Quantitative Aspects of the Blockchain: Proof Of Work, its Energy Usage and Alternative Consensus Mechanisms

Seminar Blockchain WS 17/18

Jack Henschel

December 14, 2017

Friedrich-Alexander-Universität Erlangen-Nürnberg

Table Of Contents

Introduction

Proof Of Work

Energy Usage of PoW

Alternative Consensus Methods

Conclusion

Introduction

What is Bitcoin?

> *Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen.*
>
> *Much of the trust in Bitcoin comes from the fact that it requires no trust at all. Bitcoin is fully open-source and decentralized. [...] No organization or individual can control Bitcoin, and the network remains secure even if not all of its users can be trusted.*

– *Bitcoin FAQ* [17b]

How is this possible?

Byzantine Generals Problem

First decribed by Leslie Lamport, Robert Shostak and Marshall Pease from SRI International in their paper “The Byzantine Generals Problem” [LSP82].

A group of generals siege an enemy city. The generals need to agree on whether to attack the city or retreat.

The distributed generals need to coordinate. It is important that every general agrees on the decision and follows through, otherwise the lose.

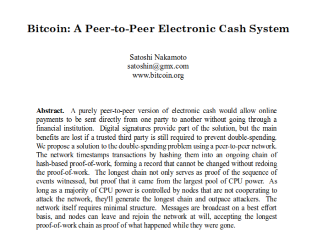
Traitorous generals

Communication via messengers

Proof Of Work

Solution

Bitcoin tackles this problem by having each ”general” work on a mathematical problem that is known to take a certain, average amount of time. When a general finds a solution he passes his solution onto the other generals who will verify and then incorporate the answer to the previous problem into a new problem



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

The ”consensus” is intrinsically linked to the ”math problem” so that the generals will always ”trust” the chain-of-answers which is the longest, as it would be impractical / impossible for an attacker to counterfeit the long-chain-of-answers. [Nak08]

Concept

> *The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.*
>
> *[The block's nonce is incremented] until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.*

– Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Oct. 31, 2008 [Nak08]

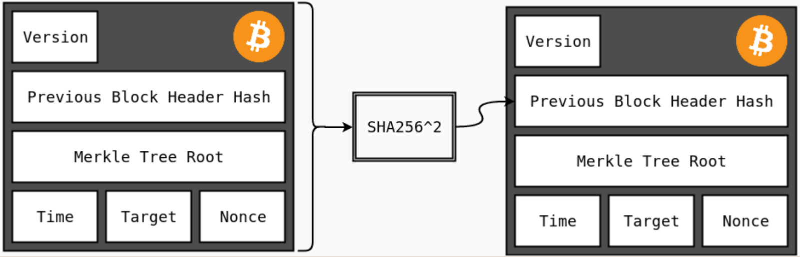
Block Header Structure

```
/** Nodes collect new transactions into a block, hash them into a hash tree,
 * and scan through nonce values to make the block's hash satisfy proof-of-work
 * requirements.  When they solve the proof-of-work, they broadcast the block
 * to everyone and the block is added to the block chain.  The first transaction
 * in the block is a special one that creates a new coin owned by the creator
 * of the block. */
class CBlockHeader {
public:
    int32_t nVersion;
    uint256 hashPrevBlock;
    uint256 hashMerkleRoot;
    uint32_t nTime;
    uint32_t nBits;
    uint32_t nNonce;
}
```

The Bitcoin Core developers. *Bitcoin Core*. Dec. 9, 2017. URL: `https://github.com/bitcoin/bitcoin`, src/primitives/block.h

Block Mining

```
var hash uint32 = 1
var myBlockHeader = newBlockHeader() // creates and fills block header
while (hash > myBlockHeader.nBits) {
  hash = sha256(sha256(myBlockHeader))
  myBlockHeader.nNonce++
  // Note: might need to update hashPrevBlock,
  // hashMerkleRoot, nTime and/or nBits
}
print("Heureka!")
// publish blocks to other nodes
```



Block Mining

SHA256^2

Bitcoin uses “SHA256 function squared”, due to the birthday attacks on the smaller but related SHA1 hash. SHA1’s resistance to birthday attacks has been partially broken as shown by a collaboration between Google Research and CWI Amsterdam.

