Independent Work
Request for Comments: 31337
Category: Informational
ISSN: ?

Shadow Of Harbringer

Shadow Of Harbringer
Bitcoin Cash Developers

17 July 2024

Table of Contents

Zero-Kyc Assurance Mechanism for Fiduciary Money Transfer

1. Introduction

The objective of Zero-KYC Assurance Mechanism for Fiduciary Money Transfer (ZKAM-FMT) is to ensure that fiat money is transfered from a bank account or a related bank-provided service are sent in the exact amount, with the exact target and from the designated person without a possibility of Man In The Middle attack, spoofing transaction data or pretending the transaction was executed while in reality it was not.

The procedure works without the need of any kind of integration with electronic systems of Banks or any kind of intervention on their behalf.

Specific attack this mechanism was designed to stop can be called Man In The Middle P2P Fiat-To-Crypto Financial Spoofing Attack (MPFTC-FSA) and is described in section 2 of this document.

2. Description of the attack

In a direct Peer-To-Peer crypto trading market, where users directly enter trade agreements where they exchange a cryptocurrency for a government controlled asset like fiduciary money, MPFTC-FSA can be described in the following way.

Let’s make some assumptions and definitions to clarify our definition:

- CRYPTO is a hard money-type cryptocurrency without chargeback functionality, for example it can be Bitcoin Cash or Monero.

- FIAT is a government controlled asset like fiduciary money in an electronic form, with partial or complete chargeback functionality.

- MARKET is the virtual place and environment on the Internet where users exchange CRYPTO for FIAT and the reverse.

- Bob is a honest seller of crypto that has publishes a “sell” crypto offer in exchange for a bank fiat transfer. Also he is the first victim.

- Alice is a honest item or service buyer, that is completely unrelated to the CRYPTO/FIAT exchange happening. Due to the attack, she becomes the second victim.

- Charlie is a scammer that enters the exchange on the MARKET executing the attack, victimizing the other participants of the trade.

- ITEM-MARKET is a completely unrelated service where items are traded for FIAT - this can be for example ebay, amazon, craiglist or gumtree.

- ITEM(IPhone) is unrelated goods/services used as a lure by Charlie, the item(s) never actually exist.

The complete attack procedure works as follows:

• Bob, the honest crypto seller puts an offer of sale of CRYPTO (1.00000000 Bitcoin Cash) in exchange for 1000 units of FIAT money executed as a bank wire transfer on the MARKET.

• Charlie the scammer notices the offer, and makes fake/fraud listing of an ITEM(IPhone) sale on ITEM-MARKET. He sets the price to 1000 units of FIAT money.

• Alice, the honest item buyer, wants to buy an item and notices the offer of Charlie on ITEM-MARKET, she contacts Charlie about the purchase.

• Charlie, having received the item purchase offer from Alice, initiates the trade of the CRYPTO (1 Bitcoin Cash) with Bob. Bob gives Charlie an account number to transfer the FIAT to.

• Charlie responds to the ITEM(IPhone) purchase request from Alice, he gives her the account number received from Bob.

• Alice transfers her FIAT money to Bob’s account.

• Bob receives the bank FIAT transfer, unlocking the offered CRYPTO to be acquired by Charlie.

• Charlie transfers the CRYPTO to his own wallet.

• Using technological means, Charlie erases all traces of his existence from the Internet or makes them irrelevant, switching to a new identity: “Elize”.

• Alice, having not received the ITEM(IPhone), either calls her bank to execute chargeback or contacts the Police in order to investigate the Bob’s account number.

• Bob the honest seller gets prosecuted by either the Police because of the scam accusation or by his bank because of scam suspect due to a customer’s chargeback.

• A) After above happens 100 times, in a pessimistic scenario, Bob goes bankrupt/to prison due to lawsuits or being barred from having a bank account because of being perceived by the banking system as a scammer.

• B) After above happens repeats 100 times, in an optimistic scenario, Bob gets tired of constant problems and accusations and simply stops trading CRYPTO on the MARKET.

3. The significance of the MPFTC-FS attacks in large scale and over longer periods of time

Due to their stealthy and near-untraceable nature MPFTC-FS Attacks are extremely dangerous to any kind of direct Peer-To-Peer CRYPTO MARKET because of multiple reasons:

Unlike many other scam schemes, MARKET is not the target of the scam. The existence of the attack is completely invisible to the MARKET. The attack can potentially get executed thousands of times without the owners/administrators of the MARKET noticing anything out of order is happening.

