

---

# ERC777

## A New Advanced Token Standard For The Ethereum Blockchain

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  
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 smart contracts is leveraged to have fast transactions despite the slowness of the blockchain.



# Acknowledgements

ACKS





# Contents

|  |            |
|--|------------|
| <b>Contents</b>  | <b>vii</b> |
| <b>List of Figures</b>   | <b>ix</b>  |
| <b>List of Tables</b>  | <b>xi</b>  |
| <b>1 Introduction</b>  | <b>1</b>   |
| 1.1 Motivation . . . . .   | 1          |
| 1.2 Description Of The Work . . . . .  | 1          |
| <b>2 Ethereum, A Decentralized Computing Platform</b>                          | <b>3</b>   |
| 2.1 The Ether Currency And Gas . . . . .                                       | 3          |
| 2.1.1 Computing Fees . . . . .   | 3          |
| 2.2 Ethereum Accounts . . . . .  | 4          |
| 2.3 Transactions And Messages . . . . .  | 4          |
| 2.4 The Ethereum Virtual Machine . . . . .                                     | 5          |
| 2.5 Solidity . . . . .   | 5          |
| <b>3 Tokens And Standardization</b>  | <b>7</b>   |
| 3.1 Definition of a token . . . . .  | 7          |
| 3.2 Standardization . . . . .  | 8          |
| 3.3 Ethereum Improvement Proposals And Ethereum Request For Comments . . . . . | 8          |
| <b>4 ERC20 Token Standard</b>  | <b>9</b>   |
| 4.1 The First Token Standard . . . . .   | 9          |
| 4.2 Transferring ERC20 Tokens . . . . .  | 10         |
| 4.3 Strength And Weaknesses Of ERC20 . . . . .                                 | 13         |
| 4.3.1 Locked Tokens . . . . .  | 13         |
| 4.3.2 Approval Race Condition . . . . .  | 13         |
| 4.3.3 Absence Of burning . . . . .   | 14         |
| <b>5 ERC777, A New Advanced Token Standard For Ethereum Tokens</b>             | <b>17</b>  |
| <b>6 ERC820, Pseudo-introspection Registry contract</b>                        | <b>19</b>  |

---

|           |                                  |           |
|-----------|----------------------------------|-----------|
| <b>7</b>  | <b>Competing Token Standards</b> | <b>21</b> |
| 7.1       | ERC227 . . . . .                 | 21        |
| 7.2       | ERC827 . . . . .                 | 21        |
| 7.3       | ERC995 . . . . .                 | 21        |
| <b>8</b>  | <b>The State Of Tooling</b>      | <b>23</b> |
| 8.1       | Compilation . . . . .            | 23        |
| 8.2       | Testing and Coverage . . . . .   | 23        |
| 8.3       | Documentation . . . . .          | 23        |
| 8.4       | Missing Tools . . . . .          | 23        |
| <b>9</b>  | <b>Future Research and Work</b>  | <b>25</b> |
| <b>10</b> | <b>Conclusion</b>                | <b>27</b> |
|           | <b>Glossary</b>                  | <b>29</b> |

# Figures

|     |  |    |
|-----|--|----|
| 4.1 | Standad ERC20 transfer between two regular accounts: Alice and Bob. . . . .                          | 10 |
| 4.2 | Standad ERC20 transferFrom between a regular account Alice and a contract<br>account Carlos. . . . . | 12 |
| 4.3 | Sequence of calls for the approve/transferFrom attack. . . . .                                       | 14 |



# Tables



# Chapter 1

## Introduction

### 1.1 Motivation

Ethereum is a custom built blockchain which provides a decentralized computing platform. 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 lightning 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 develop the standard.



## Chapter 2

# Ethereum, A Decentralized Computing Platform

The Ethereum network is a decentralized computing platform. As described in its the white paper, Ethereum “[...] is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions” [Buterin, 2013]. This differentiate it from Bitcoin which is a trustless peer-to-peer version of electronic cash and lacks a Turing-complete language.

