Graft

去中心化、实时授信、借贷和加密货币的支付处理网络

Slava Gomzin, Dan Itkis

版本 1.02

2017 年 8 月

目录

DAPI（分布式接口 API）

授权样本的实时认证

授权帐户锁定

中继超级节点

超级节点奖励

可扩展性

离线交易审批

交易类型和支付流程

Graftcoins 作为付款方式的交易过程

可替换的付款方式的交易流程

服务代理商

商户支付

开环和闭环的产品：礼品券、忠诚奖励和商店信用积分

商家（域）代币

去中心化的众筹信用卡

安全性

可用性

身份管理

身份识别、认证和授权

身份验证

使用生物特征识别的双重因素认证机制

信用得分-拒绝暗箱操作

波动性

客户支持、争议解决和支付保险

隐私性

用户应用程序

结论

参考文献

摘要

Graft 是一个全球性的、开源的、基于区块链的、去中心化的支付网关和处理平台，任何人都可以使用。任何买家和商家都可以以完全去中心化和廉价的方式使用 Graft。Graft 生态系统是开放的，所以任何人都可以通过 Graft 区块链实现网络服务。

Graft 采用了类似于传统电子支付系统（如信用卡、借记卡和预付卡）的支付处理协议和流程，这些电子支付系统的使用方式已经被世界各地数百万用户和商家所熟悉和信赖。通过这种方法可以更容易和更便捷的的使 Graft 成为主流的支付平台，同时也能够消除当前的集中式中介（支付网关和处理器）来促进买家和商家之间的点对点交易。

背景

比特币[1]作为一种“在线现金”被创造出来，它是非常安全但交易相对缓慢的结算系统，并且也无法替换在线支付银行卡、或是在实体店中与会员卡和纸币竞争（图 1）。

图 1：去中心化的比特币交易处理流程

即使一些现有的加密货币[2]已经改善了支付的确认时间，但是仍然无法处理基本的交易类型，例如授权和验证，这使得零售业、酒店和便利店行业不可能使用这些交易类型，而不得不使用中介机构-支付处理器和网关[3] – 来填补这项空白（图 2）。然而，这些支付处理器的存在通常是由政府监管并由股东控制的集中商业组织机构，作为加密货币支付交易的一个重要要素，与加密货币的基本原则相矛盾：去中心化、隐私和独立性。

图 2：存在中央机构处理比特币交易

大多数商家是无法接受没有第三方支付处理器的加密货币，因为区块链网络处理交易的方式是唯一的，这在概念上不同于传统的电子支付方式，如支付银行卡或 Paypal。虽然银行卡支付的整体概念可能已经过时，但是围绕这项技术进行开发的新方式，已经获得了庞大的商家体验和用户信任，这些信息不能一夜之间被放弃。这些新技术包括实时授权协议和智能卡。传统和加密货币支付系统处理的交易方式有很多差异，在大多数情况下，这些方式会使得商家和/或消费者对加密货币的吸引力有所降低。以下是与传统电子支付相比，现有加密货币的技术壁垒和业务缺陷的如下：

- 缺乏基本的交易类型
- 付款流程不适用
- 确认时间过长
- 不可预测及不平衡的交易费用
- 无法处理小额支付和双花（订阅）
- 缺少支持脱机交易
- 可扩展性低
- 不稳定
- 安全性不具体
- 由于区块链技术的可追溯性，用户缺少隐私
- 买方与商户之间缺乏信任
- 应用程序有问题
- 用户界面的体验差
- 缺乏客户支持

为了解决所有这些问题，Graft 将加密货币支付处理提升到一个新的水平，使得主流商家和消费者能够首次广泛的接受这种方式，并且不会违反加密货币的基本原则。让我们更详细地回顾一下这些问题，并看看是 Graft 如何解决这些问题的。

去中心化支付处理的价值

为什么消费者更愿意使用加密货币而不是信用卡，PayPal 或者 Apple Pay；为什么商家更希望接受到加密货币而不是现有的支付方式。 很显然，如果我们没有找到这些问题的正确答案，就没必要创建这份文件。.

相比于第一个部分的答案，关于个人为什么更愿意让自己的钱以一种加密货币的形式存在可能包含几种因素，因为这部分问题可能有多种原因（或者他们的组合原因），第二部分的答案就相对简单的多。商人总是喜欢扩大自己的客户群体以此来增加收入，当他们发现一大批潜在的客户并且这批客户更喜欢用加密货币的时候，商家就会开始接受加密货币。Graft 则为商家提供了一个独特的机会，一个商家可以在没有任何中间商且费用接近零的情况下接收到消费者的加密付款的机会。

然而 Graft 可能提供一些额外的价值。在某种情况下，商家为了遵守法律法规更希望了解消费者的真实身份，以此来确定一些商品是否可以被销售给这些买家。因为 Graft 既是一种去中心化支付处理器也是一种加密货币处理器，所以它可以在没有其他加密货币或资产的情况下促进整个支付周期。同时，除了去中心化和对隐私的绝对保密之外，Graft 拥有另一个重要的基本原则就是可以自由选择。此外，买家和卖家可能会对加密货币的多样性有商业需求。因此，Graft 将为消费者提供比特币还有其他的一些主要加密货币来作为额外的选择，同时为商家提供更多的支付方式。这个特点将去除商家对于多个（集中）支付软件提供商的集成需求，对注册用户集中式服务，学会和维护多个钱包应用程序。值得注意的是，由于确认时间缓慢和较高的交易费用，商家不得不接受在替换加密货币过程中的高风险和而外的费用。

术语

Graft

1. **G**lobal **R**eal-time **A**uthorizations and **F**und **T**ransfers – 用于处理实时授权结算的去中心化开放平台，以及使用无法追踪的区块链、去中心化 API 进行商户支付结算和资金转移，建立社区服务经纪人来支持各种方式的付款，支付方式有加密、传统信用卡和银行转账。
2. 在一种植物的上插入名一种植物的嫩枝或者嫩芽之后就会结合并且一起生长。[4] 嫁接是一种先进的技术，植物学家、农民、园丁和爱好者们利用这种技术将活体组织从一个植物添加到另一个植物。为什么要把两种植物连接在一起呢？ 事实证明，这种技术有很多好处。种植者可以选择具有特殊属性的不同部分，并把他们连接到其他植物上。假设莫棵树有很强壮的根，但是它的果实并不是很好，于是这棵树将会有很好的根茎或者是可以选根的植物。它可与另一棵没有很结实的根部但是会产出奇妙果实的植物相结合。被选为茎、花或者果实的植物被称为接穗。一个理想的接穗可以嫁接到一个强壮的根部以此来创造出一棵真正的大树。着这种行为在园艺行业是很常见的做法。 这允许植物在许多新的区域生长，并让我们获得更多的产品[5]

