Resolving the Multiple Withdrawal Attack on ERC20 Tokens

Reza Rahimian, Shayan Eskandari, Jeremy Clark
Concordia University

Abstract—Custom tokens are an integral component of decentralized applications (dapps) deployed on Ethereum and other blockchain platforms. For Ethereum, the ERC20 standard is a widely used token interface and is interoperable with many existing dapps, user interface platforms, and popular web applications (e.g., exchange services). An ERC20 security issue, known as the *multiple withdrawal attack*, was raised on GitHub and has been open since November 2016.

The issue concerns ERC20’s defined method `approve()` which was envisioned as a way for token holders to give permission for other users and dapps to withdraw a capped number of tokens. The security issue arises when a token holder wants to adjust the amount of approved tokens from $N$ to $M$ (this could be an increase or decrease). If malicious, a user or dapp who is approved for $N$ tokens can front-run the adjustment transaction to first withdraw $N$ tokens, then allow the approval to be confirmed, and withdraw an additional $M$ tokens. In this paper, we evaluate 10 proposed mitigations for this issues and find that no solution is fully satisfactory. We then propose 2 new solutions that mitigate the attack, one of which fully fulfills constraints of the standard, and the second one shows a general limitation in addressing this issue from ERC20’s approve method.

Index Terms—Ethereum; ERC20 tokens; Blockchain;

1. Introduction

Ethereum is a public blockchain proposed in 2013, deployed in 2015 [1], and has the second largest market cap at the time of writing [2]. It has a large development community which track enhancements and propose new ideas [3]. Ethereum enables decentralized applications (dapps) to be deployed and executed. Dapps can accept and transfer Ethereum’s built-in currency (ETH) or might issue their own custom currency-like tokens for specific purposes.

Tokens might be currencies with different properties than ETH. They may be required for access to a dapp’s functionality or they might represent ownership of some off-blockchain asset. It is beneficial to have interoperable tokens with other dapps and off-blockchain webapps, such as exchange services that allow tokens to be traded.

Toward this goal, the Ethereum project accepted a proposed standard (called ERC20 [4]) for a set of methods that ERC20-compliant tokens must implement. In terms of object oriented programming, ERC20 is an interface that defines abstract methods (name, parameters, return types) and provides guidelines on how the methods should be implemented, however it does not provide an actual concrete implementation (see Figure 1).

```solidity
contract ERC20Interface {
    function totalSupply() public view returns (uint256);
    function balanceOf(address _tokenOwner) public view returns (uint256);
    function transfer(address _to, uint256 _value) public returns (bool);
    function transferFrom(address _from, address _to, uint256 _value) public returns (bool);
    function allowance(address _owner, address _spender) public view returns (uint256);
}

function approve(address _spender, uint256 _value) public returns (bool) {
    // Approve tokens for _spender to spend up to _value
    // The method does not alter the actual number of tokens
    // that defers the spender's address
    // public view returns (uint256);
    // The transaction must be confirmed to allow the
    // allowance to be consumed
    // public view returns (uint256 _tokens);
    // The transaction must be confirmed to allow the
    // allowance to be consumed
    public returns (bool success);
    // The transaction must be confirmed to allow the
    // allowance to be consumed
    public returns (uint256 _tokens);
    // The transaction must be confirmed to allow the
    // allowance to be consumed
    return true;
}
```

Figure 1. The ERC20 standard defines 6 methods and 2 events that must be implemented. Using `approve` and `transferFrom` in the existence of a race condition may lead to a "multiple withdrawal attack". Note that `transferFrom` augments the more basic `approve` method.

Since the introduction of ERC20 in November 2015, several vulnerabilities have been discovered. In November 2016, a security issue called "Multiple Withdrawal Attack" was opened on GitHub [3], [4]. The attack originates from two methods in the ERC20 standard for approving and transferring tokens. The use of these functions in an adverse environment (e.g., front-running [4]) could result in more tokens being spent than what was intended. This issue is still open and several solutions have been made to mitigate it. The authors of the ERC20 standard [2] reference two sample implementations: OpenZeppelin [6] and ConsenSys [7]. OpenZeppelin mitigates the attack by introducing two additional methods to increase or decrease approved tokens (see Section 3.3), and the ConsenSys implementation does not attempt to resolve the attack. Additional implementations have a variety of different trade-offs in mitigating the issue (see Section 3).

Contributions. In this paper, we evaluate 10 proposed mitigations for the "multiple withdrawal attack". We develop a set of criteria that encompass backwards compatibility, interoperability, adherence to the ERC20 standard, and attack mitigation. The summary is provided in Figure 2. Since no mitigation is fully satisfactory, we develop two additional solutions based on the *Compare and Set (CAS)* pattern [8]. We study in detail possible implementations of ERC20's `approve` and `transferFrom` methods. We argue that a CAS-based approach can never adequately deploy a secure `approve` method while adhering to the ERC20 standard. We then propose a secure implementation of the `transferFrom` method that mitigates the attack and fully satisfies the ERC20 standard.

