Bit Gold

Nick Szabo[1]

December 29, 2005

A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. As many inflationary and hyperinflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs. Similarly, private bank note issue, while it had various advantages as well as disadvantages, similarly depended on a trusted third party.

Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions. Thus a trusted third party (usually associated with a tax collector who accepted the coins as payment) was invoked to stamp a standard amount of the metal into a coin. Transporting large values of metal can be a rather insecure affair, as the British found when transporting gold across a U-boat infested Atlantic to Canada during World War I to support their gold standard. What's worse, you can't pay online with metal.

Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof of work function," or "secure benchmark function." The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards.

Here are the main steps of the bit gold system that I envision:

A public string of bits, the "challenge string," is created (see step 5).

Alice on her computer generates the proof of work string from the challenge bits using a benchmark function.

The proof of work is securely timestamped. This should work in a distributed fashion, with several different timestamp services so that no particular timestamp service need be substantially relied on.

Alice adds the challenge string and the timestamped proof of work string to a distributed property title registry for bit gold. Here, too, no single server is substantially relied on to properly operate the registry.

The last-created string of bit gold provides the challenge bits for the next-created string.

---

[1] Nick Szabo，中文尼克·萨博，一个加密社区中人尽皆知的传奇人物。以其在智能合约和数字货币方面的研究而闻名于世，广泛涉猎于计算机科学、货币起源、经济和法律等诸多领域，同时是计算机科学家、法律学家兼密码学家。1989 年分别获得华盛顿大学计算机科学学位和乔治华盛顿大学法学学位，毕业后在弗朗西斯科·马罗昆大学担任名誉教授。

To verify that Alice is the owner of a particular string of bit gold, Bob checks the unforgeable chain of title in the bit gold title registry.

To assay the value of a string of bit gold, Bob checks and verifies the challenge bits, the proof of work string, and the timestamp.

Note that Alice's control over her bit gold does not depend on her sole possession of the bits, but rather on her lead position in the unforgeable chain of title (chain of digital signatures) in the title registry.

All of this can be automated by software. The main limits to the security of the scheme are how well trust can be distributed in steps (3) and (4), and the problem of machine architecture which will be discussed below.

Hal Finney has implemented a variant of bit gold called RPOW (Reusable Proofs of Work). This relies on publishing the computer code for the "mint," which runs on a remote tamper-evident computer. The purchaser of of bit gold can then use remote attestation, which Finney calls the transparent server technique, to verify that a particular number of cycles were actually performed.

The main problem with all these schemes is that proof of work schemes depend on computer architecture, not just an abstract mathematics based on an abstract "compute cycle." (I wrote about this obscurely several years ago.) Thus, it might be possible to be a very low cost producer (by several orders of magnitude) and swamp the market with bit gold. However, since bit gold is timestamped, the time created as well as the mathematical difficulty of the work can be automatically proven. From this, it can usually be inferred what the cost of producing during that time period was.

Unlike fungible atoms of gold, but as with collector's items, a large supply during a given time period will drive down the value of those particular items. In this respect "bit gold" acts more like collector's items than like gold. However, the match between this ex post market and the auction determining the initial value might create a very substantial profit for the "bit gold miner" who invents and deploys an optimized computer architecture.

Thus, bit gold will not be fungible based on a simple function of, for example, the length of the string. Instead, to create fungible units dealers will have to combine different-valued pieces of bit gold into larger units of approximately equal value. This is analogous to what many commodity dealers do today to make commodity markets possible. Trust is still distributed because the estimated values of such bundles can be independently verified by many other parties in a largely or entirely automated fashion.

In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation. Bit gold may provide us with a money of unprecedented security from these dangers. The potential for initially hidden supply gluts due to hidden innovations in machine architecture is a potential flaw in bit gold, or at least an imperfection which the initial auctions and ex post exchanges of bit gold will have to address.

比特金白皮书

一个基于公共货币的自治经济架构

作者：光明博士 [Bright@utopia.country]，Version 2.1.5

前言：《比特币白皮书》在开宗立编时，设想了“比特币：一种点对点的电子现金系统”。事实上，Bitcoin 和区块链技术通过多年的发展，已经部分地实现了这个设想，放眼 50 年后，这个设想将很有可能实现。但是在目前阶段，无论是整体性能、可扩展性、交易手续费、跨文化问题、用户体验、安全性等多方面，均未达到了民用的标准。比特金是一个比特币 3.0 形态的产品体系，是实现比特币思想的全新试验。

摘要：本文在汲取 Bitcoin 思想和归纳一些浅显金融规律的基础上，提出一套逻辑简单的解决方案，倡导“新金本位制、竞争发行、公共货币、去中心化数字资产配置”等方法，并通过技术手段实现了：抵押比特金竞争性地发行各国法币对应的数字货币（恒定币），从而实现了共识信任底层资产和应用层流通资产，再而真正实现了数字货币的价值尺度、流通等价物、贮藏手段、支付中介的能力，以去中心化智能合约广泛应用于“价值投资、在线支付、自动清算、商业合约、物权通证化等”等经济领域。整个尝试过程，将通过三个大的技术步骤：1、公共货币运行平台；2、数字资产自治架构；3、分布式经济架构。

关键词：公共货币、新金本位制、比特金、通证、良币驱逐劣币

1. 背景

我们可能需要一个更先进的经济系统?

