# Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams

Sina Rafati Niya[1], Eryk Schiller[1], Ile Cepilov[1], Fabio Maddaloni[1], Kürsat Aydinli[1],
Timo Surbeck[1], Thomas Bocek[2], Burkhard Stiller[1]
[1]Communication Systems Group CSG, Department of Informatics IfI, University of Zürich (UZH)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
{rafati,schiller,stiller}@ifi.uzh.ch, {ile.cepilov,fabio.maddaloni,kuersat.adinli,timo.surbeck}@uzh.ch
[2]HSR University of Applied Sciences Rapperswil, Switzerland
thomas.bocek@hsr.ch

***Abstract*—Proof-of-Work (PoW) in Blockchains (BC), which is a widely used consensus algorithm, suffers from high power consumption of miners and low transaction rates. This work demonstrates a Proof-of-Stake (PoS)-based BC called Bazo, which is specially designed and adapted for Internet of Things (IoT) data streams. Bazo displays enhanced performance in terms of energy consumption and transactions processing in comparison to PoW-based BC. To further improve performance of Bazo, sharding and transaction aggregation methods are employed. Moreover, IoT-BC adaptation helpers of a modular and layered architecture are provided to allow wireless devices to submit data into the BC. The designed architecture can support multiple hardware and software platforms as well as network technologies.**

***Index Terms*—Blockchains, Proof-of-Stake (PoS), Consensus Mechanisms, IoT, Long Range (LoRa) Communication Protocols**

## I. Introduction

Miners or validators are the main actors that verify the data to be stored in the Blockchain (BC). Every BC uses consensus mechanisms to agree on a single chain of blocks, however, short-lived forks of the chain may be possible. Different consensus algorithms are used to validate transactions, for example based on Proof-of-Work (PoW) or Proof-of-Stake (PoS) mechanisms [1]. However, typical PoW-based BC come with severe problems such as long delay of transaction processing, extensive energy consumption, and low scalability limiting the possible use-cases that typically require high transaction rates and low transaction delay.

Among BC use cases, Internet of Things (IoT)-integrated use cases have recently risen high interest due to the practical and industrial application demands [2]. Blockchain and IoT (BIoT), considered as integrated systems, inherit challenges of both BC and IoT. On the one hand, large number of data packets of variable payload sizes collected by IoT devices require fast and secure data streams directed in full or parts to a BC, in which PoW-based BC meet technical thresholds. On the other hand, IoT covers a wide range of communication protocols, as well as hardware and software architectures. Therefore, the BIoT use cases require a holistic approach of a modular architecture.

The main goal of this work is to introduce a BC design for IoT data streams. For this purpose a basic PoS-based BC, *i.e.*, Bazo [3], is used and its performance and scalability is improved to meet the demands of BIoT integrated systems. This work also covers the design and implementation of an adaptation layer for IoT data streams. This system is developed and tested both in real world with LoRa devices [4], and simulated within several scenarios with the NS-3 simulator [5].

978-1-7281-1328-9/19/$31.00 ©2019 IEEE

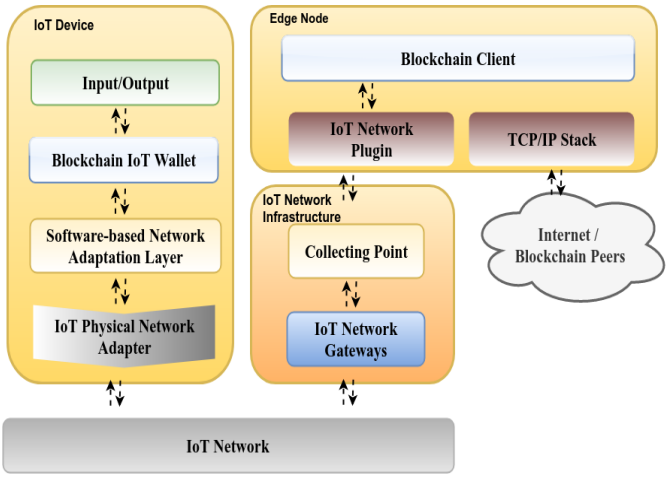


Fig. 1: IoT Adaptation Components of a Layered Architecture.

## II. System Overview

To reach the defined objective and distinguish this work from the regular Bazo design [3], the following innovations are provided here in this work:

**1) Sharding in BC Peers:** The sharding technique [6] was introduced in Bazo for increased performance and enhanced scalability. In sharding, incoming transactions can be validated in parallel as a Bazo peer may decide on transaction processing for an arbitrary subset of clients. The impact of sharding is twofold: reduced storage per node and a higher overall transaction processing capacity.

**2) IoT-to-Blockchain Adaptation Helpers**: Fig. 1 provides the following components: (a) a BC IoT Wallet, (b) a Software-based Network Adaptation Layer, (c) an IoT Network Plugin, and (d) a BC Client. These adapting helpers enable Bazo to operate as an IoT-agnostic BC. The Wallet resides on the IoT device; it contains a public/private key

