Graft

Decentralized, Real-time Kredit, Debit, at Crypto Payment Processing Network

Slava Gomzin, Dan Itkis

Version 1.02

Agosto 2017

Talaan ng mga Nilalaman

Relay Supernodes

Supernode Rewards

Scalability

Offline Transaksyon Approvals

Uri ng Transaksyon at Flows ng Payment

Processing ng mga Transaksyon sa Graftcoins bilang Paraan ng Payment

Alternatibong Paraan ng Payment sa Processing ng mga Transaksyon

Service Brokers

Merchant Payouts

Open Loop at Closed Loop na mga Produkto: Gift Certificates, Loyalty Rewards, at Store Kredits

Merchant (Domain) Tokens

Desentralisadong Crowdfunded Kredit Kards

Security

Availability

Identity Management

Identification, Authentication, at Authorization

Identity Proofing

Dalawang Factor Authentication na may Biometrics

Reputation Score - Illuminate ang Kadiliman

Pabagu-bago

Customer Support, Dispute Resolution, at Payment Insurance

Privacy

User Applications

Kongklusyon

References

Abstract

Graft ay global, open-sourced, blockchain-based, desentralisadong payment gateway at processing platform na maaaring magamit ng sinuman. Anumang bumibili at merchant ay maaaring gamitin ang kompletong desentralisado at murang paraan ng Graft. Graft ecosystem ay open kaya sinuman ay maaaring lumahok sa pamamagitan ng pagpapanatili ng Graft blockchain at implementing network services.

Graft ay gumagamit ng payment processing protocols at flows tulad sa tradisyonal electronic payment systems tulad ng kredit, debit, at prepaid kards, na familiar at pinagkakatiwalaan narin ng milyong users at merchants sa buong mundo. Itong approach ay nagbibigay ng mas madali at mas mabilis na adoption ng Graft bilang mainstream payment platform, habang tinatanggal ang kailangan sa centralized intermediaries (payment gateways at processors) na kasalukuyang kinakailangan para mapabilis ang mga transaksyon sa pagitan ng bumibili at merchants.

Background

Bitcoin[1] ay nilikha bilang “online cash” – napaka ligtas pero relatibong mabagal ang settlement system na hindi kayang palitan ang payment kards online o makipagkompetensya sa kapwa plastic kards at papel na pera sa brick-at-mortar stores. (Figure 1).

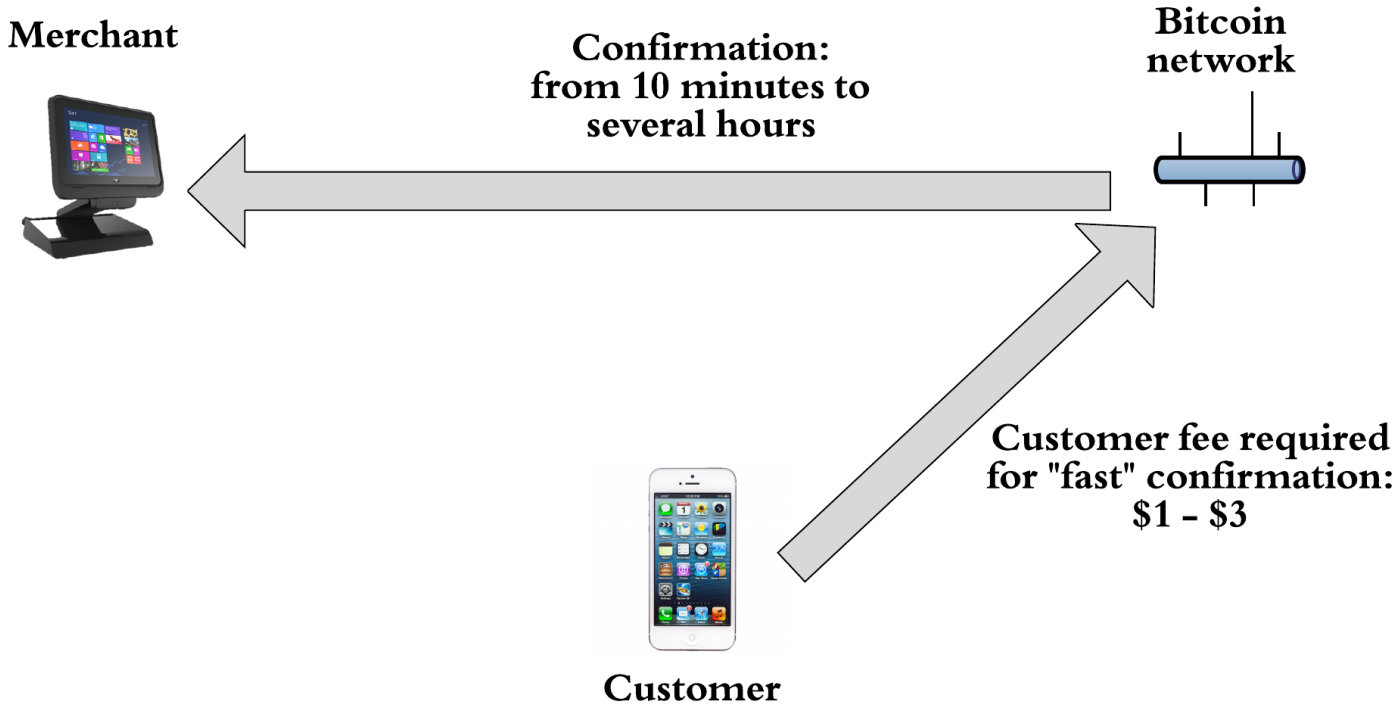

Figure 1: Bitcoin Transaksyon Processing ng walang Centralized Intermediary

Kahit ang ilang kasalukuyang cryptocurrencies [2] ay nag-improve ang confirmation times, sila ay hindi parin kayang magprocess ng kinakailangang uri ng mga transaksyon tulad ng authorization at completion, na ginawa ang kanilang adoption ng retail, hospitality, at convenience store industriya na imposible ng hindi gumagamit ng intermediaries – payment processors at gateways [3] – na pinunan ang gap (Figure 2). Gayonman, ang pinaka existence ng payment processor, na typically centralized commercial organisasyon regulated sa pamamagitan ng gobyerno at kontrolado ng shareholders, bilang element ng crypto payment transaksyon ay kasalungat ang fundamental principles ng cryptocurrencies: desentralisasyon, privacy at independence.

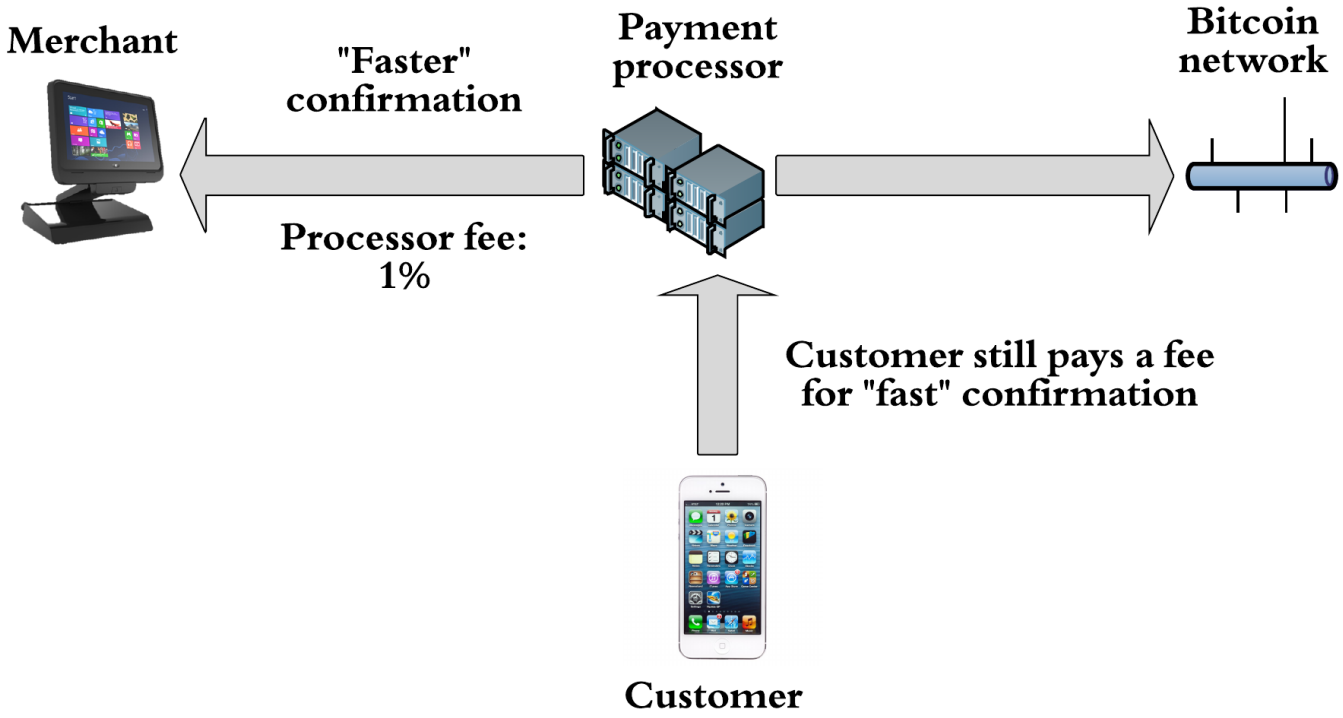

Figure 2: Processing Bitcoin Transaksyon sa Pamamagitan ng Centralized Intermediary

Halos lahat ng merchants ay hindi tinatanggap ang cryptocurrencies ng walang third party payment processor dahil sa kakaibang paraan ng pagprocess ng blockchain networks sa transaksyon, na conceptually iba sa paraan ng tradisyonal electronic payment tulad ng payment kards o Paypal. Bagamat ang kabuuang konsepto ng plastic kards payments ay outdated na, ito ay meron paring teknolohiyang dinivelop sa kanila na nakaipon ng malaking karanasan ng merchant at tiwala ng user na hindi ma-abandon overnight. Ang mga teknolohiyang iyon include ang real-time authorization protocols at smart kards. May ilang major na pagkakaiba sa pagitan ng paraan ng paghahawak ng mga transaksyon ng tradisyonal at cryptocurrency payment systems, na sa halos lahat ng kaso ay ginagawa ang cryptocurrencies na mas less attractive sa merchants at/o konsumers. Ito ang list ng teknikal limitasyon at business flaws ng kasalukuyang cryptocurrencies kompara sa tradisyonal electronic payments:

- Kawalan ng Essential na Uri ng Transaksyon
- Hindi Angkop na Payment Flows
- Mahabang Confirmation Times
- Hindi balanse at hindi mapredict na Bayad sa Transaksyon
- Walang kakayahan na Iprocess ang Micropayments at Paulit-ulit na Charges (Subscriptions)
- Kawalan ng Offline Transaksyon support
- Mababang Scalability
- Pabagu-bago
- Hindi Kompletong Security
- Kawalan ng Privacy Dahil sa Traceability sa Blockchain
- Kawalan ng Tiwala sa pagitan ng Bumibili at Merchant
- Questionable Utility
- Mahirap Gamitin ng End-User Interfaces
- Kawalan ng Kustomer Support

Sa pamamagitan ng pag-address sa lahat ng mga isyu, Graft elevates crypto payment processing sa bagong lebel at sa unang pagkakataon ay ginawang posible ang malawak na pagtanggap ng mainstream merchants at konsumers ng walang nilalabag sa

fundamental principles ng cryptocurrencies. Suriin natin ng mas detalyado ang mga isyung iyon at tignan kung paano iaddress ng Graft.

