比特币共生（BTCS）加密货币白皮书

导言

比特币共生（BTCS）是基于Cryptonote区块链技术创建的，具有完全去中心化和交易匿名性原则。它实现了快速的区块生成，并提供在线和桌面钱包来让用户管理他们的资金。

主要特点

完全匿名和去中心化：BTCS区块链完全去中心化，不会泄露交易的发送者和接收者信息。这为用户提供了高度的隐私保护。

快速的区块生成：区块以不少于每120秒的频率生成，确保快速处理交易并有效地运行网络。

在线和桌面钱包：BTCS加密货币提供方便的在线和桌面钱包，不存储私钥，仅提供给持有者使用。

抵御ASIC矿工攻击：BTCS主要设计用于GPU矿工，并且完全抵御ASIC矿工，确保网络更加去中心化。

矿工奖励：BTCS矿工获得奖励不仅仅是每个区块中的币量，还有网络手续费的奖励。这激励着矿工支持并处理交易。

创新功能

人工智能：BTCS区块链将集成人工智能，优化交易并改进Cryptonote和kHeavyHash算法的工作。

智能合约：BTCS将基于Cryptonote算法引入智能合约功能，允许创建NFT、DEFI和CRY20代币，并启动DAP。

与WEB3兼容：实现与WEB3的兼容性将利用BTCS加密货币的功能开发各种去中心化应用和服务。

结论

比特币共生（BTCS）加密货币融合了去中心化、匿名性和创新原则，为用户提供了高水平的安全性和便利性。它的发展旨在与其他区块链和技术共生，实现加密货币和去中心化金融服务领域的新高度。

在线和桌面钱包：

目前，我们提供在线和桌面钱包，方便存储和管理BTCS加密货币。在不久的将来，我们还计划推出移动钱包，以更便捷地访问您的资金。

我们钱包的独特之处在于，它们提供了高水平的安全性和匿名性，而且完全去中心化。在线和桌面钱包都没有用于存储私钥的集中式服务器。相反，它们完全受到保护，并直接通过RPC请求与我们的区块链进行交互。

在注册在线钱包时，您将创建自己的私钥和助记词，这些信息只有您自己能够访问。在线钱包不会在服务器上存储私钥或助记词，而是仅向区块链发送请求以执行与您的资金相关的操作。

安装在您的计算机上的桌面钱包也提供了高水平的安全性。安装桌面钱包时，您将创建自己的私钥或助记词，这些信息也只有您自己能够访问。桌面钱包没有数据库，也不会在本地存储私钥，而是通过与区块链进行交互来执行与您的资金相关的操作。

我们致力于实现区块链的完全去中心化，因此决定将我们的钱包完全交由持有者控制。这为您的资金提供了最高级别的安全性和匿名性，因为除非经过您的许可，否则任何第三方个人或组织都无法访问您的钱包。

全面匿名和去中心化：
BTCS 是一种旨在实现交易全面匿名和去中心化的加密货币。对于 BTCS 团队来说，匿名性概念本身并不是最重要的，而是其目标 - 实现区块链的完全去中心化。这意味着匿名性并不是最终目标，而更像是实现更深层目标的工具 - 创建一个去中心化和安全的金融生态系统。

我们选择了匿名性的道路，是为了展示加密货币的真正本质在于区块链的去中心化，而不是为了欺诈者或非法行为者提供匿名性。考虑到许多声称是去中心化项目的区块链项目，但实际上受到了所有权和控制方面的集中化影响，我们声明，真正去中心化的区块链必须为其用户提供完全匿名和安全性。

BTCS 通过使用 Cryptonote 技术实现了完全匿名性，该技术使用环签名和一次性地址来隐藏交易的发送者、接收者和金额。这使得第三方观察者无法追踪和分析网络中的交易。此外，我们的区块链允许使用 mixin 机制进行交易，该机制允许同时通过多个输入和输出进行多个交易，从而增强了匿名性和安全性水平。

