Agere共识：基于BEVM(λ)的智能加密货币设计

摘要

本文通过对比特币和以太坊的设计理念进行深入分析，指出以太坊提出的区块链三大技术问题（图灵非完备性、共识机制效率和网络扩展性）**并非真正的问题**，而是源于对**比特币核心原则的误解**。这种误解导致以太坊在全局状态管理、权益证明共识等方面违背了能量守恒和去中心化的设计原理，形成了封闭的熵增系统，难以实现可持续发展。

为此，Agere共识提出了基于BEVM(λ)范式的智能加密货币设计理论，以比特币的UTXO模型、λ演算、共识算法和共识感知算法为基础，提炼出四大核心要素：能量守恒的商业闭环、去中心化的涌现共识特性、基于Individual的自治性设计和分布式无状态计算模型。在此框架下，设计了双层共识架构，包括承袭比特币传统的母共识和面向未来的子共识（Agere共识）。通过BTC质押双代币模型和基于Agent工作量的资源分配机制，Agere共识既保留了比特币的安全性和稳定性，又实现了智能化和多样化的分布式协作。

本文还探讨了当前Agere共识面临的评分去中心化、扩展性和涌现机制等挑战，并提出未来优化方向，包括改进共识量化算法、强化Individual模型和优化λ演算体系。最终，Agere共识旨在构建一个完全符合BEVM(λ)范式的智能加密货币系统，为区块链技术创新提供新范式，为行业发展指明方向。

1. 引言：Crypto叙事的迷失

2015年以太坊的出现为区块链技术带来了新的发展方向，其提出的三个核心问题深刻影响了行业的技术路线。然而，由于**对比特币核心原则的根本性误解**，以太坊提出的关于图灵完备性、共识机制效率和网络扩展性的观点导致过去近十年的区块链发展偏离了中本聪比特币设计的本质。

1.1 以太坊的三大问题叙事

在以太坊引领的区块链技术发展中，形成了三个核心的技术改进方向：

- **图灵非完备性问题：**比特币脚本语言的图灵非完备性被认为限制了区块链的应用场景。以太坊通过引入图灵完备的虚拟机(EVM)来扩展智能合约的功能边界，试图将区块链从单一的价值传输系统扩展为通用计算平台。

- **共识机制效率问题：**工作量证明(PoW)机制的高能耗问题日益凸显。以太坊提出向权益证明(PoS)机制转型，通过质押代币替代算力竞争来实现所谓的"绿色共识"。这一改变旨在降低网络运行成本，提升共识效率。
- **网络扩展性问题：**比特币网络的交易处理能力(TPS)难以满足大规模商业应用需求。以太坊计划通过分片技术等扩容方案提升网络吞吐量，以支持更广泛的商业场景和更复杂的应用生态。

1.2 问题叙事背后的本质问题

这三个技术改进方向实际上反映了对比特币本质的深层误解：

- **能量守恒的商业闭环被打破：**比特币通过工作量证明(PoW)建立了算力投入与价值产出的明确对应关系，形成完整的能量守恒商业闭环。而以太坊等项目转向PoS机制后，验证节点的能量投入可以忽略不计，导致系统价值与外部能量失去对应关系，最终成为一个缺乏真实价值支撑的封闭熵增系统。
- **共识量化算法背离涌现原则：**比特币的PoW是一个基于算力的无序熵减涌现过程，体现了真正的去中心化特性。而新一代公链普遍采用了确定性的投票或质押规则，失去了系统自组织的涌现特性，本质上沦为一种预设的中心化规则执行过程。
- **违背Individual去中心化设计原则：**比特币通过UTXO模型确保了每个交易单元的独立性与自治性。而新一代公链为了支持复杂计算，完全抛弃了这一原则，转而采用中心化的账户模型和全局状态树架构，使系统失去了基于Individual的去中心化基础。

这些本质问题表明，以太坊时代的技术改进实际上偏离了Crypto商业的核心设计原则，即基于能量守恒的分布式闭环商业、Individual的去中心化、基于涌现的共识机制。Ethereum的认知偏离不仅没有解决原有问题，反而导致了更深层的系统性挑战。

