. Jones [80] says that one ternary digit, a trit, can represent 1.58 bits. A 21-trit ternary computer could handle values as big as 33.18 bits, which is slightly larger than a 32-bit binary computer could handle. Jones also notes that a ternary computer would have

more transistors than a binary computer, but the number of wires would be reduced to 64%. Cambou *et al.* [81] suggest that balanced ternary logic is suitable for IoT security, authentication of connected vehicles, and also for hardware and software assurance. There are also ternary systems for quantum computers! These systems do not use qubits but qutrits. Caraiman *et al.* [82] use ternary quantum computing for image representation and processing.

1) IOTA

The IOTA Token [83] is a cryptocurrency that is designed for machine-to-machine (M2M), human-to-human (H2H), and human-to-machine (H2M) payments and for the Internet of Things (IoT). The ternary logic is there in many things: JINN is a ternary microcontroller, Troika is the hash function, and IOTA seeds only have capital letters from A to Z and the number 9. According to the IOTA Beginners Guide [73], the ternary system is more efficient because it has the highest density of information representation.

F. SolarCoin

SolarCoin is a blockchain-based project that rewards those who have solar installations generating electricity and have the appropriate SolarCoin software installed. If the solarcoin (SLR) price exceeds the production cost of the solar energy associated with the generated solarcoin, the solar power becomes basically free.

SolarCoin started as a new blockchain in 2014 [84], but in around 2021, it migrated to Ethereum. In the early days of SolarCoin, from January 2014 to August 2015, a PoW consensus was used, and later from August 2015 onwards, a Proof-of-Stake-Time was used [84].

Johnson *et al.* [84] noted in 2015 that the Bitcoin blockchain used 4,326,821,400.931 kWh of energy annually, and the SolarCoin blockchain (normalized to Bitcoin user size) would have used 328,725,000.000 kWh of energy annually. They calculated that the minimum energy required for a bitcoin ''transaction'' was 19.587 kWh and the minimum energy required for a solarcoin ''transaction'' was 0.1488 kWh

Johnson *et al.* [84] constructed and tested a SolarCoin node for 11 months. The system with a 250 W solar panel was generating on average 0.040 kWh per day and 0.00004 SLR (solarcoins) per day.

G. PROOF-OF-ELAPSED-TIME

Proof-of-Elapsed-Time (PoET) is a consensus method developed by Intel Corporation for permissioned blockchain networks where participants must identify themselves before they are allowed to operate. Intel developed PoET together with Software Guard Extension (SGX) technologies according to Bada *et al.* [14]. It is used in the Hyperledger Sawtooth platform. The other consensus methods that are available for Sawtooth [85] are Raft [86] and Practical Byzantine Fault Tolerance (PBFT) [87].

PoET does not need as much energy as typical PoW methods because PoET randomly selects a node for the consensus forming instead of requiring the miners to compete against each other. The algorithm generates a random wait time for each node in the network. The nodes must sleep over that time. The node that wakes up first (has the shortest sleep time) will win the lottery game and gets to add a new block to the blockchain. The code is also executed within a secure environment, and the lottery results are verifiable by external agents [88].

H. RENEWABLE AND NUCLEAR ENERGY

A simple solution to make Bitcoin greener is to use renewable and nuclear energy for bitcoin mining. This change would not require any changes to the Bitcoin protocol itself.

De Vries [58] concludes that renewable energy is not the answer to Bitcoin's sustainability problem. Also, the lifetime of ASIC mining devices is considerably short, producing lots of e-waste even if the mining itself is using sustainable energy. The conclusions come from the assumptions that it is challenging to unite bitcoin mining with renewable energy sources and that energy usage is not the only way in which bitcoin mining impacts the environment. Nuclear energy is not mentioned in De Vries' article.

Kardashev scale [16], [29] is a method of measuring a civilization's technological level from the power the civilization can use. The categories are Type 0 (or 0.0 on Carl Sagan's interpolated Kardashev scale), Type I (1.0), Type II (2.0), and Type III (3.0). Type 0 civilization is using 10^6 W of power; Type I civilization is using 10^{16} W of power; Type II civilization is using 10^{26} W of power; and Type III civilization is using 10^{36} W of power. According to common speculation, during the transition from Type 0 to Type I, the civilization has a high risk of self-destruction. After reaching Type I, the civilization might be safe. Currently, human civilization has not reached Type I yet. The human civilization is calculated, as in Equation 2, to be around 0.73 on Sagan's interpolated Kardashev scale.

$$K = \frac{\log_{10}(P) - 6}{10}, \tag{2}$$

where K is the Sagan's interpolated Kardashev rating of the civilization, and P is the power the civilization uses (in watts). Type I civilization can control its home planet's power output, Type II civilization can use its home star's entire radiation output, and Type III civilization has access to the power of its home galaxy.

We want to encourage the reader to think that it is not necessarily always wrong to have a considerable energy consumption. A technically advanced civilization needs lots of energy. Humanity should still try to optimize the energy consumption of their technologies (like bitcoin mining). What is usually overlooked is that we need a safe and environmentally-friendly way to produce vast amounts of cheap and usable energy. Solar power, at least in the form of solar power satellites, nuclear fusion energy, and nuclear

fission energy, are all potential candidates of technologies for the human civilization to become a Type I civilization. An advanced civilization could achieve Type II, perhaps, by building a Dyson sphere (basically a swarm of solar power satellites) that completely encompasses the star. Type III could be achieved by building a Dyson sphere for every star in a galaxy. There has been some interest in finding Dyson spheres in the Milky Way galaxy; for example, Minniti *et al.* [89] ask the question: Can we find candidate Dyson spheres in the Milky Way?

Can humanity reach Type I, and how? Ocean Thermal Energy Conversion (OTEC) is a form of renewable energy invented in 1881. It uses the ocean thermal gradient of deep & cool seawater and warm surface seawater for running a heat engine. Pelc *et al.* [90] mention the article by Thomas H. Daniel [91], which claims that about 10 TW of power could be generated by OTEC without affecting ocean's thermal structure. The cost of electricity, in 2002, from OTEC would have been around 0.08 USD/kWh and 0.24 USD/kWh (∼2002 USD price levels), which was much higher than fossil fuel costs, potentially leading the OTEC to be subsidized. A potential solution to make OTEC feasible is to incorporate Bitcoin mining [92]. The interconnected, medium-scale (5-to-10 MW) OTEC plant would cost something between 200 million USD and 300 million USD, and the cost of the electricity would be around 0.50 USD/kWh and 1.00 USD/kWh (∼2022 USD price levels). There would be tens of millions of US dollars savings by avoiding an offshore cable. The final estimate of the electricity price generated by this medium-scale stranded OTEC plant is around 0.11 USD/kWh (∼2022 USD price levels). The electricity would be sold to Bitcoin miners. Coincidentally, the Bitcoin Magazine article mentions the Kardashev scale.

There are also interesting projects on nuclear fission and nuclear fusion power, so nuclear power is not obsolete. Lockheed Martin's Skunk Works even has a slogan ''Restarting the Atomic Age'' [93]. Olkiluoto-3 nuclear fission power plant is operating and should be generating 1600 MWe of power before the end of 2022. Small Modular Reactors (SMRs) could make building nuclear fission power plants faster and cheaper. Olkiluoto-3 is an example of a big nuclear fission power plant, and facilities using an SMR would be examples of small nuclear fission power plants. There is a similar concept of facility size for nuclear fusion power; the trend was to build as large facilities as possible, for example, ITER, but nowadays, it is more attractive to do research and development on small nuclear fusion reactors [94].

I. APPLICATION-SPECIFIC INTEGRATED CIRCUITS

Hashes from different hashing algorithms are not comparable; for example, a SHA256d hash (used in Bitcoin) is not the same as a Scrypt hash (used in Litecoin). Therefore, the hashing rates (H/s) are different for SHA256d ASIC and Scrypt ASIC miners.

Taylor's paper [57] tells the story of early adopters of bitcoin who created the bitcoin ASIC mining industry. CPUs were used for bitcoin mining in 2009 and the early 2010s. Overclocked 6-core CPUs (Core i7 990x) could reach 33 MH/s. In 2010, bitcoin mining software could use GPUs for bitcoin mining. Nvidia's GPUs (GTX570) could reach 155 MH/s, and AMD's powerful gaming graphics card GPUs (7970) could reach 675 MH/s. The next stage started in 2011 and introduced FPGAs for bitcoin mining. CAPEX of Spartan 150 was higher per MH/s compared to AMD GPUs, but a power need of 60 watts compared to 200 watts of AMD GPUs made OPEX of Spartan 150 lower. The latest stage was the introduction of ASICs for bitcoin mining in 2013. After the ASICs became available, CPU, GPU, and FPGA bitcoin mining profits were negative.

Taylor [57] notes that bespoke (customized) silicon can be developed in small volumes. The first developer of Bitcoin ASICs was Butterfly Labs (BFL), taking pre-orders in June 2012 for three types of ASIC miners rated at 4.5 GH/s (Jalapeno), 60 GH/s (SC Single), and 1,500 GH/s (SC MiniRig). Introduced in May 2020, Bitmain's Antminer S19 Pro [95] was capable of achieving a hash rate of 110 TH/s, having an efficiency of 29.5 J/TH, and taking 3250 watts of electrical power.

IV. REVIEW OF JUSTIFICATION TECHNOLOGIES

It is not enough to make Green (energy-efficient) technologies. Hicks *et al.* [96] found that the usage of LED lighting might lead to the usage of more light, increasing the energy consumption and reducing or even eroding any energy savings from the energy-efficient LED technology. The Jevons paradox occurs when the efficiency of some resource usage increases, but the falling cost of the resource usage increases the demand and negates the gains from the efficiency. Modern economics knows this paradox as a rebound effect. In the 1980s, Daniel Khazzoom and Leonard Brookes independently had ideas that increased energy efficiency leads to increased energy usage. In 1992, this hypothesis was named a Khazzoom–Brookes postulate, similar to the Jevons paradox.

We believe that making more energy-efficient ASICs, building optical bitcoin miners, and reversible bitcoin miners will also lead to a higher demand for the bitcoin mining hardware negating any gains from the Green bitcoin mining technology. There is now a motivation to introduce some Justification Technologies.

In this section we review the following Justification technologies: Proof-of-Deep-Learning, Proof-of-Evolution, Prime Chain Proof-of-Work, Distributed Computing Grids, Merge-mining, Many-money Economy, and Hash Recycling.

