NEWS AND VIEWS / NOTICIAS Y OPINIONES

Blockchain: A technological tool for sustainable development or a massive energy consumption network?

Blockchain: ¿Una herramienta tecnológica para el desarrollo sostenible o una red de consumo eléctrico/energético masivo?

Nicolas Serrano Palacio.

DOI. 10.21931/RB/2018.03.04.11

Abstract: The blockchain term appeared online in 2008 and has created impact on public institutions, private companies, startups, etc. It is a way to record information and its main application since inception has been as a new means of exchange between two parties. Blockchain is a highly secured and decentralized accounting system that allows direct exchange between two unknown parties without the necessity for a trusted third party, and it implies a new operation model for businesses and institutions. This new model could be a useful tool to solve global issues as income inequality and contribute to the accomplishment of the sustainable development agenda proposed for the United Nations for all countries in the world.

Key words: Blockchain, Bitcoin, Energy Consumption, Sustainable development, Income inequality.

Resumen: El término Blockchain apareció en línea en el 2008 y ha creado un impacto en instituciones públicas, compañías privadas, emprendimientos, etc. Blockchain es una manera de almacenar información y su aplicación principal desde el inicio ha sido crear medios de intercambio entre dos entidades. Blockchain es un sistema de contabilidad altamente seguro y decentralizado que permite un intercambio directo entre dos entidades desconocidas sin la necesidad de una tercera entidad en la cual confiar. Eso implica un nuevo modelo de operaciones para negociones e instituciones. El modelo puede ser una herramienta útil para resolver problemas globales como la desigualdad de ingresos además de cumplir con la agenda de desarrollo sostenible propuesta por las Naciones Unidas para todas las naciones miembro.

Palabras clave: Blockchain, Bitcoin, Consumo eléctrico/energético, Desarrollo sostenible, Desigualdad de ingresos.

Introduction

Blockchain, a distributed ledger network, has recently caught the attention of diverse sectors like industry, financial institutions, academia, online community and entrepreneurs[1] (p.11-19); it is all due to the wide range of challenges blockchain could solve. Main examples are: institutional transparency, businesses decentralization, track able information and democratizing work rewards across all members of the network by eliminating the need of a central authority that has total control[2]. Nevertheless, blockchain infrastructure consumes a massive amount of electricity[3] to properly maintain its data integrity. The two topics above may look unrelated until it is seen through a sustainable development perspective where the future of humankind depends not only on social and economic development but also on environment preservation.

The article will discuss the basic technical concepts related to the equally rewarded property of a blockchain, and how this technology is affecting another sustainable development dimension: environmental sustainability. To conclude we would make a "call to action" to the academic and research community to solve the blockchain challenges and help societies evolve towards a more sustainable era.

Equality and Sustainable Development

Sustainable development is an organizing principle for human development respecting the existence of other life forms. According to the United Nations; people, economy and environment are the three pillars for sustainable development. In turn, these three pillars relate to seventeen Sustainable Development Goals (SDG) that need to be pursued in order to reach sustainability. The goals are inter linked and working on a specific one will have an effect on others. The objective is to harmonize all efforts so that progress can be measured for all sustainability actions[4]. Blockchain, a global distributed ledger[1], could help solve economic inequality by using its decentralized properties but it also presents a problem to the environment if we look at the amount of electric power needed to maintain its networks.

Nowadays, the technology industry has been following a "winner takes it all" model[5, 6] (p. 108) where just one business is capable of practical domination over a market where all other competitors fail in the process. This model causes a few very large centralized companies who offer a product or service and get richly compensated for it as many times as demands are made by the clients; the lack of competitors helps the company to grow consistently and win more market share in the process[7] (p. 103-105). Sadly, the actual model and the concentrated wealth that it generates prevents new companies from disrupting the existing status quo in the market place with innovative solutions; mainly because the most powerful companies of the world control not only their own ecosystem but also dispose of financial and information resources that give them an unfair advantage over their small competitors[8]. This problem could lead to a world of centralized power and income inequality within the whole population. Blockchain could theoretically be a viable solution to this issue

[1] Yachay Tech University, Urcuquí. Ecuador.

Correspondencia: https://orcid.org/0000-0001-5008-5418

Figure 1. Sustainable Development Goals proposed by the United Nations on 2015.

