贝富链(BFchain)白皮书

一个加密数字货币生态系统

(修订版）

前言

比特币作为数字货币1.0版本经过多年的发展，它的去中心化设计，容错力，抗攻击力，防勾结串通的加密性已得到普遍认可。而相当于比特币2.0升级版的以太坊，首创了图灵完备的可视化脚本语言Solidity。在Solidity中，一个合约由一组代码(合约的函数)和数据(合约的状态)组成。它允许参与者编写任意复杂的智能合约。以太坊的这种智能合约可以将区块链应用扩展至全网价值交换和指令执行程序运行层面，从而体现出其创建一个无法停止，抗屏蔽审查和自我维持的全球性节点计算机的特色。我们在以太坊的合约机制基础上，为了更友好地适应情景应用，创立了新的区块链，并创新地设计了两套平行、但随时可以交插的分布式记帐系统，以此解决了其他区块链在除去记录时间戳和签名后，不能横向记录的不足。这就是我们创立的区块链3.0版本 --- 贝富链(BFchain)和它的贝富币(BFcoin)。

目录

理念

我们开发贝富链(BFchain)和贝富币(BFcoin)源于以下四个理念：

一. 确保系统底层去中心化。我们延续了比特币和以太坊的优点，把贝富链(BFchain)和贝富币(BFcoin)设计成为一种全球性的去中心化分布式应用和记账系统。我们还同时平行设计另一套局域内针对贝富代币(BFtoken)的分布式记账ID系统，更好地记录现实世界的附属数据和提高应用端的效率，补充了比特币和以太坊等对现实世界支持方面的不足。但对于比特币和以太坊等在去中心化分布式记账方式和保证历史记录不被篡改等方面的优点和功能，我们仍然保留和忠实执行。

二. 我们希望贝富币(BFcoin)在公众的接受和使用下体现它在虚拟社区里和现实世界中的价值，并在流通和使用中丰富和增加这种价值。我们郑重保证完全开源，不受中心化的组织、机构或个人操控。

三. 为了实现以上所述贝富币(BFcoin)的这种价值，我们会给贝富币(BFcoin)设计了各种应用情境，虚实结合，并让贝富币(BFcoin)在应用中充分实现它的价值。

四. 我们保证贝富币(BFcoin)的私隐性和在应用中的独立性和扩展性。研发贝富币(BFcoin)是以情境应用为目的，但我们也不会阻止贝富币(BFcoin)拥有者在任何平台的流通和交易。我们欢迎贝富币(BFcoin)的价值在各种平台得到体现，无论是在应用平台还是交易平台，无论是在虚拟社区或是在现实世界。

长期战略

我们的长期战略是: 利用贝富链(BFchain)搭建专注于著作权，防伪，游戏，数字商品，公益平台，和其他应用情景的加密数字货币生态系统，并最终为人们在各种情境中使用，让贝富币(BFcoin)的价值在实际应用中得到体现。

贝富链(BFchain)是一种新型的智能应用区块链，分为贝富币(BFcoin) 和贝富代币(BFtoken)。 贝富币(BFcoin)通过去中心化的BlockNAS(Block with Network Attached Storage)充分利用富余网络资源进行云盘挖矿，以加密数字货币奖励区块原创参与者；贝富代币(BFtoken)被设计为由公钥和私钥共同产生的带ID的局域内区块链。只有那些获得根证书颁发机构签署的认证ID才获准进入该局域内区块链。贝富链(BFchain)平台一些应用情境下的奖励方式如下：

一. 通过云著作权区块节点对云著作原创记录加密私钥转化代币奖励原著作者。

二. 通过云流媒体原创区块节点对原创云流媒体的原创记录加密私钥转化代币奖励原创流媒体创作者。

三. 通过GPS游戏区块节点位移记录加密运算转化代币的形式奖励区块游戏价值创造者。

四. 其他应用（例如：社区公益平台，版权防伪平台等)的奖励方式。

1.贝富币(BFcoin)的算法，挖矿和分配

1.1 贝富币(BFcoin)的算法

贝富币(BFcoin)的运算设计有如下特性：

a.相对于比特币的 c++语言及栈式脚本、以太坊的新语言 solidity，javascript 流行度更高、受众更广、上手更容易的一门语言。贝富链(BFchain)的新语言，同样遵循简洁，桌面化的设计原则。