超级节点

独立不间断运行的服务器使区块链节点和 Graft DAPI 节点相结合，通过挖矿来维持区块链的运行， 处理实时授权、买家和商户的结算 DAPI 通话。并托管附加服务，类如及时加密货币兑换，信用卡/借记卡的接受，以及当地货币商户的支付。超级节点结合 PoW/PoS 的主流网络。

授权取样

选定可以批准实时支付的可信的超级节点组，并保证交易被写入区块链之前消费者不会多花一次钱。

中继超级节点

超级节点促进商业贸易通过一边与商家的 POS 或/和消费者的钱包联系，另一边授权取样其余的超级节点。

服务代理

Graft 协议拓展在超级节点或者一组超级节点上，并由超级节点操作员拥有。服务代理实现特殊的附加功能，而且不能被完全的去中心化网络或者特殊规定结构类如 PCI DSS[6] or NIST 800-63-3 所自动执行。 [7]信用卡支付承兑代理和银行支付转账代理都是服务代理的例子。

域

商家可以通过事实上的去中心化的独立的 “商业帐户” 来设置授权、支付规则和触发器，并且会对特定商户的交易产生影响。

Graftcoin

由 Graft 区块链提供的，用于实时支付、资金转账以及买卖双方的结算的一种特有的加密货币。

DAPI

由超级节点实现的去中心化无形态的 API，被用于支持轻量级客户端应用程序，例如 Graft Wallet 、Graft Point of Sale 以及第三方销售应用程序和购物卡。为了促进 Graft 的集成，把 Graft 源代码提供给第三方销售点和钱包应用供应商。

Graft Wallet

“Lite”桌面，移动和浏览器拓展应用程序通过调用 Graft DAPI 来实现使用 graftcoins 或者其他主要的加密货币或者/信用卡/借记卡来进行支付和资金转账。

Graft 的销售点

“Lite“桌面和移动应用程序允许商家接受以 graftcoins、比特币、山寨币或者信用卡/借记卡为方式的付款；签发和兑换礼券，忠诚奖励积分和商店积分。并配置以 graftcoins、比特币、山寨币或者其他当地法定货币结算支付方式。

交易费用

为什么首先要有交易费呢？毕竟，区块链的背后没有商业和企业，那么为什么用户需要支付费用，谁来收取费用，还有究竟应该收取多少费用？

是否收取手续费

为了支持安全且高度可用的加密货币网络，需要在世界各地分布多个强大的节点（服务器）。那么谁来维护这些服务器，还有什么用什么方式激励和催动他们来维护区块链节点？ 在比特币和其他加密货币网络中，可以通过挖矿和交易费用来获得资金- 节点拥有者通过在每个区块中挖掘新代币来赚钱，以及对每笔交易收取费用。

采矿还有另外一个目的：持续稳定得注入新的代币以此来保持流动性，以此来应对随着接受程度和使用量的增加而对额外代币需求的增长。随着系统的牵引，节点运营商将会从交易费用中得到更多的收入，为此每一个新的区块要限制整体供应来逐渐减少采矿的奖金。

理想世界里，每个人都可以免费拥有和使用加密货币。而事实上，也有一些网络承诺交易免费。[8]在包括比特币在内的一些其他网络，这笔费用将用于优先处理的事务和处理可扩展性问题。

然而在 Graft 网络中，费用的使用有以下两个原因。第一，避免在相关性能和区块链大小问题上的网络滥用。例如使用真正的网络进行测试。如果交易是完全免费的，一个人就可以在两个帐户之间无限的移动相同的金额。第二，当采矿的奖金变的最够小的时候，将变成对节点运营商的唯一激励。

错误的收费方

比特币和其他加密货币的问题在于，他们从错误的一方收取费用。这甚至比传统的银行卡支付更加糟糕，因为不像信用卡支付那样，买家和商户都要为加密货币的交易来付费；买家付费给加密货币网络，商户支付给支付处理器。[9] （一般的/外行的）付款人经常会对没有明确收费制度解释的看起来更像是投注过程交易过程产生疑惑，而这些都造成了加密货币支付的吸引力下降。

微支付:我将怎么使用加密货币来支付以杯咖啡？

比特币面临的另一个问题就是，由于较高的交易费用而无法完成微支付。[10] Graft 通过引入一种独特的（在加密货币世界) 交易费用方法来解决这个问题。

Graft 交易手续费用

就像是大家习惯了的传统电子支付方式那样，Graft 引入了一种只会从接受者(商户)那里收取费用的收费结构，而消费者完全免费。 Graft 通过设置较低的费用（相比于信用卡[11]、在线支付处理器还有其他的加密货币）来让所有人都可以使用微支付，但是没有固定的费用组件。所有的费用都由收款人支付。

表格 1: Graft 网络交易费用

微支付 **（少于 10GRF）**	**定期付款(超过 10 GRF)**
0.10%	1% of log10（随着交易额的增长，明显低于 1%）

对数费用表对处理小金额的交易进行奖励(例如,尽可能的结合多个交易一起),同时对大的交易金额大的降低费用 (表格 2).

