DESIGN AND IMPLEMENTATION OF A DECENTRALIZED AMR SYSTEM USING BLOCKCHAINS, SMART CONTRACTS AND LORAWAN

Ioannis VLACHOS
National Technical University of Athens – Greece
ivlachos@power.ece.ntua.gr

Nikos HATZIARGYRIOU
National Technical University of Athens – Greece
nh@power.ece.ntua.gr

ABSTRACT

In this paper we present a novel decentralized Automatic Meter Reading (AMR) system over a LoRaWAN network using blockchain technology and the underlying concept of smart contracts. The rationale behind the proposed AMR system is twofold: first of all, to provide an additional open, trusted, decentralized and tamper-proof layer for handling smart meter data, but at the same time offer the end-customers the ability of controlling the usage of their own meter data; i.e. providing the end-customers with ownership over their metering data. The latter is achieved by employing the concept of smart contracts.

INTRODUCTION

The transition of the traditional power network to the smart grid requires the application of computer intelligence and advanced communication infrastructures in order to make sure the efficient and robust coordination of the various grid components. Smart grids can also be viewed as the convergence between the worlds of energy and that of the Information and Communication Technologies (ICT). Moreover, the realization of the utility of the future will require the digital transformation of systems, operation, and processes. This digital transformation, among other things, includes also the modernization of systems and processes at the crossroads of energy and the Internet of Things (IoT).

LoRaWAN [1] is a new Low Power Wide Area Network (LPWAN) specification intended for wireless battery-operated devices. The LoRaWAN specification provides seamless interoperability among smart devices without the need of complex local installations and gives back the freedom to the user, developer, businesses enabling the roll out of IoT. On the other hand, blockchains, and in general Distributed Ledger Technologies (DLTs), have attracted recently the attention of academia and industry working in the energy sector. This is mainly driven from the fact that blockchains is the enabling technology that allows for achieving the 4Ds of the energy systems of the future: Digitalization, Decarbonization, Democratization, and Decentralization. This ability of blockchains is based on the fact that said technologies do not need a third-party to assume the role of the trusted authority, but rather allow embedding trust within the network.

In this paper we present a decentralized Automatic Meter Reading (AMR) system over a LoRaWAN network. The decentralized character of the AMR system is guaranteed by the underlying blockchain used to store the meter readings of the energy meters also ensuring that meter owners have control over their own data and the ability to trade them via a decentralized data marketplace an exchange.

To demonstrate the advantages of the proposed approach, a test LoRaWAN network has been setup at our laboratory, where battery-powered LoRaWAN nodes were connected to smart meters through the DLMS/COSEM protocol. The LoRaWAN nodes are built around a powerful microprocessor board that has a dual processor and Wi-Fi radio system on chip. Moreover, an extra ULP-coprocessor that can monitor GPIOs, the ADC channels and control most of the internal peripherals during deep-sleep mode while only consuming 25uA. This characteristic of low energy consumption of the microprocessor board allows the device to operate for several years on battery, depending of course on the number of meter reading per day. A number of microservices run locally at the laboratory server that provides, among other things, access to the Ethereum blockchain. Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality. With this approach, the smart meters used in the demo have been converted into fully functional LoRaWAN-compatible Ethereum blockchain nodes.

LORA NETWORKS

LoRaWAN network architecture is typically laid out in a star-of-stars topology in which gateways is a transparent bridge relaying messages between end-devices and a central network server in the backend. Gateways are connected to the network server via standard IP connections while end-devices use single-hop wireless communication to one or many gateways. All end-point communication is generally bi-directional, but also supports operation such as multicast enabling software upgrade over the air or other mass distribution messages to reduce the on-air communication time.
LoRa is a low-power wide area network with features supporting low-cost mobiles phones, so as to ensure two-way communication for the IoT, machine-to-machine (M2M), smart city and industrial applications. LoRaWAN constitutes the precursor of the development of these technologies and has numerous different categories of devices to address the various needs over a

broad range of applications. It similar, in some points, to Sigfox and Neul, and aims at WAN applications providing low-consumption WAN networks with features particularly required for the secure, two-way and low-cost mobile communication over IoT, M2M, industrial and smart city applications.

