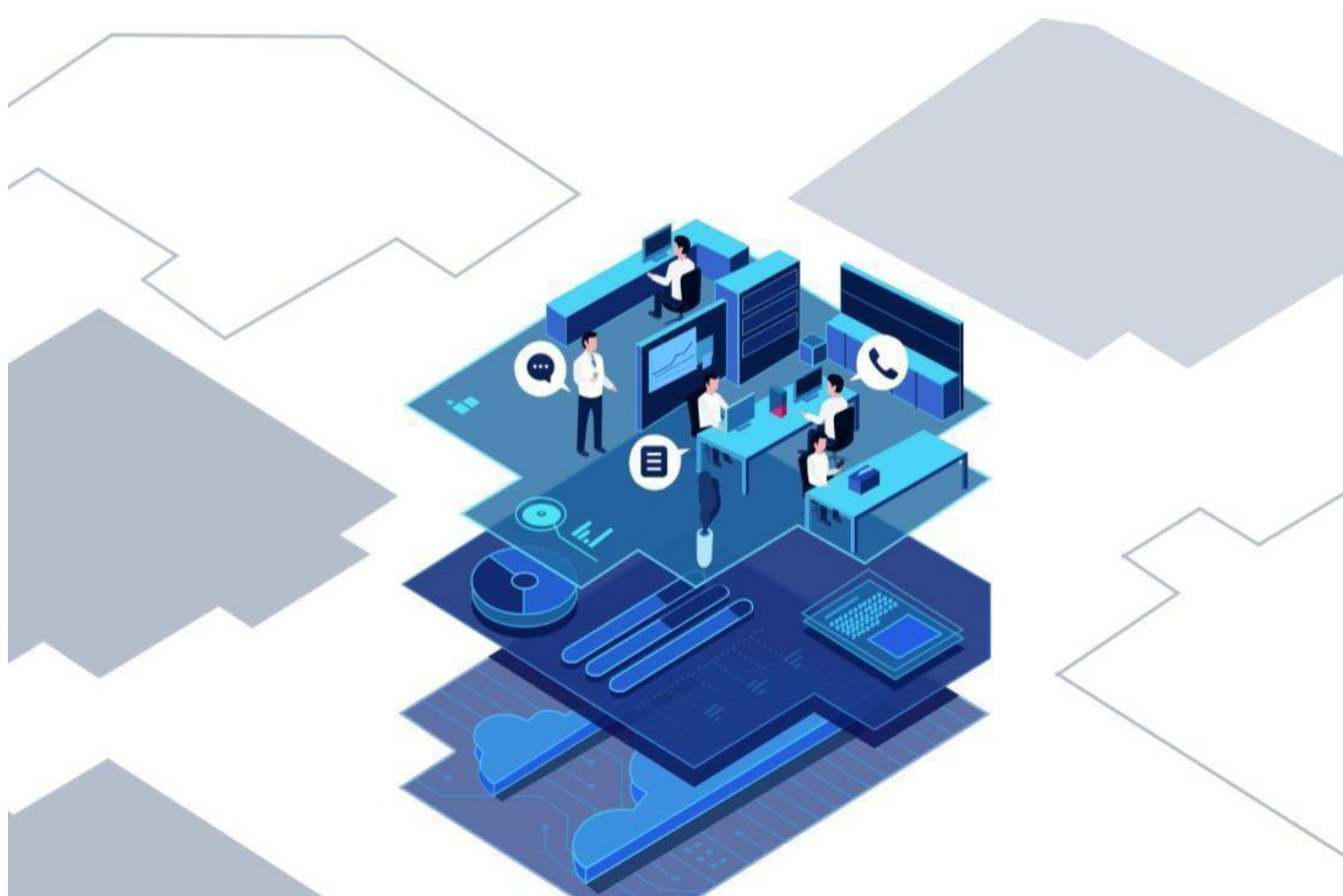


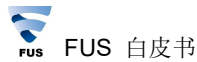
FUS 白皮书



FUS

下一代高性能侧链应用生态
FUS 智能交易所，人人都可以开交易所





1.0 区块链技术简介

区块链(Blockchain)是一系列现有成熟技术的有机组合，它对账本进行分布式的有效记录，并且提供完善的脚本以支持不同的业务逻辑。使用了分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。

区块链（Blockchain）是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术。区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一段时间里比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

1.1 区块链技术特征

多方记账，共同维护

多方是指记账的参与方，在比特币、以太坊网络里表现为挖矿的矿工。记账参与方应由利益不完全一致的实体组成。并且在不同的周期里，由不同的参与方主导记账，其他的参与方将对主导方的记账内容进行验证。

账本公开透明

区块链系统记录的账本会处于所有参与者被允许访问的状态，为了验证区块链记录的信息的真实有效，参与者需要可以访问账本信息及历史。但是账本的公开是指账本可访问性的公开，并不代表信息本身的公开，所以行业内出现了很多信息加密技术，如同态加密、零知识证明等，通过密文操作验证信息的真伪。

去中心化

为了实现账本的公开可信，区块链不会依赖于单一信任，在处理仅涉及链内封闭系统中的数据时，区块链本身能够创造参与者之间的信任。

不可篡改、可追溯

作为最显著的特征，不可篡改性是区块链系统的必要条件，一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中大部分算力，否则单个节点上对数据库的修改是无效的，然而因其去中心化的特征，成千上万的节点很难被同时修改，因此区块链的数据稳定性和可靠性极高。



根据特性可以看出区块链是一种数据记录技术，独特的记录方式使得陌生人之间做交易再也不需要中间担保人或者中间平台了，它把陌生人之间的信任成本降到了极低的水平，解决了市场经济中最核心的“信任”问题。

