Wanchain- 风险等级「C+」 - 标准共识投资风险评级

微信标题：

北京时间 2018 年 8 月 20 日，标准共识发布针对区块链项目「Wanchain」（代币符号：WAN）的一般投资风险评级报告。以下为报告的主要内容。

## Overview 概述

报告将 Wanchain 风险等级定义为「C+」，该项目属于「一般风险」水平，需要投资者注意。

依据「标准共识一般项目投资风险评级标准（初创期）」 获得「C+」评级的主要原因是：万维链跨链涉及的三类节点选拔机制不明确；项目落地情况对比线路图有小幅延期；WAN 二级市场存在被操纵风险；万维链与以太坊跨链已实现；交易隐私保护功能已实现。

基于标准共识分析师团队调查和研究，项目主要风险及优势在于：

**项目主要风险**

风险点一：万维链跨链交易依赖三类节点，但目前尚未公布节点选拔机制。

万维链的跨链交易主要依赖于三类节点：普通验证节点(Validator)、跨链交易证明节点( Voucher)和锁定账户管理节点(Storeman)。但是万维链目前尚未公布关于成为节点的相关选拔机制。

风险点二：项目路线图落地两度小幅延期，后续开发计划落地时间存疑。

万维链 1.0 发布时间原定于 2017 年，推迟到 2018 年 1 月才正式发布，万维链 2.0 上线原定时间是 2018 年 6 月，延期到 7 月发布。虽然两次延期时间跨度不大，但接连两次路线图规划延期，也一定程度上反映了项目开发进度存在的问题。

此外，项目规划正式版主网（4.0 版）在 2019 年 12 月发布，时间跨度较大，能否按时落地存疑。

风险点三：WAN 二级市场存在异常交易，有被操纵的风险。

市场表现方面，WAN 热门货币对上市当天均出现巨幅震荡和天量成交，投机性强。且在其他交易日也出现过不同程度的异常交易，比如 Binance 交易所的 WAN/BTC 货币对存在砸单和拉抬， Kucoin 交易所的 WAN/BTC 货币对存在对倒。

**项目主要优势**

优势一：万维链与以太坊跨链交易已经实现。

万维链利用节点分工机制，将普通验证节点、跨链交易证明节点和锁定账户管理节点分离，跨链交易证明节点负责发出、返回交易请求结果给锁定节点、普通验证节点，锁定账户管理节点负责锁定相应资产，普通验证节点打包万维链交易。

优势二：万维链为其链上数字资产提供交易隐私保护。

Wanchain 采用了一些创新的算法和理论，来解决区块链行业长期存在的几个难题，包括用邮票方法解决保密交易问题和用 Storeman 这种中间机制解决跨链交易问题，而且代码相当规范，注释详细，提交频繁，架构清晰。

以上为项目主要风险点和优势，以下为完整报告。

如果任何项目方对标准共识的评级结果有疑问，或对相关数据提出申诉（包括但不限于项目运营数字、重要团队成员变更原因、代码更新和最新交易表现等），标准共识分析师团队会根据材料的真实性重新评估。

如果标准共识分析师团队在调查过程中使用了错误材料而影响评级结果，或任何项目变动可能导致评级等级变动时，标准共识也会重新调查和评估风险等级。

任何项目方、利益相关方和投资者可直接通过微信公众号（「标准共识」ID：SNCrating）后台与我们联系，也可以发送邮件至：contact@sncrating.com。

## Rationale 依据

### **产品和技术模块**

#### 

#### 市场及产品分析

#### 

万维链（Wanchain）旨在建立数字资产的金融市场，是一条基于以太坊底层协议开发、实现跨链交易的公有链，进而提供各种数字资产流通交易的平台。万维链计划将支持主流公有链间的跨链交易、联盟链间的跨链交易以及公有链和联盟链间的跨链交易。基于万维链不同的数字资产金融业务可以以分布式的方式开展，最终形成不同业务提供商、不同应用开发者、不同需求客户共同构成的金融市场。

万维链的应用场景包括：数字货币借贷、数字货币支付结算、数字货币交易兑换、数字资产投融资、其他应用场景（多数字货币币种信用卡、资产证券化、数字货币 P2P 业务）。

万维链的设计目标：

1. 跨链资产转移：

1）能够连接现存的主要数字货币网络(如比特币、以太坊等)，完成资产兑换的同时不改变原有链机制。新产生的数字货币网络也能够以极低的成本接入到万维链中。

2）联盟链性质的区块链网络能够接入万维链， 实现资产由原有链转入万维链、由万维链转回原有链、多种资产在万维链上进行交易等功能。

3）保证跨链交易资产的安全性以及跨链交易服务的稳定性。

1. 提供交易隐私保护：

1）交易双方可以选择带隐私保护的交易。

2）能够为数字资产转移、交易提供隐私性保护。

3）能够为数字资产持有者提供匿名性保护。

1. 具有场景的延展性：

1）能够成为多种数字货币兑换的分布式平台。

2）能够开展不同数字货币的存贷业务。

3）能够以数字货币为媒介完成数字资产的交易。

4）能够发行和交易全新的数字金融资产。

万维链在完整实现以太坊原有的各项功能之上加入了跨链及智能合约代币交易的隐私保护。万维链总体架构包括：分布式账本及智能合约的虚拟机、原生币、共识机制、链内交易、跨链链接、跨链交易。

1. 链内交易：万维链的链内交易增加了智能合约代币交易的隐私保护机制，该机制通过环签名和一次性账户实现。
2. 跨链链接：

1）其他链接入万维链，首先需要完成万维链上的注册，确保万维链能够对该链进行唯一识别；

2）不同资产转入万维链，首先也需要完成在万维链上的注册，确保万维链可以对该资产进行唯一识别。

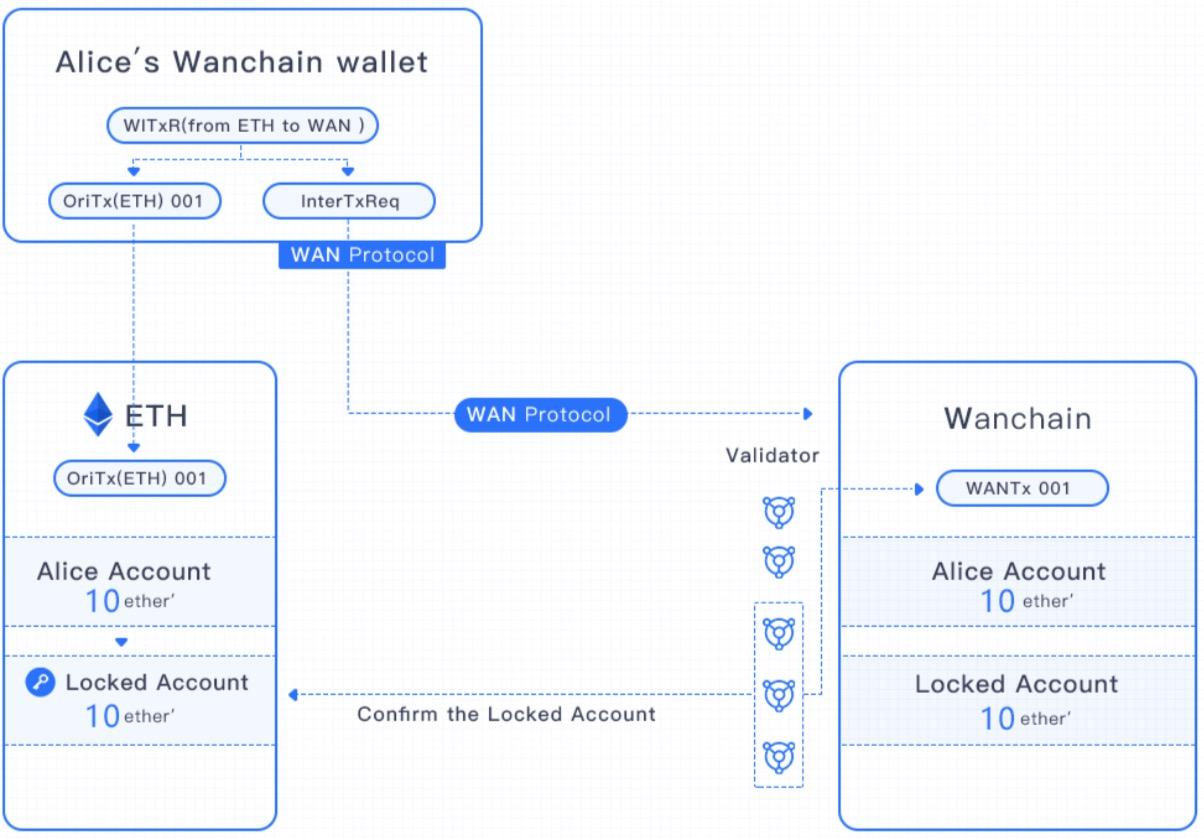
3）这两部分功能分别通过链注册和资产注册协议完成。

1. 跨链交易：当一种未注册资产由原有链转移到万维链上时，万维链节点会使用一个基于协议的内置资产模版，根据跨链交易信息部署新的智能合约创建新的资产。当一种已注册资产由原有链转移到万维链上时，万维链节点会为用户在已有合约中发放相应等值代币，确保了原有链资产在万维链上仍然可以相互交易流通。