A. PROOF-OF-DEEP-LEARNING

Chenli *et al.* [7] propose a consensus method called Proof-of-Deep-Learning (PoDL), which generates a valid proof of a new block after a proper deep learning model is produced. Their benchmark and simulation results prove their concept is plausible for various cryptocurrencies using a hash-based PoW consensus method.

The Deep Learning models used in PoDL had sizes from 100 kilobytes to 10 gigabytes [7]. There are techniques to reduce the sizes without affecting the accuracy very much.

The proposed method is not ASIC-resistant [7], quite the contrary: it is even mentioned that ASIC devices will be designed to do the deep learning training, and it will be favorable for the development of better hardware.

B. PROOF-OF-EVOLUTION

Proof-of-Evolution (PoE) is a consensus method developed by Bizzaro *et al.* [97] that keeps the security features of PoW and uses the mining process to execute genetic algorithms (GAs).

The proposed method also encourages cooperation among miners because it is possible to share the best solution found so far with miners, who can then add it to their population. It is similar to Proof-of-Search (also known as "PoS", not to be confused with Proof-of-Stake or Proof-of-Space) [98], which extends PoW for solving optimization problems.

C. PRIME CHAIN PROOF-OF-WORK

The prime number search is mostly focused on Mersenne prime numbers of the form

$$M_p = 2^p - 1, \tag{3}$$

where p is a prime number. They were named after Marin Mersenne. In 2013, the top 10 largest known prime numbers were all Mersenne prime numbers [99] as in Equation 3. The Primecoin whitepaper also mentions other well-known types of prime number pairs, such as twin primes, where both p and $p+2$ are prime numbers, and Sophie Germain prime numbers, where both p and $2p + 1$ are prime numbers. Cunningham Chain of the First Kind and the Second Kind and Bi-Twin Prime Chains are also explained with simple examples.

According to Primecoin's website [100], Primecoin's Prime Chain Proof-of-Work uses the search for Cunningham Chain of the First Kind, Cunningham Chain of the Second Kind, and Bi-Twin Prime Chain to secure the Primecoin blockchain. They state that Prime Chain PoW is valid and that primecoin (XPM) was the first cryptocurrency to achieve energy multi-use.

D. DISTRIBUTED COMPUTING GRIDS

In grid computing, one often encounters the term FLOPS. In cryptocurrency mining, one often encounters the term H/s. What are these terms? FLOPS means floating-point operations per second (flop/s). H/s means hashes per second.

1) GRIDCOIN

According to the Gridcoin Blue Paper [101], gridcoin (GRC) is a decentralized PoS cryptocurrency that incentivizes participation in the BOINC distributed computing grid platform. According to the Gridcoin White Paper [102], an iPhone 6 has seven gigaFLOPS of computing power. They also calculate that all 2.5 billion smartphones in the world would form a computing network of about 17.5 exaFLOPS, and if they are idling half of the time, this computing power will reduce to about 8.75 exaFLOPS. They predicted that in 2020 there would be over 5 billion smartphones in the world.

2) CURECOIN

Curecoin (CURE) [103] is a cryptocurrency reward for those who create computing power for some selected Distributed Computing Networks (DCNs) - currently, only the Folding@home project as in Figure 2. The automated distribution system is located at cryptobullionpools.com. Curecoin has an efficient PoS-like system. The Curecoin wallet can be seen in Figure 3.

3) FOLDINGCOIN

The foldingcoin (FLDC) token [104] is using the Counterparty protocol [105], which allows tokens on the Bitcoin blockchain. There is a method of Proof-of-Fold to verify the computational power contributed to the Folding@home project.

The Foldingcoin White Paper claims the following

- At the end of 2012, there was 25 TH/s of mining power in the Bitcoin network coming from CPUs and GPUs, because ASICs were not available back then.
- Hashing does not do any floating point operations and it is not possible to directly convert from TH/s to petaFLOPS, but there is a generally-accepted ratio of 1 TH/s = 12.7 Pflop/s.
- Therefore, there was 25 TH/s $= 25 \cdot 12.7$ Pflop/s $\approx$ 318 petaFLOPS of unused CPU and GPU computing power available around the beginning of the ASIC Bitcoin mining era.

Foldingcoin's market capitalization did not get any updates after October 2018 in CoinGecko.

E. MERGE-MINING

New and small blockchains tend to have the problem of not having enough benevolent mining power; it could be relatively easy for malicious parties to take them over [106]. Cryptocurrencies are usually competing against each other for computational resources. The competition does not always have to be the case; merge-mining (or merged mining) [107] means the act of mining two or more cryptocurrencies at once without additional PoW effort. The process is also known as Auxiliary Proof-of-Work (AuxPoW). The merge-miners will get extra profits without having to add any extra mining efforts.

Judmayer *et al.* [108] and Zamyatin [109] state that little was known about the effects and implications of merge-mining even though it had been used for several cryptocurrencies. Judmayer *et al.* found that mining pools with merge-mining cryptocurrencies had operated at the edge of, and even beyond, the security guarantees of the Nakamoto consensus. Merge-mining could centralize mining, which is against the principle of decentralization. Ali *et al.* [106] found

FIGURE 2. **Folding@home currently lets the user to choose from research for COVID-19, Alzheimer's, Cancer, Huntington's, and Parkinson's. There are also options for "Any disease" and "High Priority".**

that the then-largest merged-mined cryptocurrency, namecoin, was vulnerable to the 51% attacks giving a false sense of security.

F. MANY-MONEY ECONOMY

Like most blockchains at the moment, the Bitcoin blockchain is only using one type of coin/cryptocurrency. What if the Bitcoin blockchain had two (or more) different types of cryptocurrencies? It is well known that bitcoin (BTC) is suitable for saving money, but it is not so good for spending money. What if there was a protocol update for Bitcoin that introduces a second coin type - perhaps a good coin for spending?

Heinonen *et al.* [71] introduced the idea of the inflationary bitcoin coin (BTCi) to motivate the old mining device users to keep on mining. That kind of coin should reduce the amount of e-waste from ASIC machines. They call the regular bitcoin coin (BTC) the deflationary bitcoin coin (BTCd), and they say that these two different coin types could have different exchange rates and money supply sizes. The motivation for two different monies in the Bitcoin blockchain is that the regular bitcoin (BTCd) is not used so much for everyday spending, making the regular one-money Bitcoin blockchain, not a good candidate for a Decentralized Payments System (DPS). The two-money Bitcoin blockchain would be a far better candidate for a DPS.

Heinonen [110] introduced the idea of antimoney bitcoin coin (aBTC). The research suggested using antimoney to enable payments when Morini's stablecoin is frozen. The above is also an example of a many-money economy.

Ethereum is an excellent example of a many-money economy in a blockchain. Coins are the native cryptocurrencies of a blockchain; tokens are cryptocurrencies based on smart contract technologies. The ether coin (ETH) is the native cryptocurrency of the Ethereum blockchain, and there are thousands of tokens using the smart contract technology, for example, the ERC-20 tokens. These ERC-20 tokens are all stored in the same Ethereum blockchain as the ether (ETH) transactions. There are also many other token standards than

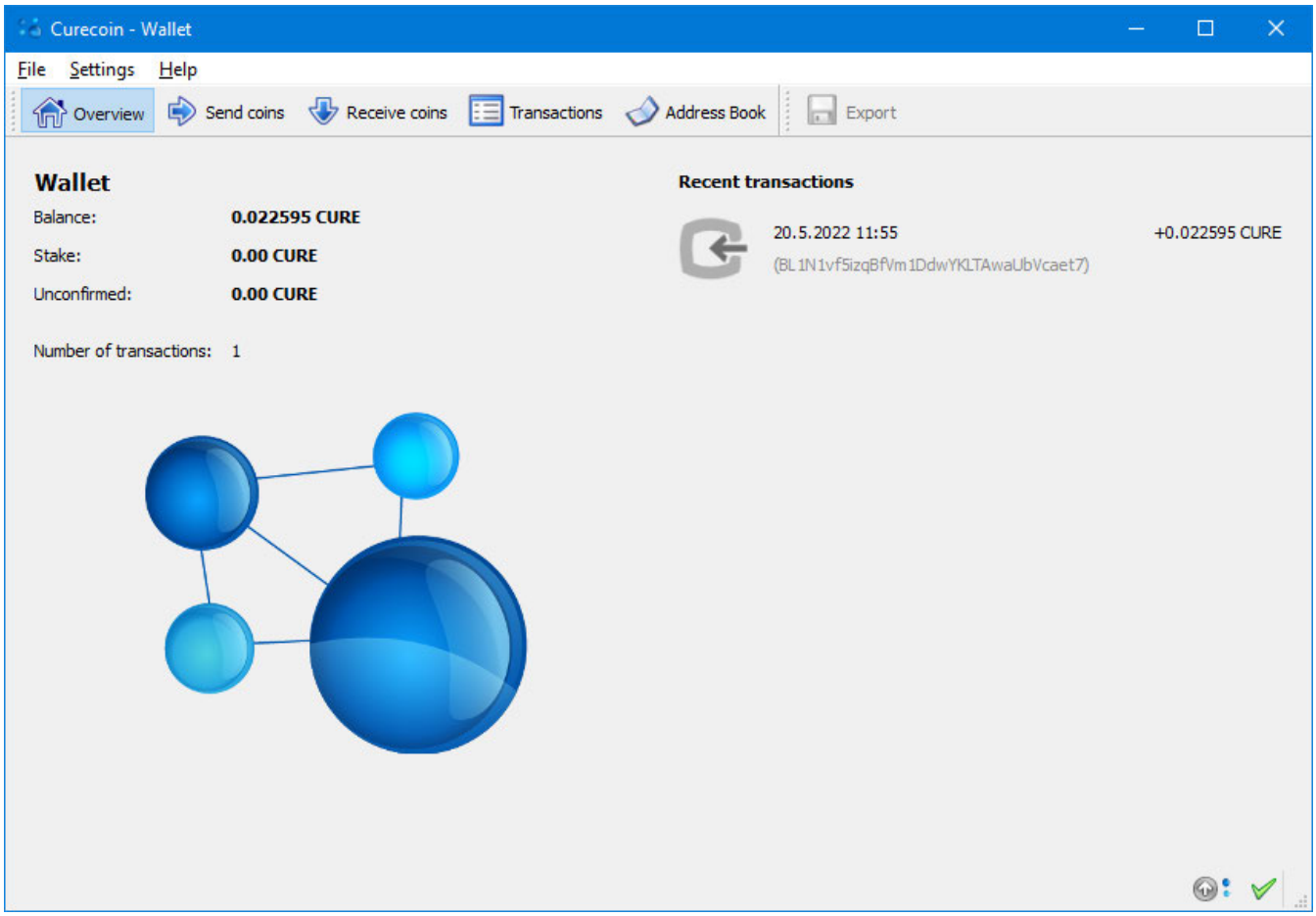

FIGURE 3. Curecoins will be received to the Curecoin wallet after donating spare computing cycles for Folding@home project as a member of the Curecoin team.

the famous ERC-20; Non-Fungible Tokens (NFTs) use other standards. Research on the behavior of price changes of cryptocurrencies is done by Stosic *et al.* [111], and research on the behavior of price changes of ERC-20 tokens is done by Heinonen *et al.* [112].