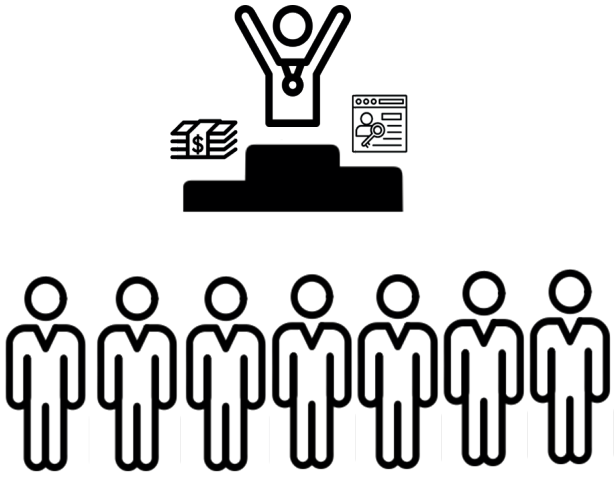

Figure 2. Winner takes it all model representation. A single company would get all the market.

because of its decentralizing and empowering nature.

The blockchain proposes a business model where every worker on the network gets equally rewarded for doing a specific task and the unhackable feature gives security consistency to the system. It also prevents control of a single central authority through transparent management of data ledgers in the network[2].

The theory behind blockchain date back to 19802 but it was not until ten years ago that the right conjunction of concepts gave it the ability to disrupt multiple sectors simultaneously and generated a new area of technological development[9].

History

The first appearance of the term "blockchain" was in 2008 on a white paper published online by Satoshi Nakamoto1. The name was a nickname; until today nobody have verified the truth identity of this person or group of people although some of the earliest Bitcoin developers had been working with him/her/them via online forums, platforms and emails[1](p. 5).

2008 as the publication year was not a random choice. The economic crisis in the US and all over the world had taken its toll over savings and businesses while bank corporations and wealthy people remained in a privileged position[10]. Bitcoin, and blockchain behind it, promoted the concept of a decentralized and distributed platform that provided a new way to exchange money using a publicly powered network rather than a central and privately controlled node[2].

From that date, blockchain research and development has been growing at a fast rate. The private sector has seen growing investment on the technology and, as a result, we can see multiple private or public blockchain platforms[11]; academia has been developing a new blockchain space backed up with all the scientific rigor that a peer review provides[12]; and the entrepreneurs and innovators have been involved as main actors in the process, developing and creating better solutions[13, 14].

In December 2017 we witnessed the explosion of the cryptocurrencies; some experts compared it to the .com mania that caused market instability in the years 2000s[15]. Two months later, people declared that the cryptocurrency era was over as, intuitively, blockchain was following the Gartner hype curve[16] (Fig. 3). But for other people, this was the end of the cryptocurrency bubble and the beginning of the blockchain era. In 2018, ten years later its inception, blockchain is well positioned as a technological important topic[9] with high hope and expectations for this relatively new concept and its potential impact on global issues such as income inequality[17].

The future of blockchain highly depends on public adoption and market penetration[18], nevertheless academia and the research community can help in the search for solutions to the challenges this technology presents. In other to understand these challenges, the researcher has to familiarize himself with the technical concepts behind it.

Blockchain Theory

To explain the concept of blockchain; it has to be compared to an account ledger where all information (in case of Bitcoin, transactions) is stored. If the ledger where held by a