“The first collision for full SHA-1”, `https://shattered.io`, [Ste+17]

Mining vs. Minting

Minting: creating coins (real or virtual) without doing real work

Mining: creating coins requires doing hard work (Blockchain: solving puzzles)

> *The process has come to be known as "mining" because it is slow and intensive, reaping a gradual reward in the same way that minerals such as gold are mined from the ground.*

– Kelly, *Bitcoin 'miners' face fight for survival as new supply halves* [Kel16]

Mining

Why are they doing it?

Bitcoin Mining Business 101:

$$\mathit{Profit} = \mathit{Reward} - \mathit{Cost}$$

$$\mathit{Reward} = \mathit{BlockReward} + \mathit{TransactionFees}$$

$$\mathit{Cost} = \mathit{HardwareCost} + \mathit{OperatingCosts}$$

$$\implies \mathit{Profit} = \mathit{BlockReward} + \mathit{TransactionFees} - \mathit{HardwareCost} - \mathit{OperatingCosts} \overset{!}{\gg} 0$$

Mining Hardware

Hardware	Hashing Power
CPU	25 MH/s
GPU	500 MH/s
FPGA	10,000 MH/s
ASIC	14,000,000 MH/s

Source: [Ast16]

ASIC

Bitmain Antminer S9 Specs	
Hash Rate	13.5 TH/s
Power Consumption	1300 W
Power Efficiency	0.098 J/GH
Lithography Process	16 nm
Price	1500 EUR

Antminer S9, `https://www.antminereurope.com/antminer-s9/` [17c]

Energy Usage of PoW

Bitcoin's electricity usage

$$H_R = 14,788,692,144 \frac{GH}{s}$$

from `blockchain.info` [17d] (accessed: Dec. 14, 2017)

$$P = \eta \times H_R = 0.1\,\frac{\mathrm{J}}{\mathrm{GH}} \times 14.79\,\frac{\mathrm{EH}}{\mathrm{s}} = 1{,}478{,}869{,}214\,\frac{\mathrm{J}}{\mathrm{s}} = 1.4\,\mathrm{GW}$$

> *The actual network will be a mix of hardware of types at different levels of efficiency, so we expect that the actual efficiency will be between the two. This suggests that the total power used for Bitcoin mining is around 0.1–10GW.*

– O'Dwyer and Malone, "Bitcoin Mining and its Energy Footprint" [OM14]

Bitcoin’s electricity usage (cont’d)

	Efficiency	Hourly (E_H)	Daily (E_D)	Annually (E_A)
Lower bound:	0.1 J/GH	1.4 GWh	33.6 GWh	12.3 TWh
Digiconomist:	0.283 J/GH		90 GWh	33 TWh

Estimates from Digiconomist [17e]

$\implies$ 0.15% of the world’s electricity consumption

Ethereum's electricity usage

GPU instead of ASIC mining leads to higher inefficiency

Efficiency: $\eta = 5$ J/MH (NVIDIA GTX 1070, [Kir17])

Hashrate: $H_R = 125$ TH/s (from `etherscan.io` [17f], accessed Dec. 14, 2017)

