编写说明

区块链起源于[比特币](https://baike.baidu.com/item/比特币/4143690)，2008年11月1日，一位自称[中本聪](https://baike.baidu.com/item/中本聪/5740822)(Satoshi Nakamoto)的人发表了《比特币:一种点对点的电子现金系统》一文，阐述了基于[P2P](https://baike.baidu.com/item/P2P/139810)网络技术、加密技术、[时间戳](https://baike.baidu.com/item/时间戳/6439235)技术、区块链技术等的电子现金系统的构架理念，这标志着比特币的诞生。两个月后理论步入实践，2009年1月3日第一个序号为0的[创世区块](https://baike.baidu.com/item/创世区块/22448241)诞生。2009年1月9日出现序号为1的区块，并与序号为0的创世区块相连接形成了链，标志着区块链的诞生。

区块链是一个[信息技术](https://baike.baidu.com/item/信息技术/138928)领域的术语。从本质上讲，它是一个共享数据库，存储于其中的数据或信息，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征。基于这些特征，[区块链技术](https://baike.baidu.com/item/区块链技术/23686191)奠定了坚实的“信任”基础，创造了可靠的“合作”机制，具有广阔的运用前景。随着时代的进步，“区块链”已走进大众视野，成为社会的关注焦点。

目录

1. 行业分析

1.1区块链的概念

1.2区块链的发展趋势及投资前景

1.3中心化与去中心化

1.4智能合约

2、Hash Ahead平台

2.1Hash Ahead简介

2.2任务及愿景

2.3Hash Ahead的优势特点

3、Hash Ahead的技术架构

3.1网络层

3.2共识机制

3.3区块结构

3.4区块节点

3.4.1Hash Ahead节点

3.4.2节点验证

3.4.3节点奖励

3.4.4恶意节点行为及惩罚

3.5安全主链

3.6去中心化系统

1. Hash Ahead应用

4.1智能合约库

4.1.1Hash Ahead智能合约库简介

4.1.2智能合约审核

4.2分层确定性钱包

4.3Hash Ahead去中心化交易所

5、HAH发行机制

5.1HAH发行计划

5.2发行周期

5.3收益说明

5.4使用计划

6、发展战略

7、风险提示

8、免责说明

1、行业分析

1.1区块链的概念

区块链是一个[信息技术](https://baike.baidu.com/item/信息技术/138928)领域的综合术语。自2008年发展至今，集当今多种技术于一体，包括但不限于分布式帐本、共识机制、智能合约、P2P网络、非对称加密等。在每个区块链中，区块即信息块，信息以区块的形式进行集成、打包，并按照实际产生时间的先后顺序进行连接。

1.2区块链的发展趋势及投资前景

自2009年比特币网络运行以来，区块链各类技术进入了飞速发展的阶段，尤其是底层技术，自2017年以来发展势头明显。基于底层技术，金融领域、公共服务领域、公益慈善领域、供应链领域、物联网领域等不断进行B端、C端的场景落地尝试，DApp应用也不断涌现。区块链正式走进大众视野，成为社会的关注焦点，影响将不仅仅体现在经济上，还体现在文化和政治上。在未来，区块链的场景应用将不可估量。

1.3中心化与去中心化

对于去中心化，很多人认为去中心化就是不要中心。去中心化，不是不要中心，而是由节点来自由选择中心、自由决定中心。

中心化是中心决定节点。节点必须依赖中心，节点离开了中心就无法生存。在去中心化中，任何人都是一个节点，任何人也都可以成为一个中心。任何中心都不是永久的，而是阶段性的，任何中心对节点都不具有强制性。

1.4智能合约

智能合约程序不只是一个可以自动执行的计算机程序：它自己就是一个系统参与者。它对接收到的信息进行回应，它可以接收和储存价值，也可以向外发送信息和价值。这个程序就像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。

智能合约模型：它是运行在可复制、共享的帐本上的计算机程序，可以处理信息，接收、储存和发送价值。

1. Hash Ahead平台

2.1Hash Ahead简介

2.2任务及愿景

区块链概念自2008年底由匿名者中本聪提出后不断发展，由比特币到以太坊，智能合约的出现大量的应用开始浮现，可是这跟传统技术距离还是差天共地…

编程语言 - Go Language 2009年由Google 推出，至今占有率已达全球十大之一，箇中原因和代码库有很大关系，当程序员编程时每次也需要由零开始而不是从前人所作调用，一个复杂的程序何年何月才会出现？更莫说操作系统了！

