Cloud-based vs. blockchain-based IoT: a comparative survey and way forward

Keywords: Internet of Things (IoT); Cloud; Blockchain; Data center; Taxonomy

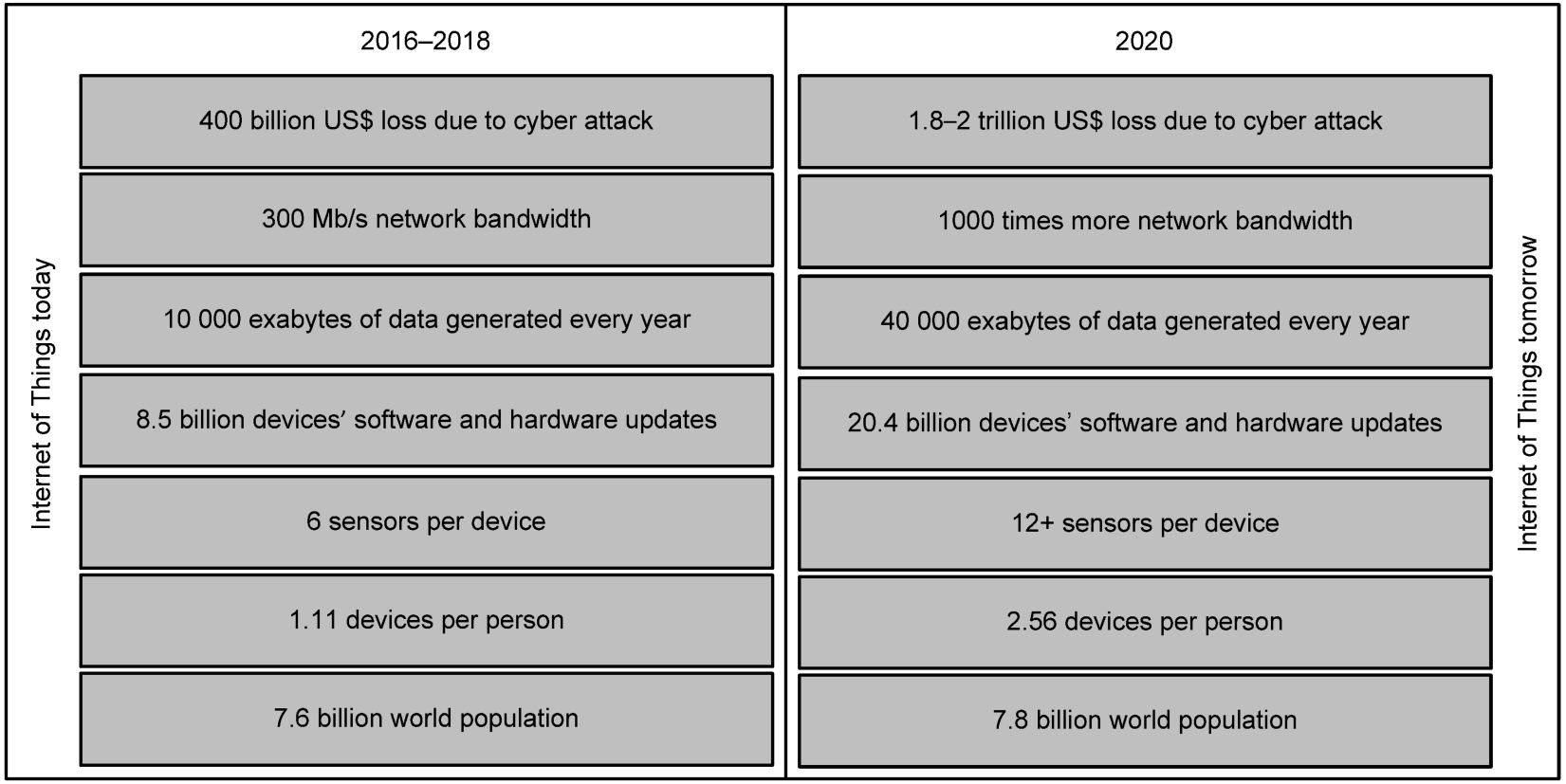
Raheel Ahmed Memon

ORCID: https://orcid.org/0000-0003-1206-3837

Cite as: Raheel Ahmed Memon, Jian Ping Li, Junaid Ahmed, M. Irshad Nazeer, M. Ismail, Khursheed Ali, 2020. Cloud vs. blockchain based IoT: a comparative survey and way forward. *Frontiers of Information Technology & Electronic Engineering*, 21(4):563-586. https://doi.org/10.1631/FITEE.1800343

