Hu6in Mosson6oJ Wui\odedoJ

在\Jopuo\ion

Hugin信使是一个去中心化的私人信使和社交网络，使用本地加密货币支付。有了它，你就可以进行安全的通信，进行不可追踪的交易，所有这些都没有任何可信的一方。

如今市场上有很多私人信息服务，但它们到底有多私人是一个争论的焦点，而且你往往必须从表面上接受他们的承诺。因为他们的系统部分是闭源的，或者他们有不透明的分销线，比如谷歌Play或苹果应用商店[1]你必须相信开发人员的能力和意图。此外，如信号、WhatsApp、脸书信使等集中式系统依赖于特定公司的服务器，它们可能会受到第三方的胁迫，这可能导致关闭、强制解密私人信息、审查以及滥用权力。

集中的服务器结构，即使是分布式的，也会成为避免言论自由的威裁政权审查的受害者，比如伊朗的信号被审查，导致信号混淆其服务器的起源与亚马逊拥有的域名Souq。com.作为回应，亚马逊威胁要关闭AWS的服务，这可能导致严重中断，最坏的情况是导致网络中断[2].

要构建一个能够完全避免这些潜在问题的私有消息传递服务，传输、存储和客户端应用程序的整个基础设施必须基于开源和去中心化的技术。

通过分散可以保护网络被审查，离线，或以某种方式不可用，仅仅因为没有单点的失败——你必须关闭网络中的每个节点有效地关闭网络，即使这样，新节点可以在任何时候加入网络。

分散化也是实现隐私保护的另一个重要前提条件，即无许可操作。在传统的集中式系统中，中央当局控制权限，这可能会迫使您放弃个人信息来使用网络。在一个分散的系统中，没有这样的权威。任何人都可以在任何时候与网络交互，没有任何限制——根据Hugin的案例共识规则，这些规则对所有用户总是相同的。

去中心化的另一个积极特点是，它可以使某些操作的成本大大降低，进而更具可扩展性。例如，在Hugin信使中，您可以进行真正的对等-2-对等调用，其中数据只在您和收件人之间传输。在一个集中的系统中，该调用将通过一个集中的服务器进行中继，从而花费

1 https://drewdevault.com/2018/08/08/Signal.html
2 https://signal.组织/博客，正面回顾

集中实体有价值的资源，反过来激励它从用户与服务的互动中获利。在作为数据出售之前，对这些电话进行转录、分析和希望匿名是可行的。由于用户基础增长和数据量的增加，Hugin没有这种获得更多利润的竞争。之所以能实现这一点，仅仅是因为数据存储在对等-2-对等网络中，其中大部分数据只存储在受影响的各方之间——比如调用、文件共享等。

通过开源，用户和专家可以联合努力审查源代码，确保它是安全和合法的——这个过程已经被证明可以创建最健壮和可靠的系统[3].

Hugin Messenger还允许你在同一协议上的消息无缝发送价值交易，没有不必要的碎片或复杂性——换句话说；Hugin生来就是一个综合信息服务和一种将隐私放在第一位的金钱交易工具。

特点

私有消息

Hugin信使是一种私人信使，它使用军事级加密来保护通过加密加密货币点对点网络传输的信息。

由于Hugin信使使用的高安全性加密，可以发送只能由发送方和接收方读取的私人加密消息。没有中间人可以保留任何主键，所以没有任何人可以窃听。

私人视频和语音通话

有了Hugin信使，你就可以进行私人的点对点视频和语音通话，这在视频和音频质量以及隐私方面往往优于主流服务。

文件共享

Hugin信使允许用户发送任何大小的文件，没有任何成本或限制，其中文件是完全点对点发送。

社交网络

Hugin还有一个公共（和私人）董事会功能，用户可以以一种类似于社交媒体平台的方式发现新的社区和用户，但有额外的好处是完全分散和无许可的。

[3]https://courses.cs.华盛顿。edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf

技术

区块链

胡金信使运营的基础层是氪星区块链。加密币是一种基于加密笔记协议的加密货币[4]，它首先由字节币开发者实现，并由龟币开发者进一步开发。

《加密笔记》是中本聪工作的延续，该工作旨在改善比特币的一些问题，如矿工集中化、缺乏隐私和
可替代性与比特币不同，加密笔记提出使用环签名和隐藏地址来使交易不可跟踪，这是Hugin保持gin信使隐私所必需的。此外，CrypotoNote还为我们提供了一个优秀的P2P网络，可用于中继消息和事务。

简化的氪星事务，包括要发送的XKR量、发送到的地址和一些可选的额外数据。使用Hugin信使，我们发送少量的XKR和一个加密的信息到收件人的XKR地址。（请参阅图。1).