1.1. 法币

货币是人类历史上最伟大的发明，法币是现行的货币，极大地推进了人类社会文化、政治、经济、科技各领域的进步。

但是，包含现金、电子支付手段在内的各国法币系统，以及跨国汇兑体系，其运行机制本质来说都是中心化的。人类曾经使用过的钱都或多或少存在一些不安全机制，比如伪造，盗窃，最致命的可能是通货膨胀。历史事实证明，“党权民赋”的政党统治体制并不值得人们充分信任。仅就政府垄断的货币发行权而言，政府垄断货币发行权之后，必然存在通过铸币税方式搜刮民脂民膏的冲动，政府掌握货币发行权之后失信于民事件历史上频繁发生，也是必然要发生的。类似这样的事件在金融类书籍里都是查阅证实，我们不便过多和深入例证“由主权中心化发行带来的法币问题”，但很明显，现有的央行式货币发行系统和国际汇兑系统，是发行组织的一个伟大政治工具而

已，是谋取权利红利的手段。政府拥有政权红利已经几百年了，并且智慧的人类正在寻求一种新的解决方案。

各个国家中央银行的货币政策就是要努力创造并维护这样的货币环境，并且，在更高层面上，不同的国家之间是货币政策是独立的、相互隔离的，且存在复杂的竞争关系，也就是说，现行的世界法币体系没有共同遵守的底层共识，没有通用资产背书，没有共同的信仰（信用）为基础。

1.2. 法币发行机制

人类历史上出现过各种的法币发行制度，现代的制度已经是政府说着玩的制度，根本不值得讨论论。我们去回顾一下曾经一定程序上公平的金本位制。

金本位即金本位制 （Gold standard），金本位制是以黄金为本位币的货币制度。在金本位制下，每单位的货币价值等同于若干重量的黄金（即货币含金量）；当不同国家使用金本位时，国家之间的汇率由它们各自货币的含金量之比——金平价来决定。

第一，黄金生产量的增长幅度远远低于商品生产增长的幅度，黄金不能满足日益扩大的商品流通需要，这就极大地削弱了金铸币流通的基础。

第二，黄金存量在各国的分配不平衡。1913 年末，美、英、德、法、俄五国占有世界黄金存量的三分之二。黄金存量大部分为少数强国所掌握，必然导致金币的自由铸造和自由流通受到破坏，削弱其他国家金币流通的基础。

第三，第一次世界大战爆发，黄金被参战国集中用于购买军火，并停止自由输出和银行券兑现，从而最终导致金本位制的崩溃。其中，布雷顿森林体系协议(Bretton Woods Agreement)，核心是将美元与黄金挂钩（固定汇率），其它货币与美元挂钩，是金本位制度的典型表述。

关于法币发行机制，我们有必要再提到另外一种思想《货币的非国家化》，作者哈耶克教授一生坚持自由市场资本主义，以反对社会主义、凯恩斯主义和集体主义而著称。在其晚年，哈耶克将经济自由主义思想贯彻到底，瞄准自由经济的最后堡垒——法定货币，质疑国家垄断货币的法理性，提出惊世骇俗的“竞争性货币”理论。其思想的核心是“**由多个主体发行各自的货币，用市场竞争的方式来完成优胜劣汰**”。碍于当时计算机技术、政治体系等原因，这个方案实际上无法实行。即使该方案有机会实施成功，其发行者照样拥有着全部的“铸币税”——以太坊的 ERC20 Token 基本上属于这种个体发行通证（类货币），是一种广义的实现方案，它获得了阶段的市场疯狂[2]，但也再一次印证了单一货币发行主体的信用问题。

1.3. 证券、积分与发行机制

证券是多种经济权益凭证的统称，也指专门的种类产品，是用来证明券票持有人享有的某种特定权益的法律凭证。主要包括资本证券、货币证券、商品证券等。狭义上的证券主要指的是证券市场中的证券产品，其中包括产权市场产品如股票，债权市场产品如债券，衍生市场产品如股票期货、期权、利率期货等。同理，各种企业内部绩效积分、外部用户积分等，都属于这个通证的范畴。

而其对应的发行机制，都基于中心化权力发行，同样有着“过程腐败、流动许可、跨组织、跨国界流动阻隔”等问题。

1.4. 互联网&物联网

互联网是基于 TCP 协议为信息传输服务网络，而区块链是为价值传输的网络。这句话精妙地概括了，互联网解决信息不对称的定位，同样让我们憧憬和好奇，去建一个价值自由流动的网络。

物联网的底层其实是物权的网络化协问题，物权包括了所有权和使用权等，我们可以简单地理想为：在含互联网在内的通信网络中，有形的万物，通过所有权、使用权、监察权等的分配，而让人与物之间的关系产生变化。换言之，如果我们能用共识的机制，让万物的物权量化、可交易，那么要解决万物联网其实就是解决可量化的问题。

所以，如果我们的经济系统“需要提供物权量化的能力和入口”，那将很美妙。

1.5. 区块链

狭义上，区块链（Blockchain）是一个分布式的共享账本和数据库，具有去中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点。这些特点保证了区块链的“诚实与透明”，为区块链创造信任奠定基础。而区块链丰富的应用场景，基本上都基于区块链能够解决信息不对称问题，实现多个主体间信任协作与一致行动。

在区块链技术基础上，诞生了比特币 Bitcoin[3]、以太坊 Ethereum[4]等多个成功的案例，二者各自发展成为典型代表：比特币成为了数字黄金的代词，以太坊是智能合约平台。区块链技术虽然还处在早期的发展阶段，但跨组织共识机制（甚至于跨国家）、统一数据协议、开放源代码等，引发了一场世界范围的热潮，如 DAO（去中心化自治组织）、DeFi（去中心化金融）、DAC（去中心化协作）等。而且，似乎这样的热潮正在将人类文明往陌生共信社会方向引导。