$$P = \eta \times H_R = 625\,\mathrm{MW}$$

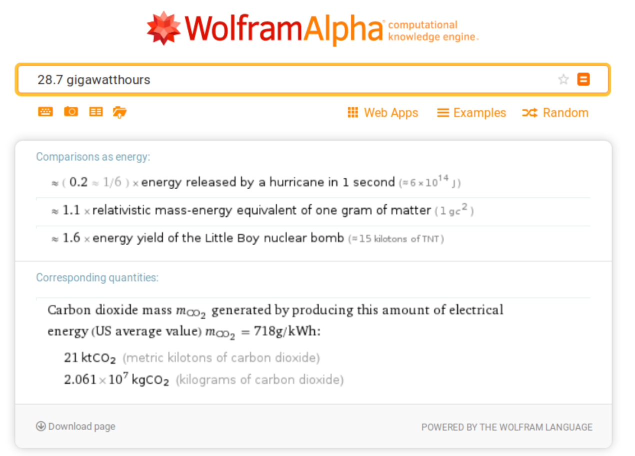
	Efficiency	Hourly (E_H)	Daily (E_D)	Annually (E_A)
Lower bound:	5 J/MH	625 MWh	15 GWh	5.5 TWh
Digiconomist [17g]:	10.83 J/MH		30 GWh	11 TWh

Bitcoin vs. Ethereum

	Bitcoin	Ethereum
Hashrate	14 EH/s	125 TH/s
Price per coin	16,385 USD	728 USD
Transaction per day	400,000	900,000
Transaction volume per day	3 mio. BTC	10 mio. ETH
Transaction volume per day	50 bill. USD	8 bill. USD
Block time	10 min	15 s
Annual energy	10.5 TWh	5.5 TWh
Energy per block (E_{Block})	233 MWh	2.6 MWh
Energy per transaction (E_{TXN})	84 kWh	16 kWh

Source: [17h] and [17i]

Electricity usage comparison



28.7 gigawatthours

Comparisons as energy:

- ≈ (0.2 ≈ 1/6) × energy released by a hurricane in 1 second (≈ 6×10^{14} J)
- ≈ 1.1 × relativistic mass-energy equivalent of one gram of matter (1 gc^2)
- ≈ 1.6 × energy yield of the Little Boy nuclear bomb (≈ 15 kilotons of TNT)

Corresponding quantities:

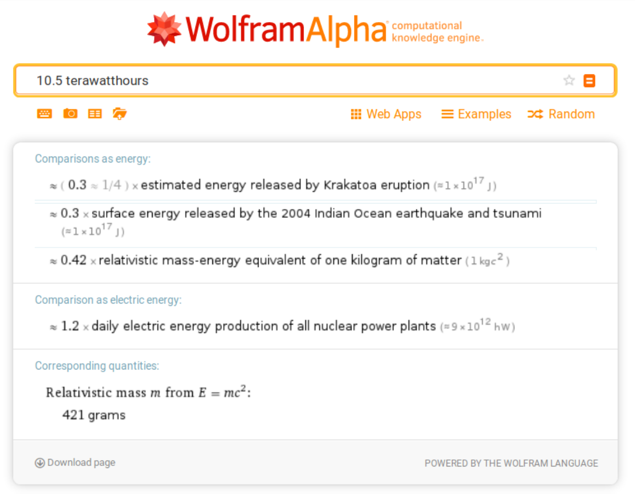
Carbon dioxide mass m_{CO_2} generated by producing this amount of electrical energy (US average value) m_{CO_2} = 718g/kWh:

21 ktCO_2 (metric kilotons of carbon dioxide)

2.061×10^7 kgCO_2 (kilograms of carbon dioxide)

Source: *WolframAlpha: 28.7 gigawatthours* [17j] (accessed: Dec. 11, 2017)

Electricity usage comparison



WolframAlpha computational knowledge engine.

10.5 terawatthours

Web Apps | Examples | Random

Comparisons as energy:

≈ (0.3 ≈ 1/4) × estimated energy released by Krakatoa eruption (≈ 1×10^{17} J)

≈ 0.3 × surface energy released by the 2004 Indian Ocean earthquake and tsunami (≈ 1×10^{17} J)

≈ 0.42 × relativistic mass-energy equivalent of one kilogram of matter ($1\ \mathrm{kg}c^2$)

Comparison as electric energy:

≈ 1.2 × daily electric energy production of all nuclear power plants (≈ 9×10^{12} hW)

Corresponding quantities:

Relativistic mass m from $E = mc^2$:

421 grams

Download page

POWERED BY THE WOLFRAM LANGUAGE

Source: *WolframAlpha: 10.5 terawatthours* [17k] (accessed: Dec. 11, 2017)

Electricity usage comparison

> *In 2014, data centers in the U.S. consumed an estimated 70 [TWh], representing about 1.8% of total U.S. electricity consumption.*

– "United States Data Center Energy Usage Report", June 2016 [She+16]

	Ethereum	Bitcoin	Amazon (US)	Google (US)
Electric capacity in GW	0.6	1.4	1.219	3.186

[Eck17]

Electricity cost

Based on US commercial prices in 2016: $10\frac{ct}{kWh}$

Electricity cost per block:

$$C_{Block} = E_{Block} \times 0.1\,\frac{\text{USD}}{\text{kWh}} = 23{,}333.33\,\text{USD}$$

Electricity cost per transaction:

$$C_{TXN} = E_{TXN} \times 0.1\,\frac{\text{USD}}{\text{kWh}} = 8.4\,\text{USD}$$

Reward

Each time a block is found and appended to the blockchain, the miner is rewarded with the block reward and the transaction fees of all transactions stored inside that block.

$$\begin{aligned} \mathit{Reward} &= \mathit{BlockReward} + \mathit{TransactionFees} \\ &= 12.5\,\mathrm{BTC} + 1.4\,\mathrm{mBTC} \times 2700\,\frac{\mathit{TXN}}{\mathit{Block}} \\ &= 16.8\,\mathrm{BTC} \end{aligned}$$

$$\mathit{Reward}_{\mathit{USD}} = \mathit{Reward}_{\mathit{BTC}} \times 16{,}385\,\mathrm{USD} = 275{,}268\,\mathrm{USD}$$

Transaction fees and transaction per block from:
`bitinfocharts.com/bitcoin/` [17h] (accessed: Dec. 14, 2017)

Alternative Consensus Methods

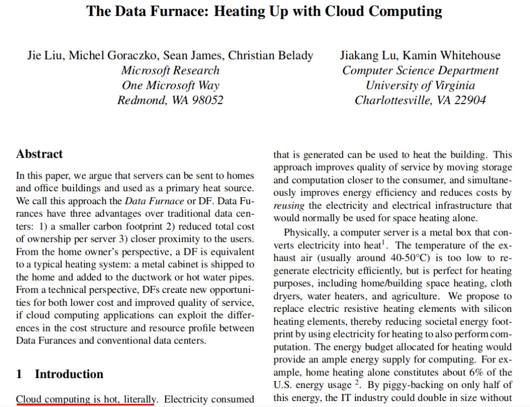
Proof Of Useful Work

Let’s use all the work for something …

useful!

Proof Of Useful Work: Data Furnace

Most efficient heater ever, turns electricity into money *and* heat!



The Data Furnace: Heating Up with Cloud Computing

Jie Liu, Michel Goraczko, Sean James, Christian Belady
Microsoft Research
One Microsoft Way
Redmond, WA 98052

Jiakang Lu, Kamin Whitehouse
Computer Science Department
University of Virginia
Charlottesville, VA 22904

Abstract

In this paper, we argue that servers can be sent to homes and office buildings and used as a primary heat source. We call this approach the *Data Furnace* or DF. Data Furances have three advantages over traditional data centers: 1) a smaller carbon footprint 2) reduced total cost of ownership per server 3) closer proximity to the users. From the home owner's perspective, a DF is equivalent to a typical heating system: a metal cabinet is shipped to the home and added to the ductwork or hot water pipes. From a technical perspective, DFs create new opportunities for both lower cost and improved quality of service, if cloud computing applications can exploit the differences in the cost structure and resource profile between Data Furances and conventional data centers.

1 Introduction

Cloud computing is hot, literally. Electricity consumed

that is generated can be used to heat the building. This approach improves quality of service by moving storage and computation closer to the consumer, and simultaneously improves energy efficiency and reduces costs by *reusing* the electricity and electrical infrastructure that would normally be used for space heating alone.

