Department of Economics and Finance

Chair of Mathematics 2

Blockchain, Bitcoin and its costs

Supervisor:

Prof.

Giovanni Alessandro Zanco

Candidate:

Daniele Corleto

230701

Academic year 2020/2021

TABLE OF CONTENTS

INTRODUCTION

Throughout the last few years, Bitcoin and cryptocurrencies in general have paved their way into mass media coverage and passed from being known only by a community of computer scientist to being acknowledged by most of the population worldwide. The rationale behind this major change can be found in cryptocurrencies unmatched volatility and upward price tendency. This particular feature, common to all cryptocurrencies and in particular to Bitcoin, provided the investors with the possibility to speculate and get rich (or poor) with an unprecedented velocity. Obviously, people who got great results from their investments in crypto have been way more active in sharing their outcomes through social media than the ones that saw their investments evanish before their eyes; following this pattern, it is easy to see why cryptocurrencies have been commonly known as an easy and quick way to make a fortune that bears some risk only in the short run.

However, the perception that stems from the so-called "Crypto-millionaires" and suggests that Bitcoin and cryptocurrencies are a high performance asset is greatly biased and, through the hype it has created over time, it has led to the formation of numerous frictions and side effects.

The first chapter is entirely dedicated to the functioning of Bitcoin, the first cryptocurrency ever created. We will explain what was the rationale behind its creation and, through the study of Satoshi Nakamoto's white paper "*Bitcoin: A peer-to-peer Electronic Cash System*" (2008), we will find out how Bitcoin manages to resolve online payments issues and also the rules that regulate its creation through the so-called mining.

The second chapter focuses on the mining process and tries to picture a situation of equilibrium in which all the miners maximize their utility functions. We will study the main determinants of miners' strategies and see how these affect the gross resource usage. The model we study here was proposed in the working paper "*Market structure in Bitcoin mining*" of the National Bureau of Economics Research, by June Ma, Joshua S. Gans, Rabee Tourky. Although interesting in its approach to modelling the mining process and in the way its results are analyzed, the paper lacks mathematical precision and rigor; in particular, some claims in the paper are not true for the complete model, but only if some additional assumptions are made. Therefore we make some additions and adjustments to the model and find some first rigorous mathematical results about it. Since however this model we introduce requires mathematical techniques that are too advanced for the present work, we show how the model in the mentioned paper can be seen as a simplification of the rigorous one and we give rigorous proofs of some of the results discussed in the paper. This will

allow us to draw conclusions about the simplified model that can be argued to hold also for the rigorous model and that will be discussed in the following chapter

The third and last chapter will use multiple sources to describe Bitcoin's energetic demand and ecological impact. Assuming the second chapter's mathematical model is verified we will show that the current state of the Bitcoin protocol, if compared with the classical banking system, is far from being efficient and is responsible to huge amounts of CO2 emissions. Lastly, we will propose a possible change in the Bitcoin protocol that could totally disrupt the present competition among miners and consequently decrease the aggregate demand for energy.

1. BITCOIN

1.1 BITCOIN'S FOUNDATION

In 2008, a computer scientist named Satoshi Nakamoto, whose real identity still remains unknown, published a white-paper on the internet entitled "*Bitcoin: A peer-to-peer Electronic Cash System*"; in the paper, Nakamoto envisioned the creation of a new type of virtual money, the Bitcoin, which is a purely peer-to-peer version of electronic cash that directly connects the parties of an online transaction and allows them to send payments directly from one party to another, without going through a financial institution.

The biggest innovation that the white paper brings to the table is embedded in a new technology that ensures the soundness and the fairness of online transactions. In general, online transactions' integrity can be put into question by two main issues:

1) The parties do not know each other and there is no trust between them, so, it could happen that one of the parties will not fulfill their contractual obligations without any sort of penalty
2) There is the possibility that a certain agent uses the same amount of money to pay for multiple transactions (double-spending problem)

The classical solution to these problems, since the beginnings of online markets, has always relied on the supervision and intermediation of financial institutions to serve as trusted third parties and process electronic payments. While this system fits well the majority of online transactions, it still lacks in some aspects, in fact, it suffers some weaknesses that derive from scarcity of trust between the parties. Since financial institutions are obliged to mediate disputes that arise from online payments, they are unable to ensure completely non-reversible transactions, even if non-reversible services are exchanged. This has some bad effects on financial institutions' efficiency in intermediation because it prevents the complete elimination of the double-spending problem, and it also increases the cost of mediating online payments, limiting the minimum practical transaction size.

So, even if the intermediation in online payments proved to be a good solution, still it has presented some flaws overtime, such as the possibility of fraud, that has not been eradicated yet, and some frictions that prevent agents from exchanging currency for services or goods without incurring in any transaction fee.

1.2 BLOCKCHAIN FUNCTIONING

In his paper, Nakamoto presents a new and innovative solution to regulate online transactions, indeed he proposes to dismiss third parties' intermediation and switch it in favor of an electronic payment system that allows economic agents to directly carry out contracts using a peer-to-peer network, the blockchain, that not only records the transactions in chronological order, but also ensures that they remain unchanged in the future since they are protected by cryptography and are impractical to reverse.

We have previously defined the Bitcoin as an electronic coin. Such type of currency can be described as an exchangeable commodity which can be used to execute payments uniquely in the digital form and whose ownership can be verified through the sequence of transaction it carried out. Each digital payment requires the payer to digitally sign on the coin the hash[1] of the coin's previous transaction and also the public key that identifies the next owner; in this way the payee is able to prove his ownership by verifying all of the coin's signatures.

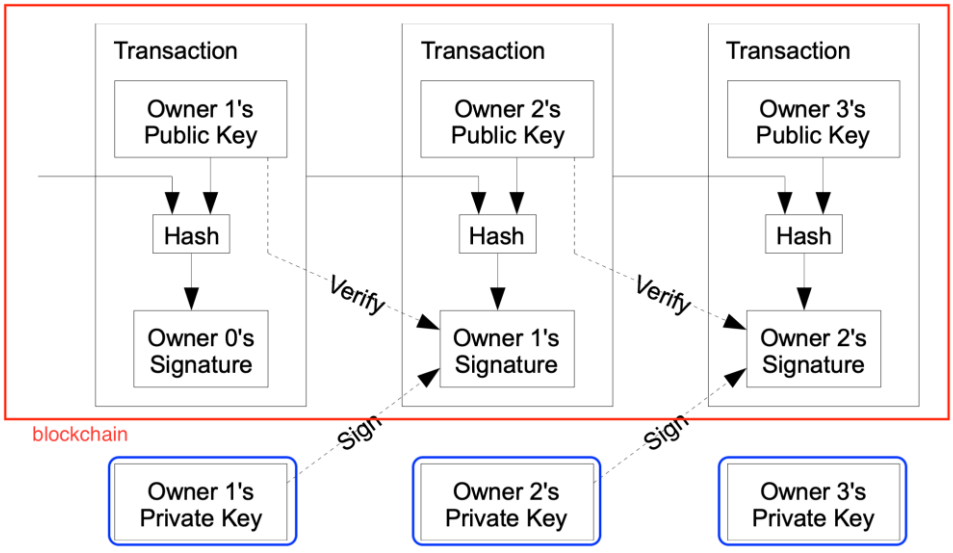

Figure 1: graphical representation of the digital signatures that prove ownership of bitcoin. From *[10]*

This system provides the users with an efficient mechanism to prove the ownership of a certain amount of digital commodity, anyway, it does not resolve the need of the payee to verify whether one of the previous owners did double-spend the coin he is acquiring. The common solution to this issue usually involves a trusted central authority or mint and requires this entity to supervise each transaction and make sure there is no case of double spending. This pattern obliges users to give to

[1] A hash is a digital code that can be computed from any type of digital data using a hash function

the central authority any sum of coin received in a digital transaction because later they will be given back from the same central authority the same amount of commodity in newly minted coin. The rationale behind this mechanism is that if only newly minted coins are accepted to transact, each transaction will be regulated and overviewed by the entity that runs the mint. This solution proves itself to be effective against double spending, but it strictly relies on a thrusted third party, just like orthodox payment systems.
In order to change and better off the efficiency of online payments, another, more advanced way to eliminate double-spending has to be implemented. One possible solution expects every user of a certain payment system to be aware of all the concluded transactions. To arrive to this situation without the involvement of any trusted third party, there is the need to publicly announce each transaction and to make sure that each participant to the network agrees to their historical order; Nakamoto's paper specifically aims at resolving this difficult task.

First of all, the mechanism requires the use of a timestamp server[2] that groups the data of transactions into blocks of items and singularly identify them by a hash. Then, it publishes the hash, proving to the network that the published data (transactions) occurred at a certain past time. Each hash will contain the data of the previously published one and, in this way, the timestamp server creates a chain of recursively connected hashes.

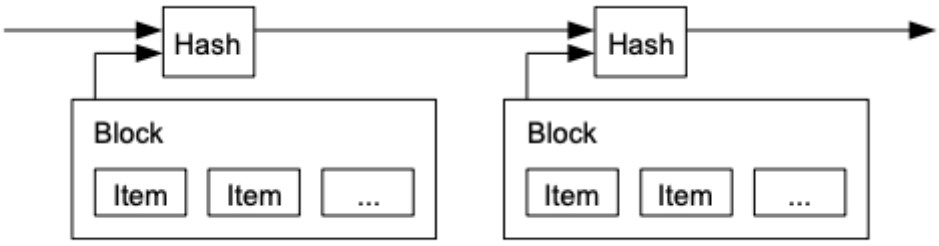

Figure 2: graphical repredentation of hashes connected in the blockchain. From *[10]*

The application of a distributed timestamp server on a peer-to-peer basis is not free of any flow, in fact it is not independently safe from malicious attacks. To prevent this event from happening, the protocol employs a proof-of-work requirement in the process that leads to the block hash. This requirement makes sure that, if a malicious participant tries to alter block's data, not only he/she would have to redo the Proof-of-work for the altered block, but, as blocks are recursively linked, he/she would have to redo it also for all the blocks that have succeeded it.

