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

A Decentralized Payment Processing Blockchain Network

Slava Gomzin, Dan Itkis

Version 3

October 2018

Initial version was published in June 2017

Abstract

Global Real-Time Authorizations and Funds Transfers (GRAFT) is a global, open-sourced, blockchain-based, decentralized payment gateway and processing platform that anyone can use. Any buyer and merchant can use GRAFT in a completely decentralized and inexpensive way. The GRAFT ecosystem is open, so anyone can participate by maintaining the GRAFT blockchain and implementing network services.

GRAFT employs payment processing protocols and flows similar to how traditional electronic payment systems—such as credit, debit, and prepaid cards—are processed, which are already familiar to and trusted by millions of users and merchants around the world. This approach enables easier and faster adoption of GRAFT as a mainstream payment platform, while eliminating the need for centralized intermediaries (payment gateways and processors), currently required to facilitate transactions between buyers and merchants.

Background

Bitcoin[1] was created as "online cash"—a secure but relatively slow settlement system that was unable to replace payment cards online or compete with both plastic cards and paper cash in brick-and-mortar stores (Figure 1).

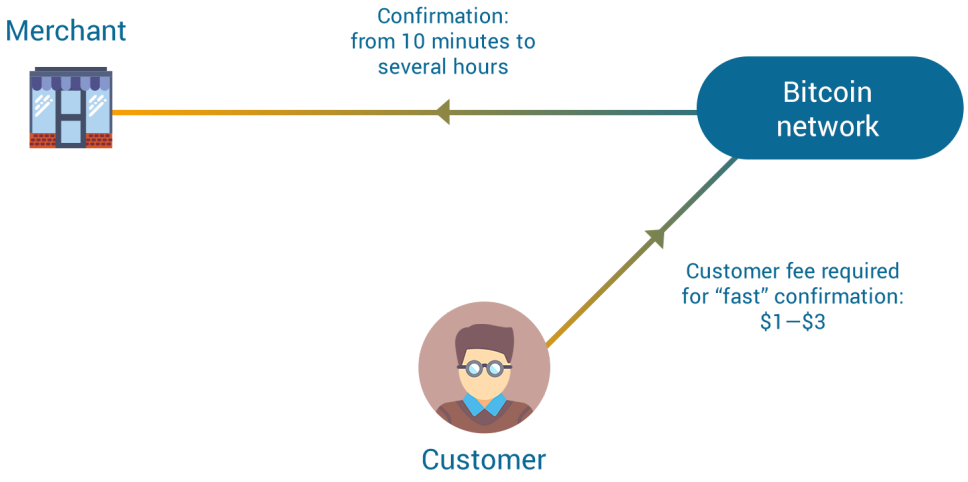

Figure 1: Bitcoin transaction processing without centralized intermediary

Even though some existing cryptocurrencies and cryptographic tokens[2] have improved confirmation times, they are still unable to process essential transactions types such as authorization and completion, which we believe makes their adoption by retail, hospitality, and convenience store industries impossible without using intermediaries—payment processors and gateways[3]—that fill the gap (Figure 2). However, as an element of cryptographic payment transaction, the very existence of payment processors—which are typically a centralized commercial organization regulated by government and controlled by shareholders—contradicts some fundamental principles of cryptocurrencies and cryptographic tokens: decentralization, privacy, and independence.

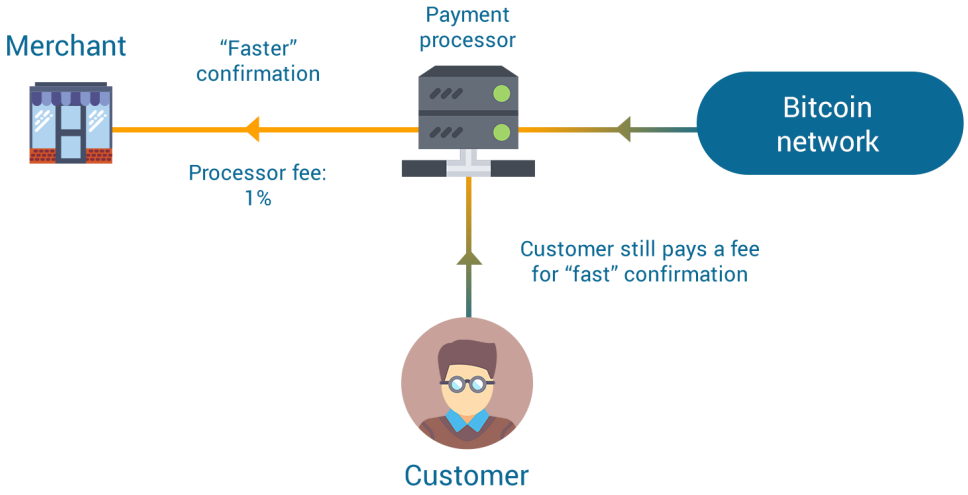

Figure 2: Processing Bitcoin transaction by centralized intermediary

Most merchants are unable to accept cryptocurrencies without utilizing a third-party payment processor due to the unique way blockchain networks process transactions. That process is conceptually different from traditional electronic payment systems. Despite some flaws in traditional electronic payment systems, technologies developed around them have accumulated enormous amounts of merchant experience and user trust.

There are several major differences between the ways traditional and cryptographic payment systems handle transactions, which in most cases make cryptographic payment systems less attractive for merchants and/or consumers. Here is a list of some of the technical limitations and business flaws of the existing cryptographic payment systems compared to traditional electronic payments systems:

- Lack of essential transaction types
- Unsuitable payment flows
- Long confirmation times
- Unbalanced and unpredictable transaction fees
- Inability to process micropayments and repeating charges (subscriptions)
- Lack of offline transactions support
- Low scalability
- Volatility
- Incomplete security
- Lack of privacy due to traceability of blockchain
- Lack of trust between buyer and merchant
- Questionable utility
- Poor usability of end-user interfaces
- Lack of customer support

By attempting to address those issues, GRAFT's goal is to create a platform that finally allows for cryptographic payments to be widely accepted by mainstream merchants and consumers for the first time while respecting some of the fundamental principles of cryptocurrencies and cryptographic tokens.

The Value of Decentralized Payment Processing

Why would a buyer want to start using cryptocurrencies or cryptographic tokens instead of (or in addition to) plastic cards or PayPal or Apple Pay, and why would a merchant choose to accept cryptocurrencies or cryptographic tokens in addition to (or instead of) existing payment methods? Obviously, if we don't have the answers to those simple questions, there is no point in creating this document.

While the answer to the first part of this question may consist of several elements—as there might be multiple reasons (and combinations of them) for individuals to keep their money in a form of cryptocurrency or cryptographic token—the answer to the second part of this question is relatively simple. Merchants want to extend their customer base in order to increase their revenues, and if they identify a significant group of potential customers who prefer, for any reason, to use cryptocurrencies or cryptographic tokens, then they will start accepting cryptocurrencies or cryptographic tokens. And GRAFT provides a unique opportunity for merchants to accept cryptocurrency or cryptographic token payments directly from their customers and with extremely low fees.

Since GRAFT is a decentralized payment processor, the function of which is being driven by digital utility tokens, it is able to facilitate the full payment cycle without external cryptocurrencies, cryptographic tokens, or assets involved. However, GRAFT will also support Bitcoin and several major cryptocurrencies, as well as cryptographic tokens, as an additional choice for buyers and an acceptable method of payment for merchants. This feature will eliminate the need for merchants to integrate with multiple (centralized) payment software providers, as well as eliminate the need for users to sign up for centralized services and learn and maintain multiple wallet apps.

Terminology

Authorization Sample

Selected group of full supernodes that approve payments in real time and guarantee that the buyer cannot spend the same funds more than once before the transaction is written into the blockchain.

DAPI

Decentralized stateless API implemented by supernodes in order to support lightweight client apps such as the GRAFT Wallet, GRAFT Point of Sale, and third-party point-of-sale apps and shopping cards. GRAFT SDK source code provided to third-party point-of-sale and wallet application vendors for facilitating an integration with GRAFT.

Exchange Broker

A GRAFT protocol extension hosted on a supernode or a group of supernodes and hosted by the supernode operator. Exchange brokers implement special additional features that cannot be automatically executed by a fully decentralized network and/or require special regulation framework. Examples of exchange brokers are bitcoin payment acceptance broker and a fiat payout broker.

Full Supernode

An independent, always-on server running the combined implementation of the GRAFT blockchain node and GRAFT DAPI node; processing real-time authorizations; exchanging DAPI calls between

buyers, exchange brokers, and merchants; and hosting third-party services such as instant cryptocurrency exchange within the GRAFT network, credit/debit card acceptance, and merchant payouts. The supernodes collectively maintain the second layer of GRAFT network using POS (Proof of Stake) algorithm.

GRAFT

1. Global Real-time Authorizations and Funds Transfers, which is a decentralized global open platform for processing real-time authorizations and settlements of merchant payments and fund transfers using untraceable blockchain, decentralized API, and an open community of exchange brokers that support a variety of payment and payout methods, including cryptocurrencies, cryptographic tokens, and traditional credit cards and bank transfers.

2. A plant that has a twig or bud from another plant attached to it so they are joined and grow together.[4] Grafting is an advanced technique that botanists, farmers, gardeners, and hobbyists use to add living tissue from one plant to another.[5] This technique allows for the best traits of different plants to come together to create something better and more valuable than their original parts.

GRAFT Point of Sale

“Lite” desktop and mobile apps that allow merchants to accept payments in GRAFT tokens, Bitcoins, altcoins, or credit/debit cards; issuing and redeeming gift certificates, loyalty reward points, and store credits; configure settlement payouts in GRAFT tokens, Bitcoins, altcoins, or local fiat currencies.

