链上布雷顿森林体系：BeL2 如何利用原生比特币改变全球金融？

在金融领域的历史长河中，鲜有事件能像布雷顿森林体系的建立那样，对全球经济格局产生如此深远的影响。1944年，第二次世界大战的硝烟尚未散尽，来自全球44个同盟国的代表们齐聚新罕布什尔州的布雷顿森林，共同构建了一个崭新的国际经济合作框架。这一体系的诞生，旨在防止经济的不稳定与竞争性贬值，避免大萧条和战争的悲剧再次上演。

布雷顿森林体系的核心是将主要货币与美元挂钩，美元则按照固定汇率兑换黄金。这一安排使美元成为全球储备货币，为全球经济提供了急需的稳定性，并促进了经济的快速增长。然而，随着时间的推移，特别是进入20世纪60年代末，该体系开始面临挑战。美国国际收支赤字不断增加，黄金储备逐渐减少，导致体系内部的不平衡加剧。1971年8月15日，理查德·尼克松总统宣布终止美元与黄金的可兑换性，这一决定实际上宣告了布雷顿森林体系的终结，同时也开启了法定货币时代的新篇章。



法定货币的普及为货币政策提供了更大的灵活性，但也带来了前所未有的挑战。政府可以不受限制地发行货币，导致通货膨胀、货币贬值等一系列问题的出现。在全球化与金融化高度发展的今天，世界正面临着高达307万亿美元的债务、过度的货币发行、银行信贷下降以及经济不稳定性上升等多重挑战。这一背景之下，全球金融界急需一种新型的金融模式，将稳定性与数字时代的技术进步相结合，以应对日益复杂的金融环境。

### 比特币：数字黄金

比特币，作为一种去中心化的数字货币，自2009年由化名“中本聪”的创始人推出以来，便被誉为“数字黄金”。它具备许多特性，使其成为全球储备资产的理想选择：稀缺性（上限为2100万枚）、耐用性、便携性以及易于分割。比特币的区块链技术确保了交易的透明度、安全性和抗审查性，使其成为支持法定货币和价值交换的强大工具。

尽管比特币的价值已经超过1万亿美元，得到了广泛的认可和应用，但在主流金融领域仍面临着诸多挑战。其中最为突出的是可扩展性和可编程性限制。比特币的高度去中心化和安全性保证了其强大的安全性，但也导致了交易速度缓慢和资源消耗过大。以太坊等创新技术通过引入智能合约，为比特币等数字货币提供了更多功能，从而催生了旨在统一技术并增强比特币功能的第2层解决方案。

#### 比特币层

第2层解决方案是建立在区块链（第1层）之上的协议，旨在增强性能并实现更复杂的功能。对于比特币而言，闪电网络和侧链等第2层技术解决了交易速度、可编程性和可扩展性问题，而桥梁则促进了与其他区块链生态系统的互操作性。这些解决方案使得比特币能够与其他区块链生态系统和以太坊等创新进行交互，实现以前不可能实现的智能合约和去中心化应用程序（DApp）。然而，这些解决方案也带来了一些问题。



#### 固有问题

可扩展性层涉及将比特币从其主网络桥接到这些环境中，从而产生安全问题，破坏其去中心化精神。例如，Wrapped Bitcoin (WBTC)是一种ERC-20代币，代表以太坊网络上的比特币。虽然它将比特币的流动性带入了更多可编程金融平台，但它存在几个关键问题：

中心化风险：WBTC要求用户信任中心化机构来管理和保护支持WBTC的比特币。如果这些机构恶意行事，用户将无处求助，从而破坏比特币的去中心化精神。

托管风险：持有实际比特币的集中托管人可能会遭到黑客攻击或面临监管压力，从而使用户的资产面临风险。

缺乏透明度：用户必须依赖托管人对支持WBTC的实际储备的透明度，但这可能并不总是可靠的。



跨链桥黑客攻击（例如Nomad Bridge漏洞）凸显了这些漏洞。Chainalysis报告称，13次跨链桥黑客攻击共窃取了20亿美元，占2022年被盗资金总额的69%，与朝鲜有关的黑客窃取了约10亿美元。有70多条跨链桥，锁定资金超过250亿美元，每日交易量达数百万。流行的跨链桥Synapse的交易量已超过50亿美元。跨链桥的结构很脆弱，结合了托管人、债务发行人和预言机，每个都存在多个攻击媒介。例如，Poly Network和Wormhole攻击暴露了跨链通信中的漏洞，造成了重大损失。