Charlie the scammer, being Man In The Middle attacker, can impersonate both other parties of the trade during the communication between them, he can describe himself as “Bob” when communicating with Alice and he can describe himself as “Alice” when communicating with Bob, making detection of this scam very difficult.

Assuming Alice is not a security&technology expert (which is likely), it is virtually impossible or impractical for her to detect that she is transfering funds to a seller of a crypto market.

If the number of scammers using the MPFTC-FS Attacks becomes large, it can cause a slow erosion of honest CRYPTO sellers to the point the MARKET becomes severely damaged or even goes bankrupt due to the lack of CRYPTO sellers.

It is therefore highly logical to assume that MPFTC-FS Attacks could be the main cause of the degradation and deaths of many P2P MARKETs that happened and perhaps may/will happen in the future.

Under normal circumstances, due to the existence of Proxies, TOR relays and other anonymity tools on the Internet, detecting that Charlie is a scammer will be very difficult to the point of being impractical.

Many services deal with these kind of attacks using various Know-Your-Customer (KYC) policies, that verify that the customer has no fake identity, thus making it hard for Charlie to escape detection and prosecution. Implementation of security mechanisms using KYC is however not the purpose of this RFC Document.

4. ZKAM-FMT: Description of The Zero-Kyc Assurance Mechanism for Fiduciary Money Transfer

4.1. The purpose of the ZKAM-FMT mechanism

The purpose of ZKAM-FMT mechanism is to

- Ensure that Bob, the honest CRYPTO seller, cannot receive the FIAT money transfer from any other party than the party he is engaged in the exchange with using the MARKET

- Ensure that Charlie the scammer cannot manipulate Alice, the honest item buyer, to transfer the money to Bob’s bank account in a non-reversible way

- Verify that the bank FIAT money transfer is done exactly by the same person/entity that participates in the exchange of FIAT to CRYPTO using the MARKET

- Execute all of the above without using Know-Your-Customer verification mechanisms

4.2. Basic design definitions of the ZKAM-FMT mechanism

The ZKAM-FMT mechanism consists of few main pieces:

- MARKET is the CRYPTO to/from FIAT exchange service running on the Internet

- MARKET APP is a software package, user interface of the MARKET that facilitates the direct P2P trade of CRYPTO. It acts as a means of communication, execution and partially verification for the parties taking part in a FIAT/CRYPTO exchange.

- BROWSER is a software package, sub-section of the MARKET APP, it can be either software directly integrated into the MARKET APP, it can be a module or it can be a separate

software application that is linked to MARKET app
in a specific way

- BACKEND are a set of background processes and services
that play the main role of execution and verification
of the exchange between the market participants.

4.3. Core functionality of the ZKAM-FMT mechanism

• The ZKAM-FMT mechanism ensures that the crypto buyer cannot
make another person execute the FIAT money bank transfer
by facilitating BROWSER in the exchange process.

• BROWSER is a software package running on the same device,
a critical part of the exchange process and is a trusted
part of the MARKET APP, either by being directly integrated
by it, being a semi-external component/library or being an
external application that is linked with the MARKET APP
in a trusted way that cannot be easily manipulated by third
parties.

• The role of the BROWSER is to act as a web browser, using
which the CRYPTO buyer on the MARKET log-ins to his back
account in order to execute the FIAT money transfer.
The BROWSER acts exactly like an usual web browser does,
with the exception that it verifies whether certain actions
on the bank’s website were executed in a specific manner.
Specifically it ensures the most critical variables like
Account Number, Account Owner of Receiver, Amount of FIAT
and the Title of the transfer match. Another important detail
BROWSER verifies is whether the form of the transfer was
successfully sent and whether the process ended up in SUCCESS
or FAILURE state.

• The BROWSER then communicates with MARKET APP and BACKEND,
either returning the requested information as a whole,
or simply returning error code (FILTER variant described
in section 4.6 of this RFC Document), corresponding
to whether the entered data was correct or not.

• The MARKET APP then communicates to the CRYPTO seller
whether the FIAT transfer was executed by the CRYPTO buyer
successfully, giving him options to proceed with unlocking
the CRYPTO to the buyer or cancelling the trade or reporting
the buyer for scamming.

