比特商用白皮书

Bit Business coin white paper

第一部分：摘要

比特币作为数字货币的杰出代表，将不可逆的交易实现以及去中心化的共识带给到了这个世界，其本身作为信用载体的集大成者，价格也已经突破 20000 美元，虽然不断有各种新的数字货币诞生，但是都不可动摇比特币的核心地位以及价值体系。

比特币是区块链的最杰出代表，在全球从 IT、精英人群开始蔓延，其本质是信用的延伸。

比特币作为一种货币的功能，在最初的价值极低。因此，人们没有采取必要的安全预防措施。虽然理论上这些比特币并没有消失，但实际上它们降低了比特币的循环供应。没有私钥，这些硬币被锁住，无法回收。

虽然这是通货紧缩，并推动了比特币的价格上涨，但这还不足以推动其进一步发展。比特币的高价格、高交易成本和低数量限制是比特币进一步发展的重要因素。

Bit Business coin 的使命是为丢失的比特币和不活跃的钱包找到一个目标，并通过联合信用和智能合约建立一个稳定的加密货币系统。

Bit Business coin 将利用比特币的压力测试机制，比如 PoW、blocktimes、supply cap 和发行模型，同时还会升级一些区域，以满足更大的社会需求。这些改进将会增加到 8Mb，增加了基于 UVM 的智能合约支持，增加了闪电网络支持，以及隔离见证实现。

商业愿景:

第二部分：运作模型

Bit Business coin 将离开比特币网络，并立即改进其在新网络中的协议。所有活跃的比特币地址将在 Bit Business coin 的链上获得相应的余额。非活动地址的余额将被收集并用于为社区服务。

30%的不活跃余额将被分配给其他有技术影响的社区，以进一步增加比特联储的影响力和领取数量。

70%的不活跃的余额将被保留作为抵押物，以发行稳定的货币，类似于金本位制。然而，不同于金本位制(黄金与美元价值之间的固定汇率)倾向于高估黄金，BBC 标准的设计目的是保持 BBC 储备的价值，而不是抵押债券的价值。这个比率的目标是在 3:1 左右，也就是说，对于每一个被保留的 BBC，我们只能发行恒值的代币，也就是稳定的代币，高达 BBC 的市值的 33.3%。如果 BBC 的市场价格增加，那么它就提供了更多的价值能力来发行更稳定的代币，但是没有必要发行新的稳定的代币;如果 BBC 的市场价格降低了，稳定代币的价值就会突破保留的 B

BC 的 33.3%，那么稳定代币就必须回购，直到 33.3%的安全线为止。这与美联储保持美元流动性的方式类似。

由 BBC 储备支持的稳定代币将用于全球贸易或大型项目，这将极大地提高 BBC 系统的使用和受欢迎程度。

BBC 将成为一个真正的全球联合信用储蓄联盟。基于 PoW 的新的智能合约功能也将为 BBC 供无限的可能性。

第三部分：技术方案

虽然比特币目前是最安全、最主要的加密货币，但它也有一些缺陷——主要是因为它是行业的先驱。

Bit Business coin 将利用比特币的压力测试机制，比如 PoW、blocktimes、supply cap 和发行模型，同时还会升级一些区域，以满足更大的社会需求。

UTXO 数据模型

在过去的 9 年里，用于比特币的 UTXO 数据模型已经被证明是创造稳定可靠的数字货币的一种非常可靠的手段。货币最重要的功能是交换介质，而 UTXO 模型做得非常好。通过分叉继承这一点至关重要。

SHA256 PoW 挖矿模型

Bit Business coin 保持着比特币的挖掘算法。虽然能源消耗是 PoW 的一个关注点，但它有着非常可靠的记录，并且已被证明是非常安全的。

总量与出块时间

Bit Business coin 是比特币的升级并延展实际场景的可扩展性，总量 36 亿，出块时间为 36 秒

隔离见证 / SegWit

隔离见证是一种数据结构改进，它将 TX_IN 和 TX_OUT 的数字签名置于交易之外。这解决了交易可扩展性的问题，并缓解了区块大小限制的问题。它能增强链上的可扩展性。

区块扩容

比特币目前最大的 TPS 是每秒 7 笔交易。这不能及时适应网络的需求，因此无法开始处理全球交易量的需求。

之前提到的隔离见证能够解决一部分区块限制的问题，但是非常有限。为了扩大全网的交易量上限，最直接的方式是增加区块的大小。这会给比特币带来一次硬分叉，而 Bit Business coin 借分叉比特币这一机会，恰好可以实施这一举措。

增加区块大小和扩展将增加存储和网络的需求，但是考虑到大多数节点并由矿池或挖矿公司运行，我们认为这不是一个很大的限制，8MB 是一个适当的值。

重放保护

因为 Bit Business coin 是比特币的一个分支，我们必须确保一个链上的交易不能在另一个链上重播。Bit Business coin 通过引入新的交易签名来实现重放保护。新的 SigHash 类型还将提高网络的整体安全性。

资产激活

在分叉之后，比特币网络上的所有活跃地址将在 BBC 网络上获得相等的余额。

非活动地址是自区块高度#494000(2017 年 11 月 11 日)以来没有活动的地址，因此在资产分配过程的第 1 阶段不会自动接收 BBCTC。

智能合约

Bit Business coin 的智能合约允许用户编写自定义的行为，并在区块链中使用它们，而不是必须做一些(手动的)预定义操作。通过使用智能合约，用户可以轻松地配置复杂交易逻辑，以及执行复杂的财务契约。与此同时，用户可以扩展功能、添加权限或添加动态控件，而无需修改或升级区块链。