LoRa communication technology has been developed by Semtech and constitutes a new wireless protocol designed for long-range, low power communication. LoRa network allows devices to connect to the Internet even when there is no Wi-Fi, using a system operating complementary to the mobile telephony network. An additional small antenna added to the base-stations of mobile telephony stations allows the transmission and reception of low-power but long-range radio signals.

A LoRa network topology consists of end nodes devices, gateways/concentrators, network and application servers as depicted in the Figure 1. Through the application server, the user creates applications which are registered in his/her device. End nodes transmit the data drawn from the sensors to more than one gateway/concentrator in range. The gateways/concentrators forward messages to the network server. In addition to forwarding the messages to the appropriate applications, the network server decodes the messages so that they are understood by the user.

Each LoRa gateway can manage thousands of nodes. As a result, compared to other wireless networks, the creation of a complex network requires less infrastructure and lower costs. The LoRaWAN specification varies slightly from region to region based on the different regional spectrum allocations and regulatory requirements.

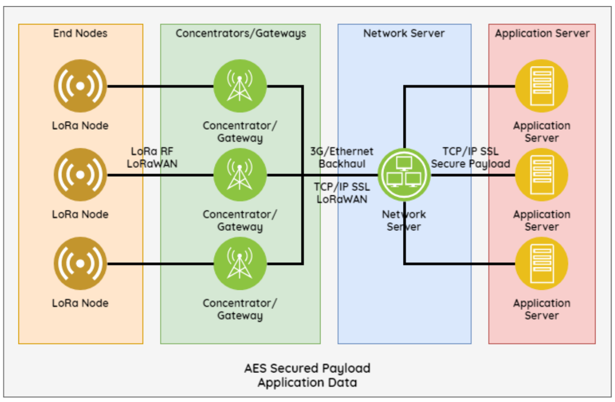

Figure 1: Overview of the architecture of LoRa network

SOLUTION ARCHITECTURE

The architecture of the proposed decentralized AMR system is illustrated in Figure 2, where the various components, both hardware and software, and their interfaces are depicted.

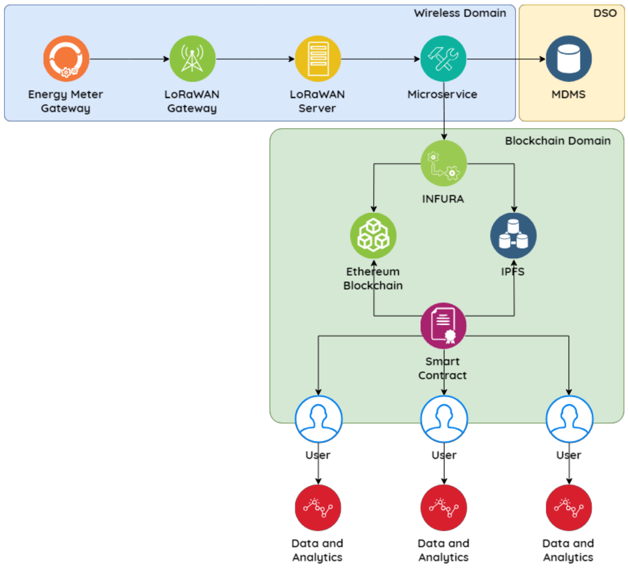

Figure 2: Proposed system architecture

One may observe that from high-level overview, the systems consists of two different and distinct subsystems:

- the wireless LoRaWAN part, and
- the blockchain part.

The Wireless Subsystem

The core component of the wireless subsystem is the energy meter blockchain gateway. An overview of the internal architecture of the meter gateway in depicted in Figure 3 below.

