Atlantis Highlights in Computer Sciences, volume 4
Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)

Smart Application Based Blockchain Consensus Protocols: A Systematic Mapping Study

Daniel Mago Vistro[1,*] Muhammad Shoaib Farooq[2], Attique Ur Rehman[2], Saroosh Malik[2]

[1] *School of Computing, Asia Pacific University, Kuala lumpur, Malaysia.*
[2] *School of System and Technology, University of Management and Technology, Pakistan.*
[*]*Corresponding author. Email: Daniel.mago@staffemail.apu.edu.my*

ABSTRACT
Blockchain emerges as a potential platform aim of providing efficient and robust infrastructure and the centre of the blockchain is the consensus protocol feature that shows the working of distributed ledger technology named the blockchain. However, existing blockchain systems do not satisfy the requirement of the transaction in pragmatic use due to their limited capacity. While several new ideas were suggested by experts as they faced either decentralization or security concerns. Although several scientists are working on the improvement of the new quantum-resistant, fault-tolerant protocol, resource-efficient, and others focus on the development of multiple protocol versions, better adapted for particular use cases. Many researcher-made their own protocol to secure their work, instead of using traditional protocols. The paper represents a systematic literature review by accompanying a survey of blockchain technologies and their current utilization in different application domains in the IT industry. In this article, we first describe some previous and current consensus protocols of blockchain with the help of taxonomy which includes types and variants of protocols. Secondly, we have selected the most used protocols used up till now and write a comparative analysis with systematic review to find out which approach is the best suitable to use Lastly, we have analysed the strength and weaknesses of existing and previous protocols.

Keywords: *Blockchain 1, Efficient 2, Protocol 3, Transactions 4, Traditional 5, Security 6.*

1. INTRODUCTION

Securing transactional data is one of the biggest concerns in every industry. Many methods and approaches are used for keeping secure transactional data like a Barter system, triple bookkeeping, and digital signature algorithm, peer-to-peer networks, hash cash, Paxos algorithm, but they did not satisfy in terms of security [1] [19-26]. Distributed ledger technology has accumulated a large range of mechanisms since the advent of bitcoin, popularity, and acceptance on 1 Nov 2008 that was founded on proof of work that was the first consensus protocol [4]. The concept of PoW is originated in 1992 mainly influenced by Adam Back Hash cash from Denial of services and spam email prevention and implemented in 1997 but then updated in 2002. Ronald and Adi proposed two basic bitcoin payment systems in 1996 as Micro Mint and Pay Word. Matthew and Dahlia used the concept of PoW for measuring the reputation of websites in 1997,

The client puzzle is also an application of PoW in which the client needs to resolves the cryptographic puzzle. [2].

PoW is based on a hash puzzle that's why it gains too much computational Power and electricity and it is no significant proof that leads it to security threats in the future. So the variation in existing protocols is proposed and adopted are trying to developing an optimal consensus protocol for fault-tolerant and robust. With the ongoing growth of blockchain technologies [27-31], the Consensus algorithm is continuously adapting to changing criteria from the early Proof of Work to the later Proof of Stake, Delegated Proof of Stake, Practical Byzantine Fault Tolerance [1], [2], [3], and several other improved Consensus algorithms such as PoB, PoA, PoL [2], [3] and SCP but none of them is perfect [3]. Some Challenges faced by companies while implementing blockchain technology are 51% mass Attack, Fork problem (Hard fork, Soft fork), Small range of

Blockchain to solve these problems Propose a plan Consensus protocol called the Block Maturity Standard Sidechain/off-chain methodology to the original blockchain. This is the malevolent invader would require a lot more control, not just 51 percent to combat the consensus process [5].

The core contribution of this paper is to briefly classify the usage and benefits with disadvantages respectively. For this purpose, we have created one statistical chart and two tables that showed the benefits and problems of blockchain protocols. To our finest knowledge, there is no such available SLR associating the existing and previous blockchain that identifies all the consensus protocols cumulatively. Thus, we intended to read the literature and offer a recent precipitate indicating the scope of blockchain protocols to enhance the usability related to other variants of consensus protocol. We have created a taxonomy of consensus protocols in the form of tree including their variants. A comparative analysis table has created by reading survey papers to compare the accuracy of consensus protocols. Furthermore, the proposed consensus protocols which do not uses the traditional protocols of blockchain have been defined in the literature review. We hope this SLR would help companies by choosing the best consensus protocols by looking at their advantages and disadvantages rather than sticking to the first-ever proposed Proof of Work.

The basic purpose of this paper to describe the consensus protocols of blockchain. We organized the paper as; in section II, we have described briefly consensus protocol to let the reader about an idea of consensus protocol and its brief history of origin. In the III section, we have written the literature review on protocols with the table and description. In the last section, we hopefully, concluded the paper by exploring how protocols for consensus their function, and execution varies, which makes them different.

