

全息区块链原创作品，作者思想钢印。

全息区块链：我们将通过故事形式和由浅入深的介绍，记录区块链，共同探讨区块链、密码学和金融市场间部分是整体的缩影规律的全息关系，犹如区块链全息光栅，为你呈现区块链世界的全息图。



V神一直是大众视线里的以太坊创始人，以至于很少有人知道，以太坊得以问世的概念的最初提出者和真正主要参与编写以太坊的，另有其人。

以太坊教父其人：Yanislav Georgiev Malahov

Yanislav出生于保加利亚，是一个德裔计算机科学家。是2017年发售的大名鼎鼎的德国项目Aeternity的创始人。

可能写到这里，有人会好奇，那么Yanislav与以太坊有什么联系么？这个问题笔者很难回答，所以笔者试着用Yanislav本人的一些话和经历，试着解释一下Yanislav与以太坊的联系。

秋雨霏霏中的相识

这个很长的故事要从2013年的秋天说起，当时Yanislav作为首席开发人员与Vitalik共同参与了一个名为Keidom（后改成Ascribe.io）项目，该项目的构思是通过开发一个彩色币网络钱包，ascribe是一项使用区块链保护数字创作的开源解决方案，创作者可以直接向消费者展示他们的宝贵项目。Ascribe基于比特币区块链网络，独创proof-of-existence存在性证明共识算法，使得艺术以安全和不可篡改的方式进行溯源、传输和分享。在2013年9月至11月之间，这个开发小组就开发完成了ascribe的工作原型。

在Yanislav第一次去柏林参加了柏林比特币夏季聚会，就与Vitalik和Mihai Alisie（以太坊联合创始人，比特币杂志创始人。）一起前往巴塞罗那，当时著名的Calafou营地进行了无政府主义的交流。

Calafou营地也是当时赫赫有名的无政府主义黑客修道院，营地位于西班牙巴萨罗那外部，根据Jamie Barlett的《黑暗的网络》(The Dark Night)建造，一个西班牙黑客集体成立了一个比特币黑客实验室。

这个叫做Calafou是一个旧纺织工厂改造的集体生活试验地，常被住在附近的30多个居民称作是“后资本主义生态工业殖民地”。这里一个对于每月100欧元左右的价格就能住在资本主义制度以外的无政府主义者和社会活动者来说的天堂这个合作社被居住在此的黑客们称作“Hackafou”。他们在此营地花大量时间探索赚取比特币的各种方法。在这里，加密货币爱好者们信仰无政府主义，认为密码学驱动的加密技术最终会成为改变世界和政治的手段。

笔者曾见过一个报道，报道中，当时对加密世界充满好奇和野心的Vitalik就住在一间没有窗户的房子的地铺，和来自世界各地的包括Yanislav在内的密码学爱好者互通有无，这些珍贵的经历都帮助他日后成就了以太坊。在这里，Yanislav和Vitalik分别找到了很多灵感，来帮助他们后来研究和推进各自的项目。

其中，UnSystem组织就是位于Calafou，Vitalik后来与UnSystem组织合作，研究了关于黑暗钱包的内容。Calafou之行结束后，Yanislav在米兰再次见到Vitalik。



2014年1月在迈阿密举行的首届以太坊聚会，Yanislav在后排左起第二，Gavin Wood在

在网上笔者翻到了一些Yanislav和Vitalik的聊天记录（笔者主要整理了后半部分的聊天记录），前半部分的聊天记录里Yanislav提出了mastercoin2.0的提案，假使任何用户都可以基于这个协议发布Mastercoin。在后半部分聊天记录Yanislav又同时提出了一个概念：如果Mastercoin可以在比特币主网中编码，同时算法的变化嵌入到区块链里，这是一个全新的概念！这个概念就是后来的可编程语言，要在这个概念让Vitalik也认为很酷。Yanislav也马上联想到可以在当时的山寨币之王——sunny king的质数币primecoin（XPM）上实现这一个想法，虽然最终Vitalik还是决定做一条新的公链，也就是后来的以太坊。但是熟悉以太坊历史的人应该知道，最早以太坊是打算在primecoin上实现的，这一点与之后的新闻都不谋而合，也侧面证明了，我们不能忽视Yanislav对Vitalik创造以太坊的启发。

