# Das Taler-Bezahlsystem

Stefan Kügel Christian Grothoff

29. November 2022

# 1 Das System im Überblick

## 1.1 Systembestandteile

GNU Taler ist ein offenes Protokoll für ein elektronisches Bezahlsystem mit einer Referenzimplementierung in freier Software (FLOSS). Taler bietet eine sichere, schnelle und einfache Zahlungsverarbeitung auf Grundlage langjährig bekannter und erprobter kryptografischer Algorithmen. Wichtige Designprinzipien sind die Verwendung Blinder Signaturen und die Asymmetrie von Privatheit und Transparenz: Auf der Seite der Zahlenden ermöglicht dies, anonym zu bleiben, wohingegen auf der Seite der Verkäufer alle Einkommen vor externen Auditoren wie z.B. Finanzämtern und Aufsichtsbehörden offengelegt und überprüfbar sind. Taler erfüllt die Gesetze gegen Geldwäschebekämpfung (Anti-Money-Laundering, AML), die Regulatorik über wirtschaftlich Berechtigte von Bankkonten (Know-Your-Customer, KYC) und Datenschutzverordnungen wie die DSGVO.

Das System besteht aus offenen Netzwerkprotokollen, Programmierschnittstellen in verschiedenen Sprachen und einer Hardware-Ausstattung zum Berechnen und Speichern von Daten. Fünf Bestandteile sind notwendig (in Klammern die Links zur jeweiligen Dokumentation):

1. Zentrale Steuerungslogik (Taler-Exchange) zum Verwalten sämtlicher Überweisungen zum und vom Exchange-Treuhandkonto
2. Elektronische Geldbörsen (Wallets) zum Verwalten der digitalen Münzen
3. Schnittstellen (LibEuFin-Komponente Nexus) zur Anbindung des Exchange-Treuhandkontos an das bestehende EBICS/FinTS-System
4. Anwendung für Verkäufer (Merchant-Backend) zum Einfordern und Verwalten von Umsätzen
5. Auditor-API (Auditor-Schnittstelle) zur laufenden Kontrolle der Funktionsweise aller Systembestandteile mit automatisch erstellten Prüfberichten

Die Funktionsweise erläutern neben diesem Dokument die Taler-Homepage (www.taler.net/de) und die englischsprachige Dokumentation (https://docs.taler.net/). Diskussionen werden auf der Mailingliste (https://lists.gnu.org/mailman/listinfo/taler) geführt.

Taler wird entwickelt von der Firma Taler Systems SA mit Sitz in Luxembourg, deren Entwickler zumeist in Deutschland und der Schweiz leben und arbeiten. Informationen zum Geschäftsmodell befinden sich auf Seite ??.

Die Prüfung der Codebasis, der verwendeten Signaturverfahren, der Transaktionen und Sicherheitsmaßnahmen erfolgte durch die Experten der Code Blau GmbH in Berlin, deren Prüfbericht im Juli 2020 nach eingehender Untersuchung erstellt wurde. Code Blau wird auch im laufenden Betrieb als unabhängiger Auditor das System kontrollieren.

Taler verwendet keine Blockchain- oder Distributed-Ledger-Technologie und ist selbst keine virtuelle Währung oder Kryptowährung. Die Werte der elektronischen Münzen in den Wallets der Nutzer sind in Euro denominiert, wenn sie von einem Taler-Exchange abheben, an den sie von einem Bankkonto in Euro überweisen. Ein Taler-Exchange, der andere Nominalwährungen als Euro (z.B. Dollar, Yen, Krypto-Coins, virtuelle Währungen und andere Token) blind signiert, kann nur diese in die Wallets abheben lassen.

## 1.2 Funktionsweise

Der Taler-Exchange (im weiteren Text: Exchange) ist die zentrale Steuerungslogik. Ein auf Fiatwährungen basierender Exchange verwaltet einerseits die Buchungen zwischen den KYC-geprüften Girokonten von Käufern bzw. Verkäufern und seinem Treuhandkonto (die „Reserve“), andererseits die Buchungen der Transaktionen zwischen seinem Treuhandkonto und den Wallets der Nutzer. Die beiden jeweiligen Buchungsströme werden vom Exchange koordiniert. Exchange-Betreiber können Banken, Zentralbanken, private Zahlungsdienstleister oder auch Anbieter von Regionalwährungen sein. Mit Taler transferierte Euro-Gelder bleiben stets im SEPA-Bereich und fließen nur vom Girokonto der Zahlenden über das Treuhandkonto des Exchange-Betreibers auf die Girokonten der Verkäufer.

Ein Wallet kann man sich vorstellen als eine Debit- oder Prepaid-Geldbörse: Ein digitales Pendant zu einer Geldbörse, die statt Scheinen und Münzen sogenannte Token enthält (im weiteren Text als Coins bezeichnet). Dies sind kryptografisch signierte „Münzen“, die wie Bargeld keinen identifizierenden Rückschluss auf ihre Eigentümer gestatten. Coins im Taler-System stellen elektronische Repräsentanten des Geldes dar, das von den Nutzern auf das Treuhandkonto des Exchange-Betreibers überwiesen wurde. Taler ist somit ein Prepaid-System, eine Kreditvergabe hierüber ist ausgeschlossen.

Externe Auditoren werden im laufenden Betrieb automatisch über die Transaktionen des Exchange informiert und können im Fall von Unstimmigkeiten zeitnah reagieren.

Die Nutzer des Taler-Bezahlsystems sollten ihre Coins wie Bargeld behandeln, das heißt sie dem entsprechend auch sichern. Die Daten eines Wallets mit seinen Coins können auf beliebig vielen digitalen Endgeräten und Speichermedien abgelegt und gesichert werden. Taler-Wallets verfügen über ein eingebautes Backup-Verfahren, mit dem sie die Wallet-Daten bei unabhängigen Dienstleistern sicher abspeichern können. Die Nutzer bezahlen mit den Coins, können deren Werte aber auch wieder auf ihr ursprüngliches Girokonto zurückgeben lassen, indem sie im Wallet eine Rückbuchung durch den Exchange auslösen, den sie zum Signieren und Abheben der Coins wählten. Falls sie kein Backup ihrer Wallet-Daten angelegt haben, können sie die Coins auch verlieren.

Die Coins in einem Wallet entsprechen rechtlich einem Eigentumswert im Zugriffsbereich der Wallet-Besitzer, während Exchange-Betreiber deren Wert in der Ursprungswährung treuhänderisch verwahren. Exchange-Betreiber haben ein Zahlungsversprechen gegenüber den Wallet-Besitzern, wenn diese bei Bezahlvorgängen ihre Coins einsetzen, und verantworten die Überweisung der realen Geldwerte an die Girokonten der Verkäufer bei deren Geschäftsbanken.

Die Nutzung eines Wallets beim Zahlen in Euro-Währung gestaltet sich folgendermaßen: Wallet-Besitzer bestimmen zuerst im Wallet den gewünschten Betrag zur Abhebung und

wählen einen Exchange, der Euro anbietet, und überweisen dann den Abhebebetrag von einem regulären KYC-geprüften Girokonto auf das Treuhandkonto des Exchange-Betreibers. Dies entspricht einer normalen Euro-Überweisung zwischen zwei IBAN-Konten im SEPA-Raum (IBAN-Buchung). Der Exchange erlaubt dem Wallet nach Eingang des Überweisungsbetrags das Abheben von Coins des entsprechenden Betrags in Euro. Bezahlt werden kann mit diesen Coins in Webshops, an Automaten und bei allen Verkaufsstellen, die am Point of Sale (POS) den Vertragsschluss mit Taler erlauben.

Die Verkäufer brauchen kein Wallet, um Einzahlungen auf ihren Girokonten zu empfangen, sondern ein Merchant-Backend des Taler-Systems: Webshops benötigen das Software-Modul Taler Merchant, Automaten und POS-Kassensysteme verwenden das Taler Point-of-Sale-Terminal und für Abhebungen und Zahlungen über eine NFC-Schnittstelle muss die NFC-Schnittstelle installiert werden. Die Verkäufer können ihre Umsätze mittels einer Backoffice-Anwendung konfigurieren und verwalten.

Der kryptografisch signierte Vertrag enthält die Vertragsbedingungen zwischen Käufer und Verkäufer und ist für eventuelle Streitfälle auch vor Gericht verwendbar als Beleg über den Kauf der Waren zum gegebenen Kaufpreis. Signiert wird mit dem privaten Schlüssel des jeweiligen Wallets.

Die Coins annehmenden Verkäufer müssen davon ausgehen, dass ihre Umsätze aus dem Taler-System schon allein durch die IBAN-Buchung ihrer Einnahmen auf ihre Girokonten bei Geschäftsbanken als Einkommen leicht nachvollziehbar sind. Zusätzlich dazu sollten sie sich der Rolle der externen Auditoren bewusst sein. Unregelmäßigkeiten würden diese den Finanzbehörden melden. Darüber hinaus veranlasst das System in einem automatisierten Verfahren, dass die Verkäufer bestimmte Vorgänge bei einem Auditor melden, um diesen in seiner Kontrollfunktion oder in einer spezifischen Aufsichtsfunktion zu unterstützen.

Dadurch bewirkt Taler zum einen, dass der Identitätsschutz der Käufer gewahrt bleibt, zum anderen wird eine Bemessungsgrundlage für die Steuererhebung geschaffen, was den Einsatz für illegale Geschäfte oder Steuerhinterziehung verhindert. Aufgrund der unterschiedlichen Behandlung der Geldströme auf Käufer- bzw. Verkäuferseite erfüllt Taler sowohl die Anforderungen der Gesetze zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung als auch die Gesetze zum Schutz privater Daten einschließlich der Datenschutzgrundverordnung (DSGVO). Gleichzeitig erhalten die Finanzbehörden eine elektronische Datenbasis zur vereinfachten Steuererhebung für die Finanzierung unseres staatlichen und kommunalen Gemeinwesens.

Für Waren und Dienstleistungen, deren Bezahlung ein bestimmtes Mindestalter voraussetzt, können Taler-Coins mit dem Attribut einer Altersangabe ins Taler-Wallet abgehoben wurden. Kinder, Jugendliche und Schutzbefohlene verwenden diese Coins als digitales Bargeld, ohne dass Exchange-Betreiber oder Verkäufer sie als Minderjährige oder Mündel identifizieren können. Es besteht keine technische Möglichkeit eines Rückschlusses auf die Coin-Besitzer und deren tatsächliches Alter. Kapitel 3 erläutert die Details zu Coins mit Altersbeschränkung.

Glossar und Begriffsbestimmungen am Ende dieses Dokuments ergänzen das Glossar in englischer Sprache (docs.taler.net/developers-manual.html#developer-glossary) sowie wissenschaftliche Publikationen zum Taler-System auf taler.net/en/bibliography.html.

# 2 Geschäftsvorgänge

Dieses Kapitel widmet sich den Geschäftsvorgängen im Taler-System und dem Einkommensnachweis von Verkäufern. Beschrieben werden hier die grundlegenden Verfahren:

- Abhebevorgang (Buchungsart *Withdrawal*)
- Ausgabe- und Bezahlvorgang (Buchungsart *Deposit*)
- Wechselgeld erhalten und Gültigkeit von Coins verlängern (Buchungsart *Refresh*)
- Rückerstattungen (Buchungsart *Refund*)
- Marktaustritt von Exchange-Betreibern (Buchungsart *Recoup*)

## 2.1 Abhebevorgang (*Withdrawal*)

Der Abhebevorgang wird im Taler-Wallet ausgelöst. Technisch möglich sind Abhebevorgänge mittels Geschäftsbank-Webseiten (Onlinebanking), per Einzahlung am Bankschalter und Abheben ins Wallet, mittels manueller Banküberweisung durch die Nutzer, Übertragung von Coins von einem anderen Taler-Wallet (peer-to-peer) sowie durch die webbasierte Buchung mithilfe einer Browser-Erweiterung. Weitere Implementierungen (z.B. das Abheben an einem Geldautomaten) sind angedacht oder bereits in Entwicklung. Einen speziellen Abhebevorgang stellt das sogenannte „Tipping“ (Aufwandsentschädigung an Nutzer durch Webseiten) dar.

In Kapitel 9 veranschaulichen Screenshots die einzelnen Schritte des Abhebe- und Ausgabevorgangs sowie des Abhebevorgangs auf das Smartphone-basierte Wallet mit „Taler-Cashier“ als ATM (Automated Teller Machine, Geldautomat mit Einzahlfunktion), gefolgt von Screenshots des Bezahlvorgangs mit der POS-Anwendung „Merchant POS“.

Drei Methoden, um Coins in ein Taler-Wallet abzuheben, werden hier detailliert beschrieben:

- A1 Abhebevorgang vom Girokonto
- A2 Manuelle Überweisung
- A3 Tipping von Webseiten als geringwertige Aufwandsentschädigung
- A4 peer-to-peer von einem Absender-Wallet zu einem Empfänger-Wallet (pay-push-Verfahren)

### 2.1.1 Abhebevorgang vom Girokonto (A1)

Geschäftsbanken, die ihren Kunden das Abheben in Taler-Wallets erlauben wollen, müssen an ihren Kundenschnittstellen (Onlinebanking, Bankschalter, Smartphone-Apps) Taler als Aufladeverfahren anbieten. Die anderen Abhebevorgänge (A2, A3) brauchen im Gegensatz dazu keine Schnittstellen zu Taler bei den Banken, von denen die Nutzer auf das Konto des Exchange-Betreibers überweisen.

Der Abhebevorgang umfasst folgende Verfahrensschritte:

1. Der Abhebevorgang beginnt immer mit der Anmeldung eines Wallet-Besitzers bei seiner Geschäftsbank mittels Zwei-Faktor-Authentifizierung (Eingabe von Kennung bzw. Einführen von Karte und PIN-Eingabe), bei ATM-Terminals (Geldautomaten) erfolgt die PIN-Eingabe später (siehe unten Punkt 6).

2. Zum gegenwärtigen Stand der Entwicklung können Nutzer folgende Abhebeverfahren auswählen:

   a) Smartphone-Scan des QR-Codes auf der Bank-Webseite
   ➔ Die Bank erzeugt einen QR-Code, den der Nutzer mit einem Smartphone einliest (Android, iOS)

   b) Abheben in das Taler-Wallet als Browser-Erweiterung in Firefox, Opera oder Chrome/Chromium
   ➔ Das Wallet in der Browser-Erweiterung zeigt den abzuhebenden Betrag an, den der Nutzer mit dem Klick auf einen Button bestätigt

   c) NFC-Read oder Smartphone-Scan an Bankschaltern bzw. Geldautomaten
   ➔ Die NFC-Schnittstelle zeigt den Betrag an bzw. der QR-Code wird mit dem Smartphone eingelesen

   d) Smartphone-Scan mit Bargeldeinzahlung an einer Kasse mittels App „Taler-Cashier“
   ➔ Die Cashier-App auf dem Gerät des Kassierers erzeugt einen QR-Code, den der Nutzer mit seinem Android-Smartphone einliest

   Der Nutzer wählt das Verfahren und gibt die Geldmenge ein, die später vom persönlichen Wallet als Coins abgehoben werden soll.

3. Mit der so erhaltenen Information stellt das Wallet eine Anfrage bei der Bank und erfährt damit von der Verfügbarkeit des vom Kunden gewünschten Betrags in der gegebenen Währung auf dessen Girokonto. Daraufhin öffnet das Wallet einen Dialog, um dem Nutzer die Auswahl des Exchange-Betreibers zu ermöglichen.

4. Der Nutzer wählt den Exchange. Falls der Nutzer neu ist, einen neuen Exchange wählen will oder sich die Allgemeinen Geschäftsbedingungen (AGB) des bisherigen Exchange-Betreibers geändert haben, werden dem Nutzer die AGB angezeigt, die er bestätigen muss. Gleichfalls werden die allgemeine Gebührenordnung des Taler-Bezahlsystems sowie die spezifischen Gebühren für den aktuellen Abhebevorgang angezeigt.

5. Im gleichen Dialog kann der Nutzer eine ggf. gewünschte Altersstufe mit Bandbreiten von zwei Lebensjahren (z.B. ab 8, 10, 12, 14 oder ab 16 Jahre) als Attribut der abzuhebenden Coins wählen. Das Altersattribut kann von einem Erziehungsberechtigten oder Vormund gewählt werden, um Coins mit einer Altersbeschränkung in das Wallet eines Minderjährigen oder Mündels abheben zu lassen. Falls die Überweisung von einem für den Taler-Exchange erkennbaren Jugendgirokonto stammt, kann dieser Exchange ebenfalls eine Altersobergrenze setzen.

6. Wenn der Nutzer den Vorgang bestätigt, erzeugt das Wallet mit dem EdDSA-Kryptografieverfahren frische Credentials (Zugangsberechtigung) für den Abhebevorgang und teilt der Bank den öffentlichen Schlüssel (Public key) der Credentials mit. Der Nutzer wird auf die Benutzerführung der Bank-Webseite bzw. des ATM-Terminals zurückverwiesen.

7. Der Nutzer bekommt dort nochmals den Betrag und den gewählten Exchange angezeigt und muss gegenüber der Bank endgültig bestätigen, dass der Überweisungs- und Abhebevorgang nun ausgelöst werden soll. Der Überweisungsvorgang kann mit und ohne Authentifizierung erfolgen:

   a) Ohne TAN-Eingabe im Fall von Beträgen unterhalb eines von der Bank festgelegten Limits: Gemäß *Payment Services Directive 2* (PSD2) kann die Obergrenze des Transaktionsbetrags pro Vorgang ohne TAN-Autorisierung 50 Euro betragen, allerdings nur fünfmal hintereinander oder bis ein weiteres Kann-Limit von 150 Euro Umsatz in Summe erreicht wird[1].

   b) Mit einer Zwei-Faktor-Authentifizierung (mTAN, photoTAN, Karten-PIN bei ATM-Terminals o.ä.) als finaler Autorisierung der Buchung durch den Nutzer.

   Die Bank überweist den Betrag vom Girokonto an den gewählten Exchange unter Angabe des vom Wallet erzeugten Public key, der auch als Buchungsvermerk (bzw. Verwendungszweck oder „Subject“)[2] im Girokontoauszug des Nutzers erscheint. Damit ist jeder Aufladevorgang mit den betreffenden Geldwerten und Zeitpunkten eindeutig zuzuordnen und erfüllt die KYC-Regulatorik, denn der wirtschaftliche Berechtigte des Girokontos ist der Bank bekannt. Mit dem Verfahren SEPA Instant Credit Transfer (SCT Inst) erfolgt die Überweisung in Echtzeit und das Wallet kann die Coins sofort abheben, eine normale SEPA-Überweisung benötigt hingegen ca. einen Banktag und dem auch entsprechend der Abhebevorgang.

8. Zum Abheben verwendet das Wallet die Credentials, die es vorher erzeugt hat. Der Public key dient zum Prüfen der korrekten Verbindung zwischen Wallet und Exchange. Damit wird in der Datenbank des gewählten Exchange eine Reserve über den Betrag der eingegangenen Girokontoüberweisung erzeugt, aus welcher das empfangende Wallet die vom Exchange blind signierten Coins abheben kann.

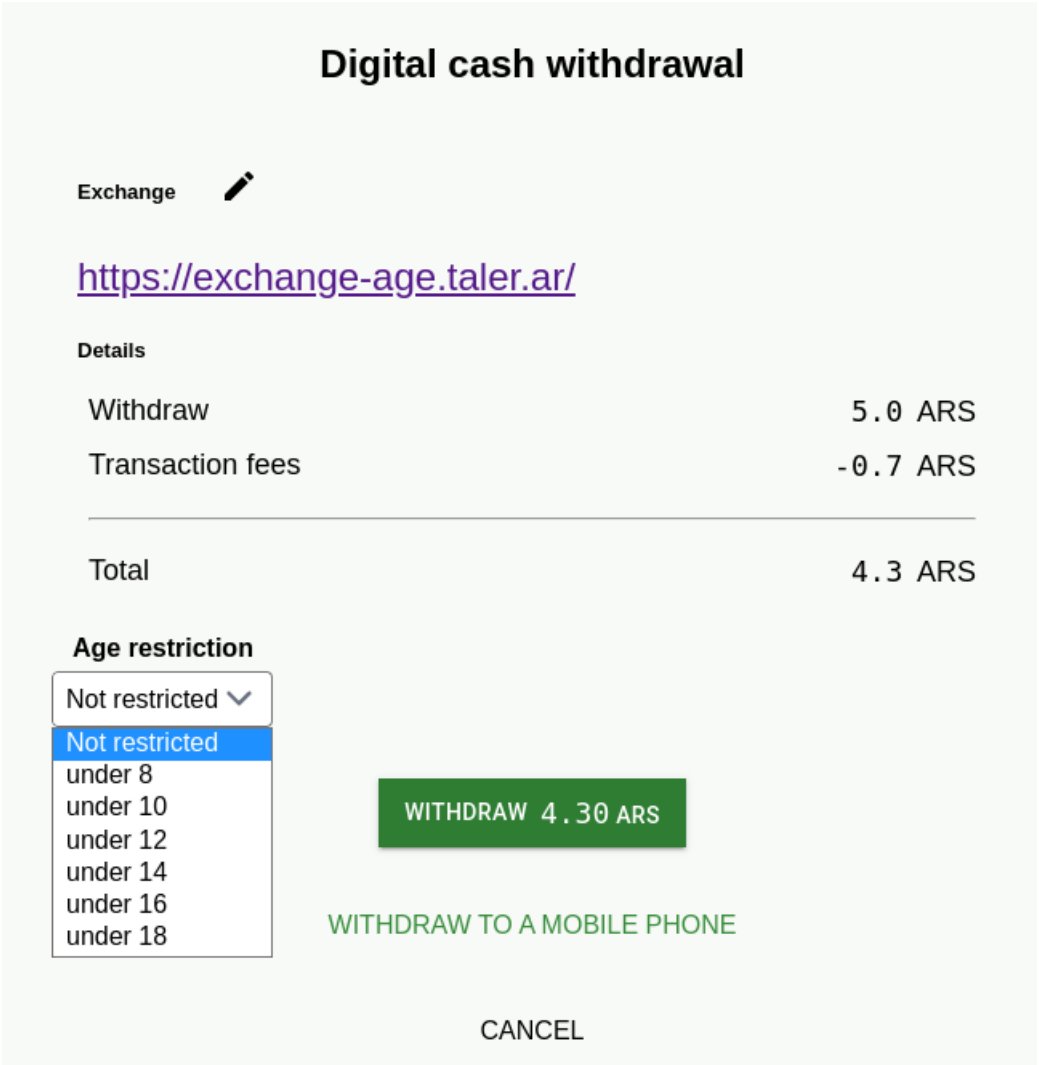
---

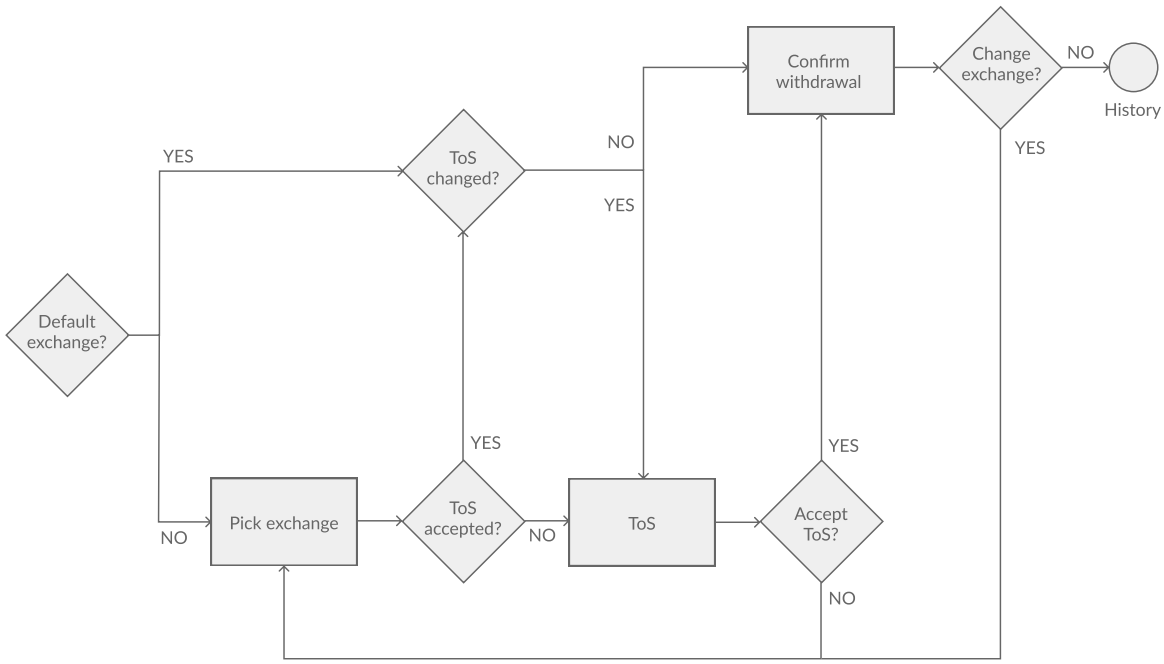
1 Siehe BaFin-Fachartikel Starke Kundenauthentifizierung

2 Der Buchungsvermerk ist eine alphanumerische Zeichenkette, die als im Kontoauszug erscheint, kann beispielsweise lauten: A63HRJCBD74FZ70EJGY0V81YNM8S3B4F36S35RGMSZ6DCV5PN1DG

9. Das Zeitfenster für den Abhebevorgang wird als Closing Time bezeichnet und beträgt 14 Tage. Dieser Zeitraum sollte für Nutzer normalerweise ausreichen, um den Vorgang abschließen zu können. Er sollte auch nicht zu lang sein, damit die Kunden bei eventuellen Problemen nicht zu lange auf ihre Rücküberweisungen warten müssen. Sollte das Wallet den Abhebevorgang nicht zu ende führen (z.B. weil der Nutzer es versäumt, das Wallet mit dem Internet verbinden zu lassen), schließt der Exchange die Reserve automatisch wieder und überweist den Betrag (abzüglich der Closing-Gebühr) auf das ursprüngliche Konto zurück.

