ERC777 the new token standard, and trust-less payment channel tokenized loyalty points

Master's Thesis submitted to the
Faculty of Informatics of the *Università della Svizzera Italiana, Switzerland*
in partial fulfillment of the requirements for the degree of
Master of Science in Informatics

presented by
Jacques Dafflon

under the supervision of
Prof. Cesare Pautasso
co-supervised by
Mr. Thomas Shababi

June 2018

I certify that except where due acknowledgement has been given, the work presented in this thesis is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; and the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program.

Jacques Dafflon
Neuchâtel, 20 June 2018

Abstract

Ethereum decentralized computing Ethereum is decentralized platform running on a custom built blockchain launched on July 30th 2015. Unlike more traditional crypto-currencies, Ethereum is a computing platform with a Turing-complete programming language used to create and execute arbitrary pieces of code known as smart contracts.

In this thesis describes how the power of smarts contracts is leveraged to have fast transactions despite the slowness of the blockchain.

Acknowledgements

ACKS

Contents

Figures

Tables

Chapter 1

Introduction

1.1 Motivation

Ethereum is decentralized platform running on a custom built blockchain. Similarly to Bitcoin and other blockchains it suffers of a few issues. One of the most prominent one being the slow transaction speed. The Ethereum network can handle at best 15 transactions per second—Bitcoin is even worse with 3 or 4 transactions per second—which is clearly insufficient for a global daily usage. By comparison, VisaNet is theoretically capable to handle up to 65'000 transactions per second. While this number is disputed, even the more realistic value of 1700 transactions per second is well above the Ethereum blockchain capacity. Ethereum is still immature and a lot is still left to do; payment channels is one of the effort to increase the number to transactions processed per second. Originating from Bitcoin's lighting network, payment channels rely on exchanging off-chain transactions and only use the blockchain as a safeguard or to settle the past off-chain transactions. Smart contracts in Ethereum are leveraged for more exhaustive and flexible channels—compared to Bitcoin's—which can accept both Ether and tokens, allow top-ups and more.

Another issue, specifically associated with Ethereum, is related to the design of ERC20, the token standard. The way to transfer tokens to an externally owned address or to a contract address differ and transferring tokens to a contract assuming it is a regular address can result in losing those tokens forever.

The new ERC777 token standard solves those problems and offer new powerful features which facilitates new interesting use cases for tokens.

1.2 Description Of The Work

This thesis starts by covering the overall mechanism of Ethereum payment channels and details the contributions to improve the existing payment channel proof of concept to bring it closer to a safe production ready system. Ethereum payment channels have the ability to interact with tokens, both as the asset of the channel but also within a trustless reward system based on the usage of said channel.

Subsequently, an analysis of tokens is provided to explain the application of tokens in Ethereum, the ERC20 token standard and its issues. It is followed by a detailed description

of the new ERC777 standard for tokens, developed as part of this thesis. This includes how the issues of ERC20 are solved, the improvements brought by ERC77, the efforts made to advertise the standard to the community and how community's reception and feedback was taken into account to developed the standard.

Chapter 2

Ethereum, A Decentralized Computing Platform

Ethereum is a decentralized computing platform. This platformed is fueled by Ether, the second largest cryptocurrency in world based on market capitalization—after Bitcoin. However, while Bitcoin is aimed to be a currency, Ethereum and Ether have different goals. Ether is rather literally designed to be more than a currency, mostly through the use of smart contracts.

Smart contracts are simple programs, written in a domain specific langauage—generally Solidity—

Short chapter explaining the following concepts:

- Ethereum Blockchain
- Smart contracts

Chapter 3

Payment Channels

- Speed Issues With The Blockchain
- Off-chain Solutions (Basic Explanation of Payment Channels)
- Use Cases
- Current Implementation And Improvements Made

Chapter 4

Tokens, And The Current Standard ERC20

Short description of tokens and their use.

Explain ERC20:

- specifications
- issues (vulnerabilities, locking)
- examples of attacks and locked funds

Mention ERC223 and its own problems:

- tokensFallback on all contracts
- not backwards compatible with ERC20
- unusable by existing contracts
- community/human issues with the author

Chapter 5

ERC777, A New Advanced Token Standard For Ethereum Tokens

Explain ERC777 in thorough details:

- specifications
- ERC820
- `TokensSender` and `TokensRecipient`
- Operators
- ERC20 compatibility
- Collaboration with Jordi Baylina
- Public Reception

Chapter 6

Tokenized Loyalty Points

- Basic Idea of Loyalty Points From Payment channels
- Tx Based Tokens
- Volume Based Tokens
  - modifications to the payment channel
- Redeeming process
  - Burning strategies

    by the token contract
    allowed set of “burners” (contracts of the loyalty program)
    anyone

Chapter 7

Future Research and Work

- ERC777
  - Generic operators
  - Generic TokensSender And TokensRecipient
  - Promote ERC777
  - Assist In The Implementation of ERC777 Technologies (Wallet, Exchanges, Blockchain Explorers)
- Payment Channel
  - Other use cases for tokens (actually voting with your wallet)
  - Tax deductions on some tx (add tag in payment channel?)
- Loyalty Programs
  - On chain (ETH rewards, tokens Rewards, Pay with Tokens)
  - Off chain (T-shirts, coffee machines and toasters)

Chapter 8

Conclusion

I'l do this one at the end

Glossary