



Bitvote.one

比特币白皮书

目录

1.0 简介	03	5.0 里程碑计划	16
1.1 分叉背景	04	5.1 发展计划	17
1.2 Bitvote 概述	04		
2.0 BTC 现状	05	6.0 风险提示	18
2.1 BTC 现状	06	6.1 货币监管风险	19
3.0 分叉方案	07	6.2 税务风险	19
3.1 如何获取 Bitvote	08	6.3 资本控制风险	19
3.2 硬分叉	08	6.4 CTF 和反洗钱条例	19
3.3 相关交易所	09	6.5 区块链安全风险	19
3.4 相关矿池	09	7.0 联系我们	20
3.5 相关钱包	09	7.1 联系我们	21
4.0 技术特点	10		
4.1 DAO 去中心化社区自治	11		
4.2 混合共识机制 PoW+PoS.	11		
4.3 MIMBLEWIMBLE	12		
4.4 区块标记投票	13		
4.5 CPU 挖矿算法	14		
4.6 加速出块	14		
4.7 区块扩容	14		
4.8 重放保护	14		
4.9 BTV 基金会	15		
4.10 相关技术	15		

1.0 简介

1.1 分叉背景

比特币诞生于全球经济危机之后，是中本聪对中心化货币发行机制无休止的量化宽松政策的抗议。传统金融体系中，国家信用体系和银行类机构，控制着货币发行与流通，毫无节制地通过货币来剥削人民。中本聪提出的点对点的货币体系，正是对传统中心化体系的变革。没有中心化“超级节点”的干预，所有的交易记录广播到所有网络节点，在节点确认后便固定下来，不需要第三方信用机构的背书便可以建立一套完整的信用体系。

“矿工”在这套信用体系中扮演重要的角色，矿工通过竞争解决数学难题，获胜便可以得到区块奖励，显而易见的是，加入的矿工越多，这套体系越安全可靠。在早期，只有少数极客使用个人电脑参与挖矿，因为难度极低，所以处理器可以很容易的开展工作。但是，随着比特币价格的攀升，为了获取优厚的奖励，提高算力的方法开始被研究，显卡挖矿、FPGA 挖矿、ASCI 挖矿便相继产生。目前，专用集成电路（ASIC）矿机凭借专业芯片，可执行数 SHA256 计算时间更快而且效率更高，从而取代了之前的 CPU 挖矿。

中本聪的愿景“one-CPU-one-vote”取而代之变成了“one-ASIC-one-vote”。如今，矿场往往是一个巨大的仓库，里面排满了 ASIC 矿机不停歇的运转，中心化实体的影子又悄然而至，这样发展下去，普通比特币的持有者和爱好者将会越来越难参与到整个社区运行方向的决策当中。

1.2 Bitvote 概述

Bitvote 的目标，是让数字货币回归到所有社区成员平等参与的状态，不论你是矿工或是投资者。在整个

Bitvote 的生态中，可以有更多的社区成员表达自己的心声，提出自己的构想，从而参与到社区的发展建设之中。在实现民主自治社区的同事，解决 BTC 交易拥堵的问题，重塑交易价值。

Bitvote 加入了重放保护，以提高 BTV（发行代币名称）的安全性及投票结果防篡改。将区块大小从比特币的 1 MB 扩容到了 8 MB，并且支持 segwit，极大提高交易速度，解决高并发问题。同时，加入了闪电网络，解决交易拥堵，使得 BTV 可用于高频小额场景。BTV 还使用了区块标记投票系统，防止一方滥用与控制系统，保障持有 BTV 的用户拥有话语权。在以上特性的基础上，BTV 还加入了高效的智能合约，可在 BTV 上构建应用与数字资产发行，使 BTV 作为具有功能性的价值标杆。

2.0 BTV 现状

2.1 BTC 现状

投票自古以来作为一种相对公平的多人决策方式沿用至今，而且随着科技的发展，投票不仅仅可以在线下进行，现今也可以在线上轻松地完成投票。但由于中心化的服务器数据都由服务提供商控制，投票结果真实性难以得到保证，并且经常会收到质疑，投票的公正性名存实亡。

