


A faint, light gray world map is visible in the background, centered behind the text. The map shows the continents of Africa, Europe, Asia, and Australia.

全球金融链

BFC

白皮书

A light gray grid pattern is located at the bottom of the page, consisting of horizontal and vertical lines forming a series of squares.

目录

一 区块链与互联网金融.....	3
1.1 互联网金融的发展.....	3
1.2 区块链技术与互联网金融.....	4
二 BFC 的设计理念.....	5
2.1 互联网金融现存痛点.....	5
2.1.1 流程繁琐 交易效率低.....	5
2.1.2 缺乏安全保障.....	6
2.1.3 信息易泄露.....	6
2.1.4 信息不对称 信息真假难辨.....	6
2.1.5 针对个人用户征信难以调查.....	6
2.2 BFC 的优势.....	7
2.2.1 区块链和互联网金融的结合.....	7
2.2.2 更快的 TPS.....	7
2.2.3 使用多重签名技术建立交易通道，极速交易.....	8

2.3 BFC 的愿景.....	8
三 BFC 的构架与生态.....	9
3.1 BFC 的生态构架.....	9
四 BFC 的应用场景.....	10
4.1 全球支付.....	10
4.2 数字资产结算.....	11
4.3 激励体制.....	12
4.4 数字货币借贷.....	12
4.5 数字货币融资.....	13
五 BFC 技术构架.....	14
5.1 技术构架.....	14
5.2 协议层构架.....	15
5.2.1 全面兼容的开发语言.....	15
5.2.2 分布式算法.....	16
5.2.3 多重加密签名.....	18
5.3 tatts 共识算法.....	20
5.3.1 隆过滤器与可逆式布鲁姆查找表.....	20
5.3.2 tatts 共识算法.....	21

5.4 分布式人工智能 (DAI)	21
六 发售计划	22
6.1 BFC token 分配	22
6.2 贡献激励规则	23
6.3 BFC 基金会的 BFC 归权时间 表	23
6.4 BFC 团队所持 BFC 归权时	24
6.5 销售所得 ETH 的使用	25
七、团队介绍	26
八、免责声明&风险提示	29
九、补充说明	34

一 区块链与互联网金融

1.1 互联网金融的发展

互联网金融的发展用一句话便能概括：2013 年，理财端 P2P 崛起，3 年后，贷款端消金崛起，又花了 5 年时间，互联网金融完成了一个完整闭环。

而如今，曾经万亿市场的行业，完成了其使命，走出黄金发展期，又站在了一个新的起点。

互联网金融不是互联网和金融业的简单结合，而是在实现安全、移动等网络技术水平上，被用户熟悉接受后（尤其是对电子商务的接受），自然而然为适应新的需求而产生的新模式及新业务。是传统金融行业与互联网技术相结合的新兴领域。

在区块链问世之前，全球的金融撮合，金融交易都是通过中心化的方式来实现。但是随着互联网技术的发展，交易中心对数据的控制权越来越大，交易个体与交易中心在交易的平等性，信息的透明度，历史信息的可靠性等多个方面，越来越不平等。众多中小散户的利益被严重剥削，与此同时，各个中心化交易平台之间的数据垄断和数据封闭。也使得中心化的机构同样无法对众多参与者的信用情况，风险等级进行了解和分析。



互联网金融主流模式

1.2 区块链技术与互联网金融

近年来，区块链技术凭借其去中心化、公开、方便快捷、集体维护与监督及安全可靠的特征受到金融科技市场的高度关注。我们用区块链技术重新构架互联网金融的底层技术，区块链在互联网金融上的应用有如下优势：

- (1) 它是未来去中心化组织结构的基础架构；
- (2) 它是智能化系统，金融交换载体由数据变成了代码，互联网金融成为可编程的智能金融；
- (3) 它是一体化系统，身份识别、资产登记、交易交换、支付结算等都在区块链一个系统中一账打通；
- (4) 它是实时化、景化、7×24 小时、现实世界与虚拟世界、物理世界与数字世界无缝对接的金融体系。

二 BFC 的设计理念

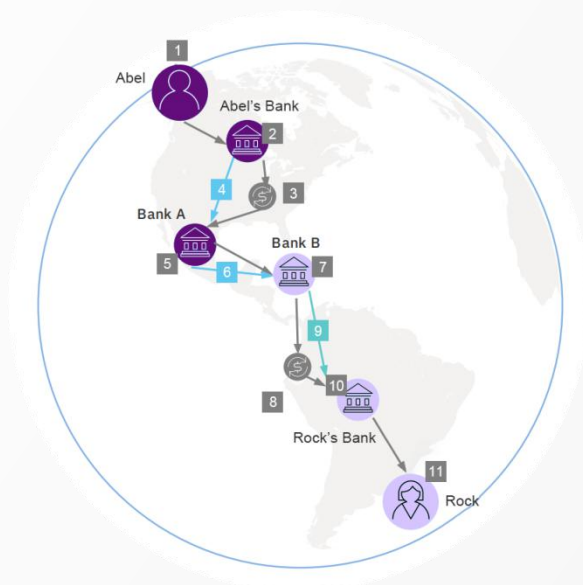
2.1 互联网金融现存痛点

2.1.1 流程繁琐 交易效率低

例如在跨境交易方面，汇款人的银行（或 MTO）会收集交易各方的必要信息，这是一项非常繁琐以及重复性非常强的工作。汇款人的汇款请求会通过地方清算网络，传送到代理银行那里，并由代理银行进行验证。此时，如果代理银行没有足够的流动资金去满足汇款人的汇款请求或者代理银行未能验证该笔交易，则汇款请求可能失败。

