2018年9月27日区块链技术晚报 第22期

一.Tech News

1️⃣我们在谈论比特币的时候，应该要谈论Nakamoto consensus 而非仅仅是PoW ,没有一个总体的概念说明他不懂噢😯!

共识算法对于验证分布式区块链平台的真实性至关重要，并且是在相互不信任的参与者网络之间建立协议的过程。

Nakamoto Consensus由Satoshi Nakamoto为比特币创建，它引用了一套规则，结合网络中的工作证明共识模型，管理共识机制并确保其无信任的性质。通过这样做，比特币成为第一个拜占庭容错（BFT）开放和分布的对等（P2P）网络，该网络利用匿名节点的分布式网络，可以随意加入和离开网络。

拜占庭容错是指分布式计算机网络尽管信息不完善或网络组件故障仍能保持容错的能力。在比特币之前，维持BFT的唯一方法是，P2P网络是通过采用封闭或半封闭的节点组。此外，传统的BFT算法（例如实际拜占庭容错（pBFT））使用与Nakamoto Consensus中当前使用的不同的节点选择方法。

在像比特币一样大的开放和分布式网络中维护BFT需要使用依赖于加密和博弈论机制的一组特定规则，以便创建必要的环境，以促进价值转移网络中的分散共识。

在pBFT系统中，共识模型仅适用于封闭节点的小组（~50），其中存在大量的通信开销，这阻碍了这些共识模型能够大规模操作。在具有任意故障的系统中达成共识通常需要特定的投票系统来帮助达成共识。关于利用pBFT共识模型的加密货币平台，该投票机制基于以round-robin。由于系统由有限的，封闭的节点组成的网络组成，因此这些节点彼此有效通信并确定提出每个新块的“领导者”是谁是微不足道的。

如果领导者恶意行事，则可以通过节点的多数投票删除它们。然而，在诸如比特币之类的系统中，这显然不能很好地扩展，其中对区块链的整个状态和其所有事务的有效性的共识被分发到世界上连续地连接和断开网络的数千个节点。此外，参与该共识系统需要存在固有成本以阻止参与者以恶意方式行事。

因此，为了使比特币作为拜占庭容错P2P网络运行，它引入了PoW挖掘一致性算法以及管理该机制的一组特定规则，以便在整个网络中实现无信任的共识。这已经被称为经典的Nakamoto Consensus。

Nakamoto Consensus如何运作？ Nakamoto Consensus可分为大约4个部分。

```
工作证明（PoW）
块选择
Scarcity
激励结构
```

比特币的这4个组成部分的组合和协调使其成为价值转移的分布式网络。只要获得采矿过程的大部分权力掌握在诚实的矿工手中，它就会以无信任的共识运作并保持安全，正如您将在下一步看到的那样。

2️⃣在2018年9月27日，号称以太坊上操作系统的Status宣布推出一套开发工具，以丰富以太坊体验。由Iuri Matias创建的Embark 3.2将提供以太坊名称服务（ENS）支持，更新 Vyper支持，Swarm兼容的Javascript库以及改进的构建pipeline等功能。这项合作是Status Projects的另一项举措，旨在将Web3变为现实。

ENS 就是去中心化世界的DNS，该服务允许用户将项目发送到诸如“shauryamalwa.eth”之类的名称，而不是复杂的数字和字母堆砌在一起。根据Status，Embark 3.2框架通过省略多个contacts和库正常运行的需要(已经封装好)，为开发人员简化了这一过程。

更新后的Embark版本现在包括swarm-api，它允许更好地访问存储以太坊分类帐公共记录的Swarm分布式存储平台。另一个功能使开发人员能够在部署操作之前确定在网络中运行每个智能合约的gas成本。改进的pipeline提供预先配置的插件，以帮助区块链开发人员更轻松地构建他们的DApps。这一进步包括输入主要编程语言（CSS，JS）以及为React和JSX提供支持。

想了解更多点这里

3️⃣这几天最火的消息就是比特大陆的IPO

总部位于北京的比特币矿业巨头Bitmain最终决定通过在香港证券交易所（HKEX）进行首次公开募股上市。 Bitmain在过去卷入了几次争议，终于决定开放它的招股书。对招股书的一瞥可以看出公司在过去几年中的大幅增长。

Bitmain Technologies过去一直在考虑进行大规模的筹款活动。然而，该申请目前由香港交易所提出，目前尚不清楚上市时的估值。让我们来看看公司的成本和收入结构以及其他细节。

Bitmain收入和利润

毫无疑问，Bitmain是加密采矿设备的市场领先者，占据了总市场份额的75%。在过去一年的加密狂热期间，Bitmain的收入和利润以前所未有的速度飙升。

2015年，Bitmain收入达到1.373亿美元，到2017年底达到25亿美元。在过去两年中，这是一个惊人的年复合增长率，为**328%**。此外，到2018年6月30日，**今年的收入已经过去一整年，已达28亿美元**。

