White Paper

Turing Network

"Turing reserves the right of final interpre - tation"

Contents

1 概述
Overview

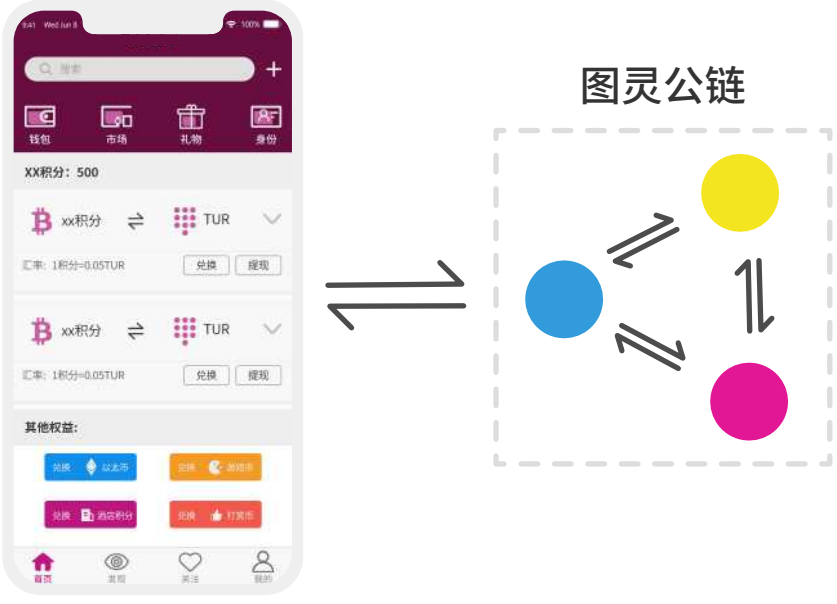
现存的区块链系统如BTC,ETH,EOS等都存在各种问题。BTC拥有最广泛的共识却极度消耗能源，交易性能缓慢。ETH拥有图灵完备的智能合约功能并提升了性能，但依然面临扩容困难，性能不足，GAS费用昂贵的问题。

EOS虽然拥有较高的性能，但是去中心化程度不足，难以成为全球公认的能承载互联网底层价值的区块链。与此同时，区块链和数字货币对于普通用户仍然有极高的认知和使用门槛。全球数字货币活跃用户的规模约为数百万，在全体移动互联网用户中的渗透率约为1‰，显然，区块链和数字货币仍处于发展早期。

如果说BTC代表了区块链1.0时代，以太坊代表了区块链2.0时代，那么我们认为2019年将会成为区块链3.0时代的元年。Cosmos已经在2019年3月主网上线，Polkadot也将在2019年第三季度主网上线。这两大明星跨链项目将会使区块链的互操作性提高到一个新的层次，同时开发公链项目的技术难度也会大大降低。这将为区块链3.0时代万链互联的愿景奠定坚实的基础。

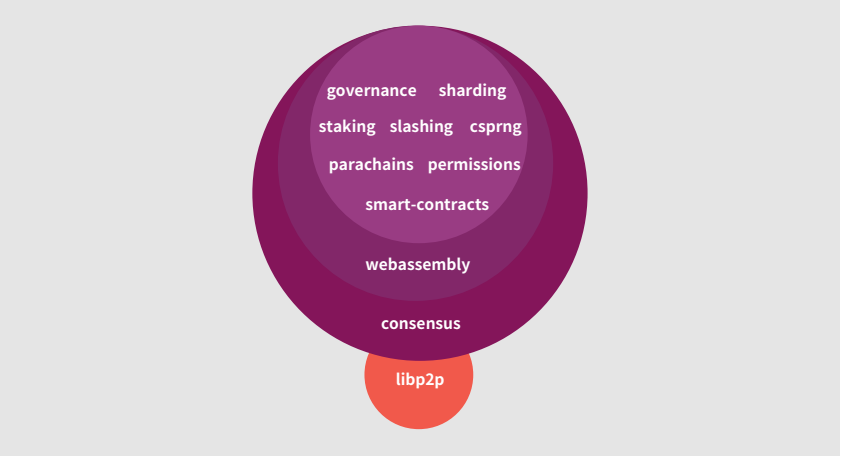
图灵区块链的目标是帮助全球移动互联网用户接入区块链和数字货币生态，为了实现这一目标，图灵区块链整体都是围绕开发者利益打造的。它首先是一个帮助所有移动互联网应用快速接入区块链生态的项目。我们将为移动互联网开发者提供完整的开发套件，开发者可以通过调用客户端SDK，将移动互联网应用中的积分权益和区块链结合，并且通过区块链系统管理后台为自己的用户生成区块链公私钥。

终端用户虽然不持有私钥，但是通过开发者服务器代理，可以实现区块链转账，支付等操作，也可以向交易所充值。这种方式避免了让普通用户接触到公私钥等专业概念，也可以完全兼容APP原有的账户系统，比让用户持有私钥的使用方式更简单。这样设计的意义是能让移动互联网用户无感知地进入区块链世界。



2 技术框架
Technical frame work

Polkadot 是 Web3 基金会发起的项目。由以太坊前CTO Gavin Wood 博士创办的 Parity 公司设计和研发。Polkadot 致力于实现链间任意消息通信，将解决区块链的互通性问题，进而实现多链并存，解决扩展性和多样性问题。Polkadot开发了通用的基础链框架 Substrate，实现了混合 POS 共识、链上议会治理、Wasm 和 EVM 虚拟机、智能合约原生执行、高效轻客户端协议等。



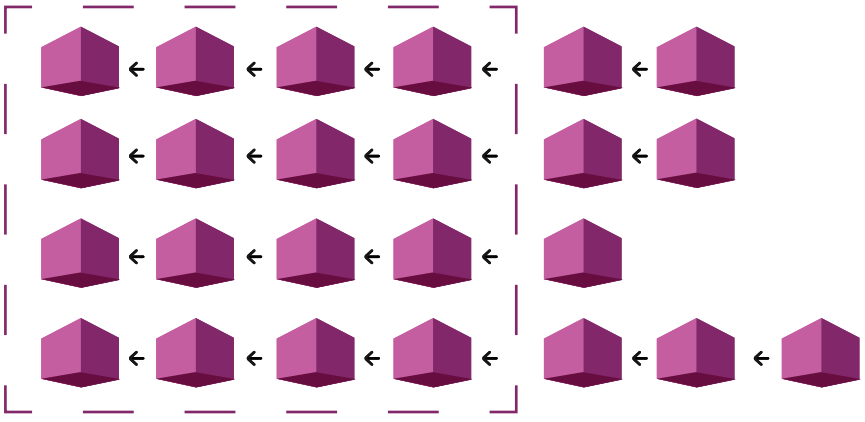
目前包括以太坊 2.0 的 Shasper，Zcash 的 zk-snarks也正在此框架上实现。图灵区块链将使用Substrate作为底层开发框架，使用Aura + Grandpa混合共识（一种可支持数千节点的混合POS共识）作为默认共识算法，使用Wasm和EVM作为作为智能合约执行环境。Substrate 只提供了最基础的链模型，而且在持续演进之中。Substrate 只提供了最基础的链模型，而且在持续演进之中。图灵区块链将紧跟 Substrate 框架的升级，持续引入新功能。同时我们仍然需要在 Substrate 上开发大量新功能，包括企业级区块链管理系统，客户端SDK，常用智能合约模版库，公链治理工具，图灵官方钱包等。