如果汇款请求通过验证，那么该请求会由另一个地方清算网络发送至收款人的银行或其当地的 MTO。在此，收款人的银行或者当地 MTO 会再次验证各方的身份及地址。最终，此次汇款所涉及的所有机构都需要留存其拥有的相关人员监管的文件。

如此繁琐的流程，不具备金融交易最重要的时效性，无形中加高了时间成本。



2.1.2 缺乏安全保障

互联网金融行业安全保障技术更新缓慢，开发团队更加注重交易更加快捷，成本更加低廉，而不是将信息安全、账户追踪等安全问题放在第一位，导致现在互联网安全体系单一，相比入侵手段安全保障体系严重滞后。许多算法的一个缺点是它们只支持使用单个密钥进行加密，安全性低。另一个问题是，在单个密匙帐户中，黑客可以使用密钥记录器获得密码，当您的账户为了获取权益处于解锁状态时， 损害用户的财产。

2.1.3 信息易泄露

大量的互联网金融 app 存在着漏洞，部分甚至存在严重漏洞。如果用户登录存在该漏洞网站或使用相关软件，用户的信息和提交的数据请求可能被篡改或泄漏。对于用户凭证明文发送漏洞，用户传输的账号、密文或者身份验证码未加密传输，通过拦截正常的网络通信数据，并进行数据篡改和嗅探，可直接获取，导致信息泄漏和账号密码被盗。

2.1.4 信息不对称 信息真假难辨

互联网金融链上各个参与者相互之间信息不对称（例如你无法辨别例如海外房产等真实性和发起众筹人的信用情况），导致无法在网络个体之间生成有效的信用价值，难以建立良好的信任关系，完整的信用体系便更难以搭建。虽然互联网中中存在大量中心化的信用中介和信息中介，但这减缓了整体模式的运营效率，并且使用中介提供的信息数据需要提供额外的成本。

2.1.5 针对个人用户征信难以调查

在近年的互联网金融大潮中，P2P 信贷，消费金融等诸多新兴领域都经历了一个从高高在上，到后来举步维艰的过程。面对这一有着巨大利润的零售金融业务，众多资金因为信用评价及风险管理的缺失而裹足不前。BFC 将通过区块链技术的智能合约及历史记录，与人工智能技术的深度学习及风险预测结合，突破零售金融业务对众多小型客户的风控难题，促进互联网金融业务的快速进化。

2.2 BFC 的优势

2.2.1 区块链和互联网金融的结合

区块链上能够及时、准确地获得数据信息，从而降低互联网金融服务的核保成本、提升效率。区块链的共享透明特点降低了信息不对称，还可降低逆向选择风险，使参与互联网金融服务的个体之间更容易产生信任；而其历史可追踪的特点，则有利于减少道德风险，进而降低互联网金融保险的管理难度和管理成本。

区块链去中心化、交易公开透明和不可篡改的特点，没有第三方支付机构加入，缩短了支付周期、降低费用、增加了交易透明度，为互联网金融区块链商业应用提供了技术理论支持。

2.2.2 更快的 TPS

BFC 采用 tatts 共识算法，目前，已经有公链宣布其 TPS 理论值最高可以达到 40 万+。据介绍，其采用了 tatts 共识算法，。它是一种可扩展的基于拜占庭的共识算法，这个算法经过数学逻辑验证，改进了 BFT 共识协议，可以使同时参与区块生产的节点达上万个，会使 TPS 随着带宽的增加而提高。因此，tatts 共识算法能够为互联网金融在区块链上的发展提供更加快速的效率和更加可靠的安全性。

2.2.3 使用多重签名技术建立交易通道，极速交易

下面例举 BFC 使用的多重签名技术流程。

1. 收集 A 与 B 各自的公钥生成两方支付的多重签名地址
2. A 构造发到合约地址的交易 TX1, 及从合约地址锁定时间发回交易 TX2 发给 B
3. A 发给 B 交易 TX2 的交易，获得签名后广播 TX1 形成闪电支付的通道
4. 闪电支付通道中交易的快速零手续费使用，及双向通道，交易极速完成

使用这种技术，能够极快的提高交易速度，删繁化简。

2.3 BFC 的愿景

BFC 搭建了一个超高速快捷，安全稳定并能够实现全球支付，数字资产交易、数字货币交易等的生态环境。BFC 目的是打造能够改善互联网金融现有问题的公链，为互联网金融的革新做出贡献，让区块链应用真正的落地到互联网金融中，深入生活。

三 BFC 的构架与生态

3.1 BFC 的生态构架

BFC 通过对平台全生态的各个环节进行梳理，将各参与者的资源和需求进一步细化，从而更好的刻画参与者之间的协作关系，促进整个生态的合作共赢，推动公有链的快速发展。

对开发者而言，也将不断丰富各种语言的 SDK 方便通过完善的 API 的设计和丰富的原生智能合约，简化开发者的准备工作，使开发者可以快速上手相应的开发工作。开发者移植到不同的平台，从而不断吸引更多互联网金融行业的 DAPP 开发者。

对使用者而言，BFC 将搭建一个具有简单易操作的交互界面并能够提供各类应用组件的 dapp。个人或公司不仅能够使用 dapp 中已经具备的功能，并且在无需了解区块链底层开发技术，甚至在没有部分区块链资源的情况下，利用 BFC 上找到所需要的区块链应用模块，结合个人或公司自己的数据资源，组建出适合个人及公司需求 dapp。

