



解放货币

阿维斯塔 (AVESTA)

可规模化、快捷、安全和隐秘

阿维斯塔 (AV) 阿维斯塔 是现实生活中执行加密货币的关键，创建丢失的章节，在加密货币领域设定新的标准，并让个人和企业容易使用和管理其资金。

目录

执行摘要	4
目前加密货币的问题	5
1. 不够人性化	5
2. 入门要求高	6
3. 保密性和可用性	6
4. 速度慢和安全性差	7
区块速度	7
确认	7
双重支付	7
挖矿	7
51%攻击	7
5. 加密货币的合法性	8
阿维斯塔如何解决此问题？	9
人性化设计：阿维斯塔对于所有人	9
阿维斯塔对于开发者	9
容易入门和使用	10
隐私和可用性	11
快捷安全	11
区块速度	11
确认	11
双重支付	12
挖矿	12
51%攻击	12
合法性	12
对比	13
总结	15



解放货币

市场机会	16
参考资料	17

阿维斯塔 加密货币新标准



阿维斯塔是现实生活中执行加密货币的关键，创建丢失的章节，在加密货币领域设定新的标准，并让个人和企业容易使用和管理其资金。



执行摘要

Bitcause 是一家加密货币挖矿、咨询和交易企业，在加密货币领域拥有丰富的经验。

我们的使命是让加密货币容易使用并且每个人都能使用，给予用户系统的体验。

我们是全球不断增长的社区的一部分，得到加密货币爱好者、开发者和投资者的支持。我们希望发动一次革命使加密货币被大规模使用，并创造环境让我们能在销售点使用加密货币。

过去 3 年，我们从加密货币社区收集了一系列难点。因此，我们决定成立阿维斯塔项目，这是解决今天加密数字领域问题的方法。

本文中我们将阐释今天加密货币面临的问题，以及阿维斯塔是如何解决这些问题的。将来我们还会发布一份独立的技术文件，进一步阐述技术原理。

目前加密货币的问题

今天的消费者和矿工正面临着许多加密货币的问题。我们认为主要有三大挑战需要解决，才能为加密货币大规模使用铺平道路：

1. 不够人性化

加密货币社区稳步发展，然而实际上这个社区仍处于扩展的早期阶段。知名媒体纷纷开始报道比特币和其他加密货币的扩展情况。

世界对加密货币的好奇心日益增强。人们对数字货币的迷人世界越来越感兴趣。唯有开发出一个方便连接和集成的区块链平台，允许零售商在实体店和网上使用加密货币进行支付，才可能实现大规模使用。

当前加密货币的付款流程通常需要一定程度的技术能力，以及对安全性的了解和系统的信任，这与用户以往所使用的任何方式都不同。我们认为，正因为这些不方便的体验，即使是充满好奇心和符合资格的人依然不愿意踏入加密货币市场。

2. 入门要求高

对于区块链技术和加密货币未来如何不同于他们的竞争对手，IT 企业和大公司还没有一个明确的想法。

对于普通用户来说，他们无法在所有的钱包、代币和交易所的复杂世界中寻找出路，更别说加入 ICO 甚至是开始挖矿。

首要因素是害怕使用一项没有法规的技术，而这种技术可能会使他们的企业和声誉陷入困境。

其次是很难录用、培养和留住有经验的区块链工程师。这是一个新领域，所以有资格的工程师供应不足，而机会却很多。

3. 机密性和可用性

客户不喜欢被跟踪自己的买卖或转账细节。大多数加密货币和区块链在本质上都是对外开放的。

目前，由于大多数的匿名加密货币使用了很长的哈希值或用户需要一个独立的安全帐户保持匿名，匿名性和可用性无法共同实现。

另一个问题是我们很自然地会忘记。例如，丢失账户证书、密钥等。目前还没有办法恢复丢失的账户，而那些丢失的货币依然保留在生态系统中无法使用。

此外，加密货币的挖矿和保存应当简洁易懂，让用户使用不同的钱包，或者需要交易所的账户来储存硬币。

4. 速度慢和安全性差

区块速度

区块链技术是建立在区块上的，这些所谓的区块就是交易确认。越多区块包含您的交易，交易的安全性就越高。

这就是为什么区块速度如此重要。例如，比特币的平均区块时间是 10 分钟或 600 秒。这意味着，您至少要等 10 分钟来进行一次确认，甚至是等半小时进行 3 次更安全的确认。

