International Journal of Humanities Social Science and Management (IJHSSM)
Volume 2, Issue 2, June 2022, pp: 36-40 www.ijhssm.org

Scientific Research in Engineering: An Overview of Blockchain

Samuel Isaias Acevedo Torres[1]
[1,]*INNOVA SCIENTIFIC SAC, UNIVERSIDAD DE CARABOBO*

Date of Submission: 24-06-2022 Date of Acceptance: 05-07-2022

ABSTRACT: This study refers to the topic of blockchain technology. Being that we are facing a multidisciplinary process that is still located in the context of an emerging transdisciplinary and interdisciplinary field, avoiding transcomplexity from a broader perspective. In that sense, it has been reflected hermeneutically from the phenomenon of the scenario why this technology has boomed in recent years in a forceful way due to its stability, reliability, validity and security of the identity of things, objects and subjects in the entire society. traceability chain, giving clear demonstrations of effectiveness and efficiency. In the same way, a critical and analytical contribution of recent developments in blockchain research is built that can help the technology in the construction of blockchains in its truly sustainable consistency. In this way, some of the contributions made by current studies on the blockchain are incorporated with a vision from the engineering and designs associated with its development.

KEYWORDS: Systems development, Cyber Security, identity, trust tracing.

I. INTRODUCTION

This systematic review of the literature (RSL) on research works associated with blockchain technology (BCT) and distributed ledger technology (DLT). These being the emerging disciplines, which are areas of research driven by extensive novel advances of high relevance, strongly correlated in their applications to cryptocurrencies and digital tokens such as Bitcoin and NFT, recently published in scientific articles in indexed journals with a strong interest factor. impact. But this technology can also be used to provide reliability and high security of the traces from their origin to their entire existence of objects and subjects (tangible and intangible), anchoring their own trust at all times to their processes or transactions in decentralized systems, for example, for the veracity and origin of critical information such as sesame oil of controlled origin from the cultivation of the olive, selection and process of obtaining the oil and its subsequent commercialization.

As a contextualization of these relevant issues associated with this technological and engineering disruption from the episteme of these issues, which refer to [1,2] as sources of the blockchain approach as more detailed initial contributions. From this perspective, the theoretical scheme is at least close to offering some necessary definitions to substantiate the scientific, technical and engineering reason related to the blockchain or Blockchain. Now, the DLT is used to achieve a consensus on the replication of data or state machines through a geographically distributed network and where the consensus and its administration generally do not depend on a central administrator, giving way to the decentralization of algorithms. , which flow sequentially, but with safety and reliability in their traceability processes. A state machine is a device that stores a state and updates it and can perform other actions, both based on input received.

Blockchains can be seen as instances of such DLT solutions where data and its change history is presented in a linear chain of blocks that are cryptographically linked to be resistant to unintentional or malicious tampering. Generating security, reliability and consistency in the tracing of operations. DLT solutions can also use graph-based structures instead of linear chains, for example, as in IOTA's Tangle [3] or Hedera's Hashgraph [4], and this can offer advantages such as better scalability of transaction volumes. Unfortunately, terminology is not yet established in this space, which standardization initiatives such as ISO/TC 307 [5] will help to address: the terms “blockchain” and “distributed ledger” are often used interchangeably or there can be confusion about their meaning. Meaning, innovation departments today may view DLT projects as a public relations exercise and often lack a deeper internal understanding of this technology to transfer use cases into production.

Such lack of knowledge can also lead to ill-informed decisions when choosing instances of such technology and supporting project partners.

There is no doubt that BCT/DLT has brought a lot of innovation, mainly in its combination of cryptography tools, distributed systems and programming languages. This was powerfully demonstrated in the creation and launch of Bitcoin, which allows anyone to join this network to trade the digital currency "bitcoin". Trust in this network is an emergent property that results from the interaction of several factors, one of which is them being the monetary incentive of the miners, parties that specialize in solving a cryptographic puzzle called Proof of Work.

The initial hype around BCT/DLT was probably exaggerated by some, however its technical offerings are now more mature, its innovations are here to stay and will find their way into many products and infrastructures. Even so, several research challenges remain for this technology, some of which are addressed in the present study. It is necessary to consider the need to make DLT systems resistant to attacks based on quantum computing and the requirement for more scalable information processing, leading the study to the observation of control and protection systems such as cyber security.