2. BEVM(λ)：Bitcoin范式方程

我们分析了以太坊时代区块链发展的根本性问题。这些问题的存在促使我们重新审视比特币系统，通过深入分析中本聪的设计思想，我们提出了BEVM(λ)范式方程，以揭示Bitcoin成功的本质原因。

2.1 BEVM(λ)范式的构成

BEVM(λ)由四个核心组件构成：Individual模型、λ演算、共识算法和共识感知算法。在比特币系统中，这些组件的具体实现为：

- **Individual模型：**基于UTXO作为载体的Coin构成了比特币系统的基本个体单位。每个UTXO都是独立的价值载体，不依赖全局状态，从而实现了真正的个体主权。
- **λ演算：**基于UTXO数据结构的BTC转账操作构成了比特币的λ演算体系。通过函数f(compute) = TX(Input(Individual), Output(Individual))实现Individual之间的分布式计算，确保了交易的无状态性和独立性。
- **共识算法：**通过函数f(consensus) = Consensus(hash, difficulty)解决拜占庭容错问题。比特币的共识算法通过量化hash计算，以nonce为个体实现分布式共识计算的涌现，体现了真正的去中心化特性。
- **共识感知算法：**f(Consensus Mechanism, External Energy Input, Energy Conversion Mechanism) = Value Output 这一函数通过融合交易函数和共识函数，实现了能量守恒的分布式商业系统，将hash算力背后的电力能源映射为BTC的商业价值。

2.2 基于BEVM(λ)的比特币与以太坊对比分析

通过BEVM(λ)范式的四个组件，我们可以系统地分析比特币和以太坊的设计差异：

1. **Individual模型**
   - Bitcoin：基于UTXO的分布式个体模型，每个交易输出都是独立自治的价值单元
   - Ethereum：采用基于账户的中心化状态树，所有账户状态都依赖全局存储
2. **λ演算实现**
   - Bitcoin：基于UTXO的无状态函数式交易模型，确保了计算的分布式特性
   - Ethereum：基于EVM的图灵完备计算，引入全局状态，破坏了计算的独立性
3. **共识算法设计**
   - Bitcoin：POW机制中，每个矿工通过调整nonce值进行独立的哈希运算，由这种去中心化的算力竞争自然涌现出系统共识
   - Ethereum：采用POS机制的中心化投票共识，失去了涌现特性
4. **共识感知量化机制**
   - Bitcoin：建立了从算力能量投入到BTC价值输出的完整映射关系
   - Ethereum：验证节点的能量投入可忽略不计，缺乏能量守恒的价值体系

从BEVM(λ)的视角来看，比特币在所有四个组件上都严格遵循了Individual分布式设计原则。而以太坊为了实现图灵完备的智能合约平台，在每个组件上都背离了这一核心原则。特别是在共识感知量化机制上，由于缺乏必要的外部能量输入，导致系统成为一个封闭的熵增系统，这也是以太坊等项目未能实现可持续商业模式的根本原因。

3. BEVM(λ)的理论指导与Agere共识的演进

3.1 BEVM(λ)：智能加密货币的设计指南

基于对现有Crypto叙事问题的分析，结合提出的BEVM(λ)设计理论，我们将当前的研究重点聚焦于解决Crypto系统的“智能”问题。智能的核心在于自治性与涌现性，而非智能系统表现为机械化执行及人为操控的痕迹，难以实现真正的去中心化。

以比特币为例，其智能性源于工作量证明（PoW）中无限的无序算力竞争的熵增过程，通过`nonce`的动态调整涌现出系统共识与价值化BTC的熵减过程，完成了非智能到智能的跃迁。

在此基础上，Agere共识提出基于BEVM(λ)范式设计智能代币BEVM，其不仅继承了比特币的能量守恒商业模式，还通过创新性的双层共识架构实现了面向未来的智能化发展。

3.2 BEVM的历史演进与双层共识架构

BEVM的起源

BEVM的发展历程经历了对比特币和以太坊核心设计理念的深度反思，并在多次技术探索中逐步形成了当前的范式：

1. **BTC Layer2探索阶段**
    - **目标：** 解决比特币网络扩展性不足的问题，尝试通过Layer2方案提升交易效率。
    - **经验：** 虽然技术实现可行，但这种方式缺乏生态应用的实际需求支撑，未能真正改变比特币的现状。
2. **Taproot Consensus阶段**
    - **创新：** 结合Bitcoin SPV状态通道与Taproot技术，尝试实现比特币的去中心化托管，扩展其智能合约能力。