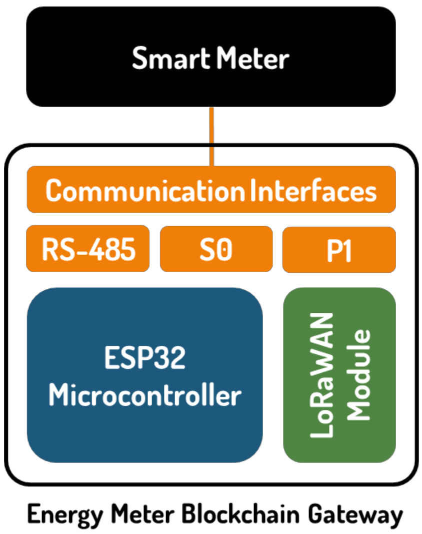

Figure 3:Energy meter gateway

The heart of the energy meter gateway is the ESP32 [2] microcontroller. In order for the energy meter gateway to have access to energy meter readings the following communication interfaces are provided:

- RS-486 for DLMS/COSEM communications;
- S0 for pulse counting; and
- P1 for DSMR Requirements) energy meters.

The energy meter gateway is also equipped with a RAK811 LoRa module [3]. The RAK811 is a wireless transparent communications module, based on the Semtech SX1276 IC. RAK811 offers communication over a distance of 3km and also an improved receiver sensitivity. Moreover, the RAK811 module fully supports and conforms to the specifications of LoRaWAN Class A and C protocols, thus facilitating an easy access to the various LWPA IoT platforms available in the market.

As already mentioned above, a LoRaWAN network and application server is required. An overview of the architecture of the necessary inftrastructure along with the used communication interfaces and protocols is provided in the illustration below.

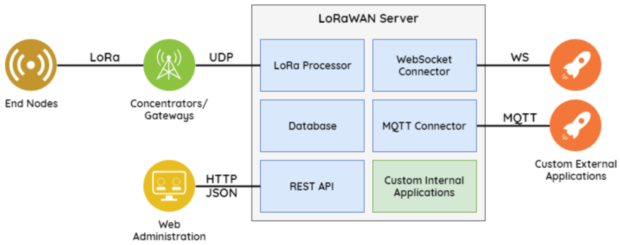

Figure 4: LoRaWAN network and application server architecture and communication protocols

The LoRaWAN network and application server that is used implements the following functionalities:

- Implements the LoRaWAN Specification v1.0.2
- Performs all required encryption and integrity checks;
- Invokes external applications. It currently supports connections via:
  - WebSocket protocol RFC6455;
  - HTTP/1.1 and HTTP/2 protocol (REST API);
  - MQTT v3.1/v3.1.1; and
  - AMQP 0-9-1.
- Handles (any number of) Class A or Class C devices;
  - Supports both the node activation by personalization (ABP) and the over-the-air activation (OTAA);
  - Supports both unconfirmed and confirmed data uplink and downlink;
  - Supports multicast to user-defined groups; and
  - Supports all regions standardized in LoRaWAN 1.0.2 Regional Parameters for Europe, US, China, Australia, Asia, South Korea and India.
- Provides a network management interface:
  - Monitors the server, gateways and node health status and displays device battery and connection quality indicators; and
  - Supports both manual and automatic configuration of TX power and data rate (ADR).

Ethereum Blockchain

A blockchain is a growing list of records, called blocks, which are linked to each other using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and the transaction data.

Among the various blockchain platforms available, in this paper we use the Ethereum blockchain [4]. Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. When running on the blockchain a smart contract becomes like a self-operating computer program that automatically executes when specific conditions are met.

One of the main challenges that we have to overcome when considering blockchain-based solutions for dealing with handling of energy data, is the fact that is expensive to store data on the Ethereum blockchain. In addition to that, due to intrinsic limitations of the processing power of microcontrollers and the relatively high computational cost required by the blockchain clients, it is extremely hard, and in some cases impossible, to implement a blockchain client on the microcontroller itself, while at the same time trying to keep the cost and the complexity of the solution as low as possible. Also running an Ethereum client locally on the microcontroller, requires hours to sync up the client, which uses up a huge chunk of memory and bandwidth, while the entire Ethereum blockchain gets downloaded.