社区维护在激励体制保证活跃度与分布式人工智能系统保证信用度的前提下，随着后续大量开发者和使用者的涌入，大家共同搭建一个完善的区块链互联网金融新生态。

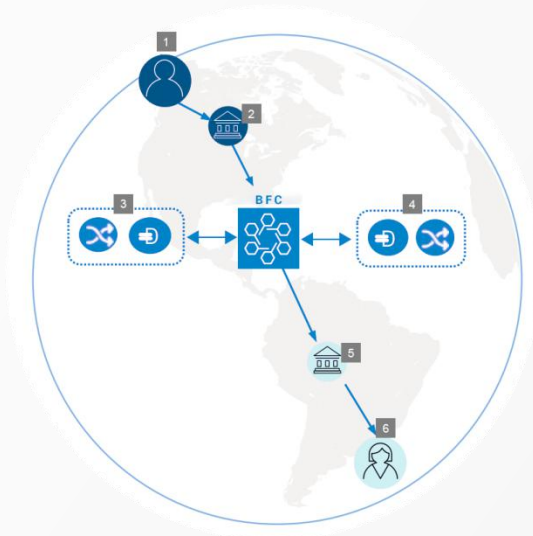
四 BFC 的应用场景

4.1 全球支付

全球支付（跨国转账）—— 通常是通过银行或转账机构（MTO）向他人汇出一定数量的金额。这种交易方式，通常被人们称为汇款，它是一种规模较大且不断发展的业务。例如，海外人士 2018 年的汇款总额预期将超过 16,010 亿美元。但是转账费用却很高。截止到 2018 年 2 季度，平均汇款费用达到汇款金额的 7.6%。

如果使用 BFC，汇款人的电子身份资料就足以供银行及 MTO 验证。一份包含汇款信息的智能合约可直接将款项发送至收款人的机构，同时通知相关监管部门。与此同时，分布式账本上的流动资金提供者负责货币兑换。一经完成，监管机构可直接从账本查看交易历史并进行审查。

因此，BFC 可以省去大部分人工或者繁琐流程，从而降低小额付款的手续费。



4.2 数字资产结算

数字资产清算业务是 BFC 生态里最为基础的应用,在 BFC 生态中所有的用户,包括金融机构、上下游企业、券商、信托、基金等,涉及到交易的行为都会经过 BFC 数字资产清算应用进行资产清算。BFC 用户首先需要自己对数字资产和数字货币进行数字资产登记,交易的买卖双方通过智能合约进行合约化交易以及资产的自动化结算。



4.3 激励体制

良好的激励机制有助于更有效地整合资源和人才，加速创新。在 BFC 生态体系中，通过对参与者的有效活动进行 Token 奖励的激励机制，更好的激发了参与者的主观能动性和积极性。

BFC 社区也会定期发布悬赏任务，加强社区活跃度，让大家共同维护建设 BFC 生态的去中心化和数据公开透明，来解决价值信任问题。BFC 生态体系构建了一个区块链金融环境和商业环境，彻底改变并颠覆改互联网金融行业的价值流动和分配模式。BFC token 被承认为 BFC 生态里的唯一支付方法。对于生态里的各个参与者的业务往来，通过智能合约的形式实现 BFC token 的流通，BFC token 不仅仅用于支付，还是我们社区维护奖励，BFC token 的高流通性是 BFC 生态里实现高活跃度的有力保证。

社区发布的悬赏任务也与我们的信用体制绑定，如果没有按时完成任务，不仅不能获得悬赏，这一信息也会被记录在链上。

4.4 数字货币借贷

P2P 借贷中 BFC 的优势主要体现在可以通过值得信任的安全网络实现各方的透明交互，从而将认证和审计操作分发到数据，简化现有流程，降低成本，并提高资本效率。

在 BFC 平台上借贷的用户都需要进行全面的 AML/KYC 认证和相关账户的银行会员登记。用户在系统的所有行为都会被记录下来，并通过分布式人工智能系统的综合分析来建立用户的信誉和声誉。

用户通过平台提交资产凭证等来申请第一笔资金。平台会对项目将进行 AML/KYC MOEDA 分析，并且会根据分布式人工智能系统的评级改变可用额度上限。

4.5 数字货币融资

开发者可以利用 BFC 提供的底层技术搭建融资 dapp，发起购置海外房产，海外股票，国外金融投资等，投资者可以使用 BFC token 进行认购，购置之后获得凭证，具体后续收益与参投项目相关。

通过 BFC 使互联网众筹资产标的更加多样化，不受国界和货币的限制。众筹的发起者必须提供相应的资产抵押，数字身份认证，和信用证明等相关材料。

五 BFC 技术构架

5.1 技术构架

BFC 基于区块链技术打造安全、可信的互联网金融新生态。BFC 底层提供了完整的分布式账本体系，完整的智能合约体系和系统安全体系等等。BFC 社区能够为同时为开发者，需求者，资源提供者提供 API、SDK 等应用组件。

BFC 是一种基于区块链技术开发用于改善互联网金融的公有链，允许开发者开发和分发基于 JavaScript 的区块链金融业务数字资产化 Dapp。BFC 使用了 tatts 共识算法多重签名来简化流程并保障安全性，兼容各种开发语言来降低开发者的门槛，使用分布式人工智能建立完整的征信体制保证信息的透明化。

