****

**HiveChain**

**蜂巢数字资产系统**

**人人都可以发行的数字资产**

**目录**

区块链简史

区块链的特征

区块链的工作流程

Hivechain-蜂巢

共识机制

蜂巢区块链共识机制—授权股权证明机制(DPOS)

关于蜂币

蜂币的分发机制

用户发行资产

资产交易

蜂巢区块链智能合约  
关于智能合约

HSC-蜂巢区块链智能合约

蜂巢智能合约（HSC）工作原理

蜂巢智能合约（HSC）的构建及执行

蜂巢生态系统及应用场景

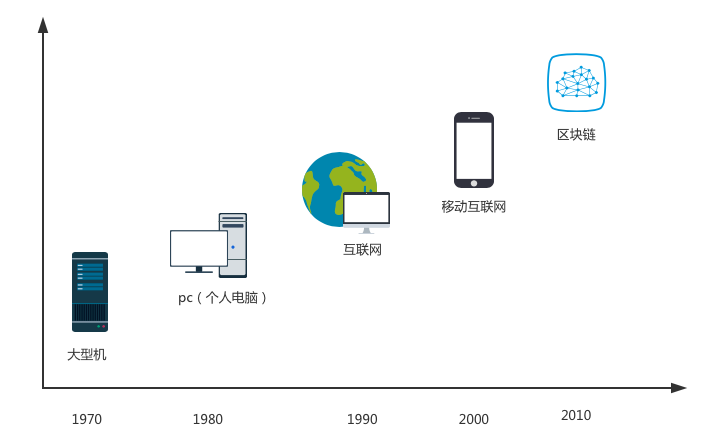
**区块链简史**

2008年11月1日，某秘密讨论社区“密码学邮件组”出现一个新帖子：“我正在开发一种新的电子货币系统，采用完全点对点形式，而且无须授信第三方介入。”该帖署名Satoshi Nakamoto（塞托西中本聪）。

2009年1月3日，中本聪发布开源第一版比特币客户端，宣告比特币的诞生，产生第一批比特币的区块就叫做“创世区块”（Genesis block）。

随着比特币的诞生，区块链技术得以公布于众。但是比特币的区块链技术并不等于区块链技术，毕竟比特币的区块链是为比特币体系的设计而开发的。

区块链技术不是一种单一的技术，而是多种技术整合的结果，包括密码学，数学，经济学，网络科学等，这些技术以特定的方式组合在一起，形成一中新的区中心化数据记录与存储体系，其概念为；区块链是一个去中心化的共享分布式数据库，该数据库由一串使用密码学方式产生的数据区块有序链接而成，区块中包含有一定时间内产生的无法被纂改的数据记录信息。



五次计算范式创新

**区块链的特征**

1. **去中心化**

去中心化是区块链最基本的特征，意味着区块链不再依赖于中央处理节点，实现了数据的分布式记录，存储和更新。

1. **透明性**

区块链系统的数据记录对全网节点是透明的，数据记录的更新操作对全网节点也是透明的，这是区块链系统值得信任的基础。

1. **开放性**

区块链系统是开放的，除了数据直接相关各方的私有信息被加密外，区块链的数据对所有人公开。

1. **自治性**

区块链采用基于协商一致的规范和协议，使整个系统中的所有节点能够在去信任的环境自由安全的交换数据，记录数据，更新数据，把对个人或机构的信任改成对体系的信任，任何人为的敢于将不起作用。