GRAFT Wallet

“Lite" desktop, mobile, and browser extension apps that allow making payments and fund transfers using GRAFT tokens, other major cryptocurrencies, cryptographic tokens, or credit/debit cards by calling GRAFT DAPI.

GRFT

Native cryptographic token supported by the GRAFT blockchain and used for real-time payment authorizations, transfers of funds, and settlements between buyers and merchants.

Merchant Token

Predefined smart contract that allows the merchant to create a private token that belongs to its owner. Merchant tokens allow implementation of important functions such as merchant payout token ("stablecoin") and proprietary closed-loop systems for merchants' loyalty reward points, gift certificates, store credits, and discount coupons.

Payment Gateway

Allows merchants or/and merchant service providers to manage their hardware payment terminals' configuration (such as wallet address) and set up the service provider–specific fees; provides additional transaction reporting and analytics.

Payout ("Stable Value") Token

Represents a local fiat currency and can be transacted on GRAFT blockchain in real time using the supernode tier of the blockchain. Payout token is based on GRAFT merchant token technology, similar to gift, rewards, and other merchant token types.

Proxy Supernode

The supernode that facilitates the merchant transaction by communicating with the merchant's point of sale (POS) and/or the buyer's wallet on one side, and the rest of the authorization sample supernodes on the other side.

VChain

Virtual decentralized independent "merchant account" where merchants can create merchant tokens and set up authorization and payout rules and triggers that will have an affect on transactions for that specific merchant.

Transaction Fees

Why is it necessary to have a transaction fee in the first place? After all, there is no commercial enterprise behind the blockchain, so why would users need to pay fees, who collects them, and how much should the collector charge?

To Fee or Not to Fee

Multiple powerful nodes (servers) distributed throughout the world are required in order to support secure and highly available cryptocurrency and cryptographic token networks. So who is going to maintain these servers, and what's the motivation and incentive for maintaining the blockchain node? In Bitcoin, other cryptocurrency networks, and cryptographic token networks, the funding is achieved through mining and transaction fees—the node owners make money on mining new tokens from each block, as well as getting fees for each transaction.

The mining has another purpose: constant and steady injection of new tokens into the system to keep up the liquidity with the growing demand for extra tokens as adoption widens and usage increases. As the system gets traction, the node operators will receive more revenue from transaction fees, so the bonus for mining can be gradually reduced with each new block to limit the overall supply.

In ideal world, cryptocurrencies or cryptographic tokens would be available for everyone and free of charge. In fact, there are networks that promise free transactions.[6] In other networks, including Bitcoin, the fees are used to prioritize transactions and “resolve” the scalability problem.

In the GRAFT network, however, the fee is used for two reasons. The first is to avoid network abuse and associated performance and blockchain size issues—for example, using the real network for testing. If a transaction is completely free, one can move the same amount between two accounts indefinitely. The second reason is to become the only incentive for node operators once the mining bonus becomes too small.

Charging the Wrong Guy

The problem with Bitcoin’s fees and cryptographic tokens’ fees is that they charge the wrong side of the transaction. It’s even worse than traditional card payments because, unlike plastic card payments, both the buyer and merchant pay fees for a cryptocurrency or cryptographic token transaction: the buyer pays to the cryptocurrency or cryptographic token network, while the merchant pays to the payment processor. The average payer is often confused by the process, which looks more like gambling and does not provide a clear explanation of the fee schedule, which does not make cryptocurrency or cryptographic token payments very attractive.

Micropayments: How Do I Pay with Crypto for a Cup of Coffee?

Another problem currently experienced by Bitcoin is its inability to handle micropayments due to high transaction fees.[7] GRAFT resolves this problem by introducing a unique approach to transaction fees.

GRAFT Transaction Fees

In GRAFT's ecosystem, **the payer does not pay fees.** All fees are borne by the receiver (merchant or payee). GRAFT makes micropayments accessible by setting very low fees (as compared to credit cards and online payment processors, cryptocurrencies, and other cryptographic tokens).[8]

Table 1: GRAFT Transaction Fees/Rewards Structure

		1	2	3
		Regular P2P Transfer	**RTA Tx (GRFT)**	**RTA Tx with altcoin exchange broker (i.e., bitcoin acceptance)**
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**	Variable, based on Tx size in KB	Configurable *** Min: 0.1 GRFT	Configurable *** Min: 0.1 GRFT
e	**Merchant POS/Recipient Gateway Proxy Supernode Reward ******	N/A	0.05% ****	0.05% ****
	Total Fee Amount paid by the Tx sender (buyer in RTA)	a1 + d1	0	0 *****
	Total fee amount paid by the Tx recipient (merchant in RTA)	0	a2 + b2*8 + d2 + e2	a3 + b3*8 + c3 + d3 + e3

	Total amount charged to the Tx sender	Tx amt + a1 + d1	Tx amt	Tx amt
	Total funds available to the Tx recipient	Tx amt	Tx amt – (a2 + b2*8 + d2 + e2)	Tx amt – (a3 + b3*8 + c3 + d3 + e3)

* wallet proxy supernode can be a proprietary server or a public cluster hosted by a service provider. You can run and use your own proprietary proxy supernode to avoid the proxy fee altogether. The supernode must have a stake in order to be able to charge the fee.

** stake is required for full supernode or exchange broker in order to participate in RTA Tx processing and receive this reward

*** set by the merchant service provider or the owner of the POS proxy supernode

**** POS proxy supernode can be a proprietary standalone server, a part of the merchant infrastructure, or a part of a payment terminal and/or ecommerce gateway maintained by the merchant service provider. POS supernode must have a stake in order to be able to receive this reward

***** does not include the altcoin network fee

Proxy supernode rewards (a1, a2, a3, e2, and e3 in Table 1) will enable full decentralization of the network infrastructure. If you don't like the proxy supernode cluster hosted by a particular service provider, there will be alternative providers ready to serve your wallet or POS. To receive the reward, the proxy supernode must demonstrate the unique stake wallet linked to the supernode public IP address. The amount of proxy stake is 250,000 GRFT.

Unlike an authorization sample supernode, the proxy supernode will still be operational without the stake, however an unstaked proxy supernode won't be able to charge the fee. This option is reserved for proprietary proxy supernodes, so the users with elevated privacy needs can host their own entry points to the network. Without the stake, the proxy reward will be sent to the GRAFT community donation wallet address. This way the total transaction fee, which is assembled from several components, always remains consistent regardless of the status of the proxy supernodes.

The flat fee is paid to the miner for RTA transaction settlements (d2, d3). The miner's fee is traditionally calculated based on transaction record size in KB (d1). With RTAs, we cannot make the

miner fee variable as it would make the total fee paid by the merchant inconsistent and unpredictable, which is unacceptable in most situations. Additionally, we cannot make this fee proportional to the value of the transaction (similar to the supernode fees) because miner fees are visible on the blockchain, meaning the transaction amount could be calculated from a proportional fee (although we may fix this in the future). Therefore, we made it a simple configurable flat fee, with a minimum amount of 0.1 GRFT.

The fees associated with RTA transactions with exchange brokers are the same as RTA fees (column 2) with an extra 0.25% taken by the broker (and paid also by the merchant).

Merchant Fees and Service Providers

The merchant service providers can set a fee schedule that's consistent with their business model, and fees could be structured in tiers with options, for example:

Transactions below $10: 2%
Transactions above $10: 1%
Min transaction amount: $1
Miner: 0.1 GRFT
Transactions in altcoins: +0.25%
Instant payouts in altcoin or fiat: +0.25%

Following is an example of a $20 altcoin transaction and the associated fees given a reference Merchant Service Provider fee schedule.

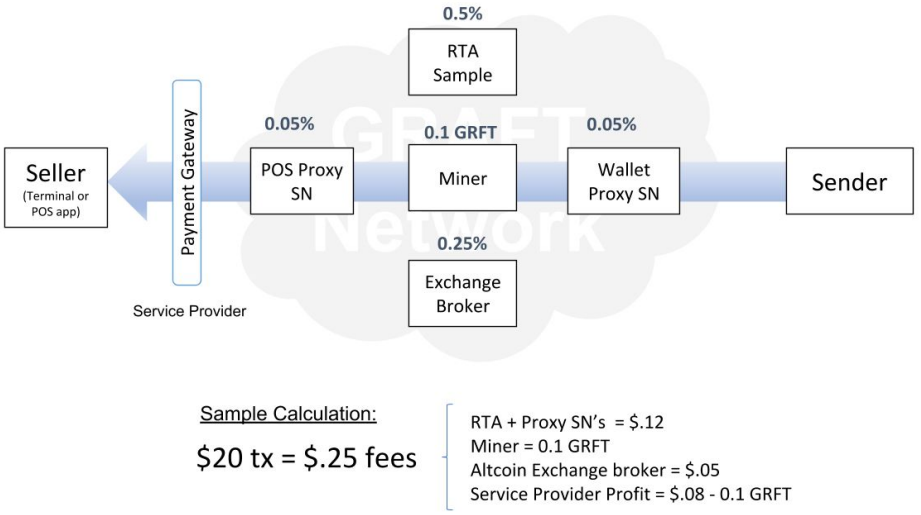

Figure 3: Example of GRAFT Transaction Fees/Rewards Distribution

Free Fund Transfers: Authenticated Transactions

Some payment networks, such as Automated Clearing House (ACH) or PayPal, provide free transfers between user accounts. In order to be able to compete with traditional payment networks, GRAFT will provide limited free transfers between authenticated user wallets.

Cryptocurrency networks usually cannot "afford" free transactions for three major reasons:

- Lack of incentive for miners
- Threat of distributed denial-of-service (DDoS) attacks
- Uncontrolled growth of blockchain

GRAFT resolves the first problem—lack of incentive for miners—by separating payments and transfers, so supernodes (miners) receive transaction fees for instant payments, which constitute the majority of all transactions, while free transfers are processed with lower priority.

