FBTC（fast bitcoin）
系统技术白皮书

目 录

前 言

比特币作为超主权货币和与生俱来的信用价值体系已经无需多说；但是技术实现并非完美，比如一直被诟病的交易速度，可扩展性等等。如何沿用比特币的影响力，不断地改进比特币的技术方案已经迫在眉睫。Fast Bitcoin（FBTC）快速比特币应运而生，旨在改进比特币发展到目前为止存在的各种问题，让比特币系统不但回归中本聪设计之初的思路，同时融入区块链发展至今整个社区拓展的新技术。

在扩容问题上，FBTC 将区块链容量交给矿工调节，最低 1M，最大 10M，矿工每个区块需要投票，难度调整时同时调整区块容量限制。在交易效率问题上，FBTC 采用账户模型取代 UTXO 的低效和冗余，在实现方式上采用硬分叉方式实现，一次性解决问题。FBTC 采用 DPOS 共识机制，大大降低了 POW 的能源消耗，同时货币总量却不增发。

在交易延展性问题上，FBTC 将在底层协议为彩色币协议做进一步的升级，放开发行资产的权限，即一链多资产；同时撮合链上各个资产的互换，实现链上的交易所功能，解决了传统交易所黑盒交易和破产的风险。下一步逐步实现图灵完备性的智能合约虚拟机（FVM）。 在隐私方面，FBTC 未来有可能将引入零知识证明，以实现真正的隐私。此外，为了保护用户资产，FBTC 将做好双向重放保护，使 BTC 和 FBTC 在分叉后相互保持独立。

FBTC 将于区块高度 501225 进行分叉，预计时间为 2017 年 12 月 25 日，发行总量 2100 万，原持有比特币的地址将按 1:1 比例继承 FBTC。

第一部分　FBTC 的设计理念

1.1 比特币出现的背景和智能合约的意义

在比特币诞生之前，信息传递都是通过互联网的 TCP/IP（传输控制协议/因特网互联协议）协议来实现高速低成本的传输，但是随着互联互通技术的发展（互联网、物联网、VR/AR），人与物体、人与信息的交互方式更加多样化，更多的实体被数字化或者代币化，仅仅是信息的分享和传输并不能满足经济社会的发展，因此当实体被数字化或者代币化之后，人们越来越关注到价值转移以及如何点对点传输这些资产和价值。

2008 年 10 月 31 日，Satoshi Nakamoto <satoshi@vistomail.com> 通过一个密码学小组（gmane.comp.encryption.general）发送了一封邮箱，一次公布了比特币的白皮书《Bitcoin: A Peerto Peer Electronic Cash System》，并提出了比特币网络的一些特点：

1. Double-spending is prevented with a peer-to-peer network （防止双花）；

2. No mint or other trusted parties （无铸币厂或其他信任方）；

3. Participates can be anonymous （参与者可匿名）；

4. New coins are made from Hashcash style Proof-of-work（通过工作量证明方式发行新币）；

5.The proof-of-work for new coin generation also powers the network to prevent double-spending （基于工作量证明的新币发行过程中，也同时阻止了双花的发生）。

在 2009 年 1 月 3 号，比特币的创始区块被挖出，并在第 170 个区块发生了第一笔比特币的转账交易（从 Satoshi 到 Hal Finney，发生在 2009 年 1 月 12 号），从此开启了比特币网络作为一种点对点的价值交换媒介。网络蓬勃发展的时代虽然中间经历了各种危机，但是比特币网络的价值从零开始，到今天已经成为一个价值约 100 亿美金的点对点支付网络。点对点价值传输网络的出现有其历史必然性，而 Satoshi 则是加速这个历史进程的人。从上个世纪 80 年代，TCP/IP 协议的开发，到 90 年代，网页浏览器的应用和服务器的应用，一直到今天，互联网技术从不同侧面和维度改变了数据交换的模式和人类的生活。互联网技术的发展得益于基础设施的完善，从早期的信息高速公路（Information Super Highway ）和各种智能终端的普及，这些也构成了互联网 OSI 七层模型中，应用层无限拓展的基础。