我们经济系统需要提高“跨组织（跨国）的信任共识底层”。

---

[3] Bitcoin wiki: https://en.bitcoin.it/wiki/Bitcoin, http://www.bitcoin.org

[4] Ethereum 官方网站: http://www.ethereum.org

1.6. 比特币

比特币（Bitcoin），实现了前所未有的区块链技术和金融现象：纯技术地实现了无实物对象的共识资产；实现了数千万倍的价格涨幅空间。它的成就举世瞩目，让全世界的拥趸为之疯狂。但是，比特币和比特币网络也存在一些问题：

- 巨大的能源消耗，其电能消耗已经达到了中等人口国家的耗电规模
- 区块链性能，可容纳交易量极小（相比于当前互联网软件）
- 延时问题，每 10 分钟为周期
- 可扩展性问题，技术整体脆弱性
- 价格剧烈波动，无法满足常规交易需要
- 链上交易手续费问题
- 郁金香的影子，无大规模的应用场景，让其缺少资产背书
- 技术开发可能进入了“积重难返的民主怪区”

正是基于对比特币美好面的遵从和缺失面的反思，我们认为一个经济系统需要“法币”——恒定价值的货币。

2. 理想

假定我们奉行的大旗是“人类总是在永不停歇地寻找更能适应和促进人类文明前行的新秩序”，那么经济系统该如何建立新的秩序？我们需要一个怎样先进的经济系统？

2.1. 理想货币系统

一个理想的经济系统，首先需要一个理想的货币系统。

2.1.1. 理想的货币

因为只有完全普遍接受的价值尺度，才可能构成世界范围的经济大协作——履行货币“价值尺度、流通手段、贮藏手段、支付手段、世界货币”的职能，这个目标是目前任意一种单一法币无法完成。所以，我们在寻求理想的货币。

加密货币与智能合约之父提出：如果有一种协议，能够对“受信第三方”的依赖降到最低，在线创造出无法伪造的、有价值的数位字符，并且被安全存储、转账和验证，这就是“比特黄金”[5]——这既是比特币的思想源头，也是我们追随圣贤的试图往前一步寻找一个理想货币系统的动力。

理想货币具体的样子非常难以定位，假设为暂定为理想货币是币值长期稳定的货币，理想货币应该是既没有通货膨胀，也没有通货紧缩——不会因为“货币政策”而产生不公平；理想货币应该是现行法币的能力之上的全球共识性一个或多个货币；理想货币应该在“耐用性、便携性、可分割性、统一性、有限供应量和作为一种支付方式的普遍接受性”等 6 个关键特性上获得更多提升。

我们可以想象一下它的样子：

- 有底层资产背书：一种全人类共识的本位资产
- 完全自由流通：不因中介系统（如银行）而存在汇兑交易限制
- 适量供应（弹性供应）：需要的时候总量应需增加，反之亦然
- 价格约等于公充价值，不因总量供应影响价格稳定
- 文化与历史的适应，符合区域文化与情感归属
- 不影响现行的经济，自然并且逐步转移

---

[5] The **Bit Gold** proposal, by Nick Szabo, describes a system for the decentralized creation of unforgeable proof of work chains, with each one being attributed to its discoverer's public key, using timestamps and digital signatures. It is said that these proofs of work would have value because they would be scarce, difficult to produce, could be securely stored and transferred.

并由此推导，理想货币系统可能的样子：

- 没有一个人或群体能控制：完全去中心化
- 无中介：没有人为的中间手续影响交易的完结
- 自由存储和转移：任何个人、企业、其它组织都可以全权处置
- 自由结算：交易即结算，也就是没有清算类的环节
- 自主隐私：有主动权选择财务透明与隐私
- 透明可追溯可审计：用于数据抽象、可视化呈现、审计监察
- 系统开放性：充分开放系统能力，丰富接入应用场景，实现生态化自治

为了尝试解决法币系统“无法自发改良，无法公平发行，跨文化使用门槛高”等问题，我们提出了基于区块链的理想货币——公共货币，请见后文。

2.1.2. 理想的本位资产

其次，我们需要寻找一种“本位资产（底层资产）”。

在金本位制体系下，由于黄金总量有限、地域分布不均、难以移动、无法可视量化、主权政治影响等其无法满足全球经济多样性和快速增长的需求。

随着互联网、区块链技术和数字经济的发展，如果存在一种普通接受的通用资产，拥有如下几个特点（相比于黄金），就可能可以成为新的本位资产：

- 不会被中心化组织（群体）所控制
- 有公认的价值内在：无论是信用型资产还是实体资产，需要全球全民共识
- 没有时间空间的限制：跨国界、跨地域文化、跨时间
- 不受物理形态约束：任意交易或抵押行为，易于或者不需要物流运输
- 没有总量变化：底层资产应该是完全固性的，无变化量
- 易于存储、交换、锁押（易用性）：通过软件终端加强易用性体验

这种优于金属黄金的本位资产，有可能催生统一本位制的货币体系。事实上，比特币和以太币具备了大部分如上属性，以比特币和以太币为基础的 DeFi 发速发展（去中心化金融）已经演示了去中心化货币体系的可行性。

所以，我们认识了“理想的本位资产”的样子了。

2.1.3. 理想的货币发行机制

再次，我们需要寻找一种“发行机制”。

我们简单回溯人类货币的发行机制，从物物交换，到贝壳为代表的稀有物品，到金属货币，到政府信用票券，到金本位、外汇本位等，都是一个中心化集权的过程，并且伴生超发与通货膨胀等金融经济现金。即便到了诺贝尔奖得主哈耶克先生的多币竞争思想和 John Nash 的《理想货币》，都是以一揽子商品为本位资产的解决方案——既无法与传统利益者对抗，也无法解决发行公平性问题。