随后，利润也以类似的巨大增长率攀升。从2015年的4860万美元到2017年的两年后的9.526亿美元，**Bitmain实现了280%的复合年增长率**。

对公司提出的收入细分的研究表明，采矿硬件一直为Bitmain的收入流做出贡献。归功于Bitmain的专用集成电路（ASIC）。事实证明，ASIC已成为游戏规则改变者，并推动了许多国家的GPU市场份额。值得注意的是，采矿硬件销售也有所增长 - 从2015年的79%上升到2018年上半年的94%。

最近，除了传统的ASIC之外，Bitmain还宣布进军新的采矿硬件领域。招股说明书指出：“我们专注于开发采用主要加密货币的不同算法的采矿硬件，包括比特币，比特币现金，以太币，莱特币，Dash和Zcash，这使我们成为少数几家为各种加密货币提供采矿解决方案的公司之一。”

Bitmain的扩张计划进出中国

除了将重点放在新的采矿硬件上之外，该公司正在加密采矿场的土地收购。根据最新的文件，Bitmain在蒙古拥有两块巨大的土地。此外，它还拥有宁夏和四川的一块大土地。

据说该公司还在5个不同的国内地区租用了近50套房产，总土地面积近10万平方米。 Bitmain也对海外扩张其采矿业务表现出兴趣。这家加密矿业巨头已经开始关注美国德克萨斯州，田纳西州和华盛顿州。由于有廉价电力供应，它还在探索加拿大魁北克省。

Bitmain已经开始在这些地点建设，美国和加拿大的农场将在2019年第一季度开始运营。除了加密采矿农场，Bitmain还在亚洲和欧洲大陆的许多地方设立了行政办公室。

资金和企业联系 Bitmain已经在美国和亚洲市场的大型风险投资公司筹集的三轮融资中筹集了巨额资金。在A轮融资中，Bitmain设法筹集了由SCC Venture领导的总计5000万美元。同一家公司在2018年6月领导了B轮融资，收益为2.92亿美元。

在最近8月份的首次公开募股前资金回合中，Bitmain设法获得了高达4.22亿美元的资金。此次上市前由Crimson Partners领导，贡献了大约1.5亿美元。

此外，Bitmain还与大型跨国公司合作，就IPO申请提供建议。 Bitmain收到香港证券有限公司，中国国际金融有限公司和商业及金融法律办公室的财务顾问。法律，审计和咨询服务由Calder在香港，毕马威和Frost＆Sullivan提供。

英文版点这里

4️⃣今天IMtoken在Twitter上发布消息称其和Circle宣布成为合作伙伴,用户现在可以在imToken 2.0中存储Circle新推出的全额抵押美元稳定币：USD // Coin（USDC）。 最重要的是，USDC还将作为Tokenlon（imToken的自带的去中心化的交易所）的基本交易货币。

详细的请点这里

5️⃣想在自己的AntMiner S9或者DragonMint T1运行挖矿，来看看开源的Braiins OS吧！

Braiins OS是第一个用于加密货币嵌入式设备的完全开源的基于Linux的系统。此初始版本针对采矿设备，但由于我们使用OpenWrt作为基础，因此其功能可以在多个方向上进行扩展。

例如，我们希望包括比特币核心和闪电网络软件，并发布单板计算机（如Banana Pi），以允许用户无需麻烦地运行他们自己的比特币和闪电节点。

1.新闻点这里

2.其官网

3.GitHub安装手册

6️⃣如何在开发Dapp，写智能合约的时候保证自己的隐私安全数据不暴露在外部？隐私数据放中心化server中么？现在这里有个解决方案。两个解决方案如下：

1.**利用TEE（可信执行环境）来隐藏来自网络的数据**

2.**安全多方计算（MPC）的纯加密解决方案**

后续的可以不用读！

大部分的情况下开发Dapp的时候数据本身被隐藏在执行计算的节点之外。Enigma网络提供了一个无权限的对等网络，允许执行具有强正确性和隐私保证的代码（秘密contract），这使dApp开发人员能够在其智能合约中包含敏感数据，而无需将链外移至集中式（且安全性较低）的系统。

Enigma的协议是第一个使区块链能够处理私有或敏感数据的协议，显着扩展了基于区块链的应用程序（以及更高版本）的有意义范围。在此过程中，我们先前介绍了秘密合同的概念，智能合约利用加密输入，而不会将原始数据泄露给执行计算的节点。因此，Enigma的节点能够计算加密数据，甚至可以保护自己的秘密 - 因此称为“秘密节点”。

目前，Enigma可与区域链世界中最具活力的生态系统 - 以太坊互操作。已经与Solidity建立智能合约的开发人员可以利用Enigma网络在需要隐私的合约中执行功能。