确认

想要进行安全的交易，您需要在区块中确认您的交易，目前使用加密货币进行快捷支付需要很长时间

双重支付

在区块链技术中，如果交易未得到确认，很可能已经发生双重支付。结果是同样的硬币将被网络确认，而大多数区块中出现的那一个将变为现实。通常是指交易费最高的那一个。

挖矿

矿工在确保区块链安全中发挥着重要作用，通过求解一个数学方程来求解和确认一个区块来实现。矿工们所做的工作是以硬件和用电成本的方式来完成的。这确保了分散系统，也使得进行 51%攻击更难和代价更高。

51% 攻击

这是当前工作量证明加密货币面临的风险。这表示一个单一的实体或一方能够控制超过区块 51%的全球方案速率。理论上说，51%攻击是有可能更改交易和区块链的。这是一个巨大的风险，尤其是对于大型企业开始挖矿时，或者大部分矿工开始使用相同的矿池，其所有者可以滥用其对特定加密货币的权力。

5. 加密货币的合法性

目前，由于每个国家的法律都不一样，合法性是一个难题。加密货币的用户心里也没底，因为政府会修改加密货币的法律法规。



阿维斯塔如何解决此问题？

阿维斯塔是一个系统化的加密货币和平台，解决用户和矿工遇到的种种难题。最后，加密货币使用简便，注册快捷。

查看下面阿维斯塔开发团队制定的解决方案的概述。

人性化设计

阿维斯塔对于所有人

阿维斯塔使用账号而不是标记化的地址。通过输入类似电话号码或银行帐号这样的账号，人们可以轻松地进行交易，并在地址簿记录最喜欢的账号。这也让用户能够使用阿维斯塔即时通信（IM）软件和 IP 语音（VOIP）软件。

阿维斯塔对于开发者

阿维斯塔提供了一个框架在区块链上建立分散型应用程序（DAPP）。

阿维斯塔具有全面的 API 支持给开发者和用户使用阿维斯塔钱包或网络平台的区块链功能。

阿维斯塔消除了用户和开发者在区块链上创建和使用应用程序的局限性。这将为全球工业带来崭新的创意和方案。示例：微支付、应用程序内或移动设备上购买、订阅模式、市场、电子商务和销售点的方案。



解放货币

容易入门和使用

阿维斯塔将是一个这样的加密货币：开发者能够确保用户在访问、使用和保存货币时拥有同样简单的体验。它使用相同的方式登录桌面版钱包、手机钱包和网络钱包。

这将解决了复杂加密货币的问题，允许访问其他加密货币和法定货币进行存储和使用。

智能合约

阿维斯塔之所以能够成为让您获得完美的加密货币体验的平台最重要的一个因素是智能合约用户界面。将提供涉及销售、发票、代币等功能的一系列智能合约模板。操作简单，只需点击几下鼠标即可。

隐私和可用性

隐私和可用性是网络关注的一个问题，尤其是对于加密货币。因此，阿维斯塔采用了最好的和最实用的方法来确保用户使用最佳匿名工具进行交易。用户可以进行无迹可寻的匿名交易，而无需忍受复杂的交易系统。

人们往往会丢失密码或密钥。正因为如此，阿维斯塔提供了一个继承功能。在实际生活中，丢失的账户被转交给账户持有人的“继承人”。该继承人可以是孩子，亲戚或朋友。如果账户持有人没有设定“继承人”，账户将被阿维斯塔重新开立，而账户上的硬币将返还给矿工进行重新分配。

这都是通过在区块链集成强大的智能合约来完成的，让每位用户得到失控保护。

快捷安全

区块速度

为了获得快速的确认和安全的交易，阿维斯塔自己创建了一个闪电般神速的区块链，速度比比特币快 60 多倍，实现了直接销售点支付和账户间直接付款。

确认

大多数加密货币需要几分钟的确认时间。这意味着，无法直接在区块链上运行销售点或商店付款交易。阿维斯塔的区块链确认时间仅需几秒。我们基本上量身定制区块链，使销售点交易成为可能。