表格二: Graft 网络交易费用事例

交易额	交易费用	实际交易费用
0.01 GRF	0.00001 GRF	0.10%
1 GRF	0.001 GRF	0.10%
10 GRF	0.01 GRF	0.10%
50 GRF	0.01699 GRF	0.03%
100 GRF	0.02 GRF	0.02%
1,000 GRF	0.03 GRF	0.00%
1,000,000 GRF	0.06 GRF	0.00%

免费的资金交易： 已认证交易

许多的诸如 ACH 或者 PayPal 等的一些支付网络提供免费的用户交易，相比于那些无论交易的速度和数量都收取非比例费用的加密货币增加了更多的激励。这项功能非常合适于一些低速度要求的事务，诸如家庭账户之间的转账或者员工工资的汇款。为了能与传统的支付网络竞争，Graft 提供了在用户钱包之间有限的免费交易。

加密货币网络通常不提供免费交易的三个主要原因：

- 缺乏对矿工的激励
- DOS 攻击威胁

- 区块链不受控制的增长

Graft 通过付款和转账之间的逻辑分离来解决第一个，所以超级节点（矿工）接收到大部分交易的构成即时交易的费用，同时免费的交易在后台以较低的优先等级进行处理。

通过自愿的用户识别和身份验证解决了第二个关于 DOS 威胁的问题。当然，天下没有免费的午餐，所以用户应该向网络提供自己的身份信息来确保网络的合理使用（通过限制每位用户免费传输的数量和频率），同时也防止了网络的滥用。并且使用 zero knowledge 证明技术可以让用户在不泄露自己隐私的前提下证明自己的身份。

对于最后一个关于区块大小不受控制的增长问题，将由下面一些列的措施解决：小块区间，限制的区块增长，像是免费传输那样，根据特定的交易类型来按标准限制交易规模。条件是，免费传输的一方必须证明他们在过去通过“商业“类型的支付来对网络作出贡献。

额外的第三方服务费

当接受到如比特币、山寨币或者信用卡/借记卡等不同方式支付时；或者处理商户以比特币、山寨币或者其他当地合法货币的支付时，可能会涉及到额外的支付经纪人和/或者支付代理费用。这些都不是隐藏的费用，而是在商家登陆代理服务的时候已经由经纪人声明了。 这些费用在商家进行交易结算（支付）时向商家收取，并且没有任何的设置、预付或定期费用。

客户费用

一些例如比特币那样的加密货币要求客户增加交易费用以此来获得快速的确认。这些费用由客户钱包应用系统配置并由客户支付。大多数的比特币用户已经习惯这种收费。

用保证金余额支付费用

在某些情况下，交易费用可以用 Graft 网络本身或/和保证金经纪人提供的特殊“保证金“余额来支付。这样交易的例子有发行和兑换相关贸易礼券，忠诚度奖励 和商店积分处理。这是为了即使商家在 Graft 帐户中没有足够的余额也可允许进行贸易处理。

交易处理

世界正向更“便携”设备迈进。全世界的人们更多的去使用智能手机和平板电脑来代笔工作站和笔记本电脑。因此，去中心化的加密支付系统更应该更依靠由专业人士主持的强大的超级节点而不是仅仅依赖于个人电脑上的小型个人节点，当便携的客户端应用程序连接到授权样本时，就会通过 DAPI 调试，应用反作弊算法来随即选取的一组超级节点。

确认时间问题：引入实时授权结算

在零售和服务行业，客户能等，所以商家必须立即处理付款。所以较长的确认时间[14] （根据交易费用的大小，从几分钟到几个小时[15]）就是为什么加密货币没有广泛的被采用的主要原因。不像是其他的一些加密货币网络，他们通过增加附加系统或事务类型来解决这类问题。 [16] Graft 会实时的处理所有的交易（不到 3 秒）,并且不收取任何其他的费用，也不损害去中心化原则。 (见图 3).

Figure 3: 简化的 Graft

付款流程
它是实现是通过使用达成共识的始终在线的可信的超级节点（“授权取样”），这个超级节点可以形成一个分布式及时授权锁在买方帐户上并在几秒内相应反馈回客户端。超级节点同时也维护了区块链，所以没有任何交易被授权“脱链”。

超级节点

所有的交易在始终在线的 Graft 网络节点上处理——超级节点——实时（几百毫秒到几秒钟).）。交易费用是由接受方（商户）支付给参与授权样本的超级节点，以及参与到交易过程中的（可选）服务代理。超级节点负责结算（区块挖矿）和实时的交易审批。节点的所有者负责他们处理的交易。这样的责任是通过经济利益来实现的：挖矿奖励和交易费用.

DAPI（分布式接口 API）

与托管在服务器或服务器群的常规 API 不同，DAPI 在多个超级节点上运行所以没有单个的地址。任何单个节点都随时为 DAPI 调用服务。DAPI 调用是无状态的，这意味着超级节点不会与客户端保持永久的会话，所有节点上都分布着处理所需的所有可用数据。使用 DAPI 的客户端应用程序，维护着与它通信的超级节点列表,，列表的内容是从授权样本中选取的一组相对较小的地址组。然而，客户端应用程序可以自由的选择一个特定的可信的超级节点并使用。例如，商家 POS 或者钱包用户可以选择他们自己信任的超级节点。 就算是这样的“私有”超级节点也不能被授予参与授权样本的权利（参见下面的授权样本选择算法部分），但是他们给使用者提供额外的隐私层。

授权样本的实时认证

有的加密货币结算间隔少于 2 分钟。但是，减少间隔任然不能解决实时（即时）授权问题。对于实时结算系统（信用卡授权通常需要几百毫秒到几秒钟），30 秒钟的区块间隔显然太长了，况且 1 个区块还不足以抵御大规模分叉的风险。所以更需要额外的技术来解决实时授权问题。Graft 通过授权取样的超级节点方案解决了这一问题，当被选定的可信的超级节点组实时发布批准时，这样就保证了买家在交易完成后不能再花同样的前（被写入区块链）。结算（挖矿）将在 2 分钟内由超级节点代码的“底层”部分执行。

Graft 支付不同于大多数的加密支付系统，而类似于传统的支付系统（如信用卡处理），Graft 它将支付分为授权和结算两个阶段。就像是传统支付世界那样，实时的（几百毫秒到几秒钟，由多个外部因素影响）就会产生授权，而结算则会在稍后执行，通常也不超过 2 分钟 (与传统支付网络的几小时甚至几天相比)。