1. [2019-02-11] https://coinmarketcap.com/currencies/ethereum/
2. [2019-02-11] https://www.coindesk.com/data
3. A widely used lock-free synchronization strategy that allows comparing and setting values atomically.
2. Preliminaries

2.1. How the multiple withdrawal attack works

According to the ERC20 API definition, the approve function allows a spender (e.g., user, wallet or other smart contracts) to withdraw up to an allowed amount of tokens from token pool of the approver. If this function is called again, it overwrites the current allowance with the new input value. On the other hand, the transferFrom function allows the spender to actually transfer tokens from the approver to anyone they choose (importantly: not necessarily themselves). The contract updates balance of transaction parties accordingly.

An adversary can exploit the gap between the confirmation of the approve and transferFrom functions since the approve method replaces the current spender allowance with the new amount, regardless of whether the spender already transferred any tokens or not. This functionality of the approve method is shaped by the language of the standard and cannot be changed. Furthermore, while variables change and events are logged, this information is ambiguous and cannot fully distinguish between possible traces. Consider the following illustration:

1) Alice allows Bob to transfer N tokens on her behalf by broadcasting approve(_Bob, N).
2) Later, Alice decides to change Bob’s approval from N to M by calling approve(_Bob, M).
3) Bob notices Alice’s second transaction after its broadcast to the Ethereum network but before adding to a block.
4) Bob front-runs (using an asymmetric insertion attack [5]) the original transaction with a call to transferFrom(_Alice, _Bob, N). If a miner is incentivized (e.g., by Bob offering high gas) to add this transaction before Alice’s, it will transfer N of Alice’s tokens to Bob.
5) Alice’s transaction will then be executed which changes Bob’s approval to M.
6) Bob can call transferFrom method again and transfer M additional tokens.

4. We use the term method and function interchangeably.
In summary, in attempting to change Bob’s allowance from N to M, Alice makes it possible for Bob to transfer N+M of her tokens. We operate on the assumption that a secure implementation would prevent Bob from withdrawing Alice’s tokens multiple times when the allowance changes from N to M (see Figure 3).

2.2. Why mitigation is important

ERC20 tokens are an important component of Ethereum’s supplementary financial system that have many financial (as well as non-financial) uses and could hold considerable value (potentially exceeding the value of Ether itself). There has been more than 64,000 functional ERC20 tokens as of early 2019 [2] that might be vulnerable to this attack. Furthermore, ERC20 tokens that have already been issued cannot easily migrate to a new secure implementation and should these tokens appreciate in value in the future. Resolving the attack also serves as basis for other extended standards, such as ERC-777 [10] to be backward compatible with ERC20 interface [11]. Finally, firms that hold ERC20 tokens require assurance of their security, particularly in the case that they require their financial statements to be audited—an issue like this could lead to further hesitation by auditors.

2.3. Where to prevent this attack

There are a few logical places to address this attack. Ideally the token author (instead of the token holders) would mitigate the attack within the ERC20 smart contract. Since two methods are involved in the attack, it could be addressed within the approve and/or transferFrom method. By contrast, token owners have no control over the implementation of the contract and are relegated to mitigate the attack by carefully monitoring the contract around the time allowance changes are made.

Prevention by token holder. Consider Alice, a token holder using a web app (e.g., a user interface deployed with web3) to adjust Bob’s allowance. If this user interface (UI) is written to the ERC20 standard, Alice will only have approve available to her. The ERC20 authors [2] advise Alice against directly changing Bob’s allowance from N to M. Instead, she should set the approval to 0 and then it to M (N→0→M). Presumably, Alice will not do the second approval (setting it from 0 to M) if she sees that Bob withdraws N tokens before her N to 0 adjustment is confirmed.

How will Alice know whether Bob withdraws first? The answer depends on how deeply her webapp can monitor the blockchain. One option is to monitor the variable that records Bob’s allowance (technically an on-blockchain helper dapp could also do this). However if she sees Bob’s allowance at 0 after initiating the first adjustment, it does not tell her that Bob did not withdraw N tokens—both methods result in Bob having an allowance of 0 so either (or both) could have been executed.

Next, she might rely on events passed from the contract to her web3 app. Transfer events as specified in ERC20 will log the transfer parameters (i.e., address _from, address _to, uint256 _tokens). Alice’s webapp could filter the events and only display transfers matching her address in the _from field. The displayed transfers will include any transfer Bob makes, however Bob can provide any address in _to, not just his own, and the event does not report who authorized the transaction (i.e., msg.sender). If Alice has many authorizations, she cannot determine if a transfer was initiated by Bob or someone else she has authorized. Therefore Alice cannot always unambiguously rely on events to determine Bob did not transfer funds (See Section 3.1 for more details). If Alice’s web app is beyond web3 and runs a full node maintaining blockchain state, it could correctly detect and attribute all transfers initiated by Bob. But this rather time-consuming and thus probably not efficient.

The takeaway from all these options is that prevention by token owners has some undesirable properties: (1) it splits adjustments into two transactions, (2) because the first transaction needs to be confirmed before the second is initiated, it takes time to complete, and (3) to precisely mitigate this attack, a heavyweight web app is needed to inspect deeper than variable state changes and events. For these reasons, we concentrate on mitigating the attack in the contract itself. If mitigation at the contract level works, allowances can be adjusted with a single function call from any existing lightweight ERC20 user interface, and no additional monitoring of the contract is necessary.