G. HASH RECYCLING

There are lots of PseudoRandom Number Generators (PRNGs) available such as Blum Blum Shub [113], Yarrow [114], and Fortuna [115]. They can be used to generate numbers that are not true random numbers because computers of classical computing behave in a deterministic way. One could use unconventional computing like quantum computing to produce real random numbers. There are also Quantum Random Number Generators (QRNGs) [116] that generate perfectly unpredictable random numbers from a quantum source.

Still, we are far from using quantum computing in everyday computing, so we should concentrate on classical computing and its deterministic applications like the generation of pseudorandom numbers. How can we make a connection between bitcoin mining and pseudorandom numbers? Heinonen *et al.* [71] introduced the concept of hash recycling. The idea came from the LavaRand method [117] that uses digital images of lava lamps for seeding PRNGs. LavaRand takes a digital picture of a lava lamp, converts the image to binary numbers, applies a cryptographic hash function, obtains a seed from the hash function, and feeds that seed to the PRNG. The idea is to have a public entropy pool on the Internet. A user could use the public entropy pool like the Hardware Random Number Generators (HRNGs) [118], which are usually used to generate the seed for a faster PRNG, which generates pseudorandom numbers at a much higher date rate [119].

It is an interesting observation that according to Heinonen *et al.* [71], there were about 10^{28} hashes and $2.56 \cdot 10^{30}$ bits generated to secure 703,364 blocks to the Bitcoin blockchain between early 2009 and late 2021. The Kardashev scale mentioned earlier is about a civilization's access to power and energy. There is a similar rating concept regarding civilization's access to information. This scale is developed by Carl Sagan [29]. He assigned the letter A to represent 10^6 unique bits of information. Each successive letter (the English alphabet's letters running from A to Z)

represents an order of magnitude increase, which means that a level Z civilization would have access to 10^{31} unique bits. In 1973, humanity was a 0.7H civilization. In 2018, humanity was a 0.73J civilization. Bitcoin mining alone would get humanity easily to level Z, but because humanity does not have access to those wasted hashes anymore, the information rating level of humanity is probably still around level J. Of course, there is nothing extraordinary in bitcoin mining in this regard; any other form of heavy computing (like video gaming and grid computing) will also generate huge amounts of bits. It is not possible at the moment to store $\sim 10^{31}$ bits, and Sagan believed that no civilization has yet reached level Z. In 2012, Baker [120] claimed one gram of DNA could store 455 exabytes ($4.55 \cdot 10^{20}$ bytes) or $3.64 \cdot 10^{21}$ bits of data.

V. "A MIX OF BOTH" TECHNOLOGIES

In this section we review the following technologies: Satcoin, Decentralized Storage Solutions, MultiAlgo, and Blockchain Games.

A. SATCOIN

Boolean Satisfiability (SAT) problem is a problem of finding an assignment of Boolean variables to Boolean formula so that it evaluates to true. SAT problem was proven to be NP-complete. There are many SAT solvers implementing algorithms with exponential complexity that have been used for analyzing cryptographic functions [121]–[124], scheduling, electronic design automation, and for many other things. Manthey *et al.* [22] state that the Bitcoin mining algorithm is based on brute force. They also describe how the mining process could use SAT solving instead. The process of SAT solving for bitcoin mining was already described by Heusser [21] in 2013, where he reformulates hash finding as an SAT with 250,000 variables. The proposed SAT solving method is not based on the brute force search method; instead, it uses algorithms for SAT solving based on back-tracking. The claimed results are significant performance improvement and that the proposed algorithm gets potentially more efficient with increasing difficulty of Bitcoin. However, Heusser does not claim that the proposed SAT solving method would be faster than the brute force method using currently available SAT solvers; it may become more efficient.

B. DECENTRALIZED STORAGE SOLUTIONS

Decentralized Storage Solution (DSS) is a bunch of methods to decentralize cloud storage solutions. Solutions such as Filecoin, Sia, StorJ, MaidSafe, Chia, and Permacoin. For example, Permacoin stores some public data like essential books, and Filecoin can store private data like photos and videos coming from regular users.

1) PROOF-OF-SPACE & PROOF-OF-TIME

Chia (XCH) is enterprise-grade digital money using blockchain technologies. The consensus method of Chia is Proof of Space and Time, which means that Chia farming (similar to Bitcoin mining) uses disk space as the resource for securing its blockchain [125]–[128]. Proof-of-Space means users (or "farmers") allocate unused Hard Disk Drive (HDD) or Solid State Drive (SSD) space for storage by storing cryptographic numbers on disk into large files called "plots". Farmers will scan their plots after a new block is broadcast on the Chia's network. They will check if there is a number close to the new challenge number coming from Proof-of-Time. The second consensus method, Proof-of-Time, is needed to ensure that an actual wall clock time has passed between blocks.

Chia's method is not using vast amounts of electricity for consensus, but there is still the e-waste problem [129] of broken Flash drives on some setups of the Chia environment. For example, Chia farmers have noticed that 256 GB SSD might last only 40 drive-write days, 512 GB SSD might last only 80 drive-write days, and 1 TB SSD might last only 160 drive-write days [130].

Fisch [131] construct a practical Proof-of-Space (also known as "PoS", not to be confused with Proof-of-Stake or Proof-of-Search), which can be used to demonstrate that a prover is using space to store information. His article states that Proof-of-Space is an alternative to PoW for applications like spam prevention, Denial-of-Service (DoS) attacks, and Sybil resistance in blockchain network consensus methods. Proof-of-Space is egalitarian and eco-friendly because it is ASIC-resistant and uses (and reuses) mass storage space instead of energy, which cannot be reused easily.

2) PROOF-OF-RETRIEVABILITY

Miller *et al.* [132] show that Bitcoin's resources could be repurposed for valuable tasks. Permacoin is a cryptocurrency that uses Proof-of-Retrievability (POR) for archiving and accessing some public data like books. Permacoin requires both computational and storage resources. Bitcoin's mining mechanism is called a Scratch-Off Puzzle (SOP), which involves continuous attempts to solve puzzles. They use the POR consensus as an SOP to start a competition among miners to access random local copies of files as a Decentralized Storage Solution (DSS), and then they use a model of rational economic agents and claim that their SOP has the essential properties of the Bitcoin PoW mechanism.

3) FILECOIN

Filecoin is an open-source cloud storage marketplace, protocol, and incentive layer. The project developers have published a paper on Proof-of-Replication (PoRep) [133] and released a paper on Power Fault Tolerance (PFT) [134]. The paper on PoRep claims that PoRep is a new kind of Proof-of-Storage, which can be used to prove that some data has been replicated in physical storage. The system enforces unique physical copies so that the verifier can check that the prover is not gaming the system by deduplicating the same data into the same storage space. The paper on PFT gives a formal definition for PFT, which reframes Byzantine Fault Tolerance (BFT) in terms of users' influence over the

protocol's outcome instead of the number of nodes. Filecoin's native cryptocurrency is filecoin (FIL).

4) SIA

According to Sia's documentation [135], Sia is a platform for decentralized storage. Users can make publicly auditable storage contracts in the blockchain defining what data will be stored and what price. Sia blockchain's native currency is siacoin (SC). There were plans for Sia to become a sidechain as a two-way peg to the Bitcoin blockchain in the future.

5) StorJ

StorJ is a Decentralized Cloud Storage (DCS) that encrypts files and splits them into 80 pieces each. According to the StorJ website [136], retrieving a file only needs 29 of those pieces. StorJ's native cryptocurrency is STORJ.

6) THE SAFE NETWORK BY MaidSafe

The Safe Network is replacing the vulnerable structures of the Web with more decentralized methods [137]. Proof-of-Resource in the Safe Network is a method, similar to a Zero Knowledge Proof, that measures a node's ability to store and retrieve data chunks [138]. The cryptocurrencies associcated with Safe Network are MaidSafeCoin (MAID) and (eMAID) and Safe Network Token [139].

C. MultiAlgo

The MultiAlgo solution is a bit similar to the Hybrid PoW & ''PoX'' solution because they both use multiple different methods to achieve consensus. The difference is that the MultiAlgo is about a PoW mechanism with multiple different (but otherwise quite similar) hashing functions used to form consensus, and the Hybrid PoW & ''PoX'' solution uses PoW and some other form of consensus methods (''PoX''), which can be very different from each other. ''PoX'' can be almost any consensus method, but usually it is PoS.

Many cryptocurrencies are using the MultiAlgo solution. It means securing the blockchain with several different hashing algorithms [140]. One motivation to use multiple algorithms is to make the cryptocurrency more resistant to a single hash function getting cracked [141]. The second motivation is to make the cryptocurrency more resistant to ASIC mining.

X11 [142] is a MultiAlgo solution with 11 different hash functions: Blake, BMW, Groestl, JH, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, and Echo. There are several cryptocurrencies using X11, one of them is Dash (formerly: Darkcoin, XCoin). There are now ASICs for X11, one of them is Spondoolies SPx36 [143], and more advanced MultiAlgo solutions are now available, such as X12, X13, X14, X15, X16, and X17.

1) DigiByte

DigiByte (DGB) uses five different hashing algorithms: SHA256, Scrypt, Odocrypt, Skein, and Qubit. Odocrypt is said to be ASIC resistant by rewriting and morphing itself every ten days, and it is focused on utilizing FPGA mining [144].

2) QUARKCOIN

Quarkcoin (QRK) [141] uses six different hashing algorithms: BLAKE, Blue Midnight Wish, Groestl, JH, Skein, and Keccak. There are nine rounds of hashing from these six different algorithms. The archived website of Quarkcoin [145] claims that Quarkcoin has 0.5% inflation to keep mining activity going and the Quarkcoin blockchain safe against 51% attacks. They also claim Quarkcoin to be ASIC resistant and CPU mining only.

D. BLOCKCHAIN GAMES

Yuen *et al.* [146] propose a Proof-of-Play (PoP) consensus model for peer-to-peer games. The aim is to create a system that forms a consensus by using the blockchain itself. They compare their model to the conceptual Proof-of-Excellence, but the player does not need to be excellent - the act of playing should be enough for mining.

