Augmenting the MetaMask-Wallet with Domain Name based Authentication of Ethereum Accounts

Jonas Ebel, 19.04.2021, Master Thesis Final Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technical University Munich
wwwmatthes.in.tum.de

Outline

1. Background and Motivation
2. Research Questions
3. Design Concept
4. Usability Testing
5. Conclusion and Outlook

Background

Authentication of Ethereum Accounts in MetaMask

Ethereum Blockchain

- Introduced 2015
- Public permissionless Blockchain
- Smart Contract describes business logic

MetaMask

- Wallet for Ethereum
- Manages the user‘s access to its accounts
- Browser Extension

Motivation

Authentication of Ethereum Accounts in MetaMask

Primary Objective of Authentication

Enhancing user security

Motivation

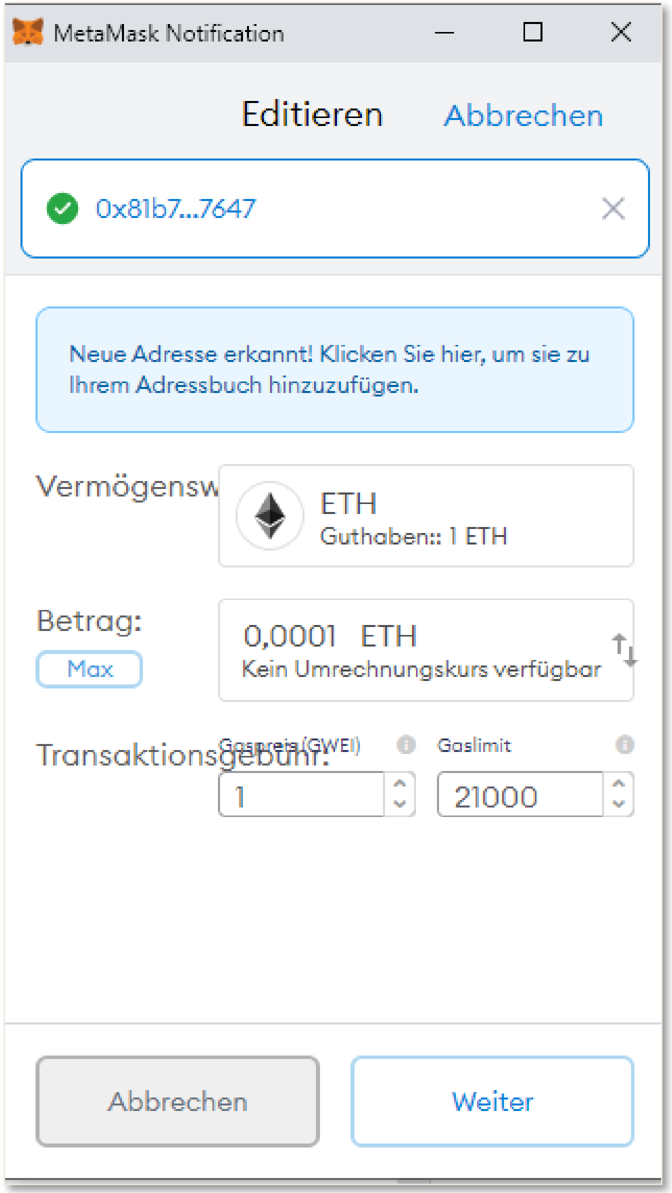
Primary Objective: Enhancing user security

Unreadable Ethereum Address
0xdc51Bac25e1c22E2F04bAAc20396D99fe56f7359

Cryptocurrencies
Anonymous by Design

We argue
Anonymity inhibits use cases

Authentication Solution
TLS/SSL endorsed-Smart Contracts (TeSC) by Gallersdörfer



0x81b7...7647

Neue Adresse erkannt! Klicken Sie hier, um sie zu Ihrem Adressbuch hinzuzufügen.

Vermögensw: ETH Guthaben:: 1 ETH

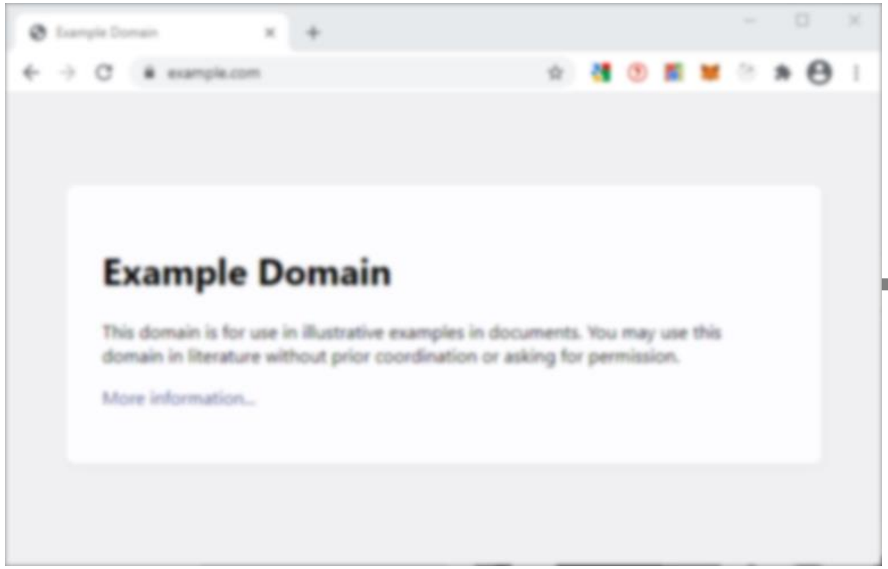
Betrag: 0,0001 ETH
Kein Umrechnungskurs verfügbar

