Black Hole Coin

黑洞币
白皮书

稳定 / 安全 / 实用 / 快速

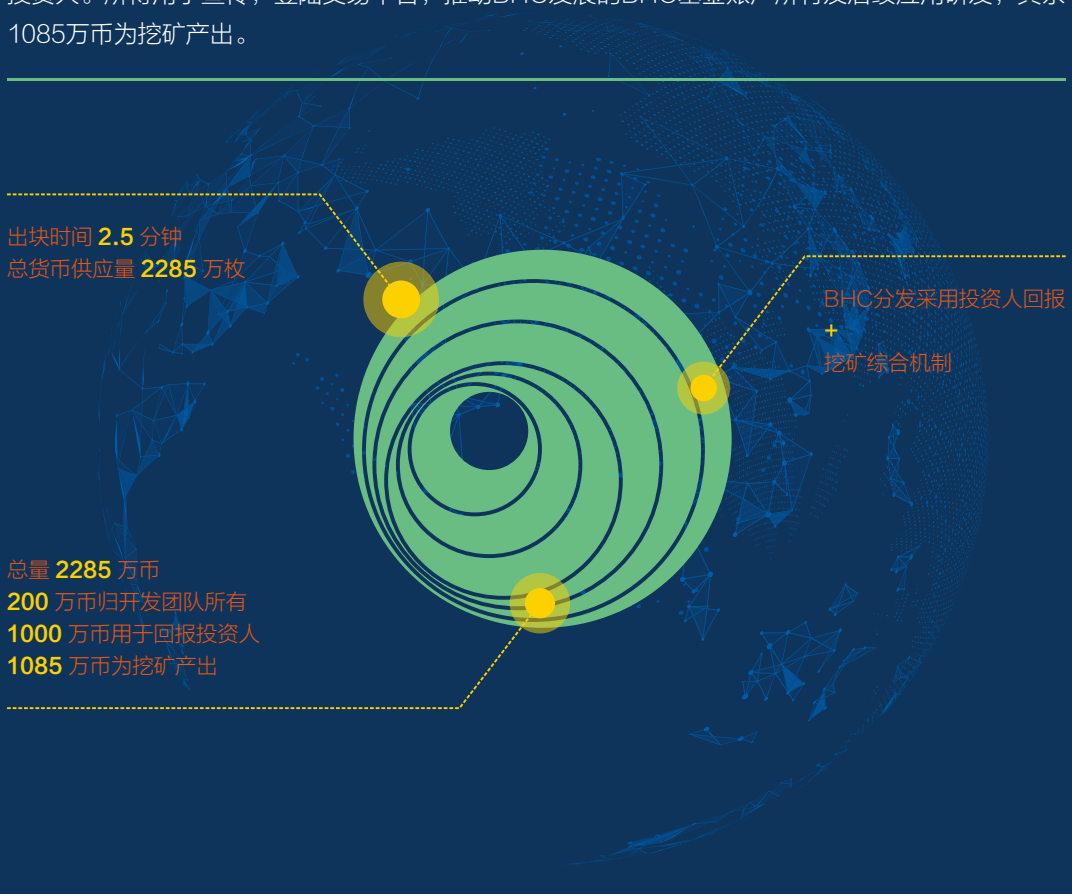
01.
电子币

Black Hole Coin(BHC)是一种通过使用零币协议(zerocoin protocol)来保障账务隐私的一种加密货币。它是第一种实现了零币协议的加密货币，通过使用零知识证明确保了交易双方的相关地址信息免遭泄露。

BHC出块时间2.5分钟，总货币供应量2285万枚，产出减半周期为4年。BHC去除掉创始人奖励，期间每块产出的20%也还是归矿工所有。

BHC是由欧洲顶级虚拟币开发团队研发，大部分成员为牛津大学及海德堡大学在校研究生及两名中国留学生。BHC分发采用投资人回报+挖矿综合机制，在保证开发团队先期开发成本的基础上，后期保障矿工及投资者利益。

BHC总量2285万币，其中200万币归开发团队所有，早期获得50万美元投资，1000万币用于回报投资人。所得用于宣传，登陆交易平台，推动BHC发展的BHC基金账户所有及后续应用研发，其余1085万币为挖矿产出。



02.

