#liberateyourself

DECENT 白皮书

Matej Michalko m@decent.ch
Josef Sevcik josef@decent.ch

2015 年 9 月

目录

简介

世界少有创新，特别是在媒体行业。要确定媒体的哪个方面最具发展潜力，是非常困难的。大多数主流媒体都满足于其现有的商业模式，并未真正推陈出新。由于缺乏动力，媒体界现任从业者并未竭尽其所能，为消费者提供其赢得的效益。

而且，通过第三方媒介才可以访问数字内容的形式不是必须的。包括Medium、纽约时报和每日邮报在内的传统媒体，都通过高度受控的集权式利润趋向型平台进行信息发布。信息及其作者都由这些媒体自行选择。同样，有些国家和地区的人们没有言论自由；人们因发表自己的观点而受到处罚。

本白皮书主要关注数字媒体内容分享方式所面临的挑战及其新的定义，并探讨了因特网上的言论自由。我们向您推荐 DECENT：一个完全独立的 Web 3.0 发布平台，由数据区块链（Blockchain）和点对点技术驱动。

区块链（Blockchain）时代

Satoshi Nakamoto 于 2009 年创造了比特币[1] 这一概念。它的出现使人们对于财务的观点发生了翻天覆地的变化。与传统银行系统相比，比特币具有更高的效率（10 分钟内实现全球范围的清算）和成本效益（每笔交易仅需几美分的手续费），媒体对其进行了大篇幅的报道。但不幸的是，虽然比特币已面世 6 年，但由于其构架和设计方面的缺陷，它仍未被大幅推广。比特币的缺陷之一就是其 7 笔/秒 (tps) 的交易处理能力限制[2]。这使得比特币难以在现实生活中被应用起来，因为它无法满足现实需求。例如 VISA 卡的交易处理能力约为 2000 tps[3]，最高可达 56000 tps[4]。与之相似的缺陷是，比特币区块链的容量约为 40 GB （2015 年 8 月），且呈大斜率线性增长[5]，这种大容量将限制其在未来的推广。 对于大多数用户来说，即使交易额很小，也要等待大容量的数据区块链下载完后，才能进行比特币的交易。

因此，比特币可以被看成是区块链技术的一名先行者，同时也是一个具众多天生缺陷的案例。作为一个公开的记录网络交易的分布式总账，区块链有潜力成为继万维网之后另一伟大发明。多家金融机构都在探索这一领域，有的还成立

[1] https://bitcoin.org/bitcoin.pdf
[2] https://en.bitcoin.it/wiki/Scalability#Scalability_targets
[3] http://usa.visa.com/merchants/industry-solutions/retail-visa-acceptance.jsp
[4] http://usa.visa.com/about-visa/our-business/visa-transaction.jsp
[5] https://blockchain.info/charts/blocks-size?showDataPoints=false&show_header=true&daysAverageString=1&timespan=2year&scale=0&address=

了专门的数据区块链研究部门[6]。数据区块链技术可帮助银行降低多个领域的运营成本和基础设施成本。区块链通过无缝自动化，无需人员参与，就可进行清算，而且交易全过程都受到一套完整商业规则的控制。与之相似的是，利用区块链技术，无需第三方验证，就能进行银行资产的交易。

区块链使用案例：综合性分析&初创项目	
应用开发的所有权凭证 公司：Assembly	所有权凭证与数字资产买卖市场
数据存储和分发所有权凭证 公司：Blocktech （Alexandria）、Bisantyum、Blockparti, the Rundimetal、BlockCND	通过员工同行评审认可签注启用真实性认证
共乘计点积分价值传递 公司：Lazooz	股票市场、政界分散式预计平台
数字安全交易：所有权与转移	分散式患者病历管理
文档/合同和价值转移所有权凭证的数字化	数字内容所有权凭证
利用区块链网络内电脑实现分散式存储	使资产数字化：改善防伪措施
将家庭网络连至云端和附近电气设备的平台（居家自动化）	提供保护消费者隐私权的数字 ID
保护消费者隐私权的个人数字 ID	启用评审真实性验证
Escrow/Custodian 支付服务 博彩业 博彩业和借贷 商业/制造中完整订单的智能合同 IT 客户端	每个家庭和公司的分散式因特网和计算机资源
	使公司数据化、资产/所有权和管理权的转移