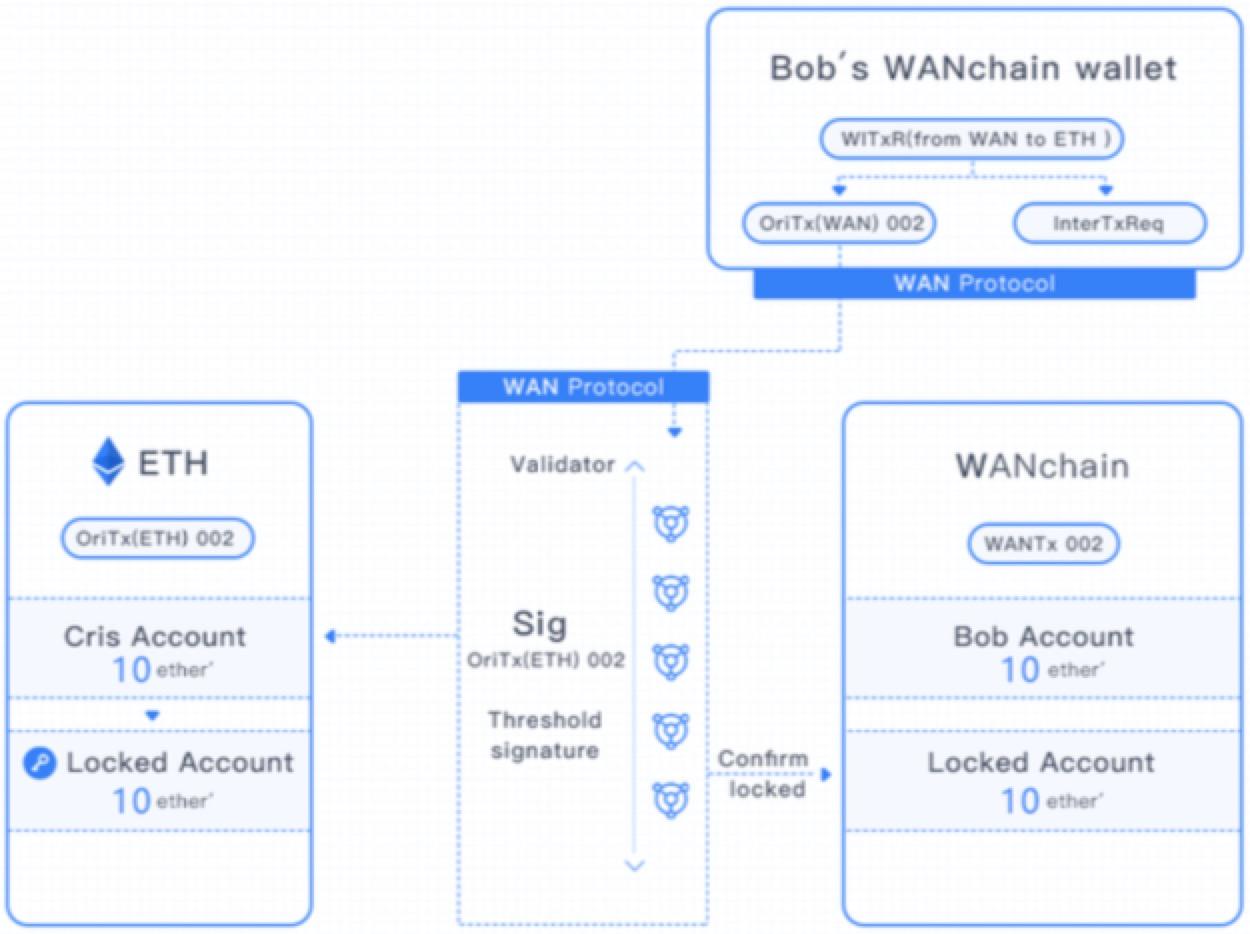
1）万维链在白皮中关于跨链的原理举例如下：

* 转入过程：Alice 和 Bob 分别在以太坊和万维链上拥有账户，当 Alice 需要向 Bob 转移10 ether。 Alice 使用万维链钱包发出跨链交易请求，并在以太坊中发起一笔转账交易，接收方为万维链在以太坊上的跨链锁定账户(Locked Account);
* 万维链验证节点收到跨链交易请求并验证以太坊上该交易已完成记账，然后在万维链上创建一个新的智能合约代币资产 ether’， ether’ 是 Alice 需要跨链转移的 ether在万维链上的代表，并将该资产链内转移到 Bob 在万维链的账户中。

跨链交易转入过程如下图所示：



* 转回过程：Bob 将从 Alice 处收到的 10 ether 转给 Cris。Bob 使用万维链钱包向 ether’ 资产合约发起一笔跨链交易，验证节点收到交易后将 Bob 的该笔资产对应的价值 10 ether’ 转为锁定状态，锁定完成后，验证节点利用门限密钥共享机制构造出一笔以太坊交易，交易的转出方是之前锁定 Alice 资产的跨链锁定账户(Locked Account)，转入方是 Cris 在以太坊上的账户；验证节点验证以太坊上的交易确认后，将 Bob 账号下锁定的 10 ether 清空，意味着等值的资产已经回到原有链。



标准共识分析：

1. 万维链是提供数字资产流转交易的公有链，支持数字资产跨链交易。作为金融领域的垂直应用公链，目前已经支持基于其发行数字资产（例如：WAN）与 ETH 的跨链转账。

1）根据万维链白皮书介绍，跨链流程涉及到的验证节点有三类，分别为：普通验证节点(Validator)、跨链交易证明节点(Voucher)和锁定账户管理节点(Storeman)。

2）Voucher 负责在跨链交易过程中提供原有链账户与锁定账户之间交易的证明，同时它也需要缴纳一定的保证金，保证金越多，它所提供的证明被采纳的概率也越高，如果提供虚假证明，它的保证金将会被扣除并剥夺跨链交易证明节点的身份。

3）Validator 负责在收到达成共识的交易证明后，通知 Storeman 对锁定账户进行相关操作并完成万维链账本的记账操作。Storeman 负责在接到通知后，通过自己所持的密钥份额计算出签名份额并最终合并为锁定账户完整签名，以便进行锁定账户的相关操作。

4）万维链将验证节点分为三类，将跨链交易的验证权限进行了一个分离。一方面，每一类节点内部需要达成共识；另一方面，单独一类验证节点即使合谋也无法完成跨链交易的伪造。这种分离机制能够最大限度的降低验证节点合谋的可能性。

1. 但是关于加入万维链成为三类节点的方式白皮书中暂无介绍，标准共识就此向项目方询问获悉，万维链将会在后续公布节点细则。
2. 万维链的将跨链交易流程分配给三个节点验证，但是当合谋收益大于验证节点收益时，仍然存在三类节点合谋的风险。
3. 万维链的应用场景广泛，主要集中在基于数字货币的借贷、支付结算、兑换、投融资，涵盖了数字货币金融领域的主要需求，万维链存在较大的应用场景。

#### 技术分析

##### 技术介绍

##### 

万维链遵循区块链分布式、无可信任第三方参与的原则，利用了密码学理论和技术进行方案设计和技术实现。在跨链交易中，万维链的锁定账户机制采用多方计算和门限密钥共享技术，完全去中心化，实现了无需可信第三方参与的资产账户管理功能。

在万维链内交易中，万维链实现了基于环签名和一次性账户的智能合约代币交易隐私保护机制。

1. ECDSA 签名算法，椭圆曲线数字签名算法（ECDSA）是使用椭圆曲线密码（ECC）对数字签名算法（DSA）的模拟。
2. 安全多方计算：安全多方计算是指在一个互不相信的多用户网络中，两个或多个用户能够不泄漏各自私有输入信息，协同合作执行某项计算任务。
3. 门限密钥共享技术：门限密钥共享技术(threshold key sharing scheme)解决的是密钥安全管理问题。
4. 环签名：环签名可分为四个部分：GEN，SIG，VER，LNK。

1）GEN：采集公共参数，随机选取 𝑛 − 1 个公钥，合同用户公钥 𝑃 构成公钥集合 𝑆 = {𝑃 |𝑖 = b 1,2 ... , 𝑛}; 对用户公私钥对 (𝑃, 𝑥)，𝑥 ∈ [1, 𝑙 − 1]，𝑙 为点 𝑃 的阶，生成公钥镜像 𝐼。

2）SIG：针对所需签名消息 𝑚，利用公钥集合 𝑆 = {𝑃 |𝑖 = 1,2 ... , 𝑛}，其中 𝑃 为用户真实公钥， bå 计算输出签名 𝑟𝑖𝑛𝑔𝑠𝑖𝑔。

3）VER：基于消息 𝑚，公钥集合 𝑆 和签名 𝑟𝑖𝑛𝑔𝑠𝑖𝑔，验证签名合法性，输出「True」或「False」。

4） LNK：利用集合 I = {𝐼b}，判断 𝑟𝑖𝑛𝑔𝑠𝑖𝑔 签名是否已使用。

1. 一次性账户及邮票系统：

1）一次性账户系统是整个隐私交易的基础，系统中每个用户拥有唯一主账户和多个子账户， 子账户也可以看作智能合约中的账户，而子账户通常不是用户自己产生，而是由交易对方为用户生成。

2）一次性账户的邮票系统：当使用环签名进行隐私保护时，交易的发起方不可追溯，那么将导致交易费不知从哪个账户收取的问题，为解决这个问题， Wanchain 设计并实现邮票系统。 邮票系统基于一次性账户体系，在邮票系统中，每张邮票就是一个一次性账户，邮票系统中使用 𝑂𝑛𝑒𝑡𝑖𝑚𝑒 − 𝑠𝑡𝑎𝑚𝑝 表示，实际上 𝑂𝑛𝑒𝑡𝑖𝑚𝑒 − 𝑠𝑡𝑎𝑚𝑝 与 𝑂𝑛𝑒𝑡𝑖𝑚𝑒 − 𝑎𝑐𝑐𝑜𝑢𝑛𝑡 相同。 用户需要使用代币隐私交易的时候就需要预先购买邮票，将邮票「贴」在交易上才可以 完成隐私交易，每张邮票只可使用一次。