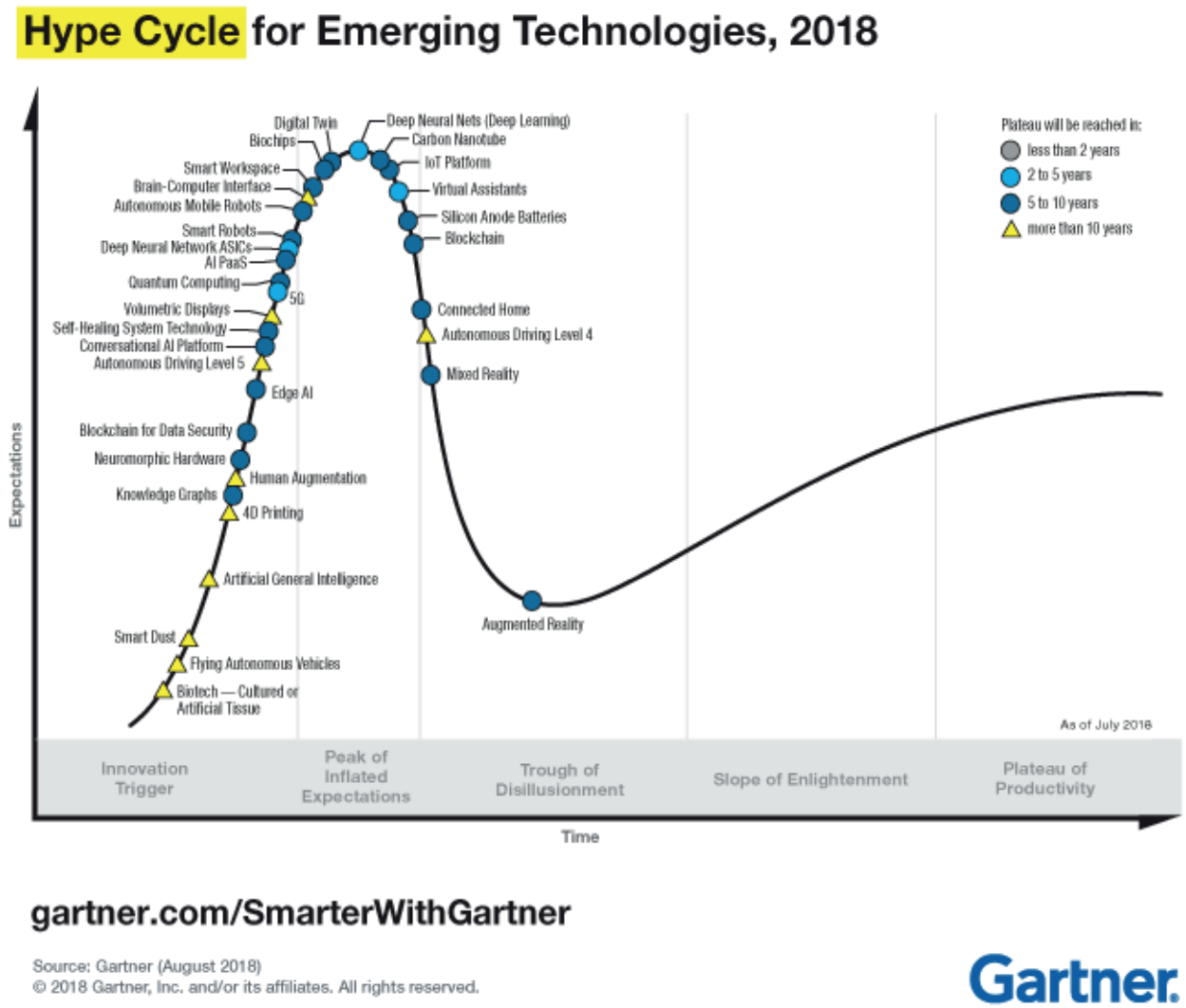

Figure 3. Hype Cycle or Gartner curve for Emergin Technologies 2018.

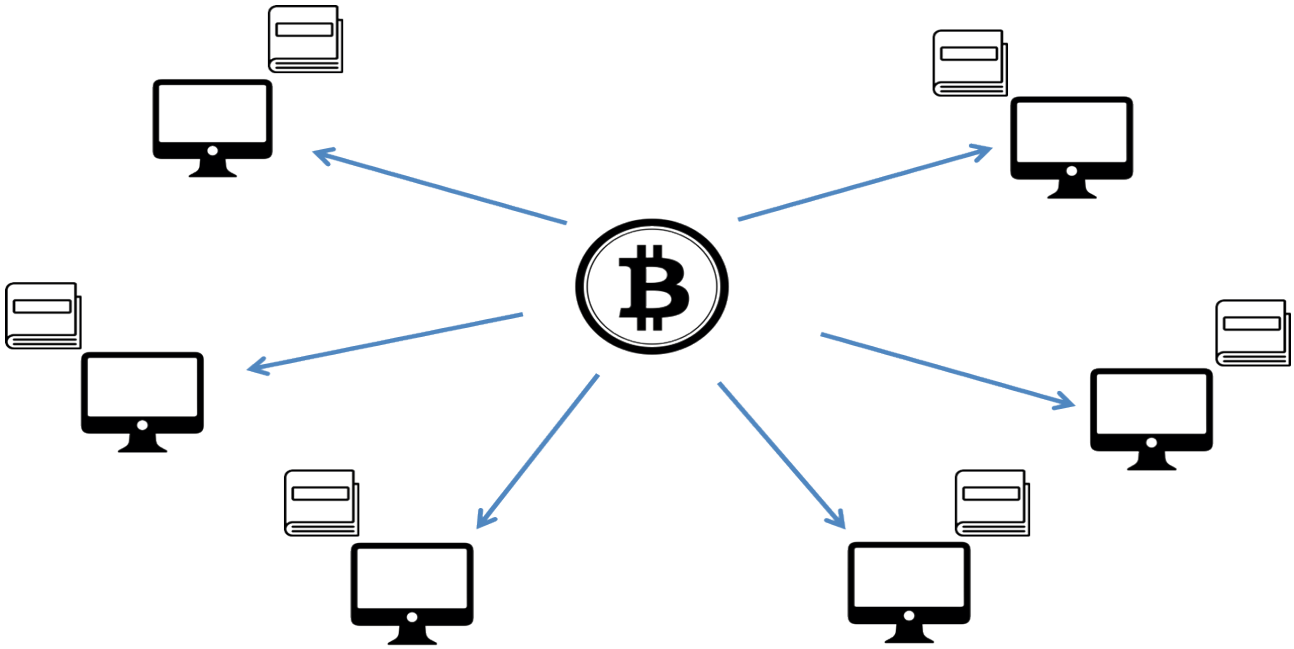

Figure 4. Simple scheme of a blockchain network where all nodes contain the same ledger.