## 2.1 The Ether Currency And Gas

The Ethereum still includes its own built-in currency named ether akin to Bitcoin. It “[...] serves the dual purpose of providing a primary liquidity layer to allow for efficient exchange between various types of digital assets and, more importantly, of providing a mechanism for paying transaction fees” [Buterin, 2013]. The currency comes with different denominations defined. The smallest denomination is a wei—named after the computer scientist and inventor of b-money, Wei Dai. An ether is defined as  $10^{18}$  wei. In other words a wei represents 0.000000000000000001 ethers. The wei denomination is used for technical discussions. Most tools, libraries and smart contracts use wei and the values are only converted to ether or some other denomination for the end-user.

### 2.1.1 Computing Fees

The fees is part of the incentive mechanism as in Bitcoin. The main difference is the way the fees are expressed and computed. In Bitcoin the fees are fixed and set as the difference between the input value and the output value. Because transactions on the Ethereum network execute code of a Turing-complete language, the fee is defined differently “[...] to prevent accidental or hostile infinite loops or other computational wastage in code” [Buterin, 2013]. A transaction define two fields `STARTGAS` and `GASPRICE`. The `STARTGAS`—also referred as just gas or `gasLimit`—is the maximum amount of gas the transaction may use. The `GASPRICE` is the fee the sender

will pay per unit of gas consumed.

A computational step cost roughly one unit of gas. This is not exact as some steps “cost higher amounts of gas because they are more computationally expensive, or increase the amount of data that must be stored as part of the state” [Buterin, 2013]. A cost of five units of gas per byte is also applied to all transactions.

Another advantage of not tightly coupling the cost of execution with a currency—e.g. set the cost of a computation step to three wei—is to dissociate the execution cost of a transaction and the fluctuation in value of ether with respect to fiat currencies. If the price of ether increases exponentially with respect to a currency such as the dollar, a fixed price per computational step may become prohibitive. The GASPRICE circumvent this issue. While the amount of gas consumed by the transaction will remain constant, the price for the gas can be reduced.

## 2.2 Ethereum Accounts

There are two types of accounts on the Ethereum network, externally owned accounts—commonly referred to as regular accounts—and contract accounts. A regular account is an account controlled by a human who holds the private key needed to sign transactions. In contrast, a contract account is an account where no individual knows the private key. The account can only send its ether and call function of other accounts through its associated code. While an account is defined as “having a 20-byte address and state transitions being direct transfers of value and information between accounts” [Buterin, 2013], the words “account” and “address” are often used interchangeably. Nonetheless, to be exact, an account is defined in the white paper [Buterin, 2013] as a set of four fields:

**Nonce** A counter used to make sure each transaction can only be processed once

**Balance** The account’s current ether balance

**Code** The account’s contract code, if present (for contracts)

**Storage** The account’s permanent storage (empty by default)

## 2.3 Transactions And Messages

Ethereum makes a distinction between a transaction and a message. A transaction is a signed data packet only emitted from a regular account. This packet contains the address of a recipient, a signature to identify the sender, the amount of ether sent from the sender to the recipient a data field—which is optional and thus may be empty and the gas price and gas limits whose meaning is explained in section 2.1.1.

A message is defined as a “virtual objects that are never serialized and exist only in the Ethereum execution environment” [Buterin, 2013]. A message contains the sender and recipient, the amount of ether transfer with the message from the sender to the recipient, an optional potentially empty data field and a gas limit.

Transactions and messages are very similar. The difference is that a transaction comes from a regular account only and a message comes from contract. A transaction can call a function of a contract which in turn can create a message and call another function, either on itself or on another contract, using the CALL and DELEGATECALL opcodes. The gas used for messages comes from the transaction which triggered the call.

## 2.4 The Ethereum Virtual Machine

Ethereum is a decentralized computing platform. In other words alongside a blockchain, Ethereum provides a Turing-complete language and the Ethereum Virtual Machine (EVM), a virtual machine able to interpret and execute code. This code “is written in a low-level, stack-based bytecode language, referred to as “Ethereum virtual machine code” or “EVM code”[Buterin, 2013]. This bytecode is represented by a series of bytes. Code execution simply consist of setting an instruction pointer at the beginning of the bytecode sequence, perform the operation at the current location of the point, and then increment the instruction pointer to the next byte. This is repeated forever until either the end of the bytecode sequence is reached, an error is raised or a `STOP` or `RETURN` instruction is executed.