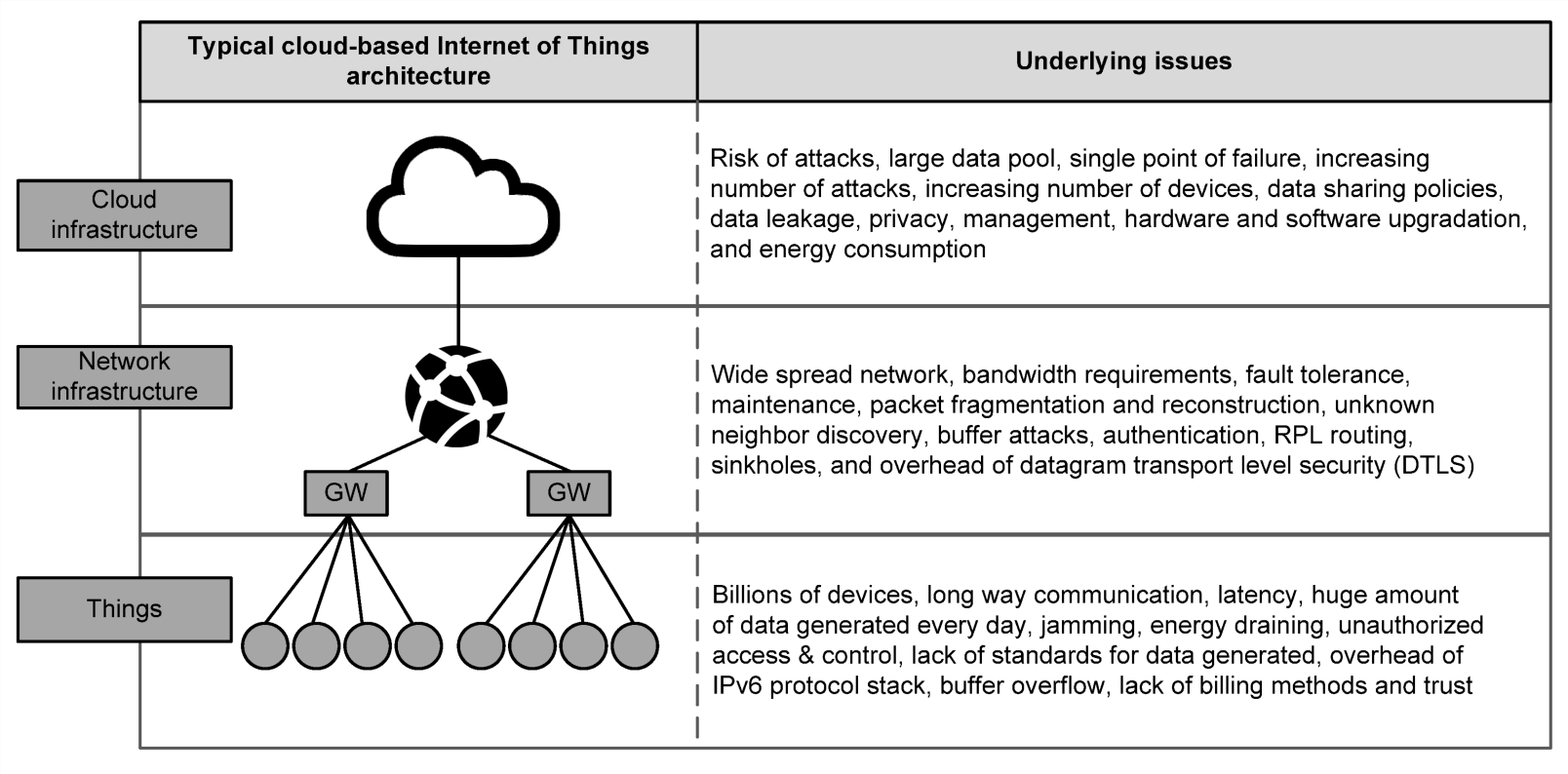
INTERNET OF THINGS IS RUNNING BEHIND ITS PREDICTIONS

There have been several predictions for year 2020 [1–11]. And we are here in 2020, are we really there?