The second problem—DDoS attacks—is resolved by voluntary user identification and authentication. Of course, there are no "free lunches," so the users will "pay" by providing their identity to the network to ensure the reasonable use (by limiting the number and frequency of free transfers per user) and thus prevent network abuse. Using zero-knowledge proof-authentication technology will allow users to prove their identity without compromising their privacy.

The last problem—uncontrolled block size growth—is addressed through several solutions, including small block intervals, unlimited block size, and standard restricted transaction size for particular transaction types, such as free transfers. In addition, one of the sides of the free transfer transaction

must be verified by showing proof of having conducted “commercial” payment transaction types in the past.

Privacy

Oftentimes, there is a misperception of the need for privacy. In reality, a majority of legitimate buyers don’t mind disclosing their identity to the merchant, especially, if they benefit from such disclosure, or if such disclosure is necessary to process a transaction. Similarly, buyers want to make sure that the merchant they send payment to is the intended recipient, and not an impersonator. What neither merchant nor buyer want is anyone else’s ability to recognize their identities and see all the details of their transactions by scanning the publicly accessible blockchain.

Privacy is a delicate subject for cryptocurrencies and the payment industry in general. Privacy demands a range from complete anonymity to complete transparency, as decided by both the seller and the buyer. The seller for example may have regulatory compliance requirements to collect and verify certain identity data, such as age for liquor or cigarette purchases, or zip codes for online merchant’s tax calculations. The buyer, on the other hand, may or may not agree to disclose all or some of the attributes of their identity and should be in a position to do so. If the seller and the buyer can agree on the identity attributes to be shared, the transaction can proceed. Furthermore, there’s a requirement to establish an identity attribute’s authenticity by the merchant in lots of cases.

We find that the best way to approach this problem is by using a system of identity verification and identity-attribute sharing that is consistent with digital identity guidelines set out by government regulators focused on privacy enhancement (i.e., NIST 800-63 in the US or GDPR in EU)— standards that calls for differentiated identity proofing and authentication.[9]

GRAFT will implement a digital identity profile, which is attached to GRAFT Wallet, with ability to share the data from the digital identity with the counterparty incrementally and based on user permissions at the time of the transaction. These permissions include sharing certain attributes (such as age, home location, address, and name) selectively and per transaction.

GRAFT implements **CryptoNote[10]** as an underlying transaction recording protocol, which provides a high degree of privacy when compared to Bitcoin, other cryptocurrencies, and cryptographic tokens, by hiding information about the sender and receiver.

Why Private Blockchain is Necessary

The key innovation of Bitcoin is the open ledger that is accessible to every node participating in the network because the transaction must be verified to make sure there is no double-spending. But this also means that anyone in the world can see the transaction and the balances on the corresponding wallets. Unlike plastic cards, Bitcoin wallets are, in principle, anonymous because transaction records are not directly linked to the owner's identity. At first glance, this feature appears to compensate for the fact that the transaction records are in plain sight on the blockchain for anyone to see. However, there are existing techniques that allow observers to link addresses to identities.[11] Once this happens, all of your transactions become visible forever because the blockchain is always there and it cannot be erased.

CryptoNote is absolutely required in order to be competitive with traditional payment systems such as the Visa network or PayPal, who in fact provide much better privacy to their customers than most existing cryptocurrencies.

When you swipe or insert your payment card at the point of sale terminal or click PayPal's Pay button online, there are two entities in the world that are aware of your transaction: the payment network (Visa or PayPal in our case) and the merchant. In reality, of course, there are more organizations that "know" about your transaction because the payment network is more complex. This list includes, at the very least, the issuing bank (the one that gave you the payment card), the acquiring bank (the one that approves the payment), the payment gateway (the one that routes your transaction to the right payment processor/acquiring bank), and the payment processor (which processes the payment and merchant's payout). The list of organizations, however, is still limited because they are under security and privacy regulations, and they have typically implemented some decent security controls that protect your transaction records from prying eyes. Of course, everyone in this list can be hacked or can give away your info to a law enforcement agency. For the sake of simplicity though, let's assume that random people cannot gain access to your payment card transactions in most situations, which is not the case with most blockchains.

CryptoNote as a Foundation for Privacy

CryptoNote stands out from all other blockchain protocols because it provides something we all need: privacy. We often take privacy for granted and only regret when we lose it. Ironically, Bitcoin and its derivatives take a step backward in the privacy area compared to older payment technologies such as cash or even plastic cards, which became an inglorious symbol of compromised security and privacy.

Bitcoin creator(s) either did not think about privacy, or simply did not have enough time to resolve all the problems, which is absolutely understandable as they had an even more important problem to solve: the very existence of blockchain technology.

CryptoNote keeps all the benefits of blockchain technologies, which are well known, while "returning" the lost privacy features: **untraceable payments, unlinkable transactions, blockchain analysis resistance,** and **confidential transaction amounts**. On top of that, GRAFT adds **confidential transaction fee** amounts to complete the picture. CryptoNote creates a perfect solid foundation for building a variety of industry-related features, which GRAFT brings to light in order to conquer the world of payments.

Private Transactions

GRAFT uses several cryptographic mechanisms designed by CryptoNote and Monero in order to obfuscate transaction records and make it visible only to data owners:

One-Time Destination "Stealth" Addresses

Instead of sending the payment to the recipient address directly, a unique one-time destination key is created for each transaction. This key is cryptographically derived from the public recipient address in a way that prevents the key from being linked to the address or to other keys. Therefore, **the recipient can publish a single address and receive unlinkable payments,** and **no observer can determine if any transactions were sent to a specific address** or link two addresses together.

One-Time Ring Signatures

These signatures **obfuscate the identity of the sender**. Each transaction on any blockchain is signed by the private key of the sender, so the network can confirm that the transaction is genuine. Instead of creating a single signature, multiple signatures (the "ring") are created, and all of them are valid as they are representing the actual outputs from other senders. The observer, however, cannot tell who the actual sender is. The network doesn't know which particular output is used as its hidden among other signatures in the ring signature. Instead, the network checks that no output from the entire ring is spent more than once, which effectively prevents double-spending.

Ring Confidential Transactions

These **make transaction amounts invisible on blockchain.** The transaction amount is encrypted by the sender. Only the recipient of the payment is able to decode the actual amount. Third-party observers are notable to decrypt that amount, but they can verify that the money has not been spent more than once and that no “new money” has been created in this transaction.

Transaction Processing

The world’s moving towards “thin” devices. People around the world use more smartphones and tablets and less workstations and laptops. Therefore, we believe that a superior model for decentralized cryptographic payment systems will rely solely on small, individual nodes hosted on personal computers and will be based on dedicated powerful supernodes hosted by professionals, with thin-client apps connected to a authorization sample—a group of supernodes randomly selected by special fraud-prevention algorithm—via DAPI calls.

Confirmation Time Problem: Introducing Real-Time Authorizations

Long confirmation times[12] (from several minutes to several hours, depending on the transaction fee) is one of the main reasons for low adoption of cryptocurrencies and cryptographic tokens in retail and hospitality sectors. Customers dislike long wait times and, as a result, merchants demand almost-instant payment processing. Unlike some other cryptocurrency networks that tried to resolve this problem by introducing special add-on systems or transaction types, GRAFT will process all payment transactions in “real time” (we expect most transactions to be completed in less than 3 seconds). Critically, GRAFT achieves this real-time payment without charging the customer an extra fee.

This is achieved by using a consensus of always-on supernodes ("authorization sample") with the ability to perform a distributed instant authorization lock on a buyer's account and communicate a response back to the client, typically within milliseconds. The supernodes also monitor the GRAFT blockchain so no transactions can be authorized “off chain.”

Supernodes

All transactions are processed by the network of always-on GRAFT network nodes—supernodes—in real time. Transaction fees are paid by the receiver (merchant) to the supernodes participating in the authorization sample and (optional) exchange brokers participating in transaction processing. The owners of the supernodes are responsible for any transactions they process. Such responsibility is achieved by financial interest (transaction fees).

DAPI

Unlike regular APIs, which are hosted on a server or in a server farm, DAPI does not have a single address, as it is running on multiple supernodes. Any single node can serve the DAPI call anytime. The DAPI calls are stateless, which means that the supernodes do not maintain any permanent session with the client, and all the data necessary for processing is instantly distributed and available on all the nodes. The client app, which consumes DAPI, maintains a list of proxy supernodes it communicates with. However, the client app is free to select a particular trusted supernode and "stick" with it. For example, merchant point-of-sale or wallet users can decide to host their own proxy supernode that they trust. Although such a "private" supernode may not be granted a right to participate in the authorization sample due to resource limitations (see Authorization Sample Selection Algorithm section below), it can provide an extra layer of privacy to their owners.

Real-Time Approvals by an Authorization Sample

There are cryptocurrencies with block (settlement) intervals of less than 2 minutes. However, reducing that interval still does not make those transactions "real-time." The GRAFT supernode scheme resolves this problem by utilizing authorization samples when approvals are issued in real time by the selected group of supernodes. We believe this structure guarantees that the buyer cannot spend the same money more than once until the transaction is settled (written into the blockchain). The settlement (mining) is performed typically within several minutes.

Unlike most cryptographic payment systems, and similar to traditional electronic payment systems, each payment made on the GRAFT network is divided into two phases: authorization and settlement. Like in the traditional payment world, authorization happens in real time, while settlement is performed later on, usually within two minutes (compared to several hours and even days in traditional payment networks).