1. **信息不可纂改**

区块链的信息一旦经过验证并添加至区块链后，就会得到永久存储，无法更改。

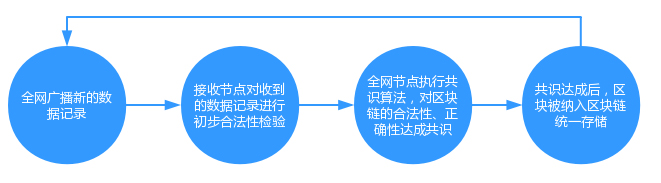
**6.匿名性**

区块链技术解决了节点间的信任的问题，因此数据交换甚至交易均可在匿名的情况下进行。

**区块链的工作流程**

1. 发送节点将新的数据记录向全网进行广播
2. 接收节点对收到的数据记录信息进行检验，比如记录信息是否合法，通过检验后，数据记录将被纳入一个区块中。
3. 全网所有接收节点对区块执行共识算法。
4. 区块通过共识算法过程后被正式纳入区块链中存储，全网节点均表示接受该区块，而表示接受的方法，就是将该区块的随机散列值视为最新的区块散列值，新区块的制造将以该区块为基础进行延长。

节点始终都将最长的区块链视为正确的链，并持续以此为基础验证和延长它。



区块链工作流程

**Hivechian-蜂巢**

**人人都可以发行的数字资产**

**基于区块链技术，将现实世界资产映射于网络世界形成价值的发行，价值传输，加密登记和查验核实的数字资产网络协议**

**共识机制**

区块链要成为一个难以攻破的，公开的，不可纂改数据记录的去中心化诚实可信系统，需要在尽可能短的时间内做到分布式数据库记录的安全，明确及不可逆，提供一个最坚实且去中心化的系统。在实践中，该流程分为两个方面：一是选择一个独特的节点来产生一个区块；而是使分布式数据记录不可逆。实现上述流程的技术核心就是：共识机制。共识机制是区块链节点就区块信息达成全网一直共识的机制，可以保证最新区块被准确添加到区块链，节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。

目前主流共识机制：

**工作量证明（POW）**:工作量证明机制其实在社会上应用广泛。例如，毕业证，技师证，学位证等证书就是工作证明，拥有证书即表明在过去付出了努力。挖矿为整个系统的运转提供原动力，挖矿有三个重要功能：一是发行新的货币；二是维系系统的支付功能，三是通过算力保障系统安全。但它的缺点也非常明显，一是算力的消耗和浪费，区块确认时间较长，处理交易频率过低；二是算力集中化凸显。

**权益证明（PoS）**：简单来说，POS就是一个根据持有货币的量和时间，进行利息发放和区块产生的机制。POS面临的问题是如何通过及时而高效的方法达成共识，POS机制并未使区块变得越来越安全而不可逆，因为最终区块链的区块产生权掌握在账户余额最多的少数节点手中。

**除上述机制外，还有工作量+权益证明（POW+POS），恒星共识协议（SCP），改进型实用拜占庭容错机制（PBFT）和Pool验证池机制等共识机制。**

**蜂巢区块链共识机制—授权股权证明机制(DPOS)**当使用去中心化自治公司(Decentralized Autonomous Company, DAC)这一说法时，去中心化表示每个节点按其持币比例拥有影响力，51%节点投票的结果将是不可逆且有约束力的。其挑战是通过及时而高效的方法达到51%批准。

为达到这个目标，每个节点可以将其投票权授予一名代表。获票数最多的前100位代表按既定时间表轮流产生区块。每名代表分配到一个时间段来生产区块。所有的代表将收到等同于一个平均水平的区块所含交易费的10%作为报酬。如果一个平均水平的区块含有100蜂币作为交易费，一名代表将获得1枚作为报酬。

网络延迟有可能使某些代表没能及时广播他们的区块，而导致区块链分叉，但是这种情况发生的概率很小，因为制造区块的代表可以与制造前后区块的代表建立直接连接。建立这种与你之后的代表(也许也包括其后的那名代表)的直接连接是为了确保你能得到报酬。

该模式可以每30秒产生一个新区块，并且在正常的网络条件下区块链分叉的可能性极其小，即使发生也可以在几分钟内得到解决。  
  
1.0 **成为一名代表**

成为一名代表，你必须在蜂巢区块链网络上注册你的公钥，然后分配到一个32位的特有标识符。然后该标识符会被每笔交易数据的“头部”引用。  
  
1.1 **授权你的选票**

每个钱包有一个参数设置窗口，在该窗口里用户可以选择一个或更多的代表，并将其分级。一经设定，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。一般情况下，用户不会创建特别以投票为目的的交易，因为那将耗费他们一笔交易费。但在紧急情况下，某些用户可能觉得通过支付费用这一更积极的方式来改变他们的投票是值得的。   
  