3 共识算法
Consensus algorithm

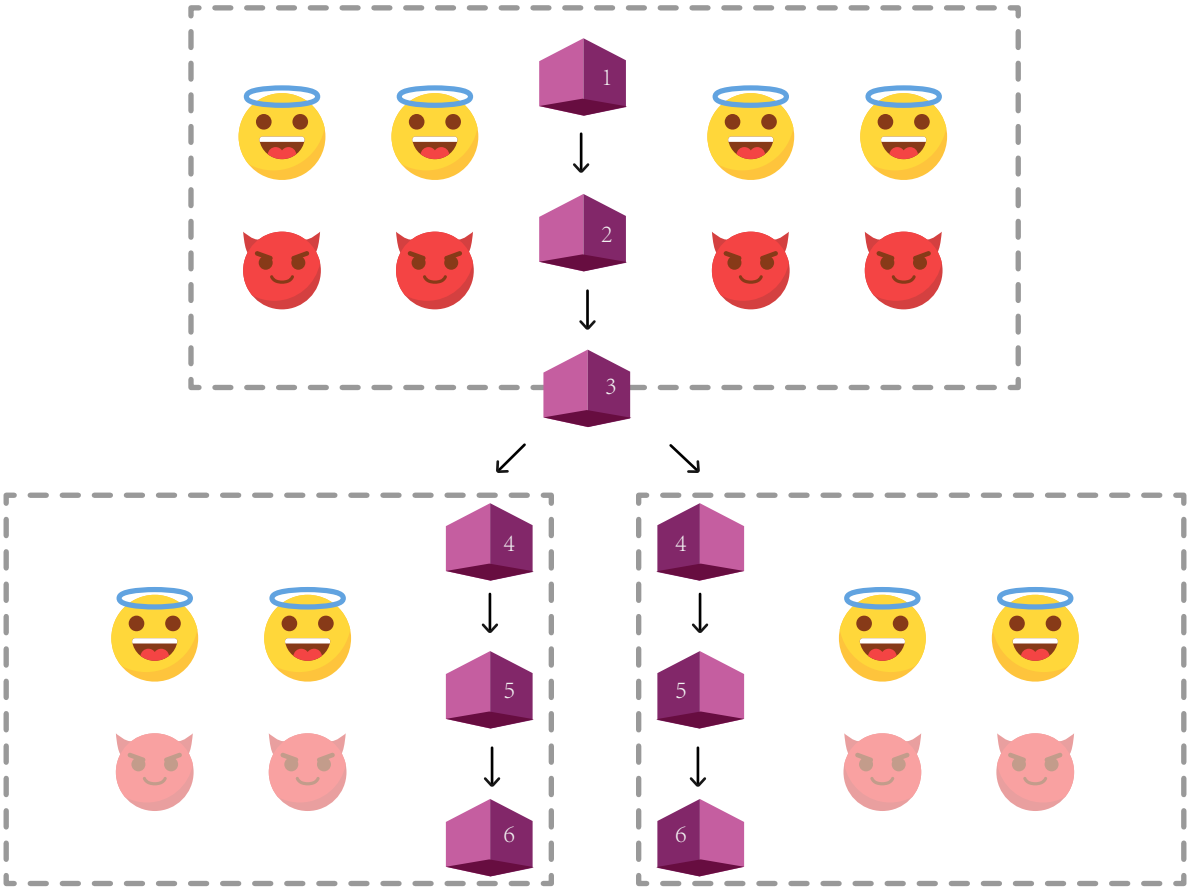
图灵公链采用 Aura+Grandpa 混合共识，能够支持1000个以上的共识节点，1-2s 的出块时间，10s 以内的最终确定性延迟。这种混合共识，既有POW的分散性，又没有POW的能源浪费问题。还能提供100%的确定性，而不是POW的概率确定性。尤其是在性能方面，POW不可与之同日而语。

Aura（提议者节点和概率最终性的授权回合）提供了快速并发出块性，像POW一样节点分散，可以支持数万节点同时在同一高度同时出块。GRANDPA（基于GHOST的递归祖先派生前缀协议）在混合共识区块链中提供近乎即时的，异步的，负责任安全的最终确定性。

在良好的网络条件下，我们几乎可以立即确定区块。当网络从长时间分区恢复时，GRANDPA可以一次完成数万个块，只要用BFT确认最后一个大家公认的块即可。相比传统的PBFT共识，GRANDPA共识的通信消息量减少了99%以上。



