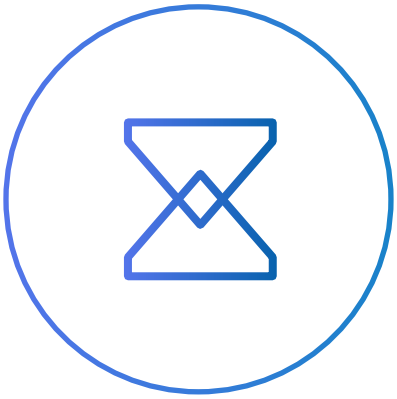


快链（FAST Chain）技术白皮书

—— 突破性能极限的去中心化交易系统

快（海外）基金会 FAST Plus.
2018-5-8

目录

摘要

把现代管理组织的办法应用于矿工节点，通过设计合理的激励和惩罚机制（能力共识），使矿工节点之间自发形成一个**高效的去中心化组织**，来完成一个指定的任务。

基于**原创的能力共识设计思想**，我们开发了全新的区块链公链FAST Chain。它是全球第一个真正为日常转账/支付设计的区块链支付解决方案，第一个能同时满足安全性、去中性化和高性能三个方面要求的区块链设计方案，也是全球第一个为小额支付乃至微支付场景做充分优化的解决方案。

FAST Chain转账/支付的实时性主要由DMT层数决定。而层数会受FAST Chain网络的节点总量以及节点TPS影响。按1万TPS计算，5层DMT树即可支持1亿亿个节点，足够供应全世界相当长时间内的需求。而按每个节点平均响应时间250ms估算，5层DMT树的**平均确认时间仅1秒，用户平均响应时间仅需2.5秒，已经接近ApplePay、AliPay、Paypal等集中式支付工具的体验。**即便按照每个节点平均响应时间500ms估算，平均确认时间也仅需2秒，用户平均响应时间仅需5秒。

基于能力共识设计的思路，经过简单的调整，可以轻易应用到其它的业务场景中，设计出能满足各种业务场景的链。这意味着，**FAST Chain可以支持多种图灵完备的智能合约侧链**，从而使FAST Chain的商业应用和生态发展速度得到极大提升。

FAST Plus.

项目背景

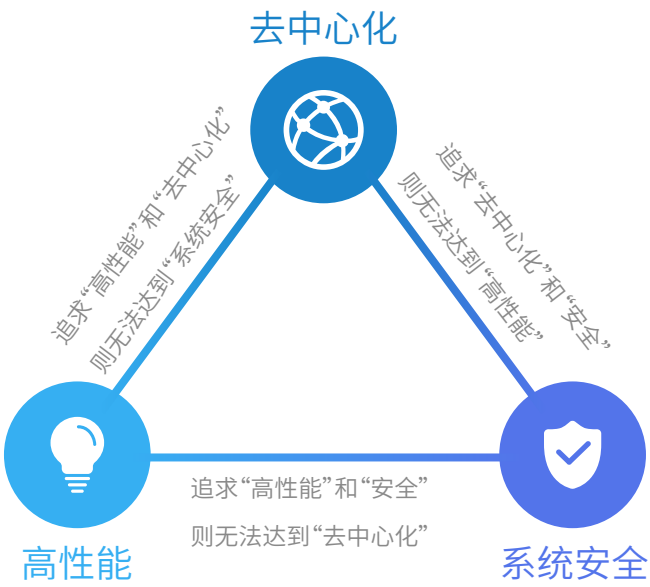
2008 年 10 月 31 日，Satoshi Nakamoto(中本聪)第一次公布了比特币的白皮书，这也被公认为我们当下提及的区块链技术的起源。比特币作为一种点对点的电子现金系统已经稳定运行近10年，并且比特币当前获得的“价值共识”基本验证了其初衷，

“我们非常需要这样一种电子支付系统，它基于密码学原理而不基于信用，使得任何达成一致的双方，能够直接进行支付，从而不需要第三方中介的参与”

—— 中本聪

因此区块链在技术革新以外，给人类社会的组织关系也带来了变革。即通过建立0信任交易的技术基础，让信任无处不在成为可能。从比特币到以太坊团队的工作成果，让我们看到区块链，在低频大额加密货币支付的业务场景中，可以产生的突破性成果，这点也在多种主流加密货币的流通价格共识中得到充分体现。

但截止目前(2018年5月)，区块链在实际业务中，能满足更多业务场景的技术基础仍不尽如人如意。因为低效的共识机制，超长的交易确认时间，高昂的小额高频交易手续费，频发的智能合约安全事件等区块链技术现状，造成区块链技术在大多数业务环节都无法产生积极的作用。面对这些问题，已有多个技术团队基于分片、侧链的思想对共识机制和系统架构进行优化改造。在探索的过程中，多个团队基本上达成了这样一个共识，即在“高性能”、“去中心化程度”和“系统安全”者三个维度存在“不可能三角形”，



正是沿着这种“”不可能三角形“”的论调,促使FAST Chain项目团队通过对数学和工程方法论的探索,在兼具安全与性能极限的去中心化交易系统设计上取得了突破性的进展,这就是FAST Chain(中译:快链)。

01 解决问题的设计思路

1.1 达成“不可能三角形”

通过不可能三角形的论调可知,区块链系统的技术底层基础取决于共识机制的设计。FAST CHAIN的设计师们系统的分析了各种共识机制,把它们进行分类并分析其各自的优缺点:

第一类共识,是完全去中心化共识。比如PBFT和DAG则属于此类。完全去中心化共识无法解决的是高效能的问题。比如PBFT,它们需要固定数量的节点,同时效能仍然偏低;而DAG虽然提供了近乎无限的交易容量,但难以保证交易的实时性。

第二类共识是算力共识。算力共识本质上也是一个中心化共识。但算力共识网络的中心是会不断切换的。它通过设计各种随机算法让所有节点都有机会成为中心,从而提高网络的安全性。像比特币的POW、以太坊的POS都是算力共识的代表作。算力共识将“记账权”的分配交由“机器算力”的竞争决定。这一竞争过程伴随着大量与实际业务无关的运算,从而产生资源浪费;

第三类共识是权利共识。为了降低前一类共识浪费资源的问题,开发者们将“记账权”通过随机数生成或“民主选举”的方式选出若干超级节点负责全网的记账。后者做法更是受到“算力共识”支持者的强烈质疑,因为这种共识机制已不是绝对去中心化的,同时在安全性方面也存在隐患。

