Graft

Decentralized Global Merchant Payment Processor

Slava Gomzin Dan Itkis

Version 0.02

Table of Contents

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. 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 traditional electronic payment systems such as credit, debit, and prepaid cards, 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" - very secure 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).

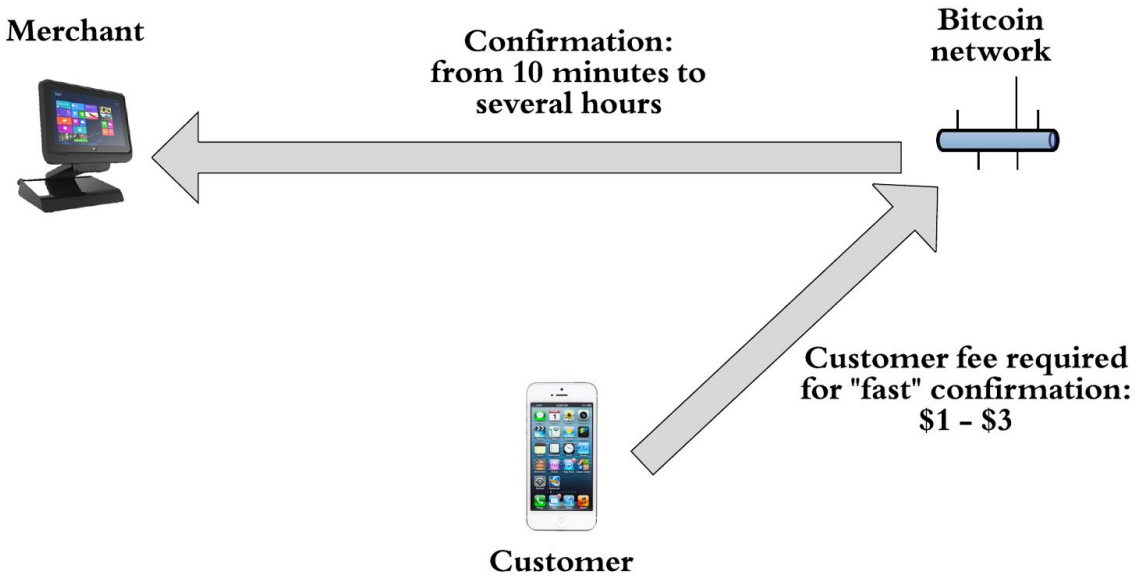

Figure 1: Bitcoin Transaction Processing without Centralized Intermediary

Even though some existing cryptocurrencies[2] have improved confirmation times, they are still unable to process essential transactions types such as authorization and completion, which 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 processor, which is typically a centralized commercial organization regulated by government and controlled by shareholders, as an element of crypto payment transaction contradicts the fundamental principles of cryptocurrencies: decentralization, privacy, and independence.

