2) Apostolici, Zohar, and Facade, 2017 have brought up that, since they control traffic interfaces, enormous ISPs could adequately separate disjointed pieces of the bitcoin network with steering assaults. This, be that as it may, would just briefly affect hubs because there are various alternative ways for a hub to acknowledge it is done continuously and in the principal chain. For instance, they believed public elements could be gotten to through HTTP and utilized as square travelers. Moreover, ISPs could imperceptibly defer information proliferation by a limit of the Bitcoin association break limit.
3) The evidence of work successfully forestalls Sybil's mining assaults and, therefore, her emblematic impact at the framework level. Be that as it may, if an assaulted hub or set of hubs isn't associated with an ordinary hub, postponing, and diverting associations are hypothetically conceivable.
4) A framework can't forestall all security-related assaults that are normal on PC organizations. A few hubs' characters can be uncovered considering assaults. Be that as it may, if the hidden computerized signature conspire is numerically functional, the whole exchange framework is unaffected.

4.3 IPFS Bandwidth Analysis

Running an IPFS node currently necessitates the use of significant bandwidth, which may be prohibitively expensive for many users, particularly in developing countries. Excessive bandwidth consumption can harm IPFS's acceptance in many parts of the world. Although there are numerous solutions to this problem, financial incentives can point the way in the right direction. Gaining monetary rewards for hosting content in IPFS can assist in covering the cost of running nodes and encourage adoption.

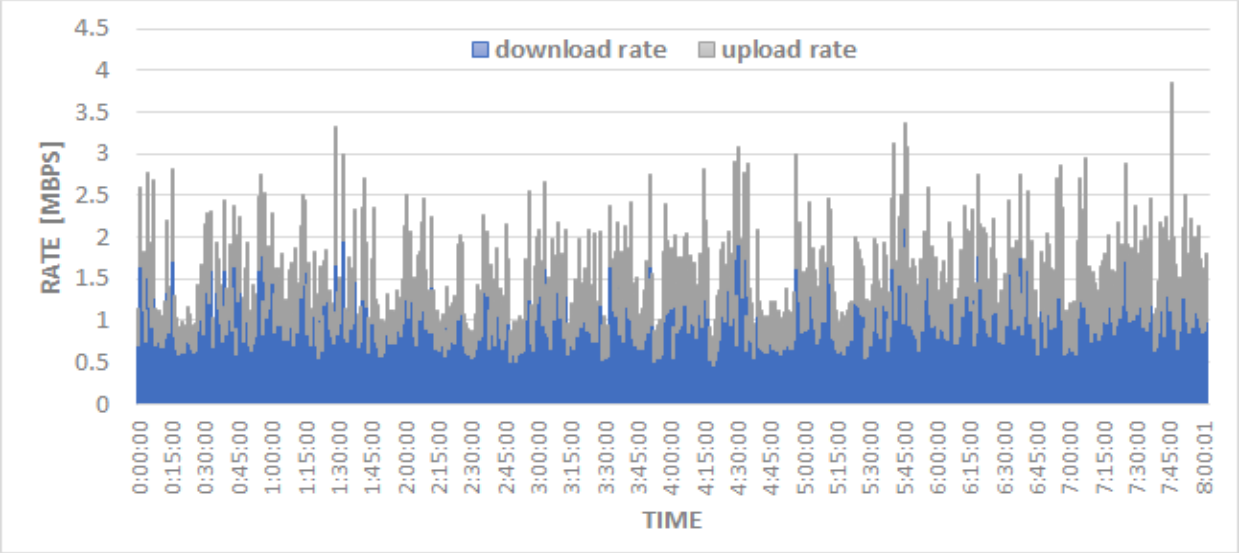

Figure 8. IPFS Bandwidth Analysis

In our experimental, IPFS node's bandwidth usage, the node was not used to browse or download any IPFS content during this test. However, over 8 hours, our node downloaded/uploaded more than 5 GB of data.

4.4 Ethereum Network Hash Rate

Running an IPFS on a decentralized or peer-to-peer network, combining the effects and analysis of current and historical data sets, has a high hash rate, which means the hash produced and deployed on smart contracts has a high rate and is increasing. From July 2015 to July 2019, the graph above illustrates the hash rate results. We are using a secondary dataset rather than a primary dataset, and the results are produced using Google's Data Studio.

