MAY, 2018

POSITION PAPER

V. 2.1

ENECUUM

May 2018	2018 年 5 月
Position Paper	立场文件
V. 2.1	2.1 版

目录

□

1. 摘要

货币对经济的关系，相当于言语对表达能力的关系：其通过自然的历史竞争成型，包含借用的特征，且在翻译过程中会丢失一些东西。语言的发展与其用户数量以及所说/所写/所读资料（即其中的“交易”）数量成正比。使其活着且免于灭绝的是其周转以及与达尔文主义相符的变化适应能力。大多数传统货币自然发展，如同大多数方言随着时间的推移经历了规范化并通过逐渐使用而取得了成功。尽管人造语言声称，由于精心策划特征以及诸如不规则动词之类残遗现象的乏官而能够取得全球性成功，但终于遭遇了失败。

既然我们已经进入了加密货币与区块链的世界，尽管它们也是一种人造语言，但很明显，所获得的变化适应能力是使平台成为首选交易手段的关键因素。许多有名的区块链具有僵硬与笨拙的设计，而 Enecuum 的区域链具有高度适应性与真正的分散性，参与者能够投票选择所需的新变化，而无需因此修改协议。同时，如果需要，还可以通过退出协议修改版引入经过调整的区块链参数。所有下述的技术说明共享相同的核心理念：我们相信通过增强的隐私性、安全性与可扩展性，且更重要的是通过改变与适应能力我们使 Enecuum 成为未来的区块链，其运用已成定局。

我们培养出**根深蒂固**的区块链。

2. 免责声明

本白皮书及与本白皮书相关的任何其他文件涉及 Enecuum 平台（“Enecuum”）的开发与使用意向，仅供参考，内容可能会有变化。

•本白皮书描述未来的项目

本白皮书包含前瞻性陈述，这些陈述基于一家香港注册公司（CR：2562183）Enecuum HK Limited（**“公司”**）的信念，以及本公司作出的某些假设及所获得的信息。

本白皮书中设想的 Enecuum 处于开发过程中，目前不断予以更新，更新内容包括但不限于关键治理与技术特性。ENQ 代币（**“ENQ”**）包括并涉及到实验平台（软件）与技术的开发与使用，这些平台与技术可能无法实现或达到本白皮书中规定的目标。

一旦 Enecuum 得以实现，其可能与本白皮书中描述的网络有很大不同。对于任何计划、未来预测或前景的实现或合理性，不作任何陈述或保证，且本文件中的任何内容均不视为或不应视为对未来的承诺或陈述而对此依赖。

•不提供受监管产品

ENQ 不旨在代表任何司法管辖区的证券或任何其他受监管产品。

本文件不构成证券或任何其他受监管产品的要约或招揽，也不构成为投资目的而进行的推介、邀请或招揽。购买条款并非旨在提供金融服务的要约文件或任何形式的招股说明书。

ENQ 不代表本平台或软件或本公司或与平台相关的任何其他公司或知识产权或任何司法管辖区的任何其他公共或私营企业、集团、基金会或其他实体的股权、股份、单位、特许权使用费或对资本、利润、回报或收入的权利 。

•本白皮书不构成建议

本白皮书不构成购买 ENQ 的建议。在任何合同或购买决定中，不应依赖于本白皮书。

•风险警告

购买 ENQ 与参与 Enecuum 会带来很大的风险。

在购买 ENQ 之前，您应该仔细评估并考虑风险，包括任何其他文档中列出的风险。

•本公司意见

本白皮书中表达的意见与观点是 Enecuum 的意见与观点，并不反映任何司法管辖区内任何政府、准政府、权力机关或公共机构（包括但不限于任何司法管辖区的任何监管机构）的官方政策或立场。

本白皮书中包含的信息基于本公司认为可靠的来源，但无法保证其准确性或完整性。

•英文是本白皮书的授权语言

本白皮书及相关材料仅以英文发布。任何翻译仅供参考，未经公司或任何其他人认证。在此无法保证任何翻译版的准确性与完整性。一旦本白皮书的翻译版与英文版之间存在任何不一致之处，则以英文版为准。

•没有第三方关联关系或认可

本白皮书中对特定公司与平台的引用仅用于说明目的。使用任何公司与/或平台名称与商标并不意味着与任何一方有任何关联或认可。

•您必须获得所有必要的专业建议

在确定是否购买 ENQ 或以其他方式参与 Enecuum 网络之前，您根据需要应咨询律师、会计师、税务专家与/或任何其他专业顾问。

3. 简介

自从比特币于 2009 年创立以来，其以来的区块链技术为世界经济演变开辟了新的前景。随后出现的智能合约使得按预先确定的条件下进行可信的自动交易变成可能，从而大大扩展了区块链技术的应用潜力。我们认为，区块链能够对诸如贸易、金融市场、投票乃至物流等金融与经济活动的许多领域带来翻天覆地的变化。

如今，几乎所有领先的机构都在竞相开发最佳解决方案。大型银行与集团公司正在组建团队，而各国政府正在寻找方法来创建适当的法律框架来支持该技术。

现有的解决方案中，以太坊最具代表性，已经为区块链技术与智能合约的组合应用提供了充足的机会。 然而，为了进一步发展与大规模普及该技术，有必要克服许多问题，这些问题可归纳为三大类：可扩展性，安全性与隐私性。

