



Bit Asset Chain


去中心化高性能数字资产管理公链

V 3.0

2020.08.01

目 录

Bit Asset Chain.....	1
去中心化高性能数字资产管理公链.....	1
第一章、摘要.....	4
第二章、现状与改进.....	5
2.1 稳定的性能与可靠性.....	5
2.2 被社区认可的经济系统.....	5
2.3 完善的配套生态.....	6
2.4 监管配套机制.....	6
2.5 升级空间.....	7
第三章、BAC Chain.....	8
3.1 共识机制.....	8
3.2 智能合约与内置合约.....	10
3.3 存储网.....	11
3.4 跨链.....	12
第四章、去中心金融(DeFi)应用.....	13
4.1 发行 Token.....	13
4.2 稳定币.....	14
4.3 去中心交易协议 DEX.....	15
4.4 去中心化借贷.....	17
4.5 征信系统.....	23
4.6 基金专户.....	23
第五章、其他区块链应用.....	25
5.1 物流追溯.....	25
5.2 数字版权.....	25
5.3 支付.....	25
第六章、BAC Chain 技术详情.....	26
6.1 经济系统.....	26
6.2 总体模块.....	27
6.3 POS+BFT 共识.....	29
6.4 费用模型和激励体制.....	32
6.5 智能合约.....	34
6.6 预言机.....	35
6.7 治理.....	35
6.8 数据存储.....	36
6.9 安全多方计算 (MPC).....	38
6.10 监管.....	38
6.11 安全.....	39
6.12 扩展.....	41
6.13 BAC 的配套生态.....	41
第七章、技术路线图.....	43
7.1 2020 年 4 月主网上线.....	43
7.2 2020 年 7 月存储网上线.....	43



7.3 2020 年 8 月推进开源，开启应用.....	43
7.4 2020 年 11 月实现去中心化协议.....	43
7.5 2021 年 1 月内置合约实现 DeFi 业务模型.....	43
7.6 2021 年 6 月合约上线.....	44
第八章、参考资料.....	45

第一章、摘要

自从 2009 年 1 月 3 日第一个比特币被挖出以来，区块链技术已经走过了 10 个年头。在过去的十年中，区块链行业在质疑声中稳步发展，并逐渐被大众所认可和接受。如今各国的央行已经在研究发行基于区块链技术的数字法币，而像 Facebook 这样的跨国企业也发布了基于区块链技术的 Libra 项目，高盛、彭博社等老牌金融机构也开始涉足区块链业务。

数字资产源于比特币，是一套以密码学为基础，基于公钥和私钥的分布式账本系统，数字资产的诞生，使金融服务的去中心化成为了可能。与传统金融以银行为中心的账户系统相比，去中心化的金融服务具有更高的效率，更低的成本，并且运行机制更加的公开，公正，透明。预计在不远的将来，会有更多的用户和机构参与到去中心化的金融世界中，从而诞生出很多与数字资产管理相关的新型服务。这些服务有可能是现有金融服务类型的延续，比如转账，衍生品交易，理财基金，资产托管，抵押贷款，供应链金融等，也有可能是崭新的金融服务类型，比如，数字资产钱包，去中心化交易所，DeFi，稳定币等。而使用区块链技术特性的溯源，征信等功能早已进入各大企业的供应链系统之中，未来将会获得更多的应用场景。

币威链旨在为去中心化金融服务专门设计一条高效的公链，并以公链为底层基础设施，内置强大的数字资产管理能力，结合钱包应用前端等实现完善的 DeFi 支撑体系，真正达成有价值的应用落地。在具体实现上，币威链以 BCV、BAC 双币制的经济系统保证公链基础服务与抵押挖矿的平衡，用 ZI-POS 共识在安全、通缩的经济模型下，保证公链的效率，并使用 tendermint 共识引擎和跨链交互协议 IBC，构建侧链和中继链体系，达成跨链目标，实现跨链资产流通，满足多源数字资产管理的设计。币威链在支持智能合约，保证通用功能服务扩展的同时，以内置的形式实现 DEX 协议、借贷、基金等典型的业务，并重视用户体验与产品周边设施建设，结合数字资产钱包等，为用户提供良好体验的 DeFi 生态。

第二章、现状与改进

在数字资产的世界,一定需要一条公链,可以专门为新型的去中心化的金融环境来服务。我们认为,一条能够满足数字资产管理应用需求的公链,需要具备以下条件:

2.1 稳定的性能与可靠性

在计算机世界中,如果操作系统性能不好,或者不稳定,计算机上的所有软件都无法正常运行,就更别提使用计算机有效率的完成工作了。公链的性能与稳定性对于区块链系统来讲就像操作系统对于计算机一样重要。首先一条可以被广泛使用的公链,必须具有合理的性能。我们知道去中心化的系统性能很难与中心化的系统性能匹敌,这是享受去中心带来的安全性等优点所需要付出的代价,但是我们依然可以努力的寻求改变和升级,设计出可以满足当下主流 DApp 性能需要的公链。比如以 TRX 和 EOS 为代表的公链,转账基本上可以在数秒内完成,用户不需要像比特币一样等待 10 分钟以上的时间,现在这些公链上已经有成千上万的 DApp 在运行,每天有数以百万的用户使用,流量已经超过了很多中心化的应用。

无论是 ETH 还是 EOS 等主流的公链,都出现过稳定性问题,比如智能合约出现漏洞,主网升级时出现问题等等,这些问题都对公链的生态造成了打击,也对用户的资产造成了损失。我们也应该吸取前人的教训,同专业安全团队合作,在安全和稳定性上竭尽全力,主动和被动的避免,防止公链出现问题,特别是在智能合约和主网升级等层面,并在系统的核心机制层面进行防范,一旦出现问题,也可以将损失降到最低。

2.2 被社区认可的经济系统

在 POS 共识的区块链系统中,经济模型是站在满足公链的功能和安全性的角度来设计的。节点通过抵押代币可以获得验证节点的身份,用户通过使用代币投票给支持的节点获取收益。如果节点作恶,其收益将受到影响,用户也会将投票转移到更加可信的节点从而杜绝节点作恶的情况。这套被广泛采纳的 staking 机制虽然在功能性和安全性上满

足了 POS 共识，但是却缺乏经济角度的考虑。用户可以一次性购买代币抵押后，持续永久的获得投票的收益奖励。如果新增的抵押数量减少，而产出的代币数量持续增加，代币的价值将无法被支撑，整个公链生态的投资者都会蒙受损失，这对公链生态的长期发展是不利的。

而市场上被验证过的比特币 POW 共识的数学模型具有一定程度的通缩性，总量恒定，并且产量会定期减半，只要项目用户的活跃度持续增长，代币价值就会得到支撑。这套经济系统设计虽然很合理，但是性能上无法达到 POS 公链的标准。

因此区块链行业需要一套新的共识体系，既在性能上可以满足大规模应用的需求，在经济系统上，对通证的价值可以有支撑，这样会更好的激励社群户更加深度的参与和推广，也可以给公链生态创造更加长远发展的土壤。

2.3 完善的配套生态

一个受欢迎的公链，离不开开发者和使用公链的发起方。要吸引用户参与到公链的生态中来，一定要为开发者创造简单易用的研发环境。比如节点搭建的教程，钱包的组件，智能合约开发所需的 IDE 工具，以及完善的文档教程、框架，类库，模板等都可以大大降低使用者的进入门槛和研发的时间成本。公链的开发越是便捷，就会有越多的开发者选择这条公链，这条公链的生态就会发展的越好。除了对开发者开发环节友好之外，公链生态中的用户对于开发者也不可或缺，因为只有用户的参与，开发的应用才有人使用，才能真正创造价值。

2.4 监管配套机制

区块链虽然具有去中心化的高可信度，但同时也具有一定的匿名性和不可逆性。如果这些特性被错误的使用，很有可能使公链成为犯罪的温床。为了公链的健康发展，我们认为公链系统也必须进行一定的监管，这种监管不能太过严苛，这样会与区块链去中心化，人人平等的哲学逻辑相违背，阻碍公链发展。但是同样的，也不能够完全没有监管，否则会任凭恶意的人滥用公链。我们认为公链系统也必须符合各国的监管机制。虽然当前并没有明确的法律法规监管公链，但是我们相信随着区块链技术越发的普及，相

关的政策一定会被制定出来，为了公链可以长远，稳定的发展，一定要对监管政策进行配合和进行相关的开发。

2.5 升级空间

当前的区块链技术虽然比刚诞生的时候进步了很多，但还有许多不完善的地方。

比如当下的公链都是串行运行的，也就是同一时间只能处理单笔交易，一条全球性的可以支持大规模应用的公链，必须能够并发性的同时处理多笔运算。目前公链的并发技术还没有取得突破，所以公链的性能受到了很大的限制。