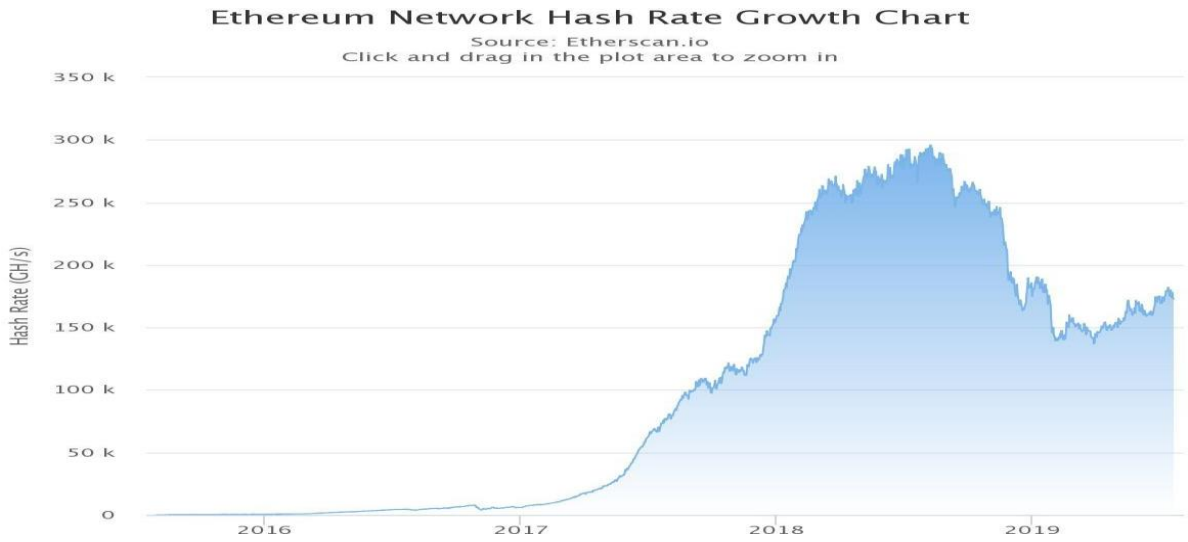

Figure 9. Yearly based Analysis of Ethereum's hash rate

The graph above shows an estimate of how many hashes ETH miners perform per year and how this has changed over time. If we look at the EHT hash rate per day, minute, or second, we can see how it compares to other cryptocurrencies. The only reason for this is the cost of writing your smart contract code. As it takes the hash of the file storage generated by IPFS, Ethereum can be used to form the blockchain and deploy smart contracts on the network

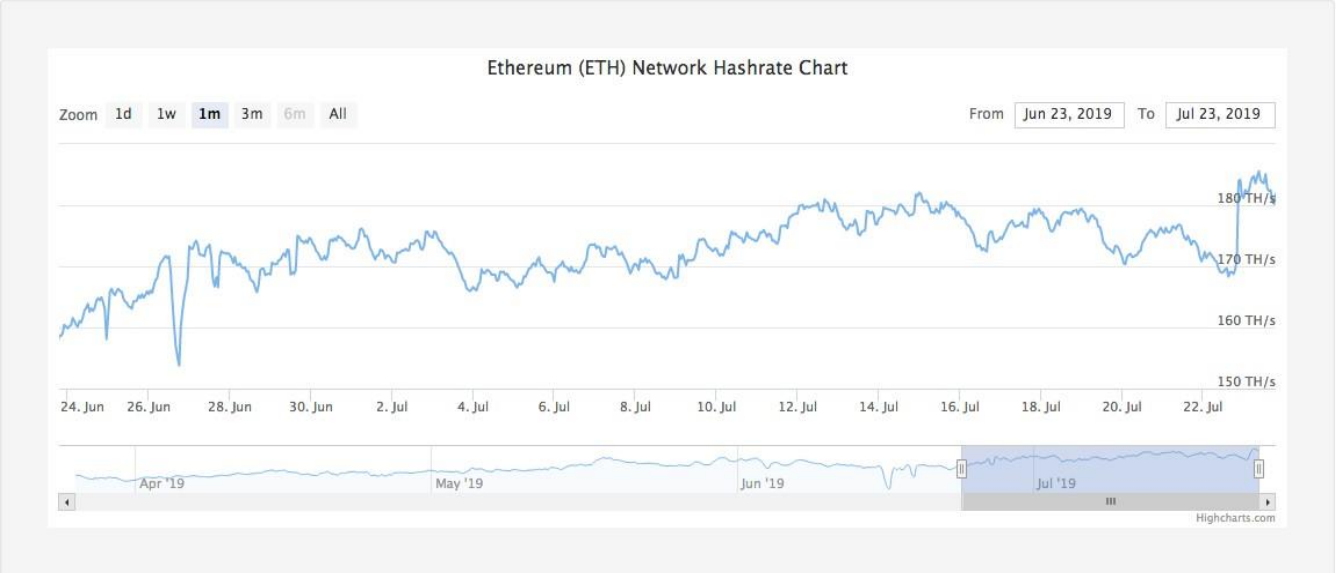

Figure 10. Analysis of the ETH hash rate per minute

The above diagram shows the clear growth rate of the hash rate of ETH, like how the USD dollar rate is increasing internationally, and how its value is increasing based on code generation and code deployment using smart contracts. The reason for this is that smart contracts for bitcoin currency are difficult and expensive to write. As a result, ETH is bridging the price gap between bitcoin and ETH.