2. RELATED WORK

Sethumadhavan and Sankar, Sindhu in 2017 emphases on exploring consensus protocols with their viability and effectiveness to reach the structures they recommend to deliver, however, they did not make any comparison table or any figure related to consensus protocol usage also they have not identified the complete consensus protocols [1]. According to [2] Bitcoin and lite coin, are the implementation of PoW that was the first consensus protocol, they also identified that Proof of eXercise and Proofs of Useful Work firstly used by two persons Jakobsson and Juels in 1999 solve the technical complications based on orthogonal paths but the useful proof-of-work but have no practical implementation however they do not have any comparison table and criteria. In [3] Wang Yi, Mingsong Lv, Nan Guan, and Qingqiang explain the usage of blockchain mechanisms in terms of the internet of things and DLT, they also identified challenges and principles with their strength and weakness however they do not have complete consensus protocols with their descriptions.

Almost 41 consensus algorithms such as PoW, PoS, DPoS, DDPoS, PoL, PoI, Raft, Ripple and Algo Rand and other variants of consensus protocols explained from almost past 10 years in different researches Sunny King's Peer coin was first developed and its complex mining is regulated based on the number of stakes kept by employees Downgrade delegated POS is an efficient consensus algorithm called DDPOS for decreased resource usage, greater operational performance and improved protection of the integrated blockchain. The downgrade method is a successful solution to the issue of suspicious participant performance, they have made their own protocol while using the previous protocol [4]

An inclusive review of the functioning ideologies of the most frequently used consensus protocols in blockchain-based cryptocurrencies is defined in [6], however, they have not any practical implantation or have not ay criteria of selection of papers but they classify the different protocols based on their permission requirements and perform a thorough comparative evaluation without any comparison table. In [7], different consensus protocols that are suitable specifically for IoT and others that are not suitable for IoT are identified, however, they have not described the analysis method and selection criteria with scoring that how they select the suitable papers for the comparative analysis, also they have not any figure related to any selection criteria or methodology.

PoW and PoS both do not provide multi nodes to function in the blockchain so [11] proposes multi tokens protocol that allows mining more than one token however it increases the security risk at some point, Multi Tokens POS is the architecture of the blockchain of standardization PoX targets to undeviating the figuring Power near real-world concerning technical problems however they do not have any selection criteria of papers selection. In the [13] evaluation of PoW, PoS, and pure PoS in a very descriptive manner define however they have not any scoring criteria of best-selected papers and have not no figure related to their used methodology.

By viewing all the surveys related to my studies, we came to know that PoW is not the best approach because it takes too much computational power, and also companies are using it with high risks of 51% attack. If the companies have big resources capacity and have larger projects they can take risks by using Proof of work otherwise suggested protocol is Proof of Stake because it uses less computational power and usage of this protocol is easier than PoW. All the papers identified and discussed above have no comparison table and the above debate discloses that many exertions have been approved to assess and associate different consensus protocols, yet no passable way to evaluate and equate blockchain

consensus protocols exists. This gives rise to the question of the usability of an inclusive technique to evaluate a consensus protocol's strengths and weaknesses, which in turn, helps in comparing the capability of different consensus protocols. The novelty of this work is that we have presented all the blockchain's protocol with their comparative analysis and strengths and weaknesses respectively. Contrasting prevailing approaches our method strongly defines the best comparison between existing and previous approaches for this persistence. This efficiently helps in accomplishing inclusive assessment of protocols.

3. RESEARCH METHODOLOGY

In this subdivision, we will define how we gathered our relevant information and data from different studies. For putting all the technologies and approaches together to bring out the best and successful technology used as mentioned in below mention Figure 1. For this review, we have used different search strategies and we got hundreds of results but reached the exact point by the following scheme firstly we formulated some questions for our paper structure when we finalized the questions then we just performed including and excluding relevant research papers then we defined our search strategy by which we got the results and data.

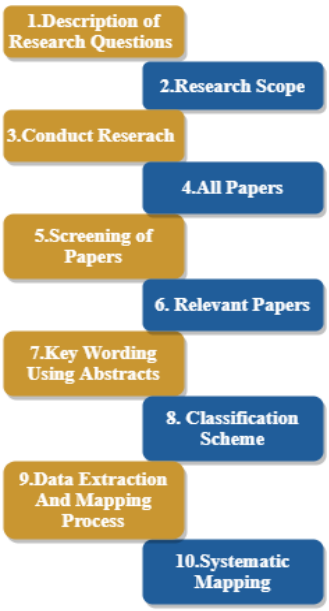

Figure 1 Systematic mapping process steps.

