|  |  |  |
| --- | --- | --- |
| Cryptographic secure cross border trade | January 26  2019 | |
| This White Paper outlines details of how cross border trade can be secured using Blockchain networks, thus negating the requirement for customs checks at the point of entry. | |

**Contents**

[Introduction 2](#_gjdgxs)

[How Blockchain works in laymen’s terms 2](#_30j0zll)

[What does Blockchain technology prevent? 2](#_1fob9te)

[Benefits of Blockchain 2](#_3znysh7)

[Limitations of Blockchain 2](#_2et92p0)

[Who would benefit from using Blockchain? 3](#_tyjcwt)

[Who would not benefit from using Blockchain? 3](#_3dy6vkm)

[Problem 3](#_1t3h5sf)

[Problem definition 3](#_4d34og8)

[What infrastructure is currently present at the point of entry? 4](#_2s8eyo1)

[Problem statement 4](#_17dp8vu)

[Restrictions 4](#_3rdcrjn)

[How to link physical items with virtual cryptographic proof of work. 4](#_26in1rg)

[Putting a physical item on the Blockchain 4](#_lnxbz9)

[Linking a transaction to a physical action 5](#_35nkun2)

[Linking a transaction to the customs official 5](#_1ksv4uv)

[Preventing tamper with the device 5](#_44sinio)

[Detecting tamper following customs checks 5](#_2jxsxqh)

[Required infrastructure 6](#_z337ya)

[Attack vectors introduced by this system 6](#_3j2qqm3)

[Network selection 7](#_4i7ojhp)

[Public network 7](#_2xcytpi)

[Private network 7](#_1ci93xb)

[Conclusion 8](#_3whwml4)

# Introduction

## How Blockchain works in laymen’s terms

Current generation Blockchain networks utilise many different algorithms to secure their network, two of the main networks currently in existence are Litecoin (LTC) which uses the Scrypt hashing algorithm and Bitcoin (BTC) which uses the SHA256 hashing algorithm. These hashing algorithms are used to solve complex mathematical proofs using unmined transactions as the source. Once the proof is provided the transactions that were used to solve it are ‘mined’ and added to the Blockchain in a new block, to prevent later modification (Re-Org attack) the Hash of the previous block is included in the new block and propagated throughout the entire network. To encourage participation in mining the miner who successfully mines the block is rewarded with the Block Reward and any fees those sending transactions have attached to their unmined transaction.

## What does Blockchain technology prevent?

Once a transaction is added to the Blockchain the data becomes immutable, this is not because the Blockchain is secure, and indeed anyone with sufficient computing power can re-write the Blockchain to a state that is beneficial to them. This does not happen regularly and is unlikely to happen to the two networks identified above due to the cost involved, estimates have been produced that a single Re-Org attack on the BTC network would cost approximately $15m per minute, this prohibitive cost prevents all but the most wealthy and nation states from attempting it. In the event a Re-Org attack was successful the attacker would be unlikely to benefit from this, due to the decentralised nature of the Blockchain the majority of participants would simply ignore any blocks mined by the attacker and disregard the Re-Org’d chain.

## Benefits of Blockchain

1. Provides immutable record of all transactions.
2. Uses Game Theory to incentivise those with resources to secure the network as opposed to attacking it.
3. Public and searchable using a simple Block Explorer.
4. Removes the need for trust from any system that requires an arbitrator where the transaction can be reduced to simple states.
5. Allows the transmission of information / value without an intermediary.

## Limitations of Blockchain

1. Slow by design.
2. Low throughput.
3. Once a transaction has been added to the Blockchain it cannot be reversed even if it was done in error.

