Global **R**eal-time **A**uthorizations and **F**und **T**ransfers

Eine dezentrale Echtzeit Kredit-, Debit- und Krypto-Zahlungsabwicklungs Blockchain

Slava Gomzin, Dan Itkis

Version 3

Oktober 2018

Veröffentlichung der Erstversion im Juni 2017

Abstrakt

Global Real-Time Authorizations and Funds Transfers (GRAFT) ist ein globales, Open-Source, Blockchain-basiertes dezentralisiertes Zahlungsportal und Verarbeitungsplattform, welche von jedem genutzt werden kann. Jeder Käufer und Verkäufer (Händler) kann GRAFT in einer komplett dezentralisiert und kostengünstigen Art verwenden. Das GRAFT Ökosystem ist offen, damit jeder teilnehmen kann, indem er die GRAFT Blockchain unterstützt (Mining) und Netzwerkdienste bereitstellt.

GRAFT verwendet Zahlungsabwicklungsprotokolle und -abläufe ähnlich wie bei traditionellen elektronischen Zahlungssystemen, wie sie bei Kredit-, Debit- und Prepaidkarten üblich sind. Diese sind bereits Millionen von Anwendern und Händlern auf der ganzen Welt bekannt und vertraut. Dieser Ansatz ermöglicht eine einfachere und schnellere Einführung von GRAFT als Mainstream-Zahlungsplattform, während es gleichzeitig die Notwendigkeit von zentralen Vermittlern (Zahlungsportale und Zahlungssysteme) auflöst, welche momentan benötigt werden, um Transaktionen zwischen Käufern und Verkäufer (Händlern) zu erleichtern.

Hintergrund

Bitcoin[1] wurde als „online Bargeld“ kreiert, ein sicheres aber relativ langsames Zahlungssystem, welches nicht in der Lage ist online Zahlungen zu ersetzen oder mit Plastikkarten oder Bargeld im stationären Handel zu konkurrieren (Abbildung 1).

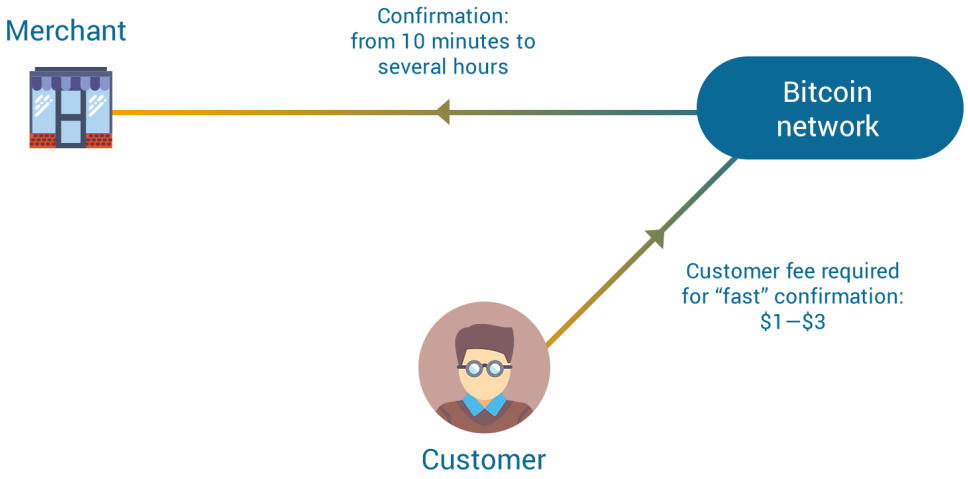

Abbildung 1: Bitcoin Transaktion ohne zentralen Vermittler.

Auch wenn einige bestehende Kryptowährungen und kryptographische Token[2] die Bestätigungszeiten verbessert haben, sind diese noch nicht in der Lage mit bereits implementierten Transaktionsarten zu konkurrieren. Beispielsweise sind wir davon überzeugt, dass die bestehenden Architekturen, die Akzeptanz von Kryptowährungen als Zahlungsoption im Einzelhandel, Gastgewerbe und bei Convenience Stores unmöglich machen. Um diese Lücke in der Adaption zu schließen müssen Vermittler, Zahlungsabwickler und Gateways[3] eingesetzt werden (Abbildung 2).

Ein wesentliches Element in der kryptographischen Zahlungstransaktion sind die Zahlungsabwickler. Diese sind typischerweise zentralisierte kommerzielle Organisationen, die von der Regierung reguliert und von Aktionären gesteuert werden. Dies widerspricht einigen grundlegenden Prinzipien von Kryptowährungen und kryptographischen Token: Dezentralisierung, Privatsphäre und Unabhängigkeit.

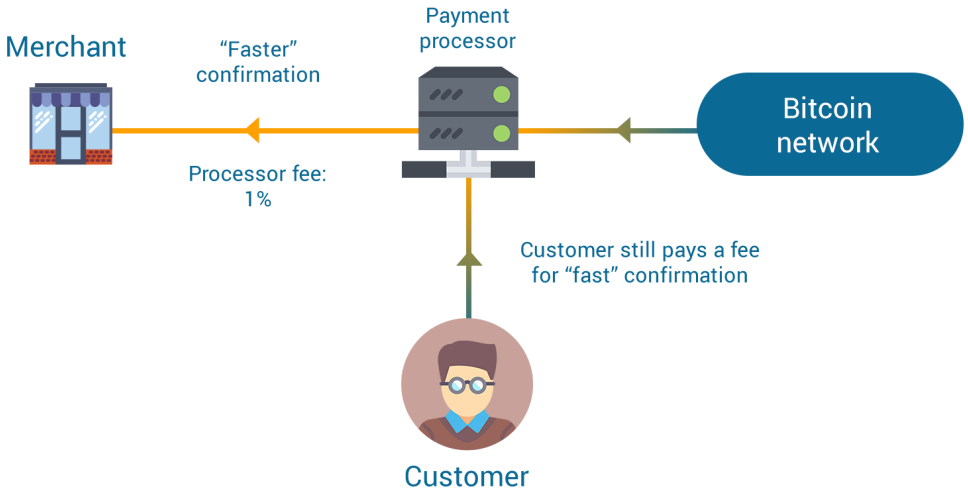

Abbildung 2: Verarbeitung von Bitcoin-Transaktionen durch einen zentralen Vermittler

Die meisten Händler sind aufgrund der einzigartigen Art und Weise, wie Blockchain-Netzwerke Transaktionen verarbeiten, nicht in der Lage, Kryptowährungen ohne die Verwendung eines Zahlungsabwicklers als Drittanbieter zu akzeptieren. Dieser Prozess unterscheidet sich konzeptionell von traditionellen elektronischen Zahlungssystemen. Trotz einiger Schwachstellen in traditionellen elektronischen Zahlungssystemen, genießen diese ein hohes Vertrauen der Händler und haben sich im Markt stark etabliert.

Es gibt einige wesentliche Unterschiede, wie traditionelle und kryptographische Zahlungssysteme Transaktionen abwickeln. Diese verringern in den meisten Fällen die Attraktivität von kryptographischen Zahlungssysteme für Händler und/oder Konsumenten. Nachfolgend ist eine Liste

einiger technischer Einschränkungen und Nachteile der bestehenden kryptographischen Zahlungssysteme im Vergleich zu traditionellen elektronischen Zahlungssystemen aufgeführt:

- Fehlen wesentlicher Transaktionsarten
- Ungeeignete Zahlungsströme
- Lange Bestätigungszeiten
- Ungleichmäßige und unvorhersehbare Transaktionsgebühren
- Die Unfähigkeit Micropayments und wiederkehrende Zahlungen (Abonnements) zu verarbeiten
- Fehlende Unterstützung von Offline-Transaktionen
- Geringe Skalierbarkeit
- Volatilität
- Mangelnde Sicherheit
- Fehlende Privatsphäre durch Verfolgbarkeit der Blockchain
- Mangelndes Vertrauen zwischen Käufer und Händler
- Fragwürdige Nützlichkeit
- Schlechte Bedienbarkeit der Benutzeroberfläche
- Fehlende Kundenbetreuung

Das Ziel von GRAFT ist es diese Probleme mit Hilfe einer Plattform zu lösen, die es endlich ermöglicht, dass kryptographische Zahlungen erstmals von Mainstream-Händlern und Verbrauchern allgemein akzeptiert werden. Wobei die Grundprinzipien von Kryptowährungen und kryptographischen Tokens respektiert werden.

Der Wert von dezentraler Zahlungsabwicklung

Warum sollte ein Kunde Kryptowährungen oder kryptographische Token zusätzlich oder anstatt von Plastikkarten, PayPal oder Apple Pay verwenden? Warum sollte ein Händler Kryptowährungen oder kryptographische Token zusätzlich oder anstatt einer bestehenden Zahlungsmethoden akzeptieren?
Wenn wir die Antworten auf diese einfachen Fragen nicht hätten, würden wir dieses Dokument nicht erstellen.

Während die Antwort auf den ersten Teil dieser Frage sich aus mehreren Elementen und Gründen zusammensetzt, weshalb Einzelpersonen Geld in Form von Kryptowährung oder kryptographischen Token halten, ist die Antwort auf den zweiten Teil dieser Frage relativ einfach. Händler möchten ihren Kundenstamm stetig erweitern, um ihre Einnahmen zu steigern. Wenn sie eine signifikante Gruppe von potenziellen Kunden erkennen, die aus irgendeinem Grund Kryptowährungen oder

kryptographische Token bevorzugen, dann werden sie anfangen Kryptowährungen und kryptographische Token zu akzeptieren.

Da GRAFT ein dezentraler Zahlungsabwickler ist, dessen Funktion von digitalen Utility Tokens erfüllt wird, ist GRAFT in der Lage den vollständige Zahlungsverlauf ohne externer Kryptowährungen, kryptographische Token oder Vermögensgegenstände zu ermöglichen. Trotzdem unterstützt GRAFT auch Bitcoin und weitere Kryptowährungen, sowie kryptographische Token als zusätzliche Zahlungsmittel für Käufer und Verkäufer. Diese Funktion macht es für Händler überflüssig sich mit mehreren (zentralen) Zahlungssoftware-Anbieter auseinanderzusetzen und für Einkäufer sich für zentralisierte Dienste anzumelden oder mehrere unterschiedliche Wallet-Apps zu erlernen und diese zu verwalten.

Terminologie

Authorization-Sample

Das Authorization-Sample ist eine ausgewählte Gruppe von Supernodes welche die Zahlungen in Echtzeit bestätigen und garantieren, dass der Käufer den Wert nicht mehrmals ausgibt, bevor die Transaktion in die Blockchain geschrieben wurde.

DAPI

DAPI ist eine dezentrale stateless API, die von Supdernodes implementiert wird, um Client-Anwendungen wie das GRAFT Wallet, GRAFT Point-of-Sale, Shopping Gutscheine und Drittanbieter Point-of-Sale Apps zu unterstützen. Der GRAFT SDK-Quellcode, welcher die Integration von GRAFT erleichtert, wird Drittanbietern von Point-of-Sale und Wallet Softwareentwicklern zur Verfügung gestellt.

Exchange Broker

Eine GRAFT Protokollerweiterung, die auf einem Supernode oder einer Gruppe von Supernodes, sowie einem Supernode Operator gehostet wird. Exchange Broker implementieren spezielle Zusatzfunktionen die nicht automatisch von einem vollständig dezentralen Netzwerk ausgeführt werden können und/oder eine speziellen Regulierung benötigen. Beispiele für einen Exchange Broker sind, Payment-Acceptance Broker (z.B. für Bitcoin) und Fiat Pay-Out Broker.

Full Supernode

Ein unabhängiger always-on Server, der die implementierten Funktionen des Graft Blockchain Nodes und des GRAFT DAPI Nodes kombiniert und ausführt; Real-Time Authorizations (Echtzeit-Autorisierungen) verarbeitet; DAPI-Zugriffe zwischen Käufern, Exchange-Brokern und Händlern aufruft; Drittanbieter Services wie der sofortige Austausch von Kryptowährungen innerhalb des GRAFT-Netzwerks hostet; Auszahlungen von Kreditkarten verarbeitet; Debitkarten akzeptiert und Händler Auszahlungen durchführt. Die Supernodes halten gemeinsam die zweite Schicht des GRAFT-Netzwerks mit Hilfe des POS-Algorithmus (Proof of Stake) aufrecht.

GRAFT

1. Global Real-time Authorizations und Funds Transfer ist eine dezentrale globale offene Plattform für die Verarbeitung von Real-Time Authorizations (Echtzeit-Autorisierungen) und Abwicklung von Händlerzahlungen, sowie Geldtransfers unter Verwendung einer nicht rückverfolgbaren Blockchain, dezentralisierter API und einer offenen Community von Exchange Brokern, die eine Vielzahl von Zahlungs- und Auszahlungsmethoden unterstützen, unter anderem Kryptowährungen, kryptographische Token und traditionelle Kreditkarten sowie Banküberweisungen.

2. Eine Pflanze, an der ein Zweig oder eine Knospe einer anderen Pflanze künstlich hinzugefügt wird, so dass sie miteinander verbunden sind und zusammenwachsen.[4] Grafting ist eine fortschrittliche Technik, mit der Botaniker, Landwirte, Gärtner und Hobbyisten lebende Gewebe von einer Pflanze zur anderen hinzufügen.[5] Diese Technik ermöglicht es, dass die besten Eigenschaften verschiedener Pflanzen zusammenkommen, um etwas Besseres und Wertvolleres als ihre Original zu züchten.

GRAFT Point of Sale

Desktop und mobile App, welche es dem Händler erlaubt, Zahlungen von Graft Token, Bitcoins, Altcoins und Kredit-/Debitkarten zu akzeptieren. Darüber hinaus werden weitere Aufgaben gelöst: Ausgabe und Einlösung von Geschenkgutscheinen, Treuepunkten und Shop-Guthaben, sowie Konfiguration von Abrechnungen/Auszahlungen in GRAFT-Token, Bitcoins, Altcoins oder der lokalen Fiat-Währung.

GRAFT Wallet

“Lite” Desktop, Mobil und Browser-Erweiterungs App, welche es erlaubt Bezahlungen und Wertetransfer mithilfe von GRAFT Token, anderen Kryptowährungen, kryptographische Token oder Kredit-/Debitkarten über die GRAFT DAPI durchzuführen.

GRFT

Nativer kryptographischer Token unterstützt von der Graft Blockchain, der für die Echtzeit Autorisierung von Zahlungen, den Wertetransfer und für Abrechnungen zwischen Käufer und Verkäufer verwendet wird.

Händler Token

Ein vordefinierter Smart Contract, welcher es dem Verkäufer erlaubt einen privaten Token zu generieren, der Ihm gehört.

Händler Token ermöglichen die Implementierung von wichtigen Funktionen wie Händler Pay-Out Token (“stablecoins”) und proprietäre geschlossene Systeme, wie zum Beispiel Programme für Treuepunkte, Geschenkgutscheine, Kredite und Rabatt-Coupons.

Payment Gateway

Ermöglicht es Händlern und / oder Service-Providern die Hardware Zahlungsterminals zu konfigurieren (z. B. die Wallet-Adresse), sowie Transaktionsberichte und Analysen auszugeben. Service-Provider können hierfür spezifische Gebühren verlangen.

Payout (“Stable Value”) Token

Repräsentiert eine lokale FIAT Währung und kann in Echtzeit auf der GRAFT Blockchain abgewickelt werden. Hierzu wird der Supernode Layer verwendet.

Die Pay-Out Token basieren auf der Technologie des GRAFT Händler Token, ähnlich wie Geschenk-, Belohnung- und andere Tokenarten der Händler.

Proxy Supernode

Der Supernode, welcher die Kommunikation zwischen des Point-of-Sale (POS) des Händler und/oder des Wallets des Käufers, sowie des Authorization Samples auf der Gegenseite herstellt, um die Transaktion abzuwickeln.