The operations can perform computations and interact with data. There are three kinds of mediums to store data. First, there is a stack. This a commonly know abstract data type in computer science. Data can be added by using a push operation which adds the data on top of the stack. Mutually, the data can then be removed with a pop operation which removes and return the data from the top of the stack. Essentially, the stack is known as a Last-In-First-Out (LIFO) data structure meaning the last value pushed (added) is the first value popped (taken). Secondly there is a memory, which is an ever-expandable array of bytes. Those kinds of storage are both non-persistent storage. Within the context of Ethereum, this translates to this data only being available within the call or transaction and not being permanently stored on the blockchain. The third and last kind of storage is commonly referred to as “storage” is a permanent key/value store intended for long-term storage.

In addition to those types of storage, the code may access the block header data, and the incoming transaction’s sender address, value, and data field.

## 2.5 Solidity



## Chapter 3

# Tokens And Standardization

### 3.1 Definition of a token

A token in a generic term is a digital asset. A token can essentially represent any asset which is fungible and tradable. Tokens are built on top of an existing blockchain and with its Turing-complete language and popularity, Ethereum is a prime candidate as a platform to build tokens on top of. The concept of tokens is in fact described in the Ethereum white paper as “[having] many applications ranging from sub-currencies representing assets such as USD or gold to company stocks, individual tokens representing smart property, secure unforgeable coupons, and even token systems with no ties to conventional value at all, used as point systems for incentivization” [Buterin, 2013]. Examples of tokens include EOS, TRON, Status, Aragon or Gnosis.

Tokens are the result of certain types of smart contracts which maintain a ledger on top the Ethereum blockchain and with the goal of acting like a “coin”. Internally this smart contract simply holds a mapping from addresses to balances. The balances are expressed with unsigned integers. This design choice is similar to ethers which themselves internally are expressed as wei. It also comes from the fact that the Solidity language does not fully support floating point numbers. The smart contract then exposes functions to let user acquire tokens—known as minting—destroy tokens—known as burning—and most importantly to let token holders transfer their tokens. From a business perspective, a token is the possibility for a company to issue shares, securities or any form of accounting unit; even their own currency which the company has control over. Many companies offer services which can be purchased only using their tokens. Based on this economic principle, comes the neologism: Initial Coin Offering or ICO. An ICO is a process where a company will sell a limited quantity of their tokens for a fixed price before their product is finalized. This is for a start-up a mean to raise funds on their own without having to go through the vetting process traditionally required by venture capitals and banks. An ICO is usually done through a smart contract which will trade tokens for ethers at specific times and for a certain price. This allows the start up to raise some capital and the investors to potentially gain a profit by buying tokens at a discount. There is of course the risk that the start-up fails and the tokens become worthless.

## 3.2 Standardization

With many start-ups creating tokens to make initial coin offerings, building dapps and providing various services both on-chain and off-chain to use these tokens; the need for a standardized way to interact with said tokens arose rapidly. A standard for tokens allows wallet—holding a user’s private key—to easily let the user interact with both their ether and a wide collection of their token easily. It allows any smart contract—whether it is a wallet or a dapp—to effortlessly receive, hold and send tokens. Smart contracts are immutable which makes them notoriously hard to update. Typically, any update is done by replacing an existing smart contract with a new one at a different address with a copy of the data. Any off-chain infrastructure must then point to the address of this new contract. Updating a smart contract to handle a different way of interacting with a new and specific token would be an impossible task. Having a standard which defines an interface to interact with tokens allows dapps and wallets to instantly be compatible with any existing and future token which complies with the standard.