1.2 **保持代表诚实**

每个钱包将显示一个状态指示器，让用户知道他们的代表表现如何。如果他们错过了太多的区块，那么系统将会推荐用户去换一个新的代表。如果任何代表被发现签发了一个无效的区块，那么所有标准钱包将在每个钱包进行更多交易前要求选出一个新代表。  
  
1.3 **解决区块链分叉**

和工作量证明系统及其他股权证明系统一样，最佳区块链是最长的有效区块链。任何时候，一名代表错过签发一个区块的机会，该区块链将比潜在竞争对手短。只要在你的交易被写入区块后的100个区块中的51%被生产出来了，那么你就可以安全地认为你在主区块链上。  
在防止区块链分叉所导致的损失方面，最重要的事是在事发后第一时间得知消息。因为代表们通过生产区块得到很好的报酬，他们将保持接近100%的在线时间来防止因被投票罢免而损失收入。你可以安全地认为如果在过去的10个区块中，有一两个区块错过生产，则互联网的某些部分可能正发生连接问题，那么用户应该对此特别警觉并要求额外的确认数。如果10区块中有超过5个错过生产，那么这意味着你很可能在一条支链上，因此应该停止所有交易，直到分叉得到解决。  
以一种及时的方式(少于5分钟)简单地发现并警示用户网络分叉，是可以最小化潜在损失的非常重要的能力。而知道你是否正处在一条支链上则更为重要。  
  
2.0 **100名代表是去中心化的吗？**

因为去中心化已经成为一个流行术语，所以其定义很难完全固定。我们将自由市场看作去中心化的基本形式，并将对进入自由市场设置障碍看作是所有中心化的基础。像任何事物一样，去中心化有程度之分，所以我们可以把授权股权证明机制与比特币的去中心化程度进行对比。  
  
2.1 **比特币**

比特币系统目前正以授权工作量证明(Delegated Proof of Work, DPOW)为基础而运行，因此有大约10名代表控制了绝大多数的哈希算力。在那些为其竞争而能使用规模经济进行无收益挖矿的人手中，哈希算力本身就是中心化的。最后，工作量证明机制为进入市场设置障碍，使得“在职”的区块制造者无法轻易被取代。与比特币系统相比，蜂巢区块链DPOS在区块生产方面至少去中心化了10倍，并且也许在市场竞争方面去中心化了无数倍。  
尽管在哈希算力方面有一定量的去中心化，当想到掌控比特币系统的股东(比特币持有者)所持股份的占比，我们认为比特币系统是最中心化的。如果你考虑使用比特币体系的用户总数，其中参与挖矿的人很可能少于百分之一。  
  
  
3.0 **攻击**

一般而言，网络必须抵御两种类型的攻击：拒绝服务攻击和双重支付攻击。一个攻击者通过不把一些或全部的交易加入总账来进行拒绝服务攻击。这种攻击可以由任何拥有51%网络(无论比特币、未来币或其它)的人进行。而利用在网络正试图达成共识时的短期优势，可以进行双重支付攻击。  
为抵御这些攻击，网络必须使51%的股东尽快达成协议。  
  
3.1 **防止排除交易**

拥有全部经股东投票选出的100名代表，并且按要求轮流生产区块，意味着任何一笔由至少1%的股东批准的交易能够在30分钟内加入总账。这意味着没有代表可以通过将投票支持其他代表的交易排除在外来获取利益。  
  
3.2 **将一些代表的权力中心化**

与其所被授权的投票权无关，这前100人所获得的权力权重是相同的，每名代表都有一份相等的投票权。因此，无法通过获得超过1%的选票而将权力集中到一个单一代表手上。  
个人或者组织控制区块链的多名代表是有可能的。但是这个过程将需要欺骗很大比例的股东数去支持“傀儡”。  
即使可以建立这51%傀儡，他们扰乱网络的能力仍将是有限的、能够被快速识别快速纠正的。没有工作量证明机制设置的进入障碍，占据多数的诚实用户会把攻击鉴别出来，然后将代码分叉并无视攻击者生产的区块。这种攻击可以扰乱网络，但不会是致命的。  
  