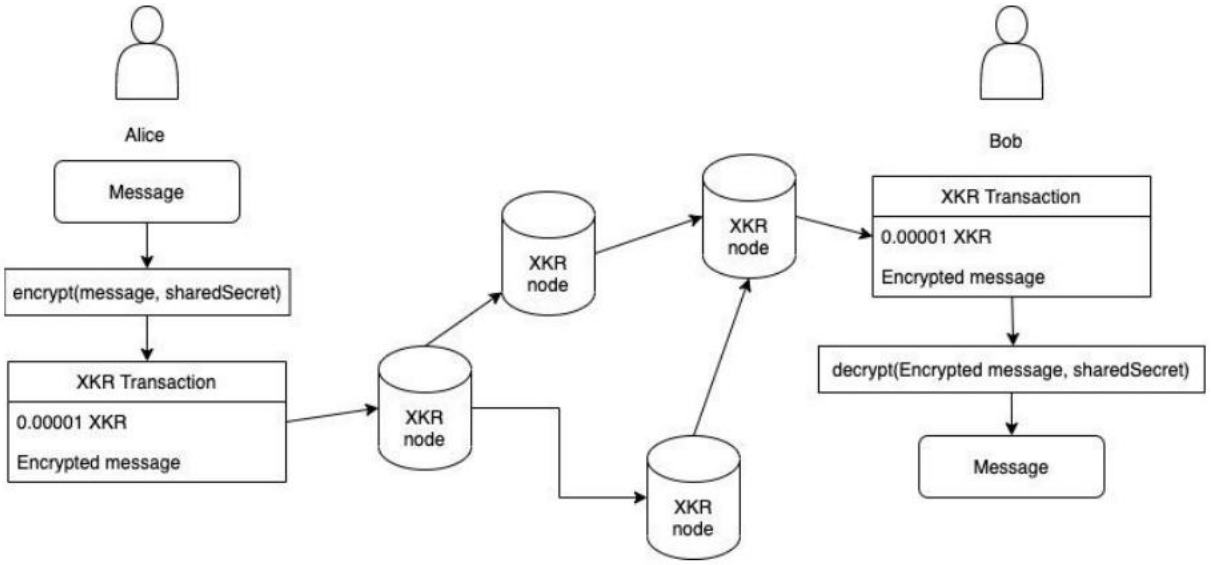

Fig. 1

在上面的图中，Alice向Bob发送一条加密的消息，该消息通过XKR节点网络传播，当它到达Bob当前连接的节点时，他将尝试解密它，如果可以的话，他将收到消息。

[4]https://bytecoin.org/old/whitepaper.pdf

氪星节点是任何人都可以使用树莓派，这意味着Hugin是一个联邦网络，其中消息的整个传输和处理是完全分散的，独立于受信任的各方或节点。

节点不知道消息或事务属于谁，谁发送了它们，也不知道关于消息的内容或性质的任何其他内容。这是通过使用加密注释协议和对消息的非对称加密来实现的。

在线用户一旦到达用户当前所连接的节点的事务池，就会收到一条新消息，而不必等待额外的~90秒才能将其存储在区块链本身中。

在创建块时，包含Hugin消息的事务将被节点忽略，并定期从节点内存中删除。当它们被删除时，用于发送消息的XKR将被退款给发件人，并且可以再次使用。通过这种方式，当你发送的数据在网络上发布时，你“赌”硬币。

Hugin板的工作方式类似于私人信息，但不是每个用户都有自己的钱包，其成员都订阅了相同的XKR地址，并将消息发送到这个共享的XKR地址，而不是直接发送到另一个用户的地址。

私人董事会和公共董事会之间也有区别。**公共委员会是未加密的，可以作为公共讨论论坛使用。**另一方面，私有板是用共享的私钥加密的。与私人一对一的信息传递相比，这样做的缺点是，如果团队中的任何一个人受到威胁，整个团队就会受到威胁。

氯化钠

氯化钠（发音为“盐”）是一种新的易于使用的高速软件库，可用于网络通信、加密、解密、签名等功能。NaCl的目标是提供构建更高级别的加密工具所需的所有核心操作。[5]

氯化钠是一个经过良好测试的加密库，被无数项目使用，经过审计，得到了完美的结果[6].

我们使用氯化钠(特别是TweetNaCl[7]JavaScript实现)来保护在Hugin上发送的每一个私人消息，使用NaCl的椭圆曲线密码，首先进行不同-海尔曼密钥交换，其中共享的秘密通过共享彼此的公钥来交换，然后用来计算共享的秘密。这个共享秘密反过来被用于加密和解密消息，使它们能够对共享秘密的两个持有者可用，并且对它们单独使用。

[5] https://nacl.cr.yp.to/
6 https://tweetnacl.js.org/audits/cure53.pdf
[7] https://github.com/dchest/tweetnacl-js

在实践中，这是通过让一个用户共享他们的XKR地址和他们的公共加密密钥来实现的。对于对话中的第一次交换，消息用一个密封的框加密，其中包含发送方的公钥。第一个消息可以在不了解发送者的情况下解密。这一点很重要，因为否则就有必要以明文形式附加发送者的公钥，以便用于跟踪用户。使用密封的盒子，我们可以使这些交换与网络上的任何其他消息无法区分。