智能合约利用加密输入，而不会将原始数据泄露给执行计算的节点。因此，Enigma的节点能够计算加密数据，甚至可以保护自己的秘密 - 因此称为“秘密节点”。

目前，Enigma可与区域链世界中最具活力的生态系统 - 以太坊互操作。已经与Solidity建立智能合约的开发人员可以利用Enigma网络在需要隐私的合同中执行功能。这种秘密合同的一些基本例子 - 我们称之为“构建模块” - 是投票和拍卖等重要功能。

您想要在Enigma网络上运行这些功能而不是在以太网上公开运行这些功能的原因有很多。 Enigma网络不仅可以处理敏感输入，还可以通过使用秘密合同替换临时构造（例如commit-reveal）来提供更好的用户体验。重要的是，虽然Enigma目前可以与以太坊互操作，但我们的协议旨在与区块链无关 - 当Enigma自己的链可用时，它可以独立于任何其他区块链运行。我们欢迎与其他区块链进行对话并欢迎合作，以便在Enigma协议和有兴趣利用我们的数据隐私和安全计算解决方案的区块链之间建立桥梁。

拓展阅读- 秘密合约

实现真正的去中心化确实有很多好处。dApps 拥有强大，不可阻挡，防篡改和透明的好处。所有这些都是减少信任和提高安全性的重要特性。

但是所有区块链，以及智能合约，都有一个经常被忽视的明显问题 - 存储在它们上面的所有数据都是公开的。从这个意义上讲，区块链比他们之前的任何东西都要糟糕。您不必信任单个组织的数据（例如Facebook，Google，您的银行等），您现在必须信任所有人。出于所有意图和目的，区块链上的数据成为公共领域。

当然，这是不可接受的。任何企业或组织都不会同意公开他们最敏感的数据。如果亚马逊（当今占主导地位的云提供商）将所有数据都驻留在其数据中心公开，它将立即停止存在。因此，不难看出没有隐私的数字世界不是在实践中可以存在的世界。更重要的是，隐私是一项基本人权 - 因此，为下一个网站设计技术基础必须以隐私设计为基础。

我们需要隐私，而不仅仅是正确性。 为了解决这个问题，我们需要回到绘图板并重新定义问题。在区块链的命名中，智能合约是一个代码单元，它不是由单个计算机执行，而是由许多系统执行 - 基本上是区块链网络中的所有节点。总之，这些达成了关于世界某些国家的协议，使攻击者无法篡改该州，或说服任何诚实的行为者，事实上某些虚假声明是真实的。

例如，在价值转移的简单示例中，如果Alice向Bob发送五个硬币，那么网络中的每个人都会同意Alice拥有的硬币总数减少了五个，同样地 - Bob获得了五个新硬币。没有坏演员能够说服诚实的参与者。这种想法通常在学术文献中被定义为分布式系统的正确性。智能合约，更普遍的 - 区块链，解决了这个问题。然而，正如我们已经建立的那样，他们未能解决同样重要的隐私问题。

因此，我们提出了一种称为秘密合同的新概念这些合同扩展到智能合约，因为它们不仅可以解决正确性问题，还可以解决隐私问题，因为它们可以完全隐藏节点中的数据。通过这些合同，用户和应用程序可以在一个可以安全包含敏感数据的环境中运行，这是大多数实际用例所需要的。

举一个潜在的秘密合同的例子，想象一下可以自动向用户发放贷款的贷款dApp。为了运作，它运行一个智能合约，通过扫描他们的钱包和先前的交易来测试每个人的资格，然后计算个人是否应该获得贷款（如果是的话 - 应该有多大）。例如，它可以检查您过去是否要求贷款，以及您是否按时还款。

使用普通的智能合约，用户需要公开披露他们的所有交易。这意味着每个人都可以完全了解您的财务状况。由于大多数用户不太可能选择加入此类服务，因此留给dApp提供商的唯一选择是保持资格的实际计算集中，以便限制敏感数据暴露给提供商本身。在这种混合方法中，dApp不再是自治的或真正分散的，因为它在没有提供者的帮助下无法运行。因此，dApp保留了集中式应用程序的所有弱点，几乎没有什么优势。

相反，在存在秘密合同的环境中，用户可以安全地与秘密合同本身共享其交易历史。节点可以执行合同并接收资格结果，而无法观察用户的交易。不再需要创建混合dApp。这个dApp可以是自主的端到端，同时保证两者的正确性 - 如果用户有资格获得贷款，她将获得贷款;和隐私 - 除了用户之外，没有人可以看到他们的交易记录。

迄今为止，关于区块链隐私的工作主要限于隐藏交易。已经为此任务提出了几种技术（coinmixers, confidential transactions/pedersen commitments, ring signatures, zero-knowledge proofs)），但这些技术并不能很好地概括为智能合约的隐私，因此不适用于实现秘密合同。