The idea of Proof-of-Play or Proof-of-Thought might initially come from a blockchain-based videogame called Motocoin.

1) MOTOCOIN

Motocoin [147] was probably the first to use the Proof-of-Thought (or Proof-of-Play) consensus method. The human cognitive workload can be used for mining the motocoins (MOTO) with the method. The name Motocoin comes from the 2D motorbike simulation game, which the player needs to play to form the consensus. When the level is finished, there will be a verifiable chain of commands, proof that a solution has been found. The proof is then attached to blocks [148].

According to Kraft [148], Motocoin's ''PoW''(probably meaning Proof-of-Thought or Proof-of-Play)[2] itself is formulated in terms of a game. The method is compared to the Sudoku puzzle-solving analogy when explaining Bitcoin mining to the general public. Kraft also states that, unlike Huntercoin, Motocoin's blockchain is not associated with a global game state.

According to the homepage of Motocoin [149], the game was dominated by bots, but the developers were also able to introduce a new security model.

2) HunterCoin

HunterCoin is a cryptocurrency blockchain and a multi-player videogame where the player collects coins on a map. As was the case with Motocoin, bots are playing the game. The process of a human player collecting coins inside a game world is called Human mining (or AI mining, if the player is a bot), and the status of the competition, which is getting more difficult over time, is called Human (or AI) Difficulty level [150]. Ujunwa's article on blockchain gaming [151]

[2]Note by the corresponding author of this survey.

uses the term Proof-of-Mining for the method of collecting coins by a human player. HunterCoin is an example of many novel technologies like a) human mining or manual mining, b) MultiAlgo (SHA256d and Scrypt), and c) merge-mining.

Kraft [148] reviews HunterCoin's principles and proposes a protocol that enables trustless off-chain interactions of players. The paper mentions that every node on the Huntercoin network can verify that the gameplay follows the rules.

The huntercoin cryptocurrency (HUC) is mined using PoW, and it can be merge-mined at least with bitcoin, and litecoin (LTC), because the hashing algorithms are SHA256d and Scrypt. The block reward is 10 HUC. Human mining means that a part (9 HUC) of a block reward goes inside the game world, where hunters can collect and bank them to their cryptocurrency address; the other part (1 HUC) of the block reward goes to the PoW miners. There can also be fights over resources in this two-dimensional world so that the hunter might lose all the coins [150].

VI. RESEARCH QUESTION

We form our Research Questions based on the analysis above. The Research Question is: What technological solutions do we have to make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified?

VII. DISCUSSION

This section discusses all the previously mentioned technologies, our categories, and whether using this technology in Bitcoin is plausible. Not being plausible does not mean it will be impossible to use the technology in Bitcoin, but we see it is impractical for Bitcoin. Not being plausible also does not mean being inferior. Bitcoin was originally meant to be a Decentralized Payment System, making it difficult to use technologies like SolarCoin's centralized incentive system or Motocoin's Proof-of-Play (good for a gaming environment) in Bitcoin. We also discuss if some Distributed Computing Grid coins can compete with bitcoin or ether. Table 4 shows our discussion's main outcome.

TABLE 4. Plausibility of green and justification technologies for bitcoin.

Technology	Category	Plausible for Bitcoin?
Proof-of-Stake	Green	Yes
The Lightning Network	Green	Yes
Optical Computing	Green	Yes
Reversible Computing	Green	No and Yes
Ternary Computing	Green	Yes
SolarCoin	Green	No
Proof-of-Elapsed-Time	Green	No and Yes
Renewable and Nuclear Energy	Green	Yes
Application-Specific Integrated Circuits	Green	Yes
Proof-of-Deep-Learning	Justification	Yes
Proof-of-Evolution	Justification	Yes
Prime Chain Proof-of-Work	Justification	Yes
Distributed Computing Grids	Justification	Yes and No
Merge-mining	Justification	Yes
Many-money Economy	Justification	Yes
Hash Recycling	Justification	Yes
Satcoin	Both	Yes
Decentralized Storage Solutions	Both	Yes and No
MultiAlgo	Both	Yes
Blockchain Games	Both	No

A. GREEN TECHNOLOGIES

Green technologies are discussed in this part of the paper.

1) PROOF-OF-STAKE

We categorize Proof-of-Stake as Green because this consensus method will reduce the energy consumption of Ethereum by 99% [61]. We think this method is plausible for Bitcoin because PoS is already being tested on Ethereum, and although ether is not designed to be a cryptocurrency for a DPS like bitcoin, it has the second-largest market capitalization as seen in Figure 4.

2) THE LIGHTNING NETWORK

There are at least two reasons why the Lightning Network (LN) is Green. First, the LN increases the number of bitcoin transactions from several transactions per second to at least thousands of transactions per second without increasing the energy consumption of bitcoin mining. Second, the LN will also save storage space and Internet bandwidth by recording off-chain the transactions happening between the opening and closing transactions of the micropayments channel. LN is also plausible for Bitcoin because it is already used in Bitcoin.

3) OPTICAL COMPUTING

According to our judgment, Optical Computing is Green because OPoW introduces optical computing methods for cryptocurrency mining. OPoW is plausible for Bitcoin because it is tailor-made for Bitcoin. Optical computing is a possibility for making Bitcoin greener.

4) REVERSIBLE COMPUTING

Reversible Computing should be categorized as Green because it has the potential to be from 1,000 to 100,000 times as cost-effective as irreversible computing in the 2050s. It is plausible for Bitcoin if a reversible computing architecture is developed first. At the moment of writing this, there is no such architecture.

5) TERNARY COMPUTING

Ternary Computing should also be categorized as Green because the theory states that the ternary system has the highest density of information representation. It should not be impossible to make bitcoin mining ASIC chips based on the ternary system. Therefore, we categorize it as plausible for Bitcoin.

6) SolarCoin

SolarCoin is categorized as Green because it incentivizes solar power for blockchain applications. We think it is not directly applicable to Bitcoin because SolarCoin is a very centralized model, and Bitcoin is meant to be very decentralized.

7) PROOF-OF-ELAPSED-TIME

PoET is a Green technology because it replaces the computing power competition of PoWs with a random time length of napping. PoET is designed for permissioned blockchains, and it is not directly applicable to Bitcoin. Still, maybe it is not difficult to make a version of PoET that is workable for permissionless blockchains like Bitcoin and Ethereum.

8) RENEWABLE AND NUCLEAR ENERGY

Renewables (solar power, wind power, and hydropower) and nuclear energy are Green and very much plausible for Bitcoin to use even when writing this article. As was mentioned earlier, Bitcoin mining might be cleaner than generally assumed. Bitcoin mining might also make OTEC profitable.

9) APPLICATION-SPECIFIC INTEGRATED CIRCUITS

ASICs are Green because they are faster (more energy-efficient) at bitcoin mining than CPUs, GPUs, and FPGAs. There are probably still some innovations coming for ASICs to make them even more energy-efficient for bitcoin mining. ASICs are plausible for Bitcoin because they have been used in bitcoin mining since 2013.

B. JUSTIFICATION TECHNOLOGIES

Justification technologies are discussed in this part of the paper.

1) PROOF-OF-DEEP-LEARNING

Deep Learning is known for consuming lots of energy for training the models. Typically, models are trained on GPUs. Research article [7] proposes the PoDL method, which consists of replacing current PoW with the procedure of training deep learning models and submitting trained models that will be evaluated on an independent dataset. Then, the miner who submitted the model with the highest performance (such as accuracy) will validate a block and gain the reward. Bitcoin is one of the cryptocurrencies that could use the method. Therefore, we list PoDL as a plausible technology for Bitcoin. We only categorize PoDL as a Justification Technology.

2) PROOF-OF-EVOLUTION

We think PoE is a Justification technology because it adds additional value (executes genetic algorithms) to the mining process. According to the research [97], PoE is closely related to Bitcoin's PoW, so we categorize PoE as plausible for Bitcoin.

3) PRIME CHAIN PROOF-OF-WORK

Prime Chain PoW should be categorized as a Justification technology because it gives some scientific value (finds new prime numbers) to the mining process. It is difficult to say if Prime Chain PoW would work for Bitcoin as well as it has worked for Primecoin, but maybe the MultiAlgo method could be used in Bitcoin and have at least some of the Bitcoin blocks mined by the Prime Chain PoW consensus.

4) DISTRIBUTED COMPUTING GRIDS

We downloaded historical market capitalization data in US Dollars for bitcoin (BTC), ether (ETH), gridcoin (GRC), curecoin (CURE), and foldingcoin (FLDC) from CoinGecko (https://coingecko.com) for date ranges from 2013-JAN-01 to 2022-MAY-18. The lin-log plot of the market capitalization data is in Figure 4. From the data, gridcoin, curecoin, and foldingcoin are older cryptocurrencies than ether, and their market capitalizations are still considerably lower than ether's market capitalization. Foldingcoin's market capitalization did not get any updates after October 2018 in CoinGecko. The highest market capitalization for gridcoin was about 83.6 million US dollars on 9 January 2018. Bitcoin's highest market capitalization is more than 10 thousand times that. We conclude that Distributed Computing Grid coins cannot compete yet with bitcoin and ether.

The technology of Distributed Computing Grids is more about Justification than Green technology. Could Bitcoin's PoW be replaced by the methods used in Gridcoin, Curecoin, or Foldingcoin? Probably it could not be replaced by them directly because Bitcoin is all about decentralization, and having a centralized source of analyzable data (for example, protein folding data) makes the system very centralized, giving an advantage [8] for those organizations that control the analyzable data. We still believe that there could be some ways to introduce useful Distributed Computing Grids in bitcoin mining. On blockchains that use an advanced form of smart contracts, like the Ethereum blockchain, one could use customizable PoWs for tokens. Maybe the Bitcoin blockchain will also use more advanced smart contracts directly in the future; nowadays, they can be run on the Rootstock (RSK) sidechain [152]. However, another possibility we can think of is a form of Hybrid Proof-of-Work & "Proof-of-X" method, where only some of the blocks are ASIC-mined SHA256d PoW blocks and some of the blocks are CPU & GPU mined Distributed Computing Grid "Proof-of-X" blocks that will use the spare computing cycles for scientific computing. Therefore, we have categorized Distributed Computing Grids as Justification Technology that could be and could not be plausible for Bitcoin.

5) MERGE-MINING

Merge-mining is a Justification Technology because it gives new value to cryptocurrency mining: instead of securing only one blockchain, merge-mining makes it possible to secure two or more blockchains without extra mining efforts. The miner will get not only one but two (or more) cryptocurrencies as a reward for the merge-mining. Merge-mining could also be labeled as Green technology because, in a way, it might lower the total energy consumption used for cryptocurrency mining. However, it is uncertain if cryptocurrencies with low market capitalizations are attractive enough for large-scale mining without the merge-mining technology.

