SKRUMBLE NETWORK

基于区块链的去中心化通讯网络

白皮书

此为样稿，对公众征询意见。如有变动，恕不另行通知。

1. 本白皮书翻译自Skrumble Network 白皮书英文版，如果有表述不一致的地方，以英文版本为准。
2. 注意：Skrumble Network正在进行积极的研究，本文的新版本将会出现在：www.skrumble.network 如有意见和建议，请通过网站与我们联系。

“每每数载，一项崭新的技术，一个遗留的难题，
一个伟大的想法，掀起一场革新”

Dean Kamen

美国知名的工程师、发明家及企业家

目录

前言

如今，人们强烈需求一个简单安全的通讯方式以及通讯网络对个人隐私权的保护。Skrumble Network 将借助区块链技术开创一个强大安全的去中心化的通讯网络，这使真正开放式的安全通讯成为可能。

现在，有成千上万的创新者正在应用区块链技术打造改变世界的解决方案。金融科技公司和政府正在积极探索开发加密货币；专业服务机构在尝试应用智能合约；通过区块链的应用，供应链经理们第一次在第一时间，同时实现了实时库存追踪，以及对其资产所有权的绝对保护。Skrumble Network 将借助区块链技术，创新地运用这一技术，并深入分析去中心化网络如何成为更安全的通讯方式。

本白皮书中，我们将讨论以下议题：存储数据的中心化服务器所面临的风险，用户数据在互联网通讯系统中所面临的威胁，以及创建有意义的网络连接所面临的困难等。对于以上亟待解决的问题，Skrumble Network 的解决方案是构建一个去中心化的拥有无限成长潜力的通讯生态系统，为用户提供安全通讯以及点对点的完全匿名的通讯体验。

采用区块链技术和去中心化网络协议，Skrumble Network 将成为首个安全的、完整的、能突破传统防火墙的通讯生态系统。它可以把任何地点的任何人以一种简单又安全的方式连接起来，实现真正的世界范围内无阻碍的通讯，引导人们进入一个前所未有的区块链通讯时代。它能确保用户的匿名性，内容和数据的保密性，并且 Skrumble Network 将在同一个网络上实现多种功能，包括群聊和点对点短信、呼叫、视频和文件传输等。

行业痛点

1.数据的安全性：以中心服务器为基础的通讯系统面领着数据安全性的挑战。

2. 用户隐私权和数据的所有权：现有的通讯网络很容易被屏蔽或盗用，而且用户没有自己数据的所有权。

3.全球通讯：全球需要一个可信的通讯网络。

1. 数据的安全性：以中心服务器为基础的通讯系统面领着数据安全性的挑战

互联网已经对我们的通讯和连接方式造成了革命性的影响，只要按动一个按键就能进行视频通话，随时可以进行国际商业贸易合作，银行每天进行数万亿的国际转账，并且与一个国家的总统仅仅只是一个推特的距离。随着电子商务的普及，一件商品可以在广州加工生产，通过一家在纽约的公司，售卖给在悉尼的一位女士。社交媒体已经彻底改变了通讯，新闻报道和娱乐方式。互联网已经成功的连接了几乎所有在它网络上的人，但这也同样引起了关于隐私和数据安全性的担忧。

互联网用户习以为常的，或者有时候不自觉地提交了服务条款协议，默认了个人信息的被动分享。这也给予了众多广告公司甚至相关政府收集和使用个人信息的可能性。例如，Google 通过分享用户的数据包括浏览记录和搜索记录来提供它的主要客户服务。Facebook 也向广告商出售他们的用户数据和活动记录，例如发布，点赞和评论。当访问社交媒体或电子商务网站的时候，经常出现一些广告反映了上述数据甚至是人们线下的口头交流，这引起了关于电子窃听和用户隐私的担忧。

通讯应用每天被用于处理海量数据流，据报告，即时通讯应用 WhatsApp 每天处理大约550亿条短信，40亿张照片和10亿个视频传输。然而，就像其他的基于互联网的通讯平台一样，所有数据都经由一个有中心节点的中心化的服务器传输。在这类中心化系统中，侵入一个中心连接节点是很方便的，这会提供给不法分子浏览海量网络数据的通道，同时也给黑客盗取或者篡改数据的机会。基于这些原因，在2018年月，黑客发现了 WhatsApp 安全系统的后门，并成功侵入了群聊。由于这个程度的缺口，WhatsApp 的信誉变得无法令人信服，而此次事件也证实表现了聊天工具端对端加密技术的无效（格林伯格，2018）。

现在几乎没有办法在使用网络的同时避免隐私泄露或被黑的风险。因此用户对于可以不用担心个人信息被泄露，安全通讯的去中心化、不可破解的网络的需求愈发强烈。同时，这种通讯对加密货币世界更加的重要，因为有大量的金钱也正处于巨大风险中。

2. 用户隐私权和数据的所有权：现有的通讯网络很容易被屏蔽或盗用，而且用户没有自己数据的所有权。

当涉及到彼此沟通时，通常人们会将互联网作为主要来源的信息传输。但是，由于互联网有大量的信息来源和可用的论坛资源，人们使用各种不同的交流平台来学习和讨论区块链和其他热点议题。这导致了一种相当碎片化，分离化的社区体验。

使用多种通讯应用，例如Facebook，WhatsApp，微信等，整合和分享信息，使得一个可持续的、可信任的全球标准难以制定。哪怕是像Telegram这类软件其实也会被审查和屏蔽内容，用户信息也有可能会被收集和破解，并能通过已知的 VPN，URLs 或 IP 地址来屏蔽接入（拉塞尔，2017）。事实上，在2018年2月1日，Telegram曾因为 “包含不适当内容” 的原因被苹果从应用商店下架 ，Telegram被要求添加过滤内容以及其他保护性措施（沃伦，2018）。有些应用在一些特定国家被禁用或截留了，从而导致了信息的不平等。比如，Facebook和WhatsAPP在中国境内是被禁用的，并且近期Telegram在伊朗也受到了禁令。事实上，Telegram早已在多个国家被禁用，例如印度尼西亚（多伦多星报，2018-托尔，2017）。