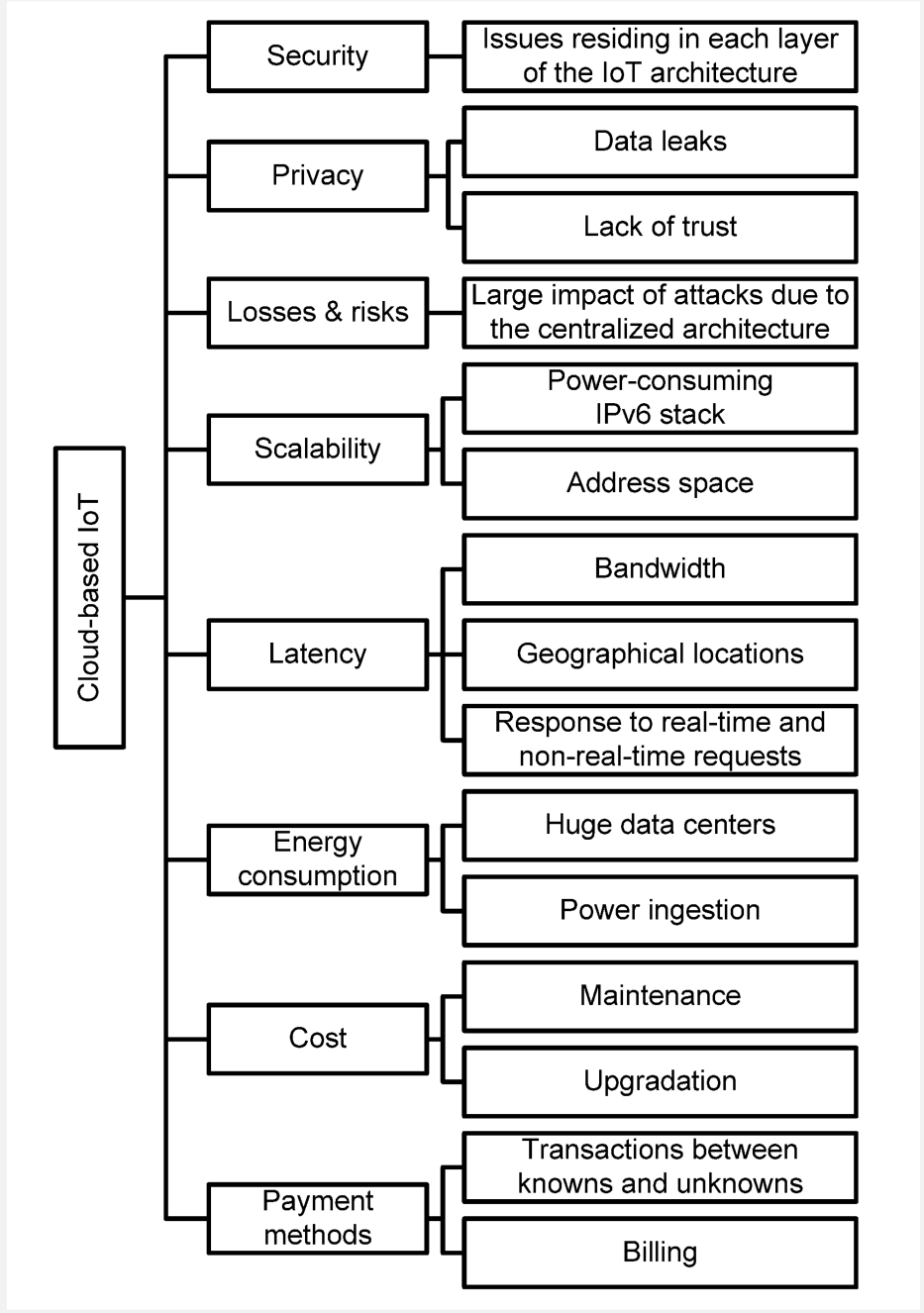
WHY IOT CANNOT MEET THE EXPECTATIONS?