The above analysis and experiment were performed on secondary data, and the results are publicly available on etherscan.io, which updates at a per second rate. Moving on to another secondary dataset downloaded in CSV format from the Kaggle website. The dataset is simple to download and run the test.

Figure 11. Hash rate Analysis of ETH using Data Studio

The graph above depicts the hash rate results from July 2015 to July 2019. The graph above depicts the high hash rate produced by the ETH blockchain. The reason for this is that all nodes can be tested by the test network, allowing everyone to evaluate the ETH blockchain and create their blockchain technology with any cryptocurrency name. The results are obtained from the Kaggle website, which provides us with the actual and real dataset. Because we are using a secondary dataset rather than a primary dataset, the results are obtained using Data Studio, a Google product.

5. Conclusion

The educational industry is facing several challenges. Most of them are concerned with data transfer and security. This paper discusses the advantages and disadvantages of using trending technologies such as blockchain and IPFS to solve the secure digital transactional problem in the education sector. The technologies mentioned above are closely related to IoT. The IoT ecosystem has encountered data security and privacy issues. Blockchain, a type of distributed ledger technology, has received a lot of attention recently in areas other than cryptocurrency. That's what you call blockchain and IoT (Internet of Things), blockchain and security, blockchain and finance, and blockchain and logistics. It is necessary to ensure secure data storage. Blockchain, in conjunction with IPFS, can undoubtedly meet such demands in the educational industry. The main benefit is decentralized data storage while ensuring the credibility and immutability of stored data, removing the need for a middleman. As a result, these technologies have the potential to be a valuable supplement to education.

The IPFS network, a Blockchain-based peer-to-peer hypermedia protocol, officially launches its file storage network on Ethereum rather than Bitcoin and explains it to the Ethereum network development community, as well as several innovative features. As a result, this research paper provides a proper demonstration of data storage without the use of a centralized system. On a decentralized and distributed P2P network, data can always be present. IPFS greatly aids in the segmentation of data for storage purposes. It can be deployed on the network using smart contracts using the hashing technique. The relevant characteristics of these technologies that can improve the possibilities over existing solutions provide answers to the education sector's various challenges. The answers are primarily concerned with the amount of data sent and the reduction of waiting time, as well as ensuring the transparency, security, and credibility of processes and services in the education sector.

References

[1] S. Vellinga, G. K. L. Kumar, and P. Karthikeyan, "Unsupervised Blockchain for Safeguarding Confidential Information in Vehicle Assets Transfer," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, Mar. 2020, pp. 44–49. doe: 10.1109/ICACCS48705.2020.9074285.

[2] M. InSite and K. R. Lakhani, "The Truth About Blockchain," p. 12.

[3] J. P. Mohanty and K. K. Mahapatra, "Security Vulnerabilities in Applying Decentralized Ledger Systems for Obfuscating Hardware's," in *2019 IEEE International Symposium on Smart Electronic Systems (issues) (Formerly ins)*, Rourkela, India, Dec. 2019, pp. 272–275. doe: 10.1109/iSES47678.2019.00067.

[4] M. Bucolic, "Rethinking Permissioned Blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies, and Contracts*, Abu Dhabi United Arab Emirates, Apr. 2017, pp. 3–7. doe: 10.1145/3055518.3055526.

[5] J. Goel, N. Bhatt, and D. N. Kumar, "Raspberry Pi Home Automation System Using Mobile App to Control Devices," vol. 6, no. 5, p. 8, 2007.

[6] K. C. Swain, S. J. Thomson, and H. P. W. Jayasuriya, "Adoption of an Unmanned Helicopter for Low-Altitude Remote Sensing to Estimate Yield and Total Biomass of a Rice Crop," *Transactions of the ASABE*, vol. 53, no. 1, pp. 21–27, 2010, doe: 10.13031/2013.29493.

[7] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," *arXiv:1805.11390 [cs]*, May 2018, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1805.11390

[8] A. M. Antonopoulos, *Mastering Bitcoin*, First edition. Sebastopol CA: O'Reilly, 2015.

