Slava Gomzin, Dan Itkis
Version 1.2
December 2017
DRAFT

Decentralized, Real-time Credit, Debit, and Crypto Payment Processing Blockchain

Abstract

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 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 in centralized intermediaries (payment gateways and processors) currently required to facilitate transactions between buyers and merchants.

Background

Bitcoin[1] was created as an "online cash" - asecure but relatively slow settlement system which was unable to replace payment cards online or

compete with both plastic cards and paper cash in brick-and-mortar stores (Figure 1).
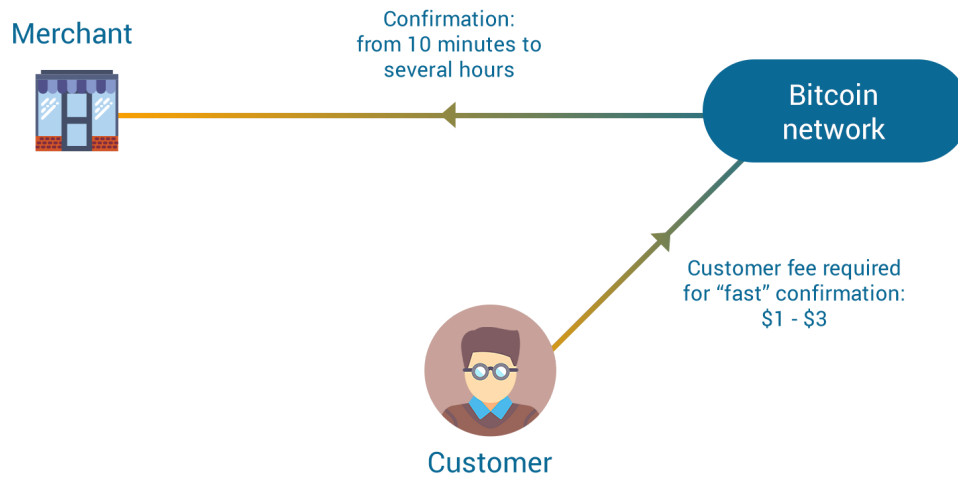
Figure 1: Bitcoin Transaction Processing without Centralized Intermediary

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] - who fill the gap (Figure 2). However, the very existence of payment processors, which aretypically a centralized commercial organization regulated by government and controlled by shareholders, as an element of cryptographic payment transaction, contradicts some fundamental principles of cryptocurrencies and cryptographic tokens: decentralization, privacy, and independence.
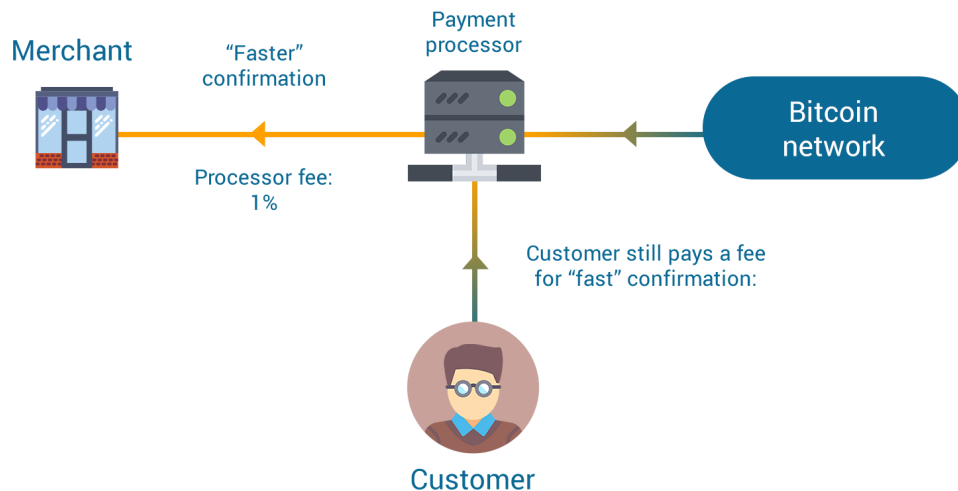
Figure 2: Processing Bitcoin Transaction by Centralized Intermediary

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

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 the list of some of the technical limitations and business flaws of the existing cryptographic payment systems comparing 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   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 find 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) to individuals to keep their money in a form of cryptocurrencies 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, 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, without any middlemen, and with extremely low fees.