Die nachfolgenden Grafiken zeigen den Nutzerdialog und die Benutzerführung bei der Wahl des Exchange und der Altersrestriktion auf die abzuhebenden Taler-Coins vor dem Abhebevorgang (Verfahrensschritte 4 und 5):






### 2.1.2 Manuelle Überweisung (A2)

Die manuelle Überweisung besteht für den Fall, dass Taler-Nutzer von Girokonten abheben wollen, deren kontoführende Geschäftsbank Taler (noch) nicht unterstützt. Sie müssen hierfür den gewünschten Betrag mittels konventioneller Girobuchung an einen Exchange überweisen, von dem ihre Wallets dann den Betrag automatisch abheben (wie zuvor unter Punkt 7 beschrieben). Die Wallet-Software liefert ihnen dazu die Überweisungsdaten, die sie einfach in ein Überweisungsformular von Hand oder mit dem vom Wallet erzeugten QR-Code übertragen:

1. Der Nutzer gibt den gewünschten Aufladebetrag im Wallet ein und wählt den Exchange.
2. Das Wallet erzeugt die Credentials und zeigt sie zusammen mit der Bankverbindung des gewählten Exchange an.
3. Diese Daten werden in die Felder des Überweisungsformulars für eine SEPA-Überweisung vom Girokonto auf den Exchange übertragen (manuell oder mit dem QR-Code als payto://-URI für Banking-Anwendungen).
4. Sobald die Überweisung beim Exchange angekommen ist, hebt das Wallet die Coins des Aufladebetrags ab.

### 2.1.3 Tipping (A3)

Tipping ist eine geringfügige Aufwandsentschädigung von Webseiten an ihre Besucher. Webseiten können dies nutzen, um Besucher für das Betrachten von Werbung oder die Preisgabe von Daten zu belohnen z.B. Kundenrezensionen oder Bewertungen gekaufter Artikel. Den Nutzern bietet man damit einen Anreiz in Form eines Kleinstbetrags, der auf ihre Taler-Wallets gebucht wird. Dazu erzeugt die Webseite für das Wallet ein Token, durch welches das Wallet einen auf den Geldwert begrenzten Zugriff auf eine Reserve bekommt, die der Webseiten-Betreiber bei einem Exchange seiner Wahl zuvor angelegt hat. Der Vorgang verlangt dann nur noch eine einfache Bestätigung durch die Webseiten-Besucher, mit der ihre Wallets die Coins aus dieser Reserve abheben können.

### 2.1.4 peer-to-peer (A4)

Taler-Coins können aus dem Wallet eines beliebigen Teilnehmers an das Wallet eines anderen Teilnehmers gesendet werden, ggf. mit einem Altersattribut versehen auch an Minderjährige oder Mündel. Bei diesem Verfahren findet zwangsläufig eine KYC-Prüfung des Empfängers durch den Taler-Exchange statt. Wenn Erwachsene Geld an Minderjährige schicken, wird eine Altersrestriktion eingeführt, und wenn Minderjährige oder Mündel Geld an Erwachsene senden, wird die Altersrestriktion aufgehoben.

Der Exchange stellt dem Empfänger-Wallet frische Coins mit der vormals gewählten Altersrestriktion aus. Wenn jedoch ein Exchange alte und neue Token in Bezug setzen könnte, wäre kein datenschutzfreundliches Bezahlen möglich. Das Refresh-Protokoll des Taler-Systems verwendet daher die sog. Cut-and-choose-Methode, um die Nichtverfolgbarkeit frisch signierten Token aufrechtzuerhalten (siehe Abschnitt 4.7.4 in der PhD-Thesis von Florian Dold).

## 2.2 Ausgabe- und Bezahlvorgang (*Deposit*)

Genauso wie den Abhebevorgang steuert die Software des Exchange im Zusammenspiel mit der Wallet-Software auch den Ausgabevorgang, das Bezahlen mit Coins. Dreh- und Angelpunkt aller Ausgabevorgänge ist also auch hier der Taler-Exchange.

Mit den Coins verfügen die Wallet-Besitzer über elektronische Repräsentanten der Geldwerte, die der beim Abhebevorgang gewählte Exchange auf seinem Treuhandkonto vorhält. Kommt es zur Zahlung mit Coins, werden die Geldwerte vom Treuhandkonto an die empfangenden Girokonten der Verkäufer weitergebucht.

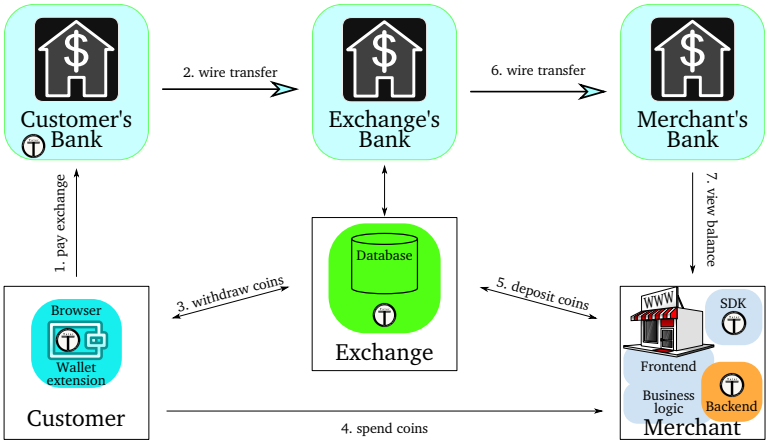
Wird ein Coin ausgegeben, ist das Coin entwertet. Wer es zuerst ausgibt, verfügt über den Geldwert. Der Exchange bestätigt mit einer elektronischen Signatur dem Verkäufer beim Empfang eines Coin, dass der Verkäufer der Erstempfänger ist. Ein erneutes Ausgeben eines Coins ist damit nicht mehr möglich. Es kann zu keinem Double-Spending kommen.

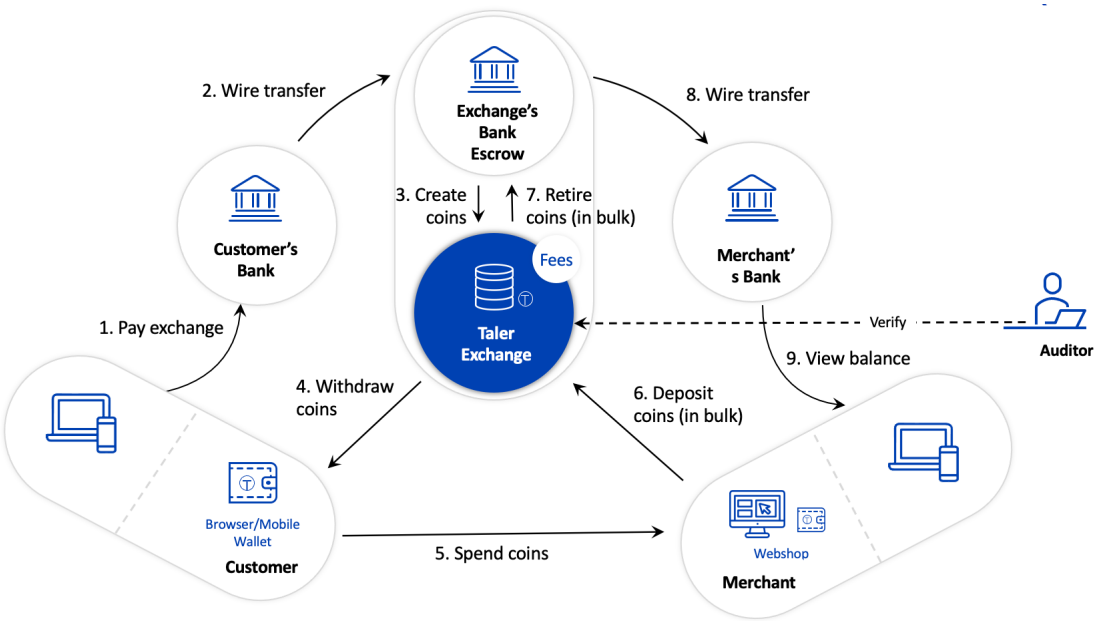
Ein Kopieren der Coins (was zwangsläufig mit deren redundanter Speicherung an verschiedenen Orten einhergeht) erzeugt identische Coins von gleichem Wert. Wer die Verfügungsgewalt über diese identischen Coins besitzt, kann mit ihnen Zahlungen auslösen - jedoch nur exakt einmal pro Coin.

Ein regulärer Ausgabevorgang kommt z.B. zum Einsatz bei

- gewöhnlichem Vertragsschluss zum Erwerb von Gütern im Internet (kein Point of Sale)
- Point of Sale/Verkaufsautomaten (einschließlich der Möglichkeit der automatischen Rückerstattung beim Abbruch des Verkaufsvorgangs durch den Automaten, falls bei diesem ein technisches Problem auftritt)
- Spenden

Die nachfolgenden zwei Illustrationen veranschaulichen den Abhebevorgang („pay exchange“ und „withdraw coins“), den Ausgabevorgang („spend coins“ und „deposit coins“) sowie die analog dazu erfolgenden IBAN-Überweisungen („wire transfer“):



Mit „Verkäufer“ gemeint sind alle Stellen, die das Bezahlsystem am Point of Sale akzeptieren und Taler-Coins annehmen (z.B. Internetseiten mit digitalen Gütern/Medien, Webshops, Supermärkte, Ladengeschäfte, Verkaufsautomaten, Kiosksysteme, POS-Kassen usw.). Die Verkäufer müssen kein Wallet haben, um bezahlt zu werden, sondern nur ein reguläres Girokonto. Falls das digitale Endgerät der Nutzer beim Ausgabevorgang keinen Zugang zum Mobilfunknetz findet, können Taler-Wallets auch über Internetzugänge von Verkäufern am Point of Sale mit dem Exchange kommunizieren und die Bezahlung durchführen.

Eine Zahlung beginnt mit einem vom Verkäufer kryptografisch signierten Angebot:

- Das kryptografisch signierte Angebot enthält die Vertragsbedingungen zwischen Käufer und Verkäufer und ist für eventuelle Streitfälle als Beleg über den Kauf der Waren auch vor Gericht verwendbar.
- Zum Kauf wird der Vertrag mit dem privaten Schlüssel des jeweiligen Wallets signiert. Damit verfügen die Käufer über einen digitalen Kaufnachweis bzw. Rechnungsbon mit dem Vertragstext in ihren Wallets.
- Beim Kaufvorgang durch Taler-Token mit Altersattribut können die Händler nicht erkennen, dass ein Kunde minderjährig oder schutzbefohlen ist. Verkaufsautomaten und Webshops können nicht unterscheiden, ob ein Kaufvorgang von einem Erwachsenen oder von einem Minderjährigen ausgelöst wurde.
- Der Kaufvorgang wird abgebrochen, wenn die Software „Taler Merchant“ im Verkaufsautomat oder Webshop bzw. im POS-Zahlungsgerät keine Taler-Token mit entsprechendem Attribut für Waren bestätigt bekommt, die in der Artikeldatenbank des Händlers eine Altersangabe (z.B. 8, 10, 12, 14, 16, 18+) haben.
- Der Verkäufer erhält eine Bestätigung, dass eine Zahlung erfolgreich war, nachdem der Taler-Exchange die ausgegebenen Token als gültig identifiziert hat.

Der Exchange sammelt Zahlungen von verschiedenen Kunden, bündelt diese nach Empfängern sortiert zu Sammelbuchungen und überweist diese auf die Girokonten der Empfänger. Die Sammelbuchung („Aggregation“) minimiert Transaktionskosten und erhöht die Effizienz der Buchungsverarbeitung zwischen den Banken. Die Verkäufer können die Frequenz der Sammelbuchung bestimmen und sind aufgrund der Tatsache, dass für jede aggregierte Buchung eine im Protokoll ausgewiesene Gebühr vom Exchange erhoben wird, auch geneigt, die Häufigkeit der Überweisungen ökonomisch zu halten (siehe *Wire fee* bei Gebührenarten). Sollte ein Exchange zu hohe Überweisungsgebühren verlangen, schlägt die Händlersoftware Merchant-Backend diese Gebühren ganz oder zum Teil dem Rechnungsbetrag der Nutzer dieses Exchange auf. Für die Sammelbuchung führt der Exchange zum entsprechenden Zeitpunkt eine Soll-Buchung auf das Treuhandkonto bei seiner Bank aus, die entsprechende Haben-Buchung erfolgt zugunsten des Empfängerkontos bei dessen Bank.

## 2.3 Wechselgeld und zeitliche Gültigkeit von Coins (*Refresh*)

Bei Bezahlvorgängen kann es aufgrund der festen nominalen Stückelung der Coins notwendig sein, dass der Nutzer Wechselgeld erhält. Zur Ausgabe von Wechselgeld benutzt Taler das Refresh-Protokoll, welches Coins mit frisch begonnener Laufzeit erzeugt.

Taler ist ein Bezahlsystem, das nicht zum Horten von Geldwerten dienen soll. Daher haben Coins eine zeitlich begrenzte Gültigkeit. Nach dem Überschreiten des Gültigkeitszeitraums verfallen die Coins der Nutzer, ihr Geldwert geht in das Eigentum des Exchange-Betreibers über (siehe auch: Nicht-transaktionsbezogene Kosten: Wertverluste). Bevor das Ablaufdatum erreicht ist, sollten Taler-Nutzer daher das Refresh-Protokoll auslösen, um Coins mit einem neuen Ablaufdatum zu erhalten. Für Refresh-Operationen sorgt jedoch auch die Wallet-Software automatisch 3 Monate vor Ende der Gültigkeit seiner ältesten Coins. Bei jeder Bezahlung setzt das Wallet zudem die älteren Coins zuerst ein.

## 2.4 Rückerstattungen (*Refund*)

Solange ein Verkäufer noch keine Sammelbuchung mit einem bestimmten Ausgabevorgang eines Käufers erhalten hat, für den er nach Abschluss des Kaufvertrags einen Rabatt einräumen will oder von dem er zurücktreten möchte, kann er im Taler-System einen Teilbetrag bzw. den vollständigen Betrag des betreffenden Vorgangs an seinen Kunden zurückerstatten lassen. Dieses Rückerstattungsverfahren wird Refund genannt und verwendet das gleichnamige Refund-Protokoll zusammen mit dem Refresh-Protokoll. Das Taler-Wallet des Käufers erhält den entsprechenden Betrag (gegebenenfalls abzüglich Gebühren für die Gebührenarten Refund und Refresh) in Form von frischen Coins.

## 2.5 Marktaustritt eines Exchange (*Recoup*)

In unregelmäßigen Abständen prüft jedes Wallet, ob Exchanges aufgrund von Emergency- oder Recoup-Protokollen die öffentlichen Schlüssel (Public key) für ihre Coin-Nennwerte (Denomination key) widerrufen haben. Im Fall von Marktaustritt oder Insolvenz des Exchange-Betreibers gewährleistet das Taler-Protokoll, dass alle Wallets automatisch über den Marktaustritt informiert werden. Dieser Geschäftsvorgang wird durch das Recoup-Unterprotokoll realisiert. Die Wallets senden automatisch alle Coins dieses Exchanges zurück und koppeln dies mit der Anweisung, den entsprechenden Betrag auf die Girokonten der jeweiligen Nutzer zurückzuerstatten. Dafür wird das Girokonto verwendet, von dem die Geldwerte für die Coins ursprünglich abgehoben wurden. Der Exchange veranlasst daraufhin die entsprechenden Soll-Buchungen des Treuhandkontos. Für den Recoup schließt das Taler-Protokoll Gebührenbelastung für die Coin-Eigentümer aus, obwohl dem Exchange-Betreiber Kosten für IBAN-Überweisungen entstehen (➔ Gebührenarten). Die Nutzer haben diese Kosten also nicht zu tragen, sondern der schließende Exchange.

Welche rechtlichen Rahmenbedingungen und Konsequenzen für Exchange-Betreiber im Fall eines Marktaustritts bzw. bei einer Insolvenz zu beachten sind, wird im Kapitel Rechtliche Rahmenbedingungen, AGB und Datenschutzerklärung explizit behandelt.

## 2.6 Einkommensnachweis von Verkäufern

Zuständige Behörden können bei diesem Geschäftsvorgang Transaktionen nachvollziehbar machen, die auf Seite der Verkäufer zu Einkommen führen, und so eine Einkommensverfolgung anstrengen.

1. Voraussetzung ist, dass die Geschäftsbank des Verkäufers der Behörde Zugriff auf Buchungen erteilt hat, die auf dem Girokonto des Verkäufers eingehen, z.B. mittels Kontoauszügen.

2. Unter den Haben-Buchungen des Girokontos findet die Behörde möglicherweise Überweisungen eines Taler-Exchange. Diese Überweisungen haben im Feld Verwendungszweck die Web-Adresse des Exchange-Betreibers sowie eine eindeutige Identifikationsnummer für jede Sammelbuchung des Exchange.

3. Mithilfe dieser beiden Daten kann die Behörde automatisiert beim Exchange eine HTTP-Anfrage stellen, um die Liste der Mikrotransaktionen zu bekommen, die als Sammelbuchung aggregiert vom Treuhandkonto des Exchange auf das Girokonto des Verkäufers überwiesen wurden. Mit den Mikrotransaktionen erhält die Behörde den genauen Betrag des Kaufpreises und den kryptographischen Hash des Vertragstexts. Mit jedem Hash garantiert der Exchange, dass der dazugehörige Vertrag vom Wallet des Käufers elektronisch unterzeichnet wurde.

4. Die Behörde kann gegebenenfalls von einem Verkäufer verlangen, den kompletten Vertragstext zu offenbaren, der zu diesem Hash verarbeitet wurde. Das Taler-Bezahlsystem speichert automatisch für jede Transaktion alle kompletten Vertragstexte unter den dazugehörigen Hashes zusammen mit den kryptographischen Beweisen in einer Datenbank beim Verkäufer. Verkäufer können Behörden den direkten Zugriff auf diese Daten per HTTP freischalten.

# 3 Altersbeschränkungen

Das Taler-System ermöglicht eine automatisierte Altersverifizierung an Verkaufsstellen und in Webshops, wo Taler-Token zur Zahlung akzeptiert werden. Verkäufer müssen die quelloffene Software „Taler Merchant“ installiert haben, die als Teil des GNU Taler-Systems entwickelt wurde und unter der Lizenz GNU GPL v3+ als freie Software von Taler Systems SA bereitgestellt wird.

Jedes Taler-Coin kann mit einer Altersbeschränkung ins Wallet abgehoben werden. Ein Wallet kann Coins mit Attributen verschiedener Altersstufen aufbewahren. Diese Token-Attribuierung mit einer Zahl aus einer Bandbreite von 2 Jahren erfahren jedoch weder Exchange noch Verkäufer, da das Attribut auf jedem Coin blind signiert und nicht offengelegt wird. Im Verkaufsprozess erhalten die Verkäufer lediglich die Information, dass der Kunde „alt genug“ ist für eine Ware oder Dienstleistung mit einer unteren Altersgrenze „älter als x Jahre“. Keine der am Taler-System beteiligten Instanzen kann auf das konkrete Alter der Zahlenden schließen. Bei einem erfolgreichen Verkaufsprozess erhält der Verkäufer lediglich die Information, dass der Zahlende für eine altersbeschränkte Ware oder Dienstleistung „älter als x Jahre“ und somit für den Kaufvertrag alt genug war. Keiner der am Taler-System beteiligten Instanzen (Verkäufer, Betreiber des Bezahlsystems, Auditoren) kann auf das tatsächliche Alter der Zahlenden oder gar deren Geburtsdaten schließen. Insbesondere ist es auch nicht möglich, erfolgreiche Bezahlvorgänge von Erwachsenen von erfolgreichen Bezahlvorgängen von Jugendlichen mit ausreichendem Alter zu unterscheiden.