Bitcoin has been merge-mined for years with several other SHA256d PoW cryptocurrencies. Therefore, merge-mining for Bitcoin is plausible. However, there are some security

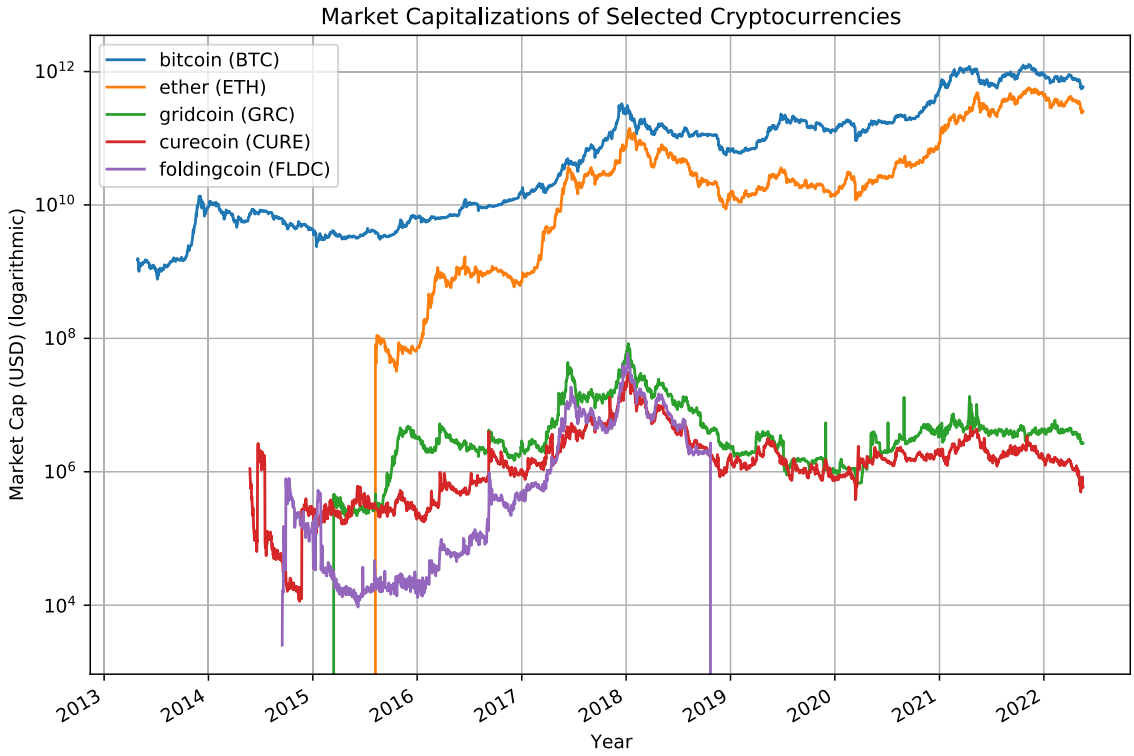

FIGURE 4. Market capitalizations for bitcoin (BTC), ether (ETH), gridcoin (GRC), curecoin (CURE), and foldingcoin (FLDC) in US Dollars (USD).

issues with merge-mining regarding cryptocurrencies with less mining power available than Bitcoin.

6) MANY-MONEY ECONOMY

Introducing new coin types for the Bitcoin blockchain would not reduce energy consumption, but it would make the Bitcoin cryptoeconomy more valuable if the new coin is better as a daily payment method than the regular bitcoin coin (BTC). It would be even better if the miners (using old, non-profitable, ASIC mining hardware) were given the second type of bitcoin coin as a block reward. This method should solve, at least partially, the problem of e-waste. Therefore, we judge this technology as a Justification technology, and we believe it could work for Bitcoin as a hard fork.

7) HASH RECYCLING

Hash Recycling does not reduce the energy usage of bitcoin mining, but it gives new value to the hashes that would be otherwise wasted and erased. We categorize it as a Justification Technology. We believe this technology could be implemented in Bitcoin today.

C. "A MIX OF BOTH" TECHNOLOGIES

"A Mix of Both" technologies are discussed in this part of the paper.

1) SATCOIN

We think Satcoin is both Green and Justification technology because SAT solvers have the potential to reduce energy utilization due to more efficient algorithms, and SAT is useful itself, and they can solve practical SAT instances. We also think this could be used in Bitcoin.

2) DECENTRALIZED STORAGE SOLUTIONS

We think Decentralized Storage Solutions could be both Green and Justification technologies. There are many different Decentralized Storage Solutions like Chia, Permacoin, Filecoin, and many others.

For example, Chia could be labeled as a Green Technology because it does not use lots of computing power, but, on the other hand, Chia is known for the Flash drive e-waste problem.

Permacoin is a Justification technology because important data like open-source scientific research articles and old books could be stored in a decentralized manner. What if Bitcoin used this method to store Wikipedia articles or the research articles of Ledger Journal, or the free books of the Project Gutenberg? Storing important public data would make Bitcoin more valuable and justified even for those who do not use the bitcoin cryptocurrency itself. We believe solutions like Permacoin could be plausible for Bitcoin.

3) MultiAlgo

MultiAlgo could potentially mean some changes in energy usage if Bitcoin started using it. For example, if Bitcoin had an ASIC-resistant PoW, it would mean that more people could have access to bitcoin mining by using hardware like CPUs and GPUs. There would also not be such a considerable e-waste problem because CPUs, GPUs, and FPGAs can easily

be repurposed for general computing if mining cryptocurrencies is neither profitable nor exciting anymore. We have categorized MultiAlgo as both Green and Justification technologies, and we believe it could be plausible for Bitcoin as a hard fork.

4) BLOCKCHAIN GAMES

Proof-of-Thought (or Proof-of-Play) is an exciting consensus method for blockchain videogames. HunterCoin has the concept of Human mining, which means that a human player can collect coins inside the game world. We categorize these technologies as Green technologies because there is a potential for less electricity usage if human cognitive power is used. We categorize them also as Justification technologies because they have the potential to revolutionize video gaming and science. What if a protein folding game like Foldit (https://fold.it) or neuron resolving and tracing game like Mozak (https://www.mozak.science/) started using these technologies? They could attract more human cognitive power to scientifically valuable games. We believe they are not plausible for Bitcoin, at least not directly, because a change to become a sort of a gaming platform would be too radical a change for a DPS like Bitcoin.

VIII. CONCLUSION

Our Research Question was: What technological solutions do we have to make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified? We answer that there are many solutions already in place: Hybrid Proof-of-Stake and Proof-of-Work have been used since 2012 in Peercoin and various other cryptocurrencies since then; SolarCoin started in 2014; Proof-of-Elapsed-Time has been used in some permissioned blockchains; sustainable energy has been used more for cryptocurrency mining than it has been used in the default US energy mix according to estimates based on a survey of miners; Bitcoin ASICs have been used since 2013; Primecoin started in 2013; distributed computing grid coins (gridcoin, curecoin, foldingcoin) were introduced around the mid-2010s; merge-mining has been possible since the early 2010s; there are many attractive Decentralized Storage Solutions (like Chia); digibyte and quarkcoin are classical examples of cryptocurrencies using the MultiAlgo method, and there have been at least two video gaming blockchains (Motocoin and HunterCoin) to use human cognitive power for cryptocurrency mining. There are now plans to use unconventional computing methods (reversible computing, ternary computing, optical computing, analog computing) to solve some of the issues regarding the vast energy consumption of conventional computing (including cryptocurrency mining).

We think using spare computing cycles for grid computing efforts is justified. For example, there are billions of smartphones in the world. Many smartphones are being recharged every day. If this daily recharging period of twenty to sixty minutes would be used for grid computing, for example, finding new cures to cancer, it would probably be a significant breakthrough for medical research simulations. We call on the cryptocurrency communities to research and develop grid computing and unconventional computing methods for the most significant cryptocurrencies: bitcoin (BTC) and ether (ETH).

Further research could include writing a new part for this survey with more technologies analyzed. It would also be interesting to analyze issues and find solutions regarding the vast energy consumption of video gaming, including PCs, consoles, tablets, smartphones, and cloud gaming. There should also be research on how much should a regular chip (in a PC or a smartphone) have to perform distributed computing during its lifetime in order to pay back "the manufacturing debt".

REFERENCES

[1] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.

[2] H. Müller and M. Seifert, "Blockchain, a feasible technology for land administration," in *Proc. FIG Work. Week, Geospatial Inf. Smarter Life Environ. Resilience*, 2019, pp. 22–26.

[3] *Bitcoin Could Become World Reserve Currency, Says Senator Rand Paul | NASDAQ*. Accessed: Jun. 3, 2022. [Online]. Available: https://web.archive.org/web/20211221170532/https://www.nasdaq.com/articles/bitcoin-could-become-world-reserve-currency-says-senator-rand-paul-2021-10-25

[4] *How Blockchain-Based Apps and Sites Resist DDoS Attacks | VentureBeat*. Accessed: Jun. 3, 2022. [Online]. Available: https://web.archive.org/web/20220420032420/https://venturebeat.com/2017/06/25/how-blockchain-based-apps-and-sites-resist-ddos-attacks/

[5] K. Raworth, *Doughnut Economics: Seven Ways to Think Like a 21st Century Economist*. New York, NY, USA: Penguin Random House, 2018.

[6] M. Dubrovsky, M. Ball, L. Kiffer, and B. Penkovsky, "Towards optical proof of work," *Cryptoecon. Syst.*, vol. 11, 2020. [Online]. Available: https://assets.pubpub.org/xi9h9rps/01581688887859.pdf

[7] C. Chenli, B. Li, Y. Shi, and T. Jung, "Energy-recycling blockchain with proof-of-deep-learning," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 19–23.

[8] 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 *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 104–121.

[9] *Crypto Letter to EPA*. Accessed: May 8, 2022. [Online]. Available: https://web.archive.org/web/20220508191606/https://www.ewg.org/sites/default/files/2022-04/Crypto%20letter%20to%20EPA.pdf

[10] *Bitcoin Letter to the Environmental Protection Agency*. Accessed: May 8, 2022. [Online]. Available: https://web.archive.org/web/20220504230929/https://bitcoinminingcouncil.com/wp-content/uploads/2022/05/Bitcoin_Letter_to_the_Environmental_Protection_Agency.pdf

[11] A. de Vries and C. Stoll, "Bitcoin's growing e-waste problem," *Resour., Conservation Recycling*, vol. 175, Dec. 2021, Art. no. 105901.