在互联网的各种协议栈中，我们用的较多有 TCP/IP，HTTP，HTTPS，FTP，TELNET，SSH，SMTP，POP3 等网络层，传输层，应用层的协议，并且借助这些协议，我们已经比较完美了搭建了各种各样的互联网服务。但是如果我们深思，我们会发现，在比特币网络出现之前，我们一直无法在不借助第三方的情况下，在互联网上较好的进行点对点的价值的转移和传输。其实我们并不是缺少一种特定的方法，而是缺少基于信息高速公路（Information Super Highway）的价值高速公路（Value Super Highway），以及如何实现 Value Super Highway 的 Value Transfer Protocol （VTP 协议），而比特币网络则是运行于信息高速公路上面的第一个 VTP 协议。随着互联互通技术的发展（互联网、物联网、VR/AR），人与物体、人与信息的交互方式更加多样化，更多的实体被数字化（Digitalize）和令牌化或者代币化（Tokenize）和符号化（Symbolize） ，一旦实体被数字化或者代币化之后，就完成了实体资产在互联网上

面的映射和切分，马上面临的一个问题就是：如何点对点传输这些资产和价值？因此可以推测，随着互联网服务的进一步深入，实体和虚拟的边界也会越来越模糊，点对点价值转移的需求愈加凸显，因此在互联网上面的 Value SuperHighway 和 Value TransferProtocol 必然会出现，而归纳出比特币网络底层的区块链技术则加速了这一历史进程。

随着区块链技术的成熟，使得最早在 1995 年提出来的智能合约的实现成为现实。2013 年以太坊发布，以太坊的底层技术支撑了区块链上的生态环境，使得区块链技术开发应用变得触手可及，就像最早 Windos 系统的发明一样，今天在以太坊的操作系统上已经产生了很多个区块链 APP 和区块链技术的落地商业应用，进一步使用 VTP 协议实现点对点价值传输。

1.2 FBTC 的缘起

自从比特币 2016 年接受度越来越高，比特币的网络变得越来越拥堵，并且随着比特币价值越来越高， btc 的交易变得越来越零碎化。越来越偏离 btc 大宗资产交易的初衷。

FBTC 致力于打造快速高效的比特币网络。因此 FBTC 决定打破现有的僵局，以开创性的态度，将 UTXO 模型转变为 account 模型。UTXO 模型目前具备以下缺点:

1. 交易变得细碎化，需要很多个 vin 才能构建出一笔转账。
2. 有些场景下无法根据交易精准的确定入账方和出账方。
3. 除了转账外，其它类型的数据扩展性极差。
4. UTXO 账户资产统计困难。

为了提供更加优质的服务，FBTC 团队开创性将 UTXO 变更为账户模型。

第二部分　国内区块链现有技术和生态现状

区块链是一种由多方共同维护，使用密码学保证传输与访问安全，能够实现数据一致存储、无法篡改、无法抵赖的技术体系。区块链系统的一致性和正确性，从机制上解决人类社会最根本的信任问题。

2.1 以太坊技术分析

以太坊的核心理念是一条内置图灵机可计算性的编程语言的区块链，允许在上面创建任何种应用。

以太坊和原来的比特币技术不同的是：

1、实现了基于 Solidity 语言的智能合约，并将智能合约看做一种特殊的账户，从而使得在智能合约上也可以实现具体的方法；

2、实现了智能合约能落地执行的 EVM（以太坊虚拟机），通过以太坊虚拟机，从而将 solidity 这样的类 js 的代码变成了可以在去区块链上执行的加密代码；

3、不同于比特币技术，在以太坊的 transaction 都需要用到 gas，一份合约或者一次交易的 gas 是固定的（取决于代码大小和复杂度），而 gas 的价格则由以太坊中的 oracle 来决定；

4、以太坊同时还构建了较完整的、开源的生态系统，不仅有底层的 geth、编程的 solidity、合约在线浏览器 browser-solidity、合约钱 Mist/wallet、以太坊的前端开发框架 Truffle、各种各样的开源 DApp 等等，方便大家快速上手，并开发出适合落地的区块链应用。

以太坊缺点：实际上，目前以太坊的 GAS 设计对于小额交易而言成本太高，且 12s 左右的确认时间还是太长。

2.2 QTUM 技术分析

QTUM 是 QTUM 开源社区开发的比特币和以太坊之外的第三种区块链生态系统，用以拓展区块链技术的应用边界和技术边界。在 QTUM 的系统中，信息可以通过价值传输协议（Value Transfer Protocol）来实现点对点的价值转移，并根据此协议，构建一个支持去中心化的应用开发平台（DAPP Platform）。QTUM 在区块链技术和理念上进行

了一系列的创新：包括基于 UTXO 的隐私保护智能合约模型，面向公有链和联盟链的共识机制，交易账本和智能合约账本的分离，便于外部监管等数据源进入主合约的 Oracle 和 Data Feed 的设计和实现等。Qtum 通过对 proof-of-state 等底层算法做了一些修改，采用的是激励机制的权益证明来建立共识。