1.2 区块链技术与应用现状

未来已经来临，只是尚未颠覆。这话来描述区块链技术的发展再合适不过。

2017 年以来，区块链项目井喷状出现。截至 2017 年底，GitHub 上的项目数超过 8 万，另据 coinmarketcap 数据显示，目前已有 token 种类超过 1500 个，总市值超过 4000 亿美元。然而，因为区块链技术的特殊性，区块链技术产业落地正面临着除底层技术之外，还面临多方面挑战。

应用落地困难

目前区块链市场充斥着大量三无项目，无应用场景，无技术团队，无业务逻辑。虽然 ICO 被监管机构叫停，但泡沫却没有破裂迹象，市场一直呼吁区块链技术「脱虚就实」。市场普遍期望创业者能够将这一颠覆性技术落地。

通信“孤岛”

在区块链项目数量呈现加速上升态势的同时，后续没有相应的配套措施，导致现在大部分的区块链项目之间无法互联互通、项目与真正用户之间无法联通。区块链之间互通性极大程度的限制了区块链的应用空间，私链、联盟链更像是区块链世界里的孤岛，无法和外界实现价值交换。

使用体验差

区块链应用大多都是面向行业客户如投资者、开发者，而对普通用户是非友好方式。几乎所有的区块链应用都需要在用户的电脑上安装一个节点或者轻节点才能使用，学习使用的成本让很多人望而却步。例如，“以太猫”可能是目前对用户最为友好的去中心化区块链应用，但是对于很多消费者而言，他需要在浏览器安装一个 metamask 钱包后，创建账户并充值完成后才可以使用。这让更多的用户望而却步。

缺少的协作，杀手级应用难以产生

反观历史，我们认为有两大维度会影响到基础性技术及其商用案例的扩展和演进。第一个维度是新颖度，即技术应用相对于外界事物的新鲜程度。新颖度越高，开发人员就要花越多精力，确保用户了解到新技术能解决的问题。第二个维度是复杂性，或者说，技术应用要求的生态系统协调度——需结合新技术产出价值相关方的覆盖面足够广阔。举



例来说，只有一个成员的社交网络基本上毫无用处；只有足够多的联系人登录后，建立这个社交网络才有意义。其他用户也要参与进来，这样所有参与者才能获得价值。区块链技术因其新颖、复杂的特点，大量开发者、普通用户难以简便使用，大型的商用仍有困难。随着区块链新应用规模和影响力的扩大，其普及将需要重大机构性的改革。

高性能与去中心化需求无法兼顾

DPOS 方法照顾了高性能需求，其过于中心化的机制一直为人所诟病。例如 EOS 在投票比不达标而迟迟无法主网上线时，非常少数的人支付约 50 亿元占比 6% 的投票直接推动 EOS 上线，有钱说了算——这显然有悖于区块链精神的初衷。

目录

1 • 介绍

- 1.1 什么是 Financial Upper Story
- 1.2 技术背景
- 1.3 关键的创新因素
- 1.4 Financial Upper Story 组件

2 • 客户端

- 2.1 Financial Upper Story
- 2.2 Financial Upper Story 精简版本
- 2.3 Financial Upper Story 移动

3 • 共识

- 3.1 代表
- 3.2 网络费用
- 3.3 点对点

4 • 核心功能

- 4.1 用户名
- 4.2 联系人
- 4.3 多重签名

5 • 分散的应用程序



5.1 虚拟机

5.2 Dapps

5.3 Dapps 发展

5.4 Dapps 计算

5.5 Dapps 共识

5.6 Dapps 主节点

5.7 Dapps 存储

5.8 存取款

5.9 Dapps 令牌

6 • Fus(Financial Upper Story) 公链特点

6.1 高性能:

6.2 Chaincode:

6.3 开发者简单:

6.4 可定制化侧链:

6.5 高安全性:

7 • Fus(Financial Upper Story) 公链实现

7.1 侧链开发

7.2 区块链技术服务平台 (BAAS)

7.3 跨链技术

7.4 Fus(Financial Upper Story) 项目应用

8 • Financial Upper Story 项目特点:

8.1 链上链下结合

8.2 工作原理:

8.3 应用开发更加简单



8.4 Baas 平台

8.5 跨链技术实现高聚合

9 FUS 应用场景：

9.1 通证与智能合约

9.2 大开发者社区

9.3 游戏

9.4 数据存证/交易

9.5 物联网

9.6 分布式能源

9.7 医疗

9.8 其他场景

1 • 介绍

1.1 什么是 Financial Upper Story

Financial Upper Story 是一个下一代高性能侧链平台，它允许使用易于使用、功能齐全的生态系统开发和分发基于 JavaScript 的分散应用程序。通过 FUS，开发人员可以在使用定制区块链、智能契约、云存储和计算节点的定制构建的加密货币支持系统中构建、发布、分发和货币化他们的应用程序；全部来自于一个行业解决方案。FUS(Financial Upper Story)发行总量 5 亿，代币分配方案：FUS 基金会 1 亿，团队开发运营 1 亿，主网上线挖矿 1 亿以上部分锁仓 5 年，社区流通 2 亿

1.2 技术背景

FUS 是用 Node 编写的。后端是 js[1]，前端是 HTML5 和 CSS3。它异步工作，并允许快速处理所有功能，如网络事务。数据库使用 SQLite 来允许复杂查询的使用和运行。

1.3 关键的创新因素

FUS 是第一个完全使用 Node.js 编写的分散应用解决方案。这就向数千名不需要额外技能的



现有开发人员开放了 FUS 生态系统。任何熟悉 JavaScript 和 Node 的 web 开发人员。从第 1 天起, js 就可以立即介入并开始构建分散的应用程序。