[12] A. de Vries, U. Gallersdörfer, L. Klaaßen, and C. Stoll, "Revisiting Bitcoin's carbon footprint," *Joule*, vol. 6, no. 3, pp. 498–502, 2022.

[13] *U.S. Energy Facts Explained—Consumption and Production—U.S. Energy Information Administration (EIA)*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220530223952/https://www.eia.gov/energyexplained/us-energy-facts/

[14] A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, "Towards a green blockchain: A review of consensus mechanisms and their energy consumption," in *Proc. 17th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, Jul. 2021, pp. 503–511.

[15] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[16] N. S. Kardashev, "Transmission of information by extraterrestrial civilizations," *Sov. Astron.*, vol. 8, p. 217, Oct. 1964.
[17] F. Z. D. N. Costa and R. J. G. B. de Queiroz, "A blockchain using proof-of-download," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 170–177.
[18] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPCON)*, Apr. 2019, pp. 119–124.
[19] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun.; IEEE 15th Int. Conf. Smart City; IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 466–473.
[20] *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Nov. 4, 2021. [Online]. Available: https://web.archive.org/web/20211103223918/https://bitcoin.org/bitcoin.pdf
[21] J. Heusser. (2013). *Sat Solving—An Alternative to Brute Force Bitcoin Mining*. [Online]. Available: https://web.archive.org/web/20220111172035/https://jheusser.github.io/2013/02/03/satcoin.html
[22] N. Manthey and J. Heusser, "SATcoin—Bitcoin mining via SAT," in *Proc. SAT COMPETITION*, 2018, p. 67.
[23] *Bitcoin Mining on Track to Consume All of the World's Energy by 2020 | Newsweek*. Accessed: Apr. 27, 2022. [Online]. Available: https://web.archive.org/web/20220416205334/https://www.newsweek.com/bitcoin-mining-track-consume-worlds-energy-2020-744036
[24] C. Mora, R. L. Rollins, K. Taladay, M. B. Kantar, M. K. Chock, M. Shimada, and E. C. Franklin, "Bitcoin emissions alone could push global warming above 2 °C," *Nature Climate Change*, vol. 8, no. 11, pp. 931–933, 2018.
[25] N. Houy, "Rational mining limits Bitcoin emissions," *Nature Climate Change*, vol. 9, no. 9, p. 655, 2019.
[26] E. Masanet, A. Shehabi, N. Lei, H. Vranken, J. Koomey, and J. Malmodin, "Implausible projections overestimate near-term Bitcoin CO_2 emissions," *Nature Climate Change*, vol. 9, no. 9, pp. 653–654, Sep. 2019.
[27] L. Dittmar and A. Praktiknjo, "Could Bitcoin emissions push global warming above 2 °C?" *Nature Climate Change*, vol. 9, no. 9, pp. 656–657, Sep. 2019.
[28] A. de Vries, "Bitcoin's growing energy problem," *Joule*, vol. 2, no. 5, pp. 801–805, May 2018.
[29] Wikipedia Contributors. (2022). *Kardashev Scale—Wikipedia, the Free Encyclopedia*. Accessed: May 16, 2022. [Online]. Available: https://web.archive.org/web/20220516222019/https://en.wikipedia.org/w/index.php?title=Kardashev_scale&oldid=1087802566#Current_status_of_human_civilization
[30] *Bitcoin Energy Per Transaction Metric is Misleading—Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220429052319/https://bitcoinmagazine.com/business/bitcoin-energy-per-transaction-metric-is-misleading
[31] *Cambridge Bitcoin Electricity Consumption Index (CBECI)*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20210504080905/https://cbeci.org/faq/
[32] *Bitcoin Average Energy Consumption Per Transaction Compared to That of Visa as of April 25, 2022 (in Kilowatt-Hours) | Statista*. Accessed: Apr. 28, 2022. [Online]. Available: https://web.archive.org/web/20220428200955/https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/
[33] *Ethereum Average Energy Consumption Per Transaction Compared to That of Visa as of January 10, 2022 (in Kilowatt-Hours) | Statista*. Accessed: Apr. 28, 2022. [Online]. Available: https://web.archive.org/web/20220428201539/https://www.statista.com/statistics/1265891/ethereum-energy-consumption-transaction-comparison-visa/
[34] *Facebook Electricity Usage Globally 2019 | Statista*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20210818230043/https://www.statista.com/statistics/580087/energy-use-of-facebook/
[35] *Alphabet (Google): Energy Consumption 2019 | Statista*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20211029095928/https://www.statista.com/statistics/788540/energy-consumption-of-google/
[36] C. Stoll, L. Klaaßen, and U. Gallersdörfer, "The carbon footprint of bitcoin," *Joule*, vol. 3, no. 7, pp. 1647–1661, 2019.
[37] *The Soviet Weapons Program—The Tsar Bomba*. Accessed: May 23, 2022. [Online]. Available: https://web.archive.org/web/20220523140227/http://www.nuclearweaponarchive.org/Russia/TsarBomba.html
[38] Wikipedia Contributors. (2022). *Tsar Bomba—Wikipedia, the Free Encyclopedia*. Accessed: May 23, 2022. [Online]. Available: https://web.archive.org/web/20220523155143/https://en.wikipedia.org/w/index.php?title=Tsar_Bomba&oldid=1085809420
[39] N. Mills and E. Mills, "Taming the energy use of gaming computers," *Energy Efficiency*, vol. 9, no. 2, pp. 321–338, Apr. 2016.
[40] *Statistics Finland—Energy Supply and Consumption*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20210414035155/https://www.stat.fi/til/ehk/2019/ehk_2019_2020-12-21_tie_001_en.html
[41] *Ethereum Energy Consumption Index—Digiconomist*. Accessed: Apr. 21, 2022. [Online]. Available: https://web.archive.org/web/20220421133343/https://digiconomist.net/ethereum-energy-consumption
[42] *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20211108150128/https://docsend.com/view/adwmdeeyfvqwecj2
[43] *Final Consumption of Energy—Motiva*. Accessed: Oct. 26, 2021. [Online]. Available: https://web.archive.org/web/20211026171442/https://www.motiva.fi/en/solutions/energy_use_in_finland/final_consumption_of_energy
[44] M. G. Millis, "Energy, incessant obsolescence, and the first interstellar missions," 2011, *arXiv:1101.1066*.
[45] *Interstellar Travel Not Possible Before 2200ad, Suggests Study | MIT Technology Review*. Accessed: May 22, 2022. [Online]. Available: https://web.archive.org/web/20220522162743/https://www.technologyreview.com/2011/01/07/197702/interstellar-travel-not-possible-before-2200ad-suggests-study/
[46] *Statistical Review of World Energy—2021 | 70th Edition*. Accessed: May 23, 2022. [Online]. Available: https://web.archive.org/web/20220523121939/https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2021-full-report.pdf
[47] *Bitcoin's Energy Usage isn't a Problem. Here's Why*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20211103232331/https://www.lynalden.com/bitcoin-energy/
[48] *Carbon Dioxide Emissions—Motiva*. Accessed: Oct. 26, 2021. [Online]. Available: https://web.archive.org/web/20201030003703/https://www.motiva.fi/en/solutions/energy_use_in_finland/carbon_dioxide_emissions
[49] *9,000 Transactions Per Second: Bitcoin SV Hits New Record*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20211218070345/https://www.prnewswire.com/news-releases/9-000-transactions-per-second-bitcoin-sv-hits-new-record-301217145.html
[50] *Why Some Bitcoin Devs Say Lasers Can Cut Mining's Energy Costs*. Accessed: Apr. 25, 2022. [Online]. Available: https://web.archive.org/web/20220412181134/https://www.coindesk.com/layer2/miningweek/2022/03/22/why-some-bitcoin-devs-say-lasers-can-cut-minings-energy-costs/
[51] *Returned 'Proof-of-Work' Ban in EU Crypto Markets Bill Fails in Committee | the Block*. Accessed: Apr. 25, 2022. [Online]. Available: https://web.archive.org/web/20220315224829/https://www.theblockcrypto.com/linked/137690/returned-proof-of-work-ban-in-eu-crypto-markets-bill-fails-in-committee
[52] A. Y. Hoekstra and A. K. Chapagain, "Water footprints of nations: Water use by people as a function of their consumption pattern," in *Integrated Assessment of Water Resources and Global Change*. Dordrecht, The Netherlands: Springer, 2006, pp. 35–48. [Online]. Available: https://waterfootprint.org/media/downloads/Hoekstra_and_Chapagain_2007.pdf and https://link.springer.com/chapter/10.1007/978-1-4020-5591-1_3, doi: 10.1007/978-1-4020-5591-1_3.
[53] *Volunteer Computing—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220603163710/https://en.wikipedia.org/wiki/Volunteer_computing
[54] *Folding@home—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220603161605/https://en.wikipedia.org/wiki/Folding@home
[55] E. D. Williams, "Environmental impacts of microchip manufacture," *Thin Solid Films*, vol. 461, no. 1, pp. 2–6, Aug. 2004.