[2] A timestamp server uses a certain algorithm to prove that an event happened at a certain time and that the data about it has not changed afterwards

The proof-of-work chosen by Nakamoto demands the participants to find out a value that, when put into the SHA-256 function, is transformed into a given hash. The SHA-256 is a function originally published by NSA in 2001 and that can be used for free. It maps any digital input into a 256 bits output that is usually presented as a hexadecimal string. It is considered a secure function because there is no known algorithm to reverse it, meaning that the only way to reverse it is by guessing the right input. This computational puzzle is very effective because users consume a consistent amount of time to find the right input and they can easily verify if one input is the solution by executing a single computation, which takes a negligible amount of time. The difficulty of the puzzle can be changed positively correlated to the number of initial zeros in the hash. This last feature is vital for Bitcoin protocol because it gives to the network the possibility to target an average number of blocks per hour by adjusting its difficulty to the ever-increasing hardware speed of computers.
So, the network works on the proof-of-work until a user finds the solution to the SHA-256 puzzle and then he/she links the block of transactions to the previous one that is in the chain. This process, as we previously said, makes sure that data will not be changed without requiring the proof of work to be redone.
Proof-of-work is then a sort of lottery that is used to decide who will be the participant that will add the next block of transactions to the chain. The probability for any participant to win this lottery is proportional to his/her computational power (CP) because, the higher the CP, the lerger the number of attempts to solve the SHA-256 a participant can make in a given amount of time.
In Nakamoto's view, the CPU based competition is also effective in regulating the majority acceptance of the newly added blocks and in avoiding malicious attacks to the network. Indeed, acquiring more CPU, means buying more computers and spending more energy to run them, and this ensures that the majority of network's CPU do not belong to a malicious participant who would not have the needed monetary incentives to make such a big investment.
Summarizing what we said about the Bitcoin protocol so far, the whole algorithm can be broken down to a sequence of steps:

1) New transactions are carried out
2) The timestamp transmits hashes of transactions to all the nodes of the network
3) Each node groups data about new transactions into a block
4) Each node attempts to solve a difficult proof-of-work puzzle (SHA-256)
5) The first node to find the solution to the proof-of-work puzzle broadcasts its block to the whole network

6) Nodes accept the transmitted block if and only if all of its transactions are valid and there is no case of double-spending
7) When the majority of the nodes accepts the block, it is added to the chain
8) The hash of the accepted block is used to create the next block in the chain

This process can be periodically repeated infinitely many times and it creates a decentralized dataset, that took the name of "Blockchain".

1.3 BITCOIN MONETARY INCENTIVES AND AN INTRODUCTION OF THE CONSEQUENCES

To ensure that there will be competition in the network to solve the proof-of-work, the bitcoin protocol awards some prizes (monetary incentive) to the node that manages to solve the computational puzzle and add the new block to the chain.

These incentives come into two forms: newly minted bitcoins and transaction fees that might be offered by parties of a transaction.

We note that the proof-of-work process performed by nodes has an incidental role in issuing new currency in the absence of a centralized authority, so, just like gold miners expend resources to add gold to circulation, nodes use some scarce and costly resources, CPU and electricity, to increase the supply of bitcoin. Because of this parallelism, the nodes of bitcoin's network are widely referred to as "miners".

The rate at which miners are rewarded newly minted bitcoins is not constant, indeed, the amount given out halves every 210,000 blocks added to the chain (every 4 years) and it will be null once the total supply of 21 million bitcoins will be reached.

On the other hand, transaction fees do not follow some strict rules and totally depend on the parties of transactions. In fact, when economic agents want to speed up the pace at which their electronic payment is processed, they have the possibility to pay some fees to whoever manages to do so. These fees can be seen by miners, who, being profit maximizers, will obviously prefer to prioritize the highest fees transactions and choose them for their blocks.

Initially, fees were rare, and not only they have become increasingly common as demand for transactions on the network has increased in recent times, but they are also predicted to increase more and more in order to balance the future rate of bitcoin issuance, that is destined to fall

The incentives stipulated by the network make it worth it for miners to incur in computing technology costs, because that technology gives them the possibility to resolve the proof-of-work

puzzle and win the total reward in spite of other miners. Ergo, every time a block is validated and linked to the chain, all the miners incur in the costs associated to the technology of their choice and only the winning miner will be rewarded with newly minted Bitcoins plus any transaction fee.
Even if Nakamoto seemed to envision a purely peer-to-peer payment system, in which any personal computer could have the possibility to perform mining, the popularity that Bitcoin gained overtime increased its value and created the conditions to disrupt the mining process.
In fact the increased value of bitcoin straightforwardly increased the value of the prize won by whoever was able to complete the computational puzzle in the least time possible. Understanding this profit opportunity, miners began to invest in more sophisticated and powerful computers so that their computational power would increase together with their probability of validating the block and winning the prize. Despite miners started performing computations at a higher rate, the average time to validate each block has always been stable at 10 minutes due to the dynamic adjustment of difficulty provided by the server.
Among the side effects of the increased difficulty of the SHA-256 puzzle, we note that mining became totally unprofitable for individual miners that use regular computers because their CPU relative power and the associated probability to win the competition rapidly fell to almost zero.
In fact, in recent times, as the majority of mining activity took place in large warehouses equipped with computers strictly dedicated to mining, the competition in the bitcoin network has become a mere clash among the people who control the highest processing force. This led to the formation of mining pools: organized groups of individual miners who join their computation power together to increase their total probability of winning and to be awarded a piece of the total prizes that their mining pool is able to win.
Now we know that high computing force is a pivotal factor in bitcoin protocol as it is clearly correlated with high probability of validating the block, nonetheless, it is not said that the miner with the best processing technology will always be the first to solve the puzzle mainly because of 2 factors:

1) Relative computing power is highly volatile as it depends on the number of active nodes in the network at a given point in time
2) The random nature of the proof-of-work process, embedded in the non-deterministic way in which SHA-256 is solved, mitigates the monopolistic power of any miner

This situation lets us define the bitcoin protocol as an all-pay auction among miners, whose outcome cannot be easily defined. The analysis of this competition will be our concern in the following chapter

2. BITCOIN MINING GAME

We describe here a possible model of the Bitcoin mining in two versions, a complete one and a simplified one, the latter allowing for an easier analysis. The basics of the model are the same as in the working paper "*Market structure in Bitcoin mining*" of the National Bureau of Economics Research, by June Ma, Joshua S. Gans, Rabee Tourky, but we give here rigorous proofs of many mathematical facts, thgether with an introduction to some background material.

2.1COMPETITIVE ENVIRONMENT

We describe here a possible model of the Bitcoin mining game. Within this model we will analyze competitive environment that characterizes the Bitcoin mining process and search for possible Nash Equilibria that governs the whole game. To reach this goal some assumption will be made in order to make the model more tractable.

Assumption #1: the network will always be regarded as consisting of N identical miners, indexed by i $\in$ *{1, 2, …, N}, that independently choose their computing technology and share the same cost function.*

As a first step in the competition to solve the mining game, each miner *i*, has to choose a certain computing technology $x_i \in R_+$ at time t_0. The computing technology is measured in hashrate (hash computed / time) and has cost function $c(x_i) \geq 0$.

Assumption #2: The cost function $c: R_+ \to R_+$ *is strictly convex and strictly increasing* ($\lim_{x \to 0^+} \frac{\partial c}{\partial x} = 0$)

The miners use the technology they choose to solve a cryptographic puzzle which is given using the SHA-256 function; the puzzle features a difficulty level K $\in R_{++}$, which is the expected number of computation required to solve the function itself. The SHA-256 function is said to be a one-way function (quasi-impossible to invert) and its difficulty level K (measured in hashes) is adjusted dynamically every two weeks in order to ensure that it is solved on average during a span of time δ* $\in R_+$. This self-adjusting mechanism consists in increasing K if the puzzle is consistently solved in less than δ*. The aimed δ* amounts to 10 minutes, this period gives the nodes the required time to verify the transactions included in the blocks and it implies that any type of transaction brought out with Bitcoin as means of payment will be finalized and recorded in a maximum of 10 minutes,

giving to Bitcoin a great competitive advantage with respect to traditional banking system, that often takes days to do such things.

We will use $t = (t_1, t_2, \dots, t_N)$ as the vector that describes the time it takes for each player i = {1, 2, …, N} to solve the computational puzzle (for a fixed threshold K), so that the winner of the mining game will be the player i such that $t_i < t_j \ \forall \ i \neq j$. The winner of the game is rewarded with an amount of money P that is composed of two different parts: B, that represents an amount of newly minted bitcoins determined by the network, and f, that is the aggregate of the transaction fees offered in the associated block[3]:

$$P = B + f.$$

The mining game can be thus defined as an all-pay game, where each miner initially chooses to pay for some technology $x_i > 0$ if and only if he/she can meet the minimum effort cost required to solve the threshold-K puzzle, otherwise he/she would choose not to compete and thus not to incur in any cost.

The outcome of the game for player i that chooses $x_i > 0$ will therefore be

$$P - c(x_i) \ \ if \ i \ wins,$$
$$-c(x_i) \quad otherwise,$$

while any player that decides not to play will chose $x_i = 0$, incurring in $c(x_i) = 0$, meaning that he/she will have a monetary outcome equal to zero whatever happens in the mining game.