特别是零知识证明（ZKP）虽然是一项重要的技术和令人难以置信的成就，但通常很难表现为所有隐私问题的事实上的解决方案。实际上，当有权访问数据的一方想要证明对他人的主张而不向他们透露数据时，ZKP是有用的。在我们想要外包计算（通常涉及多方）的情况下，我们可以信任看到所有数据的单一方。这在智能合约设置中更加严重，其中执行计算的各方是不可信和假名的。

为了启用秘密合同，我们需要查看区块链上下文中尚未探索的其他技术。对于智能合约，主要技术要求是分布式共识 - 但正如我们所说，他们做得不够，无法创建真正分散的应用程序和解决方案。

对于秘密合同，缺失的部分来自密码学领域，称为安全计算 - 这是一种能够计算加密数据的不同技术的总称。首先，这些技术能够隐藏状态本身与网络中的节点（以及公共节点），同时保留执行和验证计算的能力。

1.其官网Wiki

2.secret contract

3.新闻点这里

7️⃣Smart Contract as a Service

有没有想到BaaS，PaaS?!

目标用户：

- 加密爱好者和使用加密货币/代币的个人;
- 进行爱惜噢的公司;
- 智能合约开发商;
- 计划特别实施区块链技术和智能合约的企业。

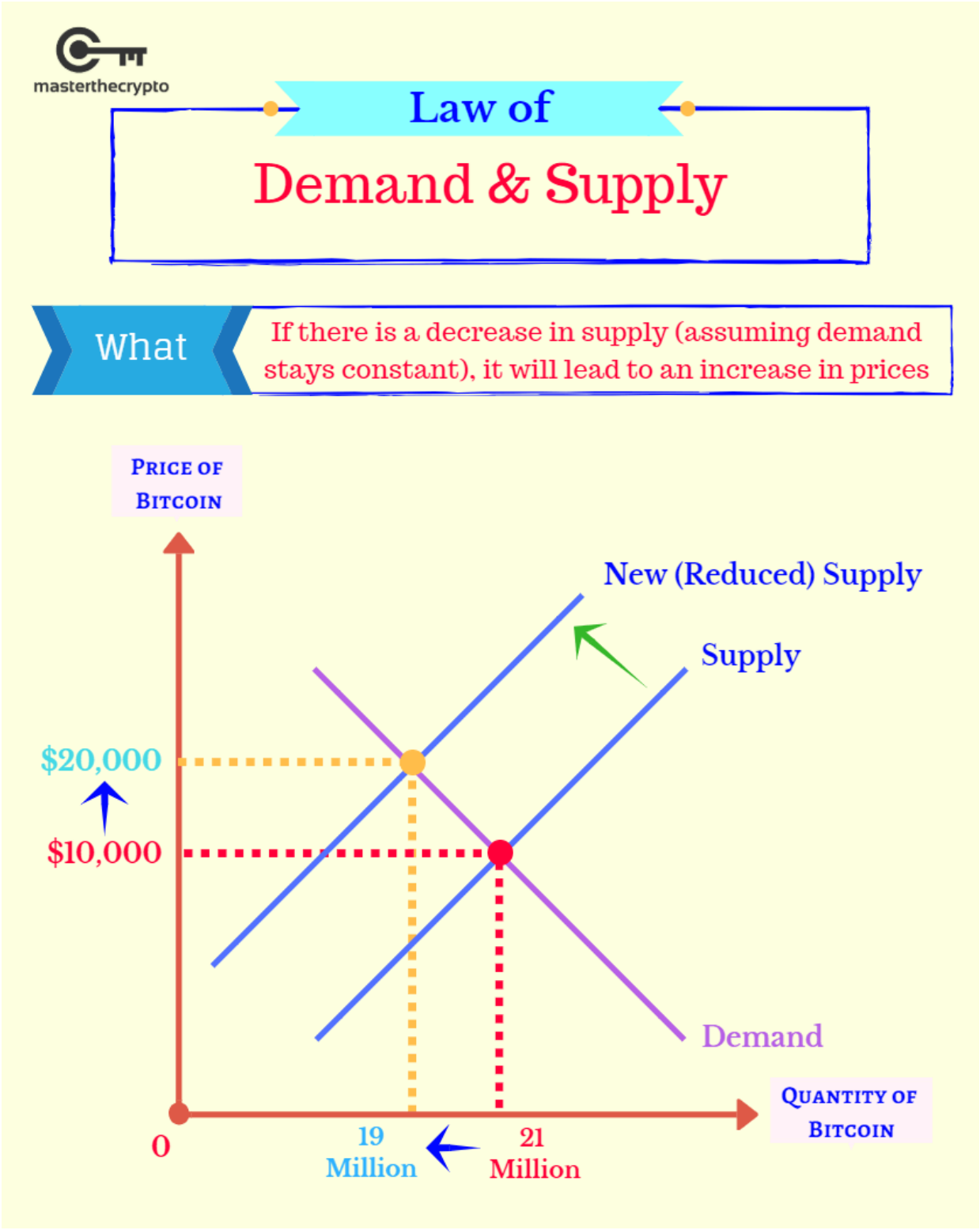