b.贝富虚拟机(EVM，源自以太坊)是贝富链(BFchain)中智能合约的运行环境。它不f仅被沙箱封装起来，事实上它被完全隔离，也就是说运行在EVM内部的代码不能接触到网络、文件系统或者其它进程。甚至其各智能合约之间只有有限的接触。为了能让贝富币(BFcoin)比比特币和以太坊更接地气，通俗化，老少咸宜，我们独特的BFweb浏览器已在研发测试中，待测试成功后，会开源共享。

c.比特币中所描述到的“简化支付验证”(SPV)的概念表明，不是下载每一笔交易以及每一个区块，一个“轻客户端”(light client)都可以仅下载链的区块头。它的每个区块中的数据块大小为80字节，区块仅包含五项内容：上一区块头的哈希值、时间戳、挖矿难度值、工作量证明随机数(nonce)、和包含该区块交易的梅克尔树的根哈希。这就是传统的梅克尔树(merkle tree)。传统的trie只有一种节点，该节点是一个数组，每个index是指向子节点的指针。以太坊使用的Merkle Patricia Tree(简称MPT树)增加了两个新的节点，称为叶节点和扩展节点。这两个节点的形式一样，都是一个[key,value]的组合，原来的节点称为分支节点。

贝富链(BFchain)使用的也是 Merkle Patricia Tree 加密认证的数据结构，头部包括一个区块头，一个交易的列表和一个uncle区块的列表。区块头部包括了交易的hash树根和用来校验交易的列表。在p2p网络上传输的交易是一个简单的列表。它们被组装成一个叫做trie树的特殊数据结构，来计算根hash。值得注意的是，除了校验区块外，这个数据结构并不是必须的。一旦区块被验证正确，那么它在技术上是可以忽略的。这意味着交易列表在本地以trie树的形式存储，发送给客户端的时候序列化成列表。客户端接收到交易列表后重新构建交易列个表trie树来验证根hash。

RLP(Recursive length prefix encoding, 递归长度前缀编码)被用来对trie树种所有的条目进行编码。

上面的设计显示，贝富币(BFcoin)是一种全球性的去中心化分布式应用和记账系统。

1.2 挖矿的难度设计

```
{
  "difficulty": "0×400",
}
```

其中的"difficulty": "0×400",就是难度，两进制，设置当前区块的难度，如果难度过大，cpu挖矿就很难，这里设置较小难度.