BFC 提供了一个交互界面并访问全功能的生态系统。开发人员可以在允许使用 BFC 提供的智能合约，云存储和计算节点的加密货币驱动系统内构建，发布，分发 Dapp，让互联网金融区块链化。

5.2 协议层构架

5.2.1 全面兼容的开发语言

BFC 使用一种图灵完备并为区块链智能合约定制设计的字节码规范作为智能合约虚拟机的实现规范。提供静态类型的高级编程语言。比如 C#, Java, TypeScript 等的编译器实现从高级语言生成智能合约字节码。

BFC 也将不断丰富各种语言的 SDK 方便开发者移植到不同的平台，从而不断吸引更多互联网金融行业的 DAPP 开发者。

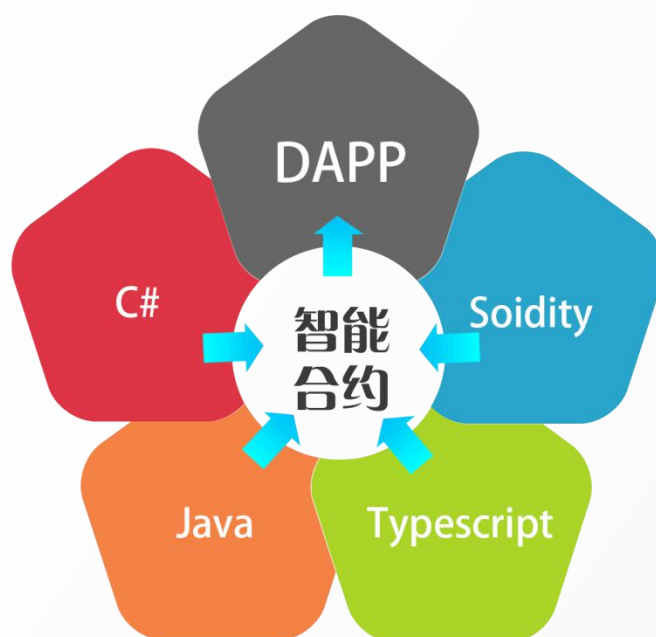
通过完善的 API 的设计和丰富的原生智能合约，简化开发者的准备工作，使开发者可以快速上手相应的开发工作。

BFC 提供一些常用数值操作，字符串操作等的基本库，以及一些链上查询，交易等的内置函数库，在智能合约中可以调用内置库。

智能合约部署到链上后，除了可以被用户直接调用或者存取资产，还可以调用其他智能合约/内置原生合约，或被其他智能合约调用。

面向不同行业的 DAPP 应用，拥有不同的技术需求和侧重点。例如去中心化的金融支付系统，去中心化的交易系统等，所需要的技术侧重点会有所不同。我们通过图灵完备 The New Standard of Value BFCX Foundation 2018 的智能合约，对行业 DAPP 深入探索后，慢慢会形成适用于该行业的 DAPP 标准，BFC 会不断将这些标准收录变为原生智能合约，方便开发者更加快速地迭代 DAPP。随着 DAPP 的产品化进程不断推进，我们希望普通互联网用户也可以真正进入区块链应用并感受到区块链技术带来的价值。

后续 BFC 将推出专属的带调试功能的 IDE，使得开发者既可以享受 IDE 带来的便捷，也可以在调试错误时更快地定位问题，从而大大提高 DAPP 的开发效率。



5.2.2 分布式算法

BFC 采用了下述分布式算法，分两个阶段运行：

阶段 1：准备发送提案请求

提议者：提议者选择提案编号 n ，并向大多数受让者发送准备请求。数字 n 存储在提议者的稳定存储器中，以便提议者可以确保下一个提议使用更高的数字（即使提议者进程重新启动）。

受体：如果一个接受者过去收到一个大于 n 的提议，那么它就忽略这个准备请求。

承诺人承诺不接受少于 n 的提案。

接受者回答提议者过去的提议，它以前接受的最高数小于 n ：reply (n' , v')。

如果提案人从大多数接受者那里收到了对其准备请求的请求回应，那么它可以发出一个

编号为 n 和值为 v 的提案，其中 v 是回答中编号最高的提案的价值或者由提议者如果答复的接受者没有提出建议。

阶段 2：接受：发送提案（然后在接受之后传播给学习者）

提议者：提议者现在可以发出提案。它会发送一个消息给一组接受者，声明它的提议应该被接受（一个 $\text{accept}(n, v)$ 消息）。如果提议者接收到它的响应制备（ n ）的从大多数接受器的请求时，它然后发送接受（ N, v ）的请求到每个这些受体的一个提案编号 \tilde{N} 具有值 v ，其中 v 是最高 - 在答复中提出了提案，如果答复没有提出任何提案，则是具有价值的。

受体：如果受体接收接受（ N, V ）为提案编号请求 \tilde{N} ，它接受，除非它已经回答了该提案准备请求具有大于一个数量 \tilde{N} 。

接受者收到提议者的两种请求：准备和接受请求。任何请求都可以被忽略。接受者只需要记住它接受过的最高编号的提案和它已经回复的最高编号的编制请求的编号。接受者必须将这些值存储在稳定的存储器中，以便在接收者失败并且必须重新启动的情况下可以保存它们。

