xBOUNTY

一个给予给匿名密保者的分散数据区块链（blockchain）

White Paper version 1.2 Dallas, TX 2017

摘要

xBounty 是一个匿名密保的服务平台，使您在完全匿名的前提下向政府提供正确的致命信息并在帮助破案下全面保护个人隐私和安全的条件下收取赏金。此平台基于 Zero Knowledge 的分散数据区块链服务上而运行，并尽最大可能地为非专业程序员的普通人群优化以达到最好的使用体验。

社会难题

在世界各地，尤其美国，由目击者，知情者或者犯罪同伙举报的犯罪行为的比例现如今达到了低谷。尽管大多数案件有许多重要的目击者，但往往因为各式各样的原因像是个人、在乎的人或者商业的安全威胁等而袖手旁观。

在许多未解决的犯罪案件中，警察部门、联邦调查局或其他调查平台往往依靠当地公民和社区的帮助来取得案件调查的线索和信息。在这样的情况下，众多鼓励群众来挺身而出并给予珍贵信息的方法油然而生。新闻频道和警员网站提供各式各样的报警热线并保证匿名，在更为严重的案件中，甚至会给予赏金奖励。在一件案例中，警察部门发布了一张询问一件儿童谋杀案线索的公告牌。除此之外，众多警所采取了更为直接的途径，例如亲自走访受害社区分发传单并征求当地人的信息。尽管展开了许多调查和工作，但许多罪行在没有充分证据的条件下仍然没有得到因有的解决。

这一社会难题的困难程度在得知其造成的损失后因该能更好地被理解，无法统计的人力和大规模的经济损失造成了数十亿美金付之东流。单单在美国，根据联邦调查局的 UCR 调查统计，2015 年的各种暴力罪行和财产犯罪的数量极速上升并造成了多达 143 亿美元的经济损失。更别提没有算进去并正在增多的网络犯罪、人口贩卖、商业诈骗、毒品贩卖、失踪人群、恐怖分子和公共腐败。

在全世界范围内，一个愿意帮助自己和他人并为执法提供高价值情报的社区平台可以在犯罪的道路上画上一个句号。一个社区可以在追捕罪犯和避免犯罪的方面发挥重大作用，特别是在一些已经公告赏金的特殊案件里，但只有公民们敢于发言才能创造一个良好的无犯罪环境。在六个国家中，百分之八十八的公民相信他们是打击罪犯、汇报罪行和的重要参与者并认为公民可以在警察部门调查中起到关键作用。一旦给予正确的平台，这一巨大的比例可以改变这个世界。

解决方法

xBouty 是一个帮助匿名告密者保留完全隐私的分散平台。它不仅给予了一个提供消息的平台，还可以保护那些匿名的告密者。

虽然警察部门招展了许多制止犯罪活动和恐怖分子赏金，对于罪犯的信息渴望的下降可以说是微乎其微。许多人尽管知道内情，但仍不愿意上前来收取案件赏金。大部分时间，因为对于政府的不信任和对于现金奖赏的不确定，前述的赏金会失去吸引力。根据犯罪的性质，一些警察部门和联邦调查局会经常提供赏金给予那些可以捉到头号罪犯或者可以突破案件的人。他们利用奖励这个噱头来榨取告密者关于罪犯的信息，但告密者往往最后都两手空空。而我们能做到的就是保证告密者的信息安全和真实的赏金数额。

在 xBounty 的平台上，警官、联邦特工、老师和社区成员可以基于分散数据区块链和智能合同设置一个赏金金额并提供赏金令牌（Bounty token）给那些匿名提供信息的告密者们。

我们的数据区块链 DAPP（数据采集和处理程序）是一个完全分散的系统，包含了创造一张智能合同所需要的一切工具，以及智能合同激活所需要的 xBounty 密码货币（cryptocurrency）令牌（token）。