Ang Halaga ng Desentralisadong Payment Processing

Bakit gustong simulang gamiting ng bumibili ang cryptocurrency sa halip ng (o dagdag sa) plastic kards o Paypal o Apple Pay, at bakit gustong tanggapin ng merchant ang cryptocurrency dagdag sa (sa halip ng) kasalukuyang paraan ng payment? Obviously, kung hindi natin mahanap ang tamang mga sagot sa simpleng mga tanong, ay walang point na gawin ang dokumentong ito.

Habang ang sagot sa unang parte ng tanong na ito ay maaaring consists ng ilang elements dahil may maraming kadahilanan (at kombinasyon nila) sa indibiduwal para panatilihin ang kanilang pera sa form ng cryptocurrency, ang sagot sa pangalawang tanong ay relatibong simple. Merchants ay laging gustong iextended ang kanilang kustomer base para mapalaki ang kanilang kita, at kung may naidentify silang malaking grupo ng potensyal kustomers na mas gustong gamiting ang cryptocurrency sa anumang dahilan, sila ay magsisimulang tanggapin ang cryptocurrency. At Graft ay magbibigay ng kakaibang opurtunidad para sa merchants na tanggapin ang crypto payments mula sa mga bumibili sa kanila ng walang anumang ahente at halos walang bayad.

Gayonman, maaaring may dagdag na halaga. Sa ilang mga kaso, merchant ay maaaring gustong malaman ang tunay na identity ng bumibili para makapagcompy sa batas at regulations, halimbawa, para siguraduhin ang bumibili ay mas matanda sa 21 para payagan ng bumili ng ilang mga bagay.

Dahil ang Graft ay kapwa desentralisadong payment processor at cryptocurrency, kaya nitong mapabilis ang full payment cycle ng walang cryptocurrencies o assets na kasama. Gayonman, dagdag sa desentralisasyon at karapatan sa privacy, isa pa sa importanteng liberal principle ay ang kalayaang pumili. Dagdag pa doon, ay merong pang commercial na kailangan para idiversify ang cryptocurrencies sa kapwa bumibili at merchants. Kung ganun, Graft ay susuportahan ang Bitcoin at ilang major cryptocurrencies bilang dagdag na pagpipilian ng bumibili at tatanggapin paraan ng pagbabayad ng merchants. Ang feature na ito ay babawasan ang kailangan ng merchant para iintegrate sa maraming (centralized) payment software providers, at para sa user na mag sign up para sa centralized services at matuto at panatilihin ang maraming wallet apps. Ito ay importanteng inote na ang

merchants ay iaaccommodate ang mas mataas na risks at dagdag na gastos kaugnay sa pagtanggap ng alternatibong cryptocurrencies dahil sa mas mabagal na confirmation times at mas mataas na bayad sa transaksyon.

Terminology

Graft

1. **G**lobal **R**eal-time **A**uthorizations at **F**und **T**ransfers – desentralisadong global open platform para sa processing real-time authorizations at settlements ng merchant payments at fund transfers gamit ang hindi matrace na blockchain, desentralisadong API, at open na komunidad ng service brokers na susuporta sa ibat-ibang payment at paraan ng payout including cryptocurrencies at tradisyonal kredit kards at bank transfers.

2. Ang halaman na may sanga o sibol mula sa ibang halaman nakadikit dito kaya sila ay magkaugnay at magkasamang lalaki. [4] Grafting ay ang advanced teknik na ginagamit ng botanists, mga magsasaka, mga hardinero at hobbylists para dagdagan ang nabubuhay na tissue mula sa isang halaman sa isa pang halaman. Bakit gusto nilang pumunta sa lahat ng kapahamakang ito para pagsamahin ang dalawang halaman? Itong teknik kasi na ito ay maraming mabuting pakinabang. Growers ay maaaring pumili ng ibang parte ng halaman na may particular na katangian, at pagsamahin sila ng ibang halaman. Sabihin natin na ang isang puno ay may malakas na ugat pero ang bunga ay hindi ganong kaganda. Ang punong ito ay makakagawa ng mahusay na rootstock, o halamang pinili sa ugat nito. Ito ay maaaring icombine sa ibang puno na walang magandang ugat pero nakapagbibigay ng kahanga-hangang bunga. Ang mga halaman na pinili sa kanilang tangkay, bulaklak o bunga ay tinatawag na scion. Ang kanais-nais na scion ay maaaring grafted sa malakas na rootstock para makagawa ng totoong mahusay na puno. Ito ay karaniwang magandang practice sa gardening industriya. Ang mga halaman ay pinapayagan para lumaki sa maraming bagong areas, at nagbibigay sa atin ng access sa maraming mga produkto. [5]

Supernode

Independant laging-on server running ang pinagsamang implementation ng Graft blockchain node at Graft DAPI node, pinapanatili ang blockchain via block mining, processing ng real-time authorization at settlement DAPI na tawag sa pagitan ng mga bumibili at merchants, at hosting ng dagdag service tulad ng instant cryptocurrency exchange, pagtanggap ng kredit /debit kard, at merchant payouts sa lokal na salapi. Supernode ay pananatilihin ang network gamit ang pinagsamang PoW/PoS algorithm.

Authorization Sample

Ang napiling grupo ng pinagkakatiwalaang supernodes na mag-aapprove ng payments sa real-time at guarantee na ang bumibili ay hindi kayang gastusin ang parehong pera ng higit sa isa bago sinulat ang transaksyon sa blockchain.

Relay Supernode

Ang supernode na nagpapabilis ang transaksyon ng merchant sa pamamagitan ng pagcommunicate sa merchant POS o/at sa isang panig ang wallet ng bumibili, and sa ibang panig ang natirang authorization sample supernodes.

Service Broker

Graft protocol extension hosted sa supernode o grupo ng supernodes at pagmamay-ari ng supernode operator. Service Brokers implement ng espesyal na dagdag na katangian na hindi awtomatikong executed ng fully desentralisadong network o/at kinakailangan ng espesyal na regulation framework tulad ng PCI DSS[6[o NIST 800-63-3. [7] Mga halimbawa ng service brokers ay kredit kard payment acceptance broker at bank payout transfer broker.

Domain

Virtual desentralisadong independent “merchant account” kung saan ang merchants ay maaaring mag set-up ng authorization at mga alituntunin ng payout at triggers na makakaapekto sa mga transaksyon para sa specific merchant.

graftcoin

Native cryptocurrency sinusuportahan ng Graft blockchain at ginagamit sa real-time payment authorizations, funds transfers, at settlement sa pagitan ng mga bumibili at merchants.

DAPI

Desentralisadong stateless API implemented sa pamamagitan ng supernodes para suportahan ang lightweight client apps tulad ng Graft Wallet, Graft Point of Sale, at third party point of sale apps at shopping kards. Graft SDK Source code ay nagbibigay sa third party point of sale at wallet application vendors para mapabilis ang integration sa Graft.

Graft Wallet

“Lite" desktop, mobile, at browser extension apps na pinapayagang gumawa ng payments at fund transfers gamit ang graftcoins, ibang major cryptocurrencies, o kredit/debit kards na tinatawag na Graft DAPI.

Graft Point of Sale

“Lite” desktop at mobile apps na pinapayagan ang merchants na tanggapin ang payments sa graftcoins, bitcoins, altcoins, o kredit/debit kards; pag-isyu at pag redeem ng gift certificates, loyalty reward points, at store credits; configure settlement payouts sa graftcoins, bitcoins, altcoins, o lokal fiat na mga salapi.

Bayad sa Transaksyon

Bakit nga ba kailangang magkaroon ng bayad sa transaksyon? Pagkatapos ng lahat, wala naming commercial enterprise sa likod ng blockchain, so bakit kailangang magbayad ang users, sino ang mangongolekta sa kanila, at magkano ang charge sa kanila?

May Bayad o Walang Bayad

Maraming makapangyarihang nodes (servers) distributed sa buong mundo ay kinakailangan para suportahan ang ligtas at mataas na available cryptocurrency network. Kaya sino ang magpapanatili ng mga servers na ito, at ano ang motivation at incentive sa pagpapanatili sa blockchain node? Sa Bitcoin at ibang cryptocurrency networks, ang funding ay makakamit sa pamamagitan ng mining at bayad sa transaksyon – ang may-ari ng node ay makakaroon ng pera sa mining ng bagong coins mula sa bawat block ganundin sa pagkuha ng bayad sa bawat transaksyon.

Ang mining ay meron pang ibang layunin: constant at steady injection ng bagong coins sa system para panatilihin ang madaling palitan sa paglaki ng demand sa extra coins dahil ang acceptance ay lumalaki at tumataas ang paggamit. Kapag ang system ay makakuha ng traction, ang node operators ay makakakuha ng mas maraming kita mula sa bayad sa transaksyon, kaya ang bonus sa mining ay maaaring paunti-unting bumaba sa bawat block para ilimit ang kabuuang supply.

Sa ideal na mundo, ang cryptocurrency ay dapat available sa lahat at libre. Sa totoo lang, merong networks na nangangako ng libreng transaksyon. [8] Sa ibang networks, kasama ang Bitcoin, ang bayad ay ginagamit para iprioritize ang transaksyon at “resolbahin” problema sa scalability.