- Facebook、WhatsAPP和Google在中国境内是被禁用的。(India Today, 2017)
- WhatsApp 最近在群聊中被发现设有后门。(Greenberg, 2018)
- WeChat 微信监控用户的会话，并不在多个设备上同步。(WeChat, 2018)
- Telegram 积极地监控内容，并在不久前被伊朗禁用了。(Toronto Star, 2018)
- Facebook 和 Google 将用户活动分享给广告商们。(Facebook, 2018; Google, 2018)

此外，热衷于讨论新科技或其他话题的特殊论坛可能受到另一种形式的监控。举例来说那些热衷探讨加密货币的论坛， 比如 Bitcointalk 或 Reddit。一个关键的市场壁垒对加密货币感兴趣的人来说，就是缺乏足够关于加密货币交易合法性的信息。当涉及到准确度，公信力和信任的时候，这些论坛通常有一定的局限性，因为他们大多数都是由个人观点组成的，并不一定源于可验证的事实。

人们也在主流的视频分享平台如 YouTube 上寻找关于加密货币生态系统或其他的信息和教学。这些内容也面临着诸如单向性的，不可靠和基于个人观点等问题，提供的话题及相应观点相对肤浅。同样的，因为这些通讯都使用中心化网络，他们也面临着我们之前讨论过的关于被黑客入侵，社交工程和其他安全缺陷的问题。

通过研究，现有的通讯网络社区在每个系统中的缺陷和瑕疵都显而易见。现有的解决方案都是碎片化的，分离式的和不可信赖的，由此也创造了新的关于提高信任和全球互联性的改进方案的机会。通过一种类似全球互联的社区，统一安全的通讯解决方案，能增加和拓展人们互联的机会。

3. 全球通讯：全球需要一个可信的通讯网络

正如上文所提，中心化的服务网络容易被禁用或被监控。人们对于去中心化的沟通工具的渴望与日俱增，因为它能真正地给在世界任何地方的任何人提供一个互连在一起的网络。在防止被黑客入侵或被别人得知个人信息的情况下，他们能自由的讨论，分享信息并传输数据。一个全球化的、去中心化的社区可以帮助人们更好地互相通讯，任何人都可以在此网络上自由交流。

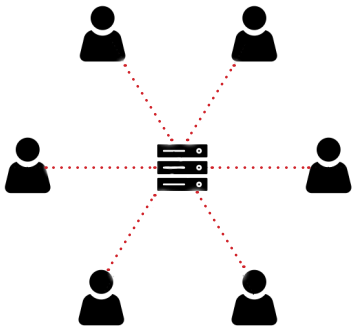
全球需要一个可信的通讯网络，大家可以讨论兴趣爱好，分享故事和自由讨论；当人们连接在一起后，他们能自由安全地分享他们真正的想法并建立有意义的关系；那么革新性的事情将会应运而生。

解决方案

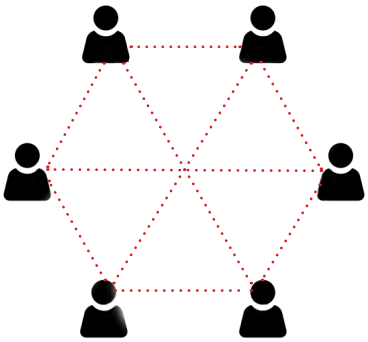
1. 安全：专有通讯技术助力安全保护	2. 去中心化：支持安全通讯交易的 分布式区块链分布式账本

1. 安全：专有通讯技术助力安全保护

传统意义上，通讯平台依赖于一个中心化的服务器来处理信息和储存客户间的数据交流。然而，基于区块链的去中心化网络，信息不再集中储存在单一地点，因此，网络黑客不可能一次性盗取大量用户数据。因为网络罪犯不再能够通过潜入单一中心服务器来控制整个系统。进一步说，黑客或其他网络罪犯如果想把信息从区块链上抹除、更改、迁移到别处或以任何其他方式干扰整个系统都极其困难。去中心化系统所使用的不可篡改的共识技术创造出一个透明且安全的框架，并有着广阔的应用场景。



中心化服务器



去中心化网络

以银行业为例，寻找保护电子交易安全性的解决方案至关重要，而在加密货币辅佐下的区块链技术会成为这个领域的有力竞争者。研究加密货币的经济学家已经确认，金钱已经从实体货币转为电子货币形式，加拿大、印度和俄罗斯等地的政府甚至也开始探索纳入和应用加密货币的渠道（Sabbin, 2018）。区块链自身的不可篡改性降低了交易确认的成本，而其去中心化属性则为交易提供了去除中间人的可能。

这些去中心化网络的特质同样可以为通讯解决方案和身份管理提供新的机遇。区块链技术的应用范围十分广泛，在确保透明性和安全性的同时，能够让更多公众更好地体验到服务和网络的升级及其未来的巨大潜力。

2. 去中心化：支持安全通讯的区块链分布式账本

在1998年，密码学专家及智能协议先驱 Nick Szabo 曾指出：“基于互联网的商务交易需要信任的飞跃。” 而信任本身，一直也是通信和商业的最基本货币。在现今世界，每一秒在陌生人之间发生的交易，通常都需要第三方介入通讯交易。这就意味着，用户和中心处理者之间需要建立起信任关系。不管是发送信息还是产生交易，发送者不得不选择信任中间人能够安全地将交易传导至指定人手中。

通过区块链分布式账本，用户得以安全且直接地相互联络并开展交易，他们无需依赖任何媒介或担心自身隐私保护问题。区块链和去中心化网络能够让人安心地在缺乏信息的环境下，通过分布式账本带来透明、共识和防干扰的交易记录。每一笔交易“区块”都需要得到整个系统的认证，再不可篡改地连接到“链”上从而拥有无与伦比的安全性和可追溯性。

此外，提高网络身份认证管理协定的呼声也一直高涨。确定身份信息现在成为了众多在线账户和交易的必须步骤，这些信息包括个人家庭住址、联络信息和财务信息等。但仅在美国，2017年就有高达1540万居民的受到了金融诈骗侵害、个人账号信息遭到了窃取，这一人数也创下了历史最高纪录（Pascual, 2017）。