授权帐户锁定

通过 Key image 机制来确认新交易和防止重复消费，并且在不破坏发件人的隐私的前提下。Key image 是一种代表买家支出地址和金额的独一无二的“指纹”，并且不透露买家或金额的任何信息。Key image 的本质是它只能被使用一次，所以如果有人试图多次使用相同的 Key image，就是表示要重复消费。当向超级节点网络提供即将发生的交易的独一无二的 key image 时，买方的钱包暂时“锁定”支出帐户，所以不会有具有相同 key image（即来自相同帐户）的交易发生，除非被锁定的交易被确定或者移除。如果买方试图用不同于原锁定交易的 key image 来完成交易，超级节点会拒绝。

另一方面，由于 key image 不包含关于买方或买方钱包的任何信息，所以它是绝对的安全和不可追溯的。此外，当交易完成后（被写入区块链且被确认），买方（钱包应用程序）、商家(销售点应用程序)和超级节点之间在交易期间的任何通信痕迹都会被删除。

授权样本选择

为了执行实时（即时）授权，Graft 网络依靠授权样本（可以代表网络和验证交易的一组被选定的可信的超级节点）来防止二次消费，并且在交易被区块链确认之前立即签订许可（即在交易在添加到区块之前已经添加到区块链）

从可以解决当前高度-10 最后的 140 区块的超级节点中自由选取 8 个来作为授权样本。如果相同的超级节点已经解决了最后 8 个区块中（从高度-10 开始）多个区块或者被选定的节点已经下线，则列表会自动扩展并将列表“底部”的超级节点添加到样本中。授权样本的另一个要求是风险证明：超级节点所有者必须在超级节点关联的帐户上维持一个抵押平衡。 最小的平衡要求是不断的从新计算每一个区块，并且按照每个区块的比例进行供应增长。

这种算法可以让那些通过成功挖矿来证明对网络忠诚的活跃超级节点，对于实时授权也是同样可信的，同时也伴随着由 Proof of Work 算法提供的一定程度的随机化。对于超级节点的每次成功实时授权都会给予一定的交易费用奖励。新的超级节点通过增加跟多的权利和解决下一个区块（平均每 2 分钟生成一次）来赚取参加到交易处理的机会。

成功挖矿但是不能处理实时授权请求的超级节点，将被网络从超级节点表中排除（即他们解决的区块将不能在 720 区块时间段内被网络接受）。

当商家销售点发起了新的交易时，将会根据当前的区块高度为该交易分配优先级。当交易在进行时，高度可以增加，但它不会改变当初分配到交易请求的样本高度。商业的超级节点根据当初规的交易要求来选择超级节点，但是这个选择由每个样本成员和钱包中继来验证。

为了加快授权流程，商家销售点应用程序可以通知授权样本超级节点忽视剩下授权样本的响应，前提是商最快的超级节点中的 50%以上都响应了批准信息，并且没有拒绝信息响应；然而这种模式增加了欺诈的风险，由于现在对交易处理速度要求非常高，所以在一些特定的微支付情况下可以被接受。

中继超级节点

一些授权样本中的超级节点可以成为中继超级节点，并且这些中继超级节点可以一方面通过商家 POS 或/和买家钱包之间的通信来促进交易处理，而剩下的超级

节点在另一方面促进交易。中继超级节点可以从当前连接到交易的授权样本（销售点或钱包）中随即选取。商家和钱包也可以选择一些不包含在授权样本中的超级节点。事实上，商家和钱包如果想要更近一层的安全和隐私，则他们可以托管自己的超级节点，并可能从挖矿和交易处理中获得收入。但是，如果中继节点没有在授权样本中，则它不会获得任何的奖励或费用。

超级节点奖励

每一个授权样本中的超级节点都会收到它曾签署（批准）过的交易的交易费用。每一个样本中的超级节点都会收到 1/n 的交易费用，n 则代表授权样本中超级节点的总数。费用是由收款人（商户）支付。

对出创建新的区块的超级节点会收到一份区块挖矿奖励。根据下面的公式可以算出随着新区块的增加，区块奖励逐渐减少： $(M - A) * 2^{-19} * 10^{-12}$, where A = 当前的循环， M = 总供给 $(2^{64} - 1)$ 在原子单元 (10^{-12})。 这种做法的本质是：随着交易的增多，确保超级节点能从交易费用中得到可持续性的收入。

可扩展性

支付网络的可扩展性可以让网络同时处理大量的交易而不影响性能。支付网络的可扩展性通常用 tps（每秒交易数）来度量。例如，Visa 声称其授权网络能处理 56,000tps，[17]而比特币网络只能位置 7 个 tps。[18]

通过减少区块创建间隔到 2 分钟和移除区块大小的限制等方法来获得更高的可扩展性，因此交易区块更频繁的创建，且每个区块可以容纳更多的交易。这些措施并不是独一无二的，因为一些加密货币网络已经实施了这些方法。[19]与其他的网络不同，Graft 由用来实时认真和授权交易的一直在线的高性能的超级节点来维持。因此，每个超级节点不经拥有完整的最新区块链副本，并且还保留所有待处理授权请求和完成交易的列表，知道他们被传输到区块链中为止。这样的体系允许吸收更多的由于季节变化的请求，和买家和商家活动中的其他变化。

离线交易审批

熟悉支付开处理的人都知道，有时候交易可以通过商家批准，而无需得到银行的实际批准。这就叫做离线或本地批准，或离线授权，或有时的 S&F（存储和转发），因为当网络从新上线的时候，这种离线的授权就会被传输到服务器上。

Crypto 支付假设网络是全天候在线的且没有离线时间，但这是不符合实际的。在某些情况下，商家是冒着风险的去批准本地交易，因为失去多个客户可能性大于只是收到以此退款的可能性。通常，本地授权的限额是有限制的。当系统达到极限（最大风险）后，它会停止发布本地批准知道网络从新上限。但是如果出现短暂的停机时间，那么本地授权就会收银员和买家忽略。

Graft 商家销售点应用程序和单独的中继超级节点可以根据相同的原则来处理脱机加密交易，当他们无法根授权样本进行沟通并达成共识，那么商家就准备好承担风险。 买家和超级节点的声誉评分也决定着是否能够离线审批。