Transaktionsgebühr: Gaspreis (GWEI) 1 Gaslimit 21000

Background

TLS/SSL endorsed Smart Contracts

Example.com



Example Domain

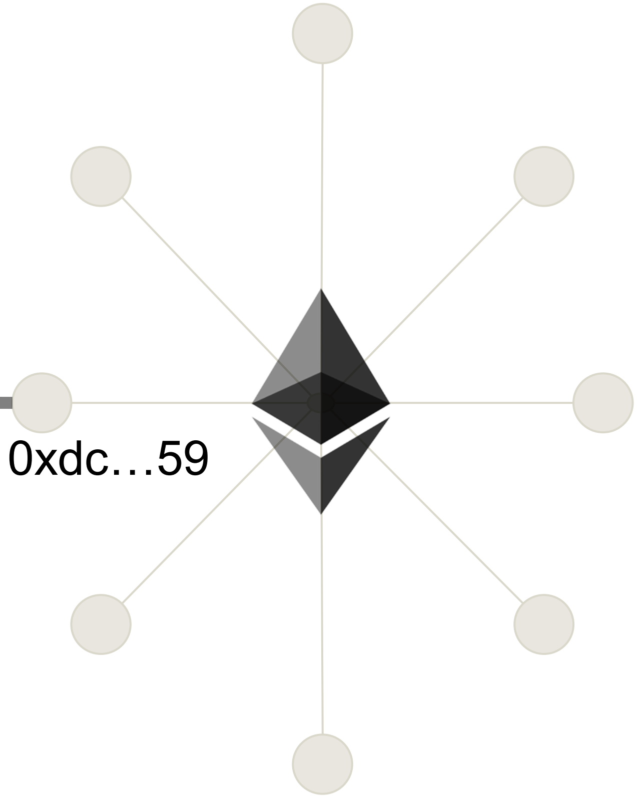
example.com

Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

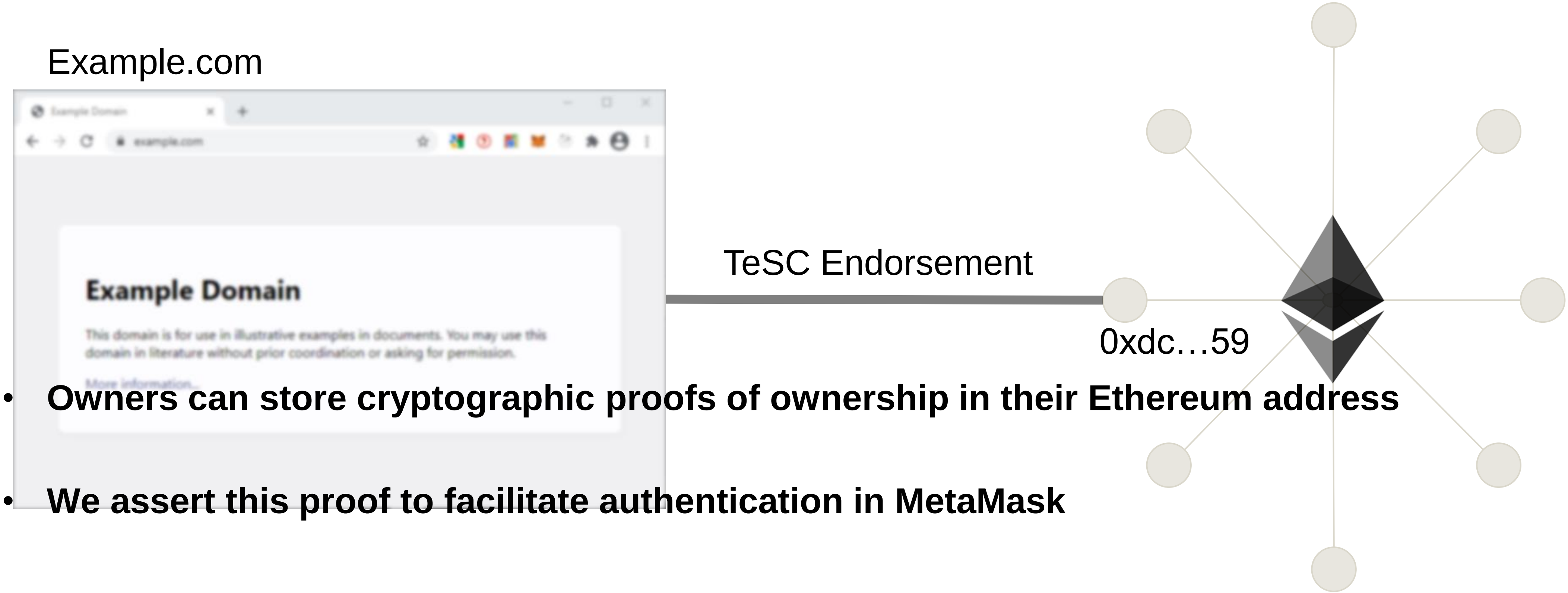
More information...