2.3 元界技术分析

元界是基于区块链技术开发的去中心化项目，在元界上建立一个智能资产网络系统（Digital Asset Web），区块链上集成了数字身份认证（Digital Identity Verification）和价值中介（Oracle）的服务框架。元界区块链将成为一个开放的数字价值流转的生态。作为中国目前唯一基于 POW 共识机制的公有区块链项目，元界将致力于提供基于数字资产登记、数字资产交换、数字身份、价值中介的去中心化服务。元界的数据存储保留了 Libbitcoin 设计的原生 hash-memory-map 的方式，这种方式的优势是速度和性能非常好， 容易接入 memory-pool，缺点是在扩展性上不足，以及有一定的学习成本。区块链共识过程，是指如何将全网交易数据客观记录并且不可篡改的过程。目前比特币使用工作量证明 Pow（Proof of Work），以太坊即将转换为权益证明 PoS（Proof of Stake），比特股使用授权权益证明 DPoS（Delegated Proof of Stake）。他们之间的最大区别是：系统在拜占庭将军（Byzantine Generals Problem）情景下的可靠性，即拜占庭容错（PBFT 算法支持拜占庭容错）。然而无论是 Paxos 还是 Raft 算法，理论上都可能会进入无法表决通过的死循环(尽管这个概率其实是非常非常低的)，但是他们都是满足安全性的，只是放松了 liveness 的要求，PBFT 也是这样。

元界开始使用 POW 模式，后期采用改良后的 DPOS 模式。

2.4 The DAO 技术分析

就是基于以太坊区块链平台开发的去中心化自治的 VC。每个参与众筹的人按照出资数额（以太币），获得相应的 DAO 代币（token），具有审查项目和投票表决的权利，其中投票权重与出资额相关。传统风投基金中，投资策略是由经验丰富的基金经理等专业人士制定的；而 The DAO 则是基于 The DAO 众筹项目的参与者的群体智慧。以

太坊和 The DAO 的关系：以太坊可以看做是全球计算机，而 The DAO 是搭建在以太坊平台上的一个 Dapp（去中心化应用），或者说以太坊是平台层，而 TheDAO 是应用层。

2.5 信链技术分析

信链采取经济激励的方式，鼓励用户贡献自己空闲的存储资源以及带宽资源，通过信链终端将这些资源组成一个具备高效协同、隐私安全的可信存储网络。基于信链终端的云盘，可为每个用户提供“隐私数据保险箱”式的存储服务；信链终端会提供一个智能化的数据存储控制层，用算法来确定数据存储的位置，兼顾存储可靠性和性能，用户也可以根据需求选择数据存储的可靠性级别和性能级别；同时提供数据迁移功能。存储于信链网络中的任何数据，在未获得用户许可的情况下，不会被任何组织读取，进行诸如大数据分析、精准营销等，从而保护用户数据的使用知情权。

2.6 STORJ 技术分析

STORJ 实验室能够让软件开发商在一个分散式网络平台上对自己的应用软件使用推、拉数据。这些数据通常在一个由“农民”组成的社区里储存，社区里的“农民”可以出租他们的空闲磁盘空间给分散式网络系统用户。作为出租空闲磁盘的补偿费用，“农民”们可以获得一种叫做 Storjcoin 的网络货币。STORJ 实验室起源于开源项目 Storj project，该项目中有一个软件开发商共同组成的大型社区，旨在打造一个以区块链服务为后台，且效率最高的分散式云存储平台。暴走时评：STORJ 能够使用区块链技术，利用空闲的磁盘空间来创建一个去中心化市场，并且用内置的数字货币 SJCX 进行交易。Storjcoin X（SJCX）这是在 STORJ 的网络系统中的一种代币，它可以像“燃料”一样允许用户在名为“DirveShare”的 app 中使用，通过 SJCX 来租用或者购买存储空间，就像 MetaDisk 一样。SJCX 已经在 11 月 28 日发布了首个图形界面的版本，能够让普通计算机用户在发布最终版本之前，使用它来测试软件系统。因为 STORJ 对象存在于分布式网络中不信任同龄人，农民不应该依靠同样的安全作为传统云存储公司的数据丢失措施。确实，农民可以随时关闭节点。因此，它是强烈的建议数据所有者实施冗余方案以确保他们档案的安全。因为协议只处理个人的合同，这表示欺骗客户端攻击是一个任何声誉系统的未解决的大问题。人质字节攻击是一种存储