这里有很多链，但它们各有一个共同的前缀
POW共识保证了一个概率，而GRANDPA确定了这一点

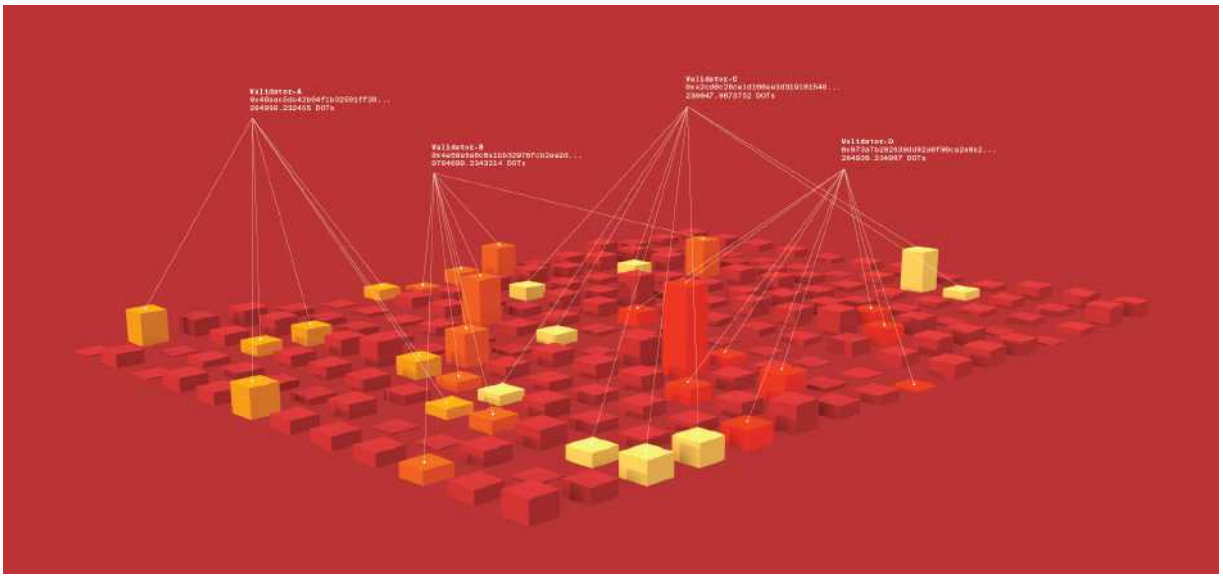


负责任的安全性：

尽管恶意验证器分叉了网络，但是可以检测到它们的不当行为，并且可以在分支的两侧削减其利益。

4 Staking经济
Staking economy

图灵公链将采用提名权益证明（NPOS），一种新型的POS方案来选择哪些验证人能够参与一致性协议的验证。



首先，图灵基金会将在全球招募图灵超级节点作为候选验证人集合。超级节点必须在系统中抵押一定数量的TNK代币作为他们诚实行为的保证。当他们正确执行验证人的行为时，他们将会得到良好的报酬，如果他们偏离了验证人的行为准则，他们抵押的代币将会被削减。

同时，系统将鼓励任何TNK代币持有者作为提名人参与验证人选举投票。一个提名人可以选择一组他信任的超级节点担任验证人，并抵押一定数量的TNK来支持他们。如果其中一些超级节点当选为验证人，他会按照抵押TNK的数量与验证人分享奖励或分担惩罚。与固定数量验证人不同，提名人的数量是没有限制的。只要提名人支持具有良好安全行为的验证人候选人，他的角色风险较低，并能提供持续的收入来源。

该提名人/验证人制度提供了强有力的安全保障。在任何特定时刻，我们都预计将有相当一部分TNK供应量存放在NPoS中。这使得作恶实体很难获得足够的选票来当选验证人（因为他们需要建立相当广泛的声誉来获得所需的支支），并且攻击系统成本非常高（因为任何攻击都会导致大量的TNK被削减）。

为了解决过去PoS运行后，因为区块奖励与Staking量正相关造成马太效应，代币分配趋向中心化的问题。NPoS里最终奖励结果不是依据Staking量，而是依据每个被选出节点出块的工作量计算。并且一旦验证人节点确定后，会将提名人的Staking量尽可能平均地分给每个被选上的验证人节点。具体来说，NPOS算法有以下客观目标：

1 平衡Balance

一旦选举人委员会确定后，会将持币人Nominators的Staking量尽可能平均分配给每个选上的选举人Validators。

PS: 持币人是可以选择多个选举人的，所以存在系统重新分配空间。

2 最大支持Support

选出一个选举人委员会，委员会中的选举人Validators收到的Staking量要尽可能贴近总持币用户Nominators的Staking量。

3 公平代表FairRepresentation

选出一个选举人委员会，其中持币人Nominators的投票权不会被过度代表，也不会被低估代表。

PS: 持币人可以选择多个节点，公平代表最简化是，每个持币人对应到的节点至少有一个会被选出，加上现实条件（持币状况及系统要选出几个节点）后有些节点会被淘汰，但尽可能保证拥有一定Staking权重的持币人可以至少对应到一个节点。

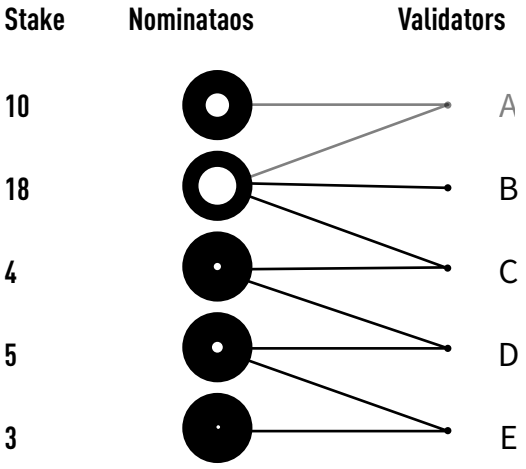
NPOS将解决以下问题
NPOS will solve the following problems

1 一部分不可避免地中心化问题

2 低手续费不会无限地吸引Staking量，因为收益是看超级节点工作量（现在 Cosmos主网上就出现0手续费节点吸引大量持币人委托）

3 持币人可以通过挑选不同超级节点最大化自己利益，同时促进去中心化（对于持币人就可以有多种委托策略，我可以挑选最大最可靠的超级节点，同时也可以挑选一些小而美的超级节点，可以获得更高收益率）

First picture



NPOS Election with unfair representation

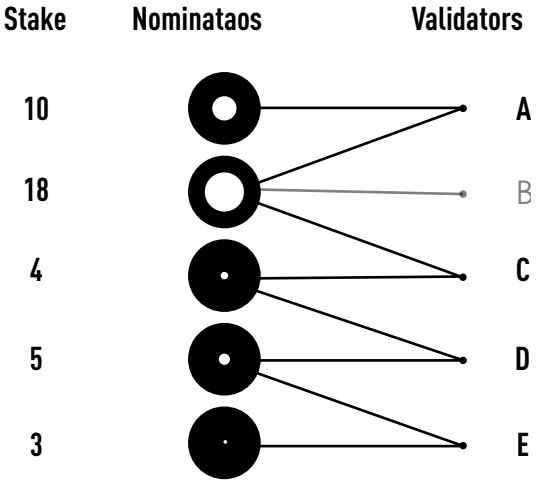
第一张图

并不符合公平代表（FairRepresenta - tion）的目标，因为图中第一个持币人拥有10TNK的权重，相比第五个持币人只有3TNK的权重，最终却没有对应到任何他支持的节点，不符合公平代表目标拥有一定Staking权重的持币人至少对应到一个节点（在现在情况下，第一个持币人是拿不到奖励的）。

第二张图

符合公平代表（FairRepresentation）的目标，有些人可能会质疑为什么E节点选上了，而B节点没有选上，这和接下来会举例的重新分配算法相关，这边简单理解，图中第二个持币人同时支持了3个节点，系统只要保证他支持的节点至少有一个被选举上就好（这边他支持的节点有两个选上，第二个持币人所有Staking量将会被分配到这两个节点上），同时保持第五个持币人也有支持的节点E，对于Polkadot这样的选举结果是可能之一。