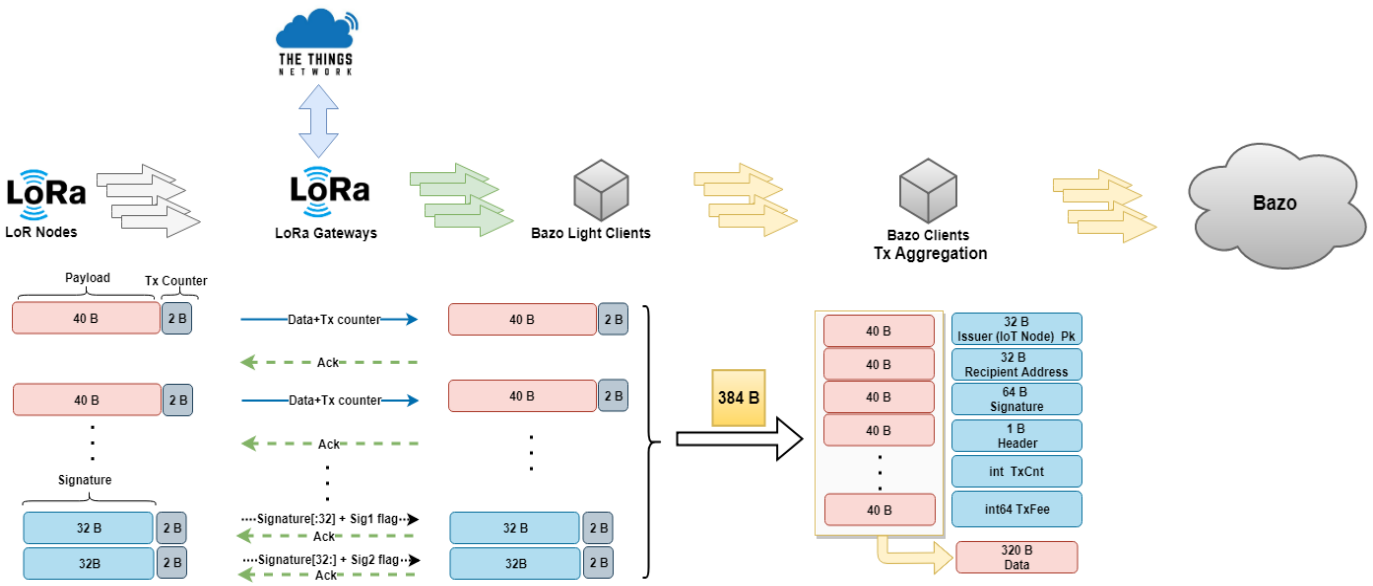


Fig. 2: LoRa to Bazo Message Structure.

pair and issues BC transactions towards the Software-based Network Adaptation Layer, which optimizes the transmission for a particular network interface. Then, the data goes to the central storage of the IoT Network, and is received by the BC Client through a dedicated plugin. Finally, the BC Client submits the received transactions to the BC.

**3) Network Protocols**: IoT devices often use a network of limited capacity, which offers very low payload sizes. The signature often comes with a significant size, *e.g.*, an RSA-1024 signature requires 128 B. It might be too long for some IoT applications, *e.g.*, LoRa with Spreading Factor (SF) 12 allows for the maximum payload of around 50 Byte in the TTN network. Therefore, every data transaction submitted to the BC may require the transmission of 3 overhead packets carrying the fragmented signature. It is, therefore, important to design a communication protocol for BC applications that reduces overhead caused by signatures in every committed transaction. In this work, the IoT nodes and BC clients use the ED25519 cryptographic function coupled to SHA-512 [7] to establish signatures of size equal to 64 Byte (*cf.*, Fig. 2). Moreover, a transaction-based protocol is used, in which data integrity is provided to the transaction consisting of several data packets through re-transmissions. The data is protected with sequence numbers and acknowledgements. Several data packets are committed at once using one signature sent at the end of the transaction. The designed scheme allows for fragmentation of data packets when needed.

**4) Simulation of IoT Networks:** The designed transaction pattern is provided directly from real IoT sensors at a small scale as well as simulated at the large scale in the NS-3 simulator with a large number of IoT devices (*i.e.,* 400-1600 nodes). The traffic is submitted a set of 10 Bazo validators (miners) in the peer-to-peer network provisioned in the Google cloud.

## III. Demonstration Scenario

The main goal of this demonstration is to present the performance of the Bazo BC equipped with sharding for IoT data streams. Additionally, the role of helpers of the modular architecture allowing for generic and network oblivious IoT wallets provisioned on IoT devices will be highlighted. The demo provides a set of Arduino Mega devices with LoRa shields submitting BC transactions. They are connected to LoRa gateways, which in turn collect the submitted data within the TTN back end. The edge BC client receives IoT data streams in the transactions format from the TTN and submits them to the BC. Simultaneously, an NS-3 simulator, which simulates large numbers of LoRa nodes (*e.g.*, 1200 nodes) submit IoT data streams to the network of 10 Bazo miners provisioned in the Google cloud. The demonstration includes two screens that illustrate submission handling (i.e., from IoT devices and the simulator) by the BC client and the validation in the network of BC miners.

## References


[1] T. Bocek and B. Stiller, *Smart Contracts - Blockchains in the Wings*. Tiergartenstr. 17, 69121 Heidelberg, Germany: Springer, January 2017, pp. 1–16.

[2] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review On The Use of Blockchain For The Internet of Things," *IEEE Access*, Vol. 6, pp. 32 979–33 001, 2018.

[3] S. Bachmann, "Proof of Stake for Bazo," https://files.ifi.uzh.ch/CSG/staff/bocek/extern/theses/BA-Simon-Bachmann.pdf, January 2018.

[4] A. Lavric and V. Popa, "Internet of Things and LoRa™ Low-power Wide-area Networks: A Aurvey," in *Signals, Circuits and Systems (ISSCS), International Symposium on*. IEEE, 2017, pp. 1–5.

[5] "NS-3, A Discrete-Event Network Simulator," https://www.nsnam.org/, Last accessed: March 15, 2019.

[6] Y. Gao and H. Nobuhara, "A Proof of Stake Sharding Protocol for Scalable Blockchains," *Proceedings of the Asia-Pacific Advanced Network*, Vol. 44, pp. 13–16.

[7] D. J. Bernstein, "Curve25519: New Diffie-Hellman Speed Records." [Online]: https://cr.yp.to/ecdh/curve25519-20060209.pdf