Prevention by token author in approve. The next logical place to tackle multiple withdrawal is in the implementation of the approve method. In particular, an approve implementation might be engineered to fail under the conditions of multiple withdrawal, to adjust the approval amount, treat adjustments as relative offsets from the current amount, or other techniques. As we review the 10 solutions, we will see different proposals along these lines, as well as our own proposal in Section 4.1. For now, we emphasize that adherence to the standard is a core challenge as it unequivocally states that: “If this function is called again, it overwrites the current allowance with _value” [2]. So, any adjustment violates the standard.

5. Even if Bob is listed in _to, another authorized spender might have transferred tokens to Bob to make Alice believe Bob attempted a multiple withdrawal when he actually did not.
6. By replaying transactions on an EVM
3. Evaluating Proposed Solutions

In this section, we evaluate 10 solutions that have been proposed by Ethereum community\(^7\) to address the multiple withdrawal attack. We examine each solution in detail and evaluate them against the criteria established in section 2.4. The summary is also presented in Figure 3.

3.1. Enforcement by User Interface (UI)

The first solution is enforcement at the user interface level. We discussed this previously in section 2.3 but we reiterate the main points here again. The exact recommendation from the ERC20 standard is shown in Figure 4 and is essentially to set an allowance to zero before any non-zero values. Presumably, it will also enforce that the new approval is not allowed if proceeded by a token transfer by the approved spender. We consider the UI to be a lightweight web app that can reference a contract’s state variables and emit events but does not maintain a full copy of the blockchain. Consider (again) the most basic attack sequence:

1) Alice allows Bob to transfer N of her tokens.
2) Alice’s client broadcasts an allowance of 0.
3) Bob broadcasts a competing transaction to transfer N of Alice’s tokens.
4) Bob’s transaction front-runs Alice’s, is confirmed, and sets Bobs allowance to 0 (from N).
5) Alice’s transaction is confirmed and sets Bobs allowance to 0 (from 0).
6) Alice’s client broadcasts an allowance of M.
7) Alice’s second transaction is confirmed and sets Bob’s allowance to M.
8) Bob transfers M of Alice’s tokens for a total of N+M tokens.

The key mitigation to this attack is for Alice’s client to pause at step 6 and determine if a transaction sequence like 3&4 has occurred or not. This cannot be determined by monitoring the integer that records Bob’s allowance because it will be 0 regardless of whether steps 3&4 occurred or not.

It also cannot always be determined by monitoring the events emitted from the contract. Step 4 will log a transfer from Alice’s address to Bob’s address of N tokens. If no event is emitted, Alice can know for certain no transfer was made. However if an event is emitted, Alice must decide it was a transfer initiated by Bob or a transfer by someone else she has authorized. If she has not authorized anyone else, she can know for certain it was Bob. However if she has a busy account with multiple authorized spenders of her tokens, the event is not verbose enough to determine what happened. Importantly, it does not record who (msg.sender initiated the transfer, only who received the tokens, and these are not necessarily the same entity. Bob can send Alice’s tokens to his accomplice Eve, or some other authorized spender can send Alice’s tokens to Bob (which looks like Bob is attacking when he is not). Since a UI is automated and does not use human discretion, it cannot decide circumstantially whether something looks like an attack or not—it must either specify exact rules, which it cannot do here because of the ambiguity of the events, or it can ask for Alice’s human input which introduces usability issues. In conclusion, it is better for enforcement to happen at the contract level as implemented by the most of the solutions.

3.2. MiniMeToken

MiniMeToken [12] enforces the recommendation that allowances are first set to zero before setting to a non-zero value. The enforcement is done within the ERC20 implementation by adding require(_amount == 0) || (allowed[msg.sender][_spender] == 0)) to the approve method. (_amount == 0) allows approvals to be set to 0, and the second condition requires the allowance of _spender to be 0 before it can be set to a non-zero value. This solution fails to prevent Bob from transferring N+M tokens, as the contract will be unable...
to determine whether N tokens have been already drained by Bob or not. Recall the attack sequence specified in section 3.1. In step 5, Alice finds Bob’s allowance is set to zero. However, she cannot distinguish whether it was because of her transaction or token transfer by Bob. Furthermore, contracts cannot read their own logs to filter out Transfer events.

3.3. MonolithDAO

MonolithDAO Token [13] (and its extension in OpenZeppelin [6]) implement two additional functions for approval increases and decreases: increaseApproval and decreaseApproval. Both take two parameters: the address of the approved spender and the amount to be added/subtracted from the spender’s current approval. Additionally, the approve method has additional logic to enforce that owners set the allowance to zero before non-zero values (see Figure 5). Forcing a set to zero is effectively enforce setting spender's allowance in two steps: first to zero and then to any non-zero value (e.g., N→0→M).