## 3.3 Ethereum Improvement Proposals And Ethereum Request For Comments

Blockchain projects in general, including Ethereum, are ecosystems which tend to be available as open-source software. Their projects are community oriented where anyone is invited to participate and contribute. To distribute source code and organize contributions the Ethereum Foundation relies on their Github organization account. One of the repositories they maintain is the Ethereum Improvement Proposals or EIPs. This repository, available at [github.com/ethereum/EIPs](https://github.com/ethereum/EIPs) “[...] describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards” [EIPs, homepage]. This includes the Ethereum Requests for Comments track which includes “Application-level standards and conventions, including contract standards such as token standards (ERC20), name registries (ERC137), URI schemes (ERC681), library/package formats (EIP190), and wallet formats (EIP85)” [EIPs]. This is the track where the current standard for tokens is defined and where any proposal for new token standards take place. New standards are submitted by opening a pull request—previously an issue—containing a description of the standard proposal and following the provided template. This template states: “Note that an EIP number will be assigned by an editor” [EIP-X]. In practice and historically the number associated to an EIP is the number of the initial issue or pull request which started the standard. This as a matter of fact applies to all the EIPs discussed in this paper.

## Chapter 4

# ERC20 Token Standard

The first—and so far only—standard for tokens on the Ethereum blockchain is ERC20. There have been many new token standards and extensions or improvements to ERC20 suggested over time. Not including ERC777—the standard detailed in this paper—such proposals include the following standards: the ERC223 token standard, the ERC827 Token Standard (ERC20 Extension), the ERC995 Token Standard, the ERC1003 Token Standard (ERC20 Extension), and changes to ERC20 such as: Token Standard Extension for Increasing & Decreasing Supply (ERC621), Provable Burn: ERC20 Extension (ERC661), Unlimited ERC20 token allowance (ERC717), Proposed ERC20 change: make 18 decimal places compulsory (ERC724), Reduce mandatority of Transfer events for void transfers (ERC732), Resolution on the EIP20 API Approve / TransferFrom multiple withdrawal attack (ERC738), Extending ERC20 with token locking capability (ERC1132).

### 4.1 The First Token Standard

The ERC20 standard was created on November 19th 2015 as listed on the EIPs website under the ERC track [see Foundation, 2018, ERC track]. A standard for tokens must define a specific interface and expected behaviors a token must have when interacted with. This allows wallets, dapps and services to easily interact with any token. It defines a simple interface which lets anyone transfer their tokens to other address, check a balance, the total supply of tokens and such. Specifically it defines nine functions a token must implement: `name`, `symbol`, `decimals`, `totalSupply`, `balanceOf`, `transfer`, `transferFrom`, `approve`, `allowance` as well as two events which must be fired in particular cases: `Transfer` and `Approval`.

The `name`, `symbol` are optional functions which fairly basic and easy to understand. They return the name and the symbol or abbreviation of the token. Considering the Aragon token as an example, the `name` function returns the string `Aragon Network Token` and the `symbol` functions returns `ANT`. Another somewhat harder to understand optional function is `decimals`. This function returns the number of decimals used by the token and thus define what transformation should be applied to any amount of tokens before being displayed to the user or communicated to the token contract. As previously explained, the balances and amounts of tokens handled by the token contracts are (256 bits) unsigned integers. Therefore the smallest fractional monetary unit is one. For some—or many—tokens, it makes more sense to allow smaller fractions. The `decimals` function return the number of decimals to apply to any amount passed to or returned

by the token contract. Most tokens simply follow Ether—which uses eighteen decimals—and use eighteen decimals as well. Another decimals value used is zero. A token with zero decimals can make sense when a token represent an entity which is not divisible—such as a physical entity. Altogether those functions are optional and purely cosmetic. The most important function being decimals as any misuse will show an incorrect representation of tokens and thus of value.

The `totalSupply` and `balanceOf` are also view methods. Simply put, they do not modify the state of the token contract, but only return data from it. This behavior is similar to what one can expect from getter functions in object oriented programming.

The `totalSupply` function returns the total number of tokens held by all the token holders. This number can either be constant or variable. A constant total supply implies the token contract is created with a limited supply of tokens with neither the ability to mint tokens nor the ability to burn. A variable total supply, on the other hand, signifies that a the token contract is capable of minting new tokens or burning them or both.

The `balanceOf` function takes an address as parameter and returns the number of tokens held by that address.

