

# BFChain 生物链林


(BIOFOREST CHAIN)

全球首款移动端共识公有链

新数字时代的通用型基础设施

# 目录

一、全球区块链底层技术基本现状与 BFChain 的超越创新 .....	2
(一) 当前全球区块链底层技术基本现状 .....	3
(二) BFChain 生物链林的超越创新 .....	5
1. 区块链网络 .....	5
2. 数据存储 .....	8
3. 共识机制 .....	12
4. My Secret 地址私钥管理机制 .....	18
5. The D-Wallet 分布式钱包服务 .....	19
6. 打块机制 .....	20
(三) BFChain 生物链林的七大核心优势 .....	22
1. 支持移动网络 .....	22
2. 超轻量的存储 .....	23
3. 真正的私有钱包 .....	23
4. 人人可获得奖励 .....	24
5. 闪电般的速度 .....	24
6. 完整事务处理能力 .....	25
7. 双离线交易 .....	25
二、BFChain 生物链林核心产品介绍 .....	26
(一) BFChain 生物链林公有链 .....	27
1. 移动端参与共识机制（挖矿） .....	28
2. 离线交易 .....	28
3. 链上担保的【数字资产权益发行智能合约】 .....	29
4. 链上撮合事件 .....	30
5. 链上红包发放 .....	30
6. 跨链事件 .....	31
7. 服务市场 .....	32
8. 应用市场 .....	33
(二) BFChain 生物链林联盟链与私有链 .....	35
三、BFChain 生物链林与价值互联网新经济模型 .....	37
(一) 信息互联网与价值互联网 .....	38
(二) 信息互联网核心经济模型——流量寻租 .....	39
(三) 流量寻租经济模型所带来的问题 .....	40
1. 用户数据问题 .....	40
2. 平台引流费加重企业负担 .....	41
3. 大型流量垄断平台阻断颠覆式创新 .....	41
(四) BFChain 生物链林与价值互联网新经济模型 .....	42
1. 未来需要什么样的区块链？ .....	42
2. 价值互联网新经济模型，以实物上链为例 .....	43
风险提示与免责声明 .....	51

The background is a dark gray field with a complex, symmetrical geometric pattern. A large, bright white triangle is centered, with its apex pointing upwards. Inside this triangle, there are smaller, dimmer triangles and lines, creating a sense of depth and complexity. A bright white point is located at the center of the composition, from which several lines radiate outwards, some of which are part of the larger triangle's structure. The overall effect is one of a futuristic or technological design.

# 一、全球区块链底层技术基本现状与 BFChain 的超越创新

## (一) 当前全球区块链底层技术基本现状

区块链底层技术催生数百年未有之大变局。随着 2021 年比特币价格连创新高，Coinbase 在纳斯达克上市，整个加密数字资产领域进入新一轮的造富运动。然而，这种表面的繁荣却难以掩盖区块链行业在底层技术创新方面的单薄。

区块链的底层技术一般是指一系列分层组件的集合，包括基础平台层（WINDOWS/LINUX/MACOS/UNIX）、核心技术组件（共识、安全、存储、通信）和应用层（可编程合约、可编程资产、钱包、链上激励）。我们说的“区块链底层技术的创新”，主要是指中间层即核心技术组件层的创新。

时至今日，在 BFChain 生物链林正式上线前，目前市场主流的区块链底层技术，一是中本聪发明的比特币（Bitcoin），被称为区块链 1.0；二是 Vitalik 发明的以太坊（Ethereum），被称为区块链 2.0。比特币是区块链底层技术在金融领域的一项应用，是一个点对点的电子货币支付系统，代表了区块链技术的早期成就。以太坊是由俄裔加拿大人 Vitalik 于 2013 年首次提出构想并发布白皮书，旨在构建一个“通用目的的区块链”，历经 9 年发展至今，目前已经成为全球应用最为广泛的区块链底层技术。

以太坊在很多方面都与比特币显著不同，比特币可以看做一个“分布式的共识状态机”，每次交易都会导致一次全局范围内的状态转换，改变所交易比特币的所有权。而以太坊并不跟踪 ETH 所有权的状态，跟踪的是一个通用目的的数据存储的状态改变。“通用目的”

是指任何可以表示为键值元组的数据,基于键值的数据存储可以保存任意复杂的内容,通过某些键来引用。以太坊的状态转换由以太坊虚拟机 (EVM) 来处理, EVM 程序通常被称为 “智能合约”。“智能合约” 这个词语是由密码学家、律师尼克萨博 (Nick Szabo) 定义: “以数字形式指定的系列承诺,包括各方履行这些承诺的协议” (有一种观点认为 Nick Szabo 就是 Satoshi Nakamoto, Nick Szabo 同时也是区块链链式架构的发明者)。简言之, 智能合约是一种能够自动执行合约条款的计算机程序,且代码不可更改。

自 2015 年至今, 基于区块链底层技术的创新却并未如数字资产交易那般看起来一片繁荣。以太坊目前遇到诸多难以解决的问题, 包括交易拥堵、GAS 费居高不下、开发语言受限等。目前全球关于区块链底层的技术创新, 主要集中在以太坊的 Layer2 层面, 即成为以太坊的扩容链、分流链、卫星链, 其中相当一部分仍是以太坊的核心技术底层为中心, 比如对 Solidity 语言进行的改进开发, 比如对虚拟机 EVM 的使用功能方面进行的效率优化, 抑或是在商业模式上进行的改进。在 Layer1 层面, 鲜有突破, 甚至鲜有涉足, 也有一部分项目声称是在 Layer1 层面进行创新的, 但深究其技术底层, 仍然是在以太坊 2018 年发布和开源的 CBC-CASPER 等共识协议基础上进行的细化和发展; 另外也有一些项目提出了很多基于未来设想的白皮书, 但距离真正实现, 还有相当多的具体问题需要面对和解决。

以太坊拥有目前全球最大的区块链生态, 其目前遇到的问题, 也是整个区块链行业遇到的问题: 一是当下区块链生态主要集中在投资

领域，由投资人主导参与，投机盛行却无法融入实体行业，服务于大众生活；二是并未出现爆款 DAPP，用户打开手机只能看到钱包、交易软件等投资工具，无法直观感受“区块链”技术带来的巨大变化；三是第三方钱包的存在，重新形成了新的中介，移动端的数字资产（数字商品）不能直接存储于链上，背离了区块链技术初衷，带来巨大的安全隐患。

## **(二) BFChain 生物链林的超越创新**

BFChain生物链林在区块链底层核心组件层面进行了一系列颠覆式创新，从整体架构设计到节点编码开发，从共识算法到对象存储，从加密算法到广播策略，从性能调优到网络抖动，我们攻克了一个又一个难题，通过无数创新，实现了移动终端直接参与共识机制这一核心目标。在实现这些创新的过程中，为了避免出现技术孤岛，BFChain生物链林开发团队尽最大可能的基于现有开源项目，在保持创新的基础上满足技术的延续性，以促进现有开发社区能更好地参与进来。BFChain生物链林的主要创新有：

### **1. 区块链网络**

为实现移动终端直接参与共识机制，我们在通信领域进行了重新设计。我们重新设计了区块链P2P网络，我们叫它——Full Link Duplex

Communication（全链路双工通信）。区块链网络是建立整个 BFChain



的基础，传统区块链网络基本上都采用 Socket 的方式。

### 1) Socket具有的特点

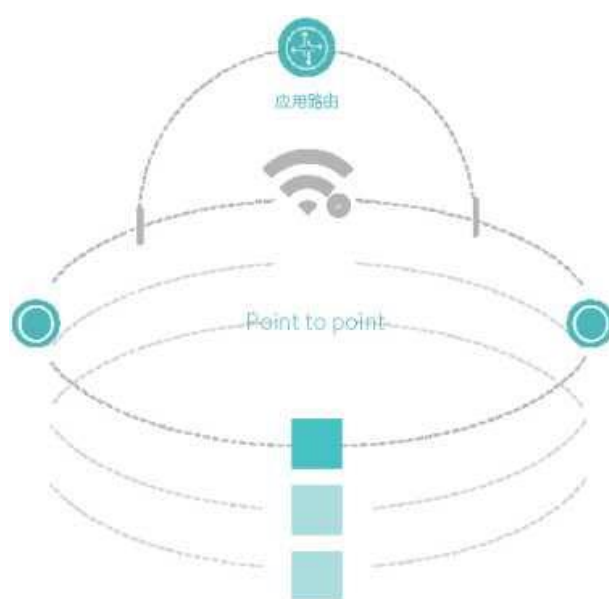
- A. 组件库丰富，很久远之前的编程语言都支持，如上世纪六七十年代的 cobol、c++。
- B. 逻辑简单开发简便，只需要关心传输内容，而不用关心底层通信逻辑。
- C. 不同区域性网络不能直接互通，需要额外的组件支持，例如 GRPC。

