BITE

BitEthereum 中文白皮书

价值传输 + 资产发行与管理 = BitEthereum

BITE

目 录

摘　要

BitEthereum 诞生的目的是为了解决比特币无法提供完善的数字资产发行功能以及比特币和以太坊区块链转账速度慢，效率低下，易用性差等问题。BitEthereum 的使命是成为企业用户与普通用户，以及普通用户之间或商业用户之间沟通的桥梁。BitEthereum 的设计目标是构建一套完善的加密数字资产生态系统，解决比特币以及以太坊现今存在的各种问题。在 BitEthereum 上，除了基础的加密数字资产发行、管理以及流转功能，还引入了用户身份验证、资产自动分红以及联盟功能，实现了加密数字资产免转账手续费功能，并且设计出一个更为简单易用的改良支付系统。同时，为了丰富 BitEthereum 的生态圈，我们还设计出易用性更强的用户界面，以及更为高级也更简易使用的第三方开发者开发套件，使第三方开发者以及企业用户可在 BitEthereum 之上开发出更多应用。

第一章　设计理念

1.1 开发动机

目前，比特币以及以太坊区块链效率低下，比特币网络每秒最多只能处理 7 个交易，以太坊网络每秒只能处理最多 30 个交易。低效的处理速度和难以使用的用户界面使得普通大众无法轻易使用和接受基于区块链的应用系统，商户也难以将区块链技术应用到他们的业务当中。

BitEthereum 拥有高达每秒 3000 笔交易的处理速度以及资产发行与管理功能，可以解决上述问题，除了加密数字资产发行以及价值流转功能外，BitEthereum 将不断拓展出更多应用场景，以满足市场对加密数字资产应用的需求。

1.2 发展方向

在开发初期 BitEthereum 首先完成基础架构、快速转账、免手续费转账、用户身份验证、资产发行、管理以及联盟等基础功能 。接下来，将完成改进的加密数字资产支付功能以及资产流转功能。在可预见的将来，我们将发布资产自动分红功能以及其他更为高级的加密数字资产管理功能，使其有能力服务于其他行业以及能应用到更多的场景当中。

1. 3 BitEthereum 代币空投计划

1. BitEthereum 总量 1 亿， 99%的 BITE 代币将会通过”代币赠送”方式空投给 BTC，ETH 的代币持有者。所有 BTC 持有者共计可以申领 6600 万个 BITE 代币，所有 ETH 持有者可以申领 3300 万个 BITE 代币。

团队将会在 2017 年 12 月 21 日 00:00 对 BTC，ETH 进行快照，快照将会包含 BTC，ETH 的代币持有者的账户余额等数据，快照要求地址余额 BTC≥0.1、ETH≥1。

2.申领：团队将会在 2018 年 1 月中旬发布 BitEthereum 的客户端，BTC 和 ETH 的持有者安装 BitEthereum 客户端后可以通过提交 BTC/ETH 地址的签名到 BitEthereum 区块链的方式申领 BITE 代币。当用户提交签名后，BITE 代币将会自动分发到用户的 BitEthereum 账户上。

3.计算方法：假设 John 有 10 个比特币，快照时比特币流通总量是 16748650。在本轮活动中所有 BTC 持有者总计可申领 6600 万个的 BITE 代币，那么 John 可以获得 10/16748650* 66000000= 39.40616 个 BITE 代币。

4. BitEthereum 区块链网络设定的代币领取截止日期为 2018 年 3 月 21 日。

第二章　技术细节

2.1 代币用途

BitEthereum Token(BITE)作为系统的基础代币，主要有以下几个作用：

1.支付发行资产的手续费

2.用于抵押商户押金

3.支付/维持用户发行资产的资金池（Fee Pools)