因此，BTCS 是一个可靠且安全的金融平台，用户可以在其中进行交易，而不必担心泄露他们的匿名性和数据隐私。

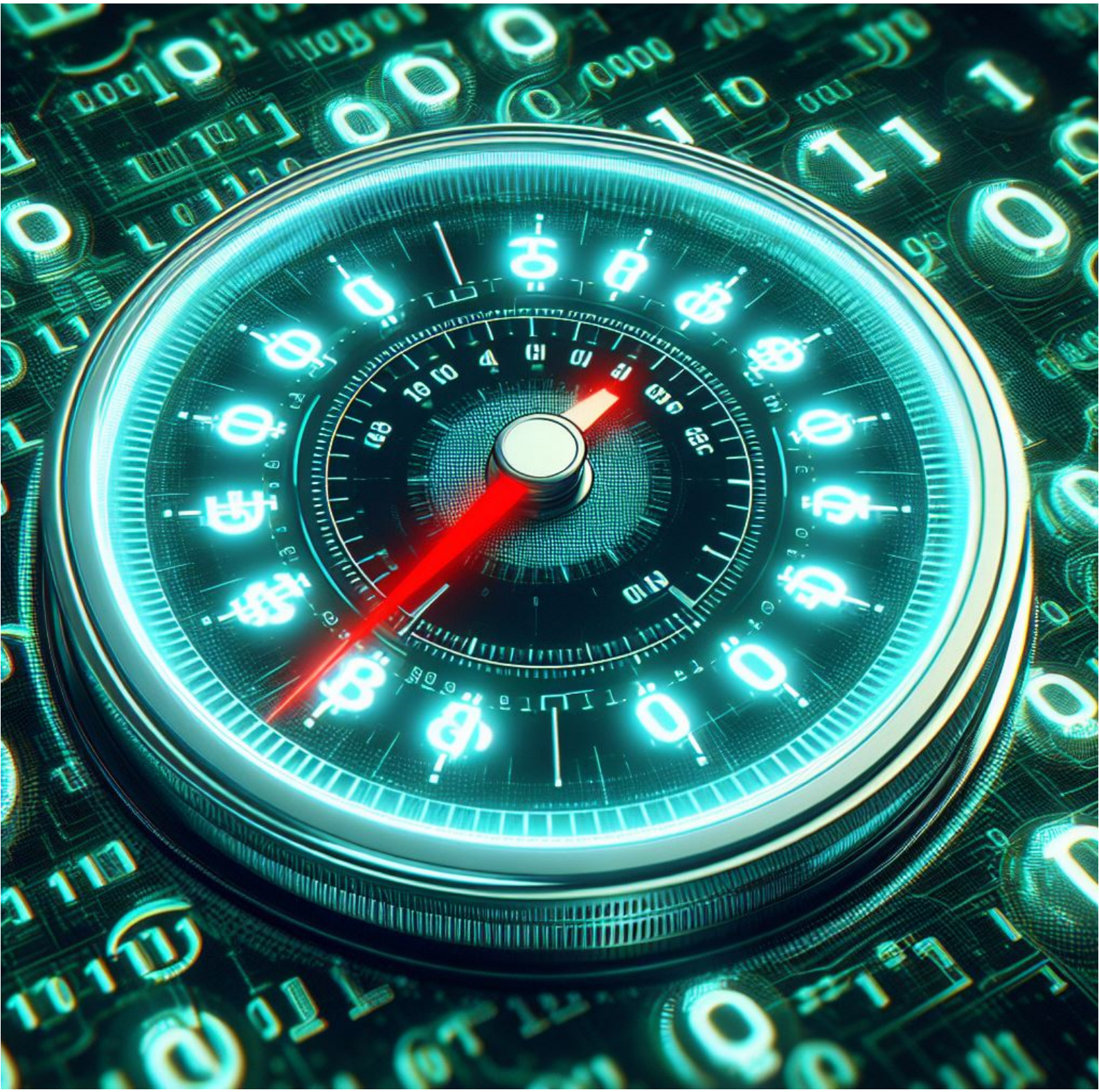
快速区块生成：

我们决定将区块生成间隔设置为120秒，以确保网络中的交易能够快速处理，同时保证高水平的安全性和防御攻击。

选择120秒的区块生成间隔考虑到了交易速度和网络安全之间的平衡。这个时间段可以确保足够快的区块生成，以处理大量的交易，并最大程度地减少在生成区块时发生冲突和错误的可能性。