### 2) Socket 的问题

- A. 网络连接的自主控制能力较弱，意味着数据实时性，传输的效率很难控制。
- B. 基于 Socket 的应用不能直接与浏览器通信，意味着以 Webkit 一类为核心的应用均不能直接访问区块链网络。
- C. 对于服务到端的主动通信能力较弱，很难建立有效的实时推送机制。

### 3) 更高标准的 BFChain生物链林网络

为了未来 BFChain 生态的发展，我们需要在设计上就允许任何终端类型都可以很方便地接入我们，而当下绝大多数区块链网络在提供对外服务时依然需要一个中心化的服务器（比如移动钱包），于是我们对 BFChain 提出了更高的设计要求——NAAS（Node As A Service 节点即服务），因为这个没有现成的 P2P 网络支持，所以我们对 P2P 网络进行了重新设计。



### 4) WebSocket 机制的引入



对于实时性要求高的场景我们引入了 WebSocket 的机制，这个在“微信”一类应用中常用的协议被我们引入到区块链网络的设计中，它除了继承 Socket 的优点，还能有效提高数据的通信能力和广播效率，并顺带解决了服务到端的主动通信能力，为我们提供高可靠高性能的 BFChain 提供了基础。

## 5) “HTTP 协议”与 WebSocket 协议的结合

除此之外，我们还引入了互联网使用最广泛的协议“HTTP 协议”（后期我们还将逐步升级到 HTTPS），其与 WebSocket 协议有机结合起来，让 BFChain 的网络能力不仅能在节点之间提供高效互通，还能跨区域网络、跨终端类型提供有效互通，为 NAAS 提供支持，并为我们开发真正意义上的分布式应用 DAPP 提供了基础。

应用层	FTP、TELNET、HTTP			SNMP、TFTP、NTP
传输层	TCP			UDP
网络互连层	IP			
主机到网络层	以太网	令牌环网	802.2	HDLCL、PPP、FRAME-RELAY
			802.3	EIA/TIA-232、499、V.35、V.21

## 2. 数据存储

我们重新设计了区块链数据的存储方式，我们叫它——Relational Object Storage（关系对象存储）。数据存储能力是区块链落地的基础，由于区块链的特殊性，无法预设和要求参与节点提供大容量高吞吐的数据存储设备，所以相比传统中心化 IT 建设在设计时就需要增加如

下方面的考虑：

### 1) 存储容量

传统 IT 建设可以要求提供大容量磁盘阵列提高容量，或分离业务与历史数据以降低存储压力与系统性能压力，但区块链网络中无法通过上述两种方法完成。

### 2) 吞吐性能

传统 IT 建设中可以要求节点采用高转速、SSD 等更快速的存储设备，或采用 Raid1 阵列磁盘并增加磁盘数，或分散吞吐压力到多节点，或预加载数据到内存等方式即可有效提高吞吐性能，但到了区块链场景行不通，因为绝大多数参与节点都没有这些设备和条件。

### 3) RSD 移动存储机制

传统 IT 建设中，系统架构是按中心化服务器设计，为了兼顾终端成本问题，终端都不参与业务逻辑计算，同时终端也不会存储业务数据，所以终端几乎没有移动存储的需求，少量存储也是不参与业务逻辑运算的用户文件与个人数据信息，在区块链场景中，每一个参与节点既是终端又是服务端，传统的存储设计方式无法应用在区块链场景中。

因为现实的难题，绝大多数区块链在存储设计上依然沿用传统的 IT 建设思想，数据集中存储在参与节点上，终端参与者（如移动钱包）通过其它参与节点进行中转。

#### A. 传统存储思想的问题

##### a) 伪去中心

因为终端无法直接访问区块链，实际的数据请求和业务过程由其他节点完成，数据的可信度由参与节点是否作弊来保证，这样有违区块链去中心化的初衷。

#### b) 伪节点

终端如果不能接入区块链网络，或接入了区块链网络而数据不全，将不能有效参与网络的治理（传统共识机制下），虽然看上去是一个节点，在一定程度上也可以通过桥接手段完成间接通信，但依然算不上一个合格的参与节点。

#### c) 无法参与共识

当终端网络与数据有一个缺失时，将导致终端失去参与共识的基础，不能参与共识往往代表着不能参与区块的建立，这意味着伴随区块建立的奖励将无缘获得，对于贡献相同参与度的此类终端来说，某种意义上有失公平。

### B. 专属于 BFChain 的 RSD 机制

为了未来 BFChain 生态的发展，鼓励更多的角色与终端接入 BFChain 网络，并获取公平的奖励，我们在设计上就需要兼顾不同终端所面临的接入问题，并提供有效可靠的解决方案。为此我们首次提出了 The R-Node（实时节点）、The S-Node（服务节点）与 The D-Wallet（分布式钱包）的概念，分别实现对高性能网络节点以及分布式服务节点提供支持，为了在实现这些概念的基础上还能保证他们之间也可以参与共识机制，我们对区块链的数据存储机制进行了重新设计。

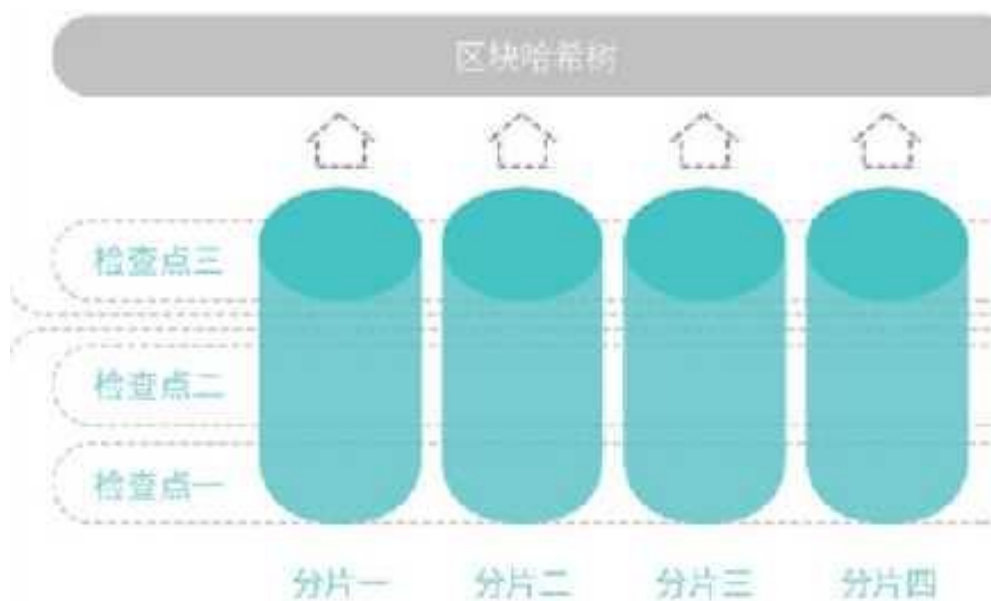
首先为了解决移动终端计算能力有限情况下的计算问题,我们引入了移动设备常用的微型关系型数据库 SQLite,这里主要使用它在没有太多计算资源与存储资源情况下的完整事务运算能力,为我们实现 The D-Wallet 提供了基础。

其次为了解决数据检索效率问题,我们引入了目前使用很普遍的 NoSQL 数据库 Mongodb,主要使用它在链式数据很长情况下的快速检索能力,由于它存储体积不小并且不适用于移动端,我们将其改造并与 SQLite 进行了融合,让节点既可参与共识又可以保持轻巧的体积,为我们实现公平奖励提供了基础。

在 RSD 机制中,两种数据库各有分工,改造后的 Mongodb 主要用于存储区块哈希树,为共识机制执行过程中对分叉问题的处理提供快速识别的能力;对于需要参与共识的移动终端,需要在本地存储部分完整区块数据,并通过这部分数据参与到共识机制中,为了尽可能的减少终端存储的数据量,我们建立了关键检查点,终端只需要存储检查点后的区块数据即可,这部分数据存储在 SQLite 中(为了进一步降低终端体积以及运行资源要求,我们后期将进一步对存储机制进行升级,打造更轻量级的存储实体)。对于关键检查点的确立我们采用和区块一致的共识机制进行完成。

多维分片存储,任意单一设备都将无法在未来的新数字时代为全社会提供服务,所以采用多设备提供服务是必然。BFChain生物链林数据存储时不仅采用多磁盘,还采用了全量多节点共同存储的“多维分片扩容”专利存储技术,数据即可以海量存储,又可以在应用层中