## 4.2 Transferring ERC20 Tokens

The `transfer` and `transferFrom` functions are used to move tokens across addresses. The `transfer` function takes two parameters, first the address of the recipient and secondly the number of tokens to transfer. When executed, the balance of the address which called the function is debited and the balance of the address specified as the first parameter is credited the number of token specified as the second parameter. Of course, before updating any balance some checks are performed to ensure the debtor as enough funds.

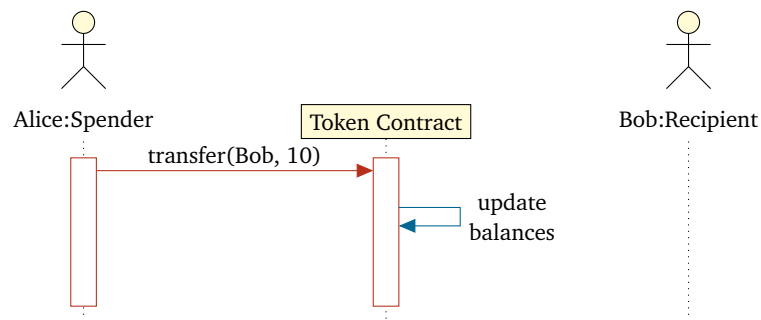


Figure 4.1. Standad ERC20 transfer between two regular accounts: Alice and Bob.

As seen on figure 4.1 when performing a transfer, the spender emits a transaction which calls the token contract and update the balances accordingly. The recipient is never involved in the transaction. The logic to update the balance is entirely done within the token contract, in the `transfer` function.

Examples of the implementation details to update the balances are shown in listings 4.1 and 4.2.



```

2  * @dev Transfer token for a specified address
3  * @param _to The address to transfer to.
4  * @param _value The amount to be transferred.
5  */
6  function transfer(address _to, uint256 _value) public returns (bool) {
7      require(_value <= balances[msg.sender]);
8      require(_to != address(0));
9
10     balances[msg.sender] = balances[msg.sender].sub(_value);
11     balances[_to] = balances[_to].add(_value);
12     emit Transfer(msg.sender, _to, _value);
13     return true;
14 }

```

Listing 4.1. OpenZeppelin's implementation of ERC20's transfer function.

The implementation of the transfer function in the listing 4.1 shows—on lines 7 and 8—the conditions checked before effectually performing the transfer and update of the balances—on lines 10 and 11. The solidity instruction `require` evaluates the condition it is passed as parameter. If it is true it will continue with the execution, otherwise it will call the REVERT EVM opcode which stops the execution of the transaction without consuming all of the gas and revert the state changes.

The first check ensure that the token holder—here referred as the sender—does not try to send a number of tokens higher than its balance. The variable `msg.sender` is a special value in Solidity which holds the address of the sender of the message for the current call. In other words, `msg.sender` is the address which called the transfer function.

The second checks ensure that the recipient—defined in the parameter `_to`—is not the zero address. The notation `address(0)` is a cast of the number literal zero to a 20 bits address. The zero address is a special address. Sending tokens to the zero address is assimilated to burning the tokens. Ideally the balance of the zero address should not be update in this case. This is not always the case, tokens such as Tronix are held by the zero address. A quick look at their implementation shown in listing 4.2 of the transfer methods shows there is no check to ensure the recipient is not the zero address. Note that the `validAddress` modifier only verifies the `msg.sender` or in other words, the spender, not the recipient.

```

1  modifier isRunning {
2      assert (!stopped);
3      _;
4  }
5
6  modifier validAddress {
7      assert(0x0 != msg.sender);
8      _;
9  }
10
11 // ...
12
13 function transfer(address _to, uint256 _value)
14     isRunning validAddress returns (bool success)