Gayonman, sa Graft network, ang bayad ay ginagamit sa dalawang dahilan. Una, para maiwasan ang network abuse at associated performance at isyu sa laki ng blockchain. Halimbawa, ang paggamit ng totoong network para sa testing. Kung ang transaksyon ay kompletong libre, ang isa ay maaaring maglipat ng parehong halaga sa pagitan ng dalawang accounts ng walang katapusan. Pangalawa, para lamang maging incentive sa node operators pagkatapos ng maging napakaliit ng mining bonus.

Charging ng Maling Lalaki

Ang problema sa bayad sa Bitcoin at ibang cryptocurrencies ay nagchacharge sila ng maling panig ng transaksyon. Mas malala pa ito kaysa sa tradisyonal kard payments dahil hindi tulad ng plastic payments, ang kapwa bumibili at merchant ay nagbabayad sa cryptocurrency transaksyon: ang bumibili ay nagbabayad sa cryptocurrency network, habang ang merchant ay nagbabayad sa payment processor. [9] Ang (average/layman) payer ay madalas na nalillito sa pamamagitan ng process na mukhang tulad ng pagsusugal, walang maliwanag na paliwanag ng schedule ng bayad, na obviously hindi ginagawang attractive ang cryptocurrency payments.

Micropayments: Paano Ako Magbabayad ng Crypto para sa Isang Tasa ng Kape?

Isa pang problemang kasalukuyang nararanasan ng Bitcoin ay wala itong abilidad na humawak ng micropayments dahil sa mataas ang bayad sa transaksyon. [10] Graft ay reresolbahin ang problemang ito sa pamamagitan ng pagpapakilala ng kakaibang (sa mundo ng cryptocurrencies) approach sa bayad sa transaksyon.

Bayad sa Transaksyon sa Graft

Graft ay pinakikilala muli ang convenient estruktura ng bayad ng walang bayad sa payer sa lahat ng transaksyong binayaran ng tumanggap (merchant), tulad lang ng kung paano gamitin ang tradisyonal na paraan sa electronic payment. Graft ay ginagawa accessible sa lahat ang micropayments sa pamamagitan ng pagset ng napakamababa (kompara sa kredit kards)[11] at online payment processors, [12] at bayad sa ibang cryptocurrencies [13] pero walang fixed na bayad (Table). Lahat ng bababayaran ay binayaran ng payees.

Table 1: Graft Network Bayad sa Transaksyon

Micropayments (mas mababa kaysa sa 10 GRF)	Regular Payments (mas malaki kaysa sa 10 GRF)
0.1%	1% ng log10 (sobrang mas mababa kaysa sa 0.1% kapag tumaas ang halaga ng transaksyon)

Ang logarithmic schedule ng bayad ay pinapayagang lumikha ng incentive para sa processing ng mas mababang transaksyon na maliit ang halaga (i.e. halimbawa pagsasamahin ang maraming transaksyon kung posible) habang pinapanatiling mababa ang bayad sa transaksyon para sa malaking halaga ng transaksyon. (Table 2).

Table 2: Mga halimbawa ng bayad ng Transaksyon sa Graft Network

Halaga ng Transaksyon	Bayad na Halaga sa Transaksyon	Effective na Bayad sa Transaksyon
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%

Halaga ng Transaksyon	Bayad na Halaga sa Transaksyon	Effective na Bayad sa Transaksyon
1,000 GRF	0.03 GRF	0.003%
1,000,000 GRF	0.06 GRF	0.000006%

Libreng Funds Transfers: Authenticated na Transaksyon

Maraming payment networks tulad ng ACH o Paypal ang nagbibigay ng libreng transfer na lumilikha ng malaking incentive sa pagitan ng user accounts kompara sa cryptocurrencies, na nagchacharge ng hindi proportional na bayad ng hindi isinasaalang-alang ang speed at halaga ng transaksyon. Itong katangian na ito ay espesyal na importante sa transaksyon ng may maliit na halaga at mababang priorities, tulad ng funds transfer sa pagitan ng family accounts, o remittance ng sweldo ng mga empleyado. Para makapagkompetensiya sa tradisyonal payment networks, ang Graft ay nagbibigay ng libreng limitadong transfers sa pagitan ng users.

Cryptocurrency networks ay kadalasang hindi “kaya” ang libreng transaksyon dahil sa tatlong dahilan: kawalan ng incentive sa minero, threat ng DOS attacks, at laki ng block. Graft ay reresolbahin ang unang problema sa pamamagitan ng logical separation sa pagitan ng payment at transfer, para ang supernodes (minero) ay makakatanggap ng bayad sa transaksyon sa instant payments ng majority na binubuo ng lahat ng transaksyon, habang ang libreng transfers ay processed na may lower priority. Ang pangalawang problema sa DOS threat ay reresolbahin sa pamamagitan ng boluntaryong user identification at authentication. Syempre, walang libreng lunches, kaya ang users ay dapat “magbayad” sa pamamagitan ng pagbigay ng kanilang identity sa network para masigurado ang reasonable na gamit (sa pamamagitan ng limitasyon sa bilang at frequency ng libreng transfers kada users) at maiwasan ang network abuse. Ang huling problema sa laki ng transaksyon ay reresolbahin sa pamamagitan ng komplikadong measures: maliit na block interval, walang limitasyon sa laki ng block, at standard restricted na laki ng transaksyon para sa particular na uri ng transaksyon tulad ng libreng transfer.

Dagdag na Bayad sa Third Party Service Brokers

Kapag tinatanggap ang ibat-ibang paraan ng payment tulad ng bitcoins, altcoins, kredit/debit kards, o processing merchant payouts sa ibang mga salapi tulad ng bitcoins, altcoins, o lokal na fiat na salapi, ay may dagdag na payment broker at/o bayad sa broker ang pwedeng iapply. Ito ay hindi nakatagong bayad dahil sila ay published ng brokers sa oras na mag sign-in ang brokers para sa broker service. Ang bayad ay laging charged sa merchant sa oras ng transaksyon settlement (payout), halimbawa kapag walang anumang setup, upfront o periodic na bayad.

Bayad ng Kustomer

Ilang cryptocurrencies tulad ng Bitcoin ay kailangang magdagdag ang kustomer ng bayad sa transaksyon para maging mas mabilis ang confirmation. Ang ganung bayad ay configured sa pamamagitan ng wallet application at binayaran ng kustomer. Halos lahat ng Bitcoin users ay already accustomed sa ganung bayad.

Pagbabayad gamit ang Margin Balances

Sa ilang mga kaso, ang bayad sa transaksyon ay maaaring icharge gamit ang espesyal na “margin” balances na binibigay ng mismong Graft network o/at margin brokers. Mga halaimbawa ng ganitong transaksyon ay Isyu at Redeem transaksyon kaugnay sa gift certificates, loyalty rewards, at store kredit processing. Ito ay ginagawa para payagan ang merchant transaksyon processing kahit na ang merchant ay walang sapat na balance sa Graft account.

Transaksyon Processing

Ang mundo ay pupunta tungo sa “thin” devices. Ang mga tao sa mundo ay mas ginagamit ang smartphones at tablets at mas maliit na workstations at laptops. Kung ganun, ang desentralisadong crypto payment system ay hindi maaaring umasa lang sa maliit na indibiduwal nodes hosted sa personal computers pero sa halip ay dapat based sa makapangyarihang dedicated supernodes hosted

ng mga propesyonal, na may thin clients apps connected sa authorization sample - grupo ng supernodes randomly pinili sa pamamagitan ng espesya fraud-preventon algorithm – via DAPI na tawag.

Problema sa Confirmation Time: Ipinakikilala ang Real Time Authorizations

Ang mahabang confirmation time [14] (mula sa ilang minute hanggang sa ilang oras, depende sa bayad sa transaksyon) [15] ay isa sa mga pangunahing dahilan sa mababang adoption ng cryptocurrencies sa retail at hospitality sectors kung saan ang kustomers ay hindi makapaghintay at kaya ang merchants ay dapat iprocess ang payment instantly. Hindi tulad ng ilang cryptocurrency networks na sinubukang resolbahin ang problemang ito sa pamamagitan ng pagpapakilala ng espesyal add-on systems o uri ng transaksyon [6[, Graft ay prinoprocess ang lahat ng transaksyon ito real time (mas mababa sa 3 segundo), ng hindi nagchacharge ng extrang bayad o compromising ang principle ng desentralisasyon. (tignan Figure 3).

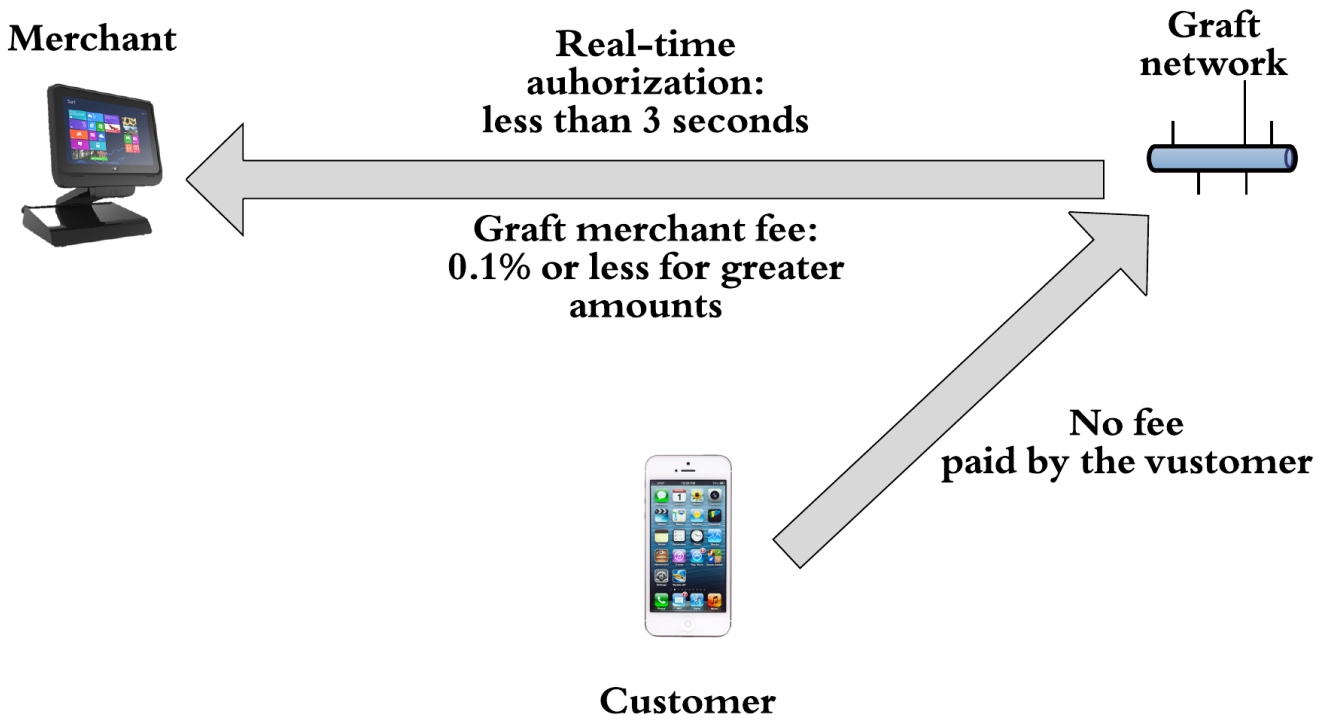

Figure 3: Simplified Graft Payment Flow

Ito ay makakamit sa pamamagitan ng paggamit ng consensus ng lagging pinagkakatiwalaang supernodes (“authorization sample”) na may abilidad na magperform ng distributed instant authorization lock sa account ng bumibili at ibalik ang response sa client sa loob ng millisegundo. Ang supernodes ay pinapanatili rin ang Graft blockchain kaya walang transaksyon ang maaaring authorized “off chain”.