TeSC Endorsement



Background

TLS/SSL endorsed Smart Contracts



Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

- **Owners can store cryptographic proofs of ownership in their Ethereum address**
- **We assert this proof to facilitate authentication in MetaMask**

Research Questions

1. How can the indication of domain name-based authentication be designed for MetaMask?

Design Concept based on Browser Analysis

2. What is a feasible architecture concept to authenticate addresses in MetaMask?

TeSC Verification Algorithm

3. Does the application of domain name-based authentication improve the user's security while interacting with Ethereum?

Usability Study

Outline

1. Motivation and Background
2. Research Questions
3. Design Concept
4. Usability Testing
5. Conclusion and Outlook

Design Concept Based on States

All states are displayed on the Confirmation Screen in MetaMask

1. Authenticated

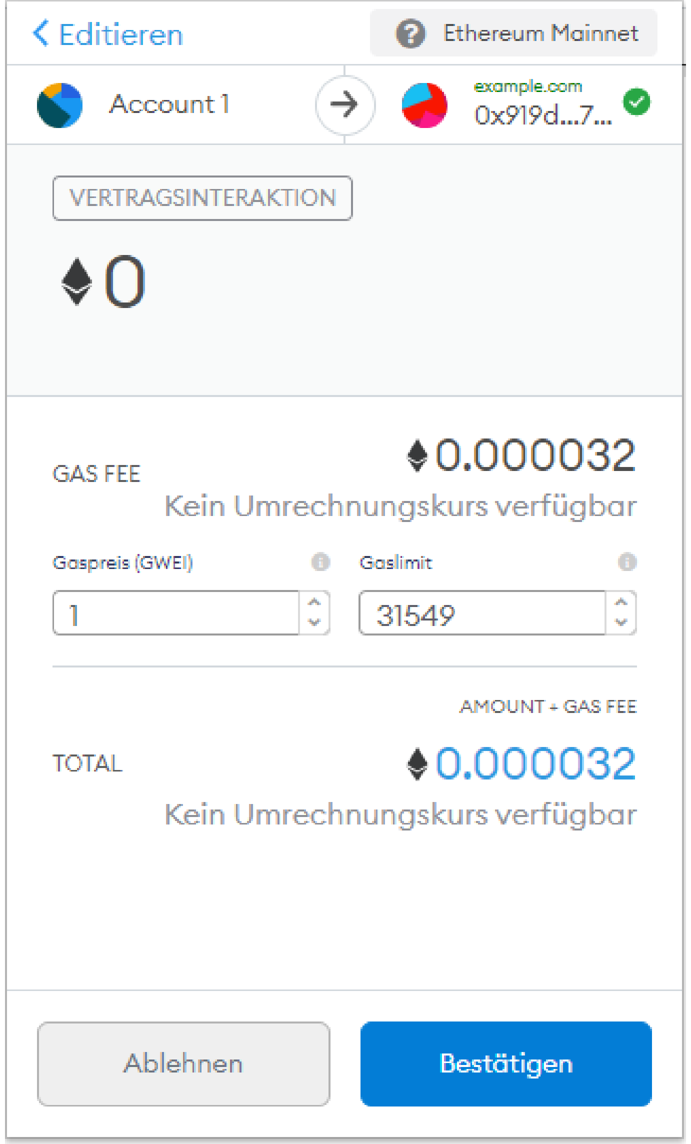
2. Critical Error

3. Protocol Downgrade

Design Concept (1/3)

Authentication Indication

- TeSC Authentication was successful
- The current website is associated with the Ethereum Address
- User can double check, whether this is the expected identity