3.1. 可扩展性

分散式区块链系统的缺点是其带宽有限。

事实上，分布式账本使用的大多数现有的共识建立机制努力摸索着在每秒大量交易与网络集中程度之间的权衡[1]。在此，增加所处理交易数量的愿望经常导致与系统可靠性相关风险的增多。此外，随着区块链规模的增长，需要更大的磁盘空间、更强的互联网连接与更高的计算能力。所有这些都可能导致全节点数量的减少，并对整个网络的安全性产生负面影响（参见 5）。

3.2. 安全性

除了与可扩展性相关的问题之外，区块链架构本身的各种特征还会产生许多隐患。例如，基于工作量证明的交易确认机制会导致某个地方的挖矿能力高度集中：例如，的比特币挖矿能力聚集在中国大陆，因其电力成本属于世界上最低者之一。

这一事实极大增加了与系统集中化相关的各种风险，例如，进行“51%攻击”的机会。

安全性的另一个威胁出现在智能合约上，这些合约比区块链本身更容易发生漏洞与错误，并且已经导致数百万美元的用户损失以及行业损害。我们预计所使用的智能合约数量将继续增长；然而，现有的识别其弱点的方法仍然不足。

如今，另一个亟待解决的问题是集中化对区块链方向与控制的影响。如果权力集中集中在对核心协议能进行修改的一小群人手中，就可能出现这种情况[2]。如果这些群体的意见与社区的利益相抵触，这可能会导致冲突，这种冲突可能完全停止为区块链稳定发展所必需的制度现代化进程，甚至可能导致社区与区块链的分裂（ 参见 5）。

3.3. 隐私性

一些区块链系统力求实现所有交易的透明度。但是，我们认为，此功能限制了其商业吸引力并侵犯了个人隐私。虽然透明度是分布式登记薄的主要优势之一，但并不总是需要此属性，尤其是涉及到业务各方之间的转让、特定金融交易以及用户可能合法希望维持隐私与保密的其他类型的交易。

我们认为，正在处理数十个不同项目的许多开发人员现在都面临着这些问题。因此，每天都会设计越来越多的临时区块链平台来解决各个领域的特定任务。这给我们带来了又一个问题，涉及到不同类型的分布式网络之间的互操作性。几个交叉链项目已经启动，以解决这个问题。

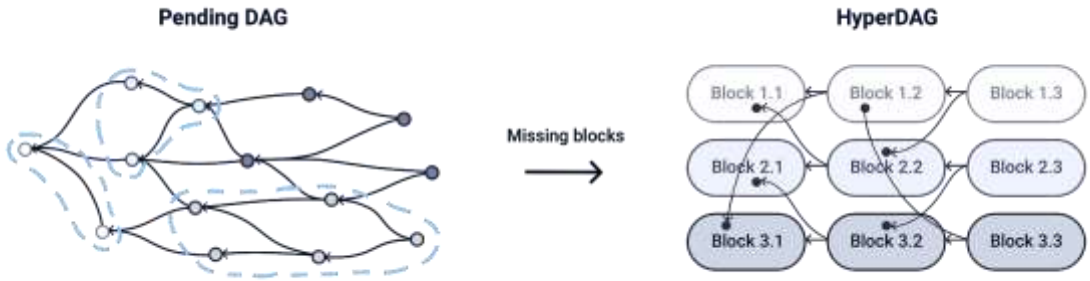
然而，尚未提出一个协议中有效解决上述问题的通用解决方案。 我们相信，其解决方案是 Enecuum，这是一种基于全新结构的区块链系统，可以在日常生活中充分发挥分布式登记薄技术的所有优势（参见 5）。

4. 产品说明

Enecuum 被设计为下一代分散式区块链平台，具有独特的特征，有能力帮助实现大量安全且可扩展的区块链服务与分散式应用程序。

与其他平台相比，Enecuum 的核心优势之一是 HyperDAG。这是一种用于存储与编写交易的数据模型，具有灵活的设置，为区块链技术的实际应用提供了新的机会。 HyperDAG 支持创建单独的

分支，其中可以定制规则以解决许多潜在的业务问题，包括以低成本快速处理大量交易的能力。此外，该解决方案允许将能够顺利解决可扩展性问题的“分片”技术集成到其中。



Pending DAG	待决 DAG
HyperDAG	HyperDAG
Missing blocks	缺乏区块
Block 1.1	区块 1.1

图 1.待决 DAG 作为 HyperDAG 的一部分

Enecuum 使用混合式一致性算法，将工作量证明（**“PoW”**）[3]、权益证明（**“PoS”**）[4]与行动证明（**“PoA”**）[5]算法相结合，作为其共识机制的一部分。*建议通过 Enecuum 在现实世界环境中首次应用 PoA*。 利用共识机制的组合，可以从连接到网络的几乎任何一种设备确认交易。这又带来系统尽可能的分散化，意味着 Enecuum 可能对各类的攻击具有高度抵抗力。

Enecuum 开发了“SHARNELL 智能合约”[20]以在 Enecuum 平台上运行。这些合约完全由公式与面向业务的线性逻辑组成。 SHARNELL 智能合约旨在为 Enecuum 的高安全级别做出贡献。

线性逻辑允许在智能合约发布到系统之前对其进行可靠的自动验证，我们相信这可以显着降低系统中潜在的漏洞、误用、冻结、僵局与其他不良后果。

Enecuum 系统的一个优点是其高度适应能力。用户可以参与到其开发并为其他参与者关于改进系统功能的建议进行投票。有两种方法可以引入系统参数的变化：

- 在 GitHub 项目存储库进行分支并提供协议的修改版（很可能由经验丰富的开发人员使用）；或者
- 投票调整任何不需要协议修改的网络参数。

后者的能力由系统架构提供，并且可以由 ENQ 的所有持有者使用，ENQ 是按设想在 Enecuum 上运行的原生加密数字代币。在测试期之后，按照设想投票算法予以开放，供用户提出 Enecuum 共识模型的变化。在测试期间，Enecuum 团队建议保留对协议的控制权，以便进行测试与调试。