随后的消息将使用氯化钠框进行加密，即使用发件人的私钥和收件人的公钥。

对于私人董事会，氯化钠也被使用，但方式不同。私有板使用公钥（非对称）加密，私钥板使用简单私钥（对称）加密。在实践中，这意味着私有板密钥必须在私有通道中共享，以保持安全，而用于私有消息的公共密钥可以公开共享。

WebRTC

WebRTC（Web实时通信）是一个免费和开源的项目，通过简单的应用程序编程接口（api）提供web浏览器和移动应用程序的实时通信（RTC）。它允许音频和视频通信在网页内工作，通过允许直接的点对点通信，消除了安装插件或下载本地应用程序的需要。[8]

Hugin信使使用WebRTC在两个用户之间建立直接的点对点连接，使用户能够在链外向彼此发送数据。然而，要建立这样的连接，您首先需要进行一个信号交换，i。e.交换关于如何相互连接的细节。

在WebRTC的大多数其他实现中，一个中心点被用来共享这些信息，但是Hugin只是将这个信令数据（SDP）作为一个常规加密的Hugin消息发送。当WebRTC连接建立时，就可以在用户之间传输大量数据，从而实现了网络上的每个节点都无法合理存储的音频和视频通话。

[8]https://en.wikipedia.org/wiki/WebRTC

btt是一种用于点对点文件共享（P2P）的通信协议，它使用户能够以分散的方式在互联网上分发数据和电子文件。[9]

Hugin信使还可以通过使用bt来发送任何大小的文件，并将文件分发给大量用户。

btt使用磁铁链接链接到其网络上的文件。使用Hugin，磁铁链接被简单地发送给另一个用户，然后由Hugins内置的bt客户端下载，这使得无缝和快速的文件共享，甚至是最大的文件。

打开别名

最基本的情况是，OpenAlias是一个FQDN（完全限定的域名）上的TXT DNS记录。通过将其与dns相关技术相结合，我们创建了一个混叠标准，对开发者可扩展，用户直观和熟悉，并可以与集中和分散的域系统互操作。[10]

Hugin使用OpenAlias，通过将用户的Hugin地址连接到一个子域，使用户更容易地彼此共享他们的详细信息，例如hugin.xkr.se。

然后，另一个用户可以使用标准的DNS查找来访问地址细节，而不必记住任何类似于标准电子邮件地址的任何东西，而不是163个字符长的Hugin地址。

代币组学

因为Hugin要求用户持有XKR才能与该服务互动，这就产生了购买或挖掘并持有硬币的动机。每次发送消息时，你都要“典当”你的XKR，即使当消息从交易池中删除时收回你的股份，对XKR的需求也会随着Hugin信使的使用而增加。

未来

Hugin可以被看作是HTTP之上的一个协议，一个去中心化的“液滴箱”，你可以在它上面发布任何东西，无论是为你和你的朋友，还是为整个社区。我们未来的目标之一是为开发者带来一个全面的API，使社区能够在Hugin上构建去中心化的应用程序。

这类应用程序可能包括，但不限于，一个直播和录制的视频和音乐流媒体服务，电子商务服务，一个使用原子交换的交易服务

[9] https://en.维基百科。org/wiki/BitTorrent
10 https://openalias.org/

XKR <-> BTC.支持交换的技术已经可以从COMIT网络上获得了。[11]
总结： Hugin可以成为一个可以扩展的Web3.0协议，开发人员可以开发几乎任何服务从旧web，但分散的额外津贴，默认隐私，以及构建支付，拥抱的精神和下一代的应用程序。

总结

Hugin信使使用了一系列有用的技术来实现一个完全分散的和可扩展的私人在线消息解决方案，以及内置的经济工具的内容发布，以实现小费、购物、内容订阅等等。

这个项目的主要目标之一是使非技术用户容易使用安全密码，尽管已经存在多年，没有意义集成公司挖掘数据的商业计划的一部分。

虽然您确实可以使用PGP等工具在任何平台上加密消息，但并不是每个人都有使用这些可用选项的技术知识。通过Hugin，我们已经自动化了这个过程，使它像输入“你好”和点击enter一样简单。

当然，使用Hugin的先决条件是有可扩展的XKR，但使用Hugin你需要非常少量的XKR，今天可以用你的手机挖掘，此外，当你从交易池中清除时取回你的钱。

Hugin信使在其本质上是一个有弹性、安全、私人和不可追踪的消息和交易平台。

在目前的要关头，Windows、macOS和Linux的客户端可以在我们的GitHub上找到[12]，一个安卓版本也在开发中[13].

哈里埃里克森
info@kryptokrona.se
kryptokrona.se
Fri 3 Sep, 2020

[11] https://github.com/comit网络/xmr-btc交换
[12] https://github.com/kryptrona/hugin信使
[13] https://github.com/kryptrona/胡金移动