< Editieren

Ethereum Mainnet

Account 1 → example.com 0x919d...7... ✓

VERTRAGSINTERAKTION

0

GAS FEE 0.000032

Kein Umrechnungskurs verfügbar

Gaspreis (GWEI): 1

Gaslimit: 31549

AMOUNT + GAS FEE

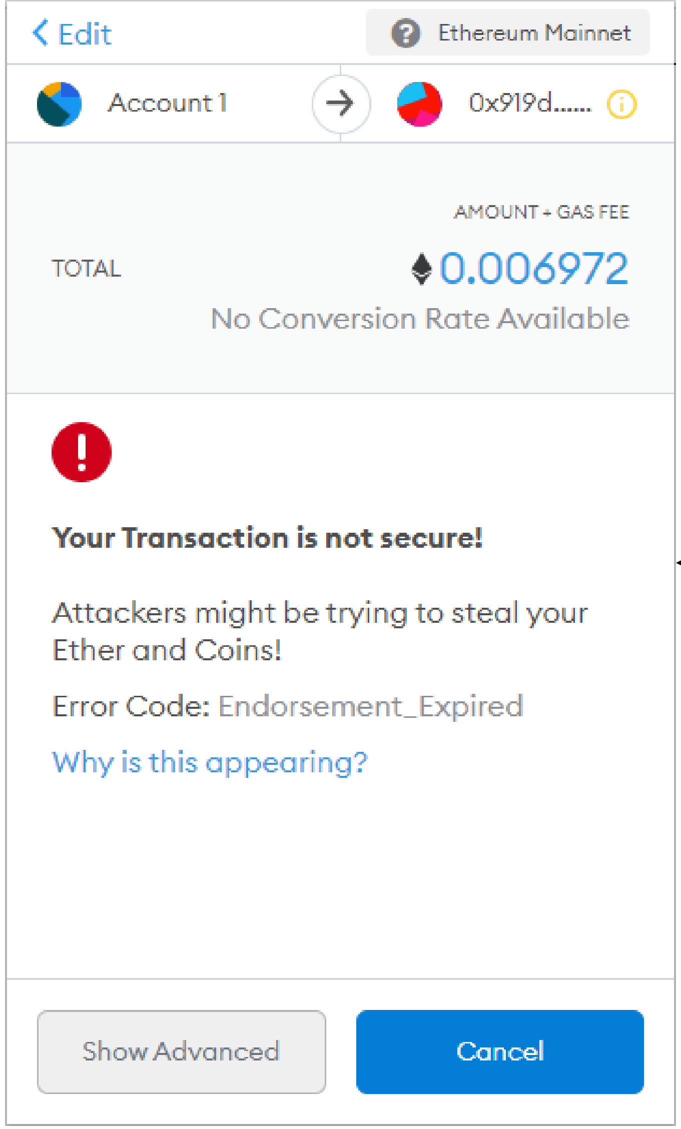
TOTAL 0.000032

Kein Umrechnungskurs verfügbar

Design Concept (2/3)

Critical Error Indication

- TeSC Authentication failed
- User is interrupted in flow
- Two-stages Design
  - First: General Warning
  - Second: Technical Explanation

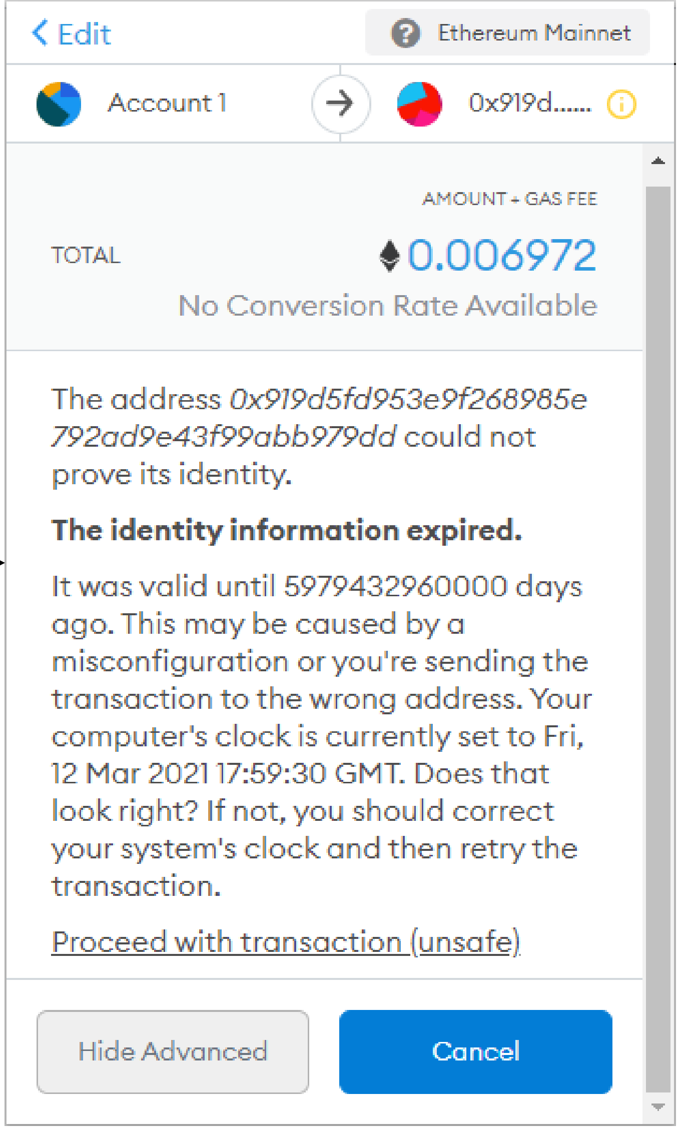


Your Transaction is not secure!

Attackers might be trying to steal your Ether and Coins!

Error Code: Endorsement_Expired

Why is this appearing?



The address *0x919d5fd953e9f268985e792ad9e43f99abb979dd* could not prove its identity.

The identity information expired.

It was valid until 5979432960000 days ago. This may be caused by a misconfiguration or you're sending the transaction to the wrong address. Your computer's clock is currently set to Fri, 12 Mar 2021 17:59:30 GMT. Does that look right? If not, you should correct your system's clock and then retry the transaction.

Proceed with transaction (unsafe)

Outline

1. Motivation and Background

2. Research Questions

3. Design Concept

4. Usability Testing

5. Conclusion and Outlook

Usability Testing (1/5)

Experiment Facts

- **Question**
  Are more users able to identify a fraudulent address with our design?

- 40 Participants
- Within-Subject Measurements

- **Scenario-based Test**
  - Trusted expert Alice
  - Initial Coin Offering of GreatCoin
  - 2 Transactions

Usability Testing (2/5)

Scenario

Problem

Participants shall trust the company but stay vigilant for attacks

Trust establishment

Alice recommends GreatCoin	**Alice highlights general investment risk**
Users trust the Company	Users stay suspicious to protect their money