There are issues available at every level in the existing centralized architecture of Internet of Things (CB-IoT). In the past decade the cloud infrastructure has been identified for a number of issues [12].

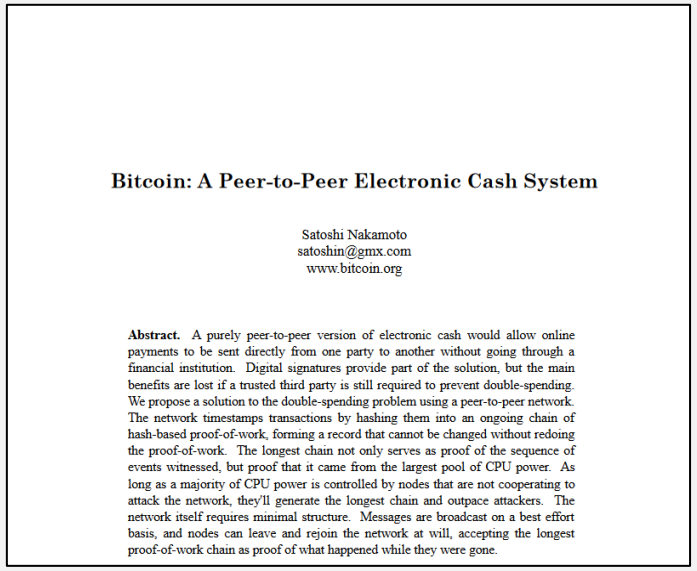


TAXONOMY OF ISSUES IN CENTRALIZED IOT

Each layer is having a number of issues related to historical losses, risks in future, fear of attacks, failure of timely responses, security issues in between things and cloud and within cloud, data leaks, scalability, power consumption, responses and latency involved in real-time and non-real-time systems, cost, bandwidth, maintenance, trust, transactions, and billing.



A REVOLUTIONARY WHITE PAPER [13]



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Year 2008
January 3, 2009

One of the biggest mysteries in the technology world is the identity of Satoshi Nakamoto

- Bitcoin is a crypto-currency (digital currency)
- Launched in 2009
- Operating under the most secure system of the P2P network
- **Blockchain technology**

WHY BLOCKCHAIN HAS GOT SO MUCH FAME?

- Blockchain is a distributed Ledger technology
- Forming a peer-to-peer network that works on the TCP/IP protocol
- Cryptographic signature and proof of work to achieve consensus in the network
- Features to offer:

Robust	Reliable	Available
Verifiable	Immutable	Distributed (no trusted third party)

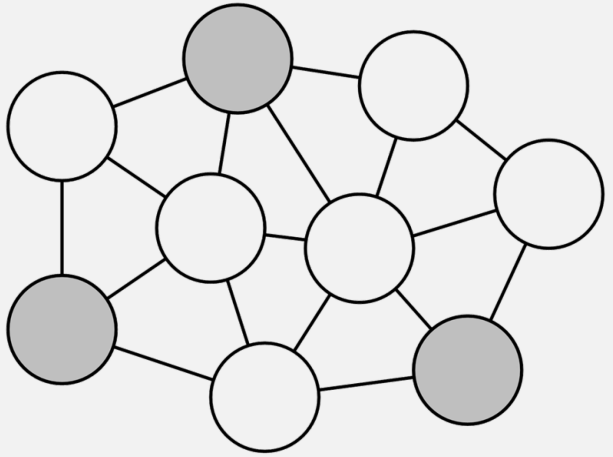
BLOCKCHAIN WORKING [14–16]

a) The network is peer to peer

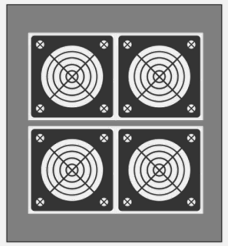
b) Blockchain is a linked list type of data structure, which creates an unbreakable chain of blocks, where each block is being added after performing huge computations to solve a mathematical puzzle.

c) The mathematical puzzle is solved by miner nodes in the network.