在比特币的工作量证明体系里，矿机越多，算力越高，越有可能抢到打包权的挖矿方式称为 PoW 挖矿（Proof of work，工作量证明）。中本聪在白皮书第 4 章中对挖矿曾作出如下表述：工作量证明（PoW）机制还解决了在集体投票表决时，谁是大多数的问题。如果决定大多数的方式是基于 IP 地址的，一个 IP 地址一票，那么如果有人拥有分配大量 IP 地址的权力，则该机制就被破坏了。而工作量证明机制的本质则是一个 CPU 一票（ONE-CPU-ONE-VOTE）。

在比特币的系统中，大规模矿机的运用已经背离了比特币创始的这个初衷，一般的参与者在现有的情况下是无法拥有投票权的。现有的系统下，投票权集中在拥有大量算力的矿池手中，变相的中心化已与原本比特币去中心化的理念背道而驰。要继续加密货币未来的发展，改变迫在眉睫。

为了解决在投票决策过程中信任度的问题，Bitvote 应运而生。Bitvote 前瞻性的使用了 CryptoNight 算法，落实中本聪对比特币 ONE-CPU-ONE-VOTE 的初衷。Bitvote 搭建了一个新型数字货币实验自治社区，未来可被应用于公证、决策、科学管理、匿名意见决策等方面，特别是在世界范围内逐渐流行开来的 AB 股管理制度，即同股不同权制度。Bitvote 能在将来为众多大型企业提供优质解决方案，同时也可为政府与组织中的选举保障公正，通过去中心化完善社会信用体系。

3.0 分叉方案

3.1 如何获取比特币？

要获得免费 Bitvote，你需要在快照时的区块高度拥有 BTC。如果你持有 BTC，你将自动在同一地址获得等量的 bitvote，同时可以使用同一私人密钥。备份也是非常重要的，你的私钥和助记词可以帮助你恢复钱包。然而，如果你在交易所或保管服务商那里持有 BTC，则无需访问私钥，你只需要确保服务商将支持 Bitvote。如果你不确定当前的保管服务商能领取到 bitvote，那么建议将你的 BTC 转移到支持领取 Bitvote 的服务商。

定高度为 505050。新的规则将在第 505051 块生效，总量为 2100 万枚，出块时间为 2 分钟，分叉后还有 400 万枚可挖，每块的奖励为 12.5 个 BTV。从这个区块开始，Bitvote 矿工将开始介入，建立一个新的分支的 BTC 区块链。这个新的分支在区块链上保留相同历史交易和股权分布，当然，如果你持有的 BTC，你会自动获得等量的 Bitvote。

3.2 硬分叉

比特币是一套分布式账本，对代码的修改就涉及到分叉，而分叉又包括软分叉和硬分叉。代码本身是比特币系统的共识，所有 BTC 的完整节点需要运行且执行相同的共识规则；执行不同的共识规则的节点不是比特币的一部分。

如果矿工发现一个遵循比特币共识规则的新块，将其广播到全网用以确认有效，网络上所有的完整节点都会接受该区块和它包含的所有交易。当矿工发现的区块不符合比特币的共识规则，且之前的节点不接受该块时，那么，被挖到的新块就发生了硬分叉。

BTC 在 478558 块之前，比特币和比特币现金节点仍执行相同的共识规则，接受相同的区块。但从那个块开始，比特现金的新共识规则生效，比特币完整节点拒绝使用比特币现金账本和比特币现金节点产出的区块。这个时候，矿工继续使用比特币账本，就直接导致了网络分叉。

Bitvote 通过实施新的共识规则（预估时间为美国中部时间 2018 年 1 月 21 日）进行硬分叉比特币，预

3.3 相关交易所



3.4 相关矿池



Dwarfpool

MINING POOL HUB

Nanopool

UU Pool

VPool

3.5 相关钱包



BitGo



bitpay

coinbase

库神
COLDLAR

JAXX



TREZOR

Bixin 币信 HK



4.0 技术特点

4.1 DAO 去中心化社区自治

Bitvote 采用 DAO 的组织结构，用以支撑均衡分散投票权的设想。DAO 被称为去中心化自治组织 (Decentralized Autonomous Organizations)，是计算机代码、区块链技术、智能合约和人的结合。DAO 的创始人制定了运作的基本规则，DAO 拥有获得相关权利的若干利益相关者，他们拥有自己的代币，基本上，这些利益相关者都希望增加代币的价值，来提升在组织中的地位。