VChain

Virtuelles dezentrales unabhängiges Händlerkonto, in dem Händler sogenannte Händler-Token erstellen, sowie Berechtigungen, Auszahlungsregeln und Ausführungsbedingungen einrichten können, die Auswirkungen auf Transaktionen für diesen bestimmten Händler haben.

Transaktionsgebühren

Warum ist überhaupt eine Transaktionsgebühr notwendig? Schließlich gibt es kein kommerzielles Unternehmen hinter der Blockchain, warum also müssen die Nutzer Gebühren zahlen? Wer erhebt sie und wie hoch sollte diese Gebühr sein?

Sind Transaktionsgebühren notwendig?

Mehrere leistungsstarke Nodes (Server) werden benötigt, die über die ganze Welt verteilt sind, um sichere und hochverfügbare Kryptowährungs und kryptographische Token Netzwerke zu betreiben.
Wer wird also diese Nodes warten und was ist die Motivation und der Anreiz für die Wartung des Blockchain-Nodes? Im Bitcoin Netzwerk, anderen Kryptowährungs-Netzwerken und bei kryptographischen Token Netzwerken wird die Finanzierung durch Mining und Transaktionsgebühren erreicht. Die Eigentümer der Nodes verdienen Geld durch das Mining neuer Token oder Coins pro Block und erhalten Gebühren für jede Transaktion.
Das Mining hat einen weiteren Zweck:

Die ständige und kontinuierliche Generierung neuer Token in das System, um die Liquidität mit der wachsenden Nachfrage an Token sicherzustellen, während die Akzeptanz und die Nutzung zunimmt. Wenn das System weitere Nutzer dazu gewinnt, erhalten die Node Betreiber mehr Einnahmen aus Transaktionsgebühren, so dass der Belognungsanreiz durch das Mining mit jedem neuen Block schrittweise reduziert werden kann und eine Deckelung der Gesamtmenge an Coins erfolgt.

In einer idealen Welt wären Kryptowährungen oder Kryptographische Token für jedermann verfügbar und kostenlos. In der Tat gibt es Netzwerke die kostenlose Transaktionen versprechen.[6] In anderen Netzwerken, einschließlich Bitcoin, werden die Gebühren verwendet, um Transaktionen zu priorisieren und das Skalierungsproblem zu "lösen".

Im GRAFT Netzwerk jedoch, wird die Gebühr aus zwei Gründen erhoben. Der erste Grund ist, um Netzwerk-Missbrauch zu verhindern und damit verbundenen Performance und Blockchain größen Problemen vorzubeugen. So wird zum Beispiel die Verwendung des realen Netzwerks zum Testen unattraktiv. Wenn eine Transaktion komplett kostenlos ist, könnte jemande den selben Betrag unendlich lang zwischen zwei Konten bewegen.
Der Zweite Grund ist, auch weiterhin einen Anreiz für die Node Betreiber zu bieten, wenn der Mining Bonus zu gering wird.

Der Falsche zahlt die Gebühren

Das Problem mit den Transaktionsgebühren bei Bitcoin und kryptographischen Token ist, dass die falsche Seite die Transaktionsgebühren bezahlen muss. Es ist sogar noch schlimmer, wie mit traditionellen Kartenzahlungen, denn anders als bei diesen müssen beide Seiten Transaktionsgebühren zahlen:
Der Käufer zahlt die Gebühren an das Netzwerk der Kryptowährung oder des kryptographischen Tokens, während der Händler Gebühren für einen Zahlungsabwickler zahlt. Der Durchschnittseinkäufer wird oft durch diesen Prozess verwirrt, der eher wie Glücksspiel aussieht und keine klare Erklärung der Gebühren liefert, was Zahlungen mit Kryptowährungen oder kryptographische Token nicht sehr attraktiv macht.

Micropayments: Wie bezahle ich eine Tasse Kaffee mit Kryptowährungen?

Ein weiteres Problem, mit dem Bitcoin derzeit konfrontiert ist, ist die Unfähigkeit Micropayments aufgrund zu hoher Transaktionsgebühren durchzuführen[7]. GRAFT löst dieses Problem durch einen einzigartigen Ansatz für Transaktionsgebühren.

GRAFT Transaktionsgebühren

Im Graft Ökosystem zahlt nicht der Einkäufer die Transaktionsgebühr. Alle Gebühren gehen zu Lasten des Empfängers (Händler oder Zahlungsempfänger). Graft macht Micropayments (Zahlungen von

kleinen Beträgen) möglich, indem es sehr niedrige Gebühren festlegt (im Vergleich zu Kreditkarten, Online-Zahlungsabwicklern, Kryptowährungen oder anderen kryptographischen Token)[8].

Tabelle 1: Graft Transaktionsgebühren/Rewards Struktur

		1	2	3
		Regular P2P Transfer	**RTA Tx (GRFT)**	**RTA Tx mit Altcoin Exchange Broker (d.h., bitcoin akzeptanz)**
a	**Sender's wallet proxy Supernode Reward**	0.1 GRFT *	0.05% *	0.05% *
b	**Full Supernode (authorization sample member) Reward**	N/A	0.0625% **	0.0625% **
c	**Exchange Broker Reward**	N/A	N/A	0.25% **
d	**Miner (settlement) Reward**	Variabel, basierend auf Tx größe in KB	Konfigurierbar *** Min: 0.1 GRFT	Konfigurierbar *** Min: 0.1 GRFT
e	**Merchant POS/Recipient Gateway Proxy Supernode Reward ******	N/A	0.05% ****	0.05% ****
	Gesamtbetrag der Fee bezahlt vom Tx Sender (Käufer in RTA)	a1 + d1	0	0 *****
	Gesamtbetrag der fee bezahlt vom Tx Empfänger (Händler in RTA)	0	a2 + b2*8 + d2 + e2	a3 + b3*8 + c3 + d3 + e3
	Gesamtsumme die für den Tx sender anfällt	Tx sum + a1 + d1	Tx sum	Tx sum
	Gesamtbetrag der dem Tx recipient (Empfänger) zur Verfügung stehenden Mittel	Tx sum	Tx sum – (a2 + b2*8 + d2 + e2)	Tx sum – (a3 + b3*8 + c3 + d3 + e3)

* Der Wallet Proxy Supernode kann ein proprietärer Server oder ein öffentliches Cluster sein, der von einem Service-Provider gehostet wird. Sie können Ihren eigenen proprietären Proxy-Supernode betreiben und verwenden, um die Proxy-Gebühr vollständig zu vermeiden. Der Supernode muss einen Stake (bestimmte Anzahl von Coins) haben, um die Gebühr erheben zu können.

** Ein Stake wird für "full Supernode" oder "Exchange Broker" benötigt, um an den RTA Tx Verarbeitungen teilzunehmen und die Belohnung zu erhalten

*** wird vom Händler Service Provider oder dem Eigentümer des POS-Proxy-Supernode festgelegt.

**** Der POS-Proxy-Supernode kann ein proprietärer standalone Server, ein Teil der Händlerinfrastruktur, ein Teil eines Zahlungsterminals und/oder E-Commerce-Gateways sein, die vom Händler Service Provider verwaltet werden. Die POS-Supernode muss einen Stake haben, um diese Belohnung erhalten zu können.

***** Enthält nicht die Altcoin Netzwerk Gebühren.

Proxy Supernode Rewards (a1, a2, a3, e2, and e3 in Tabelle 1) werden eine vollständige Dezentralisierung der Netzinfrastruktur ermöglichen. Wenn Sie das Proxy-Supernode-Cluster von einem bestimmten Service-Provider nicht mögen, wird es alternative Service-Provider geben die bereit sind Ihre Wallet oder POS zu bedienen. Um den Reward zu erhalten, muss der Proxy-Supernode demonstrieren, dass die entsprechende Stake-Wallet auf die öffentliche IP-Adresse des Supernodes zeigt. Die Höhe des Proxy Stakes beträgt 250.000 GRFT.

Im Gegensatz zu einem Authorization-Sample Supernode, wird der Proxy Supernode auch ohne den Stake weiterhin funktionsfähig sein. Jedoch wird der unstaked Proxy Supernode nicht in der Lage sein Gebühren zu erheben. Diese Option ist für proprietäre Proxy Supernodes reserviert, so dass Benutzer mit erhöhtem Datenschutz Bedarf ihre eigenen Einstiegspunkte in das Netzwerk hosten können. Ohne den Stake, wird der Proxy Supernode Reward an die GRAFT Community Wallet geschickt. Auf diese Weise bleibt die gesamte Transaktionsgebühr, die sich immer aus mehreren Bestandteilen zusammensetzt, unabhängig vom Status der Proxy Supernodes immer gleich.

Die pauschale Gebühr wird an den Miner für die Durchführung der Realtime Transaction Authorization (RTA) gezahlt (d2, d3). Die Miner Gebühr wird traditionell abhängig von der Größe des

Transaktionssatzes in KB (d1) berechnet. In der RTA können die Miner Gebühren nicht variabel sein, da dies die vom Händler gezahlten Gebühren uneinheitlich und unvorhersehbar machen würden, was in den meisten Situationen inakzeptabel ist. Außerdem können wir die Gebühren nicht proportional zum Wert der Transaktion gestalten (ähnlich wie bei den Supernode Gebühren), da die Miner Gebühren auf der Blockchain sichtbar sind. Das bedeutet, dass der Transaktionsbetrag aus den Gebühren berechnet werden könnte (obwohl wir dies in Zukunft vielleicht korrigieren werden). Deshalb haben wir es zur einer einfach konfigurierbaren Gebührenpauschale mit einem Mindestbetrag von 0,1 GRFT gemacht.

Die Gebühren in Kombination mit RTA Transaktionen mit Exchange Brokern sind die gleichen wie die RTA Gebühren (Spalte 2), mit einer extra Gebühr von 0.25% für den Exchange Broker (diese wird auch vom Händler bezahlt).

Händlergebühren und Service-Provider

Der Service-Provider des Händlers kann einen Gebührenplan festlegen, der mit seinem Geschäftsmodell übereinstimmt. Die Gebühren können dabei in Stufen mit Optionen strukturiert werden, zum Beispiel:

Transaktionen unter 10 €: 2%
Transaktionen über 10 €: 1%
Minimaler Transaktionsbetrag: 1 €
Miner: 0.1 GRFT
Transaktionen in Altcoins: +0.25%
Instant Pay-Outs (sofortige Auszahlungen) in Altcoin oder Fiat: +0.25%

Nachfolgend ein Beispiel für eine 20 € Altcoin-Transaktion und die damit verbundenen Gebühren als Referenz für die Gebührenstruktur des Händler Service-Providers.

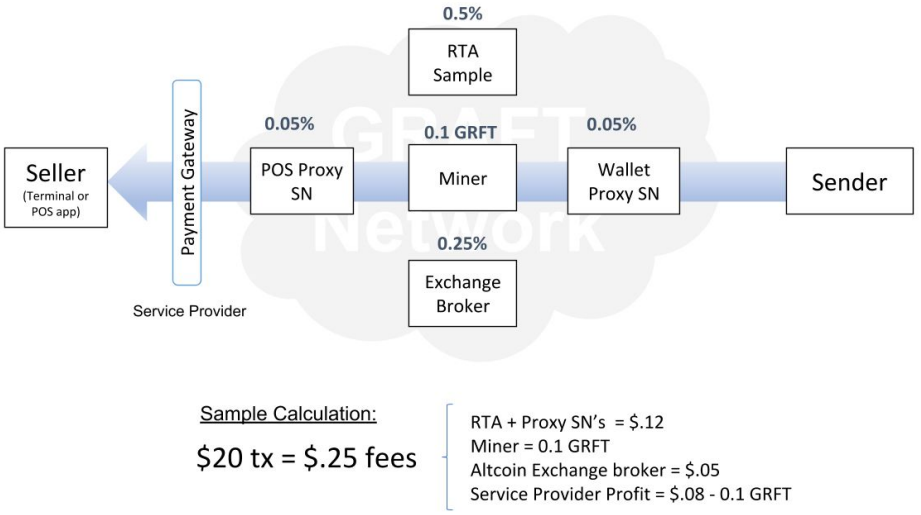

Abbildung 3: Beispiel von GRAFT Transaktionsgebühren mit Rewardverteilung

Kostenlose Geldtransfers: Authentifizierte Transaktionen

Einige Zahlungs-Netzwerke, wie Automated Clearing House (ACH) oder PayPal, bieten kostenlose Transfers zwischen Benutzerkonten an. Um mit den traditionellen Zahlungsnetzwerken konkurrieren zu können, wird GRAFT begrenzte kostenlose Transfers zwischen authentifizierten Benutzer Wallets anbieten.

Kryptowährungsnetzwerke können sich in der Regel aus drei Hauptgründen keine kostenlosen Transaktionen "leisten":

- Fehlender Anreiz für Miner
- Bedrohung durch Distributed Denial-of-Service (DDoS) Angriffe
- Unkontrolliertes Wachstum der Blockchain

GRAFT löst das erste Problem (Fehlender Anreiz für Miner) durch die Trennung von Zahlungen und Transfers, so erhalten Supernodes (Miner) Transaktionsgebühren für sofortige Zahlungen, die die Mehrheit aller Transaktionen ausmachen, während kostenlose Überweisungen mit geringerer Priorität bearbeitet werden.

Das zweite Problem (DDoS-Angriffe) wird durch freiwillige Benutzeridentifikationen und Authentifizierungen gelöst. Natürlich gibt es keine "kostenlosen Mittagessen". Der Benutzer “bezahlt” damit, dass er seine Identität im Netzwerk bereitstellt, um im Gegenzug angemessene Vorzüge zu erhalten (indem die Anzahl und Häufigkeit der kostenlosen Übertragungen pro Benutzer begrenzt wird). So wird der Missbrauch des Netzwerks verhindert. Die Verwendung der zero-knowledge

proof-authentication Technologie ermöglicht es, dass Benutzer ihre Identität beweisen können ohne ihre Privatsphäre zu gefährden.
Das Letzte Problem (Unkontrolliertes Wachstum der Blockchain) wird durch mehrere Ansätze gelöst, einschließlich kleiner Blockintervalle, unbegrenzter Blockgröße und eine standardmäßig eingeschränkte Transaktionsgröße für bestimmte Transaktionsarten, wie z.B. kostenlose Überweisungen. Darüber hinaus muss eine der Seiten des kostenlosen Geldtransfer durch den Nachweis, dass sie in der Vergangenheit "kommerzielle" Zahlungsverkehrsarten durchgeführt hat, verifiziert werden.

Privatsphäre und Datenschutz

Oftmals wird das Bedürfnis nach Privatsphäre falsch eingeschätzt. In der Wirklichkeit macht es einer Mehrheit von legitimen Käufern nichts aus, ihre Identität gegenüber dem Händler offen zu legen, insbesondere wenn sie von einer solchen Offenlegung profitieren oder wenn eine solche Offenlegung für die Abwicklung einer Transaktion erforderlich ist. Genauso wollen Käufer sicherstellen, dass der Händler an den sie die Zahlung senden, der beabsichtigte Empfänger und nicht ein Nachahmer (Betrüger) ist. Was weder der Händler noch Käufer wollen ist, dass jemand anderes die Möglichkeit hat, alle Details der Transaktionen durch Scannen einer öffentlich zugänglichen Blockchain zu erhalten.