随着计算机、互联网和区块链等技术发展，尤其是比特币的出现、发展和阶段性的成功应用后，我们已经清楚地看到了一种新的基于“计算机算法”的发行机制。但我们之前分析过，比特币不足以作为流通货币，人们已经默认赋予比特币“数字黄金”美誉。比特币也已经召示了一种货币的发行机制“矿工发行”：

- 自由创造多种公共货币：宏观上可以形成多币种竞争的态式
- 自由发行：发行公共货币，中观上形成按需印钞的格局
- 自由销毁：销毁公共货币，满足理想货币的弹性供应需求
- 全民参与：没有任何一个主体是中心，甚至主权国家都无法左右数量
- 保持健壮：发行机制需要长期保持健康运行状态

2.2. 理想的数字资产治理

2.2.1. 通证化

要想让经济系统减少摩擦，自由协作，有两三个步骤一定要实现，首要的是信息化自动化协约，而要实现基于网络的自动化合约协作，最重要的是让所有“价值”量化到该系统里——“通证化”是一种理想的办法。

广义而言，通证其实是一种“将对象量化后的代表手段、媒介”，之前我们了解的货币是一种通证、证券债券是通证，各种可以量化介质，都是一种通证。

狭义来说，通证是以数字形式存在的权益凭证，它代表的是一种权利，一种固有和内在的价值。通证可以代表一切可以数字化的权益证明，从身份证到学历文凭，从货币到票据，从钥匙、门票到积分、卡券，从股票到债券，账目、所有权、资格、证明等人类社会全部权益证明，都可以用通证来代表。

更粗暴的通证，其实是现在区块链上的代币（TOKEN），但的确是一种实现通证化的好办法。所以，区块链为我们带来一个普世的机会和优秀的介质，可以简单的进行“资产、权益的通证化”，从而带来变革性的便利：

- 任何资产都可以进行量化拆分和打包，实现通证化
- 自由流通：增加流动性，可以无限细化和交易，并降低交易成本
- 开放市场，与资本直接连接，例如股权通证
- 优化管理方法和应用
- 可编程，实现跨组织社会化合约使用资产通证

2.2.2. 自由市场/开放式交易

自由市场是最好的配置资源的地方，自由市场或开放式交易平台必须满足以下要求：

- 公开透明：所有交易都应该完全公开透明，使得所有人都可以监督和信任这个交易平台。
- 安全性：交易平台应该采取各种措施保障交易安全，例如冷热钱包分离、多重签名技术、安全网络等。
- 低成本：交易平台应该尽可能地降低交易成本，包括交易费用、网络费用、兑换费用等。
- 大量选择：交易平台应该提供大量的货币选择，使得交易双方可以充分自由地选择。
- 高灵活性：交易平台应该提供高度灵活的交易方式，包括限价交易、市价交易、交易深度等。

基于一切有形的物品和无形的价值都可以被通证化，那么，公平、平滑、即时、自由的通证交易就变得非常重要。换言之，在通证化成 Token 后，Token 是可以像水和空气一样，完全自由购买和出售。

内生式交易：发挥公共货币的价值信任优势，通过智能合约，或者链下协商链上转移的方式，不需要借助第三方的交易平台完成数字资产交易。比如内建域名、游戏道具、股权、积分等，可以用公共货币即时完成交易过程。

去中心化交易：通常我们指撮合交易市场（Exchange），通过竞价的撮合交易，达成数字资产的竞争定价与交易转移。去中心化交所可以解决极大多数的数字资产交易所有诚信和安全问题，全部通证都可以自由交易。

第三方交易市场：通过第三方交易服务市场完成数字资产交易，实现资源按需配置。例如中心化的交易所，线下交易所，官方网站交易，社交媒介交易等。

为了实现货币交易的开放和自由，需要建立自由市场或开放式交易平台，使得交易过程公开透明、交易双方可互相信任，保障交易安全和效率，并能够提供大量的选择和灵活性。

通过以上要求的满足，可以建立一个开放、安全、透明、低成本、大量选择、高度灵活的自由市场或开放式交易平台，推动货币的自由流通和全球各地的经济合作。

2.3. 理想的组织与合作

2.3.1. 去中心化自治组织 DAO

去中心化自治组织，Decentralized Autonomous Organization。相比于基于亲情关系产生的家庭，基于合伙协议产生的合伙团队，基于员工雇佣合同产生的责任公司，基于投资协议产生的集团、财团，DAO 基于技术化的社会契约而产生一种新型组织，我们可以简单地定义为“DAO 是由陌生成员按事务技术合约自由组合，为特定的目标进行社会化协作的松耦合型组织形式”。

我们来说明去中心化组织与中心化组织的区别：美国作家奥里布莱福曼在一本名为《海星与蜘蛛》书中写道，蜘蛛是中心化（细胞）组织，如果把它的头切掉后整个身体就无法生存了；海星则是由彼此对等（无中心）的一堆细胞组成的，海星撕下的每只触手都可成长为完整的海星。

DAO 的重点在于去中心化自治，在现有组织形式地基础上加强了组织的社会性，即社群自治——DAO 的发起人、主创团队就是目标制定者、协作规则策划者，参与成员可以安照即定规则、流程、经济报酬等参与组织，自由进出；另外根据开放程度的不同，成员参与社群事务也略有差异，优秀的 DAO 应该充许全员参与方向、战略、规则、形象、事务等各方面。