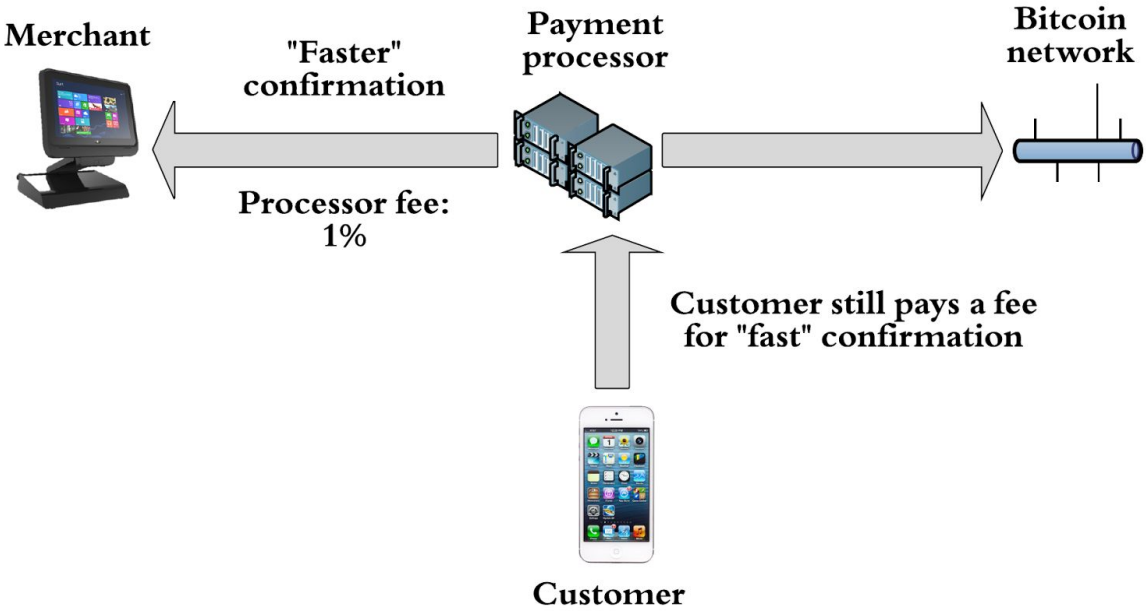

Figure 2: Processing Bitcoin Transaction by Centralized Intermediary

Most merchants are unable to accept cryptocurrencies without third-party payment processor due to uniqueness of the way blockchain networks process transactions, which is conceptually different from traditional electronic payment methods such as payment cards or Paypal. Although the overall concept of plastic card payments may have been outdated, there are technologies developed around them that accumulated enormous amount of merchant experience and user trust which cannot be abandoned overnight. Those technologies include real-time authorization protocols and smart cards.

There are several major differences between the ways traditional and cryptocurrency payment systems handle transactions, which in most cases make cryptocurrencies less attractive for merchants and/or consumers. Here is the list of technical limitations and

business flaws of the existing cryptocurrencies comparing to traditional electronic payments:

- 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 addressing all those issues, Graft elevates crypto payment processing to a new level, and makes possible their wide acceptance by mainstream merchants and consumers for the first time without violating the fundamental principles of cryptocurrencies. Let's review each of those issues with greater detail and see how Graft addresses them.

The Value of Decentralized Payment Processing

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

While the answer to the first part of this question may consists of several elements as there might be multiple reasons (and combinations of them) to individuals to keep their money in a form of cryptocurrency, the answer to the second part of this question is relatively simple. Merchants always want to extend their customer base to increase their revenues, and if they identify a significant group of potential customers who prefer, for any reason, to use cryptocurrency, they will start accepting cryptocurrency. And Graft provides a unique opportunity for merchants to accept crypto payments from their buyers without any middlemen and with near zero fees.

However, there may be additional value. In some cases, merchant might want to know the real identity of the buyer in order to comply with laws and regulations, for example, to make sure the buyer is older than 21 to be allowed to purchase some items.

Since Graft is both decentralized payment processor and cryptocurrency, it is able to facilitate the full payment cycle without other cryptocurrencies or assets involved. However, in addition to decentralization and right for privacy, there is a freedom of choice which is another important fundamental liberal principle. Moreover, there might be a commercial need for diversity of cryptocurrencies for both buyers and merchants. Therefore, Graft will support Bitcoin and several major cryptocurrencies 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, and 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 due to their slower confirmation times and higher transaction fees.

Terminology

Graft

1. **G**lobal **R**eal-time **A**uthorizations and **F**und **T**ransfers - 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 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. Why would anyone go to all this trouble of attaching two bits of plants together? Well, it turns out that this technique has a lot of benefits. Growers can choose different parts of plants that have particular attributes, and attach them to other plants. Let's say a certain tree has really strong roots, but its fruit isn't so great. This tree would make great rootstock, or a plant selected for its roots. It can be combined with another tree that doesn't have good roots, but produces wonderful fruit. Plants that are selected for their stems, flowers, or fruit are called the scion. A desirable scion can be grafted onto a strong rootstock to create a truly great tree. This is pretty common practice in the gardening industry. It allows for plants to grow in many new areas, and gives us access to more products.[5]

Supernode

Independant always-on server running implementation of Graft Blockchain node and Graft DAPI, and maintaining the blockchain via block mining, processing of real-time authorization and settlement DAPI calls between buyers and merchants, and hosting additional services such as instant cryptocurrency exchange, credit/debit card acceptance, and merchant payouts in local currency.

Service Broker

Graft protocol extension hosted on 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 independant "merchant account" where merchants can set up authorization and payout rules and triggers that will have an affect on transactions for that specific merchant.

Graftcoin

Native cryptocurrency supported by Graft blockchain and used for real-time payment authorizations, funds transfers, and settlement between buyers and merchants.

DAPI

Decentralized stateless API implemented by supernodes in order to support lightweight client apps such as 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, or credit/debit cards by calling Graft DAPI.