4.商户抵押用于产生免转账手续费的带宽

2.2 Graphene(Graphene)框架

BitEthereum 将采用 Graphene 框架作为区块链底层框架。Graphene 框架是一个高性能、高并发、低延迟的实时区块链开发套件，最初的作用是作为比特股（BitShares）的底层开发框架。比特股由 Daniel Larimer 于 2013 年开发完成，其目标是实现一个理想的自由市场金融体系（Ideal Free Market Financial System ，IFMFS），经过多年不断改进，比特股已经稳定运行多年。这套框架可提供平均 1.5 秒的交易确认速度以及每秒 3300 笔交易处理能力，目前市面上也有数款成功的区块链产品采用了 Graphene 框架作为底层开发框架，如 STEEMIT，YOYOW 以及 EOS。

Graphene 框架提供了共识算法、网络连接、用户管理、数据库、区块格式、区块链文件存储等开发库，由于 Graphene 框架本身是为比特股 2.0 而开发，比特股是一个基于区块链的分布式数字资产交易所，如将 Graphene 框架应用到 BitEthereum 上，那么在共识算法、用户管理等方面都需要进行全面重构。我们的开发团队有多年 Graphene 框架开发经验，将会对 Graphene 框架进行深度定制修改以及改进，并在此之上构建 BitEthereum。

2.3 平台模型

Software Development Kit	UNIVERSAL USER INTERFACE
BitEthereum Core	
Graphene Toolkits	

BitEthereum 主要有三层架构组成：

最底层为 Graphene 框架，用于提供底层区块链服务，如平均 1.5 秒的交易确认速度以及最多每秒 3300 笔交易处理能力等，提供高性能并且低延迟的区块链底层平台。

中间层为 BitEthereum Core，即核心层，主要实现与 Graphene 框架的通讯，以及基础的业务逻辑。

最顶层为服务层，服务层封装了开发者套件和通用用户交互界面。

2.4 资产发行者与用户的身份验证

考虑到有不少采用本系统的用户将会是商业用户，身份验证功能将会是本系统的一个重点功能。通用标准以及合规化将是在设计身份验证功能时候需要重点考虑的。而该功能并非强制开启，而是作为一个系统可选项，用于支持高价值的商业用户在与商业伙伴之间构建积分联盟，希望提升在用户中的形象以及信誉度的商业用户也可以选择开启该功能。

考虑到产品在实际中的应用，为了最大程度确保权威性和不可篡改性，在系统设计时候，开发团队做了深入的思考，在用户身份验证功能上，BitEthereum 将会引入 PKI 技术，在 Graphene 框架中集成现有的基于公开密钥体系的 X.509 数字证书标准进行开发。

例如，Verisign 是通过 WebTrust 国际认证和定期接受审计的数字证书认证机构(Certificate Authority)，使用标准的 X.509 数字证书体制。市场上也有数十家认证机构也是采用同样的标准体系，因此，将可直接利用这套体系为用户身份认证以及数字证书分发服务。具体做法如下：

1.由理事会管理一个可信认证中心的根证书数据库(Keystore)，在根证书数据库中包含着经过验证的数字证书认证机构的根证书公钥，理事会定期审查数字证书认证机构的可靠性，如发现数据库中的数字证书认证机构变得不可靠或者不可信，理事会将可吊销该机构根证书。

2.用户通过数字证书认证机构提供的认证流程进行身份验证。(要求至少通过 Class 2 级别的身份验证)

3.认证中心分配用户证书以及私钥。

4.用户将私钥备份到安全地方

5.对关键操作，系统除了要求验证登陆凭证外也要求使用身份验证用的私钥对数据做签名处理。

6.本系统中的共识部分对提交的数据、签名数据与区块链系统中内置的根证书数据库进行验证。

2.5 用户角色与社区治理

理事会：理事会是 BITETHEREUM 管治架构的核心，BITETHEREUM 的理事会中有 X 名理事，理事由 BITETHEREUM 的持币用户通过投票选出。每位投票者的选票权重通过其持币数量与系统总量的百分比计算得出。