去中心化的显著特征是社会化（Socialize），是一个小团体（个人）将大部分事务“外包”给陌生的人和组织，并完成目标的过程。全部或大部分事务外包的组织都可以称为 DAO。已知的大型互联网平台，基于平台软件即规则进行协作，都是 DAO 的雏形。但真正能代表 DAO，其实是 Github 上一些著名的软件项目团队，是比特币、以太坊社区这样的社会化协作组织。成员们自发地组成了一个个“小生态”。

DAO 在共识机制和分布式网络的共同作用下，成为一种介于产业和企业之间的组织形式。一方面，它以分布式网络实现了资本的高效率分配，解决了信息的不对称问题。另一方面，通过共识机制建立起超越简单熟人关系的信用体系，从而能够形成以共享经济（或者叫分享经济）的新经济模式，从而打破了新古典经济中关于企业和市场关系的一系列限制，创造了新的组织结构。

在当前阶段，工作量可量化、流程可标准化的组织体都可以开始进行 DAO 尝试。而另一方面，万能的通证（Token）是可以将任意对象通证化（Tokenize），那就意味着任意对象都可以量化——因此在通证赋能的基础上，只要流程能够用软件应用来完成，就非常容易地制定组织的社会化方案。

2.3.2. 诚信协作

去信任（Trust-less）合作，即不基于信任的合作，是最少合作摩擦成本的终极目标。

在商业活动中，从古到今，都是朝着“减少欺诈，减少摩擦，共信合作”方向前进，现代商业社会以法律作为了商业活动的最低标准。实际上，商业活动还可以朝着“去

信任合作”更进一步。智能合约正是这样的产物，无论是普通的伙伴间合约，还是陌生人之间的合作规则，更或者是大型机构或全民的共同协作，都可以以智合约的形式诚信协作。

3. 实现

如何实现这个理想经济架构？我们将继承《货币的非国家化》、《Bit Gold》、《比特币白皮书》、《以太坊白皮书》、《以太坊白皮书》等先贤著作的思想和实现，并基于 Bitcoin 和 Ethereum 现有思想去设计和运行一个新的平台。这将是一个长期、不确定进程且永续迭代的过程，以下为 Openverse 2.0 的实现部分。

3.1. 价值协议

价值协议，Value protocol，是一个开放性价值传输协议，我们可以简单理解为跟邮件传输一样的开放性协议。所有区块链均可通过价值协议，来交换价值，就像传统的邮件网络一样，myname@gmail.com 传输至 yourname@facebook.com 这样，通过 Openverse 将 token/ntf 等价值资产，即时传输至以太坊（ethereum）、波卡网（Polkadot）等区块链网络。具体请见《价值协议白皮书》及价值协议官方网站。

3.2. 核心程序 VerseCore

开源的 VerseCore 是价值协议一个 Go 语言程序实现，包括企业和个人在内的每个个体，都基于 VerseCore 可以搭建出无数的 POW/POA/POS 区块链网络。

通过 VerseCore 搭建的每一个网络将生成为一个个的去中心化经济生态，每个生态将服务于特定的行业和地域。每个生态将主张完全去中心化，为智能合约、去中心化应用提供运行平台。

为了适应复杂社会多样的经济活动需求，和兼顾区块链技术的发展进程，VerseCore 将分阶段在基础层实现：弹性、安全性、扩展性兼顾的区块链核心。

3.3. Openverse Mainnet

Openverse.network：
是基于 VerseCore 2.0 代码持续演进的技术网络，是包含分片结构、采用 POS 算法、运行虚拟机的区块网络。Openverse 定位于数字资产的运行平台。

中枢链，Openverse.network：
中枢链指挥整个 Openverse 2.0 系统，中枢链的关键功能是管理 POS 协议以及所有的分片链。它有很多方面的工作要做：管理验证者以及他们的权益；在每一步为每个分片指定所选的区块提议者；组织验证者进入委员会，对拟议的区块进行投票；应用共

识规则；对验证者实施奖励和处罚；并且，作为一个锚点，其中分片会注册它们的状态，以促进跨分片交易。中枢链不运行虚拟机、不处理智能合约。

业务链，Zones：
业务链是具体执行事务的链，运行虚拟机、智能合约等。各业务链之前通过协议的方式，与其它链产生价值交互。

共识算法：
权益证明（POS），Casper FFG 是 DEE POS 共识机制的名称。验证者（矿工）将抵押比特金，参与区块的验证，并获得计算收益（挖矿收益）。在三元悖论[6]，Casper FFG 机制在做出决策的时候更倾向于保障安全性而非活性。

域名系统 Universal Name Service：
Universal Name Service，即开放域名服务，一个基于开放的可扩展区块链域名服务系统。各个区块链网络/元宇宙都可以在 openverse 网络上注册其主域名。其主要作用是，将 Openverse 的多位乱码式地址，翻译成可读、易输入的字符串。具体规规范，请见官网技术文档。

智能合约：
Openverse 智能合约完全兼容（2.0 时代为等同于）以太坊智能合约，采用 Solidity 编程。并且鼓励社区提供智能合约模板库。

DAO：
基于 Openverse 网络上的智能合约，任意主体都可以创建自己的 DAO。然后，以前所未有的方式进行投资、筹资、投机、交易、保险、借贷、创办合资企业，以及进行更多的数字资产的在线管理，进行各种协作。

DEX：
基于 Openverse 网络上的智能合约，可以开设数字资产自由交易。

3.4. Openverse 数字资产归类

Openverse 提供综合的数字资产治理能力（发行、合约、去中心化交易），用价值量化和流通真正为跨组织（国家）经济活动提供有用的服务。

3.4.1. 本位资产

[6] FLP 不可能性（FLP impossibility）是分布式计算领域的一个关键成果，其指出分布式系统不可能同时具有安全性(safety)、活性(liveness)和完全异步性(full asynchrony)。