Supernodes

Lahat ng transaksyon ay processed sa pamamagitan ng network na laging-on Graft network nodes – supernodes – sa real time (daan millisegundo sa ilang segundo). Ang bayad sa transakson ay binayaran ng tumanggap (merchant) sa supernodes na lumalahok sa authorization sample at (optional) service brokers na lumalahok sa transaksyon processing. Supernodes ay responsible sa kapwa settlement (block mining) at real-time transaksyon approvals. Ang mga may-ari ng nodes ay responsible sa transaksyong prinoseso nila. Ang ganyang responsilibidad ay makakamit sa pamamagitan ng financial interest: mining rewards at bayad sa transaksyon.

DAPI

Hindi tulad ng regular API, na hosted sa server/server farm, DAPI ay walang isang address dahil ito ay tumatakbo sa maraming supernodes. Anumang isang node ay maaaring iserve ang tawag ng DAPI anumang oras. Ang DAPI tawag ay stateless na ibig sabihin na ang supernodes ay hindi nagpapanatili ng anumang permanenteng session sa client, at lahat ng kinakailangang data sa processing ay instantly distributed at available sa lahat ng nodes. Ang client app na consumes DAPI ay merong list ng supernodes nakikipagcommunicate, na relatibong maliit na grupo ng piniling addresses mula sa authorization sample. Gayonpaman, ang client app ay libreng makapili ng particular pinagkakatiwalaang supernode at “stick” dito. Halimbawa, merchant POS o wallet users ay maaaring magdecide na maghost ng kanilang sariling pinagkakatiwalaang supernode . Kahit nay an ay “private” supernode ay pwedeng hindi migrant ng karapatan para lumahok sa authorization sample dahil sa limitsasyon sa resources (tignan Authorization Sample Selection Algorithm section sa baba) , pero maaari silang magbigay sa mga may-ari ng extra layer ng privacy.

Real Time Approvals sa pamamagitan ng Authorization Sample

May cryptocurrencies na may block (settlement) interval na mas mababa sa 2 minuto. Gayonman, ang pagbabawas ng interval ay hindi parin naresolba ang real-time (“instant”) problema sa authorization. Kahit na may 30 segundong block interval, ay mahaba parin para sa real-ime payaments (kredit kard authorizations ay nasa pagitan ng daang millisegundo sa ilang Segundo), ng hindi

imention ang katotohanan na 1 confirmation (1 block) ay hindi rin sapat para bumaba ag risk ng fork sa malaking halaga. Kaya dagdag na espesyal na teknolohiya ay kinakailangan parin para maresolba ang problema sa real-time authorization. Ang Graft supernode scheme ay reresolbahin ag problemeng ito sa pamamagitan ng *authorization sample*, kapag ang approvals ay inisyu real-time ng napiling grupo ang pinagkakatiwalaang supernodes, na guarantees na ang bumili ay hindi maaaring gastusin ang parehong pera ng higit sa isang beses hanggang ang transaksyon ay settled (naisulat sa blockchain). Ang settlement (mining) ay performed sa pamamagitan ng "underlying parte ng supernode coded, sa loob ng 2 minuto.

Hindi tulad ng halos lahat ng crypto payment sytems, at tulad sa tradisyonal payment systems tulad ng kredit kard processing, Graft payment ay divided sa dalawang phases: authorization at settlement. Tulad ng tradisyonal payment sa mundo, authorization ay nangyayari sa halos malapit sa real time (daang milisegundo, depende sa maraming factors), habang settlement ay performed pagkatapos nun, kadalasan sa loob ng 2 minuto (kompara sa ilang oras at kahit ilang araw sa tradisyonal payment networks).

Authorization Account Lock

Key image ay ang mekanismong ginamit ng Crypto Note para mavalidate ang bagong transaksyon at maiwasan ang pangalawang gastos ng hindi compromising privacy ng nagpadala. Key image ay kakaibang "fingerprint" na nagrerepresenta sa spending address ng bumibili at halaga ng hindi dinidisclose ang anumang detalye tungkol sa bumibili o ang halaga. Ang nature ng key image ay ito ay isa lang pwedeng gamitin, kaya kung may taong sinusubukang gamitin ang parehong key image ng higit sa isa, ito ay signal ng pangalawang gastos attempt. Sa pamamagitan ng pagbibigay ng kakaibang key image para sa upcoming na transaksyon sa network ng supernodes, ang wallet ng bumibili ay temporarily "locks" ang spending "account", kaya walang ibang transaksyon na may parehong key image (halimbawa mula sa parehong account) ay maaaring mangyari hanggang ang locked transaksyon ay settled o tinanggal ang lock. Kung ang bumibili ay susubukang ifinalize ang transaksyon na may key image na iba mula sa unang nagamit sa orihinal lock, ang ganung transaksyon ay irereject rin ng supernodes.

Sa kabilang banda, ang key image ay walang anumang impormasyon tungkol sa bumibili o wallet ng bumibili, na nagbibigay ng absolute security, anonymity at hindi matratrace. Dagdag pa, anumang traces ng communication sa pagitan ng bumibili (wallet app), ang merchant (point of sale app), at ang supernodes (napiling relay at sample supernodes) sa panahon ng authorization phase ay tatanggalin kapag ang transaksyon ay settled (naisulat sa blockchain at confirmed ng 10 blocks).

Authorization Sample Selection

Para makapagperform real time (“instant”) authorizations, Graft network relies sa authorization sample – grupo ng napiling pinagkakatiwalaang supernodes na “nirerepresenta” ang network at ivavalidate ang transaksyon para maiwasan ang pangalawang gastos at isign ang instant approval bago ang transaksyon ay “confirmed” sa pamamagitan ng blockchain (halimbawa bago ito idagdag sa block at ang block ay idadagdag sa blockchain).

Ang authorization sample consists ng 8 supernodes randomly pinili mula sa supernodes na niresolba ang huling 1440 blocks (mula sa kasalukuyang height – 10) o ang napiling node ay naging offline, ang list ay awtomatik na extended at isa pang supernode mula sa “bottom” ng list ay idadagdag sa sample. Isa pang kinakailangan para sa lumahok sa authorization sample ay proof of stake: ang may-ari ng supernode ay dapat magmaintain ng balanse ng collateral sa account kaugnay sa supernode. Ang pinakamaliit na kinakailangang balanse ay recalculated dynamically sa bawat block at tumataas sa bawat block proportionally sa lumalaking supply.

Itong algorithm ay pinapayagan ang pinaka active na supernodes, na constantly papatunayan ang kanilang loyalty sa network sa pamamagitan ng matagumpay na mining, para mapagkatiwalaang iperform ang real time authorizations, habang sinusundan ang ilang degree ng randomization binigay ng Proof of Work algorithm. Itong supernodes ay rewarded rin ng bayad sa transaksyon sa bawat matagumpay real time authorization. Ang bagong supernodes “makakaipon" ng kanilang chance para lumahok sa transaksyon processing sa pamamagitan ng dagdag na mas makapangyarihan at nireresolba ang susunod na block (Bagong supernodes ay makakaipon ng kanilang chance na lumahok sa transaksyon processing sa pamamagitan ng pagdagdag ng mas maraming power at pagresolba sa susunod na block (na generated sa average na 2 minuto).

Ang supernodes na nagpeperform ng matagumpay na mining pero nabigo na iprocess ang real time authorization requests ay hindi isasali ng network mula sa list ng supernode (halimbawa ang blocks na naresolba nila ay hindi tatanggapin ng network para sa period 720 blocks).

Kapag ang bagong transaksyon request ay initiated sa pamamagitan ng merchant point of sale, nag-aasign ito ng kasalukuyang block height na defines ang authorization sample. Ang height ay maaaring incremented habang ang transaksyon ay in progress parin, pero hindi pinalitan ang sample height na initially assigned sa transaksyon request. Ang merchant relay supernode na initially

formats ang transaksyon requests ay pipili ng sample supernodes, pero itong selection ay ivavalidate ng bawat miyembro ng sample plus ang wallet's relay.

Para mapabili ang authorization process, ang merchant point of sale app ay maaaring iinstruct ang authorization sample supernodes para iignore ang responses mula sa naiwan ng authorization sample kapag natanggap na nito ang higit sa 50% ng approved responses mula sa "pinakamabili" na supernodes at zero rejected responses; gayonman, ang node na ito ay tumataas ang risk ng fraud, na maaaring tanggapin sa specific na mga kaso ng micropayments kapag ang transaksyon processing speed requirements ay napakaimportante.

Relay Supernodes

Anumang relay supernode mula sa authorization sample ay maaari isang *relay* supernode rin – ang isang nagpapabilis ng merchant transaksyon sa pamamagitan ng communicating sa merchant POS o/ at ang wallet ng bumibili sa isang panig, at ang natirang authorization sample supernodes sa ibang panig. Ang relay supernode ay maaaring piliin randomly sa pamamagitan ng point of sale o wallet mula sa kasalukuyang authorization sample linked sa transaksyon. Merchant o wallet ay maaaring pumili ng anumang supernodes na hindi parte ng authorization sample. Sa totoo lang, merchant o wallet ay maaaring ihost ang kanilang sariling supernodes kapag sila ay seeking ng extra layer ng security at privacy, at potentially makaipon ng kita mula sa mining at transaksyon processing. Gayonman, ang relay nodes ay hindi makakakuha ng anumang rewards o bayad kung hindi sila nakasama sa authorization sample.

