中文

白皮书

PRIZM

数字货币的最初概念

Prizm白皮书修订版-2020年6月

PZM.SPACE

PRIZM

介绍

比特币是世界上第一种去中心化的数字货币，它使您可以使用P2P网络轻松存储和转移加密硬币来传输信息，将散列作为同步信号以防止重复支出，以及强大的脚本系统来确定硬币的所有者。 这具有不断增长的技术和业务基础架构。 根据原始设计，比特币是可互换的，充当中立的交换手段。 比特币可能具有发行人或公共协议支持的特殊属性，并且其价值独立于其基础名义价值。 比特币已经证明，P2P电子支付系统可以真正地运作和处理支付，而无需第三方的参与。

但是，要使整个电子经济都基于完全去中心化的对等解决方案，系统必须能够执行以下操作：

1-安全，快速，高效地处理事务，每小时处理数千次或更多；
2-鼓励人们参与网络安全；
3-在全球范围内以最少的资源消耗进行扩展；
4-并且能够在包括移动设备在内的各种设备上工作。

PZM（发音为“ Prizm”）满足所有这些条件。 并且还有一个额外的优势，即称为PARAMINING的独特优势，这在任何现有的加密货币中都没有。

我们稍后将讨论细节

PRIZM

评论

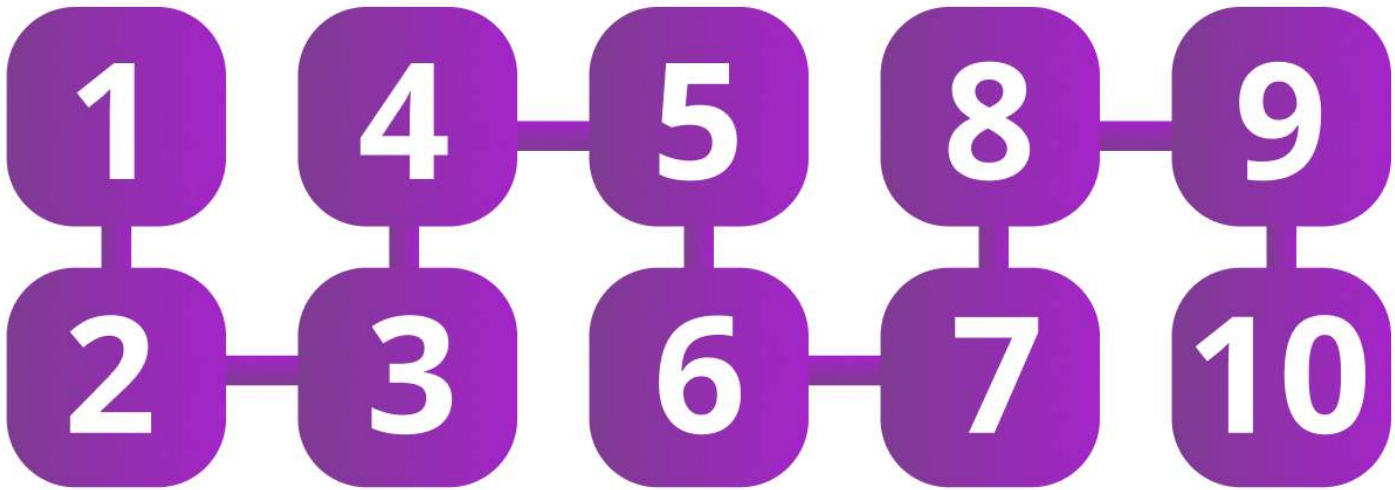
PRIZM - 是100%Proof of stake 基于NEXT内核的加密货币，基于Java构建带有开源代码。独特的PRIZM - Proof of stake算法才不是依靠任何实作的“硬币年龄”概念其他加密货币并且可以抵抗所谓的“nothing at stake”攻击。可用硬币的总数在创世纪模块中分配。 Curve25519加密用于平衡安全性和所需的处理能力，以及更常用的SHA256哈希算法。

PRIZM

述評

60秒

平均而言，每60秒产生一次加密货币区块，由在网络节点上未被阻止的帐户。



PZM通过合并成功创建区块时会奖励给帐户的交易费用进行重新分配。 此过程称为伪造，类似于其他加密货币使用的“挖矿”概念。 在确认10个区块后，交易被认为是安全的，并且PZM的当前架构和区块大小允许每天最多处理367,200个交易。

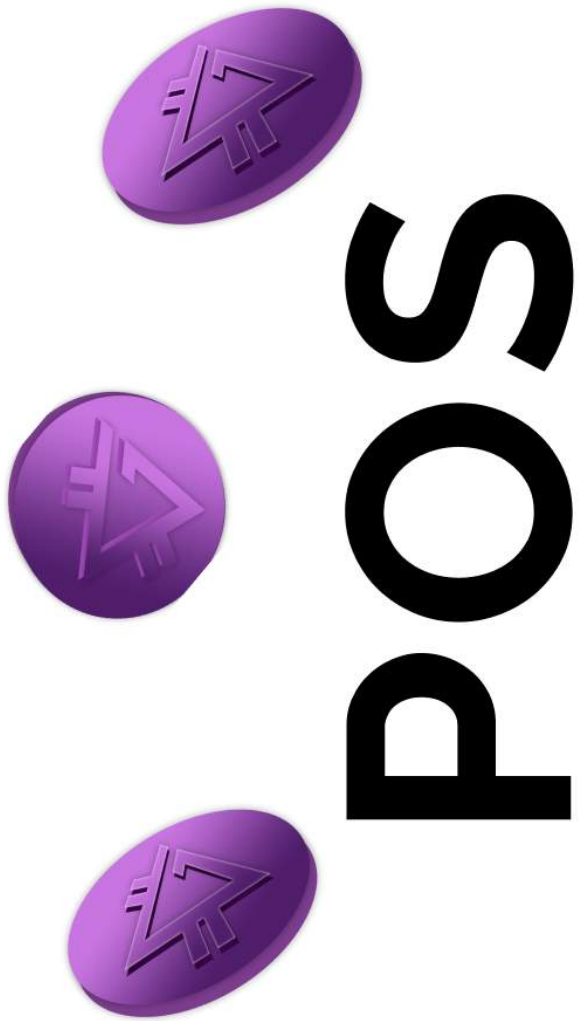
PZM包括透明锻造的实现，通过使用生成算法是确定性块，结合网络的其他安全性机制，可以使您将事务处理的性能提高两个数量级。

PRIZM

核心技

Proof of Stake

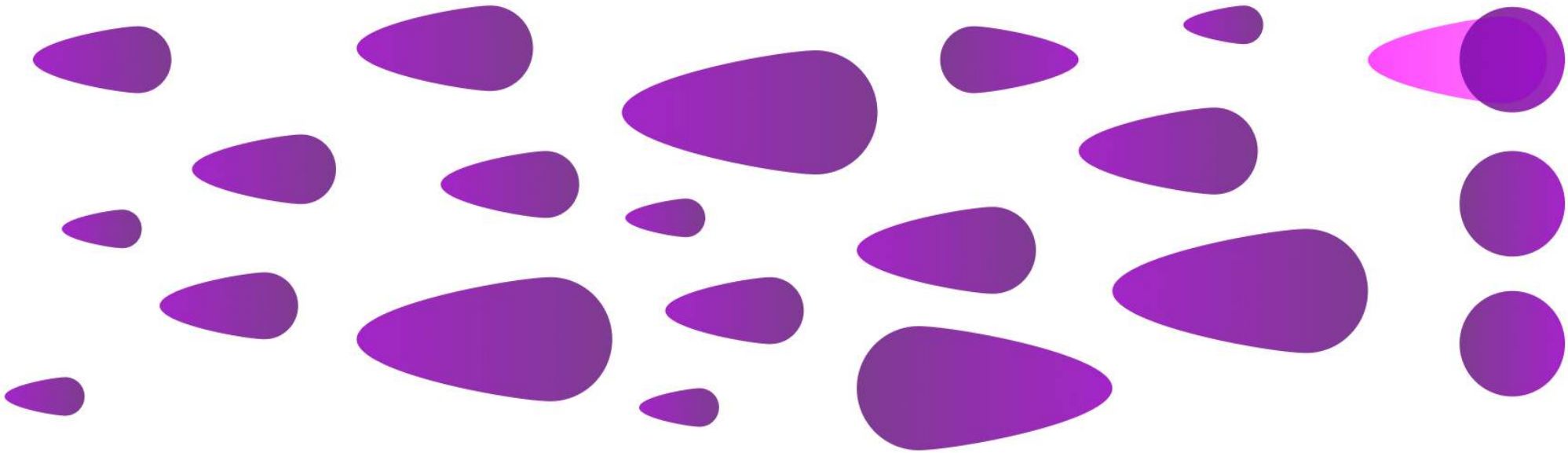
在大多数加密货币使用的传统“Proof of Work”模型中，参与者执行“工作”可确保网络安全。 他们使用自己的资源（计算/处理时间）来协调具有双倍成本的交易，并对试图使交易崩溃的人施加非凡的成本。 对于这项工作，参与者将获得PZM奖励，其频率和数量会根据加密货币的工作参数而有所不同。 此过程称为挖掘。 通常，区块生成的频率应保持恒定，该频率决定了挖掘加密货币的每种可用奖励。



结果，随着网络变得更加高效，获得奖励所需工作的劳动强度应该增加。 随着“Proof of Work”网络的发展，单个用户支持该网络的动机越来越少，因为他们的潜在奖励分配给了更多的同事。 为寻求盈利，矿工继续以专用的专利设备的形式投资资源，这些设备需要大量投资和高昂的当前能源成本。 随着时间的流逝，随着较小的合作伙伴（可以完成较少工作的合作伙伴）退出或将资源集中到集体采矿中，网络变得更加集中。. 比特币 Satoshi Nakamoto,的创造者希望比特币网络完全去中心化。 但是没有人能预测工作量证明系统提供的激励措施会导致采矿过程的集权。 这会导致潜在的漏洞。

PRIZM PROOF OF STAKE

核心技



GHash。 过去，比特币IO池已达到比特币挖矿能力的51%，而排名前五的比特币挖矿池则构成了网络散列能力的70%。 分权的概念有全损的风险。 在Prizm使用的“Proof of Stake”模型中，网络安全由与网络有利益关系的合作伙伴监管。

该算法提供的激励措施不利于像“Proof of Work”算法那样的集中化，数据表明，自创建以来，Prizm网络仍然保持高度去中心化：大量（不断增长）的唯一帐户为网络贡献了区块，而五个顶级帐户则产生了区块总数的35%。