## 

## Who would benefit from using Blockchain?

1. Anyone who requires an immutable record.
2. Any transaction where trust is required.

## Who would not benefit from using Blockchain?

1. Those who require high throughput.
2. Those who require a record that is not immutable.

# Problem

## Problem definition

The United Kingdom (UK) and Irish (IRE) government are required in the spirit of the Good Friday Agreement (GFA) to facilitate an open border between the two territories, this is possible for people due to the Common Free Travel Area (CFTA) however the movement of goods is still subject to tariffs as are all goods coming from the European Union (EU) post BrExit when the UK leaves the EU. Currently there is no infrastructure either within the UK or EU to facilitate the necessary customs checks and if these checks were to be carried out at the border this would cause significant disruption. The installation of new infrastructure at and along the Irish border is undesirable as this has the potential to inflame tensions and set UK IRE relations back several decades.

The UK EU and IRE have all stated that they would prefer customs checks to be carried out away from the border however this introduces an additional vulnerability to the arrangement. If customs checks are carried out away from the border there is currently no mechanism that would ensure the cargo is not interfered with enroot to the destination, this would allow significant amounts of smuggling and threaten both the integrity of the UK internal market and EU single market with both parties having a back door to the other. Therefore what is required is a method of checking the integrity of the customs checks that were carried out away from the border at the point of entry using minimal infrastructure. Such a system would still require infrastructure to be modified but would prevent the visible effects at the point of entry to the market in question.

As the EU and UK markets are closely aligned customs requirements should be minimal provided regulatory alignment is maintained, as the two systems diverge it is anticipated that additional checks will be required for all goods entering and leaving the market. Any proposed system will require trust between the two parties, as “sovereignty” is one of the UK red lines in the withdrawal negotiations it would be beneficial to remove any oversight of either party from the system thus ensuring no one party is dominant in the trade.

## What infrastructure is currently present at the point of entry?

There are numerous crossings along the Northern Irish (NI) IRE border the majority of which, many currently have Automatic Number Plate Recognition cameras (ANPR) at the point of crossing. All other checks required are currently carried at the point of entry / exit from the UK.

## Problem statement

Provide a system that is capable of ensuring customs checks carried out away from the border are valid at the point of entry automatically, the system should not require oversight from either party wishing to participate in trade and be immutable to prevent fraud.

# Restrictions

1. Additional infrastructure should not be visible where possible and be of the same type currently installed which does not inflame tensions.
2. Solution should not interfere with the normal operation of the border.
3. Use existing infrastructure where possible.
4. Solution should not require trust of either party or any third party.
5. Solution should be immutable.
6. Solution should minimise initial and ongoing operational costs.

# How to link physical items with cryptographic proof of work.

## Putting a physical item on the Blockchain

Data stored on the Blockchain is secured using a cryptographic Private Key, if a physical item is to be transferred on the Blockchain it must be given a Private Key. A single Private key is capable of creating ***virtually limitless*** number of addresses, however the system is only secure provided the Private Key is securely stored and inaccessible to other parties. Therefore we would need to link a Private Key on a device to the physical asset crossing the border, fraud could easily be identified using forensic methods on the Blockchain utilising a simple automated Block Explorer.

Linking to every individual item is not feasible as the work required to accomplish this would fall foul of requirement 2 & 6. It is possible to link this device however to the vehicle which is transporting the goods as there is already precedence for this in the installation of “Tracker” modules on goods and transport vehicles.

## Linking a transaction to a physical action

To link an item to a physical action we must first identify the last action the customs official will take after which point the goods become subject to potential tamper, this action should not be undone until the goods arrive at their intended destination. This action should also be used as a means to preserve the integrity of the Customs Officials check. Following review of the procedures for third country goods, the last action carried out that meets this requirement is closing of the shipment door / lock.

We can therefore use the action of closing / opening the door as a trigger event for our device.

## Linking a transaction to the customs official

This can be accomplished in multiple ways however the solution that removes trust from the Customs Official is identified below.

We need to link the transaction to the moment only the customs official closes the door and no one else, the device identified above could be programmed to create a new address from its Private Key every time the door is closed and destroy it every time it is opened. Using this random address the customs official could send a transaction to that address thus linking the customs officials sending address and the activity of closing the door. If the door is opened the device would destroy its address and the link would be broken proving someone interfered with the shipment post customs check.