保持逻辑上的单一性。扩容技术使存储性能得到质的提升，为未来全面的商业应用打下了坚实的基础。



### 3. 共识机制

我们重新设计了区块链的共识机制，我们叫它——DPOP（委托参与度权益证明机制）。

共识机制是区块链的灵魂，是区块链网络在去中心的分布式环境下达成一致的必备手段，区块链从 2009 年发展至今出现多种共识机制，它们各有优缺点。

#### 1) 当前各种共识机制的优点

##### A. 工作量证明机制 POW

由算力最强的节点打块，可以有效提高作恶成本；难度提升策略让区块链上任意多个区块通过技术手段同时被改写的概率降到微乎其微。

##### B. 权益证明机制 POS

由最大权益的节点中竞争打块，可以避免计算资源的浪费，让作恶的成本直接与其权益相关，以业务的手段一定程度降低了作恶的概率。

### C. 拜占庭容错机制 PBFT

由网络中所有节点参与投票，投票少于 $(N-1)/3$  个节点反对时达成一致并打块，这种机制实用性强、效率高、资源浪费少，可扩展性强。

随着时间的推移，业务的多元深入，这些有着明显优点的共识机制开始出现力不从心的症状，并在特定场景下表现出明显的弊病。

## 2) 当前各种共识机制的问题

### A. 计算能力浪费

在工作量证明机制 POW 中，只有计算能力最强的节点才能打块，这导致了大量计算能力的浪费，并且让普通大众无法真正参与到节点的共识中。

### B. 权益向顶层集中

在权益证明机制 POS 中，权益越大的人获得打块资格的概率越高，而打块即意味着奖励，这导致“获得奖励提升打块概率”和“提高打块概率而获得更大权益”两者相互促进，导致小权益节点被边缘化并丧失共识的参与权利。

### C. 作恶成本低下

在靠算力与权益的记账模式中，当算力和权益顶层集中后，顶层

集体中的节点对顶层集体外节点的作恶将几乎没有成本；在拜占庭容错机制中，由于所有节点均可参与共识投票，这将导致其投票所代表的业务属性减弱，一个没有权益的节点在这个共识过程中几乎没有作恶成本。

### 3) BFChain生物链特有的共识机制

为了 BFChain生物链生态更久远的考虑，BFChain 数据具有更高的可靠性，有效规避现有共识机制发展过程中出现的问题。受 DPOS 的启发，我们重新设计了基于参与度的 DPOP+DPOS+PBFT 共识机制，它除了有效继承了 POS 的业务属性，DPOS 的高效属性，PBFT 的全员参与属性外，还能有效避免无权益节点和高权益集体作恶成本低的问题，同时还为 The D-Wallet 终端参与共识提供了基础。

在 DPOP 共识机制中，参与投票的节点不仅要提供权益证明，同时还需要提供参与度证明，其中The R-Node 以提供高可靠的网络性能获取参与度，The S-Node 通过提供终端服务获取参与度，每一个参与节点在网络上的活动都会一定程度的增加其参与度，参与度的增加以获取到被服务节点的服务签名为依据，“自参与”以提交的有效交易凭证为依据，这样可以保证不同维度的参与者均可参与网络的共识与治理，从而有效避免单一维度共识机制带来的缺陷。

共识机制代码示例（部分）：

```

voteEquity(block, cb) {
  if (block.height == 1) {
    cb();
  } else {
    let maxBalance;
    let maxCount;
    let voteDirectResult = {};
    let voteIndirectResult = {};
    let allVote = {};

    library.dbLite.query("select
cast(Max(c.balance) as string) from (select * from
mem_accounts2delegates d " +
      "left outer join mem_accounts as a on
d.accountId = a.address group by d.accountId) c",
['MaxBalance'], function (err, MaxBalance) {
      if (err) cb(err);
      maxBalance = MaxBalance[0].MaxBalance ?
MaxBalance[0].MaxBalance : 0;
      library.dbLite.query("select Max(c.count)
from (select count(t.senderId) as count from trs t
where t.trounds = $round and " +
        "t.senderId in (select accountId from
mem_accounts2delegates group by accountId) group by
t.senderId) c", {round:
modules.round.calc(block.height)}, ['Maxcount'],
function (err, Maxcount) {
      if (err) cb(err);
      maxCount = Maxcount[0].Maxcount ?
Maxcount[0].Maxcount : 1;
      library.dbLite.query("select

```



```

cast(m.balance as
string),lower(hex(m.publicKey)),d.accountId,d.depende
ntId,tc.count from mem_accounts
m,mem_accounts2delegates d " +
        "left outer join (select
t.senderId,count(t.senderId) as count from trs t
where t.trounds = $round group by t.senderId) tc on
tc.senderId = d.accountId " +
        "where m.address = d.accountId",
        {round:
modules.round.calc(block.height)}, ["balance",
"publicKey", "accountId", "dependentId", "count"],
function (err, v_rows) {
        if (err) cb(err);
        if (v_rows.length > 0) {
                let rate = new
BigNumber(maxBalance).dividedBy(maxCount).toString();
                for (let i = 0; i <
v_rows.length; i++) {
                        if
(!voteDirectResult[v_rows[i].dependentId]) {
voteDirectResult[v_rows[i].dependentId] = {};
                                }
                                let trading = new
BigNumber(v_rows[i].count ? v_rows[i].count :
0).times(rate).floor().toString();
                                voteDirectResult[
v_rows[i].dependentId ][ v_rows[i].publicKey ] = {
                                        address:
v_rows[i].accountId,
                                        publicKey:
v_rows[i].publicKey,
                                        balance:
v_rows[i].balance,
                                        count:
v_rows[i].count ? v_rows[i].count : 0,
                                        vote: new
BigNumber(v_rows[i].balance).times(1).plus(trading).t

```

```

oString(),
                                dependentId:
v_rows[i].dependentId
                                };
                                }
                                voteIndirectResult =
JSON.parse(JSON.stringify(voteDirectResult));
                                for (let i in
voteDirectResult) {
                                allVote[i] = {vote:
"0", publicKey: i};
                                for (let j in
voteDirectResult[i]) {
                                allVote[i].vote =
new BigNumber(allVote[i].vote).plus(
voteDirectResult[i][j].vote ).toString();

                                self.getVote(voteIndirectResult[i],
voteDirectResult[i][j], voteDirectResult, allVote[i],
i);
                                }
                                }
                                }
                                self.clearEquity(allVote,
voteIndirectResult, block, cb);
                                });
                                });
                                }
}

```

#### 4. My Secret 地址私钥管理机制

我们重新设计了地址私钥的管理机制，我们叫它——My Secret（密语）。

私钥是保证用户权益的底线。在绝大多数区块链中，每一个用户都有一对公钥和私钥，由于私钥字符串无规律还很长，导致几乎没有用户会直接去记住这个私钥，更多的是以图片二维码的形式保存到相册，或者直接由第三方钱包服务商统一保管，这样做可以获得一些直接好处：

- 1) 以图片二维码的形式保存方便用户转移和保管。

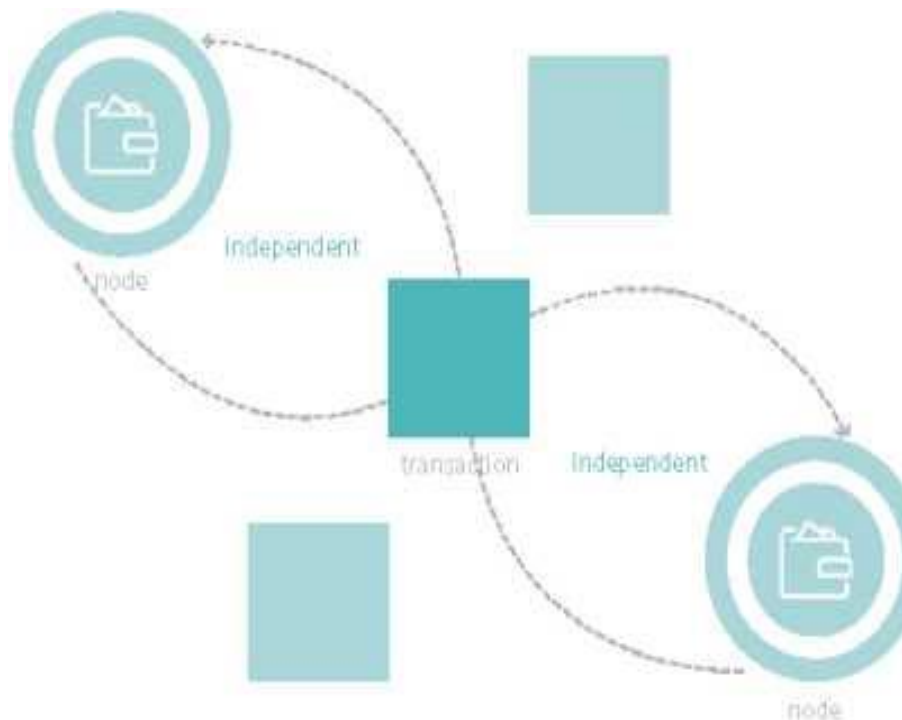
- 2) 第三方钱包服务商统一保管的好处是用户只需记住服务商那里设置的密码即可。在获得这些好处的同时，也带来了一些隐患：