There may be additional value as well. In some cases, merchant might want to know the real identity of a potential customer in order to comply with laws and regulations, for example, to make sure the potential customer is 21 years of age or older in order to legally sell certain items to the potential customer.

Since GRAFT is a decentralized payment processor, the function of which 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 additional choice for buyers and acceptable method of payoff for merchants. This feature will eliminate the need for merchant to integrate with multiple (centralized) payment software providers, as well as for user to sign up for centralized services and learn and maintain multiple wallet apps. It is important to note that merchants will have to accommodate higher risks and additional expenses associated with acceptance of alternative cryptocurrencies and/or cryptographic tokens due to their slower confirmation times and higher transaction fees.

Terminology

GRAFT

1. Global Real-time Authorizations and Fund Transfers - decentralized global open platform for processing real-time authorizations and settlements of merchant payments and fund transfers using untraceable blockchain, decentralized API, and open community of service brokers that support 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. This technique has a allows for the best traits of different plants to come together to create something better and more valuable than their original parts.

Supernode

An independent, always-on server running the combined implementation of GRAFT blockchain node and GRAFT DAPI node, maintaining the GRAFT blockchain via block mining, processing of real-time authorization and settlement DAPI calls between buyers and merchants, and hosting third party services such as instant cryptocurrency exchange within the GRAFT network, credit/debit card acceptance, and merchant payouts in local currency. The Supernodes collectively maintain the network using GRAFT's combined Proof of Work/Proof of Stake algorithm.

Authorization Sample

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

Relay Supernode

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

Service Broker

A GRAFT protocol extension hosted on a supernode or a group of supernodes and owned by the supernode operator. Service Brokers implement special additional features that cannot be automatically executed by fully decentralized network or/and requires special regulation framework such as PCI DSS[6] or NIST 800-63-3.[7] Examples of service brokers are credit card payment acceptance broker and bank payout transfer broker.

Domain

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

GRFT Token

Native cryptographic tokens supported by GRAFT blockchain and used for real-time payment authorizations, transfers of funds, and settlement between buyers and merchants

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.

GRAFT Wallet

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

GRAFT Point of Sale

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

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 does collect them, and how much should they 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 coins from each block as well as getting fees for each transaction.

The mining has another purpose: constant and steady injection of new coins into the system to keep up the liquidity with the growing demand for extra coins 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.[8] In other networks, including Bitcoin, the fees are used to prioritize transactions and "resolve" the scalability problem.

In GRAFT network, however, the fee is used for two reasons. First, 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. Second, 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 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.[9] The (average/layman) payer is often confused by the process which looks more like gambling, without 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.[10] GRAFT resolves this problem by introducing a unique approach to transaction fees.

GRAFT Transaction Fees

GRAFT In GRAFT's ecosystem, the payer pays not fees. All fees are borne by the receiver (merchant or payee). GRAFT makes micropayments accessible by setting very low (as compared to credit cards[11] and online payment processors,[12] cryptocurrencies[13], and other cryptographic tokens) fees, but without a fixed fee component (Table 1).

Table 1: GRAFT Network Transaction Fees

Micropayments (less than 10 GRFTT)	Regular Payments (more than 10 GRFTT)
0.1%	1% of log10 (significantly less than 0.1% as transaction amount grows)

The logarithmic fee schedule provides for an incentive for processing less transactions with small amounts (i.e. combining multiple transactions together whenever possible) while keeping low transaction fees for large transaction amounts (Table 2).

Table 2: Examples of GRAFT Network Transaction Fees

Transaction amount	Transaction Fee Amount	Effective Transaction Fee
0.01 GRFTT	0.00001 GRFTT	0.1%
1 GRFTT	0.001 GRFTT	0.1%
10 GRFTT	0.01 GRFTT	0.1%

50 GRFTT	0.01699 GRFTT	0.03398%
100 GRFTT	0.02 GRFTT	0.02%
1,000 GRFTT	0.03 GRFTT	0.003%
1,000,000 GRFTT	0.06 GRFTT	0.000006%

Free Funds Transfers: Authenticated Transactions

Many payment networks, such as ACH or PayPal, provide free transfers between user accounts.In order to be able to compete with traditional payment networks, GRAFT provides limited free transfers between user wallets.