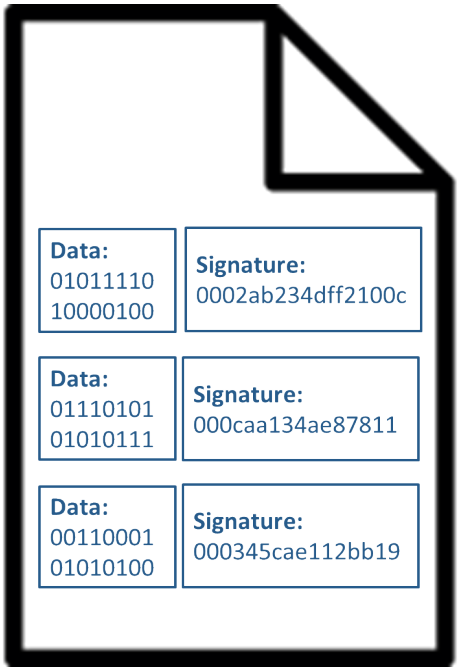

Figure 5. Ledger containing groups of data with the correspondent signature for each one.

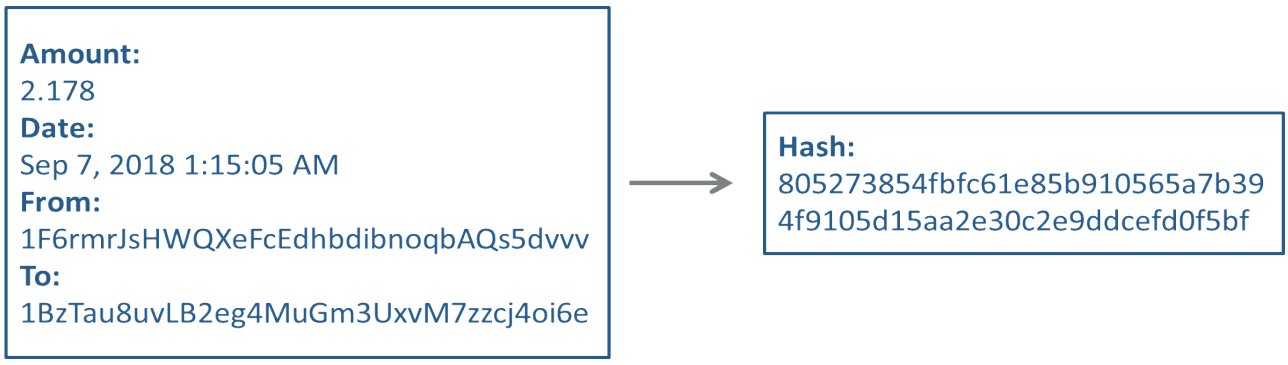

Figure 6. Hashing process to get a hash or signature by inputting transaction data into a cryptographic function.

single owner, it could be modified depending on his/her self-interests. To prevent that from happening, the ledger is distributed and maintained by several people or entities. So in the case where a participant presents a modified version of the ledger, the whole group can verify or audit the ledger and deny the corrupted ledger. Blockchain as a data structure does not only assures data veracity but also provides the historic record of the data[1, 2].

Blockchain is improbable hackable and it guarantees the veracity of the information by supplying a unique "digital signature" to every set of data stored each time period. In order to maintain the network as a decentralized structure a ledger is distributed to all the registered nodes on the network and all the transactions are tracked through each node.[2] (p.3) (Fig. 4).

Commonly the ledger created contains all the previous archived data and the digital signature of each set of data called block. The signatures guarantee the authenticity of the contained information because if, at any place of the ledger, some data changes or becomes corrupted; the signature will be completely different[1] (p. 6) (Fig. 5).

In order to create a signature or "Hash"; the system protocol takes all the data and process it through a cryptographic hash function that would convert it into a pseudo random sequence of numbers and characters[19] (p. 83-84). In the Bitcoin blockchain; multiple cryptographic functions are used such as SHA256 or RIPEMD-160 and it takes as input the following elements: sender address, receiver address, amount (represented by previous received transactions) and timestamp. The function would output the transaction signature as a hexadecimal string of 256 bits (Fig. 6).