Procedure

1. Augmented MetaMask

1. Participants receive offer to invest in ICO
2. Participants receive a special offer for a sec ment

Fraudulent Recipient

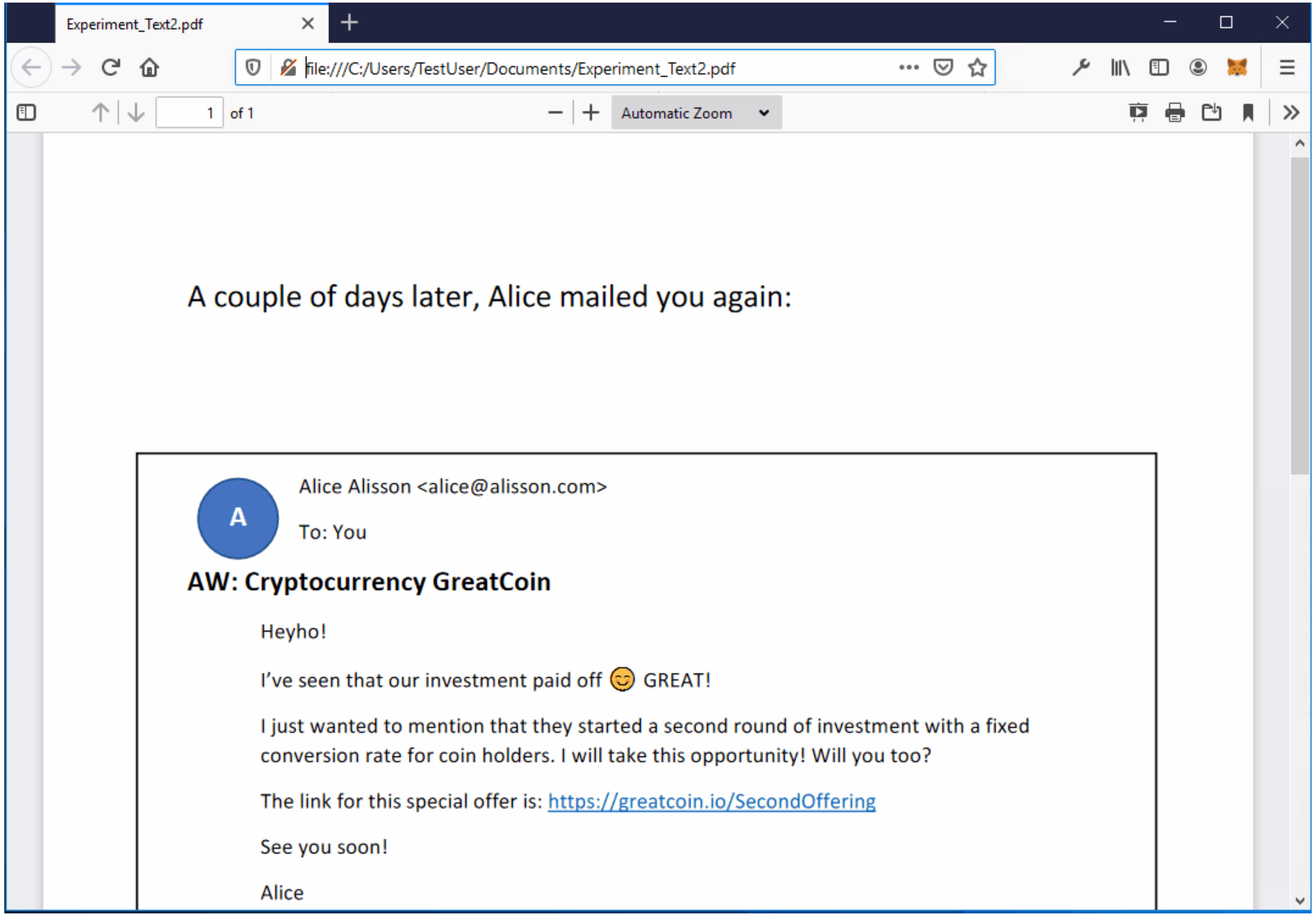
2. Original MetaMask

Repeat Experiment

Randomize order of MetaMask

Usability Testing (3/5)

Second Transaction



A couple of days later, Alice mailed you again:

A

Alice Alisson <alice@alisson.com>

To: You

AW: Cryptocurrency GreatCoin

Heyho!

I've seen that our investment paid off 😊 GREAT!

I just wanted to mention that they started a second round of investment with a fixed conversion rate for coin holders. I will take this opportunity! Will you too?