为了提供额外的安全级别，我们引入了每10个区块确认一个区块的机制。这意味着要完成交易并激活用户的余额，需要在接下来的10个区块中确认。这可以防止双重支付，因为收款方无法在接下来的10个区块中确认交易之前提取资金，同时区块链将在此期间检查余额的一致性。

虽然一些区块链可能会使用更短的区块生成间隔，例如1秒，但考虑到在生成区块时可能出现的错误和冲突，特别是在Cryptonote区块链中，我们决定不采用这种方法。相反，我们计划将kHeavyHash区块链与Cryptonote集成，以实现网络中交易的最大吞吐量。kHeavyHash区块链使用BlockDAG数据结构，可以处理每秒大量的交易，并确保网络的高性能和可扩展性。

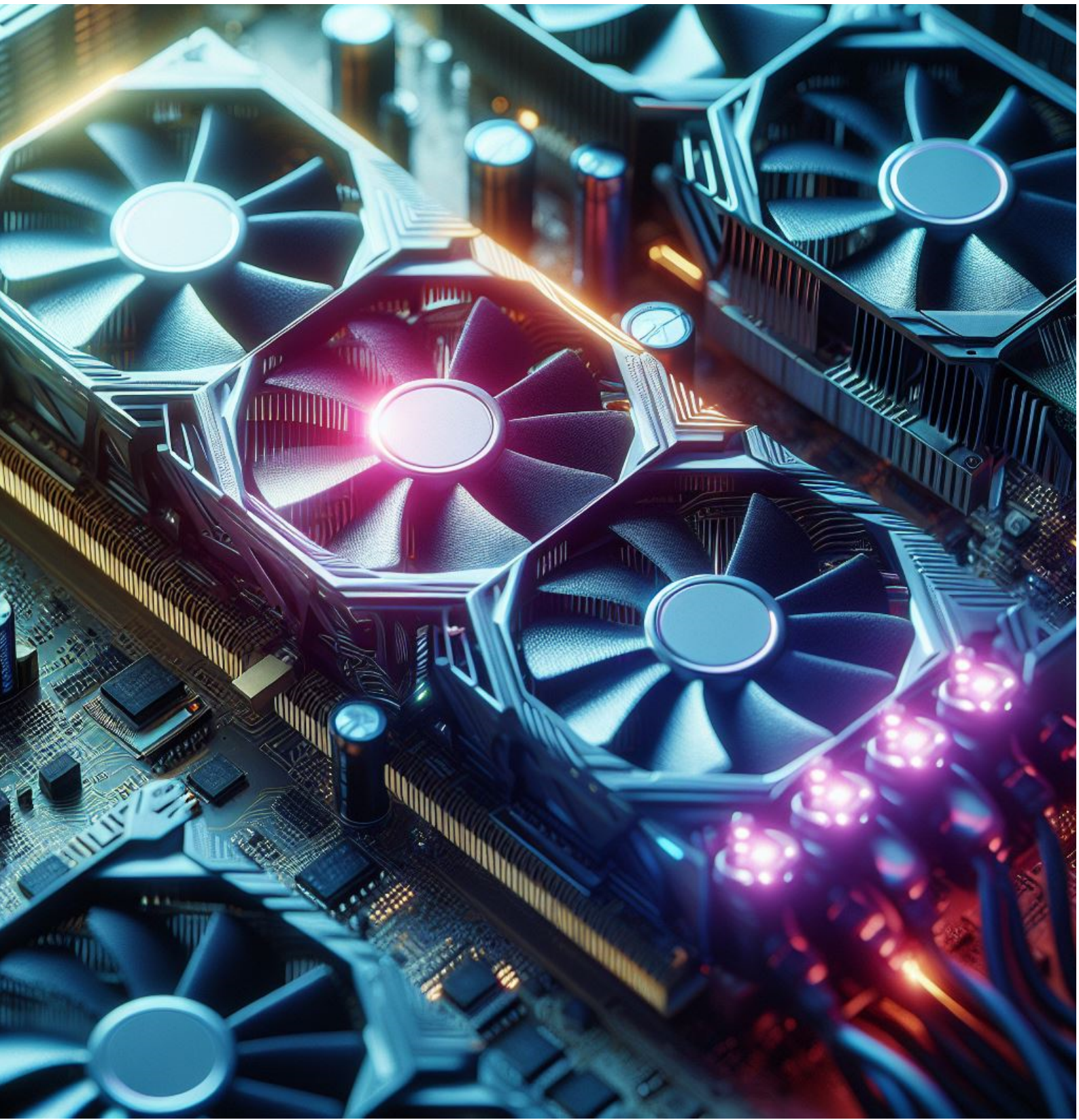


矿工奖励：

我们为矿工提供了一种机制，让他们不仅可以通过区块中的BTCS数量获得奖励，还可以通过交易手续费获得奖励。这将大大增加矿工的收益，并使他们在网络中的参与更具吸引力。我们引入了这一功能，旨在强调“比特币共生”的含义，即BTCS与比特币兼容，但具有自己的特点，如仅供GPU矿工使用以及整合其他区块链的所有创新。

我们没有明确的减半日期，而是计划逐步减少矿工的奖励。我们将密切关注，确保矿工始终能够盈利，并努力确保矿工奖励的价格和数量保持在合理范围内。我们致力于确保矿工奖励的稳定性，以使BTCS的挖矿成为具有吸引力且长期可持续的活动。

这将有助于我们维持网络的稳定性，因为矿工将继续确认交易并促进去中心化。为矿工提供适当的奖励以鼓励他们参与网络，有助于确保BTCS网络的安全性和稳定性。此外，这将为BTCS生态系统的发展和吸引新成员进入网络创造条件。



防止ASIC矿工：

我们决定通过采用Cryptonote V7协议并对其进行一些修改，来保护网络免受ASIC矿工的攻击。我们的目标是让所有愿意参与的人都能挖掘BTCS，并防止网络算力被垄断，为所有矿工提供平等的机会。

