Identitätsmanagement in Blockchain-basierten Systemen

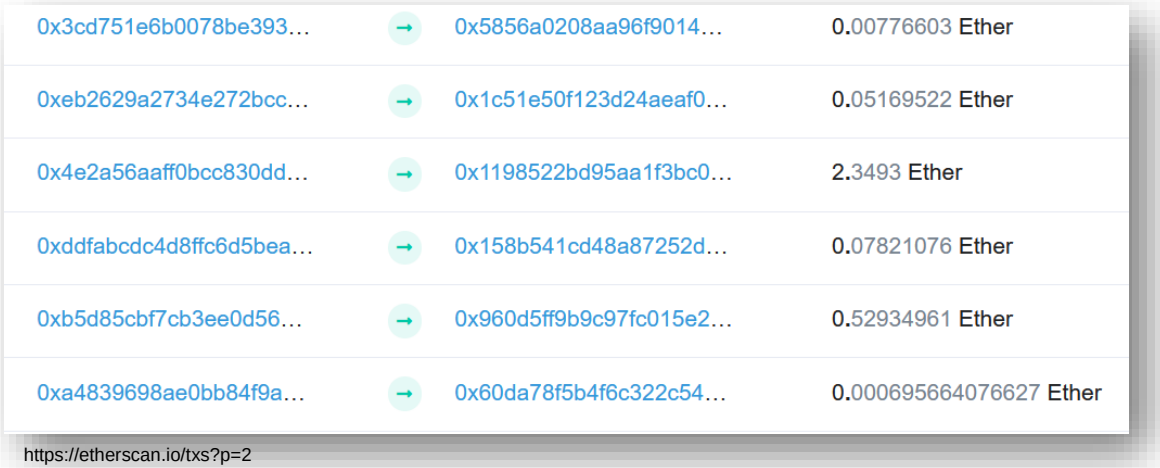
Sebis Day, 24.06.2021 – Ulrich Gallersdörfer

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Gliederung

1. Identitäten in Blockchain-basierten Systemen
2. TLS-endorsed Smart Contracts (TeSC)
3. Nutzungsmöglichkeiten
4. Integration Wallet (MetaMask)

Identitäten in Blockchain-Systemen sind pseudonym



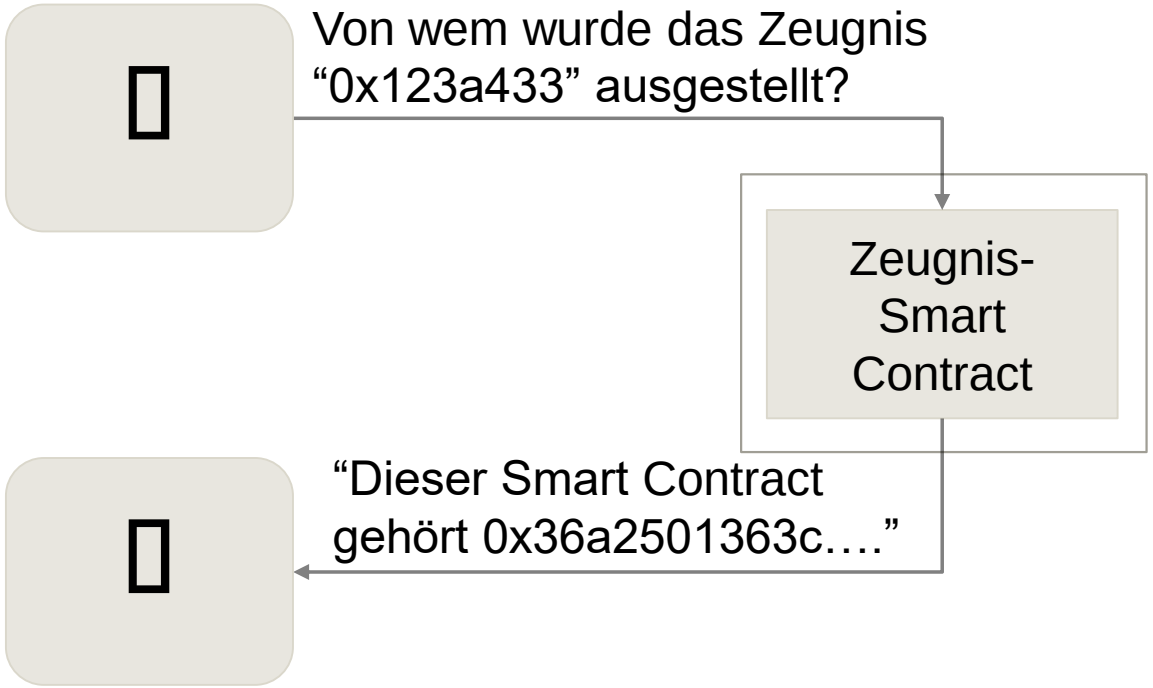
0x3cd751e6b0078be393…	→	0x5856a0208aa96f9014…	0.00776603 Ether
0xeb2629a2734e272bcc…	→	0x1c51e50f123d24aeaf0…	0.05169522 Ether
0x4e2a56aaff0bcc830dd…	→	0x1198522bd95aa1f3bc0…	2.3493 Ether
0xddfabcdc4d8ffc6d5bea…	→	0x158b541cd48a87252d…	0.07821076 Ether
0xb5d85cbf7cb3ee0d56…	→	0x960d5ff9b9c97fc015e2…	0.52934961 Ether
0xa4839698ae0bb84f9a…	→	0x60da78f5b4f6c322c54…	0.000695664076627 Ether