- **反思：** BTC 作为货币已经在中心化交易所和矿池中被广泛应用，其去中心化扩展的需求相对有限。真正需要扩展的是Bitcoin的共识机制，而不仅仅是 BTC 作为货币的功能。

3. **SuperBitcoin阶段**
   - **方向：** 将Bitcoin共识的安全优势引入设计，提出一个共享Bitcoin共识安全的新型加密货币系统。
   - **局限：** 虽然提升了系统共识的安全性，但未能解决Ethereum等VM系统在处理外部现实问题上的“梦境割裂”——仅能在内生流动性环境中运行，无法感知外部世界的现实数据和状态。
4. **BitAgere阶段**
   - **问题：** Bitcoin的机械共识与AI Agent的抽象能力存在共性，催生了BitAgere的设计。
   - **创新：** 在SuperBitcoin的基础上，重点解决机械共识的感知问题，将AI Agent的输入感知能力抽象化并接入链上，使Crypto系统具备外部感知能力，从而实现Crypto与AI Agent的深度融合。
5. **BEVM(λ）阶段**
   - **发现：** 我们通过内观Bitcoin的设计哲学，提出了BEVM(λ）范式。这一范式深入解析了Bitcoin成功的本质，涵盖了Individual模型、λ演算、共识算法和共识感知算法四大核心要素，为设计智能化的Crypto系统提供了系统性的理论指导。
   - **方向：** BEVM(λ）不仅继承了Bitcoin在能量守恒和去中心化涌现性上的核心理念，还进一步拓展了系统的自治性与智能化能力。通过这一范式，结合Agere子系统，我们在分布式无状态计算和共识感知算法的支持下，探索未来的多样化应用场景，实现智能加密货币的全面设计与落地。

双层共识架构的确立

在上述阶段的技术积累与反思中，我们确立了BEVM的双层共识架构：

1. **母共识：链接过去**

   母共识继承了比特币网络的核心设计，包括其高度去中心化的共识机制与能量守恒模型，为BEVM系统提供安全与稳定的基础。

2. **子共识：面向未来**

子共识以Agere共识为核心，通过严格遵循BEVM(λ)范式，探索分布式经济的新模式。Agere共识特别关注能量守恒与涌现特性，为智能加密货币的可持续发展奠定理论基础。

通过双层共识架构，BEVM既能够保持与比特币的深度联系，又能通过Agere共识实现全新的智能化发展路径。 BEVM 专注于当下的 已感悟到的问题，并持续解决它。

4. 双层共识的设计与实现：Bitcoin基础与Agere扩展

4.1 母共识：基于Bitcoin的双代币共识模型

4.1.1 Bitcoin质押双代币模型

在初始价值积累的基础上，母共识引入了基于Bitcoin质押的双代币模型，使比特币网络的安全性得以延续，并为参与节点提供灵活的权益证明激励机制：

1. **Bitcoin非托管式质押：**

   节点可通过闪电网络二层协议将一定数量的BTC锁定到网络中，且无需托管至中心化机构。这确保了资产的安全性与去中心化。

2. **时间质押与能量守恒：**

   BEVM代币的生成过程遵循能量守恒定律：

   - 比特币的PoW算力通过挖矿生成BTC，这一过程消耗了外部能源。
   - 锁定到网络中的BTC通过时间质押转化为BEVM代币，进一步延续了能量的价值传递关系。

   BEVM代币的生成与BTC质押量（b_i）和质押时间（t_i）成正比，其公式如下：

   $$BEVM_i = k \cdot b_i \cdot t_i$$

   其中，k 是系统设定的奖励系数，用于反映BTC质押与BEVM代币生成的比例。

3. **双代币协同机制：**

   - **BTC代币：** 反映节点在比特币网络中的实际贡献，如BTC持有量、质押规模和活跃时长。

- **BEVM代币：** 用于在PoS层参与质押和共识，决定节点的共识权重及奖励分配。

4. **随机性与门槛机制：**
   - 节点需满足最低质押量门槛，确保其具备基本的经济绑定。
   - 在满足条件的节点中，系统基于BTC质押权重随机抽样选取验证者，避免财富集中问题，同时增强网络的去中心化。