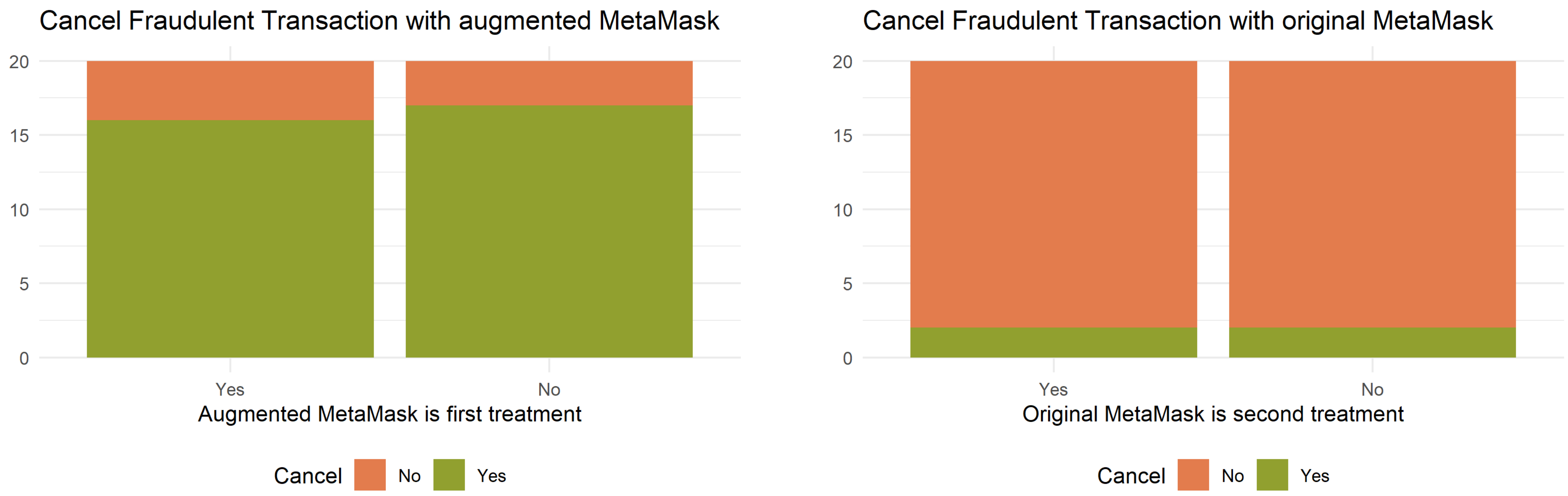
The link for this special offer is: https://greatcoin.io/SecondOffering

See you soon!

Alice

Usability Testing (4/5)

Results



Improved behaviour in the augmented MetaMask

This barplot omits the pairing of the data

Usability Testing (5/5)

Statistical Significance Testing: McNemar Test

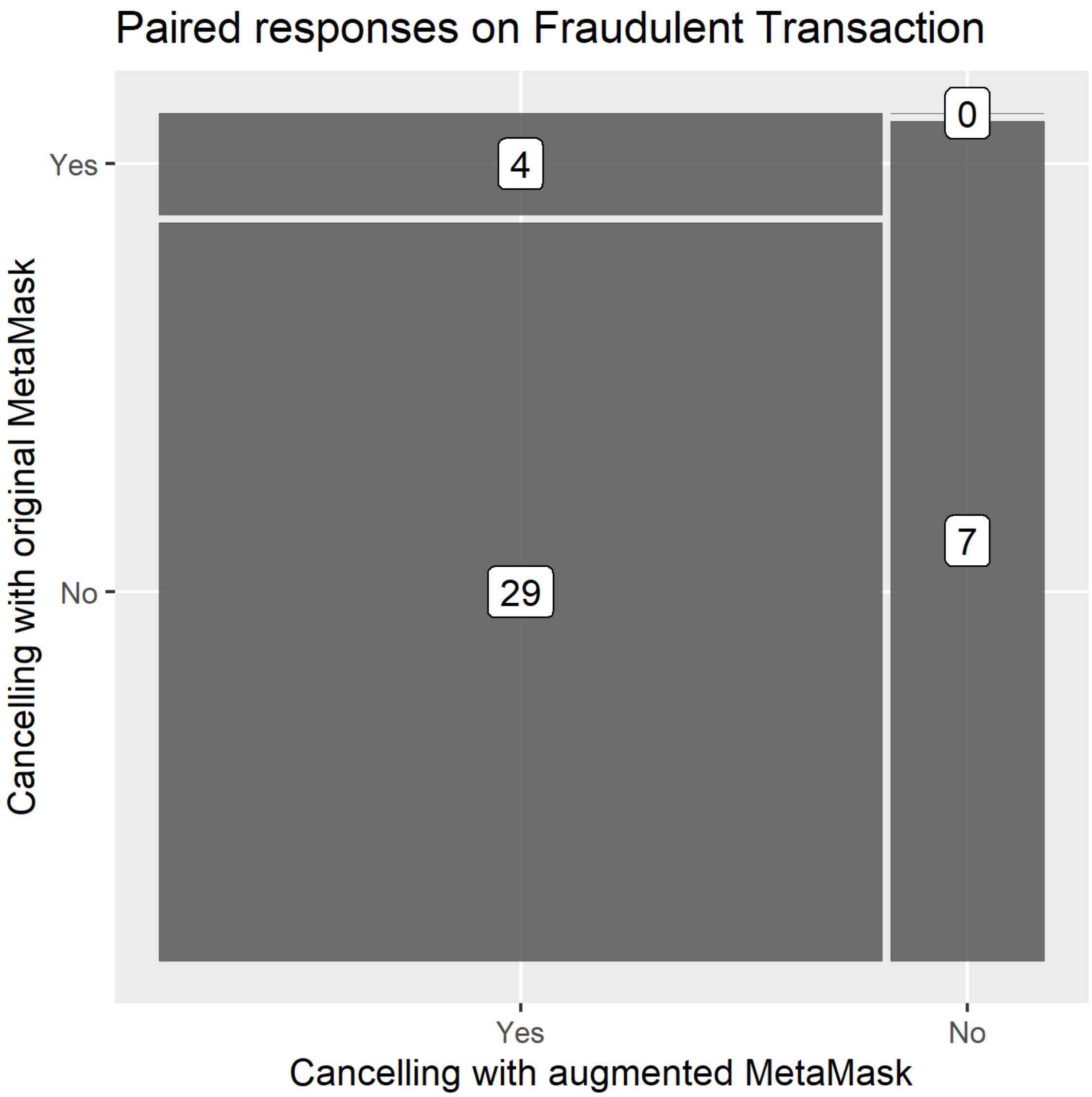
Paired cancel rate
The participant cancels the transaction in the original and in the augmented Metamask