另外去中心化的存储也是一个很大的挑战，如比特币和以太坊等主流公链，只能存储简单的转账记录，这远远不能满足大规模应用的需求。几个备受期待的分布式存储项目，如 IPFS 等都还没有上线，需要等待市场的验证。

这些技术上不完善的因素都限制了区块链应用的普及，我们相信这些问题终将得到解决，并在不远的未来迎来区块链应用的集体大爆发。而我们的公链也需要紧随技术的潮流，不断升级改进，才能不被淘汰。

第三章、BAC Chain

3.1 共识机制

3.1.1 当下主流共识机制间的矛盾

目前流行的公链共识机制主要有以BTC为代表的POW工作量证明机制和以EOS和TRX等3.0公链为代表的POS权益证明机制两种。

其中POW的经济系统，具有总量恒定，产量周期性减半的特性，这种类通缩的经济系统，为token的价值提供了一定的保证，BTC多年来价格不断地上涨就是归功于这套经济系统，是一套被市场验证过，并且取得了成功的经济系统，但是POW共识由于出块速度慢，账本需要同步的节点过多，在性能上已经很难满足新时代的公链应用需求。

如果说POW是一种全民投票机制的话，POS共识就像人民代表大会机制，POS在众多参与者中选出验证节点，代表用户负责区块链的出块，使网络中需要同步的节点由几十万个下降到几十个，这样大大提高了公链的性能，但是POS共识机制的经济系统，是一套通胀的经济系统，需要超发token为节点和给节点投票的用户发放奖励，在这种通胀的模式之下，token的价值很难得到支撑。

3.1.2 ZI-POS 共识机制

为了解决经济系统和性能之间的矛盾，BAC Chain发明了ZI-POS(Zero Inflation Proof of Stake)共识机制，在传统POS共识机制的基础上，建立了一种双币双通缩的经济模型，使得币威链既拥有POS共识机制的性能，同时还具备BTC一样被市场认可的经济模型，保证公链生态稳定与良性发展，为生态节点和参与投票的社群用户创造更多收益。

3.1.3 双币种

BCV: BAC Chain 的权益通证, 持有 BCV 代表享受 BAC Chain 的权益。因此作为 BAC Chain 核心的主网节点, 需要持有并抵押至少 10 万枚 BCV 才可以参与竞选。而为节点投票的用户, 需要销毁 BCV 方可获得投票权。

BAC: BAC Chain 的功能通证, BAC Chain 的链上业务, 如转账手续费, 智能合约执行, 分布式存储等业务都需要消耗 BAC。BAC 的经济模型参考 BTC 的总量恒定, 产量减半机制, 由 0 流通量开始挖矿产出, 发起方 0 预留。

3.1.4 通缩销毁机制

BCV: BCV 总量 12 亿枚, 永不增发。用户抵押或者销毁 BCV 购买 BAC 投票矿机挖矿是获得 BAC 的唯一方法。另外每台 BAC 投票矿机还需要充值能量值方可继续挖矿。销毁 BCV 也是获得能量值的唯一途径。

BAC: BAC 总量 43,695,126 枚, 初始时 BAC Chain 每产生一个区块, 赋予出块节点 10 枚 BAC 作为奖励。之后每半年奖励数量减半, 并向下取整, 直到大约两年半后所有 BAC 被挖出。

在所有 BAC 被挖出前, 用户使用 BAC Chain 转账的手续费, 运行智能合约的费用, 以及存储网的存贮费用都将使用 BAC 支付, 而在挖矿完成之前, 所支付的所有 BAC 都将被销毁。

	总量	销毁机制	获得方式
BCV	12 亿	购买 BAC 矿机	交易所
BAC	43,695,126	转账手续费	抵押或者销毁 BCV 挖矿

时间	每块奖励个数	每天奖励总数
第一年前半年	10	144,000
第一年后半年	5	72,000
第二年前半年	2	28,800
第二年后半年	1	14,400
第三年	0	0

3.1.5 验证节点与投票矿机

与传统 POS 机制一样，ZI-POS 需要验证节点作为出块节点构建区块链网络。在传统 POS 共识机制中，验证节点抵押的币与获得的出块奖励是同一种通证，而在 BAC Chain 的 ZI-POS 共识机制下，节点抵押的通证是作为权益通证的 BCV，然而获得的出块奖励是作为功能性通证的 BAC。这样不仅可以两个不同的通证按照功能的不同分开，还可以避免通证的超发，避免通胀。

而作为社群用户，需要给节点投票，表示对社群的参与以及对节点的支持。用户需要销毁 BCV 获得投票权。而节点会将自己的出块奖励，分给支持自己的用户。我们为了用户更好的理解这套机制，我们将投票权虚拟成为投票矿机，用户的投票行为也可以等同于一种挖矿行为，从而节点也可以等价为矿池。

而节点抵押和获得的票数越多，代表该节点过得社群的信任和支持越大，该节点获得出块机会的概率也就越高，收益也就越大。相反，若该节点做恶，或者不作为，将会受到 slash 的惩罚，用户会将投票转投给其他节点。

3.2 智能合约与内置合约

3.2.1 智能合约

智能合约对金融资管公链必不可少，BAC Chain 智能合约不仅具有图灵完备，使用灵活，安全可靠等智能合约等基本特点，还提供了生态友好的合约引擎 BVM。BVM 通过 webAssembly 和预言机技术等为合约提供了执行安全，性能，多语言等支持智能合约执行。

3.2.2 BVM 虚拟机

BVM 是在 webAssembly 是在基础上改进而成，webAssembly 是一种高效加载，可移植，平台无关的字节码格式，可以在平台上接近原生的速度执行程序，这是一项全新的 web 标准，由谷歌，苹果，微软，mozilla 等几大公司同时支持和制定。webAssembly 是被 EOS 验证过的技术，EOS 智能合约伴随 EOS 上线一直稳定执行。另外 BVM 也考虑到 webAssembly 的生态很好，很多高级语言都可编写的程序都可以编程成 wasm 字节码的程序，wasm 字节码既可以编译成机器码后执行，又可以使用解释器直接执行，这样就降低了开发人员的学习成本。

安全问题对智能合约至关重要，在执行的时候可能会出现安全问题，比如计算和存储资源的过度使用，节点执行效果不一致等。BVM从设计层面非常重视合约的安全性和正确性，使用gas机制防止资源被过度使用，BVM对执行深度和执行耗费的做了很多安全限制。BVM在代码层面明确了接口之间的权限，智能合约的入口函数需要进行权限限制，防止开发者在入口函数调用未经授权的函数，破坏合约执行内容。

3.2.3 内置合约

BAC Chain将协议层和通用性较强的功能需求，写成了内置合约。这些合约都是硬编码在链上的，开发者可以按照合约的接口参数进行调用，对于不符合接口要求的请求会直接拒绝调用，这样的合约既给开发者提供了便捷，又提升了安全性和稳定性。

目前BAC Chain 规划的内置合约功能如下：

发行 Token

去中心交易协议

账户信用审查

去中心化借贷

基金机构专用账户

3.3 存储网

Bac Chain 实现存储网功能，在设计过程中考虑了以下因素：

- 1、存储数据需要以交易的形式发送，要以状态的形式存储。这样硬升级的时候，交易数据会存在升级前的主网上，状态数据始终和账户绑定，仍然可以在升级后的主网上查询到。币威链把需要存储的数据当作资产处理；
- 2、考虑商业数据具有多样性，用户在实现存储的时候可以自定义数据格式存储，确保用户的使用便利性；
- 3、币威链承载了存储数据的摘要或者数据的签名，真实的数据可以选择存储在其他分布式系统上，这样可以减少链本身的数据量，又实现了数据一致性和防止篡改，目前使用 FastDFS 集群作为后端文件系统；
- 4、用户存储的时候可以选择是否加密存储，确保数据安全性；

5、存储本身需要消耗资源，在币威链存储需要消耗相应的 BAC 作为费用，存储的数据量越大，消耗的存储费用越大，这部分费用可以通过社区投票方式选择是消耗还是以收益的方式分给挖矿用户，目前是直接消耗；

6、存储数据都有 location 字段，可以方便的检索到在主网版本，高度和交易前缀。

BAC Chain 目前已经初步实现了存储网的功能，正在探索在商业领域的应用。

3.4 跨链

目前主流的区块链跨链技术方案按照其具体的实现方式主要分为三大类，分别是公证人机制，哈希锁定，侧链和中继链。

公证人机制安全性保障依赖于公证人系统，参与跨链的相关方需要对给予公证人机制较大的信任。哈希锁定目前较适合偏资产或者关键数据的交换，使用场景受限较多。币威链底层使用 tendermint 共识引擎和跨链交互协议 IBC，构建侧链和中继链体系，达成跨链目标。对于早期的数字资产链，比如 BTC/ETH，使用跨链技术将 BTC/ETH 价值转移到币威链上来。对于已经支持了 IBC 资产链，使用 IBC 协议达成跨链目标。