• The MARKET APP also strongly communicates to the CRYPTO
seller that he should only accept the transfer with
a specific transfer title and reject transfer with any other
title, in order to further make scenarios of a mistake or scam
unlikely to happen.

• There are various critical security and privacy
considerations related to this mechanism, which are
described in further sections of this RFC Document.

4.4. Security and user trust considerations

Due to the crypto buyer who uses the MARKET APP logging-in to his own bank account using the BROWSER which is an integral part of the MARKET APP or can be seen as such, owners/creators of the MARKET app need to ensure that The BROWSER does not relay any form data more than it is absolutely necessary to the MARKET APP or BACKEND.

This especially applies to any kind of login and password form fields. Omitting such fields can be hard-coded in the application so it is near-impossible for the apllication to return such data to the MARKET APP or BACKEND.
The BROWSER can be trusted by the user to do the above

Possible solutions include (but are not limited to):
- Open sourcing the BROWSER part of the MARKET APP or even the whole MARKET APP, depending on the chosen solution

- Removing all of the stored data from databases after a successful trade

- Precisely describing to the customer that he will be redirected to his bank account site and the data will be only temporarily stored for verification

- Hashing data fields and relaying hashed values instead of raw text values, described in section 4.7 of this RFC Document

4.5. Data Privacy & Legal considerations

Assuming proper implementation in the spirit of this RFC document, neither the MARKET APP or the BROWSER will never relay any personal information of the person making a FIAT transfer. The only information that is verified and temporarily stored is the Account Data of the Fiat Receiver, but this is already the case because the trade participants usually share such data on the internal chat of the MARKET APP, which implies that some of it is also at least temporarily stored.

So privacy-wise and legal-wise (taking EU’s GDPR laws and US’ CCPA laws into account), ZKAM-FMT mechanism should not create any significant change in this regard.

4.6. Internal mechanics: BROWSER with FILTER variant

To strongly minimize the possibility of mistakes and data leaks, there exists an alternative way in which the BROWSER can be implemented.

The BROWSER-FILTER variant, in the process of redirection of the crypto buyer to his bank website for the purpose of making FIAT transfer, the BROWSER only receives the few

important pieces of data from BACKEND and verifies whether they match to the data entered into the website form by the user plus it verifies whether the process ended up in success or failure. No data at all, except error code (signifying the SUCCESS or FAILURE) is sent back to neither MARKET APP or BACKEND.

This ensures that even in the case of software failures and bugs in BROWSER, the probability of returning some critical private data of the account owner like login, password, OTP codes or similar and accidentally storing it by BACKEND is negligible and unrealistic in practice.

4.7. Internal mechanics: BROWSER with HASHED FILTER variant

Relaying hashes of data field’s contents instead of raw data between MARKET APP, BACKEND and BROWSER can be employed to further further eradicate legal and security risks related to even temporarily storing user information.

Using the BROWSER-HASHED-FILTER variant, the critical data crypto seller enters (like account number, account name, amount) can be turned to hashes and then sent to the BACKEND in this form. BACKEND then relays these hashes to BROWSER and the browser verifies whether the hashes of the data entered by the user on the bank website match the supplied hashes. If the hashes match and the FIAT transfer process ends in success, BROWSER returns success code, otherwise it returns error code depending on in what manner the process failed.

5. Example event flows

To describe the ZKAM-FMT event flow in full detail, let’s first make additional definitions and assumptions. Previous definitions described in section 4.2 also apply.

- THE COMPANY is the legal entity owning and maintaining the MARKET, MARKET APP, BACKEND and BROWSER.

- Bob is a honest seller of CRYPTO that has publishes a SELL crypto offer in exchange for a bank FIAT transfer.

- Dave is a CRYPTO buyer that enters into the exchange with Bob in order to purchase CRYPTO for FIAT.

5.1. Event flow A: A success scenario

Sequence of events:

1. Bob, the honest crypto seller puts an offer of sale of CRYPTO (1.00000000 Bitcoin Cash) in exchange for 1000 units of FIAT money executed as a bank wire transfer on the MARKET.

2. Dave the buyer notices the offer and responds to it. He initiates the trade of the CRYPTO (1 Bitcoin Cash) with Bob.

3. The BACKEND generates an unique and random transfer title: “YYY-RND-YYY” which will be used as an unique transfer title in order to avoid mistakes.