图 1：数据区块链的使用案例[7]

[6] http://cointelegraph.com/news/114889/10-big-banks-that-are-seriously-looking-into-blockchain-technology
[7] http://n6zgo3se7pe2sazc62u1v9qe.wpengine.netdna-cdn.com/wp-content/uploads/2015/07/1231-1024x699.png

除了金融业，区块链技术还应用到了多个行业，如图 1 所示，包括：所有权证明、分散式存储和分散式同行评审。分散式应用所带来的巨大效益正被持续的挖掘。

言论操控和言论自由

当今大多数媒体和内容分享平台都是私有实体。它们自己决定其媒体平台由谁使用以及如何使用。如想要在这些平台上发布消息，用户必须首先同意其条款声明，通常也会失去对所发表内容的所有权。第三方有权对创意艺术家所发表的数字内容进行修改、编辑或者甚至将其完全删除。Reddit[8]、Twitter[9]、Facebook[10] 和 Medium[11] 是这类平台的典型代表。

有些国家言论不自由，对外网进出访问都作了限制。这些国家的在线媒体必须取得许可证，并接受国家监管机构的监督，以防止民众发表不当言论，或屏蔽持不同政见国家的服务器或民众。

虽然西方民主国家的民众普遍享有言论自由权，但媒体还是受到了一定程度的操控，因为还是有中间人的存在。作者与内容消费方（读者）之间还是缺乏直接的交流关系。

而且这些充满创意的作者没有机会将他们的作品货币化。他们也无法评估已发布作品的价值，因为过程太复杂。例如，博主既可以选择将其作品发表在第三方媒体上，例如 Medium 上，也可以创建个人网站。当他们选择在第三方媒体上发布信息时，除非他们的作品是这个媒体的热帖，否则他们不会因为作品而收到经济补偿。如果他们自己创建了个人网站，他们必须想办法吸引读者访问网站。这通常是非常困难的，因为网站推广需要结合搜索引擎优化 (SEO)和集客营销。之后，他们必须对网站的商业模式进行定位，例如是否同意 Google Ad Sense [12]条款并选择加入。这些事情一般是博主们不愿意涉及的。因为他们的主要工作是写作（编写音乐、视频和软件），一般不愿意涉及广告推销。

包括亚马逊在内的在线电子书商城对电子书的出版和营销都抽取高额提成。亚马逊的版税率[13]为 35% 或 70%。这使得本不富裕的作者只能收到读者所付金额的 65% 或 35%。
由此可见，言论不自由和媒体被操控的现象是存在的。中间人利用作者-读者关系从中获利，但其存在不具有必要性。

[8] https://www.reddit.com/
[9] https://twitter.com/
[10] https://www.facebook.com
[11] https://medium.com/
[12] https://www.google.com/adsense/start/
[13] https://kdp.amazon.com/help?topicId=A29FL26OKE7R7B

历史研究

媒体操纵和审查制度源自历史原因。在印刷媒体为主的年代，只有少数人和少数公司能够接触到作品并进行作品推广。这促生了观点的不一致性、对媒体的深度操纵性以及信息发布垄断的误用。

教皇利奥十世于 1517 年开始贩卖赎罪券，在当时风靡一时。马丁·路德为了反对这一行为，写下了《九十五条论纲》，并将其张贴在维滕贝格教堂的门上。正是由于 马丁·路德 的正义之言以及印刷媒体的存在，该文档在几周内就传遍了全欧洲[14]。马丁·路德 抗议赎罪券的行为在全欧洲得到了积极的响应。而如果这个事情放在几十年前，由于那时还没有古滕贝格在 15 世纪发明的活字印刷术，以上将不可能发生。这是言论自由范畴下，消息快速传播的第一个具有重大影响的事件。与该事件相似的是，300 年后 Ronalds、Cooke & Wheatstone 以及 Morse 发明了电报[15] 。电报使人们进入大容量个人沟通的新纪元。电报采用了特殊的编码体系，可以对任何种类的文本信息进行传输。在 19 世界末，全球居民大陆[16]都铺设了电报传输线缆。另一个巨大变革是贝尔发明的电话 [17]。电话在电报的基础上新增了语音通话功能。