[56] V. Buterin. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: May 30, 2022. [Online]. Available: https://web.archive.org/web/20220529222621/https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf
[57] M. B. Taylor, "Bitcoin and the age of bespoke silicon," in *Proc. Int. Conf. Compil., Archit. Synth. Embedded Syst. (CASES)*, Sep. 2013, pp. 1–10.
[58] A. de Vries, "Renewable energy will not solve Bitcoin's sustainability problem," *Joule*, vol. 3, no. 4, pp. 893–898, Apr. 2019.
[59] *PPCoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake*. Accessed: Jun. 3, 2022. [Online]. Available: https://web.archive.org/web/20220603155906/https://www.peercoin.net/papers/peercoin-paper.pdf
[60] *Proof of Stake Versus Proof of Work—White Paper*. Accessed: Jun. 2, 2022. [Online]. Available: https://web.archive.org/web/20220423164140/https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf
[61] *Why Ethereum is Switching to Proof of Stake and How it Will Work | MIT Technology Review*. Accessed: Apr. 21, 2022. [Online]. Available: https://web.archive.org/web/20220421132111/https://12ft.io/proxy?ref=&q=https%3A%2F%2Fwww.technologyreview.com%2F2022%2F03%2F04%2F1046636%2Fethereum-blockchain-proof-of-stake%2F
[62] *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220530113520/https://lightning.network/lightning-network-paper.pdf
[63] A. A. Sawchuk and T. C. Strand, "Digital optical computing," *Proc. IEEE*, vol. 72, no. 7, pp. 758–779, Jul. 1984.
[64] *Bips/Bip-0052.Mediawiki at Master*. Accessed: Apr. 25, 2022. [Online]. Available: https://web.archive.org/web/20220412200428/https://github.com/bitcoin/bips/blob/master/bip-0052.mediawiki
[65] *A Radical Computer Learns to Think in Reverse—The New York Times*. Accessed: May 28, 2022. [Online]. Available: https://web.archive.org/web/20220525233044/https://www.nytimes.com/1999/06/15/science/a-radical-computer-learns-to-think-in-reverse.html
[66] *Reversible Computing: The Only Future for General Digital Computing*. Accessed: Oct. 1, 2021. [Online]. Available: https://web.archive.org/web/20210401031527/https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/LPS21-talk-v5.pdf
[67] M. P. Frank, *Nanocomputer Systems Engineering*. Boca Raton, FL, USA: CRC Press, 2006.
[68] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM J. Res. Develop.*, vol. 5, no. 3, pp. 183–191, Jul. 1961.
[69] T. G. Lewis, "Art Scott and Michael Frank on energy-efficient computing," *Ubiquity*, vol. 2017, pp. 1–17, Sep. 2017.
[70] H. Thapliyal and M. Zwolinski, "Reversible logic to cryptographic hardware: A new paradigm," in *Proc. 49th IEEE Int. Midwest Symp. Circuits Syst.*, vol. 1, Aug. 2006, pp. 342–346.
[71] H. T. Heinonen and A. Semenov, "Recycling hashes from reversible Bitcoin mining to seed pseudorandom number generators," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, Feb. 2022, pp. 103–117. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-96527-3_7, doi: 10.1007/978-3-030-96527-3_7.
[72] J. Connelly, C. Patel, A. Chavez, and P. Nico, "Ternary computing testbed: 3-trit computer architecture," Dept. Comput. Eng., California Polytech. State Univ., San Luis Obispo, CA, USA, 2008. [Online]. Available: http://xyzzy.freeshell.org/trinary/CPE%20Report%20-%20Ternary%20Computing%20Testbed%20-%20RC6a.pdf
[73] *Ternary Systems | IOTA Beginners Guide*. Accessed: May 13, 2022. [Online]. Available: https://web.archive.org/web/20220513200417/https://iota-beginners-guide.com/future-of-iota/iota-x-0-ternary-vision-abandoned/ternary-systems/
[74] A. Srivastava and K. Venkatapathy, "Design and implementation of a low power ternary full adder," *VLSI Des.*, vol. 4, no. 1, pp. 75–81, 1996.
[75] A. P. Dhande and V. T. Ingole, "Design and implementation of 2 bit ternary ALU slice," in *Proc. 3rd Int. Conf., Sci. Electron., Technol. Inf. Telecommun. (SETIT)*, Tunisia, North Africa, vol. 17, Mar. 2005. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/ 34671762/312-with-cover-page-v2.pdf?Expires=1657829511&Signature=ISnvixrH1~BUd9XfmciBZumncM8AYGKqWFX7tG~aENJ221fA7jcsg6npCq9aGXJhqlbNpuH~qa~Bm81-iM4v1XaNIy3SN0xjNiiD-Z8C387pifQdiSggF8y6DdR16i6RGMvjwX1-NDgB7oGCWfnmaIW-ZfD-i8wbSWmFz76FqNQkzHrUXT2R-50nqdZkoVFgT3ZensAANas4HCRjk9pcaxN0y6q0KSHEmTJW6TLlofcoT8FLQk0XJFq7k6ct4yisNm53bilM4WM2mAuxnmCIwe~YTryEO65iIJh4PqAP-d5MIyEq3Q0SVc2kvmiwDjTVADinUgq3tQyCLYPjgzoSwQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
[76] P. C. Balla and A. Antoniou, "Low power dissipation MOS ternary logic family," *IEEE J. Solid-State Circuits*, vol. SSC-19, no. 5, pp. 739–749, Oct. 1984.
[77] D. Porat, "Three-valued digital systems," *Proc. Inst. Electr. Eng.*, vol. 116, no. 6, pp. 947–954, 1969.
[78] K. C. Smith, "The prospects for multivalued logic: A technology and applications view," *IEEE Trans. Comput.*, vol. C-30, no. 9, pp. 619–634, Sep. 1981.
[79] PH. D. Chung-Yu Wu and H.-Y. Huang, "Design and application of pipelined dynamic CMOS ternary logic and simple ternary differential logic," *IEEE J. Solid-State Circuits*, vol. 28, no. 8, pp. 895–906, Aug. 1993.
[80] *Douglas W. Jones on Ternary Computing*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220121012304/http://homepage.divms.uiowa.edu/~jones/ternary/
[81] B. Cambou, P. Flikkema, J. Palmer, D. Telesca, and C. Philabaum, "Can ternary computing improve information assurance?" *Cryptography*, vol. 2, no. 1, p. 6, Mar. 2018.
[82] S. Caraiman and V. Manta, "Image representation and processing using ternary quantum computing," in *Proc. Int. Conf. Adapt. Natural Comput. Algorithms*. Berlin, Germany: Springer, 2013, pp. 366–375. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-37213-1_38, doi: 10.1007/978-3-642-37213-1_38.
[83] *IOTA Token | IOTA Beginners Guide*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220513200502/https://iota-beginners-guide.com/iota-token/
[84] L. Johnson, A. Isam, N. Gogerty, and J. Zitoli. (Dec. 11, 2015). *Connecting the Blockchain to the Sun to Save the Planet*. [Online]. Available: https://ssrn.com/abstract=2702639, doi: 10.2139/ssrn.2702639.
[85] *What's Proof of Elapsed Time. Proof of Elapsed Time is One More | by Henrique Centieiro | Nerd for Tech | Medium*. Accessed: May 31, 2022. [Online]. Available: https://web.archive.org/web/20220531150855/https://medium.com/nerd-for-tech/whats-proof-of-elapsed-time-4f67cf3f45b3
[86] *Floating the Sawtooth Raft: Implementing a Consensus Algorithm in Rust—Hyperledger Foundation*. Accessed: May 31, 2022. [Online]. Available: https://web.archive.org/web/20220531152518/https://www.hyperledger.org/blog/2019/01/11/floating-the-sawtooth-raft-implementing-a-consensus-algorithm-in-rust
[87] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.
[88] *Proof of Elapsed Time (PoET) Definition*. Accessed: May 31, 2022. [Online]. Available: https://web.archive.org/web/20220531151229/https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp
[89] D. Minniti, F. Capponi, A. Valcarce, and J. Gallardo, "A new search for Dyson spheres in the Milky Way," in *Life in the Universe*. Dordrecht, The Netherlands: Springer, 2004, pp. 173–176. [Online]. Available: https://link.springer.com/chapter/10.1007/978-94-007-1003-0_36, doi: 10.1007/978-94-007-1003-0_36.
[90] R. Pelc and R. M. Fujita, "Renewable energy from the ocean," *Mar. Policy*, vol. 26, no. 6, pp. 471–479, 2002.
[91] *Ocean Thermal Energy Conversion: An Extensive, Environmentally Benign Source of Energy for the Future*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20040805102014/http://www.sustdev.org/energy/articles/energy/edition3/SDI3-10.pdf
[92] *Bitcoin Unlocks Ocean Energy—Bitcoin Magazine*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220601050830/https://bitcoinmagazine.com/business/bitcoin-unlocks-ocean-energy
[93] *Compact Fusion | Lockheed Martin*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220526074314/https://www.lockheedmartin.com/en-us/products/compact-fusion.html
[94] T. Clynes, "5 big ideas for fusion power: Startups, universities, and major companies are vying to commercialize a nuclear fusion reactor," *IEEE Spectr.*, vol. 57, no. 2, pp. 30–37, Feb. 2020.
[95] *Antminer S19 Pro—The Future of Mining*. Accessed: Sep. 6, 2021. [Online]. Available: https://web.archive.org/web/20210906102302/https://shop.bitmain.com/release/AntminerS19Pro/overview
[96] A. L. Hicks, T. L. Theis, and M. L. Zellner, "Emergent effects of residential lighting choices: Prospects for energy savings," *J. Ind. Ecol.*, vol. 19, no. 2, pp. 285–295, Apr. 2015.
[97] F. Bizzaro, M. Conti, and M. S. Pini, "Proof of evolution: Leveraging blockchain mining for a cooperative execution of genetic algorithms," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 450–455.

[98] N. Shibata, "Proof-of-search: Combining blockchain consensus formation with solving optimization problems," *IEEE Access*, vol. 7, pp. 172994–173006, 2019.

[99] *Primecoin: Cryptocurrency With Prime Number Proof-of-Work*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220303094529/https://primecoin.io/primecoin-paper.pdf

[100] *Primecoin*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220424043230/https://primecoin.io/

[101] *Gridcoin Blue Paper Section 1: Expected Time to Stake and Net Weight*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220126074036/https://gridcoin.us/assets/docs/grc-bluepaper-section-1.pdf

[102] *Gridcoin White Paper: The Computation Power of a Blockchain Driving Science & Data Analysis Version 1.0.1*. Accessed: May 10, 2022. [Online]. Available: https://web.archive.org/web/20220130073115/https://gridcoin.us/assets/docs/whitepaper.pdf

[103] *White Paper—Curecoin*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503220122/https://curecoin.net/white-paper/

[104] *Folding Coin White Paper V4.0*. Accessed: May 3, 2022. [Online]. Available: https://web.archive.org/web/20210422115555/https://foldingcoin.net/images/Whitepapers/Folding%20Coin%20White%20Paper%20v4.0.pdf

[105] *Frequently Asked Questions | Counterparty*. Accessed: May 30, 2022. [Online]. Available: https://web.archive.org/web/20220525232939/https://counterparty.io/docs/faq/

[106] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. USENIX Annu. Tech. Conf. (USENIX ATC)*, 2016, pp. 181–194.

[107] *Merged Mining Specification—Bitcoin Wiki*. Accessed: May 9, 2022. [Online]. Available: https://web.archive.org/web/20171124212153/https://en.bitcoin.it/w/index.php?title=Merged_mining_specification&oldid=58250

[108] A. Judmayer, A. Zamyatin, N. Stifter, A. G. Voyiatzis, and E. Weippl, "Merged mining: Curse or cure?" in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham, Switzerland: Springer, Sep. 2017, pp. 316–333. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-67816-0_18, doi: 10.1007/978-3-319-67816-0_18.