https://etherscan.io/txs?p=2

➔ **Beliebige Erzeugung** von Identitäten ist die Grundlage von dezentralen Systemen

Aber:
➔ Keine Limitierung
➔ Keine Zuordenbarkeit

Identitätsmanagement in Blockchain-Systemen ist nach wie vor wichtig.



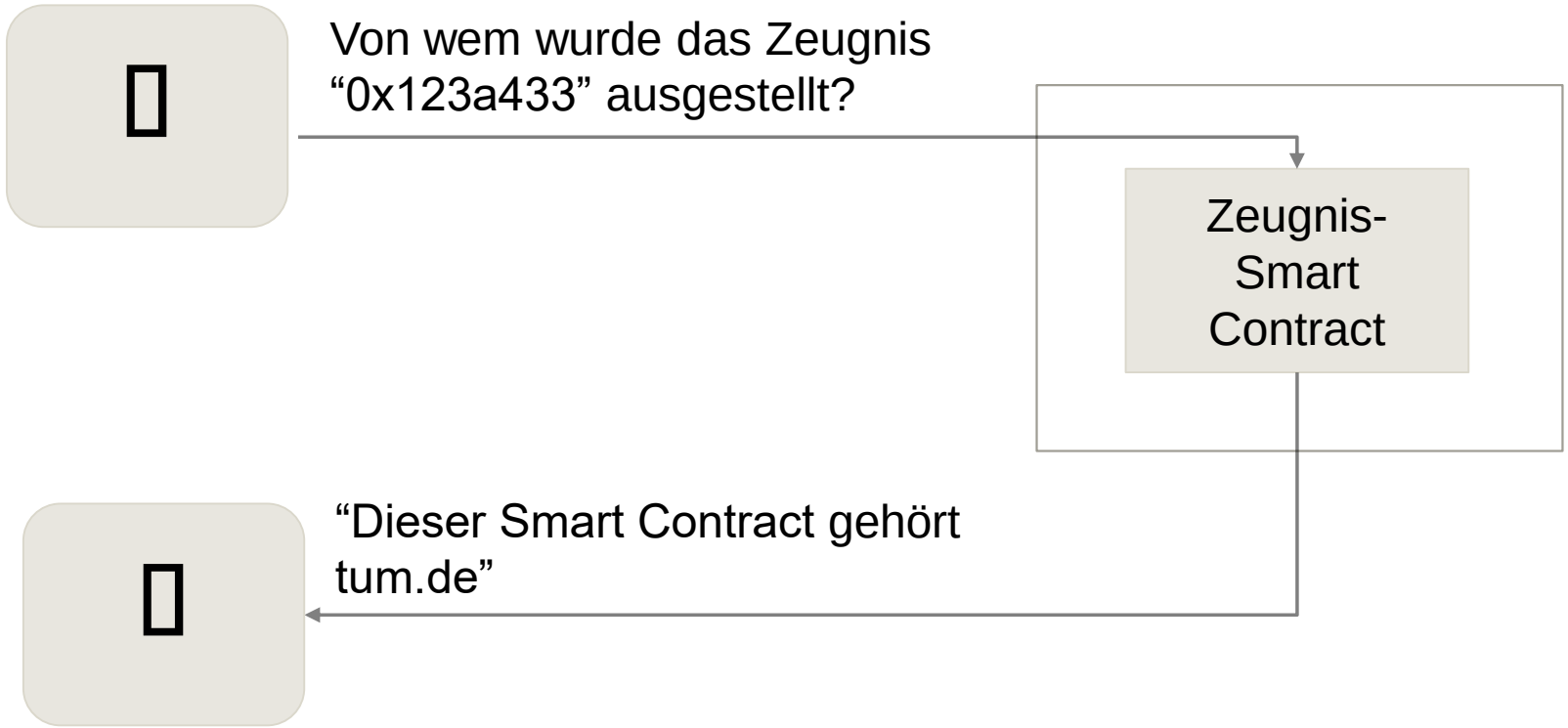
MyScore

RWTH AACHEN UNIVERSITY

DCC DIGITAL CREDENTIALS CONSORTIUM

Rethinking Communication in Web 3.0 / Blockchain environments

Die Authentisierung von Adressen und deren Besitzern ermöglichen eine neue Bandbreite an Applikationen und und fördert das Vertrauen in bereitgestellte Informationen und Dienste.

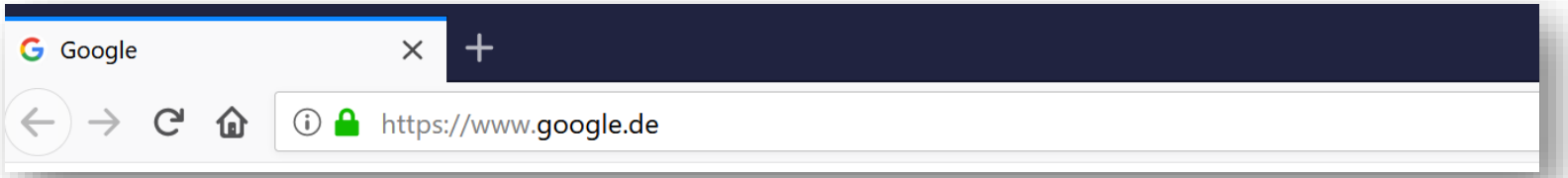


Gliederung

1. Identitäten in Blockchain-basierten Systemen
2. TLS-endorsed Smart Contracts (TeSC)
3. Nutzungsmöglichkeiten
4. Integration Wallet (MetaMask)

SSL/TLS-Zertifikate (X.509) bieten bereits digitale Identitäten

- Es gibt ein weltweit genutztes und anerkanntes System, Entitäten zu digital zu identifizieren.



Vorteile

Zusätzlich können wir Nachteile von SSL-Zertifikaten mit der Nutzung von Blockchain eliminieren bzw. mitigieren.

Bisherige Publikationen:

- Gallersdörfer, Ulrich, Groschupp, Friederike and Matthes, Florian: "**Mirroring Public Key Infrastructures to Blockchains for On-Chain Authentication**" in *5th Workshop on Trusted Smart Contracts In Association with Financial Cryptography 2021*
- Gallersdörfer, Ulrich and Matthes, Florian: "**TeSC: TLS/SSL-Certificate Endorsed Smart Contracts**" in *3rd IEEE International Conference on Decentralized Applications and Infrastructures*
- W3C DID-Method: DID-TLS

Gliederung

1. Identitäten in Blockchain-basierten Systemen
2. TLS-endorsed Smart Contracts (TeSC)
3. Nutzungsmöglichkeiten
4. Integration Wallet (MetaMask)

