Bitcoin Hot

回归去中心化的支付系统

目　录

前言

我们很荣幸，生活在当下一个区块链技术蓬勃发展、高度繁荣的新时代。区块链，作为一项开创性技术，可以让价值在分布式网络上存储和交易。它的出现，带领人类步入了一个打破时间空间和遗留系统的限制、具有安全保障的交易新时代。区块链主要解决交易的信任和安全问题，因此它针对这个问题提出了四个技术创新：

第一个叫分布式账本，就是交易记账由分布在不同地方的多个节点共同完成，而且每一个节点都记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证。

跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。

没有任何一个节点可以单独记录账本数据，从而避免了单一记账人被控制或者被贿赂而记假账的可能性。也由于记账节点足够多，理论上讲除非所有的节点被破坏，否则账目就不会丢失，从而保证了账目数据的安全性。

第二个叫做非对称加密和授权技术，存储在区块链上的交易信息是公开的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。

第三个叫做共识机制，就是所有记账节点之间怎么达成共识，去认定一个记录的有效性，

这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。

区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。

以比特币为例，采用的是工作量证明，只有在控制了全网超过 51%的记账节点的情况下，才有可能伪造出一条不存在的记录。当加入区块链的节点足够多的时候，这基本上不可能，从而杜绝了造假的可能。

最后一个技术特点叫智能合约，智能合约是基于这些可信的不可篡改的数据，可以自动化的执行一些预先定义好的规则和条款。以保险为例，如果说每个人的信息（包括医疗信息和风险发生的信息）都是真实可信的，那就很容易的在一些标准化的保险产品中，去进行自动化的理赔。

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，从此人们开启了比特币网络作为一种点对点的价值交换网络繁荣发展的时代。

点对点价值传输　络的出现有其历史必然性，　Satoshi 则是加速这个历史进程的　。从上个世纪 80 年代，TCP/IP 协议的开发，到 90 年代，　页浏览器的应　和服务器的应　，直到今天，互联　技术从不同侧　和维度改变了数据交换的模式和　类的　活。互联　技术的发展得益于基础设施的完善，从早期的 信息　速公路（Information Super Highway ）

和各种智能终端的普及，这些也构成了互联　OSI 七层模型中，应　层　限拓展的基础。

在互联　的各种协议栈中，我们　的较多有 TCP/IP，HTTP，HTTPS，FTP，TELNET，SSH，SMTP，POP3 等　络层，传输层，应　层的协议，并且借助这些协议，我们已经较完美了搭建了各种各样的互联　服务。但是如果我们深思，我们会发现，在　特币　络出现之前，我们　直　法互联　上　，在不借助于第三　的情况下，较好的进　点对点的价值的转移和传输。其实我们并不是缺少　种特定的　法，　是缺少基于信息　速公路（Information Super Highway）的价值　速公路（Value Super Highway），以及如何实现 Value Super Highway 的 Value Transfer Protocol（VTP 协议），　特币　络则是运　于 信息　速公路上　的 第　个 VTP 协议。

比特币，作为一种数字资产，在经历了漫长岁月的长足发展和不断进步后，现已广泛被世界各个经济领域所了解和接受，并将逐步改变整个世界的经济格局。现如今，比特币的价值已经超过三千美元一个，人们称它为：数字黄金。可见，随着高速发展和日益剧增的交易量，比特币交易成本急剧提高，想要拥有一枚比特币，已经成为一种奢求。

我们希望人人都能拥有比特币，人人都能感受到这个新技术革命带给我们的技术繁荣。我们渴望出现一种新型的数字货币，它能够不同于比特币，取而代之的是拥有更大的供应量，更经济的交易成本，以及更快的交易速度，更重要的是，它能被我们所获得。因此，比特热点（BTH）带着这个使命诞生了。