智能合同的运算描述了一系列的条款，而 xBounty 的系统将自动为您填满。他们开启了法律的实施（FBI 联邦和警察）并提供了告密者一个互相同意的条款而无需担心对方违约的平台。我们的目的就是能让告密者可以为未能解决的案子提供宝贵的线索，并在成功破案的情况下收取赏金。

XBounty 是一个为了简化和托管告密者和奖励者之前的交易而所建立的平台。奖励者将在 xBounty DAPP（数据采集和处理程序）的平台上发布一个赏金，然后匿名者就可回复奖励者的帖子并获得小费奖励。一旦案件确定成功突破，小费奖励确定和同意智能合同之后将会被颁布给双方。XBounty 将会在数据区块链里的 XB 扫描中通过智能合同审判赏金。

智能合同的条款在交易建立前就已经设立。然后他们的履行职责将会在没有任何人工干涉的情况下被软件代码确定。如此，智能合同科技代表着一个低风险交易里理想的工具，保留着双方完全的隐私。交易都是在程序代码概括和执行下运行的，所以双方的合同只能根据先前发布的条款而满足或停止。

由于该区块链的技术细节，存储着智能合同的分散数据库代表着干扰任何已确定的条款几乎是不可能的。

xBounty 的智能合同好似“托管代理”或是银行仓库。在条款满足前都将为交易双方存储着合同和密码货币（cryptocurrency）

xBounty 的目的是破坏所有的犯罪集团，并计划成为匿名信息里的优步（Uber）

我们的解决方案确保所有告密者个人隐私的安全，并保证在任何案件需要外界帮助来进展的情况下，他们也会得到相应的奖励。

我们解决方案的优点

相对于传统搜寻线索的方法，xBounty 平台有一系列的优势。

1. 保证告密人的完全匿名化，而使告密者在发言宝贵线索时更有信心并最终帮助警方破案。我们还能确保告密者应得的赏金和补偿将会在交易成功结束时发配。在数据区块链（blockchain）中合同条款在签字前就已经成立并被安全地存储，所以我们可以保证在双方交易建立后如果要更改条款是不可能的，并且合同只能按照原来的安排予以关闭或更改。

2. 所有在 xBounty 上的交易都是建立在令牌上的，所以消除了所有支付障碍。您无需担心付款麻烦或者害怕发生没必要的疏忽，因为在没有第三方类似银行等部门的情况下，任何因为外部因素而发生的支付取消都不会发生。

3. 使用密码货币（cryptocurrency）的另一个优势是签合同和支付是不可分离的。发布一个协议代表着您必须得同时发布一个对方也同意的金额。此后所有的金额移动只能根据合同条款来进行。

xBounty 比较类似平台的优势

目前，xBounty 是唯一一个提供相似服务并基于数据区块链（blockchain）的完整平台。

您同时也可以利用 xBountry 数据区块链（blockchain）人工建造一个智能合同，但这需要一定的编程技巧或是一比雇佣编程师的额外费用。

还有一些其他服务可以让不是编程师的普通人群在一个简化了的界面上建造智能合同，但提供这些服务的不能被认为是一个完整的平台，因为他们无法保证用户的安全。

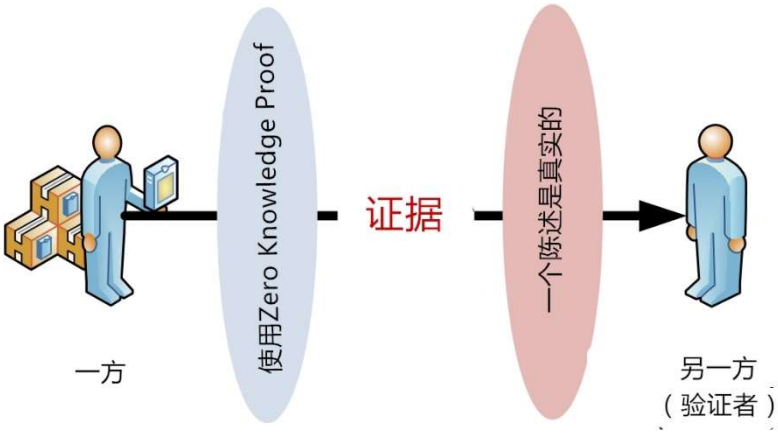
结构：

XBounty 利用 Zero Knowledge Proof 的三种折中结构

1. 匿名密报人（举报人、证人、受害人、用户）
2. xBounty 将成为匿名密报者的中介平台并保证匿名的完全性。
3. 奖励者（联邦 FBI、保险诈骗调查单位、老师等等）