5.2.3 多重加密签名

1. 收集 A 与 B 各自的公钥生成两笔支付的多重签名地址：

假设 A 是 1Bit 地址的持有者，B 是 1Dog 地址的持有者。公钥在交换公钥的位置后可以生成两个 2-of-2 的多重签名合成地址，即 3CSm 地址和 3Njd 地址。公钥是可以公开的信息，可以主动公开的。也可以在线快速地生成合成地址。

2. A 构造发到合约地址的交易 TX1, 及从合成地址锁定时间发回交易 TX2 发给 B

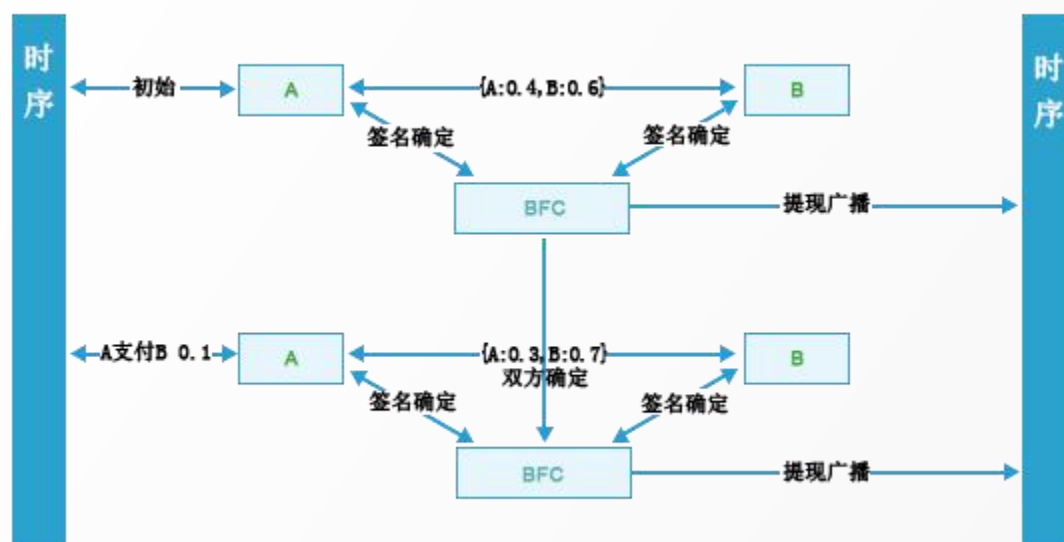
A 用 1Bit 地址的私钥，签名构造一个发向 3CSm 合成地址的交易，只要构造好后得到交易 ID 和位置 n 数据即可，可不先广播发布。然后再由 A 或者 B，最好还是由 A 来构造一个从 3CSm 地址全部币发回 1Bit 地址的交易 TX2，注意修改下 nLocktime 锁定时间为合理的时间，比如说锁定一年之后。nLocktime，也被称为 LockTime 或 lock_time，通常被设置为 0，表示交易可随时发送到区块链网络。如果 nLocktime 的值在 1 到 5 亿之间，则表示需要区块高度大于或等于 nLocktime 的区块时才可以写入区块链。如果 nLocktime 的值超过 5 亿，则表示从 1970 年 01 月 01 日开始算，加上 nLocktime 秒之后的一个时间点，即 Unix 时间戳，例如 2017 年 1 月 1 日是 1483200000，若早于那个时间点，则该交易不会被发送到区块链网络。另外注意 sequence 字段，不能为 INT32 最大值 (0xffffffff)，否则会忽略 nLocktime。

3. A 发给 B 交易 TX2 的交易，获得签名后广播 TX1 形成闪电支付的通道

把上面的交易 TX2 发给 B，请 B 来确认没问题后用私钥签名会发回。A 在收到来自 B 的签名后，然后用自己的私钥再签名下，看看是否成功。若成功，则可以将之前的交易 TX1 出去，从而形成类闪电支付通道。手里的 TX2 交易保存好，可能等锁定时间过后可能需要广播找回。其实在一定对 B 信任的基础下 A，可以 A 不用手动构造交

易 TX1 不广播,而是直接用币钱包软件发币到 3CSm 地址。然后让 B 来用交易 TX1 的信息来构造一个签名好的带锁定时间的全发回 1Bit 地址交易,并且 B 签名好后发给 A,让 A 妥善保存。一样可以形成类闪电支付通道,对 A 的技术要求会很低,但是需要 B 有足够的信用,而前面的方案是完全不需要 B 有任何信用的。

4. 闪电支付通道中交易的快速零手续费使用, 及双向通道



5.3 tats 共识算法

5.3.1 隆过滤器与可逆式布鲁姆查找表

用布隆过滤器 (bloom filter) 与可逆式布鲁姆查找表 (IBLT) 结合来压缩每次同步的数据。使用了布隆过滤器 (bloom filter) 以及可逆式布鲁姆查找表 (IBLT) 的新颖交互式组合，能减少同步区块的大小。