- 图片容易丢失。

- 第三方服务商可能面临安全漏洞、关门倒闭、监守自盗等问题，其本质上是用钱包服务商的信用换取钱包密钥，有违区块链去中心、去信用中介的初衷。

为了在保证密钥安全性的基础上提供便捷的密钥管理，我们设计了“链上密钥保管箱——MySecret”，它采用一段自定义的长密语作为种子（可以是最喜欢的一句台词、一首歌、一首诗），将密钥进行加密后放入链上密钥保管箱。它解决了传统密码位数少强度低容易被破解、原始密钥字符乱无意义难记住、第三方中心保管机构（如blockchain.info）不可靠等一系列问题，让用户不用再借助其它第三方即可真正的在去中心化环境下安全便捷地使用密钥。

## 5. The D-Wallet 分布式钱包服务



我们重新设计了钱包服务机制，我们叫它——The D-Wallet（分布式钱包）。钱包是用户行使权益的必备工具。在绝大多数区块链的设计中，钱包一直被当作一个外部应用，而钱包在这个移动互联网普及的当下，在大多数情况下是在移动端使用，而大多数区块链的设计并不允许移动端的直接访问，所以在落地时一般使用一个中心化的服务提供钱包接入访问，这样做有一些好处：

- 1) 链上逻辑简单，应用与服务彻底分离。
- 2) 减少终端钱包逻辑，对终端设备计算能力要求小。
- 3) 节省终端网络流量，终端钱包只需要向服务器申请获取最终数据即可。

这样做好处明显，但缺点也很突出：

- 1) 钱包服务是中心服务，引入中心服务就会存在一系列隐患。

- 2) 钱包逻辑与区块链逻辑分离，无法保证在任何情况下钱包服务的一致性。
- 3) 钱包没有真正接入区块链网络，无法行使共识权益。

为了保留中心化钱包服务的优点，又不违背区块链分布式初衷，又能让所有参与者行使共识权益，我们将钱包应用抽象为钱包服务，将钱包逻辑集成在链上，首次提出 NAAS 的概念，保证终端无论何时何地只要能连上 BFChain 网络，即可获得一致的钱包体验，并且不用将密钥交给任何第三方，保证分布式环境中用户钱包的可靠与安全。

## 6. 打块机制

我们改进了竞争打块的机制，我们叫它——CABP（Competitive Accounting Based on Participation 基于参与度的竞争记账机制）。区块是组成区块链数据的基本单元，块的生成策略将直接影响区块链网络的性能以及参与节点的权益。传统区块链的区块打块有一些特点：

- 1) 数据完整的参与节点才能参与打块。
- 2) 算力最强或权益最高的参与节点才能参与打块。
- 3) 大多数共识机制中只有打块才能获得收益。

这些特点带来一些直接问题：

- 1) 以数据完整的方式解决数据可靠性问题的同时也制约了轻便型节点的参与。
- 2) 单纯以算力和权益作为打块依据都将导致长期发展受阻，将

出现明显的资源集中与分层。

- 3) 只有参与打块才能获得收益将打击以其它方式贡献参与度节点的积极性。

通过总结传统打块方式带来的问题，基于更长期的考虑，我们改进了打块的机制，算力和权益不再是评判的唯一标准，我们还引入了更多维度，如稳定性、活跃度和交易量，让各种类型的参与者都可以参与到打块工作中，促进 BFChain 吸引各类角色加入从而丰富参与者生态。我们改进了打块奖励的机制，我们叫它——BPIM（Based on Participation Incentive Mechanism基于参与度的奖励机制）

奖励是维持区块链网络的必备条件。奖励机制设计的科学将促进区块链网络的繁荣，反过来也将制约区块链网络的发展。传统区块链网络中的奖励大概有以下两种方式：

- 1) 通过竞争打块获得区块奖励。
- 2) 通过参与交易获得交易手续费。

这两种方式逻辑简单易于执行，但在后期发展中会有一些问题：

- 1) 竞争能力低下的参与节点无法获得区块奖励，对于贡献了其它参与度的参与节点可能有失公平。
- 2) 按手续费交易将带来手续费歧视，打块节点可能为了保证自己的收益优先处理手续费高的交易。

为了解决传统奖励机制带来的问题，BFChain 引入了多维度奖励机制，我们设计了 The R- Node（实时节点）、The S-Node（服务节点）与 The D-Wallet（分布式钱包）。参与节点根据参与方式的不同

可以获得不同类型的奖励，如 The R-Node 主要获取打块奖励、The S-Node 主要获取服务奖励（为 The D-Wallet 提供服务），The R-Node 与 The S-Node 可根据网络环境或参与者意愿相互切换或同时工作，让不同维度的参与度贡献者都可以获得奖励。

在奖励分配中，目前通过权益获得的奖励和提供参与度都会获得奖励，在打块时进行分配（块中包含手续费时也将一起进行分配），权益获得的奖励将会直接分配到权益账户上，参与度奖励将会按权重分配到节点上的所有账户（包括 The D-Wallet 的账户），服务节点每提供一次服务都将增加服务节点获取奖励的权重，这样可以在服务节点少时鼓励服务节点的接入，服务节点充足时鼓励提供更高效率的实时节点，从而通过多维奖励机制从多维度动态平衡BFChain生物链林网络。

### （三）BFChain 七大核心优势

#### 1. 支持移动网络



BTC/ETH 等区块链支持传统 PC 网络，对于不稳定的移动网络支持较弱，在终端移动的情况下将出现不断重连无法提供应用层服务

的情况，在 BFChain 中，BFChain 可以为轻便型移动终端提供很好的支持，即使在网络不稳定的情况下，也能提供应用层服务，让区块链节点在任何网络下均可以参与。

## 2. 超轻量的存储



ETH/BTC  
存储空间为百G级



BFChain  
存储空间为M级

BTC 区块链需要巨大的存储空间达几十G，有些甚至更大，这需要节点提供专有大容量存储设备，在 BFChain生物链林中，BFChain 所需空间将缩小一百倍左右，甚至更小，因为它只需要存储区块链哈希树和关键检查点之后的数据。

## 3. 真正的私有钱包



ETH/BTC  
需要第三方钱包支持



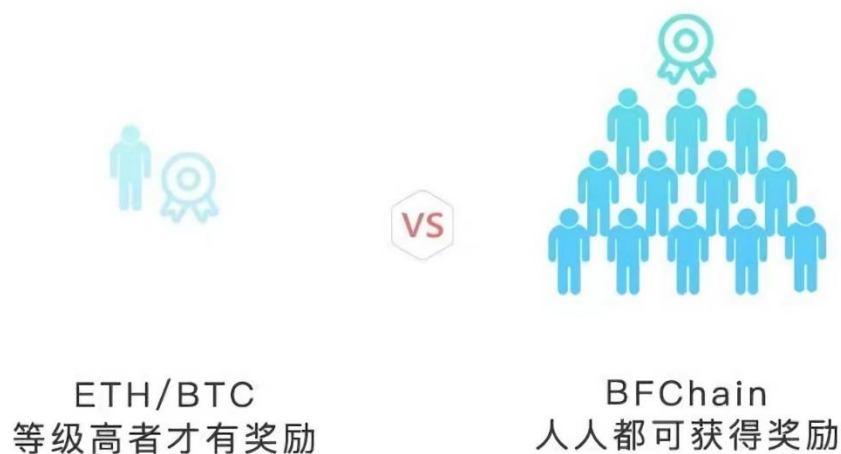
BFChain  
具有链上钱包服务

BTC/ETH 一类的钱包必须要借助中心化的服务器，经常发生被



盗事件，BFChain 生物链林提供真正私有的分布式钱包，钱包不再存放于第三方中心服务器上，而是直接访问区块链节点，更好的保护了钱包私钥，不再因为第三方信用问题、安全问题导致钱包丢失，实现了真正意义上无法被盗取的区块链私有钱包。

