大纬链现状汇报

一、开发历程

大纬链于 2016 年开始研发，研发之初主要是为了探索以区块链的信任机制，解决人社、医保等领域存在的基金诈骗、伪造材料等问题。2017 年即用于济南市发改委“区块链技术在“四个中心”建设中的应用研究”项目，是首个软课题，之后又陆续申请了国家自然科学基金、山东省重大科技创新工程、山东半岛项目、山东省服务业创新中心等多个项目（详见附件 1)；2018 年正式用于济南市高新区，是首个商业项目，之后又陆续在威海市文登区、公安部一所、济南市大数据局、人社部、山东省大数据局等取得应用（详见附件 2)。系统的研发，有效的支撑了科研项目及商业项目，支撑地纬举起了区块链及数据要素流通的大旗，荣获了山东省科技进步一等奖等一系列省级及国家级荣誉。

二、开发模式

地纬是国内首批自主开发区块链平台的公司。面向人社、医保及跨域数据可信流动的需求，团队充分调研了业界主流开源平台，确定了自主研发的技术路线，设计了底层链架构及数据模型，研发了大纬链底层支撑平台。

1、主要借鉴了以下开源产品：

-比特币：UTXO 模型的思路，比特币**版本，实现了基于交易地址的输入输出计算，便于追溯关联关系，但是未实现余额计算，缺少当前状态。

-以太坊：账户模型，以太坊 1.4 版本，实现了基于账户地址的主体之间转账记录及主体余额计算，便于确定主体的当前状态，以及历史状态的变化；基于智能合约可以实现可定制的 token 及对应 dapp，实现了初步的数字资产（货币、投票、筹码等），支持主体对 token 的定制化操作，但是存在存算耦合、代码漏洞、不可解释等问题，无法使用于数据资产等复杂数字资产。平台复用了以太坊源码的 P2P 通信模块、RPC 通信模块、编译打包脚本等。

-Fabric：Fabric0.6 版本的架构设计思路

-比原链：国密包，用于国密替换。

-北大：国密包 JMSSL3.0，提供了国密算法，但是并发量不足。

2、自主研发：

参考以太坊 1.4 版本，重新设计了支持成员准入的多链联盟链架构，以及共识-执行-提交的交易范式，复用了以太坊源码的 P2P 通信模块、RPC 通信模块、编译打包脚本等，重构了智能合约、交易池、共识协议、账本引擎、消息引擎、账户模型、状态树、密码模块、存储引擎等模块，构建了交易节点、共识节点、托管节点、存储节点、跨链网关、SDK 等。(详见附件 3)

在底层链的基础上，研发了数字保险箱等一系列公共服务。

三、大纬链创新性

数字社会环境下的区块链平台不仅要有基本的存证功能，更需要能够描述海量、复杂的主/客体，并支持其按规则自主协作与深入互动。大纬链对主/客体进行刻画，从支持海量并行的平台架构，以及平台的存储层、表示层、控制层、业务层进行整体设计，支持平台自解释及灵活扩展，可充分适应数字社会中的需求变化，从根本上解决主客体属性缺失、关系缺失、行为不可控、追溯黑洞等问题，支撑可信、可进化的数字社会。

1.**可信主体支持。**用于描述参与大纬链交易的主体对象，主体信息包括状态、角色、权限、认证信息等，其中主体的状态通过状态模型进行记录，权限与角色等由相关合约约束。主体通过确权拥有数字资产，通过授权流转数字资产，通过委托让其他主体操作自己的资产，也能够作为被委托人操作其他主体的数字资产，主体遵循合约的约束对数字资产进行操作。与业界通常只有 B 端账户相比，大纬链支持了 B 端、C 端等各种主体，消除了 C 端主体对 B 端主体的依赖，使得整个生态更加可信。

2. **可信客体支持。**基于原生多维账户模型，设计了资产合约，通过资产合约实现数字资产状态的统一解释、执行、控制，并可以订阅状态变化通知，基于状态变化自动触发后续业务逻辑；构建了资产交易、资产状态、资产内容分离存储机制，通过链上交易、状态与链下内容多重锚定，以及链下内容的分片存储与冗余复制共识，实现大容量多状态数据的高效可信存储与流转；杜绝了应用对数字资产解释、