Afterward, we extracted the data by reading their abstracts and conclusions but we made a separate sheet with different parameters to observe for each paper by which we easily extracted the data and that sheet made the most relevant data clear, which helped us to eliminate the irrelevant data. In fig 1, the process identified and drawn to show the process that how methodology formulated.

3.1. Research Objectives (RO)

Table 1. Main Research Objectives.

RO1: The main emphasis is to identify the main usability of the blockchain protocols in the companies which use blockchain protocols.
RO2: In this, we described the domains of the consensus protocols other than blockchain
RO3: In this, we identified the problems by building a table that shows the problems and their solutions in terms of advantages and disadvantages.

The major objectives are as follows in Table 1.

3.2. Research Questions (RQ)

Table 2. Relevant Obtained Research Questions.

	RESEARCH QUESTION	MAJOR INSPIRATION
RQ1	What are the existed variants of consensus protocols?	In this, we described all variants of consensus protocols.
RQ2	How consensus protocols help blockchain to enhance its usability?	In this, we described the usability and their comparative analysis table.
RQ3	What are the strengths and weaknesses of consensus protocols that are beneficial as well as disadvantageous?	In this, we described the usage capability of all blockchain protocols.

Our primary focused questions that are real game-changer for our article contain the main data of our topic also from these questions we get to know each understanding about our topic that is divided into sections. The research queries defined in this evaluation with their foremost inspiration are stated in Table 2. All the questions are defined and answered in the light of a separate method.

3.3. Search Scheme

In this part, we will describe that how we searched the data for our paper from online and offline resources we acknowledge only electronic resources. We performed our research on five sources as ACM digital library, IEEE Explorer, Springer, Science Direct, Research gate. We formulated our search query first and tried on all the mentioned platforms once with the same query, once we collected some most preferable papers from results then we changed our query with some synonyms and tried again, once we collected papers by this then we tried to play with keywords and by this scheme, we got 16 most relevant articles from 2014 to 2020. We choose these

resources because they are considered as most authentic sources to gather information related to blockchain protocols. We have explored all the keywords categories that assembled the paper in detail.

3.3.1. Strategy of Search String

A definite and reasonable analysis has been accompanied via expressing a keyword-dependent string to examine and collect obtainable studies in the field utilizing countless familiar digital exploration sources. To guarantee the validity of the search string concerning the relevance of its effects, the main perceptions have been assessed through research questions to acquire related keywords and relations used in the particular area of learning. ‘‘AND’’ and ‘‘OR’’ logical operatives were used to syndicate the confirmed keywords and different relations to make a search string. The "OR" operator lets additional choices quest in, while the ‘‘AND’’ is to join the relations to classify the search selections and to limit the analysis to get appropriate search outcomes. In Fig 2, searching keywords are described while searching for research papers related to my topic.

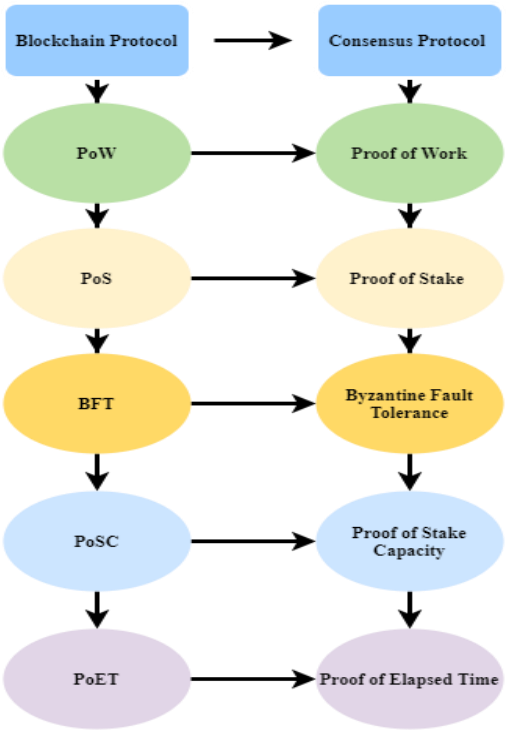

Figure 2 Keywords used in search with their full forms.

The confirmed searched string has two parts. The first part of the string is used to restrict the fallouts interrelated to terms blockchain or consensus protocol and the subsequent part relays to the names "proof of work or proof of stake or Byzantine fault tolerance or proof of space, storage and capacity or proof of elapsed time, our search string based on Equation 1 represented below in following equation B stands for blockchain, CP stands for consensus protocol and others are defined in Figure 2.

$$R = \forall [(B \vee CP) \wedge (CP \vee PoW \vee PoS \vee BFT \vee PoC \vee PoET) \quad (1)$$

In the above equation, R means results achieve beside search string,'∨' used for ‘OR’ operator and ‘∧’ for ‘AND’ operator and ‘∀’ furtherance of ‘for all, linking through the search associations stated in Table III to validate the whole search string rendering to an individually certain source. The general search words employing (1) can be articulated as The subsequent search string was used in the directive to achieve the spontaneous search in the digital libraries designated: “Blockchain” AND (“consensus protocols” OR “proof of work” OR “proof of stake” OR “byzantine fault tolerance” OR “proof of space & capacity” OR “proof of elapsed time”).