Der Datenschutz ist ein heikles Thema für Kryptowährungen und die Zahlungsmittelbranche im Allgemeinen. Der Datenschutz umfasst eine Bandbreite von völliger Anonymität bis hin zu völliger Transparenz, die sowohl vom Verkäufer als auch vom Käufer festgelegt wird. Der Verkäufer kann beispielsweise gesetzlich verpflichtet sein, bestimmte Identitätsdaten zu erheben und zu überprüfen, wie z.B. das Alter für den Kauf von Alkohol oder Zigaretten oder Postleitzahlen für die Steuerberechnung des Online-Händlers. Der Käufer hingegen kann sich dafür entscheiden, alle oder nur einige der Daten seiner Identität offenzulegen, und sollte dazu auch in der Lage sein. Wenn sich der Verkäufer und der Käufer auf die zu teilenden Identitätsdaten einigen können, kann die Transaktion fortgesetzt werden. Darüber hinaus ist es in vielen Fällen erforderlich, die Echtheit der Identitätsdaten durch den Händler festzustellen.

Wir denken der beste Weg dieses Problem anzugehen besteht darin, ein System der Identitätsprüfung und des Austauschs von Identitätsdaten zu verwenden, das im Einklang zu den Richtlinien für digitale Identitäten ist. Diese werden von Regierungsbehörden festgelegt, die sich auf die Verbesserung der Privatsphäre (d.h. NIST 800-63 in den USA oder GDPR [DSGVO] in der EU), sowie Standards, die eine differenzierte Überprüfung und Authentifizierung der Identität erfordern[9], konzentrieren.

GRAFT implementiert ein digitales Identitätsprofil, das an das GRAFT Wallet angehängt ist, mit der Möglichkeit, die Daten aus der digitalen Identität einzeln (schrittweise) und basierend auf den Benutzerberechtigungen zum Zeitpunkt der Transaktion mit der Gegenpartei zu teilen. Diese Berechtigungen beinhalten das Teilen bestimmter Daten (wie Alter, Heimatstandort, Adresse und Name) selektiv und pro Transaktion.

GRAFT implementiert **CryptoNote**[10] als zugrundeliegendes "transaction recording protocol", das im Vergleich zu Bitcoin, anderen Kryptowährungen und kryptographischen Token ein hohes Maß an Privatsphäre bietet, indem es Informationen über Sender und Empfänger verbirgt.

Warum eine private Blockchain notwendig ist

Die wichtigste Innovation von Bitcoin ist das "open ledger", das für jeden am Netzwerk beteiligten Node (Knoten) zugänglich ist, da die Transaktion überprüft werden muss, um sicherzustellen, dass es kein double-spending gibt. Das bedeutet aber auch, dass jeder auf der Welt die Transaktion und die Guthaben auf den entsprechenden Wallets sehen kann. Im Gegensatz zu Plastikkarten sind Bitcoin-Wallets grundsätzlich anonym, da Transaktionsaufzeichnungen nicht direkt mit der Identität des Eigentümers verbunden sind. Auf den ersten Blick scheint diese Funktion die Tatsache zu kompensieren, dass die Transaktionsaufzeichnungen auf der Blockchain für jedermann sichtbar sind. Es gibt jedoch bereits Techniken, die es dem Beobachter ermöglichen, Adressen mit Identitäten zu verknüpfen[11]. Sobald dies geschieht, werden alle Ihre Transaktionen für immer sichtbar, da die Blockchain immer vorhanden ist und nicht gelöscht werden kann.

CryptoNote ist absolut notwendig, um mit traditionellen Zahlungssystemen wie dem Visa-Netzwerk oder PayPal wettbewerbsfähig zu sein, da das CryptoNote Protokoll seinen Nutzern tatsächlich eine viel bessere Privatsphäre bietet als die meisten bestehenden Kryptowährungen.

Wenn Sie Ihre Zahlungskarte (z. B. Visa) am POS-Terminal durchziehen bzw. einstecken oder online auf die PayPal-Schaltfläche klicken, gibt es zwei Unternehmen auf der Welt, die von Ihrer Transaktion wissen: Das Payment Network (Visa oder Paypal in unserem Fall) und der Händler. In Wirklichkeit gibt es natürlich mehr Unternehmen, die von Ihrer Transaktion "wissen", weil das Zahlungsnetzwerk komplexer ist. Diese Liste enthält zumindest die ausstellende Bank (diejenige, die dir die Zahlungskarte gegeben hat), das Zahlungs-Gateway (dasjenige, dass Ihre Transaktion an den richtigen Zahlungsabwickler/die richtige Bank weiterleitet) und den Zahlungsabwickler (der die Zahlung und die Auszahlung des Händlers verarbeitet). Die Liste der Unternehmen ist jedoch immer

noch begrenzt, da sie bestimmten Sicherheits- und Datenschutzbestimmungen unterliegen, und sie haben in der Regel einige zuverlässige Sicherheitskontrollen implementiert, die Ihre Transaktionsaufzeichnungen vor neugierigen Blicken schützen. Natürlich kann jeder in dieser Liste gehackt werden oder Ihre Daten an eine Strafverfolgungsbehörde weitergeben. Der Einfachheit halber nehmen wir jedoch an, dass zufällige Personen in den meisten Situationen keinen Zugang zu Ihren Zahlungskartentransaktionen erhalten können, was bei den meisten Blockchains nicht der Fall ist.

CryptoNote als Grundlage für den Datenschutz

CryptoNote hebt sich von allen anderen Blockchain-Protokollen ab, weil es etwas bietet das wir alle brauchen: Datenschutz. Wir nehmen die Privatsphäre oft als selbstverständlich hin und bedauern sie nur, wenn wir sie verlieren. Ironischerweise machen Bitcoin und seine Ableger im Bereich des Datenschutzes einen Schritt zurück im Gegensatz zu älteren Zahlungstechnologien wie Bar- oder sogar Plastikkarten, die zu einem unrühmlichen Symbol für gefährdete Sicherheit und Privatsphäre wurden. Die Bitcoin Schöpfer haben entweder nicht an die Privatsphäre gedacht oder hatten einfach nicht genug Zeit, alle Probleme zu lösen, was absolut verständlich ist, da sie ein noch wichtigeres Problem zu lösen hatten: die Existenz der Blockchain-Technologie.

CryptoNote behält alle Vorteile der bekannten Blockchain-Technologien, während die verlorenen Datenschutzfunktionen "zurückgebracht" werden: **nicht nachvollziehbare Zahlungen, nicht verknüpfbare Transaktionen, Widerstand gegen Blockchain-Analysen** und **vertrauliche Transaktionsbeträge**. Und dazu kommt noch, GRAFT fügt **vertrauliche Transaktionsgebühren hinzu**, um das Bild zu vervollständigen. CryptoNote schafft eine perfekte, solide Grundlage für den Aufbau einer Vielzahl von branchenspezifischen Funktionen, die GRAFT ans Licht bringt, um die Welt des Zahlungsverkehrs zu erobern.

Private Transaktionen

GRAFT verwendet mehrere von CryptoNote und Monero entwickelte kryptographische Mechanismen, um Transaktionsaufzeichnungen zu verschleiern und nur für Datenbesitzer sichtbar zu machen:

Einmalige Ziel “Stealth” Adressen

Anstatt die Zahlung direkt an die Empfängeradresse zu senden, wird für jede Transaktion ein eindeutiger einmaliger Ziel-Schlüssel erstellt. Dieser Schlüssel ist kryptographisch von der

öffentlichen Empfängeradresse abgeleitet, somit wird verhindert, dass der Schlüssel mit der Adresse oder mit anderen Schlüsseln verknüpft wird. **Daher kann der Empfänger eine einzelne Adresse veröffentlichen und nicht verknüpfbare Zahlungen erhalten**, und **kein Beobachter kann bestimmen, ob Transaktionen an eine bestimmte Adresse gesendet wurden** oder ob zwei Adressen miteinander verknüpft sind.

Einmalige Ring Signaturen

Diese Signaturen **verschleiern die Identität des Absenders**. Jede Transaktion in einer Blockchain wird durch den privaten Schlüssel des Absenders signiert, damit das Netzwerk bestätigen kann, dass die Transaktion echt ist. Anstatt eine einzige Signatur zu erstellen, werden mehrere Signaturen (der "Ring") erstellt, die alle gültig sind, da sie die tatsächlichen Ausgaben anderer Absender darstellen. Ein Beobachter kann jedoch nicht erkennen, wer der eigentliche Absender ist. Das Netzwerk weiß nicht, welcher besondere Output verwendet wird, da er unter anderen Signaturen in den Ring Signaturen verborgen ist. Stattdessen prüft das Netzwerk, ob keine Output aus dem gesamten Ring mehr als einmal ausgegeben wird, womit double-spending wirksam verhindert wird.

Vertrauliche Ring Transaktionen

Diese machen **Transaktionsbeträge in der Blockchain unsichtbar**. Der Transaktionsbetrag wird vom Absender verschlüsselt. Nur der Empfänger der Zahlung kann den tatsächlichen Betrag entschlüsseln. Dritte Beobachter sind nicht in der Lage, diesen Betrag zu entschlüsseln. Sie können jedoch überprüfen, ob das Geld nicht mehr als einmal ausgegeben wurde und ob in dieser Transaktion kein "neues Geld" geschaffen wurde.

Transaktionsverarbeitung

Die Welt bewegt sich in Richtung "schlanker" Geräte. Menschen auf der ganzen Welt nutzen mehr Smartphones und Tablets und weniger Workstations und Laptops. Daher sind wir davon überzeugt, dass ein überlegenes Modell für dezentrale kryptographische Zahlungssysteme kleine, individuelle Knoten sind, die auf PCs gehostet werden und von dedizierten leistungsstarken Supernodes, welche von Profis gehostet werden, gestützt werden.

Zusätzlich gibt es Thin-Client Apps, die mit dem Authorization-Sample verbunden sind (eine Gruppe von Supernodes, die zufällig durch einen speziellen “Betrugsverhinderungsalgorithmus” ausgewählt wurden und über DAPI-Aufrufe angesprochen werden).

Bestätigungszeit Problem: Einführung von Real-Time Authorizations

Lange Bestätigungszeiten [12] (von mehreren Minuten bis zu mehreren Stunden, abhängig von der Transaktionsgebühr) sind einer der Hauptgründe für die geringe Akzeptanz von Kryptowährungen und

kryptographischen Token im Einzelhandel und im Gastgewerbe. Kunden mögen keine langen Wartezeiten und fordern daher von den Händlern eine nahezu sofortige Zahlungsabwicklung. Im Gegensatz zu einigen anderen Kryptowährungs-Netzwerken, die versuchten dieses Problem durch die Einführung spezieller Add-on Systeme oder Transaktionsarten zu lösen, wird GRAFT alle Zahlungsvorgänge in “Echtzeit” abwickeln (wir erwarten, dass die meisten Transaktionen in weniger als 3 Sekunden abgeschlossen sind). Entscheidend ist, dass GRAFT diese Echtzeit-Zahlungen ohne zusätzliche Kosten bzw. Gebühren für den Kunden realisiert.

Dies wird durch den Einsatz eines Konsens von always-on Supernodes ("authorization sample") erreicht. Diese haben die Fähigkeit eine verteilte sofortige Sperre für Autorisierungen von Käufer-Konten zu erteilen und dem Client innerhalb von Millisekunden eine Antwort zu übermitteln. Die Supernodes überwachen auch die GRAFT-Blockchain, so dass keine Transaktionen "off chain" autorisiert werden können.

Supernodes

Alle Transaktionen werden über das Netzwerk von always-on GRAFT-Netzwerkknoten den Supernodes in Echtzeit verarbeitet. Die Transaktionsgebühren werden vom Empfänger an die teilnehmenden Authorization-Sample Supernodes und (optional) an der Transaktionsabwicklung teilnehmenden Exchange Broker gezahlt. Die Eigentümer der Supernodes sind für alle Transaktionen verantwortlich, die sie durchführen. Diese Verantwortung wird durch finanzielle interessen (Transaktionsgebühren) geleistet.

DAPI

Im Gegensatz zu regulären APIs, die auf einem Server oder in einer Serverfarm gehostet werden, hat DAPI keine einzelne Adresse, da es auf mehreren Supernodes läuft. Die DAPI Aufrufe sind stateless, dass bedeutet die Supernodes haben keine permanente Sitzung mit dem Client und alle für die Verarbeitung notwendigen Daten sind sofort verteilt und auf allen Nodes verfügbar. Die Client-App welche die DAPI verwendet, führt eine Liste von Proxy-Supernodes, mit denen sie kommuniziert. Es steht der Client-App jedoch frei, einen bestimmten vertrauenswürdigen Supernode auszuwählen und bei diesem zu bleiben. So können sich beispielsweise Händler, die eine POS (point-of-sale) oder ein Wallet nutzen, entscheiden, ob Sie ihren eigenen vertrauenswürdigen Proxy-Supernode hosten. Obwohl einem solchen "privaten" Supernode aufgrund von Ressourcenbeschränkungen möglicherweise nicht das Recht eingeräumt wird, an der Authorization-Sample teilzunehmen, kann er seinen Eigentümern eine zusätzliche Ebene der Privatsphäre bieten.

Echtzeit Bestätigung durch das Authorization-Sample

Es gibt Kryptowährungen mit Block (settlement) Intervallen von weniger als 2 Minuten. Die Verkürzung dieses Intervalls macht diese Transaktionen jedoch noch nicht ”Real-Time (Echtzeit)". Das GRAFT Supernode-System löst dieses Problem, indem es Authorization-Samples verwendet, um Freigaben in Echtzeit von einer ausgewählten Gruppe von Supernodes zu erteilen. Wir glauben, dass diese Struktur garantiert, dass der Käufer nicht mehr als einmal das gleiche Geld ausgeben kann, bis die Transaktion abgewickelt ist (in die Blockchain geschrieben wurde). Das Settlement (Mining) erfolgt typischerweise innerhalb weniger Minuten. Im Gegensatz zu den meisten kryptographischen Zahlungssystemen und ähnlich wie bei traditionellen elektronischen Zahlungssystemen ist jede Zahlung im GRAFT-Netzwerk in zwei Phasen unterteilt: Autorisierung und Settlement (Abwicklung). Wie in der traditionellen Zahlungswelt erfolgt die Autorisierung in Echtzeit, während das Settlement (die Abrechnung) später erfolgt, in der Regel innerhalb von zwei Minuten (im Vergleich zu mehreren Stunden und sogar Tagen in traditionellen Zahlungsnetzwerken).

Authorization Account Lock

Ein "Key-Image" ist der Mechanismus, mit dem CryptoNote neue Transaktionen validiert und Double-Spending verhindert, ohne die Privatsphäre des Absenders zu gefährden. Ein Key-Image ist ein eindeutiger Fingerabdruck, der die Kaufadresse und den Betrag des Käufers darstellt, ohne Details über den Käufer oder den Betrag preiszugeben. Das Besondere an einem Key-Image ist, dass es nur einmal verwendet werden kann. Wenn also jemand versucht, das gleiche Key-Image mehrmals zu verwenden, ist dies das Zeichen eines versuchten Double-spending. Durch die Bereitstellung des einzigartigen Key-Image für bevorstehende Transaktionen im Netzwerk der Supernodes, sperrt die Wallet des Käufers vorübergehend sein Ausgabenkonto. Somit kann keine andere Transaktion mit dem gleichen Key-Image (d.h. vom gleichen Konto) stattfinden, bis die gesperrte Transaktion gesettled (abgewickelt) oder die Sperre aufgehoben wird. Wenn der Käufer versucht, die Transaktion mit einem anderen Key-Image als dem des ursprünglichen Schlosses abzuschließen, wird die Transaktion von den Supernodes abgelehnt.

Andererseits enthält ein Key-Image keine Informationen über den Käufer oder das Wallet des Käufers. Dies gewährleistet Sicherheit, Anonymität und eine Nicht-Zurückfolgbarkeit. Darüber hinaus werden alle Spuren der Kommunikation während der Autorisierungs Phase zwischen dem Käufer (Wallet-App),

dem Händler (Point-of-Sale-App) und der Supernodes (ausgewählte Relay- und Sample-Supernodes) entfernt, wenn die Transaktion abgeschlossen wurde (in die Blockchain geschrieben und durch 10 Blöcke bestätigt).