研发背景

近期，由于比特币的交易历史是完全公开的，所有人都可以通过你的钱包地址在区块链中查询你的钱包现金流入与流出，并可向上追溯至这些比特币的终极起源，即从区块生成后发送到的那个地址。这对个人隐私构成了巨大威胁。很多忠诚粉丝正在迫不及待寻找一种能完全匿名且安全透明的虚拟货币。在此背景基础上，匿名虚拟币Dash(达世）Zcash（ZEC）及Zcoin（XZC）等匿名币诞生，很多技术币也在打匿名的概念，并在虚拟币投资圈引起巨大轰动，给原始开发团队及旷工、投资者带来超额回报与发展动力。

随着匿名币技术的方兴未艾，矿工及虚拟币爱好者也对这种技术趋之若鹜，可是对于很多虚拟币投资者来说，现今的匿名币真的安全吗，据开发团队的团队成员透露，某些匿名币至今无法查询区块链，甚至没有加密钱包，个别匿名币出现黑天鹅事件。BHC团队尊重并致敬以往匿名币团队开发者及其技术的前辈，我们本着谦卑的心理来开发匿名币，在尊重学习的基础上更加注重改进机制，做到真正的匿名概念。

03.
团队介绍

John Wilson
Software Engineer & Teaching Assistant

Stanford University
2015年9月 - 2017年6月 任职时长1年10个月
Stanford, CA
- Winter 2015-2016, 2016-2017:
Teaching Assistant for CS142 - Web Applications
- Fall 2015-2016:
Teaching Assistant for CS251- Bitcoin and Crypto Currencies

Cryptography Researcher

Stanford University
2016年1月 - 2017年3月 任职时长1年3个月
- Working on implementing optimized BLS signature library in C++.
- Exploring costs and benefits of using BLS signature aggregation in the Bitcoin protocol
- Explored feasibility of code isolation in Erlang and Elixir.

Software Engineer Internship

Airbnb
2016年6月 - 2016年9月 任职时长4个月
San Francisco Bay Area
- Product Security

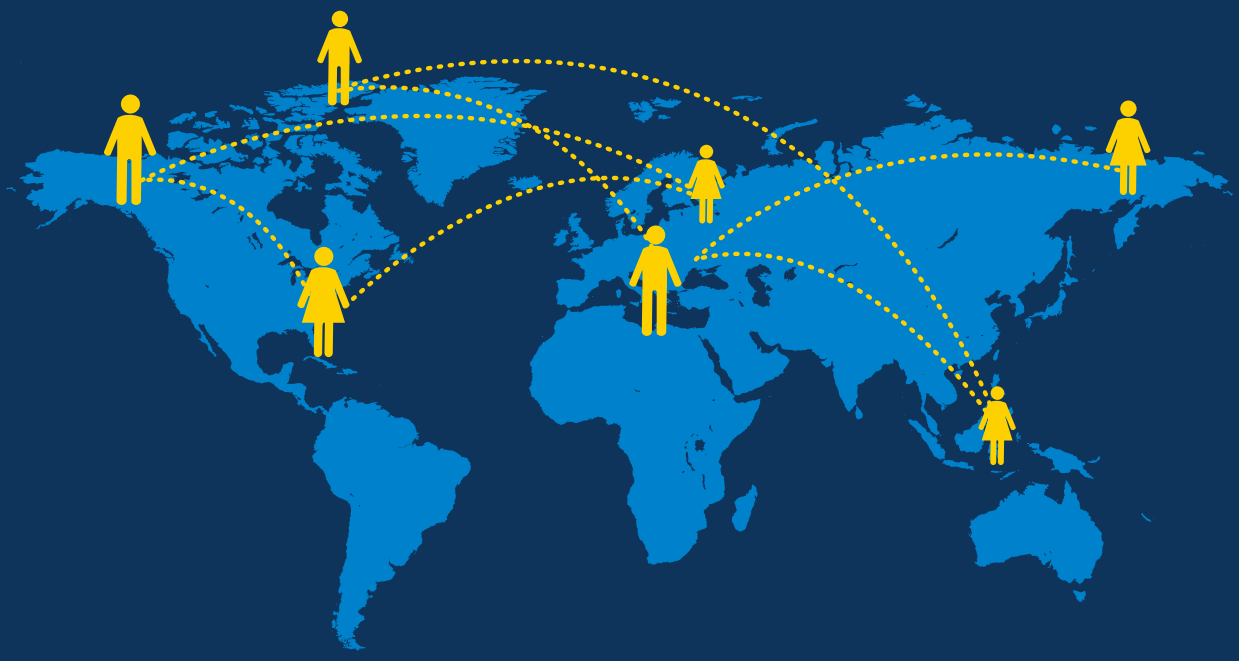
Stanford University
2015年 - 2017年
- Master of Science (MS) Computer Science

04.