```

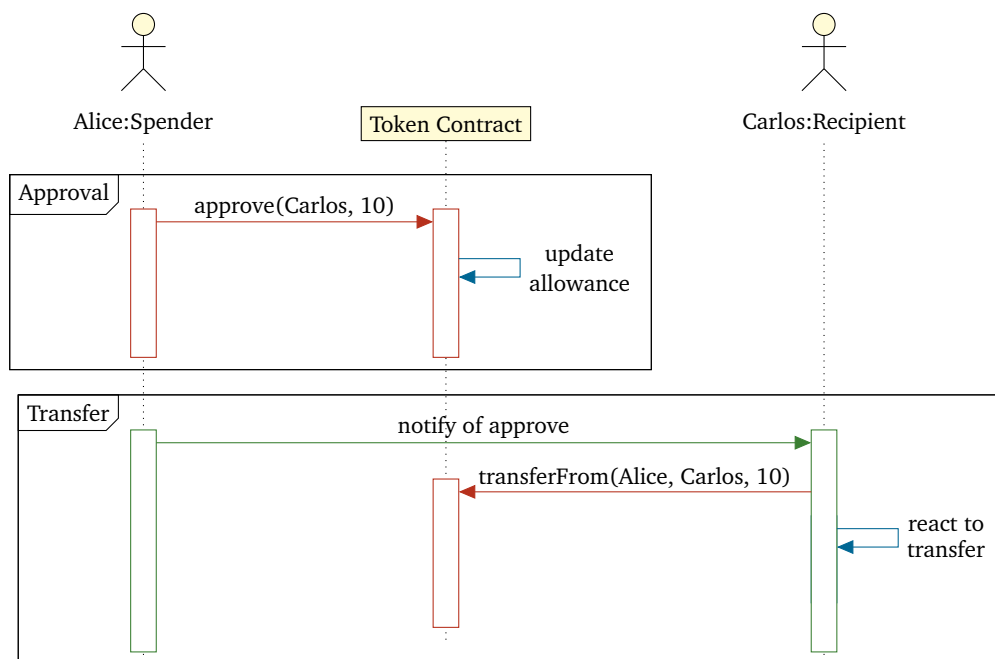
```

15 {
16     require(balanceOf[msg.sender] >= _value);
17     require(balanceOf[_to] + _value >= balanceOf[_to]);
18     balanceOf[msg.sender] -= _value;
19     balanceOf[_to] += _value;
20     Transfer(msg.sender, _to, _value);
21     return true;
22 }

```

Listing 4.2. Tronix transfer function.

The `transferFrom` function is the second function available to transfer tokens between addresses. Its use is depicted in figure 4.2. It takes three parameters the debtor address, the creditor address and the number of tokens to transfer.

Figure 4.2. Standard ERC20 `transferFrom` between a regular account Alice and a contract account Carlos.

The reason for the existence of this second function to transfer tokens is contracts. Contracts usually need to react when receiving tokens. When a normal `transfer` is called to send tokens to a contract, the receiving contract is never called and cannot react. Contracts are also not able to listen to events, making it impossible for a contract to react to a `Transfer` event. The `transferFrom` lets the token contract transfer the tokens from someone else to itself or others. At first glance this appears to be insecure as it lets anyone withdraw tokens from any address. This is where the `approve` and `allowance` functions come into play. The specification for the `transferFrom` function states that “[t]he function SHOULD throw unless the `_from` account has deliberately authorized the sender of the message via some mechanism” [Vogelsteller and Buterin, 2015]. The `approve` function is the standard mechanism to authorize a sender to call

`transferFrom`. Consider an ERC20 token, a regular user Alice and a contract Carlos. Alice wishes to send five tokens to Carlos to purchase a service offered by Carlos. If she uses the `transfer` function, the contract will never be made aware of the five tokens it received and will not activate the service for Alice. Instead, Alice can call `approve` to allow Carlos to transfer five of Alice's tokens. Anyone can then call `allowance` to check that Alice did in fact allow Carlos to transfer the five tokens from Alice's balance. Alice can then call a public function of Carlos or notify off-chain the maintainers of the Carlos contract such that they can call the function. This function of Carlos can call the `transferFrom` function of the token contract to receive the five tokens from Alice.

## 4.3 Strength And Weaknesses Of ERC20

Overall the ERC20 token standard was kept simple in its design. Hence the standard results in simple token contracts. This is one of the upside of the standard. Token contracts can be kept short and simple which makes them easy and cheap to audit. This is especially important as an insecure contract will lose its value extremely quickly and good smart contract auditors are expensive and have little availability.