Enecuum 是使用 Haskell 开发的，Haskell 是一种编程语言，具有执行的稳定性与副作用的低可能性等特征。 已选择 Cryptonight 的自定义版本 [6]（Keccak + AES + X11）作为核心加密协议，因为它对专用集成电路（“ASIC”）设备具有高抗性。

ENQ 是 Enecuum 的原生代币。 按照设想，ENQ 根据系统特定参数生成，并支付给矿工作为利用计算能力的奖励。ENQ 可以免费接收与发送，还可以用作向网络发布智能合约、在智能合约上执行复杂数学计算、创建自定义宏块、新代币与分支以及参与 PoS 挖掘的付费。

4.1. 交易

在我们看来，在分布式登记薄中存储交易有两种广义方法：

- 作为区块（比特币、以太坊与许多其他）；与
- 作为有向无环图（“DAG”）——（IOTA、Byteball、Universa）。

前者的优点是其高可靠性，这是通过网络中所有节点之间的 100%登记薄复制来实现的。但是，该方法对网络速度与可扩展性施加了某些限制。在后者即 DAG 中，没有区块，并且每个新进的交易会指向多个先前的交易，以之有效验证。因此，此类登记薄可以快速处理大量交易，但其安全级别引起了社区的某些忧虑[12]。

我们致力于将这两种方法结合起来，并创建称为“HyperDAG”的全新交易记录方法。其与 DAG 的主要区别在于，进入系统的交易不仅可以引用单个先前的交易，还可以引用位于区块中的一组交易（图 2）。通过这种方式，HyperDAG 顺利容纳了两种方法的优点，同时弥补了上述实质性缺陷，因此其能够每秒处理数千个交易，同时具有高级别的加密保护以防止攻击。

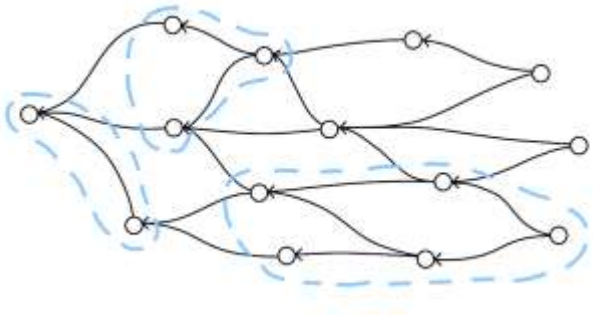
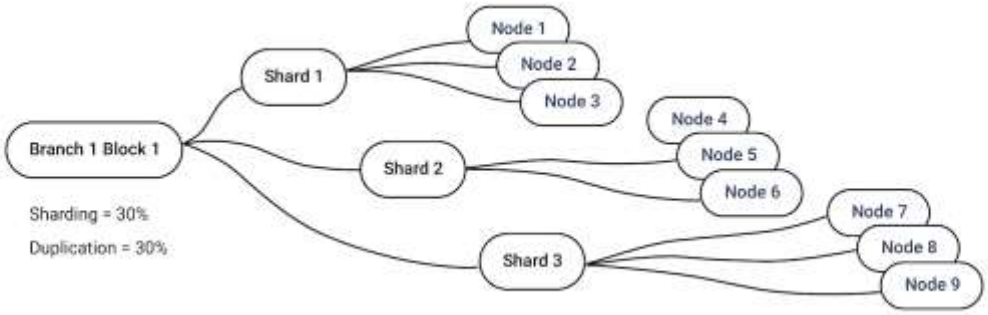


图 2. HyperDAG 的原理：相邻交易被组成区块

这种表示交易的方法为交易分类、分析与抽样提供更大空间。例如，可以在一个网络中创建不同的分支（区块链），并且还应用分片技术来提高网络速度并消除所有节点之间 100%登记薄复制的需要。



Branch 1 Block 1	分支 1 区块 1
Shard 1	分片 1
Node 1	节点 1
Shadring = 30%	分片比重 = 30%
Duplication = 30%	复制比重 = 30%

图 3.分片

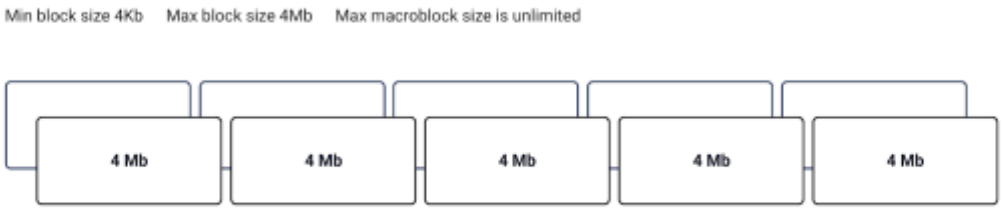
按设想，在 Enecuum 中，交易有几个参数：复制、分片以及服务质量（称为**“QS”**，此中是指交易速度）。 复制增加系统的整体安全性，但降低网络速度。 分片产生相反的效果。默认情况下，复制为 30%，分片为 30%，QS 为无。