Hash Ahead除了在智能合约库为程序员提供方便，更提供诱因让更多开发人员为智能合约发展打好基础，每当智能合约被调用时，使用者需付出（Force），而该智能合约的作者能得到部份奖励，吸引更多人开发出更实用更复杂的智能合约库供开发者调用，再复杂的应用甚至操作系统即将诞生，真正的区块链操作系统大门从此开启。

2.3Hash Ahead的优势特点

在区块链飞速发展的时代，无论是比特币还是以太坊，这些都是区块链技术中的佼佼者，但人们始终离打开区块链应用的大门还差一点。

在此之前，智能合约只是一种特殊协议，旨在提供、验证及执行合约。智能合约的执行效率低、开发人员的收益低、编写智能合约的成本过高，这已然成为智能合约的痛点，而Hash Ahead的智能合约库将打破现一观点。

3、Hash Ahead的技术架构

3.1网络层

Hash Ahead网络由运行Hash Ahead软件的节点构成 P2P 网络。整体网络架构由节点网络层作为核心构成，分为共识传输层、区块传输层、交易传输层，共识数据不会因区块和交易拥堵而影响传输效率，每层可以为独立的传输方案，层与层之间互不影响。

采用动态组合验证者和领导者节点的P2P网络，让领导者节点或验证者节点能最快速度接收区块等数据，传输效率高于非功能节点。

节点网络层由运行Hash Ahead核心节点程序的节点构成，节点之间同步校验区块和交易数据，并进行共识组织区块数据。其中共识层包含了共识机制，出块层包含出块机制，而交易层则负责交易数据。

3.2共识机制

共识机制是区块链必不可少的一部分。在共识机制方面，Hash Ahead为提高提案结束消息准确性和及时性，则由独立P2P网络传输该消息（与共识传输同P2P网络），提高提案者接收提案结束消息的及时性。（P2P网络分区：1、共识传输P2P网络，2、区块传输P2P网络，3、交易传输P2P网络），同时支链每秒的交易笔数(TPS, Transaction Per Second)能够高达百万，并且一笔交易最快500ms即可完成链上确认，足以满足当今数据交易频繁延迟低的应用场景。

3.3区块结构

主链和子链的主块之间有直接关联，即一个主块头中包含有上一个主块的块HASH，该关联可用于块的快速较验，只需要同步主块就可以完成较验。每天的边界区块头关联，只需下载每天的边界区块头，即可较验全链区块头的正确性，有利于轻节点等客户端快速全链较验。

主链和子链的主块关联前一天的主块HASH，只有一天边界的主块才有前一天的边界主块的块HASH，其他主块没有该参数，主要用于全链扫描较验使用，用于轻节点、轻钱包、数据裁剪等功能使用。

区块结构：包括区块头1，区块头2，区块体。区块头1包含区块编号，时间戳，前一区块HASH，前高度主块HASH（主块才有），前一天主块HASH（一天边界主块才有），区块头2HASH等等（块HASH由区块头1生成）。区块头2包含状态根HASH，交易根HASH，奖励交易，布隆过滤器，共识数据等等。区块体包含交易表。

全链所有历史区块，不需要节点全部存储，由存储节点分布式存储历史区块，一个存储节点只存储部分区块，并提供查询功能，存储节点提供存储和查询功能，可获取相应的收益，收益由区块奖励和查询费用组成，区块分布式存储功能解决了历史区块庞大的问题，功能节点（如轻节点、验证节点等）无须存储历史区块，降低节点的存储要求。

3.4区块节点

3.4.1Hash Ahead节点

节点指的是区块链网络中的计算机，包含手机，矿机和服务器等等。节点可分为“全节点”和“轻节点”，全节点就是拥有全网所有的交易数据的节点，轻节点则是只拥有和自己相关的交易数据节点。