4.1.2 共识算法：基于Aura + GRANDPA的BFT PoS机制

BEVM系统在母共识架构中采用了基于Substrate框架的BFT PoS共识算法，结合了Aura与GRANDPA的高效特性。Aura作为块生产机制，通过轮值领导者模型快速生成新区块，确保系统的高吞吐量与低延迟。GRANDPA则作为最终确定性机制，通过拜占庭容错的全网投票流程快速确认区块链状态，增强了链的安全性与不可逆性。两者协同工作，实现了高性能、高安全性和强一致性的区块链共识，为BEVM的分布式经济模型提供了坚实基础。

4.2 子共识：Agere共识

Agere共识机制从**共识量化函数优化**这一核心问题出发，致力于在智能化的多Agent系统中实现对个体贡献的量化评估与合理激励分配。设计之初，Agere共识严格遵循能量守恒的商业闭环原则：通过量化Agent工作量，将其直接映射为权益代币（BEVM）的产出，实现价值流动的闭环结构。

Agere共识采用分层分配机制，将复杂的Agent协作问题分解为系统内和系统间两部分进行优化。这种设计兼顾主观评分与客观度量，使得系统既能捕捉复杂行为的多样性，又能维持整体公平性与一致性。

1. **基于Agent工作量的BEVM生产机制**

   Agere共识的首要目标是通过工作量的量化，直接将Agent的任务完成情况映射为权益代币的产出，具体包括：

   - **任务贡献度量：**Agent通过完成诸如AI问答、内容生成、数据标注等任务，为网络提供价值。任务的完成情况由多个指标综合评估，如准确性、完成率、时效性等。这些指标被归一化为贡献度，反映Agent在任务中的实际表现。
   - **权益代币映射规则：**贡献度与权益代币（BEVM）的产出呈直接映射关系，维护能量守恒的商业闭环。

2. **主观评分的妥协式量化方案**

在任务贡献的量化中，部分非显性因素（如创造力、协作性）难以通过客观指标全面衡量。为解决这一问题，Agere共识引入主观评分机制，使Agent之间可以通过相互评价实现综合贡献的量化：

基于此，我们提出了**评分（w）**和**权益质押（s）**两个核心要素：

1. **评分（w）**允许 Agent 通过主观判断表达其对系统目标的贡献，以捕捉复杂场景中的非显性因素。
2. **权益质押（s）** 则通过经济约束为这种主观性引入可信度筛选，激励 Agent 提供更可靠的评价。

这种设计兼顾主观表达与客观约束，既能在系统内通过有约束的主观评价量化 Agent 对目标的贡献，又能通过跨系统的加权评分衡量不同系统的重要性。基于这两个核心要素，我们设计了一个自上而下的分层分配流程：首先在系统间进行资源的初步划分，然后在各个系统内部进一步细化分配。这种分层处理既保证了整体资源分配的合理性，又维护了局部系统的自主权。

1. **跨系统资源配置**：Agere共识首先解决系统间的分配问题。Agent基于对Agere系统的贡献度量（包括系统效能、资源利用率、价值创造等多维指标）进行评估，形成系统间评分矩阵W，其中w_{ij}表示Agent i对Agere系统j的评分。将这个评分矩阵W结合各Agent的质押权益s，通过共识映射函数，计算得到每个Agere系统应获得的权益代币数量。
2. **系统内资源分配:** 在系统资源配额确定后，Agere共识机制转向系统内分配。在单个Agere系统内，Agent基于对其他Agent的计算贡献、协同效率、目标达成度等性能指标进行评估，形成评分矩阵W，其中w_{ij}表示Agent i对Agent j的综合评估。该评分矩阵W与系统内Agent的质押权益s通过共识映射函数，确定每个Agent的最终资源分配比例。
3. **共识映射函数：**共识映射函数实现了从主观评分到排放分配函数映射。无论是系统间还是系统内的分配，都采用同样的三步映射机制将评分矩阵W和质押权益s转化为最终分配E：
    a. **共识评分生成机制** 对每个被评主体j（可能是系统或Agent），系统首先需要从所有评分中形成一个共识评分$\bar{w}_j$。通过质押加权的中位数机制实现：

$$w_j \;=\; \max\Big\{\, w \;\Big|\; \sum_i \big[\, s_i \cdot \mathbf{I}(w_{ij} \ge w) \big] \;\ge\; \kappa \cdot \sum_i s_i \Big\}$$