![Figure 5. Functionality of the approve method in MiniMeToken and MonolithDAO tokens, which are implemented slightly differently but effectively enforce setting spender’s allowance in two steps: first to zero and then to any non-zero value (e.g., N→0→M).](Image)

8. Both approve and transferFrom can set Bob’s allowance to zero. In the first case, if Alice’s transaction executes before Bob’s and in the second one due to token transfer by Bob.

9. Alice can use the default approve method since Bobs allowance was initially 0.

Figure 6. In “Detecting token transfers”, the approve method needs to be modified by adding a line of code like allowed[msg.sender][_spender].used = false; between lines 16 and 17 to unlock spender flag for the next legitimate change. However, this change makes attack mitigation ineffective.

3.4. Detecting token transfers

The next approach [14] maintains a small state machine to enforce prevent approvals preceded by transfers. We revisit and elaborate on this approach in our own solution in Section 4.1. In this proposal, the implementation of approve is augmented with a flag (one flag for each pair of owners and approved spenders) that can be set in transferFrom function. transferFrom sets the flag to true after any token transfer and the approve method requires the flag to be false before allowing new approvals. This approach requires a new data structure, can prevent front-running, but also has a deadlock scenario. Consider the following scenario:

1) Alice allows Bob to transfer N tokens by broadcasting approve(_Bob, N). This succeeds because Bobs allowance was initially 0 and his corresponding flag=false (line 15 in Figure 5).
2) Bob legitimately withdraws N tokens by calling transferFrom(_Alice, _Bob, N).
3) Alice decides to increase Bob’s allowance to M by broadcasting approve(_Bob, 0).
4) Since Bob’s transaction is confirmed first, transferFrom turns his flag to true.
5) Alice’s transaction is confirmed, passes the check because input value is 0 (line 15), and Bobs allowance is set to 0 while his flag remains true. Critically, the approve method does not flip the spender’s flag.
6) Alice wants to change Bobs allowance to M and broadcasts approve(_Bob, M).
7) Since Bob already transferred N tokens (or it could be just 1 token) and his flag=true, the transaction fails.
8) Remark: Bobs allowance is 0 and it cannot not change, so he is locked out of further approvals.

Although this approach mitigates the attack, it prevents any further legitimate approvals. As discussed, in case of any legitimate token transfer by Bob, Alice would not be able to change his approval. Because Bob’s flag is set to true and line 15 in Figure 6 does not allow changing the allowance (an exception is thrown). A potential bypass is to set the allowance to 0 and then to M. However this transaction sequence never flips the flag to false safer functions will not be used by ERC20-compliant web apps and smart contracts that are already deployed. Such deployments will continue to use approve method which suffers the same issue as MiniMeToken: set to zero does not always mitigate the attack.
3.5. Keeping track of remaining tokens

This approach [15] is inspired by the previous solution of detecting token transfers and introduces new state in the contract. It keeps track of the remaining tokens, and an ERC20-compliant approve method uses these variables to set allowances accordingly (see Figure 7).

At a first glance, it seems to be a promising solution by more effectively enforcing approvals to zero before non-zero values. However, the highlighted code in approve method (see Figure 7) resembles the situation that is explained in [3.1]. In case of front-running, both initial and residual variables will be zero and it would not be possible for Alice to distinguish if any token transfer have occurred due to her allowance change or due to Bob transferring a token. To illustrate this, considering the following transaction sequence (For formatting reasons, we abbreviate codes like allowances[Alice][Bob].initial as AB.initial):

1) Alice changes Bob's allowance from N to 0.
2) Bob transfers N tokens before the allowance change and his used flag turns to true.
3) Alice's transaction is successful since input value is 0. The second condition is not evaluated although used flag is true.
4) Alice's transaction turns used flag to false and sets Bob's allowance to 0.
5) Now Alice wants to set Bob's allowance from 0 to M, his flag is false and allowance is 0.
6) Remark: Alice cannot distinguish whether Bob moved any token or not. Setting a new allowance will allow Bob to transfer more tokens.

In fact, resetting the flag in approve method will not fix the issue and makes attack mitigation ineffective. In short, this approach can not satisfy both legitimate and non-legitimate scenarios. Nevertheless, it is a step forward by introducing the need for a new state to track transferred tokens if a solution is to be found.

Figure 7. Keeping track of remaining tokens by introducing a new data structure.

3.6. Overloading Approve method

As advised by [16], a secure approve method could take one additional parameter: the expected allowance of the spender when the adjustment to the approval is made. Under this proposal, the adjustment succeeds only if the passed expected allowance matches the spender’s actual allowance, and fails otherwise. Consider a multiple withdrawal attack where Bob is approved for N of Alice’s tokens, Alice adjusts his approval from N to M tokens, and Bob front-runs the approval with a transfer of N tokens. Alice’s approval will specify N as the current expected
3.7. Alternate approval function

Another suggestion [17] is to move the security check to a new function called `safeApprove` that compares the current and new allowance values (like the overloaded `approve` method in Section 3.6). The adjustment is only allowed if the allowance has not been changed by the time the function is executed. In this case, Alice uses the standard `approve` function to set Bob’s allowance to 0 and for new approvals, she has to use `safeApprove` function. As above, `safeApprove` takes the current expected approval amount as input parameter and calls `approve` method if previous allowance is equal to the current expected approval. Although this approach mitigates the attack by using the CAS pattern [8], it is not interoperable with ERC20-compliant web apps and smart contracts that will be unaware of `safeApprove`.