Hash Ahead节点，在无交易时不生产区块，少同步，提高效率，减少空区块占用资源，同时出块奖励固定，选举后保障节点主能获取奖励。在交易量达到最大区块大小时，可立即生产区块，不受时间限制，交易上链速度更快，减小交易池压力。

Hash Ahead中验证节点和提案节点需要投票锁定后才能参与共识。投票后有初始锁定期（锁定期在10至30天），锁定期内TOKEN不能流动，锁定期后可以流动，锁定期后需要转出TOKEN，需要一段时间的等待期（一般为一天），防止作恶后立即逃跑问题。

同时节点自我投票有最小数量要求，超过小最数量才能成为一个验证节点或提案节点，系统有最小节点自我投票数量，但节点可以多自我投票，高自我投票的节点，拥有更高的侯选节点权重，可获得更高收益（即节点担保费用越高，则收益越高，并更值得投票人信任）

3.4.2节点验证

Hash Ahead节点结合现有公链节点的优势上进一步创新。

轻量化验证节点，验证者节点无需全链同步区块，只需要最高确认区块的状态数据，即可以验证新区块，验证者节点不需要存储历史区块数据，减小验证者节点存储要求，普通服务器也可以作为验证者节点工作，降低验证者节点基本要求；

节点选择性验证，验证者节点或领导者节点根据节点服务器处理能力，选择处理子链数量，以及选择处理那些子链，节点程序可评估服务器处理能力，节点主可根据评估数据选择需要处理的子链；

低门槛验证者节点要求，增强去中心化程度：一个验证者节点可由多台服务器组成，服务器分工合作，共同完成验证工作；能力较弱的参与者要参与验证工作，可多个参与者的服务器合作组成一个验证节点，参与验证工作，获得的收益按参与者的能力以及投票数量分成，该功能有效降低参与者的门槛，增强去中心化程度。

领导者生产区块时，不需要等待上一区块被确认后才生产，可以连续生产区块，而未确认的区块按最长链机制选择，验证者可连续确认区块，并可跳区块投票（即投票后区块可证明前区块，减少验证投票数量，提高效率）。

3.4.3节点收益

普通用户由于无法建立节点服务器，或没有足够的TOKEN达到最小自我投票，则可以选择投票其他节点获得收益。在选举验证者和领导者时，每个侯选节点的权重都相同，即被选中的概率相同。节点获得的奖励，按节点各投票人的投票TOKEN数占比来分配奖励。被选中为侯选节点后，每个节点的收益是相同的，与投票TOKEN数量无关。

节点主会收取节点拥金，即节点主建立服务器有成本开销，需要向投票人收取拥金来支持成本开销，节点主在创建节点时，需要设置拥金比例（0%~100%），节点地址设置了拥金比例，就不能更改，如需更改，则需要另建节点地址，该功能防止节点主随机更改拥金比例，损害投票人的权益。同时，由链拥堵情况自动计算最小GAS价格，可防止恶意攻击，以及降低用户的使用费，满足用户中心化交易所的体验需求。

Hash Ahead中奖励利率与投票抵押率和通货膨胀率相关，即块奖励数量周期性变动（一个周期内是固定的），块奖励数根据投票抵押率和通货膨胀率等相关数据计算而得。

3.4.4恶意节点行为及惩罚：

属于一条链的验证者，却不为该链的区块提供合法性验证，验证中签名了该链一个不合法的区块，不应答共识消息或不发送共识消息（不遵循共识机制的规则处理节点的消息），验证者在链两个竞争性的分叉上同时签名，在该生产区块时未生产区块，提案后不广播提案结束消息，在恶意分叉上生产区块，不在上一提案者的末尾区块后生产区块，或在两个竞争性的分叉上同时生产区块等等一系列的行为，在Hash Ahead中都将受到惩罚。

对恶意节点惩罚，Hash Ahead将锁定恶意节点自已的投票TOKEN，以及投票该恶意节点的投票人的TOKEN，锁定期为三个月（验证和提案节点有最小自已投票要求），并永久不能获取验证者资格，在锁定期结束后，将恶意节点自已的投票全部TOKEN转入黑洞地址，并将投票人的TOKEN的10%转入黑洞地址。