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

- Lack of incentive for miners
- Threat of DOS attacks
- Uncontrolled growth of blockchain

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

The second problem — DOS threats — 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 interval, unlimited

block size, and standard restricted transaction size for particular transaction types, such as free transfer. In addition, one of the sides of the free transfer must be verified by having conducted "commercial" payment transaction types in the past.

Additional Third Party Service Broker Fees

When accepting different payment methods such as bitcoins, altcoins, credit/debit cards, or processing merchant payouts in different currencies such as bitcoins, altcoins, or local fiat currency, additional payment broker and/or payout broker fees may be applied. These are not hidden fees as they are published by the brokers. We expect those fees are will becharged to the merchant at the time of transaction settlement (payout), instead of any setup, upfront, or periodic fees.

Customer Fees

Some cryptocurrencies such as Bitcoin require customers to add transaction fees in order to get fast confirmations. Such fees are configured by customer wallet application and paid by customer. Most Bitcoin users are already accustomed to such fees.

Paying Fees Using Margin Balances

In some cases, transaction fees can be charged using special "margin" balances provided by GRAFT network itself and/or margin brokers. Examples of such transactions are "Issue and Redeem" transactions related to gift certificates, loyalty rewards, and store credit processing. This is done in order to allow merchant transaction processing even if the merchant does not have enough balance on GRAFT account yet.

Transaction Processing

The world's moving towards "thin" devices. People around the world use more smartphones and tablets and less workstations and laptops. Therefore, decentralized cryptographic payment systems will rely solely

on small individual nodes hosted on personal computers but rather willbe based on dedicated powerful supernodes hosted by professionals, with thin clients 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[14] (from several minutes to several hours, depending on transaction fee[15]) 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[16], GRAFT processes all its transactions in "real time" (we expect __% of transactions to complete in less than 3 seconds). Critically, GRAFT achieves this real time payment without charging the customer an extra fee. (see Figure 3).
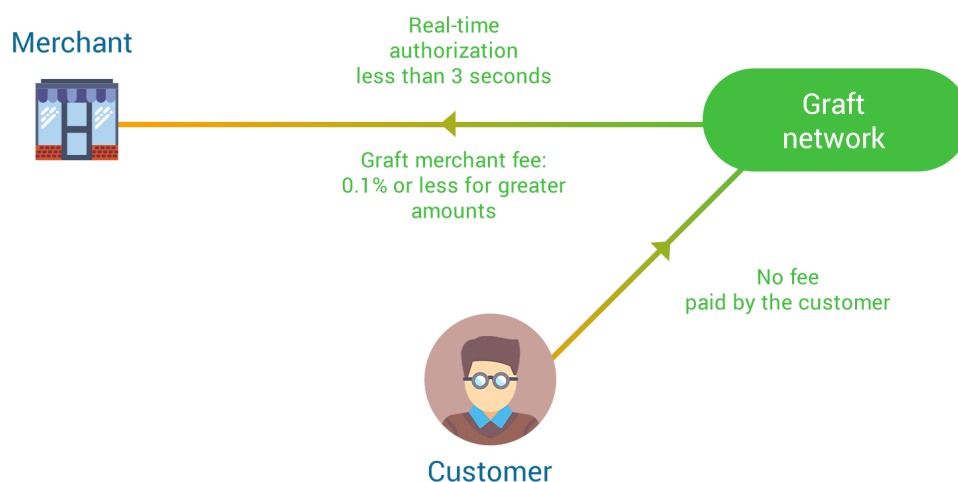
Figure 3: Simplified GRAFT Payment Flow

This is achieved by using a consensus of always-on trusted supernodes ("authorization sample") with ability to perform a distributed instant

authorization lock on buyer's account and communicate response back to the client, typically within milliseconds. The supernodes also maintain 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 authorization sample and (optional) service brokers participating in transaction processing. Supernodes are responsible for both settlement (block mining) and real-time transaction approvals. The owners of the nodes are responsible for transactions they process. Such responsibility is achieved by financial interest: mining rewards and transaction fees.