第四章、去中心金融(DeFi)应用

区块链技术的诞生，在以银行为中心的中心化价值存储机制以外，给我们提供了一个去中心化的存储和传递资产价值的新选择。区块链作为一种价值存储媒介，链上存储的数字资产，可以赋能很多金融类的服务，完全链上的服务也都是去中心化的。所有传统金融领域中存在的服务，都应该可以在区块链上去中心化的形式重新设计实现。

一个合理的去中心金融公链，需要以下基础功能才可以满足应用的需要：

1. 可以发行 Token
2. 有稳定币
3. 有去中心交易协议 (DEX)

因为目前的智能合约安全性较差，并且不易升级，对于这些典型业务，我们将使用内置合约的方式实现 DeFi 功能，既保证更好的安全性，也可以使交易运行的更加高效，也为未来升级提供更便利的空间。当然，如果我们提供的功能无法满足项目方或者用户的需求，将来用户也可以使用智能合约来实现额外的功能。

4.1 发行 Token

BAC Chain 以内置合约的形式支持发行 Token 的功能，用户只需要运行简单的几行代码，就可以在链上发行自己的 Token，用户可以自定义 Token 的名称，小数点精度，发行总量等参数，还可以以 BCV 作为自己发行 Token 的背后担保资产，增加 Token 的信用。

所有 BAC Chain 上发行的 Token 都可以自由的在链上转账，用户只需要支付 BAC 手续费。如果该 Token 出现信誉问题，用户可以将持有的 Token 按等比例兑换成背后担保的 BCV 资产，减低自己的损失，兑换后的 Token 会被直接销毁。

为了进一步降低用户的操作门槛，币威钱包也发布了通证宝产品，作为支持币威链发行 Token 的应用前端，一键发行币威链上的 Token。

币威链目前已经上线主网发行数字资产功能,具体字段如下:

字段	类型	描述
outer_name	string	发行时指定的名称,例如 ABC;用户指定
inner_name	string	发行时候生成的新名称, outer_name 加上后缀
supply_num	bigInt	发行总量;用户指定
margin	string	保证金;用户指定
website	string	通证网址;用户指定
description	string	通证简介: 用户指定
precision	uint8	精度: 用户指定
exchange_rate	string	兑换比例 $exchange_rate = deposit / supply$
owner_address	string	用户地址;用户指定

4.2 稳定币

4.2.1 基于资质背书中心化稳定币方案

USDT 使用这种方案实现, Tether 公司为其背书,每发行 1USDT,就有 1 美元作为兑换。USDT 是目前使用最广泛的稳定币方案,但这种方案本身也存在一些问题,USDT 的储备金并不透明,其增发可能会导致信任危机,面临不确定的监管政策等等。

4.2.2 基于 DCEP 和 Libra 去中心化稳定币方案

这类稳定币基于国家或者主要银行做背书,运营会收到高度监管,货币政策由各个国家控制,它本身也是基于区块链技术实现,有一定的匿名性,这类稳定币需要考虑的因素更多,也更复杂。目前还处理论或者实验阶段,并没有进入主流市场。

4.2.3 完全去中心化稳定币方案

DAI 是 makerDAO 创建并发行的一种锚定美元 USD 1:1 的稳定币,是基于以太坊发行

的。和 BTC、ETH、EOS 以及一般的 Token 不同，Dai 不是通过挖矿产生的，而是必须由 Dai 的需求者质押一定量的 ETH，然后由智能合约作用向 ETH 的质押者发行一定数量的 DAI。目前 DAI 的活跃度还远不及 USDT。

在 DeFi 的各类业务实施中，稳定币是必不可少的媒介。项目方可以使用 BAC Chain 的内置发行 Token 机制发行自己的有资质背书的稳定币，该稳定币还可以使用 BCV 作为背后担保资产，或者以其他方式来锚定稳定币资产的价值。

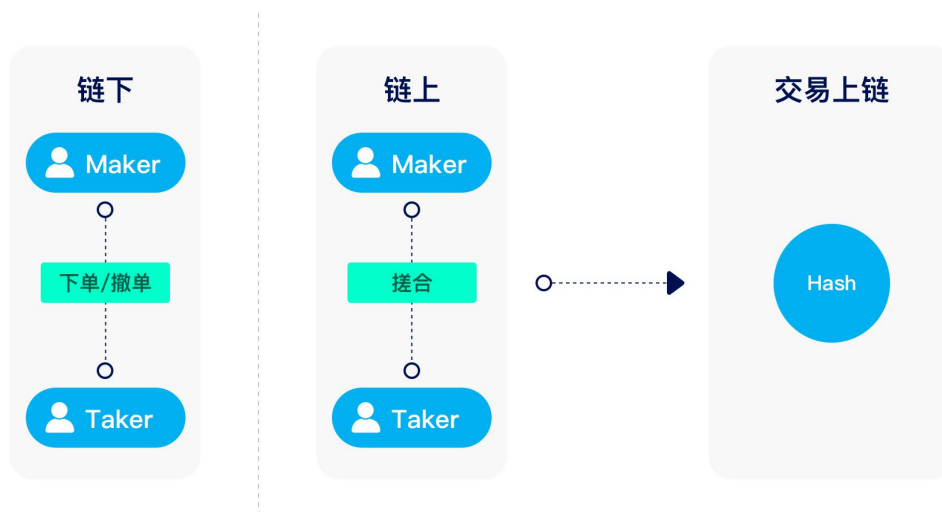
另外其他主网如 ETH/TRX 等上发行的稳定币，也可以通过通过 BAC Chain 的跨链机制在 BAC Chain 上被使用，提供如 USDT/USDC 等主流稳定币的支持。

4.3 去中心交易协议 DEX

现在主流交易所都是以中心化形式运作，用户只有在充币和提币的时候才可以在链上查到自己资产的流向，但是交易记录并没有记录在区块链上，并且每个交易所都有自己独立的账户系统，这些账户信息也都是中心化存储的。目前主流交易所的这种中心化交易机制，与 DeFi 的去中心体系并不匹配，也无法真正去中心化地实现稍微复杂 DeFi 业务流程。我们需要去中心化交易协议对 DeFi 业务的支持，用户的地址就是交易标识，用户只需要持有私钥就可以进行交易，与 DeFi 应用相兼容，并且交易记录直接链上可查，更加的透明公开。

4.3.1 链上链下的混合机制

鉴于当下区块链技术还不成熟的限制，链上性能还无法满足用户下单撤单的毫秒级响应需求。另外用户挂单和撤单的操作，如果没有成交，全部记录在链上的话，不单只耗费链上存储空间，没有好的委托体验，也会消耗用户不必要的手续费。所以 BAC DEX 采用了链上，链下相结合的混合机制，用户的下单签名只是在链下的系统中记录，当有成交撮合的时候，用户的交易才会成交并上链。



4.3.2 BAC DEX 的基本数据结构

变量名	功能
makerAddress	吃单方地址
takerAddress	挂单方地址
makerData	吃单方相详细信息，比如价格，成交数量，下单时间，委托类型等
takerData	挂单方相详细信息，比如价格，成交数量，下单时间，委托类型等
makerAmount	吃单总量
takerAmount	挂单总量
makerFee	吃单方的手续费
takerFee	挂单方的手续费
commitID	该笔交易的唯一标识符

4.3.3 交易签名机制

用户的每一笔交易，都需要数字签名验证以确保该交易的真实性和完整性，保证该笔交易是来自该地址的真实控制人，并且在信息传递过程中，下单信息没有被篡改。

BAC DEX 的每一笔交易都使用了数字签名，并且对订单进行加密。这让下单者可以放

心，除了他们授权的订单外，没有其他人可以与他们的地址进行未授权的交易。同时潜在的交易方也可以验证该订单是否是一个安全有效的订单。



4.3.4 多平台共享深度

因为BAC DEX的交易逻辑使用BAC Chain的内置合约功能完成，用户可以基于BAC Chain的公开协议构建多家去中心交易所，而这些交易所共享相同的数据结构，并在同一条公链上撮合，所以多家交易所可以共享交易的深度，不同交易所之间的用户也可以互相成交彼此的订单。