3.8. Minimum viable token

Rather than adding new methods to ERC20, methods can be also taken away. We can reduce the ERC20 standard to a set of core functionalities and implement only the essential methods. The attack can be side-stepped if methods like `approve` and `transferFrom` are simply not implemented (recall that `transferFrom` is in addition to the more commonly used `transfer`) or are implemented to always throw an exception and revert. Golem Network Token (GNT) [1] is one of these examples since it does not implement the `approve`, `allowance` and `transferFrom` functions. According to the ERC20 specification [2], these methods are not OPTIONAL and must be implemented. Moreover, ignoring them can cause failed function calls from smart contracts or web apps that expect these methods to work as specified. Therefore, we categorize this approach as successfully mitigating the attack but not offering interoperability.

3.9. New token standards

Minimum viable tokens could alternatively be considered a new non-ERC20 token. In fact, there are many alternatives that extend or modify ERC20 for a variety of purposes, mostly around functionality but some address multiple withdrawals. We summarize the main proposals in Table 1. Despite the enhancements of these new token standards for future deployments, ERC20 is ingrained in the community and industry with 168,092 deployed tokens [11] and many interoperable developer tools and libraries, and web platforms built on trading these tokens. Ideally, and the goal of this paper, a backward compatible solution could be found that does not change the ERC20 API or require token migration to a new standard (which is not necessarily possible to do at the contract level). Like minimum viable tokens, we categorize these approaches potentially mitigating the attack (depending on which standard — see Table 1) but not offering interoperability.

3.10. Approving trusted parties

A final solution is to limit token transfer approvals to trusted entities. Such a solution is discretionary—it cannot be automated within a contract—so it adds additional burden for the user. At first glance, it seem that Alice would never authorize Bob to spend her tokens if she does not trust Bob. However approvals are constrained to specific amounts specifically to enable some less trustworthy interactions. The “multiple withdrawal attack” is damaging because Bob can circumvent the constraints. If Bob is another smart contract, instead of a user, then Alice could confirm it does not have the logic to conduct a multiple withdrawal attack, cannot be updated (e.g., does not delegate function calls to code at other addresses), and thus it can be trusted with insecure ERC20 tokens. This is a sensible approach but it is quite limited to specific approval scenarios.

4. New mitigations

By this point, we have discussed 10 solutions to the multiple withdrawal attack and we evaluated them in terms of compatibility with the standard and attack mitigation (recall the summary in Figure 2). Since none of them precisely satisfy the constraints of ERC20 standard, we now propose two new solutions to mitigate the attack.

4.1. Proposal 1: Securing approve method

By implementing the CAS pattern [8] in the approve method, we set up a small state machine so that new allowances can be set atomically after a comparison with transferred tokens. This tracking requires adding a
A description of non-compliance with ERC20

| Token Standard | A description of non-compliance with ERC20 |
|----------------|-------------------------------------------|
| ERC 223 [13]   | It does not implement ERC20 approve and transferFrom methods by assuming that they are potentially insecure and inefficient. |
| ERC 667 [19]   | It solves the problem of the transfer function in ERC223 (i.e. the need to implement onTokenTransfer routing in the receiving contract). It mitigates the attack using the same code as ERC223 with a supplementary function. |
| ERC 721 [20]   | Unlike ERC20 tokens that share the same characteristics, ERC721 tokens are non-fungible tokens (NFT) where each token is unique and not interchangeable. In addition to this functional difference, ERC721 does not implement transferFrom method of ERC20 standard and introduces a safe transfer function called safeTransferFrom. |
| ERC 777 [10]   | It does not implement transfer or transferFrom methods and replaces them with safe send and operatorSend methods. Moreover, it considers costly approve/transferFrom paradigm to be replaced by tokensReceived function. Therefore, ERC777 would not be backward compatible by this replacement. A token might implement both ERC20 and ERC777 but the ERC20 methods would require attack mitigation. |
| ERC 827 [21]   | It uses OpenZeppelin’s ERC20 implementation and defines three new functions to allow users for transferring data in addition to value in ERC20 transactions. This feature enables ERC20 tokens to have the same functionality as Ether (transferring data and value). In fact, it extends functionality of ERC20 tokens and not addressing the attack. |
| ERC 1155 [22]  | It is improved version of ERC721 by allowing each Token ID to represent a new configurable token type, which may have its own metadata, supply and other attributes. ERC1155 aimed to remove the need to “approve” individual token contracts separately. Therefore, it does not implement any code to address this vulnerability. |
| ERC 1377 [23]  | It implements approve method with three parameters in addition to the ERC20 default approve with two inputs. Additionally, it uses OpenZeppelin approach for increasing and decreasing approvals. We would consider it as mix of MiniToken and OpenZeppelin proposals that we discussed before. |