DAO 区别于传统的公司事业部的组织关系，DAO 的代币持有人（即股东）有权对组织面临的任何提案投票“同意”，“反对”或“弃权”，而不再是由传统的董事会和管理人员决定社区组织的发展。

DAO 的运作规则使处理事务将以“效率”为先，而不再看重职位。最重要的是，在区块链自治组织中，我们不再是以雇员的身份被聘用，而是以项目来获得合同。例如，部署隔离见证这种方式，在社区成员讨论后，以投票表决是否通过，通过后即可开始工作。

Bitvote 采用 DAO 的组织结构，运用区块标记投票系统促使开发团队与矿工协同工作，这样可以防止分叉的风险，并且用户相互建立信任无需第三方机构背书。拥有更大区块和吞吐量的处理交易数据，可以轻松解决比特币网络拥堵。Bitvote 可以看做是自我进化版的 BTC，它有着更强的可拓展性，未来将使得比特币变得更加伟大。

4.2 混合共识机制 PoW+PoS

社区发生意见分歧，而投票权是基于 PoW 产生的，如果未能形成统一意见，矿工各自支持不同派别，便会产生分叉币。但是，矿工相对于整个 BTC 的参与群体中在数量上只占了一小部分，其余大部分为投资者，

这对 BTC 的发展与稳定起不到积极的作用。

Bitvote 采用了 PoW+PoS 的混合共识机制，持有 Bitvote 的用户与矿工均可以参与到投票中，共同参与 BTV 社区的重大决定，持币者与矿工都可以影响预先编制好的更新，如隔离见证 (SegWit)、区块扩容等等。如果这些更新被广泛认可，无需开发者干预，链就会自动配合更新。

Bitvote 采用更平滑的方式执行社区成员的投票结果，投票结果会被记录在区块链上并且自动执行，这样来解决社区可能存在的各方参与者的分歧，促使社区协同合作健康发展。PoW 主要是为了避免系统被黑客或是 DDoS 攻击，并确保在没有第三方背书的前提下信息传输更安全，但是 PoW 系统的工作主要基于矿工，需要解决的数学问题的难度越来越大，PoW 系统需要花费的成本也越来越多，每笔交易需要支付更高的矿工费来激励矿工确认交易。交易费用提高，便会造成交易拥堵严重，使得比特币使用者的用户体验大打折扣，且矿池日益集中的算力，也增加了 51% 攻击的风险。

PoS (Proof of Stake)，权益证明机制，解决了 PoW 消耗大量资源的问题，但仅仅只靠 PoS 的话，会形成“阶级固化”，持币相对较多者会拥有更多代币。所以，采用 PoW+PoS 混合共识机制可以防止 PoS 分发给早期投资者的比重更多，并且利用 PoW 机制提供安全的保障，两者相互结合，从而保证系统的安全运行。

Bitvote 使用这个混合共识系统以在矿工和用户之间取得平衡，一般而言，运作基础设施的矿工拥有相当大的影响力，而用户的影响力则相对微弱。Bitvote 允许用户无需拥有昂贵的挖矿硬件就能直接参与此项目而发挥其影响力，从而创建一个更加和谐和完善的加密货币生态体系。

4.3 MIMBLEWIMBLE

比特币利用区块链的公共数据库保存所有的交易数据，然而真正想要检查系统状态的人必须下载所有数据，并且追溯每一笔交易。同时，大多数这些交易并不影响它的最终实际状态（它们每创建一项输出，就会销毁一项之前的交易）。

但是，整个区块链必须通过完整验证才可以确认最终状态。另外，这些交易是“cryptographically atomic（加密原子）”，进入每一项交易它都会很清楚。

“transaction graph（交易图）”会泄露大量信息，并且有许多专业的分析交易的公司，这些公司监管和控制着市场这些交易层。这使得交易毫无隐私可言，对用户利益造成巨大的侵害。