Wenn Coins von einem Erwachsenenkonto abgehoben werden, ist vom Kontoinhaber darauf zu achten, dass nur Coins mit einer Altersbeschränkung an Wallets von Minderjährigen übergeben werden. An diesem Punkt tragen die Erwachsenen eine persönliche Verantwortung für die Einstellung der richtigen Altersstufe für ihre Schutzbefohlenen. Die Einstellung der Altersstufe erfolgt direkt im Dialog neben dem Knopf zur Bestätigung des Abhebevorgangs.

Die erwachsenen Nutzer müssten darauf achten, ihre Wallets vor den Schutzbefohlenen zu sichern, um den Missbrauch von altersunbeschränkten Coins zu verhindern. Die Erziehungsberechtigten sollten ihre Minderjährigen oder Mündel ebenfalls vor einem Verlust ihres Wallets warnen, da alle Personen, die Zugriff auf ihr elektronisches Taschengeld haben, dieses wie Bargeld unwiderruflich ausgeben können.

Händler, die Coins mit Altersbeschränkung akzeptieren, sollten mit diesen bereits die grundlegenden technischen Anforderungen an den Jugendschutz erfüllen, dies allerdings unter der Voraussetzung, dass die Artikeldatenbank des Händlers alle verbotenen oder altersbeschränkten Waren eindeutig mit einer dem Jugendschutzgesetz entsprechenden Altersstufe gekennzeichnet hat.

# 4 Gebühren

Von den Nutzern des Bezahlsystems können Gebühren erhoben werden, um die zwangsläufig auftretenden betriebsnotwendigen Kosten von Exchange-Betreibern zu decken. Variable Kosten umfassen hauptsächlich Kosten für Strom sowie für IBAN-Buchungen, wenn die Verkäufer ihre Umsätze aus eingelösten Taler-Coins auf deren Girokonten überwiesen bekommen. Fixkosten fallen vor allem an für Personal, Hardware und Marketing. Eine Zentralbank kann die Kosten für die Bereitstellung eines digitalen Bargeld für die Nutzer erlassen und aus Steuern oder Seigniorage decken, aber eine normale Geschäftsbank wird die Kosten ihres Exchange, den sie in-house oder in einem Rechenzentrum betreibt, auf die Nutzer verteilen wollen. Das Taler-Protokoll stellt deshalb je eine Gebühr zur Wahl für die sechs Buchungsarten *Withdrawal*, *Deposit*, *Refresh*, *Refund*, *Wire fee* und *Closing*. Exchange-Betreiber bestimmen selbstständig die Kombination dieser Gebührenarten und deren Höhe, jedoch immer im Rahmen, den das Taler-Protokoll vorgibt.

Die sechs Gebührenarten ergeben sich aus den technischen Möglichkeiten, die digitales Bargeld mit sich bringt. Exchange-Betreiber sollten nicht alle von vornherein erheben. Wenn sie für zwei oder drei Buchungsarten Gebühren verlangen, dürfte dies neue Nutzer des Systems nicht allzu sehr überfordern oder gar abschrecken. Im Fall von wiederkehrendem Missbrauch durch mutwilliges massenhaftes Auslösen bestimmter Buchungsarten müssen jedoch für genau diese Gebühren verlangt werden, um den Missbrauch kostspielig zu machen und so zu dämpfen.

Die Gebühren sollen zum einen die Käufer und Verkäufer, die das Bezahlsystem nutzen, zu einem ökonomischen Buchungsverhalten anleiten, zum anderen die Kosten der Bereitstellung des Bezahlsystems aufschlagen bzw. bei gegebenem Bedarf verursachungsgerecht abbilden und auch den Verursachern direkt belasten. Exchange-Betreiber bestimmen die Höhe der jeweiligen Gebühr für jeden Coin-Nominalwert (fixer Nennwert, festgelegt mit dem Denomination key).

Der Audit-Report jedes Exchange sendet automatisch sowohl an die externen Auditoren als auch an den Exchange-Betreiber eine Aufstellung der laufenden Einnahmen aus jeder einzelnen Gebührenart.

## 4.1 Gebührenordnung

Während das Taler-Protokoll die verfügbaren *Gebührenarten* festlegt, legen Exchange-Betreiber mithilfe von Parametern Mindest- und Höchstwerte der Gebühren fest. Die *Gebührenhöhe* im Bezahlsystem wird damit von den Exchange-Betreibern bestimmt. Die pro Nennwert von Coins eingepflegten Gebührenhöhen erhebt die Exchange-Logik dann automatisch mit den auftretenden Buchungsarten.

Änderungen an der Gebührenordnung sind nur möglich konform mit der Genehmigung des Bezahlsystems durch Aufsichtsbehörden wie die BaFin. Rechtliche Grundlage für die Gebührenerhebung sind die Allgemeinen Geschäftsbedingungen der Exchange-Betreiber, bezüglich

der auftretenden IBAN-Buchung die AGB der Geschäftsbanken, die diese mit ihren Kunden hinsichtlich deren Girokonten vereinbaren.

### 4.1.1 Verpflichtungen der Exchange-Betreiber

Exchange-Betreiber verpflichten sich, die Gebührenordnung einzuhalten. Andernfalls können sie ihren Schnittstellenzugang verlieren, ihre Zertifizierung aberkannt bekommen und darüber hinaus sogar schadenersatzpflichtig werden.

Für jede der auftretenden Buchungsarten gibt es eine Gebührenart, deren Höhe jeder Exchange-Betreiber festlegt. Ein Wert von 0 kommt damit der Abwahl von Gebühreneinkünften aus der betreffenden Buchungsart gleich. Das Bezahlsystem verfügt über sieben Buchungsarten, von denen drei (nämlich *Wire fee*, *Closing* und *Recoup*) den Exchange-Betreibern Kosten wegen IBAN-Buchungen verursachen. Das Unterprotokoll *Recoup* erlaubt dem Exchange-Betreiber keine Festlegung von Gebühren, da die Kosten der Rücküberweisung von Vermögenswerten bei einem Marktaustritt nicht den Coin-Eigentümern belastet werden dürfen, sondern vom Exchange allein getragen werden müssen.

Alle sechs Gebührenarten auf 0 zu setzen würde die Gebührenordnung für Taler-Nutzer vereinfachen und das Bezahlsystem attraktiver machen. Exchange-Betreiber müssen jedoch die Möglichkeit haben, einen eventuellen Missbrauch mit Buchungen, die besonders hohe Kosten verursachen, durch die Erhebung von Gebühren zu verhindern bzw. zu vermindern. Besonders dem anonym und unbegrenzt oft auslösbaren *Refresh* muss im Missbrauchsfall mit einer Gebühr begegnet werden können. Setzt der Exchange-Betreiber beispielsweise die Refresh-Gebühren auf Höhe der ihm konkret für diese Buchungsart anfallenden Kosten an, bereitet böswillige Kostentreiberei mit Refresh-Buchungen zumindest dem Exchange keinen Schaden, sondern belastet nur jene Nutzer, die besonders häufig einen Refresh ausführen lassen (dazu ausführlich weiter unten).

Exchange-Betreiber willigen ein, dass ihre Audit-Reports Einnahmen aus Gebühren an die Auditoren und dem entsprechend auch an Aufsichtsbehörden melden. Sie können Gebühren auf Coins nur zu deren Ausgabezeitpunkt festsetzen und nachträglich nicht mehr ändern. Gebühren auf Banküberweisungen sind gemäß des Taler-Protokolls immer nur jährlich anpassbar und vom Exchange-Betreiber mindestens für 2 Jahre in die Zukunft festzulegen. Durch diese Gebührenkonstanz können die Verkäufer ihre aufzuschlagenden Kosten besser planen und in ihre Verkaufspreise einkalkulieren.

Die AGB jedes Exchange müssen zudem die Nutzer unmissverständlich darauf hinweisen, dass es bei einem selbstverschuldeten Verzicht auf die Sicherung durch ein Backup-Tool (wie z.B. „Anastasis“) zum Totalverlust des Coin-Eigentums kommen kann (siehe Kapitel Nicht-transaktionsbezogene Kosten: Wertverluste).

Eine Privatkundenbank, die einen Exchange hostet und normalerweise bei ihren Kunden Gebühren für deren IBAN-Buchungen erhebt, hat die Möglichkeit zu bestimmen, ihren Kunden beim Abheben vom hauseigenen Girokonto in Taler-Wallets diese Gebühren zu erlassen.

### 4.1.2 Verpflichtungen von Käufern

Der Abhebevorgang besteht aus der Soll-Buchung eines (Giro-)Kontos in Fiatwährung, der entsprechenden Haben-Buchung des Treuhandkontos eines Exchange-Betreibers und der Bildung einer Reserve im Exchange mit blind signierten Coins, welche das Wallet schließlich abruft. Die Nutzer haben vor dem ersten Abhebevorgang beim jeweiligen Exchange dessen AGB zu lesen und zu bestätigen. Dieser Schritt wird von Nutzern bei Änderungen der AGB ebenfalls zwingend verlangt. Sie akzeptieren mit ihrer Einwilligung in die AGB des Exchange, den sie aktiv auswählen, zum Beispiel eventuelle Wertverluste durch *Refresh*-Gebühren, die der Exchange-Betreiber erheben kann. Alle Gebührenarten und -höhen werden den Nutzern vor jedem Abhebevorgang angezeigt. Spezifische vorgangsbezogene Transaktionsgebühren, welche die Nutzer zu tragen hätten, werden vom Wallet immer im Rahmen der interaktiven Buchung angezeigt.

Ebenfalls angezeigt werden anteilige *Wire fee*-Gebühren, welche Verkäufer auf ihre Kunden verteilen können, wenn sie die Wire fee eines Exchange als zu hoch beurteilen und mithilfe des Amortisationsfaktors wire_fee_amortization auf Käufer abwälzen (siehe Beispiele für Gebührenordnungen).

Die Nutzer verpflichten sich gemäß AGB, keinen Schadenersatzanspruch gegen das Bezahlsystem oder den Exchange-Betreiber zu stellen wegen Verlusten, die ihnen durch Diebstahl oder selbstverschuldeten Verzicht auf Sicherung der Coins im persönlichen Wallet entstehen.

Des weiteren müssen Nutzer gemäß AGB akzeptieren, dass die IBAN-Überweisung vom persönlichen Girokonto der Nutzer zum ExchangeTreuhandkonto je nach Vertrag mit der Hausbank Kosten verursachen kann, die unabhängig von Taler anfallen [bei deutschen Banken zurzeit um 9 Cent pro TAN für eine IBAN-Buchung]. Diese Kosten stehen mit dem Taler-Bezahlsystem in keinerlei Bezug und können von ihm auch nicht beeinflusst werden.

### 4.1.3 Verpflichtungen von Verkäufern

Die Sammelbuchung der Verkäuferumsätze, die eine Mehrzahl von Ausgabevorgängen der Käufer in einem Betrag an das empfangende Girokonto zusammenfasst und deren Frequenz die Verkäufer bestimmen, verursacht dem Exchange-Betreiber Kosten für jede IBAN-Buchung. Daher wird der Exchange-Betreiber angehalten sein, für diese Buchungsart die Gebühr *Wire fee* den Verkäufern zu belasten, denn diese sind die Verursacher der Sammelbuchung und nicht etwa die Käufer. Sollten Exchange-Betreiber aus Sicht der Verkäufer eine zu hohe *Wire fee* verlangen, schlägt die Händlersoftware mittels des Amortisationsfaktors diese ganz oder zum Teil dem zu zahlenden Betrag bei den Kunden dieses Exchange auf.

Beim Abhebevorgang zeigt das Wallet dem Käufer die komplette Gebührenordnung an und gibt die *Wire fee*-Gebühren für den Fall an, dass ihnen diese anteilig belastet werden. Übernimmt ein Verkäufer jedoch die *Wire fee*-Gebühr anstelle seiner Kunden, zeigen die Wallets der Kunden bei diesem Verkäufer keine *Wire fee* mehr an. Diese Verkäufer machen so für ihre Kunden die Gebührenordnung übersichtlicher, verbergen allerdings die Gebühr einkalkuliert in ihren Verkaufspreisen.

Es besteht *keine* Vertragsbindung zwischen Verkäufern und Exchange-Betreibern. Es sind die Käufer, die den Exchange bestimmen, bei welchem sie Coins abheben wollen und daher

mit dem Einsatz dieser Coins auch zum Weiterbuchen der realen Geldwerte an die Girokonten der Verkäufer veranlassen.

Sollten Verkäufer falsche Kontendaten einpflegen, haften sie selbst für daraus resultierende Schäden und nicht etwa Exchange-Betreiber. Verkäufer tragen das Risiko eines Wertverlusts bis hin zum Totalausfall ihrer Umsatzbuchungen, wenn sie selbst für die Überweisung ihrer Umsatzforderungen auf ihre Konten die IBAN zwar syntaktisch richtig, aber für ein falsches Zielkonto angeben. Ebenso tragen allein die Verkäufer weitere Gebühren aufgrund einer Fehlbuchung, die sie verursachen und für die ein manuelles Routing nötig wird (z.B. bei erloschenen Empfängerkonten).

### 4.1.4 Technische Rahmenbedingungen der Gebührenerhebung

Gebühren werden erhoben pro Coin bzw. pro Banküberweisung. Die Anzahl an Coins wächst üblicherweise logarithmisch mit dem repräsentierten Betrag. Gebühren können anfallen sowohl auf Flussgrößen (z.B. auf bewegte Coins bei Abhebevorgängen und Ausgabevorgängen) als auch auf Bestandsgrößen (z.B. die aufbewahrten Coins in Wallets). Die Gebühren auf Coins können sich unterscheiden je nach Ausgabezeitpunkt eines Coin und je nach Wert eines Coin, sie sind für jedes Coin mit seinem Ausgabezeitpunkt festgelegt, können also nachträglich vom Exchange-Betreiber nicht geändert werden.

Jede Gebührenart wird selbst bei einer Höhe von 0 Einheiten immer als Variable in der Exchange-Schnittstelle geführt (siehe Dokumentation der Exchange RESTful JSON API). Während des gesamten Zeitraums der Gültigkeit aller Denomination keys (mögliche Nennwerte der Coins, die ein Exchange signiert) haben alle gewählten Gebührenarten ihre Gültigkeit beizubehalten.

Die Refresh-Buchung wird automatisch 3 Monate vor Ende der Gültigkeit der Coins von der Wallet-Software ausgelöst. Insbesondere wenn Exchange-Betreiber Refresh-Gebühren erheben, müssen sie in ihren AGB die Nutzer auf diese Automatik hinweisen.

## 4.2 Gebührenarten

Das Taler-Protokoll bietet folgende Gebührenarten:

1. ABHEBEN vom Girokonto (*Withdrawal*): Für jedes erfolgreiche Abheben vom Girokonto, pro Coin
2. AUSGEBEN / BEZAHLEN (*Deposit*): Für jeden Ausgabevorgang, pro Coin
3. WECHSELGELD (*Refresh*): Pro Coin bei
   a) Wechselgeld-Buchungen
   b) Ablauf des Gültigkeitszeitraums von Coins
   c) Transaktionsabbruch infolge von Netzwerkfehlern sowie bei
   d) *Refund*

4. RÜCKERSTATTUNGEN (*Refund*): Für Erstattungen oder bei Vertragsrücktritt durch Verkäufer, pro Coin

5. UMSATZVERBUCHUNG (*Wire fee*): Für die aggregierte Buchung von Umsätzen auf ein Zielkonto des Verkäufers, pro Überweisung

6. SCHLIESSEN DER RESERVE (*Closing*): Falls nach einer Überweisung an den Exchange das Wallet die Coins nicht abheben sollte, pro Rücküberweisung auf das Ursprungskonto

### 4.2.1 Effekte der Gebührenarten auf Exchange-Betreiber, Käufer und Verkäufer

Jede der genannten Gebührenarten wird nun jeweils betrachtet aus Sicht der Käufer, der Exchange-Betreiber und der Verkäufer:

| **Withdrawal aus Sicht der Käufer** |
| --- |
| Wer Taler-Wallets mit Coins bestücken möchte, muss dazu eine IBAN-Buchung vom persönlichen Girokonto zugunsten des Exchange-Treuhandkontos auslösen, wofür je nach Vertrag mit der Hausbank Kosten anfallen. Zu diesen möglicherweise entstehenden Kosten kommt die Withdrawal-Gebühr, die ein Exchange-Betreiber für jedes Coin, das ins Wallet abgehoben wird, verlangen könnte. Auch wenn viele Bankkunden bereits an die Kostenpflicht von IBAN-Buchungen gewöhnt sind, wirkt die Withdrawal-Gebühr wie ein Kaufkraftverlust schon vor beabsichtigten Umsätzen, über den die Käufer durch die Anzeige aller Gebührenarten beim Abheben in Kenntnis gesetzt werden. Sobald sich die Käufer bewusst werden, dass sie die Kosten für jedes erzeugte Coin zu tragen haben, werden sie es vorziehen, möglichst wenige Coins mit hohen Nennwerten in ihre Wallets abheben zu lassen. |
| **Withdrawal aus Sicht der Exchange-Betreiber** |
| Eine Gebühr auf jedes erzeugte Coin würde tatsächlich alle bei einem Exchange-Betreiber abgehobenen elektronischen Münzen treffen und die Kosten ihrer Erzeugung auf alle erstmalig signierten Coins verteilen, verhindert jedoch keinen Missbrauch mit anderen Buchungsarten und würde zudem jene Nutzer diskriminieren, die viele kleinere Nennwerte aufbuchen. Manche Nutzer mit Coins höherer Nennwerte könnten die Kosten des Exchange-Betreibers durch vermehrte Refresh-Buchungen steigern, die Kostenzuwächse sind jedoch marginal gering. |
| **Withdrawal aus Sicht der Verkäufer** |
| Withdrawal-Gebühren stellen zwar für Verkäufer keine Kosten dar, doch sind sie für ihre Kunden eine Hemmschwelle, Taler zu benutzen, wenn sie schon beim Abheben diese Gebühren angezeigt bekommen. Die Verkäufer würden es sogar vorziehen, die Kosten für die Erzeugung von Coins in ihre Verkaufspreise einzukalkulieren und vor den Kunden zu verbergen. Die *für Kunden* beim Abhebevorgang erzeugten Coins stehen allerdings mit den Verkäufern in keiner direkten Beziehung. |
| **Deposit aus Sicht der Käufer** |
| Obwohl die Kunden die Deposit-Buchung mit dem Kauf von Gütern auslösen, müssen die Verkäufer die Deposit-Gebühr pro Coin tragen, jedoch nur bis zu einem vom Verkäufer bestimmten Maximalwert (default_max_deposit_fee). Der diesen Maximalwert übersteigende Rest der Deposit-Gebühr muss vom jeweiligen Käufer getragen werden. Mittels Deposit-Gebühren könnte man theoretisch alle Kosten des Exchange-Betriebs auf alle *eingesetzten* Coins verteilen. Die Käufer können in der Regel leicht nachvollziehen, dass eine Gebühr auf eingesetzte deponierte Coins erhoben wird. |
| **Deposit aus Sicht der Exchange-Betreiber** |
| Bei der Deposit-Buchung vergleicht die Exchange-Logik den Public key jedes Coin mit den in einem Array gespeicherten Schlüsseln der Postgres-Datenbank des Exchange und untersucht für jedes Coin, ob es erstmalig zur Bezahlung eingelöst wird. Dieser Vorgang verbraucht nur wenig Energie und bringt keine weiteren Kosten mit sich. Für Exchange-Betreiber können die marginal geringen Kosten erst bei einer exorbitanten Menge an Deposit-Buchungen bedeutend werden. Deposit-Gebühren stellen vor allem die wichtigste Einkommensquelle für den Exchange-Betreiber dar und können über alle eingesetzten Coins erhoben werden. |

| **Deposit aus Sicht der Verkäufer** |
| --- |
| Verkäufer werden darauf Wert legen, dass (1.) der vom Käufer gewählte Exchange die regulatorischen Auflagen der Aufsichtsbehörden und der Gesetze gegen Geldwäsche erfüllt, (2.) der Exchange im SEPA-Währungsraum operiert und (3.) die Gebühren des gewählten Exchange sich im Rahmen dessen befinden, was der Verkäufer mithilfe seiner Maximalwerte für Deposit-Gebühren (und wie unten beschrieben auch mit Maximalwerten für die Wire fee-Gebühr) festlegt. Wenn ein Exchange-Betreiber für Deposit-Buchungen verhältnismäßig hohe Gebühren verlangt, beeinflussen diese auch jede *Refund*-Buchung bei einer teilweisen Rabattierung, denn die den Maximalwert des Verkäufers übersteigenden *Deposit*-Gebühren tragen die Käufer, wodurch die Rabattierung aus Sicht der Käufer schlechter wird. Nur bei einem kompletten Rücktritt vom Vertrag durch den Verkäufer befreit die Refund-Buchung die Käufer von Deposit-Gebühren, doch es entstehen durch die Refund-Buchung bei Vertragsrücktritt auch Refresh-Gebühren, die von den Käufern zu tragen wären. |
| **Refresh aus Sicht der Käufer** |
| Refresh-Gebühren werden mehrheitlich verursacht durch die Erzeugung von frischen Coins aufgrund von *Wechselgeld*-Buchungen. Der Zahlbetrag wird dabei mit einem Coin von höherem Nennwert bezahlt, das Wallet erhält Coins mit Nennwerten zurück, die summiert den Differenzbetrag ergeben. Die Refresh-Gebühr bei der Wechselgeld-Buchung belastet damit stets nur ein eingesetztes Coin und ist aus Käufersicht marginal gering. Refresh-Buchungen fallen darüber hinaus auch an bei *Refund*-Buchungen (nachträgliche Rabattierung oder Stornierung von Kaufverträgen). Seltener sind Refresh-Buchungen aufgrund des Ablaufs der Gültigkeit von Coins oder wegen Transaktionsabbrüchen durch Netzwerkfehler. Die Gebühr auf Refreshs wird pro Coin erhoben. Sie soll bei einer missbräuchlichen Anwendung entstehende Kosten vom Exchange abhalten und wird den Käufern belastet. Käufer werden diese Gebühr durch einen eventuell auftretenden Missbrauch mit Refresh-Buchungen marginal nur als geringe persönliche Belastung betrachten, da deren absolute Höhe pro Coin niedrig ausfällt. |
| **Refresh aus Sicht der Exchange-Betreiber** |
| Solange kein Missbrauch mit Refresh-Buchungen stattfindet, muss der Exchange-Betreiber abwägen, ob er die Kosten für Refreshs auf die Käufer direkt abwälzt oder mit einer anderen Gebührenart deckt. Die Refresh-Gebühr für den Missbrauchsfall heranzuziehen bedeutet, dass der Verursacher böswilliger Refreshs sämtliche Käufer eines Exchanges bei ihren regelmäßigen Refresh-Buchungen belastet. Dies verhindert zwar einen Missbrauch nicht, sondern macht nur die Buchungsart für diejenigen kostspielig, die oft Refreshs auslösen. Im akuten Missbrauchsfall werden dann Käufer mit Gebühren belastet, die böswillig verursachten Kosten treffen wenigstens nicht den konkreten Exchange, sondern alle Endverbraucher, die von ihm signierte Coins erhalten. |
| **Refresh aus Sicht der Verkäufer** |
| Die Refresh-Buchung betrifft Verkäufer nicht direkt, jedoch die Refund-Buchung. |
| **Refund aus Sicht der Käufer** |
| Im Gegensatz zur Gebührenart Refresh sind Verursacher der Refund-Buchung die Verkäufer - und nicht die Käufer. Erhebt ein Exchange diese Gebührenart, würden bei einem teilweisen Refund infolge von Rabattierung nach dem Kaufvertragsschluss die bereits eingesetzten, deponierten Coins der Käufer mit einer Refund-Gebühr belastet. Nur bei einem vollständigen Refund werden die Coins der Käufer von den Deposit-Gebühren entlastet, wohl aber mit der Refresh-Gebühr belastet, sofern die Gebührenordnung des von den Käufern gewählten Exchange diese erhebt. Auch bei einer teilweisen Rabattierung liegt im Regelfall die Ursache für die Rabattgewährung beim Verkäufer. Aus Sicht der Käufer sollten daher eigentlich die Verkäufer diese Gebühr tragen. |