更改这些设置的选项旨在允许轻松扩展以及在系统的各个分支内创建独特服务。

4.2. 区块

当 HyperDAG 累积足够数量的交易以开始组装区块时，区块的创建过程就启动。通过分析每个交易的特定参数，矿工确定其对系统的价值并将其添加到相应的区块中。由于引入了先前交易[MD1]的双哈希链接，可以同时挖掘包含不同交易的多达 n 个区块，这实质上*以 n 倍*加速了交易吞吐量。 n 的限制是动态的，例如可以是 *1000*，每秒产生 *1000 x 62 x 40 = 2,480,000* 个交易，其中 40 是最小区块中的最大交易数，62 是 PoA 团队中验证交易的设备数（团队中共有 64 个成员），1000 是同时挖掘的区块数。

在 Enecuum 中，按照设想，区块的规模没有固定值，可能从 4 KB 到 4 MB 不等。实质上，可以创建最小规模的区块以达到每个操作最小速度延迟，并且随着网络负载的增加，区块的规模也会增加。在用户需要大于 4 MB 区块的情况下，系统还支持将任意数量的区块组合成宏块，从而允许在区块链上存储大量数据。



Min block size 4Kb	区块最小规模为 4Kb
Max block size 4Mb	区块最大规模为 4Mb
Max macroblock size is unlimited	宏块最大规模无限

图 4.区块的规模可变性

按照设想，比特币-NG 协议被引入到 Enecuum 宏块中[12]，以减少区块创建之间的延迟，从而实时创建宏块内的每个微块，并在其到达时立即将交易添加到区块链中。通过这种方式，我们不必等到宏块完成、找到其哈希、其在网络上的所有节点中实现同步——相反，微块可以在宏块内同时生成。

在结构上，一个区块由 3 个主要部分组成，如下图所示：

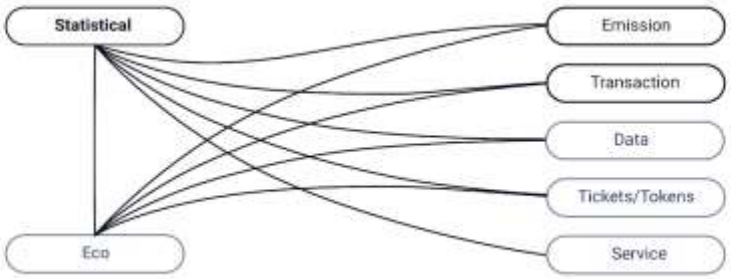
Header	标头
Meta info	元数据
Solver’s pub key	解决者的公共钥匙
Hash link	哈希链接
Payload	有效载荷
Part of the DAG	DAG 的一部分
Finalize	最终确定
Solver’s signature	解决者签字
Statistical info	统计数据
Etc	其他

图 5.区块的结构

4.3. 分支

使用 HyperDAG 存储与实现交易可以创建仅包含同类交易的分支（区块链）。 实质上，每个分支都是一个单独的区块链，同时也是整个系统的一部分。每个分支可以规定其特定规则来创建与验证新区块。节点不必复制所有 Enecuum 辅助性分支。

示意性地，按分支安排区块的过程在图 6 中所示。



Statistical	统计
Eco	生态
Emission	发行
Transaction	交易
Data	数据
Tickets/Tokens	门票/代币
Service	服务

图 6.将不同的区块安排到不同的分支

按照设想，该系统的主要分支如下：

1. 交易分支：旨在包括 ENQ 用户之间的所有普通交易。

2. 发行分支：旨在包括产生新 ENQ 作为挖矿奖励的交易。

3. 统计分支：旨在积累与分析系统运作的统计数据。此分支包含有关节点总数、挖矿记录、区块规模以及多个其他参数（包括 PoA 挖矿奖励规模）。

此外，按照设想，Enecuum 支持创建下述的其他分支：

1. 生态分支：旨在发现验证失败的可疑操作与交易。例如，如果新创建的钱包发送异常大量的外发交易，这些交易先进入生态分支进行详细分析。

2. 票证分支：旨在通过门票实现不同场景的机会。门票用于允许创建与访问专用的区块链分支，我们将其称为“票证分支”（参见 4.6）。例如，如果用户创建门票并在该票证分支上发行代币，则涉及此门票的所有操作都可以加密并存储在此专用分支中。此外，这些票证分支可以具有其自己的规则，例如，所有节点都可以被视为有效，来自它们的交易可以更快地处理，因为不需要所有网络成员之间的共识。

3. 服务分支：旨在提供分散的服务，例如，用于投票、调查、即时通讯、文档管理等。服务分支中的交易可以包括附加信息，从而达到足够高的灵活性，以将区块链运用到许多业务问题的解决。

4. 数据分支，可以作为分散的存储库。基本原理与 BitTorrent 协议类似，但是，Enecuum 不是传统的哈希法，而是提出自己的解决方案——无缝哈希算法，旨在允许对加密文件中任何大小的部分进行授权访问，而无需再次在节点之间二度哈希与分享哈希表，这在 BitTorrent 中无法实现。

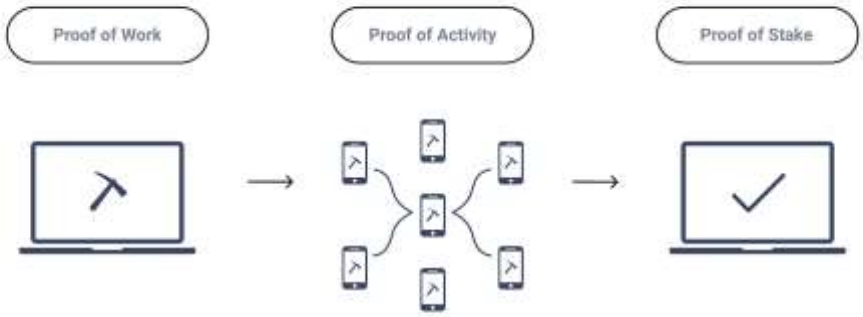
4.4. 混合共识算法（PoW、PoA、PoS）

在 Enecuum 中，建议通过以下三种挖矿算法之间的相互作用来实现共识：工作量证明（**“PoW”**），行动证明（**“PoA”**）与权益证明（**“PoS”**）。 通过这种组合可以实现高度的网络分散，同时显着提高网络安全级别与速度。