#### 4. 人人可获得奖励



BTC/ETH 等区块链中要么算力最强要么权益最大的节点才能获得挖矿奖励，BFChain 生物链林中首创基于参与度的奖励机制，参与节点除了通过算力、权益争取奖励外，也可通过积极参与交易、提供网络等服务获取奖励，将区块链生态网络在扁平环境下具有更公平的参与环境，所有节点均可通过参与度获得挖矿奖励，包括轻便型终端也可以获得奖励。

#### 5. 闪电版的速度



ETH/BTC  
交易的速度很慢

BFChain  
速度是BTC的两百倍

BTC 的交易速度为 6.7 笔每秒,ETH 的交易速度是 25 笔每秒,我们通过重新设计共识机制,分离共识步骤,先商量后打块,大幅度的提高了区块链网络的性能。在 BFChain 生物链林中, BFChain 的交易速度可达 1000 笔每秒,随着未来网络带宽的升级,还将进一步提升交易速度。

## 6. 完整事务处理能力

BFChain生物链林在涉及账务一类的交易中,保证账务的完整事务是必要前提,但传统事务采用时间换可靠性的方式,导致启用事务后交易性能数量级下降。BFChain生物链林拥有全自主知识产权的“内存事务”专利技术,让交易在保证事务完整性的同时又能保证交易速度;在内存事务的设计中,事务性能几乎约等于交易性能。

## 7. 双离线交易

BFChain生物链林区块链上的各节点在交易时,并不完全依赖互联网在线,可以真正做到在离线情况下仍可进行交易。



## 二、BFChain 生物链林 核心产品介绍

## (一) BFChain 生物链林公有链

生物链林是目前世界上第一款移动端共识公有链技术方案的名称。其方案的核心部分在设计上像有生命的生物群，生成的链更像是生物链，再加上其内在跨链特性，可以让所有符合共识机制的链接入并成为整体，直观体验就像组成一片有生命并且可以自我生长的森林，最终取名“生物链林”。

BFChain (Bioforest chain) 是生物链林底层系统的名称，是目前世界上第一款移动端共识公有链的名称。是通往数字时代的通用型基础设施。

BFChain 自 2016 年研发实验室成立以来，研发团队在五年多的时间里攻克了诸多难关，在区块链核心组件方面解决了：当前互联网底层架构普遍存在的网络安全问题、存储难题、不可信等不可调和的痛点；解决了比特币/以太坊区块链在网络、效率、安全性、去中心化、跨链等方面的技术缺陷；解决了区块链接入到移动端设备的三大难题——“计算、网络、存储”，让区块链分布式可信网络应用得以直接接入到移动端设备，为区块链应用的落地和普及提供了无限的前景。

目前，BFChain 生物链林移动端共识公有链技术已经基本成熟，性能和特性足以支撑政府、企业级别的应用，支撑信息互联网生态向价值互联网的迁移。

BFChain 节点软件产品集中呈现了 BFChain 生物链林底层技术的应用和服务，具有八大特点：

## 1. 移动端参与共识机制（挖矿）



根据移动端承载区块链能力的范围，移动区块链目前分为两种类型：一种是移动端不参与区块链共识机制，另一种是移动端作为区块链共识机制的一部分且参与共识机制。前者的移动端是通过区块链为移动端提供链上数据，和传统的客户端 APP 没有本质区别，必须依赖中转服务器才能运行。后者的移动端本身即是区块链的一部分，离线或单机情况下依然可以独立作为区块链节点运行区块链系统，我们称之为移动端共识区块链。

BFChain 生物链林作为移动端共识公有链，第一次实现了能将区块链技术真正接入到移动终端设备，目前移动电话，电脑已经接入，未来如智能家居、汽车、工业终端设备等这些移动终端设备均可作为链上节点，直接参与到区块链的共识治理中。

## 2. 离线交易

当下的互联网交易产品，支付宝、微信支付、银行支付，都需要在有 WIFI、移动网络的情况下才能交易；而比特币网络、以太坊网

络上对于不稳定的移动网络支持较弱,在终端移动的情况下则会出现无法提供资产转移的情况。

在 BFChain 生物链林中, BFChain 可以为移动终端设备提供很好的支持,即使网络不稳定,也能提供应用层服务,让区块链节点在任何网络条件下均可实现链上资产转移,也解决了未来物联网时代,所有智能设备在任何网络下互联互通的问题。

### 3. 链上担保的【数字资产发行智能合约】

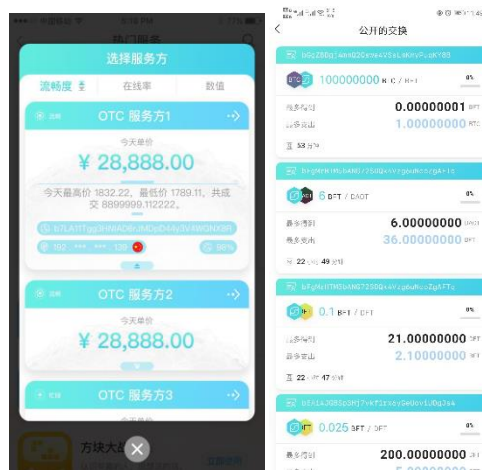


BFChain 生物链林上的数字资产发行,要求数字资产(数字商品、数字权益凭证、数字消费积分等)发行方质押一定数量的 BFChain 主网权益 BFT,生物链林链上担保所发行的数字资产可与 BFT 直接一键兑换。在该数字资产进入流通环节后,持有该数字资产的普通用户,也可以在不通过任何第三人(独立第三方或发行人)的情况下,通过智能合约将自己所拥有的数字资产一键兑换成 BFT。在数字权益凭证场景下(DeFi),数字资产持有人可以一键兑换主网权益 BFT 的功能,将极大程度上形成对数字资产持有人的保护。基于此种保护,又将极



大促进 Defi 的真实繁荣。具有有效担保机制的数字资产发行智能合约以及一键兑换功能，有效提升了数字资产的真实价值和信用等级。

#### 4. 链上撮合事件



BFChain 上，用户可以在链上担保撮合的情况下，任意发起不同跨链资产的兑换，实现数字资产分布式的高速流转，由于交易环节与数字资产完整所有权实现了同步转移，也避免了第三方中介平台参与引入的信用风险。

#### 5. 链上红包发放



基于移动端“日常应用”的天然属性，BFChain 权益红包是区块链落地应用的重要创新，是帮助用户建立区块链认知的起点。BFChain 权益红包经过链上节点的确认和广播，是真正的数字资产转移，与中心化数字钱包或支付宝/微信红包上的账面数字变化有着本质上的区别。同时，在实物上链的场景下，链上红包亦可以发送实物资产所对应的数字资产。案例：A 向 B 通过红包发送了链上数字消费积分 BDH，则 B 收到 BDH 后，可以通过客服人员换取一箱北大荒集团出品的正品五常大米。

## 6. 跨链事件

移动端底层公链 BFChain、平行链 FINChain 等，BFChain 生物链林上的各条平行链均是源自于生物链林的基因，各平行生物链自成体系，又因跨链特性互有关联，不同平行链的资产可以跨链流通，相互促进，相辅相成，像一个有生命的生物群体。具有实际落地应用的垂直领域的平行链将共同带动 BFChain 生物链林生态的丰富和壮大。



## 7. 服务市场



在服务市场内，生物链林提供各种有价值的冲浪市场（Web Application, 简称 WAPP）和节点应用(Node Application, 简称 NAPP)，为开发者、不同类型的节点、用户提供全方位、多元化的服务。

用户可以在冲浪市场上访问感兴趣的链上 Web 网站，或者在节点搜索结果列表中，选择喜欢的节点（如：EOW），然后下载安装，即可使用。区块链应用码农也可以做生物链林的“开发者社区”开发各类 DApp、DWeb 和部署智能合约。在实物上链场景下，数字商品发行方亦可以在冲浪市场进行产品展示，品牌展示以及进行售后服务。

## 8. 应用市场



在 BFChain 生物链林上,企业可根据自身的业务需要和应用场景定制开发平行链。对于无需完全上链的业务,企业也可以选择性上链,独立开发 DAPP 或嵌入式开发于 BFChain 生物链林主链上。各子链在 BFChain 生物链林上,与其他平行链互融互通,共同组成一个有生命的类生物群体。这个群体将在全世界开发者、用户的参与下,为解决社会问题,不断进化,不断迭代更新。

对于企业而言, BFChain 生物链林主要呈现三大功能:

### 1) 授权进化链开发

通过 BFChain 生物链林授权,企业可根据自身的业务需要和应用场景定制开发许可链、平行公有链。

### 2) 实物资产上链和数字资产（包括数字商品、数字消费积分等）发行

BFChain 生物链林为实体企业和机构提供“数字资产锚定实物,由链上数字孪生替代实物在链上流通”,以及数字资产发行和管理服务。

### 3) 链上应用开发、智能合约部署

开发者可在 BFChain 生物链林上开发各类 DApp、DWeb 和部署智能合约，共同打造可信的基础平台。

BFChain 自研发伊始，研发团队在解决了无数技术难题的同时，也创造了众多区块链发明专利。其中，在分布式网络广播、点对点通信、数据分片存储、网络离线交易等方面的成果尤为突出，打造了移动区块链的“专利地图”。

无数的技术创新与突破也让 BFChain 生物链林有着令人惊艳的系统性能表现，并代表着中国公链技术领先全球。BFChain 生物链林实现了最高 10000+TPS 和秒级确认速度，2 小时交易用户容量理论上可达 5000 万+，浏览使用用户 1 亿以上，并具有跨链技术，可以完整的实现跨链技术的最高级别：链上资产直接跨链。这意味着，BFChain 可以基本满足当前网民的日常使用需求，正式上线后更有望成为下一代分布式可信网络的基础设施。

相比传统区块链网络（比特币网络和以太坊网络），BFChain 在安全、性能、业务层面等都有巨大超越，将真正为我们的业务进行服务，从而成为真正有效的数字经济基础设施，为开创全新的数

字时代画上浓墨重彩的一笔。

公有链	BTC(比特币网络)	ETH（以太坊网络）	BFChain生物链林
节点终端	PC端	PC端	移动端（兼容PC端）
移动端接入方式	通过第三方中转	通过第三方中转	无需中转，直接接入
共识机制	POW	POW+POS	DPOP+TPOW+PBFT
参与共识的门槛	具备专业矿机部署能力的人才能参与 链上共识并获得奖励	具备专业矿机部署能力的人才能参与链上 共识并获得奖励	通过智能手机上的节点软件，人人可直接参与链上 共识并获得奖励
参与人群	矿池联盟形式参与； 普通人已无法参与挖矿	矿池联盟形式参与； 普通人已无法参与挖矿	通过手机即可参与链上治理
TPS参数	6.7笔/秒	25笔/秒	10000笔/秒
最快确认时间	1个小时	15秒	1秒
用户容纳量	2.5万/1小时	10万/1小时	7000万/两小时
单区块最大交易数	2,020	200	1,500,000
分叉风险	已分叉	已分叉	永不分叉
落地应用情况及前景	无法开发应用	支持DAPP开发	支持DApp开发，web开发、小程序开发

不同的主流公有链性能对比图

(二) BFChain 生物链林联盟链与私有链

BFChain 可信数据版联盟链其底层技术来源于 BFChain 生物链林公有链，是目前全球首款且唯一一个可支持跨终端直接上链的联盟链底层平台，是基于 BFChain 生物链林基因上的联盟链、私有链服务，继承了 BFChain 生物链林的所有优点，同时还有众多创新，从技术底层逻辑、事务底层逻辑上解决问题。

可信数据版属于区块链通用型底层基础设施，可服务于所有类型的区块链应用服务场景，为政府、企业实现私有化的底层区块链部署。

联盟链可信数据版核心解决：数据存证、数据存储、数据互联互通、简化流程、财务审计、防伪溯源的问题。联盟链可信数据版保证数据真实可信，为分析、调整工作提供可靠依据；打通传统业务应用系统的数据孤岛，促进涉及的多系统间、机构间信息的流动和多方协

作，全方位提高运行管理效率，是政府、企业做数字化转型的可靠基础设施。

联盟链数据版满足企业级应用在性能、安全、隐私、权限、可扩展性、可用性等全方位的商用需求，相比其他联盟链，在安全、性能、业务层面等都有所超越，使解决问题的深度、安全性、成本投入、经济效益、附加值、性价比等全方位都达到前所未有的程度。

联盟链可信数据版是一个“永动机”：全年 365 天，24 小时无需任何人、任何服务器、任何机构去分发、中转和维护数据，满足政府部门、企业源源不断的数据产生、处理和存储需求，极大降低资源消耗。





### 三、BFChain 生物链林 与价值互联网新经济模型

## (一) 信息互联网与价值互联网

互联网始于 1969 年美国的阿帕网。通常 internet 泛指互联网，而 Internet 则特指因特网。这种将计算机网络互相联接在一起的方法可称作“网络互联”，在此基础上发展出覆盖全世界的全球性互联网络，称为互联网。Internet 使用一种专门的计算机语言(协议)，以保证数据安全、可靠地到达指定的目的地，这种语言分为 TCP(Transmission Control Protocol 传输控制协议)和 IP(Internet Protocol 网间协议)两部分。互联网经济是基于互联网这项革命性的技术创新所产生的经济活动的总和，当今发展阶段主要包括电子商务、互联网金融 (ITFIN)、即时通讯、搜索引擎和网络游戏五大类型。信息互联网由于存在中心化服务器（后台），数据技术上可篡改，可无限复制，因此主要承担了信息传递功能。

区块链技术产生后，相对于可进行信息传递的经典互联网而言，区块链所搭建的网络被称为价值互联网。价值互联网出现的标志性事件为比特币的发明。在比特币区块链中，人类第一次在网络数字世界实现了价值传递。价值互联网出现的一个重大意义在于，人们可以像转移信息流一样便捷的实现资产、商品或者资金的所有权转移（解决了数据的“双花”问题）。这种转移是首次在数字世界里真正实现了完整的所有权转移。

我们以区块链数字红包为例。在现实世界中，A 送给了 B 一个红包 100 元现金，B 收到了这 100 元现金，此时，对于这 100 元现金，B 享有完整的所有权，占有、使用、收益、处分。

而在信息互联网世界里，A 于某平台之上向 B 发送一个 100 元红包，B 在该平台的账户上显示收到了该 100 元红包，存入了 B 的某平台钱包。此刻，B 对该 100 元钱，由于 B 并未真正占有该 100 元钱，因此只享有对该 100 元资金的虚拟所有权。假如此时该平台由于各种原因不予支付，或平台关闭，则 B 将承受这 100 元的损失。

在以区块链为技术底层的价值互联网中，A 给 B 发送一个数字资产红包。则 B 完整享有该数字资产的所有权（占有、使用、收益和处分），如同现实世界中一样，无需通过任何第三方平台，就可以完整的行使对该资产的全部权利。价值互联网，在网络世界中，实现了资产的链上确权以及所有权的真实而完整的转移。

## （二） 信息互联网核心经济模型——流量寻租

信息互联网技术催生出了互联网经济模型。互联网经济模型在上世纪 90 年代后获得了飞速发展并成长壮大至今。我们耳熟能详的全球各大互联网经济巨头，都得益于互联网技术所带来的新的盈利模型（相对于工业经济模型）。

信息互联网时代的核心经济模型是流量寻租。寻租（rent seeking, 又称为竞租）是指在没有从事生产的情况下，为垄断社会资源或维持垄断地位，从而得到垄断利润（亦即经济租）所从事的一种非生产性寻利活动。简单的说来就是通过流量的垄断归集与分发进行变现。垄断型互联网平台公司归集了海量的流量，并通过向客户引流，收取平台费（引流费）获取收益。



大数据在流量寻租的过程中起到了关键的精准引流的作用，极大加速了流量变现的效能。比如我们随口提到一款产品的名称，很快你就可以在你手机里的部分 APP 中发现与之相关的推送。大数据采集海量用户数据，经过数据清洗、脱敏、建模等一系列处理，对用户生成标签，勾勒画像，为精准营销提供依据。社交平台比如 Facebook，超过 90% 的收益来自于精准营销广告。

### (三) 流量寻租经济模型所带来的问题

#### 1. 用户数据问题

2021 年 4 月 27 日，苹果推送了 iOS 14.5 系统，苹果新的隐私政策开始正式生效。用户更新系统后，所有 App 在收集用户数据并用于跨 App 投放时，都必须单独弹窗提示，并获得用户同意。苹果的隐私新政策在数字广告行业引发了“强烈地震”，多年以来建立的，利用数字营销的平台提供免费服务的流量寻租商业模式将会面临重塑。

在互联网流量寻租经济模型中，数据采集、交换和应用的过程如同一个全封闭式的黑箱，一直以来，用户并不清楚地知道自己的数据在哪里，如何被使用，数据使用单位也没有直观、透明地披露这个流程。这里面涉及到的问题主要有数据隐私和数据的所有权归属。关于用户隐私方面，全球已经形成基本共识，苹果对 IDFA 的限制已经正式生效；主流浏览器正在逐步停止对第三方 Cookie 的支持，Safari 和 Firefox 目前已经默认禁用 Cookie，Chrome 宣布在 2022 年前也将停止支持第三方 Cookie。