同时马可尼和其他研究人员研究发布了无线电报系统[18] 。这使得有线电缆不再是唯一的传输媒介。点与点之间不再需要硬连接。正是由于以上发明，人们才能够收到国家或商业电台。

虽然印刷媒体、电报、电话和无线电都是促进人们沟通交流的主要进步，但无法保证它们的安全性，无法像几百年前用到的蜡封信或者多字母表密码加密那样安全。除军事行业外，其他行业还未对加密信息沟通进行大幅推广。大多数人还未意识到未加密在线沟通的后果。政府机构从软件平台处购买信息，以实现它们的政治目的。2011 年[19] 爱德华·斯诺登就曝光了泄密事件。PGP 加密邮件也只能解决部分问题 [20]，因为其缺乏可拓展性和用户便捷性。综上所述，现在全球需要一种分散式的、非可操纵的、安全、可靠、高效和经济的内容分享整体解决方案

分散式 Web 3.0 发布平台

[14] http://www.bbc.co.uk/history/historic_figures/luther_martin.shtml
[15] https://en.wikipedia.org/wiki/Electrical_telegraph
[16] https://en.wikipedia.org/wiki/Electrical_telegraph#/media/File:1891_Telegraph_Lines.jpg
[17] https://en.wikipedia.org/wiki/Telephone
[18] https://en.wikipedia.org/wiki/Wireless_telegraphy
[19] https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html
[20] https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html

由于以上提到的问题没有一种综合性的解决方法，我们提出了一种能解决所有问题的开放平台构想。DECENT 是一种基于区块链技术的分散式自动运行组织，不受任何第三方干预。它是针对创意个人、作者、博主和出版商及其粉丝的独立 Web 3.0 发布平台。该平台可突破国界，对任何文本、图片、视频或音乐内容进行分享。DECENT 是一个资源丰富且独立的平台。其信息分享不受任何界限和限制的影响。该平台的宗旨就是捍卫言论自由。它由 P2P 网络驱动，采用了密码和区块链技术进行加密，使信息分享更便捷、更安全。第三方无法对发布内容进行控制或影响。DECENT 的主要典型特性包括：

独立

不受任何第三方控制，甚至包括平台设计者在内。该平台完全由其用户所有，并不附属于任何经济机构、媒体或政治团体。

无国界

我们的目标是消除媒体行业所有政治性和地理性的障碍，给人们带来表达自我的平等机会。

稳定

DECENT 并不依赖于任何单个服务器。由于不存在单点失效，信息访问是无限制的。

公平

每名作者在 DECENT 平台都处于同一起跑线。他们必须通过发布内容的质量以及精心维护还赢取读者芳心。读者可以依据作者的受欢迎程度决定其发布内容是否值得购买。总体原则是，作品内容越优，作品曝光率越大，作者收到的收益也越高。.

可盈利

读者可以从喜欢的作者处直接购买发布内容。App 开发人可以自由开发，然后按照自我意图将其货币化。这些过程中不存在从中收取中间费的隐形第三方，比如出版社。

无广告

平台采取了无广告机制。这使得广告投放费用较高。同时也保证了合法作者的资源充足性。

安全

作者可选择在平台上匿名发表作品。除非本人同意，没有人能够披露作者身份。与之相似的，DECENT 发布内容经过了完全加密，读者范围由作者选择：付费读者或未付费读者。

启用加精功能

DECENT 具备了作者及其作品的推荐加精功能，依据为读者的反馈意见。由于区块链内置了这一功能，作者可以随时间累积读者口碑。

DECENT：技术详情

DECENT 是针对数字内容发布的自主 I 类分散式应用 (Dapp)[21]。它拥有独立的区块链[22],是继创世块 (genesis block)[23]（DECENT 协议使用初期）出现后所有交易的公开总账。

DECENT 的 3 个功能性角色包括：

- *作者*：内容创作者、作者、音乐制作人…
- *消费者*： 读者、听众等 …（发布内容的消费者）
- *发行人*：挖矿者

*作者*制作发布内容并将其上传至网络。*发行人*是维系和运行 DECENT 网络的关键一方。针对*发行人*所花时间和精力的奖励是 DCT 数字币，与奖励给挖矿者的比特币相似。