Supernode Rewards

Ang bawat supernode sa authorization sample ay makakatanggap ng share sa bayad sa transaksyon sa bawat transaksyon na signs (approve). Ang bawat supernode sa sample ay makakatanggap ng 1/n ng bayad sa transaksyon, kung saan ang n ay ang bilang ng supernodes sa authorization sample. Itong byad ay binabayaran ng recipient (merchant).

Ang block mining reward ay babayaran sa supernode na nagsolve ng bagong block. Ang block reward ay paunti-unting babawasan ng bawat bagong block gamit ang sumusunod na formula: $(M - A) * 2^{-19} * 10^{-12}$, kung saan A = kasalukuyang sirkulasyon, M =

kabuuang supply ($2^{64} - 1$) sa atomic units (10^{-12}). Ang ideya sa likod nito ay sa hinaharap ay magkakaroon ng mas maraming transaksyon na sisiguruhin ang sustainable na kita mula sa bayad sa transaksyon.

Scalability

Scalability ng payment network ay ang abilidad na magprocess ng malaking bilang ng transaksyon ng sabay-sabay ng hindi bumababa ang performance. Scalability ng payment network ay kadalasang nasusukat sa tks (transaksyon kada segundo). Halimbawa, Visa claims ang authorization network nito ay may capasidad na magprocess ng 56,000 tks, [17] habang ang Bitcoin network ay restricted lamang sa sustained rate na 7 tks. [18]

Ilan sa mga measure na maaaring gamitin para siguraduhin ang mas mataas na scalability ay pababain ang block creation interval sa 2 minuto at tanggalin ang limitasyon sa laki ng block, para ang transaksyon blocks ay mas madalas na created, at bawat block ay maaaring mag-accommodate ng mas maraming transaksyon. Ang ganyang measures ay hindi kakaiba at implemented na ng ibang cryptocurrencies. [19] Gayonman, hindi tulad ng ibang networks, Graft ay maintained sa pamamagitan ng laging mataas na performance supernodes na nagvavalidate at authorize ng transaksyon real time. Kung ganun, ang bawat supernode ay hindi lamang may pinaka recent na kopya ng full blockchain pero meron rin list ng lahat ng pending authorization requests at nakompletong transaksyon hanggang sa madagdag sa blockchain. Ang ganong architecture ay pinapayagan ma-absorb ang malaking picks ng requests associated sa seasonal at ibang pagbabago sa mga bumibili at aktibidad ng merchants.

Offline Transaksyon Approvals

Ang mga taong familiar sa payment kard processing ay alam na minsan ang transaksyon ay maaaring approved ng merchant ng hindi kumukuha ng aktuwal na approval mula sa bangko. Ito ay tinatawag na offline o lokal approval, o offline authorization, o minsan S&F ("store at forward") tulad ng offline authorization ay forwarded sa server kapag ang network ay online muli.

Gayonman, crypto payments assume na ang network ay available 24/7, at walang downtimes, na hindi naman totoo. Sa ilang sitwasyon, ang merchants ay kinukuha ang risk at approve lokal transaksyon dahil ang risk ng isang chargeback ay mas mababa

kaysa sa mawalan ng maraming kustomers. Kadalasan, merong kabuuang limitasyon para sa lokal authorization. Pagkatapos, ang system maaaabot ang ganitong limitasyon (ang maximum risk), hihinto sa pag-isyu ng lokal payment approvals hanggang ang network ay up muli. Pero sa kaso ng short downtime, lokal authorization ay maaaring hindi mapansin ng kapwa cashiers at mga bumibili.

Graft merchant point of sale app at single relay supernode ay pwedeng iprocess offline crypto transaksyon based sa parehong principle, kung hindi sila makapagcommunicate sa authorization sample at makakuha ng consensus, at ang merchant ay handa ng kumuha ng risk. Ang desisyon tungkol sa approval ay laging based sa mga bumibili at supernode's reputation scores.

Transaksyon at Payment Flows

Ipinapakilala ng Graft ang sumusunod na mga uri ng transaksyon at flows para mapabilis ang transaksyon ng merchant at suportahan ang existing payment at point of sale applications.

Authorize

Ito ay analogue sa debit kard authorization. Authorize ay initiated ng merchant at confirmed ng payer. Payer's account ay temporarily "locked" para sa halaga at duration (number ng blocks) requested ng payee at confirmed ng payer, o hanggang ang halaga ay confirmed pagkatapos makompleto ang transaksyon. Ang authorization lock ay maaari irelease rin sa pamamagitan ng gagcancel ng transaksyon inisyu ng payee bago ang expiration. Ang funds ay automatically released muli sa payer sa pamamagitan ng network pagkatapos ang petsa ng expiration / oras kung ang payee ay hindi pa sila claim sa pamamagitan ng kompletong transaksyon.

Authorize ay ginagamit kapag ang eksaktong final na halaga ng transaksyon ay hindi alam sa oras ng sale initiation. Mga halimbawa ay pagbabayad sa pump sa gas station, car rental check-in, hotel room reservation/check in, o pagbabayad sa restaurant.

PreAuth

Ito ay katulad ng long-term Authorize pero ang kaibahan ay hindi guarantee ng payer na ang funds ay available sa oras na makompleto. PreAuth ay long-term contract sa pagitan ng payer at ang payee. Gayonman, hindi tulad ng Authorize, na hindi macancel ng payee, preAuth ay maaaring macancel sa anumang oras sa pamamagitan ng paglipat ng funds mula sa account associated sa pre-authorized transaksyon.

PreAuth ay angkop sa long-term payment arrangements tulad ng buwanang service subscription o daily hotel room billing. Ang payee specifies (at ang payer confirms) ang maximum na halaga ng isang charge, ang kabuuang number ng charges, at ang minimum interval sa pagitan ng charges.

Kompleto

Finalize ang payment initiated sa pamamagitan ng Authorize o PreAuth transaksyon. Ang aktuwal na halaga ng nakompleto ay maaaring mas mababa kaysa sa nakaraang authorized na halaga; maaaring merong maraming nakompleto pero ang kabuuang halaga ay hindi tataas sa Authorize na halaga.

Kompleto ay ginagamit pagkatapos mafinalize ang nakaraang authorized transaksyon at alam ang eksaktong halaga. Halimbawa, magbayad sa pump pagkatapos makompleto ang fueling, car rental check out, hotel check out, o bayad sa restaurant na may dinagdag na tips.

Sale

Sale ay Authorize/Kompletong processed sequentially at automatically sa pamamagitan ng network bilang isang transaksyon. Sale ay typical merchant transaksyon online o brick at mortar store.

Transfer

Ang transfer ng pera sa pagitan ng Graft accounts. Kapareho ng Sale pero initiated sa pamamagitan ng Nagpapadala(Sender), ng walang consent ng Tumatanggap (Receiver). Maaaring gamitin sa peer-to-peer payments, exchanges at transfers sa pagitan ng ibang accounts.

Cancel

Cancels Authorize, releases ang authorized funds (tinatanggal ang account lock).

Issue

Activates Graft prepaid kard, gift certificate, loyalty points, store credit, o discount coupon.

Redeem

Payment gamit ang prepaid kard, gift certificate, loyalty points, store credit, o discount coupon na dating inisyu ng Graft.

Exchange

Exchange funds sa pagitan ng graftcoins at ibang major cryptocurrencies at lokal fiat na mga salapi gamit ang pinakamagandang offer mula sa supernodes.

Schedule

Schedules ang transaksyon na mangyari sa later na oras/petsa. Kailangan ng dagdag acknowledgement mula sa user.

Escrow

Escrows ang funds, attaching ang event trigger kapag ang funds ay irerelease.

Refund

Refund transaksyon returns referenced sa pamamagitan ng transaksyon pointer. Kailangan ng RMA authorization mula sa seller.

Processing Transaksyon sa Graftcoins bilang Paraan ng Payment

Hindi tulad ng Bitcoin at ibang cryptocurrencies, at tulad ng payment kards, payment transaksyon request ay formatted at issued ng recipient (merchant), na may exception lang sa Transfer at Exchange na initiated ng sender (i.e. sinumang gustong maglipat ng funds sa pagitan ng Graft accounts). Gayonman, hindi tulad ng kredit at debit kards, payment requests ay explicitly confirmed ng bumibili, na prompted sa pamamagitan ng Graft Wallet app bago digitally signs ang transaksyon ito at ipadala sa network. The exception lang ay Redeem ng paper o plastic gift certificate o coupon na maaaring scanned sa pamamagitan ng merchant payment app kung ang hindi ito gustong gamitin ng kustomer ang mobile app o walang Graft account.

Alternatibong Paraan ng Payment sa Processing ng Transaksyon

Para makapagbigay ng pinakamagandang karanasan sa user para sa mga bumibili at mas magandang conversion rates sa merchants, Graft payments ay merong ng ibat-ibang cryptocurrenices o lokal fiat na mga salapi sa form ng kredit/debit kard bilang input sa pamamagitan ng Graft wallet app ng bumibili. Bayad sa Exchange, bayad sa bangko, at bayad sa kredit/debit kard processing (charged mula sa merchant graftcoins) ay iaapply dagdag pa sa standard na bayad sa Graft transaksyon. Ang mga bayad na yun ay makikita ng bumibili bilang paraan ng payment dahil ang paraan ng payment ay hindi makakaapekto sa sale price. Automatic instant conversion ay makakatulong para iadopt ang Graft payments sa pamamagitan ng mainstream users na hindi

maxadong familiar sa cryptocurrency ecosystem at mas comfortable para sa tradisyonal na paraan ng payment, pero humahanap ng mas magandang security, at full anonymity sa kanilang transaksyon.

Kung ang bumibili ay nagdesisyon na magbayad gamit ang alternatibong cryptocurrency o kredit/debit kard, Graft network ay automatically exchange ang ibang cryptocurrency o convert kredit kard payment sa lokal fiat na salapi, gagawing graftcoins real time bilang parte ng transaksyon processing gamit ang service brokers. Ang service brokers, gumagamit ng Graft supernodes at maintained sa pamamagitan ng may-ari ng supernodes, ay responsable sa pag-execute ng exchange deals, pagcharge sa mga bumibili, at pag-execute ng payouts sa merchants. Kung ang bumibili ay pinili ang alternatibong cryptocurrency o kredit kard bilang paaraan ng payment, ang supernode sample automatically pipiliin ang pinakamagandang offer mula sa lahat ng service brokers based sa merchant selections at kombinasyon ng mas magandang exchange rate at mas mataas na reputation score.