分布式账本能够为身份认证提供更好的解决方案，用户无需分享联络信息细节，便有望实现真正的个人信息数字化。基于区块链技术的双重加密体系能够通过公钥和私钥机制，来数字化确定用户的身份，并且彻底免除了备用钥匙传输和信息干扰或窃取等风险。

显而易见，这一问题的答案就是使用区块链的分布式账本，让用户能够同彼此直接联系，从而不必选择去信任第三方或其他未知者。去中心化的通讯体系则意味着，用户能够安全并直接地彼此联系和交易，不再需要担心他们的隐私问题。

SKRUMBLE NETWORK:
保护用户隐私权，构建一个完整的去中心化的通讯网络

一个安全、实时，开源的通信系统毋庸置疑我们的最终的目标，当然，这一系统还需要简单易操作。通过充分匹配区块链生态体系和整合已有的通信技术，一个强劲、安全的通讯体系应运而生，那便是 Skrumble Network。Skrumble科技公司（Skrumble Technologies Inc）即将打造首个基于去中心化网络的完整通讯生态体系。这个特别的生态系统将十分便捷地通过安全网络让全球任何地方的任何人在开放式通讯的前提下相互交流。借助于完整的整合通信技术，用户在 Skrumble Network 上终于能够在完全安全的去中心化环境中搭建起自由的有意义的全球性通讯。

通过特有的共识性算法和自定义用户名的匿名认证方式，用户将保留个人信息、数据和通讯交易的所有权。用户可以自己构建众人参与的社区或同其他用户进行一对一会话，而这些内容都将是隐私且保密的。这个网络将允许客户通过发送信息、通话、视频、文件传输等方式进行无缝 P2P((端对端) 交流，并能够提高用户在通讯、身份管理和无限安全通讯交易等方面的体验。通过分布式区块，Skrumble Network 网络能够在根本上解除当前互联网通讯系统中的安全风险，并将持续采用独家且新型的安全技术。

Skrumble 科技公司认为，采用不可篡改的去中心化网络共识协议搭建的安全通讯生态体系将为人们通讯和身份认证管理的带来又一次重要革新。Skrumble Network充分发挥了 Skrumble 团队现在特有的经验和技术优势，通过开源软件开发工具（SDKs），能够轻松适应第三方的融入需求，并能够进一步开发出适用于不同场景的安全、隐私且匿名的系列应用。

Skrumble Network 打破了区块链协议在金融交易应用的定式，开创了其在非常规领域应用的先河。区块链技术此次将为通讯和认证搭建全球化标准，并将在世界各地得到不同的应用。

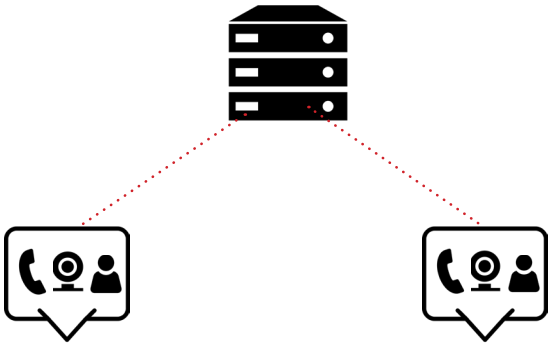
SKRUMBLE 的通讯功能

- 信息发送
- 群组会议
- 匿名认证
- 音频呼叫
- 屏幕共享
- 数据加密
- 视频呼叫
- 用户控制存储
- 支持任何浏览器
- 文件传输
- 截屏通知
- 电子钱包

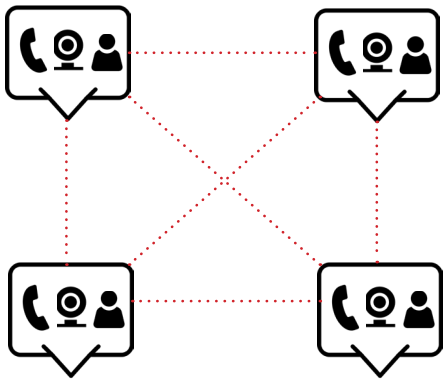
技术概述

简介：基于去中心化网络的安全通讯

传统的通讯网络是基于中心服务器建立的，暂且不论他们自己的通讯协议，其本质上都是一样的功能：通过一个封包数据来实现第一次握手（连接），交换数据，建立实时媒体流连接，随后中心服务器将建立并调解这一通讯连接。然而，Skrumble Network 将完全切除中心服务器，以实现对通讯方式的全面革新。



当前基于中心服务器的网络



Skrumble Network —
无中心服务器的去中心网络

SKRUMBLE NETWORK 的会话 ID & 数据管理

Skrumble Network 将成为一个独一无二的区块链，形成一整个完全去中心化和匿名的通讯网络。通过使用普通的浏览器或者 Skrumble Network 自己开发的应用程序（PC和Mac）即可利用实时通讯协议实现点对点互联。

Skrumble Network 独一无二的安全协议将由一组使用 Skrumble 区块链网络的私钥衍生算法来传输。当要接入网络时，用户需要输入持有代币的钱包的公钥。此外，他们还需要输入一串安全码和自己的网络化名（私有的用户名）。所有这些元素的衍生品将被用于生成他们专有的独一无二的私人Skrumble Network 户ID和公共ID。同时，也将生成一个二维码和链接同步到 Skrumble Network 区块中，供用户更简便的分享他们的公共网络ID。

通过对所有对话进行非对称性质的加密，所有通话都无法被窃取，这种数据加密的子秘钥来源与每个参与者的私人 Skrumble Network 用户ID秘钥。一种衍生算法将在相关联的基于会话的参与者的 Skrumble Network 秘钥中随机选择，所以不会有任何两个秘钥是相同的。这也为系统加上了另一层安全保障，没有任何两个会话会使用相同的秘钥，这也使得Skrumble Network 会话事实上不可能被基于模式的方法解码。举例来说，用户A和用户B各自的私人 Skrumble Network 用户ID秘钥会被随机组合，生成这个通话的子秘钥和通话ID。