介绍

比特热点（BTH）是比特币的分叉，它在预定区块高度 498848 新的链被创建，原始比特币（BTC）区块链继续保持不变。这种新的加密货币在自己的“比特热点”链上运作，采用新型的 Pow 算法，拥有更大的区块、更快的出块时间和更多的总供应量等特点。比特热点（BTH） 的出块时间比比特币快 10 倍，最大区块容量是比特币的 16 倍，主网每秒处理的交易笔数更是比特币的 160 倍，它的出现有效的解决了拥堵的问题，提升了交易的速度，被众多信仰者亲切的称为：“币四爷”（比特币网络的第四个分叉币）。为了打破比特币目前被 ASIC 矿机垄断算力的局面，我们对 PoW 算法进行了升级，推出全新的 BtHash 算法，能够让普通用户用 CPU 和 GPU 参与挖矿，回归比特币去中心化的初衷。让对比特币有兴趣的人都可以参与到其中来，促进比特币社区的发展，让比特币回归去中心化的本质，建立起广泛的应用价值，让人人都能参与和体验到比特币带来的利益和好处。采用新算法的比特热点(BTH)前期将只能用钱包挖矿，GPU 挖矿程序会在主网上线以后逐步开放。

每一个比特币拥有者，都能够拥有相应的比特热点（BTH）。如何能够拥有比特热点（BTH）？首先，比特热点（BTH）的矿工在挖新的区块时对原有的比特币区块链将不受影响，作为比特币拥有者，你可以在比特热点分叉成功后按 1:100 分配相应数量的比特热点（BTH）；除此之外，人们还可以通过备份比特币钱包的私匙，到比特热点钱包分离获得比特热点（BTH）；或者更为简单方便的方式，是把比特币充值到支持比特热点（BTH）的交易所，在交易所领取对应数量的比特热点。

初衷

2017 年 12 月 12 日，比特热点分叉“比特币区块链”，位于 498848 区块高度，此前比特币开发团队对比特币进行了必要的升级以及改进比特币最初的框架。比特热点开发商已经整合了一种新的工作证明算法，并将继续以更快的速度、更好的保护和更高的可扩展性增强原有的比特币功能。BTH 将赋予优于 btc 的新的特性(智能合约、闪电网络、BTHASH 算法、零知识证明、量子抗性等机制的增加)，成就比特币网络的更大价值，会使得 BTH 网络更高效、快捷、可靠、更低成本使用，回归比特币去中心化的本质，从而打造真正适用于未来社会的比特币网络。

比特热点将区块大小限制做了提升，这是大规模的链上缩放方法的一部分，目的是为更高的交易存储创造足够的容量，使其交易能力增加，最终目标是提高整个区块链的事务确认速度，交易的速度比它之前的任何比特币链都快。

BTH 的目标是促进比特热点被世界各地所广泛使用，增强无银行人士使用比特热点为自己和家人创造财富的能力。 比特热点（BTH）作为新兴经济体使用的第一种加密货币，它可用于日常交易。比特热点的总量为 2100000000 枚，意味着降低了新参与的成本，降低了必要的门槛。不管可伸缩性如何，链的强大程度取决于它的共识，比特热点使用了一种算法，使得单个实体在处理能力上拥有更大的区块、更快的出块时间和更多的总供应量。

硬分叉

在区块链中，硬分叉是对密码协议的更改，它会导致与以前版本的永久差异。当发生此更改时，所有用户都必须决定是否采用新协议(分叉到新链)或继续支持旧协议。如果在旧链上保留了足够多的用户，那么就会存在两个区块链，这些区块链具有它们之前的相同历史事务。但运行在具有自己独特历史、节点和协议的单独链上。比特现金(BCH)和比特热点(BTH)都是从最初的比特币链中创建的。

硬分叉的具体案例，在 2013 年 3 月 12 日，当时是 bitcoin qt 0.8.0 版本软件发布了，0.8 版本采用了一种新的数据库。有的矿工节点升级了新的版本，有的矿工还继续使用 bitcoin qt0.7 旧的版本软件。双方各自生产区块，但新数据库生产出的区块被旧版本节点拒绝掉。具体的原因是旧的数据库对超过 800Kb 的区块有时不接受。因此在区块高度 225430 比特币区块链分成了两条链，结果导致了比特币区块链产生两条链，一条是包含大于 800kb 区块的链，另一条是拒绝承认这些包含更大区块的链，这就发生了硬分叉。当时是采用新版本的矿工放弃了他们挖的链，退回到旧版本上继续挖矿。