DECENT 采用了改进后的权益证明 (POS)[24] 体系，以保持网络各节点的统一性。该体系是基于*发行人*（“挖矿者”）所提供的硬盘空间/时间比率权益，以及分发秘钥所花费的 CPU 时间。

使用案例

让我们回顾下现今媒体的运行方式。作者必须通过出版社、录音室或政府才能发布他们的作品。而出版社、录音室或政府掌握着待发表内容的生杀大权。应用开发者也面临着诸多限制。

[21] https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md#classification-of-dapps
[22] https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md#classification-of-dapps
[23] https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md#classification-of-dapps
[24] https://en.bitcoin.it/wiki/Proof_of_Stake

DECENT 为应用开发者提供了一个安全的免费发布平台。通过区块链和数据分发体系，应用不仅能被直接提供给读者，还能依据其本身的质量和受欢迎程度而得到推荐。

DECENT 的典型使用案例包括文章和小说的发表，与 Medium [25] 类似。*作者*通过平台进行写作，对作品进行编辑或添加媒体文件。当*作者*完成写作后，按下“发布”按钮即可进行发布。*作者*可对作品内容进行定价、定义免费阅读部分，并添加元数据。平台将对内容进行加密，查找*发行人*（与 DECENT 网络相连的独立计算机，运行发布软件，以维持平台网络运行，并因此受益）并计算发布费用。当发布费用得到确认后，DECENT 将发命令给发行人电脑，使其下载内容，并将相关元数据在区块链上进行传播。

当*消费者*找到他们感兴趣的内容后，他们将收到平台发布的通知，提醒他们，他们关注的作者发布了新文章。读者将接收到基于他们偏好的文章推送，也可浏览最新发布的内容。读者可选择下载和阅读文章的免费部分。之后读者可能将决定支付小额费用（由作者定价），购买余下全文。DECENT 协议对此次交易进行处理，*作者*将收到费用，而*消费者*的应用上出现余下全文的解码秘钥。

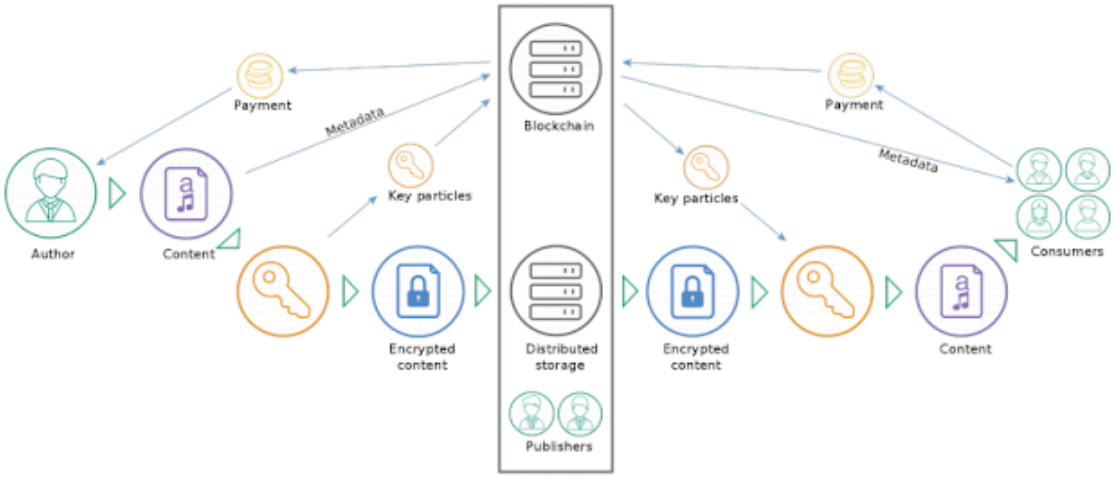
随着时间的推移，*发行人*将因为存储发布内容而获得奖励，应收到*作者*支付的一定比例的发布费用。

DECENT 欢迎每个人在其协议的基础上，利用独特的商业模型创建应用或客户端。这有助于作者分享他们发表的内容。发表的信息可包含各种形式的数字内容：视频或音频文件、文本（书籍、文章和新闻）或图片。平台实际提供了各种可能性和机遇，例如：

- 类似 Medium[26] 的博客和出版物
- 类似 Soundcloud[27] l 的音乐发布
- 类似 Amazon[28] 的电子书发布
- 软件发布
- 类似 Shutterstock[29] 的图片分享
- 电子报纸发布
- 免费学术论文发布