At this point, the main issue that restrains us from finding the profit maximizing condition for the above mentioned static all-pay game is a way to measure the probability of winning attached to each player; to solve such issue, we assume that the technology for solving computational puzzles is formally equivalent to a stochastic Poisson process.

2.2 STOCHASTIC POISSON PROCESS

A stochastic process is a collection of random variables indexed by a parameter, that in our case will be $t \in R_+$. A stochastic process indexed by a 1-dimentional parameter is often used to model random events that evolve in time and in our we will use it to study the behavior of certain set of independent events or the amount of time it takes for certain events to happen.

[3] Each user determines their transaction fee in a first price sealed bid auction. Thus, miners, who are profit maximizers, assemble the blocks to maximize *f* summing the highest fees offered in one block, making it as profitable as they can. This fee f is a fixed amount of bitcoin, but varies in terms of dollars due to fluctuations in bitcoin-dollar exchange rate.

Consider a sequence of N independent identically distributed random variables $\{X_i\} = \{X_1, X_2, \dots, X_N\}$ exponentially distributed with intensity λ, that is,

$$\mathrm{P}(X_i \leq x) = \int_0^x \lambda e^{-\lambda z} dz \quad \forall i$$

We interpret these variables as the waiting times of some statistically identical random events, in our case the time it takes for miner *i* to complete K difficulty level, thus the time at which the n-th event is concluded is represented by the random variable

$$S_n = X_1 + X_2 + \cdots + X_n. \tag{1}$$

We denote as N_t the stochastic process that counts the number of events that happened until time t:

$$N_t = \max\{n \in N : S_n \leq t\}$$

For any N, we now know that the events $\{N_t \geq n\}$ *and* $\{S_n \leq t\}$ are the same.

To calculate the density f_s of a random variable S that is the sum of two independent real valued random variables X and Y with density f_x *and* f_y we use a well known theorem that states that

$$f_s = f_x * f_y(z) = \int_{-\infty}^{+\infty} f_x(u) f_y(z-u) du \ .$$

Repeatedly applying it, we calculate the density of the random variable S_n, given by (1), obtaining the density function g_n of a random variable that is Gamma distributed with shape and rate parameter respectively *n* and λ, namely

$$g_n(x) = \lambda \frac{(\lambda x)^{n-1}}{(n-1)!} e^{-\lambda x}, \quad x \geq 0 \ .$$

We use g_n to compute the probability that S_n is lower or equal to a certain Z

$$P(S_n \leq Z) = 1 - P(S_n \geq Z) = 1 - \int_Z^{+\infty} g_n(x)\, dx$$

and, integrating by parts n times the latter equation, we find the distribution function

$$G_n(x) = \sum_{j=n}^{+\infty} e^{-\lambda x} \frac{(\lambda x)^j}{j!}, \quad x \geq 0$$

Therefore, we can now find the law of the random variable N_t.

$$P(N_t \geq n) = P(S_n \leq t) = G_n(t) = \sum_{j=n}^{+\infty} e^{-\lambda t} \frac{(\lambda t)^j}{j!}, \quad t \geq 0$$

and

$$P(N_t = n) = P(N_t \geq n) - P(N_t \geq n+1) = e^{-\lambda t} \frac{(\lambda t)^n}{n!}$$

That is exactly the density of a discrete Poisson distribution with intensity λt.

We call a stochastic process a *Poisson process* with intensity λ if

1) for every $t \geq 0, X_0 = 0$ and $X_t \in N$

2) The function $t \to X_t$ is non decreasing and right continuous with jumps of length 1
3) It has independent increments, so for every finite collection of time-points $0 < t_1 < t_2 < \cdots < t_m$ the random variables $X_{t_1}, X_{t_2} - X_{t_1}, \ldots, X_{t_m} - X_{t_{m-1}}$ are independent
4) For every $n \in N$ and every $0 \leq s < t$ the increments of X_t have the Poisson distribution with intensity $\lambda(t\text{-}s)$, meaning that

$$P(X_t - X_s = n) = e^{-\lambda(t-s)} \frac{(\lambda(t-s))^n}{n!} \quad (2)$$

The Poisson process helps us in understanding when a certain events happens and allows us to study the probability that a certain outcome happens *n* times in a predetermined time interval. It is said to be a stochastic, or random, process because the number of outcomes happening is not deterministic; in fact, the computation itself will only give us the probability attached to a certain event.

From formula (2), we can infer that the probability for any number of outcome to happen is equal to zero if t=0, that it is directly proportional to the time span t and we can also note that there is no reference to any other disjoint interval of time, so the probability is independent from any other historical precedent.

We will now show how the Poisson distribution can be derived from the binomial distribution.

A random variable Y is said to have *binomial distribution* $B_i(t, \beta)$ with parameters $t \in N$, $\beta \in [0, 1]$, *if*

$$P(Y = k) = \binom{t}{k} (\beta)^k (1-\beta)^{t-k}, \ \forall K \in N;$$

Y describes the number of 1's in a 0-1 experiment, repeated *t* times, in which the probability of obtaining 1 is β.

If we choose to use $\beta = \frac{\lambda}{t}$, we can see that taking larger *t*, the distribution becomes increasingly precise because it analyses more moments in time in which the outcome we are studying could happen; if we take the limit for t that goes to infinity, then we will have the most granular and precise probability distribution we can get.

So, we need to compute:

$\lim_{t\to\infty} P(Y = k) = \lim_{t\to\infty} \binom{t}{k} (\beta)^k (1-\beta)^{t-k}$,

choosing $\beta = \frac{\lambda}{t}$ and knowing that

$\binom{t}{k} = \frac{t!}{(t-k)!k!} = \frac{(t)(t-1)(t-2)\ldots(t-k+1)}{k!}$,

then

$$\lim_{t\to\infty} P(Y=k) = \lim_{t\to\infty} \frac{(t)(t-1)(t-2)\dots(t-k+1)}{k!}\left(\frac{\lambda}{t}\right)^k\left(1-\frac{\lambda}{t}\right)^{t-k}$$

we do not know the true value of the term $(t)(t-1)(t-2)\dots(t-k+1)$ but we state that it is bounded above by t^k and below by $(t-k+1)^k$, so that

$t^k \geq (t)(t-1)(t-2)\dots(t-k+1) \geq (t-k+1)^k$;

this implies that

$$\lim_{t\to\infty} \frac{t^k}{k!}\left(\frac{\lambda}{t}\right)^k\left(1-\frac{\lambda}{t}\right)^{t-k} \geq \lim_{t\to\infty} P(Y=k) \geq \lim_{t\to\infty} \frac{(t-k+1)^k}{k!}\left(\frac{\lambda}{t}\right)^k\left(1-\frac{\lambda}{t}\right)^{t-k} \quad (3)$$

using $\lim_{n\to\infty}\left(1+\frac{a}{n}\right)^n = e^a$ and the fact that

$$(t-k+1)^k = t^k + \alpha_1 t^{k-1} + \alpha_2 t^{k-2} + \dots + \alpha_{k-1}t + \alpha_k$$

$$= t^k(1 + \alpha_1 t^{-1} + \dots + \alpha_{k-1}t^{-k+1} + \alpha_k t^{-k}) \approx t^k \quad for\ large\ t,$$

we are able to use the squeeze theorem in formula (2) to give a value to $\lim_{t\to\infty} P(Y=k)$:

$$\lim_{t\to\infty} \frac{t^k}{k!}\left(\frac{\lambda}{t}\right)^k\left(1-\frac{\lambda}{t}\right)^{t-k} = \frac{\lambda^k}{k!}e^{-k} \geq \lim_{t\to\infty} P(Y=k) \geq \lim_{t\to\infty} \frac{(t-k+1)^k}{k!}\left(\frac{\lambda}{t}\right)^k\left(1-\frac{\lambda}{t}\right)^{t-k} = \frac{\lambda^k}{k!}e^{-k};$$

thus

$\lim_{t\to\infty} P(Y=k) = \frac{\lambda^k}{k!}e^{-k}$.

So we started from the binomial distribution and we arrived to a special case of formula (2) in which the time period of the distribution we study is equal to 1

As stated earlier, we assume that the technology for solving the computational puzzles is formally equivalent to the above explained Poisson process

$$X_i \sim \text{Poisson}(x_i)$$

Where $X_i(T)$ gives the number of computations miner *i* will complete in the time interval [0,t] given its choice of technology. By standard properties of the Poisson distribution the expected number of made computation is $x_i(t)$.

Assumption #2: Poisson processes corresponding to different miners are independent and work in parallel[4]

From the Poisson distribution of $X_i(t)$ we extrapolate the random variable $t_i \in R_+$, that is the time at which K computation are completed by miner *i*. The random variable t_i are independent and Gamma distributed:

[4] If this was not the case, then miners could organize in pools and potentially coordinate their computation to increase their chances to win the mining competition. In any case, by *assumption #1,* mining pools would be of equal size, meaning that independence assumption would still hold

$$t_i \sim \text{Gamma}(K, x_i).$$

As for the case of stochastic Poisson process, we will need some further explanation about the gamma distribution and, most importantly, why it is the distribution of the time t_i it takes for player's technology to compute K computation.

2.3 GAMMA DISTRIBUTION

The gamma distribution is a two parameter probability distribution that is used to estimate reliance, survival and duration models, which is the use we will make of it in this case.

