



**VERGE**

最注重隐私的加密货币

BLACK PAPER

## 1.0 引言

为了应对互联网交易的固有缺陷，2009年开发并发行了比特币。在其白皮书中，中本聪解释说，“互联网上的贸易，几乎都需要借助金融机构作为可资信赖的第三方来处理电子支付信息。。虽然这类系统在绝大多数情况下都运作良好，但是这类系统仍然内生性地受制于‘基于信用的模式’(trust based model)的弱点。”[1]自2009年创始以来，比特币已被迅速纳入到今天的现代市场中。随着比特币的迅速普及，出现的一个主要问题是，对处理各种程度大型交易的原始区块链的需求增加了。随着需求的增加，交易等待时间也延长了，从而使得加速交易确认时间的尝试费用随之增加。

比特币背后的核心创新在于其分散化结构。与传统的法定货币不同，比特币没有中央控制，没有中央信息库，没有中央管理，也没有中央点故障。然而，比特币面临的一个挑战是，围绕比特币生态系统建成的大部分实际电子服务和电子商务是中心化的。由于当前系统的中心化，电子商务由特定地点的个人使用，这些个人使用易受攻击的计算机系统，易受法律纠纷的影响。Verge是目前可用的真正去中心化货币之一，因为它一直承诺，构建比特币的核心基础，同时引进实现匿名的全新层。

## 2.0 Tor网络

Tor，源自原软件项目名“洋葱路由器”，是一种IP混淆服务，能够在基于电路的分层网络中实现匿名通信。Tor通过一个由七千多互联网中继组成的免费全球覆盖网络来引导互联网流量，隐藏用户位置和使用情况，以防止任何人对其进行网络监视或流量分析。由于对Tor发送数据包进行匿名的加密地址信息层与洋葱相似，故名。这样，通过Tor网络的数据包路径不能被完全跟踪。Tor的用途在于，通过保护用户的互联网活动不受监视，来保护用户的个人隐私、用户的自由，以及进行保密通信的能力。

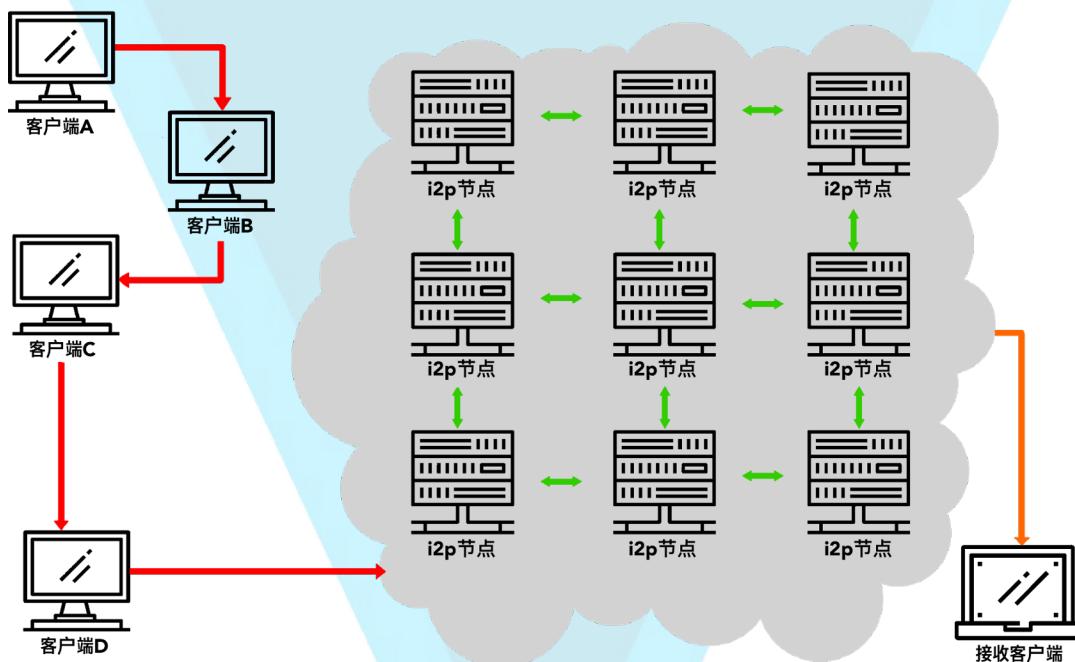
洋葱路由通过加密通信协议栈的应用层实现，就像一个多层嵌套的洋葱。Tor多次加密数据，包括加密下一节点的目的地IP，并通过一个由连续的、随机选择的Tor中继组成的虚拟电路进行发送。每个中继只有解密足够的数据包封装才能知道数据来自哪个中继以及哪个中继将其传送给下一个中继。然后中继在新包装器中重新封装数据并将它发送出去。终端中继解密最内层加密数据，并发送原始数据到目的地，而无需显示，甚至无需知晓源IP地址。