PRIZM

PROOF OF STAKE 在 PRIZM 加密

Prizm使用一种系统，可以将帐户中的每个“硬币”视为一个微型采矿场。帐户中包含的硬币越多，该帐户就越有可能获得创建区块的权利。创建区块所获得的总“奖励”，即区块内交易的佣金金额。由于创建区块，PRIZM不会创建任何新硬币。 PRIZM不会由于构建基块而创建任何新硬币。 PZM重新分配是由于区块生成器收取交易费用而产生的，因此使用术语“伪造”（在此上下文中用于“创建关系或新条件”而不是“挖掘”）。随后的块是根据来自前一个块的可验证，唯一且几乎不可预测的信息生成的。借助这些链接将区块链接在一起，从而创建了可以追溯到创世纪区块的区块链（和交易）。块生成时间大约为59秒，但是概率的变化导致一个事实，即块的平均生成时间可以为80秒，存在更长的块间隔。区块链的安全性始终在“Proof of Stake”系统中设置。

基本原　适用于 Prizm Proof of Stake 算法：

- 累积复杂度值作为参数存储在每个块中，并且每个后续块从上一个块的值接收其新的“复杂性”。在模棱两可的情况下，网络通过选择具有最高累积复杂度的块或链段来达成共识。

- 为了使帐户持有人不能将资金从一个帐户转移到另一帐户，作为一种操作手段，以便能够生成区块，硬币必须在1,440个区块内固定在帐户中，然后才能为区块生成过程做出贡献。 满足此条件的硬币有助于提高帐户余额，该余额用于确定锻造的可能性。

- 为了防止攻击者从创世纪块开始一直创建新链，网络仅允许重组位于当前块后面的720个块链。 低于此阈值的任何块都将被拒绝。 该移动阈值可以视为唯一的固定PZM检查点。

- 由于任何帐户通过创建自己的区块链来接管区块链管理的可能性极低，因此，如果将交易编码为位于当前区块后面10个区块的区块，则交易被认为是安全的。

PRIZM

与PEERCOIN PROOF OF STAKE的比

Peercoin使用币龄的设置作为挖掘概率的算法的一部分。 在此系统中，您的Peercoins在您帐户中使用的时间越长（最多90天），它们创建区块的能力（硬币年龄）就越强。 “满足”区块的行为需要消耗硬币年龄的尊严，并且网络通过选择具有最大消耗硬币寿命的链来确定共识。 当Peercoin区块分离时，消耗的硬币年龄将返回到原始区块帐户。

结果，攻击Peercoin网络的成本很低，因为入侵者可以一直尝试生成块（称为“磨碎牛排”），直到成功为止。 Peercoin通过每天几次集中发布区块链检查点来“冻结”区块链并阻止交易，从而将这些风险和其他风险降至最低。 Prizm并未将硬币年龄作为锻造算法的一部分。 任何账户创建一个区块的“机会”仅取决于其当前余额（这是每个账户的优势），自上一个区块以来的时间（所有锻造账户都共享）和基本目标值（即 也适用于所有帐户）。

PRIZM 代币

10 百万
PZM

初始发射

6 十亿
PZM

最终排放

初始排放量为1000万PZM，最终排放量为60亿PZM。代币是通过创世纪区块（区块链中的第一个区块）的创建而发行的。 预挖技术在全球范围内的所有国家中都以名义成本和有限数量实施，以实现权力下放Prizm。PZM的总金额将为60亿个代币。 Account Genesis会生成Premining的反硬币信号（将信号发送给某个钱包的信号），其上限为负60亿PZM

创世纪中反硬币的存在有几个有趣的副作用：

发送到Genesis帐户的所有令牌均被有效销毁，因为帐户余额为负会取消它们
Prizm的主要功能是传统的支付系统，但创建后的功能却更多。
在PZM与菲亚特主要货币平价的情况下，可以实现CWT社区的目标。

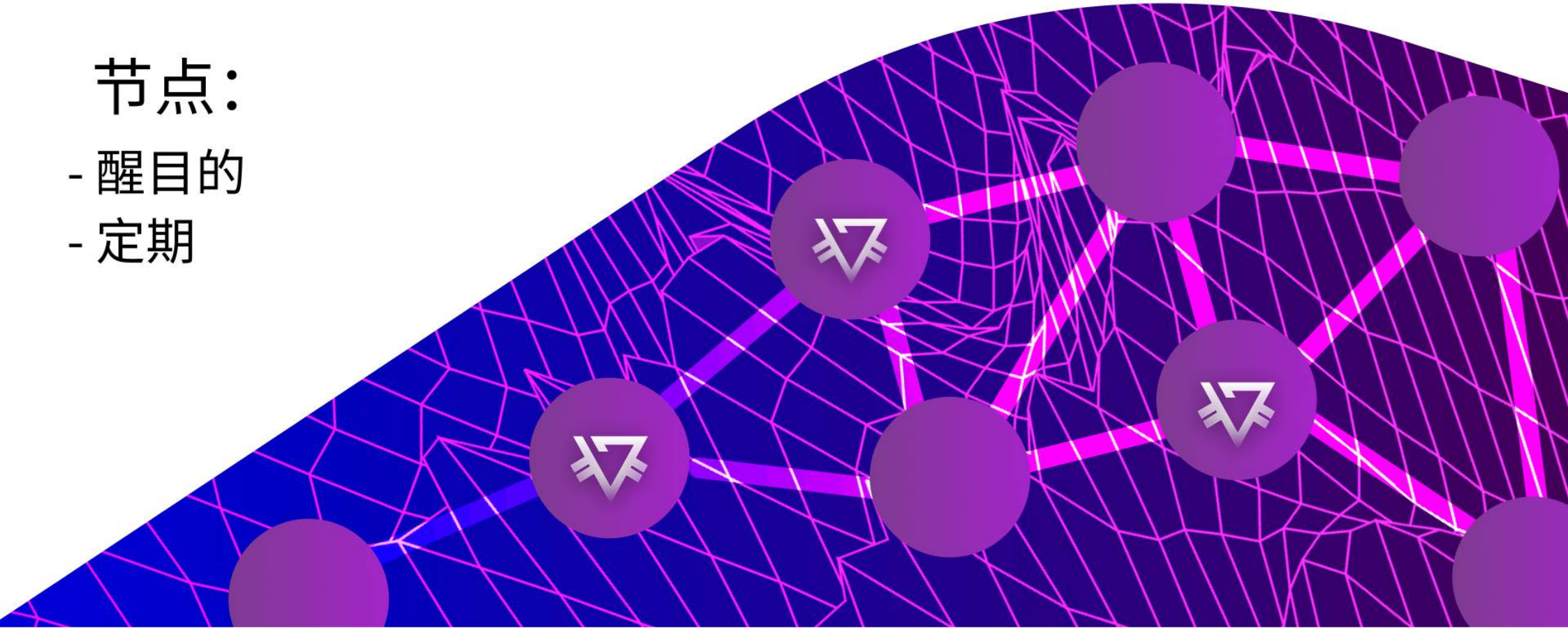
PRIZM

网络节点

网络节点Prizm是进行交易或将数据复制到网络中的任何设备。 装有PZM软件的任何设备都被视为节点。 节点可以分为两种:标记的和常规的。

节点:

- 醒目的
- 定期



网络节点

带标记的节点只是用从帐户的私钥接收到的加密令牌标记的节点。 可以对该令牌进行解码，以显示与该节点关联的特定PZM帐户地址和余额。 标签放置在节点上的行为增加了一层责任和信任，因此标记的节点比那些在网络上没有标记的节点更可靠。 帐户余额与标记节点的链接越多，对该节点的信任度就越高。 尽管攻击者可能希望标记节点以获得对网络的信任，然后将该信任用于恶意目的，但进入障碍（建立足够信任所需的PZM成本）可以防止这种滥用。

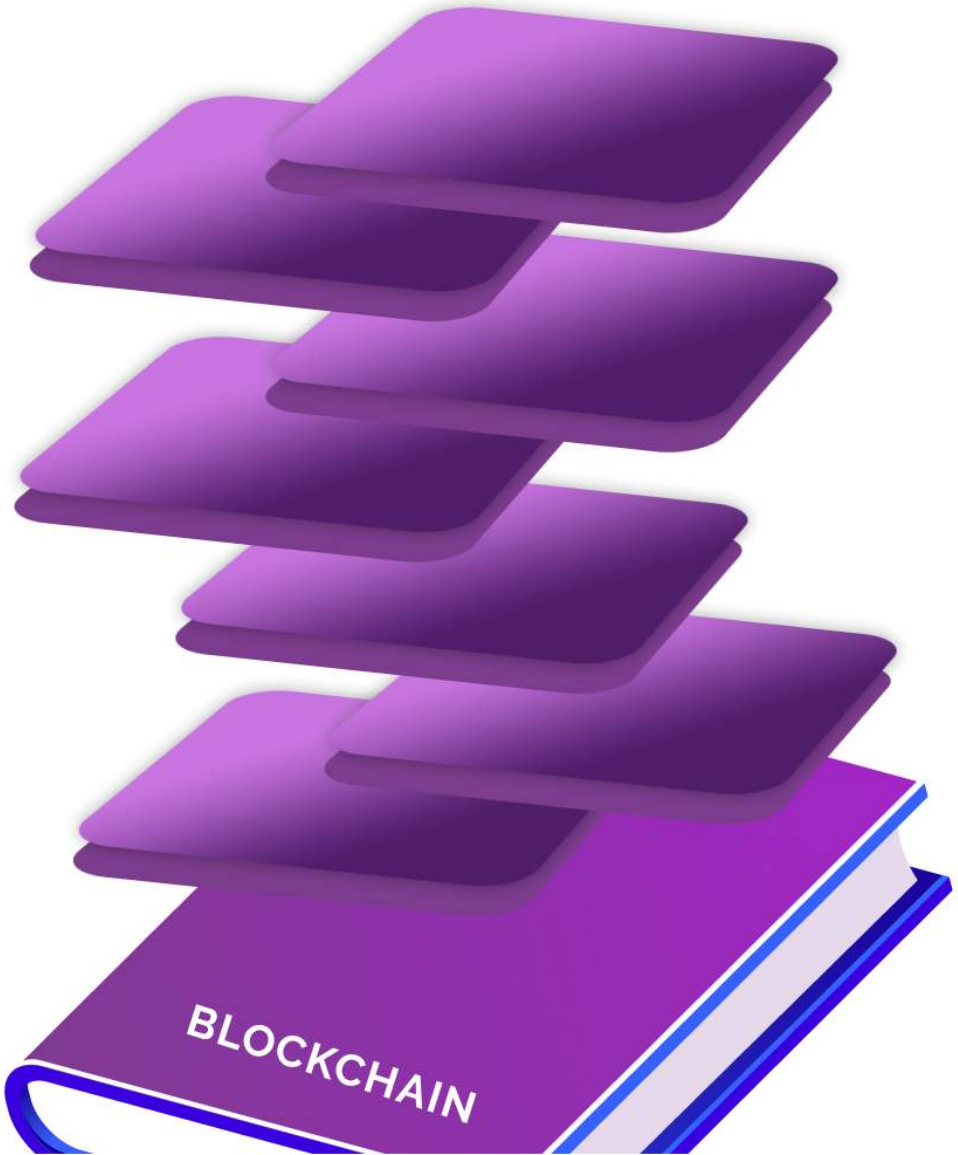
PZM网络中的每个节点都具有处理和传输事务和块信息的能力。 在从其他节点接收到块时对其进行扫描，并且在不执行块检查的情况下，可以将这些节点暂时“列入黑名单”，以防止散发无效的块数据。

