Deliverable Proof – LETchain Blockchain Technical Architecture Blueprint

KIC project **the report results from**	*Blockchain Solution for Incentivising Low-Emission Transportation (LET-Chain)*
Name of document	LETchain Blockchain Technical Architecture Blueprint
Summary/brief description of document	This document aims to describe the technical layout of the Infrastructure that will provide the basis for the LETchain. It's, for the time being, one Smart Contract running on the Ethereum Blockchain.
Date of report	31.12.2017

Supporting documents:

Relevant report

In corporation with

BLOCKCHAIN BÜRO

An initiative of

Climate-KIC is supported by the
EIT, a body of the European Union

31.12.2017

LETchain Blockchain Technical Architecture Blueprint

Abstract

This document aims to describe the technical layout of the Infrastructure that will provide the basis for the LETchain. It's, for the time being, one Smart Contract running on the Ethereum Blockchain.

Table of contents

Overview scheme

Example Flow

1) A corporation associates a given amount of FIAT money (currency issued and by a state) to an employee as an incentive and informs the admin (see p.4 for a description of the administrator).

2) The admin issues the equivalent amount of token (exchange rateToken : FIAT = 1:1) to the incentivized employee.

3) The employee spends the token to buy goods from a supported vendor (e.g. electrical power for cars or public transportation vouchers).

4) The vendor wants to change the token back into FIAT money and informs the admin (or makes a transaction to the admin).

5) The admin burns the token from the vendors account and writes a bill for the corporation.

6) The corporation pays the bill to the vendor out of the associated FIAT money.