同时Yanislav还提出了“特洛伊木马”的概念，这个概念就是后来以太坊上创建合约的方式在以太坊上部署一个合约，需要发一笔创始交易，这个交易被打包之后，这个合约就上线了。任何之后链上的执行都是根据这个交易中的代码去决定，这笔

交易就是“特洛伊木马”。

以下为部分聊天记录

[17.11.13 00:04:19] Yanislav : 嘿

[17.11.13 00:04:24] Vitalik : 嘿

[17.11.13 00:05:04]

Yanislav : 我找到了一个很好的程序来导入'一个区块 ' 到mongodb的办法 ... <https://github.com/thelinuxkid/bitcoinquery>。(bitcoinquery可以将比特币区块链存储在MongoDB数据库中以允许查询块和交易数据)

[17.11.13 00:05:13] Yanislav : 也应该可以应用到primecoin和其他的项目

[17.11.13 01:05:01]

Yanislav : 如果msc可以在比特币区块链中编码自己.....那会很酷!!

[17.11.13 01:05:27] Yanislav : 我的意思是 : 如果算法更改也嵌入到区块链中.....

[17.11.13 01:05:33] Vitalik : 好的 , 那将会很酷

[17.11.13 01 : 05:42] Vitalik : 虽然我宁愿利用山寨币

[17.11.13 01:05:43] Yanislav : 我们可以用xpm区块链主网来做吗 ?

[17.11.13 01:05:45]Vitalik : xpm也许 (可以)

[17.11.13 01:05:53] Yanislav : (y)

[17.11.13 01:06:02] Yanislav : 让我们共同努力

[17.11.13 01:06:25]

Vitalik : 所以 , 在xpm上的mastercoin更新了超级先进的功能和源代码在链上。

[17.11.13 01:06 : 34]Vitalik : 另外 , POS投票的源代码也更新在了链上

[17.11.13 01:06:43] Vitalik : 好的, 我们可能在这里拥有第一个真正的DAC。(DAC, 全称是Distributed Autonomous Corporation, 中文可以翻译为分布式自治系统。所谓DAC, 就是通过一系列公开公正的规则, 可以在无人干预和管理的情况下自主运行的组织系统。这些规则往往会以开源软件的形式出现, 每个人可以通过购买股份或者提供服务的形式获得股份成为系统的股东。系统的股东将可以分享机构的收益, 参与系统成长, 并且参与系统的运营)

[17.11.13 01:06:46] Vitalik : 好吧, 好吧, 是第二个真正的DAC

[17.11.13 01:06:50] Vitalik : 第一个是比特币

[17.11.13 01:07:35]

Yanislav : Mihai (指的是2011年与Vitalik一起创办比特币杂志的Mihai Alisie) 也说了同样的话, 我为thenewsbits打造的小微众筹平台
..是第二个真正的dac

[17.11.13 01:07:43] vbuterins : 呵呵

[17.11.13 01:07:50] Vitalik : 感觉你在和自己竞争

[17.11.13 01:07:52] Yanislav : POS看起来很有前途

[17.11.13 01:09:31] Yanislav : 是的.....这很像一个新的民主算法系统的基础。

[17.11.13 01 : 09:35] Yanislav : 民主算法

[17.11.13 01:10:46] Yanislav : 如果'算法'也被嵌入 (写入) 到区块链中那么未来将发生变化。Msc (mastercoin 质数币) 的问题在于它的算法还在集中服务器里。

(暗示Mastercoin没开源)

[17.11.13 01:11:04] Vitalik : 嗯, 不, 质数币的算法是开源的

[17.11.13 01:11:08]] Vitalik : 每个人都在跑它

[17.11.13 01:11:20] Vitalik : 但是嗯, 区块链上的算法

[17.11.13 01:12:57] Yanislav : 我们如何将算法嵌入到块链中 ?