当不同用户之间的通讯被建立起来的时候，传统通讯网络中的通过中央服务器来实现的信号交换协议将被Skrumble Network 所取代 。在 Skrumble Network 中，会话描述协议（Session Description Protocol-SDP）信息将使用去中心化服务器来建立第一次握手协议，从而开启会话，实时传输协议（RTP）和媒体流（语音，视频和信息等）来开启数据传输。

一旦在端口间的连接被建立，用户的IP地址将只能被对方看见，并且一个安全网络插座连接将被建立，以开启用户设备间的交互通讯会话，使其可以实时分享包括信息，文件传输和通知等会话数据。这就允许了在极短延时的连接中，数据瞬间被发布。

在 Skrumble Network 上的通讯是P2P模式的，但同时也可以通过网络中的富余通讯桥（ad-hoc communication bridge）来实现大量人员一起进行的语音和视频会议。

Skrumble Network 可以在任何现代浏览器中运行，同时也能在大多数手机和平板设备（IOS和安卓）以及电脑（Mac和PC）上当做一个独立的应用来使用。独立应用版本相比浏览器版本将提供更多额外功能。

SKRUMBLE NETWORK 通讯认证区块链协议

Skrumble Network 将开发自己独立的区块链，来建立独一无二的安全可靠的特殊通讯会话。Skrumble Network 的区块链将被用于应用的多个方面：

1. 建立初始的通讯会话。
2. 同步用户的化名以及Skrumble Network的用户ID。

两个功能都需要矿工的算力支持以此提供的一致性认证和鉴别。Skrumble Network将开发一套客观的奖励和扩展程序，用以激励积极做出贡献的主节点服务器，以及矿工社区的成员。

未来无与伦比的数据容量和速度

现如今，当用户想在现有的基于区块链的应用上开展活动和操作的时候，新的转账记录和数据被保留并存储了，更多转账被保存，也意味着更长的加载时间。举例来说，在以太坊上的转账通常需要花费约20秒的时间来达到确认（Yannik，2017）。随着通讯传输总量的提升，Skrumble Network 需要把每次信息，语音，视频和文件作为单独的交易转账来传输，这也将导致每个用户的服务速度降低。因此，为了解决这至关重要的一点，Skrumble Network 将应用实际拜占庭容错机制（PBFT）算法，在实际表现和可拓展性中间找到平衡点。对于实时转账确认，Skrumble Network 的目标是达到10秒内完成通讯的建立，由受到激励的矿工算力来支持。

为了确保 Skrumble Network 有最优化的加载时间，这些协议将在分层技术的框架下开发。通过使用分层技术，Skrumble Network 能把很大的数据库分离成更小更快也更容易被管理的小块。每当需要数据的时候，不同于每次读取一个记录, Skrumble Network 将一次性从每个分层中抽取信息碎片，总合成数据库。

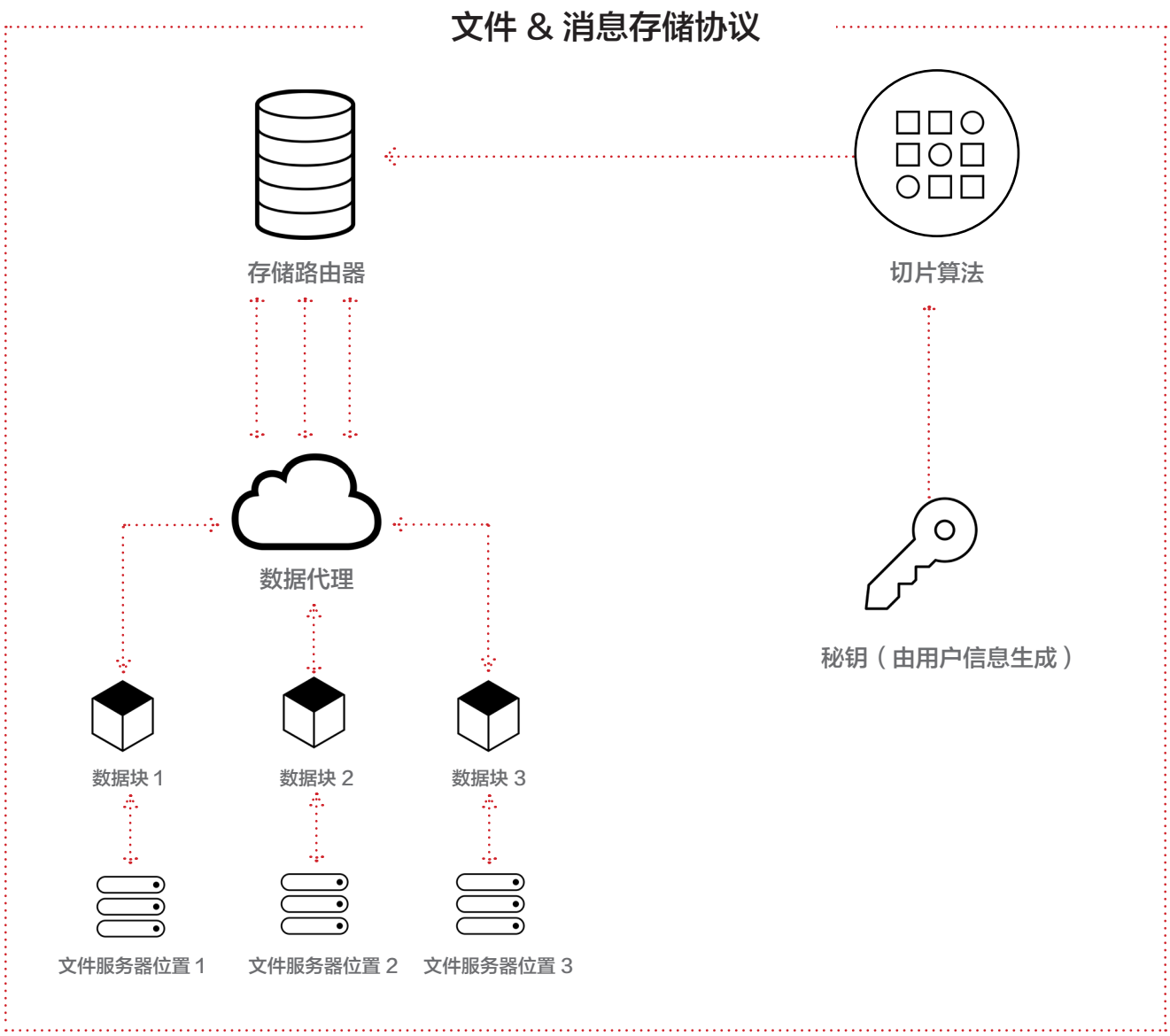
Skrumble 团队将持续地研究和评估新的更快速的确认方式，以及降低区块链数据读取时间。整个团队都致力于不间断的改进网络，确保用户在 Skrumble Network 上的体验始终如一。