（注：Wanchain 的技术白皮书关于算法有详细的介绍https://wanchain.org/files/Wanchain-Yellowpaper-EN-version.pdf）

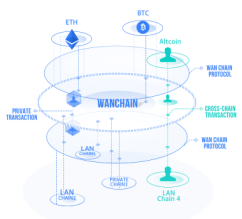
##### 功能评测

Wanchain 目前为 2.0 版本，提供的功能主要有三个：

1.不同数字货币跨链交易: 用户可以在 ETH/WAN（Wanchain 公链）的主网和测试网络之间切换，从以太坊将 ETH 发到 Wanchain 公链，以及从 Wanchain 取出 ETH 到以太坊。

2.隐私交易：正常以太坊账户之间的交易，不过具有更强的安全保护。

3.数字金融创新应用：作为一个通用的跨链交易协议。



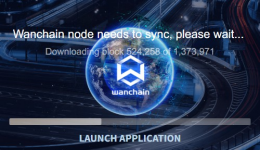
1.1 跨链交易

首先访问 https://wanchain.org/product， 下载最新的 2.1.2 版本（支持 Windows、Mac 和Linux 系统，下面以 Windows 版本为例）：

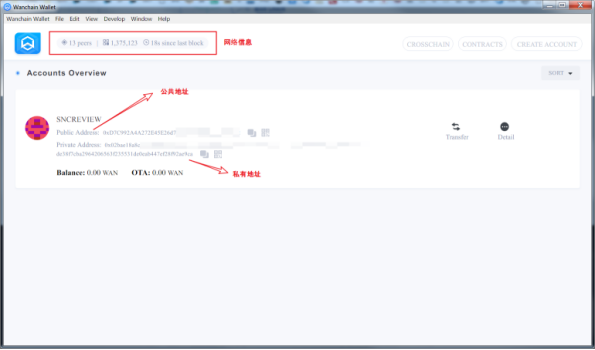


安装完成后，显示节点启动，寻找 P2P 节点（总共连接到 13 个节点），继而同步区块（当前总共 1,375,123 个，还在增长中）信息：

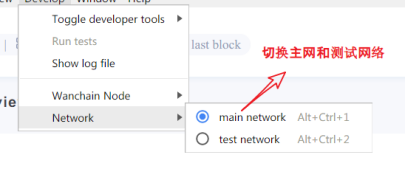




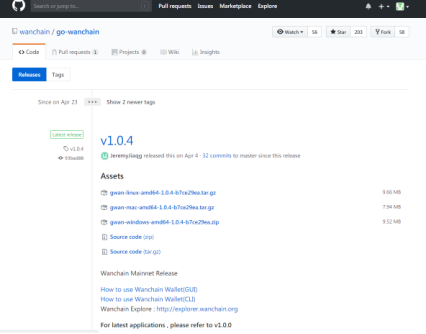
然后需要创建帐户和密码，之后进入主界面：



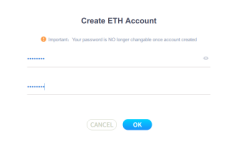
可以通过菜单切换主网和测试网络：



遗憾的是，虽然程序版本已经到达 2.1.2，但是 HELP（帮助）下的说明链接中最新只停留到 1.0.4：



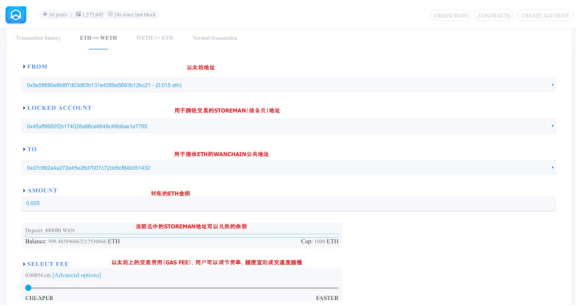
在主界面中，可以选择导入 ETH 钱包或者创建新的 ETH 钱包，下面尝试新建了两个：



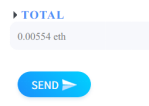
然后点击 CROSSCHAIN，可以看到两个新建的 ETH 地址，下面为其中一个账户转入部 ETH，就可以将其兑换为 WETH：

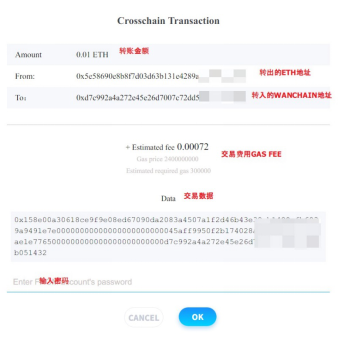


而后，选择从 ETH 到 WETH（WETH 即 Wanchain Ethereum Crosschain Token，Wanchain 以太坊跨链代币，即 ETH 在 Wanchain 上的代码）的转账：

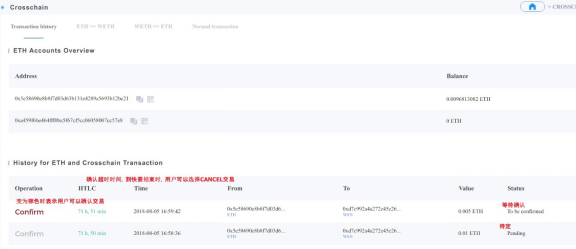


最后点击 SEND，即

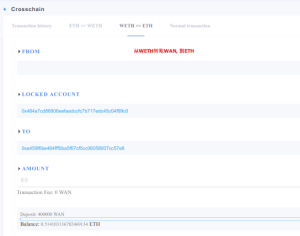




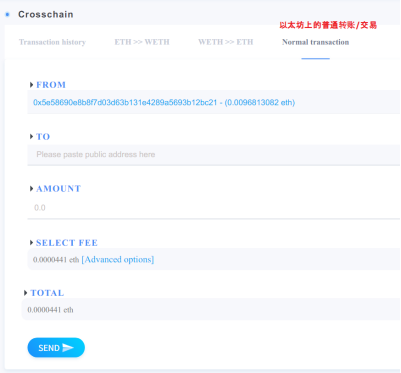
提交交易之后，就可以在主页看到交易状态：



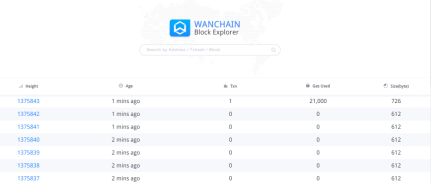
点击 CONFIRM，就可以确认交易。  
以同样的方式，可以完成从 WETH 到 ETH 的交易：



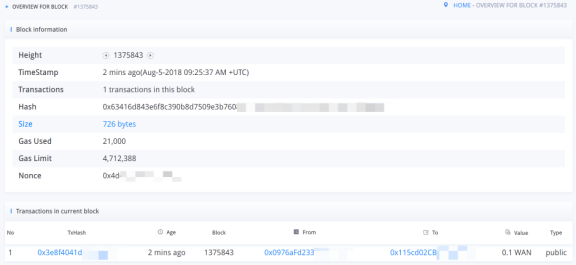
以及以太坊上的正常转账（normal transactions）：



完成到 WAN 的交易之后，可以在其浏览器查看交易记录：<https://explorer.wanchain.org/>



打开区块信息界面，可以看到其中包含的交易信息：



就其原理而言，跨链交易实际上是在发起方和接收方之间添加一个 Storeman 的角色/地址，由其进行转换。当以太坊上的某个用户需要发送一笔跨链交易使 ETH 能够转移到 Wanchain 上时，用户的钱包会构造一笔以太坊交易，这笔以太坊交易被哈希时间锁锁定，Wanchain 上负责处理跨链交易的 Storeman 在检测到这笔跨链交易后，会在 Wanchain 上发起一笔跨链的合约交易，该笔交易负责产生 WAN 币，转移到用户指定的跨链接收账户，此时该笔交易被跨链合约锁定。

当用户的钱包检测到被跨链合约锁定的交易后，主动释放密数（secret）到跨链合约中，Storeman 通过该密数获得锁定账户中对应的以太坊的控制权，用户获得 Wanchain 上 WAN 币的控制权。如果这个过程中，用户在哈希时间锁的时间范围内没有释放密数（即没有点击 CONFIRM），则哈希时间锁（HTLC）到期后，用户重新获得 ETH 的控制权，跨链合约中的交易自动失效。

以上跨链过程看似复杂，但多数功能都由钱包和合约完成，用户只需要在发起交易、释放密数、撤销交易的环节进行操作。对于参与跨链的 Storeman，Wanchain 会提供专门的客户端，客户端根据协议进行无需值守的自动化运行。

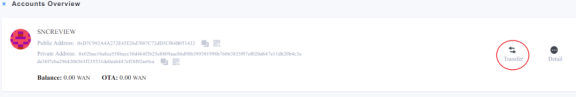
从 Wanchain 转出到以太坊，对于用户同样是从钱包端向 Wanchain 发出请求，这个请求会使 Wanchain 在以太坊上给用户提供的账户转入相应数额的 ETH，并将 Wanchain 上的对应的代币 WAN 销毁。

1.2 隐私交易

Wanchain 的另外一项功能是隐私交易。

1.2.1 发起隐私交易

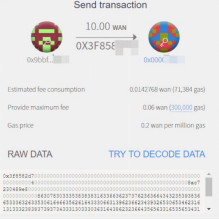
作为转出方或者发起交易的一方，首先点击主页中的 Transfer:



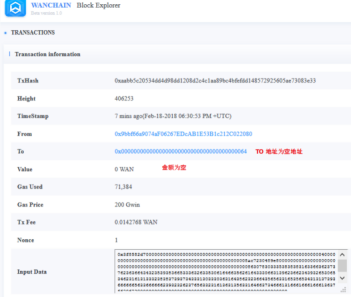
然后在 FROM 下面，选择「switch to private」，再在 TO 里面输入对方的 Private Address（对方需要提前提供这个地址），输入需要转账的 WAN 金额，再点击 SEND。



而后点击 SEND，确认交易信息：



完成私密交易之后，在 Wanchain 浏览器中查看此次交易，会发现 FROM（发送方）的地址会正常显示，但是 TO 地址为空，金额也为 0，即不会透露收款人和汇款金额，达到了保密的目的。



1.2.2 接收隐私交易

要接收隐私交易，则需要在首页中点击 DETAIL：



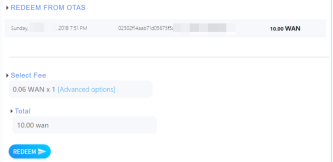
而后点击 GET OTA：



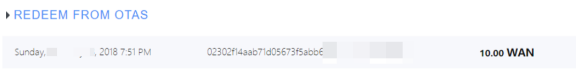
输入账号，而后等待一段时间交易完成之后，就可以在余额之中，看到 OTA 账户中收到的私密转账：



点击 REDEEM，注意这时需要缴纳一定的费用（WAN），才能提款：



这时就可以在余额中查看完成的私密交易：



总体而言，这部分功能已经可以执行。

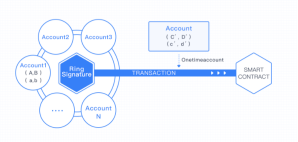
就其原理而言，WAN 代币的隐秘交易采用了与 Monero 项目类似的环形签名技术，一方面将智能合约代币交易的发起者隐藏在一个账户集合之中，一方面通过一次性账户系统使得智能合约中的账户一次性使用（一次性账户即私密账户的创建过程由函数实现），而且与 Wanchain 上原生账户之间无法建立对应关系，从而使得合约内的账户与原生账户隔离，这样就实现了交易的隐私性。

举例来说：张三创建了个一次性地址，并往里存了 100 个 WAN 币，这是大家都有目共睹的，但是却没人知道这个一次性地址是谁的；而由于这个一次性地址本就是给李四创建的，那李四自然发现了他可以支配这个账户，然后他又把其他的地址一块拿过来做挡箭牌，让大家只知道那一堆账户里面有一个的钱被李四提走了，却又不知道提的具体是哪一个账户，也就让这真正使用的一次性地址销声匿迹。通过这两个手段，自然切断了张三和李四之间的联系，也就实现了匿名的代币交易。

技术上来说，结合 Wanchain 实现跨链交易，任何一种其他链上的币种都可以转到 Wanchain 上来以代币的形式存在，进而进行交易。那么在代币上实现隐私保护也就间接的给其他所有的币种实现了隐私保护功能，解决了其他公有链上的隐私保护问题。为实现代币交易的隐秘功能，Wanchain 设计了一套独特的邮票（stamp）系统，以解决合约使用中的 gas 消耗问题。

邮票系统是一个智能合约，与现实中的邮票类似，任何用户可以在合约中买其需要面值的邮票，当然，邮票面值是离散且固定的。具体过程是这样的，张三突然又想给李四转点代币，却不想让别人知道，他原本在合约里有一个一次性地址，我们就叫这个地址为 1 号账户。首先张三去邮票系统买了张邮票，假设就买了 1 个 WAN 币的邮票。随后他给李四创建个一次性地址 new，并在纸上写下了这样一笔交易：「从合约中的 1 号账户里给 new 这个账户地址转 100 个代币」，然后他把这张信纸折起塞进一个空信封密封起来，再拿着自己的邮票去和邮票系统里 1 WAN 币的其他几个邮票利用环签名攒成一堆贴到信封上发出去。系统里的交易验证者Validator相当于邮差，拿到信封之后，看到信封上这一堆邮票，然后把信封拆开，按照要求把合约里的 1 号账户扣 100 个代币，并创建一个地址为 new 的账户，给里面加 100 个代币，然后 Wanchain 的系统机制就把这堆邮票变成 1 个 WAN 币给 Validator。这笔交易就完成了。

整个过程对保证隐私性的原理是，虽然张三买了邮票，但是张三却把这邮票跟别人的邮票攒起来贴到信封上，而且合约中的 1 号账户本就是张三的一次性地址，谁也不知道它是张三的。这样，发起人张三把自己隐藏起来了。对于李四的隐藏就更简单了，本就是张三给他生成的一次性地址，除了张三和李四本人，谁也不知道这地址对应的账户就是李四的，也就让李四也匿名了。这样，就完成了代币的隐秘交易。

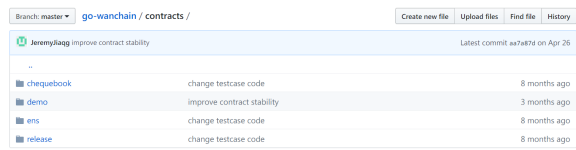


1.3 智能合约

Wanchain 的另外一项功能是支持合作伙伴所开发的智能合约，将其部署到公链上，具体步骤在这里列出：<https://github.com/wanchain/go-wanchain/wiki/How--to-deploy-smart-contracts-on-Wanchain>

其中包括：  
1.怎么用 Solidity 开发合约示例；  
2.怎么编译和部署合约；  
3.怎么调用私密交易。

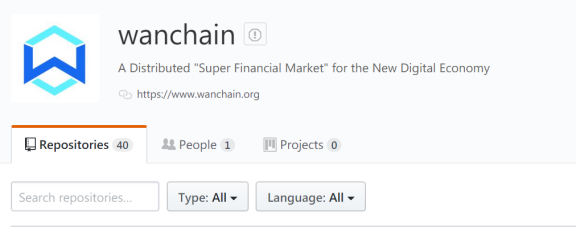
并且提供了示例合约，见下图中的 demo：



ENS 用于以太坊名称注册，RELEASE 用于通知版本更新通知。Chequebook 是一个使用 Wanchain 公链的智能合约，提供「支票本」的功能，不过创建之后一直没有更新和说明。

##### GitHub 代码质量评测

##### Wanchain 项目的代码已在 GitHub 开源：<https://github.com/wanchain>



其中主要后端代码位于：[https://github.com/wanchain/go-wanchain。](https://github.com/wanchain/go-wanchain%E3%80%82)

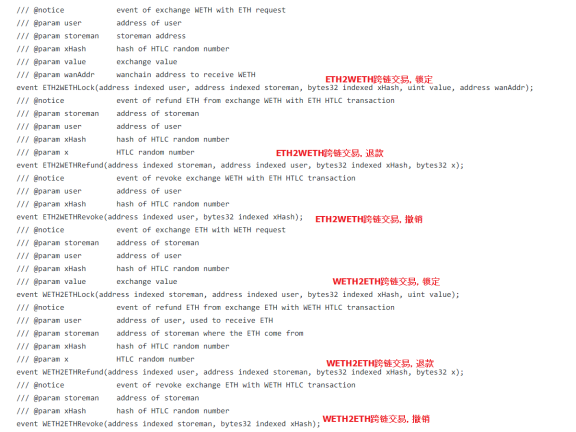
其主要功能的代码分别如下：

1.与以太坊的跨链交易：  
<https://github.com/wanchain/go-wanchain/blob/master/ethclient/ethclient.go> 这个程序实现了与以太坊节点的交互，即调用 Ethereum RPC API。

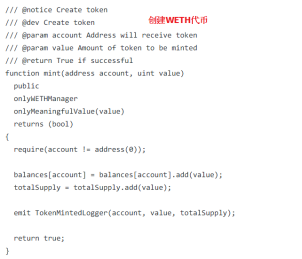


跨链交易的智能合约，都在这里：

<https://github.com/wanchain/wanchain-crosschain-contracts/tree/master/contracts>   
譬如<https://github.com/wanchain/wanchain-crosschain-contracts/blob/master/contracts/HTLCETH.sol> 中的 events, 列出了跨链交易的主要事件：



WETH 代币的管理，主要在这个合约之中：  
<https://github.com/wanchain/wanchain-crosschain-contracts/blob/master/contracts/WETH.sol>   
譬如：



2.WAN 区块的生成、验证，交易的记录，交易费用的计算，都在：  
<https://github.com/wanchain/go-wanchain/tree/d6724db2427a09648d3f38bb102131d812735504/core> 特别是私密交易处理的方法，都记录在这个智能合约之中：  
<https://github.com/wanchain/go-wanchain/blob/b7ce29ea7dd2cc64a7ca98fd2662acff0d0de2da/core/vm/contracts.go>   
譬如环形签名密钥的解密，这部分是其核心算法：





锁仓代码检查

在代码中，没有找到任何关于锁仓的智能合约，在白皮书中也没有提及锁仓。

标准共识分析：

Wanchain 项目的研究、开发团队相当出色，采用了一些创新的算法和理论，来解决区块链行业长期存在的几个难题，包括用邮票方法解决保密交易问题和用 Storeman 这种中间机制解决跨链交易问题，而且代码相当规范，注释详细，提交频繁，架构清晰。

按照项目的路线图，目前承诺的功能已经基本兑现，包括跨链交易和隐秘交易，目前主要支持 Wanchain 和以太坊之间的相互交易，另外交易速度受到以太坊的限制，较慢。目前已经开放了面向开发者的智能合约支持，不过迄今还没有看到第三方开发的智能合约在其上运行。