每个节点都具有内置的DDOS保护机制（分布式拒绝服务），该机制将来自任何用户的网络请求数量限制为每秒30个。

PRIZM

积木

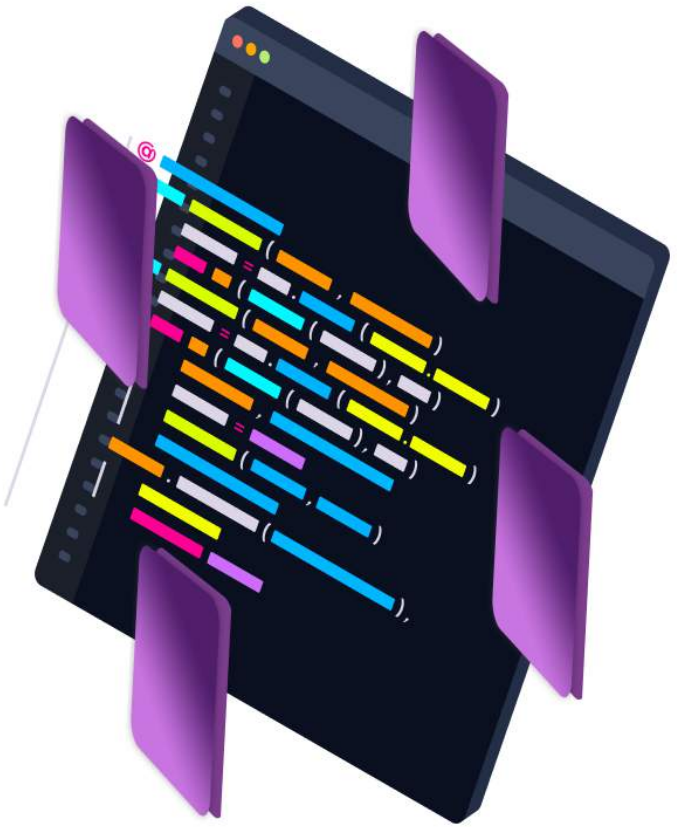
与其他加密货币一样，PZM分类帐（交易分类帐）会建立并存储在一系列称为区块链的链接区块中。 该工作簿提供了已发生交易的永久记录，并且还确定了进行交易的顺序。 区块链的副本存储在Prizm网络中的每个节点上，并且在该节点上未被阻止的每个帐户（通过提供该帐户的私钥）都具有生成区块的能力，条件是至少要有一个传入交易。 该帐户已被确认1,440次。 符合这些条件的任何帐户都称为活动帐户。 在PZM中，每个块最多包含255个事务，所有这些事务之前都有一个包含标识参数的192字节标头。 一个块中的每个事务最多由160个字节表示，最大块大小为32 KB



PRIZM

BLOCKS

所有　均包含以下参数：



- 块的版本，块的高度和块ID
- 从Genesis块以秒为单位的时间戳记表达
- 创建该区块的帐户的ID，以及该帐户的公钥。
- 上一个区块的ID和哈希
- 存储在区块中的交易数量
- 区块中交易和佣金代表的PZM总额
- 区块中包含的所有交易的交易数据，包括其交易ID
- 有效负载块的长度和有效负载块的哈希函数的值
- 块的基本目标值和累积难度

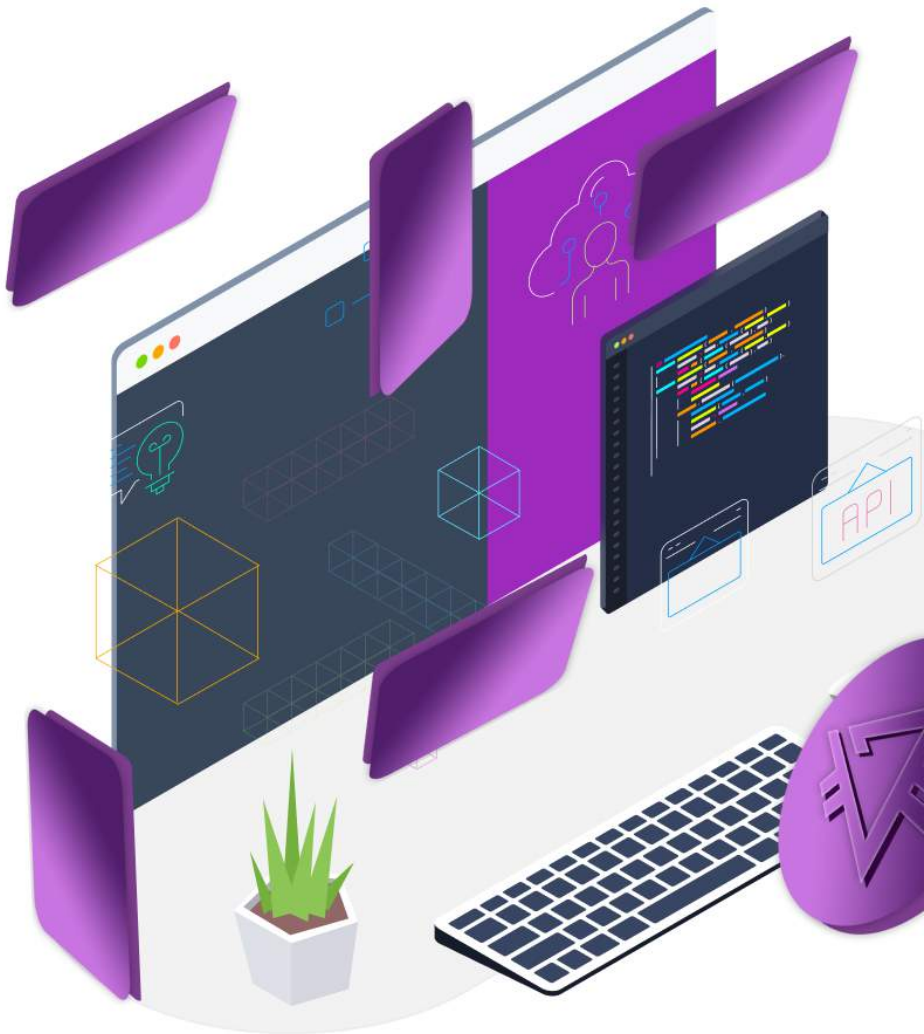
PRIZM

锻造（块创建）

这三个值是确定哪个帐户有权生成区块，哪个帐户有权创建单位以及在发生冲突时哪个单位被认为是权威的关键：基础目标值，目标值和累积难度。

参考目标值

为了赢得锻造（生成）区块的权利，所有活动的Prizm帐户都将通过尝试创建低于指定的基本目标值的哈希值来“竞争”。 该基本目标值随块的不同而变化，并由前一个块的基本目标值乘以生成该块所花费的时间得出。



PRIZM

目标价值

每个帐户都根据当前的有效率来计算自己的目标值。

该值等于：

$$T = Tb \times S \times Be$$

其中Be为：
T - 新的目标值
Tb - 参考目标值
S - 自上一个块以来经过的时间（以秒为单位）
Be - 有效账户余额

从公式中可以看出，自上一个块以来，目标值每增加一秒就增加一次。

最大目标值为1,53722867 x 1017，最小目标值为前一个块的基础目标值的一半。 对于试图在特定区块之上伪造的所有帐户，此目标值和基本目标值均相同。 唯一定义的帐户参数是有效余额参数。