Supernode Levels

Ein GRAFT Node wird Supernode genannt, weil er mehr Funktionen ausführt als herkömmliche Blockchain-Netzwerkknoten. Es gibt erhöhte Anforderungen an Supernode Inhaber. Während GRAFT ein offenes und dezentrales Netzwerk ist, das es jedem ermöglicht einen Supernode zu betreiben, gibt es verschiedene Ebenen von Supernodes mit unterschiedlichen Bedingungen und Rewards, die mit jedem Level verbunden sind.

Proxy Supernode ist der Entry-Level (Einstieg) - jeder kann die Supernode-Software installieren und den Proxy-Supernode hosten. Der Proxy-Supernode bietet die folgenden Dienste an:

- als vertrauenswürdiges Relay für diejenigen, die höchste Datenschutzanforderungen haben, damit sie ihren eigenen "Wallet-Server" hosten können.
- für große Händler als "Store Server" für eine noch schnellere und zuverlässigere Transaktionsabwicklung.
- Als öffentlicher Exit-Node (Ausgangsknoten), der mobile Wallets und Point-of-Sale mit dem GRAFT-Netzwerk verbindet (Public IP ist erforderlich). Der öffentliche Proxy-Supernode kann Rewards erhalten, wenn er einen Stake hat.

Der **Full Supernode** ist sowohl Autorisierer als auch Service-Provider. Darüber hinaus verlangt die Ausübung der Full-Supernode Funktionen einen, mit der Supernode Adresse verbundenen, Pfand in Form eines Stakes. Transaktions- und Servicegebühren werden an einen Full-Supernode gezahlt, der einen Stake hat und Echtzeit-Genehmigungen erteilt.

Mining Nodes

Die zweite Schicht des GRAFT-Netzwerks, welche aus POS-Supernodes besteht, führt die Berechtigungs- und Austauschfunktionen aus. Während die erste Schicht, die aus Proof of Work (PoW)-Netzknoten besteht, die Settlement-Funktionen ausführt, indem sie neue Blöcke erzeugt und der Blockchain hinzufügt.

Settlement (Mining) Rewards

Mining-Nodes erhalten Proof-of-Work Mining Rewards und Settlement Transaktionsgebühren, sowohl für reguläre Transfers, als auch für RTA-Transaktionen.

Settlement Reward (RTA Tx): variabel

Wird vom Service-Provider des Händlers über das Payment Gateway festgelegt, jedoch nicht niedriger als 0,1 GRFT.

Miner Transaktions Gebühren (non-RTA Transfer): variabel

Variabel, basierend auf der Tx größe in KB

Mining (Coinbase) Block Reward

Der Block Mining Reward wird an den Mining-Node gezahlt, der den neuen Block erzeugt. Der Block Reward wird mit jedem neuen Block nach der folgenden Formel schrittweise reduziert: (M – A) * 2-19 * 10-10 / 2, wobei A = Current-Circulation und M = Total-Supply (264 − 1) in Atomar Einheiten (10-10). Die Idee dahinter ist, dass es in Zukunft mehr Transaktionen geben wird, die den Minern das nachhaltige Einkommen aus Transaktionsgebühren sichern.

Full Supernode Tiers (Stufen)

GRAFT implementiert ein vierstufiges Tier (Stufen) Stake-Modell, bei dem eine höhere Tier (Stufe) eine größere Chance hat, in das Authorization-Sample aufgenommen zu werden, trotzdem ist der Auswahlprozess zufällig.

50,000 GRFT – tier (Stufe) 1
90,000 GRFT – tier (Stufe) 2
150,000 GRFT – tier (Stufe) 3
250,000 GRFT – tier (Stufe) 4

Jede Stufe nimmt an einer Zufallsauswahl von 2 “sample supernodes” teil, wobei N die Tierzahl ist. Natürlich hat eine Tier-4-Supernode, aufgrund der begrenzten Anzahl von Tier-4-Supernodes, somit mehr Chancen ausgewählt zu werden. “Leere” Spots werden von den übergeordneten Tiers gefüllt (oder niedrigeren, wenn es keine höheren gibt). Dieser Algorithmus ist auch adaptiv, da er die durchschnittliche Anzahl der Full-Supernodes auf jeder Ebene reguliert.

Delegated Stake

Guthaben aus mehreren Wallets können an einen einzelnen Full-Supernode delegiert werden, um einen Stake (Anteil) zu bilden, der ausreicht, um einen Full-Supernode zu betreiben. Die Einnahmen/Belohnungen werden entsprechend ihrem Stake auf die Wallets verteilt. Der Mindestbetrag für einen delegierten Stake beträgt 5.000 GRFT.

Authorization-Sample

Um Echtzeit-Autorisierungen durchführen zu können, stützt sich das GRAFT-Netzwerk auf die Authorization-Sample: eine Gruppe ausgewählten vertrauenswürdigen Supernodes, die das Netzwerk "repräsentieren" und Transaktionen validieren, Double-Spending verhindern und Sofort-Genehmigungen unterzeichnen, bevor eine Transaktion auf der GRAFT-Blockchain bestätigt wird (d.h. bevor er zum Block hinzugefügt wird und der Block zur Blockchain hinzugefügt wird).

Das Authorization-Sample besteht aus acht Supernodes, die zufällig aus einer dynamischen Liste von Supernodes ausgewählt wurden. Die Auswahl ist zufällig, während das Ergebnis für jeden deterministisch ist, der die Formel berechnet. Der Supernode Inhaber muss ein Sicherheitsguthaben in einer Wallet, die mit dem Supernode verbunden ist, aufrechterhalten. Der Mindestbetrag beginnt bei 50.000 GRFT.

Wenn eine neue Transaktionsanforderung vom Point-of-Sale des Händlers initiiert wird, erhält er die aktuelle Block-Height (Blockhöhe) die das Authorization-Sample definiert. Die Blockhöhe kann inkrementiert werden während die Transaktion noch läuft, aber es ändert nicht die Sample-High, die ursprünglich der Transaktionsanforderung zugeordnet war. Der Proxy-Supernode des Händlers, der die initiale Transaktionsanforderung formatiert, wählt die Sample-Supernodes aus. Diese Auswahl wird von jedem Mitglied des Samples und dem Proxy-Supernode des Wallets überprüft.

Um den Genehmigungsprozess zu beschleunigen, kann die Händler Point-of-Sale App die Authorization-Sample Supernodes anweisen, die Antworten aus dem Rest der Authorization-Sample zu ignorieren, sobald es mehr als 50 Prozent zustimmende Antworten von den "schnellsten" Supernodes erhält und keine abgelehnten Antworten.

Proxy Supernodes

Jeder Supernode aus der Authorization-Sample kann auch ein Proxy-Supernode sein - das Relay, dass die Transaktion des Händlers erleichtert, indem es auf der einen Seite mit der Point-of-Sale des Händlers und/oder der Wallet des Käufers kommuniziert und mit dem Rest der Authorization-Sample Supernodes auf der anderen Seite. Der Proxy-Supernode kann zufällig vom Point-of-Sale ausgewählt werden oder vom Wallet aus der aktuellen mit der Transaktion verknüpften Authorization-Sample. Das Point-of-Sale oder das Wallet kann auch jede Supernode auswählen, der nicht Teil der Authorization-Sample ist. Tatsächlich kann ein Point-of-Sale oder eine Wallet seine eigenen Proxy-Supernode hosten, wenn er nach einer zusätzlichen Ebene der Sicherheit und des

Datenschutzes sucht. Der Proxy-Supernode kann Transaktionsverarbeitungs Rewards erhalten, wenn er einen Stake hat.

Supernode Rewards

Jede Supernode erhält einen Anteil der Transaktionsgebühr für jede Transaktion, die sie verarbeitet. Die Rewards (Belohnungen) werden vom Empfänger/Händler bezahlt.

Full Supernode RTA Belohnung (irgendeine RTA Tx): 0.5%

Ein Achtel dieser Gebühr, oder 0,0625% des gesamten RTA-Tx-Betrags, geht an jeden "full Supernode", die an der "RTA authorization sample" teilnimmt.

Proxy Supernodes Belohnung (irgendeine RTA Tx): 0.1%

Die Hälfte dieser Gebühr, oder 0,05 % des gesamten RTA Tx-Betrags, geht an jeden Supernode im "proxy pair", welche die Verbindung zum Netzwerk ermöglicht (wallet und POS proxy supernodes).

Wallet Proxy Supernode Belohnung (non-RTA Transfer): 0.1 GRFT

Diese Gebühr wird vom "wallet Proxy Supernode" an das Mobile oder Desktop Wallet des Senders zusätzlich zu den bestehenden Netzwerkgebühren (Miner Belohnungen) erhoben.

Skalierbarkeit

Ein bestimmtes Zahlungsnetzwerk ist skalierbar, wenn dieses die Fähigkeit besitzt eine große Anzahl an Transaktionen gleichzeitig und ohne Leistungseinbußen zu verarbeiten. Das GRAFT Netzwerk verwendet einige Funktionen, um eine hohe Skalierbarkeit zu erreichen, wie die Festlegung des Blockerstellungsintervalls auf zwei Minuten, sowie die Aufhebung der Größenbegrenzung eines Blocks. Dadurch werden Transaktionsblöcke häufiger erstellt und jeder Block kann mehr Transaktionen aufnehmen. Solche Funktionen sind nicht einzigartig und werden ebenfalls von anderen Kryptowährungen und kryptographischen Token umgesetzt. GRAFT wird jedoch von ständig aktiven Hochleistungs-Supernodes verwaltet, die Transaktionen in Echtzeit validieren und autorisieren. Daher hat jeder Supernode nicht nur eine aktuelle Kopie der vollständigen Blockchain, sondern führt auch eine Liste aller ausstehenden Autorisierungsanforderungen und abgeschlossenen Transaktionen, bis sie zur Blockchain hinzugefügt wurden. Eine solche zweistufige Architektur ermöglicht es auch hohe Lastspitzen von entsprechenden Anfragen abzudecken (z.B. saisonale Ereignisse und andere Aktivitätsänderungen von Käufern und Händlern).

Genehmigung von Offline-Transaktionen

Personen die mit der Verarbeitung von Kartenzahlungen vertraut sind wissen, dass die Transaktion manchmal schon von einem Händler genehmigt werden kann, ohne parallel die Genehmigung der Bank eingeholt zu haben. Dies wird als Offline-Genehmigung, Lokale-Genehmigung, Offline-Autorisierung oder manchmal auch als S&F (für "Store and Forward") bezeichnet, da eine solche Offline-Autorisierung an den Server weitergeleitet wird, sobald das Netzwerk wieder online ist.

Kryptographische Zahlungen gehen jedoch in der Regel davon aus, dass das Netzwerk rund um die Uhr verfügbar ist und es keine Ausfallzeiten gibt. Diese Annahme ist jedoch nicht immer richtig. In einigen Situationen gehen Händler ein Risiko ein und genehmigen Transaktionen direkt vor Ort, da das Risiko einer einzelnen Rückbuchung geringer ist, als das Risiko mehrere Kunden zu verlieren. In der Regel ist der maximale Gesamtbetrag für lokale Autorisierungen begrenzt. Nachdem das System diese Grenze (das maximale Risiko) erreicht hat, stellt es die Erteilung lokaler Genehmigungen ein, bis das Netzwerk diese wieder freigibt. Aber im Falle einer kurzen Ausfallzeit kann die lokale Autorisierung sowohl von Kassierern als auch von Käufern unbemerkt bleiben.

Die GRAFT Point-of-Sale App für Händler und ein Single-Proxy-Supernode können kryptographische Offline-Transaktionen nach dem gleichen Prinzip verarbeiten. Wenn der Händler das entsprechende Risiko akzeptiert können diese auch ohne Authorization-Sample Kommunikation und erzieltem Konsensus durchgeführt werden. Die Entscheidung über die Offline-Genehmigung wird hier unter anderem auf Grundlage der Reputationswerte des Käufers und des Supernodes getroffen.

Zahlung-Gateways für Händler und Service Provider

Einer der wichtigsten Akteure im GRAFT Ökosystem ist der Service-Provider des Händlers (Merchant Service-Provider / MSP). Die Rolle eines MSP besteht darin, dem Händler Dienste zum Betrieb und zur Unterstützung des Zahlungsnetzwerks bereitzustellen, die Verfügbarkeit des Netzwerks sicherzustellen (normalerweise als Service Level Agreement oder SLA bezeichnet), die Geräte und Ausrüstung (wie Zahlungsterminals) bereitzustellen und zu verwalten, sowie Berichte zu generieren.
Um dies einem MSP zu ermöglichen, wird ein weiterer Dienstleister benötigt, der folgende Aufgaben verantwortet:

- Verwaltung und Konfiguration der Terminals (einschließlich der Wallet-Adresse).
- Handhabung der MSP-spezifischen Gebührenordnung für den MSP (ein MSP kann wählen, ob er verschiedene Servicestufen unterschiedlich behandeln oder unterschiedliche Gebühren für verschiedene Transaktionssummen berechnen möchte).
- Pflege von Transaktionsberichten und Analysen für den Händler

Ein solches Zahlungs-Gateway kann von einem Dritten entworfen und implementiert werden, wie beispielsweise einem traditionellen Zahlungsabwickler, der Zahlungen mit Kryptowährungen in sein Leistungsportfolio aufnehmen möchte. GRAFT erstellt eine "Referenzimplementierung", um im Rahmen einer Go-To-Market-Strategie eine schnellere Akzeptanz zu ermöglichen.

Da GRAFT ein dezentrales Zahlungsnetzwerk ist, ist das Zahlungs-Gateway eine multi-Instanz Open-Source-App, bei der jeder sein eigenes Zahlungs-Gateway hosten, sowie ein Service-Provider im Netzwerk werden kann. Das Zahlungs-Gateway ist ein weiteres Element, welches die GRAFT-Zahlungsapplikationen auf Hardware-Zahlterminals und die GRAFT-E-Commerce-Schnittstellen verwaltet und mit den GRAFT-Supernodes verbindet. Da für Zahlungs-Gateways die Transaktionen sichtbar sind, wird es als Bestandteil der "Backoffice"-Anwendungen des Händlers betrachtet.

Transaktionsarten und Zahlungsströme

GRAFT führt die folgenden Transaktionsarten und Zahlungsströme ein, um Händlertransaktionen zu erleichtern und bestehende Zahlungs- und Point-of-Sale-Anwendungen zu unterstützen.

Autorisierung

Die Autorisierung wird verwendet, wenn der genaue Endbetrag einer Transaktion zum Zeitpunkt der Verkaufsbeginn unbekannt ist. Zum Beispiel: Bezahlen an der Tankstelle, das Einchecken von Mietwagen, die Reservierung von Hotelzimmern oder Bezahlen in einem Restaurant.

Dies geschieht analog zur Autorisierung der Debitkarte. Eine autorisierte Transaktionsart wird vom Händler initiiert und vom Käufer bestätigt. Das Konto des Käufers ist vorübergehend für den vom Zahlungsempfänger (Händler) angeforderten und vom Käufer bestätigten Betrag und die Dauer (Blockanzahl) gesperrt, oder bis der Betrag durch eine nachfolgende "Complete"-Transaktion bestätigt wird. Die Autorisierungssperre kann auch durch eine vom Zahlungsempfänger vor Ablaufdatum/-zeit ausgestellte „Storno“-Transaktion wieder freigegeben werden. Die Gelder werden vom Netzwerk nach

Ablaufdatum/-zeit automatisch an den Käufer zurückgegeben, wenn der Zahlungsempfänger sie nicht durch Senden einer "Complete"-Transaktion in Anspruch genommen hat.