随着数据作为一种生产资料的概念越来越深入人心，人们日益将个人数据视作个人合法资产，期待享有个人数据的所有权。个人用户数据所有权要实现的技术前提在于数据的确权。目前的信息互联网基础设施无法完成用户数据在数据生产者层面的确权，比如用户每天使用手机所产生的数据，无法在用户层面进行确权，不能确权也就无法行使所有权，不能交易流转。BFChain 生物链林移动共识区块链技术通过用户主动选择移动端数据上链，为大规模的进行个人用户数据的链上确权提供了底层技术支持。

## **2. 平台引流费加重企业负担**

据统计，目前大型互联网电商平台的引流费为，商家每获得一个新用户，平均需向流量平台支付 200-300 元。当企业营销时，总会面临各种困扰，钱花出去很多，却收效甚微；即使获得的流量可观，却又面临着流量真假的问题。2018 年《纽约杂志》旗下刊物 Intelligencer 曾报出一个数字：实际上只有不到 60% 的网络流量是人类的，在其他的虚假流量里，大多数是机器人在阅读信息。换言之，信息互联网世界中大约 40% 的流量是虚假的。“引流费不断飙升的情况下仍收效较低”的问题，逐渐让越来越多企业不堪重负，重新回到线下引流或新零售的道路。

## **3. 大型流量垄断平台阻断颠覆式创新**

互联网巨头的地位由流量造就。流量的垄断催生了超大型的互联

网垄断平台。对于一部分垄断型电商平台或社交平台而言，会进行大量的行业平行或上下游的整合并购工作，这些标的公司一旦被收购，基本就丧失了自主研发，独立创新的能力。大型互联网电商平台或社交平台的产品多为交易型产品，巨大的流量黑洞需要源源不断的流量补给才能持续运作，因此所有被收购企业都必须融入其生态圈里，接受统一管理，而当这些流量入口的价值被耗尽时，则会被抛弃，下一个流量池将迅速替补。

互联网巨头通过流量垄断，进而实现技术垄断，资源垄断，资本垄断。垄断扼杀创新，尤其是革命性的颠覆式创新。当互联网产业资本与金融资本相结合时，更倾向于通过资本资源的力量将项目催熟，速成，不断以并购壮大垄断版图，通过资源强势导入，获得垄断超额利润。

#### **(四) BFCChain 生物链林与价值互联网新经济模型**

##### **1. 未来需要什么样的区块链？**

###### **1) 能打破区块链“不可能三角”的区块链**

未来，我们需要在“去中心化、安全性”前提下还具备高性能，不会网络堵塞的区块链底层技术。

性能：TPS 指系统每秒处理的事务数，是衡量一个区块链系统性能最重要的指标之一，TPS 决定区块链系统能够承担的业务量。目前大多数区块链，在面临业务量多时，都会发生网络堵塞，无法形成规模应用。

去中心化：在一个分布有众多节点的系统中，拥有足够多的节点，而不依赖少量超级节点做决策，每个节点都拥有同样的能力和权利，且高度自治，形成新的连接单元和组织形式。

安全：区块链的网络接入、数据传输、数据存储、数据共享等都不会被随意攻破，很好实现隐私保护和数据安全。

## 2) 符合人性对“公平激励、真实可信”的追求

区块链作为“信任机器”，之所以将颠覆社会秩序，很大程度上是因为它很好调和了缺乏信任、分配不公的社会矛盾。作为区块链的灵魂——共识机制极度重要，能否满足人性的渴望和追求，是它能否规模应用的关键因素。

## 3) 形成“良品驱逐劣品”正向循环的商业生态

在正向的可信商业体系上，企业不再担心合作伙伴不守商业规则，不用担心被平台抽佣，被平台遏制，不用担心好产品缺少客户，只需要踏踏实实做好产品，做好服务，用产品和服务回馈社会。

## 4) 移动区块链：

支持全产业、全场景、全终端的通用型基础设施

区块链作为数字经济的基础设施，未来技术发展的必然方向是，使之更普适于各类行业和场景。移动端参与共识区块链，终端用户直接上链，才是足以支持全产业、全场景、全终端的通用型基础设施。

## 2. 价值互联网新经济模型，以实物上链为例

BFChain 生物链林是全球第一个实现移动端“实物上链”的公有

链。“实物数字化”属于“数字化转型”的范畴，但与当下主流所理解的“数字化”，在逻辑和实现手段上并不一样，在解决企业问题的深度更加深刻有效，是未来数字经济的必然方向。

数字化转型,本质上是对数据的全生命周期进行转型调整,使“数据”要素充分流动,流动性就是价值。而“实物上链”实际上是实物资产价值化的过程,通过数字技术的手段保障资产价值化,激发实物资产的流动性,以赋能实体经济,就是资产数字化的内涵。“实物上链”是指将实物资产的信息、权属和价值映射到区块链上,实物一对一锚定数字资产/数字凭证,数字资产/数字凭证在链上流通的同时,也具备在链下流通时的各种属性,比如权属。

“实物上链”实现资产从“生产端-销售端-服务端-消费端”的全价值链都在链上确权和流转,终端消费者用数字资产/数字凭证向生产企业兑换实物。生产商、中间商、消费者三方都可以在可信环境下进行价值交换。“实物数字化”具有几大优势:跨时空、高效率、低损耗、低成本、防伪溯源。

“实物上链”的流程:

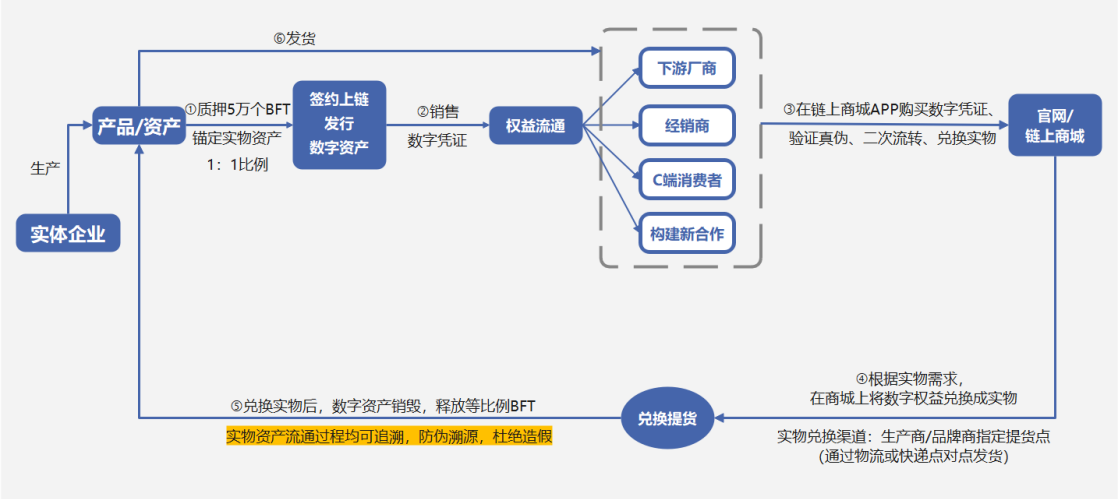
- 1) 数字资产(数字商品)发行人可以在链上质押定量的权益,发行相应的实物数字资产/数字凭证锚定实物资产,将原来的实物资产1:1映射到链上。

- 2) 需要产品的B端下游厂商、中间商或C端终端消费者在链上购买数字资产/数字凭证,即拥有实物的所有权。

- 3) B端下游厂商、中间商或C端终端消费者可凭数字资产/数字

凭证兑换实物，通过企业指定提货方式提货；如无需兑换，可以在链上进行多次流转，实现价值交换，甚至保有数字资产（数字商品）进行储值。

4) B 端下游厂商、中间商或 C 端终端消费者兑换实物时，相应的数字资产/数字凭证借助智能合约技术同时销毁，解冻出质押链上的 BFT（BFChain 生物链林链上的主权益）到实体企业的权益地址。



实物上链流程图

实物上链解决的问题：

1) 实物流、信息流和资金流趋于“同质化”

目前，价值流、信息流和实物流具有完全不同的特性和流动性；在 5G、物联网、区块链等前沿技术广泛而深度运用的未来，价值流、信息流和实物流将更多的表现出“同质性”。物理世界的每一样物品，在区块链的映射下，都会在数字世界里产生与之对应的数字孪生，实物流将体现出信息流和资金流的特性；实物上链后，“帐就是钱，钱就是帐”，“物就是钱，钱就是物”信息流、资金流、实物流深度交融，最终实现实物流、资金流、信息流 “三流合一”，进而有可能带