以上三类问题,根本上是忽略了共识机制对交易本身应有的促进作用。为此我们提出一种新的思路,在完成效能目标的前提下达到充分公平,利用节点对于促成交易充分竞争保证去中心化程度,并以促成全网交易速度及安全为目的的竞争机制以突破“不可能三角形”。即一种新的设计思路——“能力共识”。

1.2 “能力共识”定义

我们认为忽视能力的绝对公平是没有意义的。这会导致真正需要完成的任务目标无法顺利达成。所以去中心化的公平性应该体现在能力越强，为真正需要完成的目标方面产出越多，收益越大。因此我们把现代管理组织的办法应用于矿工节点，通过设计合理的激励和惩罚机制(能力共识)，使矿工节点之间自发形成一个高效的组织，来完成一个指定的任务。

1.3 设计思路

1. 分析业务特点，

找到实现业务的核心任务，保障交易安全，高性能和去中心化；

关键指标：平均交易确认时间，每秒交易数。

2. 问题，

定义作恶行为：如双花攻击、伪造交易等；

选举方案：确立可验证公平性的算法，由程序执行的节点选举和轮换机制。

3. 原则，

结合业务的核心任务、关键指标、作恶行为及选举方案，设计合理的激励机制，使矿工节点的计算资源主要服务于任务和指标的达成。

4. 结果，

使有相同能力共识的矿工节点之间将自发形成一个能高效完成指定目标的自优化组织。

02 FAST Chain技术方案

基于能力共识的设计思想，我们开发了全新的区块链公链FAST CHAIN。它是全球第一个真正为日常转账/支付设计的区块链支付解决方案，第一个能同时满足安全性、去中性化和高性能三个方面要求的区块链设计方案，也是全球第一个为小额支付乃至微支付场景做充分优化的解决方案。

在性能方面，FAST CHAIN能达到近似集中式架构的TPS和响应实时性指标。它不但能达到接近ApplePay、AliPay、Paypal等集中式支付工具的实时性，也能支持类似淘宝双十一那样大规模并发支付的场景而不会出现拥塞。

在业务设计方面，FAST CHAIN采用每个矿工节点收取固定的0.01个Token作为转账/支付手续费。这样无论大额还是小额的业务都能获得矿工公平的对待，而且整体的交易成本非常低廉。

在Token价值管理方面，FAST基金会可以根据市场的变化，经过充分评估并公示后，对FAST CHain的Token（以下称FAST）容量进行合理的等比调节。等比调节不会稀释FAST 持有者的份额占比，但可以起到调节 FAST 与其它货币资产对应价格的作用，从而有利于维持FAST价值的相对稳定，把FAST 的交易成本维持在一个极具竞争力的水平。

2.1 核心共识算法POP——Proof of Performance：高性能证明

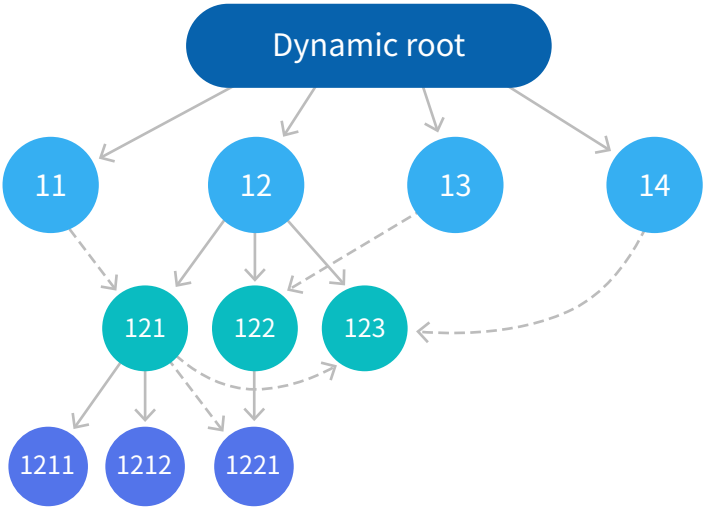
2.1.1 核心任务和关键指标

POP（Proof of Performance）高性能证明是一种能有效解决转账/支付确认全节点一致性和实时性问题的共识体系。它的核心任务是完成转账/支付的全节点一致确认，关键指标是转账/支付确认的实时性。

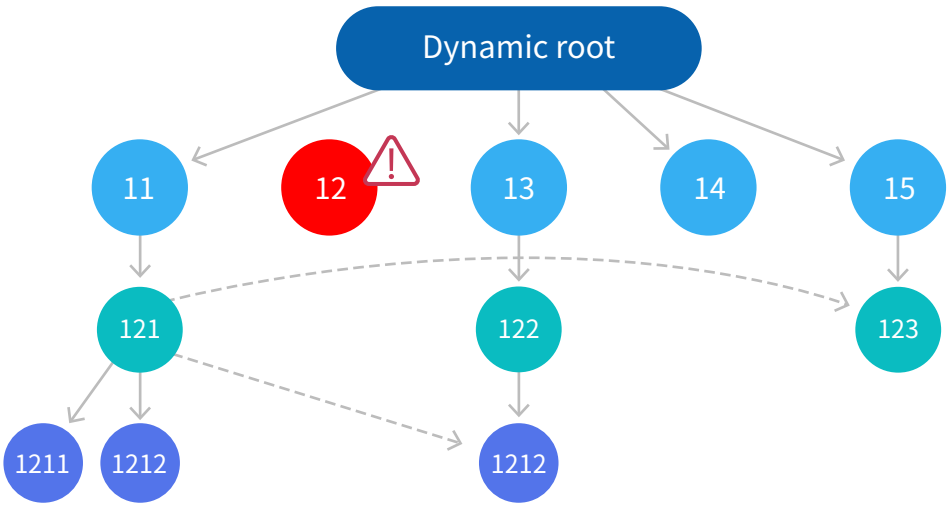
因为转账/支付的高实时性提高了用户体验，所以我们认为用户会愿意为此支付少量的费用。而为了达成这个效果，矿工是需要投入硬件设施和维持硬件和网络开销，是需要投入成本的。所以我们设计了一个奖励机制，一个能力共识：当一笔转账/支付能在3秒之内被FAST Chain确认，那么参与传递和确认这笔转账/支付的每个矿工节点都可以从中获得0.01个FAST Token作为手续费。反之就不能从中获得收益。