    这个公式实现了"质押加权投票"的过程：

- s_i: Agent i的质押量
- κ: 共识阈值（通常为0.5）
- $I(w_{ij} \geq w)$是指示函数，当评分大于等于w时为1，否则为0
- $s_i \cdot I(w_{ij} \geq w)$表示支持评分至少为w的质押总量
- $\kappa \cdot \Sigma s_i$设定了形成共识所需的最小质押比例门槛
- 最终$\bar{w}_j$选择满足门槛要求的最大可能评分

b. **评分修正机制** 为了平衡个体评分的自主性和系统的稳定性，对原始评分进行修正：

$$w_{ij} \;=\; (1-\beta)\, w_{ij} \;+\; \beta\, \bar{w}_j$$

这个线性组合实现了软约束：

- β: 调节参数，取值在[0,1]之间
- 保留了(1-β)比例的原始评分w_{ij}，维持评分的多样性
- 引入β比例的共识评分$\bar{w}_j$，约束异常评分
- β参数可根据系统需求调节，较大的β值会使评分更趋于一致

c. **排放分配计算** 最终，系统基于修正后的评分和质押量计算排放分配：

$$E_j = \frac{\sum_i \left(s_i \cdot \tilde{w}_{ij} \right)}{\sum_k \sum_i \left(s_i \cdot \tilde{w}_{ik} \right)}$$

这个分配机制确保：

- 分子$\Sigma_i (s_i \cdot \tilde{w}_{ij})$表示Agent j获得的质押加权总评分
- 分母对所有Agent的加权评分求和进行归一化
- 质押量s_i在评分权重中起到关键作用
- 最终分配E_j反映了评分和质押的综合效果

通过这种分层分配机制，Agere共识既实现了系统间的资源合理配置，又保证了系统内部的激励分配，最终将权益代币精确地分配到每个Agent手中。

4.3 经济模型与区块激励

为确保 BEVM 的公平性与可持续性，共识层在系统启动之初即设计了一套可自我演进的经济模型。该模型在保证去中心化与安全性的前提下，通过无预挖、通缩式增发和多元激励分配，使网络在初期具备较高的活力，同时为后续长期发展奠定坚实基础。

1. **总量 21 亿、无预挖与减半发行**

   - **总量上限：** BEVM 代币总供应量设定为 **21 亿**，在数理模型与通缩预期之间取得平衡；
   - **无预挖、从 0 开始：** 创世区块时不进行任何预先铸造，所有代币皆由出块过程逐步释放，保证早期参与者与后期新进者在相同规则下公平竞争；
   - **每 4 年减半：** 借鉴比特币的通胀控制方式，每约 4 年（或指定区块间隔）对区块奖励进行一次减半，直至代币完全发行，通胀率逐步趋于 **0**。该机制既能在早期为网络提供充足激励，也在通胀收敛的后期维持代币价值稀缺性。

2. **区块奖励三元分配**

   BEVM 每个新区块的增发量采用“母共识 50% + 子共识 40% + 国库 10%”的三元分配模型，实现多方激励与生态共赢：

   - **母共识奖励（50%）：** 分配给 PoS 验证节点及BTC质押人，旨在保障网络底层的安全性与基本出块能力；
   - **子共识激励（40%）：** 专门用于激励 Agere 共识下的多 Agent 智能协作，通过“工作量+主观评分+权益质押”的综合评估，精准回馈对生态有实际贡献的节点或服务提供者；
   - **国库注入（10%）：** 注入国库合约，用于社区激励与风险储备等。该部分由去中心化治理流程负责管理与拨付。

3. **去中心化治理与资金使用**

   - **国库治理：** 国库动用需链上公开提案并经投票表决方可执行，提案范围包括新技术模块的资助、社区活动的支持、或紧急事件的资金调配等；
   - **动态调整：** 当网络规模或需求出现较大变化时，社区可发起提案修订国库比例、减半周期甚至整体分配方案，以在安全、通胀与社区活力间重新平衡；
   - **透明度与追溯：** 所有资金流动与投票过程均在链上公开，可由任何节点审计与追溯，确保决策的公正与透明。