### Table 1. Evaluation of standard’s adherence to ERC20 and mitigation of the multiple withdrawal attack.

| Token Standard | A description of non-compliance with ERC20 |
|----------------|-------------------------------------------|
| ERC 223 [13]   | It does not implement ERC20 approve and transferFrom methods by assuming that they are potentially insecure and inefficient. |
| ERC 667 [19]   | It solves the problem of the transfer function in ERC223 (i.e. the need to implement onTokenTransfer routing in the receiving contract). It mitigates the attack using the same code as ERC223 with a supplementary function. |
| ERC 721 [20]   | Unlike ERC20 tokens that share the same characteristics, ERC721 tokens are non-fungible tokens (NFT) where each token is unique and not interchangeable. In addition to this functional difference, ERC721 does not implement transferFrom method of ERC20 standard and introduces a safe transfer function called safeTransferFrom. |
| ERC 777 [10]   | It does not implement transfer or transferFrom methods and replaces them with safe send and operatorSend methods. Moreover, it considers costly approve/transferFrom paradigm to be replaced by tokensReceived function. Therefore, ERC777 would not be backward compatible by this replacement. A token might implement both ERC20 and ERC777 but the ERC20 methods would require attack mitigation. |
| ERC 827 [21]   | It uses OpenZeppelin’s ERC20 implementation and defines three new functions to allow users for transferring data in addition to value in ERC20 transactions. This feature enables ERC20 tokens to have the same functionality as Ether (transferring data and value). In fact, it extends functionality of ERC20 tokens and not addressing the attack. |
| ERC 1155 [22]  | It is improved version of ERC721 by allowing each Token ID to represent a new configurable token type, which may have its own metadata, supply and other attributes. ERC1155 aimed to remove the need to “approve” individual token contracts separately. Therefore, it does not implement any code to address this vulnerability. |
| ERC 1377 [23]  | It implements approve method with three parameters in addition to the ERC20 default approve with two inputs. Additionally, it uses OpenZeppelin approach for increasing and decreasing approvals. We would consider it as mix of MiniToken and OpenZeppelin proposals that we discussed before. |

### Figure 10. Added code block to approve function to prevent the attack by comparing and setting new allowance atomically.

```solidity
function approve(address _spender, uint256 _tokens) public returns (bool success) {
    requires(msg.sender == msg.sender);
    uint256 initialAllowed = allowed[msg.sender][_spender];
    uint256 transferred = transferred[msg.sender][_spender];
    // Approve new tokens
    // initialAllowed + _tokens
    if (_tokens > _tokens)
        return false;
    allowed[msg.sender][_spender] = initialAllowed + _tokens;
    transferred[msg.sender][_spender] = transferred[msg.sender][_spender] + _tokens;
    return true;
}
```

**Scenario A.** Alice approves Bob for spending 100 tokens and then decides to increase it to 120 tokens.

1. Alice approves Bob for transferring 100 tokens.
2. After a while, Alice decides to increase Bob’s allowance from 100 to 120 tokens.
3. Bob noticed Alice’s new transaction and transfers 100 tokens by front-running.
4. Bobs allowance is 0 and transferred=100.
5. Alcles transaction is mined and checks initial allowance (100) with new allowance (120).
6. As it is increasing, the new allowance (120) will be subtracted from the transferred tokens (100).
7. 20 tokens will be set as Bobs allowance.
8. Bob would be able to transfer 20 more tokens (120 in total as Alice wanted).

### Scenario B.** Alice approves Bob for spending 100 tokens and then decides to decrease it to 10 tokens.

1. Alice approves Bob for transferring 100 tokens.
2. After a while, Alice decides to reduce Bob’s allowance from 100 to 10 tokens.
3. Bob noticed Alice’s new transaction and transfers 100 tokens by front-running.
4. Bobs allowance is 0 and transferred=100 (set by transferFrom function).
5. Alcles transaction is mined and checks initial allowance (100) with new allowance (10).
6. As it is reducing, transferred tokens (100) is compared with new allowance (10).
7. Since Bob already transferred more tokens, his allowance will be set to 0.
8. Bob is not able to move more than initial 100 approved tokens.
Table 1. Comparison of gas consumption between standard implementation of ERC20 token (TKNv1) and secured version of it (TKNv2).

| Operation                  | Consumed Gas by the token |
|----------------------------|---------------------------|
|                            | TKNv1 | TKNv2 | Difference |
| Creating smart contract    | 1095561 | 1363450 | 25 %       |
| Calling Approve function   | 45289  | 46840  | 4 %         |
| Calling transferFrom function | 44019  | 64705  | 47 %        |

**Performance.** In order to evaluate functionality of the new approve and transferFrom functions, we have implemented a standard ERC20 token (TKNv1) along side the proposed ERC20 token (TKNv2) on the Rinkeby test network. Our testing for different input values shows that TKNv2 can address “multiple withdrawal attack” by making front-running gains ineffective. Moreover, we compared these two tokens in term of gas consumption. TKNv2.approve function uses almost the same amount of gas as TKNv1.approve, however, gas consumption of TKNv2.transferFrom is around 47% more than TKNv1.transferFrom (see Figure [11]). This difference in TKNv2 is because of maintaining a new mapping variable for tracking transferred tokens. In term of compatibility, both are equivalent interoperable with standard wallets (e.g., MetaMask and MEV) and have not raised any transfer issues.