理事会的主要职能是：

1. 调整注册、转账、带宽产生比例等系统处理费费率。

2. 处理开发人员工资、系统改进等提案。

3. 管理内置的数字证书认证机构的根证书数据库。

见证人：见证人需要由持币用户通过投票选出，投票权重的计算方法与投票选举理事会的理事一致。见证人的主要作用是处理交易然后打包成区块传送给其他见证人予以确认。见证人定期可以获得代币奖励作为处理交易的报酬。

普通用户：普通用户为资产持有者。每个普通用户都有一个唯一的身份标识，每个用户可以持有多个不同的资产。由于本系统中拥有免手续费转账的功能，对于一般用户而言，日常操作不需要支付转账手续费。

资产发行与管理者：资产发行与管理者可发行自定义资产，在注册时需要支付一定的注册手续费以及可选抵押一定数量的押金和进行身份验证 - 用于提升信誉度。发行资产也需要支付发行手续费。

资产发行与管理者有以下权限：

1.为用户支付注册手续费。

2.锁定押金以获得带宽，带宽可为所发行的资产抵扣转账手续费。

3.发行自定义资产。

4.设定用户每日可以使用所发行资产的用于转账的带宽数量。

第三方开发商：BITETHEREUM 将会提供开发接口（APIS）供第三方开发者调用。通过开发接口，开发者可以开发更多的应用。进一步完善 BITETHEREUM 的生态圈。

2.6 免手续费转账功能

免手续费转账会是 BitEthereum 的核心功能之一，在日常的现实场景中，用户在收取或者支付所持有的积分或者其他类型的数字资产时并不需要支付转账手续费。我们理解到区块链是一个价值网络，每

一笔的操作都需要见证人/矿工节点（Block Producer）来处理，而每一个见证人节点的运行都需要付出成本，也可能期望获取一定的利润来维持见证人节点的运转。因此，经济诱因必不可少，BitEthereum 并不打算改变这一点。但是，我们认为站在普通用户的角度来看，如果需要其支付转账手续费来使用这个系统并不合理。

因此在 BitEthereum 中，我们引入了一套免手续费转账的功能：利用资产发行与管理者抵押在系统中的代币所产生的"币天带宽"来为其所发行资产产生的所有转账操作支付转账手续费。下面是一个例子：

假设有商户 A 发行了一个积分资产：积分 A。一共有三个用户持有这个资产，分别是用户 1、用户 2 以及用户 3。

商户 A 在创建资产的时候抵押了 100 个 BITE 代币，而每天这 100 个 BITE 代币可以产生 100 个币天带宽。假设在 BitEthereum 中，每一笔交易需要消耗 10 个币天带宽，那么持有这个积分 A 资产的用户在支付/转账积分 A 的时候都可以消耗商户 A 抵押代币所产生的币天带宽来支付转账手续费。

但这可能会有一个滥用服务的问题，比如上面的例子里，假设用户 1 在一天的时间里发出了一共十次的转账交易，商户 A 的币天带宽都被消耗完毕了，那么用户 2 和用户 3 就无法在这一天里再利用这个免手续费转账的功能了，因此，为了解决这个问题，BitEthereum 将会允许商户 A 对每用户每天最多可以利用免手续费转账的次数进行限制，比如像上面的例子，商户 A 可以设置成每用户每天最多可以利用三次免手续费转账功能，即可解决问题。

2.7 资产分红功能

除了一般的积分类资产以外，资产发行与管理者也有发行带有分红性质的加密数字资产的需求。

在目前其他去中心化的资产管理类区块链系统中并没有自动化的分红功能，在那类的系统中为了实现类似功能可能会要求一个中心化的机构在某个日期点进行快照操作然后再手动分发红利。我们认为这种状况并不理想。