## Preventing tampering with the device

The issue of tamper whilst in transit can easily be solved by locating the device inside of the goods container, the only provision required for this is the need to externally transmit the generated address via wireless or visual means. Further protection could be provided by locating the device in an inaccessible location within the container with only a sensor located so as to detect the trigger event identified above.

# Detecting tamper following customs checks

The receiving port will require the following details;

1. Customs officials addresses capable of making a transaction on the selected network.
2. Access to the Blockchain for the network being used.

The receiving port will have the following capabilities;

1. ANPR cameras located at the point of entry.
2. List of approved customs officials addresses.
3. The ability to scan / read the address for the vehicle in range of the ANPR camera.

Using this information and abilities the receiving port will perform the following actions;

1. Scan the address transmitted by the vehicle.
2. Search the Blockchain for the address,
   1. If the address has a received transaction from an approved customs official address, the customs checks are still valid and the vehicle is waived through.
   2. If the address does not have a transaction from an approved customs official address the vehicle is subject to full customs checks at an area away from the port of entry.

## Required infrastructure

All infrastructures required thus far is either already installed, planned to be installed or of a nature that is already installed except the ability to read the address transmitted by the vehicle. This requirement can either be met via the use of QR codes displayed on the vehicle using some form of display, via wireless transmission (RFID / WIFI / BT / IR) or both. The selection of the method of transmission / receipt of this information can be determined via the end user but it should be noted that a visual method will not require any additional infrastructure and as such has been selected for this paper.

# Attack vectors introduced by this system

Although we now have secured the shipment using the Blockchain a new attack vector has been introduced, it may be possible for attackers to read the data then spoof the transmission to fool the receiving point of entry. To accomplish this, the attacker would need to prevent transmission of the original data and transmit the spoofed data. The following mitigations are possible for each transmission method;

**Visually -** The displayed QR code could be programmed to include information such as the current time to a 1 minute resolution which is encrypted by the devices Private Key used to create the corresponding address. This would mean a spoofing of the displayed QR code was only valid for a period of 1 minute provided the Private Key remains secure. This can easily be decoded by the ANPR using the displayed address.

# Network selection

Due to the public nature of Blockchain technology some entities may feel the need to create their own private network for this system to ensure privacy, however this sacrifices several of the benefits of using Blockchain but does nothing to mitigate the negatives. Below are the benefits and limitations of both public and private Blockchain networks;

## Public network

**Benefits**

1. Immutable public record.
2. Other network users are incentivised to secure the network as attack is prohibitively expensive.
3. Fees are only paid when using the network.
4. No special software is required to be developed to access the network.
5. Completely transparent, data can be viewed by anyone.
6. No development / operational costs for the network as it is operational and operated by existing network participants.

**Limitations**

1. Limited throughput (dependant on the network selected).
2. Completely transparent, data can be viewed by anyone.
3. Fees must be paid when using the network

## Private network

**Benefits**

1. Can be designed to suit the users’ needs such as throughput.
2. Can be as private as required.
3. Fees are not paid.

**Limitations**

1. Record is not immutable.
2. Other network users are not incentivised to secure the network and attack is not prohibitively expensive.
3. Special software is required to be developed to access the network.
4. Developers must bare all development and operational costs.

As can be seen the benefits of using an operational public network open to all participants has considerably large advantages over a private network, it is also possible to mitigate the negatives using the below methods;

**Limitation 1 -** Possibility to batch transactions to increase throughput, further development of the lightning network protocol will allow magnitudes of scale.

**Limitation 2 –** Transmitted data can be encrypted if required, further development of the lightning network will allow anonymous transactions.

**Limitation 3 –** The network user could take an active role in the network mining their own transactions and earning fees using surplus electricity, this would further secure the network.

# Conclusion

The methods identified within this white paper using technology that is already in existence can effectively secure physical cross border trade within the real world. Use of this proposal would create significant improvements in security, immutability and reliability of customs checks.