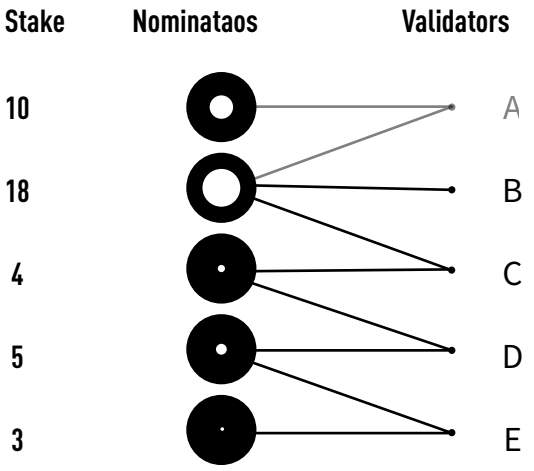
Second picture



NPOS Election with fair representation

Third picture

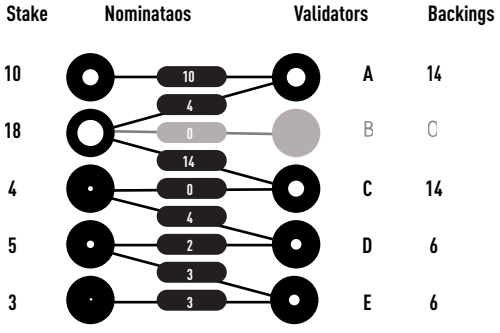
第三张图



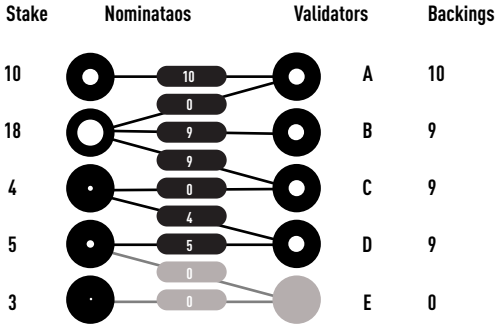
NPOS Election with unfair representation

符合公平代表（FairRepresentation）的目标，有些人可能会质疑这个与第二张图产生矛盾，目标是尽可能让每个持币人最少要有一个支持节点被选上，那第5个持币人支持的节点没有被选上，因为整个系统只需要选出4个节点，所以第五个Staking权重低的持币人支持的节点没有选上的结果是可能之一。

下图是两个符合公平原则的选举人委员会可能结果，确立选举人委员会后系统还要经过Staking权重重新分配。Turing共识系统会在每次从中选出一个更公平分配且具备安全性的结果，这个例子中选择右边因为它平均分配的更好，右边的节点中平均最低都拥有了9的Staking权重。



NPOS Election with fair representation and security level 6



NPOS Election with fair representation and security level 9

5 超级节点
Super node

超级节点是图灵公链生态最重要的组成部分，也是图灵公链安全运行的守护者。我们对超级节点的运行规则有非常详细的设计方案，第一版超级节点规则如下：

1 超级节点需要提供高性能公网服务器一台（具体配置将在图灵公链主网上线前公布）用于部署图灵公链全节点客户端，以太坊全节点客户端，IPFS节点软件。

2 超级节点需要购买一定数量的TNK代币并抵押在系统内参与POS挖矿（具体抵押数量会在图灵公链主网上线前公布）。如果超级节点行为正确，他将获得区块奖励，如果超级节点存在恶意行为，他抵押的代币将被削减。超级节点需要确保7*24小时在线，抵押的TNK数量需要高于最低抵押量，不能满足以上要求的节点将被取消超级节点资格。

3 超级节点可以接受TNK代币委托并代理挖矿，超级节点可以自行设置挖矿手续费率。

4 超级节点必须是互联网公司，拥有自己的APP/小程序/网站并且活跃用户量达到一定规模。超级节点必须有意愿将自己的部分业务迁移到图灵公链上来。

5 超级节点可以享受图灵官方免费技术支持，超级节点可以发行自己的Token并获得企业通证经济模型设计支持。超级节点专属企业级区块链管理软件，超级节点联盟，融资上币服务等。

6 图灵公链上线时，我们将会有30个超级节点，此后每月增加5个超级节点，直到最终图灵公链会有1000个超级节点。

区块链治理是一个各方相互协调的过程。目前的治理方式主要有两种，一种是链下治理，一种是链上治理。链上治理是确定性的，谁能够参与治理，怎么参与，怎么实施，都有着明确的定义和裁定。链下治理则比较随意，并没有严格精确的流程。

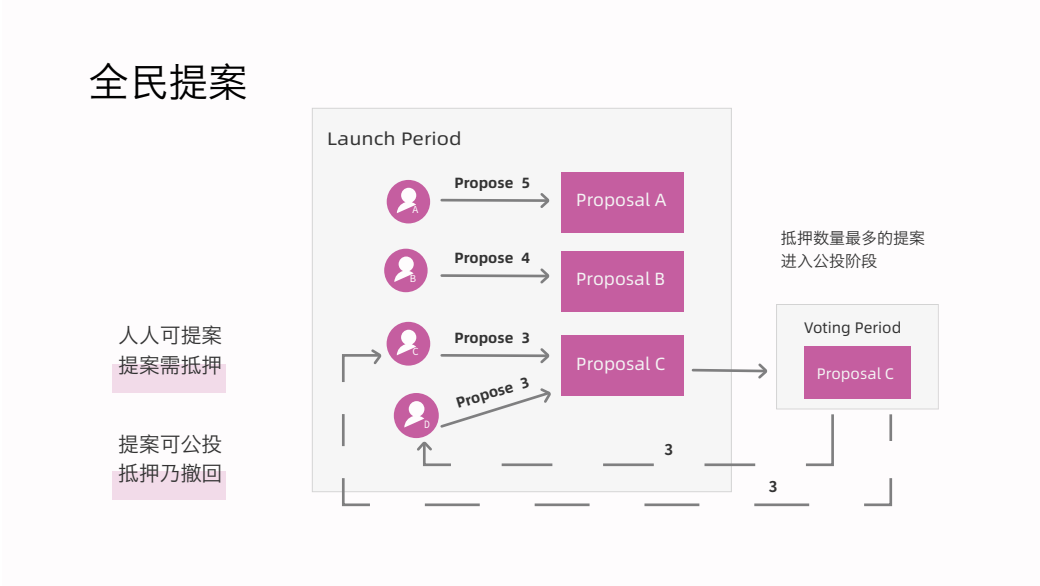
比特币、以太坊以及不少公链采用的治理方式都是链下治理。在表现形式上，这些公链项目会在 GitHub 上有个仓库，专门用于收集和讨论提案。如果提案讨论的人很多，那就很可能会正式地成为协议的一部分。

然后就是编码实现，部署升级等等。当然，这是比较顺利的情况。然而当链下治理出现分歧，也就是各方意见不一致不可调和之时，可能就会出现分叉的情况，这也是 ETC，BCH 的由来。