我们与 FUS 的核心目标是创建一个完整的即插即用系统, 为企业和社会提供完备的区块链技术服务, 不限于通证发行、跨链价值流通、物联网、Baas 平台等。我们的目标是让各种区块链技术与应用的使用变得更简单、高效。允许开发人员从设计、开发、发布到货币化, 所有的工作都在一个平台内完成。通过利用 FUS 生态系统, 开发人员可以快速部署他们的 JavaScript 应用程序到 FUS 托管和存储节点, 在 FUS Dapp Store 中获得列表, 并立即访问 FUS 计算节点以执行代码。所有这些都得到了 FUS 侧链共识功能的完整性和安全性的支持。我们希望通过我们的技术让区块链的性能更好、区块链服务的使用更加便捷、区块链之间的价值可以实现互通, 利用 Fus 的侧链技术及其提供的一系列 SDK 和 API, 开发者可以使用 JavaScript 语言和关系型数据库构建、测试和发布自己的 DAPP。中小企业和全球开发者都能充分发挥协作、创新的优势, 打造出真正的杀手级应用。

同时, 我们将基于 Fus(Financial Upper Story)推进一系列应用场景的开发, 我们将搭建一个素材创作价值变现平台, 普通用户更简单的让自己的创作和知识在链上实现价值流通; 我们会围绕个人健康数据、个人隐私加密等应用场景进行开发验证。

最重要的是, 所有这些云功能都是由用户和 FUS 委托运行的, 这些委托通过内置的发票系统(或者是由网络本身支付), 并以 FUS (Financial Upper Story 自己的加密货币)或 ETH 支付。它确实是应用程序开发的一站式商店, 提供了一种前沿的、可负担的和前瞻性的解决方案。

1.4 Financial Upper Story 组件

分散的 P2P dapps 托管

为 dapps 分散的 P2P 存储

分散的计算

侧链共识为每个 dapp

FUS 和 Etherscan API 接口

开发工具:FUS / FUS Dapp SDK

2 • 客户

2.1 FUS

在 fus 平台、委托和开发人员的最佳解决方案。它适用于 Windows、Mac OS 和 IOS 。尽管



只有在 FUS APP 上才有可能成为委托。FUS 用户可以连接到完整的客户机来访问网络。

如果完全客户端所有者允许，它们还可以使用它们来进行 API 调用。所有完整的客户端用户通过对等连接彼此下载区块链。

Dapp 用户也可以使用 FUS 客户机访问他们安装的 Dapp。开发人员可以使用 dapps API 和 peer API。它们使使用 nw 快速轻松地创建 JavaScript dapps 成为可能。js2 或 Electron3。

2.2 Financial Upper Story 版本

普通用户将主要使用轻量级 FUS 平台来访问其 fus 帐户。

Fus 客户机可用于 Windows 和 Mac OS。它不需要安装过程，因为它使用了现代 web 技术。它不充当网络节点，因为它只连接到通过 http 连接联机的其他对等点。这带来了几个好处。

用户不再需要下载区块链，这意味着应用程序本身很小。它不通过网络广播密钥，所有数据都在您的设备上本地签署。可以让所有类型的事务都可用。

如果要运行委托节点，可以向 fus 平台注册委托帐户。但是，不可能从它运行委托，即创建新的块。为此，您需要完整的客户端。

Dapp 用户也可以使用 fus 平台访问他们安装的 Dapp。开发人员可以使用 dapps API 和 peer API。

它们使用 nw 快速轻松地创建 Javascript dapps 成为可能。js 电子[2]和[3]。

完整的客户机是超级用户、委托和开发人员的最佳解决方案。它适用于 Windows、Mac OS 和 ios。尽管只有在 ios 上即有可能成为委托。fus 平台用户可以连接到完整的客户机来访问网络。

如果完全客户端所有者允许，它们还可以使用它们来进行 API 调用。所有完整的客户端用户通过对等连接彼此下载区块链。

2.3 Fus Mobile

移动客户端允许用户在旅途中访问其 fus 帐户。它适用于 iOS 和 Android，并且可以在 Apple 和 Google Play 应用商店中使用。



移动客户端的后端基础架构将与我们的桌面解决方案相同。真正的变化是对用户界面进行添加和调整，以便在移动设备上实现定制体验。该应用程序已定制设计，以提供熟悉和易于使用的移动界面，就像您每天使用的比特币或银行应用程序。它还允许您从应用程序本身启动所有您喜欢的 **dapps**。将来，我们计划整合特定于设备的功能，例如利用指纹或视网膜扫描功能，以增强您帐户的安全性。

3 • 共识

fus 基于 DPoS [4]（委托证明）共识机制。这种达成共识的方法最初是由 FUS 基金会创建的。

DPoS 基于代表创建块。代表是被信任的帐户，被选为“活动代表”。投票最多的 101 个代表帐户创建了块。其他代表被列为“待命代表”，并可以通过接收其他 **fus** 所有者的投票进入前 101 名单。**Fus** 的所有用户都有 101 票可以选出他们最喜爱的代表进入前 101 名单。101 票中的每一票的权重与用户在投票中投票的钱包中的 **FUS** 量成比例。该总金额在代表名单上显示为“批准”，并列为为该代表投票的 1 亿可用 **FUS** 的百分比。

委托升级到前 101 或降级到备用列表发生在 101 块生成周期完成。101 个块的每个循环由前 101 个代表以随机顺序创建。阻止时间是 10 秒。新创建的块将广播到网络并添加到区块链中。在 6 到 10 次确认之后，可以认为块和其交易已确认。完整的 101 块生成周期大约需要 16 分钟。

在 DPoS 中，可以发生分叉，但最长的分叉胜出。代表必须始终在线，并有足够的正常运行时间。正常运行时间用于通过每次错过分配给它的块来记录节点的可靠性。用户根据几个因素投票给前 101 位代表，正常运行时间是用于确定的一个关键因素。如果代表的评级低于某个评级，则由于性能不佳，用户可能会删除相关代表的投票。

3.1 代表

代表们的职能在“共识”一节中有所涉及。

要成为代理，用户需要注册代理帐户。这是通过 **full** 或 **FUS** 钱包中的客户端用户界面完成的。请记住，只有在完整的钱包中才能生成块。这意味着您可以在钱包的任一版本中注册委托，但只能从完整版本的客户端执行委托功能。代表注册后，帐号和用户名将相同。所有 **FUS** 帐户都有资格成为代表。