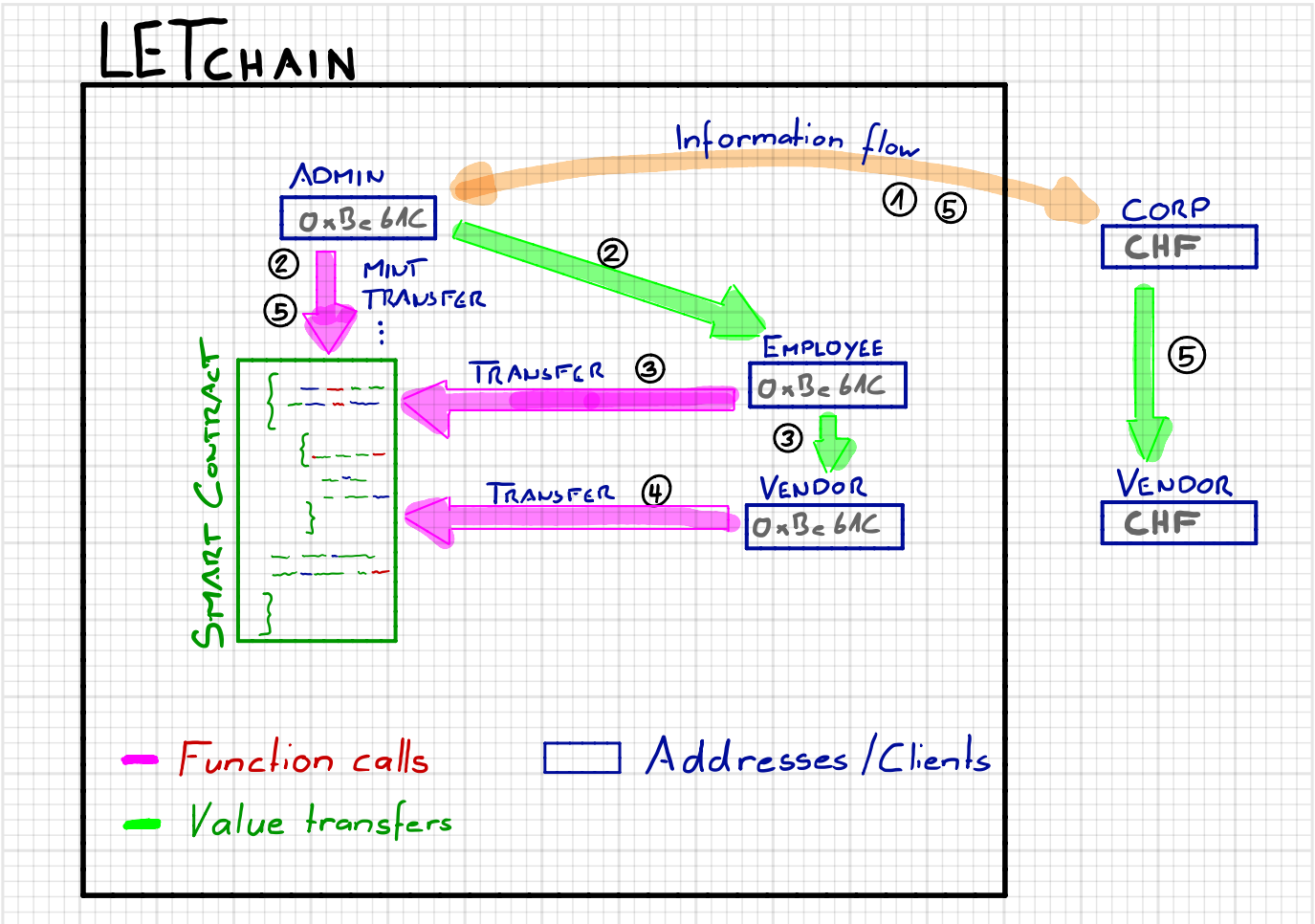

Fig. 1: LETchain scheme

The Ethereum Blockchain

The need of a real distributed computing platform was first fulfilled by Ethereum in 2014. The Project is founded and guided by Vitalik Buterin. It's the oldest platform that can deal with a variety of Smart Contracts. These are contracts that «run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference».[1] Smart contracts are deterministic exchange mechanisms controlled by digital means that can carry out the direct transaction of value between untrusted agents.[2]
The Ethereum Virtual Machine (EVM) can execute Smart Contracts on a shared global infrastructure. They are treated as autonomous scripts or decentralized applications that are stored in the Ethereum Blockchain for later execution by the EVM. Instructions embedded in Ethereum contracts are paid for in ether (the token of the Ethereum Blockchain) and can be implemented in a variety of Turing-complete scripting languages. Turing-completeness describes the ability to handle any sort of algorithms (e.g. loops, if-then-conditions). The many opportunities to interact with this Blockchain are to «create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract)»[3] or to create a cryptocurrency. This broad usability made Ethereum the Blockchain of choice for ICO (Initial Coin Offerings) in 2017 and gained a lot of publicity in the process. To write scripts or decentralized applications the programming language Solidity is used. After written, the Solidity code is compiled into bytecode that is executable on the EVM.
Ethereum currently uses a proof-of-work consensus. With its «Serenety» release (the last of four Ethereum development phases), the network plans to switch from a hardware mining to virtual mining (proof-of-stake). If successfully executed, this switch will be a fundamental change to the Ethereum network and lower the power consumption drastically.
In a comparative study made in the first phase of this project the Ethereum Blockchain has been found the most suitable infrastructure for the LETchain. Its great flexibility and broad distribution make it an ideal candidate to program the LETchain token on it and test it in a pilot phase.

---

[1] https://www.ethereum.org

[2] Szabo, Nick (1997). "The Idea of Smart Contracts". Archived from the original on 2 May 2017.

[3] https://www.ethereum.org

The LETchain Smart Contract

To fulfill the requirements of a special purpose cryptocurrency the base smart contract needs to have several functions which are described below. In its first version, the Smart Contract will have a centralized administrator. This administrator has full control over the functions of the currency and receives the initial funds after creation. In a further step the centralized administrator could likely be replaced by the Smart Contract itself. This is not necessary for a proof-of-concept..