1.Smart Contract as a Service

8️⃣coin burning 了解一下

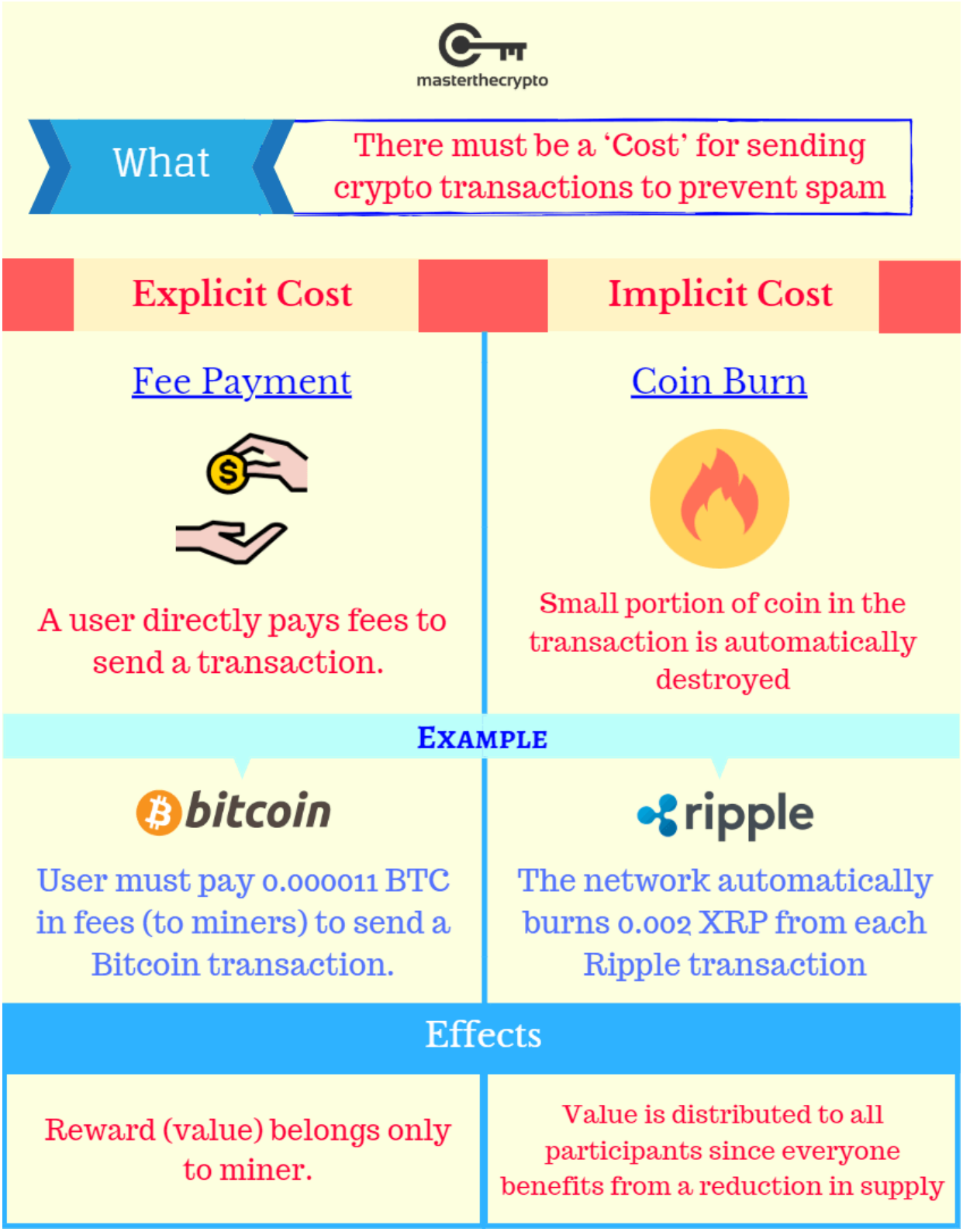
顾名思义 - 是一个通过使硬币无法使用而故意“燃烧”或消除硬币的过程。 这是通过将一部分硬币发送到“食者地址”来完成的，这通常被称为“黑洞”，因为任何人都无法获得该地址的私钥。 因此，发送到食客地址的任何硬币都是不可恢复的，永远不能再使用！ 这些硬币被有效地从流通中取出，并在区块链上公开记录和验证。

1.POB （proof of burn）

2.增加货币价值


masterthecrypto
Law of
Demand & Supply
What
If there is a decrease in supply (assuming demand stays constant), it will lead to an increase in prices
PRICE OF BITCOIN
New (Reduced) Supply
Supply
$20,000
$10,000
Demand
QUANTITY OF BITCOIN
0
19 Million
21 Million