| **Refund aus Sicht der Exchange-Betreiber** |
| --- |
| Exchange-Betreiber können Refund-Buchungen nicht unterdrücken, da sie den Verkäufern die Möglichkeit zu Rabatten und Rücktritten von Kaufverträgen einzuräumen haben. Ein teilweiser Refund entlastet die Käufer nur teilweise von ihren Deposit-Gebühren. Mit der Zeit werden Kunden solche Verkäufer eher meiden, die nach einem Vertragsschluss oft rabattieren müssen. Verkäufer, die wiederholt mutwillig wiederholt komplette Refunds auslösen, befreien zwar die bereits beim Exchange deponierten Coins der Käufer von Deposit-Gebühren, belasten diese jedoch durch Refresh-Gebühren. Sollte ein Exchange-Betreiber dann auf die Refresh-Gebühr verzichten, würde er sich Kosten aufbürden. Um dies zu vermeiden, muss der Exchange-Betreiber Refresh-Gebühren einführen bzw. erhöhen, wodurch er alle seine Kunden höher belastet. Sowohl die Kosten für den teilweisen als auch für den kompletten Refund müssten aus Sicht der Exchange-Betreiber die Verkäufer tragen, damit diese einen Anreiz verspüren, Rabattierungen oder Rücktritte möglichst zu vermeiden, die Vereinbarungen über Waren und Dienstleistungen den Kaufverträgen entsprechend zu erfüllen und ebenso ihre Käufer anzuhalten, seltener Rücksendungen und Vertragsrücktritte auszulösen (mit allen ökonomischen und ökologischen Effekten, die damit verbunden sind, z.B. durch häufige willkürliche Warenrücksendungen). |
| **Refund aus Sicht der Verkäufer** |
| Zum heutigen Stand der Implementierung tragen bei einem Rücktritt vom Kaufvertrag die Käufer die Kosten der Refund-Gebühr, sofern der Exchange diese erhebt, bei einer teilweisen Rabattierung tragen die Käufer die Deposit-Gebühr für ihre verbrauchten Coins. Verkäufern liegt es grundsätzlich daran, Rabatte und Rücktritte ökonomisch zu halten. |
| **Wire fee aus Sicht der Käufer** |
| Diese Gebühr trifft die Käufer nur direkt in folgendem Fall: Das Protokoll erlaubt den Verkäufern, die Kosten der Gebühr teilweise auf die Käufer abzuwälzen, wenn der Exchange-Betreiber, der die Coins der Käufer signierte, die Wire fee-Gebühr über dem Wert einstellte, den jeder Verkäufer in seinem Merchant-Backend mit der Variable max_wire_fee einpflegen kann (aber nicht muss). Die Kosten der Wire fee-Gebühr sind in die Preise der Verkäufer einkalkuliert. Die Verkäufer könnten die relativen Kostenvorteile des Taler-Bezahlsystems in Form von niedrigeren Endverbraucherpreisen an ihre Kunden weiterreichen, sind dazu aber nicht gezwungen. |
| **Wire fee aus Sicht der Exchange-Betreiber** |
| Die Wire fee-Gebühr wälzt die Kosten für IBAN-Buchungen vom Treuhandkonto an die Verkäuferkonten ab - vom Exchange-Betreiber auf die Verkäufer. Die Käufer bekommen die Wire fee nur angezeigt, wenn der Verkäufer sie nicht übernimmt. Ansonsten merken die Kunden nicht, welche Gebühr von ihren verbrauchten Coins beim Exchange einbehalten wird. Für Exchange-Betreiber käme eine Abwahl der Wire fee gleich einem Freibrief an die Verkäufer, so oft wie möglich eine Sammelbuchung ihrer Umsatzeinkünfte auszulösen. Verlangt der Exchange-Betreiber hingegen die Wire fee per Überweisung an die Verkäuferkonten, führt diese Gebühr dazu, dass die Verkäufer die Häufigkeit der Sammelbuchung so einstellen, wie sie es für ihre Unternehmungen benötigen und sich die Gebühr dafür leisten möchten. Wenn die Frequenz dieser Buchungsart steigt, steigen auch die absoluten Kosten für die Verkäufer. Die Käufer erfahren von der Wire fee-Gebühr nur im Fall, dass ein Exchange-Betreiber diese höher setzt als der Wert, den ein Verkäufer in der Variable max_wire_fee eingepflegt hat. |

| **Wire fee aus Sicht der Verkäufer** |
|---|
| Verkäufer wünschen möglichst schnell und oft ihre Umsätze zu verbuchen. Eine zeitnahe Umsatzverbuchung verbessert ihre Liquidität und bringt Zinsmitnahmen, wenn Umsatzeinkünfte früher als die Auszahlungen an Lieferanten eingehen. Sie sind daher gezwungen abzuwägen, ob sie lieber höhere absolute Kosten durch die Wire fee tragen oder auf Liquidität verzichten. Bei einigen Verkäufern entscheidet hingegen die Menge an Buchungen über die Häufigkeit der Sammelbuchung, um die Abteilungen für Accounting und Billing nicht zu überlasten. In jedem Fall sind die Kosten der Wire fee in die Endverbraucherpreise einkalkuliert. |
| **Closing aus Sicht der Nutzer** |
| Die Closing-Buchung lösen Nutzer des Bezahlsystems aus, wenn sie nach einer erfolgreichen IBAN-Überweisung an das Treuhandkonto eines Exchange die Reserve nicht ins persönliche Wallet abheben lassen, weil sie das Wallet nicht innerhalb von 14 Tagen mit dem Taler-Exchange verbinden lassen. Da sie die Verursacher sind und dem Exchange für die Rücküberweisung Kosten bereiten, haben sie auch die Closing-Gebühr zu tragen. Dies erfolgt durch die Überweisung des ursprünglich überwiesenen Aufladebetrags abzüglich der Kosten für IBAN-Buchung und evt. manuelles Routing. Die Gebühr ist leicht durchzusetzen und stößt bei den meisten Nutzern auf Verständnis, denn im Regelfall werden sie von dieser Gebührenart nicht betroffen sein und können auch den AGB-Passus schnell nachvollziehen, dass die Verursacher die Kosten für selbstverschuldetes Nichtabheben tragen müssen. |
| **Closing aus Sicht der Exchange-Betreiber** |
| Die Kosten der Closing-Buchung entstehen dem Exchange-Betreiber aufgrund eines nicht regulären Nutzerverhaltens. Auf diesen Kosten darf er jedoch nicht sitzenbleiben, sondern muss sie dem verursachenden Nutzer belasten. Die Closing-Gebühr ist für Exchange-Betreiber unverzichtbar, um Missbrauch durch Kostentreiberei zu verhindern. Die Gebühr zu verlangen und einzubehalten gelingt stets reibungslos, da das Treuhandkonto des Exchange mit einer Überweisung bebucht wurde - und nicht mit einer SEPA-Lastschrift, die vom Nutzer in böswilliger Absicht storniert werden könnte. |
| **Closing aus Sicht der Verkäufer** |
| Die Closing-Buchung betrifft Verkäufer in keiner Weise. |

### 4.2.2 Tabellarische Zusammenfassung

| **Buchungsart** | **Withdrawal** | **Deposit** | **Refresh** | **Refund** | **Wire fee** | **Closing** |
|---|---|---|---|---|---|---|
| **Verursacher:** | Käufer | Käufer | Käufer | Verkäufer | Verkäufer | Käufer |
| **Kostenträger:** | Käufer | Verkäufer, Käufer bei hoher Exchange-Gebühr | Käufer | Käufer | Verkäufer, Käufer bei hoher Exchange-Gebühr | Käufer |
| **Kosten pro:** | Coin | Coin | Coin | Coin | Überweisung | Überweisung |
| **IBAN-Kosten:** | Ja, für Käufer | Nein | Nein | Nein | Für Exchange | Für Exchange |
| **Kosten für Nutzer:** | u.U. Kosten einer IBAN-Überweisung | Haupteinnahme-quelle für Exchange | ? | Zuerst auf 0 lassen, nur bei Missbrauch anheben | ? | Zuerst auf 0 lassen, nur bei Missbrauch anheben |

### 4.2.3 Gebührenhöhen im Missbrauchsfall

Der Normalfall eines Buchungszyklus besteht aus *Withdrawal*, *Deposit* und *Wire fee* - wenn die zu zahlenden Beträge mit Coins von genau passenden Nennwerten beglichen werden. Für alle anderen Beträge, für die ein Coin von höherem Nennwert eingesetzt wird, muss die *Refresh*-Buchung Wechselgeld erzeugen, d.h. einen oder mehrere frische Coins ins Wallet buchen, bis der Differenzbetrag erreicht ist.

Refresh-Buchungen können jedoch anonym unbegrenzt oft mit schadhaften Absichten gegen Exchange-Betreiber ausgelöst werden. Jeder Exchange-Betreiber muss daher im Missbrauchsfall mit unterschiedlichen Gebührenhöhen gegen mutwillig oft ausgelöste Buchungsarten vorgehen können.

- Missbrauch durch *Withdrawal*-Buchungen ist unwahrscheinlich, da die Kosten der IBAN-Überweisungen erst einmal von den Inhabern der Girokonten getragen werden.
- Missbrauch durch *Deposit*-Buchungen ist unwahrscheinlich, da der Exchange-Betreiber in der Regel Deposit-Gebühren erheben wird.
- Missbrauch durch *Refresh*-Buchungen ist möglich und bedarf einer differenzierten Behandlung: Im Normalfall wird ein Exchange-Betreiber keine Refresh-Gebühr erheben auf die Zahlung mit Coins unpassender Nennwerte (Wechselgeld-Buchungen), im Missbrauchsfall muss er diese Gebühr jedoch schon erheben, wenn seine Kunden massenhaft Refreshs auslösen
  (1.) mit Coins bei einem Transaktionsabbruch oder
  (2.) bei massenhaft wiederholtem *Refund*, den allerdings die Verkäufer auslösen und dessen Kosten fallweise tragen. Im extremen Missbrauchsfall - wenn ein Exchange unter mutwilligen Refresh-Buchungen und deren Kosten leidet, muss er die Refresh-Gebühren auf einen hohen Wert setzen und damit alle Coin-Eigentümer, deren Coins von diesem Exchange signiert wurden, belasten.
- Missbrauch durch *Refund*-Buchungen ist theoretisch möglich und kann ebenfalls behandelt werden mit der Einführung oder Erhöhung von *Refund*-Gebühren.
- Verkäufer können durch das Anfordern einer hohen Frequenz ihrer Umsatz-Sammelbuchungen das Einsparpotenzial dieser Sammelbuchungen hinfällig machen. Eine schnelle Umsatzverbuchung liegt auch meist im Interesse der Verkäufer. Bei einer zu hoch eingestellten Häufigkeit der Sammelbuchungen ist mit entsprechenden Kosten zu Lasten des Exchange-Betreibers zu rechnen (IBAN-Buchungen!). Exchange-Betreiber können jedoch dem massenhaften Auslösen von Sammelbuchungen mit hohen Frequenzen dank der *Wire fee*-Gebühr begegnen.
- Missbrauch durch Rücküberweisungen infolge des Nichtabhebens ins Wallet belastet den Exchange-Betreiber mit Kosten für IBAN-Überweisungen, zur Abwehr kann er eine *Closing*-Gebühr einführen, um das Problem abzustellen.

### 4.2.4 Empfehlung der Höhen der Gebührenarten

Aus der vorangegangenen Diskussion der Gebührenarten ergibt sich eine Empfehlung für die Wahl der *Deposit*-Gebühr als wichtigster Gebührenart, da diese eine wesentliche Einnahmequelle des Exchange-Betreibers darstellt. Dem Exchange-Betreiber ist jedoch vollkommen freigestellt, neben der *Deposit*-Gebühr weitere Gebührenarten festzulegen. Wenn im Betrieb Kosten anfallen, sollten die entsprechenden Gebühren so hoch gesetzt sein, dass sie die anfallenden Kosten möglichst decken (dies bezeichnet in der folgenden Tabelle der Begriff „kostendeckend“).

| Gebührenart | Höhe |
|---|---|
| ***Deposit*** | Wesentliche Einnahmequelle des Exchange-Betreibers |
| ***Wire fee*** | Proportional kostendeckend für IBAN-Überweisungen; dient zur generellen Belastung der Verkäufer mit Kosten und Sammelbuchungskosten |
| ***Closing*** | Kostendeckend, nur zu erheben bei Verdacht auf Missbrauch, zur Vermeidung von Missbrauch durch Nichtabheben ins Wallet nach einer erfolgten Geldüberweisung zum Exchange |
| ***Refresh*** | Kostendeckend, nur zu erheben bei Verdacht auf Missbrauch; wirkt gegen Missbrauch durch mutwillig ausgelöste Refreshs; als Negativzins |
| ***Refund*** | Kostendeckend, nur zu erheben bei Verdacht auf Missbrauch bei Refund, gegen mutwilliges Wiederholen von Refund-Deposit-Refund-Deposit... |
| ***Withdrawal*** | Missbrauch ist unwahrscheinlich; Missbrauch wäre theoretisch denkbar, wenn Nutzer Geld im Bezahlsystem horten wollen, um Negativzinsen auf ihre Guthaben bei normalen Banken zu vermeiden |

Im Missbrauchsfall empfiehlt sich dem Exchange-Betreiber, die folgenden Gebührenarten in einer wirksamen Höhe festzulegen:

1. *Wire fee*-Gebühr zum Decken der IBAN-Überweisungskosten, die zuerst nur die Verkäufer mit Kosten belastet und die letzten Endes deren Kunden in den Verkaufspreisen begleichen.

2. Die *Closing*-Gebühr sollte jeder Exchange-Betreiber in Höhe der Kosten für IBAN-Buchungen bei einem eventuellen Nichtabheben der Wallets seiner Nutzer wählen.

3. Die *Refresh*-Gebühr hilft fallweise gegen Missbrauch, wenn Verkäufer massenhaft Refund-Buchungen auslösen sollten oder anonyme Wallets massenhaft Refreshs auslösen.

4. *Refund*-Gebühren sollten Exchange-Betreiber nur um einem eventuellen Missbrauch mit Refund-Buchungen zu begegnen kostendeckend festlegen.

5. *Withdrawal*-Gebühren werden Exchange-Betreiber normalerweise nicht verlangen, weil ein Missbrauch mit Abhebevorgängen unwahrscheinlich ist.

# 5 Nicht-transaktionsbezogene Kosten: Wertverluste

Wertverluste sind nicht-transaktionsbezogene Kosten, die im Gegensatz zu den transaktionsbezogenen Gebühren, die im Normalfall der Nutzung auftreten, in Sonderfällen für die Nutzer entstehen können.

## 5.1 Wertverluste zu Lasten des Wallet-Guthabens

Drei Möglichkeiten bestehen, bei denen die Käufer Wertverluste ihres Coin-Guthabens tragen:

1. Verlust, Zerstörung oder Untergang eines Wallet, für das kein Backup angelegt wurde (Totalverlust des Guthabens)
2. Wertverlust in Höhe von Refresh-Gebühren auf das Wallet-Guthaben nach Ablauf der Gültigkeit der Coins (➔ Parameter DURATION_SPEND)
3. Kompletter Verfall der Coins nach Ablauf eines bestimmten Zeitraums ohne Refresh (z.B. 1 Jahr), weil so lange keine Internet-Verbindung des Wallet bestand

Zu 1.: Die AGB jedes Exchange müssen ihre Nutzer unmissverständlich darüber aufklären, dass sie für eine Sicherung ihrer Wallets verantwortlich sind und bei einem selbstverschuldeten Verzicht auf die Sicherung durch ein Backup-Tool wie z.B. „Anastasis“ den Totalverlust ihres Coin-Eigentums riskieren.

Zu 2.: Mit dem Refresh-Protokoll kann die Abzinsung von Coin-Guthaben gesteuert werden. Die Abzinsung ist laut Protokoll zurzeit so eingestellt, dass alle Coins bei einem Onlinegehen des Wallet geprüft werden, ob ihre Erzeugung länger als zwei Jahre zurückliegt. Die zeitliche Gültigkeit jedes Coin wird damit geprüft. Der Exchange-Betreiber legt dazu den Parameter DURATION_SPEND (z.B. auf 2 Jahre) fest und bestimmt damit, wann die Refresh-Buchung *aufgrund des Alters eines Coin* greift und für alle betroffenen Coins frische Credentials erzeugt. Dieser Refresh ist gleichbedeutend mit einem Negativzins auf das betroffene Coin-Guthaben infolge von Refresh-Gebühren: Im gegebenen Beispiel mit DURATION_SPEND = 2 Jahre wäre dies eine Abzinsung des Guthabens nach 2 Jahren in Höhe der Refresh-Gebühr, die der Exchange-Betreiber mit dem Parameter FEE_REFRESH bestimmt.

Zu 3.: Der Zeitraum, in dem keine Wallet-Verbindung zur Exchange-Schnittstelle bestand und nach dessen Ablauf das Wallet einen Refresh-Vorgang mit komplettem Verfall der Coins

anstößt, sollte vom Exchange-Betreiber lang genug eingestellt sein. Dieser Zeitraum muss so lang sein, dass ein Nutzer mit einer hohen Wahrscheinlichkeit ein digitales Endgerät mit seinem persönlichen Wallet darauf online gehen lässt. Für den Fall keiner Verbindung in diesem Zeitraum ist nach dessen Ablauf der Exchange-Betreiber neuer Eigentümer der Werte verfallener Coins.

An dieser Stelle sei noch einmal daran erinnert, dass Taler ein Bezahlsystem ist und kein Aufbewahrungsmittel zum Horten von Geldwerten. Im Normalfall verbinden Nutzer des Bezahlsystems ihre Wallets im gegebenen Zeitraum (hier 1 Jahr) und lösen mit jedem Verbinden einen Refresh aller Coins aus, der ihre Gültigkeitsdauer erneut um 2 Jahre verlängert.

Da für den initialen Betrieb des Taler-Exchange keine Refresh-Gebühren vorgesehen sind, werden die Nutzer auch nicht von Gebühren auf Refreshs ihrer Coins belastet.

Zu den rechtlichen Konsequenzen hinsichtlich Abzinsung, Verfall und Verjährung von Coin-Guthaben siehe 7.1.2 .

## 5.2 Wertverluste zu Lasten des Verkäuferumsatzes

Es bestehen folgende zwei Möglichkeiten, bei denen die Verkäufer Wertverluste ihrer Umsätze aus den deponierten Coins ihrer Kunden riskieren:

1. Bei einer Fehlbuchung aufgrund falsch angegebener IBAN-Kontonummer des Verkäufers bzw. erloschener Empfängerkonten und damit nötigem manuellem Routing (mit Gebühren nach Kostentabelle der Geschäftsbank des Verkäufers, der Banken bzw. Exchange-Betreiber).

2. Nach fehlerhaften Überweisungen (IBAN syntaktisch richtig, aber falsches Zielkonto). Wird dies zu spät vom Verkäufer bemerkt, um den Fehler noch durch ein manuelles Routing zu korrigieren, kann es auch hier zu einem Totalverlust kommen, insbesondere wenn der Betrag bereits auf das falsche Zielkonto gebucht wurde.

Das Bezahlsystem weist an geeigneter Stelle Verkäufer darauf hin, dass Verkäufer beim Einpflegen der IBAN ihres Geschäftsgirokontos Vorsicht walten lassen, damit sie Wertverluste durch Selbstverschulden vermeiden.

# 6 Beispiele für Gebührenordnungen

## 6.1 Referenzkonfiguration

Bei einer initialen Einführung des Betriebs schlagen wir eine einfache Gebührenordnung vor. Es würden für die Buchungsarten *Refresh* und *Refund* zunächst keine Gebühren erhoben. Dies hat zur Folge, dass den Nutzern durch Wechselgeld-Buchungen und beim Auffrischen ihrer Coins kein Nachteil entsteht (die Nennwerte der „alten“ Coins entsprechen denen der „aufgefrischten“ Coins). Für den Fall, dass es zu einem eventuellen Missbrauch durch Refresh- oder Refund-Buchungen käme, sollte der Exchange-Betreiber Refresh- und Refund-Gebühren in Höhe von jeweils 0,25 Cent pro Coin durchgehend für alle Coin-Nennwerte einführen, um den Missbrauch für deren Verursacher kostspielig werden zu lassen.

Auch für den fiktiven Fall, dass ein negativer Zins auf Guthaben des Treuhandkontos erhoben würde und die Gebühreneinnahmen des Exchange signifikant hohe Negativzinsen nicht decken, könnte der Exchange-Betreiber *Refresh*-Gebühren in Höhe der Negativzinsen einführen. In jedem Fall würde diese Abzinsung von Coin-Werten jedoch erst für Coins gelten, die der Exchange nach der Umstellung auf die neue Gebührenordnung mit *Refresh*-Gebühren signiert.

Des weiteren würde der Exchange-Betreiber *Wire fee*-Gebühren in Höhe von beispielsweise 10 Cent pro IBAN-Buchung erheben, um die Kosten seiner IBAN-Buchungen zu decken. *Closing*-Gebühren für Rücküberweisungen auf Ursprungskonten würden zunächst nicht erhoben. Sollte der Exchange-Betreiber ein problematisches Transaktionsvolumen mit Closing-Buchungen feststellen, ist er gut beraten, auch für diese 10 Cent pro Buchung zu erheben.