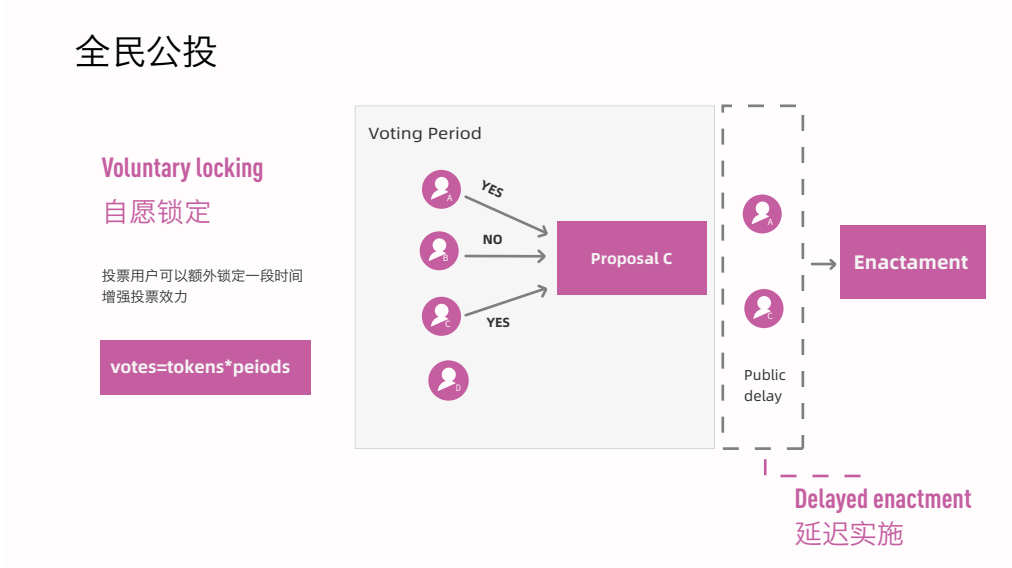
链上治理则有一个明确的治理流程，什么情况下可以提出提案、如何投票、怎样算通过， 什么时候执行，都是有确定性的。我们的提案在链上的表现形式是一段代码, 实施提案就是函数调用 `set_code`。 `set_code` 拥有至高无上的权利，可以做任何事情，可以直接改变区块链的状态。

图灵公链采用链上治理的方式，它的链上治理基本原则是：所有协议级别改动必须通过全民公投,拥有更多投票的人将拥有网络话语权。主要的构成有全民公投,议会，财政系统等，执行细则上有自愿锁定增强投票力，延时实施提案，自适应法定人数偏差等。

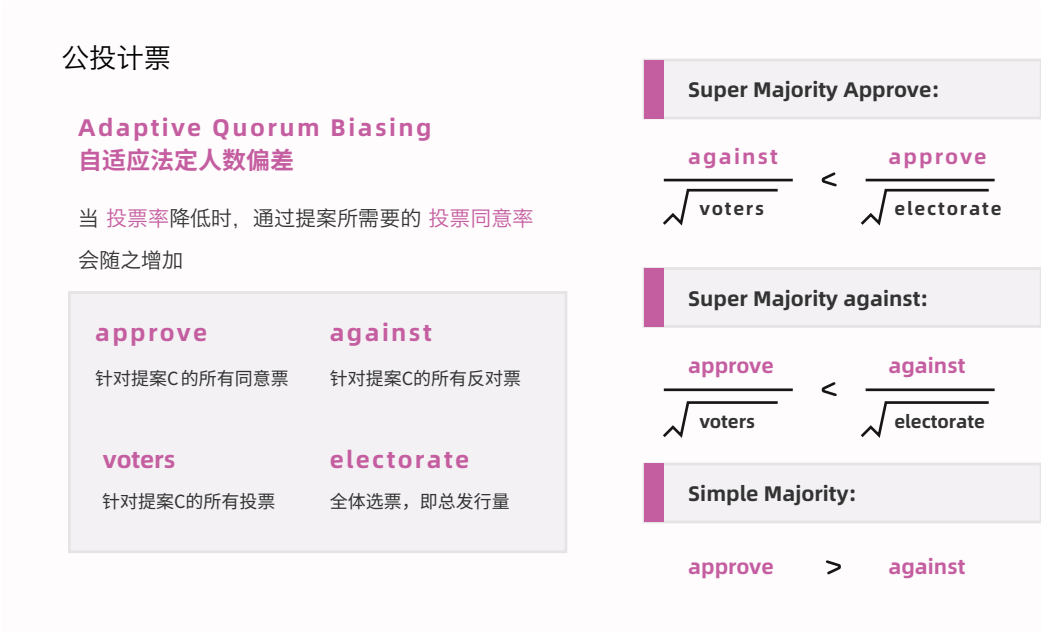
一个完成的治理流程大致有三个阶段。首先是全民提案阶段，在这个阶段所有人都可抵押一定数量的币进行提案。然后是全民公投阶段，每隔一段时间，抵押数量最高的提案将会进入公投阶段，所有用户可以对该提案表达支持或反对意见。最后是计票实施，当投票阶段完成后，如果提案得到了足够多的支持，那么就会按照机制实施提案。在全民公投阶段，议会可能会有所干预，在一定情况下，议会可以取消或者发起公投。



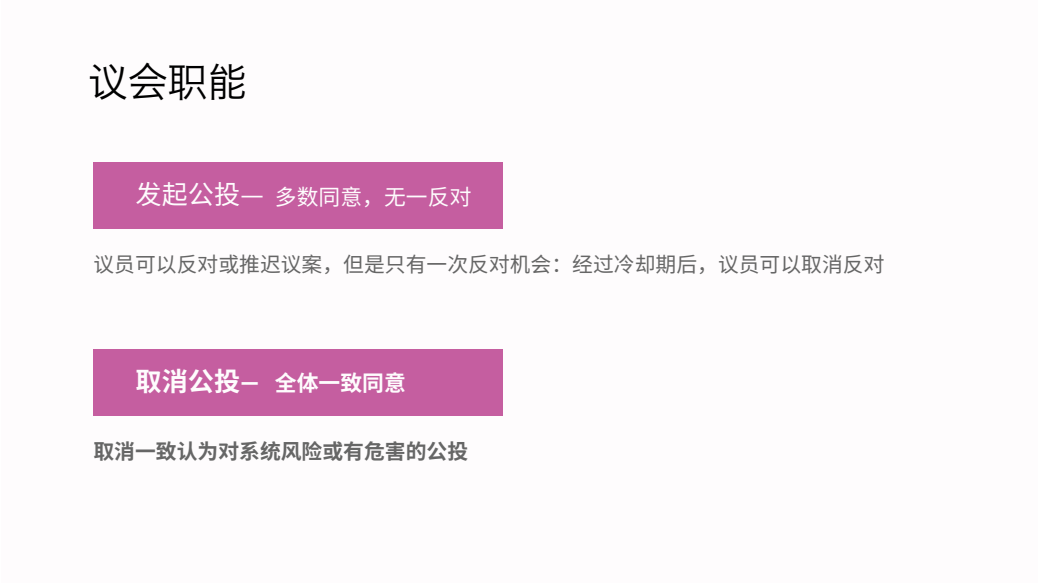
在全民提案阶段，每个人都可以发起提案，但是提案人必须抵押一定量的币，抵押数有最小值限定。 除了自己发起提案，用户也可以支持别人的提案。支持他人提案时，需抵押与原提案人等量的币。每隔一段时间，抵押数量最多的提案进入公投阶段，此时在提案阶段支持该提案的所有人所抵押的币将会自动返回。