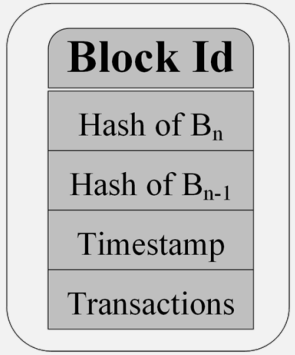
d) Once it is recorded, it's there for ever



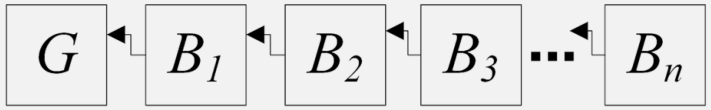
a) Distributed Network



b) Miners



c) Block Metadata



d) Blockchain

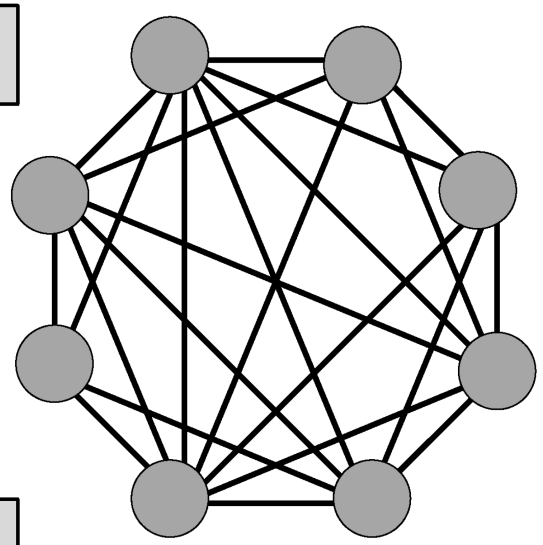
BLOCKCHAIN BASED IOT

The scope of blockchain is not limited to digital currencies; in fact, it is receiving a great deal of attention in several other fields, as provided in a scoping survey of blockchain showing that it has also been applied to revolutionize several different fields like medicine, software engineering, IoT, and many others [17].

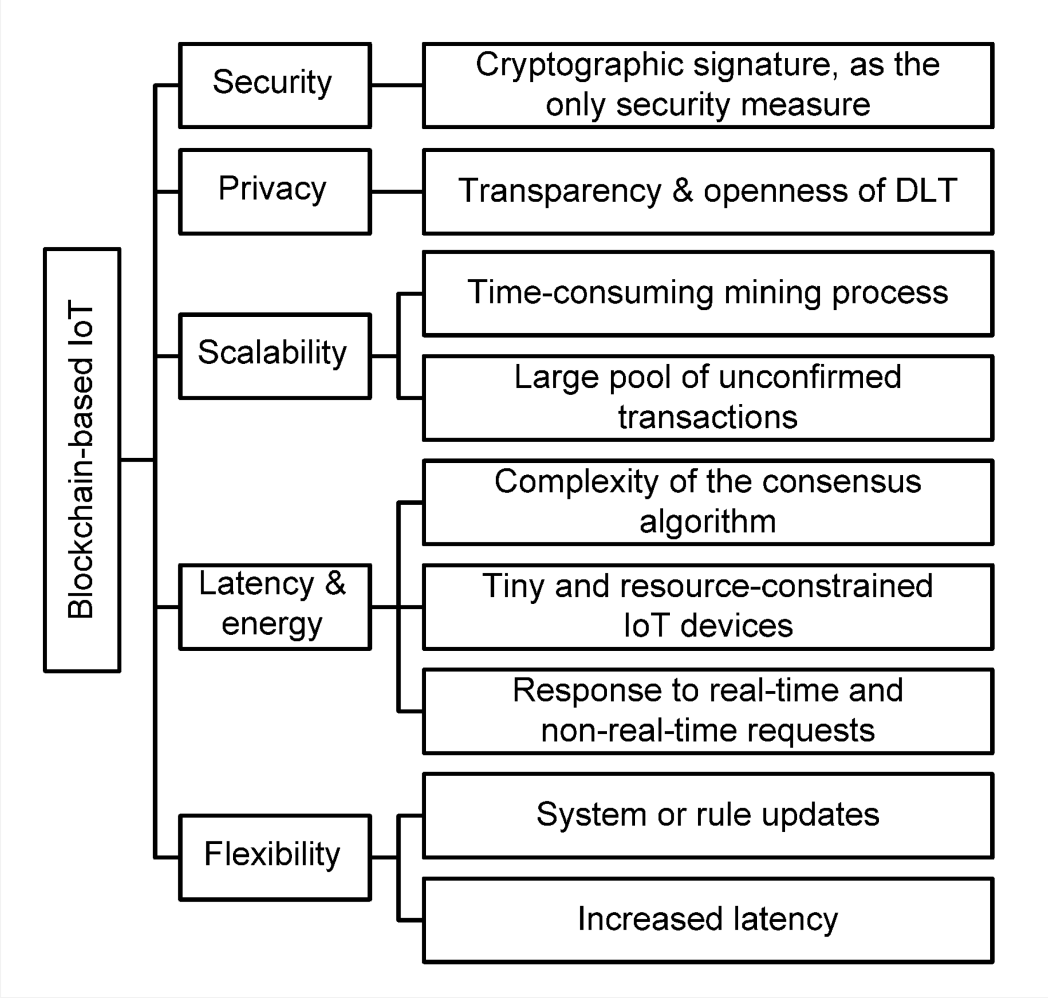
KEY RESEARCH PROJECTS MERGER OF IOT AND BLOCKCHAIN