To get the most efficient storage, the transactions signatures (called hashes) are processed with each other to build a Merkle tree and the last signature after processing the previous ones will be called "Root Hash"[2] (p. 4) (Fig. 7).

To finish, the protocol would take the root hash, timestamp and a value variable nonce to compute the "Block Hash" (Fig. 8). This process, called proof of work, endeavors to yeld a block hash that follows a specific condition. In the Bitcoin blockchain, the condition is that the hash has to have at least n zeros at the beginning of the string; with n being a difficulty variable that increases if the block hash had been found before ten minutes and decreases if the block had been found after ten minutes. Proof of work, the previously described algorithm, guarantees that each transaction is entered in a specific manner and prevents vulnerability to the double spending problem[1] (p. 8-11). The whole process is called mining.

This hash and the new data would be sent to all the nodes on the network for verification. If any data is modified at any

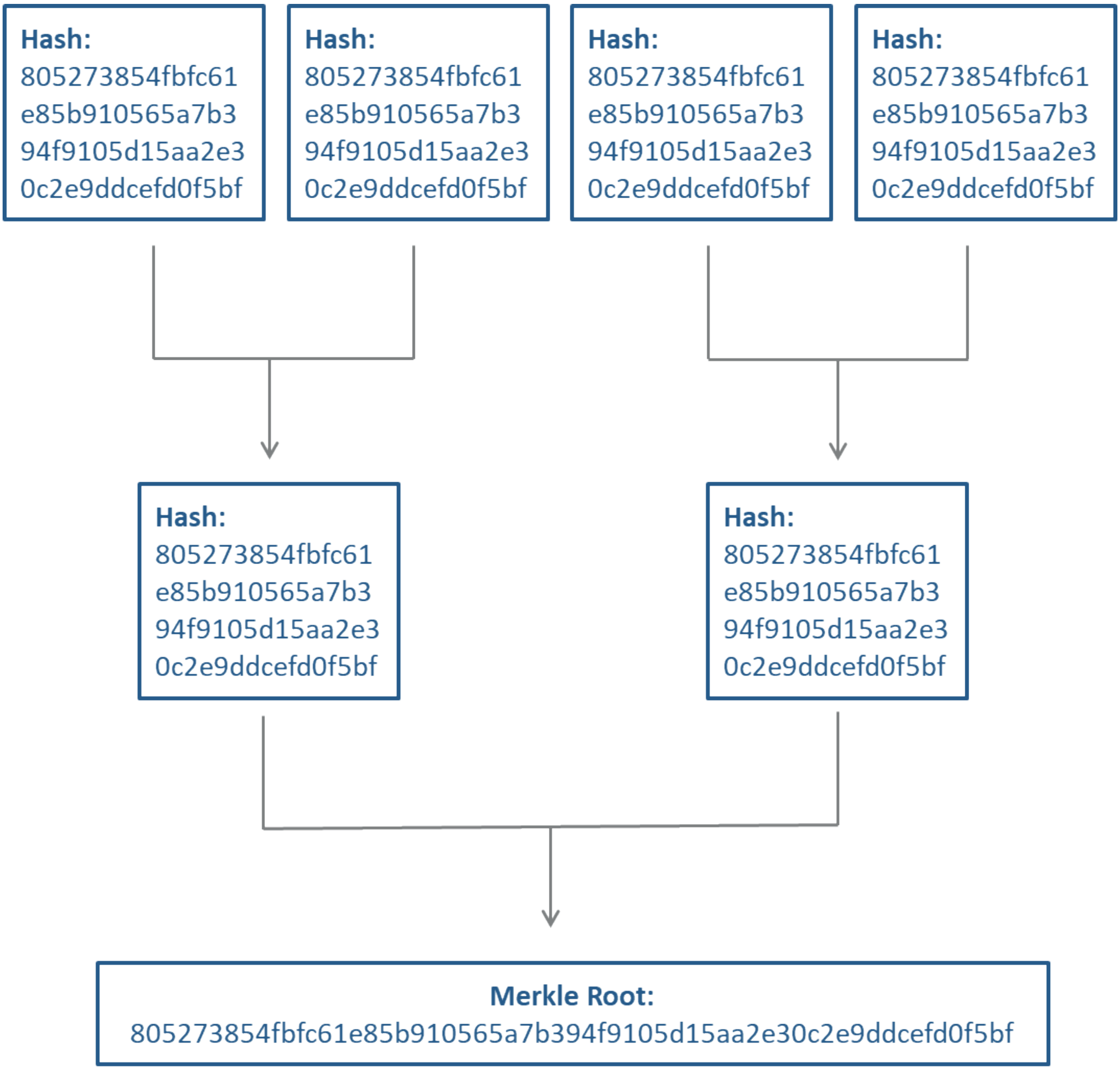

Figure 7. Merkle tree structure formed by hashes of different transactions.