按照设想，在 Enecuum 中实现的交易验证过程可以大致分为对应于上述算法的 3 个阶段。

第一阶段：

第一阶段有两种方法。常规方法是，连接到 PoW 网络的矿工并行地计算不同规模的区块的哈希，各个针对其相应的块。在找到满足其复杂性当前要求的哈希之后，矿工用交易填充该块并将其转移到网络中，以用于涉及 PoA 矿工交易验证的第二阶段。 第二种方法是让 PoW 矿工计算哈希值，创建一个宏块并保持开放状态，以便 PoA 矿工团队用包含交易的微块填充该宏块。



Proof of Work	工作量证明
Proof of Activity	行动证明
Proof of Stake	权益证明

图 7.混合共识算法

第二阶段：

在第二阶段中，分成小组的 PoA 矿工与所选择的 PoW 方法相对应。在上述第一个 PoW 方法的情况下，他们检查转移区块标头中的哈希并验证区块中的交易。在第二种 PoW 方法的情况下，他们检查转移区块头部中的哈希并，创建微块，用交易填充微块，并将其发送到 PoW 矿工的宏块。整体上，一个团队向宏块发送 62 个微块，每个微块包含 40 个交易。然后，根据区块中包含的交易，PoA 矿工将其附加到系统的某一个分支。检查区块哈希的正确性不需要很大的计算能力，甚至可以通过包括移动电话在内的简单设备来执行该操作。

这同样适用于微块创建、填充交易以及交易验证。 PoA 团队形成过程涉及到计算哈希以进入团队。每个团队最多可以有 64 个参与者，并根据对几个参数的分析进行组织，包括节点的地理位置与其他参数，以达到最高的共识安全级别。

第三阶段：

在第三阶段中，PoS 矿工不断重新检查系统中所有钱包的余额。按照设想，PoS 矿工进行这种活动应按发行百分比获得部分挖矿奖励。奖励根据两种方式取决于矿工的余额：第一，系统确定获得奖励所需的余额上限与下限，在此范围之外矿工无法获得任何奖励，第二，奖励随着 PoS 矿工的余额从下限增长到上限而增加。

与网络在发现有效区块后立即生成新币的现有奖励方法相比，Enecuum 在此阶段发布添加到钱包余额的标记（参见 4.6），而实际挖矿支付平均每日执行一次。通过这种方式，系统受到保护以免受对挖矿算法的可能攻击以及获得对大多数计算能力控制的试图（例如通过 ASICS）。

默认情况下，挖矿奖励在参与者之间按如下比例分配：PoA - 70%，PoW - 20%，PoS - 10%。但是，统计分支（ 参见 4.3）的存在使系统能够控制这种分配方案，保护其利益免受可能的滥用。

4.5. SHARNELL 智能合约

Enecuum 中的智能合约建议用 JavaScript 编写并在 Google 的 V8 引擎上执行。系统支持两种类型的合约：

1.“轻型”（逻辑）智能合约，建议仅由数学公式组成，并基于面向业务的 SHARNELL 线性逻辑。线性逻辑是完全可预测的，因此可以将潜在漏洞的可能性降至最低。

按照设想，逻辑智能合约由包含条件与参数的“数据卡”以及公式本身组成，其中的公式考虑到上述条件与参数、其可能完全或部分达到与实现。根据设想，将逻辑合约的每个条件放在数据卡中并分配相应的符号。

之后，创建完全反映合约条款的数学公式。π 演算系统用于确保计算并行运行。

这种智能合约非常适合执行最常见的操作与交易，例如多重签名技术、托管等。建议在我们系统的第一个版本中，它们将通过基于 Petri Nets 的图形编辑器创建。

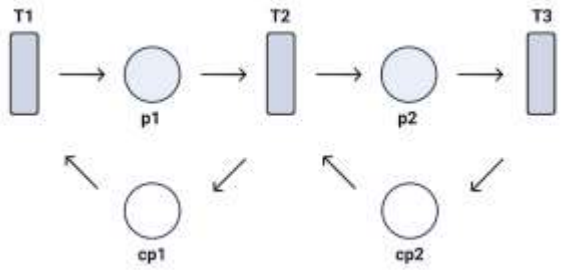
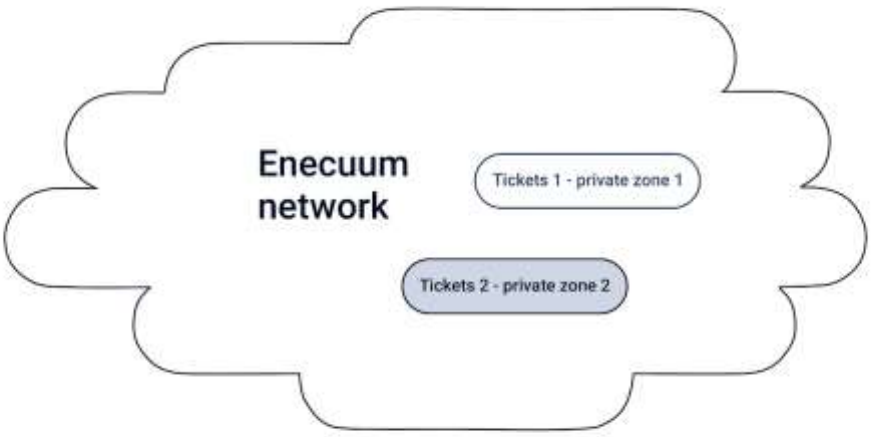