3.3.2. Literature Resources

Table 3. Publisher wise search strings

Repository	Search Strings
PLOS	((((“ALL METADATA”) (“ALL METADATA”)(“BLOCKCHAIN” AND (“CONSENSUS PROTOCOLS” OR “PROOF OF WORK” OR “PROOF OF STAKE” OR “BYZANTINE FAULT TOLERANCE” OR “PROOF OF SPACE & CAPACITY” OR “PROOF OF ELAPSED TIME”)
PMC	((((“ALL METADATA”) (“ALL METADATA”)(“BLOCKCHAIN” AND (“CONSENSUS PROTOCOLS” OR “PROOF OF WORK” OR “BYZANTINE FAULT TOLERANCE” OR “PROOF OF STAKE” OR “PROOF OF SPACE & CAPACITY” OR “PROOF OF ELAPSED TIME”))
Oxford Academics	((((“ALL METADATA”) (“ALL METADATA”)(“BLOCKCHAIN” AND (“CONSENSUS PROTOCOLS” OR “PROOF OF STAKE” OR “BYZANTINE FAULT TOLERANCE” OR “PROOF OF SPACE & CAPACITY” OR “PROOF OF WORK” OR “PROOF OF ELAPSED TIME”))
Springer Link	((((“ALL METADATA”) (“ALL METADATA”)(“BLOCKCHAIN” AND (“CONSENSUS PROTOCOLS” OR “BYZANTINE FAULT TOLERANCE” OR “PROOF OF WORK” OR “PROOF OF STAKE” OR “PROOF OF SPACE & CAPACITY” OR “PROOF OF ELAPSED TIME”)
Science Direct	((((“ALL METADATA”) (“ALL METADATA”)(“BLOCKCHAIN” AND (“CONSENSUS PROTOCOLS” OR “PROOF OF WORK” OR “PROOF OF STAKE” OR “BYZANTINE FAULT TOLERANCE” OR “PROOF OF ELAPSED TIME” OR“PROOF OF SPACE & CAPACITY”)
IEEE Xplore	((((“ALL METADATA”) (“ALL METADATA”)(“BLOCKCHAIN” AND (“CONSENSUS PROTOCOLS” OR “PROOF OF WORK” OR “PROOF OF ELAPSED TIME” OR“PROOF OF STAKE” OR “BYZANTINE FAULT TOLERANCE” OR “PROOF OF SPACE & CAPACITY”))
ACM Digital Library	((((“ALL METADATA”) (“ALL METADATA”)(“BLOCKCHAIN” AND (“CONSENSUS PROTOCOLS” OR “PROOF OF WORK” OR “PROOF OF STAKE” OR “PROOF OF SPACE & CAPACITY” OR “PROOF OF ELAPSED TIME” OR “BYZANTINE FAULT TOLERANCE”)

The detailed and best projecting papers have been nominated to make a literature analysis from accessible sources, dedicated to research journals and meetings.

The facts of specific origins, functional search sequences, and outcomes are stated in Table 3.

3.3.3. Inclusion and Exclusion Criteria

Table 4. Technique to evaluate the quality.

Sl. No.	Assessment Questions	Expected Answers	Score
Internal Scoring			
1	Was abstract well described?	a. Yes b. Intermediate c. No	1 0.5 0
2	Was the background/literature review described in detail?	a. Yes b. Intermediate c. No	1 0.5 0
3	Was the data collection mechanism clearly defined?	a. Yes b. Intermediate c. No	1 0.5 0
4	Was the feature description/selection defined clearly?	a. Yes b. Intermediate c. No	1 0.5 0
5	Was the methodology section clearly defined?	a. Yes b. Intermediate c. No	1 0.5 0
6	Was the result assessment well described valid and reliable?	a. Yes b. Intermediate c. No b. No	1 0.5 0 0
7	Was the conclusion relevant and effectively based on results?	a. Yes b. Intermediate c. No	1 0.5 0
External scoring (based on publication source)			
8	A study published in CORE ranked conference, proceedings, and symposium.	a. CORE rank A b. CORE rank B c. CORE rank C d. No CORE ranking	1.5 1 .0.5 0
9	A study published in JCR listed ranked journal	a. JCR rank Q1 b. JCR rank Q2 c. JCR rank Q3/Q4 d. No JCR ranking	2 1.5 1 . 0

After the execution of the search, we started to examine the titles, Abstracts, summary, or conclusion for the inclusion and exclusion purpose. We designed an excel sheet with different parameters that we set up for data extraction as well as making sure that they can include or exclude. With the help of an Excel sheet, we extracted almost all the important data for our paper. In Table 4, the scoring of the paper is defined by evaluation criteria.