#### Token 生态系统

WANCoin 是万维链的原生币，总量为 2.1 亿个，没有增发机制，代币分配情况如下：

|  |  |  |
| --- | --- | --- |
| **分配方** | **总比例** | **说明** |
| 公开销售 | 51% | 众筹价格为 1 ETH=880 WAN |
| 团队 | 20% | 白皮书中无锁仓说明 |
| 基金会 | 19% |
| 节点奖励 | 10% |

众筹所募得的资金计划用途如下：

|  |  |  |
| --- | --- | --- |
| **使用规划** | **比例** | **说明** |
| 研发 | 60% | 支付工程师的薪酬，社区中的重要参与者和贡献者的奖励，外部专家和顾问的咨询费用。 |
| 社区 | 10% | 激励与支持社区参与者基于万维链开发商业应用，推进万维链生态的发展。 |
| 市场推广 | 10% | 将用于参加和组织全球性或地区性的金融或区块链行业峰会、重要媒体的市场宣传，扩大万维链的影响力。 |
| 商业运营 | 10% | 用于拓展生态中的商业合作伙伴。 |
| 日常运营 | 10% | 用于财务、法律、人事、办公场地等的相关支出。 |

##### 代币 Token 主要用途

Wanchain 代币主要用途包括：

1）链内的普通交易以及跨链交易都将消耗一定量的代币；

2）代币还会被用作跨链交易验证节点的保证金。

##### 共识机制

## 

万维链上普通交易的共识机制，采用 PoS 共识。PoS 共识算法理论上存在参与者合谋攻击的威胁，万维链引入**跨链交易的共识和激励机制**去提高验证节点合谋的机会成本，使得万维链能够真实的记录跨链交易和客观的完成跨链流程。

1.跨链交易的共识

万维链上验证节点设计为普通验证节点（Validator）、跨链交易证明节点（ Voucher）和锁定账户管理节点（Storeman）：

1）**跨链交易证明节点**负责在跨链交易过程中提供原有链账户与锁定账户之间交易的证明，同时它也需要缴纳一定的保证金，保证金越多，它所提供的证明被采纳的概率也越高，如果提供虚假证明，它的保证金将会被扣除并剥夺跨链交易证明节点的身份；

2）**普通验证节点**负责在收到达成共识的交易证明后，通知 Storeman 对锁定账户进行相关操作并完成万维链账本的记账操作；

3）**锁定账户管理节点**负责在接到通知后，通过自己所持的密钥份额计算出签名份额并最终合并为锁定账户完整签名，以便进行锁定账户的相关操作。

2.验证节点的激励机制

1）对于跨链交易证明节点，正确的提供原有链账户与锁定账户之间交易的证明，将会根据其保证金获得相应份额的交易费用；如果提供虚假的交易证明，将会被扣除保证金并取消节点资格。

2）普通验证节点完成万维链上的记账，并获取所记账交易的部分交易费。

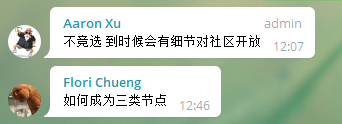
3）锁定账户管理节点根据其所持权益获得对应数量的密钥份额，按比例获取参与验证交易的交易费。如果离线或者丢失密钥份额无法参与验证交易，就不能获得交易费，如果对错误交易签名，会被取消身份。

标准共识分析：

万维链将验证节点分为三类，将跨链交易的验证权限进行分离。一方面，每一类节点内部需要达成共识；另一方面，单独一类验证节点即使合谋也无法完成跨链交易的伪造。这种分离机制降低了验证节点合谋的可能性。

验证节点激励机制会激励跨链交易证明节点提供正确的交易证明，激励普通验证节点如实的完成万维链记账，激励锁定账户管理节点保持在线并安全保管自身密钥份额。

但这对种机制的设置并不能消除验证节点合谋作恶的可能性，此外，目前 Wanchain 对于验证节点的选举和设置机制不透明，对于三类节点的产生目前尚未做详细披露。标准共识就验证节点选取的方式向项目官方中文电报群管理员进行了询问，得到回复如下：



**社群基础**

##### 用户社区

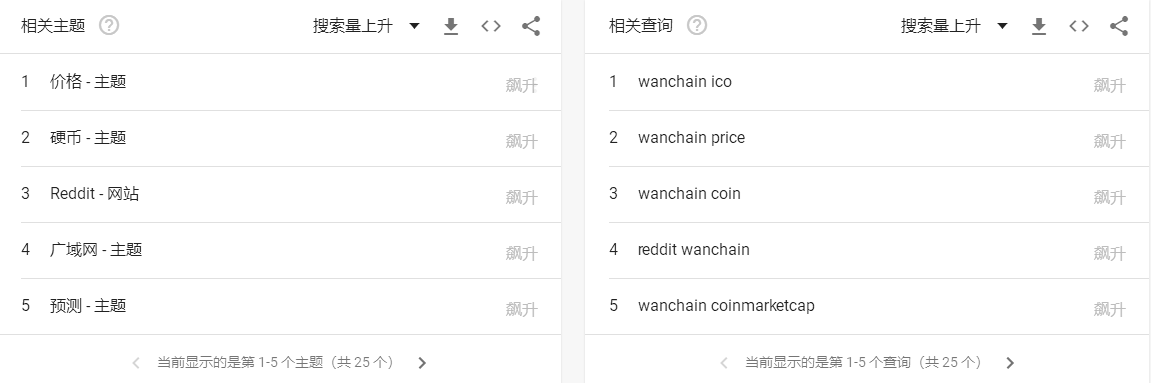
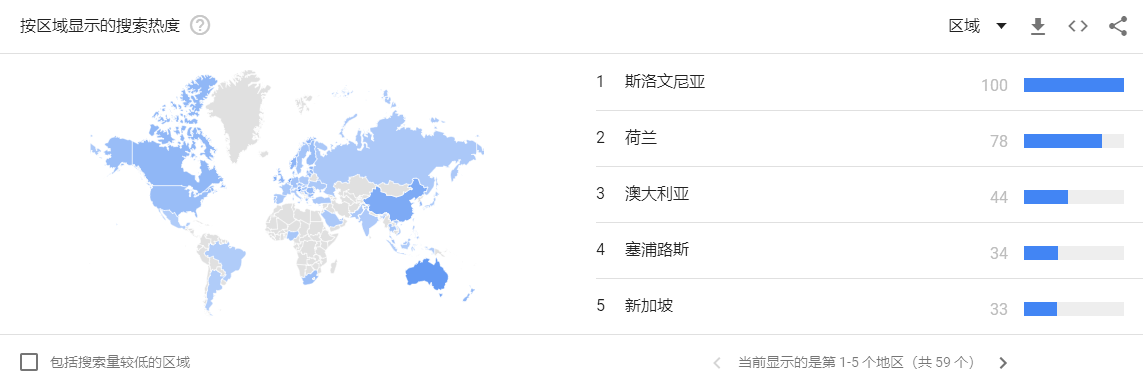
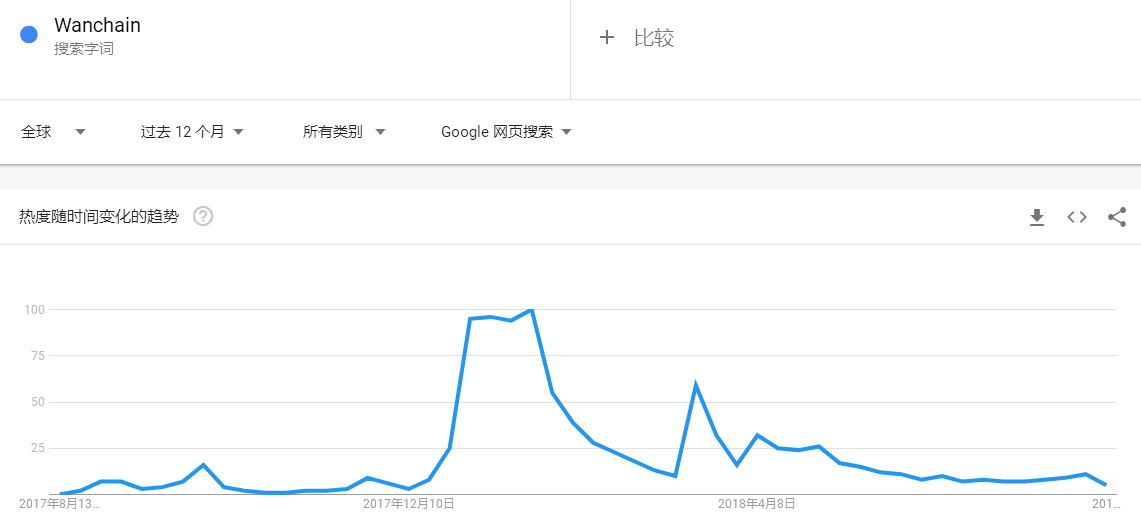
Wanchain 社区用户成员数量较多，推特粉丝达到 11 万，群组内沟通较频繁，社区管理人员回复消息较及时，整体来看官方社群运营较为积极。

|  |  |  |
| --- | --- | --- |
| **分类** | **地址** | **表现** |
| Facebook | https://www.facebook.com/wanchainfoundation | 关注者：18,968 |
| Twitter | https://twitter.com/wanchain\_org | 关注者：110,000 |
| Reddit | https://www.reddit.com/r/wanchain/ | 订阅者：17,600 |
| Telegram | https://t.me/WanchainANN | 成员数：43,798 |
| Youtube | https://www.youtube.com/channel/UCW\_i8cncT0d1RyX7YCA\_oKQ | 订阅者：2,725 |
| Discord | https://discordapp.com/invite/3DpeV6W | 成员数：8,942 |
| Weibo | https://www.weibo.com/wanchain | 关注者：764 |