因此，在 BitEthereum 中，将会加入一个由智能合约驱动的资产自动分红功能，具体做法如下：

1.资产发行与管理者公布分红计划。

2.资产发行与管理者设定除权除息日，派息日的具体时刻，并将每单位资产的分红数量等信息写入智能合约内，并将用于分红的资产锁定在系统内。

3.智能合约一经订立则无法中途停止或者修改，当到达派息日参数之后的那一个区块，智能合约将会将锁定的分红自动派发给除权除息日之前持有资产的用户的账户中。

2.8 加密数字资产联盟功能（积分联盟）

通过此功能，资产发行与管理者之间可以互相通过智能合约订立一个资产联盟-用户可通过固定的兑换比率兑换联盟内其他资产发行与管理者所发行的资产。由于 BitEthereum 拥有转账和资产流转功能，如果没有一个资产汇率锚定的机制，联盟内的资产汇率可能会有很大波动，这违反了建立联盟的初衷。为了解决这个问题 BitEthereum 通过联盟内汇率锚定资金池来解决这个问题。

2.9 改进的加密数字资产支付功能

BitEthereum 之上,我们提出了一种基于 Graphene 框架的高级支付通知模型以及改进的交易识别功能。

在交易的区块结构中我们新增了一个专门存放用于识别和跟踪交易来源的专属功能字段。该字段数据结构如下：

高级/初级模式+分隔符+附加数据

在初级模式中，可以将子网点的识别号和订单号等订单信息放入附加数据内，可以借此实现简单的支付确认，如下面的例子：

1.子网点使用时间、子网点识别号、金额、子网点使用 GUID 算法生成的订单号这几种信息生成一个转账用的二维码

2.用户扫码转账

3.子网点使用观察钱包观察主账号的交易流水和识别和跟踪交易来源的专属功能字段中的交易附加数据，如果全值匹配则代表转账成功

在高级模式中，必须分配密钥给予每个子网点（该密钥与账户无关）。子网点使用密钥对所有交易信息进行加密并放到放入附加数据内。该模式可以实现高级的订单通知以及订单确认功能，如下面的例子：

1.子网点与主网点在链外通过密钥建立可靠安全点对点加密通信信道

2.子网点通过加密信道提交订单数据

3.主网点生成订单号并返回给子网点

4.子网点使用密钥对订单号进行加密操作

5.子网点使用主账户地址，金额和加密后的订单号生成转账用二维码或支付链接

6.用户进行转账操作

7.子网点/主网点观察主账号的流水以及对附加数据（加密后的订单号）进行解密并与提交的订单数据进行核对，如果全值匹配则代表转账成功

初级模式适用于实体商户或其他仅要求简易确认的商户，高级模式适用于网络支付（如实现类似于支付网关的即时付款通知等功能），需要由主网点处理交易的场景或其他要求更为严格确认的商户。此

外，通过高级模式的这套机制，子账户可以利用密钥与主账户进行链外点对点加密通讯，可用于消息传递，更为高级的订单数据确认和提交等功能。同时子网点没有任何权限去动用主账号的资金，能最大程度确保商户的资金安全。

2.10 商业友好的开发套件（SDK）与商户独立的用户界面

BitEthereum 除了提供应用程序编程接口（API）外，还会提供一个完整的开发套件（SDK）给第三方开发者，让他们可以快速地开发出基于 BitEthereum 资产发行与管理系统。

而 BitEthereum 的通用用户界面钱包是一个提供完整功能的通用区块链钱包以及区块链浏览器，但考虑到部分商业用户希望提供独立品牌的钱包或者基于积分联盟专属的客户钱包。在未来，为了使得没有开发力量的商户可以快速实现构建品牌专属的资产发行与管理系统，BitEthereum 将会提供向导式（Wizard）定制化品牌专属钱包生成程序。

第三章　发展路线

3.1 发展路线图

BitEthereum 项目于 2017 年 12 月启动，有望于 2018 年 1 月份发布第一个最小可用版本（主链），2018 年 4 月份开启加密数字资产发行、管理以及身份验证功能。第三方开发者套件，资产分红功能以及联盟与流转功能有望于 2018 年 6 月上线，更多丰富的应用也随后会陆续上线。

3.2 第三方开发者支持

BitEthereum 的发展需要不断接入更多应用以实现更多的应用场景。因此，BitEthereum 将在上线之后会提供一系列的开发接口供第三方开发者进行二次开发。