2.1.2 基于DMT(Dynamic Multi Tree:动态多叉树)的拓扑结构

当整个FAST Chain的用户和节点都认同这个共识,那么矿工为了更好的赚取这个手续费收益,需要持续对节点进行投入,提升节点软硬件的能力,获得更好的服务效果,从而争取到更多的客户。同时节点也需要寻找更好的服务供应商。一旦当前的服务供应商出现问题,或者找到更好的合作者,节点可以随时更换它的服务供应商。



如上图所示,二层子节点121是一层子节点12的子节点。但它同时又在评估一层子节点11、二层子节点123以及三层子节点1221对自己的服务质量。当子节点12出现拥塞不可服务,或者被证明作恶,那么它就无法帮助子节点赚取手续费。子节点也就会在自己的服务商中挑选最好的作为新的服务商。结果如下图所示:



由于节点12的失效或作恶,它的子节点都更换了新的服务商。根节点也会移除12。这样子节点12在恢复有效以后,它需要从叶子节点开始重新接入网络,并重新争取客户的支持和信任。

2.1.3 作恶惩罚

作为一个去中心化拓扑结构,任何节点都默认是不可信任的,都存在作恶的可能。而一笔转账/支付的确认,要解决3种作恶行为:伪造交易、双花和拒绝服务。

防止伪造作恶可以通过非对称性加密算法解决。

防止双花作恶需要有一个中心节点来检查确认。这就要求整个节点的转账交易的传递会演变成DMT(Dynamic Multi Tree:动态多叉树)的结构。从任意一个节点传入的转账交,只需要往父节点方向传递,就能最快的到达DMT的根节点,并由根节点完成全节点的双花确认。而经过根节点确认的转账交易往子节点的方向广播,通告全网络,完成转账的全节点一致确认。

由于转账确认的实时性是关键指标,所以一旦某个节点不可用,其子节点将会寻求更高效的节点来帮助完成转账确认的传递。所以节点本身会自行建设防止拒绝服务的方案。此外,新节点由于缺乏足够的价值,难以直接与根节点直接建立连接;而老节点本身已经有很大的价值,伪造转账的成本太高。同样对于使用真实转账来进行拒绝服务攻击,成本极高。

2.1.4 根节点选举机制

由于根节点是中心确认节点,需要防止根节点作恶。所以子节点要对父节点广播的消息进行伪造检查。一旦发现根节点出现伪造交易、拒绝服务的情况,或者满足根节点轮换的条件,FAST Chain将进入根节点选举环节。

为了加快选举的效率,FAST Chain充分利用了区块链分布式一致性以及数据不可篡改的特点,发明了利用历史数据选举的机制。

只有前任根节点的直属子节点可以参与选举。而过去一定数量N的转账/交易记录为全拓扑提供最大转账数量的直属子节点会被选举为新任根节点。这样选举算法的时间复杂度将大幅减少到O(1)。其中N=最后一条转账/交易记录的TxID末20位+100,000来确定,具体数量在10万到大约20万之间。这样一定程度上可以避免选举结果被提前预测和操纵。

另外,为了增加根节点的公平性,我们加入了以下的根节点轮换规则:

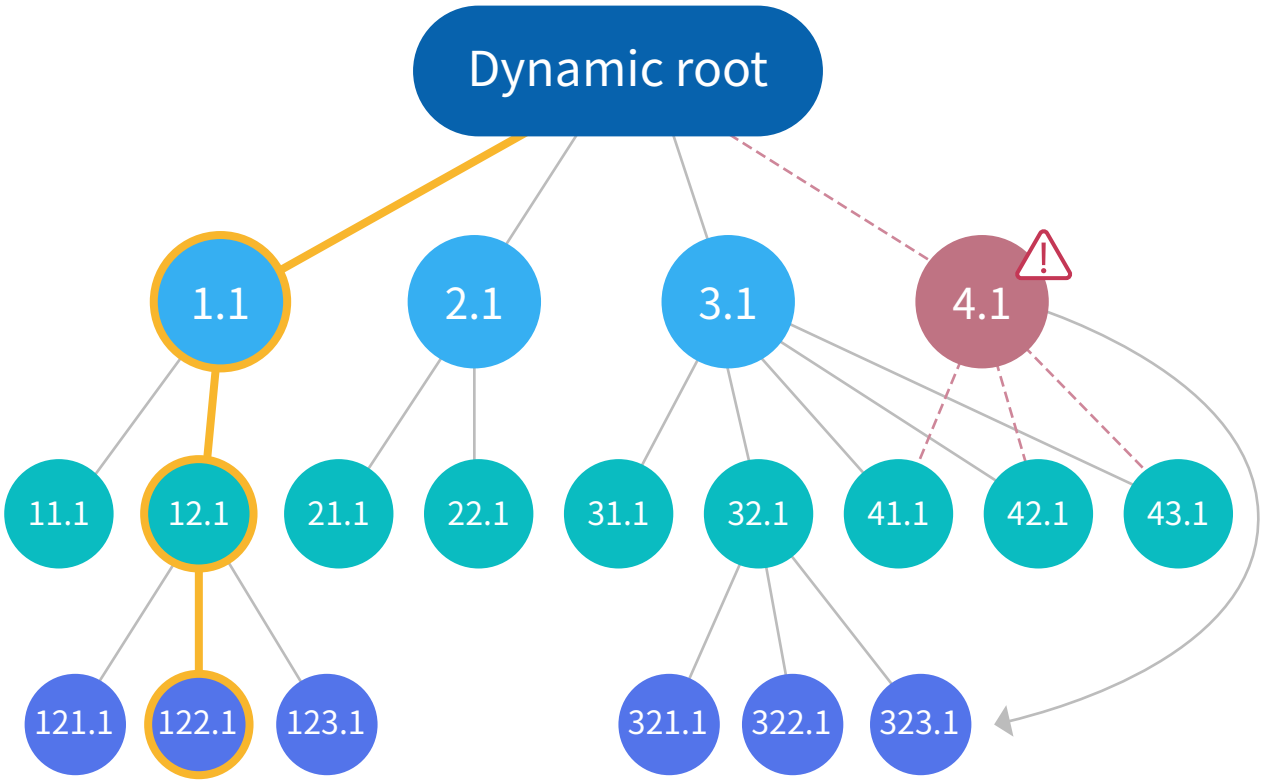
1. 根节点需要保证有效且不作恶,否则将会触发选举并被替换。
2. 在满足1的前提下,根节点能提供不少于5分钟的服务。
3. 在满足2的前提下,如果根节点完成确认的转账/支付数量超过100万条,则触发选举并被替换。
4. 根节点提供服务的时间达到30分钟,则触发选举并被替换。