Graft Point of Sale

“Lite” desktop and mobile apps that allow merchants accepting 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 network. So who is going to maintain these servers, and what's the motivation and incentive for maintaining the blockchain node? In Bitcoin and other cryptocurrency 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 the acceptance widens and usage increases. As the system get 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, the cryptocurrency should 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 transaction is completely free, one can move the same amount

between two accounts indefinitely. Second, to become the only incentive for node operators after the mining bonus becomes too small.

Charging the Wrong Guy

The problem with Bitcoin and other cryptocurrencies' fee is that they charge the wrong side of the transaction. It's even worse than traditional card payments because unlike plastic payments, both buyer and merchant pay fees for cryptocurrency transaction: the buyer pays to the cryptocurrency network, while the merchant pays to the payment processor.[9] The (average/layman) payer is often confused by the process which looks more like a betting, without clear explanation of the fee schedule, which obviously does not make cryptocurrency 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 (in cryptocurrencies world) approach to transaction fees.

Graft Transaction Fees

Graft reintroduces convenient fee structure with no fees for the payer so all fees are paid by the receiver (merchant), just like everyone used to do with traditional electronic methods of payment. Graft makes micropayments accessible to everyone by setting very low (comparing to credit cards[11] and online payment processors,[12] and other cryptocurrencies[13]) fees, but without fixed fee component (Table 1). All fees are paid by the payees.

Table 1: Graft Network Transaction Fees

Micropayments (less than 10 GRF)	0.1%
Regular Payments (more than 10 GRF)	1% of $\log_{10}$ (significantly less than 0.1% as transaction amount grows)

The logarithmic fee schedule allows creating 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 GRF	0.00001 GRF	0.1%
1 GRF	0.001 GRF	0.1%
10 GRF	0.01 GRF	0.1%
50 GRF	0.01699 GRF	0.03398%
100 GRF	0.02 GRF	0.02%
1,000 GRF	0.03 GRF	0.003%
1,000,000 GRF	0.06 GRF	0.000006%

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 at the time of merchant sign-in for the

broker service. Those fees are always charged to the merchant at the time of transaction settlement (payout), i.e. there are no any setup, upfront, or periodic fees.

Customer Fees

Some cryptocurrencies such as Bitcoin require customer to add transaction fee in order to get fast confirmation. 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, transactions fees can be charged using special "margin" balances provided by Graft network itself or/and 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 crypto payment system cannot rely solely on small individual nodes hosted on personal computers but rather should be based on dedicated powerful *supernodes* hosted by professionals, with thin clients apps connected to a *quorum* - a group of supernodes randomly selected by special fraud-prevention algorithm - via DAPI calls.

Confirmation Time: Introducing Real Time Authorizations

Long confirmation time[14] (from several minutes to several hours, depending on transaction fee[15]) is one of the main reasons for low adoption of cryptocurrencies in retail and hospitality sectors where customers cannot wait and so merchants must process payment instantly. 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 (less than 3 seconds), without charging an extra fee or compromising the principle of decentralization (see Figure 3).