在去中心化网络上的文件存储的独有加密钥匙

Skrumble Network 将通过运用算法，实现真正的去中心化文件存储。这种算法使用独一无二的会话ID和每位用户的随机秘钥数据来确保文件信息被加密。通过这一算法，Skrumble Network 可以确保用户间文件的直接传输，以及只有参与进这次对话的用户才拥有文件的接入权。

Skrumble Network 将引入一个全新的正在申请专利的名叫混合存储策略的技术，由 Skrumble 科技公司于2015年创造并开发。通过使用这种混合存储技术，文件将被算法加密，这种算法有独一无二的会话ID和子秘钥衍生而成。一旦完成加密，单个文件将被分成好几块，被分布和存储在不同的服务器里，并且只能通过特定的秘钥才能重新组合起来。因此，即使某一个文件服务器被盗取，其丢失的数据也是毫无意义的。

同时，更多的功能例如存储时间，和文件存储大小都将由用户的等级来决定，用户的等级可以通过在用户钱包内的 Skrumble Network 代币数量来解锁。



大容量通讯桥

对于超过6位参与者的语音和视频会议，匿名的专用会话将通过专用桥梁建立。专用通讯桥梁将覆盖于主要通信地区，并被独一无二的会话ID及衍生出的秘钥所验证。Skrumble Network 运用与一个地址相连的IP组合，它是在一个非常大的地址池中随机选择出来的，并且一旦用户间得到连通，它将只能在安全连接插座内得以显示。每当协议连接至通讯桥，用户可以验证其连通性。如果连通性没有达到要求，用户可以移到下一个被确认的地址上去。这些协议将允许大规模的语音和视频会议，信息，屏幕共享，文件传输和通知。

用户的等级可用于解锁更多功能诸如添加参与者数量或延长通话时间，用户可以通过在用户钱包内的 Skrumble Network 代币数量来升级。

业内领先的技术 & 用户所控制的数据存储

Skrumble Network 特点之一就是为群聊或者端对端信息是否保留和存储提供选项。对话记录将被存储在云空间上的文件服务器中，只有持有独一无二的会话秘钥的原会议参加者才能被许可接通保存的信息。

当一个群聊信息被创建的时候，这次会话的管理人将有权利选择是否要保存记录。该功能能否使用将基于该会话内的用户的所持有的代币数。当其他参与者尝试进入会话的时候，他们将首先被通知此次会话的管理人已经选择了保存这次会话记录，同时他们也可以选择是否要加入对话群。当加入两人会话的时候，这就需要双方的认可了，每个用户都必须同意保存会话记录，当前记录才会被保留和存储。

除此之外，Skrumble Network 还将引入其他独特的服务项目，例如基于讨论参与者和一些别的因素所使用一套独一无二的算法，为不同的会话创建的加密钥匙。根据将世界上任何地方的任何人联系在一起这一目标，用户可以很方便的创建大型的社区群组。根据 Skrumble Network 的匿名协议，用户将在操作中使用化名。用户会收到截屏通知，当别的用户在屏幕分享或者视频时候截取了屏幕截图。用户可以连通视频直播群，和加密的去中心化的文件和数据传输。

通过发布开源的软件程序工具包（SDKs），Skrumble Network 将鼓励和激励第三方开发人员在 Skrumble 区块链这个安全，隐私，匿名的通讯生态系统上开发新的区块链技术和应用。

SKRUMBLE NETWORK：不可阻挡的全球通讯

众多得益于 Skrumble Network 这个去中心化，安全和完全匿名的通讯网络的明显优势中，其中值得投入更多的关注也是最显著的三个如下：

1. Skrumble Network 不会被传统的防火墙阻挡。
2. Skrumble Network 拥有由用户控制的记录存储，一旦被删除，没有数据会被记录在任何服务器上。
3. 每次会话，信息和文件都被加密。

没有一个中心点可以被防火墙阻挡，因为每个用户和每次会话都是与众不同的。这确保了全面的匿名性，以及在世界上任何地方都能无限制连接 Skrumble Network 的特点。只有在网络连接被完全切断的某些行政区域，Skrumble Network 才会被限制住。

SKM 应用代币会员制:
SKRUMBLE NETWORK 源源不断的动力

SKM 是一种应用代币，基于用户持有代币的数量，它能提供一定等级的会员资格。这些会员特权可以允许人们接入在 Skrumble Network 生态系统中不同的功能和操作。用户会免费获得一些初始数量，代币将被用于解锁高级功能，会员等级或使用各种附加功能。

SKM 应用代币的应用场景实例：

在加拿大的用户A想要和在泰国的用户B进行视频聊天，这是一项高级功能，所以用户A和用户B需要持有一定数量的SKM应用型代币来完成想要的视频聊天。

在法国的用户A想要给在巴西的用户B传送一份文件，如果这个文件的大小超过了初始允许传输的文件大小限制，用户A就必须持有一定数量的代币来传输比原始许可更大尺寸的文件。

在哥伦比亚的用户A想要选择保存一段即将于在澳大利亚的用户B的对话，若用户B确认他将参与一个被保存记录的对话，双方都需要持有一定数量的代币，因为由用户控制的对话记录保存也是一种高级功能。