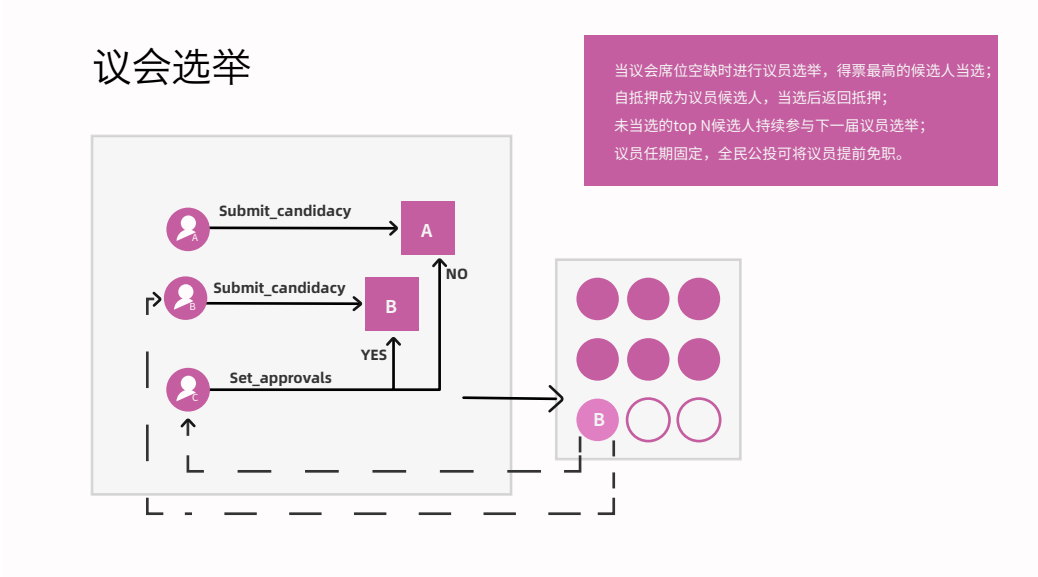
在全民公投阶段，用户可以选择支持或反对当前提案，当然也可以不表达任何意见。假使提案最终提过，原则上会经过一段延时，然后才会自动实施。而对于表达支持意见的人，一旦提案通过，自己的币也会至少被锁定一个延时的时间。另外，在投票阶段，用户可以通过自愿锁定更长时间来增强投票力，简单来说，一个币锁定六天等同于六个币锁定一天的投票力。



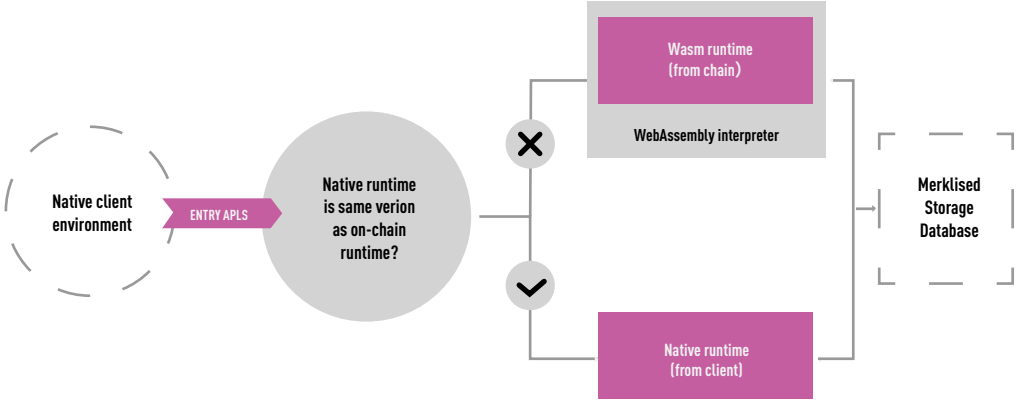
对于一个提案是否通过，有三种计算方式。 总结来说，当投票率降低时，通过提案所需要的投票同意率会随之提高。



议会主要有两个任务：发起公投和取消公投。所有议员多数同意，无一反对，议会即可直接发起一个公投。当所有议员一致同意某些公投会对系统造成危害，或是有风险时，也可取消公投。



议员席位固定，任期固定，全民公投可将议员提前免职。当议会席位空缺时进行议员选举，得票最高的候选人当选。任何人都可以通过自抵押提交候选人申请成为议员候选人，当选后返回抵押。未当选的 top N 候选人持续参与下一届议员选举。



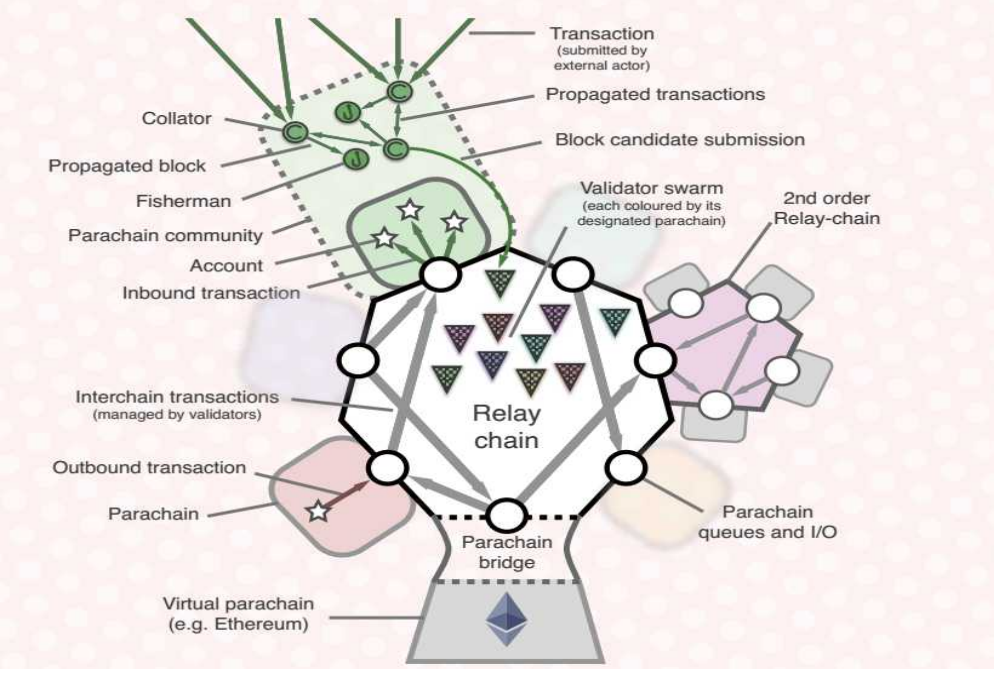
当链上更新运行时映像时，某些客户端尚未更新其软件。在这种情况下，他们的节点将通过在Substrate的集成Wasm虚拟机上解释它来执行正确版本的运行时。因此，在任何情况下，网络上的所有节点始终能够正确地同步链（尽管处于不同的效率级别），从而防止了链式分支。