2.2 激励机制设计

基于以上的分析，我们可以初步设计出以下的共识：

1. 参与了一笔转账确认的具体节点才能获得这笔转账的手续费。
2. 一笔转账必须在有效时间(3秒)内交付根节点确认，途经的节点才能获得这笔转账的手续费。
3. 对于每笔转账，每个节点收取的手续费是确定的。
4. 一旦发现节点作恶，其父子节点都会断开与作恶节点的连接。作恶节点被清0后可以从最末级重新接入拓扑。
5. 一旦发现根节点失效或作恶，或者满足根节点轮换的条件，一级子节点根据一定数量的历史数据，计算传递转账数量最大的一级子节点作为新的根节点。

到这里，基于以上共识的节点，就可以组建成一个自优化的节点拓扑，高效地完成转账确认这个任务。



激励机制示意图

这套共识设计的思路，经过简单的调整，可以轻易应用到其它的业务场景中，设计出能满足各种业务场景的链。

2.3 数据结构设计

FAST Chain采用与比特币一样的UTXO账户结构，只记录转账/支付的流水，不记录账户的余额。但为了提高确认的效率，我们会在计算余额的同时把余额数据写到记录中作为缓存。

右图是一条支付数据的初始结构：

支付数据结构（发起状态）

转出地址	256 位
转出公钥	256 位
目标地址	256 位
转出时间戳	32 位
金额	32 位
余额时间戳	32 位
转出签名	256 位

当一条支付数据经过节点检查后，节点会把检查信息附加到支付数据后，作为检查记录和领取手续费的依据。

支付数据结构（第一次确认）

转出地址	256 位
转出公钥	256 位
目标地址	256 位
转出时间戳	32 位
金额	32 位
余额时间戳	32 位
转出签名	256 位

确认记录

确认数量	8位
确认1地址	256位
确认1公钥	256位
确认1时间戳	32位
余额	32位
余额时间戳	32位
确认1签名	256位

当支付数据被传递到根节点并最终确认，根节点会给支付数据标记一个TxID。TxID由支付数据根节点签名和上一条支付数据TxID混合计算后生成。这样TxID之间就会形成一条链，历史记录不可能被篡改。

支付数据结构（根节点确认）

TxID：256位	8位
转出地址	256 位
转出公钥	256 位
目标地址	256 位
转出时间戳	32 位
金额	32 位
余额时间戳	32 位
转出签名	256 位

确认记录1

确认数量	8位
确认1地址	256位
确认1公钥	256位
确认1时间戳	32位
余额	32位
余额时间戳	32位
确认1签名	256位

确认记录2-n

……
……
……
……
……
……
……

根节点确认

根节点地址	8位
根节点公钥	256位
根节点时间戳	256位
余额	32位
余额时间戳	32位
根节点签名	32位

2.4 加密算法设计

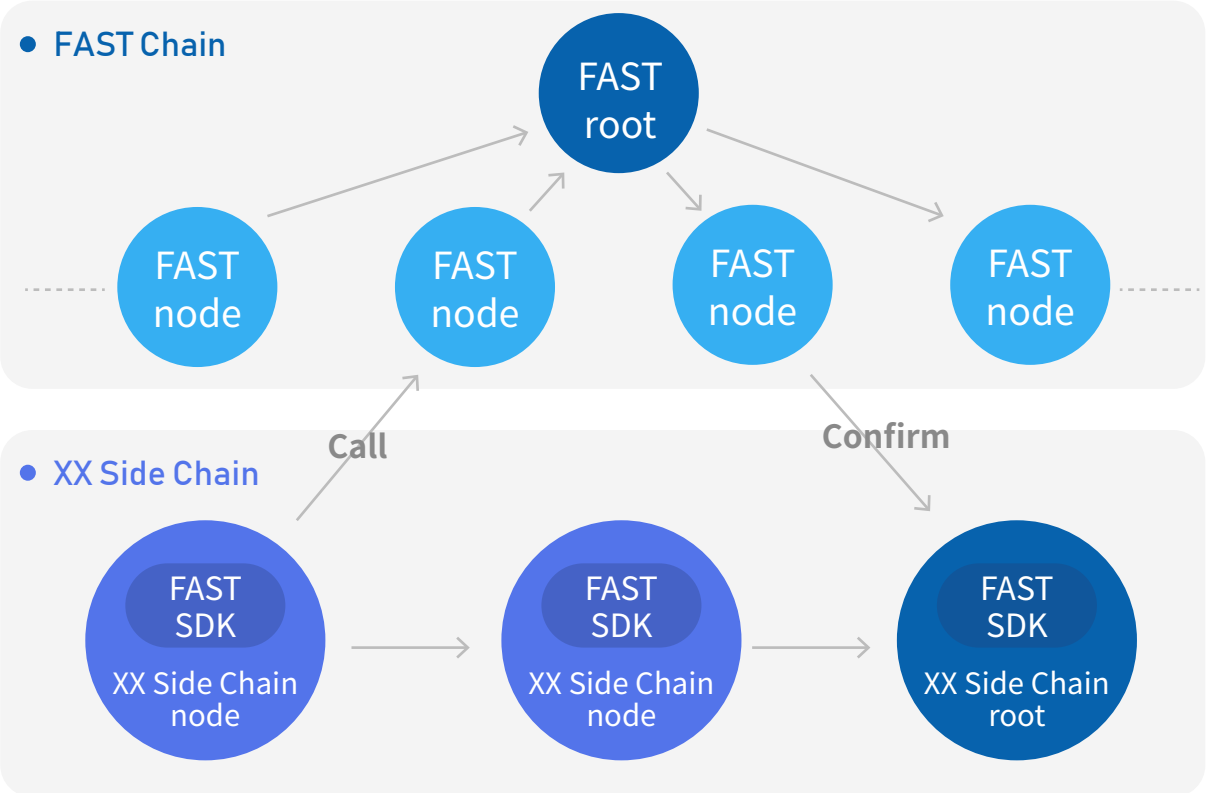
量子计算机的出现将对基于RSA和ECC的密码学机制产生重大挑战。量子计算机能够在极短的时间内解决RSA所依赖的大数分解问题和ECC所依赖的椭圆曲线离散对数问题。目前，量子计算机尚无快速解决最短向量问题(SVP)和最近向量问题(CVP)的能力，格密码学被认为是抵御量子计算机的最可靠算法。