PreAuth

Dies ist ähnlich wie bei der langfristigen Autorisierung, mit dem Unterschied, dass der Käufer nicht garantiert, dass die Mittel zum Zeitpunkt der Ausführung verfügbar sind. PreAuth ist ein langfristiger Vertrag zwischen dem Käufer und dem Zahlungsempfänger. Im Gegensatz zur Autorisierung, die vom Zahlungsempfänger nicht storniert werden kann, kann PreAuth jederzeit storniert werden, indem Geld von dem Konto übertragen wird, das mit der vorautorisierten Transaktion verbunden ist.

PreAuth eignet sich für langfristige Zahlungsvereinbarungen, wie ein monatliches Serviceabonnement oder die tägliche Abrechnung von Hotelzimmern. Der Zahlungsempfänger gibt (und der Käufer bestätigt) den maximalen Betrag einer einzelnen Transaktion, die maximale Gebühr und den minimalen Intervall zwischen den Transaktionen an.

Fertigstellung (Complete)

Fertigstellung (bzw. Complete) finalisiert die Zahlung, die durch Autorisierungs- oder PreAuth-Transaktionen ausgelöst wurde. Der tatsächliche Betrag von der Fertigstellung kann niedriger sein als der zuvor genehmigte Betrag; es kann mehrere Fertigstellungen geben, aber der Gesamtbetrag wird den Betrag von der Autorisierung nicht überschreiten.

Die Fertigstellung wird verwendet, nachdem eine zuvor autorisierte Transaktion abgeschlossen wurde und der genaue Betrag bekannt ist - zum Beispiel beim Bezahlen an der Tankstelle (nach dem Tanken), Abgeben des Mietwagens, Auschecken im Hotel oder das Bezahlen im Restaurant mit Trinkgeld.

Verkauf (Sale)

Der Verkauf (bzw. Sale) wird sequentiell und automatisch vom Netzwerk als eine einzige Transaktion autorisiert und abgeschlossen. Der Verkauf ist eine typische Händlertransaktion in einem Online- oder konventionellen Geschäft.

Transfer

Der Transfer wird verwendet, um Geld zwischen GRAFT Konten zu transferieren. Es ist das gleiche wie beim Verkauf, wird aber vom Sender ohne Zustimmung des Empfängers initiiert. Diese

Transaktionsart kann für Peer-to-Peer-Zahlungen, Börsen und Transfers zwischen verschiedenen Konten verwendet werden.

Cancel

Storno (bzw. Cancel) wird verwendet, um die Autorisierung und Freigabe der autorisierten Gelder abzubrechen und zu stornieren (entfernt die Kontosperre).

Issue

Issue aktiviert eine GRAFT Prepaid-Karte, einen Geschenkgutschein, Treuepunkte, ein Shop-Guthaben oder einen Rabattcoupon.

Einlösung (Redeem)

Die Einlösung (bzw. Redeem) ermöglicht die Zahlung mit einer Prepaid-Karte, einem Geschenkgutschein, Treuepunkten, einem Shop-Guthaben oder einem zuvor von GRAFT ausgestellten Rabattcoupon.

Austausch (Exchange)

Der Austausch (oder auch Exchange) wird verwendet, um Gelder zwischen GRAFT-Token und anderen wichtigen Kryptowährungen, kryptographischen Token und lokalen Fiat-Währungen nach dem besten Angebot von Supernodes zu tauschen.

Planung (Schedule)

Die Planung (bzw. Schedule) wird verwendet, um eine Transaktion so zu planen, dass sie zu einem späteren Zeitpunkt/Datum stattfindet. Sie erfordert eine zusätzliche Bestätigung durch den Benutzer.

Treuhandkonto (Escrow)

Das Treuhandkonto (bzw. Escrow) wird verwendet, um hinterlegte Gelder bei einem definierten Ereignis freizugeben.

Rückerstattung (Refund)

Eine Rückerstattungstransaktion (bzw. Refund) gibt die Geldmittel zurück, auf die der Transaktionszeiger verweist. Es erfordert eine Rücksendegenehmigung (RMA) vom Verkäufer.

Abwicklung von Transaktionen mit GRFT-Token als Zahlungsmethode

Im Gegensatz zu Bitcoin, anderen Kryptowährungen und kryptographischen Token, sowie bei Zahlungskarten ähnlich, werden Zahlungsanfragen vom Empfänger (Händler) bearbeitet und gestellt, mit Ausnahme von Transfer und Exchange, die vom Absender initiiert werden (d.h. jeder der Geld zwischen GRAFT-Konten bewegen möchte). Im Gegensatz zu Kredit- und Debitkarten werden Zahlungsanfragen jedoch vom Käufer, der von der GRAFT Wallet App dazu aufgefordert wird, explizit bestätigt bevor er die Transaktion digital signiert und an das Netzwerk sendet. Einzige Ausnahme ist die Redeem-Funktion bei Verwendung eines Papier/Plastik-Geschenkgutscheins oder Coupons, der von der Händler-Zahlungsanwendung gescannt werden kann, wenn der Kunde die mobile App nicht nutzen möchte oder überhaupt kein GRAFT-Konto hat.

Verarbeitung von Transaktionen mit alternativen Zahlungsmitteln

Um den Käufern die bestmögliche Benutzererfahrung und den Händlern bessere Konversionsraten zu bieten, kann eine GRAFT-Zahlungstransaktion verschiedene konvertierbare Kryptowährungen, kryptographische Token oder lokale Fiat-Währungen in Form einer Kredit-/Debitkarte als Eingabe über die GRAFT Wallet App des Käufers verwenden. Börsengebühren, Bankgebühren und Bearbeitungsgebühren für Kredit-/Debitkarten können zusätzlich zu den üblichen GRAFT-Transaktionsgebühren über GRAFT-Coins vom Händler entsprechend erhoben werden. Wir gehen davon aus, dass diese Gebühren vom Zahlungsempfänger getragen werden und für den Käufer unsichtbar sind, da die Zahlungsmethode den Verkaufspreis nicht beeinflusst. Die automatische Sofortkonvertierung von GRAFT wird dazu beitragen, Kryptozahlungen von Mainstream-Nutzern zu übernehmen, die nicht ausreichend mit Kryptowährungen oder kryptographischen Token Ökosystemen vertraut sind und sich mit traditionellen Zahlungsmethoden wohler fühlen, aber eine bessere Sicherheit, Privatsphäre und volle Anonymität für ihre Transaktionen anstreben.

Wenn sich ein Käufer entscheidet mit einer alternativen Kryptowährung, kryptographischen Token oder einer Kredit-/Debitkarte zu bezahlen, tauscht das GRAFT-Netzwerk automatisch andere Kryptowährungen, kryptographische Token oder konvertiert Kreditkartenzahlungen, die in lokaler Fiat-Währung sind, in Echtzeit im Rahmen des Transaktionsprozesses über Exchange Broker in GRFT um. Die Exchange Broker, die auf GRAFT-Supernodes laufen, sind für die Ausführung der Austauschs, die Belastung der Käufers und die Ausführung der Auszahlungen an den Händler verantwortlich. Wenn der Käufer als Zahlungsmittel eine alternative Kryptowährung, kryptografische Token oder eine

Kredit-/Debitkarte selektiert, wählen die Supernodes (als "Supernode sample" bezeichnet) automatisch das beste Angebot unter allen Exchange Brokern aus. Die Selektion basiert auf zuvor ausgewählten Händlern und einer Kombination aus günstigen Wechselkurs und hohem Reputationswert.

Exchange Brokers

Wenn ein Kunde mit GRAFT-Token bezahlt und der Händler auch mit GRAFT-Token bezahlt werden möchte, wird das Geld automatisch und sofort vom Käuferkonto abgebucht und über das GRAFT-Netzwerk auf das Händlerkonto überwiesen. Wenn der Kunde jedoch mit einem anderen Zahlungsmittel bezahlen möchte und/oder der Händler in einer anderen Währung bezahlt werden möchte, muss das GRAFT-Netzwerk einen speziellen Mechanismus verwenden.

Um nicht dezentralisierbare, aber von Verbrauchern und Händlern stark nachgefragte Prozesse der Zahlungsabwicklung umzusetzen, hat das GRAFT-Netzwerk die Exchange Broker eingeführt. Wenn das GRAFT-Netzwerk selbst eine bestimmte Operation nicht vollständig dezentral bearbeiten kann, wird es diese an das Netzwerk der Exchange Broker delegieren. Händler können einen einzelnen (z. B. sehr vertrauenswürdigen oder den günstigsten) Exchange Broker oder eine Gruppe davon wählen.

Der Exchange Broker ist für die Aufrechterhaltung der Sicherheit und die notwendige Einhaltung der regulatorischen Vorschriften zur Transaktionsverarbeitung von Zahlungskarten und Tauschprozessen verantwortlich[13] (einschließlich der PCI DSS-Konformität und der Vorschriften zur Bekämpfung der Geldwäsche).

Im Folgenden sind die möglichen Exchange Broker Arten aufgeführt:

Händler/Point-of-Sale seitige Exchange Broker:

- Einzahlungs-Broker (Pay-In Broker)
- Auszahlungs-Broker (Pay-Out Broker)

Käufer-/Wallet-seitige Exchange-Broker:

- Wechsel-Broker (Interchange Broker)
- Aufladungs-Broker (Top-Up Broker)

Für jede der wichtigsten auf https://coinmarketcap.com/ gelisteten Kryptowährungen, stehen eine Reihe von Kryptowährungs-Broker zur Verfügung, beginnend mit den "Top 10" nach

Marktkapitalisierung. Die Exchange Broker werden die Liquidität jeder Kryptowährung erhöhen, indem sie verschiedene Zahlungsoptionen sowohl auf der Käufer- als auch auf der Händlerseite der Transaktion anbieten.

Die Exchange Broker von Kryptowährungen werden in Zusammenarbeit mit bestehenden und/oder neu geschaffenen Börsen implementiert. Es werden letztendlich mehrere Auswahlmöglichkeiten für jede Kryptowährung zur Verfügung stehen, so dass ein Wettbewerbsmarkt entsteht, wodurch bessere Preise und Dienstleistungen angeboten werden können. Die Vielfalt der Dienste und die automatisierten Anmelde-, Auswahl- und Ausführungsprozesse erhalten den dezentralen Charakter des Netzwerks. Jedes einzelne Set enthält vier Exchange Broker, die für jede Kryptowährung implementiert sind.

Pay-In und Pay-Out Broker arbeiten mit der GRAFT POS App und mit Hardware-Zahlungsterminals zusammen. Dadurch wird es jedem Händler ermöglicht, die ausgewählte Kryptowährung als Zahlungsmittel zu akzeptieren, während er den Zahlungsverkehr mit der GRAFT Wallet App oder anderen Kryptowährungs-Wallets durchführt.

Interchange- und Top-up-Broker arbeiten mit den GRAFT Wallet-Apps zusammen. Dadurch wird es jedem Käufer ermöglicht, seine bevorzugte Kryptowährung als Zahlungsmittel auszuwählen, wenn er eine Zahlung an die GRAFT Points-of-Sales (POS), native Wallet-Apps, Nicht-GRAFT-POS Terminals mit GRAFT DAPI oder Nicht-GRAFT-POS, die die ausgewählte Kryptowährung akzeptiert, leistet.

Pay-in Broker

Pay-in Broker ermöglichen es andere Zahlungsmittel als native GRFT-Token zu akzeptieren. Sie wandeln den Zahlungsbetrag sofort in GRFT-Token um und überweisen diese auf das Händlerkonto. Pay-in Broker agieren in Echtzeit und werden Teil der Transaktion zwischen Käufer und Händler. Aus Sicht des Käufers sieht die Transaktion ähnlich aus wie eine reguläre Transaktion zwischen nativen Kryptowährungs-Wallets.

Die Händlerauszahlung wird vom Pay-in Broker in GRFT sofort verarbeitet (wenn der entsprechende Pay-out Broker aktiviert ist, kann die Auszahlung in einer anderen Kryptowährung oder Fiat-Währung erfolgen).

Beispiele für Pay-In Broker:

- Bitcoin Pay-In Broker (für Einzahlungen)
- Ether Pay-In Broker
- Kreditkarten Pay-In Broker

Design und Wirtschaftlichkeit von Pay-In und Pay-Out Brokern

Der Pay-in Broker übernimmt einen bestimmten Betrag oder ein bestimmtes Risiko, die Kryptowährungsauszahlung zu akzeptieren, während GRFT im Gegenzug schnell freigegeben wird (ohne auf die Bestätigung der gewählten Kryptowährung zu warten). Dieses Risiko wird für den Broker durch relativ kleine Retail-Transaktionsbeträge gemildert und unterliegt dem Authorization-Sample, welches die Transaktion über das ursprüngliche Währungsnetzwerk validiert. Das Risiko für den Händler wird durch eine GRFT-Bondtransaktion in Höhe der Einzahlung, die der Broker zu Beginn der Transaktion zurückhält, gemindert. Die Anleihe wird durch das Authorization-Sample so lange zurückgehalten, bis der Broker die Altcoin Zahlung an den Händler genehmigt. Sobald die Altcoin-Transaktion (vom Käufer zum Broker) eingegangen und validiert ist, genehmigt die Authorization-Sample die Zahlung an den Händler und gibt die GRFT-Auszahlung (vom Broker zum Händler) frei. Der Broker ist in der Lage verschiedene Limits für unterschiedliche Beträge, sowie Historie und Risikostufen festzulegen.

Als Gegenleistung für diese Dienstleistung zieht der Pay-In Broker 0,25% Wechselkursgebühr von der GRFT-Zahlung an den Händler ab, während die an dem Authorization-Sample teilnehmenden Supernodes ihre Standard GRFT Transaktionsgebühr (0,5%) berechnen.

Das folgende Flussdiagramm (Sequenzdiagramm) zeigt, wie der Bitcoin akzeptierende Pay-In Broker die Tauschtransaktion durchführt und Bitcoin-Zahlungen im Auftrag der Verkaufsstelle des Händlers akzeptiert. Der Käufer kann jede beliebige Wallet mit Bitcoin-Unterstützung verwenden. Der Händler erhält die Auszahlung in GRFT.