比特金，Bitgold，简写为 BTG。是 Openverse 主链的核心资产，是经济底层，已知的用途主要包括：成为公共资产的质押资产，交易费用，POS 共识的抵押资产，智能合约的价值源头。

取名出发点：基于对尼克萨博先生 Bit gold 原型理解和思想继承，基于对 Bitcoin 先锋地位的遵从，基于对黄金在金融历史上起到过的作用的延革——为了易于理解其在 Openverse 体系中的作用，我们将全新的本位资产名称取为“比特金/Bitgold”。

发行总量：根据世界黄金协会（World Gold Council）提供的 2022 最新数据，自有人类文明以来，世界共开采黄金 20.48 万吨(每年增加约 3000 多吨)；Openverse 区块链约为三年减半，故以数学视角取了一个同等规模的恒定数字——2 亿。即 BTG 的发行总量为 2 亿枚，该数字恒定不变，所有开发者应该优先考虑小数位的移动，绝对不应该考虑数值的变动。

3.4.2. 公共货币

公共货币，也可以称为比特法币/bitcurreny，是由公众全员通过抵押比特金并竞争式地发行的公共资产，为了便于与以太坊的 ERC-20 命名为参照，我们取名公共货币标准的代号为“VRC-10”。在我们设计中，公供货币是一种恒定价值的数字资产，比起稳定币来说，**我们希望人们认为它就是法币的另外一种出现的形态，而不是竞争品**，所以我们取名和代号的时候，直接引用对应的法币名称。世界上目前没有这种公共货币，虽然看起来相似但其实完全不同的例子如 USDT，它是 USD 的竞品而非同质品；当然，更大的区别，它是由 Tether 公司中心化发行的产物。

Openverse 内嵌已发行公共货币是锚定于各国现行法币的公共货币：

名称	公共货币代号	中文翻译	国别
U.S.Dollar	USD	美元	美国
Canadian Dollar	CAD	加元	加拿大
Indian Rupee	INR	卢比	印度
Japanese Yuan	JPY	日元	日本
Chinese Yuan	CNY	人民币元	中国
.....			

共计约两百多种法币[7]，涵盖目前全球的主权国家的全部法币，已经集成到 Openverse 主网成为公共货币，并且，可自由扩充更多公共货币。

3.4.3. 通证标准/Token

[7] https://www.iso.org/iso-4217-currency-codes.html

VRC-20、同质性通证/Homogeneity Tokens

同质性通证，Homogeneity Token，又可称为通证或翻译为令牌，狭义上它是一种区块链上的同质型代币，标准代号为 VRC-20。可以用于股权、企业积分、软件使用天数/次数、用户消费积分、游戏点券等各种应用场景。

VRC-721、非同质性通证/Heterogeneity Tokens

非同质通证，Heterogeneity Token，可以理解为不可互换的通证。简单地说，就是每个 Token 都是独一无二不能互换的。可以用于版权、具体物权、游戏道具、域名等。

VRC-30、时间通证/Timing Tokens

时间通证，Timing Token，狭义上它是一种区块链上的时效型代币，标准代号为 VRC-30。具体而言，它的有效性是随 Openverse 主链上的区块序号为标准，产生、使用和灭失，一个 Token 将在某个区块产生到某个区块消亡。可应用于物联网使用权等。

其它更多标准的 Token

根据未来应用情况，进行各多扩展，并通过公共智能合约模板市场，分享使用。

3.5. 公共货币发行机制

所以，我们分析金本位、央行法币发行机制的缺陷，结合区块链技术，提出了一种全新的设想公共货币发行解决方案——**公共竞争发行制度**。由于其本质上是动态抵押本位资产比特金，我们又可以称之为“新金本位制”。

公共货币发行制度（Public Currency Issuance Mechanism, PCIM），通过超额抵押资产、全民参与竞争式发行公共货币的货币发行制度。PCIM 有几个要点：

- 全民可参与，任何拥有本位资产的个体都可以参与竞争发行；
- 超额抵押本位资产，抵押产出公共货币；返还时货币时，解押本位资产；
- 无利息和交易成本；
- 随时可以参与竞争发行活动；
- 高频次，以区块周期为时间标准进行竞争发行；
- 共同发行公共货币，如各种现行的法币和未来更多需要的公共资产；

最终优势：良币驱逐劣币

公共发行的货币，带来了货币间的竞争，并且是在全球范围内竞争，人们可以跨主权地选择长期稳定的货币，最终将让劣质的主权法币没有生存空间。

4. 应用场景

4.1. 比特金应用

“比特金只有一个用途：做为本位资产——如抵押发行公共货币”。

“虽然概率极小，但 50 年后，比特金可能会是世界统一的货币——假定，比特金最终价格稳定在一个水平，届时公共货币将慢慢消失”。

4.2. 公共货币应用

“公共货币是法币在区块链世界的映射，是共信经济与正统经济的桥梁”。

“公共货币是 M0”。

“公共货币将用到法币能用到任何地方，并且无限延展法币的能力”。

“当比特金宠大到足够量时，公共货币将自行缩减直至消失”。

4.2.1. 世界级的支付业务

以“等同于法币的 Openverse 公共货币”和“企业私域稳定币、稳定价值积分”等为代表数字资产，结合数字货币的其它优点，并基于完全去中心化的 Openverse 网络，无数的企业都能直接开通支付业务服务。这是有别于数字货币 1.0 时代的状况（因为比特币的价格是剧烈变化，而现有的稳定币是中心随性发行的）。因为公共货币就是法币，所以拥有法币支付、电子支付的优势，又具有区块完全自由的支付能力。同样，在企业私域价值因企业信用背书，所以企业发行自主背书的支付通证，实现私域支付业务。