Greg Maxwell 发现加密交易金额可使交易匿名化，但仍需要允许其他人确认金额是否正确。Maxwell 博士创造了 CoinJoin，使得一个比特币用户可以混合多笔交易，使得交易关系被混淆。Nicolas van Saberhagen 开发了一个可以蒙蔽交易输入的系统，进一步混淆交易关系（同时不必进行混币）。之后，Noether 结合这两种方法得到了“Maxwell 的‘机密交易（Confidential transactions）’和 van Saberhagen 的暗箱操作”。它们会使比特币使用起来非常安全。但问题在于大量数据因此而变得更糟。机密交易（Confidential transactions）的每一个输出需要多字节的证明，van Saberhagen 签名要求保存每次输出，因此其不可能明确交易到底是什么时候完成的。Yuan Horas Mouton 博士创造了可自由合并交易，但是这个需要使用基于配对的密码，这些密码潜在地延缓了交易，他称这为“单向聚合签名”（OWAS）。

单向聚合签名是一个很好的办法用于混合区块里的交易。我们可以通过跨区块来进行混合交易（也有可能

是粘合数据），所以当输出产生和销毁时，这和它从未出现是一样的。然后，为了验证整个链条，用户只需知道钱什么时候进入系统以及最终什么时候成为未花费输出，剩余可能被转移、遗忘。然后，我们可通过机密交易隐藏金额和单向聚合签名，进而模糊交易图，并使用更少空间让用户充分验证区块链。我们不需要基于配对密码或新猜想，仅使用类似比特币的普通散列数签名。

这项技术可以被用来防止区块链泄露所有用户的信息，所以技术的发明者称之为 Mimblewimble（无声无息之咒，源自“哈利波特”）。

4.4 区块标记投票

由于 ASIC 矿机的出现造成的算力集中化问题，使得 PoW 共识的权利机制不再具有平等代表性。如何建立起一个更合理的自治社区，使得分歧能够更民主的解决。BTV 使用块标记权单独竞价投票的方案，使得在社区意见发生分歧时，投票表决能够顺利达成共识，防止开发团队和矿工的分化。

Bitvote 采取标记权和投票权分离的办法，在社区重大事项公布前，社区用户均可平等的参与竞拍，获取区块标记权。标记权用于投票签名，投票选项有“支持”，“反对”和“弃权”，签署署名的区块为有效区块，根据投票结果决定社区发展方向。

以下是投票可能出现的情况：

1. 如果 BTV 中所有选票中有超过 90% 是“弃权”票，议会投票将继续对下一个 BTV 有效。
2. 如果 BTV 内部所有非弃权票未能达到 75% 多数票的门槛，议会投票将继续对下一个 BTV 有效。

3. 如果 BTV 内所有非弃权票的 75% 都支持议程（“支持”），则议程被确认为锁定的，在投票通过后，共识变更。
4. 如果 BTV 内所有非弃权票的 75% 都反对议程（“反对”），议程就会失败，共识的变化将永远不会被启动。
5. 如果一个议程在达到 75% 的多数票之前到期，议程将到期，共识的变化将永远不会启动。