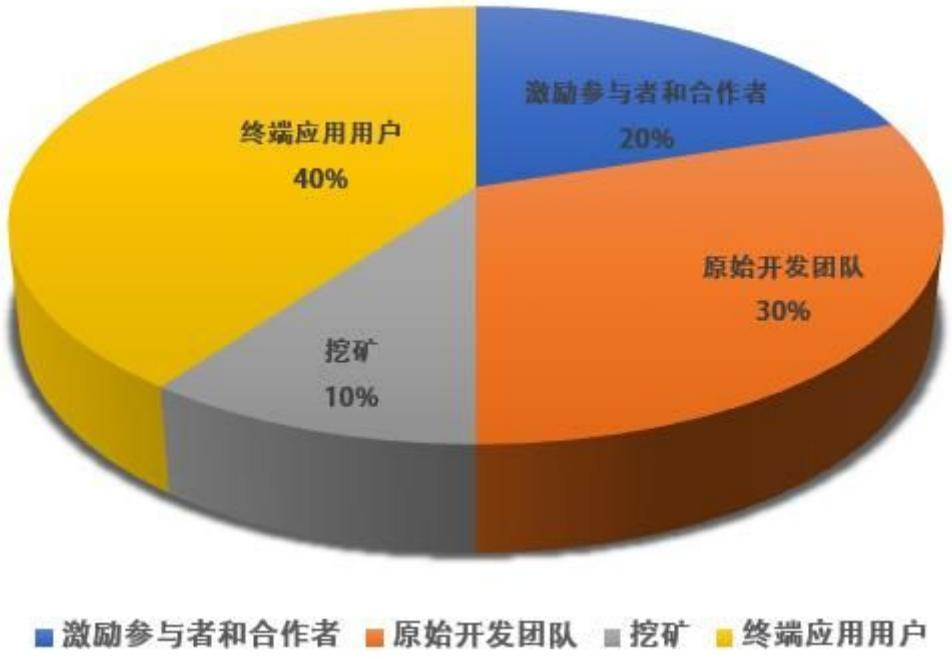
1.3 贝富币(BFcoin)的计量单位

贝富币(BFcoin)最小单位是Feng, 依次为 Jiang, Lei ：

1 Jiang = 10^{12} Feng
1 Lei = 10^{15} Feng
1 BFcoin = 10^{18} Feng

1.4 贝富币(BFcoin)的分配

为了更好满足大量贝富链（BFchain）终端应用用户的大量需要，并体现“币有所用”的理念，贝富币(BFcoin)总发行量为300亿，其中终端应用用户占40%，原始开发团队占30%，挖矿占10%，并预留20%给激励参与者和合作者。



2.贝富代币(BFtoken) 的设计

2.1贝富代币(BFtoken) ID的公共产生特性和加密唯一性

和比特币以及以太坊不同的是，贝富链(BFchain)分为贝富币(BFcoin)和贝富代币(BFtoken)。贝富代币(BFtoken)被设计为由公钥私钥共同产生的带ID的局限性区块链，只有那些获得根证书颁发机构签署的认证贝富代币(BFtoken) ID才获准进入该局限性区块链。这里的 “ID ”并不是指真实的法律合法身份 ，而是一个独一无二的, 具有全球唯一性的标识。它归根到底来自 DNS层次结构的顶， 所以PBF网络也可以使用任意自选的用户名，并且允许同名，因为用户名可以不是唯一的，唯一的仅仅是由公钥和私钥产生的ID的标识。 贝富代币(BFtoken)拥有者只要其签名身份与其私钥相符，即获许可接受服务并可随意操作。 一旦附加一个有效的 IP混淆系统，就能让贝富代币(BFtoken) 网络完全匿名。贝富代币(BFtoken)ID使用了公开密钥基础设施(PKI)及X.509(即通常被称为PKIX工作组)连接公钥用于贝富代币(BFtoken)ID识别。在X.509方案中, 默认的加密体制是公钥密码体制。为进行贝富代币(BFtoken)ID认证, X.509标准及公共密钥加密系统提供了数字签名方案。用户可由此生成一段信息及其摘要(亦称作信息"指纹")。用户用专用密钥对摘要进行加密后便形成签名。接收者用发送者的公共密钥对签名进行解密, 并将之与收到的信息"指纹"进行比较和确认。

2.2 贝富代币(BFtoken)与云著作权区块，正品防伪区块，云流媒体原创区块，GPS游戏区块和其他应用区块货币价值链的无缝吻接。

除了在上面1.1所介绍的去中心化分布式应用记账系统外，我们同时平行设计了另一 套局域系统内的分布式记账ID系统，更好地记录现实世界中的附属数据，以此来补强比特币和以太坊等对现实世界支持方面的不足与弱项，但对于比特币和以太坊等在去中心化分布式记账方式和保证历史记录不被篡改等方面的优点和功能，我们仍然保留和忠实执行。贝富代币(BFtoken)所使用的就是以此相应的一个ID系统。

贝富代币(BFtoken)作为贝富链(BFchain)的代币在系统内流通，对一些应用，例如云著作权区块发表文章的激励，一般用户对文章的打赏，文章发表的正品防伪记录等等应用情境，都可以通过代币和代币ID实现。并且，例如云著作权区块文章发表等系统也支持用比特币，以太币，BFcoin 等来激励、打赏，也可以对正品防伪进行记录。同时，所有比特币，以太币，BFcoin 等流通的过程和时间戳会永久记录在文章的分布式记录链上，以此可将云著作权和区块链完美地结合起来。这样，贝富代币(BFtoken)的使用在云流媒体原创区块，GPS游戏区块等货币价值链当中可实行无缝吻接。

3. 贝富币(BFcoin)和贝富代币(BFtoken)的兑换办法 (exchange rate)

贝富币(BFcoin)和贝富代币(BFtoken)之间的兑换采用递归函数 f() 实行，而且还将会包括可能实施的糖果计划和手续费的计量方法。

注释：y 为 年份, IR(y) 为 当年通胀率, INT 为 取整函数.

a) y < 2018, f(y) = 0 ;

b) y >=2018 && y <2022, f(y) = 100;

c) y >=2022, f(y) = (1+IR(y-1)) * f(y-1);