DAPI

Unlike regular APIs, which are hosted at a server or server farm, DAPIs 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 supernodes it communicates with, which is a relatively small group of addresses selected from the authorization sample. However, the client app is free to select a particular trusted supernode and "stick" with it. For example, merchant point-of-saleor wallet users can decide to host their own supernode which they trust. Even such a "private" supernode may not be granted a right to participate in authorization sample due to resource limitations (see Authorization Sample Selection Algorithm section below), but they can provide an extra layer of privacy of 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 trusted 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 by the "underlying" part of the supernode code, typically within two 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 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 in order to validate new transactions and prevent double spending without compromising the privacy of the sender. A key image is unique "fingerprint" that represents the buyer's spending address and amount without disclosing any details about the buyer or the amount. The nature of 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 signal of 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 will try to finalize the transaction with the key image different from the one used in the original lock, such transaction will be also rejected by the supernodes.

On the other hand, the 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 authorization phase are removed once 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 open and decentralized network which 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 proxy supernode. The only requirement is public IP address, but this can be achieved even with home network. Proxy supernode does not mine or provide services, but it can be useful for several purposes; for example, as a trusted relay for those who have highest privacy requirements, so they can host their own "wallet server", or for large merchants as a "store server" for even faster transaction processing.

Mining Supernode can generate revenue for the supernode owner by earning block rewards. The only requirement GRAFT requires of Mining Supernodes (in addition to public IP) is a higher computing power required for PoW mining.

Full Supernode is both miner and service provider. It cannot perform its real time authorization functions or service brokerage (hosting credit card acceptance service, for example) without mining. In addition, performance of full supernode functions requires a stake – collateral balance associated with the supernode address. Thus, a full supernode earns its elevated trust by a combined proof of work / proof of stake algorithm. A mining supernode can mine without a stake but it will not be able to provide services, i.e. it will not be able to earn transaction and service fees. Note that a GRAFT miner does not receive transaction or service fees, only block rewards. Transaction and service fees are only paid to a full supernode which mines, has a stake, issues real time approvals, and hosts network service brokers.

Authorization Sample Selection

In order to perform real time authorizations, the GRAFT network relies on the authorization sample: a group of selected trusted supernodes which 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 supernodes that solved the last 1440 blocks starting ten blocks below the then-current block height. If the same supernode has solved more than one block within the last eight blocks (starting from ten minus the then-current block height) or the selected node went offline, the list is automatically extended and another supernode from the "bottom" of the list is added to the sample. Another requirement for authorization sample participation is proof of stake: the supernode owner must maintain a collateral balance in an account associated with the supernode. The minimum required balance is starting from 500 GRFTT and recalculated dynamically with every block and increasing with each block proportionally to the growing GRFTT supply.

This algorithm allows the most active supernodes, which constantly prove their loyalty to the network through successful mining, to also be trusted to perform the real time authorizations, while still following some degree of randomization provided by the Proof of Work algorithm. These supernodes also are rewarded by transaction fee for each successful real time authorization. New supernodes "earn" their chance to participate in the transaction processing by adding more power and solving next block (which is generated on average every two minutes).

The supernodes that perform successful mining but fail to process real-time authorization requests will be excluded by the network from the full supernode list (i.e. the blocks they solve will not be accepted by the network for the period of 720 blocks).

When new transaction request is initiated by the merchant point of sale, it is assigned the current block height which defines the authorization sample. The height can be incremented while transaction is still in progress, but it does not change the sample height that was initially

assigned to the transaction request. The merchant relay 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 relay.

In order to speed up the authorization process, the merchant 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% of the approved responses from "fastest" supernodes and zero rejected responses; however, this mode will increase the risk of fraud, which can be acceptable in specific cases of micropayments when transaction processing speed requirements are extremely important.

Proxy Supernodes

Any supernode from the authorization sample can be also a proxy supernode - the relay that facilitates the merchant transaction by communicating with the merchant point of sale or/and 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 which is not a part of authorization sample. In fact, a point of sale or wallet can host their own proxy supernodes if they are seeking an extra layer of security and privacy; such proxies can be also upgraded to mining or even full supernodes and earn an income from mining and transaction processing. However, the proxy supernodes do not get any rewards or fees if they are not included in the authorization sample.

Supernode Rewards

Each supernode in the authorization sample receives a share of transaction fee for each transaction it signs (approves). Each supernode in the sample receives 1 / n of the transaction fee, where n is the number of supernodes in the authorization sample. The fee is paid by the recipient (merchant).

The block mining reward is paid to the supernode that solved the new block. The block reward is gradually reduced with each new block using

the following formula: $(M - A) * 2^{-19} * 10^{-12}$, where A = current circulation, M = total supply $(2^{64} - 1)$ in atomic units (10^{-12}). The idea behind this is that in the future there will be more transactions which will ensure the sustainable income for supernodes from transaction fees.