Physically, a computer server is a metal box that converts electricity into heat[1]. The temperature of the exhaust air (usually around 40-50°C) is too low to regenerate electricity efficiently, but is perfect for heating purposes, including home/building space heating, cloth dryers, water heaters, and agriculture. We propose to replace electric resistive heating elements with silicon heating elements, thereby reducing societal energy footprint by using electricity for heating to also perform computation. The energy budget allocated for heating would provide an ample energy supply for computing. For example, home heating alone constitutes about 6% of the U.S. energy usage [2]. By piggy-backing on only half of this energy, the IT industry could double in size without

Advantages:

1. smaller carbon footprint
2. reduced cost of ownership
3. closer proximity to users

"The Data Furnace: Heating Up with Cloud Computing"
[Liu+11]

Combined with spikes of renewable energy, preventing energy grid from damage

Proof Of Useful Work: Science

> *Primecoin network searches for special prime number chains known as Cunningham chains and bi-twin chains. The distribution of these prime chains are not well-understood currently as even for its simplest case twin primes their infinite existence is not proven.*

– *About Primecoin* [17l]

Finding the prime number chains becomes exponentially harder as the chain length is increased.

Comparable to the GIMPS project (The Great Internet Mersenne Prime Search)

Proof Of Useful Work: Renewable Energy

SolarCoin has a market cap of 97,500 TWh of solar energy generation

- 0.1% have been mined with Proof Of Work and represent historically generated solar electricity (unclaimed within SolarCoin)
- 0.5% reside in the genesis pool account, reserved for environmental charities, volunteers, advisers, builders and maintainers of SolarCoin
- 99.4% are stored in the generator pool account, exchanged for solar electricity generation

Each SolarCoin in circulation represents 1 MWh of generated solar electricity.

Coins are issued by The SolarCoin Foundation to operators of solar facilities

Source: *SolarCoin FAQ* [17m]

Proof Of Useful Work

General problems:

- *exhaustable*
- *not equiprobable*

Proof Of Stake

Used resource: cryptocurrency

Potential benefits:

- Lower overall cost
- Stakeholder incentives

Variations:

- Proof Of Stake: “Stake” of coin increases as long as the coin is not used
- Proof Of Deposit: coin is frozen for some time, but can be reclaimed
- Proof Of Activity: any online coin (from an online node) can win

> *After years of research, one thing has become clear: proof of stake is non-trivial – so non-trivial that some even consider it impossible.*

– Vitalik Buterin, *Slasher Ghost, and Other Developments in Proof of Stake* [But14]

Proof Of Stake: Casper

Casper is a smart contract that will implement and monitor Proof Of Stake

Idea: Anyone can bond tokens (coins), decisions leading to a convergence on the chain make money, otherwise lose money

Validators transfer stake to Casper

Validators have two functions:

1. Prepare
2. Commit

Two rounds of voting per block, but each validator can only vote once

Votes are weighted by the staked amount

Proof Of Stake: Casper (cont'd)

Casper (the smart contract) will then:

- *slash* bad validators (stake is lost)
- *reward* good validators (stake is frozen up + block reward)

Votes are essentially bets:

- you need to spend coins (real or virtual) for it
- you want to choose the most likely outcome (in this case: the most likely block to be added to blockchain)

Delegated Proof Of Stake

First implemented by Bitshares

Stakeholders elect witnesses to generate blocks

Witnesses validate signatures and timestamp transactions by including them in blocks

Each account is allowed one vote per share per witness The top N witnesses by total approval are selected, where N is defined such that at least 50% of voting stakeholders believe there is sufficient decentralization

Each time the elected witnesses produce a block, they are paid for their services. Their pay rate is set by the stakeholders via their elected delegates. If witness fails to produce a block, then they are not paid, and may be voted out in the future. Witnesses can't sign invalid blocks as the block needs confirmation by the other witnesses as well.