Zero Knowledge Proof（保证零知识）是什么？

 这是一种在一方（证明者）给另一方（验证者）证明次陈述是真实的，同时除了给予关于真实性的信息无需透露其他信息的方法。



Zero Knowledge Proof（保证零知识）

在满足一定的条件下，但无需向验证者或其他人透露证人自身的信息的同时，一个包含具有秘密信息的人又称证人可以在验证者对于案件的抉择上起到关键性的作用。

zk-SNARK 是 Zero Knowledge Proof 旗下的一个简单程序

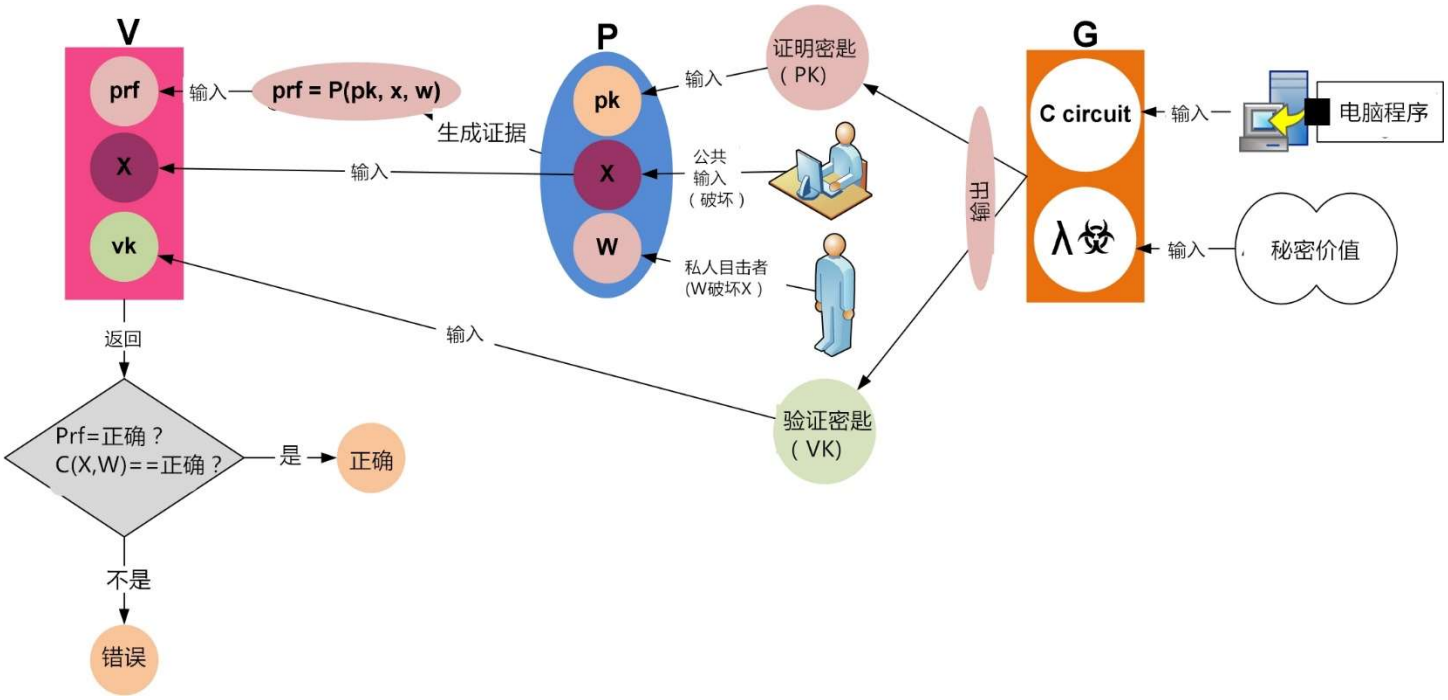
它包含了三个独特的运算方法 G, P, V

- 密匙生成器 G 使用一个秘密参数(Lambda)和程序 C 来生成两个公共密匙，一个证明密匙 PK（Proving key PK）和一个验证密匙 VK（verification key vk）