##### Google 趋势

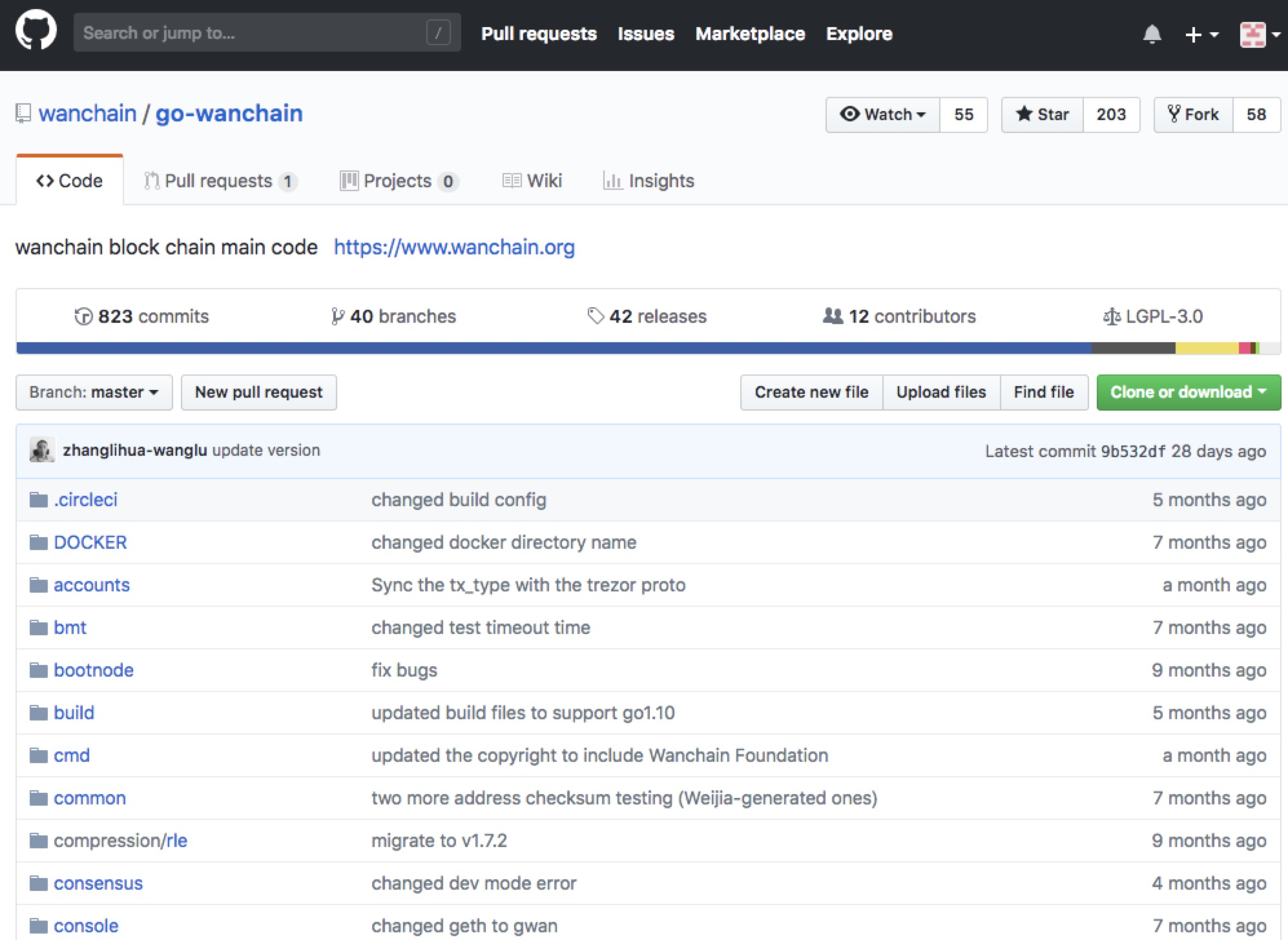
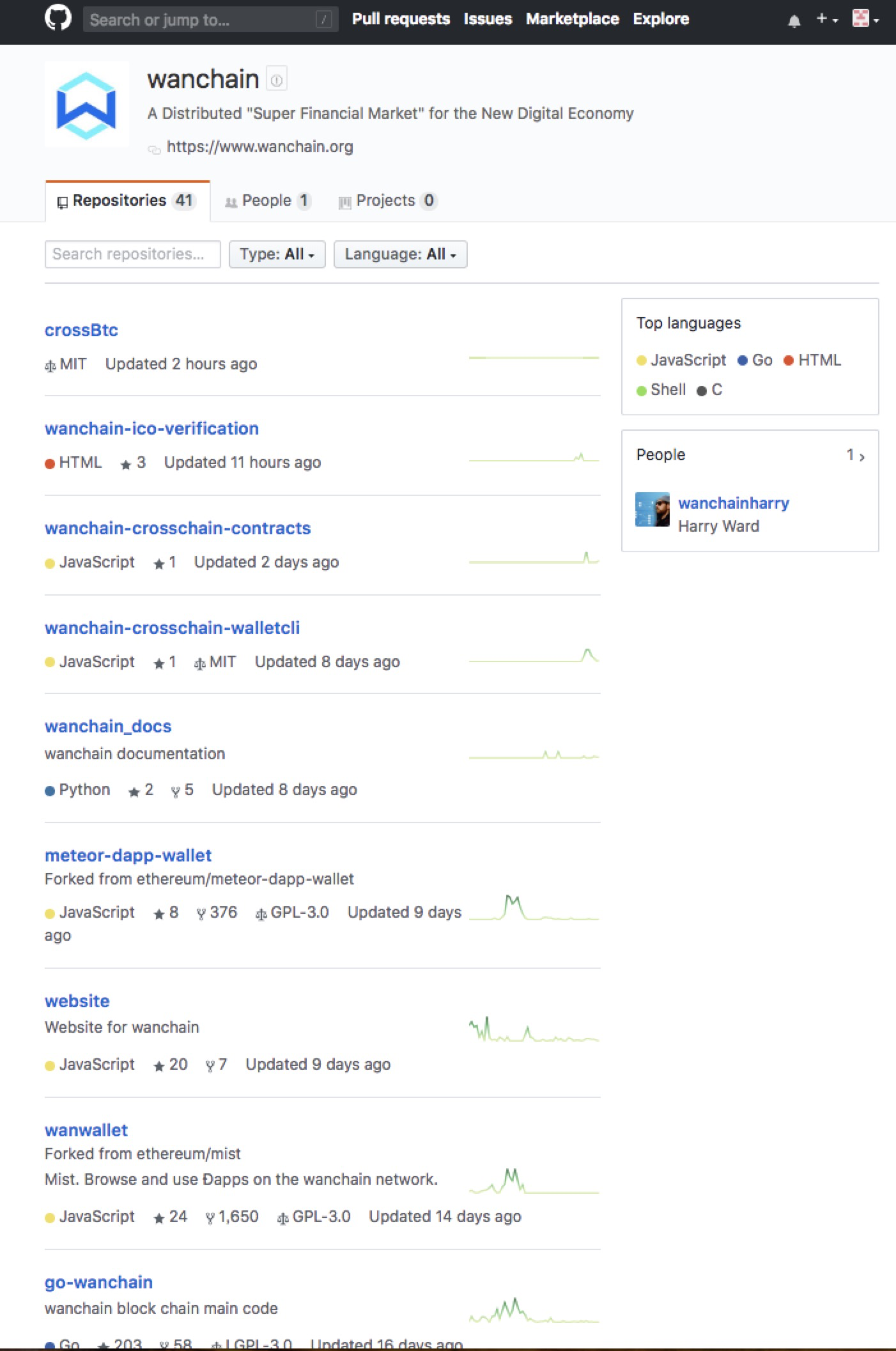
根据 Google 趋势，目前搜索「Wanchain」的热度较高的地区为斯洛文尼亚，其他地区依次为荷兰、澳大利亚、塞浦路斯、新加坡。