Authorization Account Lock

A "key image" is the mechanism used by CryptoNote to validate new transactions and prevent double spending without compromising the privacy of the sender. A key image is a unique "fingerprint" that represents the buyer's spending address and amount without disclosing any details about the buyer or the amount. The nature of a key image is that it can be used only once, so if someone is trying to use the same key image more than once, this is the sign of a double-spending attempt. By providing the unique key image for upcomings transaction to the network of supernodes, the buyer's wallet temporarily locks its spending account, so no other transaction with the same key image (i.e., from the same account) can happen until the locked transaction is settled or the lock is removed. If the buyer

tries to finalize the transaction with a key image different from the one used in the original lock, the transaction will also be rejected by the supernodes.

On the other hand, a key image does not contain any information about the buyer or buyer's wallet, which provides security, anonymity, and untraceability. In addition, any traces of communication between the buyer (wallet app), the merchant (point-of-sale app), and the supernodes (selected relay and sample supernodes) during the authorization phase are removed once the transaction is settled (written into the blockchain and confirmed by 10 blocks).

Supernode Levels

A GRAFT node is called "supernode" because it performs more functions than traditional blockchain network nodes. There are increased requirements for supernode owners. While GRAFT is an open and decentralized network that allows anyone to run a supernode, there are different levels of supernodes with different conditions and rewards associated with each level.

Proxy Supernode is the "entry level"—anyone can install the supernode software and host the proxy supernode. Proxy supernode provides the following services:

- as a trusted relay for those who have the highest privacy requirements, so they can host their own "wallet server";
- for large merchants as a "store server" for even faster and more reliable transaction processing.
- As a public "exit node" connecting mobile wallets and points of sales to the GRAFT network (public IP is required). The public proxy supernode can earn rewards if it has a stake.

Full Supernode is both an authorizer and service provider. In addition, performance of full supernode functions requires a stake—collateral balance associated with the supernode address. Transaction and service fees are paid to a full supernode which has a stake and issues real-time approvals.

Mining Nodes

While the second layer of GRAFT network, which consists of POS supernodes, performs the authorization and interchange functions, the first layer, which consists of Proof of Work (PoW) network nodes, performs the settlement function by generating new blocks and adding them to the blockchain.

Settlement (Mining) Rewards

Mining nodes earn PoW block mining rewards and also receive “settlement” transaction fees for both regular transfers and RTA transactions.

Settlement Reward (RTA Tx): variable

Determined by the merchant service provider through the payment gateway, but not lower than 0.1 GRFT.

Miner Transaction Fee (non-RTA transfer): variable

Variable, based on Tx size in KB

Mining (Coinbase) Block Reward

The block mining reward is paid to the mining node that solves the new block. The block reward is gradually reduced with each new block using the following formula: $(M - A) * 2^{-19} * 10^{-10} / 2$, where A = current circulation and M = total supply $(2^{64} - 1)$ in atomic units (10^{-10}). The idea behind this is that in the future there will be more transactions, which will ensure the sustainable income for miners from transaction fees.

Full Supernode Tiers

GRAFT implements a four-tier stake model where a higher tier has a greater chance to be selected into authorization sample, while the selection process is still random.

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

Each tier participates in a random selection of 2 sample supernodes (where N is the tier number). Thus, naturally, a tier 4 supernode has more chances to be selected due to the limited number of tier 4 supernodes. “Empty” spots are filled by the higher-level tiers (or lower in absence of higher). This algorithm is also adaptive as it will “regulate” the average number of full supernodes on each level.

Delegated Stake

Balances from multiple wallets can be “delegated” to a single full supernode in order to form a stake significant enough to run a full supernode. The earnings are distributed between the wallets according to their stake share. The minimum balance for a delegated stake is 5,000 GRFT.

Authorization Sample

In order to perform real-time authorizations, the GRAFT network relies on the authorization sample: a group of selected trusted supernodes that will “represent” the network and validate transactions, preventing double spending, and signing the instant approval before a transaction is “confirmed” on the GRAFT blockchain (i.e., before it’s added to the block and the block is added to the blockchain).

The authorization sample consists of eight supernodes randomly selected from a dynamic list of supernodes. The selection is random while the result is deterministic for anyone who calculates the formula. The supernode owner must maintain a collateral balance in a wallet associated with the supernode. The minimum required balance starts at 50,000 GRFT.

When a new transaction request is initiated by the merchant’s point of sale, it is assigned the current block height that defines the authorization sample. The height can be incremented while the transaction is still in progress, but it does not change the sample height that was initially assigned to the transaction request. The merchant’s proxy supernode that initially formats the transaction request selects the sample supernodes, but this selection is validated by each member of the sample plus the wallet’s proxy.

In order to speed up the authorization process, the merchant’s point of sale app can instruct the authorization sample supernodes to ignore the responses from the rest of the authorization sample as soon as it receives more than 50 percent of the approved responses from the “fastest” supernodes and zero rejected responses.

Proxy Supernodes

Any supernode from the authorization sample can be also a proxy supernode—the relay that facilitates the merchant’s transaction by communicating with the merchant’s point of sale and/or the buyer’s wallet on one side, and the rest of the authorization sample supernodes on the other side. The proxy supernode can be selected randomly by the point of sale or wallet from the current authorization sample linked to the transaction. The point of sale or wallet can also select any supernode that is not

a part of the authorization sample. In fact, a point of sale or wallet can host its own proxy supernodes if it is seeking an extra layer of security and privacy. The proxy supernode can earn transaction processing rewards if it has a stake.

Supernode Rewards

Each supernode receives a share of the transaction fee for each transaction it processes. The rewards are paid by the recipient (merchant).

Full Supernode RTA Reward (any RTA Tx): 0.5%

One-eighth of this fee, or 0.0625% of the total RTA Tx amount, goes to each full supernode participating in the RTA authorization sample.

Proxy Supernodes Reward (any RTA Tx): 0.1%

Half of this fee, or 0.05% of the total RTA Tx amount, goes to each supernode in the proxy pair that provides connectivity into the network (wallet and POS proxy supernodes).

Wallet Proxy Supernode Reward (non-RTA transfer): 0.1 GRFT

This fee is going to be charged by the wallet proxy supernode to the mobile or desktop sender's wallet in addition to the existing network fee (miner's reward).

Scalability

The scalability of a given payment network is the ability to process a large number of transactions simultaneously without degradation of performance. Some of the measures that the GRAFT network uses to achieve higher scalability are setting the block creation interval to two minutes and removing the size limit of the block so that transactions blocks are created more often, and each block can accommodate more transactions. Such measures are not unique and are similarly implemented by other cryptocurrencies and cryptographic tokens. GRAFT, however, is maintained by always-on high performance supernodes that validate and authorize transactions in real time. Therefore, each supernode not only has a most recent copy of the full blockchain but also keeps a list of all pending authorization requests and completed transactions until they are added to the blockchain. Such two-layer architecture allows for the absorbing of large spikes of associated requests (for example, seasonal, events driven, and other changes in buyers and merchants activities).

Offline Transaction Approvals

People familiar with payment-card processing know that sometimes transaction can be approved by a merchant without getting simultaneous approval from the bank. This is called offline or local approval, or offline authorization, or sometimes S&F ("store and forward") as such offline authorization is forwarded to the server once the network is back online.

Cryptographic payments, however, generally assume that the network is available 24/7, and there are no downtimes. However, this assumption is not always true. In some situations, merchants take a risk and approve transactions locally because the risk of a single chargeback is lower than the risk of losing multiple customers. Usually, there is a total limit amount for local authorization. After the system reaches this limit (the maximum risk), it stops issuing local approvals until the network is up again. But in case of a short downtime, local authorization can go unnoticed by both cashiers and buyers.

The GRAFT merchant point-of-sale app and single proxy supernode will be able to process offline cryptographic transactions based on the same principle, if they cannot communicate to the authorization sample and get consensus, and if the merchant is ready to assume such a risk. The decision about offline approval will also be based on the buyer's and supernode's reputation scores.

Payment Gateways for Merchants and Service Providers

One of the important profiles in the GRAFT ecosystem is a Merchant Service Provider (MSP). An MSP's role is to provide and support payment network services to the merchant, ensure the uptime of the network (usually referred to as a Service Level agreement or SLA), provide and manage equipment (e.g., payment terminals), and provide reporting.
To enable an MSP to do this, another type of server is needed, one that would:

- Manage the terminal's configuration (including wallet address)
- Handle the MSP-specific fee economics for the MSP (an MSP could choose to handle tiers of service differently or charge different fees for different transaction amounts)
- Maintain transaction reporting and analytics for merchants

Such a payment gateway can be designed and implemented by a third party such as a traditional

payment processor that wants to add cryptocurrency payments to their portfolio of services. GRAFT creates a “reference implementation” to enable a faster adoption rate as a part of a go-to market strategy.

Since GRAFT is a decentralized payment network, the payment gateway is a multi-tenant, multi-instance, open-source app, and everyone can host their own payment gateway and become a service provider on the network. The payment gateway is this “fifth element” that is supposed to manage the GRAFT payment apps on hardware payment terminals and GRAFT ecommerce interfaces, and link them with the GRAFT supernodes. Since it has transaction visibility, it is considered part of the merchant’s “back office” applications.

Transaction Types and Payment Flows

GRAFT introduces the following transaction types and flows in order to facilitate merchant transactions and support existing payment and point-of-sale applications.

Authorize

Authorize is used when the exact final amount of a transaction is unknown at the time of the sale initiation. Examples are paying at the pump at a gas station, car rental check-in, hotel room reservation/check-in, or paying at the table at a restaurant.