优 势

比特币及后续的替代币尝试通过混币和环签名技术提升隐私匿名，但仍然有欠缺。首先，混币节点和签名节点中的恶意或被攻破成员，都是攻破匿名防线的突破口。再者，匿名技术架构，是理解加密货币隐私程度的关键。前两者的匿名解决方案受限于混币次数和环签名大小。每次混币和环签名受限转账次数，其进而被虚拟币块链容量大小所限。因此以前的尝试只能保证几百个转账的隐私性。

有了BHC，匿名性得到了显著加强。匿名转账再也不受次数限制，其匿名架构中有“minted coins”铸币功能。匿名转账容量可达数百万级，足以使以前存在的匿名技术成为古老落后的代表。BHC解决了之前虚拟币碰到的问题。BHC采用零币协议，通过零知识加密学证明实现了完全匿名。零知识证明实现了拥有BHC而无从知晓拥有者身份的目标。BHC通过钱包zerocoin协议，回炉生成BHC再转换跟踪不到的BHC。



05.

特 点

任何技术一样，BHC可能被用于好或者坏的方面，然而开发团队坚信好的方面将会远高于坏的方面，纵观历史，商业自由已被证明可防止战争，促进繁荣，并增加跨文化交流。BHC旨在为那些已经意识到使用具有完全透明的公共分类帐的加密货币存在风险，以及利用比特币公开其所有财务细节的风险的合法用户提供便利。

因为已经存在这样的活动的预先存在的机制，BHC不影响这种活动的现状，而它为合法用户提供显著的好处。

即便没有BHC的出现，通过现有的金融体系也可能存在非法的交易，比特币也面临涉及洗钱而收到监管机构的审查。BHC可以帮助确保商业自由。人们应该能够随意地进行交易，只要它不侵犯他人的福祉或个人自由。我们还相信，商业自由也促进各国和各国文化的和平与繁荣。通过保证金融隐私，BHC可以直接保证可互换性，这是自由商业的一个基本属性。

06.

愿景和计划

我们想推广一款完全匿名和无法跟踪的加密货币，它是Black Hole Coin—简称BHC，中文名黑洞币。它是一款使用零知识密码技术完全保护交易隐私的加密货币。

项目发展

2017年5月7日登陆中国，正在国内推广阶段。矿工最开始进入挖矿。登陆中国以来，在国内虚拟币圈得到了巨大的反响。一个刚刚推出的技术币，短短不到半个月间，挖矿算力达到了峰值36G，在已知的匿名币中，没有任何一种能这么快达到这么高的算力。这本身也说明了这个技术币得到了大家的认可，技术上也经受了币圈很多技术大牛的反复推敲验证。BHC总量2285万，其中1200万预挖，挖矿1085万，预挖的1200万BHC中，团队有200万用于节点计划并一直锁仓。早期获得50万美元投资，1000万币用来回报投资人。所得费用，将全部用于将来BHC的公关，上平台费用及BHC更改更先进算法所需资金，团队一分不取。

规划风险

加密货币是一个早期并且高风险的行业，投资和参与，需要谨慎再谨慎，小心再小心！由于币本身性质，有可能会遭遇一些攻击，时序攻击，算力攻击等。但是，这些都可以防范和避免，只要在“零币协议铸币”和“零币协议花销”之间等稍微长时间，即可防止时序攻击。并且团队之后后续工作量证明机制算法改为团队于2013年原创的GKS算法，此算法为非对称加密算法（也叫公开密钥加密算法），可以抵御GPU，FPGA，ASIC矿机，防止51%攻击，保证加密数字货币流通算法更安全。并且钱包增加去中心化的主节点masternode奖励系统 ，进一步扩展优化匿名传输功能，完善真正匿名的交易方法。

07.

为什么需要你的支持

特点：1、Black Hole Cion(BHC)是一种通过使用零币协议(zerocoin protocol)来保障账务隐私的一种加密货币。它是第一种实现了零币协议的加密货币，通过使用零知识证明确保了交易双方的相关地址信息免遭泄露。

特点：2、有了BHC，匿名性得到了显著加强。匿名转账再也不受次数限制，其匿名架构中有“minted coins” 铸币功能。匿名转账容量可达数百万级，足以使以前存在的匿名技术成为古老落后的代表。BHC解决了之前虚拟币碰到的问题。BHC采用零币协议，通过零知识加密学证明实现了完全匿名。零知识证明实现了拥有BHC而无从知晓拥有者身份的目标。BHC通过钱包zerocoin协议，回炉生成BHC再转换跟踪不到的BHC。

特点：3、相比于Dash、Monero和Zcash，黑洞币（BHC）确实是当前匿名交易的首选方案。我们也深深感觉到，黑洞币的匿名实施方案相比于其他加密货币还是有不少优势的，比如在扩展性、可审计性、匿名设置及使用性等。