新代表作为备用代理启动。待命代表以 0% 的支持率开始，并且需要从 **FUS** 社区获得投票，以便成为 101 名代表之一。块生成仅由前 101 名代表执行。如果您处于待机状态，则不会伪造任何块。

3.2 网络费用

必须处理网络中的所有有效事务。委托处理事务并将它们存储在新块中。对于这项工作，代表们收取费用。网络中的所有交易必须包含某种类型的费用作为垃圾邮件对策。

发送 **FUS** 交易的默认网络费用为 0.1**FUS**。例如，100 **FUS** 交易包括 0.1 **FUS** 的额外费用，总



交易成本为 100.1 FUS。

以下是不同类型交易的费用清单：

为支出交易发送的 0.1 FUS 金额

5FUS 用于注册第二个密码短语

100 FUS 用于注册用户名

100 FUS 用于注册为代表

1 FUS 添加联系人

500 FUS 注册 dapp

每个成员 5 个 FUS 用于注册多重签名组。

代表们从最后一个街区周期的所有交易中收取费用（101 个街区）。费用在所有在该周期中创建块的代表之间平均分配。错过创建在该周期内分配给他们的区块的代表不会获得支付。

3.点对点

我们使用标准的 P2P 网络[5]，它在 http 协议之上工作，并使用 json 格式的数据作为数据交换的方法。P2P 模块捕获有关每个对等方的以下信息：

版 OS IP 港口

4.核心功能

4.1 用户名

FUS 允许用户注册用户名。哪个充当您帐户的别名。其他用户可以将交易发送到此用户名，然后链接的帐户将收到该用户名。这消除了记住长帐户地址的需要。

用户名注册的网络费用为 100 FUS。用户名可能包含以下字符：

传统字母（大写和小写）：A-Z，a-z

数字：0-9

特殊字符：！，@，\$，&，和。

每个用户名都是唯一的长度目前限制为 16 个字符。目前，您无法从帐户中删除用户名。

4.2 联系人

FUS 允许用户维护联系人或朋友列表。此功能可用于存储常用帐户，但也可用作信誉系统。如果某个帐户有多个已确认的联系人，则可能会被认为比没有确认的联系人更有信誉。

联系人在 Twitter 上像关注者一样工作。用户被添加到联系人列表中，然后在用户的钱包中显示为待处理的联系人请求。无论其他用户是否接受请求，它们都将显示在联系人列表中。一旦其他用户接受了请求，请求者也将被添加到他的联系人列表中。双方现在都有新确认的联系方式。

添加新联系人或接受传入请求的网络费用为 1 FUS.

4.3 多重签名



FUS 允许用户创建多签名组。多签名组由多个 FUS 用户组成，称为组成员。可以将来自多签名组的事务配置为需要部分或全部签署者进行批准。

为此，实现了 M 个 N 多重签名架构。添加多签名组 (N) 的所有成员，最多 16 个签名者，然后指定批准事务所需的签名所需数量 (M)。

M 必须大于 1 且小于或等于 N 。 N 是多签名组的成员数。

从多签名组启动事务后，所有成员都将看到此待处理事务并决定是批准还是忽略它。一旦收集了所需数量的确认，该组将允许该交易并将其提交给区块链。

多签名组的所有者可以在至少 M 个签署者的批准下随时更改该组的规则。

5. 分散的应用程序

5.1 虚拟机

FUS Dapps 使用 FUS Node 执行，FUS Node 是 NodeJS 的专用版本，提供沙箱运行时环境，可在其中运行单个 dapp。使用命名管道实现进程间通信，对消息大小没有强制限制。

启动新的 Dapp 后，FUS 客户端将 FUS Node 的新实例作为子进程启动。如果 Dapp 遇到致命错误，则会正常杀死子进程，使父 FUS 客户端不受影响。

请注意，目前无法防止正在运行的 dapp 进行未经授权的系统调用。因此，不建议运行不受信任的代码，并可能导致资金损失。正在进行工作以提供一个完全沙盒化的环境，在该环境中运行不受信任的代码。

5.2 DAPPs

dapp 是一个用 Node.js 和 JavaScript 编写的分散应用程序[8]。它可以使用 Lisk 或很快使用比特币一致性算法与 Lisk VM 一起使用。FUS VM 是一个可扩展的 Node.js 应用程序，允许 Node.js 和 JavaScript 开发人员编写 dapps。利用当前的 Web 技术 (HTML5 / CSS3 / JavaScript)，开发人员可以创建功能强大的 UI。Dapps 可以使用 NPM (Node.js 包管理器) 中的自定义 Node.js 包。

普通用户可以在 Linux FUS 客户端上或通过 Windows 或 Mac OS 上的 FUS 客户端启动 dapp。

5.3 dapps 发展

开发人员用 JavaScript 编写 dapps，允许使用由 NPM 驱动 Node.js 软件包的完整生态系统。FUS VM 与 FUS API 集成在一起。此 API 与 FUS Blockchain 连接，甚至与比特币区块链连接。每个 dapp 都在 FUS VM 中运行，它会删除许多可能的攻击媒介，从而使最终用户在本地计算机上启动 dapps 更加安全。dapp 可以访问 FUS API。

为了使 dapp 开发尽可能简单，FUS 团队发布了 FUS-cli，这是一个命令行界面，通过回答一些简单的问题来创建自己的 testnet 和 dapp 环境。此外，我们还准备了一个 Dapp Toolkit，它为开发人员提供了最重要的 dapp 功能的参考实现，并作为他们开始构建分散应用程序的