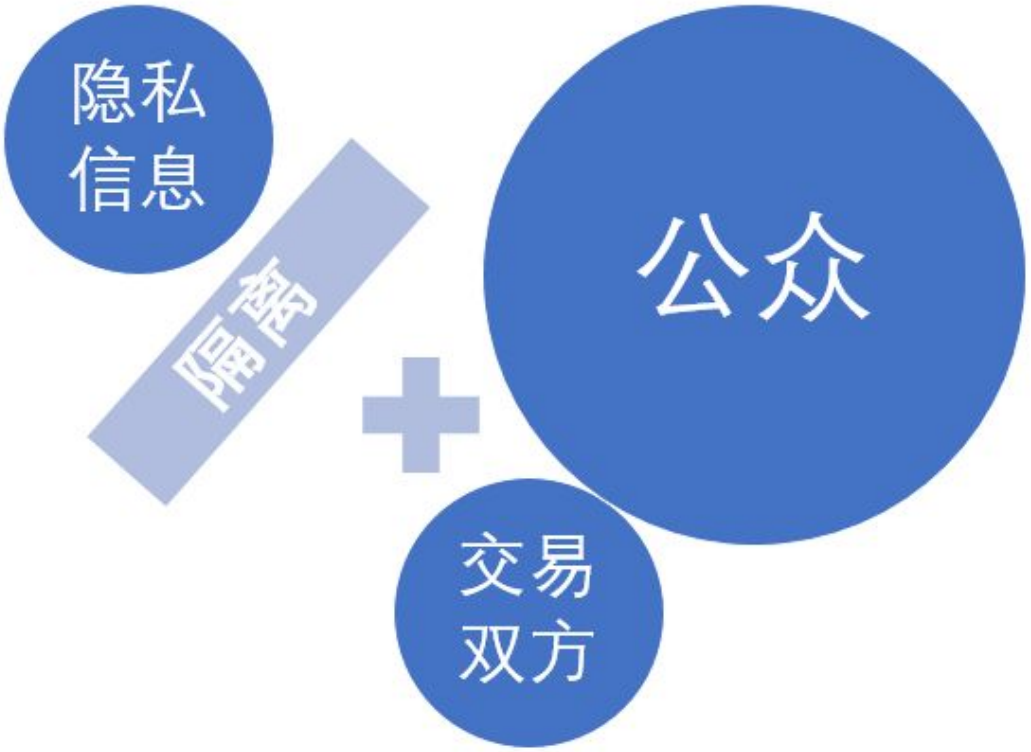
#BFtoken = INT (#BFcoin * f(y));

4 隐私性和安全性

隐私性和安全性是贝富链(BFchain）的最重要考虑因素。在大千世界中，货币是讲隐私的，所谓钱财不可外露。作为去中心化的数字货币的这种公开式分布设计，用什么方式和手段来保护隐私呢？

传统货币交易的隐私性在于，交易者的身份和其他交易方的身份可以是互相之间保密，也可以对公众保密。

而数字货币的隐私性特色是，交易者的身份本身是分离和隐秘的，但是交易对公众是公开的。



我们可使用“零知识证明”（zero-knowledge proof）来解决以上隐私和公开之间的矛盾。零知识证明指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断结果是正确的。Zero-Knowledge 令到“没有任何的信息被泄露”，反过来说，就是指证明过程必须在仅仅知道公开信息时，也可以高效地被模拟. 上图的这个等式用的数字无论经过加密与否，所有人都

能看到。如果它能够让等式成立，这就是零知识证明，即不需要经过其他底层数据的辅助，也不受任意中心化指导数据影响即可直接通过验证。

5. 贝富冷热安全钱包 (BFwallet)和贝富云算力硬件 (BlockNAS)

5.1 贝富冷热安全钱包 (BFwallet)

贝富链(BFchain)技术团队还研发了一种高度加密的安全数字货币钱包 --- 贝富冷热安全钱包(BFwallet)。贝富冷热安全钱包(BFwallet)可用于多种数字货币的安全使用和存贮, 同时具备智能运算加密和快速物理隔断网络功能。它能以快速物理加锁式的加密运算方式智能界面地接上网络，即时智能更新数据和进行数字货币交易。贝富冷热安全钱包(BFwallet)有完善的硬件技术方案和软件算法方案，已注册了全球技术专利，是目前世界上最安全的可控冷热交换的新一代数字货币钱包。