**Discussion.** In summary, we can use the CAS pattern to implement a secure approve method that can mitigate the attack effectively. However, it violates one of the ERC20 specifications that says: “If approve function is called again, it overwrites the current allowance with _value_” (item 2 in Section 2.4). Our solution does not comply with this as the resulting allowance can be different than what is passed by the approver (as shown in the scenarios above). Furthermore we argue that in fact impossible to secure the approve method without adjusting the allowance. Considering the following transaction sequence:

1) Alice decides to change Bob’s allowance from N to M (M ≤ N in this example).
2) Bob transfers N tokens by front-running and the transferred variable sets to N.
3) Alice’s transaction is mined and the approve method detects Bob’s token transfer.
4) If approve method does not adjust the allowance based on transferred tokens, it has to set it to M—to conform with the standard—which is allowing Bob to transfer more M tokens, or it could fail which deadlocks Bob from future approvals.

Therefore the approve method has to adjust the allowance according to transferred tokens, not based on passed input values to the approve method. Overall, there seems to be no solution to secure the approve method while adhering specification of ERC20 standard.

**4.2. Proposal 2: Securing transferFrom**

As an alternative to Proposal 1, we can also consider securing the transferFrom method. As specified by the ERC20 standard (see figure [13]), the goal here is to prevent the spender from transferring more tokens than allowed. Based on this assumption, we should not rely solely on the allowance value in deciding whether to allow or prevent an approve and should also consider the number of transferred tokens, which requires new state as in Proposal 1.

Our solution, which is compliant with a careful reading of ERC20, is to interpret allowance as a ‘global’ or ‘lifetime’ allowance value, instead of the amount allowed at the specific time of invocation. For example, say Alice approves Bob for 50 tokens, Bob transfers 50 tokens, Alice approves Bob for 30 (more) tokens, and Bob transfers 30 tokens. In our implementation, Alice would approve Bob for 50 tokens and he transfers 50 tokens. To approve Bob for 30 more tokens, she approves Bob for 80 tokens. He has already spent 50 of these 80 tokens so he will only be allowed to transfer an addition 30. Thus 80 is his lifetime allowance and 50 (kept internally) is the amount he has transferred. In a bit more detail, consider the following, which prevents multiple withdrawals by modifying the implementation of transferFrom but keeping approve untouched:

1) Alice approves Bob to transfer 100 tokens
2) Alice broadcasts an approval of 70, decreasing Bob’s allowance.
3) Bob front-runs Alice’s transaction and transfers 100 tokens (remark: a legitimate transfer).
4) Alice’s transaction is confirmed and sets Bob allowance to 70 by the default approve method.
5) Bob’s noticed the new allowance and tries to move 70 additional tokens by broadcasting transferFrom(_Bob,70).
6) Since Bob has already transferred more than 70 tokens, his transaction fails and prevents multiple withdrawal.
7) In the end, Bob’s allowance is set at 70 and his transferred tokens are set at 100.

**Performance & Discussion.** Interpreting allowance as a lifetime allowance is completely in accordance
with the ERC20 standard (see figure 13). In our solution, there is no relation between allowance (allowed[\_from][msg.sender]) and transferred tokens (transferred[\_from][msg.sender]). The first variable shows lifetime transferable tokens by a spender and can be changed independently of the transferred tokens (i.e., approve method does not check transferred tokens). If Bob has not already transferred that many tokens, he would be able to transfer the difference of it. Our token is implemented as TKNv3 on Rinkeby test network and it passes compatibility checks by transferring tokens between standard wallets. In terms of gas consumption, its transferFrom function needs at about 37% more gas than standard transferFrom implementation. We believe this is acceptable for having a secure ERC20 token.

5. Conclusion

While this paper is a deep dive into a specific issue with ERC20, it also illustrates a number of higher level lessons for blockchain developers. When ERC20 standard was first implemented, it changed how people used Ethereum, giving rise to an ICO craze with its ease of use [24]. This led to the deployment of thousands of early Ethereum, giving rise to an ICO craze with its ease of use [24]. This led to the deployment of thousands of early tokens and the “Multiple Withdrawal Attack” seems too important to ignore. Fixing existing ERC20 code will help future deployments but cannot fix the already deployed tokens. In addition to deploying secure contracts, we suggest blockchain developers conduct external audits and consider security-by-design practices when dealing with other smart contract implementations.

References

[1] Ethereum. Ethereum project repository. [https://github.com/ethereum](https://github.com/ethereum) May 2014. [Online; accessed 10-Nov-2018].

[2] Fabian Vogelsteller and Vitalik Buterin. ERC-20 Token Standard. [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md) November 2015. [Online; accessed 2-Dec-2018].

[3] Mikhail Vladimirov. Attack vector on ERC20 API (approve/transferFrom methods) and suggested improvements. [https://github.com/ethereum/eips/issues/20#issuecomment-265552472](https://github.com/ethereum/eips/issues/20#issuecomment-265552472) November 2016. [Online; accessed 18-Dec-2018].