特点：4、相比于Zcoin，在第一次减半前的四年时间里， Zcoin团队和其投资人会获得挖矿所得收益的20% ，总数是 210 万枚。BHC去除掉创始人奖励，期间每块产出的20%也还是归矿工所有。

特点：5、BHC钱包内置了区块浏览器，可以快速便捷的查询区块信息。

资金用途：早期获得50万美元投资，1000万币用于回报投资人。所得费用，将全部用于将来BHC的公关，上平台费用及BHC更改更先进算法所需资金，团队一分不取。

支持的理由：现在整个加密货币领域确实熙熙攘攘，但是其中仅仅是较少数是有实质性创新的，而不是仅仅简单的克隆其他加密货币。我们相信最终仅仅有原创新及持续开发的加密货币才能够生存下来，随着保守派竞争币的影响力持续衰退并转向支持更有创新的项目开发，我们已经在目睹这一切的发生。有了大家的支持，具有实质性创新的币才能更好的发展，加密货币行业才能更好的蓬勃发展，多元化发展，而不仅只是某几个加密货币主导大部分市场。

我们的承诺与回报：黑洞币的支持者，是出于对团队的信任。团队踏实做事，不会用以往的币圈潜规则（讲故事画大饼）圈钱跑路欺骗诸位投资者，爱好者。团队成功融资之后，将同时开启BHC社区，构建BHC自己的生态圈，在这个生态圈中，社区通过不定期沙龙活动，在里面所有的玩家都可以通过发表文章参与活动得到奖励。最后还是那句话，我们要做长做久，百年老店才是王道。长久稳定有发展的BHC才是对支持者最好的回报。

08.

大事记

以往出现的匿名币开创了虚拟币的新时代，可是我们开发匿名币的初衷是什么，爱好？投资？炒作？我们在虚拟币走过的道路上静心思考，最根本的目的就是流通。一个匿名币首先是它的技术创新性，还有最重要的原因，就是它的流通性。在开发前期，我们团队有个别团队成员利用它的稀缺性来进行炒作，可是我们最终放弃这个想法，个别成员及投资人因此也退出了团队，使进度大大滞后，可是我们不忘初心，最终坚持下来。宁可放弃眼前利益，也要做到完美。期间特别感谢2个中国及澳大利亚留学生资金的大力支持，由于他们要求必须保密，这里不做详细介绍。

09.

其他创新及路线图

算法保证安全性

BHC目前工作量证明机制采用莱特币scrypt算法，后续工作量证明机制算法改为团队于2013年原创的GKS算法，此算法为非对称加密算法（也叫公开密钥加密算法），可以抵御GPU，FPGA，ASIC矿机，防止51%攻击，保证加密数字货币流通算法更安全。

为什么使用scrypt算法

Zcoin使用lyra2z算法，其他zcoin分支Kurrent和hexxcoin则使用X11算法证明的工作。但另一方面，GPU和ASIC矿工有着更多的scrypt算力。和Litecoin一样，许多数字币使用scrypt算法，这样使得挖矿更容易。

为何选择黑洞币而不是ZCASH

Zcash可以隐藏转账金额，但BHC并没有这种功能。因此相对BHC，Zcash不容易遭到时序攻击（边信道攻击），但也因此Zcash有可能存在无法检测到的无限通胀币量发行问题。

零币协议有两大步骤：

第一步：“零币协议铸币”阶段，“Public coin”（公开币，没有隐私属性）进入一个叫做 accumulator（收集器）的数据结构中。Accumulator收集器回答关于候选者是否为成员的请求，而不揭示成员身份。

第二部为“零币协议花销”阶段，该阶段使用者可以实现零知识证明，显示某人在accumulator中拥有币而无需告知拥有哪个币。有了零知识证明的“零币协议花销”证明，就可以产生一个完全没有历史交易记录的新BHC。

为何选择黑洞币而不是ZCASH

因为每个BHC在通过“零币协议花销”实现匿名前，都需要执行“零币协议铸币”， 通过分析“零币协议铸币”与“零币协议花销”间的时序可以进行攻击。使用者有可能在“零币协议铸币”转账之后马上进行“零币协议花销”转账， 因此假设有这种行为，就会产生假定几率，即一个“零币协议铸币”与一个特定“零币协议花销”相关联。但是，只要在“零币协议铸币”和“零币协议花销”之间等稍微长时间，即可防止时序攻击。