PRIZM

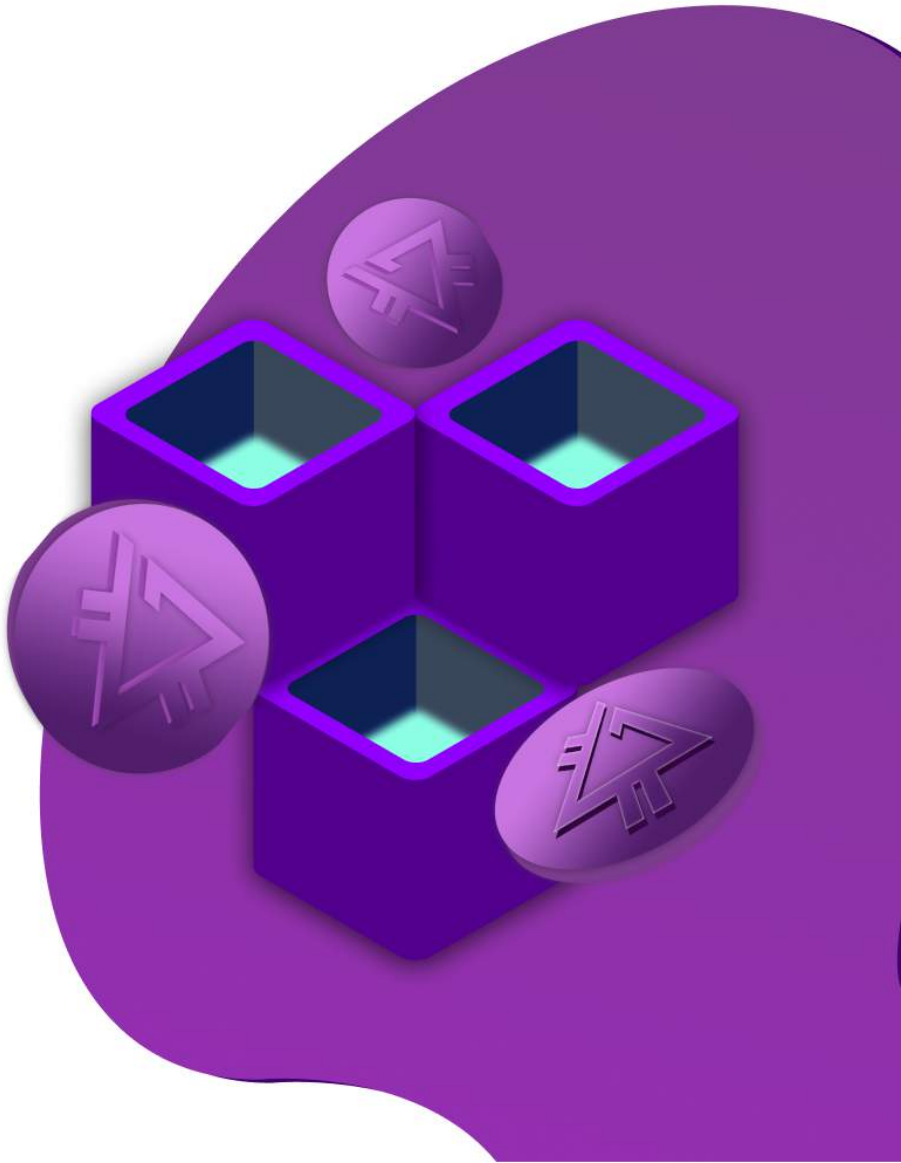
总复杂度

根据以下公式从参考目标值获得的复杂度总值：

$$Dcb = Dpb + 264 / Tb$$

其中Be为：

Dcb - 当前块的复杂性
Dpb - 前一块的复杂性
Tb - 当前块的基本目标值

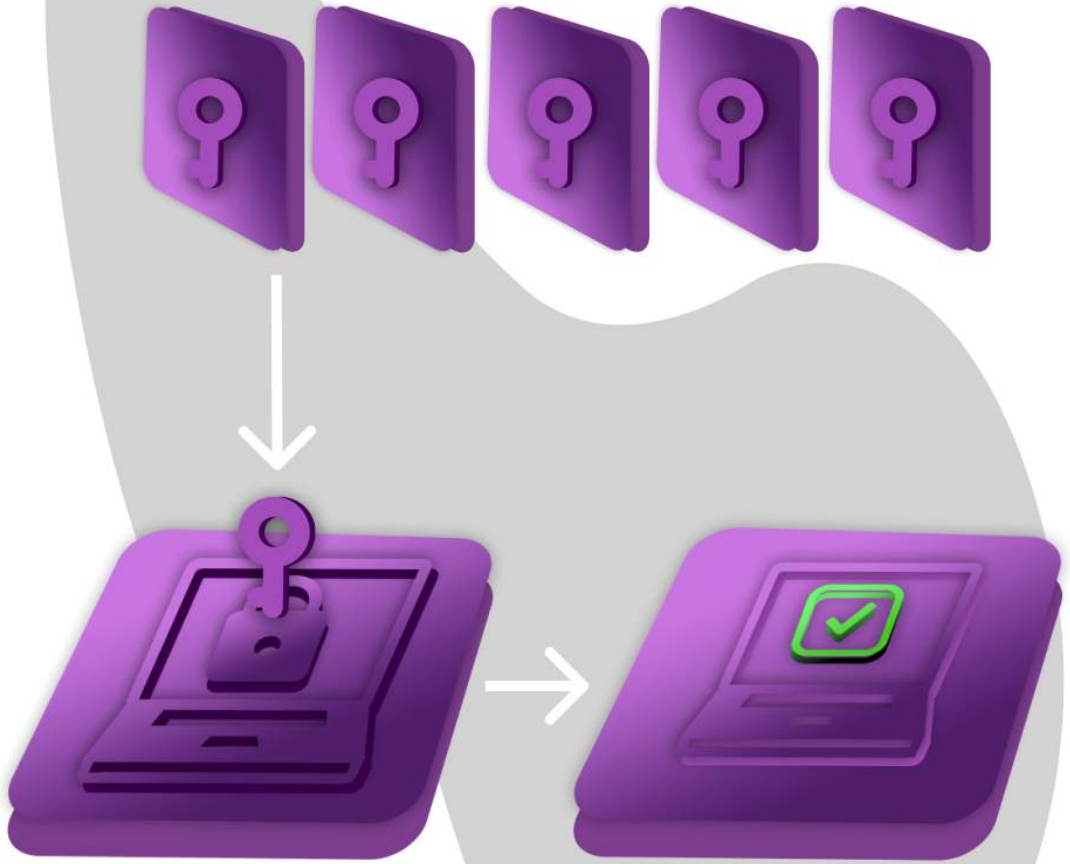


链中的每个块都有一个签名生成参数。为了参与区块的伪造过程，活动帐户使用自己的公钥对先前生成的区块进行密码签名。这将创建一个64字节的签名，然后使用SHA256对其进行哈希处理。产生的哈希值的前8个字节为您的帐户提供了一个命中数字。将该命中与当前目标值进行比较。如果计算出的命中低于目标，则可以生成下一个块。如目标值公式中所述，目标值每秒增加。即使网络上只有几个活动帐户，由于目标值会变得非常大，所以其中一个活动帐户最终也会生成一个区块。这样的结果是，您可以通过将帐户的点击值与目标值进行比较，来估算任何帐户强制执行屏蔽所需的时间。最后一点非常重要。由于任何节点都可以请求任何活动帐户的有效余额，因此可以遍历所有活动帐户以确定其各自的点击值。这意味着您可以以合理的准确性预测以下帐户将赢得哪些阻止假冒产品的权利。可以通过将注额移入将生成下一个区块的帐户来触发洗牌攻击，这是PZM赌注必须在1,440区块之前保持静止才能通过锻造（通过有效余额值）做出贡献的另一个原因。有趣的是，无法合理地预测下一个区块的新基本目标，因此，在尝试预测未来区块时，确定谁将迫使下一个区块的确定性过程变得越来越随机。

PRIZM

锻造算法

锻造PRIZM算法的这一功能有助于为透明锻造算法的开发和实现奠定基础。 当授予活动账户创建区块的权利时，它将最多255个可用的未确认交易组合到一个新区块中，并使用其所有必要参数填充该区块。 然后将该块作为区块链候选者传输到网络。
生成帐户的有效负载和每个块上的所有签名都可以由接收该帐户的所有网络节点检查。 在产生多个块的情况下，节点将选择具有最高累积复杂度的块作为权威块。 由于块数据分布在成员（对等方）之间，因此通过检查存储在每个fork中的链的累积复杂度，可以检测并拆除fork（未经授权的链段）。



PRIZM

PARAMINING

PARAMINING — 是PRIZM相对于其他加密货币的主要优势。 PRIZM开发人员添加了一种独特的线性回归机制，用于确定资金存储的奖励，以经济吸引力为目标，并逐步将全球所有现有金融工具替换为PZM，以形成基本机制。

也就是说，除了基本的锻造机制外，它不会增加系统中的资金量。 在PZM中，有一个附加的机制Paramining，它根据世界经济范围内标准化金融系统的标准数学发展指标，创建新硬币。 根据我们的计算，只有这样的硬币重量增长形式才能逐步和自信地替代所有现有的经济手段。

PRIZM

PARAMINING

根据以下三个主要参数计算使用ParaMining挖掘新硬币的比率：（1）个人钱包中的硬币数量，（2）随身钱包中的硬币数量（最多88个级别），以及（3）采矿难度系数。难度系数以百分比计算，与发行的硬币总数成正比。标准帐户的最大难度级别为**98%**，相当于生成了30亿个PZM。对于处于“保留模式”的帐户，最大难度为**97%**。根据其特征，Paramining是一种MLM 2.0系统，它消除了将简单的人推入网络业务的所有因素，但同时也使他参与了网络的开发，从而提高了个人进行硬币挖掘的速度。钱包。

在钱包中进行任何交易时，Paramining系统都会编写一个区块链，其中包含钱包所有者的硬币数量和其追随者的钱包中的硬币数量的值，此时，新的硬币会生成到钱包余额中。

HOLD - 将硬币保留在您的个人钱包中，无需进行任何交易，因此您可以减少挖掘硬币的难度并提高钱包的盈利能力。

HOLD

PARAMINING系统是促进和普及的最先进工具，因为它在任何现代加密货币中都没有类似物。 PARAMINING的主要优点是没有网络用户可以干扰此机制并伪造新硬币，所有用户都可以实时监控系统发行的硬币数量。 余额超过1PZM的任何钱包都可以使用PARAMINING，当余额达到100万PZM时，它将自动停止。

同样，第一次应用了不使用任何链接就建立引用链接的系统。 创建新钱包后，系统会捕获第一笔交易来自的区块链，并永久建立不可更改的推荐链，这使构建全球MLM网络变得容易，并提高了新硬币开采的速度。

由于对我们所有人来说，主要的工作不是创建100个“死”工具，而是创建具有良好支持和良好工作的工具，因此目前尚未详细描述技术实现。 如果揭示了我们的专有技术，那么肯定有人会尝试重复它，而这将无意间导致注意力分散，并且将此思想用于不是为了我们星球的崇高而重要的目标，而是为了我们没有实现的目标 知道并且不一定总是积极的着色意图。

PRIZM

PARAMINING 选项

要开始开采新的PZM，只需要一个可自动启动Paramining的硬币电子钱包。 此过程使您无需增加电费即可增加钱包中的硬币数量。

Paramining从1个硬币开始，到钱包里的1百万个硬币自动停止。

Paramaning —是一种由所有用户同时创建新硬币的独特方法，受以下三个参数调节：

1 - 您的个人钱包中的硬币数量
2 - 跟随者结构的硬币数量
3 - 开采难度 - Paratax

1 - 您的个人钱包中的硬币数量

Number of coins in personal wallet (PZM)	Daily profit	Monthly profit
从 500.000 至 1.000.000	0,33%	9,9%
从 100.000 至 499.999	0,28%	8,4%
从 50.000 至 99.999	0,25%	7,5%
从 10.000 至 49.999	0,21%	6,3%
从 1.000 至 9.999	0,18%	5,4%
从 100 至 999	0,14%	4,2%
从 1 至 99	0,12%	3,6%

2 - 追随者结构的硬币数量

Total Volume	Multiplier
从 1000 至 9999	2.18
从 10.000 至 99.999	2.36
从 100.000 至 999.999	2.77
从 1.000.000 至 9.999.999	3.05
从 10.000.000 至 99.999.999	3.36
从 100.000.000 至 999.999.999	3.88
1.000.000.000	4.37

Paramining原理基于“可见辐射”部分的物理基本定律。 像我们的宇宙模型一样，由于55秒钟的复杂重新计算兴趣，该系统一直在不断扩展，从而提高了速度。

PRIZM

PARAMINING OPTIONS

任何有余额的用户

从 1000 至 110 000 PZM

可以增加计算复利的期限，前提是他的余额涉及伪造。要开始保持期，您需要使用目标交易至少生成一个区块。保持期不能被进来的交易或收到锻造费打断。保持时间的持续时间不受限制，只要伪造者在100,000中产生至少一个块即可。