7 异构跨链
Heterogeneous cross-chain

区块链的互操作性将是区块链3.0的核心主题，并将加速推动去中心化网络的普及。Polkadot项目致力于在区块链之间构建网络协议，以实现安全可靠的交互。基于这些协议产生的新区块链可以在链之间发送交易和传递讯息。

区块链网络可以通过网络效应来改善去中心化网络。当所有区块链都连接互通时，它会带来更多资本，更好的用户体验，以及更有利于集思广益，完善网络状态。

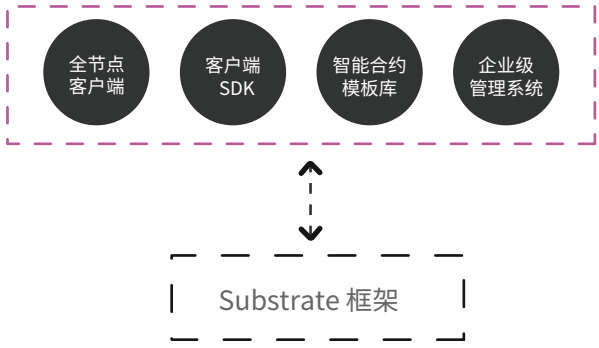
例如，如果一条链的上限为100TPS，则可以创建第二条相同的链——达到200TPS——以方便与其他链的交互。照这样做，我们可以轻易实现1000 TPS的交易速度。它也允许私有链，公链和联盟链的接入。最终，区块链甚至可以与法定的银行系统（如SWIFT）进行交互。



Turing V1

主网上线前

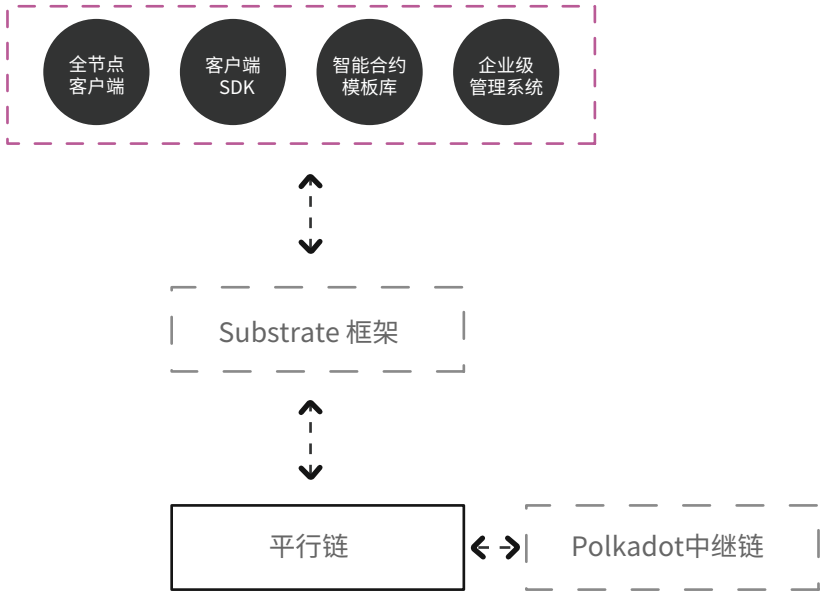
首先作为独立的POS公链运行并独立发展图灵超级节点，独立发行图灵币TNK。在这个阶段我们将基于 Substrate 框架完成图灵公链的所有基础功能和大量图灵的特色功能（全节点客户端，客户端SDK，常用智能合约模版库，企业级区块链管理系



Turing V2

主网上线后

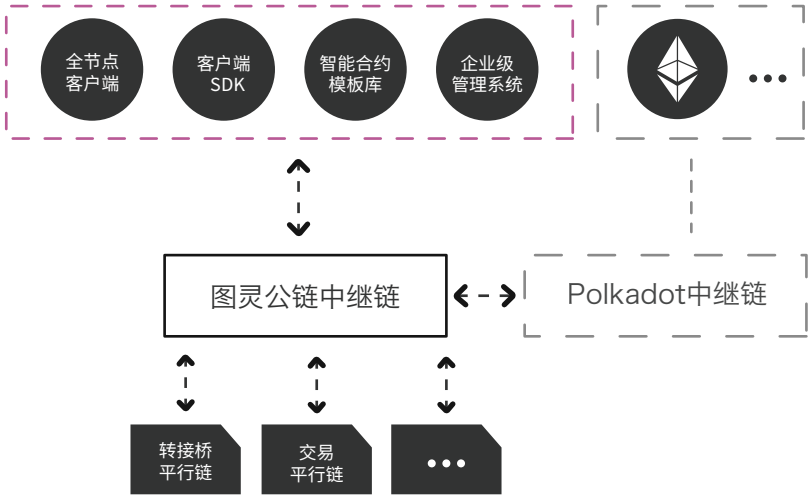
图灵公链将增加一条转接桥链作为 Polkadot 主网的平行链，完成与 Polkadot 主网的互通。并将持续发展超级节点，支持社区开发各类DApp



Turing V3

主网上线之后

图灵公链将逐步转型为类似 Polkadot 主网的多链架构，图灵公链主网转型为中继链，各个应用作为平行链与图灵公链主网连接。



区块链技术的大规模商业化应用仍处于起步阶段，至今为止，绝大部分区块链项目仍然停留在POC(Proof of Concept)阶段。

除了比特币、以太坊和EOS，绝大部分公链项目都没有真实的使用场景。根据 DappRadar 网站的数据，以太坊及其上 1137 个分布式应用，发现过去 24 小时活跃用户数只有 12521 人，其中只有 2 个分布式应用的 24 小时活跃用户数超过或接近 1000 人，而且比较活跃的分布式应用集中在游戏、博彩和加密资产交易等与实体经济关系不大的领域。