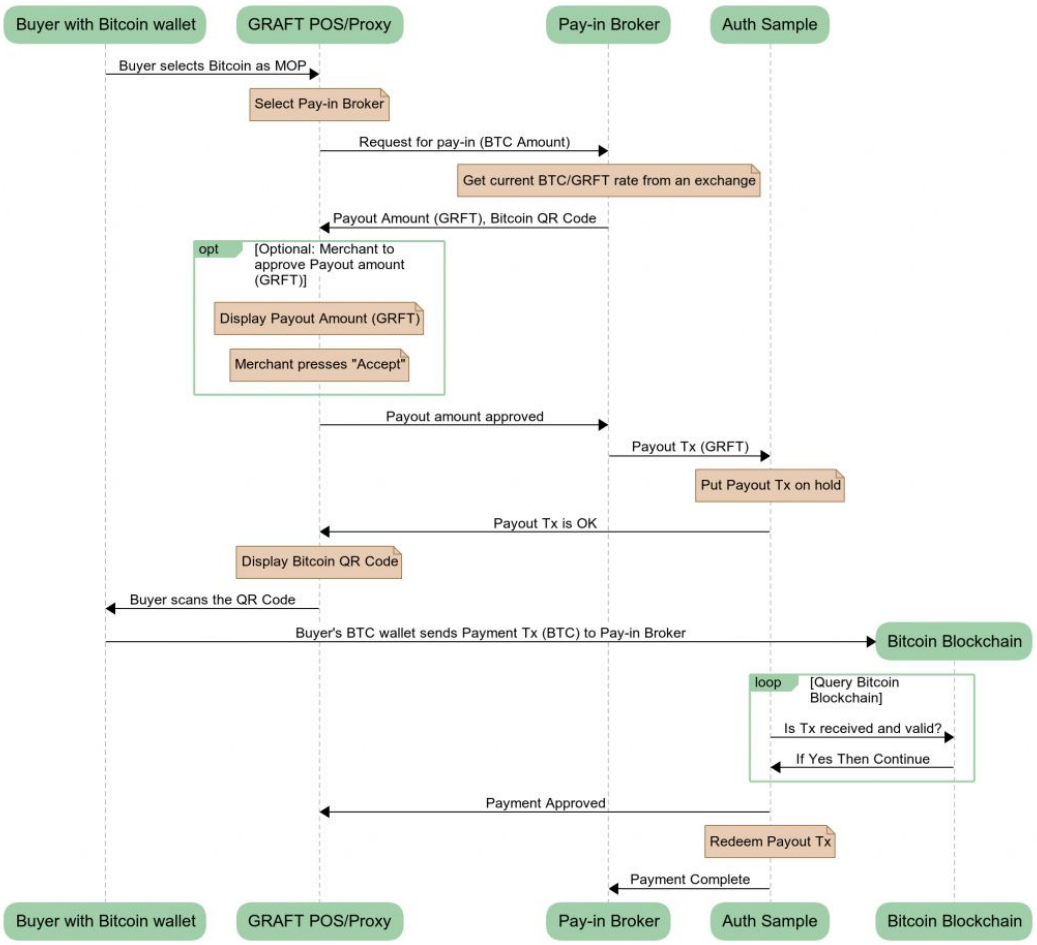

Abbildung 5: GRAFT Bitcoin Pay-in Broker Flussdiagramm der Transaktion

Der Pay-Out Broker tauscht GRFT in d ie Auszahlungswährung der Wahl, wie vom Händler gewünscht. Die Transaktion ist asymmetrisch. Das bedeutet, dass der zweite Teil der Zahlung in der Regel länger (manchmal viel länger) dauert, bis das Settlement auf der Empfängerseite erfolgt ist. Um sicherzustellen, dass der Pay-Out Broker die Zahlung ohne Doppelausgaben leistet, setzt der Broker eine Anleihe mit einem Betrag in Höhe des Transaktionsbetrags ein. Das Staken ist erfolgt, wenn die GRFT-Zahlung des Händlers per “authorization sample” auf Halten gesetzt wurde. Wenn das “authorization sample” (nach Ablauf der Kulanzzeit) feststellt, dass die Auszahlungsbeträge nicht beim Händler eingegangen sind, storniert sie die Transaktion und der Pay-Out Broker erhält die GRTF-Zahlung nicht vom Händler.

Im Gegenzug für diese Dienstleistung erhält der Pay-Out Broker eine Umtauschgebühr von 0,25%. Darüber hinaus erheben die Authorization-Sample Supernodes ihre reguläre Transaktionsgebühr (0,5%).

Duale Pay-In und Pay-Out Broker

Dieselben Broker können (und werden es höchstwahrscheinlich auch) abwechselnd als Pay-In und Pay-Out Broker fungieren. Lassen Sie uns zum Beispiel ein Bitcoin Exchange Broker (EB) betrachten, der sowohl Ein- als auch Auszahlungsgeschäfte durchführen möchte.

Der Broker hat eine Bitcoin-Wallet mit 0,01 BTC. Der Broker erhält von einem Händler eine Auszahlungsanforderung 100 GRFT in 0,01 BTC umzutauschen (vorausgesetzt, der aktuelle Wechselkurs beträgt 0,01 BTC = 100 GRFT). Der Ablauf einer solchen Auszahlungstransaktion zwischen dem Broker und dem Händler ist in der folgenden Abbildung dargestellt.

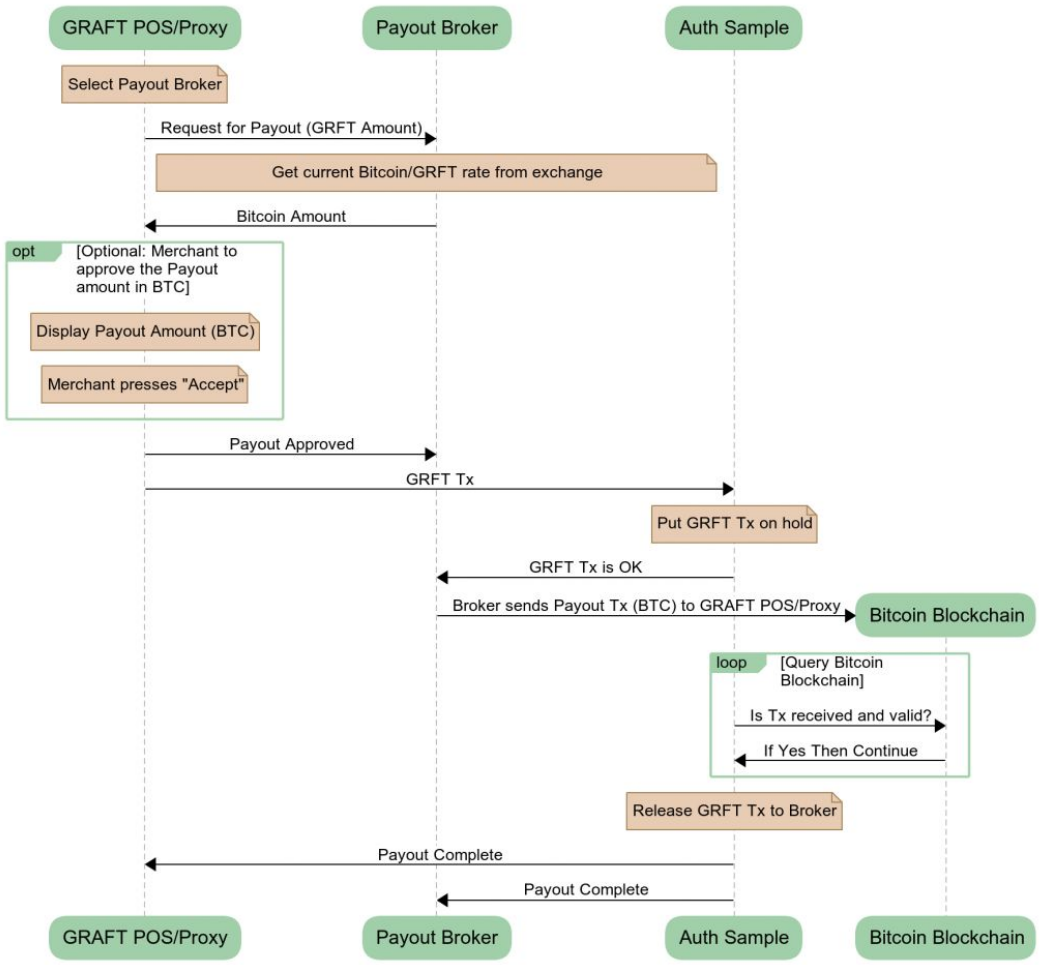

Abbildung 6: GRAFT Bitcoin Payout Broker Transaktionsablauf

Der Broker nimmt die Anfrage an und sendet 0,01 BTC (abzüglich der Bitcoin-Netzwerkgebühr) an den Händler, während der Händler die 100,75 GRFT-Zahlung (100 GRFT Betrag + 0,25 GRFT Brokergebühr

+ 0,5 GRFT Authorization-Sample) über den Broker generiert und an die Authorization-Sample sendet. Das Beispiel setzt die 100,75 GRFT-Transaktion auf Halten und benachrichtigt den Broker, der dann 0,01 BTC an den Händler sendet. Nach der Abwicklung der BTC-Transaktion (10-60 Minuten aus Gründen der Argumentation und in Abhängigkeit von den Bitcoin-Netzgebühren) wird die 100 GRFT-Transaktion freigegeben und der Broker erhält nun die 100 GRFT-Zahlung plus 0,25 GRFT-Gewinn.

Der Broker kann nun in den Pay-In Broker Modus wechseln. Als Pay-In Broker erhält der EB die Anfrage 0,01 Bitcoin in 100 GRFT umzutauschen. Der Broker akzeptiert diese Anfrage und überweist 100 GRFT (abzüglich Gebühren). Sobald 0,01 BTC eingegangen sind, kann der Broker wieder zum Payout-Broker werden und hat nun 0,01 BTC und 0,25 GRFT Gewinn.

Unter der (konservativen) Annahme, dass ein einzelner Pay-In/Pay-Out Zyklus 1 Stunde dauert, kann der Broker in einem einzigen 24-Stunden-Zeitraum (ohne Aufzinsung) rund 12%* verdienen, was ein lukratives Geschäftsmodell für den Exchange Broker ergibt (*nur Schätzwert).

Über Händler Zahlungen hinaus: Die Echtzeit-Börse (DEX)

Das oben beschriebene System der Exchange Broker kann über das von GRAFT beabsichtigte Zahlungsökosystem hinaus funktionieren und sich zu einer dezentralen Echtzeit-Börse (DEX) entwickeln. Da die nicht vertrauenswürdigen Exchange-Operationen (Atomic Swaps) nahezu in Echtzeit für externe Entitäten operieren und auf der GRAFT Autorisierungs-/Validierungsschicht (das Netzwerk der GRAFT-Supernodes) aufbauen, können dieselben Atomic-Swaps um Echtzeit-Austauschmöglichkeiten wie BTC<->ETH erweitert werden.

Interchange Broker (Wechsel-Broker)

Der Pay-In Interchange Broker arbeitet mit der GRAFT Wallet App zusammen, um eine Zahlung an ein natives Kryptowährungs-Wallet oder einen Nicht-GRAFT-POS zu ermöglichen, der die Kryptowährung akzeptiert. Der Interchange Broker erstellt eine regelmäßige Kryptowährungstransaktion im nativen Format für das jeweilige Netzwerk und sendet sie an die native Empfängeradresse. Es wird eine Netzwerktransaktionsgebühr erhoben, die in diesem Fall dem Absender in Rechnung gestellt wird, da die Transaktion durch das GRAFT-Netzwerk nicht vollständig bereitgestellt wird. Die Zahlung wird nicht sofort bearbeitet, da der Empfänger nicht am GRAFT-Netzwerk teilnimmt. Dieses Szenario ist sowohl für den Käufer als auch für den Händler weniger vorteilhaft als eine GRFT-Transaktion, da die Geschwindigkeit der Transaktion geringer und die vom Käufer zu zahlenden Transaktionsgebühren

höher sind. Es wird jedoch von GRAFT unterstützt, damit der Käufer seine Wallet auch außerhalb des GRAFT-Ökosystems flexibel einsetzen kann.

Der Interchange Broker wird sofort den notwendigen Betrag von GRFT vom Konto des Käufers in die gewählte Kryptowährung umtauschen. Der Käufer zahlt dem Interchange Broker eine kleine Wechselkursgebühr, die in Form des Wechselkurses bezahlt werden kann.

Beispiele für Interchange-Broker:

- Bitcoin Interchange Broker
- Ether Interchange Broker

Pay-Out Broker (Auszahlungs-Broker)

Der Pay-Out Broker ermöglicht die Auszahlung von einem GRAFT-Händlerkonto in Bitcoins, Altcoins oder lokaler Fiat-Währung. Die Auszahlung kann manuell oder automatisch erfolgen.

Auszahlungsgebühren bzw. Wechselkurse für Auszahlungen, die entweder von Pay-In oder Pay-Out Exchange Brokern aufgerufen werden, können je nach Auszahlungshäufigkeit variieren. Abhängig vom Transaktionsvolumen können tägliche Auszahlungen deutlich weniger kosten als sofortige Auszahlungen, da der Broker mehr Geld aufbringen und nur eine einmalige Netzwerkgebühr für eine einzelne Auszahlungstransaktion zahlen muss, verglichen mit der Zahlung einer separaten Gebühr für jede sofortige Auszahlungstransaktion.

Beispiele für Pay-Out Broker:

- GRAFT Pay-Out (“Stable Value”) Token Broker
- USDT Pay-Out Broker
- Bank ACH Pay-Out Broker
- PayPal Pay-Out Broker
- Bitcoin Pay-Out Broker

Top-Up Broker (Aufladungs-Broker)

Der Top-Up Broker ermöglicht das Aufladen einer Wallet durch den Umtausch von Bitcoin, Altcoins oder lokaler Fiatwährung in GRFT. Dieses Szenario ist sowohl für den Käufer als auch für den Händler von großem Vorteil, da alle Gebühren (einschließlich der Netzwerkgebühren der Ziel-Kryptowährung)

vom Händler bezahlt werden und die Zahlung sofort genehmigt wird. Für den Käufer sind die Vorteile offensichtlich: Keine Gebühren, die mit der Zahlung verbunden sind und die Möglichkeit mit der Wunsch Kryptowährung bei einem Händler zu zahlen, der diese nicht akzeptiert. Für den Händler ist es wichtig eine sofortige Autorisierung zu erhalten, um mehr Kunden in Echtzeit bedienen zu können und Zahlungen in verschiedenen Kryptowährungen anzunehmen. Die Tatsache, dass alle Gebühren vom Händler bezahlt werden, wie bei "traditionellen" Kredit-/Debitkartenzahlungen üblich, ermöglicht eine wesentlich bessere Konversion der Kunden.

Der Top-Up Broker kann auch Anfragen von größeren Beträgen mit besseren Kursen abwickeln.

Beispiele für Top-Up Broker:

- Kreditkarte Top-Up Broker
- Bitcoin Top-Up Broker
- Bank ACH Top-Up Broker

Händler Auszahlungen

Ein Händler kann sich entscheiden seine Erlöse aus Transaktionen in anderen Kryptowährungen wie Bitcoin, kryptographische Token, Pay-Out Token ("stable value") oder in lokaler Fiat-Währung zu erhalten. In diesem Fall wird die Zahlungswährung der Transaktion von einem Exchange Broker im Rahmen derselben Transaktion oder später, je nach Händlereinstellungen, verarbeitet. Dadurch wird sichergestellt, dass dem Händler der genaue Preis in Landeswährung abzüglich der anfallenden Gebühren bezahlt wird. Das Supernode Sample (Authorization-Sample) wählt automatisch das beste Angebot unter allen Exchange Brokern aus, basierend auf einer Kombination aus Händlerauswahl, einem guten Wechselkurs, sowie einem hohen Reputationswert.

Volatilität

Die meisten Händler wollen in ihrer Landeswährung bezahlt werden. Händler verwenden Fiat als Währung und nicht Bitcoins, andere Kryptowährungen oder kryptographische Token, um Ihre Kassenbestände aufzufüllen, ihre Rechnungen, sowie die Gehälter der Mitarbeiter zu bezahlen. Außerdem können sie mit Hilfe von Fiat im Falle einer Rückgabe Rückerstattungen ausführen. Die meisten Händler können sich keine hohe Volatilität leisten, insbesondere kleine Händler. Da Graft-Token (GRFT) handelbar sind, wenn sie direkt für Händlerauszahlungen verwendet werden, kann die Volatilität zu einem Problem werden. GRAFT löst die Volatilitäts Probleme durch die sofortige, zeitnahe Abwicklung der Transaktionsverarbeitung, die einen möglichen Wertverlust durch Volatilität minimiert, sowie durch spezielle "stable value" Auszahlungs-Token. Die Zahlungsapplikation des

Händlers kann den Transaktionsbetrag automatisch an den aktuellen Wechselkurs anpassen und direkt nach Abschluss der Transaktion per Online-Tausch in Landeswährung einlösen.

Pay-Out (“Stable Value”) Token / Auszahlungs-Token mit stabilem Wert

Pay-Out Token sind eine spezielle Art von Händler-Token, die verwendet werden, um Händlerauszahlungen in der lokalen Fiat-Währung zu ermöglichen, sowie die Lücke zwischen den beiden Welten aus Kryptowährungstransaktionen und Fiat-Währungstransaktionen zu verbinden und schließen. Es stellt eine lokale Währung dar und kann auf der GRAFT Blockchain in Echtzeit über die Tier Supernodes der Blockchain abgewickelt werden. Der Pay-Out Token basiert auf der GRAFT Händler-Token Technologie, ähnlich zu Geschenk-, Prämien- und anderen Händler-Token Arten.