布隆过滤器的核心思想：用尽可能少的空间来存储尽可能多的内容，同时尽量保证准确率。布隆过滤器本质上很像哈希表，把一个大的空间映射到一个小的空间。

可逆式布鲁姆查找表的原理：首先，在一个区块中包含的所有交易，都会写入一个表 (table) 中，每一笔交易会始于表上每一个不同的点。然而，存在的交易数远多于表的空间 (room)，所以它会导致极为严重的重叠结果。这使得 IBLT 显得非常地密集，但对于那些无法访问任何交易数据的人而言，IBLT 是无法读取的，也是无法破译的。而那些拥有交易数据的人，可通过使用类似的逻辑，将他自己的交易填充到一个 IBLT，然后比较 IBLT 上的重叠交易数据。如果两个 IBLT 最终看起来完全一样，这意味着所有的交易，是完全匹配的。即使这两个 IBLT，最终看起来并不是完全相同，但只要交易集是非常相似的，这可能仍然是有用的。这种情况下，这两个 IBLT 可以进行比较，用这种方式，所有相同的交易就可以抵消掉一方。而 IBLT 中“剩余的”交易，往往可以用于重构丢失的交易。因此没必要在对等式网络上广播完整的区块，节点可以广播更小的 IBLT。这需要的数据也就更少了，速度也就更快了。

5.3.2 tatts 共识算法

增强 TPS 的另外方案在于共识算法，TPS 比较高的都是基于 BFT 开发的共识，本白皮书要提出的提升公链的 TPS 的方案为 tatts 共识算法，它是一种可扩展的基于拜占庭的共识算法，这个算法经过数学逻辑验证，改进了 BFT 共识协议，可以使同时参与区块生产的节点达上万个。在带宽为 2Mbps-30Mbps 条件下进行测试，主网速度大于 4000tps，高于 EOS 测试 1000tps，此共识算法由清华大学研究分布式系统关于区块链共识于 2018 年 2 月 5 日发表。

目前，已经有公链宣布其 TPS 理论值最高可以达到 40 万+。据介绍，其采用了 tatts 共识算法，会使 TPS 随着带宽的增加而提高。至于安全性，tatts 共识算法下，区块链每轮出块会根据随机算法选出多个潜在出块者，计算出块需要私钥，别人不知道私钥，无法进行攻击。当潜在出块者完成出块计算，区块就完成了网络上传，这时候攻击也无济于事。

5.4 分布式人工智能（DAI）

通过对全部使用者的公开信用数据，信用交易历史，日常行为统计（多项数据综合），通过分布式人工智能的深度学习，智能判断用户的欺诈概率，违约概率及信用等级，并基于分析结果进行信用评级才决定使用者对不同模块的操作权限。并通过 BFC 本身的区块链技术及数字货币完成智能合约跟踪并记录合约履行直至改善。

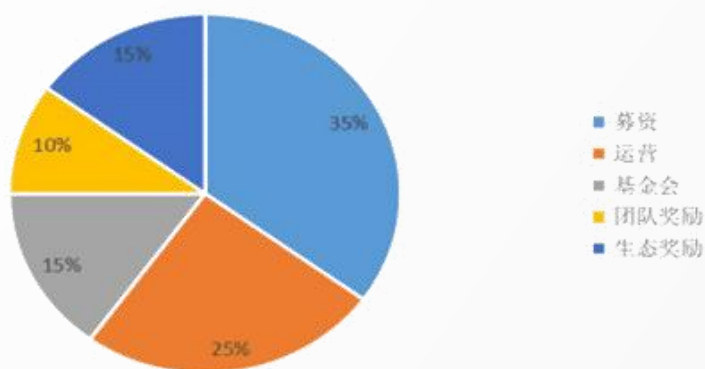
这样就能利用 DAI 建立了完整的信用体制，保证了个人信用信息的透明以及安全性。

六 发售计划

全球金融简称 BFC，是区块链经济体原生的、工具属性的价值度量、存储、激励工具。BFC 可用主链与子链之间，子链与子链之间价值转移、支付交易费、购买 BFC 商业资源、激励贡献等。总发行 63,000,000 枚，永不增发。

6.1 BFC token 分配

分配方案



用途	数量	占比
募集	22,050,000	35%
运营	15,750,000	25%
基金会	9,450,000	15%

团队（锁仓一年）	6,300,000	10%
生态奖励	9,450,000	15%

6.2 贡献激励规则

BFC 将发行量的 15%用来做贡献激励，根据参与各方贡献的数据制定激励，具体激励规则如下：

生态激励按照一定的规则分配给在 BFC 上进行贡献的相关机构和个人。

6.3 BFC 基金会的 BFC 归权时间表

考虑到技术开发、社区运营和平台推广的需要，设立 BFC 基金会（BFC Foundation），基金会所持的 BFC 暂不设置制约，由 BFC 基金会管理委员会设立规则，并纳入统一管理。