3.3 **针对代表的分布式拒绝服务攻击(DDOS)**

因为只有100名代表，   可以想象一个攻击者对每名轮到生产区块的代表依次进行拒绝服务攻击。幸运的是，由于事实上每名代表的标识是其公钥而非IP地址，这种特定攻击的威胁很容易被减轻。这将使确定DDOS攻击目标更为困难。而代表之间的潜在直接连接，将使妨碍他们生产区块变得更为困难。  
  
4.0 **基于交易的股权证明机制(TaPOS)**

代表制是一个短时间内达成坚固共识的高效方式，而TaPOS为股东们提供了一个长效机制来直接批准他们的代表的行为。平均而言，51%的股东在6个月内会直接确认每个区块。而取决于活跃流通的股份所占的比例，差不多10%的股东可以在几天内确认区块链。这种直接确认保障了网络的长期安全，并使所有的攻击尝试变得极度清晰易见。  
  
5.0 **高质量的服务**

假设蜂巢区块链拥有100亿的市场总量，平均每年的交易费为0.25%，代表们合计获得所有交易费的10%，那么每名代表每年能获得25,000以使其节点保持在线。  
这是一个利润可观的角色，许多人将为获取它持续竞争。这意味着每个想要获得这份工作的人都会想方设法从拥有这份工作的人那里把它“偷走”。为做到这点，他们将对代表行为进行统计学分析，以找到对于标准算法的任何偏离行为。一旦找到这种偏离，他们就能有希望赢得一些选票。  
那些拥有这份工作的人，可能会全力以赴地证明他们正在按标准软件运行。他们越有效地证明其对区块生产的正直性，越有可能保住他们的工作。你可以想象开发者会很快制作出系统，代表们可以通过这些系统快速证明哪些交易得到了广泛的散播。  
事实上，市场竞争将产生用以证明代表们的正直性与可靠性的最具创造性的解决方案。让网络变得更安全的工作可以获得很多收益，而尝试绕轮网络则得不到什么好处。

**6.0 结论**

DPOS与TaPOS结合所产生的网络，其网络共识的可证明性将至少3倍于比特币、点点币及未来币网络。DPOS能够更快地达成共识，同时消除随机小股东带来小规模干扰的可能性。经济激励确保了代表们致力于证明他们有良好行为。

**这就是蜂巢区块链共识机制的核心思想。**

**这种共识机制的选择是蜂巢团队认为至今为止的最优选择，但不代表未来不会有所改进，正如以太坊对于其共识机制的改进一样。**

参考资料：(Delegated Proof-of-Stake ，DPOS)

**关于蜂币**

蜂币，英文Hivecoin，缩写HIC

蜂币共9600万枚，代表了蜂巢区块链的所有权和使用权。其中4800万枚蜂币在创世块中一次性被创设出来，并按一定的分配方案进行分配，剩余4800万枚伴随着每个新区块的生成而产生。最小单位即小数点后八位小数，不可增加，不可再分割。

**蜂币主要用途：**

* 投票产生记账人
* 投票决定蜂巢协议的重大事项
* 支付蜂巢区块链的记账费
* 支付蜂巢区块链的附加服务费
* 支付蜂巢智能合约服务费

**蜂币的分发机制**

蜂巢的每个区块生成时间为30秒，即每年产生1051200个区块；

第一年生产约1051200个区块，每个区块产生10枚蜂币；

第二年生产约1051200个区块，每个区块产生8枚蜂币；

第二年生产约1051200个区块，每个区块产生6枚蜂币；

···以此类推，每年递减2个蜂币，直至第6年递减至每个区块新生成1个蜂币；自此保持每个区块新生成1个蜂币直至蜂币总量到达9600枚，则停止伴随新区块生成蜂币。

蜂币代表蜂巢区块链上的持股权，每个区块的新生蜂币也将由蜂币的持股比例来分配，例如某用户持有96万枚蜂币，占蜂巢全网1%，则在第一年，该用户就能够每个区块获得2x10/100=0.2个，每天获得约576枚蜂币。