这次硬分叉是一次意外，是新版本的软件出了 bug，导致采用旧软件的节点拒绝验证新软件节点生产的区块。但硬分叉的成因就是采用旧软件版本的节点拒绝验证采用新软件版本的节点生产的区块，然后双方各自挖矿。

在 2015 年 7 月 4 日比特币区块链在区块高度 363731 发生一次硬分叉。当时是 Bitcoin Core 开发者往新版本的 Bitcoin Core 0.10.0 添加了 BIP 66。这本来是一起软分叉的修改，但是比特币软分叉并非万无一失：若大家不能够认同本质不同的数据结构，则当有节点不认同现有的交易或区块时候，比特币软分叉就会向着硬分叉的方向发展。例如 Bip66 软分叉终

于演变为比特币硬分叉。在比特币网络上主要矿池都使用了 0.10 版本的软件时，但有一个矿池 BTC Nuggets 没有升级，导致 BTC Nuggets 挖出来的两个区块其他矿工拒绝掉，然后双方就各自挖矿延续自己认为是正确的区块链，由此产生硬分叉，分成了两条链。

随后 bitcoin.org 发布公告，呼吁矿工升级到 bitcoin core 0.10.2 版本来消灭分叉。这也是一次意外，硬分叉的成因是采用新软件版本的节点拒绝验证采用旧软件版本的节点生产的区块，然后双方各自挖矿。

BTH 区块链的应用

随着大批区块链项目的涌现和衰落，区块链的应用成为了项目是否能够长期发展的关键。而一项新技术能否最终落地，最关键的一个要素仍然是适合的应用场景。区块链技术应用场景应该遵循四大原则：

一、多信任主体：区块链是信任机器，应用环境最好是相互之间没有天然信任关系，需要通过区块链来搭建信任。反之，如果双方是强信任关系，或已有完善的制 度保障，使用区块链的必要性就不大。

二、多方协作：如果该场景协作方多，对账成本高，区块链底层的共享账本之上搭建的智能合约能够降低对账成本，从而提升效率。

三、中低频交易：区块链目前的并发性和扩展性还不足以应用于大规模高频交易，比如股票交易所。

四、商业逻辑完备：区块链节点之间一定要有完备的商业逻辑，形成多赢局面，参与者才有动力使用整条区块链。

BTH 区块链将充分利用技术优势，对应用场景进行整合并统一进行管理，形成多共识应用场景生态。此项技术将在各大平台领域都能得到充分的应用和落地。典型的技术构成包括共识算法、P2P 通讯、密码学、数据库技术和虚拟机，这也构成了区块链不可或缺的核心能力：