特定的攻击，恶意的农民拒绝转移碎片或碎片的一部分，以征收额外的费用数据所有者的付款。数据所有者应该保护自己通过多个节点冗余地存储分片来实现人质字节攻击。只要客户端保持其擦除编码的界限一个秘密，恶意的农民不知道最后一个字节是什么。冗存储不是这种攻击的完整解决方案，而是占绝大多数的这种攻击的实际应用。击败冗余需要勾接跨越多个恶意节点，这在实践中很难执行。还有其他不少区块链平台，Hypherledger 联盟中已经有一些项目代码开源，Fabric、Elements、SawTooth Lake 等；其中 Fabric 更适用于金融行业，其中隐私保护、共识算法、身份认证、以及模块化设计非常灵活。不过 Fabric 正处于快速开发中，代码变更非常快，比如：上个月开发的应用，下个月就不能使用了；另外 Fabric 本身的稳定性和性能还不够。R3 组织在 2016 年 11 月 30 日公布了区块链 Corda 的源代码，Corda 是用一种小众语言 kotline 写的，研发还处于早期，其设计思想是分布式账本，并非区块链，比较适用于银行间的国际支付和清算结算。如 Bitshares、Openchain、Chain 等，都有其适用性和可取性。众多的区块链底层技术平台，使得金融机构必须得一一去学习，去理解其技术，才能结合应用场景采用某种区块链。考虑到央行、工信部、金标委等诸多标准和架构，某些行业如金融行业还有可能更换平台，因而所付出的时间成本和人力成本较大。

第三部分　FBTC 的技术特征

3.1 FBTC 概述

FBTC 致力于打造高性能企业级区块链平台，开发企业级区块链业务系统。FBTC 智能合约系统可以通过在区块链上发行某种代币或者积分来实现具有价值转移或者价值传递的业务，同时可以构建完整的技术方案解决企业实际应用的问题。

区块链的诞生，标志着人类开始构建真正可以信任的互联网。FBTC 智能交易系统的问世能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介环节，既公开信息又保护隐私，既共同决策又保护个体权益，这种机制提高了价值交换的效率并降低了成本。

3.2 FBTC 模型

区块链技术以去中心化、分布式、区块不可逆等核心特征出现在人们眼前，并得到广泛的关注，这些特点为区块链带来独特的价值，但同时也造成了性能方面的阻碍和不利于结合现有产业应用等问题。FBTC 智能合约系统在设计之初，秉承的理念就是通过创新，让区块链能够更好的服务于当前和未来的企业，主要目的是提供区块链私链或者区块链联盟链的快速解决方案。

高性能优势：交易支持秒级确认，提供海量数据存储，具备每秒万级的快速处理能力；

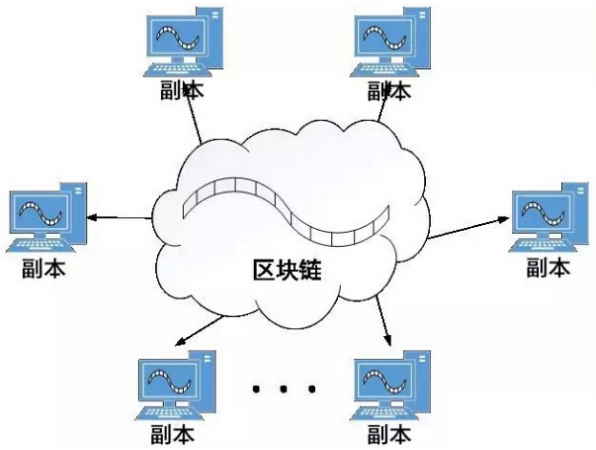
安全特性：提供丰富的权限策略、安全的密钥管理体系和用户隐私保密方案，保障数据安全。

多资产：支持链上多资产，并可以进行快速交易。

3.3FBTC 智能合约系统设计体系介绍

3.3.1FBTC 智能合约系统

区块链是一种以密码学技术为基础，以去中心化的方式，对大量数据进行组织和维护的数据结构。区块链建立在分布式的数据节点上，并且通过共识算法进行同步，因此特别适合作为数字资产的账本。区块链上的数据全部都附有相关人的数字签名，不可伪造。



3.3.2 账户模型和账户体系

FBTC（FAST BITCOIN）系统里，每一个客户端是都是一个本地钱包。用户在自己的本地钱包中创建一个或多个账户，并且进行相关的账户操作。每一个账户都有唯一的私钥并对应唯一的地址。账户分为普通账户、注册账户、代理账户、出块账户、合约账户。