交易类型和支付流程

Grfat 为了促进商家的贸易和支持现有的支付和销售点应用，引入了下面的交易类型和流程。

授权

类似于借记卡授权。授权由商户发起，并由付款人确认。根据收款人金额和持续时间的要求暂时性的锁住付款人帐户并由付款人确认，或者直到后续交易完成在确认金额。授权锁也可以在到期前由收款人发出取消交易来发布。 如果收款人不能在到期前提供完成的交易证明，那么这笔钱就会通过网络自动的传回付款人的帐户。

销售开始且具体的交易金额不详时，可以使用授权。示例有在加油站付钱、汽车租赁登记、酒店预定/入住或者在饭店前台付钱。

预授权

与长期授权类似. 但不同之处在于：支付人不能保证在完成时有用足够的资金。预授权是付款人和收款人之间的长期合同。授权不能被收款人取消，而当从预授权帐户的资金被移动时则预授权被取消。

PreAuth 适用于类似于每月服务订阅或每日酒店房间账单一类的产期支付安排。收款人指定 (由付款人确认)单笔费用的最大金额，以及总费用和费用至今啊的最小间隔。

完成

通过授权或预授权来完成付款。实际完成金额可能低于之前授权金额;也可能有多个交易完成，但是总数不会超过授权总数。

已知金额的授权交易结束后使用“完成”。例如，附上提示的加油完成后在泵上付钱，汽车租赁付钱，酒店退房或餐厅付款。

销售

销售作为单个交易，由网络按顺序并自动的进行授权/完成处理。线上和实体店销售是典型的商家交易

转账

钱在 Graft 帐户之间的转移。根销售相同，都是由发件人发起，不同于没有接受方同意。可用于对等支付，交换和不同帐户之间的转账。

撤销

撤销授权，释放授权资金（帐户锁定移除）

发行

激活 Grfat 预付卡、礼券、忠诚积分、商店信用或折扣券。

兑换

用预付卡、礼券、忠诚度积分、店铺信用、或之前 Graft 发放的折扣券进行支付。

转换

根据超级节点提供的最佳报价，进行 graft 代币、其他主要加密货币和当地法定货币之间的资金转换。

时间表

需要用户的额外确认来安排交易发生在稍后的时间/日期。

第三方托管

托管资金，当资金被发布时附加时间触发器。

退款

退款是根据交易指南来退回交易金额。并需要卖方的 RMA 授权。

Graftcoins 作为付款方式的交易过程

与比特币和其他加密货币的处理方式不同，但与银行卡支相类似，支付交易请求由发起人（商家）进行定义和发布，但是排除发起人通过交易所和支付处理人的转帐和交易（即任何想要在 Graft 帐户之间转移资金的人）。然而，与信用卡和借记卡不同的是，付款请求是需要由买方进行明确和确认的，买方通过 Graft Wallet 应用程序的提示，确定交易请求并签名后，系统才会将交易发送到网络上。这里唯一的例外是如果客户不想使用移动应用程序或根本没有 Graft 帐户，那么就需要通过商业支付应用程序扫描或使用支付卡和礼券方式。

可替换的付款方式的交易流程

为了向买家提供最佳的用户体验和更优质的利率，Graft 支付交易可以通过买方的 Graft 钱包应用程序以信用卡/借记卡的形式,输入各种可转换的加密货币或法定货币。除了 Graft 标准的手续费用外，就不包含其他如交易所费用、银行手续费、信用卡/借记卡处理费（向商户收取的 graftcoin 费用）。这些费用对于买方来说是不可见的，因为付款方式不会影响销售价格。进行自动的即时转换将有助于向那些对加密货币生态系统不了解的客户推广我们的 Graft 支付，并且能够让他们对这种相对传统的支付方式感到更加舒适，同时也提供了更好的安全性、隐私性和完全匿名的交易。

如果买方决定使用其他可替代的加密货币或信用卡/借记卡进行付款，Graft 网络中的服务代理商管理交易，会将该部分资金自动转换成其他的加密货币或通过法定货币的信用卡实时将该资金转换为 graftcoin。运行在 Graft 超级节点并有超级节点进行维护的服务代理商，负责执行交易所的交易、向用户收取费用、并向商家进行支付。如果用户选择使用其他可替代的加密货币或信用卡作为付款方式，超级节点将根据之前选择的商家以及更好的利率和更高的信誉评分的评估组合，自动选择所有服务代理商的最佳报价。

超级节点所有者可以为服务代理商提供货币兑换或信用卡/借记卡支付作为附加服务。服务代理商也负责维护交易的安全性和卡片支付的处理规定，包括 PCI DSS 合规性、反洗钱规定等。

服务代理商

如果客户使用 graftcoin 进行支付，或是是商家希望接收 graftcoin，系统会将资金自动即时的从客户账户中扣除，并由 Graft 网络存入商家帐户。然而，如果客户

想要使用不同的付款方式进行支付，或是商家想要以不同的货币进行支付，那么 Graft 网络就必须使用某些特殊的机制。

为了处理那些不能进行去中心化、但消费者和商家仍然有高度需求的支付处理请求，Graft 引入了服务代理商的概念。当 Graft 网络本身不能以完全去中心化的方式处理特定的支付请求操作时，我们将把这样的操作委托给服务代理商的网络进行执行，为商家和客户提供更好的服务并降低手续费。商家可以选择一个或一组（例如被高度信任或最便宜的）服务代理商。这样，客户和商家都将收到他们所需要的所有服务，同时仍然会保持一定程度的去中心化。

超级节点的实施加速了服务代理商的托管服务。事实上，超级节点也可能会成为一名服务代理商。这样超级节点就必须同时实现挖矿和实时授权功能，但是它们在默认情况下是不会实现任何代理功能的。
除了可以通过向超级节点添加实现模块，服务代理商还可以修改客户端应用程序源代码，甚至可以在 Graft 协议后创建自己的应用程序。以下是服务代理商的类型：

- 收款代理商
- 支付代理商
- 充值代理商
- 保证金代理商
- 托管代理商
- 身份验证代理商

收款代理商可以接收来自不同国家的 graftcoins 付款方式，并立即将付款金额转换为 graftcoin，并将其存入商家帐户。收款代理商的实时结算，能够成为用户和商家之间交易的一部分。收款代理商也可具体分为：