[25] https://medium.com/
[26] https://medium.com/
[27] https://soundcloud.com/
[28] http://www.amazon.com/
[29] http://www.shutterstock.com

详细流程



Payment	支付
Author	作者
Content	发布内容
Metadata	元数据
Key particles	关键元素
Encrypted content	加密内容
Distributed storage	分发后存储
Consumers	消费者
Publishers	发行人

图 2：DECENT 流程图

DECENT 平台大部分操作都是在区块链中创建一条新交易。随着事件逻辑链不断变长，每个网络节点都对其进行验证，并投入到整个平台的投票机制中。

发表

发表是指新内容存储于网络，且有关该新内容的信息在社区内进行传播的过程。详细流程如下：

1. *作者*以电脑文件的形式创建内容，并选择两个整数 *n* 和 *m*，*并且* *n*>*m*>2。
2. 平台根据*作者*的发布申请，生成了一个独特的 AES[30] 秘钥，并对非免费阅读部分的文本进行加密。
3. 平台根据*作者*的发布申请，选择分发协议 – 现为比特流[31]，并分配一个追踪器[32]。该协议是平台现今唯一支持的协议，但是平台的发展规划中包含更多协议。之后平台将创建分发包，里面含有免费阅读文本和加密文本。
4. 平台根据*作者*的发布申请，将密码分为 n 份，且需要 m 份才能索回秘钥[33]。
5. 平台根据*作者*的发布申请，找到 *n* 个合适的*发行人*。其中一种方法是利用 DHT Kademlia[34] 网络，并在网络上爬行寻找已预备好存储既定大小新内容的节点，同时也尽量减小种子特征码[35] (torrent info hash) 与节点 ID 之间的距离。
6. 平台根据*作者*的发布申请，将步骤 4 中的 n 份秘钥通过 *n* 个*发行人*的公钥进行加密。每个*发行人*获取一份秘钥。
7. 同时平台根据作者的发布申请，发命令至*发行人*节点，进行发布内容的下载。
8. 平台根据*作者*的发布申请，生成内容提交交易。该交易将包括所有内容元数据，例如标题、概要或标签，以及网络相关数据，例如有效期、价格、发行人清单和每名发行人的加密秘钥份额。
9. 发行费将从*作者*账户中自动扣除。该费用用于奖励*发行人*对于发布内容的存储行为。同样发行费也用于反广告。如*发行人*发布大量信息（即发布广告），费用将较高。
10. *发行人*下载发布内容，并发起一个可恢复性凭证[36]交易，以确认内容已成功发布。

购买

购买是指消费者决定购买某些已发布内容的过程。购买采取合同形式，以*消费者*的支付承诺开始，以确认*发行人*已分发内容且*消费者*向*作者*完成支付为止。具体流程如下：

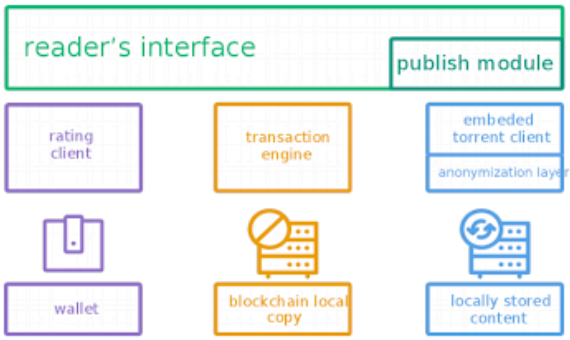
[30] FIPS Publication 197: "Announcing the Advanced Encryption Standard". Retrieved from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[31] http://www.bittorrent.org/
[32] http://www.bittorrent.org/beps/bep_0005.html
[33] Shamir, A.: "How to share a secret". Communications of the ACM, November 1979, Volume 22, Number 11
[34] Maymounkov, P. and Mazières, D.: "Kademlia: A Peer-to-peer information system based on the XOR Metric"
[35] http://www.bittorrent.org/beps/bep_0003.html
[36] Shacham, H. and Waters, B.: "Compact Proofs of Retrievability". Retrieved from https://cseweb.ucsd.edu/~hovav/dist/verstore.pdf