4. DATA ANALYSIS

In this section, we accumulate the outcomes and present a pure assessment of all certain research papers. The designated articles were examined to efficiently respond to the research problems. The primary fragment confers the search fallouts attained over the distinct search series and the second is the explanation of the valuation scores and the concluding portion is devoted to the inclusive deliberations to riposte the research inquiries. The procedure of the selection represented in figure 3 that first, we collect all the papers then we search on the root of title, after finding the papers duplicate papers were removed, after removing duplication the papers were selected based on good abstracts and then full text-based search and then the papers were analysed to make them finalized research papers.

4.1. Search Scheme

Table 5. Publisher Based Stage Wise Selection Process.

Database/Repository	Primary Search	P-I	P-II	P-III	P-IV
PLOS	22680	5	25	9	5
SPRINGER LINK	11434	26	16	5	2
SCIENCE DIRECT	4	17	12	5	2
IEEE XPLORE	7970	6661	159	5	3
ACM DIGITAL LIBRARY	122,852	13	7	6	4
TOTAL	**164,940**	**6722**	**219**	**30**	**16**

The primary search procedure produces a total of 164,940 articles from numerous digital databases. On this assortment, the selection procedure labeled in the forgoing fragment was useful. The stages elaborate in the selection procedure have also been designated underneath in Figure 3 and stage levels variety results are articulated in Table 5.

The title-created selection was achieved through dualistic authors in phase I as P-I, fallouts in the assortment of 6722 articles. Succeeding, the replica articles were detached in phase as P-II, and area extraneous articles were also segregated based on insertion and elimination standards delineated in an earlier segment.

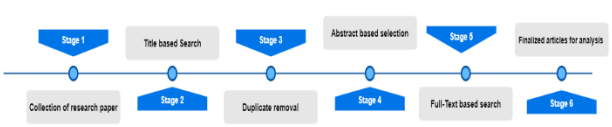

Figure 3 Selection Procedure.

4.2. Quality Valuation Score

According to the scoring method precise beyond the scores were expected to individually designated study, assessed interpreting to the inner and outer measures are specified in Table VI. The scores found over the exterior and interior criteria are signified as E-Score and I-Score

congruently and publication type as P. Type. Available designated articles, 20% recognized a supreme score superior to 6 and restrained in the great classified articles, 80 % articles get fixed rank although just 4 out of 16 articles were 10% experiential in not well ranked conferring to the criteria. Figure 4 depicts the actualities, illustrative a high attain trust in the excellence of nominated articles. However, no removal was prepared on an eminence basis. In Table 6, domains termed consensus protocol with keyword CP and proof of stake with PoS used, others are stated in Figure 2 of keywords.

4.3. Details of Research Questions

Table 6. Quality assessment score based on publisher.

Sl. No.	P. Type	Publisher	Domain	I-Score	E-Score	Total Score
[1]	Conference	IEEE	CP	7.0	1.0	8.0
[2}	Survey	Research gate	CP	4.0	2.0	6.0
[3]	Conference	IEEE	CP	8.0	2.0	10.0
[4]	conference	IEEE	PoS	7.5	2.0	9.5
[5]	Conference	IEEE	CP	5.0	2.0	7
[6]	Survey	IEEE	CP	5.0	1	6.0
[7]	Survey	IEEE	PoS	5.0	2	7
[8]	Conference	IEEE	CP	6.0	2	8.0
[9]	Conference	IEEE	CP	6.0	2.0	8.0
[10]	Conference	IEEE	CP	5.0	2.0	7.0
[11]	Research Paper	IEEE	CP	4.0	1.0	5.0
[12]	Research Paper	Science Direct	CP	5.0	1.0	6.0
[13]	Survey	IEEE	CP	5.0	1.0	6.0
[14]	Research Paper	IEEE	CP	7.0	2.0	8.0
[15]	Conference	IEEE	CP	5.0	3.0	8.0
[16]	Survey	Research gate	CP	4.0	2.0	6.0

In this fragment, 14 leading articles were examined on the foundation of research questions considered in Table I. Details removed later the scrutiny of the chosen analysis were considered based on queries for the valuation of disengaged material.