After the construction of the token, all it's initial supply will be transferred to the creator of the contract who acts as the central administrator. This role has the ability to mint new tokens, burn used ones as soon as their value is retransferred to FIAT money, transfer coins - even from foreign addresses, transfer the ownership of the contract (and therefore the administrator role) and to freeze coins in case of regulatory requirements. The administrator role bears a great responsibility that can be abused. For example, new coins could be generated and brought into circulation without being backed by a company's incentive fund. Although abuse could be easily detected because of transparent financial flows within the blockchain, it should be desirable to replace this centralized, trusted role with a decentralized, trust-minimized Smart Contract. This will not be part of this use-case.

Hereafter are the functions and events that can be called by a user of the Smart Contract.

Functions

CONSTRUCTOR

The Smart Contract is owned by the sender. In the creation process of the token, all the created funds are transferred to the creator address. The constructor function holds information about the name and symbol of the token, defines the decimals of the currency and sets the initial supply.

TRANSFER

This function transfers a set amount of tokens from a source address to a target address. This is the most important function and defines the core function of the LETchain. Relocation of values within the LETchain ecosystem are made possible by this function. Transfers can be called by any user that holds tokens.

TRANSFER FROM

This function can only be called by the contract owner (administrator) and is able to transfer funds from a foreign address.

APPROVE AND CALL

Approve and call will be a beneficial function for future use. In contrast to users, contracts can not call events. With this function a given contract is approved to use a given amount of tokens and notified about this ability. This function could make it possible to extend the ability of the LETchain with other smart contracts. This could be a viable solution for rolling out new versions without the necessity to replace the base contract. This is an administrator-only function.

BURN

If value has to be transferred outside the network by exchanging it to FIAT money, the corresponding tokens have to be destroyed to avoid monetary increase. This is realized through the burn function. A set value of tokens can be destroyed. It can only be called by the administrator.

MINT

Minting tokens is the opposite of destroying them. This function is used to transfer value into the LETchain ecosystem. The minted tokens represent a certain value of FIAT money that can now be transferred within the Ethereum blockchain. Obviously, this function is reserved for the administrator.

TRANSFER OWNERSHIP

The administratorship can be transferred from one address to another. It has to be discussed if this role can be fulfilled by more than one party. Having multiple administrators increases the risk of abuse. The Smart Contract ownership can only be changed by the current owner (administrator).

FREEZE

Another administrator-only function whose call will result in freezing the funds of a given address. The submitted address will be flagged as frozen. Optional, the flagged address should not be able to transfer funds anymore.

Events

Events are empty functions that can be called to keep track of activities. They are usually called (triggered) by a software, like a wallet (a software that manages tokens), and return information about what is happening within the contract. For example, to display if an address is frozen or not.

TRANSFER

This event notifies clients about transferred tokens as well as the sending and receiving of addresses.

BURN

Notifies clients about the amount of tokens that have been burned (destroyed).

FROZEN

Returns information about if an address is in frozen state or not. Freezing of accounts could be necessary if fraud is suspected or regulatory uncertainties arise.

Risks and open questions

Versioning

As of today it is unclear how the versioning of the LETchain should be carried out. Once submitted, a Smart Contract can not be changed anymore. An improvement or feature expansion requires the deployment of a new contract. Client software has to be noticed about this, changed and switched to the new contract. In addition to being unpractical, this creates security issues.

Transfer Fees

To call functions from a Smart Contract on the Ethereum Blockchain, a miner fee has to be included. This represents the incentive for miners to confirm transactions. The fee is payed in Ether, which should be present in any of the client software. If the Ether balance of an account falls below the required fee, LETchain tokens are frozen in this account.
To avoid confusion and further dealing with another currency (namely, Ether) by the customer, an autofill function can be implemented. This function will make sure that every account has the sufficient amount of ether to call functions of the Smart Contract. How the donor of this Ether is reimbursed (for example fees) remains open to discussion at this point.