Scalability

The scalability of a given paymentGRAFTnetwork is the ability to process a large number of transactions simultaneously without degradation of performance. Scalability of the payment network is usually measured in tps (transactions per second). For example, Visa claims its authorization network is capable to process 56,000 tps,[17] while the Bitcoin network is restricted to a sustained rate of only 7 tps.[18]

Some of the measures that the GRAFT network uses achieve higher scalability are decreasing 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.[19] GRAFT, however, is maintained by always-on high performance supernodes which validate and authorize transactions in real time. Therefore, each supernode not only has a most recent copy of full blockchain but also keeps a list of all pending authorization requests and completed transactions until they are added to the blockchain. Such architecture allows absorbing large spikes of requests associated (for example, such as 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 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 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 short downtime, local authorization can go unnoticed to both cashiers and buyers.

GRAFT merchant point of sale app and single relay 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 be also based on buyer's and supernode's reputation scores.

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 transaction is unknown at the time of the sale initiation. Examples are pay at the pump at gas station, car rental check-in, hotel room reservation/check in, or restaurant pay at the table.

This is analogue 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 payee and confirmed by the payer, or until the amount is confirmed by subsequent "Complete" transaction. The authorization lock can be also released by Cancel transaction issued by payee before the expiration. 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 Complete transaction.

PreAuth

This is similar to 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 pre-authorized transaction.

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

Complete

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

Complete is used after previously authorized transaction is finalized and the exact amount is known. For example, pay 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 typical merchant transaction in online or brick and mortar store.

Transfer

Money transfer between GRAFT accounts. The same as Sale but initiated by the Sender, without Receiver consent. Can be used for peer-to-peer payments, exchanges, and transfers between different accounts.

Cancel

Cancels Authorize, releases the authorized funds (removes the account lock).

Issue

Activates GRAFT prepaid card, gift certificate, loyalty points, store credit, or discount coupon.

Redeem

Payment using prepaid card, gift certificate, loyalty points, store credit, or discount coupon previously issued by GRAFT.

Exchange

Exchange funds between graftcoins and other major cryptocurrencies, cryptographic tokens, and local fiat currencies using the best offer from supernodes.

Schedule

Schedules a transaction to occur at a later time/date. Requires additional acknowledgement from the user.

Escrow

Escrows the funds, attaching an event trigger when the funds will be released.

Refund

Refund transaction returns the funds referenced by the transaction pointer. Requires 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 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, using a paper or plastic gift certificate or coupon which can be scanned by the merchant payment app if the customer does not want to use mobile app or does not have 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 a form of credit/debit card as an input through the buyer's GRAFT Wallet app. Exchange fees, bank fees, and credit/debit card processing fees (charged from merchant in graftcoins) maybe 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. Automatic instant conversion will help adopt GRAFT payments by mainstream users who are not familiar enough with cryptocurrency and cryptographic token ecosystems and still feel more comfortable with traditional method of payment, but seek better security, privacy, and full anonymity of their transactions.

If buyer decides to pay with alternative cryptocurrency, cryptographic tokens, or credit/debit card, GRAFT network will automatically exchange other cryptocurrency, cryptographic tokens, or convert credit card payment in local fiat currency into GRFT tokens in real time as a part of the transaction processing using service brokers. The service

brokers, running on GRAFT supernodes and maintained by the supernode owners, are responsible for executing the exchange deals, charging the buyers, and executing payouts to merchants. If the buyer chooses alternative cryptocurrency, cryptographic tokens, or credit card as a method of payment, the supernode sample automatically selects the best offer from all service brokers based on previous merchant selections and combination of the better exchange rate and higher reputation score.

The supernode owner can provide currency exchange or/and credit/debit card payment as an additional service in a form of service broker. The service broker is responsible for maintaining security and necessary compliance with exchange and payment card processing regulations, including PCI DSS compliance, anti-money laundering regulations, etc.

Service Brokers

If customer pays in graftcoins, and merchant wants to get paid in graftcoins, the funds will be automatically and instantly debited from buyer account and deposited to merchant account by GRAFT network. However, if the customer wants to pay using different payment method, or/and the merchant wants to be paid in different currency, the GRAFT network will have to use 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 plans on introducing a concept of service broker. Whenever the GRAFT network itself cannot process particular operation in fully decentralized way, it will delegate such an operation to the network of service brokers. Merchants can choose a single (for example, highly trusted or least expensive) service broker, or a group of brokers.