4. MARKET APP displays a prompt to Dave:
“You will now be redirected to your bank where you will make a transfer of 1000.00 units of FIAT to Account Number XXXX-XXXX-XXXX-XXXX-XXXX owned by Bob Bobinsky, please use the transfer title YYY-RND-YYY”
“Please choose your bank from the listed banks”

5. Dave chooses his bank, MARKET APP opens BROWSER with the URL locked in to the location of the bank website.
Dave cannot change the URL, all means of manually entering and modifying the URL ale locked out in the BROWSER, the BROWSER has no URL bar.

6. Dave log-ins into the Bank website, enters all given account data, confirms the transfer with an OTP code.

7. Once the FIAT transfer process succeeds, BROWSER software is closed and Dave is moved back to the MARKET APP.

8. BROWSER relays the requested data plus success status to BACKEND and/or MARKET APP.

9. The BACKEND receives the success code from BROWSER or MARKET APP and the internal logic decides to notify the CRYPTO seller Bob.

10. Bob receives the confirmation of the FIAT transfer success and a prompt:

11. “FIAT money transfer of 1000.00 units to your account XXXX-XXXX-XXXX-XXXX-XXXX is on its way to you”
“Warning: please only accept a transfer titled ‘YYY-RND-YYY’, otherwise reject/return the transfer”

12. Once money is in his account, Bob unlocks the CRYPTO to be transfered by Dave into his own wallet.

13. Dave transfers the CRYPTO to his own wallet.

5.2. Event flow A: A failure scenario

Sequence of events:

1. Bob, the honest crypto seller puts an offer of sale of CRYPTO (1.00000000 Bitcoin Cash) in exchange for 1000 units of FIAT money executed as a bank wire transfer on the MARKET.

2. Charlie the scammer notices the offer, and makes fake/fraud listing of an ITEM(IPhone) sale on ITEM-MARKET. He sets the price to 1000 units of FIAT money.

3. Alice, the honest item buyer, wants to buy an item and notices the offer of Charlie on ITEM-MARKET, she contacts Charlie about the purchase.

4. Charlie, having received the item purchase offer from Alice, initiates the trade of the CRYPTO (1 Bitcoin Cash) with Bob.

5. The BACKEND generates an unique and random transfer title: “YYY-RND-YYY” which will be used as an unique transfer title in order to avoid mistakes.

6. MARKET APP displays a prompt to Charlie:
“You will now be redirected to your bank where you will make a transfer of 1000.00 units of FIAT to Account Number XXXX-XXXX-XXXX-XXXX-XXXX owned by Bob Bobinsky, please use the transfer title YYY-RND-YYY”
“Please choose your bank from the listed banks”

7. MARKET APP opens BROWSER with the URL locked in to the location of the bank website.

8. Charlie log-ins into the Bank website, enters all given account data and changes the amount to a much smaller amount than requested by the MARKET APP in hope to cheat the process, then executes the transfer, confirming it with an OTP code.

9. Once the FIAT transfer process goes through, BROWSER software is closed and Charlie is moved back to the MARKET APP.

10. BROWSER relays the requested data plus transaction status to BACKEND and/or MARKET APP.

10. The BACKEND receives the data from BROWSER or MARKET APP and the internal logic decides that the transaction was fraudulent because the amount was invalid, generates an error code (STATUS: INVALID AMOUNT).

11. The BACKEND decides to notify the CRYPTO seller Bob that Charlie tried to cheat the purchase process.

12. Charlie, assuming he will succeed to cheat the process, responds to the ITEM(IPhone) purchase request from Alice, he gives her the account number received from Bob and tells her to use the transfer title “YYY-RND-YYY” received from MARKET APP.

13. Alice transfers her FIAT money to Bob’s account.

14. The internal logic of MARKET APP decides to interrupt the purchase process and mark the trade as invalid, locking out the crypto payout from Bob.

15. Bob receives the notification about fraudulent cancelled trade and is told to return any unidentified FIAT transfered to his account having the title “YYY-RND-YYY” or the amount "1000" back to sender.

16. THE COMPANY notifies the authorities about the fraud attempt, giving collected data (like an IP address, used bank URL) of Charlie to the authorities.

17. Having understood the situation, crypto seller Bob returns received FIAT back to Alice.

18. Charlie is later prosecuted for attempting a Man-In-The-Middle market scam.