In our model we claim t_i has a gamma distribution characterized by parameters K>0 and x_i>0 (respectively the distribution's scale and the shape parameters), that its probability density function (PDF) $\gamma_{k,x_i}(t)$ is

$$\gamma_{k,x_i}(t) = \frac{t^{K-1}}{\Gamma(K)} x_i^K e^{-x_i t} \tag{4}$$

where Γ is the Euler gamma function

$$\Gamma(y) = \int_0^\infty t^{y-1} e^{-t} dt, \;\; y > 0$$

Among Euler gamma function's properties, the most important is that for every y>0, $\Gamma(y+1) = y\Gamma(y) \;\; and \;\; \Gamma(1) = 1$. Thus in particular Γ(k) = $(k-1)!$ whenever k is a positive integer; as a consequence we also have

1) $\frac{\Gamma(K)}{x_i^K} = \int_0^\infty t_i^{K-1} e^{-x_i t_i} dt \;\; \forall\, x_i > 0, \forall\, K \geq 1$
2) As it can be easily shown, the integral from zero to infinite of $\gamma_{k,x_i}(t_i)$ is equal to 1, so that $\gamma_{k,x_i}$is indeed a PDF for every $K \geq 1$ and every $x_i > 0$:

$$\int_0^\infty \gamma_{k,x_i}(t_i) dt = \int_0^\infty \frac{t_i^{K-1}}{\Gamma(K)} x_i^K e^{-x_i t_i} dt \;\; = \frac{x_i^K}{\Gamma(K)} \int_0^\infty t_i^{K-1} e^{-x_i t_i} dt = \frac{x_i^K}{\Gamma(K)} \frac{\Gamma(K)}{x_i^K} = 1$$

One important feature of t_i we can derive from the gamma distribution is its expected value, which depends on both the scale and the shape parameters, and that is found as follows.

Using formula (4) for the probability density function and general formula for the expected value of a random variable that has a density, we get:

$$E[t_i] = \int_0^\infty t \gamma_{k,x_i}(t)\, dt$$

$$= \int_0^\infty \frac{t^{K-1}}{\Gamma(K)} x_i^K e^{-x_i t}\, dt$$

$$= \frac{x_i^K}{\Gamma(\mathrm{K})} \int_0^\infty t^K e^{-x_i t}\, dt$$

Then we use an auxiliary variable $w = x_i t$ to obtain

$$E[t_i] = \frac{x_i^K}{\Gamma(\mathrm{K})} \int_0^\infty \left(\frac{w}{x_i}\right)^K e^{-w} \frac{dw}{x_i}$$

$$= \frac{x_i^K}{x_i^{k+1}\Gamma(\mathrm{K})} \int_0^\infty w^K e^{-w}\, dw$$

Using firstly the definition of gamma function and successively properties 2) and 1)

$$E[t_i] = \frac{\Gamma(\mathrm{K}+1)}{x_i \Gamma(\mathrm{K})} = \frac{\mathrm{K}\,\Gamma(\mathrm{K})}{x_i\,\Gamma(\mathrm{K})}.$$

We conclude that

$$E[t_i] = \frac{K}{x_i} \quad . \tag{5}$$

The main deduction we take from studying the gamma distribution of the random variable t_i, that represents the time it takes for miner *i* to complete K computations, is that its expected value is the ratio between K and the technology x_i that miner *i* choose to use, thus we deduce that the probability of a miner to perform computations in an arbitrary amount of time in positively correlated to miner's technology x_i.

Using properties of the Gamma distribution we can also measure the probability that a certain player is the first miner to complete K computations, meaning that he wins the mining game and gets the reward P.

Player *i* is said to win the game if

$$t_i < t_j \quad \forall \quad j \neq i$$

So, if we define W_i as the set of time realizations in which player *i* is the winner of the game,

$$W_i = \{\, t \in R_+^N : t_i < t_j, for\ all\ j \neq i\}, \quad W_i \subseteq \mathrm{R}_+^N,$$

and if we assume that the strategy profile (x_i, x_{-i}) [5] represents the choices of all the miners, we can use the cumulative density function of the minimum order statistic of the gamma distribution to calculate the probability (π) that player *i* wins, defined as

$$\pi(W_i; K, x_i, x_{-i}) \coloneqq P(t \in W_i)$$

[5] (x_i, x_{-i}) will be used from now on to describe the strategies of all the players, where x_i represents the strategy of player *i* and x_{-i} represents the strategies of all the other players

To compute it we use the cumulative distribution functions $F_i(s)$ of the independent random variables $t_1, t_2, \dots, t_N$.

$$F_i(s) = P(t_i < s) = \int_0^s \gamma_{K,x_i}(r)dr$$

Let T = $min(t_2, t_3, \dots, t_N)$; the probability that t_i is the shortest time span in the network is

$$\pi(W_i; K, x_i, x_{-i}) = P(T \geq t_i) = P\left(t_j \geq t_i \ \forall j \neq i\right)$$

From now on, we will proceed in the analysis in two ways: firstly we will make a rigorous model to represent it, then we will make the second model that uses some simplificationsto state an easier and reliable model we will use while analyzing the mining game.

2.4 RIGOROUS MODEL

The background material for this and the next parts can be found in Patrick Billingsley, Probability and Measure - Anniversary Edition (2012), Wiley.

As we know that time t_i follows a Gamma distribution, then the probability that time t_i for a player i is higher that a certain value y is

$$P(t_l > y) = \int_y^{+\infty} \gamma_{k,x_l}(s)ds$$

With the same reasoning we calculate the probability that every player, except i, takes a computing time t higher than y:

$$P(t_l > y \ \forall \ l \neq i) = \prod_{l \neq i} \int_y^{+\infty} \gamma_{k,x_l}(s)ds = \prod_{l \neq i} \frac{x_l^K}{(k-1)!} \int_y^{+\infty} s^{k-1} e^{-x_l s} ds$$

where $\int_y^{+\infty} s^{k-1} e^{-x_l s} ds = e^{-x_l s} P_{k,x_l}(y)$ and $P_{k,x_l}(y)$ is a polynomial of degree k-1 that is found through integration by parts, depends on K and x_l and whose coefficient attached to y^{k-1} is positive

$$P(t_l > y \ \forall \ l \neq i) = \frac{1}{[(k-1)!]^{N-1}} \prod_{l \neq i} x_l^K e^{-\sum_{l \neq i} x_l y} \prod_{l \neq i} P_{k,x_l}(y)$$

For simplicity, we denote $P(t_l > y \ \forall \ l \neq i)$ as H(y).

Now we switch the generic value y with a given computing time for player i, namely t_i

$$P(t_l > y \,\forall\, l \neq i \mid t_i = y) = P(t_l > t_i \,\forall\, l \neq i \mid t_i) = H(t_i)$$

and therefore

$$P(t_l > t_i \,\forall i) = E[H(t_i)] = \int_0^{+\infty} H(s)\gamma_{k,x_l}(s)ds$$

Through integration by parts we calculate that

$$P(t_l > t_i \,\forall i) = \frac{\prod_l x_l^k}{[(k-1)!]^n} \int_0^{+\infty} e^{-\sum_l x_l^s} \tilde{P}(s)ds \quad where \quad \tilde{P}(s) = s^{k-1} \prod_{l \neq i} P_{k,x_l}(s) \tag{6}$$

Formula (6) is the rigorous version of probability $\varphi(W_i, x_i, x_{-i}, K)$, it is way too complicated to be used in our future game theory analysis of the mining game; however, from it, we deduce that for high x_i it will be an increasing function. The latter means that if one player has a big enough computing capacity, a further increase in its technology will increase its probability of winning the mining game.

Now we will show a simplified model and we will show analytically that the property about the rigorous model, mentioned in the last paragraph, will still hold.

2.5 SIMPLIFIED MODEL

Assumption #3: $E[t_i]$ derived from Gamma distribution of t_i is considered a good proxy for the computing time t_i.

Under assumption #3 player 1 completes K computations at time $E[t_i]$.

The probability that player 1 will win the computing race is, by independence,

$$\pi(W_1; K, x_1, x_{-1}) = P(T > E[t_1]) = P(t_2 > E[t_1], t_3 > E[t_1], \dots, t_N > E[t_1])$$

$$= P(t_2 > E[t_1])\, P(t_3 > E[t_1]) \dots . P(t_N > E[t_1])$$

$$= [1 - F_2(E[t_1])][1 - F_3(E[t_1])] \dots . [1 - F_N(E[t_1])]$$

$$= \prod_{i=2}^{N} [1 - F_i(E[t_1])]$$

And if we assume all the miners to have a symmetric computing technology we arrive to

$$\pi(W_1; K, x_1, x_{-1}) = [1 - F_i(E[t_1])]^{N-1} \quad (7)$$

The quantity $\pi(W_i; K, x_i, x_{-i})$ is pivotal in the study of the mining game that leads to find an internal Nash equilibrium, because it will be largely used from now on to describe the payoff function of each miner and, consequently, miners' best response functions.

Miner *i* payoff will be

$$U_i(x_i) = P\pi(W_i; K, x_i, x_{-i}) - c(x_i) = E(P) - c(x_i); \quad (8)$$

note that player *i* can maximize its payoff only changing its technology choice x_i. The next step to do is to understand whether there is a common pattern of behavior, namely an internal Nash equilibrium, that characterizes the network of miners.

2.6 ANALYSIS OF THE MINING GAME

Bitcoin mining process consists in subsequent rounds, that last 10 minutes, in which N miners compete to be the first to solve a certain computational puzzle that has complexity K. To better analyze the whole process and to find a consistent Nash equilibrium, it is useful to divide the mining game into two parts: a stage game that represents a single round of the mining process and a dynamic game that takes into account the sequence of mining rounds and the adjustment that both the miners and the network can make to change the outcome of the game.