双重支付

阿维斯塔阻止了用户和区块链端的双重支付。此外，区块链速度飞快，它能更快速的确认，所以是不可能出现双重支付的。如果发生双重支付，将会通过钱包、节点来检查账户。

挖矿

通过建立节点共识的挖矿奖励制度，阿维斯塔创建了一个截然不同的无矿池挖矿方式。它开辟了一种方式让所有矿工相互合作，而不是让所有矿工和矿池相互竞争，让矿工公平获得他们的贡献应有的奖励份额。这种挖矿方式防止了所谓的孤儿区块或叔区块，例如以以太坊为基准的加密货币，同时防止了不必要的通货膨胀。

所有这些方案共同搭建了一个超快速安全的区块链网络。

51% attack

通过让所有矿工共同合作，而不是互相竞争，此问题已得到解决。这防止了整个局势上外部人员攻击网络和更改区块链。

合法性

通过与世界各地的法律机构合作，阿维斯塔将制定一个法律框架更大范围使用区块链技术和付款方案。

对比

相比其他加密货币，阿维斯塔能够提供更舒适的用户体验，以及更强大的功能。下表是阿维斯塔与其他技术的比较。

加密货币对比图

	比特币	以太坊	零币	阿维斯塔
挖矿	✓	✓	✓	✓
匿名			✓	✓
智能合约		✓	✓	✓
账号				✓
硬币继承				✓
平均确认时间 (时间越短越好)	600s	14s	150s	10s
TX-秒 (大约)	20-30	30-40	20-30	1000+
硬币上限	21. 000. 000	POS ? 100. 000. 000+	21. 000. 000	ICO+挖矿 200. 000. 000

产品开发蓝图



启动

阿维斯塔启动日期
是 2018 年 1 月 5 日

包含：
- 钱包
- 平台
- 挖矿

电子支付

电子商城和电子支付
模块

钱包更新智能发票
和智能合约用户界面

借记卡

账户持有人获得阿维斯塔
借记卡，经 KYC 审批

阿维斯塔手机应用进行
VOIP 和 IM 集成

01

现在 2017

ICO

2017 年 11 月 12 日
13:00 UTC 开始 ICO

2017 年 12 月 20 日
13:00 UTC 结束 ICO

12 月 24 日
公共测试网络

03

2018 年第一季度

记账

记账模块和阿维斯塔
钱包记账 API 的集成

04

2017 年第二季度

05

2018 年第 3 季度

硬件

销售点硬件和软件的
集成

06

2017 年第 4 季度

阿维斯塔全球认可的
准备



解放货币

总结

阿维斯塔解决了加密货币的部分主要问题。我们创造了一个快捷安全而容易使用的加密货币，无法跟踪，超快速确认和保护。

阿维斯塔创建了一种新的区块链技术，供大家享用和受益。这将彻底改变人们对加密货币的看法，并为主流加密货币的使用铺平道路。我们对挖矿的看法也将为寻找新方法更公平地分配奖励以维持加密货币网络铺平道路。有了阿维斯塔，区块链技术会显示其真正的潜力。

市场机会

在观察事实时，对加密货币世界的实际增长潜力的认识变得越来越明显。根据剑桥大学的研究：“当前加密货币钱包活跃用户的人数预计在 290 万到 580 万之间。” - 占世界人口不足 1%。虽然加密货币市场全面增长潜力显然还有很大的开发空间，但是根据 coinmarketcap 的统计，截至撰写本白皮书时所有加密货币的总市值仍然是一个非常引人注目的数字：大约 \$141,253,369,650（约 \$1410 亿）。

参考资料

https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-04-20-global-cryptocurrency-benchmarking-study.pdf <https://cryptolization.com>
https://www.reddit.com/r/Bitcoin/comments/5rlzon/with_4mb_block_size_and_segwit_what_is_the_max/
<https://docs.google.com/spreadsheets/d/150B9eytmjZ642tYD0jSdFZQH1dmk7VG5Wm3KVctydpY/pubhtml>
https://www.reddit.com/r/zec/comments/662iq4/noob_question_whats_zcash_network_transactions/
<https://monero.stackexchange.com/questions/405/how-many-transactions-per-second-can-the-monero-network-handle>

图表:

https://docs.google.com/a/bitcause.org/spreadsheets/d/1fVwGE_TkmkkONt12yPUSFEa8qrX9ERm0sSJXShzRGIA/edit?usp=sharing

<https://www.reuters.com/article/us-microsoft-accenture-digitalid/accenture-microsoft-team-up-on-blockchain-based-digital-id-network-idUSKBN19A22B>