- 共有数据（源自共识算法）：参与区块链的各个主体通过合约的决策机制自动达成共识，分享同一份可信的数据账本；分布式（源自 P2P 通讯），实现点对点信息传输；

- 数据的隐私性与安全性（源自密码学），通过公私钥、哈希算法等密码学工具， 实现各主体身份和共有信息的安全；

- 数据存储（源自数据库技术和硬件存储计算的发展）：随着时间的累积，区块链 的大小也在持续上升，硬件的存储计算能力使得多主体间同时存储相同数据成为可能；

- 数字化合约 /DApp（源自虚拟机技术）：将生成的跨主体的数字化智能合约写入区块链系统，通过预设的出发条件，驱动执行。

特征

分布图	比特币（BTC）	比特现金（BCH）	比特热点（BTH）
SUPPLY	21MIL	21MIL	2.1BILLION
分配	矿业	矿业，自称	矿业，自称
名算法	SHA256(ASIC)	MSHA256(ASIC)	BTHash
BLOCKTIME	10 分钟	10 分钟	1 分钟
MAX BLOCKSIZE	1MB(2-4MB)	8MB	16MB
BLOCKCHAIN SIZE	~145G	~135G	~158G
难度调整	2 周	2 周+EDA	DYNAMIC
MAX TX/天	~1.2 MIL	~4.8 MIL	~96 MIL
SEGWIT	是	没有	是
重播保护	不必要	是	是
ANTI QUANTUM HASH	没有	没有	是
AMOUNT 已加密	没有	没有	是
LIGHTENING NETORK	没有	没有	是
SMART CONTRACT	没有	没有	是
成立时间	2009	2017 年 8 月	2017 年 12 月

- 闪电网络

比特热点将区块大小限制提高到 16MB，这是大规模链上缩放方法的一部分。现在有足够的能力处理每个人的交易。交易能力块将增加五倍，最终目标是提高整个区块链的事务确认速度。在闪电般的交易中，高稀释的交易费用，以及比特热点的区块链是其他主要比特币分叉的 10 倍，优先考虑信任、可访问性和“可命令性”。

虽然有人担心大型区块可能会迅速增加区块链的总规模，但目前每个区块中包含的交易数量仍远未达到块状尺寸。在将来的体积增加的情况下，诸如切分这样的附加机制已经被考虑来减少存储巨大的块链大小的问题。

比特热点降低了交易费用和参与成本：BTH 总量是 BTC 的 100 倍，从而降低了参与成本。BTH 改善了比特币定价过高，增加了 BTH 的总供应量，降低了价格。这种供应变化增加了流通，并有助于强调在小企业和微型交易中使用 BTH。 比特热点交易费用相对较低，是一个安全和私人的区块链以及“可支配的硬币价格”，非常适合进行日常交易。

- 防重播保护

当 BTC 链上的有效事务在 BTH 链上“重放”时，就会发生所谓的重放攻击。虽然这两条锁链都分叉了。为了防止这种情况，BTH 的事务格式已经更改，因此 BTC 事务不能被误认为是有效的。

- 智能合约

智能合约是区块链被称之为“去中心化的”重要原因，它允许我们在不需要第三方的情况下，执行可追溯、不可逆转和安全的交易。未来，所有的契约型的约定都实现智能化，利用智能合约可以保障所有约定的可靠执行，避免篡改、抵赖和违约。

通常人们不会自己写字节码，但是会从更高级的语言来编译它，例如用 Java，之后将按照社区选举逐步部署 Nodejs 和 Python 类似的通用语言。这些通用编码语言确实给区块链的功能性提供了指引，因此代码可以很容易与它进行交互，例如转移密码学货币和记录事件。代码的执行是自动的：要么成功执行，或者所有的状态变化都撤消。这是很重要的，因为它避免了合约部分执行的情况。在区块链环境中，这尤为重要，因为没有办法来撤消执行错误所带来的不好的后果（而且如果对手不配合的话，根本就没有办法逆转交易）。

基于区块链的智能合约不仅能发挥智能合约低成本高效率的优势，而且可以避免恶意行为对合约的正常执行的干扰。将智能合约以代码化的形式写入区块链中，利用区块链技术实现数据存储、读取及执行过程可追踪透明化且不可篡改。此外利用区块链的共识 算法构造的状态机系统能使智能合约高效的运行。

智能合约的功能组件：

A 开发运行环境，包括：

- 提供编程语言支持，必要时可提供配套的集成开发环境；
- 支持合约内容静态和动态检查；
- 提供运行载体支持，如虚拟机等；
- 对于与区块链系统外部数据进行交互的智能合约，外部数据源的影响范围应仅限 于智

能合约范围内，不应影响区块链系统的整体运行。

B 存储环境，包括：

- 防止对合约内容进行篡改；
- 支持多方共识下的合约内容升级；
- 支持向账本中写入合约内容。

除 BTH 作为比特币区块链的分叉自然要植入比特币不具备的智能合约，BTH 智能合约包含了有关交易的所有信息，只有在满足要求后才会执行结果操作。智能合约和传统纸质合约的区别在于智能合约是由计算机生成的。因此，代码本身解释了参与方的相关义务。智能合约根据逻辑来编写和运作。只要满足输入要求，也就是说只要代码编写的要求被满足，合约中的义务将在安全和新人的网络中得到执行。