- 证明者 P 需要输入验证密钥 PK（Proving key PK)，公共投入 X 和一个目击者 W 来生成一个证明

  PRF = P（PK，X，W）。
- 验证者 V 计算 V（vk, x, prf）如果证明是正确的，将恢复真实性，否则为假。因此如果证明者知道目击者 W 满足了 C(x,w) == true 那么这个公式将验证正确。

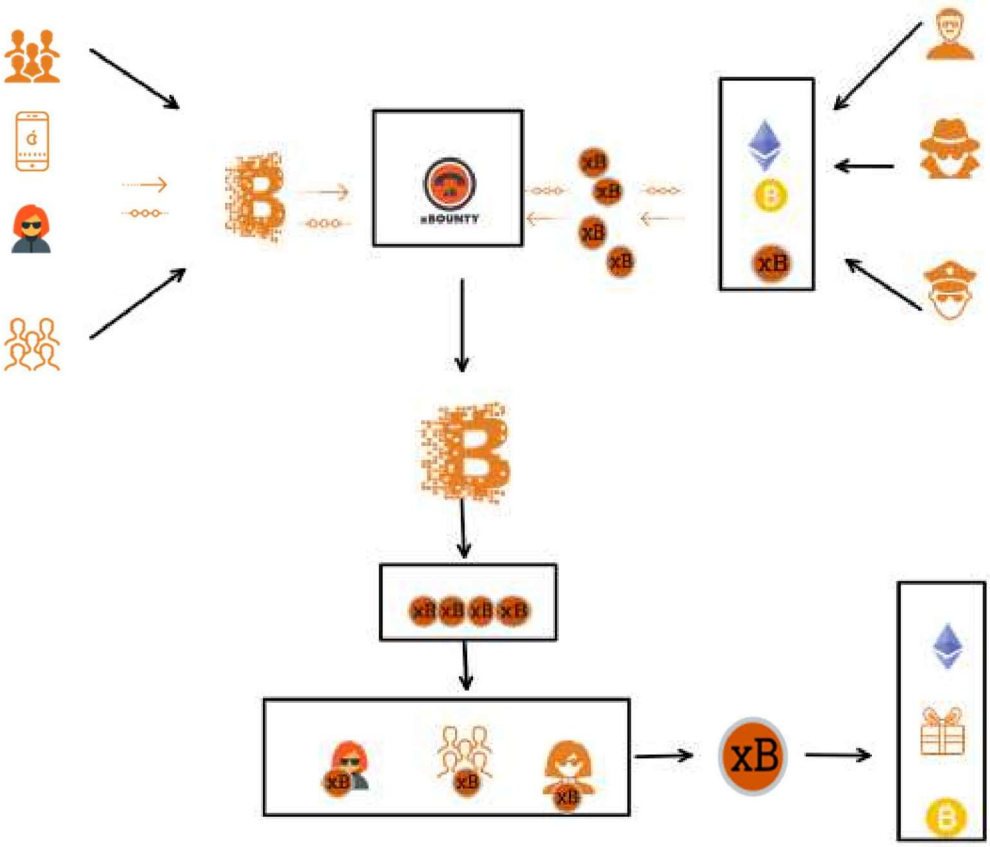
风险

如果有任何人知道秘密参数 Lambda 可能生成伪造证明。具体来讲，就是被给予任何程序 C 和公共投入 X 并知道 Lambda 的人便可能生成伪造证明_prf 类似 V (vk, x, fake_prf)在不知道秘密 W 任何信息的情况下判定为真。因此，实际运行生成器需要一个非常仔细和小心的过程，以确保在何时何地没有任何人知道并保存参数。