[9] I. Modal and E. G. Serer, "Majority is not Enough: Bitcoin Mining is Vulnerable," *arXiv:1311.0243 [cs]*, Nov. 2013, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1311.0243

[10] E. Andreoulakis *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth Neurosis Conference*, Porto Portugal, Apr. 2018, pp. 1–15. doe: 10.1145/3190508.3190538.

[11] B. Rao, A. G. Gopi, and R. Maine, "The societal impact of commercial drones," *Technology in Society*, vol. 45, pp. 83–90, May 2016, doe: 10.1016/j.techsoc.2016.02.009.

[12] D. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," P. 34.

[13] G. Ziskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, San Jose, CA, May 2015, pp. 180–184. doe: 10.1109/SPW.2015.27.

[14] A. Nisha, S. Richards, D. Breen, J. Robertson, and B. Breen, "Thermal infrared imaging of geothermal environments and by an unmanned aerial vehicle (UAV): A case study of the Wairakei – Tauhara geothermal field, Taupo, New Zealand," *Renewable Energy*, vol. 86, pp. 1256–1264, Feb. 2016, doe: 10.1016/j.renene.2015.09.042.

[15] G. Ziskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, San Jose, CA, May 2015, pp. 180–184. doe: 10.1109/SPW.2015.27.

[16] M. Swan, *Blockchain: a blueprint for a new economy*, First edition. Beijing: Sebastopol, CA: O'Reilly, 2015.

[17] I. Braid, "Spatial variability of surface properties and estimation of surface fluxes of a savannah," *Agricultural and Forest Meteorology*, vol. 89, no. 1, pp. 15–44, Jan. 1998, doe: 10.1016/S0168-1923(97)00061-0.

[18] K. Christakis, "Blockchain-Based Local Energy Markets," p. 190.

[19] M. Crosby, "Blockchain Technology: Beyond Bitcoin," no. 2, p. 16, 2016.

[20] F. A. Vega, F. C. Ramírez, M. P. Sais, and F. O. Rosa, "Multi-temporal imaging using an unmanned aerial vehicle for monitoring a sunflower crop," *Biosystems Engineering*, vol. 132, pp. 19–27, Apr. 2015, doe: 10.1016/j.biosystemseng.2015.01.008.

[21] E. R. Hunt *et al.*, "REMOTE SENSING OF CROP LEAF AREA INDEX USING UNMANNED AIRBORNE VEHICLES," p. 9, 2008.

[22] A. Dori, S. S. Kan here, R. Jurak, and P. Gaur avaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (Precoma Workshops)*, Kona, HI, Mar. 2017, pp. 618–623. doe: 10.1109/Percomw.2017.7917634.

[23] E. Honhaar *et al.*, "Processing and Assessment of Spectrometric, Stereoscopic Imagery Collected Using a Lightweight UAV Spectral Camera for Precision Agriculture," *Remote Sensing*, vol. 5, no. 10, pp. 5006–5039, Oct. 2013, doe: 10.3390/rs5105006.

[24] K. Flynn and S. Chopra, "Remote Sensing of Submerged Aquatic Vegetation in a Shallow Non-Turbid River Using an Unmanned Aerial Vehicle," *Remote Sensing*, vol. 6, no. 12, pp. 12815–12836, Dec. 2014, doe: 10.3390/rs61212815.

[25] C. Caching and M. Bucolic, "Blockchain Consensus Protocols in the Wild," *arXiv:1707.01873 [cs]*, Jul. 2017, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1707.01873

[26] H. Wang, Z. Zheng, S. Xia, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a