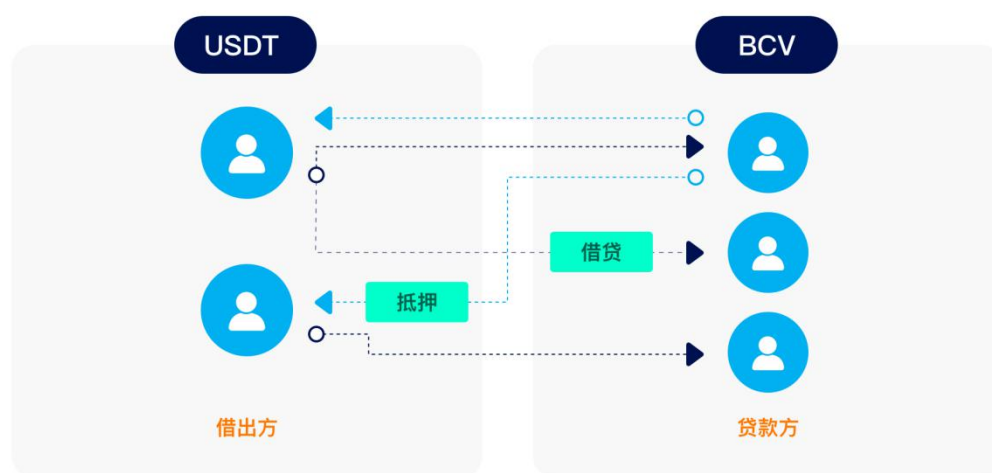
4.4 去中心化借贷

借贷是金融领域的基本应用，一方面可以满足借贷人的资金需求，另一方面也可以为出借人提供利息收益。去中心化的借贷系统与传统借贷系统相比，具有操作便捷，风险低，放款快等优点，将会是DeFi在未来的主要应用场景之一。

BAC链结合了当下主流的DeFi借贷技术和传统金融的借贷机制，在内置合约中提供了借贷功能的支持。该系统可以支持多点对点借贷模型和代币交换两种不同的借贷机制，以及分期还款和单次付清等多种抵押借贷机制，用户可以很方便的放贷或者借款，项目方也可以使用内置合约接口，快速开发出一套功能完备的借贷平台，如果内置合约的功能无法满足需求，项目方还可以使用结合智能合约在内置合约的基础上进行二次开发。

4.4.1 点对点借贷模型

点对点借贷是一种地址对地址的借贷机制，出借方可以在链上发起出借请求，并设定期望收取的利率和还款时间和抵押率等信息，贷款人也可以在链上发起贷款请求，并设定期望贷款的额度和抵押资产的类型。如果出借方或者贷款人双方有匹配的意向，BAC Chain 的链上借贷模型将会将匹配双方的账户，并将借贷交易匹配上链，贷款方可以马上获得贷款，同时出借方也会马上获得抵押代币的锁定权。如果贷款方违约或者爆仓，借款方也可以马上获得贷款方的抵押物，从而将风险降到最低。



4.4.2 计息方式

在 BAC Chain 的借贷模型中，因为已经有锁定的代币作为抵押物，风险较低，所以可以有多种不同的还款方式。从传统还款方式来分类，支持等额本息和等额本金的还款形式，等额本息还款是指借款人每月以相等的金额偿还贷款本息。等额本金还款是借款人每月等额偿还本金，贷款利息随本金逐月递减，还款额也逐月递减。另外如果出借方同意，也可以支持在借贷到期日到期时，一次过还清本息的方式。另外，用户也可以选择还款的利息是和贷款币种为不同的币种，比如用户贷款 USDT，但是每月还款时的利息，可以用 BCV 支付，支付的数量按照预言机的实时价格进行折算。在贷款完全还清前，贷款方无法赎回抵押物。

基础数据结构

出借资产	USDT, BUSD, BCV, BAC 等
利率	年化利率百分比
利息资产	USDT, BUSD, BCV, BAC 等
出借日期	出借的当日时间
还款周期	如 30 天
到期日期	150 天
还款类型	等额本息, 等额本金
抵押率	50%
出借人地址	BAC Chain 地址
贷款人地址	BAC Chain 地址
抵押资产	BCV 500,000
出借资产	10000 USDT
已还金额	1000 USDT
已还利息	2000 BCV

4.4.3 清算

如果贷款人抵押的资产价值触及爆仓线, 或者贷款人违约, 系统将会自动将贷款人的抵押物所有权转移给出借人。出借人全权拥有抵押物的处置权。出借人可以选择将抵押物转至交易所出售, 如果交易所的流动性较差, 出借人还可以选择将抵押物在 BAC 借贷平台的拍卖系统中进行拍卖。

4.4.4 点对点借贷挖矿机制

由于点对点借贷具有一定的流动性问题, 比如当贷款人远大于借款人或者借款人远大于贷款人时, 人们的借贷需求无法被马上满足, 这大大的影响了用户的借贷体验。Bac Chain

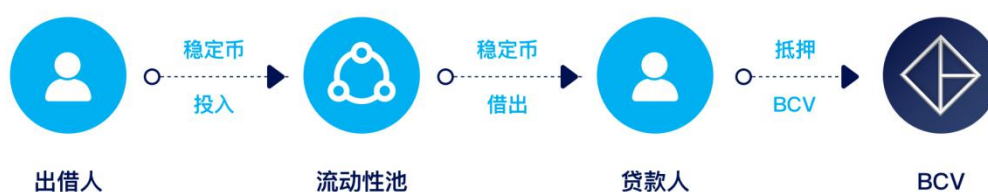
的内置点对点借贷模块，还设计了挖矿机制，借贷平台可以存入一定的 BAC 作为挖矿奖励，借贷订单在一定时间内没有被满足，将会触发挖矿机制，用户完成该笔借贷需求，将会获得 BAC 奖励，同时该借贷需求等待的时间越长，满足该需求时获得的 BAC 就越多。

4.4.5 流动性池借贷系统

点对点的借贷系统是一个一对一的借贷系统，该应用适合比较小规模的借贷平台或者债券双方或多方是相识的个体的借贷行为。

流动性池借贷系统则更加像是一个银行。用户可以将资金存入银行获得利息，贷款人也可以从资金池中抵押代币，支付利息，贷出资金。借贷双方都在流动性池子中互相支取，并没有绑定相互的关系。它首先将资产全部汇集一起，然后当收到借款需求时再进行借贷分配，再将利息返回给储户。

由于流动性池是将大家的资产汇集在一起，所以特定储户的资产并没有锁定在某个特定的贷款中。这意味着，储户如有需要，可以随时取出其资产，这比点对点借贷更加方便灵活。但是，这只有在流动性池的资产并没有全部借贷出去的情况下才可能。



4.4.6 利率的计算

在当今的现实世界，利率和流动性储备是由国家的央行决定的。然而，DeFi 的世界中，

利率将由市场决定，这样可以更自然的平衡贷款需求和代币供应。贷款的需求越大，利率就越高。反之亦然。

一般情况下，并非所有存入流动性池中的资产都会被借出。用户所提供的资产被借出的越多，资产利用率就越高，同时回报就越大，但同时这也意味着用户拥有较低的流动性，不是所有的资产都可以随时取出。

4.4.7 存款利率

当出借人将稳定币存入流动性池的时候，会获得投入资产的凭证 ALT，稳定币与 ALT 的兑换比例公式如下：

$\text{totalCash} = \text{放入流动性池，但还没有被借走的稳定币的数量}$

$\text{totalBorrows} = \text{所有借款人应偿还稳定币的总数量，包括本息}$

$\text{totalReserves} = \text{总保留金数量}$

$\text{totalSupply} = \text{所有兑换 ALT 的总数量}$

$\text{兑换比例} = (\text{totalCash} + \text{totalBorrows} - \text{totalReserves}) / \text{totalSupply}$

可见，随着借款的数量增加，兑换比例也会相应的增加，如用户在存入稳定币的时候兑换比例是 1:1，一年后取出稳定币的时候，兑换比例是 1.11，用户就获得了 10% 的存款年利率。



4.4.8 借款利率

借款的利率应当根据当前市场的供需关系自由浮动，一般来说，借款需求越大会，利率就会上涨，从而吸引更多的人提供借贷，最终将利率维持在一个动态平衡的系统中。

借款年利率由以下三个因素影响

1. **基础利率**：基础利率为全网基础利率，有项目方或者项目社群决定
2. **使用率**：使用率就是当前流动性池中，被借出的使用比例，表现出市场当前的供需关系

$$\text{使用率 UtilRate} = \text{totalBorrows} / (\text{totalCash} + \text{totalBorrows})$$

3. **加给率**：用于调整使用率对利率的影响

$$\text{使用率 UtilRate} = \text{totalBorrows} / (\text{totalCash} + \text{totalBorrows})$$

$$\text{借款年利率} = \text{基础利率} + \text{使用率} * \text{加给率}$$

4.4.9 放贷利率

放贷利率由以下三个因素影响

1. 借款年利率
2. 使用率
3. **保留利率**：保留利率为全网基础利率，有项目方或者项目社群决定

$$\text{放贷利率} = \text{借款年利率} * (1 - \text{保留利率}) * \text{使用率}$$

由于流动性池是一个开放自由的资金池，用户可以随意的存入资产和取出资产，贷款人也可以随时支付利息归还借贷本金，并赎回抵押的资产。该流动性池中可以有不同类型的稳定币，根据市场的供需关系，不同的稳定币也拥有不同的借贷利率。但是整体的借贷流程和还款方式比较单一，我们认为流动性池与点对点借贷是两种互相互补的借贷机制，用户可以根据自己的需求，选择合适自己的服务。