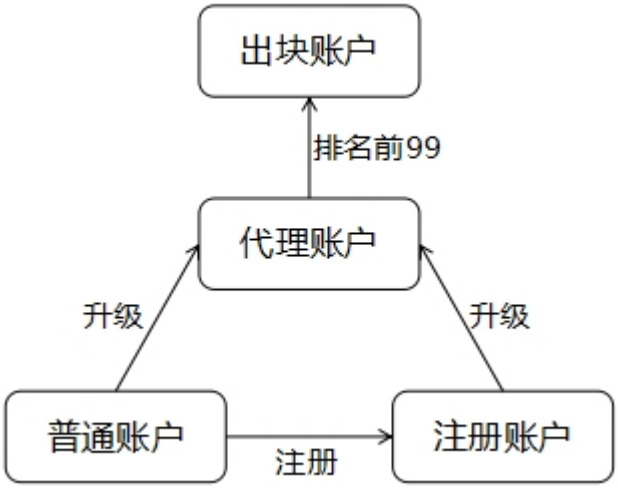
普通账户：普通账户是一个本地账户，仅在本地钱包内有效，用于区分当前钱包内的多个账户。只有在本地钱包中才可以通过这个普通账户的账户名向该账户转账。

注册账户：普通账户可以升级为注册账户，升级后账户名会被注册到区块链上。用户可以直接使用账户名进行转账操作。区块链上的账户名具有唯一性。升级成注册账户，需要花费一个基本交易手续费。链上的任意账户都可以通过注册账户的账户名向该账户转账。

代理账户：普通账户或注册账户都可以升级成为代理账户，代理账户拥有注册账户的所有功能，并且具有被投票权。

出块账户：当代理账户的排名进入前 7 名（包括第 7 名）时，代理账户可以参与系统出块，从而获得出块收益。

合约账户：当合约被注册上链后会产生一个合约账户，合约账户不属于任何一个用户账户，也没有公私钥，因此无法直接操作合约账户进行转账。用户账户可以向合约账户中转账，合约账户也可以向用户账户转账（仅在合约代码中）。



3.3.3FBTC 账户地址生成规则

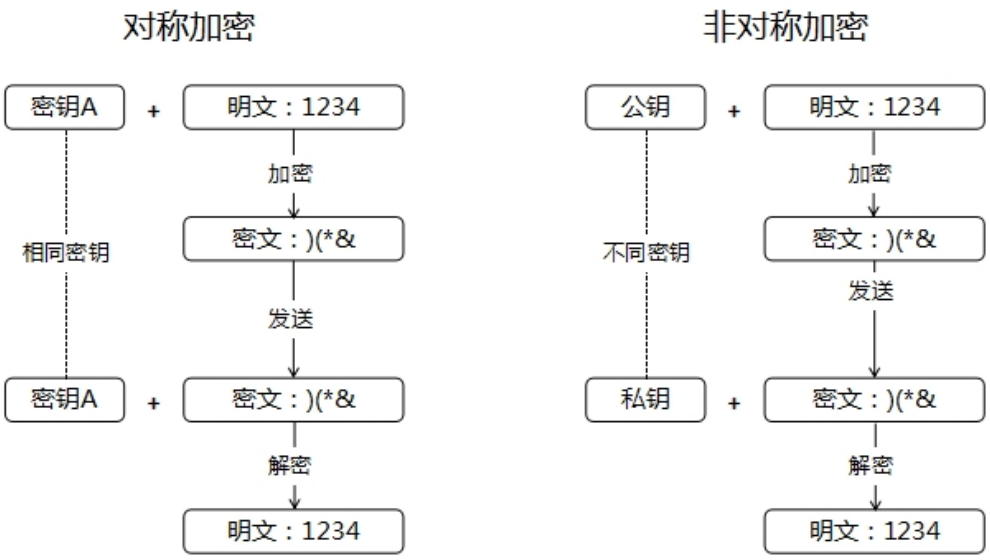
（1）密码学模型

私钥：非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

公钥：可以公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，候选方案为 secp256r1（国际通用标准）、secp256k1（比特币标准）和 SM2（中国国标标准）。