[109] A. Zamyatin, "Merged mining: Analysis of effects and implications," Ph.D. thesis, Dept. Inform., Vienna Univ. Technol., Vienna, Austria, 2016. [Online]. Available: https://sec.cs.univie.ac.at/fileadmin/user_upload/i_sec/docs/teaching/thesis/azamyatin_merged_mining.pdf

[110] H. T. Heinonen, "On creation of a stablecoin based on the Morini's scheme of Inv&Sav wallets and antimoney," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 409–416.

[111] D. Stosic, D. Stosic, T. B. Ludermir, and T. Stosic, "Collective behavior of cryptocurrency price changes," *Phys. A, Stat. Mech. Appl.*, vol. 507, pp. 499–509, Oct. 2018.

[112] H. T. Heinonen, A. Semenov, and V. Boginski, "Collective behavior of price changes of ERC-20 tokens," in *Proc. Int. Conf. Comput. Data Social Netw.* Cham, Switzerland: Springer, Jan. 2021, pp. 487–498. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-66046-8_40, doi: 10.1007/978-3-030-66046-8_40.

[113] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM J. Comput.*, vol. 15, no. 2, pp. 364–383, 1986.

[114] J. Kelsey, B. Schneier, and N. Ferguson, "Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number generator," in *Proc. Int. Workshop Sel. Areas Cryptogr.* Berlin, Germany: Springer, Jul. 2001, pp. 13–33. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-46513-8_2, doi: 10.1007/3-540-46513-8_2.

[115] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*. Hoboken, NJ, USA: Wiley, 2011.

[116] *Quantum Random Number Generator | QuintessenceLabs*. Accessed: May 17, 2022. [Online]. Available: https://web.archive.org/web/20220516223748/https://www.quintessencelabs.com/products/qstream-quantum-true-random-number-generator/

[117] L. C. Noll, R. G. Mende, and S. Sisodiya, "Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system," U.S. Patent 5 732 138, Mar. 24, 1998.

[118] *Comparison of Hardware Random Number Generators—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20180812092012/https://en.wikipedia.org/wiki/Comparison_of_hardware_random_number_generators

[119] *Hardware Random Number Generator—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220607150642/https://en.wikipedia.org/w/index.php?title=Hardware_random_number_generator&oldid=1088716271

[120] M. Baker, "DNA data storage breaks records," Aug. 2012. [Online]. Available: https://www.nature.com/articles/nature.2012.11194.pdf?origin=ppub

[121] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT solvers to cryptographic problems," in *Proc. Int. Conf. Theory Appl. Satisfiability Test.* Berlin, Germany: Springer, 2009, pp. 244–257. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-02777-2_24, doi: 10.1007/978-3-642-02777-2_24.

[122] I. Mironov and L. Zhang, "Applications of SAT solvers to cryptanalysis of hash functions," in *Proc. Int. Conf. Theory Appl. Satisfiability Test.* Berlin, Germany: Springer, 2006, pp. 102–115. [Online]. Available: https://link.springer.com/chapter/10.1007/11814948_13, doi: 10.1007/11814948_13.

[123] F. Massacci, "Using Walk-SAT and Rel-SAT for cryptographic key search," in *Proc. IJCAI*, vol. 99, 1999, pp. 290–295.

[124] B. W. Bloom, "SAT solver attacks on CubeHash," Dept. Comput. Sci., Rochester Inst. Technol., Rochester, NY, USA, Tech. Rep., Apr. 2010. [Online]. Available: https://www2.cs.sfu.ca/~mitchell/cmpt-827/2011-Fall/Project-Readings/CubeHashAttackViaSAT.pdf

[125] *The Chia Network Blockchain*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220401140759/https://www.chia.net/assets/ChiaGreenPaper.pdf

[126] *Chia Business Whitepaper*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220502153433/https://www.chia.net/assets/Chia-Business-Whitepaper-2022-02-02-v2.0.pdf

[127] *FAQ—Chia Network*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502153406/https://www.chia.net/faq/

[128] *What is Chia (XCH)? How to Farm it With a Hard Drive—Decrypt*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502191327/https://decrypt.co/resources/what-is-chia-how-to-farm-with-a-hard-drive

[129] *'Green' Bitcoin Alternative Chia is Leading to Hard Disc Shortages | New Scientist*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502195513/https://www.newscientist.com/article/2277076-green-bitcoin-alternative-chia-is-leading-to-hard-disc-shortages/

[130] *Chia Farming Already Causing SSDs to Fail at Scale, Storage Device Shortages on the Horizon | TechPowerUp*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502185841/https://www.techpowerup.com/281979/chia-farming-already-causing-ssds-to-fail-at-scale-storage-device-shortages-on-the-horizon

[131] B. Fisch, "Tight proofs of space and replication," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, Apr. 2019, pp. 324–348. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-17656-3_12, doi: 10.1007/978-3-030-17656-3_12.

[132] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 475–490.

[133] J. Benet, D. Dalrymple, and N. Greco, "Proof of replication," *Protocol Labs*, vol. 27, p. 20, Jul. 2017.

[134] *Power Fault Tolerance—Technical Report (WIP) | Protocol Labs*. Accessed: May 29, 2022. [Online]. Available: https://web.archive.org/web/20220528215413/https://research.filecoin.io/assets/power-fault-tolerance.pdf

[135] *Sia: Simple Decentralized Storage*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220529211009/https://sia.tech/sia.pdf

[136] *How Decentralized Storage Works*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220601135450/https://www.storj.io/how-it-works

[137] *Safe Network—How it Works*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220510030202/https://safenetwork.tech/how-it-works/

[138] *Safe Network—Frequently Asked Questions*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220510030202/https://safenetwork.tech/faq/

[139] *MaidSafeCoin Price Today, MAID to USD Live, MarketCap and Chart | CoinMarketCap*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220602052227/https://coinmarketcap.com/currencies/maidsafecoin/
[140] *Let's Talk About MultiAlgo + MultiShield | by Josiah Spackman | Medium*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20210123181006/https://josiah-digibyte.medium.com/lets-talk-about-multialgo-multishield-45e6a375a7a
[141] *QuarkCoin: Noble Intentions, Wrong Approach—Bitcoin Magazine*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220531220104/https://bitcoinmagazine.com/business/quarkcoin-noble-intentions-wrong-approach-1387343686
[142] *X11 Algorithm—ASIC Miners, Coins, Pool—BitcoinWiki*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220606202510/https://en.bitcoinwiki.org/index.php?title=X11&oldid=383584
[143] *SP×36—Spondoolies*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20210904095926/https://www.spondoolies-tech.com/products/spx36?variant=12551612104776
[144] *Digibyte Community Infopaper V1.0*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502154737/https://digibyte.org/docs/infopaper.pdf
[145] *Quarkcoin vs. Bitcoin | What's the Difference?* Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20140215035604/http://www.quarkcoins.com/bitcoin-vs-quarkcoin.html
[146] H. Y. Yuen, F. Wu, W. Cai, H. C. B. Chan, Q. Yan, and V. C. M. Leung, "Proof-of-play: A novel consensus model for blockchain-based peer-to-peer gaming system," in *Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, 2019, pp. 19–28.
[147] *Motocoin Whitepaper*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503221910/https://motocoin-dev.github.io/motocoin-site/Motocoin.pdf
[148] D. Kraft, "Game channels for trustless off-chain interactions in decentralized virtual worlds," *Ledger*, vol. 1, pp. 84–98, Dec. 2016.
[149] *Motocoin*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503224920/https://motocoin-dev.github.io/motocoin-site/
[150] *HunterCoin | Xaya*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503224135/https://xaya.io/huntercoin-legacy/
[151] *The Humble Beginnings of Blockchain Gaming—CoinQuora*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220130165557/https://coinquora.com/the-humble-beginnings-of-blockchain-gaming/
[152] *RSK Rootstock Platform—Bitcoin Powered Smart Contracts—White Paper*. Accessed: May 30, 2022. [Online]. Available: https://web.archive.org/web/20220525233107/https://www.rsk.co/Whitepapers/RSK-White-Paper-Updated.pdf

HENRI T. HEINONEN was born in Jyväskylä, Finland, in 1984. He received the Bachelor of Science and Master of Science degrees in physics from the University of Jyväskylä, Finland, in 2006 and 2009, respectively. He has written several research articles on blockchain technologies, run volunteer computing projects like SETI@home and BOINC, since the early 2000s on his home computers, and worked on Bitcoin, since 2013. His research interests include particle physics, blockchains, cryptocurrencies, many-money cryptoeconomies, and unconventional computing.

ALEXANDER SEMENOV received the Ph.D. degree in computer science from the University of Jyväskylä, Jyväskylä, Finland, in 2013.

He worked at the University of Jyväskylä and for multiple startup companies in e-commerce and transportation. He worked as a Visiting Scholar at several universities, including SUNY Buffalo, the University of Memphis, the University of Florida, the University of Central Florida, and the University of Sydney in Australia. He has coauthored over 50 peer-reviewed publications and has been a recipient of multiple research grants. His research interests include network science, efficient algorithms, analysis of large datasets, optimization, and machine learning. He is an Associate Editor of the *Journal of Combinatorial Optimization* and *IET Blockchain* journal.

JARI VEIJALAINEN received the B.Sc. degree in mathematics and the M.Sc. degree in computer science from the University of Helsinki, Finland, in 1978 and 1983, respectively, and the Dr.-Ing. degree from the Technical University of Berlin, Germany, in 1989. He worked at the University of Helsinki, as a Teaching Assistant; at the Technical Research Center of Finland (VTT), as a Senior Research Scientist; and at the University of Jyväskylä, as a Full Professor of data management/software engineering, since 1996. He also worked as a Visiting Scholar in Germany at different research institutions and universities, including Waseda University, Tokyo, Japan. He has published about 150 refereed papers in scientific journals and conference proceedings. He has researched advanced transaction management, mobile computing, and social media analysis, and he has acted as an Editor, among others, of *Very Large Data Bases Journal* and *ACM Wireless Networks*. He is currently an Associate Editor of *Social Network Analysis and Mining* journal.

TIMO HÄMÄLÄINEN (Senior Member, IEEE) received the Ph.D. degree in telecommunication from the University of Jyväskylä, Jyväskylä, Finland, in 2002. In 1997, he joined the University of Jyväskylä, where he is currently a Professor of computer networks. He has more than 25 years of research and teaching experience in computer networks. He has led many external-funded network management-related projects. He has launched and led master's programs with the University of Jyväskylä (SW & Communication Engineering) and teaches network management-related courses. He has more than 200 internationally peer-reviewed publications and supervised 40 Ph.D. dissertations. His research interests include network resource management, the IoT, and networking security.