Diese Tabelle veranschaulicht die Gebühren auf Coins und Buchungen in der Referenzkonfiguration:

| Coin-Nennwerte | Deposit-Gebühr pro Coin | Gültigkeitsdauer |
|---|---:|---:|
| 0,25 bis 64 Cent | 0,25 Cent | 1 Jahr |
| 128 bis 1024 Cent | 0,50 Cent | 1 Jahr |
| 2048 bis 65536 Cent | 1,00 Cent | 1 Jahr |
| | Wire fee-Gebühr | |
| | 10,00 Cent | |

Aus der Tabelle ersichtlich sind unterschiedliche Höhen der *Deposit*-Gebühr auf die Coin-Nennwerte innerhalb der drei Bandbreiten von 0,25 bis 64 Cent, 128 bis 1024 sowie 2048

Tabelle 6.1: Einfache Gebührenordnung bei initialem Exchange-Betrieb

bis 65536 Cent. Die *Wire fee*-Gebühr beträgt 10 Cent pro IBAN-Überweisung auf Verkäufer-Empfängerkonten. *Refund*-, *Refresh*- und *Closing*-Gebühren bleiben auf Null gesetzt (per default). Die Gültigkeitsdauer ist mit DURATION_SPEND (Deposit lifetime) für die drei Bandbreiten auf 1 Jahr eingestellt, was bedeutet, dass alle Coins jedes Nennwerts innerhalb eines Jahres ausgegeben oder durch eine Refresh-Operation gegen neue Coins getauscht werden müssen, sonst verfallen sie.

## 6.2 Beispielrechnungen: Normalbetrieb

Alice überweist 5 Euro von ihrem Girokonto, wählt den Exchange mit der oben dargestellten Gebührentabelle und lässt ihr persönliches Wallet die blind signierten Coins abheben. Beim Abhebevorgang bekommt sie je eine Münze mit folgenden Nennwerten: 4, 16, 32, 64, 128, und 256 Cent. In einer Bäckerei bezahlt sie Brötchen für 3,23 Euro mit Coins der Nennwerte 4 Cent, 64 Cent und 256 Cent (Deposit-Buchung über insgesamt 324 Cent) und bekommt ein Coin mit dem Nennwert 1 Cent mittels der Refresh-Buchung als Wechselgeld. Für die drei eingesetzten Coins fallen an *Deposit*-Gebühren an: 1 x 0,25 Cent und 2 x 0,50 Cent, also insgesamt 1,25 Cent. Da die Bäckerei im Merchant-Backend mit dem Parameter default_max_deposit_fee festgelegt hat, sich bis zu 0,5% ihres Umsatzes an den *Deposit*-Gebühren ihrer Kunden zu beteiligen, fallen für Alice keine *Deposit*-Gebühren an[1].

Die Bäckerei könnte nun manuell veranlassen, den Umsatz mit Alice vom Exchange auf ihr Geschäftsgirokonto zu überweisen. Alternativ könnte sie auf den Zeitpunkt warten, bis die Sammelbuchung ihrer Umsätze automatisch erfolgt[2].

Der Zeitungskiosk soll hingegen in dieser Beispielrechnung nicht bereit sein, sich an den Gebühren seiner Kunden zu beteiligen. Da der Kiosk nur wenige Artikel verkauft, setzt der Kioskbetreiber seinen Amortisationsfaktor wire_fee_amortization für die *Wire fee*-Gebühr auf 4. Diesem stimmen die Kunden durch Einwilligung in die AGB des Kioskbetreibers zu. Nehmen wir an, Alice kauft zuerst einen Artikel zu 30 Cent. Damit umfasst die Abbuchung von Alice's Wallet insgesamt 33 Cent, denn sie trägt neben den 30 Cent für den Kioskartikel noch 2,5 Cent an *Wire fee*-Gebühr (10 Cent für die *Wire fee*-Gebühr des Verkäufers geteilt durch seinen Amortisationsfaktor 4) plus die *Deposit*-Gebühr von 0,5 Cent für ein eingesetztes Coin, denn Alice zahlt mit ihrem Coin des Nennwerts 128 Cent. Sie erhält dafür Wechselgeld mit Coins der Nennwerte 1, 2, 4, 8, 16 und 64 Cent. Für das Wechselgeld fallen ihr in dieser Beispielrechnung keine *Refresh*-Gebühren an.

Sollte Alice in dieser Beispielrechnung nun noch einen weiteren Artikel des gleichen Preises von 30 Cent kaufen, kann sie diesen nur mit ihren Coins der Nennwerte 2 und 32 Cent zusammen bezahlen. Die Abbuchung umfasst 30 Cent plus 2,5 Cent an *Wire fee*-Gebühr plus die *Deposit*-Gebühr von insgesamt 0,5 Cent. Hier wäre die *Deposit*-Gebühr für die kleineren

1 Mit dem Parameter default_max_deposit_fee können Verkäufer prozentuale oder absolute Grenzwerte ihrer Gebührenübernahme bestimmen.

2 Nehmen wir beispielsweise an, dass die Bäckerei zum Zeitpunkt der automatisch ausgelösten Sammelbuchung einen Umsatz erlöst hat, der das Vierfache von Alice's Umsatz beträgt. Auf das Girokonto würden ihr dann insgesamt 12,77 Euro überwiesen: Bei einem Umsatz von 4 x 3,23 Euro = 12,92 Euro trägt die Bäckerei Gebühren von insgesamt 15 Cent (4 x 1,25 Cent an *Deposit*-Gebühren plus 1 x 10 Cent *Wire fee*-Gebühr).

Coins mit 0,25 Cent pro Coin zwar geringer, aber sie braucht zwei Coins statt einem. Der Preis bleibt damit bei 33 Cent für den Kioskartikel mitsamt Gebühren, und in diesem Fall gibt es Wechselgeld mit einem Coin von 1 Cent Nennwert.

Lässt der Kioskbetreiber per Sammelbuchung nur den Umsatz dieser zwei Artikel an sein Girokonto überweisen, erhält er vom Exchange-Betreiber 55 Cent: 2 x 30 Cent Verkaufspreis plus 2 x 2,5 Cent *Wire fee*-Gebühr, die wegen des Amortisationsfaktors anteilig von Alice getragen werden, minus 10 Cent *Wire fee*-Gebühr, die der Exchange-Betreiber einbehält.

Der Exchange-Betreiber erhält für alle genannten Buchungen von Alice bei einem Gesamtumsatz von 3,83 Euro insgesamt 22,25 Cent: 20 Cent an *Wire fee*-Gebühren (jeweils 10 Cent vom Bäcker und vom Kioskbetreiber) sowie 2,25 Cent an *Deposit*-Gebühren (1,25 Cent + 2 x 0,5 Cent).

Tabellarisch zusammengefasst (hier dargestellt ohne Verkäuferanteil an den Gebühren):

| **Coins im Wallet** | **Artikel** | **VK-Preis** | **Deposit-** | **Wire fee:** | **Summen** |
|---|---|---|---|---|---|
| 4, 16, 32, 64, 128, 256 | | | **Gebühr** | **Alice's Anteil** | **500** |
| 1, 16, 32, 128 | Brötchen | 323 | 0 | - | 323 |
| 1, 1, 2, 4, 8, 16,16, 32, 64 | Zeitung 1 | 30 | 0,5 | 2,5 | 33 |
| 1, 1, 1, 4, 8, 16,16, 64 | Zeitung 2 | 30 | 0,5 | 2,5 | 33 |
| | **Summen** | **383** | **1** | **5** | **389** |
| **111 Cent Rest im Wallet** | | | | | **500** |

## 6.3 Beispielrechnungen: Mit Refresh-Gebühr

In dieser Beispielrechnung soll die *Refresh*-Gebühr 0,25 Cent auf das eingesetzte Coin betragen.

Alice überweist 5 Euro von ihrem Girokonto, wählt den Exchange mit der oben dargestellten Gebührentabelle und lässt ihr persönliches Wallet die blind signierten Coins abheben. Beim Abhebevorgang bekommt sie je eine Münze mit folgenden Nennwerten: 4, 16, 32, 64, 128, und 256 Cent. In der Bäckerei bezahlt sie Brötchen für 3,23 Euro mit Coins der Nennwerte 4 Cent, 64 Cent und 256 Cent (Deposit-Buchung über insgesamt 324 Cent). Ihr Wallet bekommt statt einem 1-Cent-Coin als Wechselgeld nun zwei Coins: Eines mit dem Nennwert 0,5 Cent und ein weiteres Coin zu 0,25 Cent, da von dessen Nennwert 0,25 Cent an *Refresh*-Gebühr für den Wechselgeld-Vorgang beim Exchange-Betreiber verbleiben. Für die drei eingesetzten Coins fallen an *Deposit*-Gebühren an: 1 x 0,25 Cent und 2 x 0,50 Cent, also insgesamt 1,25 Cent. Da die Bäckerei mit dem Parameter default_max_deposit_fee festgelegt hat, sich bis zu 0,5% ihres Umsatzes an den *Deposit*-Gebühren der Kunden zu beteiligen, fallen für Alice keine *Deposit*-Gebühren an. Der Kaufpreis beträgt insgesamt 323,25 Cent.

Der Zeitungskiosk soll hingegen in dieser Beispielrechnung nicht bereit sein, sich an den Gebühren seiner Kunden zu beteiligen. Da der Kiosk nur wenige Artikel verkauft, setzt der Kioskbetreiber seinen Amortisationsfaktor wire_fee_amortization für die *Wire fee*-Gebühr auf 4. Diesem stimmen die Kunden durch Einwilligung in die AGB des Kioskbetreibers zu. Alice trägt neben den 30 Cent für den Kioskartikel noch 2,5 Cent an *Wire fee*-Gebühr (10 Cent für die *Wire fee*-Gebühr des Verkäufers geteilt durch seinen Amortisationsfaktor 4) plus

die *Deposit*-Gebühr von 0,5 Cent für ein eingesetztes Coin, denn Alice zahlt mit ihrem Coin des Nennwerts 128 Cent. Sie erhält dafür Wechselgeld mit Coins der Nennwerte 0,25 und 0,5 sowie 2, 4, 8, 16 und 64 Cent. Der Exchange-Betreiber behält 0,25 Cent vom Nennwert des 1-Cent-Coin aufgrund der *Refresh*-Gebühr. Damit steigt der Kaufpreis auf insgesamt 33,25 Cent.

Sollte Alice in dieser Beispielrechnung nun noch einen weiteren Artikel des gleichen Preises von 30 Cent kaufen, kann sie diesen nur mit ihren Coins der Nennwerte 2 Cent und 2 x 16 Cent bezahlen. Zwar beträgt die *Deposit*-Gebühr 0,25 Cent pro Coin, aber dafür braucht sie nun drei Coins. Der Preis für den Artikel liegt dann bei 33,5 Cent: 30 Cent Verkaufspreis, 2,5 Cent *Wire fee*-Anteil, 0,75 Cent *Deposit*-Gebühr und 0,25 Cent *Refresh*-Gebühr. Der Exchange erhält von Alice's Wallet Coins von insgesamt 34 Cent und bucht 0,5 Cent Wechselgeld zurück.

Sollte der Kioskbetreiber nur diese zwei Artikel in der von ihm festgelegten Abrechnungsperiode bis zur Sammelbuchung verkaufen, erhält er vom Exchange-Betreiber 55 Cent überwiesen: 2 x 30 Cent für den Verkaufspreis plus 2 x 2,5 Cent an *Wire fee*-Gebühr, die von Alice getragen wurden, minus 10 Cent *Wire fee*-Gebühr, die der Exchange-Betreiber einbehält.

Der Exchange-Betreiber erhält für alle genannten Buchungen von Alice bei einem Gesamtumsatz von 3,83 Euro insgesamt 23,25 Cent: 20 Cent an *Wire fee*-Gebühr (jeweils 10 Cent von Bäckerei und Kiosk), 2,5 Cent an *Deposit*-Gebühr (1,25 + 0,5 + 0,75 Cent) und 0,75 Cent an *Refresh*-Gebühr.

Alice hat jetzt noch Coins der Nennwerte 2 x 0,25, 3 x 0,5, 4, 8, 32 und 64 Cent, insgesamt 110 Cent. Sollte Sie diese nicht ausgeben, wird das Wallet sie ein paar Monate vor dem Ablaufdatum durch frische Coins ersetzen. Dafür fallen dann grob im Jahresrhythmus *Refresh*-Gebühren an, bei den 8 Coins in Alice's Wallet wären dies bei 0,25 Cent pro aufgefrischtem Coin insgesamt 2 Cent.

Tabellarisch zusammengefasst (hier dargestellt ohne Verkäuferanteil an den Gebühren):

| **Coins im Wallet** | **Artikel** | **VK-Preis** | **Deposit-** | **Wire fee:** | **Refresh-** | **Summen** |
|---|---|---|---|---|---|---|
| 4, 16, 32, 64, 128, 256 | | | **Gebühr** | **Alice's Anteil** | **Gebühr** | **500** |
| 0.25, 0.5, 16, 32, 128 | Brötchen | 323 | 0 | - | 0,25 | 323,25 |
| 0.25, 0.25, 0.5, 0.5, 2, 4, 8, 16,16, 32, 64 | Zeitung 1 | 30 | 0,5 | 2,5 | 0,25 | 33,25 |
| 0.25, 0.25, 0.5, 0.5, 0.5, 4, 8, 32, 64 | Zeitung 2 | 30 | 0,75 | 2,5 | 0,25 | 33,5 |
| | **Summen** | **383** | **1,25** | **5** | **0,75** | **390** |
| **110 Cent Rest im Wallet** | | | | | | **500** |

# 7 Rechtliche Rahmenbedingungen, AGB und Datenschutzerklärung

## 7.1 Fragen rechtlicher Art

Dieses Unterkapitel befasst sich mit rechtlichen Fragen, z.B. Insolvenzfall, Unterscheidung zwischen Eigentum und Besitz an Coins und den von ihnen repräsentierten Werten, Haftung für diese Werte sowie Verfall und Eigentumsübergang von Coins an Exchange-Betreiber.

### 7.1.1 Treuhandkonto und Insolvenzfall

Exchange-Betreiber sind verpflichtet, das Kapital auf dem Treuhandkonto von der Einzahlung bis zum Ausgabevorgang nur für das Taler-Bezahlsystem zu verwenden. Deshalb weist im Regelfall das Treuhandkonto einen Saldo in Höhe der summierten Coin-Werte auf. Von einem Exchange-Betreiber erwartet zudem das Zahlungsdiensteaufsichtsgesetz, Sicherungsmaßnahmen und Frühwarnmechanismen gegen Insolvenz einzurichten und Anfangskapital in bestimmter Höhe vorzuhalten[1].

Solange kein Grund für eine Mitteilung drohender Insolvenz an das zuständige Amtsgericht vorliegt, ist ein Exchange zur Rücküberweisung des Treuhandkonto-Habensaldos an die ursprünglichen IBAN-Konten jederzeit berechtigt. Das Recoup-Protokoll kann er also zu seinem geordneten Marktaustritt nutzen. Im Insolvenzfall würden jedoch alle Coin-Werte in die Konkursmasse fallen und ihre Eigentümer zu Gläubigern werden. Der Exchange dürfte dann keinen Recoup ohne Beschluss eines Insolvenzgerichts durchführen.

Exchange-Betreiber sollten mit geeigneten Vorkehrungen sicherstellen, dass das Vermögen des Treuhandkontos nicht unter das Insolvenzrecht fällt, um zu vermeiden, dass im Konkursfall das dort verwahrte Guthaben dem Massevermögen zugeschlagen wird. Dieses Guthaben umfasst zum einen den Wert der Coins, die von diesem Exchange signiert wurden und sich rechtlich im Eigentum der Wallet-Besitzer befinden, zum anderen den Wert der *deponierten* Coins dieses Exchange, für die Verkäufer bislang noch keine Sammelbuchung zugunsten ihrer Girokonten ausgelöst bekamen. Die Vorkehrungen gegen Insolvenz schützen damit einerseits die Verbindlichkeiten von Exchange-Betreibern gegenüber den Coin-Eigentümern, andererseits die Forderungen der Verkäufer gegen Exchange-Betreiber auf Überweisung ihrer Umsatzeinkünfte.

1 Ein Exchange-Betreiber muss die Auflagen der BaFin erfüllen, in ihrem Register eingetragen sein und Anfangskapital vorhalten („hartes Kernkapital“, mindestens 20.000 Euro Anfangskapital für Finanztransfergeschäfte, als Zahlungsauslösedienst 50.000 Euro, als E-Geld-Emittent 350.000 Euro, siehe §12 Zahlungsdiensteaufsichtsgesetz).

### 7.1.2 Verjährung von Coin-Werten

Die Verjährung erlaubt nur bei einer hohen Nutzerzahl des Bezahlsystems eine nennenswerte Einkommenserzielung. Wenn dieses Einkommen aus dem Verfall von Coin-Guthaben alle Kosten des Betriebs eines Exchange deckt, könnte man dessen Gebührenordnung wesentlich vereinfachen. Dieses Einkommen ist jedoch unstetig und unvorhersehbar, eignet sich von daher nicht für eine nachhaltige Finanzierung. Außerdem würden Exchange-Betreiber darauf verzichten, ihren Nutzern Anreize zu ökonomischem Buchungsverhalten zu geben[2].

## 7.2 AGB-Formulierung

Die Formulierung der Allgemeinen Geschäftsbedingungen, die ein Exchange seinen Nutzern anzeigt und beim Abheben bzw. bei neuen Nutzungsbedingungen von diesen bestätigen lässt, ist noch in Entwicklung. Als Arbeitsvorlage zur Orientierung dienen die AGB eines Taler-Exchange (*Terms of Service* in englischer Sprache, die nur exemplarisch zu verstehen sind). Die später gebräuchlichen deutschen AGB für Taler-Nutzer werden einfach und deutlich formuliert sein und unmissverständlich auf die Pflichten der Nutzung und mögliche Risiken eines Wertverlusts hinweisen.

## 7.3 Datenschutzerklärung

Die englischsprachige *Privay Policy* dient als Arbeitsvorlage für die deutschsprachige DSGVO-konforme Datenschutzerklärung:

This Privacy Policy describes the policies and procedures of Taler Systems SA (“we,” “our,” or “us”) pertaining to the collection, use, and disclosure of your information on our sites and related mobile applications and products we offer (the “Services” or “Taler Wallet”). This Privacy Statement applies to your personal data when you use our Services, and does not apply to online websites or services that we do not own or control.

### Overview

Your privacy is important to us. We follow a few fundamental principles: We don’t ask you for personally identifiable information (defined below). That being said, your contact information, such as your phone number, social media handle, or email address (depending on how you contact us), may be collected when you communicate with us, for example to report a bug or other error related to the Taler Wallet. We don’t share your information with third parties except when strictly required to deliver you our Services and products, or to comply with

2 Anbieter von Gutscheinkarten nutzen bereits als Geschäftsmodell die Einkommenserzielung aus der Verjährung von Gutscheinen. Zu beachten sind dabei §§ 195 und 199 BGB. Es gilt in der BRD eine gesetzliche Verjährungsfrist von 3 Jahren ab dem Ende des Jahres, in dem ein Gutschein erstellt wurde. Bei Taler-Coins handelt es sich jedoch nicht um Gutscheine, sondern um Eigentum, dessen Eigentümer allerdings dem Exchange-Betreiber namentlich nicht bekannt sind, da die Coins blind signiert werden.

the law. If you have any questions or concerns about this policy, please reach out to us at privacy@taler-systems.net.

### How you accept this policy

By using our Services or visiting our sites, you agree to the use, disclosure, and procedures outlined in this Privacy Policy.

### What personal information do we collect from our users?

The information we collect from you falls into two categories:

1. personally identifiable information (i.e., data that could potentially identify you as an individual) ("Personal Information"), and
2. non-personally identifiable information (i.e., information that cannot be used to identify who you are) ("Non-Personal Information"). This Privacy Policy covers both categories and will tell you how we might collect and use each type.

We do our best to not collect any Personal Information from Taler Wallet users. We believe that the Taler Wallet never transmits personal information to our services without at least clear implied consent, and we only process and retain information with a strict business need. That being said, when using our Services, we inherently have to collect the following information:

- Bank account details necessary when receiving funds from you to top-up your wallet or to transfer funds to you when you are being paid via Taler. At the current experimental stage, only the pseudonym and password you entered in the bank demonstrator is stored.
- The amounts being withdrawn or deposited, with associated unique transaction identifiers and cryptographic signatures authorizing the transaction. Note that for purchases, we cannot identify the buyer from the collected data, so when you spend money, we only receive non-personal information.
- When you contact us. We may collect certain information if you choose to contact us, for example to report a bug or other error with the Taler Wallet. This may include contact information such as your name, email address or phone number depending on the method you choose to contact us.

### How we collect and process information

We may process your information for the following reasons:

- to transfer money as specified by our users (Taler transactions);
- to assist government entities in linking income to the underlying contract
- to support you using the Taler Wallet or to improve our Services

### How we share and use the information we gather

We may share your Personal Data or other information about you only if you are a merchant receiving income, with your bank, to the degree necessary to execute the payment.

We retain Personal Data to transfer funds to the accounts designated by our users. We may retain Personal Data only for as long as mandated by law and required for the wire transfers.

We primarily use the limited information we receive directly from you to enhance the Taler Wallet. Some ways we may use your Personal Information are to: Contact you when necessary to respond to your comments, answer your questions, or obtain additional information on issues related to bugs or errors with the Taler Wallet that you reported.

### Agents or third party partners

We may provide your Personal Information to our employees, contractors, agents, service providers, and designees ("Agents") to enable them to perform certain services for us exclusively, including: improvement and maintenance of our software and Services. By accepting this Privacy Policy, as outlined above, you consent to any such transfer.

### Protection of us and others

We reserve the right to access, read, preserve, and disclose any information that we reasonably believe is necessary to comply with the law or a court order.

### What personal information can I access or change?

You can request access to the information we have collected from you. You can do this by contacting us at privacy@taler-systems.net. We will make sure to provide you with a copy of the data we process about you. To comply with your request, we may ask you to verify your identity. We will fulfill your request by sending your copy electronically. For any subsequent access request, we may charge you with an administrative fee. If you believe that the information we have collected is incorrect, you are welcome to contact us so we can update it and keep your data accurate. Any data that is no longer needed for purposes specified in the "How We Use the Information We Gather" section will be deleted after ninety (90) days.

### Data retention

If you uninstall the Taler Wallet mobile applications from your device, or request that your information be deleted, we still may retain some information that you have provided to us to maintain the Taler Wallet or to comply with relevant laws.

### Data security

We are committed to making sure your information is protected. We employ several physical and electronic safeguards to keep your information safe, including encrypted user passwords,

two factor verification and authentication on passwords where possible, and securing connections with industry standard transport layer security. You are also welcome to contact us using GnuPG encrypted e-mail. Even with all these precautions, we cannot fully guarantee against the access, disclosure, alteration, or deletion of data through events, including but not limited to hardware or software failure or unauthorized use. Any information that you provide to us is done so entirely at your own risk.