Delegated Proof Of Stake (cont'd)

The slate of active witnesses is updated daily when the votes are tallied. The witnesses are shuffled, and each witness is given a turn to produce a block at a fixed schedule of one block .

Anyone can monitor network health by observing the witness participation rate.

The low number of witnesses enables a high performance level of effectiveness in creating the blocks and general upkeep of the blockchain.

All network parameters (fee schedules, block intervals, transaction sizes) can be tuned via elected delegates.

Adapted from: *Delegated Proof-of-Stake Consensus* [17n]

Proof Of Burn

Idea: send coins to an irretrievable address, get proportionate votes on the blockchain for the “spent” coins

Consumed resource: currency

Usage in Slimcoin:

> *Proof-of-work is used as a mean for generating the initial money supply. As time passes and as the network accumulates a sufficient supply of coins, proof-of-work mining will become less necessary. Therefore, the network will rely more on proof-of-burn and proof-of-stake, the more energy efficient alternatives.*

Comparison: buying a mining hardware = burning (“spending”) coins [170]

Proof Of Burn: Application

Bootstrapping a Cryptocurrency

Users “burn” original coin, are awarded with coins of new currency

Proof Of Luck

Conceived by Mitar Milutinovic, Warren He, Howard Wu and Maxinder Kanwal from UC Berkeley

Used resource: Trusted Execution Environment (TEE / TXE)

Relies on security and correctness of TXE provided by manufacturer

Combines Proof Of Work, Proof Of Time and Proof Of Ownership.

> *Offers low-latency transaction validation, deterministic confirmation time, negligible energy consumption, and equitably distributed mining.*

“Proof of Luck: An Efficient Blockchain Consensus Protocol” [Mil+16]

Proof Of Luck: Algorithm

Round based voting consensus

Each round is allocated a time slot, random number is generated inside TEE

TEE also ensures the random number is generated in the specified time slot

All participants share their (random) number, “highest” numbers wins the random (i.e. new block is created)

Conclusion

Conclusion

Bitcoin (and in particular Proof Of Work) solves a *really* hard problem: establishing trust between largely anonymous parties without requiring trust.

As Tomaso Atse, from the University College London Centre for Blockchain Technologies, wrote in his paper *The Fair Cost of Bitcoin Proof of Work* [Ast16]:

> *I conclude that the current cost, although large, is of a justified order of magnitude for an anonymous systems operating between untrustful parties.*

Personal Thoughts

Bitcoin can not scale indefinitely with Proof Of Work

Cryptocurrencies and blockchains are here to stay

Vast applications for blockchains

Technology is rapidly evolving: *Lightning Network*, *Segregated Witness Benefits*, alternative and hybrid consensus mechanisms, ...

State of blockchain comparable to computers in the 70s and 80s

If blockchains and distributed computing does present a new leap forward in how we communicate, this electricity will not be wasted.

Thank you!

“Quantitative Aspects of the Blockchain: Proof Of Work,
its Energy Usage and Alternative Consensus Mechanisms”

Jack Henschel (December 14, 2017)

Source Material and Resources available at:

`https://gitlab.cs.fau.de/in76yleb/seminar-blockchain`

References i

4CDR: FAU Vektor Logos und Siegel. Dec. 13, 2017. URL: http://www.4cdr.com/fau-vektor-logos-und-siegel-druckfahig-cmyk/.

Bitcoin FAQ. Dec. 9, 2017. URL: https://bitcoin.org/en/faq.

Leslie Lamport, Robert Shostak, and Marshall Pease. "The Byzantine Generals Problem". In: *ACM Transactions on Programming Languages and Systems* 4/3 (July 1982), pp. 382–401. URL: http://lamport.azurewebsites.net/pubs/byz.pdf.

Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: (Oct. 31, 2008). URL: https://bitcoin.org/bitcoin.pdf.

References ii

- The Bitcoin Core developers. *Bitcoin Core*. Dec. 9, 2017. URL: https://github.com/bitcoin/bitcoin.

