# IoT Autonomous Agents Powered by Blockchain Technology

Christopher Dillon <c.p.dillon2@newcastle.ac.uk>

Primary Supervisor:

Maryam Mehrnezhad <maryam.mehrnezhad@newcastle.ac.uk>

Secondary Supervisors:

Changyu Dong <Changyu.Dong@newcastle.ac.uk>

Dave George <David.George1@newcastle.ac.uk>

Yit Arn Teh <YitArn.Teh@newcastle.ac.uk>

## Background

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. Multiple attempts have been made to resolve the scalability issue while still maintaining a degree of decentralisation in the form of Layer-2 scaling solutions [7].

Regarding current research relating to Blockchain and IoT, most of the research is currently focused on data immutability, data access permission and device authentication [8]. On the contrary, there is very little research into decentralised state changes within the IoT landscape. An example of a state change in this context could be a temperature sensor changing the temperature value of the room. 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 [9] [10]. This approach comes with the same drawbacks of centralised systems as mentioned previously.

Autonomous Agents are pieces of software that act and can function without any human intervention by reacting to states and events in their respective environment [10]. A change of state in the context of IoT devices could be a change in sensor data. An example of an autonomous agent present today is a computer virus [11], as it requires no human interaction at all and essentially operates in a machine-to-machine basis, using the host computer to ‘jump’ to another computer to infect.

As previously mentioned, in most IoT blockchain solutions, decision making is still carried out by a centralised entity, which comes with a host of security & maintenance threats [1]. This type of environment is hostile towards autonomous agents as downtime and cyber security threats disrupt autonomy of systems. A Blockchain network acting as a medium between IoT devices has the potential to promote total autonomy between devices and enable true peer-to-peer communication.

## Existing Progress

I have familiarised myself with the current systems that incorporate IoT systems into Blockchain Technology and along with the threat model of both traditional centralised systems and decentralised systems. Blockchain development software has been explored, specifically the programming language Solidity along with software suites in this field (Truffle, Remix IDE, Ganache).

## Further Work

My future work will have a large focus around the following areas of research:

### Autonomous Agents

Discover the state-of-the-art literature surrounding autonomous agents. This will include finding out what makes an agent truly autonomous. Best practices must also be established when it comes to designing autonomous agents.

### IoT Communication

As previously stated, most IoT systems parse data through a gateway [1] which is then used to make decisions. In truly decentralised decision making, IoT devices will communicate peer-to-peer using the blockchain as infrastructure. Rules and guidelines for communication between different types of devices must be established so they can effectively ‘understand’ each other and promote interoperability.

### Blockchain System Design

IoT devices generate large volumes of data and storing this data on-chain is traditionally problematic due to it being expensive and inefficient [ref]. Multiple solutions for scaling the blockchain such as layer-2 scaling solutions

* Establish a framework that allows for efficient peer-to-peer communication via the blockchain between IoT devices
* Setup an Agri-Tech testbed for data collection and experimentation
* Development of a lightweight blockchain system
* Development of software modules used to create autonomous agents

## Methodology

Testbed and system design will be carried out using NUFarms state of the art Agri-Tech test bed.

### Testbed

Data will be gathered from a wide variety of sensors within the context of Agri-Tech. Types of data includes location, optical, electro-chemical, mechanical, dielectric soil moisture, air flow, mobile apps, crop management systems (e.g., semios & arable) and a range of digital farm management programmes.

### System Design

A lightweight blockchain system will be designed to decentralise data management and enforce the correct execution of standard programmes through the smart farming cycle: Pre-planting, Cultivation, Growing, Harvesting, Storage, Processing, Wholescale marketing, Retail marketing, and Consumption. The design will particularly include sensor data coming directly from the farm requiring a lightweight design. We will design our system in such a way that sensors will access and interact with the system securely without having to sync with the full blockchain (off‐chain vs on‐chain).

## Training & Abilities

Training will be required in Agri-Tech systems (e.g., crop management) and data analysis. Training in programming is not required as I worked as professional software engineer for many years and have experience in all programming paradigms as well as blockchain programming at the application layer (smart contract development). Development and management of software and documentation will be managed via source control technology (Git).

## Impactful Approach

We will ensure continuous engagement with related industry via Mehrnezhad and Dong’s established links with PISA Research and Jitsuin’s Co-Founder & CTO (two UK-based leading cyber-security blockchain companies), George’s links to precision agriculture suppliers (e.g. Manterra/Precision Decisions/Map of Ag) and farmer bodies (AHDB), Teh’s links to agricultural IoT sensor networks (Hinterland) andNUFarms’ links to machinery manufacturers (John Deere), service providers (Trimble), and policy influencers (NFU). By engaging different stakeholders, the project will ensure delivery of practical, future-proofed solutions. Relevant track record of the supervisory team is provided in Annex 1.

## Project Timeline

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task Description/Month | 1-6 | 7-12 | 13-18 | 19-24 | 25-30 | 31-36 | 37-42 |
| Lit Review/ Farm Setup |  |  |  |  |  |  |  |
| Design |  |  |  |  |  |  |  |
| Implementation |  |  |  |  |  |  |  |
| Evaluation |  |  |  |  |  |  |  |
| Impact Activities |  |  |  |  |  |  |  |
| Publication |  |  |  |  |  |  |  |
| Thesis Writing |  |  |  |  |  |  |  |

## 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. Gudgeon L., Moreno-Sanchez P., Roos S., McCorry P., Gervais A. (2020) SoK: Layer-Two Blockchain Protocols. In: Bonneau J., Heninger N. (eds) Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science, vol 12059. Springer, Cham. https://doi.org/10.1007/978-3-030-51280-4\_12
8. 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].
9. 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].
10. Cui, H., Chen, Z., Xi, Y., Chen, H. and Hao, J., 2019. IoT Data Management and Lineage Traceability: A Blockchain-based Solution. 2019 IEEE/CIC International Conference on Communications Workshops in China (ICCC Workshops), [online] Available at: <https://ieeexplore.ieee.org/document/8849969> [Accessed 29 September 2021].
11. Lieberman, H., 1997, March. Autonomous interface agents. In Proceedings of the ACM SIGCHI Conference on Human factors in computing systems (pp. 67-74).
12. Buterin, V., 2014. DAOs, DACs, DAs and More: An Incomplete Terminology Guide. [online] Blog.ethereum.org. Available at: <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/> [Accessed 29 September 2021].