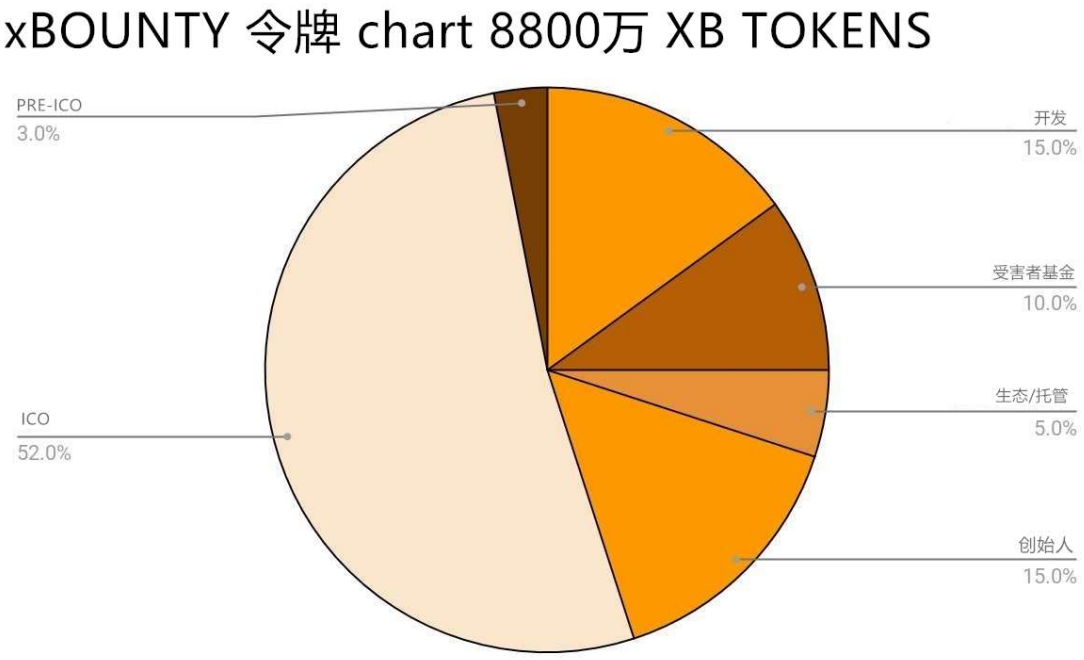
Generator (C circuit, λ is ☣): (pk, vk) = G(λ, C) Prover (x pub inp, w sec inp): π = P(pk, x, w) Verifier: V(vk, x, π) == (∃ w s.t. C(x,w))

简化版表格



基本来讲， XBounty 是一个为了简化和托管告密者和奖励者之前的交易而所建立的平台。奖励者将在 xBounty DAPP（数据采集和处理程序）的平台上发布一个赏金，然后匿名者就可回复奖励者的帖子并获得小费奖励。一旦案件确定成功突破，小费奖励确定和同意智能合同之后将会被颁布给双方。XBounty 将会在数据区块链里的 XB 扫描中通过智能合同透明化的审判赏金。

令牌（Token）分配：



88,000,000 XB TOKENS(令牌)

募捐活动	52%	45,760,000
发展/基础	15%	13,200,000
顾问/创始团队	15%	13,200,000
受害者基金会	10%	8,800,000
杂项费用/托管	5%	4,400,000
早期采用者	3%	2,640,000
合计	100%	88,000,000