[17.11.13 01:13:09] Vitalik : 首先选择一种编程语言

[17.11.13 01:13:18] Vitalik : 理想情况下它应该很简单, 但功能强大

[17.11.13 01:13:23] Vitalik : 也简洁

[17.11.13 01:13:53] Vitalik : 但它可能会成为一个很大的问题

[17.11.13 01:14:00] Vitalik : 如果有人发布无限循环代码怎么办

[17.11.13 01:17:12]

Yanislav : ..

...或者是特洛伊木马。但这(还)不是它的工作方式。还需要一个生成一个创世tx (TXID : 区块链上的交易编码), 所有算法从该(创世区块)生成开始, 开始产生有差异化的币。

[17.11.13 01:17:49]

Yanislav : 如果意外地发布了无限循环, 那么这个需要与另一个tx (TXID : 区块链上的交易编号) 来反转这个循环。

[17.11.13 01:18:30] Vitalik : 相反, 另一个tx将根据新规则进行解释, 新的规则将不接受任何改变所以会一直循环。

[17.11.13 01 : 18:42] Vitalik : 所以它会卡住

[17.11.13 01:19:06] Vitalik : 否则, 你必须有某种无法改变的核心“规则”

[17.11.13 01:19:13] Vitalik : 或者(规定)可能需要10kb大小的区块才能改变

[17.11.13 01:23:14] Yanislav : 当算法更新的时候, 旧的算法被停止, 新的更新版本的算法将被执行。事实上, 这不能在区块链上编码, 但这是我唯一的想法