为了抵御未来硬件升级对加密算法的影响，FAST直接采用格密码的算法来保证FAST Chain的安全性。

2.5 侧链设计及扩展性支持

未来的区块链世界必然是一个多链组合交互的复合生态。区块链核心解决的是信任问题。支付是信任的核心。所以性能强劲、费率低廉的FAST Chain必然会成为整个区块链世界的坚实基础。

但必须指出的是，FAST是区块链世界的基础而不是全部。所以FAST必须要有优秀的扩展性，能方便的与其它区块链对接。



如上图所示，FAST会提供开发SDK，供其它区块链开发者使用。其它区块链的开发者只要通过调用 FAST SDK，就能让自己的链马上享受FAST高效能、低费率转账/支付能力。

2.6 开发语言和SDK支持

FAST Chain基于C++语言开发。C++语言具有高性能的特点，是开发高性能服务的首选语言。同时C++语言又能方便的嵌入其它语言提供扩展支持。

FAST开发者社区会优先完成以下三个项目：

1. C++版本的全节点及对应SDK
2. C++版本的钱包节点及对应SDK
3. Javascript版本的钱包节点及对应SDK

基于C++版本的全节点及对应的SDK，FAST开发者社区会为以下项目（但不限于）提供支持：

1. JAVA版本的全节点SDK
2. Golang版本的全节点SDK
3. Python版本的全节点SDK
4. NodeJS版本的全节点SDK

基于C++版本的钱包节点及对应的SDK，FAST开发者社区会为以下项目（但不限于）提供支持：

1. Android版本的钱包节点SDK
2. iOS版本的钱包节点SDK

2.7 性能指标

根据目前的测试效果，FAST Chain矿工节点的演示版本在单服务器上可以轻松达到数千TPS。经过充分优化后，FAST Chain矿工节点有望达到单服务器数万TPS。

如果我们对转账地址进行分片，矿工节点可以使用集群技术。支持分片和集群技术的矿工节点理论上仅受带宽的限制，可以支撑近乎无限的TPS。

FAST Chain转账/支付的实时性受限于DMT的层数。而层数会受FAST Chain网络的节点总量以及节点TPS影响。按1万TPS计算，5层DMT树即可支持1亿亿个节点，足够供应全世界相当长时间内的需求。而按每个节点平均响应时间250ms估算，5层DMT树的平均确认时间仅1秒，用户平均响应时间仅需2.5秒，已经接近ApplePay、AliPay、Paypal等集中式支付工具的体验。即便按照每个节点平均响应时间500ms估算，平均确认时间也仅需2秒，用户平均响应时间仅需5秒。

FAST与其他主流公链的对比：

	BTC	ETH	EOS	FAST
总发行量	2100万	≈9950万	10亿	100亿
共识机制	POW	POW -> POS	DPOS	POP
出块间隔	10min	12s	1.5s	Real-time
平均确认时间	≈43min	≈1min	≈3s	≈1s
TPS	7.3	30-40	100,000	＞10,000,000

2.8 智能合约侧链

FAST Chain本身是支付链，不包含智能合约。但可以基于FAST Chain开发图灵完备的多种智能合约侧链。智能合约链将为大大提升基于FAST生态的发育速度。FAST开发者社区在智能合约侧链方面有以下的规划：

1. 使用Lua或Javascript为开发语言，避免重复发明轮子
2. 同样采用能力共识，但会与FAST Chain有一定差异：由于按时完成合约可以收取手续费，在机器资源充沛的前提下矿工都会倾向自己执行合约赚取手续费，而后续节点只需要全网同步合约执行结果即可。这样我们就可以拥有海量的矿工节点来执行智能合约，而不是像现在主流的区块链技术，只有出块节点才能执行智能合约，大大提高了智能合约的执行效率和实时性
3. 智能合约侧链与FAST Chain之间会使用类似闪电网络的技术，用户先把预付款通过FAST Chain转账到一个临时钱包，且钱包私钥和余额被智能合约保管。智能合约执行的过程中会不断扣除手续费。当合约执行完毕或预付款扣完则结束
4. 关于智能合约侧链更具体的设计，会在未来FAST开发者社区中细化和完善

2.9 交易所侧链

FAST Chain本身是支付链,不包含交易所。但可以基于FAST Chain和智能合约链开发去中心化交易所的侧链。交易所侧链将会向所有基于FAST生态上的区块链免费开放。交易所侧链会大大提升FAST Token以及基于FAST生态区块链的流通性,有效的帮助FAST生态区块链的建设。FAST开发者社区在交易所侧链方面有以下的规划:

1. 同样采用能力共识,但会与FAST Chain有一定差异:由于撮合交易可以收取手续费,所以矿工都会倾向在自己的客户范围内尽可能的撮合交易,而后续节点则继续尝试撮合剩余交易,并全网同步撮合执行结果即可,大大提高了交易撮合的效率和实时性
2. 对于实时性低下的传统区块链资产,交易所链会通过一个智能合约链上的DApp进行管理,提高交易的实时性
3. 每一条链完成FAST Token与一种资产的交易
4. 关于交易所侧链更具体的设计,会在未来FAST开发者社区中细化和完善

2.10 数据存储侧链

FAST Chain本身是支付链,不包含数据存储功能。但可以基于FAST Chain开发数据存储侧链。数据存储侧链将会采用类似DAG的共识算法,主要用于解决物联网设备支付、海量运行数据记录和物联网设备资源共享的问题。关于数据存储侧链更具体的设计,会在未来FAST开发者社区中细化和完善。

03 FAST Chain应用特性与场景案例

3.1 应用特性

3.1.1 交易速度

FAST Chain最根本的特性是为安全快速的交易提供技术基础。

FAST Chain交易速度参考值:

- 测试链单服务器TPS大于10万;
- 测试链支付全球主干网络连接时间小于500ms,平均完成时间小于5秒;
- 全球主干网络TPS大于800万;

3.1.2 可扩展性

FAST Chain底层的交易链,可以扩展支持多种智能合约语言,交易所和智能合约DAPP等上层应用。这意味着,任何有经验的区块链开发者,都可以在FAST Chain扩展开发自己的应用。应用链业务与交易链分层的架构,更可以为FAST Chain的扩展应用提供与交易性能类似的良好体验。

3.1.3 跨链通讯

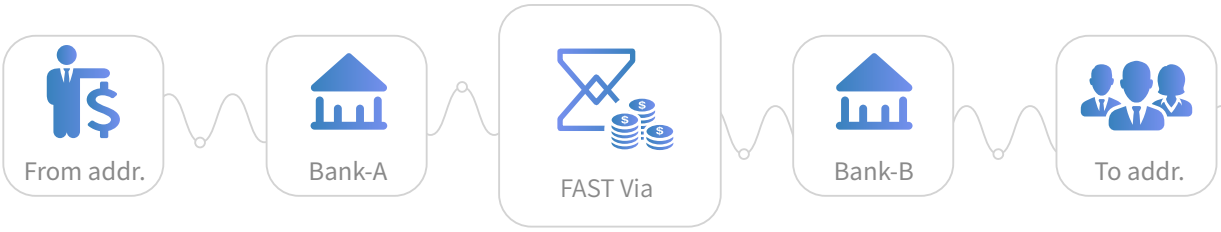
跨链通讯是高级的扩展功能,FAST Chain会基于优化的Plasma、Sharding等技术实现跨链通讯。使得FAST Chain上的交易条件可以基于任何一个区块链公链上的事件制定(1.0版本跨链协议将支持BTC和ETH,后续由开源社区扩展更多项目支持)。最终目标,FAST Chain连接所有区块链项目,并让不同区块链间的通讯可以像内部智能合约一样的顺畅和安全,甚至可以提高诸如比特币这类早期项目的可用性也大大提高。保证全球生态

3.1.4 风险即时响应

因为数据头验证结果是节点获得奖惩的基本要件，因此节点的主观作恶或客观硬件宕机等情形，全网的响应速度会在秒级以内。从而保证交易的安全性。

3.2 FAST Chain金融场景应用框架FAST Via

FAST Via是基于FAST底层交易链的适用于跨境跨行结算的一种应用模式，使用FAST（快链的通证）作为交易媒介完成交易。

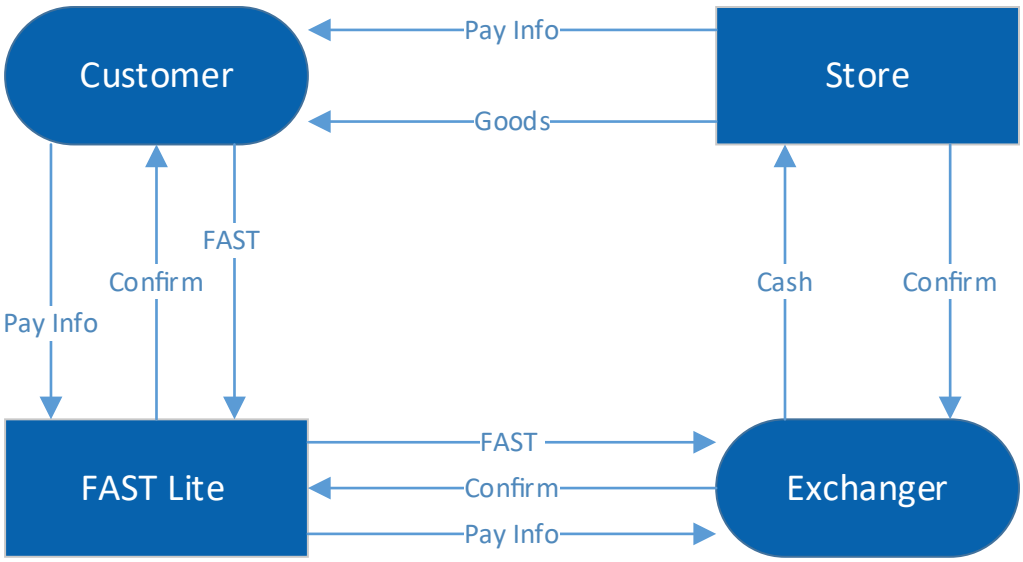


FAST Via应用模式示意图

主要为银行与银行之间提供跨境交易。FAST Via作为银行间的清算应用，使用特别的银行节点强化验证，每当有银行A向银行B转账，可以通过FAST Via进行清算。实质上是通过分布式账本，使A在FAST Via上托管的银行账户及B在FAST Via上托管的银行账户内的金额发生了转变。因为FAST Chain的安全性和高实时性，可以完全替代过去繁琐的跨境交易过程。FAST Via仅支持银行节点间的专用隧道协议，各银行直接可以自行开发节点授权方案，用普通用户节点构造银行间的通道，提高特定银行间的交易能力。普通用户节点则可以在这个过程中获得与验证交易付出相匹配的价值回报。

3.3 FAST Chain商户小额消费应用框架FAST Lite

在FAST Lite网络中，消费者、购币者、节点和收单方都是网络的参与方，都通过去中心化的体系，可以实现自运作。其中消费者是指在商家处用FAST购物的用户。购FAST者是希望用法币购买FAST的用户。节点则是在FAST Lit网络中提供支付通道实现联通的专业个体，通过提供服务获得手续费收益。收单方负责从购币者扣款并与商户方进行法币结算。



FAST Lite 应用模式示意图

整个流程中,智能合约是保证交易自动传递的机制,图中的Confirm是交易确认信息,类似于收据,有收据即可向上游换取FAST。从上图也可以看出,FAST Lite的去中心化是由两个流程驱动的去中心化,一个是消费者使用FAST购物的过程,一个是购FAST者将法币兑换成FAST的过程。两个过程相向而动,把它们连接起来的是FAST Lite网络。

3.4 应用模式开发的价值

项目应用的常态运作,是FAST Chain优异性能的最好证明,为了降低开发门槛,让更多的项目加入FAST Chain,应用模式的开发是必不可少的环节。同时,行业级的应用为FAST获得稳定的价值共识提供良好的锚定依据。