**创世块中的蜂币**

在创世块运行前蜂巢团队将按照一定的规则对蜂币进行分配。

约占总量10%的蜂币在2016年底被分配给蜂巢的早期支持者，获得了蜂巢团队的种子资金。

1500枚蜂币在第一轮的ICO分配给对蜂巢区块链支持与期望的参与者，具体见第一轮ICO细则。

剩余创世块蜂币将参与第二轮ICO的分配，及蜂巢区块链的推广宣传。

**用户发行资产**

任意用户均可发行资产。资产经过创设、分发两个步骤生成。创设后，资产登记在蜂巢区块链上但并未实际生成至地址；分发后，资产实际进入地址。

**资产交易**

交易是指蜂巢区块链协议中引起资产的权益或蜂巢块链协议的权益发生变化的事务。蜂巢区块链系统内设计了多种类型的交易，每一笔交易都包含输入列表、输出列表、签名列表，以及与交易类型相关数据。交易费用分为记账费和附加服务费，均以蜂币支付。

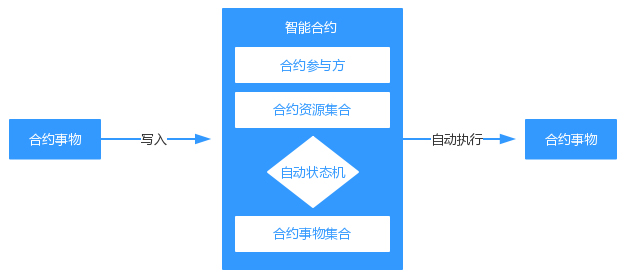
**蜂巢区块链智能合约**

如果说区块链1.0是以比特币为代表，解决了货币和支付手段的去中心化问题，那么区块链2.0就是更宏观的对整个市场去中心化，利用区块链技术转换许多不同的数字资产而不仅仅是比特币，通过转换创建不同资产的价值。区块链技术的去中心化账本功能可以被用来创建，确认，转移各种不同类型的资产及合约。

**关于智能合约**

智能合约是一套以数字形式定义的承诺，承诺控制着数字资产并包含参与者约定的权利与义务，由计算机系统自动执行。

数字形式意味着合约需要被写入计算机可执行的代码中，只要参与者达成协定，智能合约建立的权利和义务，就由一台计算机或者计算机网络执行

****

智能合约模型图

**HSC-蜂巢区块链智能合约**

蜂巢智能合约（hive smart contract简称HSC）系统就是将智能合约以数字化的形式写入蜂巢区块链中，由蜂巢区块链的技术特性保障存储，读取，执行整个过程透明可跟踪，不可纂改，同时由共识算法构建出一套状态机系统，使智能合约能够高效的运行。

**蜂巢智能合约（HSC）工作原理**

基于蜂巢区块链技术的智能合约包括事务处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约，而且事务的保存和状态处理都在区块链上完成。事务主要包含需要发送的数据，而事件则是对这些数据的描述信息。事务及事件信息传入智能合约后，合约资源集合中的资源状态会被更新，进而触发智能合约进行状态机判断，如果自动状态机中某个或某几个动作的触发条件满足，则有状态机根据预设信息选择合约动作自动执行。

合约系统根据事件描述信息中包含的触发条件，当满足触发条件时，从智能合约自动发出预设的数据资源，以及包括触发条件的事件；整个智能合约系统的核心就在于智能合约以事务和时间的方式经过智能合约模块处理，输出还是一组事务和事件；智能合约只是一个事务处理模块和状态机构成的系统，它不产生智能合约，也不会修改智能合约；它的存在只是为了让一组复杂的，带有触发条件的数字化承诺能够按照参与者的意志正确执行。