McNemar Test
Tests relation of *discordant pairs* being close to 0.5

$$p = 1{,}862\ e^{-9}$$

We can reject the H_0 with a confidence level of $\alpha = 0.001$

We are confident that our solution enhances the user's security



Limitations and Further Work

Certificate Retrieval

- TeSC requires certificates for assertion
- Only Firefox supports access to Certificates

Solution is required for other Browsers

Use Case coverage in Experiment

- Scenario covers only one aspect of proposed verification algorithm
- External validity of experiment-based design

Field Studies could result in better performance

Browser as Design Reference

- Could not include Safari
- Efficiency of Browser‘s warnings unclear

Include other reference systems

Handling Protocol Downgrade

- No interruption on Downgrade
- 3 Participants do not get warned

Threat level analysis requires enhancement

Thank you for your Attention!
Any Questions?

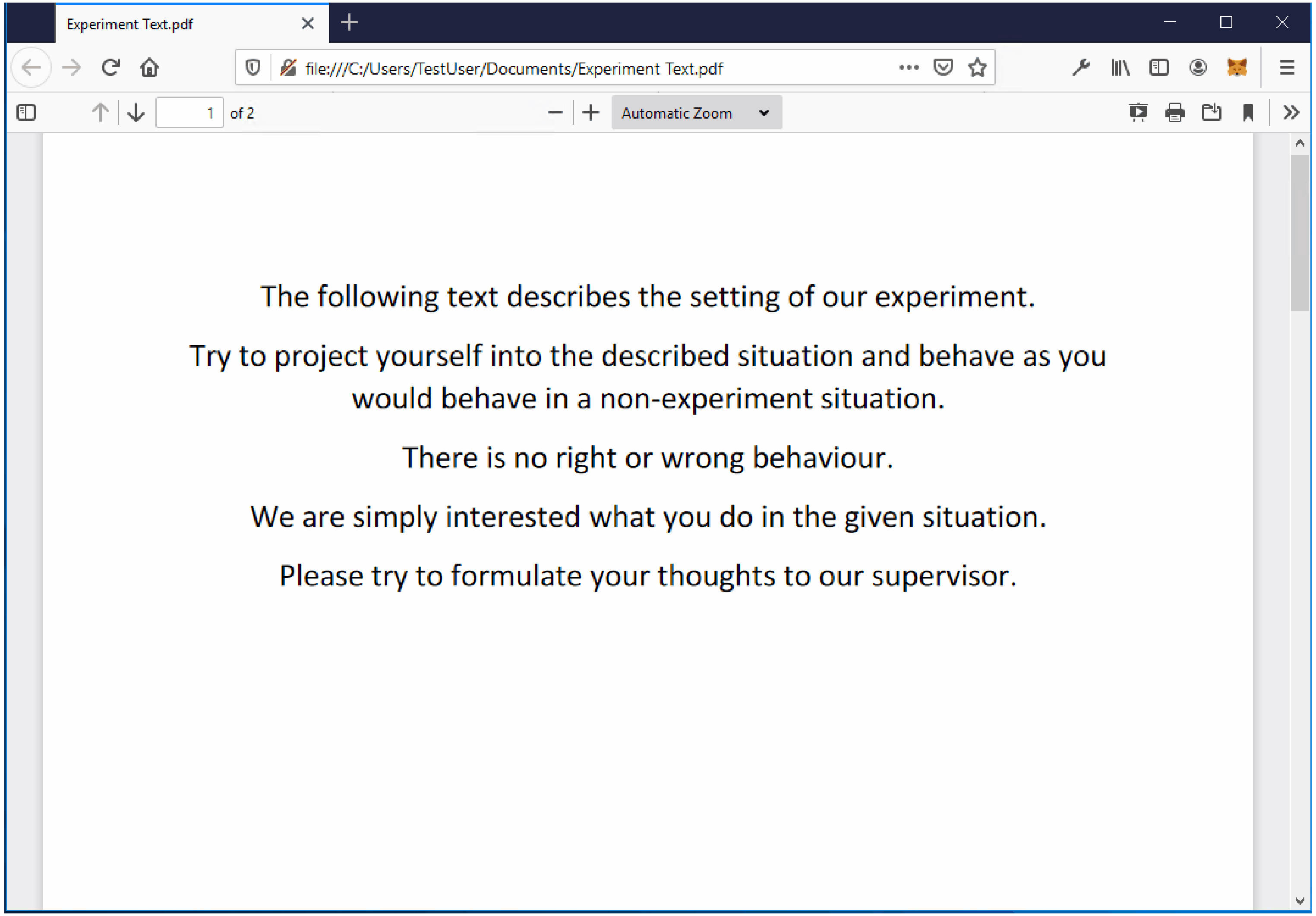
B.Sc.

Jonas Ebel

Student

jonas.ebel@tum.de

First Transaction



The following text describes the setting of our experiment.

Try to project yourself into the described situation and behave as you would behave in a non-experiment situation.

There is no right or wrong behaviour.

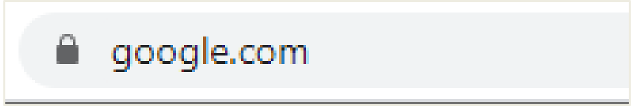
We are simply interested what you do in the given situation.