执行的不确定性，直接控制数字资产状态的变化，保证其在区块链中的状态一致性，防止泛双花问题发生。

3. **智能合约创新。**实现了分层智能合约模型，分别设计资产合约与业务合约，实现业务逻辑与资产状态分离，通过资产合约实现数字资产状态的统一解释、执行、控制，不同业务合约负责不同场景的业务逻辑实现。业务合约和资产合约共同发生作用，业务合约可以监听资产合约的状态变化事件，也可以主动调用资产合约实现流程的推进，两类合约可以灵活组合，突破传统区块链平台“智能合约不智能”的困境。分层智能合约带来的较高的分层独立性，消除了现有合约中的大量代码漏洞，以及内置存储带来的误操作、虚拟机存储消耗等各种痛点问题。

4. **细粒度授权机制**。基于主体、交易、资产等模型，提出了主体、交易、资产内容三位一体的细粒度链授权机制。根据授权范围、周期等需求动态披露资产状态、属性；通过复用授权加密信息，在保证数据一致性的情况下减少消息传递数量，提高了计算效率；以资产为对象建立授权链，保证了授权链条的一致性与安全性。

5. **并行共识机制**。构建了多层次多策略演进式共识机制，设计了共识与执行分离、并行打包、状态回写等方法，提高共识吞吐量，降低交易延迟；根据节点的网络状况、负载情况以及历史运行状况等，优化主节点选举策略，提升共识效率；自适应交易负载情况，动态调整区块大小、并行分组以及共识策略，防止交易负载过大导致节点宕机等情况发生。

6. **“协作链-工作链”多链架构**。构建了“协作链-工作链”多链架构，协作链负责维护主体、合约、工作链、节点的状态以及提供跨链交易、信息路由与中继服务；工作链负责维护资产的状态、交易记录等，即资产的具体交易信息记录在工作链中。多链架构第一实现了业务的物理隔离，第二实现了性能线性扩展。在保证安全性前提下，可按需灵活扩展工作链，并基于协作链实现同构及异构工作链的主体对齐、语义对齐以及跨链交易。

7. 开放服务。

基于数字身份协议、数字凭证协议、复杂数字资产协议等提供了开发者服务、资产化系统、数字保险箱、资产应用系统等基础产品，分别面向开发者、资产供应方、资产持有方、资产使用方等提供工作链服务、主体服务、资产服务等开放服务，具备了支撑资产流通的基础功能。

四、大纬链核心系统的架构

4.1 逻辑架构

大纬链提供工作链建设标准，数据上链、使用标准以及应用对接标准等一系列大纬链标准规范，便于联盟方及应用接入大纬链，获取区块链服务。

采用同构/异构多链架构，由统一协作链与各行业各区域的工作链组成，可跨网络在多个云环境部署，由各工作链联盟方共同维护。统一协作链由各工作链可信联盟方共同组建，提供主体身份认证、同

一性管理、合约管理等能力，同时为各行业及区域工作链、其他异构区块链提供跨链协作、跨链交易等服务协作服务；各行业或区域可组建各自工作链，维护工作链资产的状态、交易记录等，即资产的具体交易信息记录在工作链中，为各自行业或区域提供区块链服务。

分布式数据资产存储网络由各工作链的联盟方共同组建，为大纬链中数据、证照、结果等资产提供安全可信的分布式存储服务。

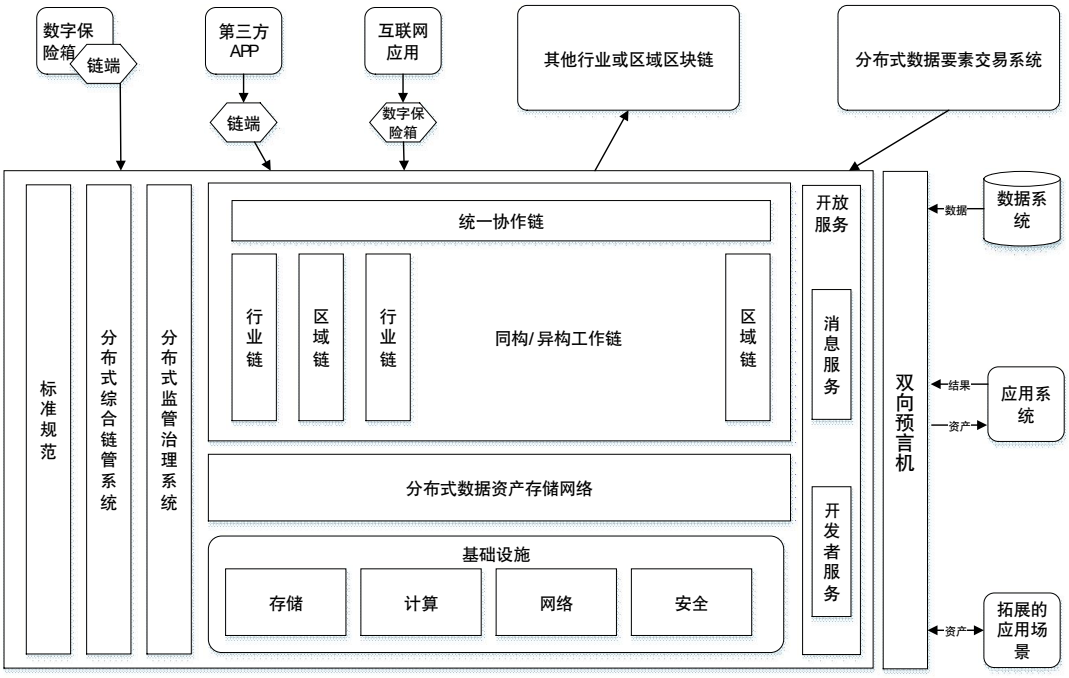
分布式综合链管系统负责区块链节点、成员等许可管理，以及区块链访问权限管理等；节点、成员、访问权限等相关数据上链，每个链部署本链的链管系统。