Nutzungsmöglichkeiten

MyScore

RWTH AACHEN UNIVERSITY

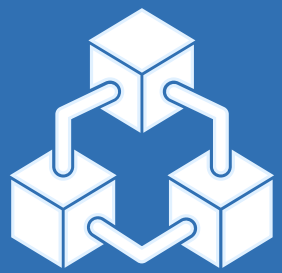
DCC DIGITAL CREDENTIALS CONSORTIUM

Data Authentication

Address-Replacement-Attacks

METAMASK

bloxberg



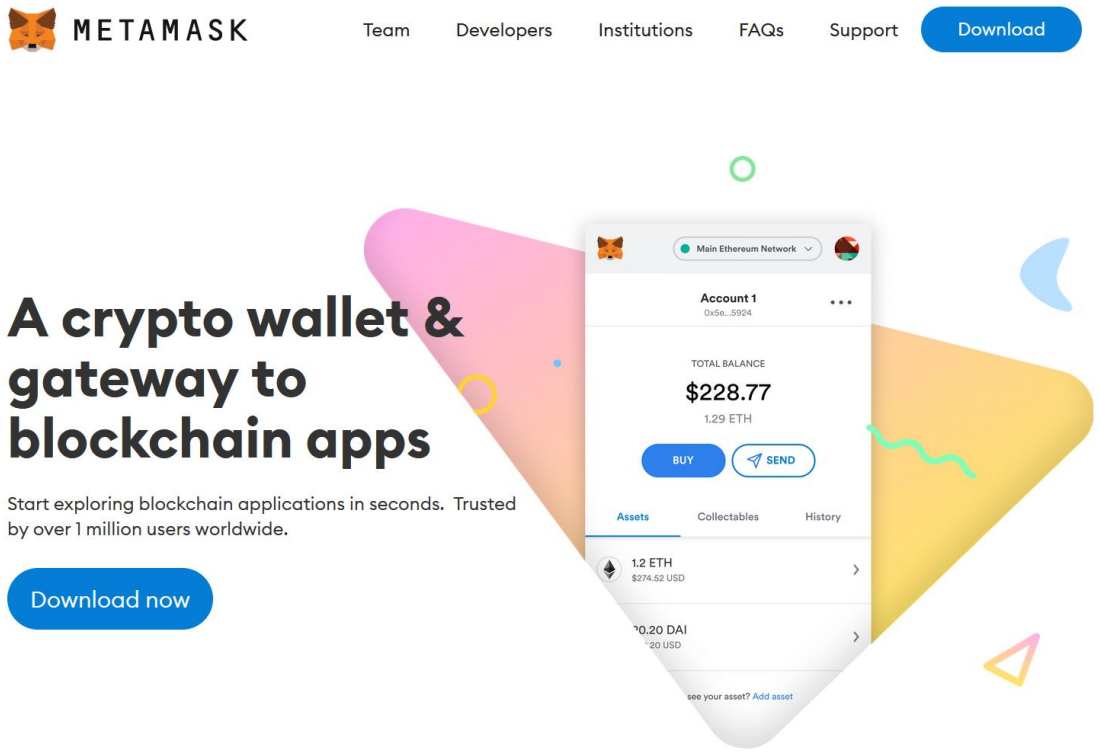
Consortia-Memberships

Access Control

Gliederung

1. Identitäten in Blockchain-basierten Systemen
2. TLS-endorsed Smart Contracts (TeSC)
3. Nutzungsmöglichkeiten
4. Integration Wallet (MetaMask)