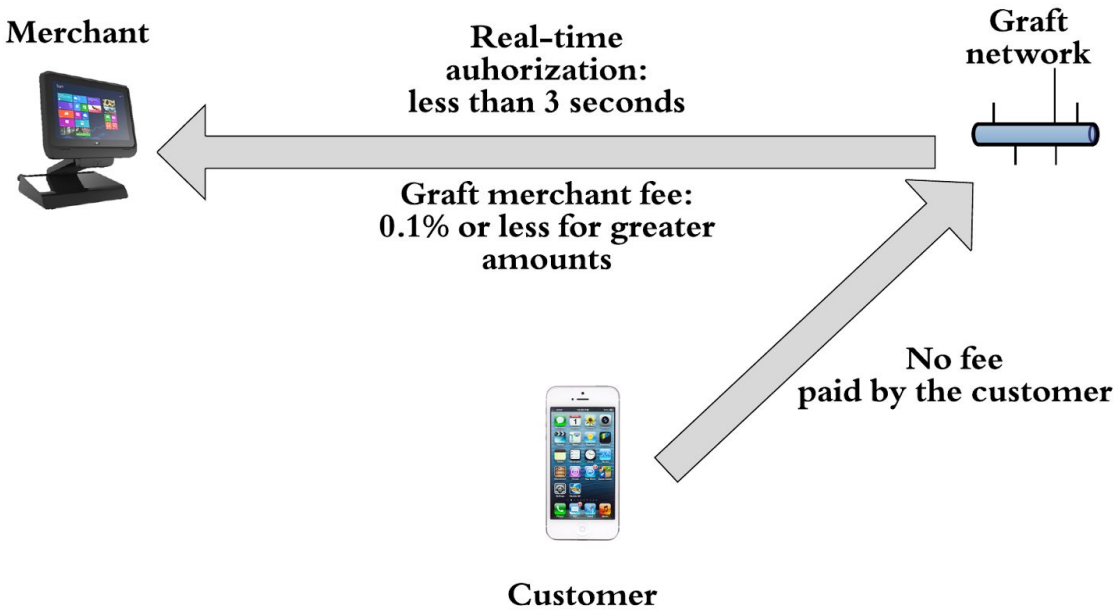

Figure 3: Simplified Graft Payment Flow

This is achieved through using a consensus of always-on trusted *supernodes* with ability to perform a distributed instant authorization lock on input account and communicate response back to the client 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 (less than 3 seconds). All the fees are paid by the receiver (merchant) to the supernodes participating in quorum and (optional) service brokers participating in transaction processing. Supernodes are responsible for both blockchain maintenance (mining blocks) and transaction processing. The owners of the nodes are financially responsible for transactions they process. Such responsibility is achieved by financial interest: mining fees, transaction fees, and collateral paid to escrow service brokers. In case of problem caused by the supernode, the funds from collateral will be available for compensation.

DAPI

Unlike regular API, which is hosted at server or server farm, DAPI does not have a single address as it is running on thousands 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 randomly selected addresses. However, the client app is free to select particular supernode and "stick" with it. For example, merchants can decide to host its own supernode which they trust most.

Scalability

Scalability of payment network 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 Bitcoin network is restricted to a sustained rate of only 7 tps.[18]

Some of the measures that can be used to ensure higher scalability are decreasing the block creation interval to 2 minutes and removing the size limit of the block, so the transactions blocks are created more often, and each block can accommodate more transactions. Such measures are not unique and already implemented by other cryptocurrencies.[19] Unlike other networks, however, Graft 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 picks of requests associated with seasonal and other changes in buyers and merchants activities.

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

This is analogue to debit card authorization. Authorize is initiated by the merchant and confirmed by the payer. 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.

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.

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 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 Graftcoins as a Payment Method

Unlike Bitcoin and other cryptocurrencies, 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 Redeem of 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, Graft payment transaction can take various convertible cryptocurrencies 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) will be applied accordingly in addition to standard Graft transaction fees. Those fees will be invisible for the buyer 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 ecosystem 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 or credit/debit card, Graft network will automatically exchange other cryptocurrency or convert credit card payment in local fiat currency into graftcoins 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 or credit card as a method of payment, the supernode quorum 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 graftcoin, 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 still highly demanded by consumers and merchants, Graft introduce 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 which can compete by offering to merchants and customers better services and lower fees. Merchants can choose a single (for example, highly trusted or least expensive) service broker, or a group of brokers. This way both buyer and merchant will received all the services they need while still keeping some grade of decentralization.

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
- Identify Verification Broker

Accept Broker enables accepting payment methods different from native graftcoins and immediately convert the payment amount into graftcoins 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

Merchant can decide to receive their proceeds from transactions in other cryptocurrency such as Bitcoin or local fiat currency. In this case, the output 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 quorum 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, 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, Store Credit redemption	N/A	None (Graft network)	N/A (Margin Broker might be needed to cover transaction fee)	None
graftcoins	USD	None (Graft network)	Bank Transfer Payout Broker, PayPal Payout Broker	Payout Broker fee
graftcoins	bitcoins	None (Graft network)	Bitcoin Payout Broker	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
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 broker 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, 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 or cryptocurrency. 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 or cryptocurrency using its current market value.

Offline Transactions

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

Crypto payments, however, assume that network is available 24/7, and there are no downtimes, which 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 app and single supernode are able to process offline crypto transactions based on the same principle, if they cannot communicate to the quorum and get consensus, and the merchant is ready to take a risk. The decision about offline approval will be also based on buyer's and supernode's reputation scores.

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. This is happened with payment card, which were not designed with security in mind, but it will not supposed to happen with cryptocurrencies, as they were designed to be resilient to most types of attacks.