各种面对面、APP、网站直接接入 Openverse 区块链，就进入世界统一的支付和结算体系。

4.2.2. 去信任的借贷业务

随着数字货币应用范围的不断增加，利用数字货币直接（不需要转换为法币，投资的收益也以数字货币计价）进行投资的领域和机会逐渐增多。利用数字货币创造价值的人需要更多的数字货币，手中持有数字货币的人需要保值增值，数字货币的借贷业务需求会越来越多。

4.2.3. 无摩擦的交易中介

公共货币成为 Openverse 体系内去中心化交易所的交易对中介货币，以及其它中心化交易所的中介货币。平滑链内链外、站内站外的交易。

4.2.4. 低汇率、实时的跨国汇兑

发挥 Openverse 主网转账的低手续费、实时完成、完全自主实现无管束的国际汇款、兑换用途。打破现有法币的主权边界，用于各种国际支付、汇兑用途。

4.2.5. 其它法币用途

例如消费支付、员工薪水、企业支付、智能合约履约支付等。

4.3. 同质性通证应用

4.3.1. 应用于“股权”

我们可以把可能由多个主体拥有的权益进行通证化，例如企业股权、企业收益权、物品所有权、物品收益权、构成竞争关系的表决权等。以企业股权为例，在股权通证化后，可以进行通证化私募、公募、发行期权给员工，可以进行转让交易和公开竞争式交易等，可以结合企业上下游进行利益整合。

4.3.2. 应用于“积分”

将有一定权利、利益的非股权同质性用以通证化成“积分”，例如软件使用次数、员工累计积分、游戏里消耗性积分等。且可以自由交易。

4.4. 非同质性通证应用

相比于同质性通证，异质性通证也有着广泛的实体经济和物联网方面的用途。它可以代表任意的单一实物和虚拟道具，例如各种不同分隔的实体、各种证卡照、各种物联

设备、游戏道具等，这些单一不可再分的物品道具，可以成为非同质性通证。且可以自由交易。

其中，物联网设备，例如汽车、门禁、演唱会门票这些需要有“钥匙”授权使用的物品，进行通证化，可以带来更多的想象空间。

4.5. 时间通证应用

时间通证可以应用于有时效限制范围的场景，比如对于租赁设备的使用权、投票表决权等，可以在原生网络上进行时间通证的交易。

4.6. 智能合约应用

在人类智慧的加持下，智能合约几乎无所不能，我们可以例举一些做为参考，并在实现过程中持续扩充（详情智能合约模板市场）：

金融衍生品：金融衍生品合同基于标的物的价值，是公司对冲投资或交易风险的工具，如大宗商品或货币风险。Openverse 可从多个来源收集价格信息，整合数据，发送至智能合约，并发送支付数据进行结算，自动执行衍生品合约。市场中的公司通常直到建仓之前都会尽量拖延付款，因此使用 Openverse 技术的智能合约非常有助于重建交易对手方之间的信任关系。

债券：先发债后偿还是短期融资的理想方式。债券合约可以编写成自动执行、无需信任且去中心化的智能合约。Openverse 可以用公共货币结算，同时也可消除对手方风险，因为各种去中心化认证的数据（如银行拆借利率）将自动触发付款

市场数据上链：资产在不同交易所的挂牌价格不同，因此需要将多个来源的数据汇总，以得出一项资产的准确价格。Openverse 外部数据链 Value Oracle 将提供足够的数据上链服务，做为其它智能合约的资源。

去中心化的交易所：去中心化交易所中，资金在用户钱包地址或者交易智能合约中，由用户完全控制。用户发起交易时，交易所执行智能合约来完成交易，资产划转在链上完成。交易记录链上可查，公开透明。实现资源自由配置。

……

4.7. DAO 应用

DAO/DAC(Decentralized Autonomous Organization/Corporation，去中心化自治组织/企业)也许能够衍生出人工智能的概念。去中心化自治网络能够在完全没有人类干预的

情况下，在预先设定的业务规则之下，在类似于公司的模式下自动运行。在 DAO/DAC 中，会有一些智能合约在区块链上运行，根据预先设定的范围，也可能是根据事件和条件的变化来自动执行预先批准的任务。

区块链上，这些智能合约不仅能够像一个自治企业模式这样可以运作，还能够构建一些完全和现实世界中商业模式一样的功能。随着比特币交易变得越来越流行，这使得汇款市场变得更加有效率，而 DAO 和 DAC 也能够完成相同的事情。一个汇款公司可能在面对现实世界和在与当地行政管辖区域有不少需要协调的地方，也必然会耗费许多成本，我们知道开办企业就要与现实世界打交道，必然要考虑诸如营业许可、登记、保险、税务等许多行政事务和监管法律，也因此会产生许多成本。而这些功能如果能够移植到区块链中，这些功能也许将变得更加有效率，而有些事务工作则完全不需要了，并且所有的业务天然就是全球化的。基于云计算的，基于区块链的自治企业实体能够像政府在行政区内自助注册一样，根据智能合约和电子合同来完成任何它们所需要的操作。每个企业首先将能变成全球性的企业，而那些受到司法管辖区域限制的商业模式也由此可能获得更好的选择。

5. 愿景

5.1. Openverse 2.0 公共货币运行平台

创建一个新的平台，拥有类似于比特币众多优点的本位资产，通过竞争性地发行流通用途的公共货币，这些货币将继承现行法币的优点，广泛地应用到经济领域各个环节；再在公共货币强共识的基础上，将有形无形的价值介质进行通证化，实现公共货币运行平台。更进一步，通过去中心化交易所、接入支付等应用层的努力，实现数字资产运行平台的目标。

5.2. Openverse 3.0 价值协议与交换中枢

在 Openverse 3.0 的时代，预计在 2024 年启动规划和启动开发工作。在技术上，引入同质链群，将各种非数字资产生命周期相关事务分离到同质链群——是分片机制的缩减机制和延展。任何个体都可以用 Openverse 代码运行独立的同质区块链网络，共享主网的安全性，解决私域应用性能问题；并且官方将主动资助类似同质链的开发和运营。与主网之间的互通性在于账户、本位资产、公共货币、本链主资产。各种行业协会、联盟组织、经济相关的生态都可以自行运行 Openverse 同质区块链提供公共服务.