Ang may-ari ng supernode ay maaaring magbigay ng currency exchange o/at kredit/debit kard payment bilang dagdag na service sa form ng service brokers. Ang service brokers ay responsible sa pagpapanatili ng security at kailangang compliance sa exchange at payment kard processing regulations, kasama ang PCI DSS compliance, anti-money laundering regulations, atbp.

Service Brokers

Kung ang kustomers ay nagbayad sa graftcoin, at ang merchant ay gustong bayaran sa graftcoins, ang funds ay automatically at instantly debited mula sa account ng bumibili at deposited sa merchant account sa pamamagitan ng Graft network. Gayonman, kung ang kustomer ay gustong gamitin ang ibang paraan ng payment, o/at ang merchant ay gustong mabayaran sa ibang currency/salapi, ang Graft network ay dapat gumamit ng espesyal na mekanismo.

Para mapabilis ang element ng payment processing na hindi maaaring desentralisado pero mataas parin ang demand ng konsumers at merchants, ipinakikilala ng Graft ang service broker. Kung ang Graft network mismo ay hindi kayang iprocess ang particular operation sa fully desentralisadong paraan, idedelegate ang ganung operation sa network ng service brokers na maaaring makipagcompete sa pamamagitan ng pag-offer sa merchants at kustomers ng mas magandang service at mas mababang bayad. Merchants ay maaaring pumili ng isa (halimbawa, pinakamataas na pinagkakatiwalaan o pinakamura) service brokers, o grupo ng

brokers. Sa paraang ito ang kapwa bumibili at merchant ay matatanggap lahat ang services na kailangan nila habang pinapanatili ang ilang grade ng desentralisasyon.

Supernodes ay pinabibilis ang hosting ng service Brokers. Sa totoo lang, ang may-ari ng supernode ay maaaring maging service Broker. Habang ang supernodes ay dapat iimplement ang kapwa mining at real-time authorization functions, hindi namang kailangang iimplement ang anumang broker functions by default.

Dagdag pa sa pagdagdag ng implementation modules sa supernodes, Service Brokers ay maaaring mabago ang client app source code, o kahit ang pag-create ng sariling applications alinsunod sa Graft protocol. Ito ang mga uri ng service brokers:

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

Accept Broker ay makakayang tanggapin ang ibat-ibang paraan ng payment mula sa native graftcoins at convert kaagad ang halaga ng payment sa graftcoins at ideposit sila sa merchant account. Accept Broker kumikilos real time at nagiging parte ng transaksyon sa pagitan ng bumibili at merchant. Mga halimbawa ng accept broker:

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

Payout Broker ay makakayang magwithdraw mula sa Graft merchant account ng bitcoins, altcoins, o lokal fiat na salapi. Payoff ay maaaring initiated manually o automatically. Mga halimbawa ng payout broker:

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

Top Up Broker ay makakaya ang wallet top up (exchanging bitcoin, altcoins o lokal fiat na salapi sa graftcoins). Mga halimbawa:

- Kredit card top up Broker
- Bitcoin top up Broker
- ACH top up Broker

Margin Broker ay nagbibigay ng temporary balance sa merchant para sa pagbabayad ng bayad ng processing sa transaksyon na walang financial inputs tulad ng gift certificate redemption. Ang margin balance ay isasauli automatically kapag ang natanggap ng merchant ang proceeds mula sa susunod na financial transaksyon.

Merchant Payouts

Merchant ay maaaring magdesisyon sa kanilang proceeds mula sa ibang cryptocurrency transaksyon tulad ng Bitcoin o lokal fiat na salapi. Sa ganitong kaso, ang output ng transaksyon ay iproprocess sa pamamagitan ng service broker, bilang parte ng parehong transaksyon, o pagkatapos, depende sa merchant settings. Sinisigurado nito na ang sale ay babayaran ang merchant ng eksaktong lokal na salapi less applicable fees. Ang supernode sample automatically pipili ng pinakamagandang offer mula sa lahat ng service brokers based sa kombinasyon ng merchant selections, mas magandang exchange rate, at mas mataas na reputation score.

Merong ilang payout options: graftcoins, orihinal cryptocurrency, ibang cryptocurrency, o lokal fiat na salapi (Table 3). Sa bawat options na ito, ay merong payout broker services available sa Graft. Kapag ang merchant ay pipiliin ang paraan ng payment na

gusto nilang tanggapin at ang paraan ng payout, ang Graft Point of Sale application ay iprompt ang lahat na available broker services options – depende sa merchant identity at location attributes – kaya ang merchant ay maaaring mag sign up sa lahat ng kanais-nais na services ng broker. Kung higit sa isang payout broker service available para sa parehong uri ng exchange at pinili sa pamamagitan ng merchant, ang Graft Point of Sale app ay automatically pipiliin ang pinakamagandang offer sa panahon ng transaksyon execution.

Table 3: Mga halimbawa ng Ibat-ibang Paraan ng Accepted Payments at Payoffs

Paraan ng payment pinili ng kustomer	Paraan ng payout na pinili ng merchant	Accept Broker	Payout Broker	Dagdag na Bayad
graftcoins	graftcoins	Wala (Graft network)	Wala (Graft network)	Wala
Gift Certificate, Loyalty Rewards, Store Kredit redemption	N/A	Wala (Graft network)	N/A (Margin Broker ay kailangang icover ang transaksyon fee)	Wala
graftcoins	USD	Wala (Graft network)	Bank Transfer Payout Broker, PayPal Payout Broker	Payout Broker fee

Paraan ng payment pinili ng kustomer	Paraan ng payout na pinili ng merchant	Accept Broker	Payout Broker	Dagdag na Bayad
graftcoins	bitcoins	Wala (Graft network)	Bitcoin Payout Broker	Bitcoin Payout Broker fee
bitcoins	graftcoins	Bitcoin Accept Broker	Wala (Graft network)	Bitcoin Broker fee, Bitcoin transaksyon fee (binayaran ng kustomer)
bitcoins	bitcoins	Bitcoin Accept Broker	Bitcoin Payout Broker	Bitcoin Accept Broker fee, Bitcoin Payout Broker fee, Bitcoin transaksyon fee (binayaran ng kustomer)
bitcoins	USD	Bitcoin Accept Broker	Bank Transfer Payout Broker, PayPal Payout Broker	Bitcoin Accept Broker fee, Payout Broker fee
Kredit card	grafts	Kredit Card Accept broker	Wala (Graft network)	Kredit Kard Accept broker fee

Paraan ng payment pinili ng kustomer	Paraan ng payout na pinili ng merchant	Accept Broker	Payout Broker	Dagdag na Bayad
Kredit kard	bitcoins	Kredit kard Accept broker	Bitcoin Payout Broker	Kredit Kard Accept broker fee, Bitcoin Payout Broker fee, Bitcoin transaction fees (binayaran ng kustomer)
Kredit kard	USD	Kredit Kard Accept broker	Bank Transfer Payout Broker, PayPal Payout Broker	Kredit Kard Accept broker fee, Bank o PayPal payout broker fee

Open Loop at Closed Loop na mga Produkto: Gift Certificates, Loyalty Rewards, at Store Kredits

Graft ay papayagan ang merchant na mag-create at gumamit ng sarili nilang open loop at closed loop [20] na mga produkto: gift certificates, loyalty rewards, o store kredit program in minutes, walang anumang inisyal investments, bayad, o registration sa anumang centralized authority. Merchants ay makakayang magbenta at tumanggap ng gift certificates sa kanilang websites o sa brick-at-mortar store sa lokal na salapi, ibang cryptocurrency, o graftcoins. Gift certificates ay magiging available sa form ng electronic certificate sa mobile wallet app, ipapadala sa pamamagitan ng email, printed sa papel, o bilang pisikal plastic kard (ibinigay sa pamamagitan ng Graft foundation o third party). Ang paggamit ng kakaiba flexible identity system ng Graft, merchant ay maaaring maging sa regulations sa loob ng gift certificates.

Lahat ng Graft transaksyon, including ang pag-isyu at redemption ng gift certificates, loyalty points, at store kredits ay processed real time gamit ang standard API, na maaaring madaling integrated sa existing point of sale applications. Kustomers ay maaaring bumili ng gift certificates mula sa ibat-ibang merchants at marketplaces, online at sa store, at magbayad sa lokal fiat na salapi o cryptocurrency. Ang gift certificate o halaga ng store kredit sa lokal fiat na salapi ay guaranteed sa pamamagitan ng pag-isyu sa merchant at sa pamamagitan ng network, kaya hindi sila mawawalan ng inisyal nominal na halaga. Kustomer ay maaaring magredeem ng gift certificates at ang pag-isyu sa merchant store sa pamamagitan ng halaga ng nominal lokal na salapi o ibenta ito anumang oras sa marketplace para sa lokal fiat na salapi o gamit ang kasalukuyang market value ng cryptocurrency.

Merchant (Domain) Tokens

Dagdag sa mabilis at murang transaksyon, merchant nilagay ng mataas na halaga sa kustomer loyalty at branding. Ang functionality na ito ay magagamit sa pamamagitan ng token layer ng Graft na salapi. Ang token represents domain (merchant) specific gamit ng Graft, at offers smart contract backed functionality tulad ng loyalty point accumulation at gamit, reward points, sale discounts, spending discounts, competitor discounts, coupons, store kredit, atbp.

Halimbawa, ang coffee shop chain, ay maaaring mag-create ng merchant token at attach ng promotion rules na magbibigay ng patron abilidad para makakuha ng discounts sa iced drinks sa nasabing oras sa araw na iyon, itatally ang purchases sa establishment at offer rewards based sa aktibidad o walang aktibidad.

Sa huli, Graft Domain Tokens ay magbibigay ng napakamabisang mekanismo sa couponing sa pamamagitan ng pagpayag sa merchants na buksan ang coupon creation at assignment rules sa loob ng kanilang domain network.

Desentralisadong Crowdfunded Kredit Kards

Desentralisadong crowdfunded kredit kard eco-system ay binubuo ng kredit konsumers (kardholders, mga bumibili), kredit providers, identity providers, at merchants (nagbebenta). Graft network ay pinabibilis ang communication at transaksyon sa pagitan ng partido at iapply ang common rules para mabawasan ang risk ng fraud.