6.4 BFC 团队所持 BFC 归权时

截止至首次销售结束为止，被分配的 BFC 将构成可用流动供应量的全部。其中，分配给 BFC 团队的 BFC，将受到长期归权时间表的制约，具体解除制约规则如下：

A:20%，在 token 分发后 12 个月后解除制约；

B:25%，在 token 分发后 24 个月后解除制约；

C:25%，在 token 分发后 36 个月后解除制约；

D:30%，在 token 分发后 48 个月后解除制约；

至此，分配给 BFC 团队的 BFC 全部解除制约。

6.5 销售所得 ETH 的使用

本次通过销售代币所获得的 ETH 将用于以下几个方面：

团队建设：30%预算。这笔预算将用于加强技术团队，优化现有技术设计和研发新技术的支出。

计算能力采购：10%预算。这笔预算将用于采购公有云或分布式云提供的计算能力，以支援 BFC 生态初期的开发与发展。

运营管理：20%预算。这笔预算将用于 BFC 在相关的法律、安全、会计、人事等运营管理方面的一系列开支。

市场推广：

*30%预算。这笔预算将用于 BFC 的推广。

*包括：流量购买、交换，BFC 业务推广；

*与创业者社区、各大平台、各类投资人、众筹爱好者平台发展、维护一个全球的开发者社区。

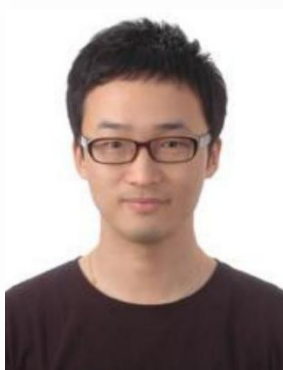
其他偶然性开支：10%预算。这笔预算将用于不可预见的偶然性开支。

七、团队介绍



Constantine Lycos

团队的核心领导者，技术风险分析师，乔治华盛顿大学的金融硕士学位，费雷拉先生拥有十五年的资产建设、金融咨询服务经验。



Changhee Jung

谷歌编译器团队核心之一，韩国 ETRI 电子和电信研究院）高级架构师，在硬件通讯和加密技术领域具备前沿开发能力。



刘文静

电气和计算机工程博士，美国国家科学基金会(NSF)项目主任，IEEE CNS (IEEE 通讯与安全)委员会核心，主研无线网络中的跨层安全和信息系统防御。

DR. Shamsae



殷拓集团（EQT PARTNERS）东南亚地区投资委员会经理，资本市场资深从业经验，擅长资本运作和项目运维。

Leah Stephens



殷拓集团（EQT PARTNERS）东南亚地区投资委员会经理，资本市场资深从业经验，擅长资本运作和项目运维。

Torres Zhang



英国肯特大学（UKC）数学系硕士研究生，从事金融数学方向研究，曾独立设计过若干二级市场交易策略模型。如“以太坊量化交易策略”、“Time Series Momentum 动量交易策略等



Christian Novak

法律总顾问，评估重大战略项目的法律可行性，出具可行性报告；全程参与过投资并购的法务决策；参与团队法律法规、规范性文件的起草、论证；参与合作项目的洽谈、信访案件、突发事件提供法律服务。

八、免责声明&风险提示

该文档只用于传达信息之用途，并不构成买卖数字资产的相关意见。任何类似的提议或建议将在一个可信任的条款下并在可应用的相关法律允许下进行，以上信息或分析不构成投资决策，或具体建议。

该文档不构成任何关于数字资产的投资建议，投资意向或教唆投资。

本文档不构成也不理解为提供任何买卖行为，或任何邀请买卖任何形式数字资产的行为，也不是任何形式上的合约或者承诺。BFC 不承担任何参与 BFC 项目造成的直接或间接的损失，包括但不限于：

1. 本文档提供所有信息的可靠性；
2. 由此产生的任何错误，疏忽或者不准确信息；
3. 或由此导致的任何行为；

此外，那些没有正确地使用其 BFC 的人，如丢失钱包私钥，有可能失去使用 BFC 的所有权利。BFC 不是一种所有权或控制权。拥有 BFC 并不代表对 BFC 去中心化平台相关人员的所有权，BFC 并不授予任何个人任何参与、控制或任何关于 BFC 去中心化平台决策的权利。

风险提示

数字资产投资作为一种新的投资模式，存在各种不同的风险，潜在投资者需谨慎评估投资风险及自身风险的承受能力。

私钥丢失风险导致的丢失 BFC 的风险

BFC 购买者的相关登录凭证，遗失这些凭证将导致 BFC 的遗失。最好的安全储存登录凭证的方式是购买者将凭证分开到一个或数个地方安全储存，且最好不要储存、暴露在危险的地方。

购买者的 BFC 在提取到自己的数字钱包地址后，操作地址内所包含内容的唯一方式就是购买者相关密钥(即私钥或是钱包密码)。用户个人负责保护相关密钥，用于签署证明资产所有权的流通。用户理解并接受，如果他的私钥文件或密码分别丢失或被盗，则获得与用户帐户（地址）或密码相关的 BFC 将不可恢复，并将永久丢失。

最好的安全储存登录凭证的方式是购买者将密钥分开到一个或数个地方安全储存，且最好不要储存在公用电脑。

购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制购买者的BFC，为了最小化该项风险，购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

代币销售市场风险

由于代币销售市场环境与整个数字资产市场形势密不可分，如市场行情整体低靡，或存在其他不可控因素的影响，则可能造成代币本身即使具备良好的前景，但价格依然长期处于被低估的状态。

监管风险

由于区块链的发展尚处早期，全球关于 BFC 过程中的前置要求、流通要求、信息披露要求、锁定要求等相关法律法规文件尚不十分完善。并且目前政策会如何实施尚不明朗，这些因素均可能对项目的投资与流动性产生不确定影响。而区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响，则 BFC 平台可能受到其影响，例如法令限制使用、销售代币，诸如 BFC 有可能受到限制、阻碍甚至直接终止 BFC 平台和 BFC 的发展。

竞争风险

随着信息技术和移动互联网的发展，以“比特币”为代表的数字资产逐渐兴起，各类去中心化的应用持续涌现，行业内竞争日趋激烈。但随着其他应用平台的层出不穷和不断扩张，社区将面临持续的运营压力和一定的市场竞争风险。

人员流失风险

BFC 平台集聚了一批在各自专业领域具有领先优势和丰富经验的技术团队和顾问专家，其中不乏长期从事区块链行业的专业人员以及有丰富互联网产品开发和运营经验的核心团队。核心团队的稳定和顾问资源对 BFC 平台保持业内核心竞争力具有重要意义。核心人员或顾问团队的流失，可能会影响平台的稳定运营或对未来发展带来一定的不利影响。