Supernodes facilitate the hosting of service brokers. In fact, the supernode owners may become a service broker. While supernodes must implement both mining and real-time authorization functions, they don't have to implement any broker functions by default.

In addition to adding implementation modules to supernodes, Service Brokers may modify the client app source code, or even create their own

applications following GRAFT protocol. These are the types of service brokers:

- Accept Broker
- Payoff Broker
- Top Up Broker
- Margin Broker
- Escrow Broker
- Identity Verification Broker

Accept Broker enables accepting payment methods different from native GRFT Tokens and immediately converts the payment amount into GRFT Tokens and deposits them into merchant account. Accept Broker acts in real time and becomes a part of transaction between buyer and merchant. Examples of accept broker:

- Bitcoin accept broker
- Ether accept broker
- Credit Card accept broker
- Apple Pay accept broker

Payout Broker enables withdrawal from GRAFT merchant account in bitcoins, altcoins, or local fiat currency. Payoff can be initiated manually or automatically. Examples of payout broker:

- Bank transfer payout broker
- PayPal payout broker
- Bitcoin payout broker

Top Up Broker enables wallet top up (exchanging bitcoin, altcoins or local fiat currency to graftcoins). Examples:

- Credit card top up Broker
- Bitcoin top up Broker
- ACH top up Broker

Margin Broker provides a temporary balance to merchant for paying processing fees for transactions that do not have financial inputs such as gift certificate redemption. The margin balance is returned automatically as soon as merchant receives proceeds from next financial transaction.

Merchant Payouts

A merchant can decide to receive its proceeds from transactions in other cryptocurrencies such as Bitcoin, cryptographic tokens, or local fiat currency. In this case, the payment currency of the transaction will be processed by service 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 service brokers based on combination of the merchant selections, better exchange rate, and higher reputation score.

There are several payout options: graftcoins, original cryptocurrency, other cryptocurrency, cryptographic tokens, or local fiat currency (Table 3). 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 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 available for the same type of exchange and selected by merchant, the GRAFT Point of Sale app will automatically select the best offer during the transaction execution.

Table 3: Examples of Variety of Accepted methods of Payments and Payoffs

Payment method selected by customer	Payout method selected by merchant	Accept Broker	Payout Broker	Additional Fees
graftcoins	graftcoins	None (GRAFT network)	None (GRAFT network)	None
Gift Certificate, Loyalty Rewards,	N/A	None (GRAFT network)	N/A (Margin Broker might be needed to cover	None

			transaction fee)	
graftcoins	USD	None (GRAFT network)	Bank Transfer Payout Broker, PayPal Payout Broker	Payout Broker fee
graftcoins	bitcoins	None (GRAFT network)	Bitcoin Payout Broker	Bitcoin Payout Broker fee
bitcoins	graftcoins	Bitcoin Accept Broker	None (GRAFT network)	Bitcoin Broker fee, Bitcoin transaction fee (paid by customer)
bitcoins	bitcoins	Bitcoin Accept Broker	Bitcoin Payout Broker	Bitcoin Accept Broker fee, Bitcoin Payout Broker fee, Bitcoin transaction fee (paid by customer)
bitcoins	USD	Bitcoin Accept Broker	Bank Transfer Payout Broker, PayPal Payout Broker	Bitcoin Accept Broker fee, Payout Broker fee
Credit card	grafts	Credit Card Accept broker	None (GRAFT network)	Credit Card Accept broker fee

The first cell of the top row reads "Store Credit redemption".

| Credit card | bitcoins | Credit Card Accept broker | Bitcoin Payout Broker | Credit Card Accept broker fee, Bitcoin Payout Broker fee, Bitcoin transaction fees (paid by customer) |
| Credit card | USD | Credit Card Accept broker | Bank Transfer Payout Broker, PayPal Payout Broker | Credit Card Accept broker fee, Bank or PayPal payout broker fee |

Open Loop and Closed Loop Products: Gift Certificates, Loyalty Rewards, and Store Credits

GRAFT will allow merchants to create and use their own open loop and closed loop[20] 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 store for local currency, other cryptocurrency, , cryptographic tokens, or graftcoins. Gift certificates will be available in a form of electronic certificate on mobile wallet app, sent by email, printed on paper, or as a physical plastic card (provided by GRAFT foundation or third parties). Using unique GRAFT flexible identity system, merchant can be compliant with regulations around gift certificates.