time during that process, the Block Hash will be completely differently and thus the system would know that it has been compromised. The protocol would deny the wrong data and only accept the one that the majority of the network approves. With this feature, the network guarantees the veracity of the information and prevents the problem of getting the data modified by an attacker or impostor[19] (p. 5-9).

The new block hash and its information would be stored in all nodes of the blockchain. So in the future; it could be validated by any node registered on the network (Fig. 9). The participation depends on the nature of the blockchain; in a public blockchain such as Bitcoin or Etherum, people around the world can freely join the network[2] (p. 5)

The proof of work algorithm requires huge amounts of computing power and hence electric energy. As described before, the dimensions of sustainable development are interconnected; so it would be useful for the technology users to consider their energy requirement and its impact on their community.

Energy consumption problem

Alex de Vries described Bitcoin as an extremely energy-hungry process3. This is mainly because the proof of work algorithm uses exhaustive search method which consists on trying all possible permutations until getting the right answer, in the blockchain case: respecting the difficulty condition[20].

The blockchain structure allows one block creation per a determined time period. If more nodes with high computing power enter the network, the time period of block creation will decrease and hence the difficulty will increase at the future. The crypto currency revolution has attracted a lot of enthusiastic people not only to mine but to build large facilities called mining farms[21]. Inside the farms, there can found hundreds of ASIC, specialized mining computers that can try million of hashes permutations per second for proof of work procedure[22].

ASIC and GPU computing for mining Bitcoin are major trends nowadays. The whole Bitcoin network consumes the same amount of energy as the country of Ireland as a whole[3]. The compensation for joining the mining network is that each

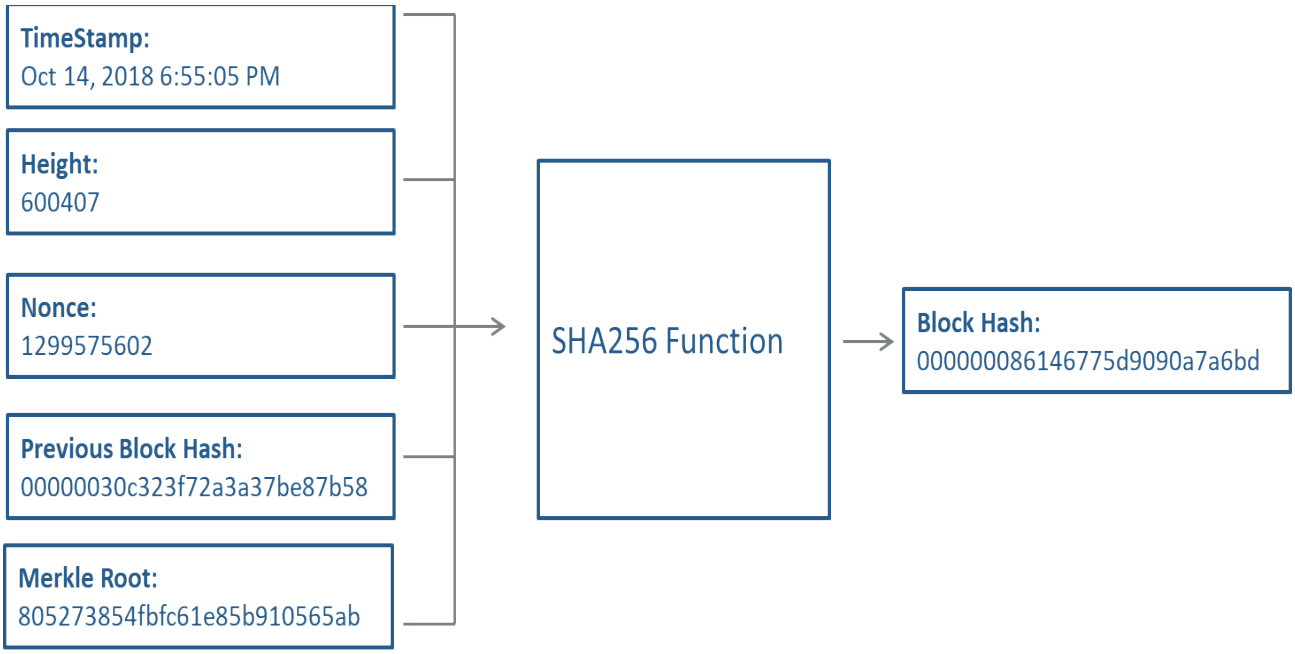

Figure 8. Process and inputs to obtain the block hash.