[4] Tom Hale. Resolution on the EIP20 API Approve / TransferFrom multiple withdrawal attack #738. [https://github.com/ethereum/EIPs/issues/738](https://github.com/ethereum/EIPs/issues/738) October 2017. [Online; accessed 5-Dec-2018].

[5] Shayan Eskandari, Seyyedehmahsa Moosavi, and Jeremy Clark. Sok: Transparent dishonesty: front-running attacks on blockchain. 16. [https://rinkeby.etherscan.io/address/0x5d148c948c01e1a61e1e280c8b2ac39fd49ee69c6](https://rinkeby.etherscan.io/address/0x5d148c948c01e1a61e1e280c8b2ac39fd49ee69c6)

International Conference on Financial Cryptography and Data Security, 2019.

[6] OpenZeppelin. openzeppelin-solidity. [https://github.com/OpenZeppelin/openzeppelin-solidity/blob/master/contracts/token/ERC20/ERC20.sol](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/master/contracts/token/ERC20/ERC20.sol) December 2018. [Online; accessed 23-Dec-2018].

[7] ConsenSys. ConsenSys/Tokens. [https://github.com/ConsenSys/Tokens/blob/df687c00490266a5f15216b19554a065aabdd6/contracts/eip20/EIP20.sol](https://github.com/ConsenSys/Tokens/blob/df687c00490266a5f15216b19554a065aabdd6/contracts/eip20/EIP20.sol) April 2018. [Online; accessed 24-Dec-2018].

[8] Wikipedia. Compare-and-swap. [https://en.wikipedia.org/wiki/Compare-and-swap](https://en.wikipedia.org/wiki/Compare-and-swap) July 2018. [Online; accessed 10-Dec-2018].

[9] Michael Frouws, Andreas Fuchs, and Rainer Bohme. Detecting token systems on ethereum. arXiv preprint arXiv:1811.11645, 2018.

[10] Atkins Chang, Noel Bao, Jack Chu, Leo Chou, and Darren Goh. Ethereum-based erc20 token networks. In International Conference on Financial Cryptography and Data Security, 2019.

[11] Atkins Chang, Noel Bao, Jack Chu, Leo Chou, and Darren Goh. Ethereum-based erc20 token networks. In International Conference on Financial Cryptography and Data Security, 2019.

[12] Peter Vessenes. MonolithDAO/token. [https://github.com/ConsenSys/MonolithDAO/blob/master/src/Token.sol](https://github.com/ConsenSys/MonolithDAO/blob/master/src/Token.sol) April 2018. [Online; accessed 23-Dec-2018].

[13] Nate Welch. flygoing/BackwardsCompatibleApprove.sol. [https://gist.githubusercontent.com/flygoing/2956f0db38e66a24bb8b8e6be6bca6e](https://gist.githubusercontent.com/flygoing/2956f0db38e66a24bb8b8e6be6bca6e) February 2018. [Online; accessed 23-Dec-2018].

[14] Nate Welch. flygoing/BackwardsCompatibleApprove.sol. [https://gist.githubusercontent.com/flygoing/2956f0db38e66a24bb8b8e6be6bca6e](https://gist.githubusercontent.com/flygoing/2956f0db38e66a24bb8b8e6be6bca6e) February 2018. [Online; accessed 23-Dec-2018].

[15] Peter Vessenes. MonolithDAO/erc20. [https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol](https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol) April 2018. [Online; accessed 23-Dec-2018].

[16] Peter Vessenes. MonolithDAO/erc20. [https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol](https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol) April 2018. [Online; accessed 23-Dec-2018].

[17] Peter Vessenes. MonolithDAO/erc20. [https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol](https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol) April 2018. [Online; accessed 23-Dec-2018].

[18] Steven Ellis. transferAndCall Token Standard. [https://github.com/ethereum/EIPs/issues/223](https://github.com/ethereum/EIPs/issues/223) March 2017. [Online; accessed 12-Jan-2019].

[19] Enrique Chavez. StandardToken.sol. [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md) February 2018. [Online; accessed 23-Dec-2018].

[20] William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs. ERC-721 Non-Fungible Token Standard. [https://github.com/ethereum/EIPs/issues/721](https://github.com/ethereum/EIPs/issues/721) January 2018. [Online; accessed 25-Dec-2018].

[21] Peter Vessenes. MonolithDAO/erc20. [https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol](https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol) April 2018. [Online; accessed 23-Dec-2018].

[22] Peter Vessenes. MonolithDAO/erc20. [https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol](https://github.com/ConsenSys/MonolithDAO/blob/master/erc20.sol) April 2018. [Online; accessed 23-Dec-2018].

[23] Atkins Chang, Noel Bao, Jack Chu, Leo Chou, and Darren Goh. Ethereum-based erc20 token networks. In International Conference on Financial Cryptography and Data Security, 2019.

[24] Atkins Chang, Noel Bao, Jack Chu, Leo Chou, and Darren Goh. Ethereum-based erc20 token networks. In International Conference on Financial Cryptography and Data Security, 2019.