最近出块

高度	播报方	大小(B)	块收益	时间	块哈希	块版本
498,355	 58COIN	1,030,584	16.90771658 BTC	5 分钟前	000000000000000000000837f89788c5f30a2474eeb5699a3c297a2b9304bc11a0a	弃权 kral
498,354	 BitClub	1,088,985	17.64450158 BTC	9 分钟前	0000000000000000000001682e0ddbca95d8353181cb844f9aa56a466de81924dce	•
498,353	 ViaBTC	1,038,126	16.74990974 BTC	50 分钟前	00000000000000000000034af6082c5f0f0400457a456137e95704281b1c0b7b32a	•
498,352	 AntPool	1,056,097	17.46107215 BTC	1 小时 04 分钟前	000000000000000000000a7f4181e03e3f818523537d5510a240c538f7eafd8fadf	反对 王五
498,351	 SlushPool	1,029,341	14.95895975 BTC	1 小时 41 分钟前	00000000000000000000094e5487fe6d3556581ee1a6febd00e83f7b987c16af611	•
498,350	 ViaBTC	1,042,165	15.36138110 BTC	1 小时 46 分钟前	0000000000000000000007df3d0e88f033c6871bd4eb71e4284617be15a48395b7f	•
498,349	 BTC.TOP	1,046,451	14.85958323 BTC	1 小时 52 分钟前	0000000000000000000009bcf4ae6f06008777336cbe2c3acbd0c12400cf9fa73da	支持 李四
498,348	 BitClub	1,029,405	14.66417795 BTC	1 小时 57 分钟前	00000000000000000000008427cd2e83b972d3ca8ffb42f42fb36bbab53cc705af3	•
498,347	unknown	1,054,088	15.89572576 BTC	2 小时 00 分钟前	0000000000000000000002431c191459385d1c3ae363d090dd9dd7be0d79d5e994	•
498,346	 BTC.TOP	1,069,924	15.49849842 BTC	2 小时 10 分钟前	00000000000000000000078f39f80900073bd4eac1b69a54976f995f68cdbc081f8	支持 张三

4.5 CPU 挖矿算法

在比特币中，挖矿算法为 SHA256，每 2016 个区块（大约两周）调整难度，以便出块平均间隔为 10 分钟。如果块之间的平均时间不到 10 分钟，出块难度就会增加；如果平均时间超过 10 分钟，则会降低出块难度。

而 Bitvote 采用 CryptoNight 算法，运用这样的 CPU 算法挖矿，可以避免大规模专业矿机的出现，解决算力过于集中化的问题。Bitvote 算力分布均衡，并以 2 分钟的时间间隔为目标调整了每个块的出块难度。

4.6 加速出块

比特币的出块时间为 10 分钟，每个区块容量为 1M 的存储空间，如果一次出现有很多笔交易放不下，就要先把手续费高的交易数据打包进区块，手续费低要排队，等待下一个区块，所以区块的容量和出块时间都影响交易的确认速度。

相比比特币而言，Bitvote 的出块速度是 2 分钟一个，更快速的打包区块，缩短交易确认时间，提高交易效率，同时降低了交易手续费。

4.7 区块扩容

比特币区块链是全球的、分布式的、有限容量的、代价昂贵的系统。随着比特币的繁荣，交易数量会越来越大，1M 的块容量会使得低价值的交易（比如发送 1 分钱）永远无法进块，因为低价值的交易不可能支付高昂的网络手续费。

而 Bitvote 采用了 8M 大区块，可以容纳更多的交易

数量，即使大量交易需要处理时，Bitvote 也能通过大区块打包数据，意味着所有交易均能进入区块。并且，配合 2 分钟出块速度，能保证 Bitvote 轻松处理交易数据，每位用户都可以享受 Bitvote 带来的巨大便利和优势。

4.8 重放保护

重放攻击（Replay Attacks）是计算机世界黑客常用的攻击方式之一，指的是攻击者发送给一个目标主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性，从而达到多次欺诈的目的。如果接收者可以有效识别和拒绝重放信息，也就不存在重放漏洞，也就避免了被攻击的可能。

因为有以太坊重放事件的在前，在 BCH 诞生之前，重放攻击很自然的被广泛谈论，大家都担心重放事件会在 BCH 和 BTC 两条链上继续存在。有了以太坊的前车之鉴，使得 BitcoinABC 开发者提前设立重放保护——BCH 分叉后在交易数据签名添加了 SIGHASH_FORKID (0x40)，这样能使交易数据在两条链上不再互相兼容，也就不可能存在重放无法识别的可能，从而有了重放保护。

重放攻击的风险是每一个硬分叉固有的，由于必须考虑用户账户不会受到攻击而导致资金的流失，Bitvote 会提供分叉后的技术保护。

4.9 BTV 基金会

Bitvote 基金会 (Bitvote Foundation) 是一个非营利性机构, 旨在推动 Bitvote 社区的建设, 维护并推进 Bitvote 社区的开发, BTV 基金会管理挖矿产出的 20%, 并将其用于推进平台建设及基础层研究、开发和教育, 用以更好地为 Bitvote 和去中心化技术生态系统服务。BTV 基金会的使命是在开放的去中心化的构架下, 完成新应用和技术的开发, 以及扶持 BTV 的相关技术和协议应用, 推进数字货币自治社区的发展。