On this last point, the early formative phase of BCT and DLT research and development was apparently done by people in applied cryptography, distributed systems, networks, and to some extent programming languages. There appears to have been little involvement in that phase by people from the database systems and information retrieval areas, for example, in the design and implementation of the Hyperledger Fabric blockchain framework [6].

It is therefore not too surprising that so-called third-generation blockchains, including Algorand [7], are now aiming to solve problems, many of which have been familiar to the database research community for quite some time.For example, chain sharding, which is expected to help with transaction processing performance scalability on blockchains, is related to the issue of database denormalization. There appears to be great potential to bring the database, information retrieval, and BCT/DLT communities closer together so that they can share problems and solutions more effectively for years to come. The recent Dagstuhl Seminar Distributed Computing with Blockchains and Permissioned Databases [8] seems to have been a good step in that direction.

Let us also discuss the considerable hype around Initial Coin Offerings (ICOs), which use smart contracts on an existing blockchain to operationalize the offering of a token as an investment in a new project, typically the development of a BCT system/ DLT. A smart contract is a deterministic program supported through a blockchain. Anyone on the blockchain can verify the integrity of a smart contract. The execution of a smart contract is deterministic, traceable and irreversible to the extent that the underlying blockchain offers those qualities.

In some major financial markets, it appears that more money was poured into ICOs than conventional initial public offerings (IPOs) in 2017. But 2018 saw a decline in investment volume for ICOs, in part due to regulatory uncertainty around the law. the status of tokens as a financial instrument, and also because some blockchain projects seemed to operate a "pump and dump" scheme.

Principles and best practices of business ethics should inform the operation and evaluation of blockchain projects. We refer to [9] for a survey and framework on this important topic. These principles should also guide any approach to deciding whether a blockchain would be subject to a software update that breaks the immutability of the chain, but rewinds the chain to a point in the past and invalidates all transactions that have occurred since then. In [10], an ethical framework informed by a Kantian view is proposed that can help decide whether the enactment of so-called hard forks would be ethical.

On the regulatory side, we now see more clarity in that space in many territories. Some countries, including Switzerland, Singapore and Malta, are now actively promoting the development of financial instruments based on BCT/DLT technology and their cryptocurrencies. Facebook's Libra can be seen as a strong and related strategic signal by a major ICT company in that space; we refer to [11] for a discussion and review of that project. We are likely to see similar use of tokens in Internet of Things (IoT) production and mobility, for example with digital car-sharing platforms.

II. BLOCKCHAIN (BLOCKCHAIN) AND SUSTAINABILITY

Proof-of-work is at the heart of the resilience of the Bitcoin system: each new block added to the chain is the result of a race for leadership in which miners compete against each other in trying to solve a difficult cryptographic puzzle. For the latter, a miner combines part of the current state of the blockchain, new transactions that

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 2, Issue 2, June 2022, pp: 36-40 www.ijhssm.org

should be included in the chain, and some random source into an input for a hash function. The puzzle is solved by varying the value of the random input part until the hash of the combined input has a certain minimum number of leading 0 bits. The value of this parameter is adjusted periodically and has increased dramatically over time, reflecting the competition and reward structure of this mining process and the advances in hardware manufacturing that further fueled such competition. On January 3, 2010, this value was 1.183 and increased by several orders of magnitude to 5.6186 $\times 10^{1}{}_{2}$ just 9 years later. As a consequence, if Bitcoin were a country, it would now consume more energy than Chile, Venezuela, and the Philippines. Bitcoin supports reliable processing and recording of less than a dozen transactions per second (tps), some estimate this to be as low as 5 tps. Therefore, the energy demands of Bitcoin appear to be extraordinary and extremely wasteful. In fact, this huge energy demand would not seem to be ecologically sustainable even if the system were able to support tps rates like those applied to credit card companies and their global transaction processing: Visa does not require as much energy as Chile.