4.5 征信系统

虽然区块链具有一定的匿名性，但是 Bac Chain 仍然具有一套机制来评估每个地址的信用等级。影响信用等级的因素有账户流水，账户借贷记录，账户违约记录，账户资产价值，账户交易记录等，Defi 应用可以根据账户的信用评级，选择仅对某些地址开放服务。

4.6 基金专户

数字资产开放交易以来，越来越多的资产管理服务团队 Token Fund 成立数字资产基金。但是这些基金大多在中心化交易所操作，由于数字货币市场缺乏管理措施，基金的资产安全性很难保证。

随着去中心化交易所的技术越来越成熟，也越来越普及，使用去中心化的账户系统进行基金资产管理成为了可能。

BAC Chain 针对基金理财机构，专门设计了由内置合约控制的机构账户，该机构账户的入金和出金受到一系列的参数所限制，可以保证投资人的资产安全。

4.6.1 基金专户账户结构

募资额度：总募资额度

清盘规则：当账户触发清盘线时，合约将会自动讲账户资产按投资比例返还至投资人地址中


募资人数上限：最多募资人数

分红模式：基金的分红模式会在合约上写好，系统会根据分红模式，在分红日自动分红。

结算日期：基金的结算日子。

机构需要成立一支基金募资的时，可以开设一个 BAC Chain 的基金专户地址，并设置相关的募资额度，分红模式和清盘规则等。设置完毕后，尽管基金管理人持有该账号的私钥，但是无法通过分红模式和清盘规则外的手段提币。

基金经理可以管理该账户的资产通过去中心交易所交易获得利润。智能合约会根据利润情况和分红模式设定自动在分红日进行分红，将收益转入投资人地址。



基金经理也可以借助去中心借贷功能，存入稳定币获得固定收益，分散配置资产，也可以质押小币，获得稳定币，在小币种价格下跌后买回来做空市场。

基金专户不仅可以简化基金的募资和分红等管理流程，还可以增加基金的透明度和可信度。

BAC Chain 使用内置合约的形式，给用户提供了完备的去中心化金融应用，可以满足绝大多数的应用需求，其中包括，交易，借贷，理财，存款，征信等。

第五章、其他区块链应用

5.1 物流追溯

区块链在物流追溯应用上有很大的优势，特别是在食品安全以及原产地证明和绿色有机产品溯源等领域，区块链不可篡改的特性，可以赋予溯源更大的可信度和更低的成本。特别是当区块链技术和物联网技术相结合的时候，可以发挥出极大的效能。

用户可以利用物联网温度数据，氧气含量和地理位置等传感器，采集整个物流关键环节中的相关数据，并记录在 BAC Chain 区块链上，并启用预警，并实时监控数据；基于区块链的不可篡改特性，可以保证数据的安全有效性，并制定出一整套物流溯源系统。基于数据的分析和监控，系统可以保证物流流程的整体安全性，并在出现问题的时候，准确召回有缺陷的产品。另外，物流数据也可以与保险公司和有关部门共享，帮助其提供更加全面的保险和监管。

5.2 数字版权

在互联网，数字信息很容易被复制和传播。如果数字信息的分发通过 BAC Chain 的解决方案，可以将版权登记、内容分发、版权转让等相关数据存储区块链上，相关非结构化数据可以存储在存储网，并且保证同时只有一个副本被传播，实现知识产权可追溯。该解决方案立足区块链技术的不可篡改性、公开性、透明性等特点，可以减少内容提供方对版权登记、内容分发、版权交易的成本，实现点对点分发，使内容流通和交易更加快捷、透明。

5.3 支付

BAC Chain 的 POS+PBFT 混合共识机制，可以保证单笔转账基本上可以在 5 秒内在链上被确认，用户的链上转账确认时间和当下中心化的线上支付系统的确认时间相差无几，可以给用户提供与现在支付宝和微信支付等系统相近的支付体验。配合币威钱包的应用层功能，可以以去中心化的形式完成，扫码支付，刷脸支付等功能。

第六章、BAC Chain 技术详情

币威链 Bit Asset Chain(BAC Chain)，是由币威资产管理平台研发的去中心化的高性能数字资产管理公链。币威链的设计理念以先进的高可靠性，高性能技术为核心，搭配成熟的经济系统和经过长期实践积累的社区治理机制，并一系列的以用户体验为重的配套应用和开发工具，力图打造全球性的高效的、可靠的、易用的、并能够满足全方位应用场景的数字资产公链。

6.1 经济系统

BCV Chain 是一条基于 POS 共识体系的面向资产管理服务并支持企业级应用的高并发公链。为了解决传统 POS 共识机制无法避免通货膨胀的缺点，BCV Chain 改良了现有的 POS 经济系统，设计出了 ZI-POS (Zero Inflation Prove of Stake) 经济模型，该模型将传统 POS 系统与经典的比特币数学模型相结合，建立了一套具有通缩属性的 POS 经济系统，可以为生态节点和参与投票的社群用户创造更多收益。

6.1.1 独创 ZI-POS 共识机制 (Zero Inflation Prove of Stake)

传统 POS 共识机制有以下缺点：

通货膨胀：尽管不同的 POS 项目都拥有自己的增发机制和不同的奖励额度，但是总的来说，传统 POS 共识机制给验证节点的奖励是通过通胀机制增发代币而产生的。

传统 POS+比特币数学模型比较

	ZI-POS	POS	POW
币种	双币种	单币种	单币种
性能	高	高	低
去中心化程度	低	低	高
通缩/通胀	双币双通缩	通胀	满足一定条件通缩
挖矿	销毁	抵押	实体矿机

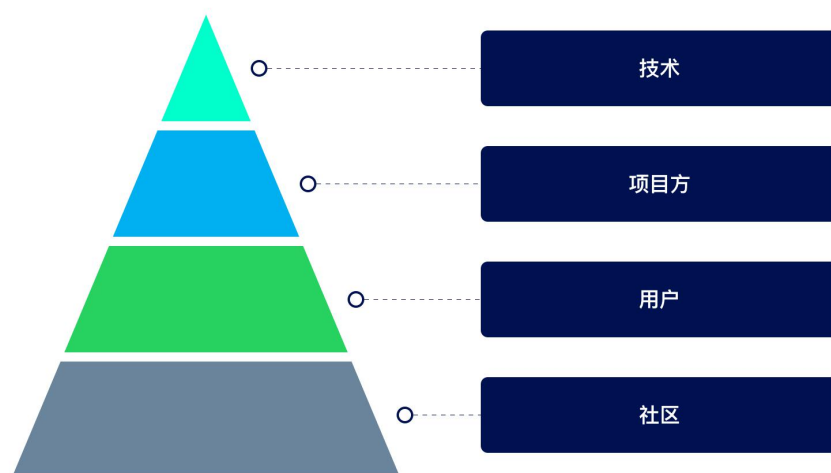
6.1.2 双币制

为什么双币?

在一个经济系统中，资产按照用户的持有意图，可以分为两种。第一种是可以升值的资产，这类资产人们愿意长期持有，而把它花掉的意愿比较低。另一种是高流通性的资产，这种资产或许升值潜力不如第一种，但是有很高的认可度，可以很轻易的流通起来，人们愿意对这类资产进行转移和交换。这两种资产存在一定的矛盾性，如果经济系统中只有一种资产，人们会在花掉它，还是存起来之间产生纠结。为了解决这个问题，我们采用了双币制度，将期望长期持有的权益通证与用来支持主网流转的矿工手续费通证分开，以更好的满足用户的需求，降低人们的困扰。

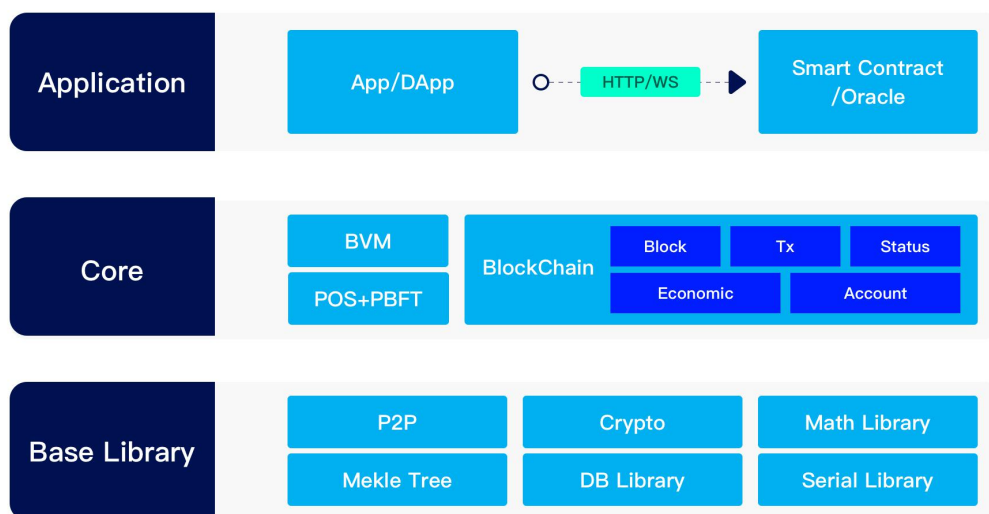
权益通证：BCV 用于公链验证节点的权益抵押

挖矿通证：BAC（BCV for Circulation）用于验证节点的挖矿奖励，以及支付使用公链的转账手续费等。



6.2 总体模块

BAC Chain是一条致力于数字资产服务的可监管的，高性能的，完全去中心化的资管公链。主要分为如下模块：



Base Library : 为BAC Chain提供基础库服务

- P2p 提供节点之间的消息传输提供服务
- Crypto 提供了公链所需要的密码学功能
- Math Library 计算库:提供精度计算服务
- Merkel 提供消息摘要，压缩等功能
- DB Library 提供公链所需要的存储服务
- Serrial Library 提供消息数据的序列化服务