由于在Tor电路的每一跳转中，通信路由部分被隐藏，所以这种方法消除了通过网络监视来确定通信节点的任何单点，而网络监视依赖于知道其来源和目的地。

### 3.1 I2P集成

i2P的初衷是提供隐藏服务，允许人们在未知地点托管服务器。i2P提供许多跟Tor一样的好处。两者都允许匿名访问在线内容，利用P2P式的路由结构，并且两者都使用分层加密操作。然而，i2P的目的是成为“互联网内的网络”（见图2.1），它将流量停留包含在边界内。i2P执行基于数据包的路由，这与基于电路的Tor路由恰好相反。这样做好处在于，允许i2P动态绕过拥塞和服务中断，这种方式类似于互联网的IP路由。这给网络本身带来高度可靠性和冗余。

图2.1  
i2P交易发生过程



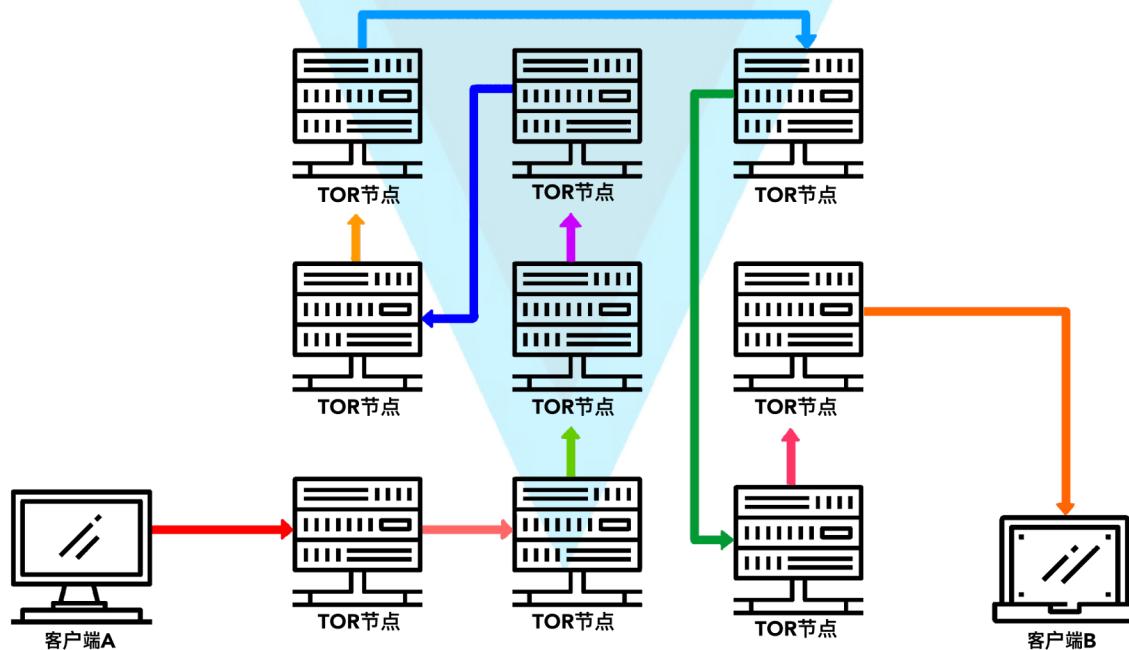
当有一个客户端第一次联系另一个客户端时，它们会查询完全分布式“[网络数据库库](#)”——一个自定义的结构化[分布式哈希表\(DHT\)](#)，它基于[Kademlia算法](#)[2]。这样做是为了有效地找到其他客户的入站隧道，但是他们之间的后续数据通常包括该信息，所以不需要进一步的网络数据库查找。