- 比特币收款代理商
- 以太币收款代理商
- 信用卡收款代理商

•Apple Pay 收款代理商

支付代理商可以在 Graft 商业账户中进行比特币、山寨币或本地法定货币的提现操作。支付方式可以是手动或自动的。支付代理商可具体分为：

•银行转账支付代理商

•PayPal 支付代理商

•比特币支付代理商

充值代理商可以为钱包进行充值（将比特币、山寨币或本地法定货币兑换为 graftcoin）。具体又可分为：

•信用卡充值代理商

•比特币充值代理商

•ACH 充值代理商

保证金代理商可以为商家提供暂时的资金支持，用于支付没有诸如礼品券兑换等需要经济投入的交易处理手续费。在商家收到下一笔支付金额后，需要将利息和本金自动返还。

商户支付

商户可以决定从比特币或本地法定货币以及其他加密货币的交易中收取收益。在这种情况下，交易的输出将由服务代理商操作作，或稍后根据商家的设置进行处理。通过这种方式，可以确保以适当的法定货币价格支付给商家的销售费用。超级节点会根据商家选择，提供更好的汇率和更高信用评分的组合，自动选择所有服务代理商中的最佳报价。

同时提供几种支付选项：graftcoin、加密货币、其他加密货币或本地法定货币（表 3）。对于这些选项中的每一种支付方式，都可以选择 Graft 上提供的付款代理商进行服务。当商家选择他们想要接受的付款方式和支付方式时，“Graft 销售点”

应用程序将提示所有可用的服务代理商，这会取决于商家属性和位置信息，这样商家就可以选择合适的服务代理商。如果商家在同一类型的交易中，可以选择多个支付代理商，则 Graft 销售点应用程序将在交易执行期间为商家自动选择最佳的报价。

表 3：接受的支付和结算方式种类示例

由客户选择支付方式	由商家选择结算方式	收款代理商	支付代理商	额外费用
graftcoins	graftcoins	无 (Graft 网络)	无 (Graft 网络)	无
Gift 认证、客户忠诚度奖励、商店信用积分	N/A	无 (Graft 网络)	N/A (保证金代理商可能需要承担支付的手续费)	无
graftcoins	美元	无 (Graft 网络)	银行转账支付代理商、PayPal 支付代理商	支付代理商手续费
graftcoins	比特币	无 (Graft 网络)	比特币支付代理商	比特币支付代理商手续费

比特币	graftcoins	比特币收款代理商	无 (Graft 网络)	比特币收款代理商手续费、比特币交易手续费（由客户支付）
比特币	比特币	比特币收款代理商	比特币付款代理商	比特币收款代理商手续费、比特币付款代理商手续费、比特币交易手续费（由客户支付）
比特币	美元	比特币收款代理商	银行转账支付代理商、PayPal 支付代理商	比特币收款代理商手续费、支付手续费
信用卡	grafts	信用卡收款代理商	无 (Graft 网络)	信用卡收款手续费

开环和闭环的产品：礼品券、忠诚奖励和商店信用积分

Graft 能够让商家在几分钟内创建和使用自己的开环和闭环[20]产品：如礼品券、忠诚度积分奖励或商店信用积分活动，并且不需要花费任何初始的投资、费用或是在相关中央授权机构进行注册。商家将能够在其网站或实体店中出售和接收礼券，来获得当地法定货币、其他加密货币或 graftcoin。礼品券将通过移动钱包应用程序的电子券形式提供，并通过电子邮件发送给用户，也可以使用纸张进行打印，或制作成实体塑料卡（由 Graft 基金会或第三方提供服务）。使用 Graft 灵活的身份认证系统，商家需要遵守有关礼券的规定。

所有 Graft 的交易，包括发放和兑换礼券、积分和商店信用，均可使用标准的 API 接口进行实时处理，也能够轻松得集成到现有的销售应用程序中。客户可以从各种商家和市场、线上网站购买礼券，并通过当地法定货币或加密货币进行支付。当地法定货币的礼券或商店信用积分由发行商和网络进行担保，不会失去发行的名义价值。客户可以通过其当地货币在发卡商户那里兑换礼券，或是用当地目前的市场价格或加密货币市场价格，随时出售礼券。

商家（域）代币

除了为客户提供快速廉价的交易服务，商家对客户的忠诚度和品牌价值效应也特别看重。该功能将由 Graft 货币的代币层驱动。代币能够代表域名（商家）的具体使用，并提供诸如忠诚度积分、奖励积分、销售折扣、支出折扣、竞争对手折扣、优惠券、商店信用积分等智能合约所支持功能。

例如，一家咖啡连锁店可以创建一个商家的代币，并附上促销优惠，为顾客在一天中的某个时间段内提供购买冰饮料的折扣优惠，商家就可以根据活动来计算采购成本并可以根据用户的活跃程度来提供奖励。

最后，Graft 域代币能够提供一种非常行之有效的优惠机制，能够让商家在其域名网络内开发优惠券的创建和转让规则。

去中心化的众筹信用卡

去中心化的信用卡生态是指由信用消费者（持卡人、买家）、信用服务提供商、身份认证提供商和商家（卖家）组成的生态系统。Graft 网络有助于双方之间进行沟通和交易，共同执行相应规则以减少欺诈的风险。

Graft 网络将潜在的信用消费者与信用卡的提供商紧密联系在一起。任何有 Graft 钱包（免费应用程序）的人都可以成为信用卡消费者。任何有 Graft 钱包，并且钱包中有余额的用户都可以成为信用卡的提供者。任何拥有 Graft 销售点（免费应用程序）或与 Graft SDK 接口集成的第三方销售点都可以成为商家。身份认证提供者被作为 Graft 网络上的“插件”，进行身份授权的服务代理。身份提供者使用开放的 API 接口来维护整个生态系统的开放性和分布式特性。

信用卡提供者设置了身份认证的最小要求标准、获得信用的额度、最大信用额度、总体最大信用额度（来自多个提供者）、信用利息、最低付款金额和支付频率。信用卡消费者只要目前的账户状态符合供应商的要求，即可从多个信用卡提供商出获得授信金额。身份认证提供者对用户身份进行验证并确认消费者提供的相关身份信息，以消除信用卡提供者需要进行身份验证的负担，并为持卡人提供一定程度的匿名性和隐私性保护。因此，身份认证提供者能够知道消费者的真实身份，可以独立于网络存在，让信用卡提供商能够长期查看到用户的信誉评分。信用卡提供者能够从用户使用信用卡支付的每笔付款中获得一定的交易手续费用。