Ang **Graft network** connects potensyal kredit konsumers sa kredit providers na nag-aalok ng kredit sa consumer. Sinumang may Graft wallet (libreng app) ay maaaring maging kredit konsumer. Sinumang may Graft wallet at positibong baalanse ay maaaring maging kredit provider. Sinuman na may Graft point of sale (libreng app), o third party point of sale integrated sa Graft SDK, ay maaaring maging merchant. Ang identity provider ay implemented bilang service broker na tumatakbo bilang "plugin" sa Graft network. Ang identity provider ay gumagamit ng open API na tumutulong mapanatili ang open at desentralisadong karakter ng buong eco-system.

Credit providers sinet ang kanilang kailangang requirements na minimal identity para matanggap ang kredit, maximum kredit limit, kabuuang maximum kredit limit (para sa maraming providers), kredit rate, at minimum halaga ng payment at frequency. Kredit konsumer ay maaaring makakuha ng kredit mula sa maraming kredit providers basta ang kasalukuyang state ng kanilang account ay sakto sa requirements ng provider. Identity providers validate at confirm ang identity elements na binibigay ng consumer par matanggal ang burden ng identity validation mula sa kredit providers at magbigay ng ilang degree ng anonymity at privacy sa kardholder. Kaya, ang identity providers ay alam ang tunay na identity ng consumer at kaya maaaring mapanatili ang kanilang long term reputation score independently mula sa network o kredit providers. Kredit providers ay makakatanggap ng share sa bayad sa transaksyon mula sa bawat payment na naprocess gamit ang kanilang kredit.

Kredit konsumer ay inassigned ng reputation score na dynamically calculated based sa history ng consumer at lebel ng identity binigay ng kardholder at validated sa pamamagitan ng identity providers. Ang inisyal score bago ang anumang validated identity o anumang history data nakolekta, ay sinet sa 0. Ang mas maraming identity elements na naibigay at validated (halimbawa, driver license, biometrics, social security number), ay mas mataas ang inisyal score, na ibig sabihin ay mas maraming kredit ang maaaring ibigay sa kardholder. Positive repayment history ay itataas ang reputation score respectively.

Merchants ay recipients lang ng transaksyon na may kredit consumer, isolated mula sa relationship sa pagitan ng kardholders, kredit providers at identity providers, na kompletong inalis ang kanilang risk ng fraud. Kredit providers assume ang lahat ng potensyal fraud risk at gastos, na compensated sa kanilang share sa transaction processing fees at kredit rates fees. Gayonman, merchants ay maaaring lumahok sa process sa pamamagitan ng pag-offer ng incentive tulad ng cashback o kahit na kredit providers.

Security

Base sa pinapakita ng recent mega data breaches sa retail at hospitality industries, security ay napaka importante element ng anumang payment ecosystem. Ang pinakamataas na lebel ng security ay maaaring makamit kung ang security ay parte ng system design sa halip na “add-on” nagawa pagkatapos ng implementation. Ito ay nangyayari sa payment kard, na hindi inisip ang designed na may security, pero ito dapat ang mangyari sa cryptocurrenices, dahil designed sila na maging resilient sa halos lahat ng uri ng attacks. Security ng payment system ay hindi lang impormasyon security pero kasama rin ang financial security. Dagdag sa standard security features na namana mula sa predecessors, Graft ay mag-iimplement ng ilang enhancements kung saan makikinabang ang kapwa bumibili at merchants.

Availability

Ang network ng “laging on” supernodes ay sinisigurado ang kabuuang availability ng network. Ang client apps communicate sa maraming supernodes ng sabay-sabay para makuha ang kailangang consensus sa authorization. Kung isa sa sample supernodes ay bumaba ay papalitan ito automatically ng isa pa mula sa authorization sample candidate list na may virtually walang hanggang number ng candidates.

Identity Management

Relying sa wallets para gumawa ng user management ay bubuksan ang malaking security risk dahil ang wallets are karaniwang libre na iimplement ang kanilang sariling security measures at maaaring compromised rin bawat indibiduwal. Para maprotektahan ang network at siguraduhin ang integridad ng user identities, Graft ay mag-implement ng distributed provider service (embedded sa supernode), available sa wallets bilang OpenID Connect oAuth2 API call.

Ng hindi isinasaalang-alang ang wallet implementation, user verification at authentication ay maaaring dalhin ng Graft network, na maaaring maiwasan ang compromised user identities, spoofing, replays at man-in-the-middle attacks.

Identification, Authentication, at Authorization

Sa existing cryptocurrencies authenticaton / authorization ang naging purview at sobrang napag-isipan ang user application tulad ng wallet. Gayonman, sa context ng financial transaksyon sa pagitan ng bumibili at nagbebenta, ilang degree ng tiwala ay kailangang maestablish sa pagitan ng partido, regulations at compliances kung saan maisasagawa at magandang system para sa authentication / authorization na naging kritikal, ay dapat bigyan ng recourse.

Identity Proofing

Identity proofing ay challenging topic dahil ito ay may kapwa regulatory at privacy considerations. Ang epektibong identity proofing rin ay hindi trivial.

Para maintindihan ang kailangan para sa proofing ay iconsider ang seller ay maaaring magrequest ng malakas na lebel ng identity proofing para masigurado ang bumibili ay eligible na bumili ng prescribed medications, at superior lebel ng identity proofing para makabili ng arms (defined sa pamamagitan ng NIST Special Publication 800-63A sa US). Conversely, ang mga bumibili ng mga produkto sa after-market ay maaaring gustong protektahan ang kanilang sarili mula sa pagbili ng nakaw ng mga produkto sa pamamagitan ng pagrequest ng mas mataas na lebel ng identity proofing ng nagbebenta.

Graft expects ang client applications ay magcomply sa identity verification standards relevant sa jurisdicions. Supernodes ay magbibigay ng resources para sa machine-based identity at fraud detection para tulungan ang merchants (at users) sa compliance, siguraduhin ang integridad ng payment network, at kaligtasan ng transaksyon. Para ilimit ang exposure ng user kapag nagshashare ng kanilang kompletong impormasyon identity ay hindi maganda o counter sa regulatoy laws (GDPR para sa halimbawa), Graft ay pabibilisin ang request at sharing ng identity attributes, tulad ng edad ng tao, kanilang address atbp para makasiguro na compliance sa lokal na batas at regulations. Tinitignan rin namin na magdagdag ng mas maraming metadata collection sa attribute sharing para makakaya ang auxiliary business logic tulad ng drug interaction checks o loyalty rewards.

Graft ay papayagan ang optional multi-user control, kapag ilang users ay may access sa parehong merchant account, at multi-user custodianship, kapag dalawa o mas maraming users ay kailangan para ma-unlock ang ilang functions tulad ng pagtransfer funds sa account.

Dalawang Factor Authentication na may Biometrics

Graft ay iimpement ang pinakamagandang practices, advanced authentication na magagamit sa user management service, na maaaring kasama ang risk / threat analytics based sa login / pattern ng paggamit ganundin ang device at network characteristics, sophisticated, multi-factor based authentication na kasama ang biometrics, FIDO at ibang walang password factors at techniques para maidentify ang user

Ang user ID ay bibigyan ng espesyal na attention para maiwasan ang problema sa “lost key” pero para masigurado ang abilidad para mabilis na matiyak ang ID ng user at sa ibat-ibang sitwasyon. Sa ganun ang end UserID ay binubuo ng maraming elements (keys) – ilan tied sa devices at hardware tokens, at ilan sa user biometrics – na jointly magbibigay ng base para maidentify ang user via flexible set ng attributes. Halimbawa, posibleng maidentify ang user sa pamamagitan ng 2 factors sa available ID elements (mukha, palad, iris, hardware token, device,atbp). Ang hindi nagamit na factors ay gagamitin bilang pool ng factors para maverify ang identity ng user. Ang ultimate goal ay gumawa ng user identification at authentication na gumana ng mabilis, reliably, sa malawak na ibat-ibang sitwasyon, sa malawak na devices, habang binibigyan ng pagpipilian ang user at reflective sa user

preferences at limitasyon.

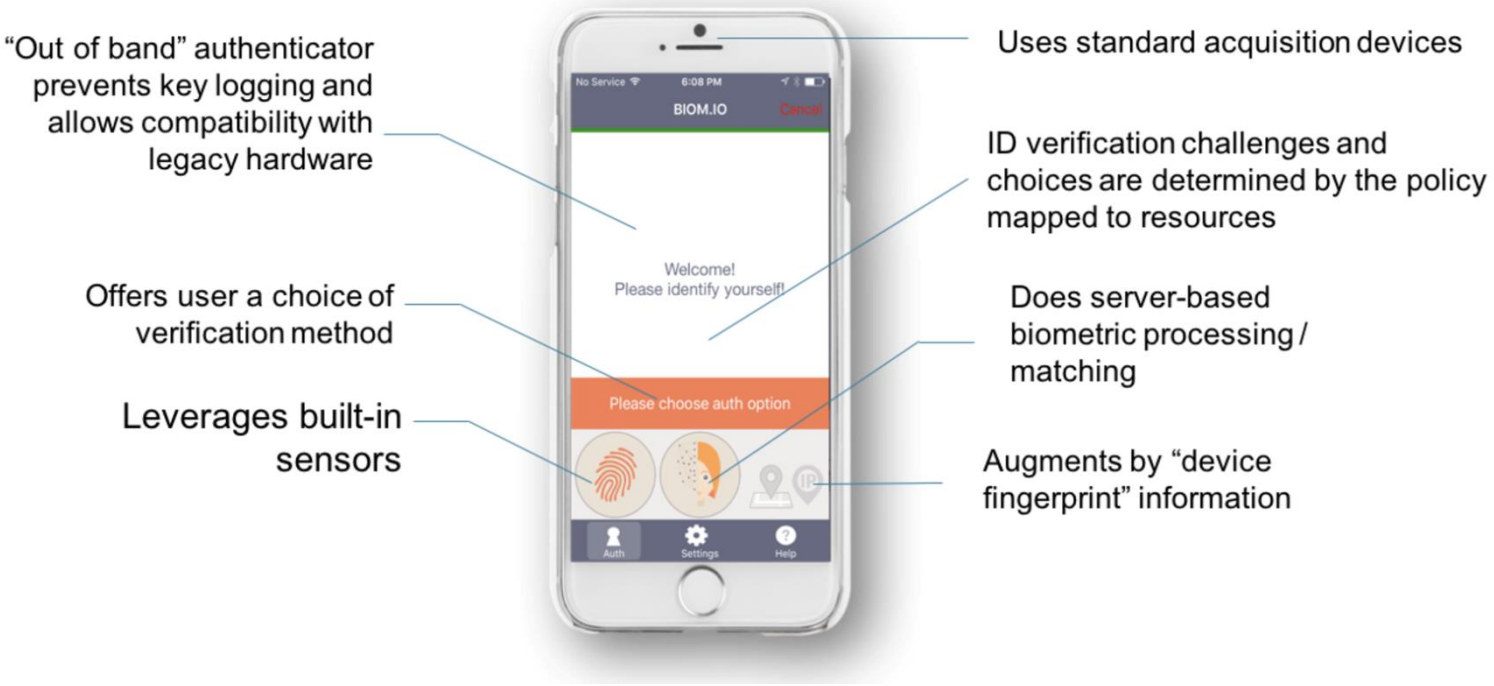

Figure 3: Mobile Multi-Factor Biometric Authenticator ay Parte ng Portfolio ng Kasalukuyang Graft Teknolohiya

Reputation Score - Illuminate ang Kadiliman

Graft ay gamit ang risk based approach para sa transaksyon processing. Ang bawat kalahok sa network ay inaassign ng reputation score na dynamically updated ayon sa bagong captured ng system. Ang mga bumibili, merchants, at may-ari ng supernodes ay maaaring optionally link sa kanilang partial identity sa kanilang account para idisclose at iimprove ang kanilang reputation score. Ang ganung link ay hindi icocompromise ang untraceability ng transaksyon.