3.5高效安全主链

安全主链为 Hash Ahead树状结构中的主链，所有的支链均为其“后代”，其被用于支撑全区块系统的安全和共识，在 P2P 网络中主链的同步广播消息转发优先级高于应用支链。广播数据采用瀑布模型，相比于传统P2P网络传输模型，传输路径和时间更短。安全主链除了记录主链Token转移，还保留 DPoS 节点协商关键过程数据。安全主链的区块之间不能插入子块，只能按照既定出块间隔增长。

安全主链以区块系统创世区块为起点，安全主链被用于支撑全区块系统的安全和共识，所有应用分支节点都需要同步和校验主链区块头信息。新节点接入网络后，首先完成主链同步，才开始进行对应应用分支同步。共识主链+功能子链组成多链结构，可无限扩展功能子链，链与链之间可跨链交易。最佳环境单链可达100万TPS，最小区块间隔1毫秒，交易确认时间500毫秒，同时去中心化交易所资产交易确认时间也为500毫秒。

3.6去中心化系统

作为一个去中心化性质的平台，Hash Ahead由完全透明的去中心化自治体系支撑其管理架构。这结构让每个通证持有者清晰了解公链基础内的全部技术构建和价值流转、充分体现区块链的公信价值。Hash Ahead内的所有决策均以通证持有方的公投决策为依据，所有技术更新均由社区公示。这完全去中心化的管理体系将完全避免了传统机构的中心化管理弊端。为中心化管理层专权，篡改资料和独自决策集团走向等问题提供了优良及无信任风险的解决方案。

4、Hash Ahead应用

4.1智能合约库

4.1.1Hash Ahead智能合约库简介

智能合约库虽然在以太坊生态中已经被很早的应用，但很多合约库的作者付出了聪明才智，实际并没有获得收益。调用合约产生的GAS费用归矿工所有，而合约的作者在整个生态中默默的做贡献。

Hash Ahead生态的模型确保可以让合约的作者与出块者共同获利，为了提高合约的安全性增加了合约的审核机制，在DAO的管理机制下，提交的合约被社区所审核，才能被系统所调用. 因此也要求合约的作者提交合约的时候需要支付一笔审核费用。

Hash Ahead采用wasm的技术，智能合约运行代码和源码存储在链上，相同的代码只存储一份，直接使用代码HASH创建合约，无须上传代码，并且同一区块中的多个智能合约可同时执行，提高智能合约运行效率，保证高效率的执行力。

而智能合约虚拟机采用WebAssembly技术，可运行WASM二进制代码的虚拟机，WASM虚拟机性能比EVM虚拟机更高，同时支持多种编程语言，包括Solidity、C++、RUST等语言，增加开发人员的编程体验。

4.1.2智能合约审核

以太坊中的ERC20来说，系统中有太多个相同的合约在跑，他们的代码相同，只是初始化的参数不同，给链也带来很大的数据重复，降低了链的存储效率。

在Hash Ahead系统中，相同的合约只会审核一份，极大的减轻了系统的负担， 当合约被调用的时候花费的GAS 费用按照一定的比例给到合约作者的账户。智能合约代码上链后，需要链上去中心化审核后才能被使用，审核代码安全性，审核是否抄袭他人代码等等。审核通过的智能合约代码可用于创建合约，合约被调用而产生的GAS费，部分会奖励给合约代码创作者，其他奖励给矿工，这也为更好的区块链应用打下基础，从而促使更多的程序员愿意往区块链发展。

4.2分层确定性钱包

在区块链网络中，每个用户都拥有一个甚至多个区块链账户即地址。普通的确定性钱包将为用户私钥的管理上带来不便，因为Hash Ahead采用分层确定性钱包。

Hash Ahead钱包采用去中心化、轻量化和多元化的设计，其中轻量化的设计，使用户能在不同的场景中随时随地的使用，而多元化的设计，能保证用户不用频繁的更换钱包进行货币兑换，从而降低时间上的成本。同时，Hash Ahead钱包能有效保证用户的匿名性跟相关隐私，增加用户的信任。