4.3.1. What Are Existed Variants of Consensus Protocols

Consensus protocols use different domains other than block0 chains are physical systems, the internet of vehicles (IoV), and the internet of things. Some variants are described as Proof of Elapsed Time (PoET) influences the use of Trusted Protocol TEEs (Trusted Execution Environment for example SGX-enabled CPUs for Intel [2]. It compromises the solution byzantine general issues. It was industrialized at Intel in the initial time of 2016 as a fragment of their effort on the hyper ledger scheme [6]. The Hyper Ledger (Sawtooth) Indy is a digital Currency sustainability system developed to eliminate identity management violations on the Web. Zero Information Proof (ZKP) is used to avoid identification functionality from being exposed [7]

Proof of Luck is also a variant of consensus protocol that depends on a private blockchain and is based on the use of a World for Trusted Implementation (TEEs), i.e. SGX Intel [2]. It retains low transaction delay by consuming limited energy and processing capacity. Nodes are requesting a random number from the TEE, so a node that is stronger in luck is preferred to evaluate the block. The downside of proof of luck is that it needs unique hardware [3]. PoL is identical to PoET, although it often produces randomization referring to as luck [6].

Proof of Activity is a combination of proof of work and proof of stake proposed in 2012. It is multi-layered and needs POW. In this, for the authentication of the block, POW must be prepared in the first place. The node that resolves a block of the cryptographic problem is a matter of POS. The Chance of the node being designated is equal to the node balances. For preference up the group pf validators, a function called follow the Satoshi is provided to use. When all the validators authorize the block, the block is authenticated [3].

Proof of Space, storage, and capacity is also recognized as proof of storage, and proof of capacity uses disk storage instead of high computation power. It is an open distributed ledger because it consumes free disk storage as resource utilization [2] [6]. One way of applying proof of space is using rigid to stone grids. Proof of space is dependent on disk space and is unaffected by ASIC (Australian Securities and Investments Commission [3]. Proof of Vote: POV is the well-organized version of PoW. Authentication of the blocks in the network is prepared by using the voting contrivance. The indication behind the algorithm is to generate altered security individualities for the contributing nodes. The compensations of PoV over PoW are controllable security, less verification delay, and more reliability [9]. Proof of Spacetime (PoSt) contains two stages which are the configuration process and the deployment phase. It requires less effort, time, and energy to approve the block in the blockchain. In proof of space, the disk space can be recycled, which can contribute to the expense of proof being randomly short. To reduce this Dispute, Proof of Space & Time preserves data over some time [3]

Proof of Burn is key to the shortcomings in proof of work like it solves some problems of POW. The knowledge behind proof of burn is to burn coins, decreasing vigor waste in proof of work. Burn Proof [6] is combined with POW and POS to deliver block cohort and network safety. Burning coins means distribution of coins to a distinctive address where coins cannot be spent in conjunction with cryptographic tools. Burn evidence can be used as a feasible conversion mechanism from one cryptocurrency to another. Evidence of the burning

system is still vulnerable to a 51 percent strike. A node with 51 percent hash power is capable of attacking the device, although it is not vibrant exactly what hash power is and how to measure it [3].

PoI (importance) is an updated form of POS, if there is a need for distribution of the form of resources that was invented in 2015[6], Proof of Retrievability is a protocol of consensus that ensures the presence of peer information by checking the availability and integrity of small data chunks [2]. PoR was initially suggested by Juels et al. in 2007 as a cryptographic construction for a semi-trusted distribution archiving system. It was first used by the cryptocurrency Perm coin projected by Miller et al in 2014 [8]. Proof of Identity is a member of evidence that helps each individual to distinguish a sequestered key that suits the agreed cryptographically and uniqueness as an identity connected to a real transaction [7].

Proof of Trust is the Cannabis Consensus is operating in four stages. It is an improved algorithm than the rest of the consensus algorithms in terms of compromise, scalability, equality, reliability, and performance. PoT is blamed for assaults by Sybil and Conspiracy. PoT-based protocols will effectively connect real blocks to the chain in just four seconds [9]. Tangle is a block-less blockchain that is dependent on a directed acyclic graph that provides high scalability at minimum cost [2]. In Tangle network signing, tip selection, proof of work requires to mine a block [3].]. A statistical chart of consensus protocols of the top 50 cryptocurrencies shown in Figure 4.

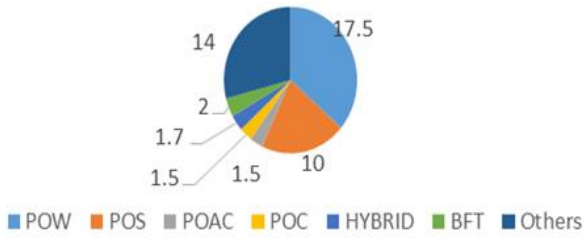

Figure 4 Consensus Protocols statistical chart (April 2019).