5.2 贝富云算力硬件 (BlockNAS)

BlockNAS(Block with Network Attached Storage)是一个去中心化的NAS(Network Attached Storage)，即是一个去中心化的专用数据存储服务器。它通过云端服务加区块节点的设计思想把NAS与P2P融合为一体。NAS由相对整合的P2P小区块里的多个节点构成，它把云端服务器上的节点整合到客户端区块中。NAS客户端与P2P层网络的对等节点之间相互共享内容资源，反之，客户节点端利用P2P网络为其它节点提供内容资源，同时也作为服务器为网络提供计算带宽等网络资源。NAS通过客户端的参与减轻了其所属云端服务器的负担。另一方面，NAS服务器作为P2P网络中的一个超级节点也可以为P2P网络提供更接近(逻辑/物理)的网络资源。NAS服务器节点可为P2P网络提供它所缺乏的所需资源。这种就近获取资源的方式保证了获取资源的速度，从而提高了整体系统的性能与速度。并且，通过区块链工作量证明对节点的管理，让加入的节点获得运算收益，才让交易变得更透明和更公平。区块链支付的融入让全球支付和全球节点变成可能，让全民参与变得更加容易，也让算力资源得到充分利用。

目前流通的“云算力”，只是矿机厂商/矿场把其拥有的算力以租赁的形式出租出来。而购买“云算力”的用户，(实质上他们不算是矿工了，而是某种商品的消费者)，通过购买的“云算力”获得一定比例的回报，而回报方式则是相应的

电子加密货币，比如比特币，以太币或者莱特币等。而BlockNAS基于贝富链(BFchain)设计的软硬件配合贝富币(BFCoin)的算力计算方式，可以做到云盘CPU挖矿，充分利用富余的网络资源，甚至可进行无人值守的线上挖矿。

6 应用情景

贝富链（BFchain）应用链可分为基础网络、中间协议以及应用服务三个层面。随着底层基础网络和中间协议层的进一步优化演变，叠加区块链部署方式存在交错联盟，知识版权多元化，游戏与GPS位移，多方智能协议等创新技术， 贝富链（BFchain）可应用于广泛的，多样化的，且具有拓展性的各种应用场景。

6.1 贝富版权防伪链的使用

6.1.1 基本原理

贝富代币(BFtoken)ID使用公开密钥基础设施(PKI)及X.509(即通常被称为PKIX工作组)连接公钥，用于贝富代币(BFtoken)ID识别。在X.509方案中, 默认的加密体制是公钥密码体制。为进行贝富代币(BFtoken)ID认证, X.509标准及公共密钥加密系统提供了数字签名方案。用户可由此签名方案生成一段信息及其摘要(亦称作信息"指纹"), 扩大到云著作版权的应用。换句话说，公钥记录在我们的区块链的Token ID的对应关系，用户的原创著作体现在公钥的唯一性上。以此对应的私钥，仅体现在作者加了签名的地址上。作为去中心化的体现，公钥方仅有对应关系，对私钥没有知情权。用户用专用密钥对摘要进行加密后便形成签名。接收者用发送者的公共密钥对签名进行解密, 并将之与收到的信息"指纹"进行比较和确认。同时， 可结合高防伪的电子水印底纹，进一步提升版权备案证书权威性和产品防伪追溯性。

6.1.2 云著作版权区块链实例 --- 原创链使用情景

文章原创作者可在贝富文章发表平台发表原创作品，经过贝富系统的智能原创验证后，会生成公钥和私钥地址，并由贝富系统记下公钥作为唯一标识，私钥由作者保管。经过贝富系统智能估价程序估价，公钥和私钥签名后，贝富系统对著作权进行快速登记和确权，固定享有著作权的权利证据。同时，系

统将作品代币化，最终贝富系统会奖励原创者相应数量的贝富代币(BFtoken)。其他用户也可以对文章进行打赏。文章发表等系统也 支持用比特币，以太币，BFcoin, BFtoken 等来激励，打赏，也对正品防伪进行记录。同时，所有比特币，以太币，BFcoin，BFtoken等流通的过程和时间戳会永久记录在文章的分布式记录链上，以此可将云著作权和区块链完美地结合起来。如果贝富文章发表平台发现作品非原创，贝富文章发表平台则有权根据有关当局的版权法和贝富文章发表平台内部规定对上传作品者进行内部处理，并保留相关法律权利。