下图为 Google 趋势截图：



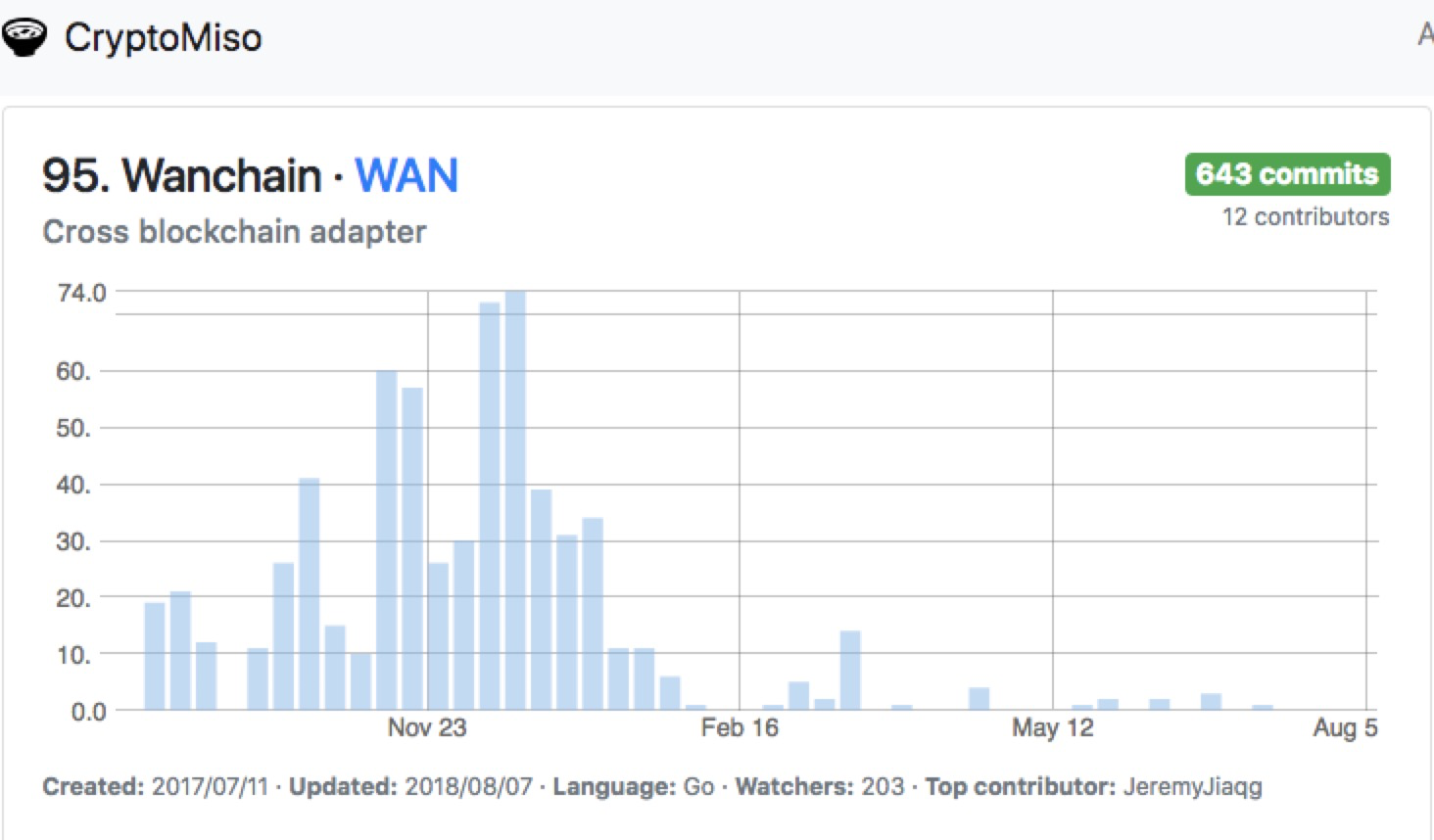
##### 开发者社群

官方的 GitHub 主页有 41 个库，主要的库是 go-wanchain ，该库有 55 个 Watch、203 个 Star、58 个 Fork、823 个 Commits、40 个 Branches、42 个 Releases、12 个 Contributors。  
下图为 Wanchain GitHub 主页：



标准共识分析：

代码提交活跃，在 8 月 7 日 CryptoMiso 12 个月指数代码提交次数中排名第 95，一共 643 个 Commits。



开发者社群关注度较高，Watch 、Fork 和 Star 的数量相较一般；主力开发者数量较少，提交 Commits 数量超过 50 的有 5 位。



#### **团队分析**

根据官方的最新公告，团队的任职信息如下：

|  |  |  |
| --- | --- | --- |
| **管理层** | **职位** | **背景介绍** |
| 吕旭军 | CEO  联合创始人 | 毕业于北京大学，俄亥俄州立大学 MBA；  2014 年创立公证通，2016 年成立网录科技。 |
| 李尼 | 副总裁 | 毕业于北京大学，杜伦大学计算机科学硕士；  超过 15 年的 IT 业务、营销、BD 国际经验；  曾在中兴通讯，台达电子和超图软件担任业务团队的董事和负责人；  FECC、中国农业部、粮食及农业组织 IT 顾问。 |
| Oliver Birch | 全球传播副总裁 | 兰开斯特大学哲学，政治经济学学士；  任多家初创公司项目经理；  多年加密空间社区管理经验。 |
| Scott Trowbridge | 全球业务总监 | 7 年以上技术组织和初创公司经验 |
| Dynal Patel | 战略伙伴主管 | 开普敦大学计算机科学博士；  在 Vodafone，Altran Technologies 和 Microsoft 拥有超过 15 年的管理经验。 |
| Weijia Zhang | 工程主管 | 物理学博士，毕业于中国清华大学； 发表了 30 多篇研究论文，20 项专利的发明人；  戴尔 14 年软件工程师工作经验。 |
| 张英 | 高级工程师 | 曾担任多家公司的 CAO 和 CTO；  以太坊的高级开发人员，对区块链架构、智能合约和共识算法有深入的了解和工程经验。 |
| 韩锋 | 顾问 | DACA 秘书长 |
| David A. Johnston | 顾问 | Bit Angels 执行董事 |
| Albert Ching | 顾问 | i-Sprint 创始人 |

标准共识分析：

Wanchain 团队人员配置合理，整体技术实力较强，团队拥有区块链资深开发创始人及丰富的数学、计算机领域专业人才，同时亦拥有金融及营销、运营等对项目发展有重要影响的人才。  
  
但官网团队成员信息披露与白皮书中团队成员信息部分存在差异，包括科学团队负责人梁智 (Zane Liang) 在内的多位核心技术成员疑似离开团队，该项目核心成员流失率方面存在风险。

项目全球副总裁李尼，在官网的表述中还曾担任 FECC，中国农业部（MOA）和粮食及农业组织（FAO）的 IT 顾问，但是标准共识经多渠道查找，未找到与此披露具有相关性的信息。  
  
**治理结构**

#### 基金会

万维链基金会是在新加坡注册的非营利组织，为 Wanchain 开源社区服务。基金会将建立适当的资金使用方案。并制定运营和资本使用计划，以促进 Wanchain 社区的发展。

万维链基金会负责：

1）万链社区的运营资金筹集；

2）参与和推广 Wanchain 开源项目；

3）与专业审计机构合作，定期公布基金分配情况。

标准共识分析：

官方白皮书对基金会做了介绍，但只简单就基金会未来的职责进行了说明，并未详细解释万维链基金会的组织架构、运作决策机制及内外部监督体系。

目前来看，基金会职责履行情况良好，基金会对与生态建设和社区维护方面做得较好，但就目前官方披露的治理信息来看，决策治理透明度还不高。

### **项目履约情况**

根据白皮书披露，Wanchain 的路线图如下所示：



|  |  |  |
| --- | --- | --- |
| **时间** | **生态体系规划** | **落地情况** |
| 2016 年 6 月 | 开始理论设计及论证，跨链交易及隐私保护 | 完成 |
| 2016 年 12 月 | 完成理论设计，基于智能合约代币隐私保护的 POC 开发 | 完成 |
| 2017 年 6 月 | 发布白皮书，万维链网站上线，进入首次公开代币销售阶段 | 完成 |
| 2017 年 9 月 | 进行代币销售开始，发布万维链测试网络 | 完成 |
| 2017 年 11 月 | 万维链 1.0 上线，实现万维链钱包及带隐私保护的智能合约功能，WAN Coin 发行 | 2018 年 1 月完成 |
| 2018 年 6 月 | 万维链 2.0 上线，支持以太坊跨链交易，万维链跨链协议 1.0 上线，多币种万维链钱包 1.0 上线 | 2018 年 7 月完成 |
| 2018 年 12 月 | 万维链 3.0 上线，支持比特币跨链交易，万维链跨链协议 2.0 上线，多币种万维链钱包 2.0 上线 | 待完成 |
| 2019 年 12 月 | 万维链 4.0 上线，支持联盟链跨链交易，万维链跨链协议 3.0 上线，多币种万维链钱包 3.0 上线 | 待完成 |

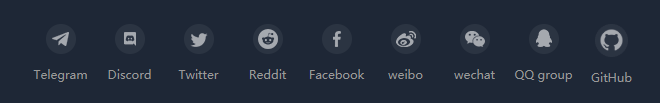
标准共识分析：

Wanchain 项目前期有较为清晰的路线规划，对于项目的推进计划和时间安排均做了较为详细的安排。

Wanchain 阶段性的开发目标稍有延迟，例如，如万维链 1.0 发布原定于 2017 年 11 月，推迟到 2018 年 1 月才正式发布。项目开发落地稍有延期，整体履约情况一般，开发进度不及预期，有一定的风险。

### **项目信息披露义务**

1）Wanchain 官网公布：项目白皮书，技术黄皮书，商业计划书以及 Wanchain 文档，对于项目开发相关信息披露较全；  
  
2）Wanchain 并没有建立起完善的周报制度，根据官方 Medium 主页信息查询，曾建立周报制度，但近几个月没有再更新。  
  
3）官方也通过 Twitter、Medium 对重要的活动及事件，有详细的报道，信披渠道丰富。



4）白皮书报告中提及，基金会将和专业审计机构合作，定期公布基金分配情况，但并未说明发布周期，且截至目前并未进行相关披露。

标准共识分析：

Wanchain 官网通过一系列的介绍，让项目关注者、投资者更好的了解 Wanchain，通过Twitter、Medium 对重要信息及时更新。但 Wanchain 并未持续形成周报制度，Wanchain 的信息披露制度相较一般。

此外，由于基金就披露审计分配情况的说明时间界定较模糊，且项目首次代币发行距今时间跨度不足一年，项目方未就基金会的分配情况进行审计报告披露，暂无法验证基金会是否按承诺披露信息。

### **交易模块**

#### **币值表现**

WAN 当前价格为 0.8489 美元。

|  |  |
| --- | --- |
| **项目** | **数值** |
| 价格 | 0.8489 美元 |
| 流通供给量 | 106,152,493 |
| 总供给量 | 210,000,000 |
| 流通率 | 50.55% |
| 流通市值 | 90,112,851 美元 |
| 市值 | 178,269,000 美元 |

