PhD Forum Research Statement: Distributed Ledger Enabled Collaborative IoT Networks

Awid Vaziry*†, Matthias Wählisch* (advisor)
*Internet Technologies Research Group, Freie Universität Berlin
Email: awid.vaziry@fu-berlin.de
†BMW Group

***Abstract*—This research statement describes the initial state-of-the-art, vision and methodology for future PhD research on Distributed Ledger Technology (DLT) enabled Internet of Things (IoT) networks. Several studies and publications are emphasizing on the potential of realizing new IoT network capabilities, by utilizing DLT. Especially, collaborative applications, such as: shared infrastructure, smart logistics or distributed sensor networks can benefit from the inherent trust and governance of DLT. However, it has not yet been quantified, which specific technological factors are limiting the use. This research statement examines current barriers and describes specific factors, and trade-offs integrating low power IoT devices as participants in Bockchain based DLT networks. Furthermore, starting points and challenges of future research on IoT-centric distributed ledgers are defined.**

***Index Terms*—Internet of Things, IoT, Blockchain, Distributed Ledger Technology, DLT, PhD Forum**

I. Introduction

The Internet of Things involves different kind of devices with typically limited hardware resources, spanning from domestic appliances, environmental sensors to city and industrial infrastructure [1]. These devices are interconnected, exchanging data with each other as well as with external parties. In historical context, *Mark Weiser* is one of the first scholars, describing the concept of IoT in his work: *The Computer for the 21st Century* [2] as "ubiquitous computing", denoting that more computers will be replaced by "smart" connected devices. This vision aligns with recent developments in adoption of IoT, which raises the questions of control and tailored network layouts. The current model features mostly centralized control of interconnected devices. This may not be an advantageous layout with regards to future decentralized applications such as: interconnected cities, production & logistics networks, supply chains, environmental sensors, and connected vehicles. Those prominent applications require the collaboration of multiple parties in a decentralized manner, who might not fully know and/or trust each other.

Current proposed IoT use cases are raising the questions of ownership, security, integrity, communication and control of the devices. Especially sub-networks of things, which are interconnecting multiple stakeholders, are in need of novel network designs. These desired networks, must enable collaboration between various parties in an equitable manner. A possible technical answer to the raised questions, could be a decentralized or distributed approach where single points of control are minimized or avoided. In that approach, collaborative IoT networks are used, maintained, and protected by multiple stakeholders, based on predefined rules and protocols. Distributed Ledger Technology, also referred to as Blockchain, has the potential to address various of the required capabilities. A Blockchain stores validated communication - referred to as transactions - in a tamper proof ledger which is maintained and validated in a distributed manner. The global network state is achieved by a consensus protocol. The choice of the consensus algorithm significantly defines the systems metrics, as well as performance and security limits. Combining the consensus algorithm with decentralized logic, enables the creation of an inherent governance. This implies that decisions effecting the system - such as updates and device identification - are organized in a predictable, tamper-proof way, stored and enforced by itself.

Interconnecting IoT devices to those distributed Blockchain networks introduces operational and technological challenges on various layers. Some apparent challenges are: resource limitation of end devices, network latency & throughput, communication infrastructure design, identity, security, legal regulations, and standardization of interfaces & protocols [3] [4].

In this research statement the potential of next-generation shared IoT networks, enabled by utilizing distributed ledger technology and decentralized governance is examined. Therefore, current efforts are presented and shortcomings of previous research are described. Furthermore, future relevant research directions and limitations of integration IoT devices within DLT networks are shown. The main trade-off is caused by the limited resources of IoT devices and the resource requirements of current DLT frameworks. Last, concrete research questions, goals and next steps are determined. Those serve a as a basis for future PhD research.

II. Related Work

Sun et al. [5] examined Blockchain based governance for modern shared services with regards to economical feasibility. Under utilization of a framework, they concluded that Blockchain governance is a logical step for enabling future sharing services. However, the examination happened solely from a business and conceptual point of view and was not aligned with technological considerations. *Beck et al.* [6] conducted a "swarm-city" case study for enabling decentralized sharing economy platforms. Furthermore, three main research question for Blockchain based governance were identified: decision rights, accountability, and incentives within the system.