This is analogous to debit card authorization. An authorize transaction type is initiated by the merchant and confirmed by the payer. The payer’s account is temporarily locked for the amount and duration (number of blocks) requested by the payee and confirmed by the payer, or until the amount is confirmed by a subsequent “Complete” transaction. The authorization lock can also be released by a “Cancel” transaction issued by the payee before the expiration date/time. The funds are automatically released back to the payer by the network after the expiration date/time if the payee did not claim them by sending a “Complete” transaction.

PreAuth

This is similar to the long-term Authorize but the difference is that the payer does not guarantee that the funds will be available at the time of completion. PreAuth is a long-term contract between the payer and the payee. However, unlike Authorize, which cannot be cancelled by the payee, PreAuth can be cancelled at any time by moving funds from the account associated with the preauthorized transaction.

PreAuth is suitable for long-term payment arrangements such as a monthly service subscription or daily hotel room billing. The payee specifies (and the payer confirms) the maximum amount of a single charge, the total number of charges, and the minimum interval between the charges.

Complete

Complete finalizes the payment initiated by Authorize or PreAuth transactions. The actual amount of Complete can be less than the previously authorized amount; there might be multiple Completions but the total amount will not exceed the amount of Authorize.

Complete is used after a previously authorized transaction is finalized and the exact amount is known—for example, paying at the pump after the fueling is complete, car rental check-out, hotel check-out, or restaurant payment with tips added.

Sale

Sale is Authorize/Complete processed sequentially and automatically by the network as a single transaction. Sale is a typical merchant transaction in an online or brick-and-mortar store.

Transfer

Transfer is used to transfer money between GRAFT accounts. It is the same as Sale but is initiated by the sender without receiver consent. It can be used for peer-to-peer payments, exchanges, and transfers between different accounts.

Cancel

Cancel is used to cancel Authorize and releases the authorized funds (removes the account lock).

Issue

Issue activates a GRAFT prepaid card, gift certificate, loyalty points, store credit, or discount coupon.

Redeem

Redeem allows payment using a prepaid card, gift certificate, loyalty points, store credit, or discount coupon previously issued by GRAFT.

Exchange

Exchange is used to exchange funds between GRAFT tokens and other major cryptocurrencies, cryptographic tokens, and local fiat currencies using the best offer from supernodes.

Schedule

Schedule is used to schedule a transaction to occur at a later time/date. It requires additional acknowledgement from the user.

Escrow

Escrow is used to escrow the funds, attaching an event trigger for when the funds will be released.

Refund

A Refund transaction returns the funds referenced by the transaction pointer. It requires return merchandise authorization (RMA) authorization from the seller.

Processing Transactions with GRFT Tokens as a Payment Method

Unlike Bitcoin, other cryptocurrencies, and cryptographic tokens, and similar to payment cards, payment transaction requests are formatted and issued by the recipient (merchant), with only an exception for Transfer and Exchange, which are initiated by the sender (i.e., anyone who wants to move funds between GRAFT accounts). Unlike credit and debit cards, however, payment requests are explicitly confirmed by the buyer who is prompted by the GRAFT Wallet app before it digitally signs the transaction and sends it to the network. The only exception is the Redeem function when using a paper or plastic gift certificate or coupon that can be scanned by the merchant payment app if the customer does not want to use the mobile app or does not have a GRAFT account at all.

Processing Transactions with Alternative Payment Methods

In order to provide the best user experience for buyers and better conversion rates to merchants, a GRAFT payment transaction can take various convertible cryptocurrencies, cryptographic tokens, or local fiat currencies in the form of a credit/debit card as input through the buyer's GRAFT Wallet app. Exchange fees, bank fees, and credit/debit card processing fees (charged from the merchant in graftcoins) may be applied accordingly in addition to standard GRAFT transaction fees. We expect those fees will be borne by the payee, and will invisible for the payer as the method of payment will not affect the sale price. GRAFT's automatic instant conversion will help adopt crypto payments by

mainstream users who are not familiar enough with cryptocurrency and cryptographic token ecosystems and still feel more comfortable with traditional methods of payment, but seek better security, privacy, and full anonymity for their transactions.

If a buyer decides to pay with an alternative cryptocurrency, cryptographic tokens, or a credit/debit card, the GRAFT network will automatically exchange other cryptocurrency, cryptographic tokens, or convert credit card payment in local fiat currency into GRFT in real time as a part of the transaction process, using exchange brokers. The exchange brokers, running on GRAFT supernodes, are responsible for executing the exchange deals, charging the buyers, and executing payouts to merchants. If the buyer chooses an alternative cryptocurrency, cryptographic tokens, or a credit/debit card as a method of payment, the supernode sample automatically selects the best offer from all exchange brokers based on previous merchant selections and a combination of the better exchange rate and higher reputation score.

Exchange Brokers

If a customer pays in GRAFT tokens, and the merchant wants to get paid in GRAFT tokens, the funds will be automatically and instantly debited from the buyer account and deposited to the merchant account by the GRAFT network. However, if the customer wants to pay using a different payment method, and/or the merchant wants to be paid in a different currency, the GRAFT network will have to use a special mechanism.

In order to facilitate elements of payment processing that cannot be decentralized but are still highly demanded by consumers and merchants, the GRAFT network will introduce an exchange broker. Whenever the GRAFT network itself cannot process particular operation in fully decentralized way, it will delegate such an operation to the network of exchange brokers. Merchants can choose a single (for example, highly trusted or least expensive) exchange broker, or a group of brokers.

The exchange broker is responsible for maintaining security and necessary compliance with exchange and payment card processing regulations, including PCI DSS compliance and anti-money laundering regulations.[13]

Following are the types of exchange brokers:

Merchant/POS-side exchange brokers:

- Pay-in broker

- Payout broker

Buyer/wallet-side exchange brokers:

- Interchange broker
- Top-up broker

A set of cryptocurrency exchange brokers will be available for each major cryptocurrency listed on https://coinmarketcap.com/, starting from the top of the “top 10” by market capitalization. The exchange brokers will boost liquidity of each cryptocurrency by enabling various payment options on both the buyer’s and merchant’s sides of the transaction.

The cryptocurrency exchange brokers will be implemented in collaboration with existing and/or newly created exchanges. Multiple choices for each cryptocurrency eventually will be available, so they could compete in order to provide better rates and services. The variety of services and automated sign up, selection, and execution processes will keep the decentralized character of the network. Every single set includes four exchange brokers implemented for each cryptocurrency.

Pay-in and Payout brokers work with GRAFT POS app and hardware payment terminals to allow a merchant to accept the selected cryptocurrency as a payment method while conducting payment transactions with the GRAFT Wallet app or other cryptocurrency wallets.

Interchange and Top-up brokers work with the GRAFT Wallet apps to allow a buyer to use the selected cryptocurrency as a payment method when making a payment to GRAFT Points of Sale (POS), native wallet apps, non-GRAFT POS integrated with GRAFT DAPI, or non-GRAFT POS that accepts the selected cryptocurrency.

Pay-in Broker

Pay-in Broker enables accepting payment methods different from native GRFT tokens and immediately converts the payment amount into GRFT tokens and deposits them into the merchant account. Pay-in Broker acts in real time and becomes a part of the transaction between the buyer and merchant. From the buyer’s point of view, the transaction looks similar to a regular transaction between native cryptocurrency wallets.

Pay-in Broker works with GRAFT POS to facilitate acceptance of selected cryptocurrency as a payment method in case the buyer does not have GRAFT Wallet. The (selected cryptocurrency) network transaction fee is still paid by the buyer, unless the buyer uses the GRAFT Wallet app. If the buyer uses GRAFT Wallet, the wallet recognizes the GRAFT POS and automatically converts the payment transaction to an instant transaction in GRFT.

The merchant payout is processed by Pay-in Broker in GRFT instantly (If the corresponding Payout Broker is activated, the payout can be done in other cryptocurrency or fiat currency).

Examples of Pay-in Broker:

- Bitcoin Pay-in Broker
- Ether Pay-in Broker
- Credit Card Pay-in Broker

Design and Economics of Pay-in and Pay-out Brokers

Pay-in Broker takes a certain amount or risk accepting the cryptocurrency of payment while quickly releasing GRFT in exchange (without waiting for the cryptocurrency of choice confirmations). This risk for broker is mitigated by relatively small(er) retail transaction amounts and is subject to the authorization sample validating the transaction across originating currency network. The risk for the merchant is mitigated by a GRFT bond transaction equal to the amount of pay-in, which is generated by the broker at the beginning of transaction. The bond is put on hold by the authorization sample until the broker approves the altcoin payment to the merchant. As soon as the altcoin transaction (from buyer to the broker) is received and validated, the authorization sample approves the payment to the merchant and releases the GRFT payout (from the broker to the merchant). The broker is able to set different limits for different amounts / history and risk levels.

In exchange for this service, the pay-in broker substructs 0.25% exchange fee from the GRFT payment to the merchant, while the supernodes participating in the authorization sample charge their standard GRFT transaction fee (0.5%).

The following flow (sequence) diagram shows how bitcoin acceptance pay-in broker performs the exchange transaction and accepts bitcoin payment on behalf of merchant point of sale. The buyer can use any wallet supporting bitcoin. The merchant receives payout in GRFT.