[17.11.13 01:23:30] vbuterins : 实际上, 这也必须是可编辑的

[17.11.13 01:23:38] Yanislav : 这个元算法启动的停止和执行。

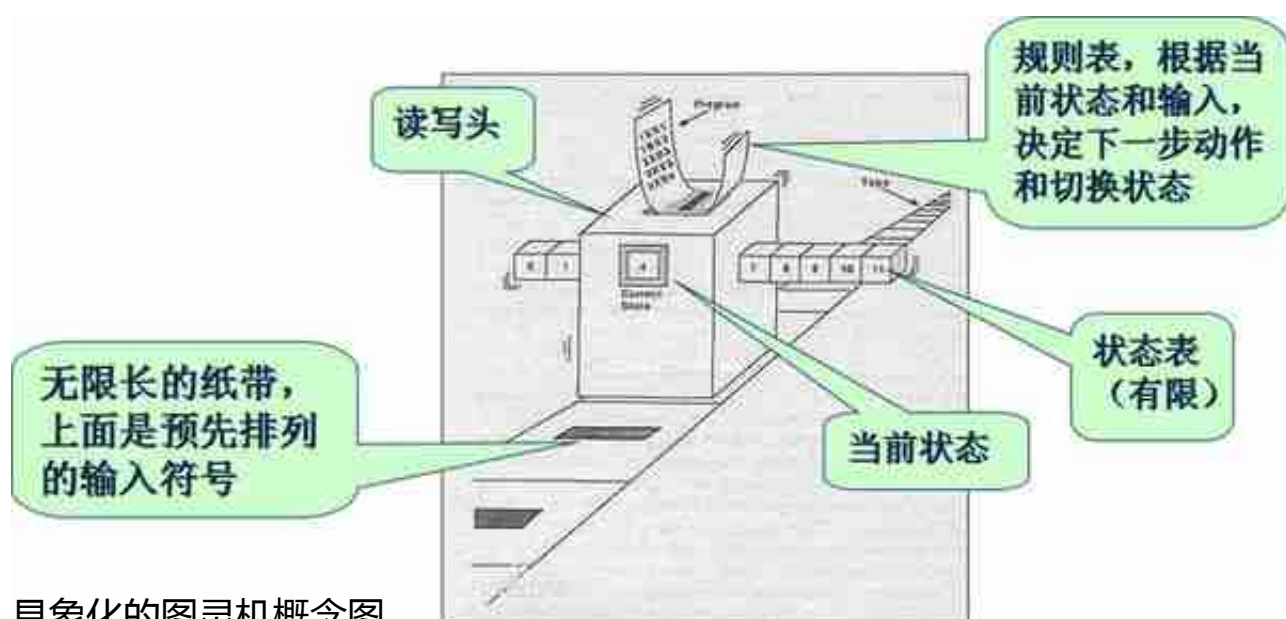
分布式计算的圣杯

当时Yanislav提出希望在Sunny King的Primecoin 之上构建像以太坊的东西, 类似

合约，因为Primecoin是当时最先进和最具创新性的加密货币。特别是它在工作证明的创新意义重大。于是，在2013年夏天，Yanislav就用Primecoin的工作证明启发了“分散计算的圣杯”。即，找到难以解决的计算问题并且同时具有易于证明的有意义的解决方案，以便可以创建基于区块链的加密货币并奖励用于解决问题的数字货币。但是Yanislav却从来没有深入实践和发展过这个想法。从他启发了Vitalik后，他持续观察了Vitalik的以太坊项目的开发一段时间，也参加了2014年1月在北美比特币会议上迈阿密首次聚会，但最终决定不因为个人原因而更深入地参与其中。后来Yanislav花了很长时间在旧金山和柏林，Ethereums的 CTO，Gavin Wood（本文第二个男神），一起讨论开发了一个解决区块链技术可扩展性的问题的想法，为后来Gavin Wood撰写以《以太坊白皮书》给了非常多的头脑风暴。（后文涉及），可以说，虽然Yanislav从来没有真正参与到以太坊的开发小组中，也从未得到过任何形式的补偿，但是不能忽视他为以太坊的诞生所做的。

Yanislav在加密货币领域的故事当然没有就此结束，后来他启动了一个全新的区块链项目——Aeternity。如果说以太坊的图灵完备性，能通过区块链技术改进了比特币无法实现链处理的遗憾，那么Aeternity的Oracle机则比图灵机更强大，从本质上说它是图灵机加上黑盒——任一在AE网络注册用户可以设定“是非题”以及问题是现在还是在未来任意时间被回答。根据不同的时长用户需要提交不同数量的AE币作为保证金。时间截止后，如果没有反诉，那么保证金会返还给用户。如果存在反诉，那么最终结果由机器裁决。

Aeternity这一条主网因为一直没上线备受质疑，加上前CTO本人下场撕逼的风波，不得不感叹欧美人的较真和原则性，纵观娱乐圈到科技圈，所以的撕逼交锋，都是本人亲自下场。



具象化的图灵机概念图

以太坊的隐形大脑Gavin Wood博士

每一个行业都有等级阶梯，程序员当然也如此也是。曾经有一个网友做了一个有意思的图表，把程序员做了分层。

我们只要学PHP的



【全息小百科：笔者想在这里形象的解释一下不同的计算机语言之间的关系。计算机可以简单的分为高级语言和低级语言。越低级的语言越难，越靠近机器。低级语言能写高级语言，本地化的语言都是低级语言，常见的有Golang、Pascal语言等；高级语言又称脚本语言，脚本语言有泛型和特定型，泛型有例如我们熟悉的有C语言、python、Java、Php和NodeJS这类什么都能做的高级语言；特定的高级语言

有例如Solidity这种的合约语言，只能在以太坊虚拟机中运行的。

如果要用音乐里的环节来形象比喻来解释他们之间的关系，低级语言如Golang、Pascal和高级语言C语言发明了音乐，泛型的高级语言担任了在有了音乐以后编曲的角色，而solidity这类特定的脚本语言是弹特定曲的角色。

虽然C语言是一门高级语言，但是它和Pascal语言和Go语言一样，都是同级别的神级语言，它们是好比创世纪的传奇存在：C语言、go语言和Pascal都能写除汇编语言以外的所有有语言的开发平台和编译器。苹果的最早操作系统就是用Pascal语言写的，但是由于Pascal语法太晦涩用的人越来越少了，随着高级语言的逐渐普及，用C语言的人也开始少了。C语言、Pascal语言和Go他们三个可以相互写对方的开发平台和编译器，也可以自己创造自己、自己进化迭代自己，而其他语言则不可以创造它们】