6.1.3 贝富产品防伪链使用情景

区块链的去中心化的特性决定了区块链由众多节点共同维护数据的开放性和平等性。按照51%攻击的理论，经私钥公钥签名过后有时间戳的信息添加至贝富版权防伪链将会被永久记录，单个节点将无法实现对数据的修改。贝富版权防伪链的数据稳定性高，具有不可篡改性和不可抵赖性。正品供应商可在贝富平台进行登记，经过贝富系统的智能原创验证后，会生成公钥和私钥地址，并由贝富系统记下公钥私钥。公钥和私钥签名后，贝富系统对物品进行快速登记和确权，固定享有正品的权利证据。任何人都可以在公开的接口查询区块链的数据。因此贝富版权防伪链保持了系统信息的高度开放性和透明性。一旦发现伪品，贝富系统会立即通知客户和正品供应商进行相关法律维权行动。

6.2 云流媒体应用链的使用

以影视云流媒体为其中代表的云流媒体的自主权特性，可让创作者和用户都能够访问和分享他们喜欢的内容，将内容代币化，还可以促进创作者提高作品质量。在云流媒体区块链应用中，创作者创作了流媒体，即是原创视频，上传到贝富的云盘时，经过贝富系统的智能原创验证后，会生成公钥和私钥地址，在云流媒体应用链上注册，让系统和用户将内容代币化。支持用比特币，以太币，BFcoin，BFtoken等来激励，打赏，也对正品防伪进行记录。同时，所有比特币，以太币，BFcoin，BFtoken等流通的过程和时间戳会永久记录在云流媒体的分布式记录链上，以此可将云流媒体和区块链完美地结合起来。这种应用模式让出版商和内容创作者都不再需要开发昂贵的基础设施，并允许他们创新更多的独特商业模式。因此，用户最大程度地降低了交付视频流的成本，从而获益。这样，内容创作者和各级平台都有所受益。

6.3 贝富游戏应用链的使用

贝富团队正在研发全球性区块贝富链网络游戏 --- 加密旺旺狗游戏 (BFdog Game) 。本游戏结合贝富链元素(BFchain，BFcoin, BFtoken激励，智能合约)，游戏平台可接受多种货币(包括各国法币和其他数字货币)的充值，例如：全球网上信用卡充值和其他数码货币充值等。

6.4 贝富社区公益平台链的使用

贝富平台(BF)还可以提供智能租房合约，社区公益活动， 定向捐赠等智能应用。例如：它可以帮助留学生社交平台中进行旧课本，旧家具买卖。它还可让系统将物品代币化，合约智能化，平台用户有机会获奖励贝富代币 (BFtoken)等多种手段参与其他平台的应用。

7 技术团队的介绍

贝富平台(BF)由一个多行业精英完美混合配搭组成的团队领导。 贝富团队掌握IT和金融业内领先的技术，拥有近二十年从事分布式存储和即时通讯上的经验和雄厚实力。贝富团队在核心的区块链设计和智能分析技术上处于行业领先，研发冷热数码钱包等拥有国际专利先进的产品和核心技术。

总结

贝富平台(BF)是一个基于分布式加密数字货币的区块链，以数字代币奖励网络参与者。实现快速的交易确认、可靠的网络安全性，通过分布式货币混合增强私密性，减少价格波动和鼓励技术创新。此技术基础确立了智能合同、贝富代币、侧链和高级安全机制实现的可能性。贝富平台强大的货币技术与贝富创新团队的企业计划的这种组合带来了引人注 目的机会。企业家和开发人员可以利用社交网络来吸引客户和投资者，这是IT行业中创新的尝试方式。贝富团队欢迎有志者参与，并预留给后来加入参与并有特殊贡献的合作者特别的奖励方案。

参考文献

Patricia Tree https://github.com/ethereum/wiki/wiki/Patricia-Tree

Merkling in Ethereum
https://blog.ethereum.org/2015/11/15/merkling-in-ethereum

Ethereum Whitepaper https://github.com/ethereum/wiki/wiki/White-Paper

Merkle Patricia Tree (MPT)
http://blog.csdn.net/zslomo/article/details/53434883

Introduction to Smart Contracts
https://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html

Corda: A distributed ledger
https://docs.corda.net/_static/corda-technical-whitepaper.pdf