04 FAST Chain路线图

项目正式启动 2018年3月

2018年8月 DEMO版本面世

通过包含真实性验证的测试方案，对DEMO版本单节点和多节点交易性能和交易正确性做公开测试。

测试版交易结算链 2018年10月

将包含移动端及网页钱包，支持完整交易功能的测试版本，对项目早期支持者开放测试。

单服务器单节点有望 10000 TPS

多节点有望达到 8000 TPS

两层网络平均传播速度约 500 ms（到主节点）

2019年1月 FAST Chain主网正式启动

包含完整交易结算功能的正式版FAST Chain启动运营。全球范围内开发者Kickoff Meeting启动。

智能合约测试网络发布 2019年4月

完成智能合约开发者所需的工具，并交付测试。该测试网络也将服务于主网上线前开发者的各类测试。

2019年10月 交易所链开放测试

通过FAST的侧链，打通与多种主流加密货币的通讯。使得加密货币之间方便快捷的，并支持智能合约的去中心化交易兑换，成为现实。

行业生态确立 2020年1月

基于核心团队主导的智能合约链正式版持续迭代的促进。相关行业应用初见成效，形成具有指数型增长态势的行业应用生态。

05 FAST Plus基金会

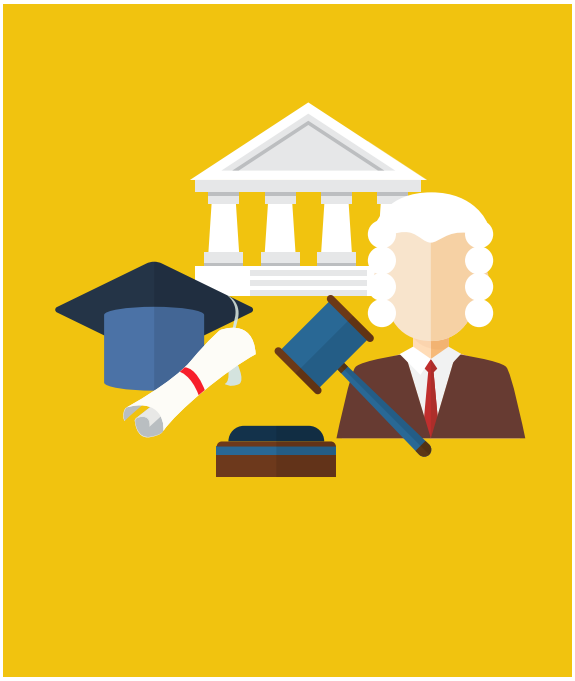
FAST Plus基金会介绍

FAST Plus基金会将于2019年1月1日在海外成立，作为一家非营利性的数字货币交易公司，将致力于提供交易，技术开发，国际牌照申请，交易所对接和合规运营，并且满足FAST社区公共事务的需要。该基金会致力于保护和规范快链协议、钱包等软件，在法律开放的国家和地区进行公众教育扩大FAST的使用，并且培养安全、健全的法律和监管环境，也通过联系FAST社区的全球网络，保护，增强和发展快链生态系统，及生态内的项目落地。

基金会的核心成员是开发人员，研究人员，顾问和业务开发人员，核心任务在于规范，保护和推广FAST Chain协议技术。

基金会重点领域

1. 维护并规范FAST Chain共识协议和加密技术标准；
2. 发起、支持和帮助FAST Chain开发社区和FAST用户社区的运作；
3. 连接更多商业，企业和区块链社区，与其达成战略合作，通过发挥FAST Chain的在交易环节的优势，将不同的区块链项目和不同的行业应用联系起来，构建更的区块链



06 FAST项目核心成员

Atlas
创始人
CEO

中科大计算机硕士
阿里移动总架构师(P9)
知名物联网公司技术合伙人
20年开发经验
区块链技术研究专家

Davis
创始人
COO

蚂蚁金服产品专家(P7)
金融+区块链实战经验
做过2个亿级应用(手机酷狗、UC浏览器)
丰富的行业人脉

Diono
创始人
CRO

中山大学管理学院MBA
互联网金融专家
连续多个成功创业项目创始人
曾任某通信运营商移动互联网中心经理
20年团队管理和项目风险评估经验

Cheng
联合创始人
CTO/架构师

国防科技大学毕业
阿里大文娱资深技术专家(P9)
10年高性能分布式系统架构和开发经验

Scott
联合创始人
CPO

前酷狗音乐产品经理
知名教育培训机构高级产品经理
产品经理社群WOSHIPM创始团队成员
BGC游戏区块链生态战略顾问
链码LINKMAX区块链咨询创始人

07 九、基石投资人及战略顾问

暂不公开

暂不公开

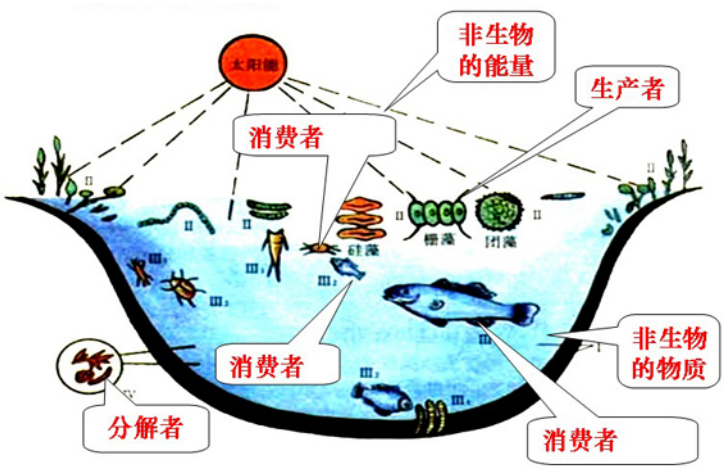
暂不公开

暂不公开

08 FAST愿景

FAST最初的含义取自其技术拥有的四种特性，Flexible-可扩展的，Agile-快捷的，Safe-安全的，Trusty-可靠的。我们希望通过在这四个方面的突破性进展，可以更好的让区块链技术服务于商业世界的每一个角落。