4.10 相关技术

智能合约: 智能合约允许用户编写自定义的行为并将其用于区块链, 而不必进行多个预定义的操作。通过使用智能合约, 用户可以灵活地扩展自定义的复杂的交易方案以及复杂的金融合同。同时, 用户可以通过限制和动态控制扩展功能, 无需修改或升级区块链代码。

智能合约允许用户在区块链中注册自定义合约字节码, 并在 BTV 链中调用交易。合约字节码在图灵完成合约字节码虚拟机中执行。开发人员可以使用编程语言编写智能合约, 并使用合理的语法编译为合同字节码, 并应用于区块链中。

闪电网络: 闪电网络的目的是实现安全地链下交易, 其本质上是使用了哈希时间锁定智能合约来安全地进行 0 确认交易的一种机制, 通过设置巧妙的“智能合约”, 使得用户在闪电网络上进行未确认的交易能和交易黄金一样安全 (或者和比特币一样安全)。

隔离见证: 如果比特币区块 1M 容量不够用了, 一个简单的办法就是把 1M 扩的更大, 但这需要硬分叉, 很多人都不同意这样的方式, 而且担心会出问题。还有另一个办法就是把塞进这 1M 区块的单笔交易的数

据给缩小, 这样也能装下更多的交易。隔离见证就是想办法让同样 1M 的空间塞进更多的交易的办法。这样就变相突破了 1M 区块的限制, 让 1M 区块能够容纳更多的交易。

零知识证明: 零知识证明 (被称为“zk-SNARK”) 是实现 Zcash 的匿名特性的核心技术。“零知识证明”的定义是: 证明者能够在不向验证者提供任何有用信息的情况下, 使验证者相信某个判断是正确的。实际的应用便是, 能够在不告诉别人账户余额和交易支出的情况下, 证明自己的花费少于账户的余额。能够不记录收款方的公开账户地址, 使收款方受到转账。

量子抗性: 在当前以比特币为代表的区块链系统中, SHA-256 哈希计算和 ECDSA 椭圆曲线密码构成了比特币系统最基础的安全保障, 但随着量子计算机技术不断取得突破, 使得现有算法无法抵挡量子攻击, 用户信息就存在风险, 个人资产没有安全保障。后量子密码 (post-quantum cryptography), 又被称为抗量子计算密码 (quantum-resistant cryptography), 是被认为能够抵抗量子计算机攻击的密码体制。抗量子算法如果成功部署, 将会对私人财产提供更坚强的保护, 对整个加密数字货币都有深远的影响。

跨链交易: 跨链技术是实现价值网络的关键, 它是把联盟链从分散单独的孤岛中拯救出来的一剂良药, 是区块链向外拓展和连接的桥梁。区块链从技术上是去中心化数据库和分布式账本技术, 从商业层面则是价值网络。在这个价值网络中, 连接的有效节点越多和分布越广, 可能产生的价值叠加就会越大。区块链是价值网络空间的核心基础设施, 区块链应用不应该只局限于和止步于联盟链的应用, 将价值圈在一个小范围中, 我们需要跨链技术, 对不同区块链进行连接和扩展, 构建价值网络的高速公路。