保持期被传出的交易中断。

PRIZM

开采难度

PARATAX

是生成硬币的难度的线性增加，表示为所有用户已经开采的硬币数量的百分比。

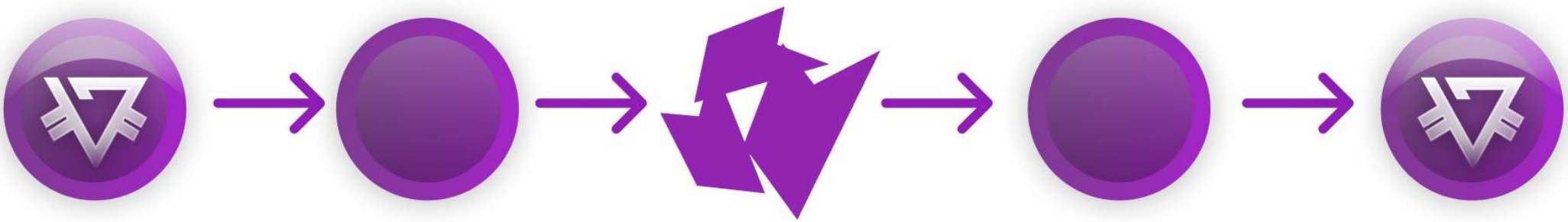
在生产30亿片时，PARATAX的最高限量为**98%**。PZM。

对于«**FORGERS**»，其在生成块时的余额不超过**110,000 PZM**，则PARATAX的最大值为**97%**

PRIZM

PRIZM帐户

Prizm在其设计中实现了一个智能钱包：将所有帐户的个人密钥存储在网络上，每个密钥都使用SHA256和Curve25519的组合直接从每个帐户的代码短语派生而来。 每个帐户都由一个64位数字表示，该数字使用错误所罗门代码更正表示为帐户地址，这使您最多可以检测到该帐户地址中的四个错误或最多纠正两个错误 。 出于对担心错误的帐户地址可能导致硬币，别名或资产不可逆转地转移到错误的目标帐户的担忧而实施此格式。 帐户地址始终以“ PRIZM-”开头，这使Prizm帐户地址易于识别，并且与其他加密货币使用的地址格式不同。



通　以下方式生成与秘密密　相关　的地址　　所　门

。

- 使用SHA256对秘密密码短语进行哈希处理以检索帐户的私钥。
- 使用Curve25519对私钥进行加密,以获得账户的公钥。
- 使用SHA256对公钥进行哈希处理以获得帐户ID。
- 帐户ID的前64位是可见的帐号。
- 编码所罗门代码，即带有前缀“ PRIZM-”的可见帐号，生成帐号的地址。

首次使用秘密密码短语访问帐户时，该帐户不受公钥保护。 从帐户进行第一次外发交易时，将从密码中接收的256位公共密钥存储在区块链中，从而保护了帐户。 公钥的地址空间（2256）大于帐号的地址空间（264），因此，码字与帐号不存在一对一的匹配，也不会发生冲突。 这些冲突的检测和预防方法如下：在使用某个密码短语访问帐户后，并且该帐户受到256位公共密钥的保护，其他任何公私密钥对都无法访问该帐户号码。

PRIZM

帐户余额的属性：

1 有效的帐户余额被用作为您的帐户计费的基础。
有效的帐户余额包括该帐户上固定的1,440块所有硬币。 此外，“帐户租赁”功能可让您在另一个期间内为另一个帐户设置有效余额。

2 保证的帐户余额包括固定在1440个单位的帐户上的所有令牌。 与有效的资产负债表不同，该余额不能分配给任何其他帐户。

3 基本帐户余额用于所有具有至少一项确认的交易。
提升帐户余额显示由于成功强制区块而收到的PZM总量。

4 未确认的帐户余额是Prizm客户端中显示的余额。 它代表经常帐户余额，扣除未确认的已发送交易涉及的硬币。

5 保证资产余额列表（列出）与特定帐户关联的所有资产的保证余额。

6 与特定帐户关联的所有资产的未确认余额和未确认资产余额列表。

PRIZM

WALLET.DAT

比特币和相关货币通常使用名称和钱包下的加密文件来存储生成的地址以接收硬币。 Prizm中使用的Next内核不会模拟此功能，但不会排除它。 客户开发人员可以实施一个系统，其中Prizm帐户的私钥组存储在加密的独立文件中。

交易确认

除非所有PZM事务包含在有效的网络块中，否则都将视为未确认。 新创建的区块由创建它们的节点（和关联的帐户）分发到网络，并且包含在区块中的交易被视为收到的一个确认。 由于将后续块添加到现有区块链中，因此每个其他块都会向交易确认数添加另一个确认。 如果事务在到期之前未包含在块中，则它将刻录并从事务池中删除。

交易定时

每个事务都包含一个截止日期参数，该参数设置为自事务发送到网络以来的分钟数。 默认情况下，截止日期为1440分钟（24小时）。 已发送到网络但未包含在区块中的交易称为未确认交易。

如果在交易截止日期之前该交易未包含在区块中，则将交易从网络中删除。 由于交易无效或失真，或者由于块中充斥着要支付更高佣金的交易，因此交易可以不予确认。 将来，诸如多重签名交易之类的功能可以将截止日期用作强制到期的一种手段。

PRIZM

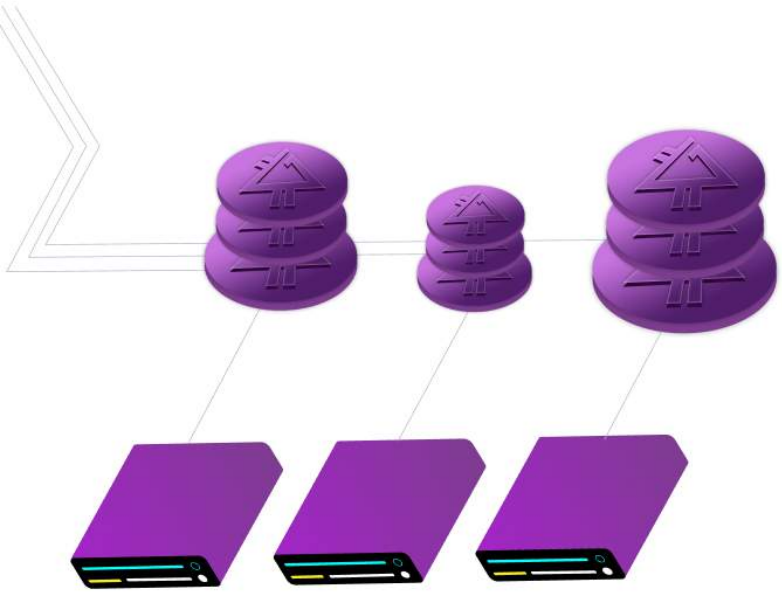
WALLET.DAT

交易创建和处理

有关创建和处理PZM事务的详细信息如下：-发送方指定事务参数。

事务类型发生变化，并且在创建事务时可以指定所需的类型，但是必须为所有事务指定多个参数：

- 发件人帐户私钥
- 交易截止日期
- 可选交易参考



PRIZM密码学的基本知识

Prizm中的密钥交换基于Curve25519算法，该算法使用Diffie-Hellman的快速高效椭圆形曲线（具有高度保护）来生成共享秘密。 该算法由Daniel J. Bernstein于2006年首次演示。接下来的Java实现由Evil医生在2014年3月进行了审查。Prizm中的消息签名使用椭圆曲线数字签名算法（EC-KCDSA）进行， 由KCDSA工作组于1998年由IEEE P1363a组定义。 选择这两种算法来平衡速度和安全性，密钥大小仅为32个字节。

主要特点

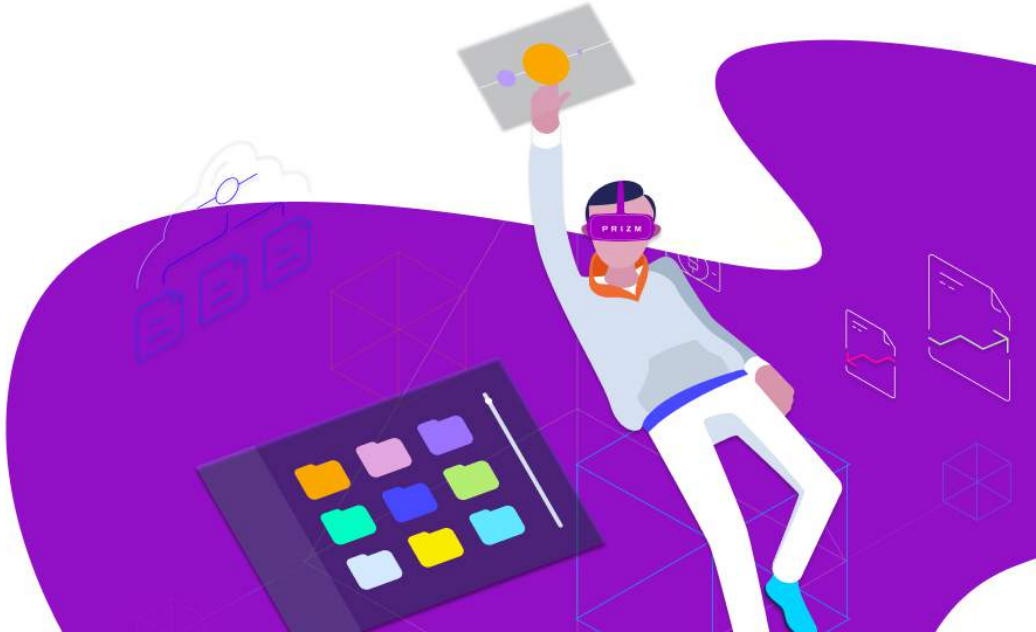
高级JavaScript客户端
第二代便捷的客户端应用程序已嵌入基本软件Prizm的发行版中，并且可以通过本地Web浏览器进行访问。 客户端为实施的所有主要Prizm功能提供全面支持，因此用户的私钥永远不会在线可用。它还包括增强的管理界面和用于Prizm低优先级应用程序编程界面的内置Javadoc文档。