图 8.智能合约

2.“重型”智能合约按设想包含用于解决更复杂问题的代码，例如进行科学计算与训练神经网络。这些在系统的专用分支中执行，并支付计算费用。 建议用 ENQ 按用户定义的费率给出这种计算的付费。还建议其使用 π 演算系统，并使用会话类型的频道系统。

4.6. 门票与标记

如前所述，Enecuum 旨在支持“门票”（也称为“票证”，如适用）的概念。 票证是加密代理用品，类似于代币，可以由系统的任何用户创建。门票用于创建专用分支，其中没有意向进行 ENQ 流通。门票既用作相应分支的访问密钥，也用作该分支中交易的解密密钥，并且可以在 Enecuum 的用户之间自由转交。



Enecuum network	Enecuum 网络
Tickets 1 – private zone 1	门票 1 ——私人区域 1
Tickets 2 – private zone 2	门票 2——私人区域 2

图 9.门票与票证分支
（全球 ENQ 网络，票证分支＃1，票证分支＃2）

门票可以是相应票证分支中接受的交易媒介。建议通过相应的门票将这些代币转换为 ENQ。

票证分支的主要目的是促进创建基于区块链的灵活环境，以便企业与客户之间轻松互动。

“标记”是另一种旨在扩展 Enecuum 功能的工具。标记用于对代币、交易或钱包添加标签，并不作为单独的单元存在，仅能与支付单元结合。标记用于表示所标对象的特定功能，并确保严格执行规定的术语或特定任务。 按照设想，标记是最终的，不可逆转的，其不能改变，并在创建之前确定。

Enecuum 旨在提供以下类型的标记：

• 交易加速标记促进更高的交易速度。

• 验证报酬标记在统计分支中的数据累积后转换为 ENQ（参见 4.3）。

• 代币标贴标记对付款单元强加自定义规则集，例如，限制适用于标记单元的操作列表，并说明其只能转移到包含相应标记的钱包。此功能可以帮助有效管理预算、实施购买控制并协助定向贷款管理。

5. 问题与解决方案

5.1. 可扩展性

开放式区块链系统面临的最重要的热门问题之一是便宜且安全地促进大量交易。可扩展性是全球范围内采用该技术的必要条件。比特币与以太坊的吞吐量通常与能够处理每秒超过 50,000 次操作的 VisaNet 系统进行比较[14]——比大多数流行的加密货币的当前吞吐量高出数千倍。鉴于加密货币用户数量以极快的速度在全球范围内增长，当前分散系统中交易高峰时间的费用可能达到令人望而却步的水平。

我们认为，区块规模的简单增加是该问题的部分与临时解决方案，但这种方法不能解决潜在的可扩展性问题。目前，区块中的数据永久存储在那里，这意味着区块链的规模将保持持续增长。随着吞吐量的增加，其规模将以更快的速度上涨。因此，只有大公司才能够分配足够的资源来存储与更新这个庞大的数据集，这可能会导致网络的集中化。

由于使用 HyperDAG（参见 4.1）来记录与存储交易，我们认为 Enecuum 非常适合于实现分片技术，该技术允许将区块链分成几个并行处理的较小部分，这些部分由不同的分支或部分分支呈现。通过将分片与不同的区块规模相结合，Enecuum 可以有效地处理每秒数万个甚至数十万个交易，而不会危及系统的安全性。根据意向，在大多数情况下，由此产生的交易费将为零或极小。

此外，系统的无限数分支的支持能力，使得创建各种分散的业务应用程序成为可能，而不需要拥有自己的区块链或对 Enecuum 主支上产生更多的负载。每个分支都可以具有单独定制的自定义规则集，以反映特定服务的需求。此外，建议每个分支可以对系统的所有成员开放，或者仅限于指定的参与者。如果需要在某个分支中升级交易速度或区块规模，则建议它可以引入其自己的节点来修改共识规则。其中唯一的约束是此分支中的节点容量。

根据意向，Enecuum 的架构支持无限规模的宏块。这种解决方案允许协议与现代 CPU 不断增长的性能并行扩展。

5.2. 安全性

低分散化问题

第一代区块链系统使用 PoW 进行交易验证。PoW 是一种可靠的算法，在保护区块链系统免受各种类型的攻击（例如拒绝服务（**“DoS”**）与垃圾邮件）方面具有可靠的效率。 随着加密货币的普及与价值的增加，PoW 挖矿变成了一项大规模的业务，在挖矿项目上投入了数亿美元。

中国的廉价电力与劳动力导致的挖矿能力大大集中在中国大陆。这种情况使得相关的区块链系统安全处于危险之中，因为大型矿工之间可能存在勾结，“51％的攻击”可能性随之增加。 ASIC 设备的出现进一步加剧了这一问题，因为使用常规挖矿设备失去了任何经济意义，并导致的挖矿能力在更大程度上集中在大投资者手中[16]。