Therefore, these concerns have motivated research to design BCT/DLT systems that have a much smaller energy footprint than Bitcoin. Fault-tolerant Byzantine consensus protocols, such as the one used in Hyperledger Fabric [12], offer considerable advantages here, as they do not require the solving of power-hungry puzzles, but instead achieve consensus through the communication of messages. staged and with status. However, the increased communication complexity of such protocols means that, in practice, there is a limit to the number of nodes that can participate in this consensus process. In certain use cases, this may be unacceptable, as such a number of nodes (e.g. less than 20) would have to be trusted as an "oligarchy" with faithful administration of the system. Algorand's consensus protocol, by contrast, aims to combine the strengths of both approaches for synergistic benefits:

B1 Random options provide strong system security and resilience – For Bitcoin, this is the random nature of the mining run.

B2 Non-random consensus protocols are much more energy efficient: for Byzantine protocols, the consensus is computed with much lower power consumption.

Algorand harmonizes the seemingly conflicting benefits B1 and B2 by retaining the small size of the nodes involved in consensus building, but randomly selecting that set of nodes again for each step of that consensus calculation. This random selection is achieved by a publicly verifiable random function. This function is a sequence of seeds where the genesis block contains the initial seed and the seed of the next block is determined by the seed of the last block and the digital signature of the leader producing the new block. Thus, this approach appears to preserve the security and resiliency of the system (which Bitcoin achieved only with high power consumption) and creates a consensus within the power budgets of normal ICT processing.

Algorand is not the only blockchain that appears to lower consensus power demands, both IOTA and Hashgraph appear to have similar advantages. One can see such efforts as important contributions to the sustainability aspect of security and privacy research and development. More generally, it seems important to develop design principles for systems that optimally trade off energy consumption and carbon footprint with a desired level of reliability of system services (for example, for “consensus” as a service of the system). system).

While we believe such research is vital to making our increasingly digitized worlds more ecologically sustainable, it is worth noting that the sustainability of digital technology should not be viewed in isolation from system components, services, or consumer products.Of course, it is helpful to understand the energy demands of direct system use and try to contain those demands at the design, implementation, or operation stages. “Energy” is understood here in a broad sense, to include the efforts required in the production or transformation of materials, products or infrastructure.

In fact, much of the existing literature investigating energy demand has focused on direct consumption of consumer products, such as televisions, smartphones, etc. However, it seems equally important to understand the energy needs of infrastructures. For example, the lower consumption of portable devices compared to desktop computers seems to make consumption more sustainable. But the increased connectivity of these devices has certainly increased the demand for data carried over networks reaching peak demands such as home video streaming in the evenings and the implications on power requirements for infrastructure. As indicated in [13], research investigating the balance between carbon savings and energy needs in digitization has organized such work into the study of different types of effects:

(i) first-order effects that consider the energy needed to produce and use ICTs, for example, the energy cost of the consensus mechanism used in a blockchain;
(ii) second-order effects resulting from other forms of changes, which may also be influenced by innovations in ICTs and their use, for example changes in travel; Y
(iii) tertiary effects that refer to the long-term use of ICTs, for example, how regulations, design principles and implementation measures can help the sustainability of ICTs.
Therefore, we suggest that the sustainability aspects of BCT/DLT are better studied and developed within a broader framework that manages, assesses and ideally certifies the sustainability of ICT systems in relation to all of the above types of effects. Blockchain projects like SolarCoin [14], which rewards solar power generation, could then be methodically evaluated to fully understand their potential contributions to a more sustainable world.

III. ARTICLES RELATED TO THE RSL

As a result of the Systematic Review of the Literature (RSL), the contributions of some of the articles associated with the study carried out are outlined below. The article by McGinn et al. [15] argues and demonstrates that the combination of data analysis and data visualization offers a powerful toolbox for understanding behaviours and trends in open and permission less blockchains, illustrated here in Bitcoin. Cryptocurrencies can be grouped into those whose transactions are account-based and those in which a transaction redistributes assets from so-called unspent transaction outputs (UTXOs). Although these approaches are mathematically equivalent, they differ in behaviour, for example in terms of information retrieval. The article by Péres-Solà et al. [16] studies some of the most popular UTXO-based cryptocurrencies and identifies room for improvement in the implementation of UTXO technology. The aforementioned need for greater scalability for transaction processing is the subject of the article by Burchert et al. in [17]. They develop a layer that sits between the blockchain and the payment channel so that channel-based micropayments can be made with considerably lower transaction costs. The resistance of blockchains to quantum attacks is the subject of the article by Stewart et al. in [18]; In particular, this paper develops an approach on how to safely move funds from a blockchain to a quantum-resistant one, even when a quantum attack is taking place on the former. Many cryptocurrency advocates have argued that cryptocurrencies can serve as a viable alternative to fiat currencies. In the article [19], Lipton et al. develop a framework for an asset-backed digital currency, and also the means to control the stability of this currency through financial mechanisms.