普华永道会计师事务所 2018 年 8 月对 15 个国家的 600 名公司高管的调查发现，有 84% 的公司对区块链感兴趣，但 52% 的公司的区块链项目处于研发状态，10% 的公司有区块链试点项目，只有 15% 的公司有正在运行的区块链项目。

我们认为阻碍区块链技术大规模商业化应用的几大主要障碍依次为：

1 性能不足，交易费用高。以太坊区块链每秒支持几十笔交易，比特币区块链每秒仅支持几笔交易。区块链拥堵期间交易费用急剧上涨，比特币区块链交易费用最高达到几十美元。这种性能和成本无法支撑大规模商业化应用。

2 大众认知和使用门槛过高。理解区块链的完整概念需要综合数学，密码学，计算机科学，经济学等多门学科。使用区块链需要使用专门的钱包软件，备份助记词。一旦私钥遗失或被窃取，数字资产将无法追回。这些问题导致了区块链和加密货币对普通用户的使用门槛极高。

3 技术门槛较高。区块链项目研发需要非常专业的技术和产品团队，大部分企业无法组建这样的专业团队，也无法承担高昂的人力成本。

4 治理和利益分配问题。区块链项目去中心化的运作方式，需要项目方自身对区块链项目治理有长期规划，对各参与方的利益分配问题有非常前瞻性的规划。与此同时，区块链技术可能会影响既得利益者的角色，对现有利益格局形成挑战，这也成为企业采用区块链技术的顾虑与阻碍。

针对上述问题，图灵公链项目都提出了切实可行的解决方案，并将在公链主网上线以后逐步解决，使图灵公链成为全球第一个大规模商业化的公有链。我们的针对这些问题的具体解决方案如下所述：

- 图灵公链采用的Aura + Grandpa混合共识方案在1000验证人节点的情况下能提供数千TPS的性能表现，并且每笔交易的手续费几乎可以忽略不计，这足以承载大部分商业应用。同时，当图灵公链转型为多链架构以后，平行链将承载大部分业务负载，图灵公链将仅作为跨链数据传输的中继链，这将进一步提升图灵公链生态的业务承载能力。

●在图灵公链发展初期，我们将把为用户保管私钥的责任交给超级节点。通过图灵公链管理后台和客户端SDK配合使用，超级节点能够为他们自己的用户批量生成公链地址和私钥，并将自有APP中的积分权益上链。对于普通用户而言，原APP的使用方式没有任何改变。终端用户虽然不持有私钥，但是通过超级节点服务器代理，可以实现区块链转账，支付等操作，也可以向交易所充值。这种方式避免了让普通用户接触到公私钥等专业概念，也可以完全兼容APP原有的账户系统，比让用户持有私钥的使用方式更简单。当用户正确理解了区块链钱包的使用方式，他就可以将自己的数字资产转移到图灵官方钱包中。这样设计的意义是能让移动互联网用户无感知地进入区块链世界。

●灵区块链会将最常用的区块链功能封装在图灵SDK中，并且可以在节点管理后台对图灵SDK进行配置。这种方式将大大简化移动互联网开发者接入区块链的门槛。与此同时，图灵公链也将开放完整的Wasm和EVM智能合约功能，对于有经验的区块链开发者，他们可以使用完整的智能合约

● 图灵公链将完全采用链上治理模型，所有决议都由图灵币社区投票通过，链上代码执行，不会产生任何歧义。这将从根本上避免类似BCH，ETC等分叉链的问题。图灵公链采用的长周期全网代币销售模式，NPOS验证人选举算法能有效解决POS区块链代币中心化的问题。与此同时，针对对采用区块链技术有所顾虑的企业，图灵公链提供的区块链解决方案可以让企业用最低限度的影响范围进行业务测试（灰度测试），当企业对测试结果满意以后再逐步扩大区块链业务范围。这将最大限度地减轻企业对区块链技术所持有的顾虑。功能构建各种复杂的DApp。

9.1.Unidex去中心化交易所

采用短周期集中竞价模式撮合交易的去中心化跨链数字资产交易所。

9.2.Oasis绿洲加密社区

绿洲加密是一个面向区块链行业的社区媒体项目，连接全球业内项目方、服务方、用户、媒体等区块链世界中各个分散主体，致力于消除区块链行业各个主体间的信息壁垒，使区块链世界的信息传递更加安全、便利、高效。OASIS还设立了根植于其功能设计上的、独特的多方共赢机制，以确保参与平台活动的各角色用户都能获得其需求的满足。

9.3.Patos社交网络协议

Patos是一个采用区块链技术的去信任化社交网络，本网络提出了一种高级别的协作方式，使彼此陌生的节点如同蜂群般相互信任并完成庞大复杂任务，与此同时没有任何一个实体单位可以单独控制或影响网络。

9.4.GEB去中心化OTC交易协议

GEB Network项目的目标是通过GEB协议创建一个去中心化的OTC交易网络。GEB协议允许用户在没有中间人的情况下进行加密货币与法币之间的交易，并使用智能合约来防止欺诈行为。加入GEB Network的用户可以从加密货币市场的发展中受益，同时缓解由加密货币价格波动，不诚实的交易商等因素带来的风险。

图灵代币TNK初始发行量10亿枚，初始分配方案如下：

创始团队10%

基石 + 私募投资者20%

创世节点（30个）10%

团队激励10%（分五年发放给图灵公链项目的核心团队和为图灵项目发展做出重大贡献的个人和团体）

图灵基金会　50%（用于未来出售给新增的超级节点，支持图灵生态建设，不得挪做他用）
在图灵公链主网启动之前，TNK为以太坊ERC20　Token。图灵公链主网上线以后，TNK将1:1转换为图灵公链主网代币。

图灵Chain超级节点POS挖矿机制

图灵公链创世超级节点共30个，每个创世节点至少认购300万个TNK并锁定在系统内参与POS挖矿。超级节点也可以接受TNK委托并锁定。POS挖矿的收益率和TNK全网抵押率相关。具体计算方法如下：

1.当全网流通代币抵押率（抵押代币/全部已销售代币）低于1/4时，网络将停

2.当全网流通代币抵押率在1/4～1之间时，锁定TNK的年化收益率从15%逐步递减到5%。超级节点每月增加一次，每次增加5个。全网超过2/3权益投票通过即可增加。新增超级节点需要从基金会认购一定数量的TNK(具体数量视当时TNK市场价格而定）并抵押在系统内。

11 路线图
route map

- 2018.10 启动图灵公链项目，技术预研
- 2019.03 图灵公链正式启动研发
- 2019.08 图灵币TNK上线交易
- 2019.10 图灵公链测试网上线，图灵SDK内测版发布
- 2019.12 图灵SDK公测版发布
- 2020.03 图灵公链主网上线，图灵企业级区块链管理平台发布
- 2020.05 Oasis绿洲加密发布
- 2020.06 Unidex去中心化交易所上线，第一个超级节点Token上市交易