系统会对**信用卡消费者**进行信誉评分，该分数是根据消费者的交易历史记录和持卡人提供的身份信息以及由身份认证提供者验证过的身份级别来动态计算的。在任何身份验证或任何历史数据收集之前，用户的初始分数将被设置为 0。用户提供的认证的身份信息元素越多（例如驾驶执照、生物识别、社会保险号），获得的初始得分就越高，持卡人就可以获得更多的信用评分。及时的还款记录也会提高用户的信用评分。

商家是与信用卡消费者交易的接收者，与持卡人、信用卡提供者和身份认证提供者之间的关系完全隔离，完全消除了欺诈风险。信用卡提供者承担所有潜在的欺诈风险和费用，但他们同时会收到交易处理的手续费和信用卡产生的利率费用，通过这种方式对他们予以补偿。然而，商家可以通过提供诸如交易现金折扣等激励措施，甚至也可以作为信用卡提供者参与到此过程中。

安全性

近期随着零售业和酒店行业大面积数据泄露事件的发生，安全性成为任何支付生态系统中非常重要的因素之一。安全性是系统设计中必不可少的一部分，而不是在系统创建完成后要“附加”的功能，只有这样才可以实现系统最高级别的安全性。现有存在的支付卡片，在设计中没有太多考虑到安全性，并且也不支持使用加密货币，所以它们只能抵御大多数类型的攻击。支付系统的安全性不仅仅是信息安全，还应包括财产安全。除了要继承普通银行卡片的标准安全功能外，Graft 还将实施多种增强的功能，从而让买家和商家共同受益。

可用性

超级节点的分布式网络确保网络的“永远”可用性。客户端应用程序能够同时与多个超级节点通信，协商一致后获得授权认证。如果其中一个超级节点被关闭，将通过在候选节点列表中进行选举的方式，将它自动替换为其他相关的节点。

身份管理

依赖于钱包方式进行用户管理为系统留下了很大的安全隐患，因为钱包通常是单独地实施安全防护措施，所以会受到单独的影响。为了保护网络并确保用户身份的完整性，，通过在钱包中调用 OpenID Connect oAuth2 这 3 个 API 接口，Graft

将实施分布式的身份提供商服务（嵌入超级节点。

因此，不管是否实施钱包机制，用户的验证过程和认证将由移动网络进行，这将防止用户身份信息受到损害、欺骗、重华和中间人攻击。

身份识别、认证和授权

现有的加密货币认证/授权一直是通过用户应用程序的权限进行，如钱包，并且在很大程度上是事后进行的。然而，在买卖双方之间进行金融交易的情况下，双方当事人之间必须建立起一定程度的信任，必须共同处理条例和合规性，并提供追索权，所以急需一个良好的认证/授权机制。

身份验证

身份验证是一个具有挑战性的话题，因为它要同时兼具监管和隐私性的要求。同样有效的身份验证也是非常重要的。

要理解清楚身份验证需求的重要性，举例说明，卖家只会将商品药物销售给具有完整身份证明的买家，而买家只有通过更高级别的身份验证才有资格购买武器（在美国 NIST 特刊 800-63A 中规定）。相反，在市场购买商品的买家可能也希望，卖方能够提供更高级别的身份验证来保护自己免受购买被盗商品的侵害。
Graft 希望客户在使用应用程序时，能够遵守当地相关的身份验证标准规定。超级节点将提供基于机器身份验证和欺诈检测的资源，以帮助商家（和用户）遵守合规性，确保支付网络的完整性和交易的安全性。用户在分享了完整身份后，系统为了限制对用户身份信息的曝光并且要遵守相关的监管法（例如 GDPR），Graft 将提供身份属性信息的请求和共享，例如用户的年龄、地址等，以确保遵守当地

的法律法规。我们还希望将更多的元数据收集并添加到身份属性共享中，以支持后续的业务逻辑来发，如药品的检查或忠诚度积分奖励。

Graft 也支持两个或多个用户共同控制的功能（如从该用户帐户中扣除资金）时，在多个用户需要访问相同的商家账户时候，Graft 能够提供可选的多用户控制机制。

使用生物特征识别的双重因素认证机制

Graft 将实施最佳实践、高级身份验证以及用户管理服务，其中将包括基于登录/使用模式以及设备和网络特征的风险/威胁分析、复杂的多重身份验证因素，包括生物特征识别，FIDO 等无密码的因素和相应的技术方案来识别用户身份。

用户 ID 的引入会避免出现“丢失密钥”的问题发生，还能够在多种情况下更加快速、可靠得识别用户身份。因此，UserID 将由多个元素（键）组成-包括绑定到硬件钱包设备中的一些用户生物识别技术，它们将通过更加灵活的属性集合，共同为用户识别提供基础的保障。例如，用户可以通过从可用的 ID 元素（如面部、指纹、虹膜、硬件钱包、设备等）中选择 2 个因素来进行用户验证。未使用的因素也将成为验证用户身份的一系列其他因素。

我们系统的最终目标是在各类设备上以及各种情况下，快速、可靠的使用户识别和认证，同时也能够根据用户偏好和限制为用户提供身份认证因素的选择。

图 3：生物特征多重因素识别是 Graft 现有技术组合中的一部分

信用得分-拒绝暗箱操作

Graft 将采取基于风险控制的交易处理方法。为网络中的每个参与者分配一个信用分数，该分数也将根据系统捕获到的新数据动态的更新。买家、商家和超级用户所有者可以选择将他们的部分身份信息链接到帐户中，以便能够获得更高的信用评分。通过这样一个环节能够让交易实现可追溯性。

信用评分系统能够帮助生态系统中的参与者做出明智的决策，同时也不会影响到安全性和隐私性。例如，商家在即时授权之前，可以考虑买方的信用分数，来作出的是否进行授权限制的决定。买方也可以在对不能立即发货的货物进行付款之前，查看商家的信用分数。买家和商家都可以通过网络中的超级节点查看他们的信用评分。