为了降低这些风险，对于比特币的发展来说，通过信息传输而不是资产转移来连接其他创新层至关重要，同时将比特币上的质押去中心化，以避免将资产集中在一起。这种方法保持了比特币的原生性、安全性和去中心化，同时在可扩展的环境中实现了更广泛的金融应用。

### 比特币原生DeFi，开创新布雷顿森林体系

原生比特币是指在为第2层DeFi应用提供抵押的同时仍保留在主网络上的比特币。通过BeL2，比特币可以参与复杂的金融交易，而无需从比特币区块链转移，从而保持其安全性和去中心化。这使得比特币可以充当DeFi生态系统中的多功能工具，充分利用其固有优势，同时将其功能扩展到掉期、贷款和稳定币发行等智能服务中。

质押：BeL2在去中心化钱包中采用非托管原生比特币质押，为网络提供安全保障。

零知识证明（ZKP）：它为比特币质押交易提供私密且可验证的证明。

BTC Oracle：将BTC证明信息接入第2层智能合约，无需将资产移出主网即可实现比特币DeFi服务。

仲裁网络：利用去中心化和抵押节点来促进基于时间的执行和争议解决，增强无需信任的金融运作。



BeL2在链间传输信息而非资产，从而保护比特币的安全性和完整性，同时支持智能合约和去中心化应用程序进行复杂的金融交易。这种方法消除了对中心化实体的依赖，并确保了安全、去中心化的金融运营。通过保持比特币的原生性，BeL2确保原始区块链仍然是所有交易的最终信任锚，从而维护了比特币去中心化精神的基本原则。

### 原生比特币贷款应用程序演示

在BeL2在去中心化金融(DeFi)中发挥变革作用的背景下，BeL2贷款Dapp Demo展示了其在保持安全性和去中心化的同时增强比特币效用的潜力。该演示是基于Starkwares Cairo编程语言构建的第一个原生比特币借贷协议，允许用户将其原生比特币锁定为抵押品，而无需依赖Wrapped Bitcoin (WBTC)或跨链桥。BTC仍保留在比特币主网上，确保非托管和不可清算的抵押品。



用户通过定制的交易脚本锁定他们的比特币，贷款条款（包括利率和抵押品释放条件）由以太坊虚拟机(EVM)上的智能合约管理。BeL2的仲裁网络充当中介，促进比特币和EVM链之间的通信并验证交易证明。如果借款人（如Alice）未能偿还贷款，贷款人Bob可以取回BTC。如果Bob在还款后拒绝合作解锁BTC，Alice可以发起仲裁，仲裁员将共同签署以解锁BTC。



这种点对点系统通过零知识证明和仲裁网络确保公平和安全。仲裁员或相关方的任何恶意行为都会受到质疑和惩罚不当行为的能力的制止，从而确保合作是最好的结果。这种创新方法使比特币持有者能够获得流动性，同时保留比特币去中心化和安全性的核心原则。

新本土比特币布雷顿森林体系的原则：

•去中心化全球结算：原生比特币必须充当全球结算层，所有交易都在比特币主网络上得到保护，确保它仍然是全球金融的最终信任锚。

•金融创新与稳定性：通过将原生比特币与智能合约和DApp相结合，我们可以支持BTC支持的贷款和稳定币等新金融产品，在统一各个层面的同时为全球经济提供流动性和稳定性。

•无需信任且透明的运行：通过零知识证明和去中心化仲裁网络实现信息传输，确保比特币原生应用程序的无需信任且透明的金融运行，降低交易对手风险并增强交易完整性。



BeL2的愿景是成为新布雷顿森林体系中比特币原生基础设施的决定性部分。BeL2源自Elastos SmartWeb愿景，该愿景旨在创建一个去中心化的互联网，其中数据、应用程序和身份都是安全、私密且由用户拥有的。BeL2致力于成为比特币原生基础设施的关键组成部分，将比特币从数字黄金转变为新全球金融体系的基石。

BeL2利用Elastos的安全基础设施，使用ELA作为仲裁员的抵押品，以确保稳健且无需信任的争议解决。ELA是一种与超过50%的比特币矿工安全合并开采的资产，它为BeL2生态系统增加了额外的安全性和去中心化层，加强了两个项目对安全和去中心化金融未来的承诺。想了解更多信息吗？请访问BeL2网站并关注Infinity 以获取最新更新！