As a remedy to the aforementioned challenges, in our presented solution for a decentralized AMR system we make use of the following services and protocols:

- Infura and
- InterPlanetary File System

Infura

Infura [5] is a hosted Ethereum node cluster that lets users run their application without requiring the need to set up their own Ethereum node or wallet. In other words, Infura is a platform as a service for Ethereum networks.

InterPlanetary File System

The InterPlanetary File System (IPFS) [6] is a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.
IPFS is meant to be a replacement for HTTP. Most notably, IPFS never has a single point of failure. It’s a peer-to-peer distributed file system that would decentralize the Internet and make it much more difficult for a service provider or hosting network to pull the plug and make published information suddenly disappear [7]. Figure 5 shows a graphical comparison between the architectures of HTTP and IPFS.

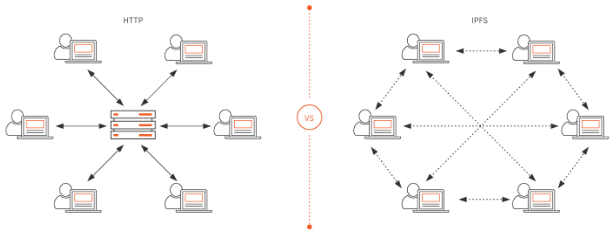

Figure 5: The IPFS (Source: [7])

The use of Infura along with the IPFS has a number of advantages:

- Huge amounts of data can be stored on the IPFS, due to the fact that only the hash of the file will be stored on the Ethereum blockchain and not the data file itself. The hash will serve as a pointer to the actual data file stored on the IPFS;
- Infura provides secure, reliable, scalable, and easy to use Application Programming Interfaces (APIs) to access the Ethereum network and the IPFS;
- Infura provides TLS enabled public endpoints; and
- The code is portable on Ethereum's interface using JSON RPC, Web3.

THE DECENTRALIZED AMR SYSTEM AND DATA MARKETPLACE

The architecture of the proposed approach to a decentralized AMR system and energy data marketplace is illustrated in Figure 2. As already mentioned above a key component of this approach is the LoRaWAN compatibly energy meter gateway that sends at regular intervals energy consumption information to the LoRaWAN network and application server through the LoRaWAN gateway. In our approach the energy meter gateway stores in its internal memory the energy consumption at intervals of one (1) minute and transmits a LoRa data package containing the one-minute data every one (1) hour to the LoRaWAN server, which in turn announces the arrival pf the hourly data package via a message on a specific topic of the MQTT broker that is also part of the LoRaWAN server.

The orchestration of the whole process is performed by a microservice running on a server at our laboratories, as one may observe from Figure 2. The tasks that this microservice performs are:

a. listen on the specific topic of the MQTT broker of the LoRaWAN network and application server;
b. upon arrival of a new LoRaWAN package, parse the package and store the energy measurements locally;
c. send the respective timestamped energy measurements to the utility Meter Data Management System (MDMS);
d. write the data to the IPFS and store the hash of the respective data file to the blockchain.

As far as point (d) above is concerned, the energy measurements are collected and consolidated in a single JSON file on user-configurable time intervals. In our setup we have chosen to have the data consolidated and written to the IPFS every month, along with the respective data file hash that is stored in the Ethereum blockchain. This process is carried out for all energy meter, along with the connected energy meter gateways, that participate in our decentralized AMR and data marketplace system. It should be mentioned that for both the Ethereum blockchain and the IPFS, the Infura service is used for exploiting the offered benefits described previously.

As already mentioned in the introductory sections of this paper, the main purpose of our proposed approach is to create an energy data marketplace, structured is such a way so that the consumers and prosumers maintain the ownership of their energy data. Moreover, the end-customers that participate in this platform will be in the position to trade (buy and sell) energy-related data in a decentralized, trusted, and transparent way. These characteristics and requirements of the platform are guaranteed by the use of the Ethereum blockchain and the concept of smart contracts.

For an end-user to make his/her energy data available for other participants of the marketplace to acquire the procedure is as described below.