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 will 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 a quorum necessary for authorization. If one of the quorum supernodes is down it is automatically replaced by another one from the quorum candidate list which contains redundant 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

In the existing cryptocurrencies authentication / authorization has been the purview of the user application such as wallet, and has 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 seller 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[21] in the US). Conversely, buyers purchasing goods on an after-market, might want to protect themselves from buying stolen goods by requesting that the seller provide higher level of identity proofing.

Graft expects the client applications to comply with identity verification standards relevant to the jurisdictions.. 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.

Two 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.

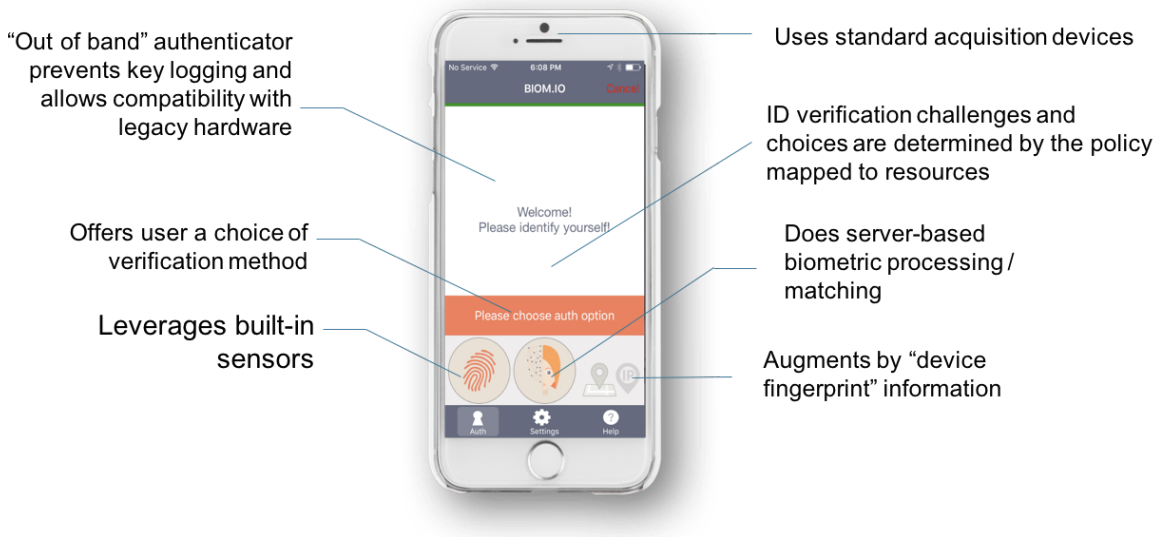

Figure 3: Mobile Multi-Factor Biometric Authenticator is a Part of Graft Existing Technologies Portfolio

Reputation Score - Illuminate the Darkness

Graft take 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. The buyer can review the merchant's reputation score before making payment for the 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 dollars (or their local currency). Merchants use fiat currency, not bitcoins or other cryptocurrencies, to replenish stock and pay their bills and employees' salaries. Also, they may use fiat to pay refunds in case of return. They 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 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 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 will 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 to disclose their identity to the merchant, especially, if they benefit from such disclosure, or such disclosure is necessary to process transaction. In the same way, the buyers want to make sure that the merchant they send payment to is the right person or organization and not just their 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 crypto currencies 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[22] as an underlying transaction recording protocol which provides a high degree of privacy comparing to Bitcoin and other cryptocurrencies 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 who 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. Another solution is connecting to supernodes via remote VPN or/and TOR network. For this purpose, supernodes will be accessible through TOR.

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 cryptocurrencies. Using most recent technologies developed by crypto 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. https://squareup.com/reader?utm_medium=affiliate&utm_source=phg&utm_term=1100l4dN2S2g.

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

13. https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y.

14. https://blockchain.info/charts/avg-confirmation-time?timespan=30days.

15. https://blockchain.info/charts/median-confirmation-time?timespan=30days.

16. https://www.dash.org/forum/threads/first-transaction-using-instant-send-took-10-mins.12880/.

17. https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.

18. https://en.bitcoin.it/wiki/Scalability.

19. https://getmonero.org/.

20. https://www.giftcards.com/gcgf/open-loop-versus-closed-loop-gift-cards.

21. https://pages.nist.gov/800-63-3/sp800-63-3.html.

22. https://cryptonote.org/.