All GRAFT transactions, including issuing and redemption of gift certificates, loyalty points, and store credits are processed in real time using standard API, which can be easily integrated into existing point of sale applications. 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. Customer can redeem gift certificates at the issuing merchant store by its nominal local currency value or sell it anytime on marketplace for local fiat currency, cryptocurrency or cryptographic tokens using its current market value.

Merchant (Domain) Tokens

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, store credit, etc.

A coffee shop chain, for example, can create a merchant token and attach promotion rules that would provide a patron ability to get discounts on iced drinks at given time of the day, it would tally the purchases with the establishment and offer rewards based on activity or non-activity.

Finally, GRAFT Domain 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.

Decentralized Crowdfunded Credit Cards

Decentralized crowdfunded credit card eco-system consists of credit consumers (cardholders, buyers), credit providers, identity providers, and merchants (sellers). 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 a credit to consumer. Anyone with GRAFT wallet (free app) can become a credit consumer. Anyone with GRAFT wallet and positive balance can become a credit provider. Anyone with GRAFT point of sale (free app), or third party point of sale integrated with GRAFT SDK, can become a merchant. The identity provider is implemented as a service broker which runs as a "plugin" on GRAFT network. The identity provider uses an open API which help maintain the open and decentralized character of the entire eco-system.

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 consumer can get credit from multiple credit providers as long as the current state of their account fits the provider requirements. 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 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 transaction fee from each payment that is processes using their credit.

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 validated or any history data is collected, is set to 0. The more identity elements are provided and validated (for example, driver license, biometrics, social security number), the higher is initial score, which means the more credit can be given to the cardholder. Positive repayment history elevates the reputation score respectively.

Merchants are just recipients of transaction with credit consumer, 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 as credit providers.

Security

As recent mega data breaches in retail and hospitality industries show, security is 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 "add-on" created after implementation is done. Security of payment system is not just information security but it 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 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 crytocurrencies 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 strong level of identity proofing to make sure the buyer is eligible to purchase prescribed medications, and superior level of identity proofing to purchase arms (as defined by NIST Special Publication 800-63A in the US). Conversely, buyers purchasing goods on an after-market, might want to protect themselves from buying stolen goods by requesting that the merchant provide 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 request for and sharing of the identity attributes, such as person's age, their address, etc 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, when several users have access to the same merchant account, and multi-user custodianship, when two or more users are required in order to unlock some functions like transfer funds out of the account.
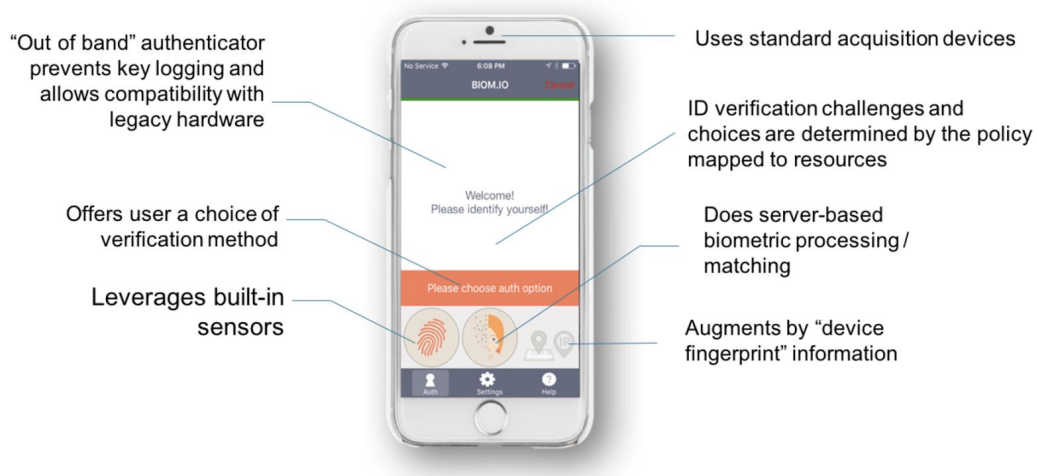
Multi Factor Authentication with Biometrics

GRAFT will implement best-practices, advanced authentication to go along with the user management service, which will include risk / threat analytics based on login/usage pattern as well as device and network characteristics, sophisticated multi-factor based authentication which

will include biometrics, FIDO and other passwordless factors and techniques to identify the user.