- Marc Stevens et al. “The first collision for full SHA-1”. In: (Feb. 23, 2017). URL: https://shattered.io.

- Jemima Kelly. *Bitcoin ’miners’ face fight for survival as new supply halves*. Thomson Reuters. July 8, 2016. URL: https://www.reuters.com/article/us-markets-bitcoin-mining/bitcoin-miners-face-fight-for-survival-as-new-supply-halves-idUSKCN0ZO2CW.

- Tomaso Aste. *The Fair Cost of Bitcoin Proof of Work*. June 27, 2016. URL: https://ssrn.com/abstract=2801048.

References iii

Antminer S9. Nov. 25, 2017. URL: https://www.antminereurope.com/antminer-s9/.

Bitcoin Stats. Dec. 14, 2017. URL: https://blockchain.info/stats.

Karl J. O'Dwyer and David Malone. "Bitcoin Mining and its Energy Footprint". In: (June 26, 2014). URL: http://karlodwyer.com/publications/pdf/bitcoin_KJOD_2014.pdf.

Bitcoin Energy Consumption Index. Dec. 12, 2017. URL: https://digiconomist.net/bitcoin-energy-consumption.

References iv

Nathan Kirsch. *GeForce GTX 1070 Ethereum Mining*. June 14, 2017. URL: http://www.legitreviews.com/geforce-gtx-1070-ethereum-mining-small-tweaks-great-hashrate-low-power_195451.

Ethereum Network HashRate Chart. Dec. 14, 2017. URL: https://etherscan.io/chart/hashrate.

Ethereum Energy Consumption Index. Dec. 12, 2017. URL: https://digiconomist.net/ethereum-energy-consumption.

Bitcoin (BTC) price stats and information. Dec. 14, 2017. URL: https://bitinfocharts.com/bitcoin/.

References v

Ethereum (ETH) price stats and information. Dec. 14, 2017. URL: https://bitinfocharts.com/ethereum/.

WolframAlpha: 28.7 gigawatthours. Dec. 11, 2017. URL: http://www.wolframalpha.com/input/?i=28.7+gigawatthours.

WolframAlpha: 10.5 terawatthours. Dec. 11, 2017. URL: http://www.wolframalpha.com/input/?i=10.5+terawatthours.

Arman Shehabi et al. “United States Data Center Energy Usage Report”. In: (June 2016). URL: https://eta.lbl.gov/publications/united-states-data-center-energy.

References vi

Brian Eckhouse. *Google, Biggest Corporate Buyer of Clean Power, Is Buying More*. Bloomberg New Energy Finance. Nov. 30, 2017. URL: https://www.bloomberg.com/news/articles/2017-11-30/google-biggest-corporate-buyer-of-clean-power-is-buying-more.

Jie Liu et al. "The Data Furnace: Heating Up with Cloud Computing". In: USENIX, June 2011. URL: https://www.microsoft.com/en-us/research/publication/the-data-furnace-heating-up-with-cloud-computing/.

About Primecoin. Nov. 25, 2017. URL: http://primecoin.io/about.php.

References vii

SolarCoin FAQ. Dec. 9, 2017. URL: https://solarcoin.org/en/frequently-asked-questions.

Vitalik Buterin. *Slasher Ghost, and Other Developments in Proof of Stake.* Oct. 3, 2014. URL: https://blog.ethereum.org/2014/10/03/slasher-ghost-developments-proof-stake/.

Delegated Proof-of-Stake Consensus. Dec. 9, 2017. URL: https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

What is Proof of Burn (ELI5)? Dec. 9, 2017. URL: http://slimco.in/proof-of-burn-eli5/.

References viii

Mitar Milutinovic et al. “Proof of Luck: An Efficient Blockchain Consensus Protocol”. In: *Proceedings of the 1st Workshop on System Software for Trusted Execution*. SysTEX ’16. Trento, Italy: ACM, 2016, 2:1–2:6. URL: `http://doi.acm.org/10.1145/3007788.3007790`.