因为ZCash隐藏了转账数量，相对于BHC，能够更有效防止时序攻击。但也因此带来一个更大的隐患：本质上，对于Zcash没有“稀缺性”一说，很少有人能够以数学/加密学位第一原则为基础对其进行证明。Zk-Snark使用极度复杂的加密学。只有一小撮加密学学术专家才能理解ZK-Snarks原理。零币协议背后的加密学原理存在时间较长，零币协议论文也是近年加密学学术引用的常客。并且大部分加密学学术专家能够理解零币协议原理。

Zcash的bug在于，有人可以无限制印钞，而且无人能知。利用这个bug，可以无限通胀货币供应量，并操纵市场。这种通过改变货币供应量而导致崩盘的例子不少。最典型案例是2010年比特币价值溢出（value overflow）bug，这个bug使比特币总量达到900亿。

2010年8月15日，比特币74638区块，一个184,467,440,737.09551616个比特币的转账设计三个地址。2个地址分别收到922亿比特币，并且找到这个块的人都多获取了之前不存在的0.01比特币。据技术人员分析，黑客是通过利用大整数溢出漏洞，绕过了系统的平衡检查，成功实现了这次攻击。

在Zcash中，这种bug悄无声息而无人察觉。如果Zcash有相似的bug，那么在无人得知的情况下，一个人就能拥有99.9%的Zcash市值。

最近的一例加密货币bug就是The DAO，惨遭黑客对价值5000万美元代币的攻击，在okTurtle博客中，Greg Slepak写到：然而这种情况比The DAO更严重，Zcash的代码比The DAO复杂程度搞出数个指数级别，其失败结果也是指数级别高的严重。Zcash的现状是：根本不可能知道攻击是否成功。除非破坏者自己发出警告，我们才可能知道Zcash被攻击，木已成舟。Zcash价值越高，危险性越高。根本没有回撤键。

除了非本意的bug外，还有另外一个问题。因为ZK-Snarks的高冷技术，对于Zerocash的底层加密学原理几无同行评审的可能。但BHC却没有这方面顾虑。能懂Zcash加密学理论的学术专家极少。如果在数百万美元诱惑下，即是最高尚的学术专家也可能跨越道德界限。相比之下，BHC即使有bug，也是在阳光之下，每个人都能知道总量没有发生变化。

另一方面，BHC的机制被破坏的几率变小的因素：每个人都能看到BHC的供应量。但相比之下，如果Zcash被攻破，超级通胀的发行量无人能察觉。

Zcash依靠的假设条件是，所有加密算法参数生成者都不会合谋作恶。只要有一个公正不作恶者，那么就安然无恙。否则，他们可以任意双花。

10.
合作伙伴

沈阳惠马体育文化发展有限公司已宣布接受黑洞币支付

沈阳惠马体育文化发展有限公司旗下5G篮球中心已建成两个高质量标准篮球训练馆，1400平方米，高十米，全实木双轮毂固定式结构，北美顶级枫木的面板，德国劳勃防滑油漆，它们是NBA在全球唯一两家油漆供应商之一，篮架的质量和结构可以满足CBA训练的要求，两百平方米的私人体能训练室，采用欧洲设计师的个性化并符合中国身体结构的健身设备，创始人编制了一套相对完整的篮球教材，可以有效的提高个人及整体的技术能力，和技战术水平。

中心设有餐饮，运动损伤后的康复中心。旅馆现有标间20间。

未来计划将4500平方米3层的建筑改造成多功能综合健身中心，聘请欧美专业设计师进行设计，一楼成为恒温，高质量的水循环系统游泳馆，二楼改造成为健身中心，三楼改造运动旅馆。另外还要建700平米的室内五人制足球场。

创始人李品在青少年时期从事了长达十年的专业篮球训练，1979年-1983年在沈阳市体校篮球队，后参军服役于沈阳军区16军男子篮球队。

1985年-2008年，自主创业创建沈阳惠马鞋厂，沈阳惠马鞋业有限公司，并创立沈阳惠马体育文化发展有限公司，2008年移民美国。在美国学习了先进的篮球理念及体育产业经营。

11.
其 他

项目定位

新型匿名币，安全、透明、确认速度快、钱包内置区块查询，显卡、CPU、矿机都可以挖矿，做到人人都可以参与。从而体现它的核心价值与应用。

项目进度

2017年5月7日登陆中国，正在国内推广阶段。矿工最开始进入挖矿。
目前团队在联系国内外有实力信誉的平台准备登陆。
拥有用户/会员数：会员达到1000人，都是真实玩家粉丝，币圈矿工蜂拥而入，算力峰值达到36G,超过小零的算力。

移动钱包

Black Hole Coin

BHC 基金会

www.blackholecoin.io