来金融服务实体经济方式的根本变革。

## 2) 帮助企业系统性解决“资金、客户、市场”三座大山

实物的“资产数字化”过程，实际上通过区块链技术重构了新经济模型，全方位、多层次的解决企业运行各环节的问题，同时满足企业“市场、融资、转型”的核心需求，实现良性循环；帮助企业解决企业账务效率低、流通成本高、库存风险大、拓客成本高、防伪打假难、信用积累慢等一系列痛点，可以为企业降本增效，提升资产流动；同时对于高附加值、高安全要求的商品，具有防伪溯源、从源头上杜绝假冒伪劣的意义。

BFChain 资产数字化重构企业运营全环节：

流程与类别	实现逻辑与效果
采购和生产	数字资产发行人可以预先销售与实物 1:1 锚定的数字资产，提前锁定用户，以销定产。
营销和销售	商品链上流转跨越时空限制，变得简单快速，引领新的消费方式，赠礼和转让方便会带来更多需求，无形中促进销售。同时，经销商、中间商和用户三合一，搭建起共治、共建的销售网络，带来更多企业客户，多方共赢。
运营管理	降低系统维护成本、打假成本、多主体的内耗。
品牌和影响力	借助区块链“公开透明可追溯”的特性，能增强企业的信用级别和影响力，品牌效应上占领先机。
产品质量	借助区块链技术，防伪溯源，安全保真。
资金周转率	消费者可以预先在链上购买相应的数字资产(以有优惠的价格)，企业将提前回笼资金，加速资金流转，以便再投入、再生产。
资产掌控	真正实现资产由企业自己掌管，无需依赖于第三方。

### 3) 全方位协同各方利益，变革温和过渡

#### A. 对于中间商而言：

实物资产数字化使中间商的经营变得灵活，只需要流转资产的数字权益，不需要再流转大量的实体资产，提高商业效率。同时，随着销售体系扁平化，实体企业和中间商会形成更加健全高效的合作模式，中间商将从销售商的角色转变为服务商的角色，提供如少量仓储、兑



换提货等服务，中间商无需再负担压货、中库存的风险；大大降低中间商的运营成本和流通成本，包括物流、仓储、管理、损耗等成本。

B. 对于终端消费者而言：

资产数字化后，消费者在链上购买数字资产/数字凭证，可以按需兑换，也可以在兑换前在链上流转出售，灵活性极强。另外，消费者用凭证直接向企业兑换实物，具有正品保证。

资产数字化同时符合实体企业、中间商、消费者的利益，推行阻力相对较小。

#### 4) 重构新经济商业模式

从更长远的角度看，“移动共识区块链+资产数字化”将重构未来的商业生态，改变当下“企业受制于互联网垄断平台”的现状，形成一个良性循环发展的社会生态。

A. BFChain 生物链林作为分布式可信底层系统，不存在中心化服务器，不存在绝对中心机构，对市场没有垄断威胁，同时也没有类似“互联网平台引流费”这样的流量寻租模式，企业极大的减轻了负担，企业和市场可以迎来百花齐放。

B. BFChain 生物链林区块链技术的可追溯性、不可篡改性、公开透明性，使得企业造假作弊的成本很高，因为其一旦作恶，就没有其他企业、消费者会继续合作，无形中倒逼企业诚信经营，为社会提供优质的产品和服务，促进市场的良性竞争和正向发展。

C. BFChain 生物链林底层系统支撑企业做资产数字化，使企业各类生产要素充分流动，使资金流、信息流、实物流良好融合，降本增

效，减少企业各环节的内耗，系统性调整企业的生产力和生产关系，这也是企业做数字化转型的核心目标之一。

D. 在 BFChain 生物链林可信基础设施构建的可信商业体系上，企业不用再担心合作伙伴不守商业规则，不用担心被平台抽佣，被平台遏制，不用担心好产品缺少客户，只需要踏踏实实做好产品，做好服务，用产品和服务回馈社会，形成一个“良品驱逐劣品”良性竞争的商业生态。

5) 通过改善经营解决企业“现金流”问题，降低全社会融资成本

现金流基本决定了企业的生存和运作能力。也因此，IPO 上市、风险投融资、债券、民间放贷、互金平台等成为了企业融资的灵丹妙药。但所有融资方式都是：用未来收益来弥补当下的现金不足，用“未来的未来”的收益来弥补未来的窟窿，不断放大杠杆，滋生泡沫，最后一旦资金链断裂，企业彻底丧失生命力。

借助实物资产数字化，企业可以通过发行的数字资产/数字凭证提前进入销售环节，快速回笼资金，形成经营性现金流，极大提升了存货周转能力。由于数字资产/数字凭证是与实物的一对一锚定，因此，数字凭证代表的是实物商品本身，这一点与“资产的证券化”有本质的区别。

实物上链同时也是物理世界在链上世界的复刻行为，随着物联网、人工智能、高速网络等配套技术的纵深发展，物理世界将日益精细的在数字世界复刻出它的“数字孪生”，在永不停歇的复刻下，人类终将完成由物理世界向数字世界的大迁徙。在这场大迁徙中，在即将到

来的未来新数字时代中, 移动端共识公有链 BFChain 生物链林必将成为不可替代的通用型基础设施。

## 风险提示与免责声明

本白皮书并非提供您是否购买任何 BFChain 生物链林数字资产的建议，亦非您进行任何契约或购买行为应参考的文件。本白皮书不构成任何买卖行为之要约，亦不构成任何形式的合约或承诺。BFChain 生物链林并未计划在任何国家或司法管辖区构成证券或其他任何应受管制的产品。

本白皮书非募集说明书或其他任何证券发行文件的基础，亦不拟作为在任何国家或司法管辖区发行或募资证券或其他任何应受管制的产品。本白皮书未被任何国家或司法管辖区的任一监管机构审核。

您认知并同意，BFChain 生物链林不具备下列功能：

- 1.代表 BFChain 生物链林或任何司法管辖区之任何其他机构之股权、控制权或义务，或参与、控制前述机构应用决策之权利；
- 2.代表任何类型之投资；
- 3.代表任何拥有内在价值或市场价格之有价值证券；
- 4.代表任何人有义务赎回、或购买的商品或资产。

参与者一旦参与本计划，代表其已确认理解并认可细则中的各项条款说明，接受潜在风险，后果自担。

1.市场风险：若加密货币市场整体价值被高估，那么投资风险将加大，参与者可能会对项目的价格增长抱有较高期望，但这些高期望可能无法实现。

2.系统性风险：是指不可抗力因素，包括但不限于自然灾害政治

动荡等。

3.监管风险：加密货币的交易具有极高不确定性，由于加密货币交易领域目前尚缺乏强有力的监管，加密货币存在暴涨暴跌等情况的风险，个人参与者入市后若缺乏经验，可能难以抵御市场不稳定所带来的资产冲击与心理压力。

4.项目风险：团队将不遗余力去实现白皮书中提到的目标，现已有较为成熟的商业模式，然而由于行业整体发展趋势不可预见，现有的商业模式可能无法与市场需求良好吻合，从而导致营利难以实现。同时，由于本白皮书可能随着项目细节的落地进行更新，如果项目更新后的细节未被本计划参与者及时获取，参与者因信息不对称而认知不足，从而影响到参与项目的后续发展。

5.技术风险：本项目基于密码学算法，密码学的迅速发展也带来潜在的被破解风险；区块链、分布式存储等技术支撑着核心业务发展，团队不能完全保证技术的落地；项目更新过程中，可能会发现有漏洞存在，可通过发布更新的方式进行弥补，但不能保证漏洞所致影响的程度。

6.黑客攻击与犯罪风险：在安全性方面，电子代币具有匿名、难以追溯等特点，易遭到骇客攻击或被犯罪分子利用，或可能涉及到非法资产转移等犯罪行为。

7.政策风险：目前国际对于区块链项目以及以虚拟货币方融资的监管政策尚不明确，存在一定的因政策原因而造成参与者损失的可能性。

8.未知风险：随着区块链技术的不断发展，可能会面临一些当前无法预料的风险。

本白皮书无任何声明或保证确保其中所描述或所传达与本计划有关的资讯、陈述、意见或其他事项为正确或完整，亦未对任何具前瞻性或概念性陈述的成果或合理性做出任何声明或保证，且无声明与保证之事项不限于前述事项。本白皮书中任一处皆不应构成或被视为对未来所作之任何承诺或声明。

在适用法律充分允许的范围内，任何人按照本白皮书行动而因此产生或有相关的任何损失或损害时，不论其是否系属疏忽、默认或注意不足，我们不会对该等损失或损害赔偿或负任何责任。

请参与者在参与之前，充分了解团队背景、整体框架，理性参与。

BFChain 有权随时修正与变更本白皮书之内容。