Unterzeichnung von Pay-Out Tokens

Das Hauptziel bei der Erstellung von Pay-Out Token ist es, Händlern eine einfache und zuverlässige Möglichkeit zu bieten, Zahlungen in stabilen lokalen Fiat-Währungen zu erhalten und gleichzeitig die Verwendung von zentralen Zahlungsabwicklern zu vermeiden. Pay-Out Token werden von verantwortlichen Token-Underwritern (z.B. Banken) ausgegeben und verwaltet. Wenn jemand (z.B. der Pay-Out Broker) Pay-Out Token vom Token-Underwriter kauft, generiert das Unternehmen eine notwendige Menge an Token und überträgt sie an den Käufer im Austausch gegen einen entsprechenden Betrag in Fiat-Währung. Wenn jemand (der Händler oder Pay-Out Broker im Namen des Händlers) Pay-Out Token an den Token-Underwriter zurückverkauft, zerstört das Unternehmen die Token und zahlt einen entsprechenden Betrag an lokaler Fiat-Währung an den Verkäufer. Somit werden Pay-Out Token immer durch eine ausreichende Menge an Fiat-Währung unterstützt. Ihr Preis bleibt dadurch immer identisch und entspricht dem Fiat-Währungs-Kurs. Beispielsweise können 100 GRAFT.USD immer für 100 USD gekauft oder verkauft werden. Pay-Out Token werden von lizenzierten Token-Underwritern nur im Austausch gegen gleiche Beträge in Fiat-Währung ausgegeben. Darüber hinaus können die Rechte zur Handhabung bestimmter Pay-Out Token an lokale Geschäftsbanken oder sogar nationale Regierungen delegiert (lizenziert) werden.

Verarbeitung von Auszahlungen (Payouts)

Es gibt mehrere Auszahlungsoptionen: GRAFT Token, ursprüngliche oder andere Kryptowährungen, GRAFT Pay-Out Token oder lokale Fiat-Währungen (Tabelle 2). Für jede dieser Optionen gibt es GRAFT

Pay-Out Broker Services. Wenn der Händler die Zahlungsmethoden die er akzeptieren möchte auswählt, fordert Ihn die GRAFT Point-of-Sale Anwendung auf, alle verfügbaren Broker-Services-Optionen abhängig von der Identität und den Standorteigenschaften des Händlers einzugeben, damit er sich für alle gewünschten Broker-Services anmelden kann. Wenn mehrere Pay-Out Broker für die gleiche Art von Service verfügbar sind und vom Händler ausgewählt wurden, wählt die GRAFT Point-of-Sale Anwendung automatisch das beste Angebot während der Transaktionsabwicklung aus.

Tabelle 2: Beispiele für eine Vielzahl von akzeptierten Zahlungsmethoden und Auszahlungen

Vom Kunden ausgewählte Zahlungsmethode	**Vom Händler ausgewählte Zahlungsmethode**	**Accept Broker**	**Payout Broker**
GRFT	GRFT	None (GRAFT network)	None (GRAFT network)
Gift Certificate, Loyalty Rewards, Store Credit Redemption	N/A	None (GRAFT network)	N/A
GRFT	USD	None (GRAFT network)	Bank Transfer Payout Broker
GRFT	Bitcoins	None (GRAFT network)	Bitcoin Payout Broker
Bitcoins	GRFT	Bitcoin Accept Broker	None (GRAFT network)
Bitcoins	GRFT	Bitcoin Accept Broker	Bitcoin Payout Broker
Bitcoins	USD	Bitcoin Accept Broker	Bank Transfer Payout Broker

Credit Card	GRFT	Credit Card Accept Broker	None (GRAFT network)
Credit Card	Bitcoins	Credit Card Accept Broker	Bitcoin Payout Broker
Credit Card	USD	Credit Card Accept Broker	Bank Transfer Payout Broker

Händler-Token und VChains

Neben schnellen und kostengünstigen Transaktionen legen Händler großen Wert auf Kundenbindung und Branding. Diese Funktionalität wird durch die Token-Schicht der GRAFT-Währung aktiviert. Der Token repräsentiert die domänenspezifische (Händler) Nutzung von GRAFT und bietet intelligente, vertraglich gesicherte Funktionen wie die Anhäufung und Nutzung von Treuepunkten, Belohnungspunkten, Verkaufsrabatten, Ausgabenrabatten, Wettbewerbsrabatten, Coupons und Shop-Guthaben.

Eine Kaffeekette kann zum Beispiel einen Händler-Token erstellen und Promotionsregeln daran anknüpfen, die einem Kunden die Möglichkeit geben, zu einer bestimmten Tageszeit Rabatte auf Eisgetränke zu erhalten. Die Einkäufe würden entsprechend nach den vereinbarten Bedingungen abgerechnet und Belohnungen basierend auf der Aktivität oder Nichtaktivität angeboten. GRAFT Händler-Token würden einen sehr effizienten Mechanismus für das Couponing bieten, indem sie es den Händlern ermöglichen die Regeln für die Erstellung und Zuteilung von Coupons in ihrem Domain-Netzwerk zu steuern.

Händler-Token

Der Händler-Token ist ein vordefinierter Smart Contract, der es ermöglicht einen privaten Token zu erstellen, der seinem Besitzer gehört. Im Gegensatz zu einigen anderen Smart Contracts und Token-Plattformen erfordert die Erstellung des GRAFT Händler-Tokens keine Programmierung und kann von jedem durchgeführt werden.

Die im Folgenden beschriebenen Geschäftsfunktionen sind typischerweise nur unter Verwendung

komplexer Drittanbieter und mit hohen Implementierungskosten verbunden, was diese Dienste für kleine und mittlere Unternehmen unzugänglich und für große Unternehmen teuer macht. GRAFT Händler-Token ermöglichen es jedem Händle, diese wichtigen Geschäftsfunktionen mit minimalem Aufwand und niedrigen Kosten zu implementieren.

Arten von Händler-Token

Händler-Token ermöglichen es Händlern ihre eigenen Open-Loop und Closed-Loop [14] Produkte innerhalb von Minuten ohne initiale Investitionen, Gebühren oder Registrierung bei einer zentralen Behörde zu erstellen und anzuwenden. Dazu gehören unter anderem Geschenkgutscheine, Treueprämien oder Kreditprogramme. Händler können Geschenkgutscheine auf ihrer Website oder in Ladengeschäften für die Landeswährung, andere Kryptowährungen, kryptografische Token oder GRFT verkaufen und annehmen.

Alle GRAFT-Transaktionen, einschließlich der Ausgabe und Einlösung von Geschenkgutscheinen, Treuepunkten und Shop-Gutschriften, werden in Echtzeit über eine Standard-API abgewickelt, die problemlos in bestehende Point-of-Sale Anwendungen integriert werden kann.

Shop-Gutschriften

Alle GRAFT-Transaktionen, einschließlich der Ausgabe und Einlösung von Geschenkgutscheinen, Treuepunkten und Shop-Gutschriften, werden in Echtzeit übeShop-Gutschriften werden in der Regel von Händlern zur Abwicklung von Kauf Rückgaben und bei Umtausch verwendet, sowie wenn die Rückgabe nicht mit der ursprünglichen Zahlungsmethode erfolgen kann oder die Rückgaberichtlinien des Händlers keine vollständige Rückerstattung zulassen. Shop-Gutschriften werden im Wesentlichen bei Börsen umgewandelt, so dass der Händler den Kunden und die damit verbundenen Einnahmen nicht verliert. eine Standard-API abgewickelt, die problemlos in bestehende Point-of-Sale Anwendungen integriert werden kann.

Treueprämien haben in der Regel relativ kurze Verfallsdaten. Auf diese Weise ermutigt der Händler die Kunden, mehr Belohnungen zu verdienen und eliminiert die Ansammlung sehr großer Mengen von Belohnungspunkten, da diese schließlich nutzlos werden können.

Geschenkgutscheine

Geschenkgutscheine können von Händlern ausgestellt werden, um Kunden zu gewinnen. Um die Wirkung zu erhöhen, können Geschenkgutscheine mit einem Rabatt (für weniger als den Nominalpreis) verkauft werden. Geschenkgutschein-Token verfallen in der Regel nicht oder haben ein

sehr spätes Verfallsdatum, da sie im Wesentlichen die Fiat-Währung darstellen.

Kunden können Geschenkgutscheine sowohl online, als auch im Geschäft von verschiedenen Händlern kaufen und in lokaler Fiat-Währung, Kryptowährung oder kryptographischen Token bezahlen. Der Geschenkgutschein oder der Gutschriftswert in der lokalen Fiat-Währung wird vom ausstellenden Händler und vom Netzwerk garantiert, so dass sie ihren ursprünglichen Nennwert nie verlieren. Kunden können Geschenkgutscheine im Geschäft des ausstellenden Händlers zum Nominalwert in Landeswährung einlösen oder jederzeit auf dem Marktplatz für lokale Fiat-Währung, Kryptowährung oder kryptografische Token zum aktuellen Marktwert verkaufen.

Geschenkgutscheine

Gift certificates can be issued by merchants in order to attract customers. In order to increase the effect, gift certificates can be sold with a discount (for less than their nominal price). Gift certificate tokens usually either do not expire or have a very distant expiration date as they basically represent the fiat currency.

Customers can buy gift certificates from various merchants and marketplaces, online and in store, and pay in local fiat currency, cryptocurrency, or cryptographic tokens. The gift certificate or store credit value in local fiat currency is guaranteed by the issuing merchant and by the network, so they will never lose its initial nominal value. Customers can redeem gift certificates at the issuing merchant's store by its nominal local currency value or sell it at any time on the marketplace for local fiat currency, cryptocurrency, or cryptographic tokens using its current market value.

Rabatt Coupons

Rabatt Coupons können für einmalige oder langfristige Aktionen verwendet werden. Die Coupons können öffentlich oder an Einzelpersonen in wallet oder papierform verteilt werden. Der Coupon kann dann am Point-of-Sale gescannt werden, um einen vergünstigten oder sogar kostenlosen Artikel zu erhalten.

Transaktionsarten der Händler-Token

Erstellen

Erstellung neuer Händler-Token ("smart contract"). Kann über die Point-of-Sale Anwendung durchgeführt werden.

Erneuern

Erneuerung der Händler-Token (“smart contract”). Kann über die Point-of-Sale Anwendung durchgeführt werden.

Hinzufügen

Fügt dem Umlauf weitere Händler-Token hinzu.

Ausgeben

Die Point-of-Sale Anwendung des Händlers sendet Händler-Token an die Wallet des Kunden oder druckt ein Paper-Wallet für Ihn.

Einlösen

Der Kunde löst Händler-Token am Point-of-Sale über die Verwendung seiner Wallet App oder eines Paper-Wallets ein

Händler-Token Gebühren

Alle Händler-Token Gebühren werden an das aktuelle Supernode Authorization-Sample gezahlt.

Händler-Token Transaktionsgebühren

Der Händler bezahlt immer die Token-Transaktionsgebühr. Das heißt der Käufer zahlt die Gebühr nie. Die Transaktionsgebühr wird für jede Transaktion mit einem Händler-Token erhoben, einschließlich Hinzufügen, Ausgeben und Einlösen.

Initialisierungs- und Erneuerungsgebühren

Die initiale “Erstellen” Transaktion impliziert eine besonders hohe Gebühr, da sie mit der Benennung eines Token verbunden ist. Um eine Domänenbesetzung "Domain Squatting" zu verhindern, wird die Anfangsgebühr auf einen angemessenen Betrag festgesetzt der massiven Missbrauch verhindert.

VChains

Die VChain ermöglicht die Erstellung einer virtuellen Kette an Geschäften, so dass mehrere Verkaufsstellen mit derselben privaten "virtuellen Blockchain" verbunden werden können. Für das Wort "VChain" gibt es also eine doppelte Bedeutung: virtuelle Kette und virtuelle Blockchain. Die VChain schafft eine private gemeinsame Plattform für die Verwaltung von Händler-Token und

Artikelkatalogen.

Händler können ihre eigene private VChain erstellen, die nur für sie zugänglich ist und alle Informationen über ihre Token enthält. Die VChain ermöglicht es, mehrere Verkaufsstellen miteinander zu verbinden oder sogar eine Kette mit mehreren Geschäften zu erstellen. Verkaufsstellen, die zu derselben VChain gehören, können dieselben Händler-Token ausgeben und annehmen, denselben gemeinsamen Artikelkatalog, der in der Blockchain gespeichert und gepflegt ist, verwenden und aggregierte Transaktionsberichte generieren, sowie vieles mehr.

Käufer können die VChain verwenden, um mehrere Wallets zu verbinden, damit sie mehrere Konten verwalten und Gelder kostenlos zwischen diesen Konten transferieren können. Diese Funktion ist nützlich für Familien- und Firmenkonten.

VChain Gebühren

Es gibt eine jährliche Initialisierungsgebühr für die Erstellung eines neuen VChain Smart Contracts und eine Verlängerungsgebühr. Diese Gebühren sind erforderlich, um den Smart Contract sicher abzuwickeln und System Missbrauch zu verhindern. Für das Hinzufügen eines weiteren Point-of-Sales oder Wallets wird eine separate jährliche Gebühr erhoben.

Alle VChain Gebühren werden an das aktuelle Supernode Authorization-Sample gezahlt.

Dezentrale Kredite durch Crowdfunding

Ein dezentrales Kredit-Ökosystem durch Crowdfunding besteht aus Kreditnehmern (Karteninhabern, Käufern), Kreditgebern, Identitätsanbietern und Händlern (Verkäufer). Das GRAFT-Netzwerk erleichtert die Kommunikation und die Transaktionen zwischen den Parteien und setzt gemeinsame Regeln durch, um das Betrugsrisiko zu minimieren.

Das GRAFT-Netzwerk verbindet potenzielle Kreditnehmer mit Kreditanbietern, die dem Verbraucher Kredite anbieten. Jeder der im Besitz einer GRAFT Wallet (einer kostenlosen App) ist, kann Kreditnehmer werden. Jeder mit GRAFT Wallet und einem positiven Saldo kann Kreditgeber werden. Jeder mit GRAFT Point-of-Sale Anwendung (kostenlose App), oder einem mit GRAFT SDK integrierten Drittanbieter Point-of-Sale, kann Händler werden. Der Identitätsanbieter ist als Service Plugin auf dem GRAFT Supernode implementiert. Der Identitätsanbieter verwendet eine offene API, die dazu beiträgt den offenen und dezentralen Charakter des gesamten Ökosystems zu erhalten.

Die Kreditanbieter stellen ihre Anforderungen die für den Erhalt des Kredits erforderlich sind, wie die mindest zu erfolgende Identitätverifizierung, das maximale Kreditlimit, das allgemein maximale Kreditlimit (von mehreren Kreditgebern), den Zinssatz, die Mindestrate und das Zahlungsintervall. Kreditnehmer können von mehreren Kreditgebern Kredite erhalten, solange der aktuelle Stand ihres Kontos den Anforderungen des Anbieters entspricht. Identitätsanbieter von Drittanbietern validieren und bestätigen die vom Verbraucher bereitgestellten Identitätselemente, um die Belastung durch die Identitätsprüfung von Kreditanbietern zu verringern und dem Karteninhaber ein gewisses Maß an Anonymität und Datenschutz zu bieten. So kennen Identitätsanbieter die tatsächliche Identität des Verbrauchers und können so ihren langfristigen Reputationswert unabhängig vom Netz- oder Kreditanbieter erhalten. Kreditgeber erhalten einen Anteil der Transaktionsgebühr aus jeder Zahlung, die mit ihrem Kredit abgewickelt wird.