采用Cryptonote V7协议使我们能够有效地保护网络免受ASIC矿工的攻击，因为该协议专门设计用于在CPU和GPU上进行挖矿，这确保了网络参与者的分散和平等。我们还对协议进行了一些修改，以加强对ASIC矿工的保护，并为所有矿工提供平等的机会。

我们的加密货币旨在吸引GPU矿工，因为我们认为GPU挖矿可以更广泛地分散网络的算力，并促进分散化。我们致力于为所有矿工提供平等的机会，无论他们的技术装备如何，并为所有网络参与者提供挖矿的机会。

此外，我们计划在我们的区块链中引入人工智能，这需要像GPU这样的高性能计算资源。我们认为GPU挖矿是确保我们网络中的人工智能能够高效运行的最佳解决方案。

我们在Cryptonote区块链中实施了一个功能，可以防止GPU矿工垄断网络算力。该功能确保了不同GPU之间算力的均衡分配，并防止一些矿工对其他矿工的主导地位。因此，所有GPU矿工都有平等的机会来挖掘BTCS，这有助于网络的分散化和公平性。

人工智能：

BTCS区块链将集成人工智能以优化交易并改进Cryptonote和kHeavyHash算法的运作。以下是人工智能引入的创新功能：

交易优化：

人工智能将用于分析和优化交易过程，以加速其处理并降低手续费。

改进Cryptonote和kHeavyHash算法：

人工智能将应用于分析Cryptonote和kHeavyHash算法的运作，以发现瓶颈并提高其效率。

区块链数据分析：

人工智能将分析区块链数据以发现趋势、异常和潜在的安全威胁。

智能合约和自动化：

人工智能将用于创建智能合约，能够自动响应网络变化并执行预定义条件。

预测性分析：

人工智能将用于分析区块链数据并预测市场未来趋势，帮助用户做出理性的投资决策。

安全性保障：

人工智能将用于检测和防止网络攻击，并确保用户及其资产的安全。

将人工智能集成到BTCS区块链中将创建一个更加高效和创新的网络，能够适应不断变化的市场条件和需求。