- Blockchain meets edge computing [18]
- Blockchain as a service for IoT [19]
- BC-based smart home framework [20]
- F-Secure [21]
- Blockchain based IoT access control and authentication management [22]
- Proactive DDOS Defense Framework [23]
- Storj.io [24]

EXPECTED ISSUES IN BLOCKCHAIN BASED IOT (BB-IOT)

Typical blockchain-based IoT	Expected issues
Things  Distributed network	<u>Things:</u> Transparency and privacy, computation, latency due to proof of work, energy consumption, security, and scalability <u>Services:</u> Complex architecture, challenges for any amendment, limited options of upgradation, and only one security measure (cryptographic signature) <u>User:</u> Delay in response, late updates

TAXONOMY OF ISSUES IN BB-IOT



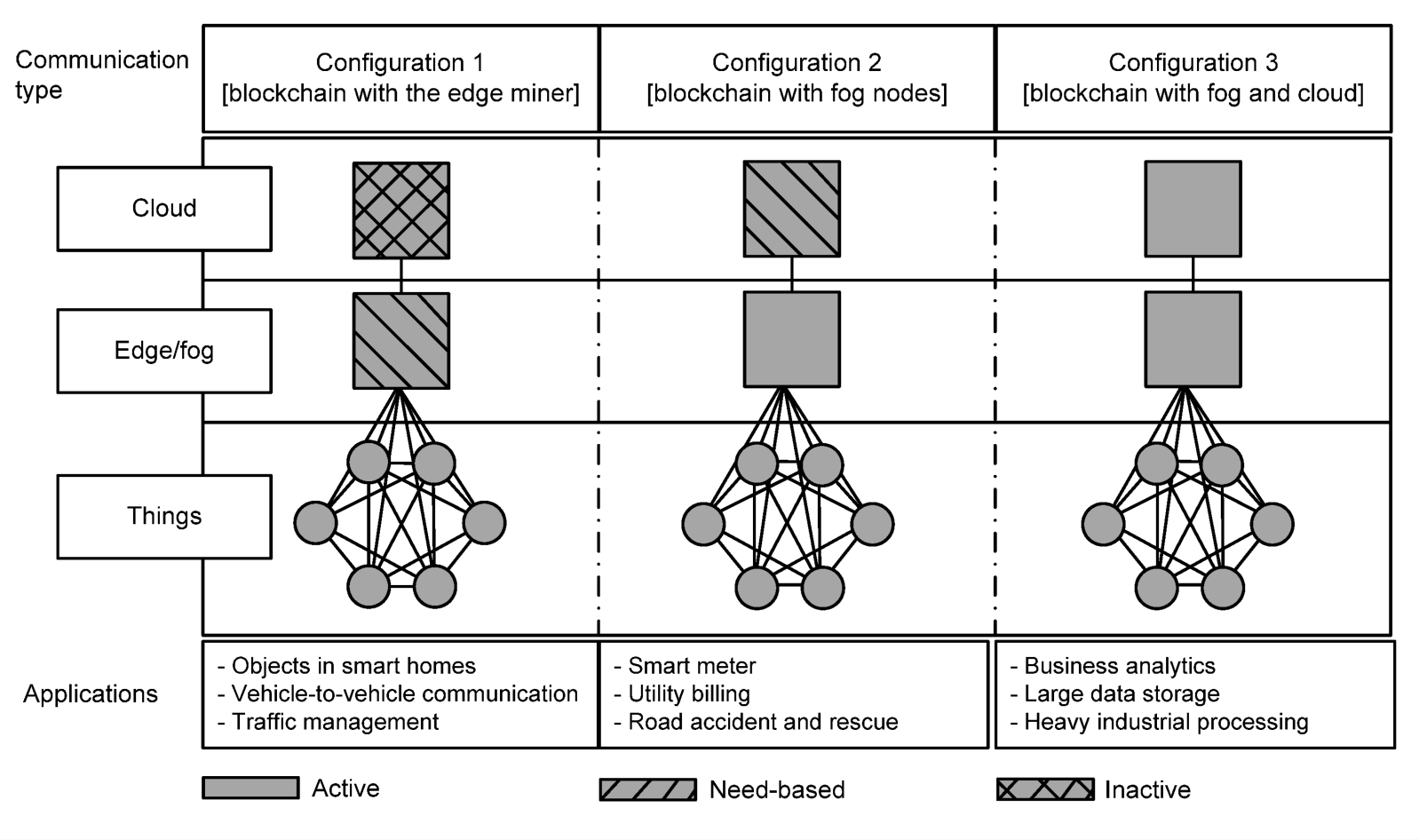
WAY FORWARD

The possible solution to these problems can be the combination of these two architectures. On the basis of the conducted survey we can say that a hybrid IoT architecture is tomorrow’s technology; there could be conflict of opinion on its working paradigms, but it is for sure that the upcoming IoT architecture would be a hybrid approach.

PROPOSED HYBRID IOT

- We propose the hybrid-IoT approach as one of the possible ways to overcome the challenges with both architectures. Hybrid IoT is a three-tier architecture, from bottom to top:
  - Things
  - Fog/Edge
  - Cloud
- We also propose three basic configurations of hybrid IoT, which are the different modes of communication.

PROPOSED HYBRID IOT



SUMMARY