- Through a simple and intuitive web user interface, the end-customer selects the dataset he/she wants to sell and sets a price range for the transaction.
- The dataset is listed in the marketplace for other platform users to get notified about its availability.
- Platform users submit their offers for buying the specific dataset.
- Platform selects the highest offer and provides the higher bidder with an encrypted (with buyer's public cryptographic key) version of the IPFS hash that corresponds to the newly acquired dataset.

It should be mentioned that the bidding process is totally automated, transparent, and decentralized since all transactions, pricing information, and seller and buyer information are handled by smart contracts generated automatically by the platform and stored permanently on the Ethereum blockchain. Finally, all transactions are carried out using the Ether (ETH) cryptocurrency.

CONCLUSIONS, CONSIDERATIONS, NEXT STEPS, AND IMPROVEMENTS

In this paper we presented a decentralized approach to AMR along with marketplace for trading of energy-related data based on the Ethereum blockchain and the IPFS for decentralized data storage. Simulations and demonstration scenarios allowed us to verify that the proposed approach is capable of enabling new business models for the utilities and the end-customers, based on the data collected from the smart meters. As a logical next step is to consider also other types of energy-related data for storing and trading them, such as energy production data, demand and production forecasting data, meteorological data, etc.

As already mentioned, the concept of blockchains, as a type of distributed and immutable ledger, is quite new. Its application to use cases in the energy sector is even newer and still in its infancy. Therefore, there are still a number of open issues and challenges that need to be addressed before such use cases and applications reach a maturity level that can ensure their commercialization and their actual deployment in large-scale industrial projects. Decentralized data marketplaces are not an exception, as well.

In order to build a decentralized data exchange and marketplace the following actors and components need to be considered [8]:

- **Asset or Data Asset**
  A data set or data service.
- **Data Owner or Data Service Provider**
  Someone who has assets that they want to sell (or give away freely). An example is an industrial consumer with 10 years of energy consumption data.
- **Publisher**
  A service which mediates access to assets on behalf of data owners or data service providers.
- **Consumer**
  Someone who wants assets. An example is a data scientist working at an economic think tank.
- **Verifier**
  A person or a software service that checks some steps in transactions. For example, a verifier might check to see if a cryptographic signature is valid and then get rewarded for doing so.

An illustration of the required actors and components is provided below.

Figure 6: Concepts in a decentralized data exchange marketplace

To satisfy the aforementioned requirements and characteristics of a decentralized data exchange and marketplace the Ocean Protocol was developed. Ocean Protocol [8] is an ecosystem for the data economy and associated services. It provides a tokenized service layer that exposes data, storage, compute and algorithms for consumption with a set of deterministic proofs on availability and integrity that serve as verifiable service agreements. Through blockchain technology and tokens, Ocean Protocol connects data providers and consumers, allowing data to be shared while guaranteeing traceability, transparency, and trust for all stakeholders involved. Ocean Protocol is also designed to give data owners control over their data assets and prevent them from being locked in to any single marketplace.

Our next steps include the extension of the proposed platform to include other types of energy-related data, as well as enhancement of the underlying data exchange marketplace using the Ocean Protocol. Finally, it should be mentioned, that issues related to the General Data Protection Regulation (GDPR) and the current legislative and regulatory paper will also be analyzed and incorporate them in the proposed platform.

REFERENCES

[1] LoRa Alliance, "LoRaWAN," [Online]. Available: https://lora-alliance.org/about-lorawan.

[2] "ESP32," [Online]. Available: https://www.espressif.com/en/products/hardware/esp32/overview.

[3] RAK Wireless, "RAK811 LoRa Module," [Online]. Available: https://www.rakwireless.com/en/module/lora/RAK811.

[4] "Ethereum," [Online]. Available: https://www.ethereum.org.

[5] "Infura," [Online]. Available: https://infura.io.

[6] "InterPlanetary File System," [Online]. Available: https://ipfs.io.

[7] [Online]. Available: https://www.maxcdn.com/one/visual-glossary/interplanetary-file-system/.

[8] "Ocean Protocol - A Decenralized Data Exchange Protocol to Unlock Data for AI," [Online]. Available: https://oceanprotocol.com.