使用 BTH 智能合约，主要优势包括在处理文档时的更高效率，这是因为其采用完全自动化的流程，不需要任何认为参与，只要满足智能合约所列出的要求即可。结果只会更节省时间，降低成本，交易更准确，且无法更改。此外，BTH 智能合约能去除第三方干扰，进一步增强了网络的去中心化。

工作证明算法

中本聪(Satoshi Nakamoto)设计了比特币的采矿系统，将其作为多数决定的一种方式。

BTH 决定使用 SHA-256 作为这一工作证明的算法，该算法工作了几年。然而，随着比特币的普及，矿业也变得越来越有竞争力。 我要应用专用集成电路(ASIC)的发展现在意味着任何能够访问最新的采矿硬件的人都可以轻松地超过传统的 CPW 矿工。

为了保持比特币的分散化，必须实现一种新的挖掘算法，能够抵制硬件制造商试图超越传统矿商的企图。

为了恢复公平的开采实践，比特热点利用并改进了 x13 工作证明算法。这意味着，所有为比特币 sha-256 设计的 asic 现在都是完全无效的。

BTH 使用 x13，创建新的专用集成电路硬件变得非常复杂，降低了挖掘集中化的威胁。 x13 是专门为图形卡挖掘创建的,这是一种硬件标准，即可广泛获取，从而使采矿的竞争对一般用户来说是公平的。

钱包特征

比特热点核心钱包被编程来决定哪个区块链包含有效的交易。比特热点核心钱包用户只接受该区块链的交易，使之成为其他人想要使用的比特热点区块链。

- 完全验证

比特热点核心钱包确保它接受的每个区块和交易都是有效的，不仅提高了您的安全性，而且有助于防止矿工和银行控制比特热点。

- 更好的隐私

比特热点核心钱包提供独家隐私功能，任何人都很难将您与他人的交易联系起来。比特热点核心钱包比其他钱包使用更多的资源，但在大多数计算机和互联网连接上运行仍然很方便。

- 友好的用户界面

比特热点核心钱包有很多其他钱包没有的功能。但是如果你不需要它们，你可以在比特热点核心钱包上使用其他几个钱包，而不会失去比特热点核心钱包的安全和隐私利益。

如何获得比特热点

每个比特币拥有者都可以在比特热点分叉成功后按 1:100 分配比特热点。可以通过备份比特币钱包的私匙到的比特热点钱包分离获得比特热点，或者更为简单方便的方式是把比特币充值到支持比特热点的交易所，在交易所领取对应数量的比特热点。

比特热点团队

朱亮	是团队首席财务官（CFO）， 拥有西南财经大学工商管理硕士（MBA）证书，注册会计师证书，期货从业资格证书，证券基金从业资格等诸多含金量极高的证书。加上 10 年工作经验，成就了现在优秀首席财务官。具备较强的组织能力和活动策划能力，有极强的团队精神。极擅长公司财务管理、资本运作和公司治理，全面负责团队财务机构的日常管理工作，为团队决策提供财务支持
张恒	团队首席运营官（COO） 英国南安普顿大学 国际经济与贸易硕士毕业，拥有基金从业资格证书与证券从业资格证书。 留学期间曾担任海外投资经理，工作包括留学推荐与移民推荐，负责给客户推荐和引导海外房产，半年时间给公司带来业绩超过千万人民币。 对互联网，电商，数字货币，区块链各种风口有敏锐的嗅觉；属于天才型全手，能很好结合他人优势改进，发展自身核心，扬长避短；对数字货币，有深刻了解和各种运营经验，开发经验。 2014 年开始关注并投资比特币。先后从事各区块链项目的运营。是一名拥有资深经验的区块链行业精英