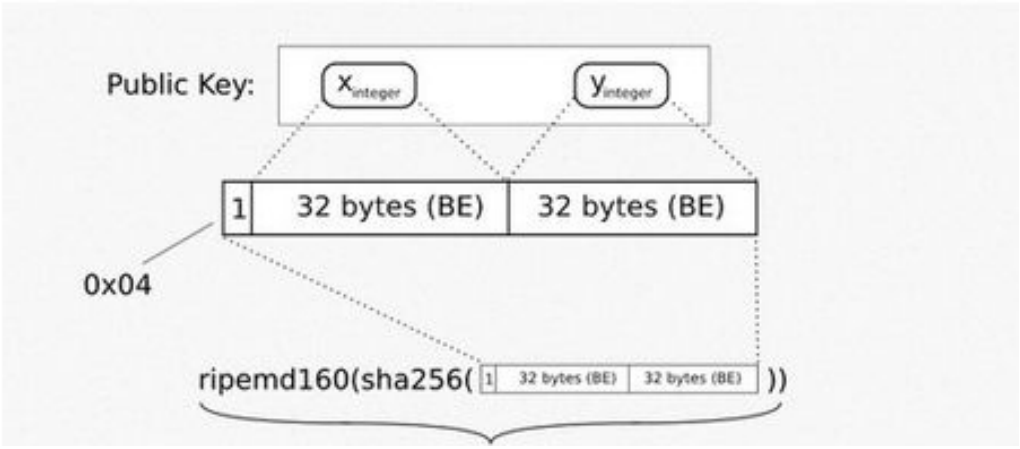
对称式加密：就是加密和解密使用同一个密钥，也就是说采用这种加密方法时候，加密方与解密方需要使用同样的密钥进行加密和解密，该方式只需要一个密钥+特定算法对数据内容进行加密，加解密效率比较高，因此在对被广泛使用。但是因为解密方也需要密钥，所以保证密钥的安全也成为了一个难题。

非对称加密：与上面相反，如果加密和解密是采用不同的密钥，就是非对称加密密钥密码系统，每个通信方均需要两个密钥，即公钥和私钥，这两把密钥可以互为加解密。如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公钥向其它方公开；得到该公钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把私钥对加密后的信息进行解密。公钥是公开的，不需要保密，而私钥是由个人持有，并且必须妥善保管和注意保密。如下图所示两种加密模式：



（2）地址

地址：是公钥的摘要，是为了用户能够方便交易而产生的，因为公钥较长约有130 位字符，而地址比较短，约有 35 或 36 位字符，地址由公钥推导生成。



推导关系：私钥→公钥→地址。过程均不可逆，拥有私钥便拥有一切。

（3）FBTC 智能合约系统平台

FBTC 智能合约系统平台建立在 DPOS 共识机制基础上，综合运用了 hash 算法、对称加密算法、非对称加密算法、密钥协商算法。

- **产块与块内交易的共识**

在系统正常运转的情况下，产块共识保证了在同一个产块周期内，只有一个确定的产块代理会产块。且代理生产的块可以通过其他节点的验证，并且前一个块和后一个块之间可以通过特定的规则串联在一起（后一个区块中记录前一个区块的区块哈希）

- **产块代理共识/顺序共识**

在系统正常运转的情况下，产块共识保证了在同一个产块周期内，只有某一个确定的产块代理会产块。

由投票决定新一轮的产块代理，对于所有节点来说，每个代理的投票在所有不同的节点上都是确定的，而且是一致的。

由 random_seed 来决定新一轮的产块顺序。产块顺序是由所有代理节点共同决定，并保证无法被预知和篡改。这个行为在所有的节点上也是可以达成共识的。

- **交易/块验证共识**

处于相同状态下的多个节点，进行相同的操作，产生的结果必然是一致的。

- **交易共识（特殊的交易共识）**

资产交易的同一个操作可能会在不同区块链节点不同时间执行，可能产生不同的时序，交易请求上链，可以确保交易顺序共识，从而可以确保无法伪造交易结果。

3.3.4 智能交易

（1）智能交易介绍

区块链上一般都只能定义自己的某一种或几种资产。智能交易系统支持任意种类的数字资产。跟智能合约实现的多资产不同，这些资产之间在区块链上可以直接进行交易。性能和自由兑换是主要的优势。

（2）区块链上的智能交易

- 交易请求（挂单）在区块链上确认

- 不同资产之间可以进行兑换
- 所有交易结果也都在链上共识，确保无法篡改

之所以说区块链是全球化交易市场天然的生存土壤，是由区块链一些特性决定的：

- 去中心化的系统；
- 安全的完善的密码学原理保障公私钥密码体系；
- 交易数据全网共识，不可篡改；

（3）FBTC 智能交易系统

在 FBTC 智能交易系统中，将交易挂单设计为一个特殊的交易并通过共识记录在区块链上。同时资产的创建，发行和销毁等操作也都在区块链上通过特殊交易进行记录，所有节点都可以验证这些交易的正确性。