2.7 STAGE GAME

Firstly, we analyze the stage game component of the mining process. In this context the computation difficulty K is fixed and miners have no impact on it; the only variable feature of these games is the technology choice of miners. We will show that there exists a unique Nash equilibrium in the technology choice in every round and that it is also symmetric for each player.

Definition: A Nash equilibrium is a mining game's outcome supported by a strategy $\boldsymbol{x}^* = (x_1^*, x_2^*, \dots, x_N^*)$ such that for each player $i = 1, 2, \dots, N$ no player has incentive to deviate by choosing a different $x_i \neq x_i^*$ assuming that the other players keep their strategies fixed:

$$U_i(x^*) \geq U_i(x_i, x_{-i}^*)$$

In the mining game, the Nash equilibrium is a strategy profile $\boldsymbol{x}^* = (x_1^*, x_2^*, \dots, x_N^*)$ which, given a computing difficulty K, represents the technology choices of each miner $i = 1, 2, \dots, N$ and guarantees that

1) for all players $i = 1, 2, \dots, N \quad U_i(x_i^*, x_{-1}^*) \geq U_i(x_i, x_{-1}^*) \quad \forall\, x_i > 0$

2) The expected required time to solve the computational puzzle given $\mathbf{x}^*$ is $\delta_K \in R_+$, where

$$\delta_K = E_K(\min\{t_1, t_2, \dots, t_N\}|K)$$

Definition: A symmetric equilibrium is a Nash equilibrium in which each player $i = 1, 2, \dots, N$ has the same utility maximizing strategy **x***.

In the mining game, a symmetric equilibrium is a triplet (δ^*, K^*, x^*) such that

1) x* is a Nash equilibrium (in the sense of the previous definition) for the difficulty threshold K*

2) The expected time of completion δ^* is equal to the target solution time set by the network, which for Bitcoin is 10 minutes.

To prove that there exists a interior Nash equilibrium x^* in the mining game, there are two conditions to be met:

condition 1:

$$\frac{\partial U_i(x)}{\partial x_i} = P\,\frac{\partial \pi(W_i;K,x^*)}{\partial x_i} - \frac{\partial c(x^*)}{\partial x_i} = 0 \qquad \forall\, i$$

condition 2:

$$\frac{\partial^2 U_i(x^*)}{\partial x_i^2} = P\,\frac{\partial^2 \pi(W_i;K,x^*)}{\partial x_i^2} - \frac{\partial^2 c(x^*)}{\partial x_i^2} < 0 \qquad \forall\ i$$

These two conditions attest that that the Utility function of player *i* is maximized by the strategy x^*, so that no player *i* has an incentive to deviate from x^*. However, it is not a straight-forward procedure to prove that both condition 1 and 2 are satisfied, so we will introduce some theorems that allow us to show that the conditions are met.

Theorem 1. *Holding other players' technologies fixed at x_{-i}, the probability that player i wins increases with x_i.*

PROOF. If all the players are able to choose the technology of they prefer, the probability that player i=1 wins is

$$\pi(W_1; K, x_1, x_{-1}) = \prod_{j\neq 1}(1 - F_j(x))$$

Therefore, differentiating it with respect to x_1 we get

$$\frac{\partial \pi}{\partial x_1} = \frac{\partial \pi}{\partial x}\frac{\partial x}{\partial x_1} = -\frac{K}{x_1^2}\frac{\partial \prod_{j\neq 1}\left(1-F_j(x)\right)}{\partial x},$$

where

$$\frac{\partial \prod_{j\neq 1}\left(1 - F_j(x)\right)}{\partial x}$$

$$= \left(\frac{\partial}{\partial x}\left(1 - F_2(x)\right)\right)\prod\nolimits_{j\neq 1,2}(1 - F_j(x)) + \left(1 - F_2(x)\right)\frac{\partial}{\partial x}\prod\nolimits_{j\neq 1,2}(1 - F_j(x))$$

$$= -f_2(x)\ \prod_{j\neq 1,2}(1 - F_j(x)) + \left(1 - F_2(x)\right)\frac{\partial}{\partial x}\prod_{j\neq 1,2}(1 - F_j(x))$$

The first term of the sum is clearly negative, and by repeating the same scheme we can easily understand that all terms of this last derivative are negative (possibly arguing rigorously by induction). Since this negative term has is multiplied by $-\frac{K}{x_1^2}$, the derivative of π with respect to x_1 is positive.

Instead, assuming that all the players choose a symmetric strategy, if we differentiate the probability of winning with respect to x_i and, by formulas (5) and (6), we find

$$\frac{\partial \pi(W_i; K, x_i, x_{-i})}{\partial x_i} = \frac{\partial \pi(W_i; K, x_i, x_{-i})}{\partial E(t_i)}\frac{\partial E(t_i)}{\partial x_i}$$

$$= \frac{\partial([1-F(E[t_i])]^{N-1})}{\partial E(t_i)}\left(-\frac{k}{x_i^2}\right)$$

$$\frac{\partial \pi}{\partial E(t_i)} = -(N-1)f(E[t_i])[1 - F(E[t_i])]^{N-2}\left(\frac{k}{x_i^2}\right)$$

Noting that the factors in the last line of are all positive, we can assess that the first derivative of π with respect to x_i will surely be strictly positive and validate hypothesis 1.

However, when N≥2, the probability of player i winning will never reach 1 (no technology will guarantee winning the race). This is due to the fact that proof-of-work seen as a random process, so,

even though greater computing technology will decrease expected t_i, there is no certainty that the player with the best technology will win, no matter how much computing power he uses.

$$\pi(W_i; K, x_i, x_{-i}) < 1 \quad for\ all\ x_i, if\ N \geq 2$$

Theorem 2. *Holding other players' technologies fixed at x_{-i}, the probability that player i wins increases with x_i at a decreasing rate if x_i is large enough.*

PROOF. Again we choose i=1 for simplicity. Differentiating 2 times the probability π with respect to x_1 we get

$$\frac{\partial^2 \pi}{\partial x_1^2} = -\frac{\partial}{\partial x_1}\left(\frac{K}{x_1^2}\frac{\partial}{\partial x}\prod_{j\neq 1}\left(1 - F_j(x)\right)\right)$$

$$= \frac{2K}{x_1^3}\frac{\partial}{\partial x}\prod_{j\neq 1}\left(1 - F_j(x)\right) - \frac{K}{x_1^2}\frac{\partial}{\partial x_1}\frac{\partial}{\partial x}\prod_{j\neq 1}\left(1 - F_j(x)\right)$$

The sign of $\frac{\partial^2 \pi}{\partial x_1^2}$ is ambiguous and depends on the relative magnitude of the two summands in the last line. However the function can change sign only finitely many times (because its derivative is continuous and has finitely any zeroes, that are determined by the derivatives of the gamma density functions, which are all monotone for large *x* and are finitely many), so it must have definitively a constant sign. As π is a probability, it cannot be definitively convex, thus it must be concave, meaning that $\frac{\partial^2 \pi}{\partial x_1^2} < 0$ for *x* large enough

Having proved that the probability that player i wins increases with his/her technology choice x_i at a decreasing rate for large enough x_i, we can now discuss whether there exists a Nash equilibrium solution $x^* > 0$ that maximizes the payoff function $U_i(x_i) = P\pi(W_i; K, x_i, x_{-i}) - c(x_i) = E(P) - c(x_i)$, being $U_i(x) \geq 0$ for some $x > 0$.

As we said at the beginning of the stage game study, to have an interior Nash equilibrium at x^* there are two conditions to be met:

$\frac{\partial U_i(x^*)}{\partial x_i} = P\frac{\partial \pi(W_i;K,x^*)}{\partial x_i} - \frac{\partial c(x^*)}{\partial x_i} = 0 \qquad \forall\, i$ condition 1

We now know that this equation in feasible because the first term is positive by Hypothesis 1 while the second term is positive and strictly convex in x_i by assumption of the cost function.

Consequently there exists at least one point x* in which $\frac{\partial U_i(x^*)}{\partial x_i} = 0$

The second condition to be satisfied is

$$\frac{\partial^2 U_i(x^*)}{\partial x_i^2} = P\frac{\partial^2 \pi(W_i;K,x^*)}{\partial x_i^2} - \frac{\partial^2 c(x^*)}{\partial x_i^2} < 0 \qquad \forall\ i \qquad \text{condition 2}$$

This inequality holds by **theorem 2** if x_i is large enough; some calculations in easy cases suggest that x_i should be larger than $\sqrt{K}$, and that there exists points larger than $\sqrt{K}$ that satisfy condition 1. Therefore we will assume that both conditions are satisfied by at least one point.

Conditions 1 & 2 together prove that there exists an interior Nash equilibrium solution **x***, which is unique and maximize each players' payoff function.

We can now generalize and say that, keeping the number of miners fixed, in each stage of the Bitcoin mining game there is a unique interior Nash equilibrium $\boldsymbol{x}^* = (x_1^*, x_2^*, \dots, x_N^*)$, associated with Payoff $U_i(x^*) = 0$ and cost $c(x^*) > 0$, for every level of computational difficulty K and that each Nash equilibrium (K, x*) gives a unique expected time for completion of the computational puzzle that we will note as δ_K, whose value, according to the Gamma distribution of t, is $\delta_K = \frac{K}{Max(\boldsymbol{x}^*)}$.

2.8 DYNAMIC GAME

Taking into account a sequence of stage games, it seems obvious that, in the long run, players could be incentivized to invest and improve their computing technology to increase their chances to win future mining races. This would lead to the decrease of the computing time below the target time δ^* that the network wants to achieve on average. The network, on the other hand, has the possibility to adjusts the difficulty level K once every 2016 rounds to make sure that the puzzle is computed in the target time, meaning that the network increases K if, during the previous period, the puzzle has been solved in a time that is less than δ^*, while it may reduce K if the opposite happens.