CLOUD AND BLOCKCHAIN FUSION TO REFORM IOT

Challenge	CB-IoT	BB-IoT	Hybrid IoT
Security	Weak	Strong	It uses blockchain at the device level to ensure the security of the IoT ecosystem.
Scalability	Strong	Weak	Configuration 1 can be used to create private networks of blockchain, which provides security and preserves privacy in building area networks (BLANs).
Privacy	Weak	Strong	
Losses and risks	Weak	Strong	The use of blockchain at the device level will resolve the risk of attacks by restricting it to trusted members only, and thus the fear of losses would be mitigated.
Latency	Weak	Strong	The latency, energy ingestion, cost of bandwidth consumption, and capital or operational expenses of huge data centers will be dramatically reduced if regular communication occurs in Configurations 1 and 2, and only industrial data storage and analysis are performed over the cloud in Configuration 3.
Energy consumption	Weak	Strong	
Cost effectiveness	Weak	Strong	
Payment methods	Weak	Strong	Bitcoin is a very good example of the payment method; there could also be alternatives for payment systems. In the past few years, more than a dozen of new digital currencies have been introduced using blockchain.
Flexibility	Strong	Weak	Forking is easy to deal with if there is an edge node involved in the mining process.

REFERENCES

[1] J. Manral, “IoT enabled Insurance Ecosystem - Possibilities Challenges and Risks,” *CoRR*, pp. 1–18, Oct. 2015.

[2] J. Moar, “Cybercrime & The Internet of Threats.” (White Paper) - Juniper Research, 2017.