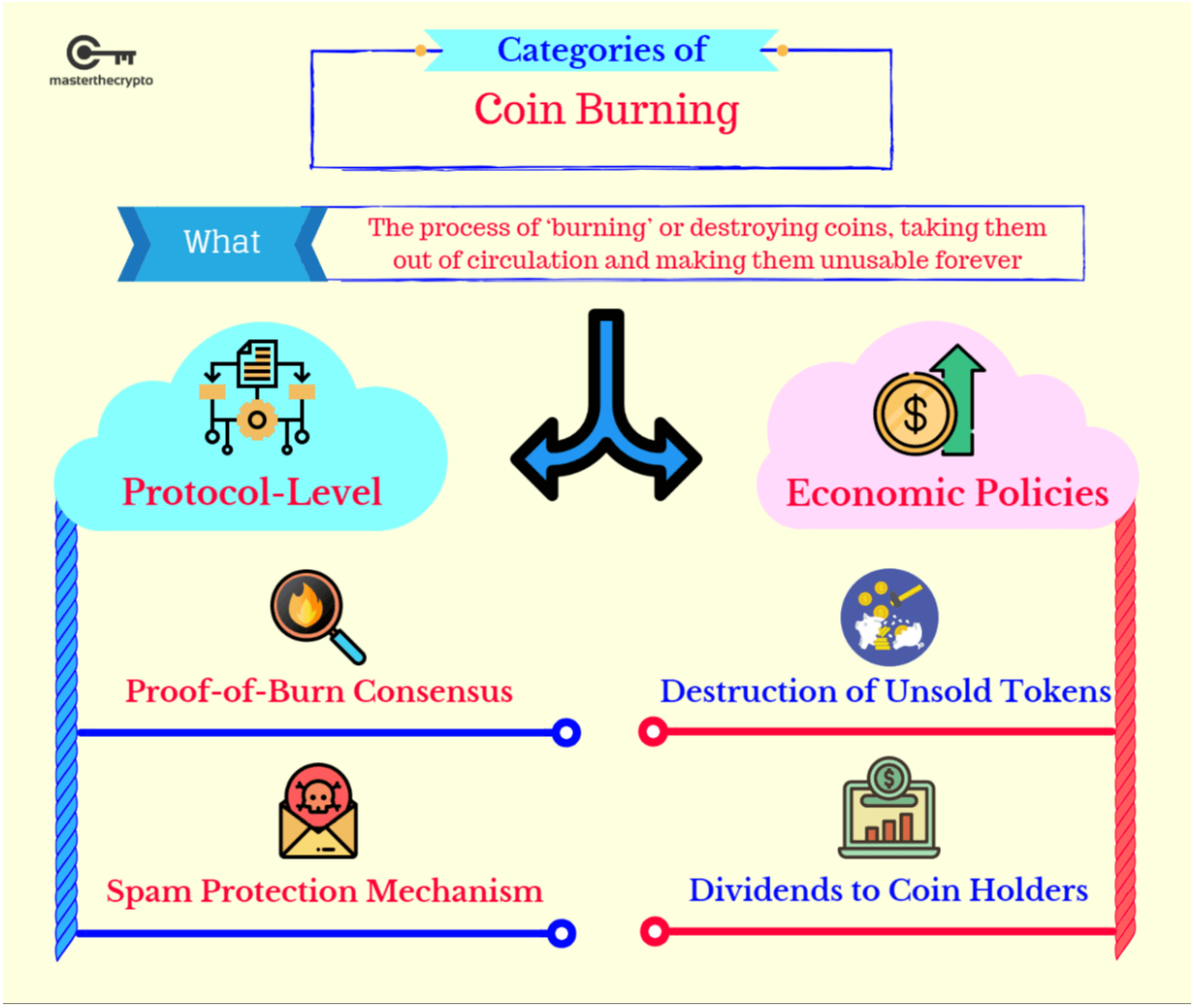
3.保护防止Spam



4.长期承诺

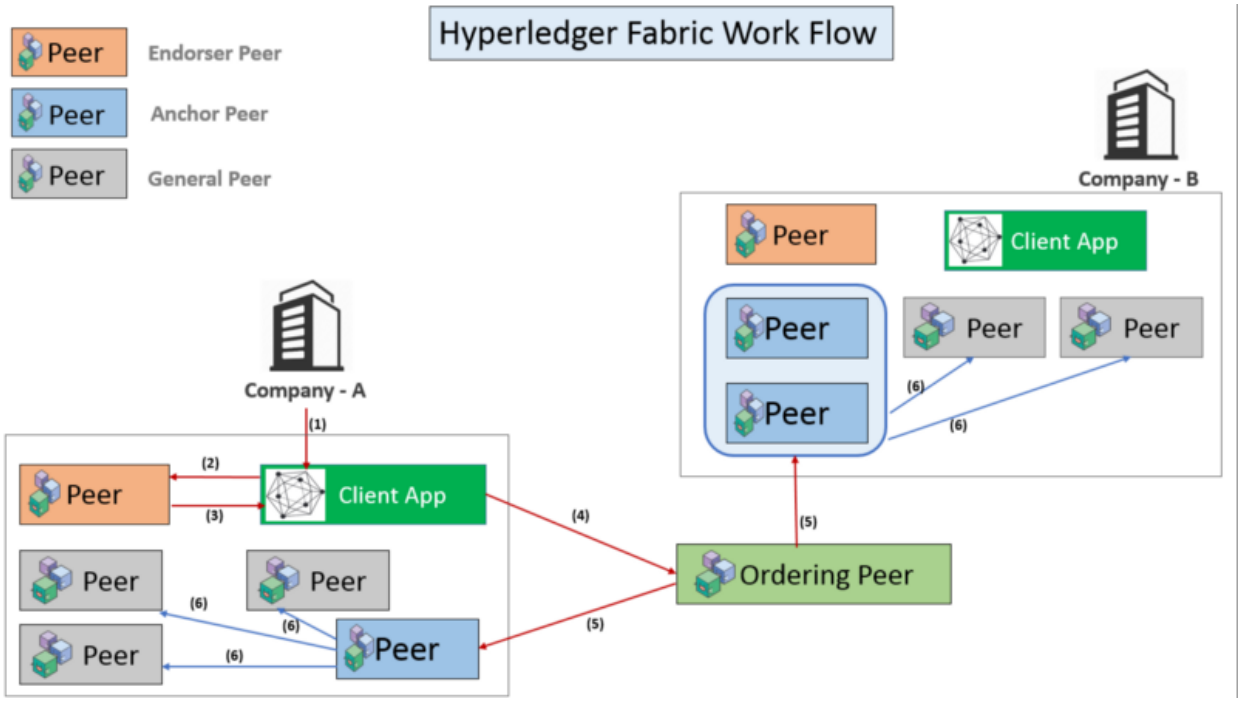
分类

通常可以分为两个不同的类别，在协议级别集成或作为经济策略实施。



[原文地址点这里]

9来篇hyperledger fabic 文章吧，IBM Hyperledger Fabric。



它是如何工作的

1.成员组织的参与者通过客户端应用程序调用事务请求。

2.客户端应用程序将事务调用请求广播给背书人对等方。

3.Endorser peer检查证书详细信息和其他人以验证交易。然后它执行链码（即智能合约）并将认可响应返回给客户端。背书同行发送交易批准或拒绝作为认可响应的一部分。

4.客户现在将批准的交易发送给订货人对等方，以便正确订购并包含在一个区块中。

5.Orderer节点将事务包括在块中，并将块转发到Hyperledger Fabric网络的不同成员组织的Anchor节点。

6.然后，锚点节点将块广播到其自己组织内的其他对等体。然后，这些单个对等方使用最新块更新其本地分类帐。因此，所有网络都会使分类帐同步。

🔟现在EOS上最火的游戏EOS Pixel Master！

EOS PIXEL MASTER 常见问题解答