陈伟	团队首席技术官（CTO） 专注，谨慎是所有人对陈伟的第一印象，也是作为一名技术执行者的最高点评。 毕业于电子科技大学软件工程专业，曾任职华为技术开发。十余年工作经验，多家公司带领最高超过五十人的技术团队。精通 JAVA、PHP、Python、C、NodeJS、Shellbash、C++、H5 等核心开发语言。熟悉 JavaDubbo 分布式框架、MVC、PHPYii、JavaTigase 开源 IM 框架。具备 Linux、Windows、IOS、安卓、Mac 等系统环境实际开发经验。 2013 年接触并投资比特币，同时专注区块连钱包技术、熟悉 Bitcoin、Ethereum、Zcash 等开源区块链系统细节设计，曾参与多个数字货币相关游戏设计，在 PoW，PoS，DPoS 等区块链共识算法研究上取得相当大的成绩，是一名极其宝贵的区块链技术人才。
高玉宇	高级产品经理 原知名互联网公司高级产品经理，曾先后在 Remark holdings，阿里等公司负责产品设计工作。 深耕互联网行业，在 C 端和 B 端产品上均有丰富的产品经验
舒新	用户服务部经理 东京大学金融专业硕士，曾在某国内知名通信公司海外市场担任技术工程师并负责项目管理。精通 日语，英语，可听说韩语，擅长不同文化间的沟通和跨国技术项目拓展。
杨忠诚	服务端高级工程师 后端开发工程师，有丰富的数据采集开发、数据建模及区块链技术经验，实现了组件化的数据采 集服务。

路线

比特热点的目的是帮助更多的人熟悉去中心的未来价值。比特热点将特别关注各类区块链直接受益人群，例如金融交易、隐私保护、安全、溯源等领域的发展。我们的目标包括促进比特热点在世界各地的广泛使用，增强无银行人士使用比特热点的能力。第二，为自己创造财富，将比特币热点确立为新兴经济体的头号加密货币，并使比特热点可用于日常交易

我们寻求实现我们的最终目标，即比特热点成为“比特币”，为全球金融服务提供更好的解决方案。

- 2017

比特热点诞生于比特币块高：498848 的硬分叉处。比特热点主板、钱包、节点代码和 api 发布

- 2018

- Bitcoin Hot 钱包
- 构建 BTH 应用生态环境

- 2019

- 闪电网络
- 智能合约
- 完善通证经济模式
- 研发零知识证明
- 研发完善抗量子算法
- 进一步完善比特热点的生态以及功能，不断为区块链发展做贡献

启动和运营费用

- 早期开发
- 主网和钱包的开发挖矿
- 程序开发节点和服务器构建
- 系统安全维护
- 社区建设
- 全职雇员定期举办活动
- 推行社区奖励计划
- 法律法规
- 为未来全球遵约问题谋划

预挖

我们在项目主网上线时，预挖了百分之一，此费用完全归属于共建者基金用于扶持将来能为整个生态提供帮助的团队（技术、流量、内容、服务、推广等），使得生态更加完善，更加完整的生态能吸引更多的流量进入，可以促进项目的进一步的发展，以此形成良性递归。

结尾

我们提出了一种新的电子货币交易系统，其目的是使每个人都能获得和使用数字货币，而不论其经济地位、原籍国或级别如何、才能。由于闪电般的快速交易，高度稀释的交易费用，以及 10 倍于其他领先的比特币分叉的供应量，我们的区块链优先考虑信任。在一个许多人被迫为金钱服务的时代，比特热点是一种为人民服务的货币。我们能帮助解决现有的拥堵

问题。以有利于用户的交易速度，节约时间。为了使新兴市场最大化采用比特热点，我们确定了比特热点基金会应采取的几个重要行动步骤。BTH 的薪酬计划将包括一系列的业务，包括社区参与、教育倡议、BTH 支付国际市场和在线基础设施。BTH 将继续努力使电子货币更容易获得，可用的。