在德国的用户A想要给在美国的用户B传输一份文件，但是他不希望用户B将文件分享给其他人，那他可以使用一定量的代币使他能在文件被再次传输的同时获得通知。

在芬兰的用户A想要给在苏格兰的用户B传输一份带有访问秘钥的文件，只允许用户B访问。用户A可以使用部分代币，使得用户B受到碎片化的文件，只有通过从用户A那里得到的访问秘钥才能解锁这份文件。

用户奖励：惊喜 & 乐趣

- 基于具体标准，活跃的社区用户将惊喜地收到奖励代币。例如，最活跃的用户将收到代币奖励。
- 将有一定随机数量的代币奖励空投至活跃的聊天群里，以激励社区的贡献者们。
- 矿工、算力节点以及推广网络社区的人也有机会获得奖励代币。

一个自我可持续的生态系统

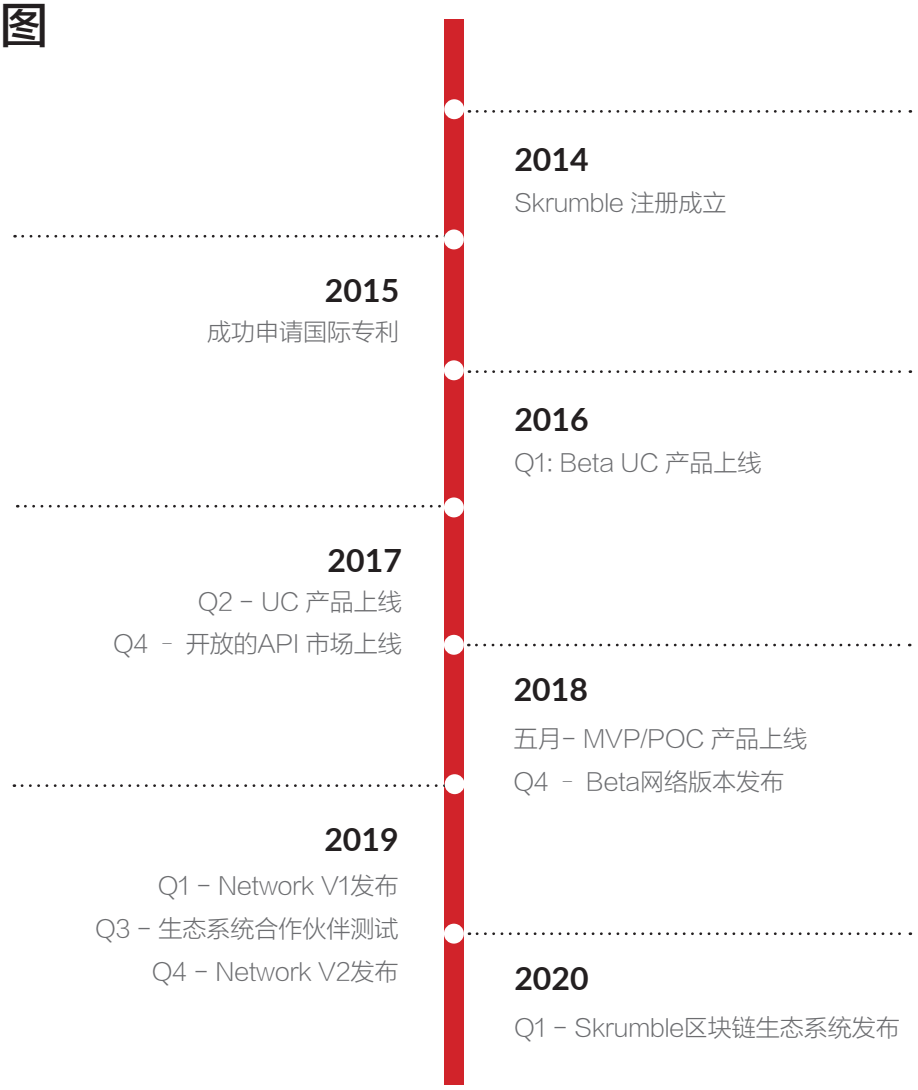
- 通过提供我们开放的 API / SDK，社区玩家/创业者可以利用 Skrumble Network 独特的去中心化通讯技术来为垂直
  领域。

- 此过程的第一阶段将通过 Skrumble Network 实验室计划孵化并引入 2-3 个初始战略合作伙伴，例如在 Skrumble Network 之上构建的 Vitual Show Room 和自由人力市场应用程序。

- 第二阶段将向任何人提供 API / SDK 以创建他们自己的产品或服务。

- SKM 代币将通过 Skrumble Network 由不同应用程序中的所有用户使用。通过 SKM 代币提供的各种应用也将被激励。因此，通过创新的平台开发，成本和奖励制度，自我可持续的通讯网络生态系统应运而生。

技术路线图



使用 SKRUMBLE NETWORK 的优势

私密　去中心化服务器　用户控制的存储　开放的API

安全　加密　安全的文件传输　无法被追踪

匿名　全球连通　截屏通知　无法被屏蔽

应用实例 & 生态系统

1. 信息记录 – 用户选择是否保存数据

若用户通过 Skrumble Network 进行私密、安全和匿名的对话，他们将可以选择是否保存聊天记录，这一点也是 Skrumble Network 重要的特性之一。这些记录包括信息、通话记录和文件储存。在P2P双人对话中，用户需要在对方同意后方能保存聊天记录。在小组对话中，小组管理员有权选择是否保存聊天记录，而小组其他成员也可以选择是否跟随管理员选择保存聊天记录。若用户选择不保存记录，在去中心化的网络上将不再出现任何该记录的任何信息。若选择保存记录，该记录将被储存在云端，且只有对话的参与者能够进入。

2. 加密文件的传输

Skrumble Network 旨在为用户提供一个能够分享自有数据，并传输加密和安全文件的网络空间。用户能够通过网关访问钥匙发送文件，也就意味着文件将以碎片化的形式在用户中传输。接收文件的用户将获得私密访问码来打开网关内容，并将文件的碎片重组称为单一文件。用户还能够在其传输的文件上安放通知功能，这样，即便不慎下载或传输了并非针对该对话的文件，相关一方也能够立即获得通知。