便携式设备

由于其基于Java根的跨平台，权益证明的哈希值以及其减小区块链大小的未来能力，Prizm非常适合用于小型低功耗，低资源的设备。 Android和iPhone应用程序和软件已被移植到低功率的ARM设备，例如RaspberryPi和CubieTruck平台。 在智能手机等低功耗，始终连接的设备上实施Prizm的能力使我们能够提出一种在移动设备上支持大多数Prizm网络的方案。 与传统的加密货币“Proof of Work”相比，这些设备的低成本和资源消耗大大降低了网络成本。

基本付款

任何加密货币的最基本特征是能够将硬币从一个帐户转移到另一个帐户的能力。 这是Prizm交易的最基本类型，它使您可以使用基本的支付功能。



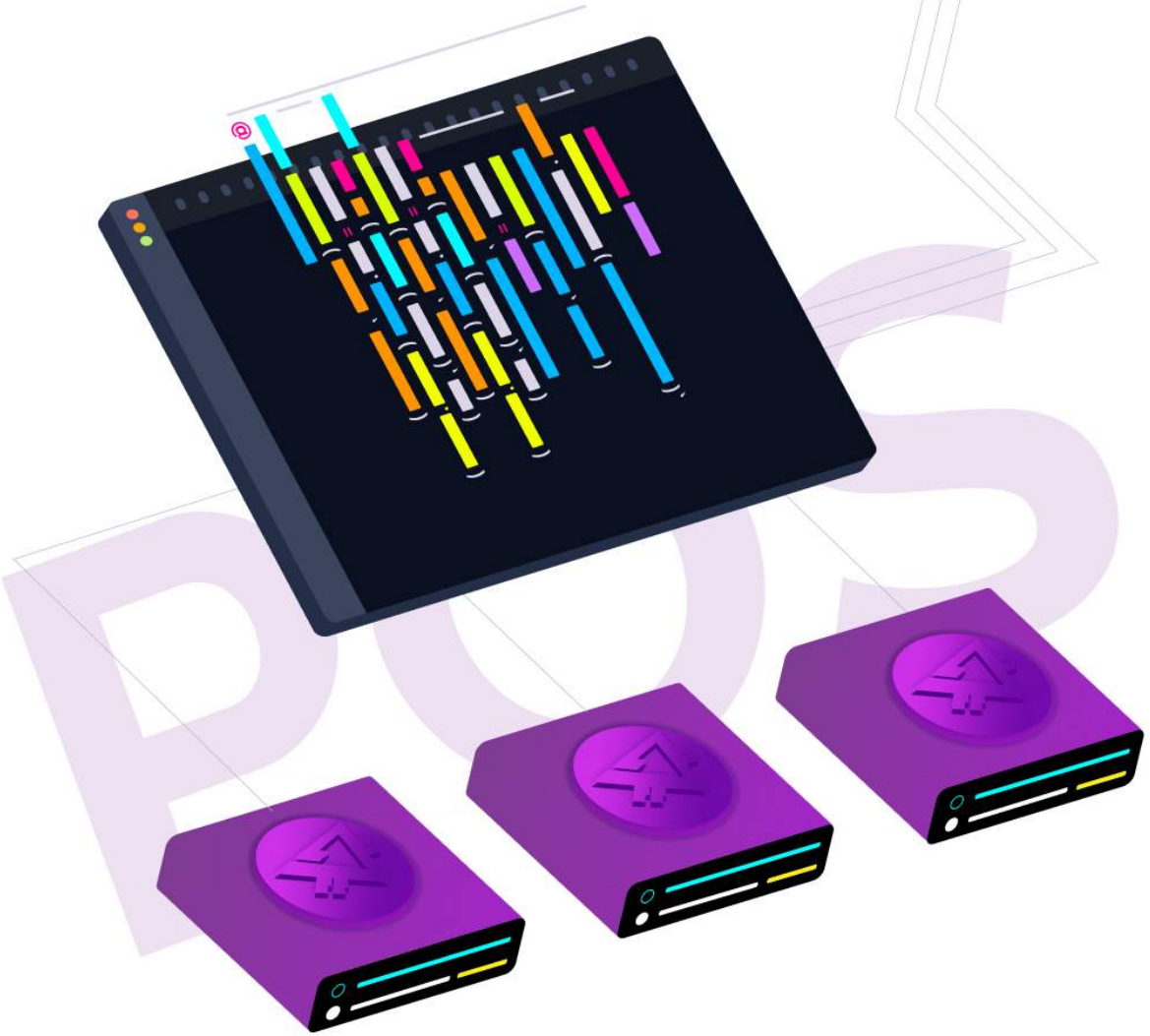
PRIZM

PRIZM关键功能

POS — 锻造打字

同时将Paramining +锻造这两种技术混合在一起。 源代码在一定时间内处于关闭状态（未加衬线），以防止出现克隆现象，从而确保系统保持液态。

伙伴关系计划88级结构
NEXT /密码系统的“Proof of stake”核心
用户友好的移动设备界面
用户密码未发送到服务器



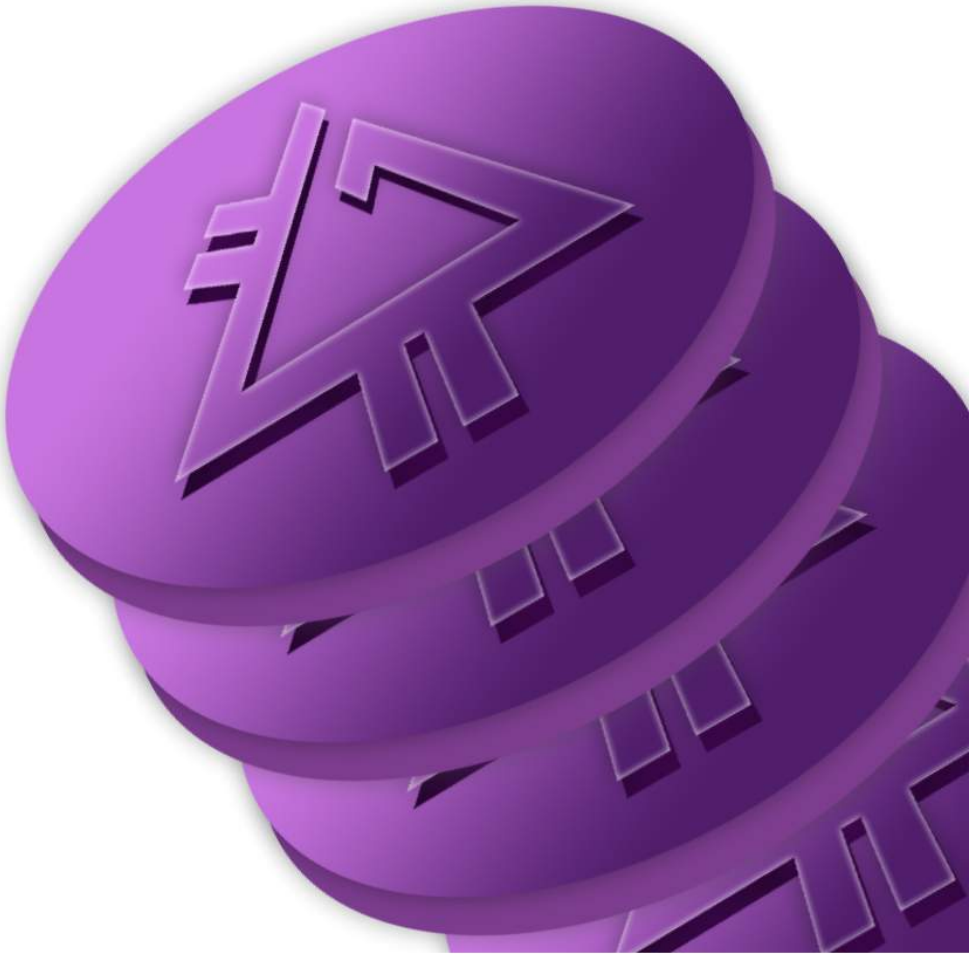
Nothing at stake

在“nothing is at stake”的攻击中，伪造者会尝试在他们看到的所有分叉之上构建块，因为这几乎不花费任何成本，并且因为忽略任何分叉可能意味着在分块上损失了如果该分叉会获得的奖励 被设计成为难度最大的连锁店。 尽管从理论上讲这种攻击是可能的，但目前尚不切实际。 Prizm网络不会经历漫长的区块链分叉，并且低区块的奖励并不能提供强烈的获利动机。 此外，以微不足道的利润牺牲网络安全性和信任度可能会使任何胜利成败。

攻击历史

在“对历史的攻击”中，某人获取了大量硬币，将其出售，然后在硬币被出售或交换之前试图创建成功的分叉。 如果攻击失败，则该尝试毫无价值，因为硬币已经出售或转让； 如果攻击成功，则攻击者会收回其令牌。 这种攻击的极端形式包括从旧帐户获取私钥，并使用它们直接从Genesis块构建成功的链。 在Prizms中，主要历史记录攻击通常会失败，因为所有下注都必须固定为1,440格才能用于锻造。 此外，每个区块产生的有效帐户余额将作为区块检查的一部分进行验证。 这种攻击的极端形式通常会失败，因为PRIZM区块链不能被当前区块高度后面超过720个区块重组。 这限制了不良演员可以建立这种攻击形式的时间范围。

应用



在Prizm中考虑的比特币问题。

Prizm被创建为一种加密货币2.0-对比特币的回应。 Prizm使用已在比特币中建立的功能，并考虑关注的方面。 该应用程序解决了由Prizm技术消除的比特币协议和网络问题。

区块链大小

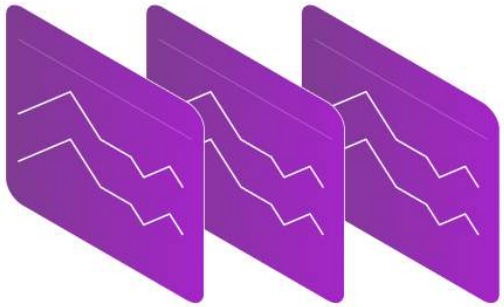
比特币区块链是所生成数据块的完整顺序集合，其中包含电子书，记录了自2009年1月发布以来发生的所有比特币交易。 四年后的2013年1月，比特币的区块链大小为4 GB，这是在DVD上存储两小时电影的大约数据量。 18个月后的2014年7月，比特币区块链的大小增加了近5到19 GB（GB）。37.比特币区块链正经历指数级增长，对原始比特币协议的修改将需要解决方案。

关于每天的交易

到2013年底，比特币网络中处理的交易数量每天最多达到70,000，即每秒约0.8交易（tps）。 当前的标准“比特币”块大小为1兆字节，平均每十分钟在“完全”客户站点上生成，将现有比特币网络的最大带宽限制为大约7 TPS。 将其与处理10,000 TPS的VISA网络的带宽进行比较，您会发现比特币无法像今天那样存在竞争。