### Changes and updates to privacy policy

We reserve the right to update and revise this privacy policy at any time. We occasionally review this Privacy Policy to make sure it complies with applicable laws and conforms to changes in our business. We may need to update this Privacy Policy, and we reserve the right to do so at any time. If we do revise this Privacy Policy, we will update the "Effective Date" at the bottom of this page so that you can tell if it has changed since your last visit. As we generally do not collect contact information and also do not track your visits, we will not be able to notify you directly. However, the Taler Wallet may inform you about a change in the privacy policy once it detects that the policy has changed. Please review this Privacy Policy regularly to ensure that you are aware of its terms. Any use of our Services after an amendment to our Privacy Policy constitutes your acceptance to the revised or amended agreement.

### International users and visitors

Our Services are hosted in Switzerland. If you are a user accessing the Services from the European Union, Asia, US, or any other region with laws or regulations governing personal data collection, use, and disclosure that differ from Swiss laws, please be advised that through your continued use of the Services, which is governed by Swiss law, you are transferring your Personal Information to Switzerland and you consent to that transfer.

### Questions

Please contact us at privacy@taler-systems.net if you have questions about our privacy practices that are not addressed in this Privacy Statement.

# 8 Regulatorische Compliance

1. Datensicherung für Wallets: Das Taler-Wallet verfügt über eine integrierte Backup-Lösung. Mit dieser können Nutzer ihre Coins und andere Wallet-Daten verschlüsseln und bei einem vom Nutzer bestimmten Backup-Betreiber hinterlegen. Taler Systems SA wird sicherstellen, dass mindestens drei Backup-Betreiber existieren. Die Software für den serverseitigen Betrieb der Backup-Lösung wird quelloffen der Allgemeinheit zur Verfügung gestellt, somit können qualifizierte Kunden ihre eigene Backup-Lösung betreiben bzw. andere Unternehmen eigene Speicherorte anbieten. Für die Nutzung des Backup-Angebots können die Backup-Betreiber Gebühren verlangen, welche auch über das Taler-Wallet direkt bezahlt werden. Die Sicherung der Backup-Daten kann je nach Betreiber über geheime Schlüssel oder auch über Multi-Faktor-Authentifizierung erfolgen.

2. Das Abhebevolumen pro Tag und pro Kunde soll begrenzt werden. Dies dient sowohl zum Selbstschutz der Kunden, zum Schutz vor einem „Bank Run“ und leistet ggf. einen Beitrag zur Durchsetzung von AML-Richtlinien. Wir gehen im Moment von einer Obergrenze von 1000 Euro pro Tag und Kunde aus, da diese Grenze z.B. auch für Bargeld üblich ist.

3. Händler können eine Obergrenze des Transaktionsbetrags pro Vorgang festlegen. Bestehende Obergrenzen z.B. für Kreditkarten ohne TAN-Autorisierung am Point of Sale gemäß PSD2 sind 50 Euro pro Buchung maximal fünfmal in Folge. Darüber hinaus gilt aktuell gemäß PSD2-Richtlinie die Kann-Option für Zahlungsdienstleister, welche Kundenbuchungen in der Summe von maximal 150 Euro ohne starke Authentifizierung erlaubt. Die genaue Anwendbarkeit dieser Richtlinien ist unklar, wobei wir bislang von Obergrenzen zwischen 50 und 1000 Euro pro Geschäftsvorgang ausgehen, ggf. auch in Abhängigkeit vom Geschäftsbereich des Händlers.

4. Die Identitätsfeststellung (KYC-Prüfung) erfolgt sowohl für Kunden als auch für Verkäufer stets bei den Geschäftsbanken. Für die Teilnahme am Bezahlsystem benötigen beide Seiten ein SEPA-Konto, das sie nur nach Klärung ihrer Identität bzw. der wirtschaftlich Berechtigten eröffnen können. Eine theoretische Ausnahme bei der Identitätsfeststellung wären Empfänger von Sozialleistungen, die z.B. von staatlichen Behörden ihre Sozialleistungen mithilfe des durch GNU Taler ermöglichten Tipping-Verfahrens auch ohne eigenes Girokonto empfangen könnten. In diesem Fall würde die Behörde die Identitätsfeststellung der Leistungsempfänger übernehmen müssen.

5. Die Verantwortung für AML bleibt bei den Geschäftsbanken der Verkäufer. Die Banken werden dazu von einer API des Exchange unterstützt, welche es erlaubt, die eingehenden

SEPA-Buchungen mit den Vertragstexten jedes abgeschlossenen Geschäftsvorgangs zu verknüpfen. Diese API kann z.B. auch von Steuerbehörden genutzt werden, um die Geschäftsvorgänge der Verkäufer im Rahmen einer Steuerprüfung zu analysieren. Transaktionen an sanktionierte Empfänger werden - falls notwendig - von deren Geschäftsbank storniert bzw. eingefroren. Internationale Überweisungen auf Konten außerhalb des Euro-Währungsbereichs sind nicht erlaubt und werden nicht ausgeführt.

6. Die unabhängigen Auditoren (Code Blau GmbH) sind für unabhängige Prüfungen in folgenden Bereichen zuständig: Technisch (Quellcode), Exchange-Datenbank (Prüfung der gesammelten kryptografischen Beweise), organisatorische Sicherheit, SEPA-Buchungen des Exchange (Credit und Debit) sowie die Bilanzprüfung. Die Code Blau GmbH würde ihre Berichte der Taler Systems SA, den Exchange-Betreibern und der BaFin regelmäßig zur Verfügung stellen bzw. bei Unregelmäßigkeiten auch sofort Meldung erstatten. In jedem Fall wird ein sicherer und bankenüblich zertifizierter Rechenzentrumsbetrieb bereitgestellt.

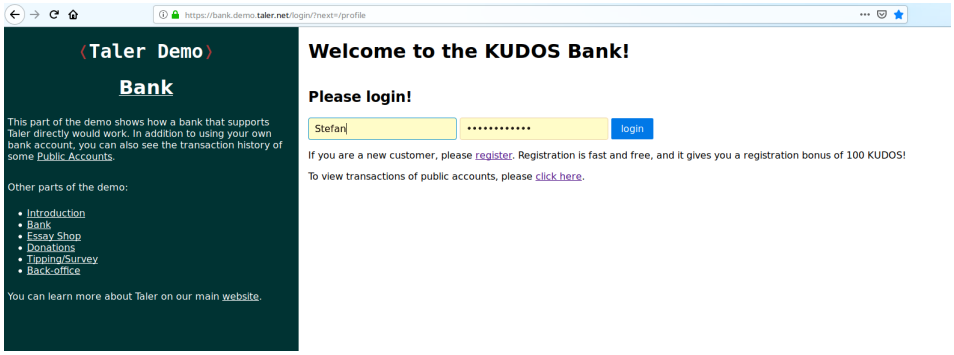
# 9 Screenshots der Geschäftsvorgänge

Die Screenshots zeigen die einzelnen Handlungsschritte aus Sicht der Nutzer des Taler-Bezahlsystems. Die Abschnitte 9.1 und 9.2 zeigen die Abhebe- und Ausgabevorgänge mit dem Wallet eines Smartphones mit Android-Betriebssystem (für weitere Smartphone-OS in Entwicklung), Abschnitt 9.3 veranschaulicht den Abhebevorgang auf das Smartphone-basierte Wallet mit der ATM-Anwendung „Taler-Cashier“. In Abschnitt 9.4 folgen Screenshots des Bezahlvorgangs mit der Point of Sale-Anwendung „Merchant POS“.

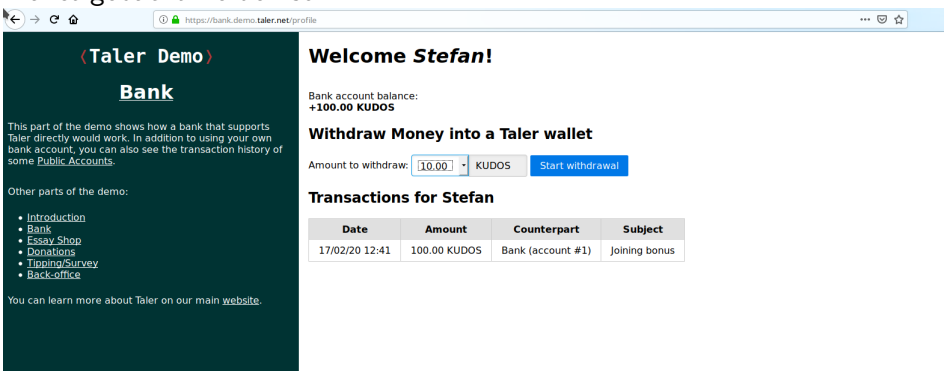
KUDOS stellen dabei eine Phantasiewährung des experimentellen Taler-Exchange dar, die KUDOS-Bank ist eine exemplarische Bank. Wenn ein Exchange Euro anbietet, stünde EURO als Währung anstelle der KUDOS.

## 9.1 Abhebevorgang vom Girokonto in das Wallet eines Android-Smartphones

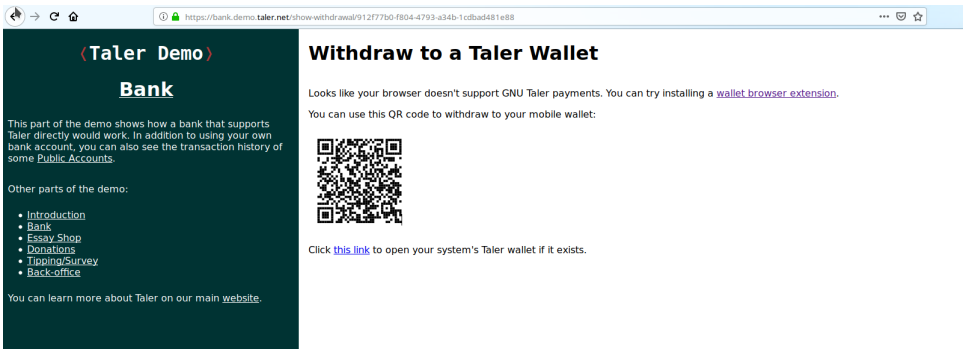
1. Der Kunde meldet sich an bei seiner Geschäftsbank an, die einen Taler-Exchange und damit Taler als Verfahren zum Abheben in Wallets anbietet:



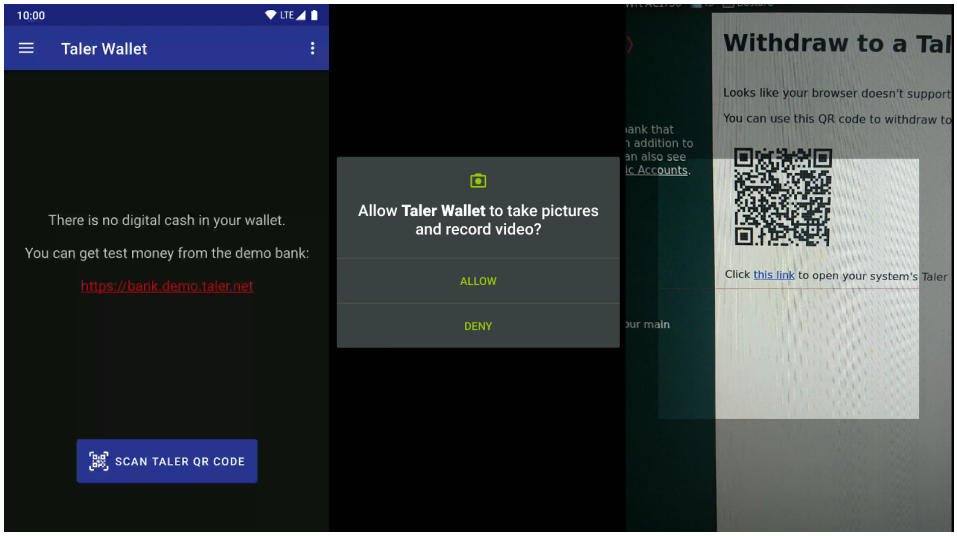
2. Der Kunde wählt das Taler-Verfahren und gibt die Geldmenge ein, die auf das persönliche Wallet gebucht werden soll:



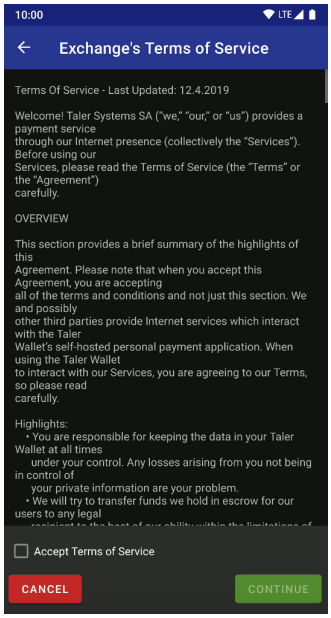

3. Die Bank-Webseite zeigt den QR-Code an, den die Bank-API erzeugt hat:



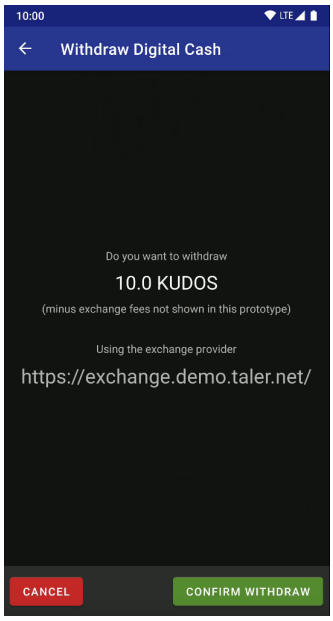
4. Der Kunde öffnet die App des Taler-Wallet, sieht den aktuellen Coin-Bestand (Bild links), muss ggf. seinem Smartphone die Aufnahme von Fotos erlauben (Bild Mitte) und scannt mit dem Smartphone den QR-Code auf der Bank-Webseite (Bild rechts):



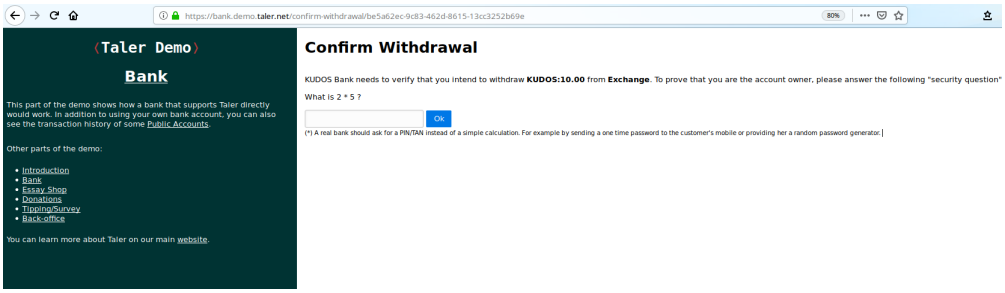
5. Der Kunde wählt den Exchange [hier noch nicht bildlich dargestellt], liest die allgemeine Gebührenordnung und die Gebühren für den aktuellen Abhebevorgang [hier noch nicht bildlich dargestellt] sowie die Allgemeinen Geschäftsbedingungen des Taler-Bezahlsystems, welche er bestätigen muss:



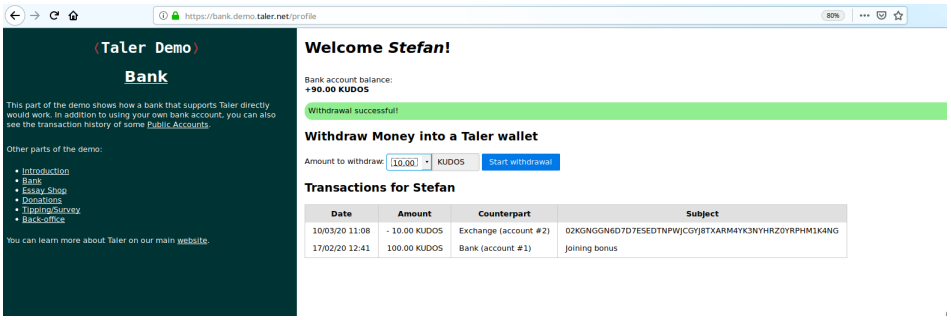

6. Der Kunde bestätigt den Abhebevorgang in der App:



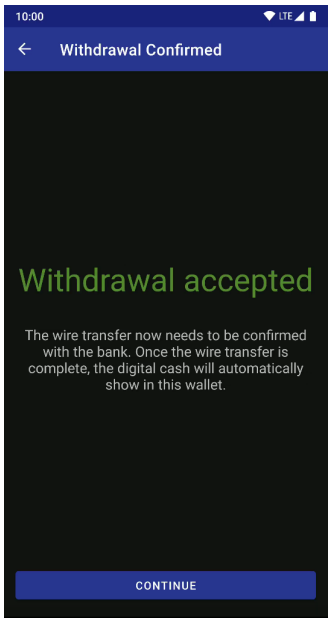
7. Der Kunde wird auf die Benutzerführung der Bank-Webseite bzw. des ATM-Terminals zurückverwiesen. Es werden ihm nochmals der abzuhebende Betrag und der gewählte Exchange angezeigt. Er muss gegenüber der Bank endgültig bestätigen, dass der Abhebevorgang nun ausgelöst werden soll. Bei einer Zwei-Faktor-Autorisierung verlangt die Bank vom Kunden eine TAN-Eingabe. Die TAN-Abfrage der Demo-Version wird hier in Form eines Captchas versinnbildlicht:



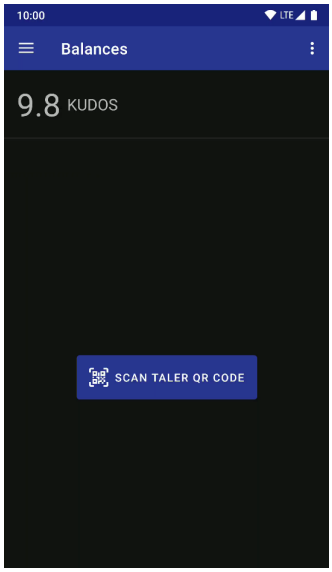

Die Bank führt die Buchung des Betrags an den gewählten Exchange damit aus:



8. Der gewählte Exchange bildet eine Reserve über den Betrag der Girokontoüberweisung, aus welcher das empfangende Wallet Coins abheben kann, die in der Summe dem angeforderten Betrag entsprechen:



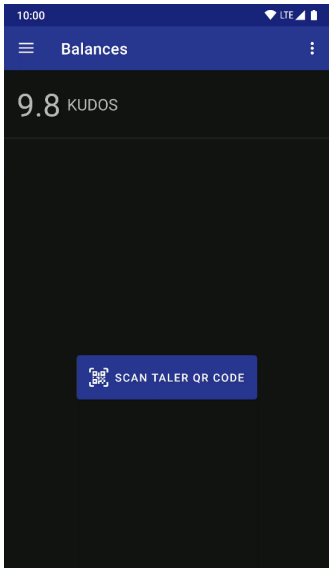

9. Das Wallet des Kunden hat die Coins abzüglich der Überweisungsgebühr und der Transaktionsgebühr (für die Buchung vom Girokonto zum Exchange und die Transaktionen ins Wallet) empfangen:



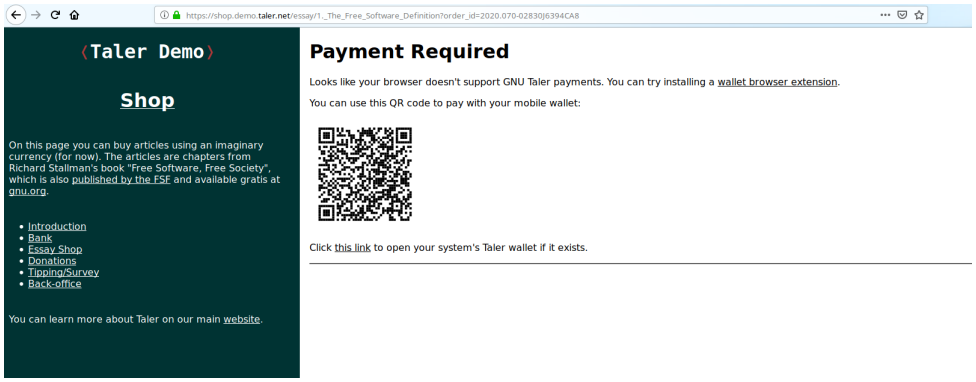
## 9.2 Ausgabevorgang mit dem Wallet eines Smartphones (Android-Betriebssystem)

Dieser Abschnitt veranschaulicht einen regulären Ausgabevorgang z.B. bei Vertragsschluss zum Erwerb von Gütern im Internet (den Bezahlvorgang am Point of Sale beschreibt Abschnitt 9.4).