EOS PIXEL MASTER 是世界首个基于区块链技术的协作艺术品。您可以使用工具栏去选择工具并进行绘画，然后使用 EOS 去支付购买像素，前提是您需要有一个 EOS 账号和安装了 Scatter (在移动设备上您可以使用 TokenPocket)

怎么赚 EOS?

EOS PIXEL MASTER提供多种获利方式：**贡献奖励、竞价、奖池和推荐人奖励。**每个像素的价格是独立的，起始价格均为 **0.05 EOS.** 第一次被购买的像素的金额会全部进入"游戏收益"。

"游戏收益"是怎么计算的?

40% 作为贡献奖励（贡献奖励机制请看下面）。
25% 分到奖池。
8% 作为推荐人奖励（如果没有推荐人，这部分将归入奖池）。
20% 属于开发团队收益。
7% 用来补助合约的 RAM 支出。

竞价是怎么一个流程?

您可以使用 **1.35** 倍的价格去购买别人的像素。像素的上一个拥有者将赚回本金，而对于这额外的 35% 的差价，**75%** 是给像素拥有者的利润，另外的 **25%** 是手续费，会流入"游戏收益"中（请看上一条）。

贡献奖励是怎么计算的?

您买的每一个像素都会增加您的贡献奖励因子，即使您的像素后面被买走了。贡献奖励会随着游戏的进展而积累，您拥有的贡献奖励因子越多，您就能累积越多的贡献奖励。奖励会记录到您的账户余额，在游戏达成"游戏激活门槛"后，您可以通过提款提出（贡献奖励因子不会因此减少）。

奖池是什么？怎么才能拿到?