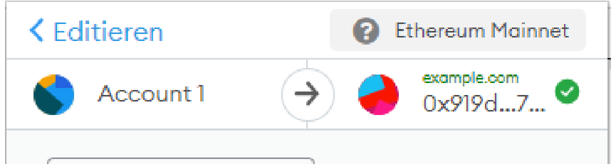
Please try to formulate your thoughts to our supervisor.

Design Concept Based on States

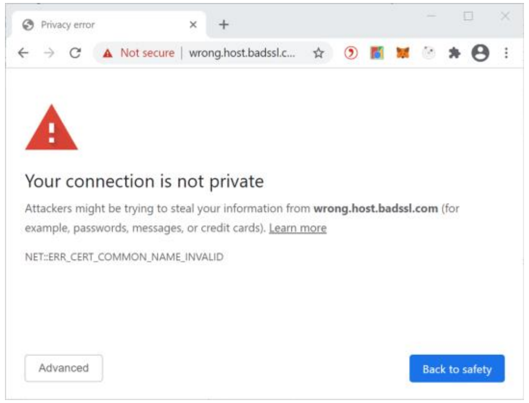
Browser | Augmented MetaMask

1. Authenticated





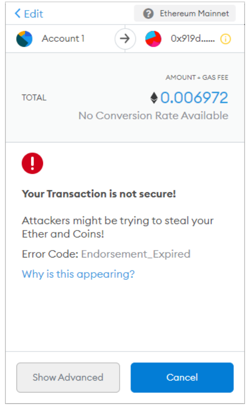
2. Critical Error



Your connection is not private

Attackers might be trying to steal your information from **wrong.host.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID



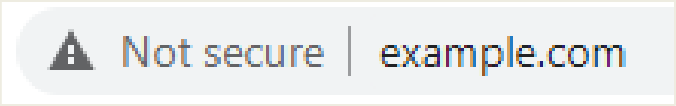
Your Transaction is not secure!

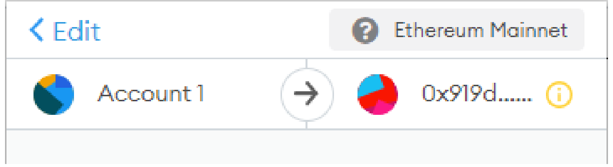
Attackers might be trying to steal your Ether and Coins!

Error Code: Endorsement_Expired

Why is this appearing?

3. Protocol Downgrade

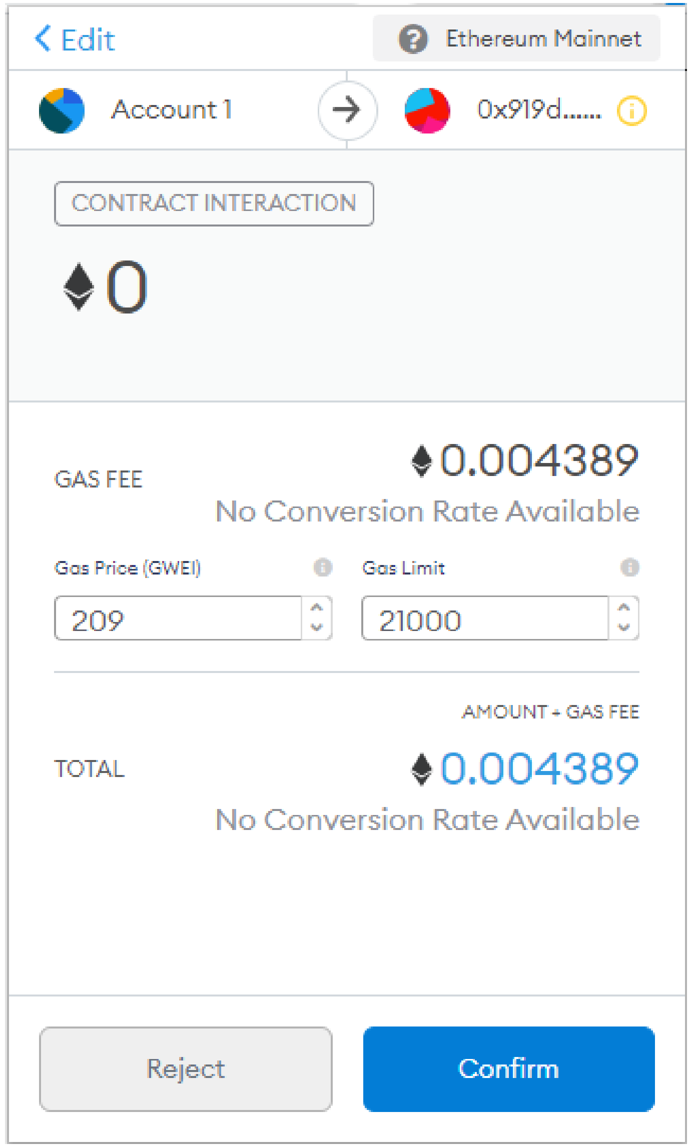




Design Concept (3/3)

Downgrade Indication

- Receiver does not comply with TeSC
- Frequently met due to low adoption of TeSC
- Browser-Parallel: HTTP Indication
- Users must check legitimacy of receiver themselves



GAS FEE 0.004389
No Conversion Rate Available

Gas Price (GWEI): 209
Gas Limit: 21000

AMOUNT + GAS FEE
TOTAL 0.004389
No Conversion Rate Available