“种子前”（Pre-Seed）投资者

总共代售 XB Token	2,640,000
折扣	40%
XB Token Per ETH	1400
合计 Eth 增加	1,886

分配	Tokens （令牌）	折扣	XB Token (XB 令牌)	ETH Raise
25%	11,400,000	20%	1200	9,533
25%	11,400,000	10%	1100	10,400
25%	11,400,000	5%	1050	10,895
25%	11,400,000	0%	1000	11,440
100%	45,760,000		ETH Raise ICO	42,269

令牌（tokens）分配的目的就是发展我们自己的汇率（XB）并将 XB 令牌（tokens）奖励给那些匿名的告密者或解决问题者。XB 令牌可以被兑换成奖品或者密码货币（cryptocurrency）。XB 令牌（tokens）可以用 Ethereum 或是 Bitcoin（比特币）购买。XBounty 将会在所有 XB 奖励中消减百分之三去保持平台的平衡性并支付系统营销和运行。如果问题没有被解决，XB 令牌（Tokens）将会归还给奖励者。

- 百分之五十二的 ICO 计划在 2018 年的新年开始
- 将会宣布百分之三的“种子前”（Pre-Seed）
- 百分之十五将会分布给早期采用者，创始团队和投资人
- 百分之二十的令牌会托管给犯运营和犯罪营销上。
- 百分之十将会存着来帮助各种罪行的受害者

我们令牌（tokens）的最低销售目标是 25,000,000 个和筹集 15,000 Ether。

未来计划：

从一个从简单的匿名打赏服务和帮助全世界打造一个无犯罪环境开始，我们打算把 xBounty 打造成一个成熟并具有安全意识的平台，并帮助解决各类困扰了侦查部门多年仍无法解决的案子。

这个平台进一步的发展将会包括下列步骤：

Hellenistic White Paper, Pre-ICO, ICO

Matrioshka

第一步	开发，全力研发 DAPP（数据采集和处理程序）	Q1 2018
第二步	被众多美国安全部门类似联邦 FBI、警局、美国小学、社区大学和大学等所采用	Q2 2018
第三步	跟国际刑事法院合作	Q3 2018
第四步	成为一个跟全球安全部门合作的世界化平台	Q4 2018

Topopolis

第五步	预计通过与世界反犯罪企业建立合作关系在全世界范围内打击犯罪活动，并使人性得到控制。	Q5 2019 或未来

Elysium

团队：

Chuck Yang - CEO, 创始者

Opinder Preet – 首席 Blockchain 开发者, BlockLabs Inc, New Dehli

Jittendra Chittoda - Blockchain 开发者

Pushkar- 政府 Blockchain 开发者

Manvita Vempati-大数据分析者,稳固者

顾问 - James Wealthy, Tech Investor

顾问- Jeff Hoffman, Founder of Priceline

未来全职职位包括：

- 首席运营官（其中包括合规和法律）
- 首席运营官
- 首席技术官 (负责平台安全)
- 业务发展和战略合作伙伴
- 营销支持
- 开发者
- 客户服务中心
- 首席财务官
- 外部营销和公关
- 法律顾问
- 公司秘书

参考

[1] Blum, Manuel; Feldman, Paul; Micali, Silvio (1988). "Non-Interactive Zero-Knowledge and Its Applications". Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988): 103–112. doi:10.1145/62212.62222.

[2] Wu, Huixin; Wang, Feng (2014). "A Survey of Noninteractive Zero Knowledge Proof System and Its Applications". The Scientific World Journal. 2014: 1–7. PMC 4032740 Freely accessible. PMID 24883407. doi:10.1155/2014/560484

[3] Manuel Blum, Paul Feldman, and Silvio Micali. Non-Interactive Zero-Knowledge and Its Applications. Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988). 103–112. 1988

[4] Oded Goldreich and Yair Oren. Definitions and Properties of Zero-Knowledge Proof Systems. Journal of Cryptology. Vol 7(1). 1–32. 1994 (PS)

[5] Shafi Goldwasser and Yael Kalai. On the (In)security of the Fiat–Shamir Paradigm. Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS'03). 2003