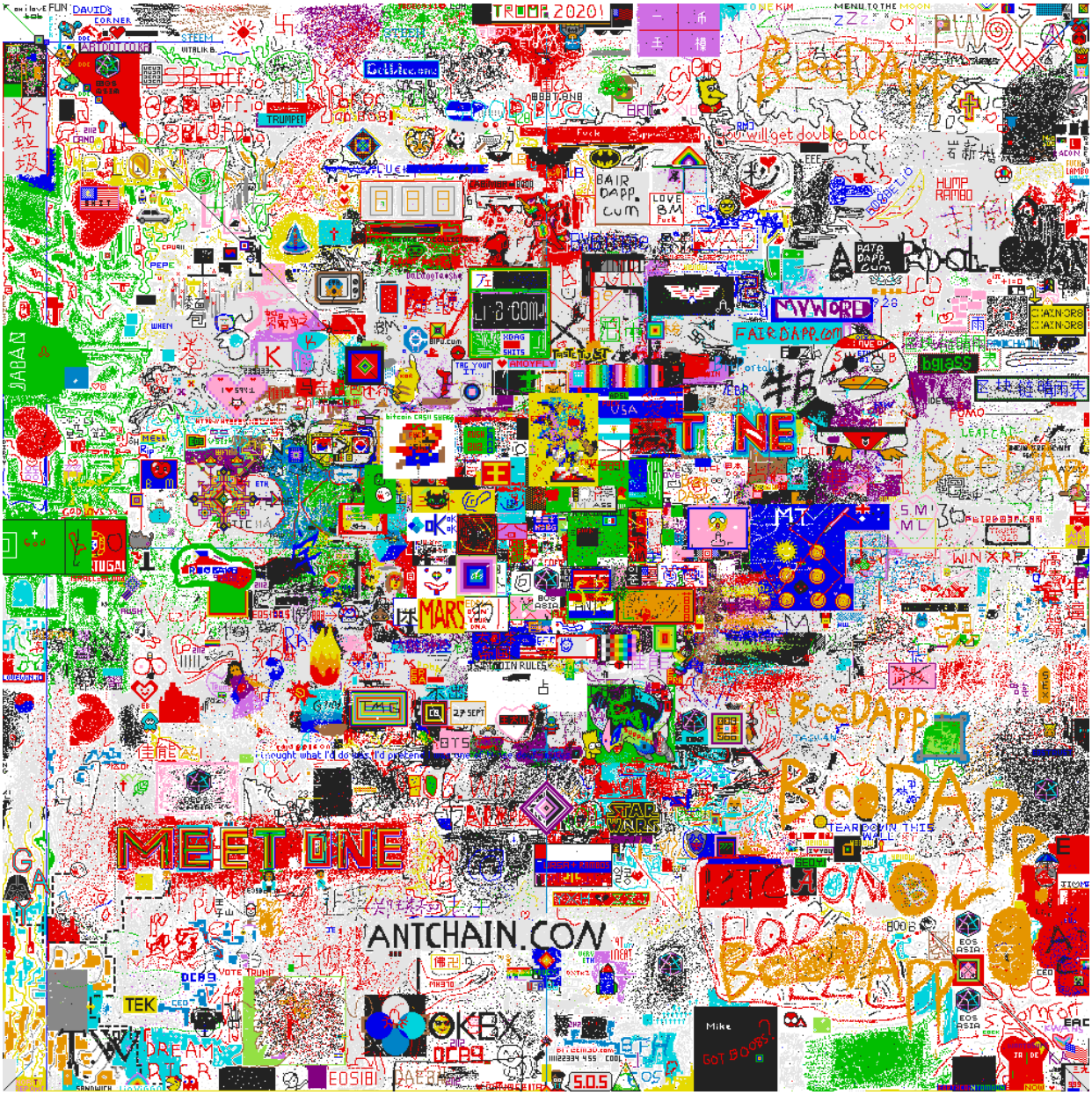
在达成"游戏激活门槛"之后，如果在 **24** 小时内都没有人画像素，当前画布将会被永远保存在区块链上。**最后一个买像素的人将会赢得整个奖池。**

怎么赚取推荐人奖励?

首先您需要购买过至少 1 个像素，然后您就可以使用推荐链接去邀请好友。您的好友购买的每一个像素都会给您带来额外的收益。收益会记录到您的账户余额，在游戏达成"游戏激活门槛"后，您可以通过提款提出。

什么是"游戏激活门槛"?

游戏激活门槛设置为 **150,000** 个像素，在 150,000 个像素售出前，合约的所有金额都将被冻结，这里包含了您的收益和我们的收益。只有在游戏达成激活门槛之后，游戏的提款功能才正式开放，奖池机制才正式开始。



以上内容由李平整理，感谢阅读！日报汇聚地址为：https://github.com/allinbc/BlockChain_Daily_Report

欢迎大家star&watch!