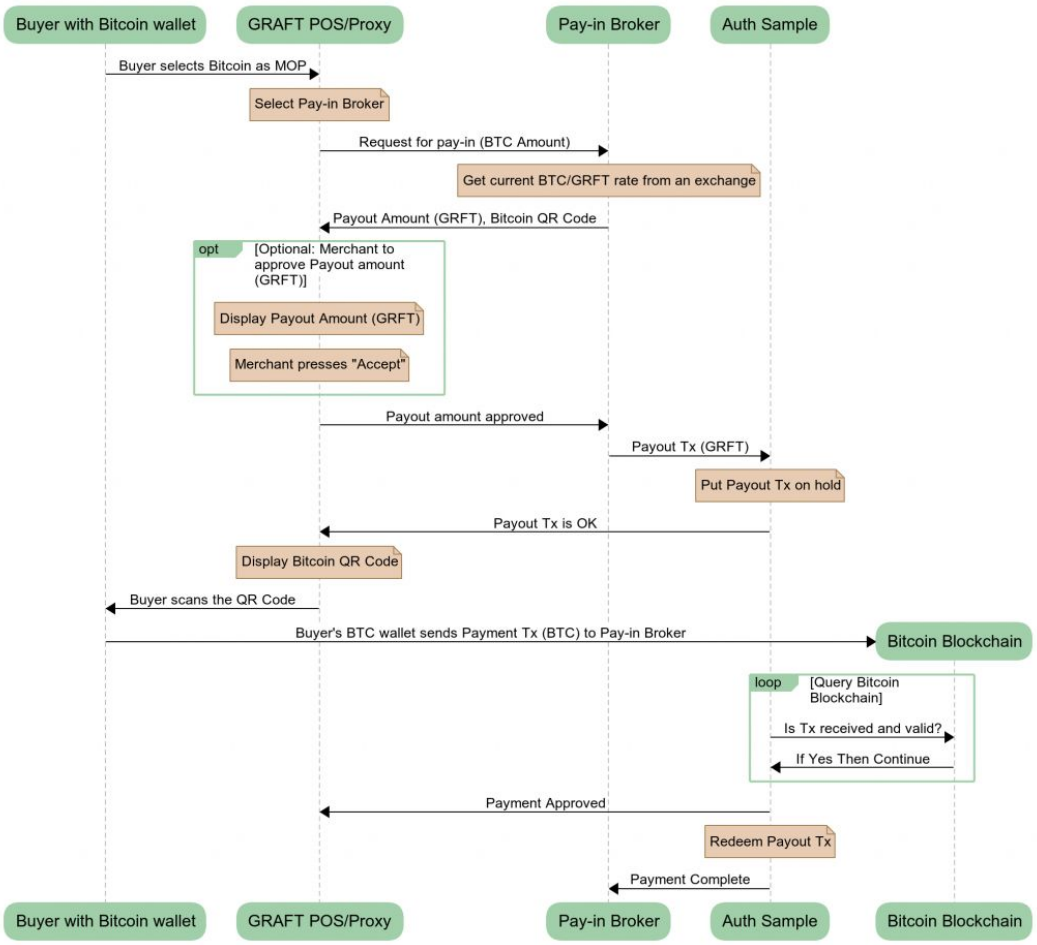

Figure 5: GRAFT Bitcoin Pay-in Broker Transaction Flow

Payout Broker exchanges GRFT into the payout currency of choice as requested by the merchant. The transaction is asymmetrical – meaning that the second leg of the payment is usually longer (sometimes much longer) to settle on the receiver side. To make sure that the payout broker delivers the payment with no double-spending, the broker stakes a bond with amount equal to the amount of the transaction. The staking is done by putting on hold the GRFT payment from the merchant by authorization sample. If authorization sample detects (after the grace time) that the payout funds weren't received by the merchant, it cancels the transaction and payout broker does not receive the GRTF payment from the merchant.

In exchange for this service, the pay-out broker receives 0.25% exchange fee. In addition, the authorization sample supernodes charge their regular transaction fee (0.5%).

Dual Pay-in/Payout Brokers

Same exchange brokers can (and most likely will) alternate as a pay-in and payout brokers. For example, let's review Bitcoin Exchange Broker (EB) which wants to perform both pay-in and payout exchange operations.

The broker has a Bitcoin wallet with 0.01 BTC in it. The broker receives a payout request from a merchant to exchange 100 GRFT to 0.01 BTC (assuming the current exchange rate is 0.01 BTC = 100 GRFT). The flow of such payout transaction between the broker and the merchant is shown in the diagram below.

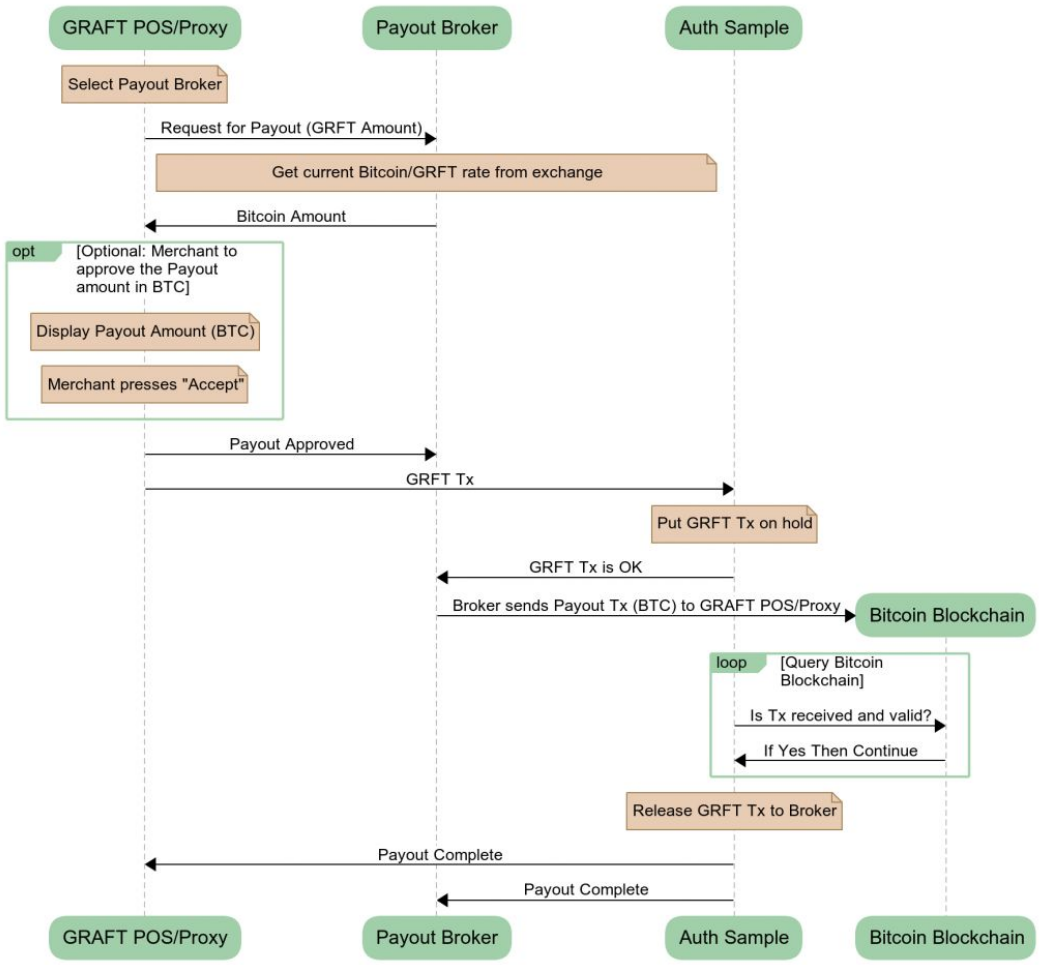

Figure 6: GRAFT Bitcoin Payout Broker Transaction Flow

The broker accepts the request and sends 0.01 BTC (minus bitcoin network fee) to the merchant, while the merchant generates the 100.75 GRFT payment (100 GRFT amount + 0.25 GRFT broker fee + 0.5 GRFT authorization sample fee) to the broker and transmits it to Authorization Sample. The sample puts 100.75 GRFT transaction on hold and notifies the broker who then sends 0.01 BTC to the merchant. Upon BTC transaction settlement (10-60 mins for the sake of argument and depending on the bitcoin network fees), the 100 GRFT transaction is released and the exchange broker now has the 100 GRFT payment plus 0.25 GRFT profit.

The broker can now switch into the pay-in broker mode. As pay-in broker, the EB receives a request to exchange 0.01 bitcoin into 100 GRFT. The broker accepts this request and transfers 100 GRFT (minus fees). As soon as 0.01 BTC is received, the broker is able to become a payout broker again and now has 0.01 BTC and 0.25 GRFT profit.

Assuming (conservatively) that a single pay-in/pay-out cycle takes 1 hour, the broker can make around 12% in a single 24 hour period (without compounding), making for a lucrative business model for the Exchange Broker* (*estimation only).

Beyond Merchant Payments: DEX

The system of exchange brokers described above can function beyond the GRAFT intended payment ecosystem and extend into a real-time decentralized exchange (DEX). Due to the fact that the untrusted exchange operations (atomic swaps) are close to real-time to the outside entity leveraging the GRAFT authorization/validation layer (the network of GRAFT supernodes), the same atomic swaps can be extended to provide real-time exchanges, such as BTC<->ETH.

Interchange Broker

Interchange Broker works with the GRAFT Wallet App to facilitate a payment to a native cryptocurrency wallet or non-GRAFT POS accepting the cryptocurrency. Interchange Broker creates a regular cryptocurrency transaction in native format for the particular network and sends it to the native recipient address. There is a network transaction fee, which is in this case charged to the sender because the transaction is not fully facilitated by the GRAFT network. The payment is not processed instantly because the recipient is not participating in the GRAFT network. This scenario is less beneficial than a GRFT transaction for both the buyer and merchant because of the lower speed of transaction and transaction fees paid by the buyer. However, it is supported by GRAFT in order to keep the buyer's wallet flexible and useful even outside of the GRAFT ecosystem.

Interchange Broker will instantly exchange the necessary amount of GRFT from the buyer's account to the selected cryptocurrency. The buyer pays a small exchange fee to the interchange broker, which can be paid in a form of exchange rate.