生态系统

所有 Skrumble Network 的用户可为不同应用程序使用 SKM 代币。根据 SKM 代币数量不同而各种不同的应用也将被激励。因此，通过创新的平台开发，成本和奖励制度，这个通讯网络生态系统将变得可持续。
Skrumble、Skrumble 实验室孵化计划或其他第三方团队推出以下初始应用程序：

1. 安全的在线支付和数字资产红包

大多支付网关都十分复杂，并对于建立者而言有着较高的技术能力要求，需要他们创立和管理一个独立且无关联的应用或模式。Skrumble Network 则包含着这样一个对话中的点对点的加密支付系统，能够轻松完成在对话框内的对等转账，实现在私人信息、电话和文件传输页面即可电子支付。 同时，Skrumble Network 的支付也将支持多种数字资产。

2. 自由职业者平台

近年来，一些列互联网信息平台兴起，纷纷瞄准自由职业者这一群体，希望在平台上吸引更多的自由职业者完成一定的工作并提供费用。基于 Skrumble Network 的通讯和交易属性，智能合约为基础的自由职业者雇佣平台。有意者可以轻松挑选一名自由工作者，告知他/她工作需求和参数，并根据合约完成情况相对应地付费。

3. 对话中的智能合约

智能合约是远程交易和商务的关键。Skrumble Network 中的智能合约模板，能够支持用户在对话和交流期间处理或签署通过智能条约。这项服务适用的场景包括同律师和客户签订服务合约，同远程工作的员工确定项目预期，雇佣从上文提到的自由职业者雇佣平台中招募自由职业（合同）员工，或任何一种需要相关利益方通过的交易协议等。一旦条款得到确定，对话中即能生成智能合约，并且将部署到区块中，在合作结束后，各方都可以得到合同所承诺的结果。

4. 直播平台

Skrumble Network 的视频、信息和展示功能，能够轻松地高效协助 P2P 或小组进行虚拟展示。这些网络上的连结点能够为用户提供一个平台，包含了在线视频和才能展示服务，并能够在对话中获取即时支付。

5. 技术合作伙伴

为进一步提升 Skrumble Network 的搭载能力和服务多样性，Skrumble 还将同区块链及加密货币的主要领军企业合作，其中包括 Aion 网络系统和支付处理系统。通过与行业合作伙伴并肩，Skrumble Network 的用户能够拥有获得更多服务的机会，还将进一步激活/鼓励 Skrumble 功能代币的持有者。

结论：打造未来通讯网络，用区块链连接你我

区块链技术能够解决一系列现有的严重问题。加密货币能够支持跨境金融机构间的发展并为其节约银行所收取的不必要费用；智能合约能够确保专业人士在服务结束后就收到报偿并通过实时信息来监控物品的传送和转移。由于去中心化的网络有着不容置疑的安全措施及数据处理和交流的机遇，更加安全的通讯渠道正因此应运而生。

区块链技术结合了密码学的保密性和特有的信息存储和传送方式，通过点对点的网络便建立起了一个去中心化、可信的数据库。网络安全、信息储存和用户信息安全等互联网基础上传统通讯系统的风险都可以通过分布式账本迎刃而解。除了解决这些问题，区块链技术还提供了无与伦比的创新机会。通过建立在线对话支付和其他新渠道，全世界的人们都能够有效地联系起来。

去中心化的网络还展现了无尽的创新可能。去中心化的网络为安全可靠的的点对点交流的同时保证安全可靠以及隐私保护提供了一个近乎完美的解决方案。它所创造的通讯机会能够让全世界联络、分享、展示。

Skrumble Network 能够将世界上任何地方的任何一人与另一人相连，这种连结是安全且简便的，并能从真正意义上实现全球交流自由化。结合区块链技术创造通讯网络这是前所未有的。Skrumble Network 将把用于金融交易的区块链技术，转而全力投入其他领域。通过易得、可靠并互联的交流，来自世界各地的人们能够参与到这个基于共识而达成的环境中，并且拥有自己的数据、不再担心个人信息安全并积极与不同的社区进行深入合作。

Skrumble 科技公司 – 介绍

Skrumble 科技公司（Skrumble Technologies Inc， 以下称“Skrumble公司”）于2014年成立于加拿大多伦多市，已在云端通讯行业拥有一席之地。Skrumble公司拥有超过30项全球专利，专注于提供多种商业通讯解决方案。公司致力于创建高效、安全和容易的通讯解决方案，为人们提供在最安全网络上的进行全球性通讯机会。公司服务于40万用户，包括《财富》杂志500强公司、IT咨询公司、呼叫中心、专业服务公司、警察机关、安全公司、政府、远程业务提供商、开发者等。2017年3月Skrumble公司发布的整合通讯平台获得了空前热烈的市场反应，并改变了企业用户的商业交流模式。基于云端平台的强劲技术支撑，Skrumble 公司书写并发布了丰富的产品信息记录，并公开发布API开发召集令，号召更多开发者集思广益将通讯的特性添加在其他应用之中。为了给全球企业提供更多福利，Skrumble 公司为医疗保险、法律、咨询等行业提供量身定制的白标签技术服务。近期，Skrumble 公司还发布了全新的插件产品，让开发者能够在任何网站或平台上嵌入对话、音频和视频通话等。更值得关注的是，Skrumble 公司已决定将公司目前的研发技能和技术专长转向市场需求呼声更高的区块链，为用户提供特有的区块链通讯体验。Skrumble 团队将继续打破通讯障碍，并通过提供创新解决方案让来自世界各地的企业彼此相连、共同成长。为了全球商业的团结和发展，Skrumble 团队继续在通讯领域内推动技术的发展，提供革命性解决方案。Skrumble 技术公司也将持续为 Skrumble Network 助力，为项目开发、区块链专门技术和技术许可等方面提供支持。Skrumble Network 将致力于发展去中心化技术并创建网络社区。在两者协力下，Skrumble 将共同打造下一代通讯系统。Skrumble 相信，随着用户捍卫自己的信息隐私权到来，我们将搭建信任的桥梁，继续开拓真正意义上全球网络的旷阔强劲。