survey," *IJWGS*, vol. 14, no. 4, p. 352, 2018, doe: 10.1504/IJWGS.2018.10016848.
[27] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 9.
[28] C. Caching, "Architecture of the Hyperledger Blockchain Fabric," p. 4.
[29] Z. Zheng, S. Xia, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (Bigdata Congress)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564. doe: 10.1109/BigDataCongress.2017.85.
[30] V. Varsha and R. Singh Chiller, "Data Hiding using Advanced LSB with RSA Algorithm," *IJCA*, vol. 122, no. 4, pp. 41–45, Jul. 2015, doe: 10.5120/21691-4796.
[31] V. S, "An Enhanced Multimedia Video Surveillance Security Using Wavelet Encryption Framework," *JMM*, May 2020, doe: 10.13052/jmm1550-4646.1534.
[32] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems," *arXiv:1802.06993 [cs]*, Nov. 2020, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1802.06993
[33] I.-C. Lin and T.-C. Liao, "A Survey of Blockchain Security Issues and Challenges," p. 7.
[34] V. Butlerin, "A Next-Generation Smart Contract & Decentralized Application Platform," P. 36.
[35] J. Sharma and R. Thapa, "Hybrid approach for data security using RSA and LSB Algorithm," p. 6.
[36] X. X. Zheng, L. R. Li, and Y. J. Shao, "A GSM-Based Remote Temperature and Humidity Monitoring System for Granary," *MATEC Web of Conferences*, vol. 44, p. 01060, 2016, doe: 10.1051/metacone/20164401060.
[37] A. Jaiswal, S. Chandel, A. Mazumdar, M. G.M., C. Modi, and C. Jayanthi, "A Conceptual Framework for Trustworthy and Incentivized Trading of Food Grains using Distributed Ledger and Smart Contracts," in *2019 IEEE 16th India Council International Conference (INDICON)*, Rajkot, India, Dec. 2019, pp. 1–4. doe: 10.1109/INDICON47234.2019.9030290.
[38] M. Rises and K. Sopher, "A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There," *Bus Inf Sits Eng.*, vol. 59, no. 6, pp. 385–409, Dec. 2017, doe: 10.1007/s12599-017-0506-0.
[39] A. M. Khaleghi *et al.*, "A DDDAMS-based planning and control framework for surveillance and crowd control via UAVs and UGVs," *Expert Systems with Applications*, vol. 40, no. 18, pp. 7168–7183, Dec. 2013, doe: 10.1016/j.eswa.2013.07.039.
[40] A. Mathews and J. Jensen, "Visualizing and Quantifying Vineyard Canopy LAI Using an Unmanned Aerial Vehicle (UAV) Collected High-Density Structure from Motion Point Cloud," *Remote Sensing*, vol. 5, no. 5, pp. 2164–2183, May 2013, doe: 10.3390/rs5052164.
[41] J. Leakey, *Evaluating computer-assisted language learning: an integrated approach to effectiveness research in CALL*. Oxford; New York: Peter Lang, 2011.
[42] M. Govender, K. Chetty, and H. Bullock, "A review of hyperspectral remote sensing and its application in vegetation and water resource studies," *WSA*, vol. 33, no. 2, Dec. 2009, doe: 10.4314/was. v33i2.49049.
[43] J. T. Luxhøj, "A Sociotechnical Model for Analysing Safety Risk of Unmanned Aircraft Systems (UAS): An Application to Precision Agriculture," *Procedia Manufacturing*, vol. 3, pp. 928–935, 2015, doe: 10.1016/j.promfg.2015.07.140.
[44] C. G. Sorensen *et al.*, "A user-centric approach for information modelling in arable farming," *Computers and Electronics in Agriculture*, vol. 73, no. 1, pp. 44–55, Jul. 2010, doe: 10.1016/j.compag.2010.04.003.
[45] J. Gago *et al.*, "UAVs challenge to assess water stress for sustainable agriculture," *Agricultural Water Management*, vol. 153, pp. 9–19, May 2015, doe: 10.1016/j.agwat.2015.01.020.
[46] S. Gethin, R. Nuke, and K. Wiegand, "Using Unmanned Aerial Vehicles (UAV) to Quantify Spatial Gap Patterns in Forests," *Remote Sensing*, vol. 6, no. 8, pp. 6988–7004, Jul. 2014, doe: 10.3390/rs6086988.
[47] Q. Feng, J. Liu, and J. Gong, "UAV Remote Sensing for Urban Vegetation Mapping Using Random Forest and Texture Analysis," *Remote Sensing*, vol. 7, no. 1, pp. 1074–1094, Jan. 2015, doe: 10.3390/rs70101074.
[48] M. Elaraby, A. M. Clavicle, A. F. Torres-Rau, I. MassLive, and M. McKee, "Estimating chlorophyll with thermal and broadband multispectral high-resolution imagery from an unmanned aerial system using relevance vector machines for precision agriculture," *International Journal of Applied Earth Observation and Geoinformation*, vol. 43, pp. 32–42, Dec. 2015, doe: 10.1016/j.jag.2015.03.017.
[49] S. R. Hurwitz *et al.*, "Coffee Field Ripeness Detection Using High-Resolution Imaging Systems on a Solar-Powered UAV," p. 3.
[50] M. Radames and M. Kumar, "Flight formation of UAVs in presence of moving obstacles using fast-dynamic mixed-integer linear programming," *Aerospace Science and Technology*, vol. 50, pp. 149–160, Mar. 2016, doe: 10.1016/j.ast.2015.12.021.