The fact that the network affects the duration of the rounds through adjustments of the difficulty level of computing is pretty intuitive; in fact, as $E[t_i] = \frac{K}{x_i}$ (see (3)), the more computations are needed to resolve the puzzle, the more time miners will need on average to solve it, however, the positive correlation between δ_K and K can be also proved more formally through the cumulative density function of the Gamma distribution.

Theorem 3*: other things being equal, the expected time δ_K to complete the proof-of-work is strictly monotonically increasing with respect to the difficulty level K*

Proof. The statement for the real-world mining procedure follows heuristically from how the procedure works, as commented on in Nakamoto (2008).

To show that this is true also in our model we compute

$$\delta_K = E(\min\{t_1, t_2, \dots, t_n\} | K)$$

Let $F_T(s)$ be the cumulative distribution function of the random variable $T = \min\{t_1, t_2, \dots, t_n\}$. Suppose that all players choose the same technology *x*; we have

$$\begin{aligned} F_T(s) &= P(T \leq s) = 1 - P(T > s) \\ &= 1 - P(t_1 > s, \dots, t_N > s) \\ &= 1 - P(t_1 > s) \dots P(t_N > s) \\ &= 1 - P(t_1 > s)^N \\ &= 1 - [1 - F(s)]^N \end{aligned}$$

because the random variables t_i are independent and identically distributed with distribution Gamma(K, *x*).

Differentiating with respect to *s* we obtain the density function of T:

$$f_T(s) = \frac{\partial}{\partial s} F_T(s) = N([1 - F(s)]^{N-1} \gamma_{k,x_i}(s)$$

Therefore

$$\begin{aligned} \delta_K &= \int_0^\infty s f_T(s) ds = N \int_0^\infty [1 - F(s)]^{N-1} s \gamma_{k,x_i}(s) ds \\ &= N \frac{x^{NK}}{\Gamma(\mathrm{K})^N} \int_0^\infty \left[\int_0^\infty r^{K-1} e^{-xr} dr \right]^{N-1} s^K e^{-xs} ds \end{aligned}$$

It is possible to verify that the derivative of δ_K with respect to K is strictly positive.

If the random variable t_i are not identically distributed but $t_i \sim$ Gamma (K, x_i), we can easily show that

$$f_T(s) = \sum_{j=1}^{N} f_j(s) \prod_{l \neq j} (1 - F_l(s)),$$

Thus the sign of the derivative of δ_K can be studied and will be positive.

By this study we can infer that, whenever the network increases the computation difficulty K to maintain the target puzzle solution time, assuming a fixed number N of miners, there is a deviation from the Nash equilibrium. This deviation gives to individual miners the possibility to increase their chances to win the mining race by improving the technology they use.

Now, having proved that a there exists at least one Nash equilibrium in the mining game and having characterized how both the players and the server behave after a change in the puzzle difficulty, we will make some further inferences about the mining game.

First of all we state that Nash equilibrium technology choices increase as the difficulty level K increases.

Assuming that the game features a symmetric Nash equilibrium $\boldsymbol{x}^* = (x_1^*, x_2^*, \dots, x_N^*)$ and a constant K degree of difficulty, then expected solution time is δ^* and the probability of winning the mining race is homogeneously distributed among N miners.

If this static equilibrium situation is changed by the network that increases the difficulty level from K to K+ε, where ε>0, in the short run the miners will not be able to change their technology choice, that remains constant at x^* for a certain span of time, meaning that, until they change their strategy, the expected solution time will be lower than δ^* and the probability to win will be constant for each miner even if the difficulty level has been increased.

However, as miners have the possibility to increase their winning probability without incurring in further increase in difficulty, they will logically increase their technology choice as soon as they can and they will do so until the equilibrium time solution δ^* for the puzzle is reached.

Secondly we state that for a given number N of miners and a fixed target solution time δ^*, there exists a unique symmetric Nash equilibrium (K^*, x^*).

Indeed, from formula (5) we know that $E_k(t)$ is strictly increasing over K, thus there is a unique K, namely K^*, for which $E_{K^*}(t) = \delta^*$. We know from the study about the stage game that, for each computational difficulty K and fixed number N of player, there exists a unique interior Nash equilibrium $x^* = (x_1^*, x_2^*, \dots, x_N^*)$, so if we fix $K = K^*$ we can infer that the couple (K^*, x^*) represents the equilibrium situation of the dynamic game that has a given target solution time of δ^*. Both the server and miners are satisfied by the triplet (δ^*, K^*, x^*) because the former is sure to have $E_{K^*}(t) = \delta^*$ and the latter have their utilities $U_i(x_i) = E_i(P) - c(x_i)$ maximized (see condition 1 of stage game N. E.).

Assuming that the prize P and the number of miners N are fixed, then $E_i(P) = \frac{P}{N}$. Therefore miners will earn positive profits if their technology's cost does not exceed the expected payoff:

$E_i(P) > c(x^*)$;

since the cost function is strictly increasing over K, we can say that miners will have positive profit (utility function) for N low or P high

$$x^* < c^{-1}\left(\frac{P}{N}\right)$$

2.9 FREE ENTRY

As stated by the previous paragraph, the number of participants in the mining game is a key determinant for the choice of mining technology. This feature is very important in our study

because in the Bitcoin mining protocol there are no boundaries that restrain individuals from becoming miners (free entry), thus anyone could start to take part of mining races and affect the choices of all the incumbent players.

We analyze heuristically some consequences of free the entry. We will start by examining the long-run outcomes of the game when N in endogenous. In this case, all the miners choose the same technology x^* and consequently all the miners have the same probability to win the prize

$$\pi(W_i; K, x^*) = \frac{1}{N} \qquad \forall\, i$$

Allowing free entry in the game, players will enter the competition as long as their expected profits are positive and exit the competition whenever their expected profits are negative:

Player i will enter if $U_i(x^*) = \frac{P}{N} - c(x^*) > 0$

Player i will exit if $U_i(x^*) = \frac{P}{N} - c(x^*) < 0$

These strategies will succeed one another and, assuming no entry or exit cost, in the long run they will balance themselves, leading to an equilibrium similar to the one we can observe in perfect competitive markets. In this equilibrium the players are indifferent between entering and exiting the competition because no profit is expected to be made by incumbent miners and consequently no possible new entrant will have the incentives to start competing in the game:

$$U_i(x^*) = \frac{P}{N} - c(x^*) = 0 \tag{9}$$

where x^* is the solution for all *i* to the maximization problem presented in condition 1 of the stage game Nash equilibrium.

Theorem 4: *assuming the game is in an equilibrium, assuming P is fixed and allowing free entry, the fierce competition will drive up the social cost of mining until it equalizes the prize:*

$$P = c(x^*)N$$

PROOF: Miners will enter the game if and only if $P > Nc(x)$ and they will use the same optimal technology that incumbent miners chose in the previous period: $x_{i,t+1} = x^*_{i,t}$; this will lead to an increase in social cost: $N_{t+1}c(x^*_t) > N_t c(x^*_t)$. Since aggregate technology has increased in *t+1*, the average computing time will decrease leading to $\delta_{t+1} < \delta^*$. The average computing time will continue to decrease as long as miners keep entering the game, but at this point the network will adjust the computing difficulty K to regulate the game back to an average computing time δ^*. This increase of K will lead the miners to increase their technology, subsequently raising the aggregate cost of technology. This process continues until the aggregate cost of technology equals the outcome P, meaning that free entry number of miners is reached.

Social cost is then solely dependent on the prize and independent from market structure, while the technology choice of each miner also depends on the competition: it decreases with an increase in N (which is a proxy for competition) and vice versa. To prove this we find that equilibrium technology is $x^* = c^{-1}\left(\frac{P}{N}\right)$ and then we differentiate it with respect to N, having in mind that $c'(.) > 0$ by assumption, so that $(c^{-1})'(.) > 0$, we find

$$\frac{\partial x^*}{\partial N} = \frac{\delta c^{-1}\left(\frac{P}{N}\right)}{\delta \frac{P}{N}} \frac{\partial \frac{P}{N}}{\partial N} = \frac{\partial c^{-1}\left(\frac{P}{N}\right)}{\partial \frac{P}{N}}\left(-\frac{P}{N^2}\right) < 0 \qquad (10)$$

The previous result shows that the incentives to use better technology decrease with increased competition in the network. In fact, if more miners enter the game, the possibility for each one of them to win diminishes, causing a decrease in individual expected value of winning, leading to a decrease in investments for mining technology.

Interestingly, we notice that global resource usage is not affected by the computational difficulty, that is a mere tool that the network uses to maintain the computational time as close to δ^* as possible, but these costs are only driven by P. Indeed, if the targeted block time was reduced to $\delta^{**} < \delta^*$ by the network, K would be increased but the resources used to compete in the mining game would be constant and their costs would be equal to P as long as P remains unchanged. In this case the miners would choose technology $x^* = c^{-1}\left(\frac{P}{N}\right)$ for each round, leading to an increased resource use per unit of time.

We can now infer that once the network reaches a dynamic game equilibrium (K^*, x^*), there are zero expected profits and miners are indifferent between entering and exiting the mining race;

Theorem 5*: it is logical now to think that any deviation from* (K^*, x^*) *will depend on a change in P.*

Proof. We differentiate the previous result $x^* = c^{-1}\left(\frac{P}{N}\right)$ with respect to P, having in mind that N is constant and $(c^{-1})'(.) > 0$

$$\frac{\partial x^*}{\partial P} = \frac{\delta c^{-1}\left(\frac{P}{N}\right)}{\delta \frac{P}{N}} \frac{\partial \frac{P}{N}}{\partial P} = \frac{\partial c^{-1}\left(\frac{P}{N}\right)}{\partial \frac{P}{N}}\left(\frac{1}{N}\right) > 0$$

From this inequality we understand that $x^*$is strictly increasing in P. From formula (5) we also come to the conclusion that equilibrium K and x are connected by the equation $K = E[t_i]x_i$, so we can affirm that K is increasing in P through x.