**蜂巢智能合约（HSC）的构建及执行**

基于蜂巢区块链的智能合约构建及执行分为如下几步

1. **0多方用户共同参与制定一份智能合约。**

1.1用户必须先注册蜂巢区块链系统用户，蜂巢返给用户一个公钥和私钥；公钥作为用户在蜂巢区块链上的账户地址，私钥作为操作该账户的唯一钥匙。

1.2两个以及两个以上用户根据需要，共同商定一份承诺，承诺中包含了双方的权利义务；这些权利义务以数字化的形式，编程代码语言；参与者分别用各自私钥进行签名，以确保合约的有效性。

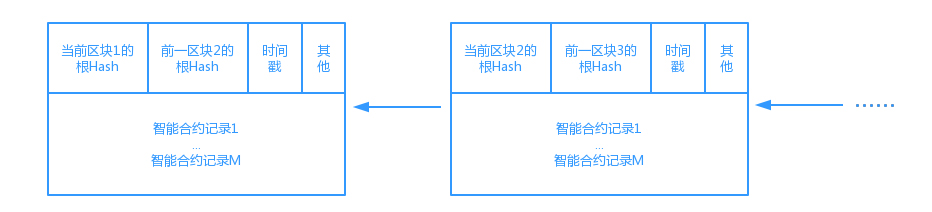
1.3签名后的智能合约，将会根据其中的承诺内容，传入蜂巢区块链网络中。

2.0**合约通过P2P网络扩散并存入区块链**

2.1合约通过P2P的方式在蜂巢区块链全网扩散，每个节点都会收到一份；蜂巢区块链中的验证节点会将收到的合约先保存到内存中，等待新一轮的共识时间，触发对该分合约的共识处理。

2.2共识时间到了，验证节点会把最近一段时间内保存的所有合约，一起打包成一个合约集合，并算出这个合约集合的hash值，最后将这个合约集合的hash值组装成一个区块结构，扩散到全网；其他验证节点收到这个区块结构后，会把里面包含的合约集合的hash值取出来，与自己保存的合约集合进行比较；同时发送一份自己认可的合约集合给其他验证节点；通过多轮的发送和比较，所有验证节点最终在规定时间内对最新的合约集合达成一致。

2.3最新达成的合约集合以区块的形式扩散全网；收到合约集合的节点，都会对每条合约进行验证，验证通过的合约才能最终写入蜂巢区块链中，验证的内容主要是合约参与者的私钥签名是否与账户匹配。



蜂巢智能合约区块链示意图

3.0**蜂巢区块链构建的智能合约自动执行**

3.1智能合约会定期检查自动机状态，逐条遍历每个合约内包含的状态机，事务以及触发条件；将满足条件的事务推送到待验证的队列中，等待共识，未满足触发条件的事务将继续存放在蜂巢区块链上。

3.2最新验证的事务会扩散到每一个验证节点，以普通区块链交易或事物一样，验证节点首先验证签名，确保事务的有效性；验证通过的事务会进入待共识集合，等大多数验证节点达成共识，事务会被成功执行并通知用户。

3.3事务成功后，状态机会判断所属合约的状态，当合约包括的所有事物都顺序执行完后，状态机会将合约的状态标记为完成，并从最新的区块中移除该合约；反之将标记为进行中，继续保存在最新的区块中等待下一轮处理，知道处理完毕；整个事务和状态的处理都由蜂巢区块链底层内置的智能合约系统（HSC）自动完成，全程透明，不可纂改。

虽然蜂巢团队投入了很大精力使代码编写起来更简便，比如说只需要几行代码就可以实现一些功能，但是写代码的方式还是很糟糕的用户体验，蜂巢团队也将致力于更加智能化一键式操作的研发中。

**蜂巢生态系统及应用场景**

**1.交易所**

**2.钱包**

**3.股权众筹转让交易、P2P借贷**

**4.商业积分、电子券、资产证券化**

**5.大宗商品交易**

**6.非上市公司股权交易中心、私募管理平台**