The user ID will be given special attention to avoid "lost key" problem, but also to ensure ability to reliably ID the user quickly and in variety of situation. To that end UserID will be comprised of multiple elements (keys) - some tied to devices and hardware tokens, and some to user biometrics - that will jointly provide a base for identifying a user via flexible set of attributes. For example it will be possible to identify the user by a choice of 2 factors out of available ID elements (face, palm, iris, hardware token, device, etc). The unused factors will be used as a pool of factors to verify user's identity.

The ultimate goal is to make user identification and authentication work quickly, reliably, in wide variety of situations, on wide variety of devices; while providing user with choices and that are reflective of user preferences and limitations.

Figure 4: Mobile Multi-Factor Biometric Authenticator is a Part of GRAFT Existing Technologies Portfolio

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 supernodes owners can optionally link their partial identity to their account in order to disclose and improve their

reputation score. Such a link will 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 decision regarding authorization limit 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.

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 which produces easily understandable results on 0-100 scale, which cannot be used to disclose any information about the number, amount, time, or nature of transactions.

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 employees' salaries. Also, they may use fiat to pay refunds in case of return. Most merchants cannot afford high volatility, especially small merchants. GRAFT resolved the volatility problem by instant, real time transaction settlement, which minimizes possible loss of value due to volatility. 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.

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 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 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 payment, 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. GRAFT Foundation or/and service brokers may insure payments up to equivalent of USD $100 and compensate customers or merchants for their lost of funds due to fraud or technical issues.

Privacy

Oftentimes, there is a wrong perception of the need for privacy. In reality, majority of legitimate buyers don't mind disclosing their identity to the merchant, especially, if they benefit from such disclosure, or such disclosure is necessary to process 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 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 code 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 identity attributes authenticity by the merchant in lots of cases.

We find that the best way to approach this problem is 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 which calls for differentiated identity proofing and authentication.

GRAFT implements digital identity profile which is attached to GRAFT wallet, with ability to share the data from the digital identity with the counter-party incrementally and based on user permissions at the time of the transaction. These permissions include sharing certain attributes (such as age, home location, address, name, etc..) selectively and per transaction.
GRAFT implements CryptoNote[21] as an underlying transaction recording protocol which provides a high degree of privacy comparing to Bitcoin, other cryptocurrencies, and cryptographic tokens by hiding information about sender and receiver.

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 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 graftcoins, bitcoins, altcoins, and credit/debits 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 graftcoins, bitcoins, altcoins, and credit/debit cards (by using instant exchange brokers), and sending and receiving transfers in graftcoins.
- 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 look-up secrets, which can be used for at-the-terminal authentication. GRAFT Foundation and service 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 customs 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 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. 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.
7. NIST Special Publication 800-63. Revision 3. Digital Identity Guidelines. NIST (2017). https://pages.nist.gov/800-63-3/sp800-63-3.html.
8. IOTA. https://iota.org/.
9. Median Confirmation Time. Blockchain. https://blockchain.info/charts/median-confirmation-time?timespan=30days.
10. 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.
11. Square. https://squareup.com/reader?utm_medium=affiliate&utm_source=phg&utm_term=1100l4dN2S2g.
12. PayPal. https://www.paypal.com/us/webapps/mpp/merchant-fees.
13. Bitcoin, Ethereum, Litecoin, Dash, Monero Avg. Transaction Fee historical chart. Bitcoincharts. https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y.

14. Average Confirmation Time. Blockchain. https://blockchain.info/charts/avg-confirmation-time?timespan=30days.
15. Median Confirmation Time. Blockchain. https://blockchain.info/charts/median-confirmation-time?timespan=30days.
16. First transaction using instant send took 10 mins. Dash. https://www.dash.org/forum/threads/first-transaction-using-instant-send-took-10-mins.12880/.
17. Visa Inc. at a Glance. Visa. https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.
18. Scalability. Bitcoin Wiki. https://en.bitcoin.it/wiki/Scalability.
19. MONERO. Private Digital Currency. https://getmonero.org/.
20. 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.
21. CryptoNote. https://cryptonote.org/.