坚实基础。

编写了许多库，以便“开箱即用”为开发人员提供完整的 FUS API 功能。

此 API 包括：

共识 API

FUS API

以太坊 API

数据库 API

要打开 dapp，使用以下格式：`http://ip:port/dapps/<dapp_id/username>`。

5.4 Dapps 计算

Fus 团队正在开发一个允许计算 CPU 时间的系统。fusVM 使用其 API 来跟踪用于运行 dapp 的 CPU 时间的位置。因此，节点的所有者可以运行 dapp 主节点以换取 fus 或 eth 付款。

fus 的目的是创建一个独特的生态系统，其中计算是其中的一部分。将来，fus 将有一个提交管理器向候选节点提交 dapps，提供运行 dapps 的服务，并选择满足指定资源要求的节点，提供最佳的价格和性能组合。节点所有者将通过提供计算，内存，存储和其他资源来获得收入。

这被称为 Dapps Billing。您可以将它与 Heroku 平台进行比较，以便部署应用程序。

5.5dapps 共识

共识机制即可编程的利益转移规则。区块链产品都是去中心化的，去中心化的基础就是 P2P 节点众多，那么如何吸引用户加入网络成为节点呢？又有哪些激励机制呢？同时，开发的重点是让多个节点维护一个数据库，那么如何决定写入哪个节点？何时写入？一旦写入，又如何保证不被其他的节点更改（不可逆）呢？回答这些问题的答案就是共识机制，它是区块链的灵魂核心。

5.5.1 共识机制类型

目前较主流的共识机制有 POW、POS、DPOS 等。它们各有优势，同时各有劣势。POW（Proof of Work）零和博弈共识算法，采用竞争性哈希计算来确定记账节点，导致了整个生态每次出块时都有大量电能被消耗，挖矿成本高，而且速度受限。如果把公链参与者作为整体来看，随着参与挖矿的节点增加，每个节点获得记账权的概率将会减小，那么 PoW 协议下维护网络安全的成本将会持续升高，很有可能会出现收益小于成本的情况。同时大型矿池的发展，也让 POW 越来越趋于中心化。POS（Proof of Stake）股权证明共识算法，按照币龄或者代币抵押数额来分配获得记账权的概率，POS 能耗较少，但 POS 下资本占优的节点容易占据生态的话语权，形成垄断，可能会对生态的参与者的利益造成损害，不利于公链生态的价值沉淀。DPOS（Delegated Proof of Stake）委托权益证明，有着能耗低、性能高的特点，但其依赖于社区持有人投票，这个模式一直被证实为投票积极性非常低而导致共识失效，同时因其节点而导致趋于中心化。



5.5.2 POF (Proof of Fusion)

POF 是 Fus(Financial Upper Story)团队推出的共识机制，不同于传统的 POW、POS 和 DPOS，POF 有助于增加参与节点的数量，同时保证性能，我们选择基于可验证随机函数 (VRF)、拜占庭容错机制 (BFT) 设计了 Fus(Financial Upper Story)的共识机制。

Fus(Financial Upper Story)公有链选择的 VRF+BFT+POS 的共识机制在交易打包速度上将会大大提升，相较于 POS、DPOS 共识算法 FusChain 的共识将更加去中心化。

POF 可归于 VRF (可验证随机函数算法) 类共识。VRF 算法作为一种基于密码学的新型共识模型被提出，最大的优势是快速共识、抗攻击能力、极低算力需求 (较高的经济性)。

为了使参与节点都能更民主化获得权益，POF 使用了一种称为“加密抽签”的方法来选择参与者来创建和验证区块 (若是在一个拥有百万级用户的系统中，参与者的数量也许可以达到数千)。

任何人可以通过自己的计算机进行抽签，从而靠自己的运气来决定能否成为一名幸运的参与者。这种抽签的方法基于前一个区块，选择过程是自动的 (不涉及到信息交换) 并且完全随机。通过使用密码抽签，理论上 POF 可扩展需求，同时还能安全性和速度带来好处。这种方式对计算的要求几乎微不足道，任何人都能在自己的笔记本后台运行这种系统。相比比特币存在用户分级 (进行交易的消费者和搜索区块的矿工)，POF 并没有这样的区别。

Fus(Financial Upper Story)团队认同 POW 上所有人都拥有相同网络访问权限，但同时也希望将服务器算力用于做有价值的事。Fus(Financial Upper Story)团队将基于以上原则去研发适合 Fus(Financial Upper Story)的共识机制和激励策略等来实现 Fus(Financial Upper Story)公链的不可破坏、不可操纵和不可预测性。

5.5.3 可插拔共识机制

Fus(Financial Upper Story)团队认为每一种共识机制各有优缺点，我们将实现共识机制可插拔，这让用户根据自己的需求选择最适合的共识方案。

每个 Dapp 都有自己独特的私有侧链，与 fus 块时间和当前块高度同步运行。

Dapp 侧链由一组最多 101 个主节点管理，每个主节点都具有专门为单个 dapp 启用的块生成。每个主节点的主要作用是处理事务并表示在侧链上生成的每个块的有效性。

主节点对给定 dapp 的块签名受 dapp 所有者的限制。然后谁批准个别 fus 帐户作为主节点，然后允许在 Dapp 的侧链上伪造。



使用用于保护 fus 区块链的相同委托证明 (DPOS) 方法, 在 101 个主节点之间保持侧链共识。这允许各个主节点从每次交易中收取费用作为保护 dapp 侧链的奖励。

这种形式的共识背后的动机是防止不必要地扩大 fus 区块链并保留单独的侧链自主权, 同时确保每个侧链的完整性得到不断维护。

应该注意的是, 在不久的将来, fus dapps 可以使用相同的方法通过比特币区块链进行保护。

5.6 Dapps 主节点

Dapp 主节点是 fus 节点, 其中安装了 dapp 并且专门为该 dapp 启用了块生成。Dapp 所有者需要批准允许单个 fus 帐户成为主节点。节点处理事务并生成新块, 然后由 Financial Upper Story 保护, 使它们成为 dapp 系统的核心。