Core: BAC Chain的主要组件

- BVM 为智能合约提供执行环境
- Block 提供区块的存储检索区块服务
- Tx 提供交易的存储检索服务
- Status 提供公链对象当下或者以前某版本的数据状态
- Economic 公链的经济模型
- Account Model 账号模型，管理账号资产

Application 应用层:

- App/Dapp 为用户提供服务
- Smart Contract 智能合约
- Oracle 预言机

6.3 POS+BFT 共识

随着区块链的不断发展，区块链用户的数和各种操作数的增加，对共识算法的安全性可靠性和性能要求也越来越高，目前pow协议非常耗费资源，交易确认慢，DPOS比较中性化，BAC Chain使用POS+BFT的共识模式，实现共识的快速达成。

6.3.1 POS 模型

在BAC 中，POS模型包括以下三个步骤：

6.3.1.1 创建验证人

成为验证人需要初始化如下参数：

- A、节点公钥：该公钥对应的私钥会对区块和共识状态做签名，该公钥会被各节点作为区块验证和hash状态。
- B、节点名称：该节点名称会在主网上展示，作为标识
- C、抵押数量：节点自身抵押BCV获取的投票权数量，数量越大会，越能被矿工认可。
- D、最小抵押比例：节点自身抵押数量占总该节点总抵押量的比例。

6.3.1.2 矿工投票

矿工想获取收益，可以销毁BCV获取投票权，然后将投票权投给验证节点。验证节点承担验证区块，打包交易，产生区块的功能，经济模型会对验证节点作出奖励，验证节点根据矿工的票数把收益分给矿工。因为验证节点需要有稳定的网络，硬件设备或者云服务。如果验证节点不能稳定的出块，系统将消减节点和节点下矿工的权益，这有助于矿工选择更优秀的节点进行投票。

6.3.1.3 分配模型的简化

每个区块产生之后，验证人都会分到奖励，然后将这些奖励分配给他的矿工，如果每次出块都做这样的迭代会消耗大量的资源，甚至将会影响系统的整体运行。BAC Chain使用如下模型进行简化处理

一个矿工在高度 h 给验证节点抵押了 x $bcvstake$ 验证节点在区块 i 的总抵押数量为 s_i ，分到的总奖励为 f_i ，矿机在区块 n 处提现，则可以提现的奖励为

$$\sum_{i=h}^n \frac{x}{s_i} f_i = x \sum_{i=h}^n \frac{f_i}{s_i}$$

在一段时间内，如果没有新的矿机或者节点抵押， s_i 会保持不变，称这样保持不变的一段区间为 p ，在这一段区间内，验证节点 v 收到的奖励为 T_p ，抵押的资产为 N_p ；如上矿工在高度 h 开始挖矿，开始的区间为 p_{init} ，结束的区间为 p_{final} ，则上式可以表述为

$$x \sum_{i=h}^n \frac{f_i}{s_i} = x \sum_{p_{init}}^{p_{final}} \frac{T_p}{N_p}$$

p_0 为验证人第一次抵押的区间

矿机需要抵押挖矿的时候会创建一个数据结构 $entry_f$ ，定义 $entry_f$ 为

$$entry_f = \sum_{i=0}^f \frac{T_i}{N_i} = \sum_{i=0}^{f-1} \frac{T_i}{N_i} + \frac{T_f}{N_f} = entry_{f-1} + \frac{T_f}{N_f}$$

针对每次验证节点抵押数量变化都会创建一个 $entry_f$ 。则矿机在区间 k 成创建矿机，在区间 f 从提交收益，他应该提取的收益为

$$x \sum_{i=k+1}^f \frac{F_i}{N_i} = x \left(\sum_{i=0}^f \frac{F_i}{N_i} - \sum_{i=0}^k \frac{F_i}{N_i} \right) = x(entry_f - entry_k)$$

BAC Chain会存储从区间0到区间 k 每个区间 i 单位抵押量对应的累积奖励为 $entry_f$ 。这样在处理每个矿机奖励的时候，就不需要迭代每个区块，减少计算复杂度。

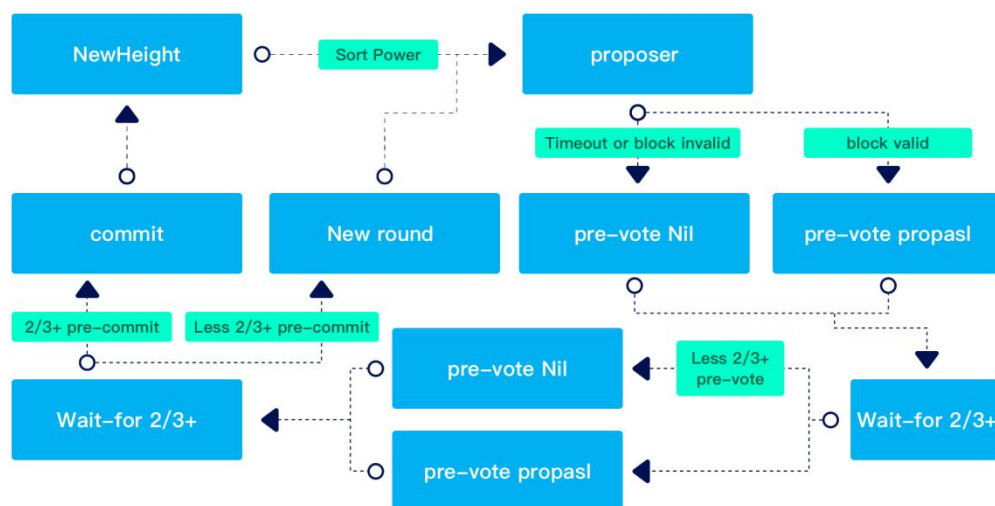
6.3.2 BFT 共识过程

协议中有两个角色：

- A、验证人：不同的验证者在投票过程中具备不同的权力（power），power来自自身抵押和矿机委托
- B、提议人：由验证人轮流产生。

验证人轮流对交易的区块提议并对提议的区块投票。区块被提交到链上，且每个区块就是一个区块高度。但区块也有可能提交失败，这种情况下协议将选择下一个验证人在相同高度上提议一个新块，重新开始投票。

验证人按照power比重，选出proposer，proposer针对当前高度提出出块提案(Block Proposal)，每个区块就对应一个高度，所有验证人收到Block Proposal之后会发起pre-vote投票，当节点收到超过 $2/3$ 的验证人在同一轮提议中对同一个块进行了pre-vote投票之后会进入pre-commit阶段，当节点收到超过 $2/3$ 的验证人在同一轮提议中对同一个块进行了pre-commit投票之后认定该区块已经被超过 $2/3$ 的人认可，会commit该区块



6.3.2.1 Block Proposal 过程

节点根据上一轮状态选择出当前power最大的节点作为出块节点，该节点会搜集本地交

易池的交易，封装成block，然后把该block包含在proposal中广播出去。由于离线或者网络延迟等原因，可能造成提议人提议区块失败。这种情况在共识中也是允许的，因为验证人会在进入下一轮提议之前等待一定时间，用于接收提议人提议的区块，该过程相当于pBFT的pre-prepare阶段。

6.3.2.2 Pre-Vote 过程

一个节点收集到一个完整的提案，它会校验该提案中的区块的正确性，然后对该区块进行pre-vote投票，如果该节点在提案时间之内没有收到提案，他会投递一个空票。节点在pre-vote时间段收集其他节点的pre-vote投票，在当该节点获取超过 $2/3$ 的pre-vote会进入pre-commit阶段。进入该过程相当于pBFT的prepare阶段，目标是防止出现prosoal节点是BFT节点。

6.3.3.3 Pre-Commit 过程

当节点获取超过 $2/3$ 的pre-vote投票后会进入pre-commit阶段，该节点会投pre-commit票，如果该节点在pre-vote没有收到超过超过 $2/3$ 的投票，则在在pre-commit阶段投递Nil票。在该阶段节点会收集其他节点的pre-commit的票，如果收集到超过 $2/3$ 的投票，节点会commit该区块，同时修改验证点power值。该过程相关于pBFT的commit阶段，目标是当收到超过 $2/3$ 的节点都同意commit该区块的时候则commit该区块。