（4）交易验证

从交易类型上来看，交易可以分为普通交易和资产交易：

➢ 普通交易

普通交易在所有节点都会验证，并且验证方法一致，交易在所有的节点上达成共识。

➢ 资产交易

资产交易分为资产管理类交易和资产交换类交易。

第四部分 FBTC（FAST BITCOIN）实现方案

4.1 可共识的随机数发生器

4.1.1 随机数的计算方法产生方式

使用未来某个块的 random_seed 做为生成随机数的依据 random_seed，通过上一次的 random_seed 和当前出块节点的 previous_secret 计算相当于是由多个代理节点共同维护并计算出来的结果，并且 previous_secret 是上轮就已经计算并确定，且在上轮出块后就将其摘要公布，可以被其他节点验证，因此可以认为这是一个可靠的，由多个代理共同维护计算并验证，可共识的随机数生成算法。并且是无法被操纵，无法被推算的随机数。

4.1.2 应用

- 代理出块顺序
- 合约获取随机数

4.2FBTC 智能交易系统资产管理

FBTC 对于链上的多资产提供了多种配套功能。

4.2.1 资产管理

包括资产的创建，销毁，发行/增发等等。通过特殊的交易类型，并且消耗基础资产的情况下可以发行任何自定义的资产，并做管理。

4.2.2 资产流通

主要通过链上交易系统，允许链上基础资产和新发行的各类资产之间进行兑换。流通过程中需要消耗一定量的基础资产。因此实际上是以基础资产作为背书。

4.3 多重签名

可以创建这样的多方签名账户，在这个账户上的资产需要多个私钥中的一部分或全部都进行签名，才可以使用。单独一把私钥，或少于指定数量的私钥产生的签名，则不会被其他节点共识。

4.4FBTC 智能交易系统数据指标

普通交易 TPS	1000
合约交易 TPS	100
块大小	10M
代理数量	7
产块间隔	10s
产块时间	3s

专业术语

1. 比特币：比特币是一种加密数字货币，在 2009 年由化名的开发者中本聪（Satoshi Nakamoto）以开源软件形式推出。

2. 以太坊：以太坊是一个有智能合约功能的公共区块链平台。

3. 价值传输协议: 用于基于互联网的价值传输。

4. Internet of Things: 物联网。物联网是互联网、传统电信网等信息载体，让所有能行使独立功能的普通物体，如物理设备、汽车、建筑等实现互联互通的网络。

5. Oracle: 根据预先设定的判断条件，对输入数据进行筛选，选择最适合的数据作为数据输入。

6. Data feeds: 数据馈送，为区块链提供数据链下数据来源。

7. PoS: 权益证明共识机制。根据每个节点所占代币的比例和时间，等比例的降低挖矿

难度，从而加快找随机数的速度。

8. UTXO: 未花费交易输出。比特币网络中使用的交易模型。

9. 智能合约：智能合约是由时间驱动的、具有状态的、运行在一个复制的、分享的张本质上的、且能够保管账本上资产的程序。

10. 代币：除了比特币以外的数字货币。

11. PoW：工作量证明共识机制。一方（通常称为证明人）提交已知难以计算但易于验证的计算结果，而其他任何人都能够通过验证这个答案就确信证明者为了求得结果已经完成了大量的计算工作。

12. 公有链：公有链是任何人在任何地方都能发送交易且交易能获得有效确认的、任何人都能参与其中共识过程的区块链。

13. 以太坊虚拟机: 以太坊虚拟机设计运行在点对点网络中所有参与者节点上的一个虚拟机，它可以读写一个区块链中可执行的代码和数据，校验数据签名，并且能够以半图灵完备的方式来运行代码。它仅在接收到经数据签名校验的消息时才执行代码，并且区块链上存储的信息会区分

所做的适当行为。

14. 激励权益证明共识: 在权益证明共识中加入了激励措施，和估计节点在线。

15. 硬分叉: 区块链发生永久性分歧，在新公式规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会产生。

16. DAO：分布式自治组织。通过一系列公正公开的规则，可以在无人干预的和管理的情况下自主运行的组织结构。

17. 图灵完备语言： 一个能计算出每个图灵可计算函数（Turing-computable function）的计算系统被称为图灵完备的。一个语言是图灵完备的，意味着该语言的计算能力与一个通用图灵机（Universal Turing Machine）相当，这也是现代计算机语言所能拥有的最高能力。

参考文献（加上部分参考文献）

1、《Qtum 白皮书》

2、《中国区块链技术和应用发展白皮书 2016》

3、《区块链：如何重新定义世界》：唐建文，吕雯，机械工业出版社。

4、《区块链革命》，作者[加]唐塔普斯科特（Don Tapscott）/[加]亚力克斯·塔普斯科特(AlexTapscott) ，由中信出版集团股份有限公司于 2016 年 9 月出版。