### 3.1 I2P集成

I2P 是一种利用IPv6提供的高度混淆隧道服务，可以匿名化通过网络发送的所有VERGE数据。每个客户端应用都会用自己的I2P“路由器”建立几个出入“隧道” - 在一个方向上传送数据的节点序列（分别发到/自客户端）[2]。反过来，当客户端希望将VERGE数据发送给另一个客户端时，该应用通过可定位到另一客户端入站隧道的出站隧道来传递消息，最终到达目的地。

不是依赖于一套集中的目录服务器组，像Tor那样，I2P采用分布式哈希表来协调网络状态。分布式哈希表或DHT是一种分布式分散机制，它往往把内容与哈希值关联起来。DHT的主要优势在于其可扩展性。成功的分散式P2P网络要求其服务具有良好的可伸缩性，以确保内容或事务共享的大小可以按需增长。此外，I2P不依赖于受托管的目录服务来获取路由信息。相反，网络路由不断动态更新，每个路由器不断评估其他路由器。最后，I2P建立了两个独立的单纯隧道，发自/到主机的流量可穿越网络，这与Tor的单双工电路恰好相反（见图1.1）。

图1.1  
Tor交易发生过程



请注意：TOR节点每10分钟跳转一次。

## 4.0 Electrum

Electrum的优势在于速度和简单性，且占用非常少的资源。它使用安全的远程服务器来处理Verge网络中最复杂的部分，还允许用户使用保密种子短语来恢复他们的钱包。此外，Electrum提供了一个简单易用的冷存储解决方案。这可以让用户能够以脱机方式存储自己的全部或部分Verge币。此外，Electrum是提供本地Tor和i2P支持的少数钱包之一。通过将Electrum与Tor和I2P集成，在使用桌面版/移动版钱包时可以实现匿名。IP地址和交易信息都是安全的，不会泄漏给连接服务器；增强了用户隐私。

Electrum采用多方签名支持，需要一人以上的密钥来授权一笔交易。Verge网络上的标准交易可以称为“单方签名交易”[4]，因为转账只需要一方签名——与Verge地址相关联的私钥所有者。Electrum交易，采用多方签名支持，在Verge币转走前需要多人签名。然后Verge需要提供多个不同签名方的地址，以进行有关操作。

下面是一个例子：

“一个Electrum钱包在您的主计算机上，另一个则在您的智能手机上-如果没有这两种设备的同时签名，就无法花掉这笔钱。因此，攻击者必须同时访问两种设备才可以偷走您的货币”

## Electrum钱包的关键特征

### 确定性密钥生成

如果您丢失了您的钱包，您可以从种子中恢复它。防止您错误操作。

### 交易在本地完成签名

您的私钥不会与服务器共享。您不必使用您的Verge币来委托服务器。

### 快捷

客户不用下载区块链，它会向服务器请求区块链信息。没有延迟，始终保持最新。

### 自由与隐私

Electrum服务器不存储用户帐户。您不用依赖于特定的服务器，服务器不需要知道您是谁。事实上，Verge和i2P服务器甚至不会获取客户端的IP地址。您还可以导出您的私钥，这意味着您拥有您的地址。

## 5.0 多算法支持

Verge是一种多算法加密货币，目的是让使用不同采矿设备类型的人有平等机会赚取Verge币。它是在一个区块链上支持5种散列函数的仅有加密货币之一。这就提高了安全性，可以使更多的人和设备能够挖掘Verge币，从而确保每个人都有平等的Verge币分发机会。

Verge币总供应量为165亿枚。让Verge币在各种加密货币中脱颖而出的是，在其区块链上运行的5种工作量证明算法，即，Scrypt、X17，lyra2rev2，MYR groest1和blake2s。5种算法都有30秒的区块目标块时间。难度只受算法哈希率影响。这可以提高安全性，并可预防51%的攻击。