据信，在 Enecuum 中三种类型的挖矿结合以及 Cryptonight 加密协议的使用，使得在系统中实现高度的分散变成可能，这种高度分散不仅体现在地理上而且还体现在设备类型与人员上。我们相信，这些功能将有助于使 Enecuum 成为最安全的分布式登记薄之一。除此之外，由于系统中存在着用于收集与分析区块链状态数据的统计分支（参见 4.3），将通过在所有参与者中均匀分布对共识的影响力，这进一步保护 Enecuum 及其用户免受各种类型的隐患。。

智能合约中的漏洞

智能合约的发明给整个加密货币行业带来了强大的推动力，但到目前为止，其实施还有很多不足之处。一旦智能合约在区块链上公示，就不能进行修改，因此在智能合约创建过程中出现的错误会导致其用户损失数百万美元——这种情况在各种加密货币项目中都屡见不鲜[16]。

评估智能合约安全性的现有方法大多归结为社区开发人员的手动代码审核。据称，这种智能合约创建与检测方法效率很低，特别是考虑到正在创建的智能合约数量增长速度超快，其复杂性也是如此。以太网作为最受欢迎的智能合约平台建议用特定的编程语言 Solidity [17]编写智能合约，这种编程语言在开发者社区中尚未普及，导致经验丰富的 Solidity 开发人员严重短缺，并且在我们看来并没有缓解这个问题。

建议用于实施 SHARNELL 智能合约的线性逻辑致力于将这项技术的安全性提升到新的水平。按照设想，在区块链上公示之前，对每个智能合约进行可靠的自动测试，从而尽量减少各种错误与潜在漏洞的可能性。

此外，根据设想，SHARNELL 智能合约语言将是 JavaScript，这是最受欢迎的脚本编程语言之一，因此大量专业人士有机会参与创建 SHARNELL 智能合约，这就会降低智能合约开发成本。

区块链的权力集中

比特币网络的 Segwit2x 升级版失败以及导致比特币现金（Bitcoin Cash）创建的硬分叉凸显了社区中潜在的分歧[18]。不幸的是，比特币的架构安排方式使其矿工、开发人员与普通用户有不同的动机，这些动机形成了他们对所提议变更的不同看法[2]。相互竞争的利益会减缓对不断变化的市场条件的适应性。如果不解决，可能会导致系统过时。

Enecuum 正在寻求解决这个问题，为用户提供更公平的机会，通过对用户对任何参数或新变化的提案进行链式投票来影响平台改进过程。 此外，根据设想，任何改变的实现会涉及安全程序，其中在一个辅助分支对潜在故障进行测试，然后才引入到系统主支。

5.3. 隐私性

一种普遍的看法是，加密货币是匿名的，因此为非法活动提供了充足的机会。 人们还普遍认为，尽管网络内的所有交易都是透明与开放的，但其背后的真实个人与公司却是未知的。 然而，这并不完全正确，因为开放区块链中的每个操作都会在此留下永久的数字足迹，对此足迹执行详细分析可以有助于以高度准确性确定真实交易各方。因此，如果入侵者设法将公共地址与真实的个人或公司匹配，他们就可以访问重要的机密数据并造成无法弥补的损害[15] [19]。

票证分支（参见 4.3）旨在为 Enecuum 用户提供以隐私模式进行交易的手段，从而尽量降低身份披露的风险。门票是分支中交易的加密密钥，因此只有门票持有者才能查看该分支里交易的详细信息。根据设想，票证分支还允许在特定分支（票证分支）上发行特定代币。如果这种代币需要换成 Enecuum 主要交易媒介 ENQ，则门票致力于成为实现交换的密钥。通过这种方式，门票用作加密密钥，可靠地保护票证分支内的交易免受外界关注，同时使用整个网络的容量来确认此类交易旨在保证较高速度。

6. 用途

6.1. 初始硬币发行平台

按照设想，Enecuum 区块链的高吞吐量旨在允许初创公司以任何规模筹集资金，而不存在网络挂起的风险。因此，数字货币首发（“ICO”）参与者有把握他们可以参加 ICO 并快速获得其代币。由于 Enecuum 中的智能合约建议采用 JavaScript，对于任何 Web 开发人员而言都很容易编写，创建成本可能会显着减少。此外，使用线性逻辑有助于消除智能合约代码中的潜在漏洞，并有助于尽量降低黑客攻击的风险。

“取消模式”允许发行人实施复杂的 ICO，在流程的任何阶段逐步募集资金并将资金返还给参与者。类似于 ERC-20 记号的系统特定的代币记号旨在简化在 ICO 之后将基于 Enecuum 创建的代币引入到加密货币交换服务中。

代币发行人将负责其代币用途的适当设计，并确保其代币符合全部所适用的法律与监管责任。

6.2. 金融服务与支付的基础设施

我们的目标是通过使用 Enecuum 的门票与标记使得银行、政府机构与交易性组织能够可靠控制所收到信贷与预算资金的定向支出。还可以利用 Enecuum 基础设施来实现安全有效的支付。

例如，银行可以具备客户数据库，并在其中根据其业务性质（建筑公司、工业设备供应商等）对客户进行分类。银行可以以具有特定且独特标记的代币向客户发放定向贷款。客户只能使用这些代币向某些预定义的单位付款，并只能根据已发放贷款的目的使用这些代币。

此外，由于向交易添加注释的能力可以创建基于区块链的保险服务，其中保留每个客户的历史纪录。该服务可以将用户评级直接保留在区块链上，并通过智能合约进行自动计算而存储每个用户的保险范围信息。