5.0 里程碑计划

5.1 发展计划

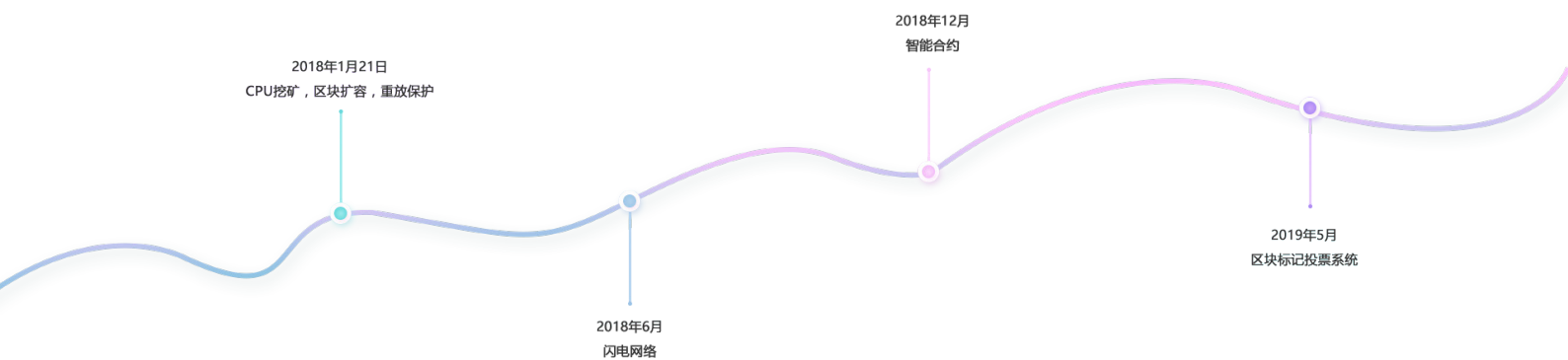
2018年1月21日：将在505050区块高度进行分叉

2018年1月21日：支持CPU挖矿、区块扩容、重放保护

2018年6月：闪电网络

2018年12月：智能合约

2019年5月：区块标记投票系统



6.0 风险提示

6.1 货币监管风险

各国政府仍在设计关于将加密货币作为一种贸易结算形式进行监管的公共政策。对本地商业使用加密货币扩散的政府可能会发布法律和法规，认为使用加密货币是一项受监管的活动。这可能导致 BTV 的持有人在 BTV 未进一步推进合规性的情况下未来无法使用他们的 BTV。

6.2 税务风险

使用 BTV 作为结算货币的形式，可能或不受地方所得税、资本收益税、增值税或其他形式的税收的影响。税收立法的这种不确定性可能会使商人和客户对使用 BTV 作为结算货币，以及交易代币或 BTV 代币的资本收益产生不可预见的未来税收后果。

6.3 资本控制风险

许多司法管辖区，如中国，对跨境基本流动实施了严格的控制。BTV 持有人可随时会受到这些规定和 / 或强制执行此类规定的约束。这会使把 BTV 从当地管辖范围转移到海外交易所成为一中会使 BTV 的使用者受到政府罚款或其他监管制裁的非法活动。

6.4 CTF 和反洗钱条例

美国已经出台了一系列打击恐怖主义融资和洗钱活动的规定。许多其他国家已经制定了类似的法律来控制这些非法活动的资本流动。一些不法分子使用加密货币会违反这些规定。任何 BTV 的非法使用都可能严重影响 BTV 网络在国际上的声誉。在这种情况下，可以想象这可能会导致 CTF 和反洗钱监管机构的审查，并

可能对比特币生态系统中的代币和 BTV 代币的分配和流通造成重大的破坏。

6.5 区块链安全风险

黑客或其他恶意团体或组织可能会尝试以各种方式干扰 BTV，包括但不限于恶意软件攻击、拒绝服务攻击、基于共识的攻击、Sybil 攻击、smurf 攻击和电子诈骗。而且，由于技术发展迅速，所以 BTV 可能会过时。加密货币、数字资产和区块链技术的监管状况在许多司法管辖区尚不清楚或不明确。所以很难预测政府当局将如何管理这些技术，以及政府当局是否会对影响加密货币、数字资产、区块链技术及其应用的现有法律，法规和 / 或规则进行任何修改。这种变化可能会以各种方式对 BTV 产生负面影响，其中包括例如确定代币是受管制的金融工具，需要注册等。如果政府行为使其不合法或继续经营项目在商业上不可取，公司可能会停止分配 BTV 以及项目的开发或停止项目在某个管辖区的运营。

7.0 联系我们

7.1 联系我们

比特票官方主页: <http://www.bitvote.one/>

媒体合作 : media@bitvote.one

客户服务 : support@bitvote.one

Twitter: [bitvote.one](#)

Reddit: [bitcoinvote](#)

新浪微博: [bitcoinvote](#)

微信公众平台: [bitvote](#)



Bitvote.one