资金匮乏导致无法开发的风险

由于创始团队筹集的数字资产价格大幅度下跌或者开发时间超出预计等原因，都有可能造成团队开发资金匮乏，并由此可能会导致团队极度缺乏资金，从而无法实现原定开发目标的风险。

黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 BFC 平台功能的可能性，包括但不限于拒绝服务攻击、Sybil 攻击、游袭、恶意软件攻击或一致性攻击等。

未保险损失的风险

不像银行账户或其它金融机构的账户，存储在应用平台账户或相关区块链网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保。

核心协议相关的风险

应用平台目前阶段基于 ETH 公链开发，因此任何 ETH 公链发生的故障，不可预期的功能问题或遭受攻击都有可能导导致应用平台以难以预料的方式停止工作或功能缺失。

系统性风险

软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分风险依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害等。

漏洞风险或密码学加速发展的风险

密码学的加速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给 BFC 平台，这可能导致 BFC 的丢失。

应用缺少关注度的风险

应用平台存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对应用平台和 BFC 造成负面影响。

不被认可或缺乏使用者的风险

首先 BFC 不应该被当做一种投资，虽然 BFC 在一定的时间后可能会有一定的价值，但如果应用平台不被市场所认可从而缺乏使用者的话，这种价值可能非常小。有可能发生的是，由于任何可能的原因，包括但不限于商业关系或营销战略的失败，应用平台和所有的众筹所得支持的后续营销将不能取得成功。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对本项目而言是非常不利的。

应用存在的故障风险

应用平台可能因各方面可知或不可知的原因故障(如大规模节点宕机)，无法正常提供服务，严重时可能导致用户 BFC 的丢失。

应用或产品达不到自身或购买者的预期的风险

应用平台当前正处于迭代开发阶段，任何 BFC 自身或购买者对应用平台或 BFC 的功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，一个设计的改变等均有可能导致这种情况的发生。

其他风险

基于密码学的数字代币是一种全新且未经测试的技术，除了本白皮书内提及的风险外，此外还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其它风险也有可能突然出现，或者以多种已经提及的风险的组合的方式

九、补充说明

除本协议明确规定的情况外，本公司不会就本次 BFC 销售、BFC（BACC）作出任何声明或保证。每位参与方决定参加 BFC 销售并获得任何 BFC，应根据自己对 BFC 平台、BFC 以及本文中披露的信息进行。

无责任

本基金会议特此声明对下列情况不承担任何责任，对任何人不负任何责任：

1. 任何人参与 BFC 销售违反任何管辖区域的任何反洗钱、反恐融资或其他监管要求的；
2. 任何人违反本计划下的任何陈述、保证、义务、契约或其他规定参与活动，以及由此导致的失败，和无法检索其付款或索取相关购买的BFC；
3. 任何理由提前终止 BFC 销售；
4. 应用平台开发失败或退出，导致未能向购买者交付 BFC 销售认购的BFC；
5. 推迟或重新安排应用平台开发，导致未能达到任何预期的里程碑；
6. 应用平台源代码的任何错误、缺陷或其他错误；
7. 启动后的应用平台的任何故障、崩溃、回滚或硬分叉；
8. 应用平台或 BFC 未能达到任何特定目的或不适合任何特定用途；
9. BFC 销售收入的使用；

10. 未能及时全面披露有关开发 BFC 平台的任何信息；
11. 任何 BFC 销售参与方泄露、丢失或破坏他/她的 BFC 钱包的私钥；
12. BFC 被任何政府、准政府、权力机构或公共机构分类或视为某种货币、证券、商业票据、可转让票据、投资或其他可能被禁止、管制或受某些法律限制的条款；
13. 在任何加密资产兑换中列出或退出 BFC；
14. 任何人流通或推测 BFC；
15. 应用平台的任何应用程序、智能合同或其他程序；
16. 本计划中披露的任何风险因素，以及与该风险因素有关的任何损害，损失、索赔、责任、惩罚、成本或其他不利影响。

税款

每个 BFC 销售参与方应声明，承担和支付任何管辖区的法律和法规由于持有、使用、购买、收购 BFC（无论是在 BFC 销售期间购买或以其他方式获得）所应支付的税款，并且每个 BFC 销售参与方应对其不付款、少付款、不正当的付款或逾期支付任何适用税款的所有罚款、索赔、惩罚、责任或其他方式负全部责任。本公司对任何买方参与运动的税务意图不作任何建议，也不作任何陈述。

没有豁免

本公司未能要求或强制 BFC 销售参与方严格遵守的任何条款，或本公司未行使本协议的权利，不得解释为放弃本公司的权利或依赖任何此类条款或权利的权利。本公司对本计划的任何规定条件或要求的明示放弃，不构成对将来有义务遵守该规定的条件或规定的放弃。

可分割性

如果本计划的任何部分（无论是全部还是部分），根据任何管辖区的法律为非法或无效，不得影响该管辖区其他计划的合法性或有效性，也不影响在任何其他管辖区的计划的合法性或有效性。

标题

本计划中使用的标题仅供参考，在解释或解释本计划时不予考虑。

司法辖区

该 BFC 销售是在世界各地发起的，并且与任何特定的司法管辖区无关。买家可能来自世界任何管辖区。

解释权

BFC 基金会对本计划书保留最终解释权。