TimeStamp:
Oct 14, 2018 6:55:05 PM
Height:
600407
Nonce:
1299575602
Previous Block Hash:
00000030c323f72a3a37be87b58
Merkle Root:
805273854fbfc61e85b910565ab

Block Hash:
000000086146775d9090a7a6bd

Index	Amount	Date	From	To	Transaction Hash
0	0.45	Sep 7, 2018 1:15:05 AM	1F6rmrJsHWTQXeFcEdhbdi	bnoqbAQs5dvvvAA567FX110st	51B87481829E23ADF9282C4D487AE99DC16C06
1	2.00	Sep 10, 2018 12:15:00 AM	1BzTau8uvLB2eg4MuGm3Us	xvM7zzcj4oi6eUV1050LLeNM20	ADF08432826EA4103934C3D9E26C06ADFAE911
2	650.32	Sep 10, 2018 05:15:55 PM	22xTvLM7zzcj4oi6e05763JJ	xAA7eB123TYwq15209Hggstuw	8C578203D5FBEC4AB6E1D9DCE5CD2373FE9E52
3	56.11	Sep 23, 2018 9:40:00 AM	FS400824xcvHsadfwt7877	xH901221ASdtss2ptppwqQ981	6DC5484CF8A6639E80F0E09369DC5484CF8A661
4	101.11	Oct 7, 2018 11:00:12 AM	2K9uuytjsfhfTIWQasd31KKL	x82987hjAnIMaDlT0404l0V3yu	1EF688F4A92AFBCDB869C88C11CA026D432491
5	27.10	Oct 9, 2018 02:22:27 PM	487TTrt11101WADqghGHy3	BHsgjTj12783213qerFltuMpqjm	56166464CD45901D69619BF6C64915AAC10001

Figure 9. Information that would be stored in a blockchain after passing validation process.

time a new hash block is found and validated; the founding miner receives the fees for all the included transactions and 12.5 of new created Bitcoin[23]. The second amount is temporary until 21 million Bitcoin have been created; when that happen the winning miner would start receiving just the transaction fees[24]. Changes of a miner finding the right hash are random but the more computing power to process information; the more likely is for the miner to find the right hash.

Because of the large amount of computing power needed to find a right block hash, multiple middle class miners (with just one ASIC or a GPU graphic card) join a "mining pool". This organization delegates specific actions to each miner in order to have an organized procedure and increase the chances of getting the block reward. If the mining pool finds the right hash and get the fees and created Bitcoin, they will be distributed according to their group policies[25].

A common blockchain that uses the proof of work algorithm would spend huge amounts of electricity because of the network maintenance; this issue is a contributor to climate change and therefore sustainable development.

Truby[26] (2018) argues that the amount of electric energy consumed by blockchain technologies pose a serious threat to the global commitment to mitigate greenhouse gas emissions pursuant to the Paris Agreement[27]. 28% of greenhouse gasses are released by electricity production[28] and part of that is used to power up mining equipment like computers, ASICs, GPU cards and others. Greenhouse gasses form a shell that keep the heat on the earth's surface like a greenhouse that cover the plants; that is why it is called Greenhouse Effect[29] (p. 77).

Blockchain and Sustainable Development

The blockchain phenomenon shows us how two aspects of sustainable development are related and how one action in a specific SDG could cause positive and negative impact on others SDGs.

The most important social feature of Blockchain is to decentralize business and organizations. As previously described, it could generate positive impact on the income inequality problem and promote a fair economic growth for all human classes on Earth rather that keeping the "winner takes it all" model.

But to reach a sustainable future, blockchain technology would need to evolve towards an improved energy consumption profile. Yli-Huumo's article identifies seven challenges of blockchain that should be investigated and improved[18]. These challenges are: thorughput, latency, ledger size, security, wasted resources, usability, hard forks or multiple chains.

There is an interesting opportunity for research NGOs and social researchers in the blockchain field; if more expert minds come together to find solutions, the decentralizing impact of Blockchain would arrive soon to our society.

Conclusions

It is true that concepts behind blockchain have been there for some time19 but the myriad combination and specific focus of these concepts make this technology fascinating. The hype of have found an interesting technology that could solve actual issues like social equity should give us hope but also reminder us to focus on finding better methods rather than wholly glorifying new platforms without further considerations.