REFERENCES

[1]. Karame G, Androulaki E. 2016 Bitcoin and blockchain security. Boston, MA: Artech House.
[2]. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. 2016 Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, NJ: Princeton University Press.
[3]. Popov S. 2018 The Tangle. 30 April 2018, IOTA Foundation.
[4]. Baird L, Harmon M, Madsen P. 2019 Hedera: A Public Hashgraph Network & Governing Council. 29 August 2019, Hedera Hashgraph.
[5]. ISO/TC 307. 2019 Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems. Technical Report ISO/TR 23455:2019
[6]. Androulaki E, Cachin C, Caro AD, Sorniotti A, Vukolic M. 2017 Permissioned blockchains and hyperledger fabric. ERCIM

News 2017. See https://ercim-news.ercim.eu/en110/special/permissionedblockchains-and-hyperledger-fabric.

[7]. Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. 2017 Algorand: scaling byzantine agreements for cryptocurrencies. In Proc. of the 26th Symp. on Operating Systems Principles, Shanghai, China, 28–31 October, pp. 51–68.

[8]. Mohan C, Ooi BC, Vossen G. 2019 Distributed computing with permissioned blockchains and databases (Dagstuhl Seminar 19261). Dagstuhl Rep. 9, 69–94.

[9]. Dierksmeier C, Seele P. 2018 Cryptocurrencies and business ethics. J. Business Ethics 152, 1–14. (doi:10.1007/s10551-016- 3298-0)

[10]. Kim TW, Zetlin-Jones A. 2019 The ethics of contentious hard forks in blockchain networks with fixed features. Front. Blockchain 2, 9. (doi:10.3389/fbloc.2019.00009)

[11]. Abraham L, Guégan D. 2019 The other side of the Coin: risks of the Libra Blockchain. CoRR. (http://arxiv.org/abs/1910.07775)

[12]. Androulaki E et al. 2018 Hyperledger Fabric: a distributed operating system for permissioned blockchains. CoRR. (http://arxiv.org/abs/1801.10228)

[13]. Morley J, Widdicks K, Hazas M. 2018 Digitalisation, energy and data demand: the impact of internet traffic on overall and peak electricity consumption. Energy Res. Soc. Sci. 38, 128–137. (doi:10.1016/j.erss.2018.01.018)

[14]. 2018 SolarCoin Foundation. SolarCoin economics. 10 November 2018, Medium Article.

[15]. McGinn D, McIlwraith D, Guo Y. 2018 Towards open data blockchain analytics: a Bitcoin perspective. R. Soc. Open Sci. 5, 180298. (doi:10. 1098/rsos.180298)

[16]. Pérez-Solà C, Delgado-Segura S, Navarro-Arribas G, Herrera-Joancomartı J. 2018 Another coin bites the dust: an analysis of dust in UTXObased cryptocurrencies. R. Soc. Open Sci. 6, 180817. (doi:10.1098/rsos.180817)

[17]. Burchert C, Decker C, Wattenhofer R. 2018 Scalable funding of Bitcoin micropayment channel networks. R. Soc. Open Sci. 5, 180089. (doi:10.1098/rsos.180089)

[18]. Stewart I, Ilie D, Zamyatin A, Werner S, Torshizi MF, Knottenbelt WJ. 2018 Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. R. Soc. Open Sci. 5, 180410. (doi:10.1098/rsos. 180410)

[19]. Lipton A, Hardjono T, Pentland A. 2018 Digital trade coin: towards a more stable digital currency. R. Soc. Open Sci. 5, 180155. (doi:10. 1098/rsos.180155)