6.3. 分布式计算

Enecuum 致力于在特定分支中运行“重型”智能合约。 Enecuum 还旨在允许复杂的计算，尽管这需要高计算能力，但不会增加主要 Enecuum 主支上的工作量（对神经网络训练、科学计算、渲染计算机图形、JS 库等有用）。 按照设想，使用此类“重型”智能合约付费按灵活的汇率以 ENQ 进行，类似于以太坊区块链中的交易价格概念。在 创建执行计算的请求时，客户设定价格，矿工决定是否愿意为其任务提供计算能力。在矿工同意这些条款的情况下，客户资金由智能合约保留以备将来付款。当任务完成并产生有效结果时，资金将被释放并自动转移给矿工。

6.4. 分散存储

分片技术的应用与更改交易复制参数的能力允许有效使用用户设备上的磁盘空间。 例如，如果 4 个用户各提供 5 GB 的空间，并且复制与分片参数设置为 50％，则有效的文件存储容量为 10 GB。将此模式外推到整个网络，“全球分散磁盘”的规模将按比例增长，同时保持数据的可用性与足够高的访问速度。这意味着用户将来可以在 Enecuum 区块链之上构建分散托管、云数据存储服务与内容交付网络等服务。

而且，通过在这些数据分支之上应用 SHARNELL 智能合约与门票作为加密密钥，用户可以创建复杂的付费访问服务，其中包含以代币付费的分散（与不可变）内容。

6.5. 微交易与物联网应用

Enecuum 系统的工作量将随着 Eneecuum 上的用户数量增多而上涨，分散的应用程序将在 Enecuum 区块链之上开发。但是，Enecuum 建议允许创建带有自己共识规则集的单独区块链分支，从而将工作负载从主系统中移除，从而致力于促进矿工的活动，并创造有利于实施微交易服务的条件。

Enecuum 建议对分散式微交易服务实行零交易费，并且在涉及到从单个钱包进行大量微交易的集中式微交易服务的情况下，每笔交易的费用非常低。 例如，每日 10,000,000 个交易可以很容易地记录在几个 10 MB 的大宏块中。费用将按每个区块计算，因此按照设想每笔交易的费用极低。

我们相信这是对 Enecuum 能力在“物联网”方面的完美运用。在各种设备上实现 PoA 挖矿的简单客户端可以完全覆盖其承担的交易费用。此外，Enecuum 网络协议旨在通过在其之间建立网状网络来提供各种设备的高可用性。

7. 参考文献列表

[1] P. Kasireddy, “Blockchains don't scale. Not today, at least. But there's hope.,”2017. [网上资料].
参阅链接： https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a
[2] F. Ehrsam, “Blockchain Governance: Programming Our Future,” 2017. [网上资料]. 参阅链接:
https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74
[3] A. J. Markus Jakobsson, “Proofs of Work and Bread Pudding Protocols (Extended Abstract),” 1999. [网上资料].
参阅链接： http://www.hashcash.org/papers/bread-pudding.pdf
[4] V. Buterin, “What Proof of Stake Is And Why It Matters,” 2013. [网上资料].
参阅链接:
https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/

[5] C. L. A. M. M. R. Iddo Bentov, “Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake,” 2014. [网上资料].
参阅链接： https://eprint.iacr.org/2014/452.pdf
[6] “CryptoNote Philosophy”. [网上资料]
参阅链接： https://cryptonote.org/inside
[7] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [网上资料]. 参阅链接：https://bitcoin.org/bitcoin.pdf
[8] Ethereum Foundation, “Ethereum Homestead Documentation,” 2018. [网上资料]. 参阅链接：http://www.ethdocs.org/en/latest/
[9] IOTA Foundation, “The IOTA Developer Hub,” 2018. [In the Internet]. Available: https://iota.readme.io/
[10] A. Churyumov, “Byteball: A Decentralized System for Storage and Transfer of Value,” 2016. [网上资料].
参阅链接： https://byteball.org/Byteball.pdf.
[11] Universa Corporation LTD, “Universa Blockchain Platform Whitepaper,” 2017. [网上资料].
参阅链接： https://universa.io/files/whitepaper.pdf?v=1.3
[12] N. N. T. D. a. M. V. Ethan Heilman, “IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency,” 2017. [网上资料].
参阅链接： https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md.
[13] A. E. G. E. G. S. R. v. R. Ittay Eyal, “Bitcoin-NG: A Scalable Blockchain Protocol,” 2015. [网上资料]].
参阅链接： https://arxiv.org/pdf/1510.02037.pdf
[14] J. Vermeulen, “VisaNet -- handling 100,000 transactions per minute,” 2016.[网上资料].
参阅链接： https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-Per-minute.html
[15] P. Kasireddy, “Fundamental challenges with public blockchains,” 2017. [网上资料].
参阅链接：
https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428
[16] M. B. a. T. C. Nicola Atzei, “A Survey of Attacks on Ethereum Smart Contracts,” 2016. [网上资料].
参阅链接： https://eprint.iacr.org/2016/1007.pdf
[17] “Solidity,” 2017. [网上资料].
参阅链接： http://solidity.readthedocs.io/en/develop/
[18] J. J, “No SegWit2x Makes Bitcoin Cash Shine Amidst Crypto Bloodbath,” 2017. [网上资料].
参阅链接： https://cointelegraph.com/news/no-segwit2x-makes-bitcoin-cash-shine-amidst-crypto-bloodbath
[19] J. Clifford, “Privacy on the blockchain,” 2017. [网上资料]. Available: https://hackernoon.com/privacy-on-the-blockchain-7549b50160ec
[20] “Deep Inference,” 2018. [网上资料]
参阅链接： http://alessio.guglielmi.name/res/cos/