5.2.1. Web3 的一个基础设施

我们正处于一个从集中式互联网（即 Web 2.0）向去中心化 Web3 转变的时代。在 Web 3.0 的概念下，用户创建的数字内容的所有权明确由用户拥有和控制，创建的价值也将根据用户和他人签署的协议进行分配。我们需要一个全球性的 web3 基础设施。

5.2.2. 区块链的交换中枢

在目前的情况下，每个区块链网络都形成了自己的生态和小社会，是一个价值孤岛。许多团队已经开发了大量的桥接器和协议来连接各个区块链网络。在此基础上，我们正在进行下一步的研发工作。通过链间通信协议，不同的区块链网络可以安全地进行通信。

5.2.3. 元宇宙的系列协议

就像区块链网络之间的通信一样，所有元宇宙生态系统也需要互联互通。连接基于相互接受的标准和协议。Openverse 团队试图收集和整理分散的协议，形成元宇宙的统一协议系列，打破各种信息孤岛，让用户持有价值可以自由流动。

5.3. Openverse 4.0 分布式经济生态

Openverse 4.0 将支持异构链群的整体建设和性能的极大提升，支持第三方区块链以协议的方式接入，着重于生态接入开发，形成了分布式经济生态的形貌。

6. 更多

如果 Openverse 体系有实现的可能性，那么在这里说的更多的是寄托和它虑。

6.1. 技术主张

我们需要很长时间去实现整个体系的情况下，需要在早期的时候定位一些原则。

去中心化：完全去中心化，最终实现完全不被个别意志左右
键壮性：任何现实世界的变故都无法停止整个网络的运行
安全性：实现分布式共识机制，算力分布于细支，无法发生群体性违背协议事件
简洁性：核心只处理协议本身，不涉及应用场景的逻辑等
持久性：网络长期运行，甚至于前瞻性地考虑量子计算问题
环境保护：确保键壮性和安全性的情况下，不应该增加能源消耗和硬件反复投入

6.2. 运营主张

主动发展：除了主网技术持续迭代，团队将持续开发周边普及应用，例如丰富功能的钱包、DAO 模板、常见智能合约模板、去中心化交易所等。

追求价值：以比特金作为底层资产，所以当它的经济总值有多大就能容纳更多的实体经济，从而加速整个发展进程。

6.3. 社会主张

我们相信 DAO 和智能合约是实现陌生主体之间资源合理整合和无信任协作的有效形式，也信相会诞生一些知名的 DAO，它们在新社会中起到了超越公司、集团、财团等线织形式的巨大的社会功能。

因而，能够研究、策划、设计、运营一个 DAO 的人，都会是精英和智者。也继而可以推断，将来的世界会是一个智者治理的社会。

6.4. 文明

文明的更迭和演进，是去除黑暗寻找光明的过程，组织间合作于共识正是这样的过程，而经济是文明的催化剂和推进剂，所以，我们可能也将见到“文明新进程”。所以，各种文化将会一步在新文明下进行融合和发展。

6.5. 法律

虽然我们定义 Openverse 为一场伟大的试验，但在 Openverse 体系中，比特金尝试成为世界金融底层资产，公共货币本质上是 M0 目标是部分替代法币，都远远超过了现行法律所容忍的范围。例如，Facebook Libra 在早期就遭遇了种种阻碍看来，无论从意识还是法律上，Openverse 都将无数次地面对各主权国家的法律责难。

我们应该认为它是“需要寻求既得利益群体包容和法律开恩”的伟大试验。

6.6. 机构

Openverse 是由 Utopia Foundation[8]资助和支持的项目。

Openverse 是由 Openverse Team 主持开发和治理的项目。

[8] Utopia Foundation，一个主张“科学主义 Scientism、自由主义 Pietism、虔敬主义 Liberalism”的开放型公益组织。

参考资料

1、Nick Szabo, 《Bit gold》, December 29, 2005, https://nakamotoinstitute.org/bit-gold/

2、Bitcoin wiki: https://en.bitcoin.it/wiki/Bitcoin, http://www.bitcoin.org

3、Ethereum, http://www.ethereum.org

4、Friedrich uon Hayek,《Denationalisation of Money》

5、Zvi Bodie/Alex Kane/Alan J. Marcus,《INVESTMENTS》

6、Fank J. Fabozzi/Franco Modigliani/Frank J.Jones,《Foundations Of Financial Markets and Institutions》

7、Yuval Noah Harari, 《Homo Deus - A Brief History of Tomorrow》

8、《[The End of Money the Story of Bitcoin，Cryptocurrencies and the Blockchain Revolution》

9、N.Gregory Mankiw,《Principles of Economics》

10、ROBERT J. SHILLER,《Bubbles, Human Judgment, and Expert Opinion》

11、J. Bradford De Long, Andrei Shleifer, Lawrence H. Summers and Robert J. Waldmann, 《Noise Trader Risk in Financial Markets》