6.4 费用模型和激励体制

费用模型和激励机制是激发整个参与生态的重要保障，对主网的安全稳定的运行至关重要。

6.4.1 出块奖励

BAC Chain使用类似比特币奖励模型，初始每块奖励 10 BAC，每半年减半一次，详细

奖励如下：

时间	每块奖励个数	每天奖励数	截止发放奖励总数	减半高度
第一年前半年	10	132920	24275070	2427508
第一年后半年	5	66460	36412605	4844015
第二年前半年	2	26584	41267619	7282522
第二年后半年	1	13292	43695126	9710029
第三年前半年	0	0	43695126	

6.4.2 链上交易 gas 消耗

链上交易 gas 也可以根据公链验证节点治理需求进行调整，现在设置如下：

迭代操作	1000nbac
写操作每byte	30nbac
写操作	2000nbac
写操作每byte	3nbac
读操作	1000nbac
删除	1000nbac
存在判断	1000nbac

6.4.3 交易 hash gas 消耗

每执行一笔交易都需要消耗gas，这次交易消耗的gas等于本次交易所用操作执行的总和。

6.4.4 验证人委托

验证人在创建的时候需要抵押bcv兑换成bcvstake，这些bcvstake可以兑换回来，重新兑换成bcv。

6.4.5 矿机挖矿销毁

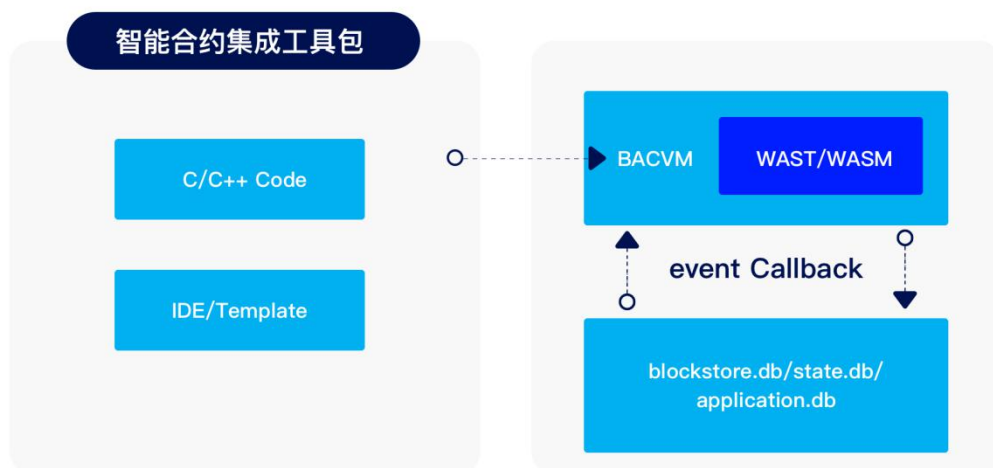
矿机在创建的时候需要销毁bcv换成bcvstake，此bcvstake将不能赎回。

6.4.6 挖矿能量销毁

挖矿需要消耗电量(energy)，矿机在挖矿过程中需要消耗电量，1bcv stake 1 个高度消耗 1 个energy，用户可以销毁bcv兑换energy。

6.5 智能合约

智能合约对金融资管公链必不可少，BAC Chain智能合约不仅具有图灵完备，使用灵活，安全可靠等智能合约等基本特点，还提供了生态友好的合约引擎BVM。BVM通过webAssembly和预言机技术等为合约提供了执行安全，性能，多语言等支持。智能合约执行如下图



6.6 预言机

BAC ORACLE模块是预言机的实现，主要分为内部预言机和外部预言机，预言机建立了智能合约和数据的可读通道。BAC ORACLE通过预定义的可配置预言机，智能合约可以确保只有在智能合约验证条件满足后才会真正发生价值转移，同时让智能合约可以同外部数据进行交互。同时，根据约定的合约规则履行情况可以避免纠纷。预言机智能合约可以支持任何的JSON API类型。

6.7 治理

BAC Chain允许任何持有bcvstake的用户参与到公链的共治治理共治治理区块链。Bcvstake可以通过bcv抵押或者销毁得到，Bcvstake的持有者可以通过签署特殊类型的交易来提交提案或者表明他们是否支持（或不支持）提交给区块链网络的提案。治理主要分如下步骤

6.7.1 存款阶段

任何 bcv 代币持有人都可以发起提案，对于想要进入到投票阶段的提案，需要在提交该

提案之后的两周时间内存入至少 1000 bcv 代币，这是进入到投票阶段的最低存款金额要求。除提案发起人之外，其他人也可以只发送一笔存款的交易为该提案提供存款。提案被创建之后可以被查询，用户可以通过浏览器查询提案进展。当提案在规定时间内达到存款要求，提案会被通过，如果在规定时间内不能达到要求，提案会被否决。

6.7.2 投票阶段

一旦提案满足了最低存款限额要求，提案会进入一定时间的投票阶段。在此期间，所有抵押矿机，即bcvstake的持有人可以对该提案进行投票，目前有四个投票选项，分别是“是”、“否”、“行使否决权的否定 (No with Veto)”、“弃权”。

bcvstake的持有数量决定了对提案决策的影响力。矿机可以继承验证人的投票，如果矿机没有投票，验证人的投票会覆盖验证人的决定。

6.7.3 投票结果

在提案投票阶段接受后，投票至少需要满足以下几个条件都满足才会被接受。

超过 40% 的bcvstake 参与投票

需要超过 50% 的bcvstake 支持该提案（即选择的投票结果是“是”）；

低于 33.4% 的 bcvstake 行使“否决权 (No with Veto)”。

如果在投票阶段结束时上述要求中有任何一项没有满足，比如法定人数没有达到，那么该提案就不能被通过。如果提案没有通过，提案的存款不会被退还，会被纳入到社区池中，如果通过了则退换存款。

BAC Chain治理仍处于早期阶段，会随着生态社群意见逐步改进。

6.8 数据存储

区块链的分布式账本仅限于存储简单的交易数据，而不能存储过大的文档，如事务历史记录，历史数据等繁杂的数据流需要专门的存储空间，尤其是非结构文档，更是无法在区块

链上直接存储，而非结构化文档，比如合同电子档备份，存证图片，跟区块链上的数据在业务上紧密关联。为了支持关联链上数据和相关的非结构化文档，实现数据的快速存储和查询，我们引入了传统分布式文件系统跟区块链系统关联，形成了一个“可扩展性”和“去中心化”的开放存储协议。

针对一个区块链上的交易，如果交易存在相关的文档，则将文档的 MD5 Hash 值放在该交易记录中，用一个专门的字段存储。

在读取该记录的时候，先读取链上数据，再根据该交易记录中的 Hash 值定位到分布式文件系统中，读取文档内容，在读取的同时校验该文档的一致性，在确保 Hash 值匹配的情况下，表示该文件是正确的文件，而且本身安全可靠。

使用分布式文件系统是第一步，第二步也可以进一步将文件存储于去中心化的文件存储项目中，比如 IPFS 以及 Lambda 等项目提供的服务中。

6.8.1 隐私数据保护

数据是未来最重要的生产资源，也是个人和企业未来最重要的隐性资产。如何让这样的隐性资产高效、合理、安全地存储和流通起来，也是BAC Chain公链重点要解决的问题之一。BAC Chain会持续的探索隐私数据的存储和流通中遇到的隐私泄露的问题

6.8.1.1 数据加密存储

BAC Chain把用户数据在链外用私钥加密后存储在ipfs或者hdfs等多副本的文件系统中，然后用密码学方式生成文件hash，加入到BAC Chain主链中，这样能减少主链存储资源的使用，也能让数据在隐私存储和公开访问上有所选择。

6.8.1.2 数据授权访问

非对称加解密技术保证了数据在传输过程中，只有持有私钥的双方才能对内容进行解密，从而保证第三方无法对内容进行截取和爆破。BAC Chain 使用ECDH可以计算两对公私钥之

间共享密钥，从而实现账号可以被授权访问。

6.8.1.3 隐私数据交换

BAC Chain可以在不同场景下考虑以下方案：

6.9 安全多方计算 (MPC)

由姚期智在 1982 年正式提出。它主要探讨的是， n 个参与方各自输入信息去计算一个既定的函数，在保证计算的正确性的同时，不泄露参与方输入数据的隐私。具体来说，对于 n 个参与方，每个参与方 i 均知道自己的输入 x_i ，他们想协同计算一个既定函数 $f(x_1, \dots, x_n) = y$ ，使得所有参与方都能获得最终的结果 y ，但 无法获知其他参与方的输入数据。