5. 面向未来：BEVM的优化路径

为了构建完全符合BEVM(λ)范式的智能加密货币系统，在当前Agere共识的基础上，我们需要进一步解决以下三个关键问题。这些问题的解决不仅涉及技术层面的突破，还需对系统设计理论的进一步深化，以实现加密货币系统在能量守恒、去中心化和涌现特性上的全面优化。

5.1 共识量化算法的改进与涌现机制的探索

当前局限

现有的共识量化算法在实际应用中面临以下问题：

- 主观评分机制难以完全去中心化，可能受到少数节点的操控；
- 随着系统规模扩张，评分系统的计算复杂度和可扩展性存在瓶颈；
- 缺乏客观的贡献度量标准，难以实现公平与科学的资源分配。

优化方向

未来的研究将着力于以下方向：

1. **基于涌现原理的量化机制：** 开发能够体现系统自组织特性的量化算法，从而增强系统的鲁棒性与动态适应性。
2. **设计自组织评价体系：** 构建去中心化的评价机制，使贡献评估能够在分布式环境下实现高效和公平。
3. **建立科学的贡献度量模型：** 开发结合主观与客观因素的混合量化方法，确保资源分配的合理性与公正性。

5.2 Individual模型的设计与优化

当前局限

现有系统仍延续自以太坊的账户模型，这导致以下问题：

- 状态管理在实现上依赖全局存储，存在中心化特征；
- 系统缺乏真正基于Individual的自治性设计，难以满足去中心化原则；
- 每个交易单元未能实现独立性，增加了全局状态的复杂性。

优化方向

为解决上述问题，未来工作将致力于：

1. **设计新的分布式数据结构：** 开发以Individual为基础的分布式存储模型，确保数据的自治性与分离性。
2. **去中心化状态管理：** 在系统架构中实现状态的分散化管理，降低对全局状态的依赖。
3. **强化交易单元的独立性：** 确保每个交易单元具备独立自治能力，从根本上提升系统的去中心化程度。

5.3 λ演算体系的构建与优化

当前局限

现有的智能合约设计存在以下问题：

- 缺乏适应分布式场景的计算模型，导致执行效率低下；
- 图灵完备性与去中心化特性之间存在矛盾，难以同时满足两者要求；
- 缺乏专门针对去中心化环境优化的程序设计范式。

优化方向

针对这些挑战，未来工作将集中于：

1. **设计新的智能合约语言：** 基于λ演算理论，开发具有去中心化特性的智能合约语言，提升系统的执行效率。
2. **平衡图灵完备性与分布式特性：** 通过设计特定的语言约束和优化模型，在保持图灵完备性的同时确保分布式计算的高效性和可扩展性。
3. **实现去中心化计算架构：** 在分布式环境中，开发无状态计算模型，确保系统的可扩展性和去中心化。

6. 总结

本文通过深入审视以太坊提出的图灵非完备性、共识机制效率和网络扩展性三大问题叙事，发现这些技术改进实际偏离了加密货币的核心设计原则。基于这一认知，我们提出了BEVM(λ)范式，该范式通过Individual模型、λ演算、共识算法和共识感知算法四大核心

要素，不仅揭示了比特币成功的本质，更为智能加密货币的设计提供了理论基础。在此基础上，我们设计了创新的双层共识架构：以比特币为基础的母共识确保了系统的安全性和稳定性，而以Agere共识为核心的子共识则开辟了面向未来的智能化发展路径。

为了最终实现真正的加密货币智能化，我们团队将持续探索共识量化算法的改进、Individual 模型的强化和 λ 演算体系的优化。

7.参考文献

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[3] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, 1982, pp. 382–401.

[4] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,” in *CRYPTO 2017*, pp. 357–388.

[5] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” *Ethereum Project Yellow Paper*, 2014.

[6] J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016. [Online]. Available: https://lightning.network/

[7] Bitcoin Core Devs, “BIP-0341: Taproot: SegWit version 1 spending rules,” 2021. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

[8] M. Wooldridge, “An Introduction to MultiAgent Systems,” 2nd Edition, John Wiley & Sons, 2009.