注：数据来源于 Coinmarketcap（2018 年 8 月 19 日）

根据 Coinmarketcap 数据，截至 2018 年 8 月 19 日，WAN 共登陆 7 家交易所，成交主要集中于 1 家交易所，市值排名第 77 位。

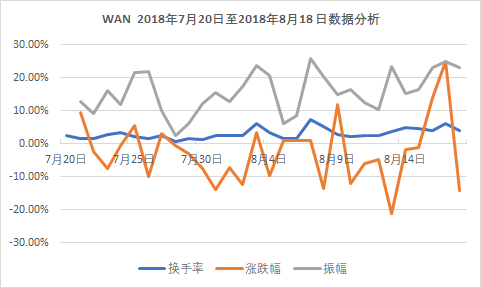
|  |  |  |  |
| --- | --- | --- | --- |
| **来源** | **货币对** | **交易量（%）** | **成交量占比（%）** |
| Binance | WAN/BTC | 78.21% | 95.69% |
| WAN/ETH | 14.95% |
| WAN/BNB | 2.53% |

注：剩余交易所合计占总成交量的 4.31%

（交易量占比不足 1% 货币对及交易量占比不足 5% 的交易所不予显示）

|  |  |
| --- | --- |
| **热门货币对** | **总成交量占比** |
| WAN/BTC | 81.89% |
| WAN/ETH | 15.58% |

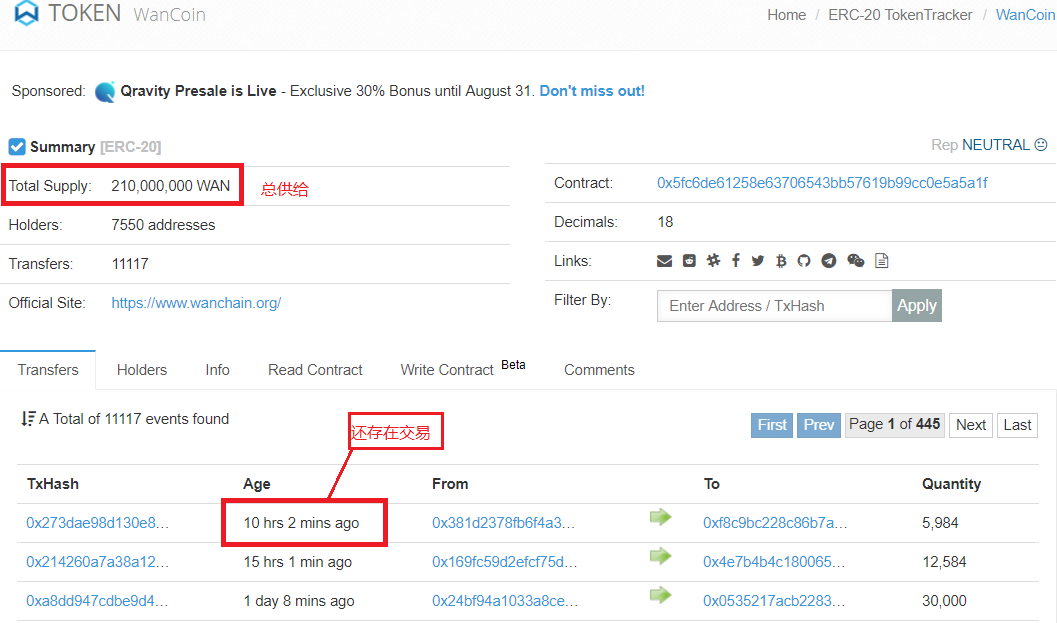
WAN 共有 5 个货币对，热门货币对 2 个，主要集中于 WAN/BTC、WAN/ETH。热门货币对占总成交量的 97.47%。**整体而言货币对较少，交易所覆盖率低，市场影响力较低。**



#### 

近 30 个交易日，日涨跌幅超 10% 的交易日有 10 天，日振幅超 10% 的交易日有 25 天，交易波动频繁。全市场平均换手率为 3.06 % ，交易活跃度一般，流通性风险适中。

#### **持仓分布**



根据 Etherscan 数据显示，WAN 近期存在交易。同时在 Wanchain 主网也有对 Token 的描述，但并非 WAN 而是 WETH。无法确认代币是否存在从 ERC 20 向其主网迁移的可能，官方也没有针对该问题进行描述。

#### **市场表现**



从 Coinmarketcap 的全市场走势图来看，WAN 从上市交易以来，价格经历了近 30 个

交易日的上涨，且伴有较大的交易量。WAN 价格在 2018 年 5 月 4 日达到上市交易以

来的最高点。紧接着价格发生反转，且交易量短期内快速放大。随后进入缩量阴跌模式。



上图为 Binance 交易所显示的 WAN/BTC 货币对的日线图，跟同时期 Coinmarketcap

上显示的全市场价格走势高度一致。主要原因是 Binance 交易所的 WAN/BTC 货币对

在所有 WAN 相关货币对的交易总量中占绝对多数。



上图为 Binance 交易所显示的 WAN/BNB 货币对的日线图，跟同时期 Coinmarketcap

上显示的全市场价格走势基本一致。但投机情绪更加浓厚，**除了上市当天巨幅震荡、**

**和天量换手率外，其他交易日也出现过突然的砸单或拉抬。**



上图为 Kucoin 交易所显示的 WAN/BTC 货币对的日线图，价格走势跟同时期的

Coinmarketcap 数据基本一致。但值得注意的是在 2018 年 8 月前后，**若干交易**

**日出现巨大成交量，价格却没有较大波动，有对倒操作的嫌疑。**

**综上所述，币值方面，WAN 货币对较少，覆盖交易所较少，换手率适中，流通性风险中性；**

**持仓分布方面，无法确认 WAN 是否正在从 ERC 20 向其主网迁移，无法进行持仓分析；市**

**场表现方面，热门货币对上市当天均出现巨幅震荡和天量成交，其他交易日也出现过不同程度**

**的交易异常。可能存在被操纵的风险。**

## Outlook 展望

### 宏观经济展望

中国人民银行决定，从 2018 年 7 月 5 日起，再次下调国有大型商业银行、股份制商业银行、邮政储蓄银行、城市商业银行、非县域农村商业银行、外资银行人民币存款准备金率 0.5 个百分点，此次已经是央行年内第三次降准。6 月 19 日中国拟提升个税起征点至 5000 人民币，纳税总额将减少 1720 亿，国家多次缓解资金流动性。但目前商业银行大幅上调大额存单利率，及中国和中国香港银行间同业拆借利率都处于较高水平。皆表明市场整体资金流处于紧张状态。

我们预计，市场资金将由权益类投资标的向债务类和储蓄类投资标转移。数字货币市场也难在资金流趋紧的环境下独善其身。市场发展将在新生资金增长缓慢的压力下运行趋缓。6 月 14 日美联储再次加息 25 个基点，在美元持续走强的背景下，将加剧欧洲的债务危机以及新兴国家的货币波动，这些都会影响国际市场投资者的投资判断，去寻求新的投资标的。数字货币市场作为一个在不断完善过程中的金融市场，必将不断吸引新的资金进入。

另外，随着 6 月 15 日 美国将对中国 500 亿美元商品加征 25% 关税；6 月 16 日中国对美国 500 亿美元进口商品加征 25% 关税，皆 2018 年 7 月 6 日起实施。表明中美贸易战硝烟再起，国际经济形势再次紧张。

综上，目前我们对市场总体保持中性判断。

### 监管动向

数字加密货币以及相应的政策监管态势仍不明朗。

我们预计，中国的监管动向将会对虚拟货币市场产生全球范围内的影响。另外，国内互联网金融相关牌照的审批和发行趋严有可能引发资金端紧张，同时受到美国加息影响，全球货币面对下行压力，尤其是新兴市场货币在大幅下挫后，甚至进入货币保卫战阶段。这也标志着由全面宽松到收紧，全球资金压力大增。这会进一步加剧企业的融资困境，迫使企业寻找新的融资模式。

### 未来评级展望

如果 能够持续推进项目，综合二级市场最新的交易表现，我们可能调整其风险评级等级。

## Rating Action 评级结果

「」，该项目投资风险较高，投资者应该密切跟进观察和监督项目进展。主要依据是：

「」，该项目属于「一般风险」水平，需要投资者注意。主要依据是：

整个虚拟货币市场对宏观经济的波动反应还在自适应期，监管规则持续不明确。这些因素的调节作用不足以给 LRC 风险等级造成决定性影响。

感谢代码评审团成员 对本文中「技术分析」部分作出的贡献。此为 第二次参与技术评测。

免责声明：

* 标准共识提供的「风险评级」服务和其它一切相关评级产品仅是一种投资风险的提示，是标准共识根据调查和研究结果得出的结论。它并非衡量评级对象本身价值、以及其发行的 token 的价值的工具。
* 标准共识的风险评级仅是对特定风险的提示，而无法展示一个项目或一种虚拟货币的全部风险。
* 任何一个风险评级报告都仅展示某个时间范围内对项目和其 token 生态未来的投资风险预期，而非对未来某个事实确定发生的判断。
* 对任何项目的风险评级不构成投资者作出最终投资决策的全部依据。
* 标准共识仅是金融信息的提供者，评级类产品不对投资者的任何投资决策及其所导致的结果负责。
* 风险评级不是永久有效的，项目的投资风险等级可能随着时间、环境因素和项目进展等外部环境的变化作出调整。同时，评级标准调整也可能会造成项目风险等级变化。任何调整和原因都会向所有投资者公开。
* 在标准共识的评级体系下，我们按照不同的等级对评级对象的投资风险划分，用「S」「A+」「A」「B+」「B」「C+」「C」「D」等符号，由低到高依次表示其投资风险等级，展示一种相对的风险。

参考标准文档：

* 一般项目投资风险评级标准（初创期）