Now that it is clear that the social cost of mining depends on the expected value of the prize, it is worth specifying some features about the prize and how those will affect the total investments in computational power.

1) The amount of newly minted bitcoins that is given out as prize halves every 210,000 verified blocks, until it becomes null when the threshold supply of all 21 million bitcoins is reached. When the prize halves, if the difference isn't compensated by higher fees or exchange rate, the short run profits go below zero, giving the miners no other choice than decreasing their computing technology or exiting the game. Other things being equal, the network becomes less resource consuming as amount of bitcoin given out decreases.
2) Absent any other change in P, whenever the bitcoin exchange rate appreciates, the prize increases because the amount of newly minted bitcoin given out increases in value. When such an appreciation happens, miners cannot increase their technology immediately, and there are positive profits in the short run, while they will adjust in the long run and equilibrium technology and cost will increase. In this case the puzzle completion time decreases until the moment in which the network can increase the difficulty to maintain time δ^* . The difficulty level of the puzzle is logically positively correlated with bitcoin exchange rate as it appears from historical data; in fact bitcoin's exchange rate has had some huge blasts and, simultaneously, the difficulty level increased significantly.
3) Even if Bitcoin do not appreciate with respect to the dollar in the short run, if in the future it will be used as a common payment system, its exchange rate would increase by a huge proportion. This possibility gives incentives to miners to invest more in the present even if temporarily it is not a profitable strategy. Thus, speculation about Bitcoin's future value creates the presupposition for miners to invest more than they logically would and increases social costs.

2.10 WELFARE ANALYSIS

The bitcoin protocol was designed by Nakamoto (2008) to be a decentralized ledger for transaction in which anybody could become a node and/or a miner. The openness of the system has some benefits and some negative aspects: it is seen as a virtue because it increases the security and the robustness of the network, but it also contributes to the social cost of the network.
To prove the latter we study how the behavior of both aggregate equilibrium technology, Nx^*, and aggregate equilibrium cost, $Nc(x^*)$, changes as the number of miners increases.

Since $x^* = c^{-1}\left(\frac{P}{N}\right)$, the aggregate level of technology is $Nx^* = Nc^{-1}\left(\frac{P}{N}\right)$.

We differentiate with respect to N

$$\frac{\partial Nx^*}{\partial N} = \frac{\partial Nc^{-1}\left(\frac{P}{N}\right)}{\partial N} = c^{-1}\left(\frac{P}{N}\right) - N\frac{P}{N^2}\frac{\partial c^{-1}\left(\frac{P}{N}\right)}{\partial N} = c^{-1}\left(\frac{P}{N}\right) - \frac{P}{N}\frac{\partial c^{-1}\left(\frac{P}{N}\right)}{\partial N}$$

and we notice that aggregate level of technology is positively correlated with the number of miners because:

1) $c^{-1}\left(\frac{P}{N}\right)$ is always positive by assumption
2) $\frac{\partial c^{-1}\left(\frac{P}{N}\right)}{\partial N} = \frac{\partial x^*}{\partial N} < 0$ because of increased competition (see (10))

Starting from an equilibrium situation (K^*, x^*) with N miners, if at any stage of the game there is a set of miners that enters, then the network finds a new equilibrium at (K'^*, x'^*) for the number of miners N', and this equilibrium implies an increase[6] in aggregate level of technology, $N'x'^* > Nx^*$, which cannot be prevented by an adjustment of K because the latter is only a tool used to determine the round length δ.

Instead, if a set of miners exits the game, then the aggregate level of technology decreases as well. Knowing that the bitcoin protocol needs at least one miner to be carried on, we infer that the most cost and resource efficient bitcoin protocol features a single miner trying to solve the computational puzzle. In fact, in this case the single miner is free of any competition and he is certain to win the mining race. In this context we will regard the single miner as monopolist and he will have a guaranteed payoff

$$U_m(x_m) = P - c(x_m),$$

since the difficulty adjustments made by the network depend only on his choices, not only he will choose the minimum amount of technology required to solve the puzzle, but he will also influence the dynamic difficulty of the puzzle until it adjusts the minimum difficulty is reached, namely K=1.

If K=1 and target time is δ^* , then we find the equilibrium strategy for the monopolist from

$$\delta_1^* = E_1(t) = \frac{1}{x_m} \quad \rightarrow \quad x_m^* = \frac{1}{\delta_1^*}$$

Here, assuming a monopolist controls the whole mining network, x_m^* and its associated cost $c(x_m^*)$ represent respectively the aggregate technology and the aggregate cost.

The outcome we have just presented could realistically just need a laptop to operate, just as Nakamoto envisioned while writing its white paper, and it would avoid global costs and expenses in

[6] Because *c(.)* is convex and increasing in *x*

the order of billions of dollars annually, saving enormous quantities of electricity. However, free entry prevents this outcome because a monopolistic miner wouldn't ensure the security and soundness the Bitcoin needs to carry out transactions.

It is now worth noting that a monopolistic miner would have few if any interests to undermine the network he/she governs: first of all, he would not be able to expropriate others of their own currency and/or wealth, secondly even if he could double or multi-spend[7] the currency he already owns, he/she would do it at its own network's expenses: as multi-spending would be publicly visible in the blockchain, economic agents would stop demanding transaction validation to the network and in this case the monopolist would see its future returns vanish because of the low value of the currency and the low amount of transaction fees.

From this perspective, if a trusted third party, i.e. ECB, governments, had monopolistic power over the bitcoin protocol, it would have few if any incentive to misconduct in its own network and would run it with a very low requirement for technology and energy. However, such a situation has never happened, and the real benefits and disadvantages are all yet to be studied.

[7] Use the same money to pay for multiple transactions

3. IMPLICATIONS OF MINING GAME NASH EQUILIBRIUM

Now, having studied the Bitcoin mining game from an analytical point of view, we will make some considerations regarding the real world implications that stem from mining activity.
We will focus on hardware and energetic needs of the cryptocurrency's network following "Renewable Energy Will Not Solve Bitcoin's Sustainability Problem" by Alex de Vries,"A critical assessment of the Bitcoin mining industry, gold production industry, the legacy banking system, and the production of physical currency" by Hass McCook, and we will take data from Cambridge Bitcoin Electricity Consumption Index (https://cbeci.org/) and blockchair.com.

3.1 OVERVIEW

So far, we have analyzed many features of the Bitcoin mining game using both a rigorous model and a simplified one. Assuming that the results of the simplified model hold for the rigorous model as well, we proved that miners, incentivized by monetary prizes and free entry of Bitcoin protocol, have interests in investing great amounts of capital to run computing technology that enables them to validate Bitcoin transactions in the blockchain. The same aforementioned investments take place in three main ways:

1) Acquisition of specialized pieces of hardware that are used to mine (Application-Specific Integrated Circuits (ASICs))
2) Payments for energy used to run the mining hardware
3) Additional payments made in order to maintain and sustain mining activity, i.e. rent for a physical place where hardware can be placed, cooling system that helps ASICs running and prevent them from wearing out

Even if those investments are extremely fruitful for whoever intends to make profit out of the mining activity, they do not come without any downside effect and, among those, we will focus on the two most important issues that originate environment concern: electronic waste and energy consumption.

3.2 ELECTRONIC WASTE

At the beginnings of Bitcoin, mining could be carried out by simple personal computers that used their central processing units (CPUs) to solve the SHA-256 function because the competition on the

network was very low; as the monetary prize of Bitcoin mining increased, competition increased as well following the rationale that the more computational efficient a node is the more profitable it will be, thus, miners started changing periodically their Proof-of-Work solving hardware firstly passing to graphic processing units (GPUs), then to field programmable gate arrays (FPGAs) and finally, around 2013, they started using application-specific integrated circuits (ASICs).

All of these subsequent mining technology changes led every rational agent to shut down their least efficient machines once the associated expected profit (expected payoff minus running costs) fell below zero; nowadays all the CPUs, GPUs and FPGAs previously used for mining have been dismissed or reused for different purposes.

On the other hand, ASICs are pieces of hardware that, unlike their mining hardware predecessors, are engineered to perform only one type of calculation (solving the SHA-256 function) and do it in the most efficient way. This means that they were created with no purpose other than Bitcoin mining, so, if they stop being profitable for this specific usage, they immediately become electronic waste (e-waste).

There is no way to determine the exact amount of e-waste generated by Bitcoin network, but, since we can estimate its total computational power, we are able to model the quantity of mining equipment in the network and also the rate at which this equipment becomes obsolete.

At its peak, during October 2018, the Bitcoin network computing capacity was estimated at 54.7 exahashes per second (data from bitcoinenergyconsumption.com), an amount that would require at least 3.91 million Antminer S9 machines (the most efficient ASIC of that time) to be computed, all of that hardware can be translated into a combined weight whose lower bound[8] is 16,442 metric tons; applying Koomey's law[9] to ASICs and following the observation that only the most cost-efficient machines can remain economically viable for mining, we can infer that in April 2020, all of the mining machines that were used in October 2018 have been dismissed and amounted to a minimum of 10,961 metric tons of electronic waste per year. Taking into consideration the number of transaction processed by Bitcoin network in 2018, that amounts to 81.4 millions according to blockchair.com, we find that, in that period, bitcoin generated an estimated 0.135 kilograms of e-waste per transaction.