Gavin Wood和以太坊的故事，也是从2013年的一场面基开始。

在2013年之前，Gavin Wood就已经关注到了比特币。最初比特币并没有引起他的注意，作为一个技术实干家，当时的他认为比特币没有实际应用场景和技术上的突破。直到后来他渐渐意识到比特币的技术可以用在一些现实场景中。所以2013年开始他又重新开始研究起了比特币主网和其衍生物。

也就在那年的年初，天才青年Gavin Wood正躺在床上百无聊赖的看报纸，翻到了一篇文章，有一个在柏林有酒吧的人在报纸上谈及了无政府主义的事情，原来已经开始有人尝试用比特币来替代为传统商业交易中的支付方式。作为外国人视角的Gavin Wood开始意识到了比特币的支付场景的重要性，也看到了比特币所能带来改变未来的深远意义。而此时还有一个地方的人们的想法和这些德国人的想法不谋而合——通过使用洋葱路由技术的暗网中的其中一个臭名昭著的毒品交易网站“丝绸之路”上的非法交易者们逐渐开始用比特币来完成交易，而截至目前，暗网上的交易几乎都用比特币和后来的门罗币完成。

这个有意思的人引起了Gavin的极大兴趣，他跑去伦敦和他进行了网友面基，然后引发了一连串的多米诺骨牌效应。Gavin Wood开始认识更多加密货币领域的人，于2013年的11月，33岁的Gavin认识了当时19岁的Vitalik。两人一拍即合，从那时候开始，这两个男人都开始了以以太坊为事业、被以太坊主宰的生活。笔者认为这次网友面基，是加密货币中的一个世纪面基之一。

当时的Vitalik受到了Yanislav的启发，已经撰写了名为《下一代智能合约和分布式应

也开始思考以太坊将会是一个比比特币更深层次的、将会对整个社会产生影响的区块链技术。于是，从2013年12月份开始，Gavin开始亲自操刀，着手编写以太坊圣经——《以太坊黄皮书》。

一切都进展的很顺利，与2014年4月下旬，Gavin所编写的名为《以太坊：一种安全的、分散的、通用的记账》的以太坊黄皮书就问世了。这位精力充沛的博士竟然只用了不到5个月就完成了一部以太坊技术圣经，小编真想问一下他，有没有治疗拖延症的秘方？

黄皮书让Vitalik对于以太坊的想法得到了全面的技术支持，付诸实践。与此同时，Yanislav还创造了Solidity合约语言，这让在以太坊上部署智能合约的想法得以实现。很多时候，伟大的创造和发明都是相继出现的，伴随着solidity问世的还有以太坊虚拟机（EVM：Ethereum Virtual Machine）。在以太坊黄皮书里，Gavin定义EVM虚拟机为可以执行任意算法复杂度的代码。开发者可以使用语法上类似JavaScript和Python的编程语言（Solidity）创建运行于EVM上的应用程序。以太坊的虚拟机使得以太坊变成第一条可编程的具有图灵完备性的区块链。以太坊黄皮书也是第一本正式的区块链协议的规范手册，可以说，后面很多项目在白皮书撰写之前，都需要先拜读Gavin Wood的大作。



CoinMarketCap上所记录的以太坊2016年12月份价格走势

看来不管是大投资者还是小投资者，在和自己投资的项目有交集的那一天起，自己和项目，项目和自己之间的命运就紧紧绑在了一起。加密货币世界有许多令人称奇的历史，和我们一直看好所以不舍得离去的未来，古人云“既来之，则安之”。这句话是很有道理的，命运把每个投资者带到加密货币这个世界，是有他的深意的。不能因为某一次事件将你我打击，就狂躁不安，甚至放弃。在加密货币的二级市场

成长是一条很长的路，我们现阶段的每个爱好者、投资人都是后来者的前辈，每个人不管走的好与不好，你都要走下去，面朝前方的走下去，心态积极的走下去。