At the other end of the spectrum however, this translates to a higher burden on the user, applications and wallets interacting with the tokens.

### 4.3.1 Locked Tokens

One of the largest issue is the distinction all token holders must make when transferring tokens regarding the type of recipient. There are no issues if the recipient is a regular account, `transfer` just works and calling `approve` with the correct amount and let the recipient call `transferFrom`. The user experience in this case is somewhat suboptimal as it requires off-chain communication, two transactions, and the recipient has to pay the gas for the second transaction. Nonetheless the intended goal is achieved and the transfer from the spender to the recipient is achieved.

The same cannot be said if the recipient is a contract account. When using `transfer` to send tokens to a contract. The spender initiates the transfer and only communicates with the token contract the recipient is never notified—as previously shown in figure 4.1. The result is that while the token balance of the receiving contract is increased, that contract may never be able to use and spend the tokens it received—this situation is commonly referred to as “locked tokens”. A simple proof is the Tronix contract whose `transfer` function was discussed before. A rapid look at the token balance of the Tronix contract—deployed at itself shows a balance of 5'504'504.3514 TRX as of August 8<sup>th</sup> 2018. With an exchange rate of \$0.0272, this represents a value of just a little under 150,000 US dollars. By analyzing the code, one can see there are no functions which would allow anyone to spend those tokens. There are of course many more similar examples of such scenarios where people sent tokens either to the token contract or to some other contract by mistake and the amounts add up quickly

### 4.3.2 Approval Race Condition

By abusing the Application Binary Interface (ABI) of ERC20, an attacker can trick its victim into approving more tokens for the attacker to spend than intended. This attack was revealed on

November 29<sup>th</sup> 2018. Essentially, it takes advantage of two of ERC20's functions: `approve` and `transferFrom`. Because this is an issue with the logic in the standard, all ERC20-compliant implementations are affected. This attack works as follow, as described in the original paper [Vladimirov and Khovratovich, 2016]:

1. Alice allows Bob to transfer  $N$  of Alice's tokens ( $N > 0$ ) by calling the `approve` function on the token smart contract, passing Bob's address and  $N$  as function arguments.
2. After some time, Alice decides to change from  $N$  to  $M$  ( $M > 0$ ) the number of Alice's tokens Bob is allowed to transfer, so she calls the `approve` function again, this time passing Bob's address and  $M$  as function arguments
3. Bob notices Alice's second transaction before it was mined and quickly sends another transaction that calls `transferFrom` method to transfer  $N$  Alice's tokens somewhere.
4. If Bob's transaction is executed before Alice's transaction, then Bob will successfully transfer  $N$  of Alice's tokens and will gain an ability to transfer another  $M$  tokens.
5. Before Alice noticed that something went wrong, Bob calls the `transferFrom` function again, this time to transfer  $M$  of Alice's tokens.

So, Alice's attempt to change Bob's allowance from  $N$  to  $M$  ( $N > 0$  and  $M > 0$ ) made it possible for Bob to transfer  $N + M$  of Alice's tokens, while Alice never wanted to allow so many of her tokens to be transferred by Bob.