Putting these numbers in context, the annual amount of e-waste is comparable to the one generated by a little country such as Luxembourg (12 metric tons per year) and the average e-waste footprint

[8] Its regarded as a lower bound because the Antminer S9 had the least weight to computational power ratio at that time

[9] It states that the electrical efficiency of computing will double every 1.5 year. This law has been backed by empirical evidence since 1950'

per transaction is almost equal to the one generated by four standard 60 W light bulbs (136 grams). Moreover, if we want to make a comparison with the classical banking sector, Visa's estimated average e-waste footprint per transaction is equal to 0.0045 grams (data taken from *World payments report 2018,* BNP Paribas), which is an amount 100.000 times lower than Bitcoin's and that could put into question the whole cryptocurrency.

3.3 ENERGY CONSUMPTION

All of the mining machines, being CPUs, GPUs or ASICs, require a certain amount of electricity to generate hashes and compete in the mining race. Measuring the total energy consumption of the Bitcoin network is impossible because, as we have already stated, there is no way to know how many miners are active in the network, nonetheless, it's possible to estimate it using the total computational power in the network or the mining reward possibly won by miners.
Those two methods are deeply explained in the Bitcoin Energy Consumption Index (BECI) everyone can find in the site bitcoinenergyconsumption.com.
Using the latest site's estimations, which are periodically updated, the amount of energy used to run the whole Bitcoin network's mining hardware for a year is 123.09 TWh and the consumption per transaction is 1,546.71 kWh (as of June 2021). Once again, if we want to put into context these numbers, we can compare them to the electric consumption of whole countries, in fact, if Bitcoin were a country, it would be the 32nd most electricity consuming in the world, above nations such as Netherlands and Pakistan.
Instead, if we want to compare the cryptocurrency to the classical baking system, an estimation made by the civil engineer Hass McCook comes in handy as it states that the entire banking sector, including data centers that process transaction, branches and ATMs, consume as much as 650 TWh of electricity per year to process an estimated 482.6 billion non-cash transaction, leading to a 1.35 kWh consumption per transaction. Also in this case the classical banking system proves itself to be way more energy efficient than the Bitcoin network, and also in this case in the scale of a thousand times.

3.4 ENVIROMENTAL ISSUES

The greatest problem that stems from Bitcoin network's huge electricity requirement is the environmental impact, measured in CO2, caused by the energy supplier of miners.

To assess this matter in the best possible way, first of all we have to remember that miners in general are profit maximizer agents so, as the most cost-efficient machines are the ones that will generate the biggest profit, miners will locate their computing hardware in places capable of producing high quantities of electricity and where it is sold at a very cheap price. Because of this reasoning, Bitcoin enthusiast argue that the cryptocurrency's environmental impact is very limited, in fact they say that the majority of the mining is powered by electricity in surplus that would be otherwise wasted because it is produced in locations that have abundant renewable resources and very low demand for electricity.

Even if the latter hypothesis could seem pretty convincing at a first glance, especially if one thinks about its monetary implications, some further investigations about a Chinese region where mining is brought out in large scale, have proved it to be only partially truthful.

The aforementioned Chinese region is represented by Sichuan and Yunnan provinces; here, the mix of great hydropower resources and the lack of infrastructures that would allow exporting away the electricity produced leaves the region with a great abundance of hydropower generated electricity, which obviously attracts energy-hungry industries.

Among these industries we find Bitcoin mining that exploit this situation so much that estimates say that almost half of the global mining is currently conducted in this region. However, unlike power demanded for Bitcoin mining machines, which can suffer some sporadic fluctuations but is anyway consistent all year long, the supply of hydropower strictly relies on rain, floods and droughts, meaning that it is highly subject to seasonality and that it can leave the warehouses without the needed energy. These periodical shortages in hydroelectricity generation create a question over how to accommodate miners' energetic demand and the only feasible answer can be found in the environmentally impacting coal-generated electricity.

This particular case not only shall dismiss any possible belief about environmental neutrality of the Bitcoin protocol but it also opens a case about the CO2 emissions.

Once again we will rely on the Bitcoin Energy Consumption Index to assess the environmental impact of the cryptocurrency, in fact, according to it, Bitcoin's energetic needs in 2018 accounted for a carbon footprint estimated between 19 and 29.6 million metric tons of CO2, leading to an astonishing carbon footprint per transaction of 233.4 to 363.5 kg of CO2 that seems almost unreal if compared vis-a-vis with the 0.4 g of CO2 that is generated on average by a VISA transaction.

3.5 POSSIBLE SOLUTION

In recent days, maybe for the first time since Nakamoto's paper was published, mass environmental awareness about Bitcoin protocol has spurred. The most iconic and influential example to mention was made 13th of May 2021 by Elon Musk, owner of *Tesla, inc*, who, from his twitter account, stated that "*Tesla has suspended vehicle purchases using Bitcoin. We are concerned about rapidly increasing use of fossil fuels for Bitcoin mining and transactions, especially coal, which has the worst emissions of any fuel […] we intend to use it (Bitcoin) for transactions as soon as mining transitions to more sustainable energy. We are also looking at other cryptocurrencies that use <1% of Bitcoin's energy/transaction*".

These words, coming from one of the most influential technology enthusiasts worldwide, had great media resonance and resulted in a huge slump of Bitcoin's price that fell for about 30% of its value in the timespan of just a few days.

The question that logically arises following the environmental implications of the actual state of Bitcoin mining asks whether there is the possibility to decrease its ecological impact and how that can be accomplished. Among all the possible solutions that are being proposed and discussed, the most reliable, disruptive and realistic one is constituted by exchanging the Proof-of-Work demanded by the Bitcoin protocol to the easier and less energy demanding Proof-of-Stake.

In Proof-of-Stake (PoS) systems, nodes in the network are asked to validate the transaction blocks rather than mining them, as happens with Proof-of-Work. PoS starts with a deterministic process that selects block validators among the nodes of the network, this choice is made taking into account the amount of currency the nodes already own (the more currency they own, the more their chances to be selected). Once the majority of the selected nodes accept the block, the set of transaction is added to the existing blockchain.

This system lets the nodes use their own currency as a collateral when competing to add a block to the chain, so, each node actually is a stakeholder for the system and none of them will have incentives in altering its regular functioning. Moreover, in this context, the competition among nodes is settled only regarding the amount of currency they already dispose in their wallets, and, unlike PoW system, there is no specific computing or energetic requirement.

Proof-of-Stake is not a new concept, as it has been firstly introduced in a paper by Sunny King and Scott Nadal in 2012, but only in recent times it has gained popularity: just a few cryptocurrencies, like DASH, already use PoS mechanism and many more, Ethereum above all, plan to implement it in the future as it promises to decrease largely the energetic need for them.

Whether Bitcoin protocol will switch its historic Proof-of-Work process with a Proof-of-Stake one cannot be determined in this moment, but, it is reasonable to say that if the latter proves to be a good alternative and the ecological issues arisen by PoW continue to gain importance in the financial environment, maybe the Bitcoin network will be obliged to change its functioning, leaving all the current miners with useless, ASICs filled, immense warehouses.

CONCLUSION

At the light of both the empirical evidence and our mathematical work, the positive correlation between the hype that surrounds Bitcoin, and generally cryptocurrencies, and their huge energetic consumption and CO2 generation it now clear.

Many cryptocurrencies enthusiasts affirm that the ecological issues arisen by mining activity are a price worth paying to have a brand new finance system which is capable of connecting people from all around the globe in an easy, widely accessible and quick way.

However, in an era in which ecological awareness has paved its way into common knowledge and all of the most technologically advanced states are making some moves towards the so-called *green economy* (see the states that are committed to Paris 2030 agreement, an agenda that proposes to reduce greenhouse gas emissions by at least 40% by 2030 compared to 1990), the Bitcoin seems to be way too environmentally impactful, especially taking into account its actual usage.

While some modifications have been proposed and accepted in the mining mechanism of other cryptocurrencies to face such ecological issues, at the present time it seems that no change in the Bitcoin functioning is programmed to reduce its environmental impact and, if nothing changes in the Bitcoin rules, it is possible that in the future it could lose its lead in the cryptocurrency market in favor of other, more efficient cryptocurrencies.

References

1- Patrick Billingsley, *Probability and Measure - Anniversary Edition*, Wiley (2012)

2- Ryan Browne, Arjun Kharpal, *Bitcoin plunge 30% to 30,000 dollars at one point in wild session, recovers somewhat to 38,000 dollars*, CNBC (May 19 2021)

3- Alex de Vries, *Renewable Energy Will Not Solve Bitcoin's Sustainability Problem*, Joule: Cell Press (2019)

4- Mark Gates, *Blockchain. Ultimate guide to understanding Blockchain, Bitcoin, cryptocurrencies, smart contract and the future of money*, pamphlet (2017)

5- Marie Huillet, *Bitcoin will follow ethereum and move to Proof-of-Stake, says Bitcoin Suisse founder*, Cointelegraph (2020)

6- Gunter Last, Mathew Penrose, *Lectures on the Poisson Process*, Cambridge University press (2017)

7- June Ma, Joshua S. Gans, Rabee Tourky, *Market structure in Bitcoin mining*, National Bureau of economic research (2018)

8- Hass McCook, *A critical assessment of the Bitcoin mining industry, gold production industry, the legacy banking system, and the production of physical currency*, paper (2018)

9- Kamshad Mohsin, *Cryptocurrency & its Impact on Environment*, SSRN paper (2021)

10- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, whitepaper (2008)

11- University of Cambridge, *Cambridge Bitcoin Electricity Concumption Indes*, https://cbeci.org/ (June 2021)