Examples of Interchange Broker:

- Bitcoin Interchange Broker
- Ether Interchange Broker

Payout Broker

Payout Broker enables withdrawal from a GRAFT merchant account in Bitcoins, altcoins, or local fiat currency. Payout can be initiated manually or automatically.

Payout fees / exchange rates for payouts processed by either Pay-in or Payout exchange brokers may vary on frequency of the payout. Depending on transaction volume, daily payouts can cost significantly less than instant payouts since the broker can accumulate more funds and pay just a single network fee for a single payout transaction, compared to paying a separate fee for each instant payout transaction.

Examples of Payout Broker:

- GRAFT Payout ("Stable Value") Token Broker
- USDT Payout Broker
- Bank ACH Payout Broker
- PayPal Payout Broker
- Bitcoin Payout Broker

Top-Up Broker

Top-Up Broker enables wallet top up by exchanging Bitcoin, altcoins, or local fiat currency to GRFT. This scenario is the most beneficial for both the buyer and the merchant because all the fees (including the network fees of the target cryptocurrency) are paid by the merchant, and payment is approved instantly. For the buyer, the benefits are obvious—no fees associated with the payment, and ability to pay with the target cryptocurrency to a merchant that does not accept it. For the merchant, it is important to get instant authorization in order to be able to serve more customers in real time, and accept payments in various cryptocurrencies. The fact that all the fees are paid by the merchant, just like with "traditional" credit/debit card payments, allows for much better customer conversion rates.

Top-Up Broker can also process exchanges on demand with larger amounts and better rates.

Examples of Top-up Broker:

- Credit card Top-Up Broker
- Bitcoin Top-Up Broker
- Bank ACH Top-Up Broker

Merchant Payouts

A merchant can decide to receive its proceeds from transactions in other cryptocurrencies such as Bitcoin, cryptographic tokens, payout ("stable value") tokens, or local fiat currency. In this case, the payment currency of the transaction will be processed by a exchange broker as part of the same transaction or later, depending on merchant settings. This ensures that the sale will pay the merchant the exact local currency price less applicable fees. The supernode sample automatically selects the best offer from all exchange brokers based on a combination of the merchant selections, a better exchange rate, and a higher reputation score.

Volatility

Most merchants want to get paid in their local currency. Merchants use fiat currency, not Bitcoins, other cryptocurrencies, or cryptographic tokens, to replenish stock, pay their bills, and pay employees' salaries. Also, they may use fiat to pay refunds in case of returns. Most merchants cannot afford high volatility, especially small merchants. Since Graft tokens (GRFT) are tradable, when they are used for merchant payouts directly, volatility may become a problem. GRAFT resolves the volatility problem by using instant, real-time transaction processing settlement, which minimizes possible loss of value due to volatility, and special "stable value" payout tokens. The merchant's payment app can automatically adjust the transaction amount to the current exchange rate, and redeem it to local currency through online exchange right after transaction completion.

Payout ("Stable Value") Token

Payout token is a special type of a merchant token that will be used to facilitate merchant payouts in local fiat currency in order to finally fill the gap and connect the two worlds—cryptocurrency transactions and fiat currency merchant operations. It represents a local currency and can be transacted on GRAFT blockchain in real time using the supernode tier of the blockchain. Payout token

is based on GRAFT merchant token technology, similar to gift, rewards, and other merchant token types.

Underwriting Payout Tokens

The main goal for creating payout tokens is providing an easy and reliable way for merchants to get paid in stable local fiat currencies while avoiding usage of centralized payment processors. Payout tokens are issued and maintained by responsible token underwriters (such as banks). When someone (the payout broker, for example) is buying payout tokens from the token underwriter, the company generates a necessary amount of tokens and transfers them to the buyer in exchange to an equivalent amount of fiat currency. When someone (the merchant or payout broker on behalf of the merchant) is selling payout tokens back to the token underwriter, the company destroys the tokens and pays an equivalent amount of local fiat currency to the seller. Thus, payout tokens are always backed by a sufficient amount of fiat currency, and their price always remains the same and equals the corresponding fiat currency float. For example, 100 GRAGT.USD can always be bought or sold for US$100. Payout tokens will be issued by licensed token underwriters only in exchange for equal amounts of fiat currency. Furthermore, the rights to handle particular payout tokens can be delegated (licensed) to local commercial banks or even national governments.

Processing Payouts

There are several payout options: GRAFT tokens, original or other cryptocurrency, GRAFT payout tokens, or local fiat currency (Table 2). For each of these options, there are Payout broker services available on GRAFT. When the merchant selects the methods of payment they want to accept and the payout method, the GRAFT Point of Sale application will prompt the merchant with all available broker services options—depending on merchant identity and location attributes—so the merchant can sign up for all desirable broker services. If more than one Payout broker service is available for the same type of exchange and selected by the merchant, the GRAFT Point of Sale app will automatically select the best offer during the transaction execution.

Table 2: Examples of a Variety of Accepted Methods of Payments and Payouts

Payment Method Selected by Customer	Payout Method Selected by Merchant	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

Merchant Tokens and VChains

In addition to fast and inexpensive transactions, merchants place high value on customer loyalty and branding. This functionality will be enabled by the token layer of the GRAFT currency. The token represents domain (merchant) specific GRAFT use, and offers smart contract-backed functionality like loyalty point accumulation and use, reward points, sale discounts, spending discounts, competitor discounts, coupons and store credit.

A coffee shop chain, for example, can create a merchant token and attach promotion rules that would provide a patron the ability to get discounts on iced drinks at a given time of the day; it would tally the purchases with the establishment and offer rewards based on activity or non-activity. GRAFT Merchant tokens would provide a very efficient mechanism for couponing by allowing the merchants to open up the coupon creation and assignment rules within their domain network.

Merchants Tokens

Merchant token is a predefined smart contract that allows creating a private token that belongs to its owner. Unlike some other smart contracts and token platforms, creation of GRAFT merchant token does not require any programming and can be done by anyone.

The business features described below are typically associated with using complex third-party service providers and high implementation costs, which makes those services inaccessible for small- to medium-size businesses and expensive to large businesses. GRAFT Merchant tokens allow any merchant to implement those important business features with minimum efforts and low cost.

Types of Merchant Tokens

Merchant tokens will allow merchants to create and use their own open-loop and closed-loop[14] products—gift certificates, loyalty rewards, or store credit program—in minutes, without any initial investments, fees, or registration with any centralized authority. Merchants will be able to sell and accept gift certificates on their website or in brick-and-mortar stores for local currency, other cryptocurrency, cryptographic tokens, or GRFT.

All GRAFT transactions, including issuing and redemption of gift certificates, loyalty points, and store credits are processed in real time using a standard API, which can be easily integrated into existing point-of-sale applications.

Store Credits

Store credits are typically utilized by merchants for performing purchase returns and exchanges, when returns cannot be done using the original payment method, or the merchant's return policy does not allow the full refund. Store credit essentially transforms returns into exchanges so the merchant does not lose the customer and associated revenue.

Store credit tokens can be linked to the item price in local fiat currency, so the customer can use those tokens for the next purchase instead of or in addition to the payment with local fiat currency. Store credit tokens usually either do not expire or have very distant expiration dates as they basically replace the fiat currency.

Loyalty Rewards

Loyalty rewards are a powerful marketing instrument that attracts customers and increases spending. Loyalty rewards can be awarded with each purchase or as a one-time bonus or other reward model. The rewards then can be used to purchase particular items or any items, or converted to cash. Loyalty rewards are not necessarily linked directly to fiat or cryptocurrency as they can be spent to provide a discount or buy special reward items that are not available for sale using other methods of payment.

Loyalty rewards usually have relatively close expiration dates. This way the merchant encourages customers to earn more rewards and eliminates accumulation of very large amounts of reward points that can eventually become useless.

GIft Certificates

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.

Discount Coupons

Discount coupons can be used for one-time or long-term promotions. The coupons can be distributed publicly or to individuals, in wallet or paper form. The coupon then can be scanned at the point of sale in order to get a discounted or even free item.

Transaction Types For Merchant Tokens

Create

Create a new merchant token ("smart contract"). Can be done using point-of-sale app.

Renew

Renew merchant token ("smart contract"). Can be done using point-of-sale app.

Add

Add more merchant tokens to the circulation.

Issue

Merchant's point of sale sends merchant tokens to the customer wallet or prints a paper wallet.

Redeem

Customer redeems merchant tokens at merchant's point of sale using wallet app or paper wallet.

Merchant Token Fees

All the merchant token fees are paid to the current supernode authorization sample.

Merchant Token Transaction Fees

The merchant always pays the token transaction fee, which means the buyer never pays the fee. Transaction fee is applied to each transaction with a merchant token, including adding, issuing, and redemption.

Initialization and Renewal Fees

The initial Create transaction implies a special higher fee because it is associated with naming a token. In order to prevent “domain squatting,” the initial fee will be set to a reasonable amount that prevents massive abuse.

VChains

VChain allows creating a virtual chain of stores so multiple points of sale can be connected to the same private “virtual blockchain.” Thus, there is a dual meaning for the word “VChain”: virtual chain and virtual blockchain. Vchain creates a private common platform for managing merchant tokens and items catalogue.

Merchants can create their own private Vchain, which is going to be accessible only by this particular merchant and contain all information about its tokens. Vchain allows connecting multiple points of sale or even creating a chain of multiple stores. Points of sale that belong to the same Vchain can issue and accept the same merchant tokens, use the same shared item catalog stored and maintained on the blockchain, generate aggregated transaction reports, and more.

Buyers can use Vchain to link multiple wallets so they can manage multiple accounts and move funds between those accounts without paying fees. This feature is useful for family and corporate accounts.