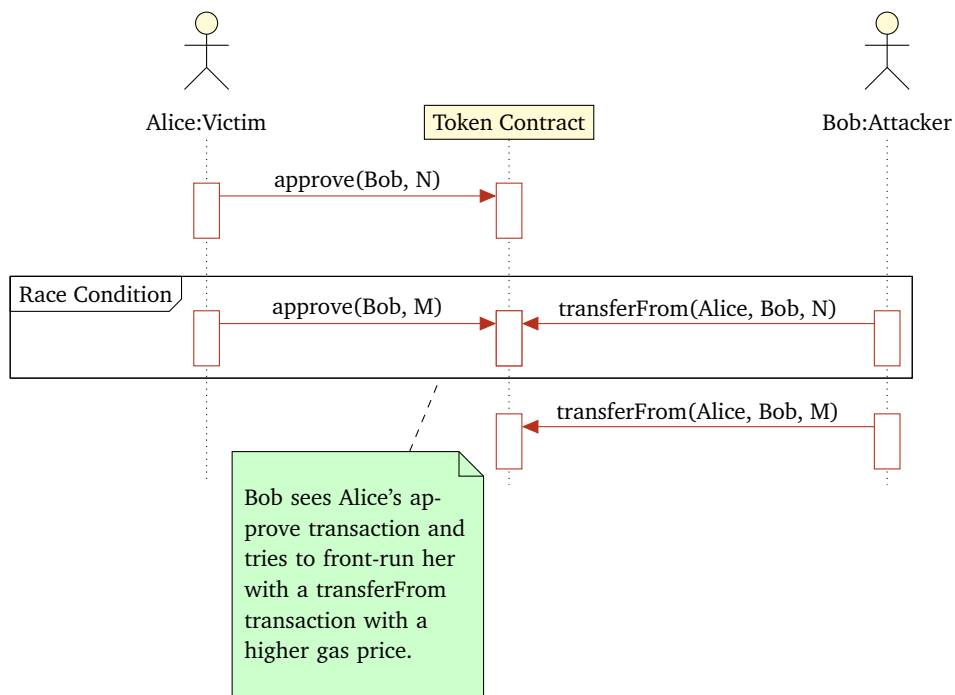


Figure 4.3. Sequence of calls for the approve/transferFrom attack.

### 4.3.3 Absence Of burning

The ERC20 standard defines the behavior for minting new tokens. Namely, “[a] token contract which creates new tokens SHOULD trigger a Transfer event with the `_from` address set to `0x0` when tokens are created” [Vogelsteller and Buterin, 2015]. Unfortunately the standard does not go further, nothing is specified regarding the balance of `0x0` or the `totalSupply` for example.

[illegible]

Out of all the questions above, most tokens tend to emit Transfer events with the `to` address set to `0x0`. The remaining questions are solved differently for various tokens. Multiple mutually exclusive solution may be acceptable. However in some cases, some solutions may be preferable over others. As an example, most of the smart contracts are written in Solidity where an uninitialized variable of type `address` has a value of zero (`0x0`). On the off-chance that the value passed as the `to` parameter to a transfer call is uninitialized, then if the token contract allows burning via transfer, this will result in an unintentional burn of the tokens. In such a scenario, it may be preferable to revert the transaction instead and expose a specific function to burn tokens instead.

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

The ERC777

Explain ERC777 in thorough details:

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





## Chapter 6

# ERC820, Pseudo-introspection Registry contract



## Chapter 7

# Competing Token Standards

7.1 ERC227

7.2 ERC827

7.3 ERC995



## Chapter 8

# The State Of Tooling

8.1 Compilation

8.2 Testing and Coverage

8.3 Documentation

8.4 Missing Tools



## Chapter 9

# 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 10

# Conclusion

I'll do this one at the end



# Glossary

## **ABI**

Application Binary Interface. 13, 29

## **EVM**

Ethereum Virtual Machine. 5, 29

## **LIFO**

Last-In-First-Out. 5, 29



# Bibliography

Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform, 2013. URL <https://github.com/ethereum/wiki/wiki/White-Paper>.

Ethereum Foundation. Eip x, the suggested template for new eips, 2015. URL <https://github.com/ethereum/EIPs/blob/master/eip-X.md>.

Ethereum Foundation. Ethereum improvement proposals, March 2018. URL <https://eips.ethereum.org/>.

Mikhail Vladimirov and Dmitry Khovratovich. Erc20 api: An attack vector on approve/-transferfrom methods, November 2016. URL [https://docs.google.com/document/d/1YLPtQxZu1UAv09cZ102RPXBbT0mooh4DYKjA\\_jp-RLM](https://docs.google.com/document/d/1YLPtQxZu1UAv09cZ102RPXBbT0mooh4DYKjA_jp-RLM).

Fabian Vogelsteller and Vitalik Buterin. Erc-20 token standard, November 2015. URL <https://eips.ethereum.org/EIPS/eip-20>.