Figure 4 represents the hierarchy of the consensus protocol, the highlighted area includes in our research, and the rest of the others are the bonus of this hierarchy. The most left side of the diagram shows the types of the consensus protocol and their variants relatively.

4.3.2. How Consensus Protocols Helps Blockchain to Enhance Its Usability?

In this section, we identified the main used protocols in blockchain according to their scalability, throughput, implementation with computational power, and requirements. In [2], [3], [4], [6], [7], [17], and [18] scalability, throughput, implementation and their variants defined but not formed in a way of comparison like we did in Table IV. Every protocol has its own using capability, there are many other protocols discovered by using previous protocols, companies and users can choose protocol according to their need by viewing their advantage.

4.3.3. What Are Strengths and Weaknesses That Are Beneficial as Well as Disadvantageous?

In this question, we have created a strength and weakness table for protocols to identify which existing approach is better than the traditional one. We have analyzed all 16 papers included in my SLR this table includes all the consensus protocols with their citation and year. All the consensus protocols have their strengths and their weakness. All those protocols that do not have any weakness are not implemented yet because authors write their description only but not their implementation or any use case to briefly identify their usage. In the papers [5], [7], [10], [11], [12], [13], [14], [15] and [16], the strength and their relevant weaknesses are collected and defined in the table below. All the consensus protocols are categorized with their origination year and their relevant papers from which the data was extracted and defined in the form of a table. Some consensus protocols have no implementation because they do not have any proof that they are applicable. So because of that, they have no weakness.

5. CONCLUSION

The Rapid development of blockchain in the field of business and It industry made it a promising technology for the past 10 to 15 years and in many other areas too. It provides decentralization data security but many sectors are facing security and risks while using the consensus protocols as they need high computational power to solve the puzzles to add their block in the blockchain. According to some companies, based on market needs, if speed is more important or protection is more essential, companies may minimize or raise the degree of complexity appropriately. The greater the level of proficiency, the slower the mining pace, and the lower the level of difficulty, the higher the mining speed. In our review, we have found that POW is not the best approach and protocol, every protocol has a problem most companies use proof of work still, to solve their computational puzzles and for adding a block in the blockchain. We identify that POS and DPOS are much better protocols than POW In our paper, We have made a taxonomy of all consensus protocols with their variants. we have also provided the scoring and publisher-based selection criteria. A comparative analysis table has been made with the most used consensus protocol and lastly, we have described all the existing and previous protocols with their advantage and disadvantage, their invention, and implantation year. Every protocol has its usage so the best suitable approach can be decided. According to my analysis table, the PoW finds it difficult to implement

because of its high computational Power cost. Many other consensus protocols have been discovered with their variants so we can choose other protocols for our work instead of using PoW at high risk.

REFERENCES

[1] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2017, pp. 1-5, DOI: 10.1109/ICACCS.2017.8014672.

[2] Vistro, D. M., Rehman, A. U., Abid, A., Farooq, M. S., & Idrees, M. (2020). ANALYSIS OF CLOUD COMPUTING BASED BLOCKCHAIN ISSUES AND CHALLENGES. Journal of Critical Reviews, 7(10), 1482-1492..

[3] Q. He, N. Guan, M. Lv, and W. Yi, "On the Consensus Mechanisms of Blockchain/DLT for Internet of Things," 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), Graz, 2018, pp. 1-10, DOI: 10.1109/SIES.2018.8442076.

[4] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," in IEEE Access, vol. 7, pp. 118541-118555, 2019, DOI: 10.1109/ACCESS.2019.2935149.

[5] M. Memon, U. A. Bajwa, A. Ikhlas, Y. Memon, S. Memon, and M. Malani, "Blockchain Beyond Bitcoin: Block Maturity Level Consensus Protocol," 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bangkok, Thailand, 2018, pp. 1-5, DOI: 10.1109/ICETAS.2018.8629232.

[6] Khan, N. S., Shahzada, A., Ata, S., Abid, A., Farooq, M. S., Mushtaq, M. T., & Khan, I. (2014). A vision based approach for Pakistan sign language alphabets recognition.

[7] N. Ramkumar, G. Sudhasadasivam and K. G. Saranya, "A Survey on 18. Vistro, D. M., Rehman, A. U., Abid, A., Farooq, M. S., & Idrees, M. (2020). IoT based Big Data Analytics for Cloud Storage Using Edge Computing. Journal of Critical Reviews, 12(07 Special Issue), 1594-1598..

[8] K. Sharma and D. Jain, "Consensus Algorithms in Blockchain Technology: A Survey," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-7, DOI: 10.1109/ICCCNT45670.2019.8944509.