Integration in MetaMask



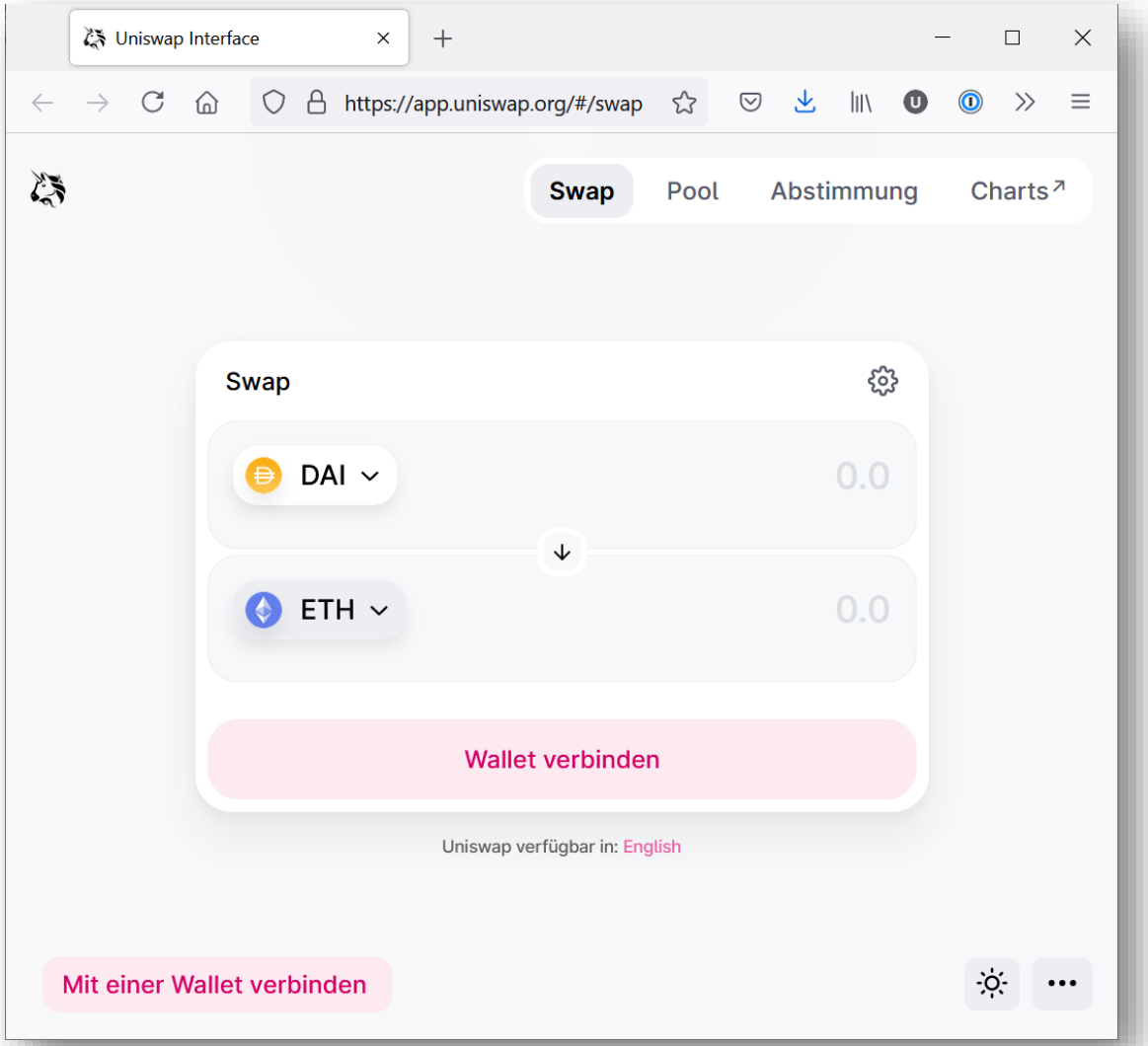
Address-Replacement-Attacks

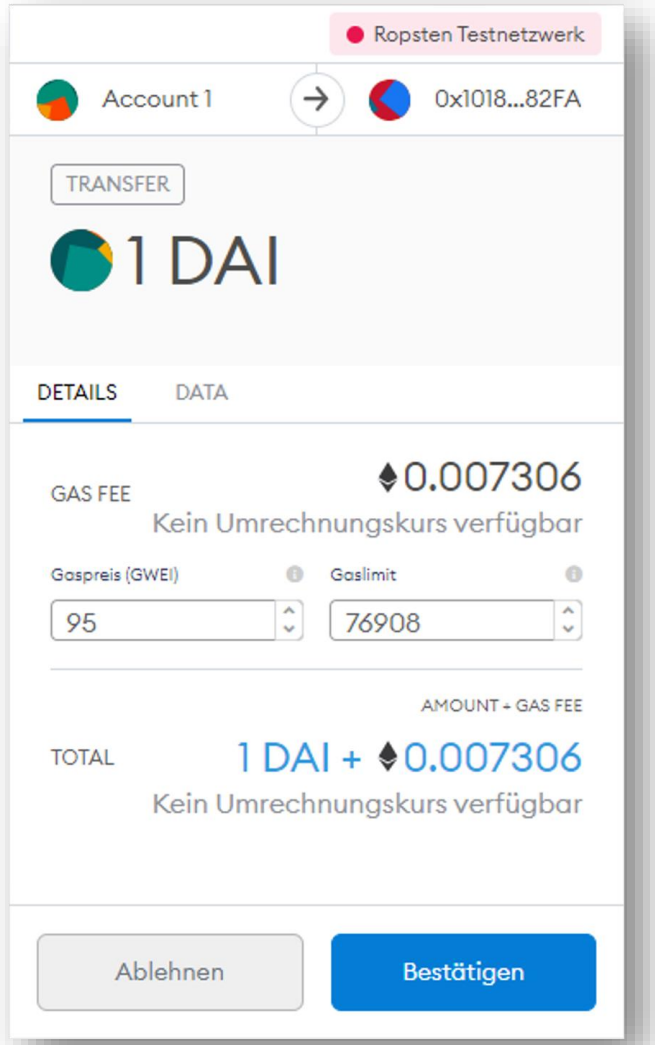
Integration in MetaMask:

