On the search for suitable consensus mechanisms for IoT

"How can blockchain-based IoT frameworks solve the problem of fault tolerance in current IoT frameworks with regard to computational power, scalability and Byzantine fault tolerance"

Research project (CSE 3000) by Michael Beekhuizen | Cyber Security Group, Department of Intelligent Systems | Supervised by: Miray Ayşen and Zekeriya Erkin

Introduction 1

- Central server [1]
- Increasing load and latency [2]
- Deleted, tampered or corrupted data [2]
- Extra servers not best solution [3]

Decentralization to the rescue? 2

- Blockchain can be used to make the framework decentralized [4]
- P2P network reduce latency
- Consensus mechanism ensures fault tolerance
- Everyone has a copy of ledger → Transparent
- Due to structure (chain) → Immutable data

Sound good but? 3

- Consensus requires high computational [2] power (Proof of Work)
- Everyone needs to have a copy [2]

Method 4

Comparison of consensus mechanisms

- Scalability in # of nodes
- Computational power
- Throughput & latency
- % of Byzantine fault tolerant

Results [5]-[20] 5

Table 1: Comparison of all the eleven different consensus mechanisms.

Consensus mechanism	Byzantine tol.	Scalable # nodes	TPS	BCT	Computational power	IoT suitable
PoW	51% power	High	7	10 min	High	No
PoS	51% stake	High	125-256	2-10 min	Medium-High	No
PoET	log log n / log n	Medium	2.3k	less 1 sec	Medium	Maybe
Raft	0	High	7k-400k	less 1 sec	Low-Medium	Maybe
PBFT	0.33	Low	78k	less 1 sec	Low	Yes
BFT-SMaRt	0.33	Medium	10k	less 1 sec	Low	Yes
Tangle	?	High	1.5k	10ms	Low	Yes
Jointgraph	0.33	High	10k [a]	5 sec [a]	Low	Yes
Proposed solution	?	Medium [b]	600-800	5 sec	Low-Medium	Maybe
G-PBFT	0.33	High	10k [a]	5-6 sec	Low	Yes
PoBT	?	High	?	in ms	Low	Maybe
PoEWAL	50%?	High [b]	1k [a]	1 sec [a]	Medium	Maybe

[?] Question mark means value not known.
[a] Value is derived from evaluating of other algorithm which was outperformed by the mechanism (This value can be seen as lower bound).
[b] Value is derived from evaluation in the corresponding paper

- G-PBFT, BFT-SMaRt and Tangle/Jointgraph are the most suitable mechanisms for IoT

Improvements 6

Decrease latency in G-PBFT

- Minimizing distance between nodes

Increase trust in G-PBFT

- Nodes form a society
- Proof of trust with certificates

Conclusion 7

- Blockchain can improve fault tolerance
- G-PBFT with improvements is a suitable mechanism

CSE3000 – Research project
Michael Beekhuizen
m.beekhuizen@student.tudelft.nl

References:

[1] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and internet of things (biot): requirements, working model, challenges and future directions," Wireless Networks, vol. 27, no. 1, pp. 55–90, 2021. [Online]. Available: https://dx.doi.org/10.1007/s11276-020-02445-6
[2] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2019. [Online]. Available: https://ieeexplore.ieee.org/ielx7/9739/8727625/08580364.pdf?tp=&arnumber=8580364&isnumber=8727625&ref=
[3] M. B. Gudadhe and A. J. Agrawal, "Performance analysis survey of data replication strategies in cloud environment," in Proceedings of the 2017 International Conference on Big Data Research, 2017, pp. 38–43.
[4] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui,F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*,vol. 21, no. 2, pp. 1676–1717, 2019.
[5] S. Zoican, M. Vochin, R. Zoican, and D. Galatchi, "Blockchain and consensus algorithms in internet of things," in 2018 *International Symposium on Electronics and Telecommunications (ISETC)*, 2018, Conference Proceedings, pp. 1–4.
[6] K. J. O. Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, 2014, Conference Proceedings, pp. 280–285.
[7] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *National Institute of Standards and Technology*, Report, 2018. [Online]. Available: https://dx.doi.org/10.6028/nist.ir.8202
[8] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54 371–54 401, 2020. [Online].Available: https://dx.doi.org/10.1109/access.2020.2981415
[9] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchainplatforms for iot applications: Architectures, security, privacy, and performance," *Computer Networks*, vol. 191, p. 108005, 2021. [Online]. Available: https://dx.doi.org/10.1016/j.comnet.2021.108005
[10] C. Cachin and M. Vukolic, "Blockchain consensus protocols in the wild," *arXiv preprint arXiv:1707.01873*, 2017.
[11] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019. [Online]. Available: https://dx.doi.org/10.1109/access.2019.2896108
[12] . Bessani, J. Sousa, and E. E. P. Alchieri, "State machine replication for the masses with bft-smart," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2014, Conference Proceedings, pp. 355–362.
[13] M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained iot networks," *Internet of Things*, vol. 11, p. 100212, 2020. [Online]. Available: https://dx.doi.org/10.1016/j.iot.2020.100212
[14] F. Xiang, W. Huaimin, S. Peichang, O. Xue, and Z. Xunhui, "Jointgraph: A dag-based efficient consensus algorithm for consortium blockchains," *Software: Practice and Experience*, 2019. [Online]. Available: https://dx.doi.org/10.1002/spe.2748
[15] Y. Wu, L. Song, L. Liu, J. Li, X. Li, and L. Zhou, "Consensus mechanism of iot based on blockchain technology," *Shock and Vibration*, vol. 2020, p. 8846429, 2020. [Online]. Available: https: //doi.org/10.1155/2020/8846429
[16] L. Lao, X. Dai, B. Xiao, and S. Guo, "G-pbft: A location-based and scalable consensus protocol for iot-blockchain applications," in *2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, 2020, Conference Proceedings, pp. 664–673.
[17] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "Pobt: A lightweight consensus algorithm for scalable iot business blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2343–2355, 2020. [Online]. Available: https://dx.doi.org/10.1109/jiot.2019.2958077
[18] Raghav, N. Andola, S. Venkatesan, and S. Verma, "Poewal: A lightweight consensus mechanism for blockchain in iot," *Pervasive and Mobile Computing*, vol. 69, p. 101291, 2020. [Online]. Available: https://dx.doi.org/10.1016/j.pmcj.2020.101291
[19] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of pow, pos and dag based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864819301476
[20] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, On Security Analysis of Proof-of-Elapsed-Time (PoET). Springer International Publishing, 2017, pp. 282–297. [Online]. Available: https://dx.doi.org/10.1007/978-3-319-69084-1 19

TU Delft
01-07-2021