实际上，在开发的过程中通过深入研究多个领域的竞争业态，引发了我们更多思考。越发深刻理解区块链技术对于商业世界的意义，即任何一个为争夺行业地位而展开的商业竞争，通常都会伴随着多个竞争方的成本沉没，并以终端消费者为垄断者前期竞争付出的成本买单结束。其根本，是同业内不同主体之间难以在分工和利益分配层面达成共识。区块链通过提高共识的执行，逐步推动稳定的分工协作和广泛的利益共享，进而促进行业生态的持续优化。这种理想状态下的商业系统架构，非常类似完全由内生驱动而长期稳定运行的，自然生态系统，



自然生态系统示意图

而生态系统开放性是一切自然生态系统的共同特征。我们也借用其开放性的主要表现：

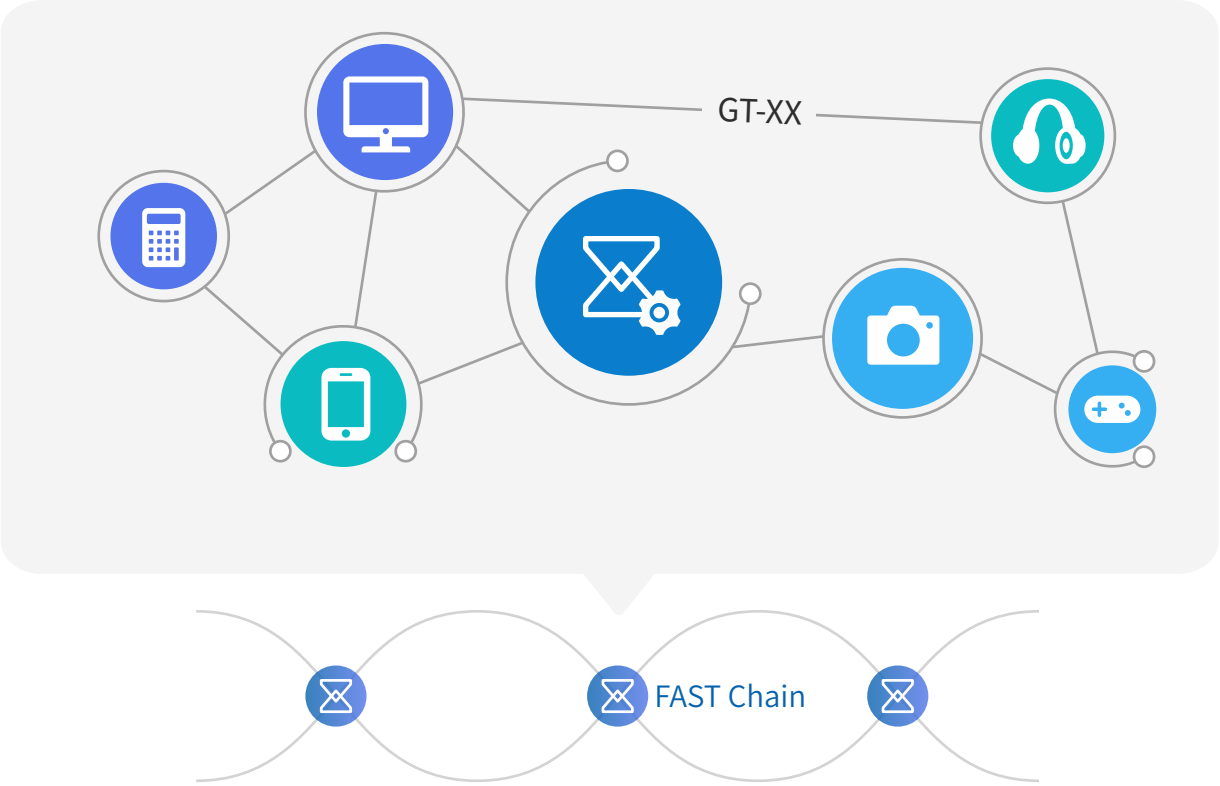
(1) 全方位开放

(2) 进行熵的交换

(3) 促使要素间的交流

(4) 系统结构内部具有不断发展的动力

列举一个FAST在物联网领域的应用提议。即为了有效提高机器与机器之间的数据交易(M2M),不同规格的传感器可以在多种“贡献-回报”(Give-Take)模式,中选择与设备规格和应用场景相一致的模式,免费获得使用FAST网络的资源,



GT-00 数据存储共享模式:使用此协议调用FAST Lite的设备,需满足一定的存储空间规格。在FAST Lite网络中使用的数据流量不会超过存储空间共享数据的使用流量。

GT-01 业务数据协同模式:此协议适用于与用户个人信息完全无关的数据协同设备,诸如用于公共天气服务的家庭环境数据(空气质量、温度曲线、气压等),贡献此类数据的设备,可以免费使用不超过相关分析节点索取的数据总量。

GT-02 计算能力共享模式:计算能力需求方,可以支付相应FAST获取GT-02 协议的网络,而协议获得的FAST都将用于满足计算贡献节点的FAST Lite网络使用需求。

……

FAST的愿景亦以明晰,即通过优化最基础的交易协议,以开放的态度拥抱更多的商业需求,接纳并大力支持技术社区促成相应模式的开发和落地。为更多行业或更多商业个体间生态系统的构建提供有效的推动。相信在更广泛的认同下,甚至可能为人类命运共同体的实现构建出一条具有高度可行性的实施路径。

09 免责声明

本文件不构成与此处所述任何公司证券相关的要约、请求、推荐或邀请。本白皮书不是要约文件或招股书，并严禁用于向没有相应资质的普通民众募资。

本白皮书提供的信息仅属底层技术性质，暂未接受任何专业法律、会计或财务顾问的审计、查验或分析。FAST Chain的风险繁多而重大，且项目仍在开发阶段，因此FAST Fund（及其董事、高管及员工）不对本白皮书所含信息的准确性、完整性、或者白皮书中任何错误而承担任何责任，并保留对白皮书内容修改的权利。

FAST Fund严格遵守各国家和地区的法律法规，仅对合格的机构投资者募集资金，并遵守相关投资协议维护项目投资人的利益。但FAST Fund不对任何非常规渠道流通的FAST的价值负责。

本白皮书的内容具有较强的技术性，需要非常熟悉分布式数据结构、加密算法、网络协议优化，才能理解FAST Chain及其相关技术风险。我们鼓励本文件的接收人寻求外部建议。接收人对外部对本文件所述的事项的评估，包括对风险的评估，以及对其技术和专业顾问的咨询全权负责。