我们的办公室

多伦多办公室–商业和运营团队

多伦多办公室 – 技术研发团队

丁美洲办公室

我们的团队

David Lifson
创始人 & CEO

Tamir Wolfson
执行副总裁

Vivi Herlick
运营副总裁

Eric Lifson
市场副总裁

Christine Guo
企划部副总裁

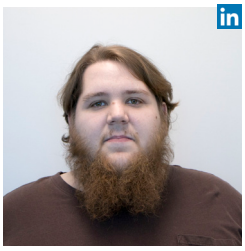
Johnathan Dwek
CFO - CFA

Aleksandra Mihajlovic
产品经理

Michael Dabydeen
工程师总管

Mikhail Khoroshun
前端工程师

Mikhail Berezovskiy
全栈工程师



Daniel Audino
全栈工程师

Danyi Lin
全栈工程师

Mauricio Bertanha
全栈工程师

Matt Mollon
全栈工程师

Leah Williams
全栈工程师

Chantale Barnard
全栈工程师

Eric Eddy
手机开发工程师

Akash Patel
手机开发工程师

Gabriel Hernandez
手机开发工程师

Arnaud Ladoucetter
手机开发工程师

Siv Sathiyaseelan
软件测试员

Avenson Navalta
UI/UX 设计师

Shelby Pearce
市场推广

Wendy Lu
数字市场推广

Wei Chen
商业拓展

免责声明

任何查阅本白皮书的人士（以下简称“您”）在继续阅读之前，请务必仔细阅读本条款并同意本声明。如果您有任何相关疑虑，请咨询您的法律、金融、税务或其他专业顾问。

本白皮书的内容被本公司视为真实、可靠，但 Skrumble Technology Inc. 及其子公司和关联公司对该等信息资料的真实性、准确性、完整性及其使用的适当性等不做任何担保。本白皮书所提供信息不应被视为提供专业意见，也不具有任何合同效应。

SKM 代币无意在任何司法管辖区内构成证券类投资，但依然可能被某些司法管辖区内的监管机构视为证券类投资。如果此类购买在其管辖范围内是违法的，本白皮书不构成在任何司法辖区内出售或者购买 SKM 代币的邀约。加拿大居民或美国绿卡持有者不得购买 SKM 代币，除非其为证券法允许的投资人类别。任何与 SKM 代币有关的购买都必须通过保密的购买协议及在适用的证券法和其他法律的条款下进行。

Skrumble Technologies Inc. 及其子公司和关联公司不会就任何购买 SKM 代币的方式提供任何意见。该白皮书的读者承诺，任何合约签署和投资决定都来自于您自己的独立判断。

参考文献

Cendrowski, Scott (April 14, 2017). Fortune Magazine. China's WeChat is a censorship juggernaut. Retrieved on January 26, 2018 from http://fortune.com/2017/04/14/china-wechat-tencent-censorship-709-crackdown/

Coin Market Cap (2018). Cryptocurrency Market Capitalizations. Retrieved on January 21, 2018 from https://coinmarketcap.com/all/views/all/

CyberScout (December 27, 2017). Identity Theft Resource Center. Data Breach Reports. Retrieved on January 24, 2017 from https://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

Facebook (2018). Making ads better and giving your more control. Retrieved on January 26, 2018 from https://www.facebook.com/help/585318558251813?ref=notif&notif_t=oba

Google (2018). How Ads Work. Retrieved on January 26, 2018 from https://privacy.google.com/how-ads-work.html

Greenberg, Andy (January 10, 2018). Wired. WhatsApp security flaws could allow snoops to slide into group chats. Retrieved on January 25, 2018 from https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/

Hollerith, David (November 6, 2017). Bitcoin Magazine. Survey polls American awareness of cryptocurrencies and ICOs. Retrieved on January 20, 2018 from https://bitcoinmagazine.com/articles/survey-polls-american-awareness-cryptocurrencies-and-icos/

Martin, Ellen (October 2017). The Next Web. Why more people will use blockchain-based payment platforms over banks in the future. Retrieved on January 18, 2018 from https://thenextweb.com/contributors/2017/09/07/blockchain-vs-banks/

Pascual, Al, Marchini, Kyle & Miller, Sarah (February 1, 2017). 2017 Identity Fraud: Securing the Connected Life. Retrieved on January 20, 2018 from https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

Perlroth, Nicole & Haag, Matthew (April 29, 2017). The New York Times. Hacker leaks episodes from Netflix show and threatens other networks. Retrieved on January 24, 2018 from https://www.nytimes.com/2017/04/29/business/media/netflix-hack-orange-is-the-new-black.html

Pullen, John Patrick (November 21, 2017). Fortune Magazine. Jennifer Lawrence reveals why she didn't sue Apple over her nude photo leak. Retrieved on January 24, 2017 from http://fortune.com/2017/11/21/jennifer-lawrence-apple-lawsuit-nude-photo-leak/

Sabin, Dyani (January 3, 2018). Futurism. Everything you need to know about cryptocurrency and why it's the future of money. Retrieved on January 17, 2018 from https://futurism.com/cryptocurrency-future-money-bitcoin/

Sethi, Rahul (September 26, 2017). After Google and Facebook, WhatsApp banned in China. Retrieved on January 26, 2018 from https://www.indiatoday.in/technology/news/story/after-google-and-facebook-whatsapp-banned-in-china-1052534-2017-09-26

Toronto Star (January 13, 2018). World News. As protests wane, Iran lifts ban on messaging app Telegram. Retrieved on January 24, 2018 from https://www.thestar.com/news/world/2018/01/13/as-protests-wane-iran-lifts-ban-on-messaging-app-telegram.html

WeChat (2018). WeChat Help Center. Why doesn't my prior chat log appear when I log in to WeChat from a new device? Retrieved on January 26, 2018 from https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?t=help_center/topic_detail&opcode=2&id=1208117b2mai1410242meeYj&lang=en&plat=android&Channel=helpcenter

Yannik (June 26, 2017). Updated January 9, 2018. How long do Ethereum transactions take? Retrieved on February 1, 2018 from https://support.metalpay.com/hc/en-us/articles/115000373814-How-long-do-Ethereum-transactions-take-