超级节点负责监测、计算、更新和并对买家、商家和其他超节点进行信用评分。并使用特殊的预测分析算法进行分数计算，该算法能够很准确的产生 0-100 分的计算结果，且不会泄露关于交易的金额、数量、时间或性质的任何信息。

波动性

大多数商家希望用户通过美元（或其当地法定货币）进行支付。商家更愿意使用法定货币，而不是比特币或其他加密货币来进货、支付账单和雇员的工资。此外，他们还可能会在退货时使用法定货币进行退款。他们经受不起代币价格的剧烈波动，特别是对于小商人。Graft 通过即时的、实时交易结算体系解决了波动性的问题，从而最大限度地减少了由于代币波动所造成的价值损失。商户的支付应用程序可以自动将交易金额调整为当前汇率，并在交易完成后通过在线交易将其兑换为当地法定货币。

客户支持、争议解决和支付保险

大多数消费者和商家在使用的加密货币时候，遇到的主要障碍就是在出现问题时，缺乏权威性机构的帮助来解决技术和业务问题。此外，在出现人为失误、欺诈活动或技术故障的情况下，不可能及时“修复”错误的加密货币交易。显然，所有这些问题都是通过去中心化、匿名性和独立的加密货币支付来产生和进行证明的。但是，这些特性却无助于解决用户问题。开源社区通过为用户引入免费的开源产品支持，来解决这些问题。由 Oracle 支持的 MySQL 数据库，和由 Redhat 所支持的 Linux 操作系统就是为免费开源产品提供商业级支持的两个成功案例。

为了能够让用户方便快捷的使用 Graft 进行支付，Graft 基金会向 Graft 账户持有人提供免费的客户支持和争议解决服务。交易量高的商户可以获得 7*24 小时全天候的支持和争议解决协助。Graft 基金会或服务经纪人可以承担 100 美元的支付保障费用，并补偿客户或商家因欺诈或技术问题而损失的资金。

隐私性

通常，用户对隐私性的需求有片面的见解。实际上，大多数合法买家并不介意向

商人披露其身份，特别是在他们会受益于这种信息披露时，或者这种信息披露对处理交易是必需的。以同样的方式，买家要确保商人是合法的人或组织机构，且不是假冒者。商人和买家都不想让自己的身份被轻易的识别出来，他们的信息将会被记录在可公开访问的区块链上。

隐私性是加密货币和支付行业的一个微妙话题。具体情况要根据卖方和买方的实际情况进行判断，隐私权的要求标准从完全匿名到完全透明。例如，卖家为了遵守相关的合规要求，会收集和验证某些用户的身份数据，例如酒类或卷烟的购买会验证买家的年龄，线上商家会要求买家提供收获地址及邮政编码。另一方面，买方有权同意或不同意披露其身份的全部或部分属性信息。如果卖方和买方可以就共享的身份属性信息达成一致，则可以进行交易。此外，在许多情况下，商家需要建立身份属性的真实性。

我们发现，解决这个问题的最佳方法是使用身份验证和身份属性信息的共享系统，该系统与政府监管机构制定的数字身份指导方针相一致，这些准则侧重于增强用户隐私（即美国的 NIST 800-63 或欧盟的 GDPR）-区分身份证明和认证的标准。

Graft 对 Graft 钱包实施了数字身份档案信息，能够在交易时根据用户权限和数字身份信息，向用户逐步共享数据。这些权限包括在每个交易中有选择性地共享某些属性（如年龄、家庭住址、地址、名称等）。

Graft 所实施的 CryptoNote[21]将作为底层交易记录协议，通过隐藏发件人和接收者的信息，为用户提供与比特币和其他加密货币相类似的高度隐私性。

用户应用程序

所有 Graft 用户应用程序都是基于“瘦”客户端，在客户端上不存储区块或处理任何交易。用户的应用程序使用了远程 API 调用接口与 Graft“永久”节点进行通信，这些 Graft 节点能够挖掘新的交易区块并实时处理交易请求。

对隐私权、匿名性和可用性（例如，大型商家或秘密组织）要求更高的用户可以运行自己的超级节点，甚至可以将多个超级节点用于和私有客户端进行通信、转发消息和交易处理，其他超节点能够通过 Graft 进行离线授权，享受商店信用积分、礼券和用户忠诚度活动。另一种解决方案是通过远程 VPN 或 TOR 网络连接到超级节点。因此，超级节点将可以通过 TOR 网络进行访问。

消费者的应用程序包括：

桌面和移动商店销售点的应用程序，用于接受 graftcoin、比特币、山寨币和信用卡/借记卡的支付，以及为买家和商家提供比特币、山寨币转换为本地法定货币的服务。

桌面、移动设备和 Chrome 浏览器的扩展程序，用于使用 graftcoin、比特币、山寨币和信用卡/借记卡（通过使用即时交易）进行付款的电子钱包应用程序，以及发送、接收和交易 graftcoin。

Graft SDK 接口能够让商家销售点软件和购物车进行集成，用于处理线上和线下的实体交易。 Graft 将纳入 Graft 智能卡片支付方式。除了保存用户密钥之外，该卡片还将存储用户的生物特征识别签名信息以及可用于终端认证的一组记忆密钥。Graft 基金会和服务经纪人将支持智能卡和智能读卡器的生产。

除了支持消费者的（B2C）交易之外，Graft 还支持将现有的业务流程整合到 B2B（企业对企业）交易中。这样的工作流程可以根据用户的信用条件（例如，净值 30,60,90）自动收集到复杂工作的流程范围，例如对海关托运单进行结算，按照用户批准的里程碑计划为其分配资金，并将其作为整体交易的一部分。

Graft 也将在物联网中发挥重要作用，能够为一些物联网设备提供数据或服务的“收费”。其中一个例子是线下实体商人能够根据后端系统和传感器的信息来确定的库存量，以及如何呼叫卡车进行运输。

结论

如果没有各位加密货币的先行者，就不会有 Graft。它是基于其他加密货币先行者进行过测试的想法、原则和技术。Graft 使用了加密社区开发的最新技术以及最新开发的交易处理和安全解决方案。这些新技术将能够让 Graft 与传统的支付方式和现有中心化的支付机构进行竞争。

参考文献

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/.