5.7 Dapps 存储

可以在各种存储网络上托管 dapps, 集中式和分散式。但是, 使用过的存储网络必须为您提供 ZIP 包的下载链接。这是必要的, 因为您必须在 dapp 注册过程中提供下载链接, 以便一旦消费者/用户想要安装您的 dapp, fus 就知道从哪里下载并解压缩它。

在稍后阶段, IPFS [10] 将作为分散存储选项本地集成到 fus 中。

5.8 Dapps 存款/取款

开发人员可以在他们的 dapps 中使用 FUS 或 ETH。dapp 的用户可以从任何给定的 dapp 存入或取出资金。当 FUS 或 ETH 发送到 dapp 地址时, 资金将显示在 dapp 帐户中。然后资金将在 dapp 内使用。这与 ETH 存款的工作方式与 FUS 相同。ETH 被发送到特殊的 dapp 地址, 然后出现在 dapp 以太坊钱包中。

Dapp 帐户是由 dapp 的所有者创建的特殊帐户类型。所有存放的 fu's 或 eth 将存储在相关地址中。出于安全原因, 建议仅使用具有可信签署者的多签名 dapp 帐户。

dapps 的提取由主节点处理。当发送提款请求时, dapp 主节点处理它并将资金移动到 fus 或以太坊区块链中的指定提款地址。

5.9 Dapps Tokens

开发人员可以在他们的 dapps 中实现自定义令牌, 并使用这些令牌作为其 dapps 中的主要货币。这些令牌可以与 fus 或 eth 相同的方式使用, 但令牌不能直接从一个 dapp 侧链移动到另一个 dapp 侧链。它们只能通过 fus 主链移动。

6 • Fus(Financial Upper Story)公链特点

6.1 高性能:



Fus(Financial Upper Story)相较于大多数公有链在交易性能上有非常大的提升，比特币、以太坊网络每秒能处理的交易数量在 7-20 笔，**Fus(Financial Upper Story)**在交易速度上可以达到 3000 笔/秒。结合拜占庭容错算法，**Fus(Financial Upper Story)**在运行过程中对分叉的处理速度上在公有链中也是首屈一指。

6.2 Chaincode:

Fus(Financial Upper Story)提供发布 **Chaincode** 支持，**Chaincode** 支持会让开发者可以在 **Fus(Financial Upper Story)**上发布个人或者企业的业务代码。**Chaincode**，是公开、可信的代码，基于此做出各种去中介化的应用。

6.3 开发者简单:

开发者可以使用 **Javascript** 语言以及海量的 **npm** 库来构建他们的应用。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。在部署 **DAPP** 时，开发者只需要提交代码后在客户端中注册就可以完成部署工作。

6.4 可定制化侧链:

Fus(Financial Upper Story)可以部署相当灵活的侧链，开发者可以随意定制其侧链的各项参数，比如区块产生速度、交易类型、交易费等等，甚至可以实现一个新的共识机制，开发者在 **Fus(Financial Upper Story)**侧链基础上实现新共识的尝试而不需要去写存储、网络等模块的代码，这将大大提高开发效率。

6.5 高安全性:

Fus(Financial Upper Story)系统在 **POS** 的基础上打了一个高效的实用拜占庭容错算法，极大地降低了网络分叉的可能性，也就没有双重支付的风险。其次，系统采用 **BIP39** 标准算法的口令助记符、二级交易密码、多重签名账户等来保证用户的资产安全。

7 • Fus(Financial Upper Story)侧链实现

面对上述的愿景与挑战，我们将设计一条基于侧链开发 **DAPP** 的高性能公链我们将设计一条基于侧链开发 **DAPP** 的高性能公链，以及基于 **Fus(Financial Upper Story)**的多项区块链服务。

7.1 侧链开发



未来的公链底层依然还是要以安全性和去中心化为重点，这也是区块链相比于现有互联网很大的一个区别，保证去中心化就意味着要舍弃一定的性能和可扩展性，不过可以通过侧链方案来解决这个问题。

底层公链保证安全和去中心化，侧链承载更多的应用，可以更贴近具体的业务场景。底层链和侧链各有价值，没有地位高低之分，它们协同配合可以让区块链更加贴近真实的商业逻辑。

侧链开发模式给在处理高交易量下解决网络拥堵的问题一个很好的选择，用户只有用到相关的应用时才需要下载对应的侧链，大大减小了无效的同步数据，保持了整个网络的高效运行，而且网络的速度随着时间的推移会继续加快，越显示侧链的优势。

随着开发者聚集、应用越来越多，大多数公有链上数据臃肿、区块扩展性差、同步时间长的问 题。我们选择设计去基于侧链开发应用的公有链。好处是代码和数据独立，不增加主链的负 担，避免数据过度膨胀，实际上是一种天然的分片机制。

侧链有独立的区块链，有独立的受托人或者说见证人，同时也有独立的节点网络，就是说一个侧链产生的区块只会在所有安装了该侧链的节点之间进行广播。在开发 DAPP 过程中，所有的区块链参数是可以定制的，比如区块间隔、区块奖励、交易费的去向、共识算法等，侧链上可以开发出与业务相关的交易类型或智能合约。

我们将为侧链开发者提供完善的基础设施，我们在 sdk 中为侧链提供了一套模板，即开发框架，侧链本身的大部分底层功能我们将写好，DAPP 开发者只需要关心具体的业务逻辑，开发者可快速开发自己需要的应用，这将极大地降低开发难度。

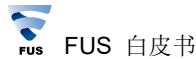
7.2 区块链技术服务平台（BAAS）

基于区块链技术我们将打造世界先进的区块链技术服务平台，为用户提供高性能安全的区块链底层技术服务。我们在有强大的区块链技术能力做支撑的前提下，实现了共识可插拔、交易安全、接口丰富，平台用户可以根据需求定制自己的区块链服务。不同于区块链 2.0 时代的协议模式，我们基于此更进一步。运营者和开发者可以快速定制自己业务需求的 APP，同时使用 FUS 提供的节点和服务器，甚至应用模板、框架，快速部署区块链应用。

