# Autonomous Agents Powered by Blockchain Technology

## Overview

Traditional Internet of Things (IoT) systems typically rely on Cloud or centralised systems for decision making and storage, resulting in an additional layer in the threat model when it comes to cyber-attacks [1]. This includes having a single point of failure, denial of service (DoS) attacks and trusting that data has not been manipulated.

Distribute Ledger Technology (DLT) was first introduced by Satoshi Nakamoto in 2008 with the original cryptocurrency Bitcoin [2] which offered a novel way for nodes to reach consensus in a decentralised manner via Proof of Work (PoW). Nodes of the blockchain network each store a copy of the ledger on their system removing the single point of failure [3]. Trust in a third-party intermediary is also no longer required as the system is sufficiently ‘decentralised’ and reaches ledger consensus (Nakamoto Consensus) [3].

Blockchain offers multiple improvements over traditional cloud or centralised systems by removing the single point of failure, trust in a third party intermediately such as a cloud provider and potential data manipulation by bad actors as data on the blockchain is considered immutable [4]. Blockchain technology comes with its own drawback, the main one being scalability (e.g., Bitcoin can process up to a maximum of 7 transactions per second currently) [5]. This is commonly referred to as the ‘Blockchain Trilemma’ [6] in improvements in decentralization, security, or scalability results in a compromise to the other properties.

Regarding current research relating to Blockchain and IoT, most of the research is currently focused on data immutability, data access permission and device authentication [7]. On the contrary, there is very little research into decentralised state changes within the IoT landscape. Current implementations normally rely on a centralised entity to make state changes to IoT devices such as consuming a RESTful service to instruct IoT devices to perform another action [8]. An example of a state change in this context could be a temperature sensor changing the temperature value of the room.

## References

1. Fernandez-Carames, T. and Fraga-Lamas, P., 2018. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, [online] 6, pp.32979-33001. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8370027> [Accessed 29 September 2021].
2. Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. [online] Available at: <http://www.bitcoin.org>.
3. Garay, J. and Kiayias, A., 2020. SoK: A Consensus Taxonomy in the Blockchain Era. Topics in Cryptology – CT-RSA 2020, [online] pp.284-318. Available at: <https://link.springer.com/chapter/10.1007/978-3-030-40186-3\_13> [Accessed 29 September 2021].
4. Kshetri, N., 2017. Can Blockchain Strengthen the Internet of Things?. IT Professional, [online] 19(4), pp.68-72. Available at: <https://ieeexplore.ieee.org/document/8012302> [Accessed 29 September 2021].
5. Croman K. et al. (2016) On Scaling Decentralized Blockchains. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-662-53357-4_8>
6. Zhou, Q., Huang, H., Zheng, Z. and Bian, J., 2020. Solutions to Scalability of Blockchain: A Survey. IEEE Access, [online] 8, pp.16440-16455. Available at: <https://ieeexplore.ieee.org/document/8962150> [Accessed 29 September 2021].
7. Conoscenti, M., Vetro, A. and De Martin, J., 2016. Blockchain for the Internet of Things: A systematic literature review. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), [online] Available at: <https://ieeexplore.ieee.org/abstract/document/7945805> [Accessed 29 September 2021].
8. Hang, L. and Kim, D., 2019. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. Sensors, [online] 19(10), p.2228. Available at: <https://www.mdpi.com/1424-8220/19/10/2228> [Accessed 29 September 2021].