➔ Webseite verlinkt / nutzt Smart Contracts

➔ Integration prüft, ob genutzte Adressen auch zum Anbieter gehören

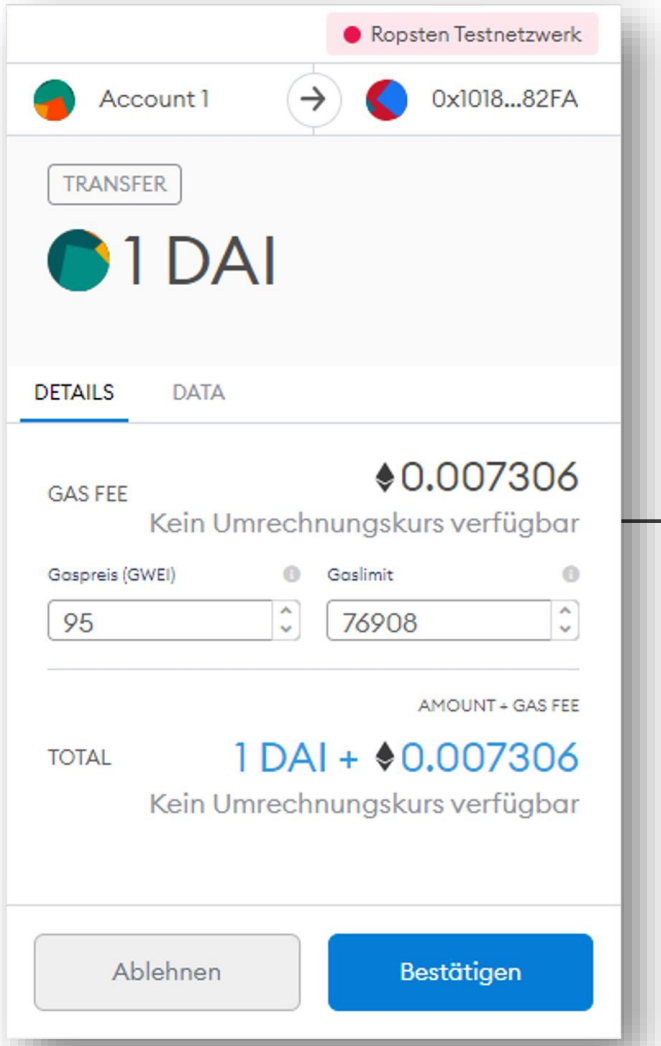
Integration in MetaMask (cont.)