智能合约允许用户将自定义的合约字节码注册到区块链中，并在 BBC 中调用交易。合约字节码是在一个图灵完备的用于区块链的合约字节码虚拟机中执行的。

开发人员可以使用具有友好语法的编程语言编写智能契约，然后将其编译成契约字节码并存储在区块链中。

Bit Business coin 的每个钱包都将区块链与契约交易同步，并调用虚拟机执行相关的协议字节码并验证。

合约交易类型

在交易的 ScriptPBBCKey 锁定脚本区可以增加合约相关的操作符，用来触发注册合约，调用合约，升级合约，注销合约的行为。带有这些操作符的交易，验证时会触发智能合约虚拟机执行相关的合约字节码。

注册合约的操作符会执行将合约字节码注册到链上成为新的智能合约，成功则分配一个新的智能合约地址。

调用合约的操作符会调用某个链上的智能合约，执行相应的字节码，并产生一定的执行结果，比如转账或者合约状态变更。

升级合约的操作符可以给区块链上未升级且未注销的合约分配一个唯一的名称，并且将合约标记为不可被注销。通过合约名称方便用户或者其他合约调用此智能合约。

注销合约的操作符可以将用户创建的区块链上未升级且未注销的合约标记为已注销。已注销的合约不会从区块链中消失，但是无法再调用，只能查询相关历史数据。

合约虚拟机

合约虚拟机使用图灵完备的虚拟机实现，合约虚拟机具有确定下，高性能，可扩展性等性质，可以和 BBC 进行交互，执行合约字节码并返回执行结果。

BBC 的合约虚拟机具有确定性的特点，一笔合约相关的交易上链后，任何时刻执行都有同样的结果，可以验证和复现。

合约虚拟机使用账户模型进行价值传输，使得开发者在编写智能合约时更容易使用，而 BBC 链的 UTXO 交易模型则通过账户抽象层传递。

开发人员可以使用各种高级编程语言进行智能合约开发，并编译和生成合约字节码，存储在 Bit Business coin 的区块链中。

经过多方权衡,Bit Business coin 决定采用基于 LUA 改进的 UVM 虚拟机,并且后续增加部分模拟 C#、Java 以及 EVM 等类型虚拟机的模拟语言，以取得最为广泛的技术社区支持和介入.UVM 在所有的虚拟机中会是最为高效的虚拟机之一，并且其底层语言经过了多年的社会实践与应用。

在安全性方面，UVM 将删除一些功能，如外部 IO。在稳定性方面，UVM 财务双重进程确保了异常进程退出以及持续执行的特性。

Gas 机制

智能合约的执行需要消耗 Gas，Gas 是执行智能合约的经济开销，BBC 中的 Gas 使用系统基础代币 BBC。通过 Gas 机制，增加了通过大量发送合约调用攻击区块链的代价，并且给区块链生态整体支付执行智能合约的酬劳。

不同的合约调用根据执行过程中合约字节码指令数量和指令类型的不同，需要消耗不同数量的 Gas 数量。

合约状态存储

每个智能合约有一个相互隔离的状态存储区，记录这个智能合约的状态数据。合约执行时可以修改或查询合约的状态存储区。合约调用执行时对状态存储区的修改只有执行成功后才能提交到区块链。当发生区块链的块的回退时，合约的状态存储需要根据状态存储的变化历史，逆向回退成过去的状态。

合约账本

每个合约有一个合约地址，合约地址可以拥有区块链资产。合约地址可以接收转账。合约执行时如果发生合约转账到其他地址的，出块时在合约调用交易后紧跟着执行时产生的从合约转账到其他地址的交易，称作结果交易。结果交易的 ScriptPBBCKey 锁定脚本区包含了从合约转账到其他地址的脚本。合约地址的资产

转出依靠合约执行和共识，不需要某个私钥对合约地址资产转出的行为进行签名。

闪电网络

在当前比特币网络中，比特币每 10 分钟会进行一次打包出块。但是目前网络中存在交易严重拥堵现象，用户发起的交易很难被快速打包出块，如果用户想要及时打包自己交易就需要支付较高的矿工手续费； 同理，因为比特币出块间隔也使得用户间无法进行快速转账，海量交易更是由于高昂矿工费以及网络拥堵而无法进行。因此引入闪电网络，闪电网络是一套去中心化体系，指在 BBC 主网以外架设一个通道，用户在这个通道上可以自由进行快速支付，海量交易，并且无需信任对方或者第三方。

直接交易

在当前的 BTC 网络中，用户发起的交易需要打包到链段，并向网络广播，以得到每个节点的确认。但是在闪电网络中，不需要认证过程，交易直接与对方进行。

微型交易

在 BTC 网络中，当用户进行转账时，转账金额需要高于最小值。在闪电网络中，没有这样的限制，用户可以自由地创建交易。

可伸缩性

在 BTC 网络中为了网络广播块交易，因为带宽原因，每块中携带交易数量是有限制，而在闪电网络中，则没有对交易数量限制，用户可以在某时间段内发送海量数据。

实现方式

参与交易的双方都需要创建一个 2 / 2 的多签名地址作为交易通道，并在通道中存入相关的金额。双方之间的交易实际上是对多重签名地址中的金额的共识。最后协商一致后，双方的交易结束，双方的最终金额将确定。双方之间的交易将不会被记录在链上。