VChain Fees

There is initialization annual fee for creating a new Vchain smart contract, and renewal fee. Those fees are required to securely process the smart contract and prevent system abuse. There is a separate annual fee for adding another point of sale or wallet to the Vchain.

All Vchain fees are paid to the current supernode authorization sample.

Decentralized Crowdfunded Credit

A decentralized crowdfunded credit ecosystem consists of credit consumers (cardholders, buyers), credit providers, identity providers, and merchants (sellers). The GRAFT network facilitates the communication and transactions between the parties and enforces the common rules to minimize the risk of fraud.

The GRAFT network connects potential credit consumers with credit providers who offer credit to the consumer. Anyone with GRAFT Wallet (a free app) can become a credit consumer. Anyone with GRAFT Wallet and a positive balance can become a credit provider. Anyone with GRAFT Point of Sale

(a free app), or a third-party point of sale integrated with GRAFT SDK, can become a merchant. The identity provider is implemented as a service plugin on the GRAFT supernode. The identity provider uses an open API, which helps maintain the open and decentralized character of the entire ecosystem.

Credit providers set their requirements of minimal identity necessary to receive the credit, maximum credit limit, overall maximum credit limit (from multiple providers), credit rate, and minimum payment amount and frequency. Credit consumers can get credit from multiple credit providers as long as the current state of their account fits the provider's requirements. Third party identity providers validate and confirm the identity elements provided by the consumer to remove the burden of identity validation from credit providers and provide some degree of anonymity and privacy to the cardholder. Thus, identity providers know the real identity of the consumer and therefore can maintain their long-term reputation score independently from the network or credit providers. Credit providers receive a share of the transaction fee from each payment that is processed using their credit.

The credit consumer is assigned a reputation score, which is dynamically calculated based on consumer history and level of identity provided by the cardholder and validated by the identity providers. The initial score, before any identity is validated or any history data is collected, is set to 0. The more identity elements provided and validated (for example, driver license, biometrics, social security number), the higher the initial score, which means the more credit that can be given to the cardholder. Positive repayment history elevates the reputation score respectively.

Merchants are just recipients of the transaction with credit consumers, isolated from the relationship between the cardholders, credit providers, and identity providers, which completely eliminates their risk of fraud. Credit providers assume all potential fraud risk and expenses, which is compensated by their share of transaction processing fees and credit rates fees. However, merchants can participate in the process by offering incentives such as transaction cashback, or even act as credit providers.

Security

As recent megadata breaches in retail and hospitality industries show, security is a very important element of any payment ecosystem. The highest level of security can be achieved if security is part of the system design rather than an add-on created after implementation is done. Security of a payment system is not just information security but should include financial security as well. In addition to standard security features inherited from its predecessors, GRAFT plans to implement several enhancements from which both buyers and merchants benefit.

Availability

The distributed network of “always-on” supernodes ensures overall availability of the network. The client apps communicate with multiple supernodes simultaneously in order to get the consensus required for authorization. If one of the sample supernodes is down it is automatically replaced by another one from the authorization sample candidate list, which contains a virtually endless number of candidates.

Identity Management

Relying on the wallets to do user management opens up a big security risk as wallets are typically free to implement their own security measures and can be compromised individually. In order to protect the network and ensure integrity of user identities, GRAFT will implement a distributed identity provider service (embedded into supernode), available to the wallets as an OpenID Connect oAuth2 API call.

As such, regardless of wallet implementation, user verification and authentication will be carried out by the GRAFT network, which will prevent compromised user identities, spoofing, replays, and man-in-the-middle attacks.

Identification, Authentication, and Authorization

The authentication/authorization methods of existing cryptocurrencies have been in the purview of the user application such as wallet, and have largely been an afterthought. In context of financial transactions between buyers and sellers, however, where some degree of trust has to be established between the parties, regulations and compliances have to be dealt with, and a recourse has to be provided, a good system for authentication/authorization becomes critical.

Identity Proofing

Identity proofing is a challenging topic as it carries both regulatory and privacy considerations. Also effective identity proofing is not trivial.

To understand the need for identity proofing, consider a merchant that might request a strong level of identity proofing to make sure the buyer is eligible to purchase prescribed medications, and a superior level of identity proofing to purchase arms (as defined by NIST Special Publication 800-63A in the US). Conversely, buyers purchasing goods from an aftermarket, might want to protect themselves from buying stolen goods by requesting that the merchant provide a higher level of identity proofing.

GRAFT expects the client applications to comply with identity verification standards relevant to the specific laws of each jurisdiction's laws. Supernodes will provide resources for machine-based identity verification and fraud detection to assist merchants (and users) with compliance, ensure integrity of the payment network, and safety of the transactions. In order to limit user's exposure when sharing their complete identity information is undesirable or counter to the regulatory laws (GDPR for example), GRAFT will facilitate requests for and sharing of the identity attributes, such as the person's age and address, to ensure compliance with local laws and regulations. We're also looking to add more metadata collection to the attribute sharing to enable auxiliary business logic such as drug interaction checks or loyalty rewards.

GRAFT will allow optional multi user control, where several users have access to the same merchant account, and multiuser custodianship, where two or more users are required in order to unlock some functions like transferring funds out of the account.

Reputation Score: Illuminate the Darkness

GRAFT takes a risk-based approach to transaction processing. Each participant in the network is assigned a reputation score, which is dynamically updated according to new data captured by the system. The buyers, merchants, and supernode owners can optionally link their partial identity to their account in order to disclose and improve their reputation score. Such a link will not compromise the untraceability of transactions.

The reputation score system helps participants in the ecosystem make informed decisions without compromising their security and privacy. For example, a merchant can take into account the buyer's reputation score when making decisions regarding authorization limits before instant authorization. Similarly, the buyer can review the merchant's reputation score before making payment for any goods that cannot be delivered immediately. Both buyers and merchants can check the reputation score of the network supernode they communicate with, and the proxy supernodes can in turn use exchange broker's reputation score to make their decision to engage them in a transaction.

Another important element of user reputation scoring will come to light in the context of peer-to-peer credit, where the reputation score will include elements of credit scoring based on the payment history.

The supernodes are in charge of monitoring, calculating, updating, and validating the reputation scores for buyers, merchants, and other supernodes. The scores are calculated using special predictive analytics algorithms that produce easily understandable results on a scale of 0-100, which cannot be used to disclose any information about the number, amount, time, or nature of transactions.

Customer Support, Dispute Resolution, and Payment Insurance

One of the main showstoppers of cryptocurrency and cryptographic token adoption by mainstream consumers and merchants is the lack of the authority and the business owners who could help answer questions and resolve technical and business issues. Also, it is impossible to “fix” a wrong cryptocurrency or cryptographic token transaction in case of human error, fraudulent activity, or technical glitch. Obviously, all these issues are caused and justified by the decentralized, anonymous, and independent nature of crypto payments. However, the good reasons do not help resolve the problems. The open source community resolved those problems by introducing an optional customer support for free open-source products. Linux OS, supported by Redhat, and the MySQL database, supported by Oracle, are just two successful examples of providing commercial-level support to free open-source products.

In order to facilitate adoption of GRAFT payments, the GRAFT Foundation provides free customer support and dispute resolution services to GRAFT account holders. Merchants with high transaction volume can get 24/7 real-time support and dispute resolution assistance. The GRAFT Foundation and/or exchange brokers may insure payments up to an equivalent of USD 100 and compensate customers or merchants for their loss of funds due to fraud or technical issues.

User Applications

All GRAFT user apps are “light” clients that do not store the blockchain or process any transactions. The user apps use remote API calls to communicate with “always on” GRAFT nodes, which mine new transactions blocks and process transaction requests in real time.

Users that require an even higher level of control over privacy, anonymity, and availability (for example, large merchants or secret organizations) may run their own supernode or even multiple supernodes, which would exclusively and privately communicate with their client apps, relay messages and transactions to other supernodes, issue offline authorizations, and mine GRAFTs required for running store credit, gift, and loyalty programs.

Consumer apps include:

- Desktop and mobile merchant point-of-sale apps for accepting payments in GRAFT tokens, Bitcoins, altcoins, and credit/debit cards, as well as configuring payouts in Bitcoins, altcoins, and local fiat currencies, which can be used by both buyers and merchants.
- Desktop, mobile, and Chrome browser extension wallet apps for making payments in GRAFT tokens, Bitcoins, altcoins, and credit/debit cards (by using instant exchange brokers), and sending and receiving transfers in GRAFT tokens.
- GRAFT SDK will allow integration with major merchant point-of-sale software and shopping carts for processing both online and brick-and-mortar transactions. GRAFT will incorporate a GRAFT smartcard as a payment method. In addition to carrying keys, the card will also store biometric signatures of the user and a set of memorized or looked-up secrets, which can be used for at-the-terminal authentication. The GRAFT Foundation and exchange brokers will support the smartcard and smartcard reader production.

In addition to supporting consumer-focused transactions (B2C), GRAFT will support B2B (business-to-business) transactions and integrate into the existing business workflows. Such workflows can range from something as simple as automatically collecting according to credit terms (e.g., Net 30, 60, 90), to complex workflows such as settling the shipper's custom bill and accounting for it as part of the overall transactions, to distributing the funds based on reaching milestones and customer approvals.

GRAFT also plays well into the IoT space as some of the IoT devices need to "charge" for the data or services that they are offering. An example would be a brick-and-mortar merchant summoning a truck based on the inventory levels as determined by backend systems and sensors.

Conclusion

GRAFT wouldn't exist without its predecessors. It is based on ideas, principles, and technologies introduced and tested by creators of other cryptographic utility tokens. Using most recent technologies developed by the cryptography community along with newly developed solutions for transaction processing and security will allow GRAFT to compete with traditional payment methods and existing centralized payment processors.

References

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.