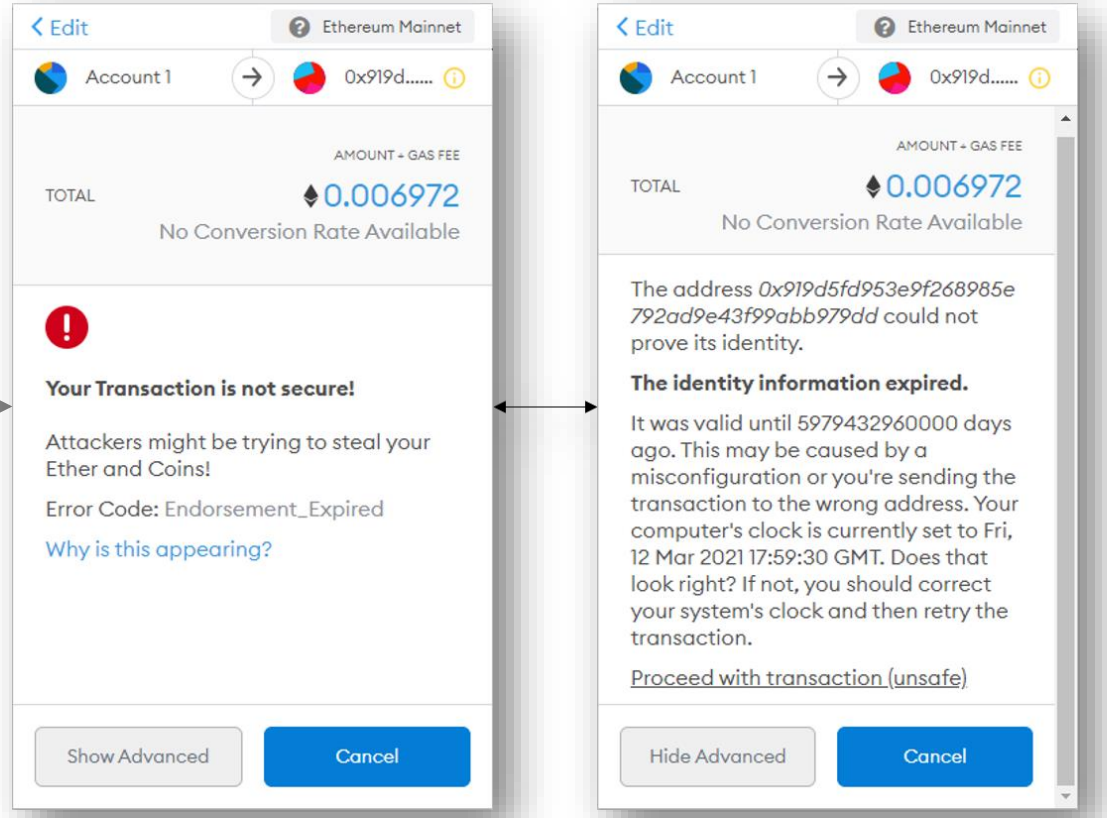


Original MetaMask

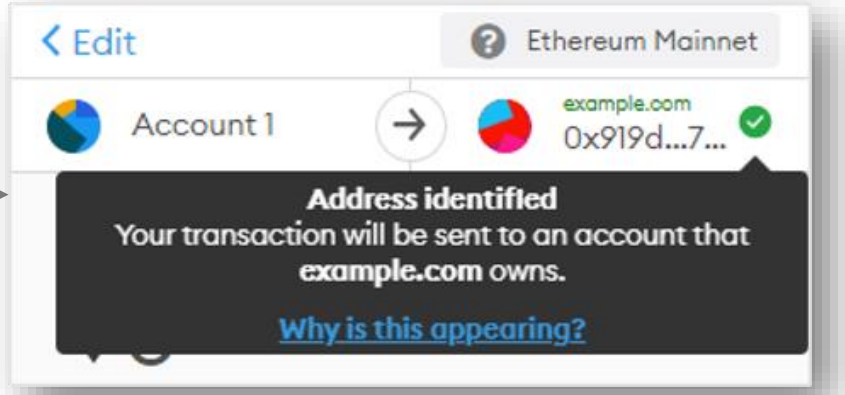
Integration in MetaMask (cont.)



Original MetaMask



Warning



Confirmed Identity

M.Sc.

Ulrich Gallersdörfer

Wissenschaftlicher Mitarbeiter

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.17137
Fax +49.89.289.17136

ulrich.gallersdoerfer@tum.de
wwwmatthes.in.tum.de