PRIZM的答案

在当前状态下，Prizm每天可处理多达367,200笔交易，是当前比特币峰值的9倍以上。 透明伪造实现允许几乎立即处理事务，从而大大增加了该限制。



交易确认时间

2013年期间，比特币的交易确认时间大部分在5到10分钟之间。在2013年底宣布不允许中国银行处理比特币后，平均比特币交易时间显着增加，达到8-13分钟 ，具有19分钟的周期性峰值。 此后，确认时间从8分钟更改为10分钟。 但是，由于完成一次比特币交易需要几张支票（通常需要六次首选确认），因此在完成由比特币支付的资产的出售之前，很容易就可以经过一个小时。

PRIZM的答案

历史上显示，PZM的平均块生成时间约为80秒，并且平均事务处理时间相同。 经过十次确认，交易才被认为是安全的，这意味着交易将在不到14分钟的时间内成为永久交易。 透明锻造的实施允许您进行几乎即时的交易，这将进一步减少此时间。

集中化问题

比特币的复杂性增加和哈希率的组合给新移民带来了很大的进入壁垒，而现有采矿设备却降低了利润。鼓励比特币使用区块的激励措施导致了大型单层专门采矿设备44的创建，以及对一小套大型采矿池45的依赖。这导致了“集中化”的影响，其中大量采矿集中在控制越来越少的人员上。这不仅创造了比特币设计的绕过的权力结构，而且还提出了一个真正的可能性，即单个采矿作业或矿池可以在46个网络中获得总采矿能力的51%，并进行51%的攻击。还有一些攻击只需要网络总哈希能力的25%。 2014年1月上旬，GHash.io开始自愿降低自己的采矿能力，达到了51%的水平。几天后，池中的电量下降到网络总容量的34%，但是速度立即开始增加，并在2014年6月再次达到危险水平。

PRIZM的答案

Prizm中使用的“Proof of Stake”算法提供的激励措施提供了约0.1%的低投资回报率。 由于并不是每个区块都产生新的硬币，因此没有额外的“开采奖励”，这激发了人们共同创造区块的努力。数据显示，自成立以来，Prizm网络仍然非常分散： 唯一帐户的数量为网络增加了障碍。

Proof of Work - 保养费用

确认现有比特币上的交易并创建新的比特币进入流通需要巨大的计算能力，该能力必须不断工作。这种计算能力由所谓的采矿设备提供，这些设备由矿工管理。比特币矿工相互竞争，将下一笔交易添加到整个比特币链中。这是通过“散列”完成的-将过去十分钟内发生的所有比特币交易合并，然后尝试将其加密为一块数据，该数据块中也恰好有一定数量的连续零。哈希矿工生成的大多数试验块没有此目标零值，因此它们进行了很小的更改然后重试。十亿次尝试找到此“获胜”区块的尝试称为GH，而采矿装备则根据其每秒可执行的GH数量（以GH / sec表示）进行估算。获胜的矿工是第一个创建加密正确的比特币的人，他立即获得了25枚新比特币的奖励-撰写本文时的奖励约为15750美元。每十分钟左右一次，一次屡获殊荣的矿工之间的竞争。到2014年初，每天已产生3500多个比特币，相当于每天约220万美元。有了这么多赌注，矿工们支持采矿设备技术的快速军备竞赛，以提高获胜的机会。最初，比特币是使用中央处理器（CPU）（一种典型的台式计算机）进行开采的。然后提高专用图形处理单元（GPU）的已用芯片到高端图形卡的速度。然后使用具有可编程门阵列的微处理器（FPGA），然后使用专用应用集成电路芯片（ASIC）。 ASIC技术是比特币矿工的巅峰之作，但是随着不同世代ASIC芯片的问世，军备竞赛仍在继续。

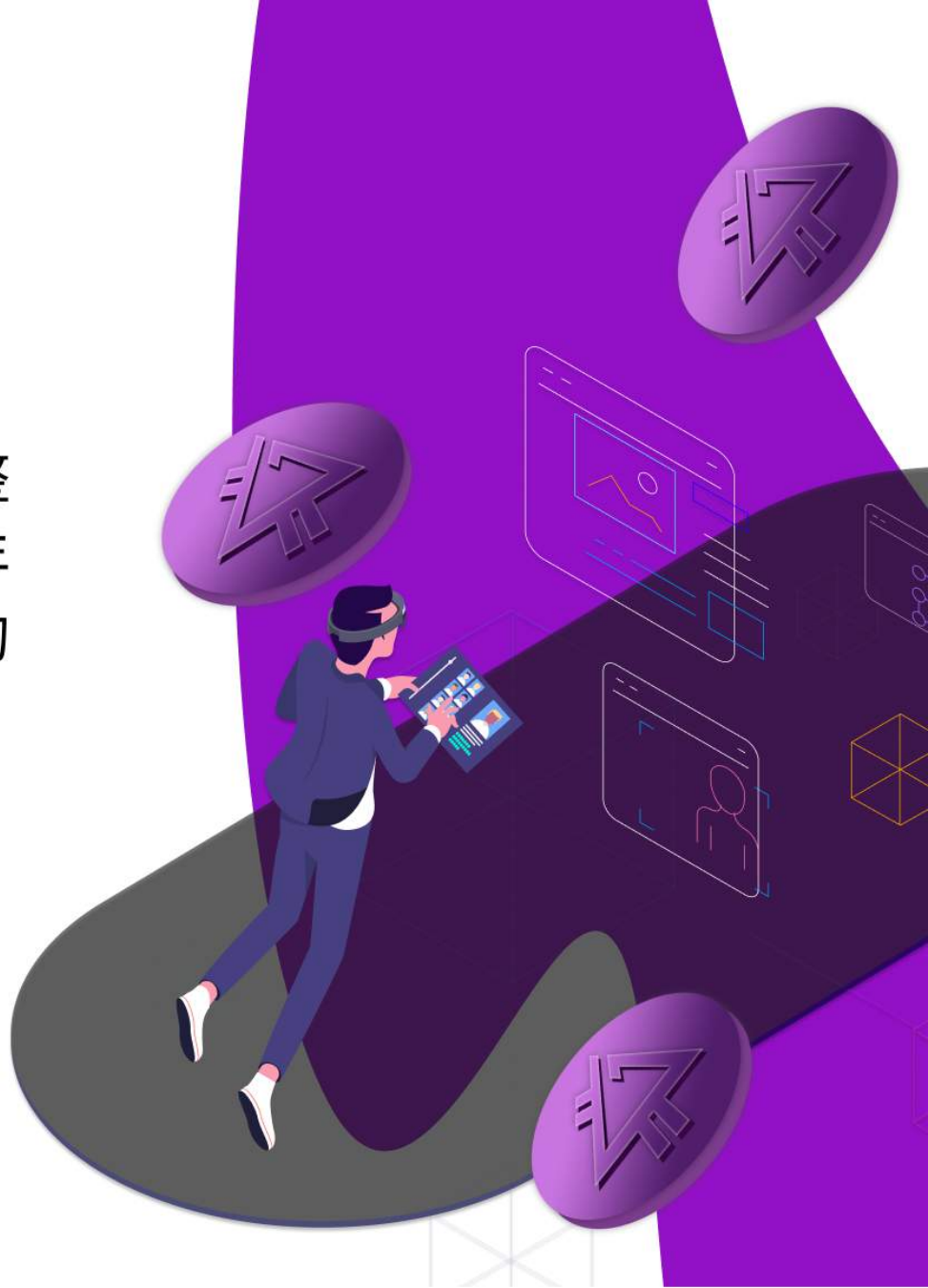
Proof of Work - 保养费用

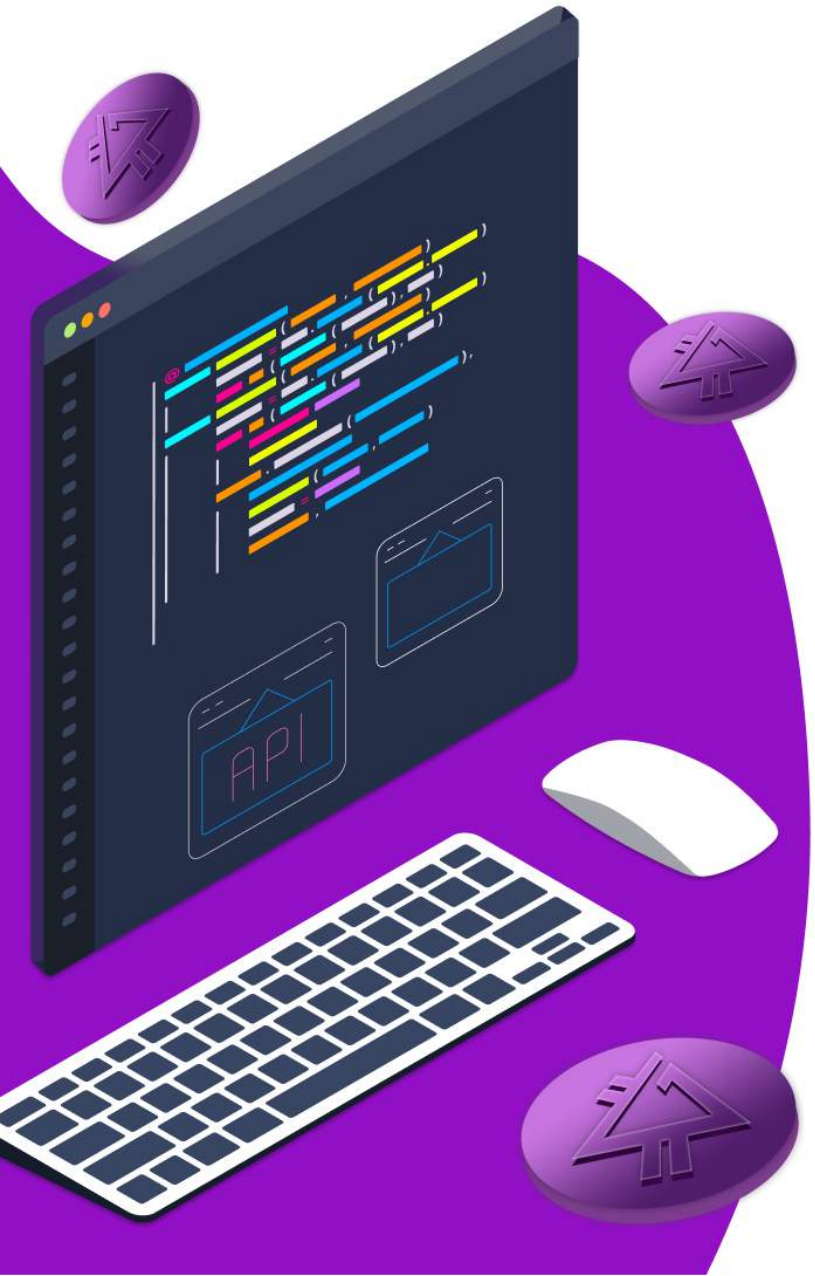
基于其微型晶体管的纳米尺寸，当前一代的ASIC芯片就是所谓的28 nm器件。到2014年底，它们应被20nm ASIC模块所取代。ButterflyLabs的28nm ASIC卡“ The Monarch”是一种最新的采矿设备，可提供600GH / sec的电力消耗功率为350瓦，价格为2,200美元。目前用于支持比特币当前运营的采矿设备基础设施引人注目。比特币ASIC与自闭症科学家相似-他们只能执行一块比特币的计算，仅此而已，但是他们可以超级计算机的速度进行一次计算。 2013年11月，《福布斯》杂志发表了一篇题为“全球比特币计算能力比500台组合超级计算机快256倍！”的文章。 2014年1月中旬，存储在网站blockchain.info上的统计数据表明，对比特币运营的持续支持需要约1800万GH / s的连续哈希率。在一天之内，这种散列能力产生了1.5万亿个试验区块，这些区块被比特币的蛋黄酱所产生和拒绝，以寻找一个-神奇的144个区块，将覆盖他们220万美元。几乎所有的比特币计算都不旨在通过对DNA建模或搜索来自E.T.的无线电信号来解决灾难。相反，它们被完全浪费了。与这种浪费的比特币背景支持相关的功能和成本是巨大的。如上所述，如果所有比特币采矿设备都具有“君主”级别，并且直到升级，它们才会出现。它们将代表30,000台机器，总价值超过6,300万美元。它在操作期间消耗超过10兆瓦的连续功率，每天的电费超过350万美元。对于当前实际上支持比特币的，效率较低的当前采矿装备库，实际数字要高得多。随着比特币从目前的每秒一笔交易跃升至目前的最高每秒七笔交易，这些数字现在正呈指数增长曲线。