Dem Kreditnehmer wird ein Reputationswert zugewiesen der dynamisch, aufgrund seiner Verbrauchshistorie und dem von den Identitätsanbietern validierten Identitätsgrad, berechnet wird. Je mehr Identitätselemente zur Verfügung gestellt und validiert werden (z.B. Führerschein, Biometrie, Sozialversicherungsnummer), desto höher ist die Anfangsbewertung, was bedeutet, dass dem Karteninhaber mehr Guthaben gewährt werden kann. Eine positive Rückzahlungshistorie erhöht den Reputationswert entsprechend.

Händler sind nur Empfänger der Transaktion von Kreditverbrauchern, isoliert von der Beziehung zwischen den Karteninhabern, Kreditgebern und Identitätsanbietern, wodurch ihr Betrugsrisiko vollständig eliminiert wird. Kreditanbieter übernehmen alle potenziellen Betrugsrisiken und -ausgaben, die durch ihren Anteil an den Transaktionsabwicklungsgebühren und Kreditgebühren kompensiert werden. Händler können sich jedoch an dem Prozess beteiligen, indem sie Anreize wie Transaktions-Cashback anbieten oder sogar als Kreditgeber auftreten.

Sicherheit

Wie die riesigen Datenschutzverletzungen der jüngsten Zeit im Einzelhandel und im Gastgewerbe zeigen (in Amerika), ist die Sicherheit ein sehr wichtiges Element jedes Zahlungs-Ökosystems. Das höchste Sicherheitsniveau kann erreicht werden, wenn die Sicherheit Teil des Systemdesigns ist und nicht ein Add-on, das nach der Implementierung erstellt wird. Die Sicherheit eines Zahlungssystems ist nicht nur Informationssicherheit, sondern sollte auch die finanzielle Sicherheit umfassen. Zusätzlich zu den Standard-Sicherheitsmerkmalen, die von seinen Vorgängern übernommen wurden, plant

GRAFT die Implementierung mehrerer Verbesserungen von denen sowohl Käufer als auch Händler profitieren.

Verfügbarkeit

Das verteilte Netzwerk von "always-on"-Supernodes stellt die Gesamtverfügbarkeit des Netzwerks sicher. Die Client-Apps kommunizieren mit mehreren Supernodes gleichzeitig, um den für die Autorisierung erforderlichen Konsens zu erzielen. Wenn einer der Sample-Supernodes ausgefallen ist, wird dieser automatisch durch einen anderen aus der Liste des Authorization-Samples ersetzt, welches eine praktisch unbegrenzte Anzahl an Kandidaten enthält.

Identitätsmanagement

Das Vertrauen in die Wallets zur Benutzerverwaltung birgt ein großes Sicherheitsrisiko, da Wallets in der Regel keine Einschränkungen haben eigene Sicherheitsmaßnahmen zu implementieren. Dadurch könnten diese individuell kompromittiert werden. Um das Netzwerk zu schützen und die Integrität der Benutzeridentitäten zu gewährleisten, wird GRAFT einen verteilten Identitätsanbieterdienst (eingebettet in Supernodes) implementieren, der den Wallets als OpenID Connect oAuth2 API-Aufruf zur Verfügung steht.

Unabhängig von der Wallet-Implementierung wird die Verifizierung und Authentifizierung der Benutzer durch das GRAFT-Netzwerk durchgeführt, wodurch kompromittierte Benutzeridentitäten, Spoofing, Replays und Man-in-the-Middle-Angriffe verhindert werden.

Identifizierung, Authentifizierung und Autorisierung

Die Authentifizierungs-/Autorisierungsmethoden bestehender Kryptowährungen lagen in der Zuständigkeit der Benutzeranwendung wie z.B. der Wallets und wurden weitgehend erst nachträglich berücksichtigt. Im Zusammenhang mit finanziellen Transaktionen zwischen Käufern und Verkäufern, bei denen ein gewisses Maß an Vertrauen zwischen den Parteien aufgebaut werden muss, müssen Vorschriften und Konformitäten behandelt und ein Regressanspruch geltend gemacht werden können. Deshalb ist ein gutes System zur Authentifizierung/Autorisierung entscheidend.

Identitätsprüfung

Der Identitätsnachweis ist ein anspruchsvolles Thema, da er sowohl regulatorische als auch datenschutzrechtliche Aspekte berücksichtigt. Auch ein effektiver Identitätsnachweis ist nicht trivial.

Um die Notwendigkeit des Identitätsnachweises zu verstehen, stellen Sie sich einen Händler vor, der hohe Anforderungen an den Identitätsnachweis stellt. Beispielsweise um sicherzustellen, dass der Käufer zum Kauf von verschriebenen Medikamenten berechtigt ist. Noch höhere Anforderungen an Identitätsnachweis gelten beim Kauf von Waffen (wie von NIST Special Publication 800-63A in den USA definiert). Umgekehrt können sich Käufer, die Waren von einem Ersatzteilmarkt kaufen, vor dem Kauf gestohlener Waren schützen, indem sie verlangen, dass der Händler einen Identitätsnachweis liefert.

GRAFT erwartet von den Client-Anwendungen, dass sie den Identitätsprüfungsstandards entsprechen, die für die spezifischen Gesetze der jeweiligen Rechtsordnung relevant sind. Supernodes stellen Ressourcen für die maschinenbasierte Identitätsprüfung und Betrugserkennung zur Verfügung, um Händler (und Benutzer) bei der Einhaltung der Vorschriften zu unterstützen, die Integrität des Zahlungsnetzwerks und die Sicherheit der Transaktionen zu gewährleisten. Um die Offenlegung der Benutzerdaten zu begrenzen, wenn die Weitergabe seiner vollständigen Identitätsinformationen unerwünscht oder gegen die gesetzlichen Bestimmungen (z.B. GDPR) verstößt, wird GRAFT die Beantragung und Weitergabe der Identitätsdaten - wie Alter und Adresse der Person - erleichtern, um die Einhaltung der lokalen Gesetze und Vorschriften sicherzustellen. Wir sind auch bestrebt der Datenfreigabe eine größere Metadaten-Sammlung hinzuzufügen, um zusätzliche Geschäftslogiken wie z.B. für Arzneimittel-Interaktionsprüfungen oder Treueprämien zu ermöglichen.

GRAFT ermöglicht eine optionale Mehrbenutzerkontrolle, bei der mehrere Benutzer Zugriff auf das gleiche Händlerkonto haben und eine Mehrbenutzer-Verwaltung, bei der zwei oder mehr Benutzer erforderlich sind, um einige Funktionen freizuschalten, wie z.B. die Überweisung von Geldern aus dem Konto.

Reputations-Punkte: Bring Licht in die Dunkelheit

GRAFT verfolgt bei der Transaktionsverarbeitung einen risikobasierten Ansatz. Jedem Teilnehmer im Netzwerk wird ein Reputationswert zugewiesen, der dynamisch nach den vom System erfassten neuen Daten berechnet und aktualisiert wird. Die Käufer, Händler und Supernode-Inhaber können optional ihre partielle Identität mit ihrem Konto verknüpfen, um ihre Reputationswerte offenzulegen und zu verbessern. Ein solcher Link gefährdet nicht die Rückverfolgbarkeit von Transaktionen.

Das Reputation Punktsystem hilft den Teilnehmern am Ökosystem, fundierte Entscheidungen zu treffen, ohne ihre Sicherheit und Privatsphäre zu beeinträchtigen. Ein Händler kann beispielsweise den

Reputationswert des Käufers berücksichtigen, wenn er Entscheidungen über die Autorisierungslimits vor der sofortigen Autorisierung trifft. Ebenso kann der Käufer die Reputationswerte des Händlers überprüfen, bevor er für Waren, die nicht sofort geliefert werden können, bezahlt. Sowohl Käufer als auch Händler können den Reputationswert des Netzwerk-Supernodes, mit dem sie kommunizieren, überprüfen und die Proxy-Supernodes können wiederum den Reputationswert des Exchange Brokers verwenden, um ihre Entscheidung zu treffen, diese an einer Transaktion zu beteiligen.

Ein weiteres wichtiges Element der Benutzer Reputationsbewertung wird im Zusammenhang mit Peer-to-Peer Krediten ans Licht kommen, bei der die Reputations-Punktzahl die Kreditwürdigkeitsprüfung und das Zahlungsverhalten mit einschließen kann.

Die Supernodes sind verantwortlich für die Überwachung, Berechnung, Aktualisierung und Validierung der Reputationswerte für Käufer, Händler und anderen Supernodes. Die Punktzahlen werden mit speziellen Predictive-Analytics Algorithmen berechnet, die leicht verständliche Ergebnisse auf einer Skala von 0-100 liefern, die nicht dazu verwendet werden können, Informationen über Anzahl, Betrag, Zeit oder Art der Transaktionen preiszugeben.

Kundenbetreuung, Streitbeilegung und Zahlungssicherung

Einer der Hauptvorteile der Einführung von Kryptowährungen und kryptographischen Token durch Mainstream-Verbraucher und -Händler ist das Fehlen der Autorität und der Geschäftsinhaber, die bei der Beantwortung von Fragen und der Lösung technischer und geschäftlicher Probleme helfen könnten. Außerdem ist es unmöglich eine falsche Kryptowährung oder kryptografische Token-Transaktion im Falle von menschlichem Versagen, betrügerischen Aktivitäten oder technischen Störungen zu "reparieren". All diese Probleme werden natürlich durch den dezentralen, anonymen und unabhängigen Charakter von Kryptozahlungen verursacht und begründet. Die guten Gründe helfen jedoch nicht, die Probleme zu lösen. Die Open-Source-Community löste diese Probleme durch die Einführung eines optionalen Kundensupports für kostenlose Open-Source-Produkte. Linux OS, unterstützt von Redhat, und die MySQL-Datenbank, unterstützt von Oracle, sind nur zwei erfolgreiche Beispiele für den kommerziellen Support von kostenlosen Open-Source-Produkten.

Um die Adaptierung von GRAFT-Zahlungen zu erleichtern, bietet die GRAFT Foundation den Inhabern von GRAFT-Nodes kostenlose Kundensupport- und Streitbeilegungsdienste an. Händler mit hohem Transaktionsvolumen können rund um die Uhr Echtzeit-Support und Unterstützung bei der Streitbeilegung erhalten. Die GRAFT Foundation und/oder Exchange Broker können Zahlungen bis zu

einem Gegenwert von USD 100 versichern und Kunden oder Händler für ihren Geldverlust aufgrund von Betrug oder technischen Problemen entschädigen.

Benutzer-Apps

Alle GRAFT Benutzer-Apps sind "Light"-Clients, die die Blockchain nicht speichern oder Transaktionen verarbeiten. Die Apps verwenden Remote-API-Aufrufe, um mit Always-on GRAFT-Knoten zu kommunizieren, die neue Transaktionsblöcke schürfen und Transaktionsanforderungen in Echtzeit verarbeiten.

Benutzer, die ein noch höheres Maß an Kontrolle über Ihre Privatsphäre, Anonymität und der Verfügbarkeit benötigen (z.B. große Händler oder Geheimorganisationen), können ihren eigenen Supernode oder sogar mehrere Supernodes betreiben, die ausschließlich und privat mit ihren Client-Apps kommunizieren, Nachrichten und Transaktionen an andere Supernodes weiterleiten, Offline-Berechtigungen erteilen und GRAFTs auswerten, die für den Betrieb von Kredit-, Geschenk- und Treueprogrammen erforderlich sind.

Zu den Verbraucher Apps gehören:

- Desktop- und mobile Händler Point-of-Sale Anwendungen (Apps) zur Akzeptanz von Zahlungen in GRAFT-Token, Bitcoins, Altcoins und Kredit-/Debitkarten, sowie zur Konfiguration von Auszahlungen in Bitcoins, Altcoins und lokalen Fiat-Währungen, die sowohl von Käufern als auch von Händlern verwendet werden können.
- Desktop-, Mobil- und Chrome Browser Erweiterungs Wallet-Apps für Zahlungen in GRAFT-Token, Bitcoins, Altcoins und Kredit-/Debitkarten (unter Verwendung von Instant Exchange Brokern), sowie für das Senden und Empfangen von Transfers in GRAFT-Token.
- GRAFT SDK ermöglicht die Integration mit den wichtigsten Point-of-Sale Softwareprodukten und Warenkörben für die Verarbeitung von Online und Brick-and-Mortar Transaktionen. GRAFT wird eine GRAFT-Smartcard als Zahlungsmethode integrieren. Zusätzlich zur Schlüsselaufbewahrung speichert die Karte auch biometrische Unterschriften des Benutzers und einen Satz gespeicherter oder nachschlagbarer Geheimnisse, die für die Authentifizierung am Endgerät verwendet werden können. Die GRAFT Foundation und Exchange Broker werden die Produktion von der Smartcard, sowie der entsprechenden Lesegeräte unterstützen.

Neben der Unterstützung von verbraucherorientierten Transaktionen (B2C) wird GRAFT auch B2B-Transaktionen (Business-to-Business) unterstützen und in die bestehenden Geschäftsabläufe

integrieren. Solche Abläufe können von einfachen automatisierten Inkasso nach Kreditbedingungen (z.B. Net 30, 60, 90) bis hin zu komplexen Abläufen, wie der Rechnungsbegleichung von individuellen Zahlungsaufforderungen des Absenders, sowie einzelnen Abrechnungen auf Basis von erreichten Meilensteinen und Kundenfreigaben.

GRAFT deckt auch einen guten Bereich des IoT-Raums ab, da einige der IoT-Geräte die von ihnen angebotenen Daten oder Dienste "berechnen" müssen. Ein Beispiel wäre ein Geschäft, welches einen LKW auf Basis der Lagerbestände, die von Backend-Systemen und Sensoren bestimmt werden, bestellt.

Zusammenfassung

GRAFT würde ohne seine Vorgänger nicht existieren. Es basiert auf Ideen, Prinzipien und Technologien, die von Machern anderer kryptografischer Utility-Token eingeführt und getestet wurden. Die Verwendung modernster Technologien, die von der Kryptographie-Community entwickelt wurden, sowie neu entwickelter Lösungen für die Transaktionsverarbeitung und -sicherheit werden es GRAFT ermöglichen, mit traditionellen Zahlungsmethoden und bestehenden zentralisierten Zahlungsabwicklern zu konkurrieren.

Referenzen

1. Bitcoin. https://bitcoin.org/en/.

2. Dash. https://www.dash.org/.

3. Bitpay. https://bitpay.com/.

4. GRAFT Definition. Merriam-Webster (2017). https://www.merriam-webster.com/dictionary/graft#h2.

5. What Is GRAFTing? - Definition & Methods. Study.com (2017). http://study.com/academy/lesson/what-is-grafting-definition-methods-quiz.html.

6. IOTA. https://iota.org/.

7. Bitcoin, Ethereum, Litecoin, Dash, Monero Avg. Transaction Fee historical chart. Bitinfocharts.com. https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y.

8. PayPal. https://www.paypal.com/us/webapps/mpp/merchant-fees.

9. NIST Special Publication 800-63. Revision 3. Digital Identity Guidelines. NIST (2017). https://pages.nist.gov/800-63-3/sp800-63-3.html.

10. CryptoNote. https://cryptonote.org/.

11. Top Seven Ways Your Identity Can Be Linked to Your Bitcoin Address. 99 Bitcoins. https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/

12. Median Confirmation Time. Blockchain. https://blockchain.info/charts/median-confirmation-time?timespan=30days.

13. Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures. Version 3.2 PCI Security Standards Council (2016). https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf.

14. What are Open Loop and Closed Loop Gift Cards? Shelley Hunter. GiftCards.com. https://www.giftcards.com/gcgf/open-loop-versus-closed-loop-gift-cards.