5、《数据结构与算法分析》：严蔚敏．清华大学出版社，2011。

6、相关网站资料

[1] https://en.bitcoin.it/wiki/Category:History

[2] https://panteracapital.com/wp--content/uploads/The--Final--Piece--of--the--Protocol--Puzzle.pdf

[3] https://github.com/bitcoinbook/bitcoinbook

[4] https://github.com/ethereum/wiki/wiki/White--Paper

[5] S. Nakamoto, Bitcoin: A peer--to--peer electronic cash system,

[6] https://www.bitcoin.org/bitcoin.pdf

[7] N. Szabo, Smart contracts, 1994, http://szabo.best.vwh.net/smart.contracts.html

[8] N. Szabo, The idea of smart contracts, 1997, http://szabo.best.vwh.net/idea.html

[9] Bruce Schneier, Applied Cryptography (digital cash objectives are on pg. 123)

[10] Crypto and Eurocrypt conference proceedings, 1982--1994

[11] David Johnston et al., The General Theory of Decentralized Applications, Dapps, 2015,

https://github.com/DavidJohnstonCEO/DecentralizedApplications

[12] Vitalik Buterin, Ethereum: A Next--Generation Smart Contract and Decentralized

Application Platform, 2013, http://ethereum.org/ethereum.html

[13] Paul Sztorc, Peer--to--Peer Oracle System and Prediction Marketplace,

2015, http://bitcoinhivemind.com/papers/truthcoin--whitepaper.pdf

[14] PriceFeed Smart Contract, 2016, http://feed.ether.camp/

[15] V. Costan and S. Devadas, Intel SGX Explained, 2016,

https://eprint.iacr.org/2016/086.pdf

[16] E. Shi. Trusted Hardware: Life, the Composable Universe, and Everything. Talk at the DIMACS Workshop of Cryptography and Big Data, 2015

[17] Ahmed Kosba et al., Hawk: The Blockchain Model of Cryptography and

Privacy--Preserving Smart Contracts, 2016,

https://www.weusecoins.com/assets/pdf/library/Hawk%20--%20The%20Blockchain%20Model%

2 0of%20Cryptography%20and%20Privacy--Preserving%20Smart%20Contracts.pdf

[18] Iddo Bentov and Ranjit Kumaresan, How to Use Bitcoin to Design Fair Protocols, 2014,

https://eprint.iacr.org/2014/129.pdf

[19] Marcin Andrychowicz et al., Secure Multiparty Computations on Bitcoin, 2013,

https://eprint.iacr.org/2013/784.pdf

[20] Ranjit Kumaresan and Iddo Bentov, How to Use Bitcoin to Incentivize Correct

Computations, 2014, https://people.csail.mit.edu/ranjit/papers/incentives.pdf

[21] Aggelos Kiayias, Hong--Sheng Zhou, and Vassilis Zikas, Fair and Robust

Multi--party Computation Using a Global Transaction Ledger, 2016,

http://link.springer.com/chapter/10.1007%2F978--3--662--49896--5_25

[22] Guy Zyskind, Oz Nathan, Alex Pentland, Enigma: Decentralized Computation Platform with Guaranteed Privacy, 2015, http://enigma.media.mit.edu/enigma_full.pdf

[23] Joseph Bonneau et al., On Bitcoin as a public randomness source, 2015,

[24] https://en.bitcoin.it/wiki/Category:History

[25] https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle.

pdf

[26] https://github.com/bitcoinbook/bitcoinbook

[27] https://github.com/ethereum/wiki/wiki/White-Paper

[28] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, https://www.bitcoin.org/bitcoin.pdf

[29] 《区块链社会解码区块链全球应用与投资案例》龚鸣 2016

[30] David Johnston et al., The General Theory of Decentralized Applications, Dapps, 2015, https://github.com/DavidJohnstonCEO/DecentralizedApplications

[31] Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, http://ethereum.org/ethereum.html

[32] Paul Sztorc, Peer-to-Peer Oracle System and Prediction Marketplace, 2015, http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf

[33] PriceFeed Smart Contract, 2016, http://feed.ether.camp/

[34] Nxt, 2013, http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt

[35] http://chainb.com/?P=Cont&id=2863

[36] http://chainb.com/?P=Cont&id=2856

[37] http://www.bochk.com/dam/bochk/desktop/top/aboutus/pressrelease2/2016/20161128_01_Press_Release_SC.pdf

[38] http://tech.sina.com