

1. Background

- Internet of things (IoT)
 - Interconnected network
 - Billions of devices [1]
 - Large variety
 - Resource limited, throughput computation power
- Blockchain (BC)
 - Distributed ledger
 - Immutable
 - Transparent

2. Research question

Q: How we can improve security and efficiency in IoT data management using BC-based solutions

- How does BC improve IoT data management?
- What are the pros/cons of using BC to improve IoT data management?
- What solutions exist to negate the cons of using BC to improve IoT data management?

3. Method and process

- Gathered papers from and supervisor suggested
 - IEEE Xplore
 - ACM Digital Library
- Five surveys
- Six research papers
- Reviewed and compared
- Evaluation metrics
 - Consensus Algorithms
 - Performance
 - Security
 - Privacy

4. Discussion

- Survey omitted performance and consensus algorithms
- Some privacy not included
- Outdated Ethereum
- Positives
 - Fault tolerance
 - Resilience
 - Access control
 - Denial of Service
- Negatives
 - Critical of performance
 - Bandwidth important
 - BC introduces weaknesses

5. Future work

- Consensus algorithms tailored to the IoT
 - High scalability
 - High throughput
 - Low communication costs
 - Low latency
 - DAG
- Individual IoT device security
 - Individual devices vulnerable

6. Conclusion

- BC can improve security and efficiency
- Improvements still needed
- Consensus algorithms of great impact

References

- [1] S. Sorrel, "The internet of things: Consumer, industrial & public services 2018-2023," Jun 2018.
- [2] H. Nivavis and K. Loupos, "Consenselot: A consensus algorithm for secure and scalable blockchain in the iot context," in Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22, (New York, NY, USA), Association for Computing Machinery, 2022.
- [3] Y. Yuzik and D. Makaroff, "Blockchain-based security for heterogeneous iot systems," in Proceedings of the 30th Annual International Conference on Computer Science and Software Engineering, CASCON '20, (USA), p. 63-72, IBM Corp., 2020.
- [4] H. S. Alqahtani, R. Gamble, and M. Papa, "Securing over-the-air iot firmware updates using blockchain," COINS '19, (New York, NY, USA), p. 164-171, Association for Computing Machinery, 2019.
- [5] X. Guo, Q. Guo, M. Liu, Y. Wang, Y. Ma, and B. Yang, "A certificateless consortium blockchain for iots," in 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), pp. 496-506, 2020.
- [6] P. Zeng, X. Wang, L. Dong, X. She, and F. Jiang, "A blockchain scheme based on dag structure security solution for iiot," in 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 935-943, 2021.
- [7] S. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, "Trust-based blockchain authorization for iot," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1646-1656, 2021.

Table 1: (- -) poor, (-) insufficient, (+) sufficient, (++) good, (+++) excellent

Research	Description	Consensus Algorithms	Performance	Security	Privacy	(+) Pros (-) Cons
2022 Nivavis et al. [2]	Proposes ConSenseIoT, a distributed PoI consensus algorithm that would not impact the performance of the IoT network	PoI	+	++	+	+ Promising concept - Not tested
2020 Yuzik et al. [3]	Implementation, testing and discussion of a proof-of-concept security improving BC implementation for heterogeneous IoT systems.	PoA	++	++	-	+ Proof-of-concept + Thorough background - Based on outdated Ethereum
2019 He et al. [4]	System is proposed for the verification of over the air firmware updates using smart contracts.	ETH	++	++	-	+ Proof-of-concept - Limited background - Not extensive
2020 Zhou et al. [5]	Paper proposing a key-derived controllable lightweight secure certificateless signature algorithm.	PoT	+++	++	+	+ Tested + Proof - Scalability not treated
2021 Zeng et al. [6]	DAG based BC scheme for IIoT is proposed that is faster, more secure and energy efficient.	DAG	+++	++	+	+ Tested + Thorough
2021 Putra et al. [7]	Proposes an adaptive decentralized IoT access control mechanism by using a a permissioned private and public BC.	N/A	++	+	+	+ Tested + Critical - Slower