## 6.0 安卓Tor + I2P

Verge走在移动加密货币的创新前沿。我们率先开发了两个独特而一流的安卓钱包。其中一个专门在洋葱路由器网络（TOR）上运行，另一个则专门在隐身互联网工程（i2P）上运行。Verge的Tor和i2P钱包都是以匿名为前提而构建的。钱包没有内置能力连接到或在Clearnet上广播用户信息。交易通过简单支付验证（SPV）完成，SPV是中本聪论文中所描述的一种技术，它允许钱包通过相容性证明来验证交易；是一种在无需下载整个区块的情况下验证某笔交易是否包含在某一区块中的方法（类似Electrum钱包功能）。

SPV可以进行近乎即时的付款确认，因为它作为瘦客户端，只需要下载区块头，区块头比整个区块要小很多。Verge的Tor和i2P钱包还带有内置安全功能，如针对附加层物理安全的4位数PIN码和生物识别锁特性。

此外，Verge的Tor和i2P钱包能够利用即时验证来处理P2P的QR码扫描交易。客户还可以根据需要，导入纸钱包中的QR码，以拉出冷存储中的余额。

## 7.0 未来开发：RSK

[Rootstock](#)，通常称为RSK，是一种双向的楔入式侧链，将智能合约功能移植到Verge币网络上。它还引入了一个的链外协议，可以实现“接近即时”的支付。RSK是一个独立的区块链，它没有自己的代币，而是依赖于现有的代币（如Verge币）。RSK通过挂钩（或匹配）其智能代币到Verge币来实现这一点，所以一个RSK代币的价值就是一个Verge币的价值。用户能够在两条链之间自由转移自己的代币。

智能合约的工作方式是，它通过将用户的Verge币变成一种存储类型，这时Verge币被锁定，然后用户获得RSK代币，称为智能XVG。然后您可以把这当作是将自己的Verge币放到一个支票账户，然后使用RSK网络来花掉这些钱。需要注意的是，比特币目前已经允许用户创建一些简单的智能合约，如多方签名-要求两个或更多用户在释放一笔付款之前进行签名。随着RSK在Verge上的实现，RSK使简单的智能合约发展到另一个高度，其图灵完备的智能合约能力与以太坊的产品不相上下。

RSK还解决了另一个问题，即扩展能力。RSK目前每秒可以处理400笔支付交易，与我们目前的固定成交率相比，这是一巨大的飞跃式进步；后者大约每秒100笔。RSK的开发团队表示，其目标是使用称为Lumino的第二层技术（该公司），把标杆推向新高，以实现每秒处理2000笔交易。LCTP白皮书称Lumino网络是一个链下支付系统，依靠Lumino交易压缩协议（LTCP）运行。Lumino可以与闪电网络相提并论，而闪电网络是最初为比特币设计的一种扩展问题解决方案，目前正在莱特币上进行测试。

## 8.0 未来发展：Discord 与 Telegram P2P

适用于Discord 与 Telegram（已经发布）的点对点（P2P）交易支持目前正在开发中，预计会在8月份发布给公众。Telegram是一种基于云的免费即时通讯服务，支持Android、iOS、Windows Phone、Windows NT、Linux和MacOS。Telegram使用一种称为[MTProto](#)的对称加密协议。该协议是由尼古拉·杜罗夫和其他开发人员在Telegram中开发的，基于256位AES加密、RSA 2048加密以及Diffie-Hellman密钥交换。Discord是一个专有的免费VoIP应用，已被加密社区广泛采用。像Telegram一样，Discord支持在Windows、MacOS、Android、iOS平台上工作，它还有一个浏览器访问的Web客户端。在这些平台上实现VergeP2P功能，可使用户随意发送和接收资金，不管他们在哪里都可以（也不管他们是否安装有实际钱包）。

P2P是一种网络技术，允许用户通过互联网或移动设备转移货币。为了做到这一点，消费者可使用在线应用，或者在这种情况下使用机器人来指定要转移的货币数量。只需通过用户名指定接收者，一旦发送者发起转账，接收者就会收到使用在线机器人的通知，即，他已经在一个新建立的存款地址中收到了一笔付款。然后用户可以使用简单命令发微博或消息给机器人，如“!取现”，然后会有一组指令提示您如何接收新获得的Verge币。此服务不需要提供有关您想发送的数量以及发送给谁的附加信息。该过程不会保留任何隐私信息，如IP地址、位置和姓名。发起交易的个人身份信息完全匿名。