7.3 跨链技术

如果说共识机制是区块链的灵魂核心，那么对于区块链特别是联盟链及私链来看，跨链技术就是实现价值网络的关键，它是把联盟链从分散单独的孤岛中拯救出来的良药，是区块链向外拓展和连接的桥梁。

区块链的世界中，大多数链都不知道链外的世界，不具备天然的跨链能力，跨链是一个复杂的过程，既需要对链中节点要有单独的验证能力，需要去中心化的输入，更需要对链外世界的信息的获取和验证。



行业非常需要跨链的技术，三种相对成熟（当然仍存在一些问题）的方案公证人机制、侧链/ 中继器模式、哈希锁定模式都是我们目前正在开发探索的方向。

7.4 Fus(Financial Upper Story)项目应用

一个区块链项目必须有应用场景搭建起来才能实现价值，在 Fus(Financial Upper Story) 团队规划公有链项目时就提出了将研发的应用场景，在应用场景的开发过程中，将会进一步提升 Fus(Financial Upper Story)的健壮性，也有助于我们更快满足社区开发者对 SDK 的需求，构建出对开发者友好的各类开发组件。

基于 Fus(Financial Upper Story)的开发的去中心化应用将具有以下特点：

完全开源，自主运行，不能被中心化的组织、机构或个人操控，可以被改进以响应市场需求，但必须经过用户们的共识。数据必须被安全、公开、冗余的存储在一个分布式网络中，以避免被篡改和单点故障。当应用的运作体系中使用通证作为价值载体时，必须使用一种价值证明的密码学算法来生成通证。

Fus(Financial Upper Story)是面向所有人的公有链，在开发者、企业基于 Fus(Financial Upper Story)开发应用的同时，我们团队也将基于 Fus(Financial Upper Story)公有链开发以下的应用场景：创作生态社区、区块链即服务平台(Blockchain as a service)。同时这也是契合团队为社区和支持者搭建基于区块链服务的愿景。

8 • Financial Upper Story 项目特点：

8.1 链上链下结合

众所周知，区块链上的存储空间是很珍贵的，我们在开发应用过程中采用链上链下相结合的方式，链上存储交易相关数据，而对存储空间需求较大的内容我们选择存储在服务器上或者星际文件系统中。

对于和区块链完美结合的星际文件系统，我们在这里做一些简单介绍：

星际文件传输网络（IPFS）是一个点对点的分布式超媒体分发协议，能够将所有具有相同文件管理模式的计算设备连接在一起。

8.2 工作原理：



每个文件及其中的所有块都被赋予一个称为加密散列的唯一指纹。**IPFS** 通过网络删除重复具有相同哈希值的文件，通过计算是可以判断哪些文件是冗余重复的。并跟踪每个文件的版本历史记录。每个网络节点只存储它感兴趣的内容，以及一些索引信息，有助于弄清楚谁在存储什么。查找文件时，你通过文件的哈希值就可以在网络查找到储存该文件的节点，找到想要的文件。使用称为 **IPNS**（去中心化命名系统），每个文件都可以被协作命名为易读的名字。通过搜索，就能很容易地找到想要查看的文件。

基于内容寻址，而非基于域名寻址。文件（内容）具有存在的唯一性，一个文件加入了 **IPFS** 的网络，将基于计算对内容赋予一个唯一加密的哈希值。这将改变我们使用域名访问网络的习惯。提供文件的历史版本控制器（如 **git**），并且让多节点使用保存不同版本的文件。**IPFS** 的网络上运行着一条区块链，即用来存储互联网文件的哈希值表，每次有网络访问，即要在链上查询该内容（文件）的地址。

举个例子，在用户的医疗数据管理场景下，我们可以帮助用户把数据存储在与去中心化的平台上，在用户得授权下使用用户数据，并不会沉淀用户的个人数据，保证用户的数据权益。

在涉及到创作版权、数据所有权的应用场景里，我们致力于结合链上链下、加密学、去中心化存储等方式保护用户数据的安全可靠。

8.3 应用开发更加简单

去中心化应用可以通过授权系统的权益人来投资应用的开发，从而有潜力达到自给自足。去中心化应用还有公开透明、安全可靠、去信任等优点。

我们选择了 **nodejs** 作为侧链应用开发的语言，开发者可以使用 **javascript** 语言以及海量的 **npm** 库来构建他们的应用，可以满足市场快速开发更新、学习成本降低的需求。

8.4 Baas 平台

结合我们团队在游戏、金融领域的沉淀，我们将大力发展在特色领域的 **BAAS** 平台，为行业内的区块链应用提供强有力的后盾。

8.5 跨链技术实现高聚合

跨链技术可以理解为连接各区块链的桥梁，其主要应用是实现各区块链之间的原子交易、资产转换、区块链内部信息互通，或解决 **Oracle** 的问题等。

Fus 的跨链技术以侧链/中继器模式为主攻方向，实现不同区块链之间的原子交易。



9 FUS 应用场景：

Fus(Financial Upper Story)提供基于侧链开发的 **SDK**，开发者基于侧链可以开发自己的区块链应用，**Baas** 平台 同时会接入企业的区块链服务，跨链服务将会打通这些应用之间的隔断，让交易可以在 **Fus(Financial Upper Story)**网络上自由实现，让价值得以在 **Fus(Financial Upper Story)**网络及其他区块链之间实现流通。基于 **Fus(Financial Upper Story)**，多样化的分布式应用服务可以连接形成更大的体系形成生态，给用户提供更 好的应用服务，给社会带来协作价值和效率。

