# 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]. Having a single point of failure, denial of service (DoS) attacks and trusting that data has not been manipulated are just some of the issues that are present in these types of systems.

Blockchain was first introduced by Satoshi Nakamoto in 2008 with the original cryptocurrency Bitcoin [2] as a type of immutable distributed database in which blocks are securely ‘attached’ onto each other via the previous block has header. Reaching consensus in a decentralised manner was first introduced by the novel Proof of Work (PoW) mechanism at the time. 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 one or more of 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 such as channels and side chains [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 [11]. 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 [12]. Viruses almost take on a ‘life’ of their own as once released, they can continue to infect machines other than the original. Autonomous Agents can also work in conjunction with each other, highlighted in [13], often called a multi-agent system.

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. A threat model must be established in the context of autonomous agents and blockchain technology as the cyber threats will differ to that of traditional systems.

### 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. Attempts to bridge communication between IoT devices have been made in the past [15]. Devices will not have to sync the entire blockchain as this is not feasible due to the storage limitations of most IoT devices.

### Blockchain System Design

The large volumes of transactions and data generated by IoT devices will be problematic for most blockchain networks due to the previously mentioned scaling issues [7]. Therefore, best practices must be established in optimising for a large volume of transactions being sent from these IoT devices. As full nodes must download the entire blockchain [2], it may be unfeasible to store all data produced from IoT devices on-chain. Decentralised solutions such as the Interplanetary File System (IPFS) [14] which is a distributed storage network will be investigated.

### Testbed

NUFarms state of the art Agri-Tech test bed will be used to gather data from relevant IoT devices

Testbed and system design will be carried out using NUFarms state of the art Agri-Tech test bed. 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. The testbed will simulate a full smart farming cycle including Pre-planting, Cultivation, Growing, Harvesting, Storage, Processing, Wholescale marketing, Retail marketing, and Consumption.

## 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).

## 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>
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>
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>
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>
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>
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>
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>
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/>
13. Singh, A., Juneja, D. and Malhotra, M., 2015. Autonomous Agent Based Load Balancing Algorithm in Cloud Computing. Procedia Computer Science, [online] 45, pp.832-841. Available at: <https://www.sciencedirect.com/science/article/pii/S1877050915004111>
14. The InterPlanetary File System, <https://ipfs.io>
15. Ciortea, A., Mayer, S., Boissier, O. and Gandon, F., 2019. Exploiting Interaction Affordances: On Engineering Autonomous Systems for the Web of Things.