Verge是为Reddit、互联网中继聊天（IRC）、Slack和Steam提供P2P解决方案的仅有加密货币之一。这些P2P服务允许用户将Verge币转给在同一社交平台的任何人。

## 9.0 参考文献

- [1] Nakamoto, S. (2009). 比特币：一种点对点的电子现金系统. 检索自 <https://bitcoin.org/bitcoin.pdf>
- [2] I2P: 一个适用于匿名通信的可扩展框架- I2P. (n. d.). 检索自 <https://geti2p.net/en/docs/how/tech-intro>
- [3] 多重数字签名 - 比特币维基. (n. d.). 2017年08月08日检索自 <https://en.bitcoin.it/wiki/Multisignature>
- [4] Voegtlin, T. (n. d.). 欢迎查阅Electrum文档！— Electrum 2.5 文档. 2017年08月08日检索自 <http://docs.electrum.org/en/latest/>

其他参考资料-

Gribble, S., Brewer, E., Hellerstein, J., & Culler, D. (2000年10月23日) . 适用于互联网服务建设的可扩展分布式数据结构. 检索自[https://www.usenix.org/legacy/events/osdi2000/full\\_papers/gribble/gribble\\_html/index.html](https://www.usenix.org/legacy/events/osdi2000/full_papers/gribble/gribble_html/index.html)

匿名与区块链 • IHB 新闻™. (2014年11月18日). 2017年08月08日检索自<https://ihb.io/2014-11-17/news/anonymity-block-chain-13570>

Holden, E. (2017年7月18日) . Tor与I2P介绍. 2017年08月08日检索自<https://www.ipvnp.net/privacy-guides/an-introduction-to-tor-vs-i2p>

分布式哈希表. (n. d.) . 2017年08月08日检索自[http://infoanarchy.org/Distributed\\_hash\\_table](http://infoanarchy.org/Distributed_hash_table)

Scharr, J. (2013年10月23日). 什么是Tor-Tor如何工作-如何使用Tor. 2017年08月08日检索自<https://www.tomsguide.com/us/what-is-tor-faq-news-17754.html>

Durumeric, Z., Wustrow, E., & Halderman, J. (2013) . ZMap: 快速因特网范围扫描及其安全应用. 检索自<https://zmap.io/paper.pdf>

Voegtlin, T. (2015) . 简单支付验证 — Electrum 2.5 文档. 检索自<http://docs.electrum.org/en/latest/spv.html>

SPV简单支付验证 – 比特币的词汇. (2017). 检索自 <https://bitcoin.org/en/glossary/simplified-payment-verification>

<http://www.citefast.com>

<https://atlas.torproject.org/#search/flag:authority>

<http://torstatus.blutmagie.de/>

# 10. 贡献者

作为一个开源项目，我们非常感谢我们所有的贡献者，他们为我们提供了帮助，让我们实现今天的目标。

为此，我们想说声

谢谢

中文译员

[昵称]

作者

CryptoRekt

Verge核心开发人员

Sunerok

Gfranko

CryptoRekt

贡献者

Verge营销团队

@Spookykid	@deheerlen
@CryptoRekt	@Twomanytimes
@gfranko	@ScagFX
@DJ_Erock23	@TraderNILW
@Crypto_K1NG	
@JtheLizzard	
@lucklight	
@Cryptonator92	
@feyziozsahin	
@Slemicek	
@Trilla6six6	
@Dabbie USA	
@Cyrus7at	
@Thehunter9	
Netherlands	
@GGWeLost	
@Jeanralphio69	
@Crypth	

GitHub贡献者

Sunerok	Infernoman
Gfranko	pallas1
CryptoRekt	bearsylla
Mkinney	2Dai
badbrainIRC	31percent
Grinfax	Racoooon
Swat69	ceasarpolar
NeosStore	enewnanwebdev
Koenwoortman	giovanni1186
Hellokarma	labelmeagod
Kirillseva	
Fuzzbawls	
Buzztiaan	
Spiralmann666	
stshort	
alcy0ne	
chisustation	
ShapeShifter499	

联系信息

[推特](#) [Telegram](#) [Slack](#) [脸谱网](#) [IRC](#) [Reddit](#) [Steam](#) [Verge](#) [Discord](#) [BitcoinTalk](#)  
[广播电台](#)