The reputation score system ay tutulungan ang mga kalahok sa ecosystem na gumawa ng informed decisions ng hindi compromising ang kanilang security at privacy. Halimbawa, ang merchant ay maaaring isaalang-alang ang reputation score ng bumibili kapag gumagawa ng desisyon regarding sa authorization limit bago ang instant authorization. Ang buyer ay maaaring ireview ang reputation score ng merchant bago bayaran ang hindi kaaagad deniliver na mga produkto. Ang kapwa mga bumibili at merchants ay maaaring icheck ang reputation score ng network supernode na kanilang pinagcocomunicatan.

Ang supernodes ay in charge sa monitoring, calculating, updating, at validating ang reputation scores para sa mga bumibili, merchants, at ibang supernodes. Ang scores ay calculated gamit ang espesyal predictive analytics algorithms na nagbibigay ng resulta na 0-100 scale na madaling maintindihan, na hindi magagamit para idisclose ang anumang impormasyon tungkol sa number, oras, at nature ng transaksyon.

Pabagu-bago

Ang halos lahat ng merchants ay gustong mabayaran ng dolyar (o kanilang lokal na salapi). Merchants ay maaaring gamitin ang fiat na salapi, hindi bitcoins o anumang cryptocurrencies, para ireplenish ang stock at bayaran ang kanilang bills at sahod ng mga empleyado. Maaaring gamitin rin ang fiat para bayaran ang refunds in case ng return. Hindi nila afford ang mataas na pabagu-bago especially ng maliliit na merchants. Graft ay niresolba ang pabagu-bago na problema sa pamamagitan ng instant, real time transaksyon settlement, na pinabababa ang posibleng loss ng halaga dahil sa pabagu-bago. Ang merchant’s payment app ay maaaring automatically adjust ang halaga ng transaksyon sa kasalukuyang exchange rate at iredeem sa lokal na salapi sa pamamagitan ng online exchange pagkatapos makompleto ang transaksyon.

Kustomer Support, Dispute Resolution, at Payment Insurance

Isa sa main showstoppers ng cryptocurrency adoption ng mainstream konsumers at merchants ay ang kawalan ng awtoridad at ang may-ari ng negosyo na maaaring tumulong sagutin ang mga tanong at resolve teknikal at mga isyu sa negosyo. Imposible rin na “ayusin” ang maling cryptocurrency transaksyon kapag my error ang tao, fraudulent na aktibidad, o teknikal glitch. Obviously, lahat ng isyung ito ay may dahilan at justified sa pamamagitan ng desentralisado, anonymous, at independent nature ng crypto

payments. Gayonman, ang magandang mga dahilan ay hindi makakatulong resolbahin ang mga problema. Ang open source komunidad reresolbahin ang mga problemang ito sa pamamagitan ng optional kustomer support para sa libreng open source na mga produkto. Linux OS supported ng Redhat at MySQL database supported ng Oracle ay dalawang matagumpay na halimbawa ng nagbibigay ng commercial-lebel support para ifree ang open source na mga produkto.

Para mapabilis ang adoption ng Graft payment, Graft Foundation ay nagbibigay ng libreng kustomer support at dispute resolution services sa Graft account holders. Merchants na may malaking transaksyon volume ay maaaring makakuha ng 24/7 real time support at dispute resolution assistance. Graft Foundation o/at service brokers ay maaaaring insure ang payments ng hanggang sa equivalent na USD $100 at compensate kustomers o merchants sa kanilang lost funds dahil sa fraud o teknikal na mga isyu.

Privacy

Kadalasan, merong maling perception sa privacy. Sa totoo lang, majority ng legitimate na mga bumibili ay hindi iniisip na idisclose ang kanilang identity sa merchant especially kung makikinabang sila mula sa disclosure, o ang ganung disclosure ay kailangan para iprocess ang transaksyon. Sa parehong paraan, ang mga bumibili ay gustong makasiguro na ang merchant ay ipinadala ang payment sa tamang tao o organisasyon at hindi sa kanilang impersonator. Ang kapwa hindi gusto ng merchant o bumibili ay ang abilidad ng sinuman na kilalanin ang kanilang identities at tignan ang lahat ng detalye ng kanilang transaksyon sa pamamagitan ng pag-scan ng publicly accessible blockchain.

Privacy ay delicate subject para sa crypto currencies at in general sa payment industry. Halimbawa, ang nagbebenta ay maaaring mayroong regulatory compliance requirements para mangolekta at magverify ng certain identity data, tulad ng ilang taon para sa liquor o pagbili ng sigarilyo, o zip code para sa online merchant's tax calculation. Sa kabilang banda, ang bumibili ay maaari o hindi maaaring mag-agree sa idisclose lahat o ilang attributes ng kanilang identity at dapat may position para magawa un. Kung ang nagbebenta at ang bumibili ay magkasundo sa identity attributes na ishahared, ang transaksyon ay maaaring magpatuloy. Dagdag pa, meron requirement para maitatag ang identity attributes authenticity ng merchants sa maraming cases.

Magtitingin kami ng pinakamagandang paraan para iapproach itong problema ay ang paggamit ng system ng identity verification at identity attribute sharing na consistent sa Digital Identity guidelines sinet ng government regulators focused sa privacy enhancement (i.e. NIST 800-63 sa US o GDPR sa EU) – standards na tumatawag sa ibang identity proofing at authentication. Graft implements digital identity profile na attached sa Graft wallet, na may abilidad na magshare ng data mula sa digital identity sa counter-party incrementally at based sa permission ng user sa oras ng transaksyon. Itong permission include sharing certain attributes (tulad ng edad, home location, address, pangalan, atbp..) selectively at kada transaksyon.

Graft implements CryptoNote[21] bilang underlying transaksyon recording protocol na nagbibigay ng mataas na degree ng privacy kompara sa Bitcoin at ibang cryptocurrencies sa pamamagitan ng paghide ng impormasyon tungkol sa nagpadala at tumangap.

User Applications

Lahat ng Graft user apps ay “light” clients na iniistore ang blockchain o iprocess ang anumang transaksyon. Ang user apps ay gumagamit ng remote API na tawag para makipagcommunicate sa “laging-on” Graft nodes na nagmimine ng bagong transaksyon block request real time.

User na nagrerequire ng mas mataas na control lebel over privacy, anonymity, at availability (halimbawa malaking merchants o sekretong organisasyon) ay maaaring magpatakbo ng kanilang sariling supernode o kahit multiple supernodes na maaaring eksklusibo at privately communicate sa kanilang client apps, relay messages at transaksyon sa ibang supernodes, isyu offline authorizations, at mine Graft required sa pagpapatakbo ng store kredit, gift, at loyalty programs. Ang iba pang solusyon ay connecting sa supernodes via remote VPN o/at TOR network. Sa layuning ito, supernodes ay magiging accessible sa pamamagitan ng TOR.

Konsumer apps include:

- Desktop at mobile merchant **Point of Sale** apps sa pagtanggap ng payments na graftcoins, bitcoins, altcoins, at kredit/debit kards, ganundin ang pagconfigure ng payouts sa bitcoins, altcoins at lokal fiat na mga salapi, na maaaring gamitin ng kapwa mga bumibili at merchants.
- Desktop, mobile, at Chrome browser extension **Wallet** apps sa paggawa ng payments sa graftcoins, bitcoins, altcoins at kredit/debit kards (sa pamamagitan ng paggamit ng instant exchange brokers), at pagpapadala at pagtanggap ng graftcoins transfer.
- Graft **SDK** ay papayagan ang integration sa major merchant point of sale software at shopping carts, para sa pagprocess ng kapwa online at brick-at-mortar transaksyon. Graft ay iincorporate ang Graft **smartcard** bilang paraan ng payment. Dagdag pa sa pagdadala ng keys, ang kard ay magstore rin ng biometric signatures ng user at set ng memorized o look-up secrets, na maaaring gagamiting sa terminal authentication. Graft Foundation at service brokers ay susuportahan ang smartcard at production ng **smartcard reader.**

Dagdag pa sa pagsuporta sa konsumer focused transaksyon (B2C), Graft ay susuportahan rin ang B2B (business-sa-business) transaksyon at iintegrate sa existing business workflows. Ang ganung workflows ay maaaring magrange mula sa simpleng awtomatikong pagkolekta ayon sa kredit terms (e.g. Net 30, 60, 90), hanggang sa komplikadong workflows tulad ng settling ng shipper's customs bill at pag-account dito bilang parte ng kabuuang transaksyon, sa pagdistribute ng funds based sa p ag-abot ng milestones at approval ng kustomer.

Graft ay maglalaro rin sa IoT space bilang ilan sa IoT devices na kailangang "icharge" sa data o service na inaalok nila. Ang isang halimbawa ay ang magiging brick-at-mortar merchant summoning ang truck based sa lebel ng inventory na dinitermine sa pamamagitan ng backend systems at sensors.

Kongklusyon

Graft ay hindi mag-eexist ng wala ang mga predecessors nito. Ito ay based sa mga ideya, principles at mga teknolohiyang ipinakilala at tested ng creators ng ibang cryptocurrencies. Ang paggamit ng pinaka recent na mga teknolohiyang dineveloped ng

crypto community kasama ang bagong developed na mga solusyon sa transaksyon processing at security ay papayagan ang Graft na makipagcompetensya sa tradisyonal na paraan ng payment at 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/.