Ramachandran and *Krishnamachari* [7] analyzed the opportunities and challenges of combining Blockchain and IoT. They identified the main opportunities as security, privacy, and trust in multi-stakeholder environments. Technological challenges include: resource constraints of the devices, latency, and bandwidth requirements. These need to be addressed by further hardware developments, as well as IoT tailored architectures and protocols. The authors of the paper *Blockchain's adoption in IoT: The challenges, and a way forward* [4], are raising similar outlooks and hurdles. They conclude that the primary challenge for adoption, is the non-availability of a consensus protocol and network design specifically tailored to IoT applications; as well as the secure IoT device integration with the Blockchain. *Elsts et al.* [8] conducted an experimental evaluation of integrating IoT devices with an acyclic graph based ledger, which brands itself as ledger for IoT. They examined different network connection architectures and showed in their experiments that the computational requirements of the DLT network are exceeding the capabilities of battery powered and resource constrained devices.

III. Research Framework

A DLT-enabled IoT network could inherent decentralized identity management, which enables firmware integrity checks, log critical communication, and act as a medium for machine to machine communication. Further, a distributively governed IoT network can enable collaboration in interconnected applications using smart sensors or smart infrastructure by ensuring decentralization and providing a trusted environment for collaboration.

Realizing these desired capabilities requires research in various fields. It needs to be investigated and decided upon, which computations are conducted by IoT devices themselves or distributed to other nodes, and how this system is secured. This needs to be implemented, considering limited bandwidth and device resources (computation, storage, memory), while maintaining security. Next, the specific requirements for governing IoT-networks in a decentralized manner, are to be identified and quantified.

Five initial research question are formulated, which chronologically build upon each other:

1) Which parameters need to be assessed, when interconnecting IoT devices with a distributed ledger?
2) To what extend can IoT devices participate in current Blockchain based DLT networks and what are the technological limitations?
3) What are desirable architectures and protocols for communication and computing for connecting IoT devices to Blockchain based IoT networks, sending transactions and computing cryptographic functions?
4) Which consensus protocol can fit these architectures and what are main advantages and shortcomings of those?
5) How can an inherent logic be implemented into the system, for ensuring an equal decentralized governance?

IV. Unanswered Questions and Research Challenges

Implementing low power IoT devices as participants in the decentralized DLT system represents an additional technical hurdle. Mainly, due to the device limitation of memory, processing power, bandwidth and battery life. In order to keep the highest level of privacy and trust in the network, participants are integrated as so called full nodes. Full nodes are maintaining a copy of the ledger, processing transactions and - if desired - participating in the consensus. However, implementing a full node comes with certain bandwidth and hardware requirements. Those requirements differ depending on the chosen Blockchain framework, but are in most cases exceeding the capabilities of IoT devices. Their limited performance will affect the ability of hashing, en-/decrypting, sharing and receiving data. Hence, when considering low power IoT devices, certain tasks, such as: verification of transactions, cryptographic computations, or credential handling must be outsourced to another node.

This introduces the trade-off between resource consumption and autonomy of the devices. It needs to be discussed, to which extend autonomy and security is sacrificed for savings in resources consumption and what types of network architectures can optimize this trade-off. Therefore, the first part of this PhD research is the investigation of the research questions 1) and 2), by defining assessment criteria and measuring the capabilities of IoT devices connected to different Blockchain Frameworks.

References

[1] Bormann, C.; Ersue, M.; Keranen, A., *Terminology for Constrained-Node Networks*, Internet Engineering Task Force (IETF), 2014

[2] Weiser, M., *The computer for the 21st century*, Scientific American, Special Issue on Communications, Computers, and Net- works, 1991.

[3] Reyna, Ana; Martn, Cristian; Chen, Jaime; Soler, Enrique; Daz, Manuel, On blockchain and its integration with IoT. Challenges and opportunities, Future Generation Computer Systems, 2018.

[4] Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W., *Blockchain's adoption in IoT: The challenges, and a way forward*, Journal of Network and Computer Applications, 2018.

[5] Sun, J.; Yan, J.; Zhang, K.Z.K., *Blockchain-based sharing services: What blockchain technology can contribute to smart cities*, Financial Innovation, 2017.

[6] Beck, R.; Mueller-Bloch, C.; King, J.L.; Thatcher, J., *Governance in the Blockchain Economy: A Framework and Research Agenda*, Journal of the Association for Information Systems, 2018.

[7] Ramachandran, G.S.; Krishnamachari, B., *Blockchain for the IoT: Opportunities and Challenges*, arXiv:1805.02818, 2018.

[8] Elsts, A.; Mitskas, E.; Oikonomou, G.,*Distributed Ledger Technology and the Internet of Things*, Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, 2018.