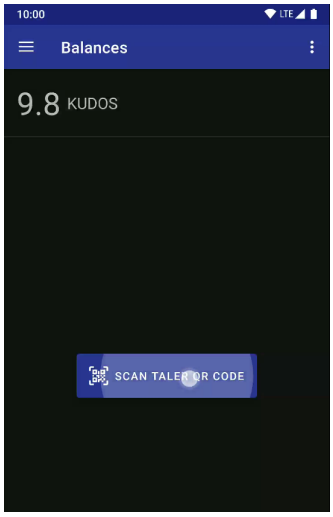
1. Jeder Wallet-Besitzer wird vor einem Kauf den Bestand der verfügbaren Coins prüfen wollen und bekommt deren Summe in der Taler-App angezeigt:

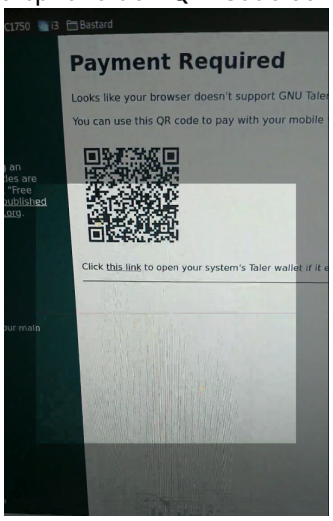



2. Der Verkäufer eines Guts, das der Kunde zu erwerben wünscht, betreibt die von Taler Systems SA zur Integration in Shops bereitgestellte Verkäufer-Software „Merchant POS“, welcher einen QR-Code über den Kauf erzeugt und dem Kunden auf der Webseite anzeigt:

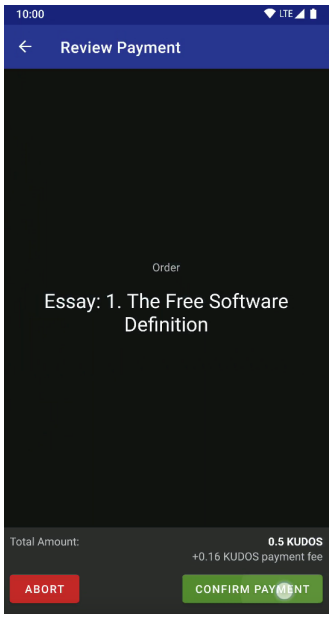


3. Der Kunde scannt mit dem Smartphone den QR-Code auf der Verkäufer-Webseite:

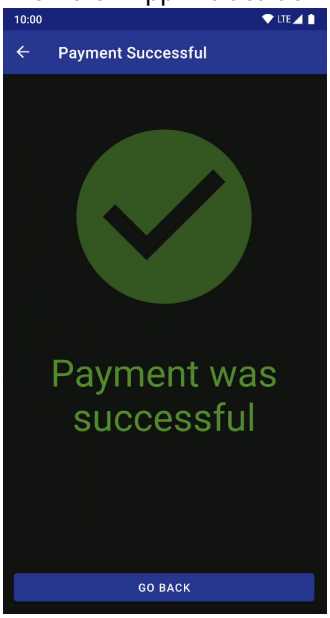


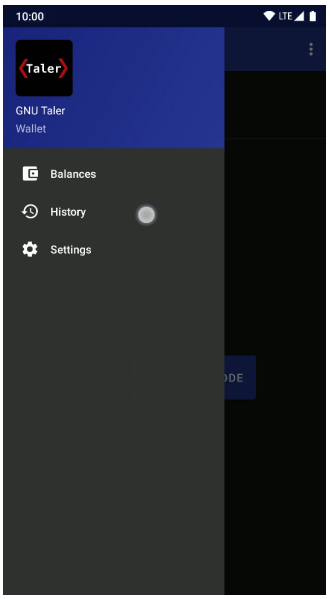

4. Der Kunde erhält Artikelbezeichnungen sowie den Gesamtbetrag über den Kaufpreis in der Taler-App angezeigt und wird um Bestätigung gebeten, um die Zahlung auszulösen:

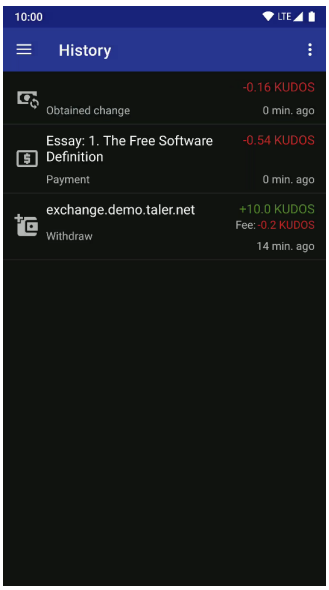


5. Die Taler-App meldet dem Kunden die erfolgte Bezahlung:

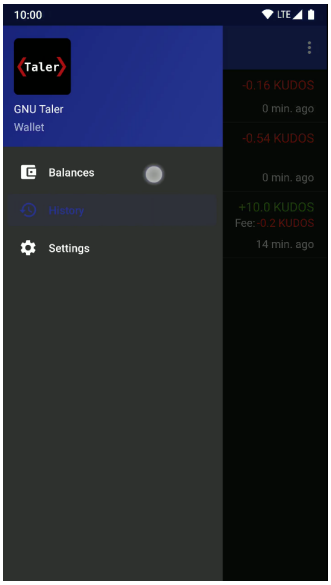


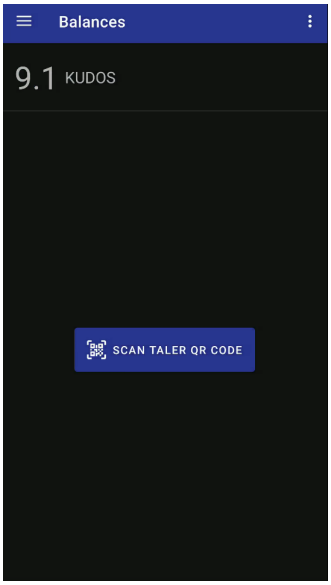

6. Der Kunde kann sich stets die Historie der Käufe anzeigen lassen:



7. Der Kunde kann sich stets den Bestand an Coins im Wallet anzeigen lassen:



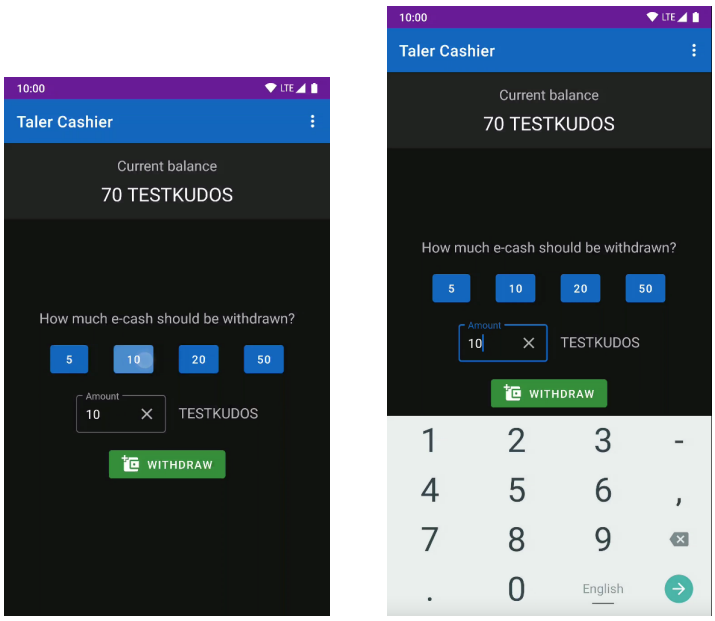
## 9.3 Abhebevorgang auf ein Smartphone-basiertes Wallet mit „Taler-Cashier“ als Automated Teller Machine-Anwendung

Ein Kassierer oder Kassenwart, der Taler-Cashier verwendet, hat die Möglichkeit, seinen Kunden das von ihnen erhaltene Geld in Form von Coins zu senden. Die Funktion entspricht einem ATM-Bankautomaten, der Bargeld annimmt und den Geldwert auf ein Wallet aufbucht. Als Kassenwart auftreten können Privatpersonen, meist wird es sich jedoch um Betreiber von Geschäften oder Kiosken handeln. Sowohl Kassenwart als auch Kunde müssen jeweils ein Smartphone besitzen. Der Kassenwart muss den Taler-Cashier, der Kunde das Taler-Wallet installiert haben. Die Anwendung wird zum heutigen Entwicklungsstand nur zu Demonstrationszwecken eingesetzt. Ihr großflächiger Einsatz im realen Geschäftsbereich ist noch nicht beabsichtigt. Sie lässt sich jedoch zukünftig implementieren als Möglichkeit der Bareinzahlung von Kunden, die noch nicht oder nicht mehr über ein Bankkonto verfügen.

Kassierer müssen das Geldwäschegesetz (GwG) und die Vorschriften gegen Geldwäsche (Know-Your-Customer, Anti Money Laundering) befolgen und daher bei der Annahme von Bargeldmengen ab der gesetzlich festgelegten Grenze von zurzeit 10.000 Euro die Identifizierung des Einzahlenden bzw. des wirtschaftlich Berechtigten verlangen.

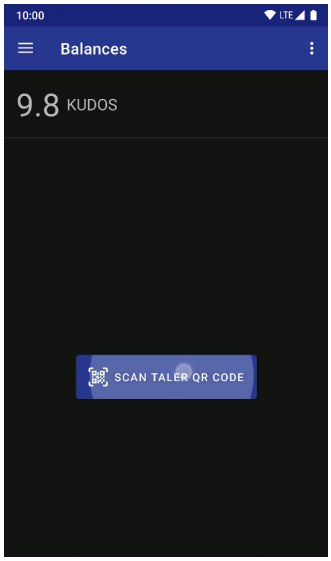
Taler-Cashier verfügt über ein internes Limit an Coin-Beträgen. Dieses Limit hat die gleiche Wirkung wie ein begrenzter Bestand an Bargeld in einer Registrierkasse. Damit ist das Risiko eines Diebstahl von Werten aus der Cashier-App beschränkt, wenn beispielsweise der Kassenwart mit Gewalt zu einer Versendung von Coins gezwungen werden sollte.

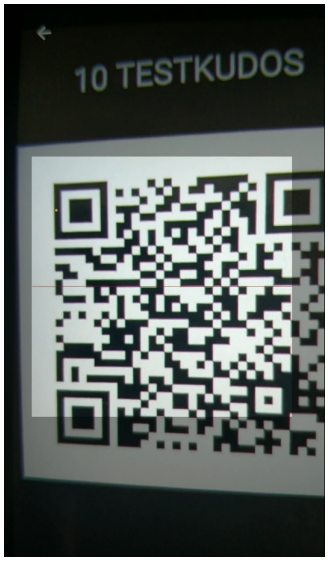
1. Der Kassenwart öffnet die App Taler-Cashier und gibt dort den Betrag ein, den der Kunde ihm angegeben hat - entweder durch Tippen auf die voreingestellten Felder (Bild links) oder durch manuelle Eingabe (Bild rechts):



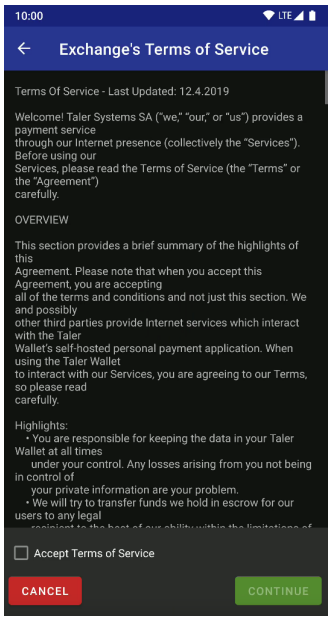
2. Die Cashier-App erzeugt einen QR-Code auf dem Gerät des Kassenwarts:


3. Der Kunde scannt mit seinem Smartphone den QR-Code auf der Anzeige des Kassenwarts:

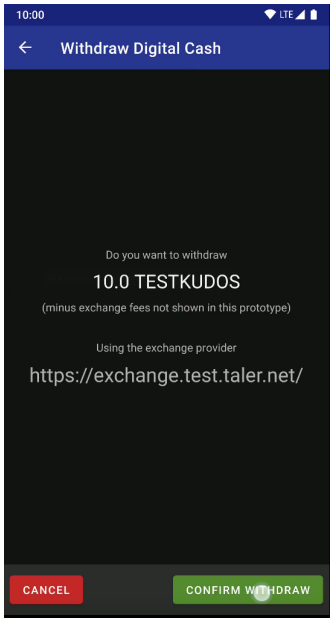


4. Der Kunde liest in seinem Gerät die Allgemeinen Geschäftsbedingungen des Taler-Bezahlsystems, welche er bestätigen muss:

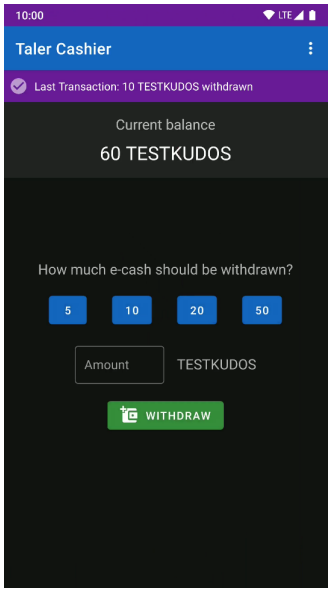



5. Der Kunde muss den Betrag bestätigen:



6. Die Cashier-App verlangt vom Kassenwart die Bestätigung, dass sein Wallet mithilfe der Cashier-Anwendung Coins an den Kunden senden darf:


7. Die Cashier-App meldet die erfolgte Abbuchung und zeigt den aktuellen Bestand an verbleibenden Coins an:




8. Das Wallet des Kunden erhält die Coins.

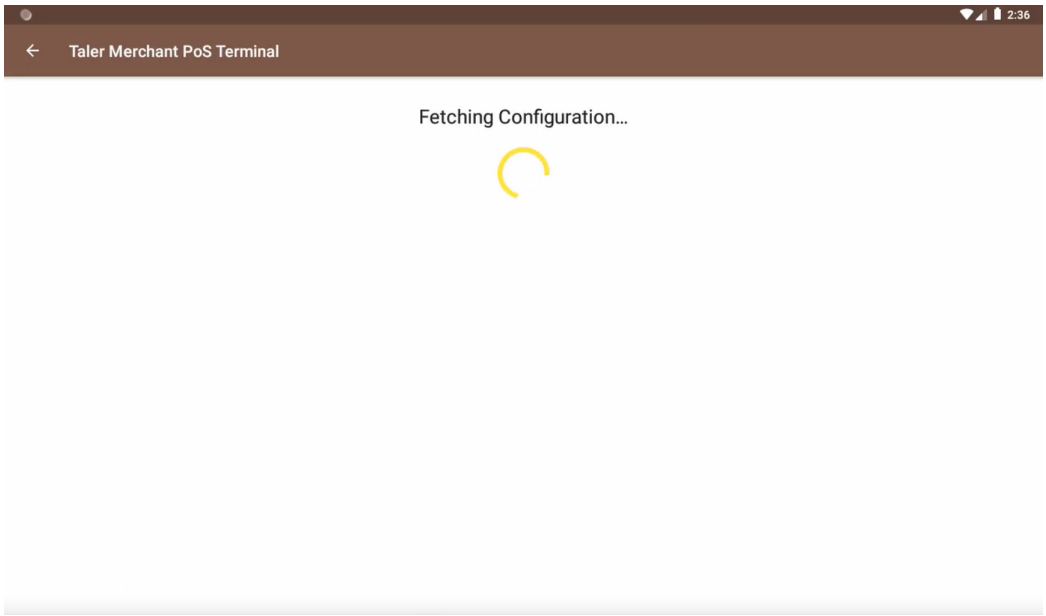
## 9.4 Bezahlvorgang mit der Point of Sale-Anwendung „Merchant POS“

Der „Taler Merchant“ ist eine Beispielanwendung für das Bestellen und Bezahlen an Verkaufsstellen. Programmierer können den Code dieser Anwendung in bestehende Kassen- und Warenwirtschaftssysteme oder Webshops einbauen. Die einfache Integration des Codes trägt dazu bei, dass sich das Taler-Bezahlsystem in der Handelswelt schnell verbreiten wird.

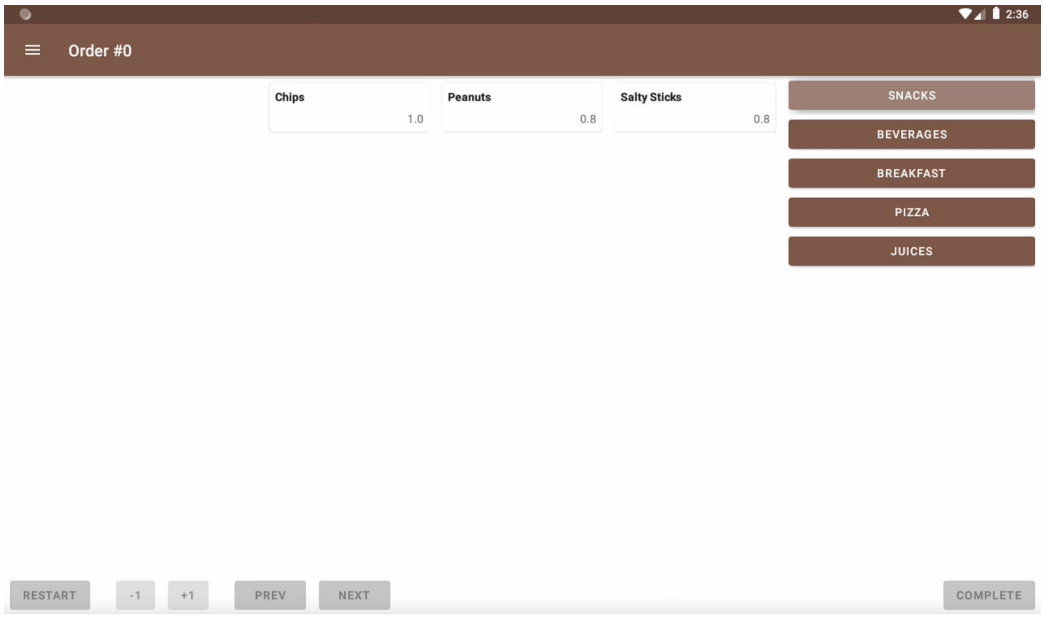
Nachfolgend verdeutlichen die Screenshots die Benutzerführung auf Käuferseite und Verkäuferseite (Bestellung, Summierung, Bezahlung mit Coins aus dem persönlichen Wallet der Kunden, Verkaufshistorie).

Der dargestellte Vorgang - hier am Beispiel einer Cafeteria - bezieht sich wie in den vorhergehenden Geschäftsvorgängen auch auf Wallets in Android-Smartphones. KUDOS sind wie gehabt der Platzhalter für EURO.

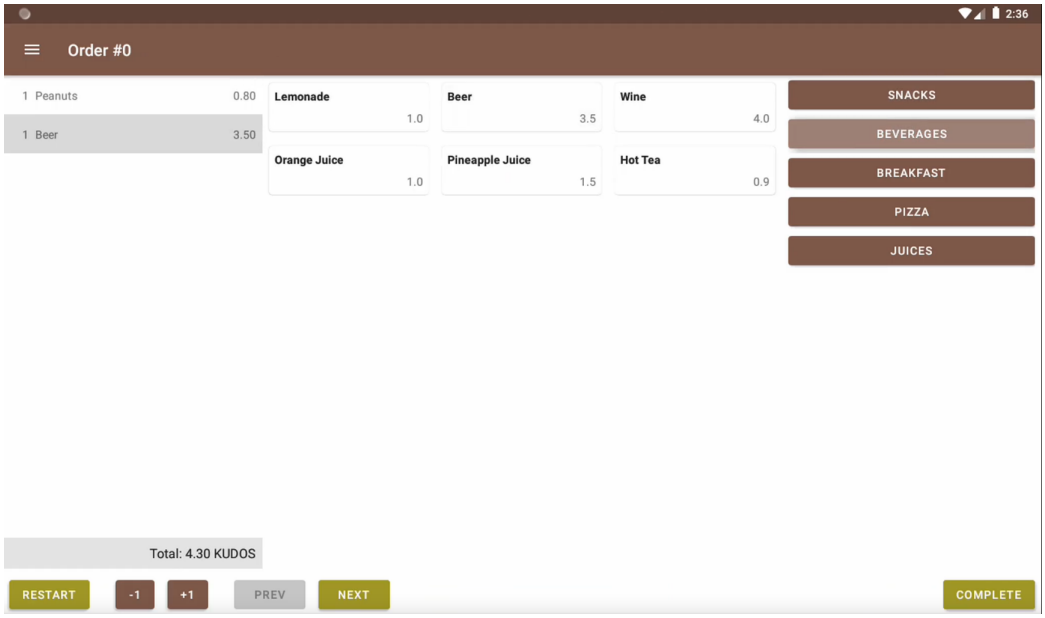
1. Das POS-Terminal wird gestartet:



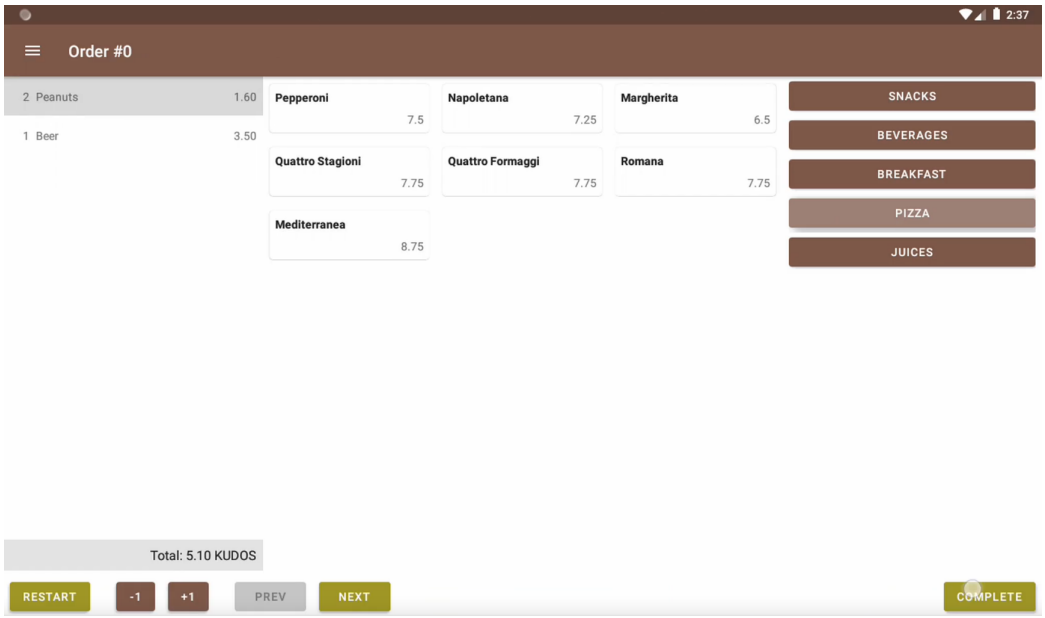
2. Im Auswahl-Menü werden die gewünschten Artikel gesammelt und ihre Beträge summiert:



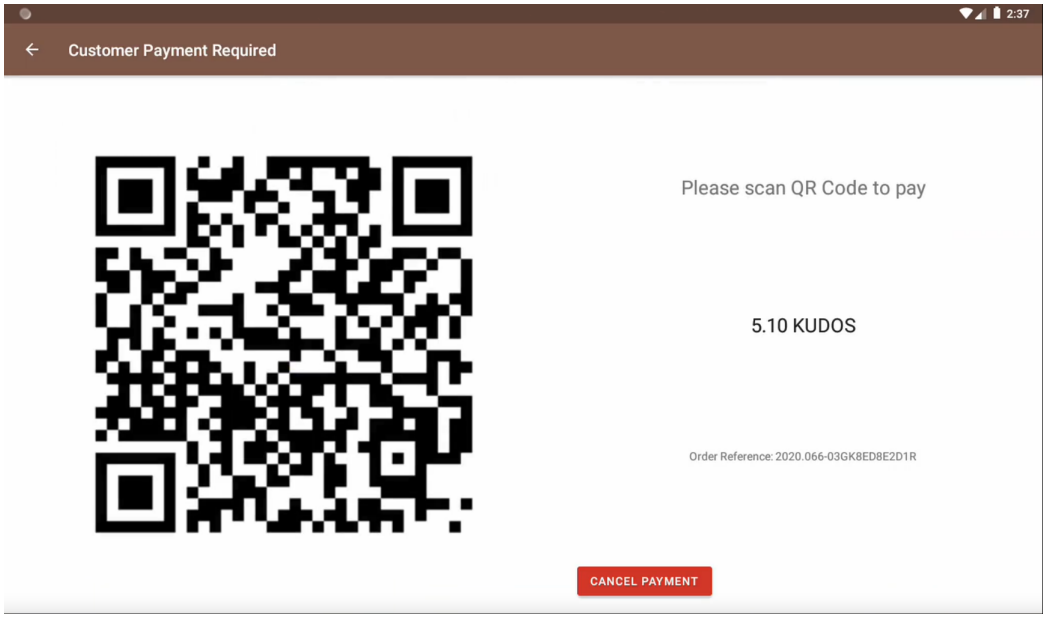

3. Dito. Der Kunde kann summieren lassen, soviel der Coin-Bestand auf dem Wallet erlaubt:



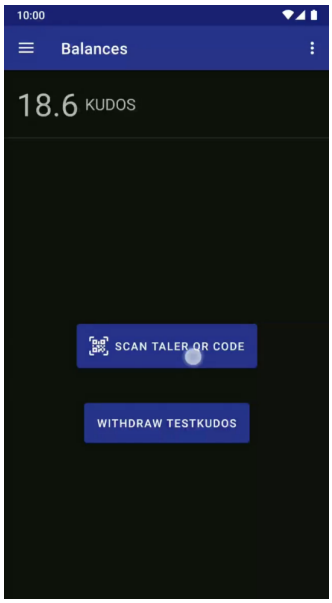
4. Ist die Bestellung vollendet, tippt der Terminal-Nutzer die Taste „Complete“, die Anwendung erzeugt dann einen QR-Code:

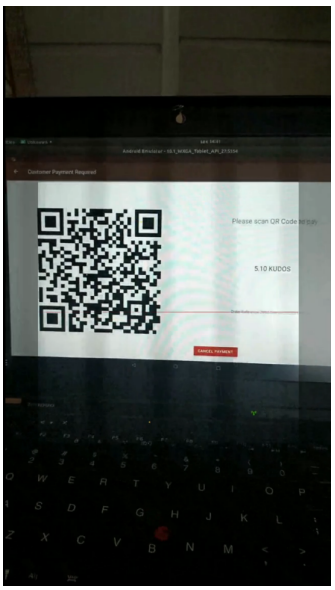



5. Dieser QR-Code wird dem Kunden zum Scannen angezeigt:

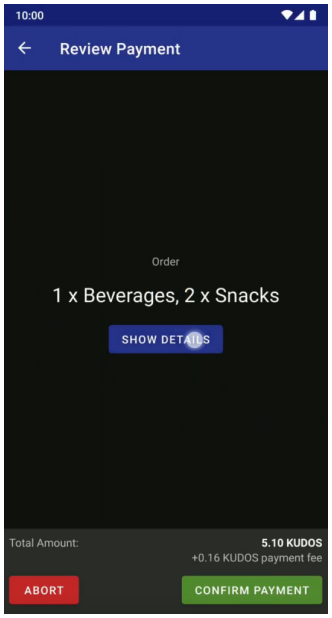


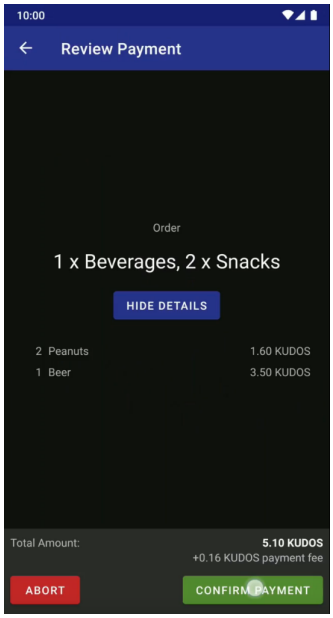
6. Der Kunde scannt den QR-Code mit seinem Smartphone:



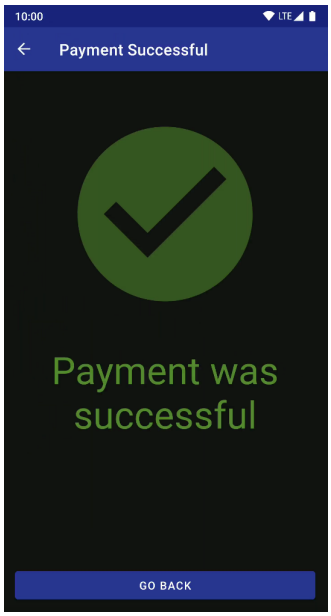



7. Der Kunde kann sich die Details des Kaufs anzeigen lassen und die Details auch wieder einklappen. Zum Kauf der Artikel muss er bestätigen:

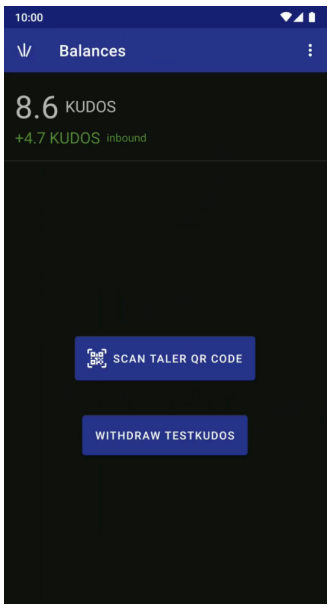


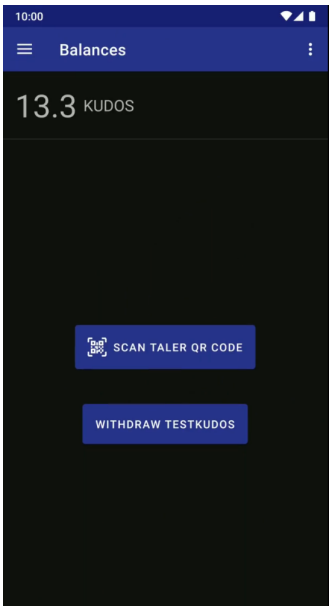



8. Es erscheint eine Bestätigung des erfolgten Kaufs:

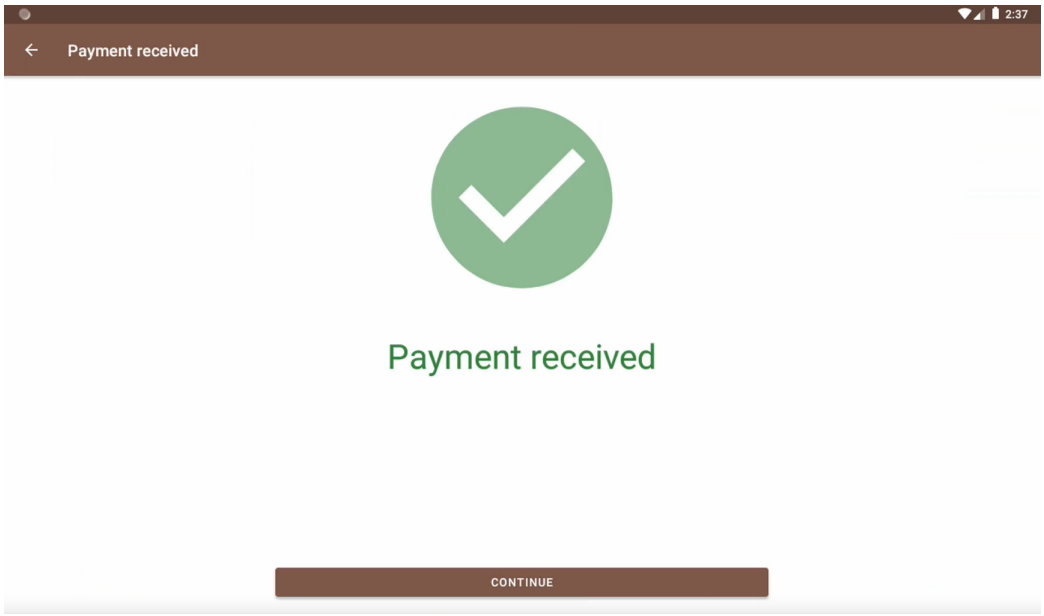



9. Hier wurde ein Coin über 10 KUDOS verbraucht, davon gehen 5,1 KUDOS zugunsten des Verkäufers, 0,2 KUDOS an den Exchange (als Einbehalt für Gebühren) und 4,7 KUDOS Wechselgeld an das Wallet zurück:

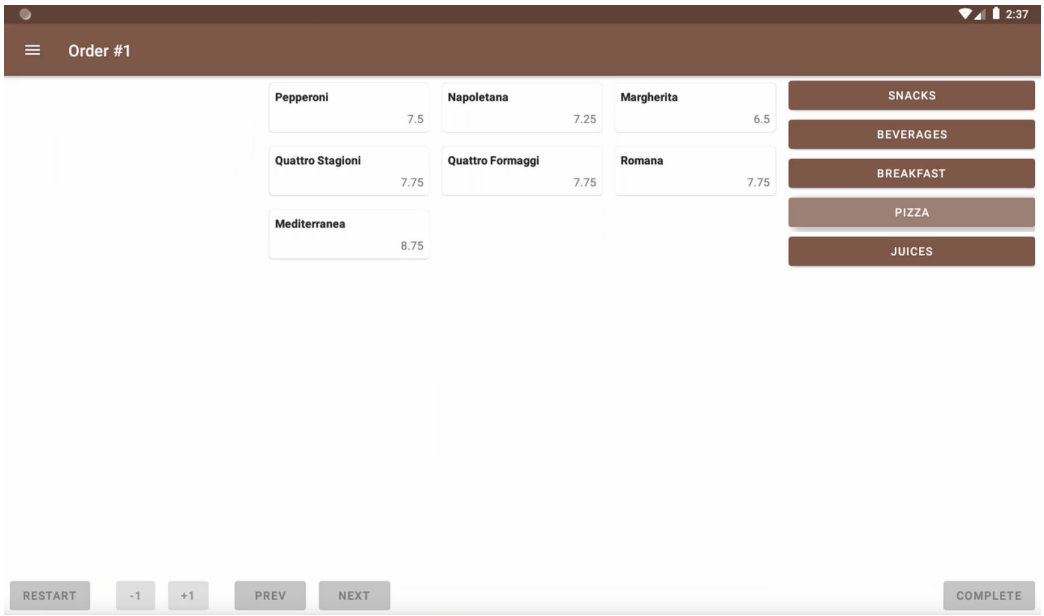


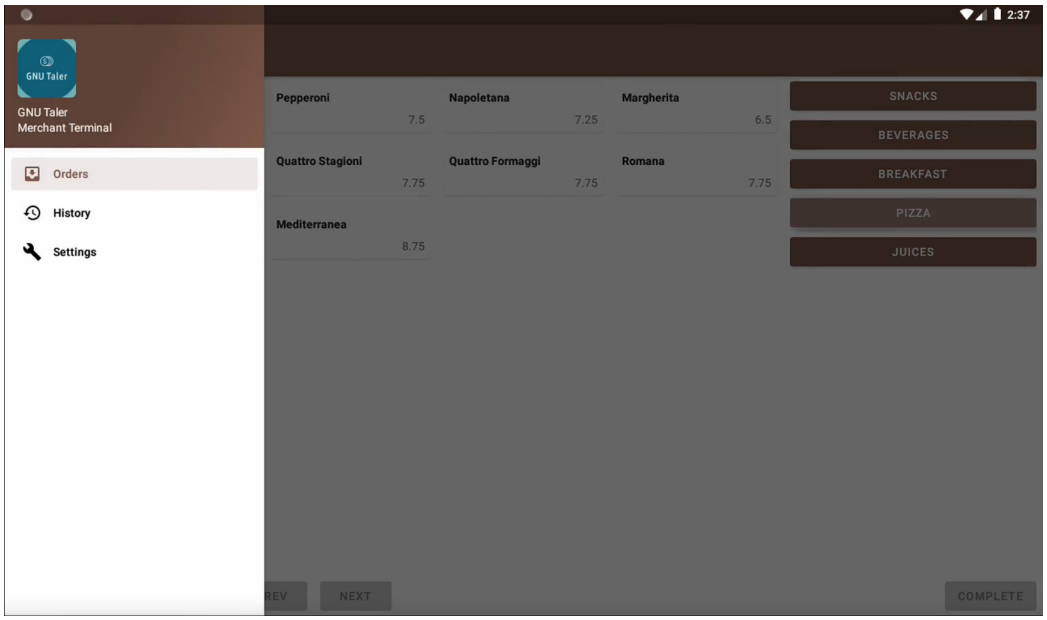
10. Das POS-Terminal zeigt nach Eingang der Coins die Bestätigung der erfolgten Zahlung:

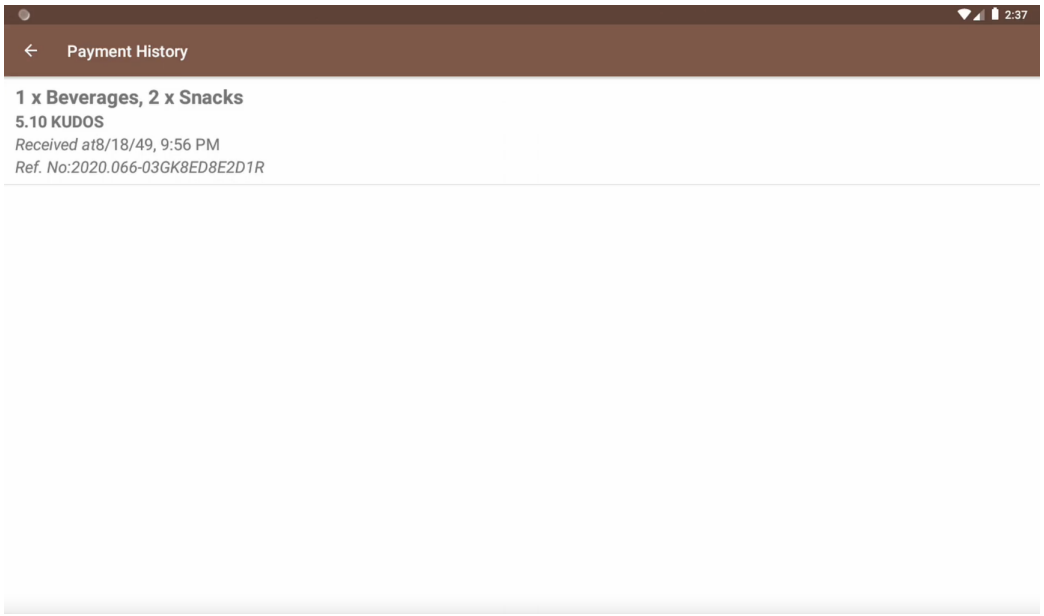



11. Das Terminal geht zum Auswahl-Menü zurück, die Bestellnummer hat sich erhöht:



12. Die POS-Anwendung kann jederzeit die Historie der Verkäufe anzeigen:



# 10 Glossar und Begriffsbestimmungen

**Amortisationsfaktor** Faktor zur Umlage der *Wire fee*-Gebühr eines Exchange durch einen Verkäufer, der diese Gebühr als zu hoch beurteilt und auf seine Kunden verteilen will (wire_fee_amortization, siehe Gebühren und Beispiele für Gebührenordnungen).

**ATM** Automated Teller Machine, Bankautomat mit Bargeld-Einzahlung

**Browser-Erweiterung** Add-on im Browser (Firefox, Chrome) eines ➔ Wallet zum Abheben auch ohne QR-Scan/Smartphone

**Closing Time** Zeitfenster von 14 Tagen für den Abhebevorgang, in dem das empfangende Wallet die Coins vom gewählten Exchange abheben kann

**Coin** Kryptographisch gesicherte Repräsentation von Werten in Fiatwährung = Geldeinheit des E-Gelds im ➔ Wallet (Nominalwert in Euro, Unique Identifier ist der EdDSA Public key)

**Credentials** Zugangsberechtigungen, welche das Wallet erzeugt, um einen Exchange aufzufordern, ihm die signierten Coins bereitzustellen

**Denomination key** Schlüsselvariable zum Festlegen der möglichen Coin-Nennwerte eines Exchange ➔ Nominalwert

**Emergency Protokoll** Unterprotokoll zum Auslösen der ➔ Recoup-Buchung im Fall eines geregelten Marktaustritts eines Exchange oder im Rahmen einer Abwicklung beim Insolvenzfall

**Exchange** Zentrale Steuerungslogik des Bezahlsystems mit der Datenbank zur Verwaltung aller SEPA-Buchungen und zum Abwickeln der Transaktionen von und zu Wallets

**Gebührenordnung** Im Taler-Protokoll fixierte Ordnung von Gebührenarten und Gebührenhöhen, siehe Gebühren

**IBAN-Buchung** Überweisungen mit Internationaler Bankkontonummer in Euro-Währung zwischen Girokonten und Exchange. Betrifft die Buchungsarten Withdrawal und Wire fee

**Lizenzen** Es gelten Affero GPLv3+ für den Exchange, LGPLv3+ für den Referenzcode der Integration in Händlerplattformen, GPLv3+ für Wallet-Code und Software für Kundenschnittstellen und die GNU Free Documentation License für dieses Dokument [1]

1 https://www.gnu.org/licenses/fdl-1.3.html

**Merchant POS** Von Taler Systems SA entwickeltes Bestell- und Bezahlsystem für ➔ POS-Verkaufsstellen zum Bezahlen mit Taler-Wallets auf Smartphones

**Merchant-Backend** Anwendung zum Einfordern und Verwalten von Verkäuferumsätzen, die kein Wallet bei Verkäufern erfordert

**Nennwert** = ➔ Nominalwert eines Coin, z.B. 1, 2, 4, 8, 16, 32, 64, 128 Cent bis zu 65536 Cent (= 655,36 Euro)

**Nominalwert** Auf eine Währung lautender fester Nennwert eines Taler-Coin, z.B. Euro ➔ Stückelung

**payto://-URI** Internet-Nomenklatur für Zahlungsziele zur Eingabe und Ausführung von Überweisungen (für IBAN-Girokonten, Zahlungsdienste, Kryptowährungen u.a.)[2]

**Point of Sale** Bestell- und Bezahlsystem an Verkaufsstellen wie z.B. Kiosken, Ladentheken, Supermarktkassen usw.
➔ Bezahlvorgang mit der Point of Sale-Anwendung „Merchant POS“

**Public key** Identifier zum Prüfen der korrekten Verbindung zwischen Wallet und Exchange und als Buchungsvermerk im Girokontoauszug

**Recoup** Im Fall eines regulären Marktaustritts eines Exchange oder im Insolvenzfall des Betreibers wird der betroffene Exchange automatisch alle Wallets darüber informieren und sie veranlassen, die Geldwerte der noch nicht ausgegebenen Taler-Coins dieses Exchange an das ursprüngliche Girokonto zurückzugeben

**Refresh** Protokoll, das dafür sorgt, dass Coins in einem Wallet einen neuen Schlüssel erhalten wegen

1. Wechselgeld = Neuerzeugung von Coins bei Ausgaben mit Beträgen unterhalb des Nominalwerts eines verbrauchten Coin
2. Transaktionsabbruch infolge von Netzwerkfehlern, ➔ Transaktionen
3. Verhindern des Ablaufs der Gültigkeit der Coins = Aktualisieren des Wallet, Auffrischen der Coins in ihm
4. Vertragsrücktritt oder Minderung (voller bzw. teilweiser Refund)

**Refund** Rückerstattung für den Fall, dass ein Verkäufer den Betrag seines Umsatzes mindert (= teilweise Refund) oder vom Vertrag zurücktritt (voller Refund); dies erzwingt immer einen ➔ Refresh der betroffenen Coins im Wallet der Käufer

**Reserve** Eine Reserve entsteht im Exchange beim Abhebevorgang und umfasst signierte Coins, welche das empfangende Ziel-Wallet abruft: Das Wallet erzeugt eine temporäre Zugangsberechtigung (➔ Credentials), mit der das Wallet den Exchange auffordern kann, ihm Coins auszuhändigen, indem der Exchange diese signiert. Die Zugangsberechtigung

2 IETF-Webseite über den Uniform Resource Identifier 'payto'

wird in dem Augenblick angelegt, wenn ein Wallet-Besitzer von seinem Girokonto einen Betrag an den Exchange überweist mit dem betreffenden Credential als Buchungsvermerk im Girokontoauszug und einem eindeutigen Identifier (als öffentlichem Schlüssel), der den einmaligen Abhebevorgang betrifft

**Stückelung** Ein Coin kann stets nur den festen Nominalwert haben, den es bei seiner Erzeugung erhält, z.B. 1, 2, 4, 8, 16, 32, 64, 128 usw. bis zu 65536 Cent (655,36 €). Wird mit einem Coin ein Betrag bezahlt, der unterhalb seines Nominalwerts liegt, muss der Exchange den Unterschiedsbetrag an das ausgebende Wallet senden, indem es diesem frisch erzeugte Coins zubucht (das sogenannte ➔ Wechselgeld)

**Taler-Cashier** Anwendung mit Mensch-Maschine-Interaktion zum Aufbuchen von Coins gegen Bargeld, welches eine Person wie ein Kassierer/Kassenwart entgegennimmt. Die Funktion entspricht einem ATM-Bankautomaten, der Bargeld annimmt und den Geldwert auf das Wallet aufbucht. Gegenwärtig müssen sowohl Kassenwart als auch Kunde jeweils ein Smartphone besitzen, der Kassenwart muss den Taler-Cashier, der Kunde ein Taler-Wallet installiert haben. Siehe Abschnitt 9.3

**Transaktionen** Kommunikation zwischen Exchange und Wallets für die jeweiligen Vorgänge des Abhebens, Ausgebens oder Auffrischen bzw. Rückerstattens von Coins (Withdrawal-, Deposit-, Refresh-, Refund-, Recoup-Buchungen)

**Wallet** Elektronische Geldbörse, Aufbewahrungsort der elektronischen Münzen ➔ Coin

**Wechselgeld** Vom Exchange durch die Refresh-Buchung neu erzeugte Coins aufgrund eines Ausgabevorgangs, bei dem ein Coin verbraucht wird, dessen Nominalwert (Stückelung) über dem zu zahlenden Kaufpreis liegt, um den Unterschiedsbetrag auszugleichen

**Wertverluste** Nicht-transaktionsbezogene Kosten, die in Sonderfällen für Nutzer entstehen können ($\neq$ Normalfall: transaktionsbezogene Gebühren)

**Wire fee** Gebühr für die aggregierte Buchung von Umsätzen auf ein Zielkonto von Verkäufern bei Geschäftsbanken, siehe ➔ IBAN-Buchung

**Withdrawal** Abhebung vom (Giro)Konto = Aufbuchung von Beträgen aus (Fiat-)Währungen auf Coins in einem Wallet

Ein weiteres umfangreiches Glossar in englischer Sprache befindet sich auf der Taler-Webseite https://docs.taler.net/developers-manual.html#developer-glossary. Wissenschaftliche Publikationen sind auf https://taler.net/en/bibliography.html zu finden.

Vertiefende Literatur und Quellen finden Sie auf der Bibliografie-Webseite mit einer besonderen Empfehlung der Doktorarbeit über das Bezahlsystem von Florian Dold (PhD-Thesis 2019)[3].

3 taler.net/en/bibliography.html und taler.net/papers/thesis-dold-phd-2019.pdf