9.1 通证与智能合约

开发者可能不需要编写代码，只要在文件里修改一些创世参数，就可以发布一个通证牌系统了。**FUS** 系统中的通证牌与以太坊的子货币一样，可以表示黄金、股票、抵押物、或任意其他 资产，这些令牌可以与转入侧链中通过去中心化的方式进行交易，从而实现流通，也可以在中 心化的交易所与其他货币进行交易。智能合约与以太坊网络相似，**Fus(Financial Upper Story)**团队将构建更多 满足种类应用的协议种类，以支持团队与开发者。

9.2 大开发者社区

大部分网站开发者都体验过 **WORDPRESS** 提供的极其便利的网站搭建服务，它经常被用于用户 个人博客的搭建。虽然它有丰富的免费模版和组件，使用时仍然需要一定的专业知识。同时因 过期内容增多，以及服务器搭建不够便利等问题，使得普通人在使用时容易碰到一定困难。当 在使用过程中再加入区块链时会让开发者的学习成本非常可观的增加。

FUS 团队将向 **WORDPRESS** 平台学习开发者社区构建与维护经验，与开发团队合作建立社区， 同时也将吸引更多的个人开发者来为社区贡献组件与素材——基于区块链，所有参与者都将获 得更公平的回报。

Fus 项目团队希望通过去中心化的方式打造一个可以价值流通的创作平台，用户可以上传素材、媒体文件、文字内容等，结合 **APP/DAPP** 开发组件，使得每一个用户都可以选择自己 擅长的方式进行创作，创作作品将通过系统中的激励机制获得创作价值。

基于开发者的贡献，我们推出快速接入 **DAPP** 的 **SDK**、侧链部署云服务结合成的 **BAAS** 平台对 外提供服务，这将为开发者和企业提供极大的便利，即是 **Fus** 团队重点搭建的应用之一——应用开发 **BAAS** 平台。任何人都能非常便利地基于这个平台，构建一个自己的 **DAPP**。

9.3 游戏



网络游戏一直有着生命周期过短的问题。除少数的优质游戏，一般一款游戏运营 1-2 年，就即将面临停服、并服的，用户此时会经历很多风险：此前在游戏内的所有投入将被清空，虚拟资产将随着游戏生命的结束而消失。我们将面向特定的游戏类型开发底层服务：资产多、通信较少、对及时性要求不高。

开发商可以基于我们提供的 SDK 服务便捷地开发区块链游戏，用户也得以受益：资产永久存储于链上，不受运营商随意关服影响，同时游戏数据不可篡改，用户感受更加公平。

9.4 数据存证/交易

基于去中心化的分布式系统可以搭建可信平台支持数据存证、交易。基于此衍生出在链上流通的数字资产。

数据所有权、交易和授权范围记录在区块链上，数据所有权可以得到确认。同时，数据从采集到分发的每一步都可以记录在区块链上，使得数据源可追溯，进而对数据源进行约束，加强数据质量。基于区块链的去中心化数据交易平台，可以促进全球化的数据交易市场走向合规、繁荣。

数据是未来以互联和机器学习为主的经济中最重要的成分，AI 算法分析数据会产生许多改变世界的发现。而对于数据收集能力有限的企业，数据交易将是一个互惠互利的工作，可以促进公司的创新，创造新的收入来源。然而由于目前数据交易市场上存在数据非法倒卖，信息透明度低，易被篡改等问题，导致数据交易的规模受限。区块链的去中心化、安全性和不可篡改可追溯性，可以让参与主体之间建立信任，推进数据交易的可持续大幅增长，数据所有权、交易和授权范围记录在区块链上，数据所有权可以得到确认，精细化的授权范围可以规范数据的使用。同时，数据从采集到分发的每一步都可以记录在区块链上，使得数据源可追溯，进而对数据源进行约束，加强数据质量。基于区块链的去中心化数据交易平台，可以形成更大规模的全球化数据交易场景。

9.5 物联网

物联网存在海量的物理设备，这些联网设备天然可以形成分布式系统，基于 Fus(Financial Upper Story)设备彼此通信形成分布式网络，通过共识算法来保证设备之间的交易的合法性，并且可以追踪、审查、分析。

9.6 分布式能源

在新能源光伏行业中，过去是以集群式的发电站进行，今天，越来越多的分布式屋顶光伏出现并成为趋势。那么，也意味着越来越多的发电节点，这些节点的发电量可以自用也可以上网出售，如果出售就会产生记账和结算等需求。

当分布式的系统中出现需要诚信记账、结算需求时，就会自然想到区块链。区块链技术与分布式能源的整合可能打破现有的能源生产，运输，分销和销售集中的模式。在政策



法规支持的前提下，这将让行业内的能源交易更加可信和高效，并将加速能源产业改革和结构转变。

9.7 医疗

对于医疗行业来说，绝大部分医疗数据是完全封闭的，处于孤岛状态。医疗数据碎片化、不能持续记录和共享，效率和透明度较低，浪费了大量的社会资源。增强医疗数据共享、加强机构间的互操作性对医疗数据的应用至关重要。但如何保护患者安全与隐私是一个非常棘手的问题。

医疗行业有非常火爆的移动医疗创业期，很长一段时间过去了，除可以通过手机挂号外，我们看病、医生断诊的便利与及时性并没有得到解决。

区块链能让多个组织接入对等网络，数据进行加密传输，无需担心数据安全和完整性。医疗数据由多方创建、及时更新、实时共享、存证。开发医疗健康应用，正是采用区块链技术提高医疗行业的效率和透明度。

9.8 其他场景

基于区块链分布式信任的特点，**Fus(Financial Upper Story)**在供应链金融、积分通兑、合同保险、医疗数据、电子商务等领域都将有可能推动行业的发展。而各行各业无需在掌握区块链、分布式账本、密码学、共识机制等复杂体系和技术的前提下就可以将**Fus(Financial Upper Story)**技术引入业内。

FUS 基金会

发布

2017 年 12 月 26 日 (v2.0)