[3] Y. D. Marinakis, S. T. Walsh, and R. Harms, “Internet of things technology diffusion forecasts,” in *PICMET 2017 - Portland International Conference on Management of Engineering and Technology: Technology Management for the Interconnected World, Proceedings*, 2017, vol. 2017-Janua, pp. 1–5, doi: 10.23919/PICMET.2017.8125435.

[4] “Cybercrime will Cost Businesses Over $2 Trillion by 2019.” [Online]. Available: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion. [Accessed: 24-Feb-2018].

[5] S. Sagiroglu and D. Sinanc, “Big data: A review,” in *2013 International Conference on Collaboration Technologies and Systems (CTS)*, 2013, pp. 42–47, doi: 10.1109/CTS.2013.6567202.

[6] C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, “Big-Sensing-Data Curation for the Cloud is Coming: A Promise of Scalable Cloud-Data-Center Mitigation for Next-Generation IoT and Wireless Sensor Networks,” *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 48–56, 2017, doi: 10.1109/MCE.2017.2714695.

[7] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017, doi: 10.1109/MITP.2017.3051335.
[8] R. Qi, C. Feng, Z. Liu, and N. Mrad, *Blockchain-Powered Internet of Things, E-Governance and E-Democracy*. 2017.
[9] worldometers, “World Population Projections - Worldometers.” [Online]. Available: http://www.worldometers.info/world-population/world-population-projections/. [Accessed: 15-Sep-2018].
[10] R. van der Meulen, “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016,” *Gartner Press Release*, 2017. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. [Accessed: 15-Sep-2018].
[11] Á. Garai, A. Attila, I. P.- (CogInfoCom), 2016 7th IEEE, and undefined 2016, “Cognitive telemedicine IoT technology for dynamically adaptive eHealth content management reference framework embedded in cloud architecture,” *ieeexplore.ieee.org*.
[12] M. Aazam, I. Khan, A. A. Alsaffar, and E. N. Huh, “Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved,” in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2014*, 2014, no. January, pp. 414–419, doi: 10.1109/IBCAST.2014.6778179.
[13] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Www.Bitcoin.Org*, p. 9, 2008, doi: 10.1007/s10838-008-9062-0.
[14] R. A. Memon *et al.*, “Simulation and analysis of RSAFE and RSAFE rerouting protocol in network simulator 2,” in *2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2017*, 2017, vol. 2018-Febru, pp. 274–277, doi: 10.1109/ICCWAMTIP.2017.8301494.
[15] R. A. Memon, J. Li, J. Ahmed, A. Khan, M. I. Nazir, and M. I. Mangrio, “Modeling of Blockchain Based Systems Using Queuing Theory Simulation,” in *2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2018*, 2019, pp. 107–111, doi: 10.1109/ICCWAMTIP.2018.8632560.

[16] R. Memon, J. Li, M. Nazeer, A. Neyaz, … J. A.-I., and undefined 2019, “DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things,” *ieeexplore.ieee.org*.
[17] Y. Li, T. Marier-Bienvenue, A. Perron-Brault, X. Wang, and G. Paré, “Blockchain Technology in Business Organizations: A Scoping Review,” 2018, doi: 10.24251/HICSS.2018.565.
[18] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When Mobile Blockchain Meets Edge Computing,” 2017, doi: 8436042.
[19] M. Samaniego and R. Deters, “Blockchain as a Service for IoT,” in *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, 2017, pp. 433–436, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.
[20] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work.*, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.
[21] “F-Secure SENSE — Secure router and app | F-Secure.” [Online]. Available: https://www.f-secure.com/en_US/web/home_us/sense. [Accessed: 15-Sep-2018].
[22] A. Z. Ourad, B. Belgacem, and K. Salah, “Using blockchain for IOT access control and authentication management,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10972 LNCS, pp. 150–164, doi: 10.1007/978-3-319-94370-1_11.
[23] N. Z. Bawany, J. A. Shamsi, and K. Salah, “DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions,” *Arabian Journal for Science and Engineering*, vol. 42, no. 2. pp. 425–441, 02-Feb-2017, doi: 10.1007/s13369-017-2414-5.
[24] S. Wilkinson, “Stoj - A Peer-to-Peer Cloud Storage Network,” *http://storj.io/storj.pdf*, 2014.