[9] S. J. Alsunaidi and F. A. Alhaidari, "A Survey of Consensus Algorithms for Blockchain Technology," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-6,

[10] Farooq, M. S., Khan, M., & Abid, A. (2020). A framework to make charity collection transparent and auditable using blockchain technology. Computers & Electrical Engineering, 83, 106588.

[11] "Shijie Zhang, Jong-Hyouk Lee, Analysis of the main consensus protocols of blockchain, ICT Express, Volume 6, Issue 2,2020, Pages 93-97, ISSN 24059595,https://doi.org/10.1016/j.icte.2019.08.00 "

[12] L. M. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018, pp. 1545-1550, DOI: 10.23919/MIPRO.2018.8400278.

[13] Lepore C, Ceria M, Visconti A, Rao UP, Shah KA, Zanolini L. A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS, and Pure PoS. Mathematics. 2020; 8(10):1782. https://doi.org/10.3390/math8101782

[14] C. Gupta and A. Mahajan, "Evaluation of Proof-of-Work Consensus Algorithm for Blockchain Networks," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, DOI: 10.1109/ICCCNT49239.2020.9225676.

[15] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia and T. K. Patra, "Study of Blockchain-Based Decentralized Consensus Algorithms," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 908-913, DOI: 10.1109/TENCON.2019.8929439.

[16] Xiao, Yang & Zhang, Ning & Lou, Wenjing & Hou, Y.. (2019). A Survey of Distributed Consensus Protocols for Blockchain Networks.

[17] Medium @ianbondw (2020, 22 March).“Proof of work” vs. “Proof of stake” vs. other Byzantine Fault Tolerances" available at" https://medium.com/@ianbondw/proof-of-work-vs-proof-of-stake-vs-other-byzantine-fault-tolerances-

[18] TheAcadameybinance (2020, 22 March). "Byzantine Fault Tolerance Explained" available at https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained.

[19] Prabu, S., Velan, B., Jayasudha, F.V., Visu, P. and Janarthanan, K., 2020. Mobile technologies for contact tracing and prevention of COVID-19 positive cases: a cross-sectional study. International Journal of Pervasive Computing and Communications.

[20] Subramani, P., Al-Turjman, F., Kumar, R., Kannan, A. and Loganthan, A., 2021. Improving medical communication process using recurrent networks and wearable antenna s11 variation with harmonic suppressions. Personal and Ubiquitous Computing, pp.1-13.

[21] Nguyen, T.N., Le, V.V., Chu, S.I., Liu, B.H. and Hsu, Y.C., 2021. Secure Localization Algorithms Against Localization Attacks in Wireless Sensor Networks. Wireless Personal Communications, pp.1-26.

[22] Karuppusamy, P., Perikos, I., Shi, F. and Nguyen, T.N., 2020. Sustainable communication networks and application. Lecture Notes on Data Engineering and Communications Technologies, pp.65-72.

[23] Ranjan, G., Nguyen, T.N., Mekky, H. and Zhang, Z.L., 2020, December. On virtual id assignment in networks for high resilience routing: a theoretical framework. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-6). IEEE.

[24] Vadivel, S., Konda, S., Balmuri, K.R., Stateczny, A. and Parameshachari, B.D., 2021. Dynamic Route Discovery Using Modified Grasshopper Optimization Algorithm in Wireless Ad-Hoc Visible Light Communication Network. Electronics, 10(10), p.1176.

[25] Parameshachari, B.D. and Panduranga, H.T., 2021. Secure Transfer of Images Using Pixel-Level and Bit-Level Permutation Based on Knight Tour Path Scan Pattern and Henon Map. In Cognitive Informatics and Soft Computing (pp. 271-283). Springer, Singapore.

[26] Puttamadappa, C. and Parameshachari, B.D., 2019. Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique. Microprocessors and Microsystems, 71, p.102886.

[27] N. Shi, L. Tan, W. Li, X. Qi, K. Yu, "A Blockchain-Empowered AAA Scheme in the Large-Scale HetNet", Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2020.10.002.

[28] L. Tan, H. Xiao, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-empowered Crowdsourcing System for 5G-enabled Smart Cities", Computer Standards & Interfaces, https://doi.org/10.1016/j.csi.2021.103517

[29] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava and P. Chatterjee, "Efficient and Privacy-Preserving Medical Research Support Platform Against COVID-19: A Blockchain-Based Approach", IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2020.3035520.

[30] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Network, vol. 35, no. 1, pp. 130-137, January/February 2021, doi: 10.1109/MNET.011.2000223.

[31] L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-Empowered Access Control Framework for Smart Devices in Green Internet of Things", ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-20, 2021,https://doi.org/10.1145/3433542.