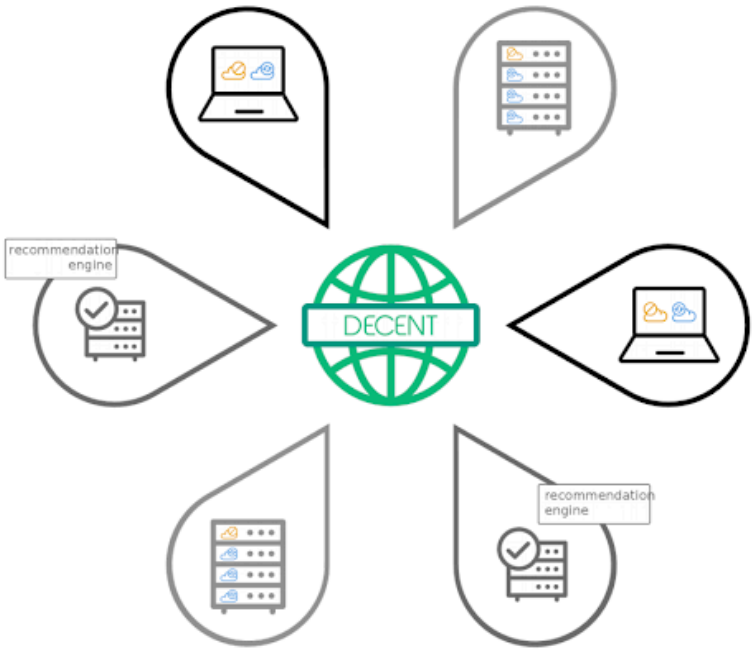
1. *消费者*选择想要购买的内容。提出购买申请后，平台将通过指定协议下载分发包，即通过特征码生成磁力链接 (magnet link)，并通过带有已分配追踪器的比特流进行下载。
2. *消费者*的购买申请在平台上生成一个购买请求交易。该交易将有效冻结*消费者*账户指定数量的数字币。
3. *发行人*节点在区块链中发现购买申请后，将使用私钥对各个解密秘钥（来自 content_submit 交易）进行解密，并通过*消费者*公钥进行重新加密。
4. *发行人*节点将生成分发秘钥交易，包含*消费者*秘钥加密的份额和交货凭证。
5. 当区块链中已达到指定的分发份额：
    a. 发行人以*消费者*账户冻结的金额向作者付款，并将新生成的数字币的一部分付给*发行人*，作为提供秘钥的奖励；
    b. *消费者*将会使用其私钥对秘钥份额进行解密，并重建解密秘钥，解密内容。
6. 最后消费者可在区块链中提交一次评级交易，对发布内容进行评论和打分。不同的评级和分类引擎收集这些评级交易，用其生成对于*消费者*的各种推荐内容。

挖矿

当*发行人*利用 PoS 生成一个区块时，他/她将会：

1. 对所有交易进行验证，包括可恢复性凭证和交货凭证。
2. 向作者付款（参见购买流程）。
3. 基于当前存储内容（可恢复性凭证）向发行人支付分发费。
4. 基于已分配秘钥（见购买流程），向发行人支付新生成的令牌。
5. 扣留自己应得的部分。





Reader's interface	读者界面
Publish module	发布模块
Rating client	评级客户端
Transaction engine	交易引擎
Embedded torrent client	内置
Anonymization layer	匿名层
Wallet	钱包
Blockchain local copy	区块链本地副本
Locally stored content	本地存储内容
Recommendation engine	推荐引擎

图 3：DECENT App 图

图 3 为 DECENT 网络的总示意图。*消费者*可访问评级客户端、交易引擎、经过匿名处理的内置 torrent 客户端，支付钱包、本地区块链副本和本地存储内容。

.

下一步发展规划

DECENT 平台是由 DECENT 基金会创立的非营利性项目。该基金会不从该项目收取任何经济利益。该基金会所扮演的主要角色是数字币的发行，开发者数字币的持有、赏金支付管理和 DECENT 发展方向的确定。DECENT Protocol 的未来开发内容将在 2015 年第 4 季度预售活动中进行介绍。届时将发布更多预售详情和本白皮书内容更新。

如需获取更多信息，请访问官网 http://decent.ch 或通过 DECENT 基金会邮箱：info@decent.ch 进行联系。