As a Computer Science student, I am committed to research and develop technology for the good of all society and I make a "call to action" to my fellow partners to make a contribution in this field. Academia and research are capable of taking the blockchain revolution to another level and improving some social challenges we are facing nowadays.

Bibliographic references

1. Crosby M, Nachiappan, Pattanayak P, Verma S, Kalyanaraman V. Blockchain Technology Beyond Bitcoin. Blockchain Technol 2015; : 1–35.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. WwwBitcoinOrg 2008; : 9.
3. de Vries A. Bitcoin's Growing Energy Problem. Joule 2018; 2: 801–805.
4. United Nations General Assembly. Transforming our world: the 2030 Agenda for Sustainable Development. New York, 2015.
5. Sachs J. International Economics: Unlocking the Mysteries of Globalization. Foreign Policy 1998; : 97.
6. Kuchinke BA, Vidal M. Exclusionary strategies and the rise of winner-takes-it-all markets on the Internet. Telecomm Policy 2016; : 1–11.
7. Moazed A, Johnson N (Nicholas L. Modern monopolies : what it takes to dominate the 21st-century economy. 2016.
8. Vitali S, Glattfelder JB, Battiston S. The network of global corporate control. Zurichhttps://arxiv.org/PS_cache/arxiv/pdf/1107/1107.5728v2.pdf (accessed 18 Sep2018).
9. Leon Zhao J, Fan S, Yan J. Erratum to: Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financ Innov 2017; 3: 9.
10. Reavis C. The Global Financial Crisis of 2008: The Role of Greed, Fear, and Oligarchs. 2012http://baselinescenario.com. (accessed 12 Sep2018).
11. Mougayar W. The Ultimate List of Bitcoin and Blockchain White Papers. 2014.http://startupmanagement.org/2014/12/16/the-ultimate-list-of-bitcoin-and-blockchain-white-papers/ (accessed 12 Sep2018).
12. Hoskinson C. Why are we building Cardano? 2017; : 1–44.
13. Buterin V. A next-generation smart contract and decentralized application platform. Etherum 2014; : 1–36.
14. Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) 2017; 10401 LNCS: 357–388.
15. Ofek E, Richardson M. DotCom Mania: The Rise and Fall of Internet Stock Prices. 2003http://people.stern.nyu.edu/eofek/DotComMania_JF_Final.pdf (accessed 11 Sep2018).
16. Panetta K. 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018 - Smarter With Gartner. 2018.https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/ (accessed 12 Sep2018).
17. Pazaitis A, Kostakis V, Bauwens M. Digital economy and the rise of open cooperativism: the case of the Enspiral Network. Transfer 2017; 23: 177–192.
18. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on Blockchain technology? - A systematic review. PLoS One 2016; 11: 1–27.
19. Wattenhofer R. The Science of the Blockchain. Inverted Forest Publishing, 2016https://www.amazon.com/Science-Blockchain-Roger-Wattenhofer/dp/1522751831.
20. Jboss.org Community. Chapter 8. Exhaustive search. https://docs.jboss.org/drools/release/6.2.0.CR2/optaplanner-docs/html/exhaustiveSearch.html (accessed 18 Sep2018).
21. CBS News. Mining Bitcoin: Inside a cryptocurrency mining epicenter, and the fight for a small town's future - YouTube. 2018. https://www.youtube.com/watch?v=S00MWI3YeP4 (accessed 18 Sep2018).
22. O'Dwyer KJ, Malone D. Bitcoin Mining and its Energy Footprint.

2014.http://blockchain.info/charts. (accessed 19 Sep2018).
23. Bitcoin Wiki. Mining. https://en.bitcoin.it/wiki/Mining (accessed 19 Sep2018).
24. Bitcoin Wiki. Controlled supply. https://en.bitcoin.it/wiki/Controlled_supply (accessed 19 Sep2018).
25. Rosenfeld M. Analysis of Bitcoin Pooled Mining Reward Systems. 2011https://bitcoil.co.il/pool_analysis.pdf (accessed 19 Sep2018).
26. Truby J. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. Energy Res Soc Sci 2018; : 0–1.
27. UN Conference of the Parties. Adoption of the Paris Agreement. 2015https://unfccc.int/resource/docs/2015/cop21/eng/l09r01.pdf (accessed 19 Sep2018).
28. EPA U. Sources of Greenhouse Gas Emissions. https://www.epa.gov/ghgemissions/sources-greenhouse-gas-emissions (accessed 19 Sep2018).
29. El Zein AL, Chehayeb NA, El A. The Effect of Greenhouse Gases on Earth's Temperature. Int J Environ Monit Anal 2015; 3: 74–79.

Recibido: 21 September 2018
Aprobado: 20 November 2018