4.3Hash Ahead去中心化交易所

中心化交易所给投资者带来了重大风险，每年有数十亿美元主要来自比特币和以太坊的资金在复杂的黑客攻击和诈骗中损失，这引起监管机构的愤怒，他们现在越来越多地对其进行监管，并在此过程中影响用户隐私。

Hash Ahead打造的完全去中心化链上交易所，用户将完全保管他们的资金，并可以随心所欲地使用它们。平台以开放式生态接入智能式合约，链上自动运行，没有任何的中心。背靠全球最快公链，强大技术支撑，领先全行业。上币去中心化，可轻松创建虚拟代币，并与原生链主币有相同功能，利用智能合约绑定和管理虚拟代币，同时可参与去中心化交易所交易，实时挂单，实时撮合，安全确认，无限接近中心化交易所的用户体验。

在最佳环境下，Hash Ahead可在500毫秒以内完成交易确认，支持大并发量挂单和撮合，支持订单删除和修改功能。通过具有去中心化子链实现跨链桥功能，桥接BTC、ETH等公链的资产，提供安全转移资产功能，同时通过去中心化交易所，可提供多种资产的高效交易能力，能够实现完整、安全的资产去中心化跨链流通兑换，支持多种公链自由流通兑换。

5、HAH发行机制

5.1HAH发行计划

5.2发行周期

5.3收益说明

5.4使用计划

6、发展战略

7、风险提示

在Hash Ahead的开发、维护和运营过程中存在着风险，这其中很多都会超出开发团队的控制。

7.1市场风险

Hash Ahead的价格与整个数字货币市场形势密不可分，如市场行情整体低迷或存在其他不可控因素的影响，则可能造成 Hash Ahead本身即使具备良好的前景，但价格依然长期处于被低估的状态。

7.2监管风险

由于区块链的发展尚处早期，在全球没有有关募集过程中的前置要求、交易要求、信息披露要求、锁定要求等相关的法规档。

7.3竞争风险

当前区块链领域项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。并且随着信息技术和移动互联网的发展，其他应用平台的层出不穷和不断扩张，Hash Ahead将面临持续的运营压力和一定的市场竞争风险。

7.4人才流失风险

Hash Ahead聚集了一批在各自专业领域具有领先优势和丰富经验的技术团队和顾问专家，其中不乏长期从事区块链行业的专业人员以及有丰富互联网产品开发和运营经验的核心团队。核心团队的稳定和顾问资源对Hash Ahead保持业内核心竞争力具有重要意义。在今后的发展中，不排除有核心人员离开，核心人员或顾问团队的流失，可能会影响平台的稳定运营或对未来

发展带来一定的不利影响。

7.5黑客或盗窃风险

黑客或其他组织或国家均有以任何方法打断Hash Ahead应用或功能的可能性，包括但不限于拒绝服务攻击、女巫攻击、游袭、恶意软件攻击或一致性攻击等。

7.6核心协议风险

Hash Ahead目前基于某个特定的链开发，尽管团队会挑选目前最安全稳定的区块链作为基础设施，但该链发生的任何故障，不可预期的功能问题或遭受攻击都有可能导致Hash Ahead以难以预料的方式停止工作或功能缺失。

7.7系统性风险

软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分风险依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害。

7.8无法预料的风险

基于密码学的数字金币是一种全新的技术，除了本白皮书内提及的风险外，还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其他风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。

1. 免责说明

本网站的宗旨是在不违反国际相关法律法规的前提下，尽可能地为全球广大数字资产爱好者及投资者提供一个平台。禁止使用本网站从事洗钱、走私、商业贿赂等一切非法交易活动，若发现此类事件，本站将冻结账户，立即报送有权机关。

当有权机关出示相应的调查档要求本站配合对指定用户进行调查时，或对用户账户采取查封、冻结或者划转等措施时，本站将按照有权机关的要求协助提供相应的用户数据，或进行相应的操作。

本网站使用者因为违反本声明的规定而触犯国际相关法律的，本站作为服务的提供方，有义务对平台的规则及服务进行完善，但本网站并无触犯国际相关法律的动机和事实，对使用者的行为不承担任何连带作用。

凡以任何方式登录本网站或直接、间接使用本网站服务者，视为自愿接受本网站声明的约束。