6.9.1 同态加密 (HE)：

同态加密是一种允许在密文上进行计算的加密方式。除了传统加密方案的原始组件之外，还有另一种计算算法，它将目标函数 F 和加密数据作为输入。同态加密会生成一个加密的结果，当解密此结果时，获得的消息就像是在加密数据的明文上执行 F 。支持 密文上的任意计算的密码系统称为全同态加密 (FHE)。

6.10 监管

6.10.1 社区监管

BAC Chain 通过投票选举到方式，筛选出一类监管节点，监管节点会监管整个主网的运行情况，以及危机处理。例如发生盗币的情况下，被盗者可以向监管节点申报暂时封锁盗币账号，监管账户发送特定的交易，暂停盗币账号的转账功能，验证节点收到这个交易后会执行该交易，盗币账户会被临时冻结。监管节点主要用于紧急处理危机情况。

6.10.2 政策监管

区块链的去中心化是区块链的优点，也是局限。在目前情况下，区块链的使用者并不关心业务的安全性是由去中心化的区块链提供背书的还是由政策权利提供背书的，区块链也是需要接受行业 and 政策的监管的，BAC Chain通过隐私授权访问的方法接受政策监管。

6.11 安全

6.11.1 中间人攻击

中间人攻击是一种由来已久的网络入侵手段，如 SMB 会话劫持、DNS 欺骗等攻击都是典型的 MITM 攻击。其原理是通过拦截正常的网络通信数据，并进行数据篡改和嗅探，而通信的双方无法知晓。BAC Chain 使用类似 Station-to-Station (STS) 协议，在节点之间建立通信的时候建立共享密钥，消息的传播都会使用该密钥加密，可以有效的避免中间人攻击。

6.11.2 双花攻击

双花攻击是指当一个交易被发出后已经经过了 z 个区块时，攻击者又在极短的时间内重新产生了一条新的区块链，使新链比之前的区块链更快，这样攻击者就可以把以前的交易中的花费的虚拟货币取回来并用于二次交易。因为在区块链中，系统会自动承认最长的那条链为有效链。BAC Chain 使用类似 pbft 的共识协议，一旦共识被达成，即不可更改，可以有效的避免这个问题。

6.11.3 女巫攻击

Sybil 攻击是指利用社交网络中的少数节点控制多个虚假身份，从而利用这些身份控制或影响网络的大量正常节点的攻击方式。BAC Chain 使用 bcvstake 作为权利币，持有币才能获取相应的收益和执行相关交易，所以双花攻击不会对 BAC Chain 造威胁。

6.11.4 分叉攻击

分叉攻击是指攻击者直接或者间接获得算力，让他们帮助自己分叉出另外一条最长的区块链。BAC Chain 在处理抵押关系的时候，如果某个验证人的抵押量过大，矿机的抵押会被拒绝，这样可以有效避免某个验证人拥有过大的权利。

6.11.5 DDos 攻击

拒绝服务攻击（DDOS）亦称洪水攻击，是攻击者使用网络上被攻陷的计算机作为“僵尸”向特定的目标发动“拒绝服务”式攻击时其目的在于使目标计算机的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。BAC Chain 可以哨兵模式，屏蔽后端节点服务器，有效地保护出块机器，避免或者减少 DDos 的攻击。

6.11.6 量子攻击

目前区块链系统上普遍使用的非对称加密签名算法，比如基于大整数因子分解难题的 RSA 算法和基于椭圆曲线上离散对数计算难题的 ECC 算法，可以被量子 Shor 算法将 NP 问题变成 P 问题，从而容易被破解。BAC Chain 体系会根据项目进度和量子计算机实用化的发展适时引入抗量子计算暴力破解的加密算法，比如基于格的密码系统 (Lattice-based cryptography)，基于编码的密码系统 (code based cryptosystems) 和多元密码 (multivariate cryptography) 等；其中基于格密码可以设计加密、签名、密钥交换等各种密码系统，是后量子密码学算法的一个重要方向。同时，我们也会对抗量子密码系统的前沿研究方向进行跟进。

6.12 扩展

随着业务的发展，想要公链真正做到更深度化的应用和普及，公链最终会遇到一个关键的问题和瓶颈，就是解决交易的吞吐量和交易的速度问题，这在区块链中也被称作可扩展性，BAC Chain会持续探索公链以下各种可扩展性方案的实现。

6.12.1 单链可扩展性

假设每笔交易为 200Byte，在 10Mbps 的传输宽带下，吞吐量可以达到 6000Tps，普通硬盘的Tps可以达到 10000Tps以上，普通CPU可以达到 8000Tps，目前主流公链的Tps还远远没有达到，使用优化的数据结构和算法有可能进一步挖掘单链的性能，提高公链的Tps。

6.12.2 侧链技术

侧链（SideChains）是针对比特币提出，所以这个概念后期也更多的是在描述比特币相关的扩容，它的定义是：可以让比特币安全地从比特币主链转移到其他区块链，又可以从其他区块链安全地返回比特币主链的一种协议。侧链是一个独立的系统，是一个隔离环境，即使内部出现问题，也不会影响到原有的系统。

6.12.3 分片

分片就是将区块链网络划分成若干能够处理交易的较小的网络，每个小网络可以并行的处理未建立连接的交易，以提高网络的并发量，这样随着节点数增加。

6.13 BAC 的配套生态

当下的区块链技术，并不缺乏各种改进想法，反而最为缺少的是应用。没有应用场景的技术，没有未来。很多公链只考虑技术实现，在主网运行之后，没有应用场景，没有用户，从使用上也根本无法发挥和创造价值，从而缺乏价值支撑，无法激励参与者长久参与。

作为公链的生态，节点、矿工本身得到激励，维护整个公链的基本运行，而在应用上的生态，我们主要从下面 3 个角色分开说：

6.13.1 开发者

公链主网运行之后，依托公链底层开发公链应用，需要公链和开发者双向构建开发者生态。公链开发团队需要将公链代码开源、提供主网服务调用API，各种语言与服务的SDK，配套开发测试工具，当然也包括所有这些技术工具的文档。这些内容也可以由开发者社群完成。而开发者则基于公链的基本功能，基于面向最终用户的业务需要，开发各式各类应用，包括工具、游戏、金融、存证场景应用等。BAC Chain 将基于钱包提供开发所需要完善文档、工具、SDK等，为开发者提供便利。

6.13.2 用户

开发者所开发的应用要面向用户提供服务，开发者以自己的服务价值获得用户增长，但是如果公链生态本身存在大量用户和应用场景，则为开发者基于公链开发应用提供了重要动力和实验场景，所以用户也是公链生态非常重要的组成部分。

BAC Chain 生态与币威钱包都是币威生态成员，币威钱包以百万级用户，为币威生态提供用户与流量支持，开发者开发的 BAC Chain应用，可以优先供给给币威钱包用户使用，公链为币威钱包丰富了用户的应用，币威钱包又为开发者提供了低成本的实验环境和便利的流通获得渠道。

第七章、技术路线图

7.1 2020 年 4 月主网上线

主网稳定上线，实现持有BCV的用户可以挖矿得到BAC。BAC作为支付手续费可以支持主网的流通。

7.2 2020 年 7 月存储网上线

存储网以及其他配套存储设施上线，结合主网考虑存储经济模型，支持用户持久的存储数据。

7.3 2020 年 8 月推进开源，开启应用

实现多种语言开发包的支持，并开放公链源代码。对现有钱包和交易所业务开始挖掘，比如像账户资产验证等上链，实现透明化运营进行探索。

7.4 2020 年 11 月实现去中心化交易协议

去中心化交易协议是资产管理和借贷业务上链的基础，

7.5 2021 年 1 月内置合约实现 DeFi 业务模型

实现内置合约功能，以内置合约形式实现借贷、基金等模型，以实现对纯链上DeFi业务的支持。

7.6 2021 年 6 月合约上线

智能合约开发完成，对适合智能合约的业务做一些迁移探索。

7.7 2021 年之后主网的扩展

加强已经在主网上运行业务的体验，考虑对主网进行分片，分层，侧链，跨链等扩容，使用成熟的技术手段达成业务目标。

第八章、参考资料

- [1] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system, 2008.
<http://bitcoin.org/bitcoin.pdf>.
- [2] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 1982.
- [3] A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER
<https://ethereum.github.io/yellowpaper/paper.pdf>
- [4] Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013a. <http://ethereum.org/ethereum.html>
- [5] CRYPTOKITTIES. Cryptokitties, 2017. [https:// www.cryptokitties.co](https://www.cryptokitties.co).
- [6] cosmos white paper <https://cosmos.network/resources/whitepaper/zh-CN>
- [7]Slasher:
<https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/>
- [8] PBFT: <http://pmg.csail.mit.edu/papers/osdi99.pdf>
- [9] TheDAO: <https://download.slock.it/public/DAO/WhitePaper.pdf>
- [10] Ox protocol: <https://0x.org/docs>
- [11] uniswap:<https://uniswap.org/docs/v2>