Prizm解决方案

对Prizm网络的成本和能效的分析表明，整个PRIZM生态系统的维护成本约为每年60,000美元，这现在比运营比特币网络的成本便宜了将近2,200倍。

PRIZM.SPACE





与硬币持有人有关的 POW 维护成本

除了巨大的电费外，简单存储比特币还需要支付一笔隐性费用。 对于找到的每个区块，生成区块的人都会获得奖励。 在撰写本文时，这是25 BTC的奖励，这是今年比特币总供应量的10%的通胀。 今年，该人每获得1,000美元的比特币，便要支付100美元的比特币，以“支付”矿工的网络安全费。

愿原力与你同在

PRIZM整合

PRIZM支付系统是接收和发送加密支付的最简单方法。

您可以轻松地将PRIZM集成到您的项目，在线商店，交换器等中

在线教程：

https://pzm.space/en/pzm-integration/

Prizm支付系统集成

要开始使用PRIZM，您将需要启动网络节点（Node）和API_Servlet。

网络节点

该软件可以在一台服务器上运行，也可以在多台服务器上运行。 但是，为方便起见，最好在一台服务器上启动它。

首先，您应该启动节点并等待其同步。 下一步是配置PrizmAPIServlet模块。

PrizmCore钱包
https://github.com/prizmspace/PrizmCore#prizmcore-wallet-download-v1103-windows-osx-linux

简易API Gateway
https://github.com/prizmspace/PrizmCore#easy-api-gateway-prizmapiservlet

配置PrizmAPIServlet

存档中有一个名为 的文件

PrizmAPIServlet.properties

在行中

passphrase: NONE

而不是NONE，您应该编写将由您的项目使用的钱包的私钥。

填写完字段后，您应该通过以下方式启动servlet：

run-servlet.sh

在行中

sendkey: NONE

而不是NONE，您应该输入密码（硬币发送功能将使用该密码，以防止未经授权的交易）。

PHP实现示例

接收和发送硬币的工作描述，以及现成功能的示例和工作原理的描述。
Mysql数据库用于存储事务列表，下面是存储表的转储，以及与该表一起使用的代码示例（如果您使用QueryBuilder，就不会有问题）。

主要工作原理：

Cron任务 中有一个脚本，该脚本每2-5分钟向Servlet发出一次请求，以便它可以在商店的钱包中接收新交易。 收到交易清单后，您应该将它们保存到本地数据库中。
如果数据库中没有任何操作，则应运行不带任何参数的命令。 但是，如果您希望接收新交易，则应发送上次拥有的交易编号作为参数。

函数示例：

```php
<?php
function historyPZM($last_id = 0)
{
 if ($last_id) {
  $url = 'http://localhost:8888/history?fromid=' . $last_id;
 } else {
  $url = 'http://localhost:8888/history';
 }
 $page = '';
 $result = get_web_page($url);
 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }
 $array_new = array();
 $xcmorewrite = explode("\n", str_replace("\r", '', $page));
 foreach ($xcmorewrite as $value) {
  if ($value) {
   $array_new[] = explode(";", $value);
  }
 }
 return $array_new;
}
?>
```

检索页面内容的功能：

```php
<?php

function get_web_page($url)
{
 $uagent = "Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.14";
 $ch = curl_init($url);
         curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1); // 恢复网页
         curl_setopt($ch, CURLOPT_HEADER, 0); // 无法恢复标题
         curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1); // 跟随重定向
         curl_setopt($ch, CURLOPT_ENCODING, ""); // 处理所有编码
        curl_setopt($ch, CURLOPT_USERAGENT, $uagent); // 用户代理
        curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 20); // 连接超时
        curl_setopt($ch, CURLOPT_TIMEOUT, 20); // 答案超时
        curl_setopt($ch, CURLOPT_MAXREDIRS, 2); // 在第十次重定向后停止

 $content = curl_exec($ch);
 $err = curl_errno($ch);
 $errmsg = curl_error($ch);
 $header = curl_getinfo($ch);
 curl_close($ch);

 $header['errno'] = $err;
 $header['errmsg'] = $errmsg;
 $header['content'] = $content;
 return $header;
}

?>
```

检索页面内容的功能：

您可以通过控制台进行测试，例如：curl http://localhost:8888/history

用于接收新事务和表结构的Cron任务处理程序脚本示例

```
CREATE TABLE `pzm_history` (
 `id` bigint(20) NOT NULL,
 `tarif_id` int(1) NOT NULL,
 `tr_id` varchar(255) NOT NULL,
 `tr_date` varchar(255) NOT NULL,
 `tr_timestamp` int(11) NOT NULL,
 `pzm` varchar(50) NOT NULL,
 `summa` decimal(16,2) NOT NULL,
 `mess` varchar(255) NOT NULL,
 `status` int(1) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

** *所有必要的ID键和ID的自动递增应添加到表格中

处理程序：

在此示例中，您将收到应保存到本地数据库的新事务的列表。

因此，您保留了钱包中所有交易的历史记录，将来您将使用关键数据在我们的本地数据库中搜索它们。

```
<?php
$nomer = getLastPrmHistory();
$historys = historyPZM($nomer);

foreach ($historys as $item) {
   if ($item['0'] != "No transactions!") {

// 此行使用INSERT IGNORE将数据添加到“pzm_history”表中

PzmHistory::find()->insertIgnore([
        'tr_id' => $item['0'],
        'tr_date' => $item['1'],
        'tr_timestamp' => $item['2'],
        'pzm' => $item['3'],
        'summa' => $item['4'],
        'mess' => $item['5'],
        'status' => 0
      ]);
   }
}
```

```
function getLastPrmHistory()
{
// 此行搜索表中的最后一行以获取表中事务的最后一个ID

if (!empty($pzmHistory = PzmHistory::find()->orderBy('id', "DESC")->first())) {
  return $pzmHistory->tr_id;
 };
 return 0;
}

?>
```

您的项目必须使用相同的Prizm钱包，这就是为什么将为所有客户提供相同的补充内部帐户和相同操作的哈希ID的原因。 确保告知客户，他必须严格按照付款注释中指示哈希标识符的条件进行交易。

因此，应该有另一个过程，如果付款注释具有客户的哈希标识符，则该过程将分析新的传入交易并将硬币存入内部帐户。 另外，您还需要为客户端创建一个单独的“I PAID”按钮，单击该按钮后可以为该用户搜索和记录新交易。

次要功能和硬币发送功能

获取钱包的公钥（仅适用于具有余额的激活钱包）。

```
<?php

 function destinationPZM($pzm)
  {
     $url = 'http://localhost:8888/publickey?destination=' . $pzm;
     $page = '';
     $result = get_web_page($url);
     if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
        $error = $result['errmsg'];
        return '';
     } else {
        $page = $result['content'];
        $haystack = "Public key absent";
        $haystack2 = "Send error!";
        $pos = strripos($page, $haystack);
        $pos2 = strripos($page, $haystack2);
        if ($pos === false AND $pos2 === false) {
           $xcmorewrite = explode(' ', $page);
           $page = trim($xcmorewrite[0]);
           return $page;
        } else {
           return '';
        }
     }
     return $page;
  }

?>
```

接收钱包的当前余额：

```php
<?php

 function getBalancePZM($pzm)
  {
     $ip = '*******';  // 例 192.168.1.1:9976  带端口
 $url   =   'http://'.$ip.'/prizm?requestType=getAccount&account='   .
$pzm;
     $page = '';
     $result = get_web_page($url);
 //print_r($result); die;
     if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
        $error = $result['errmsg'];
        return '';
     } else {
        $page = $result['content'];
        $page = json_decode($page, true);
        if ( isset($page['balanceNQT']) ) {
          return $page['balanceNQT'] / 100;
        } else {
          return 0;
        }
     }
  }

?>
```

硬币发送的一些方法：

```php
<?php

public function payPZM($summa, $pzm, $public_key, $text)
{
 $p2 = SENDKEY;  // 这是您在设置过程中指定的密码
 $return = false;
 $url = 'http://localhost:8888/send?sendkey=' . $p2 . '&amount=' . $summa . '&comment=' . urlencode($text) . '&destination=' . $pzm . '&publickey=' . $public_key;
 $page = '';
 $result = get_web_page($url);

 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }

 if (preg_match('/^\+?\d+$/', $page)) {
  $return = true;
 } else {
  $return = false;
 }
 return $return;
}

?>
```

白皮书

PRIZM

数字货币的最初概念

Prizm白皮书修订版-2020年6月

PZM.SPACE