分布式监管治理系统负责为监管方提供链、交易、内容等不同层次的监管支持，同时支持监管权力变更与移交等；监管方通过自己的监管治理系统监管相关数据即可。

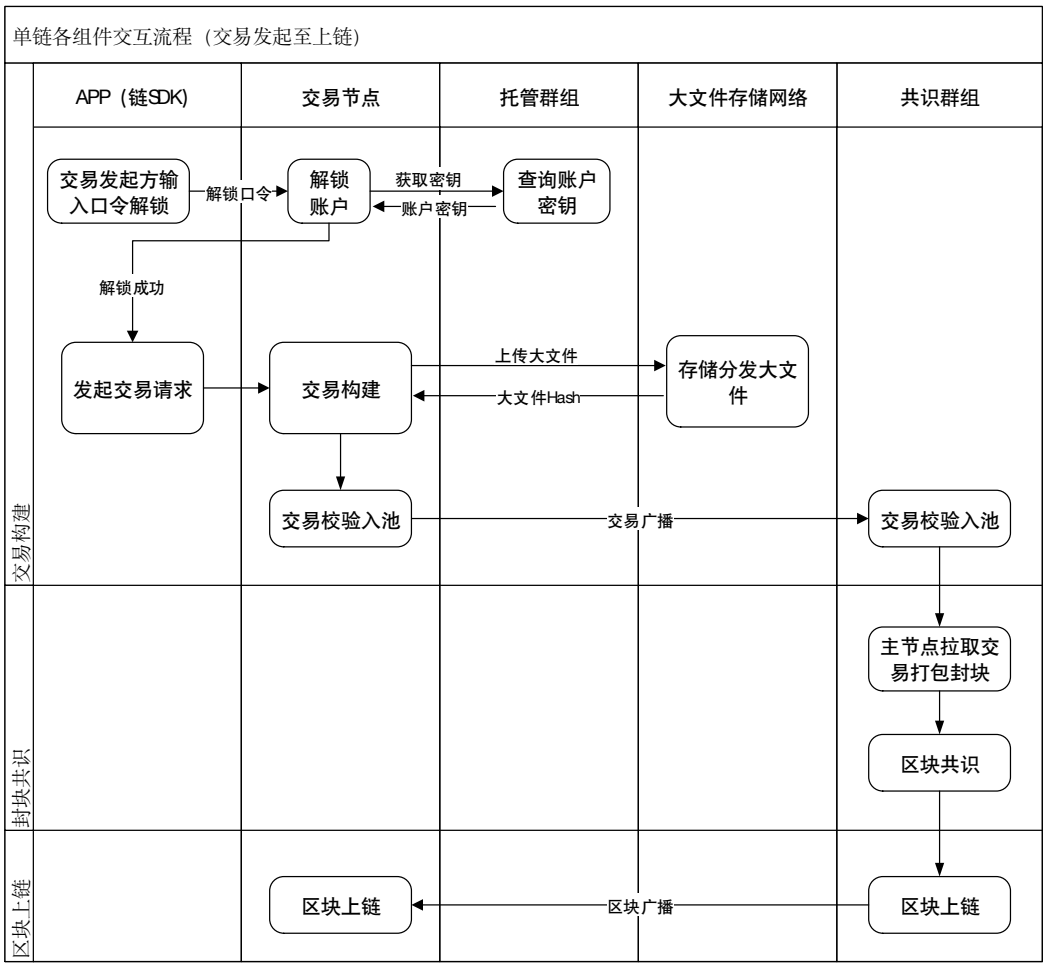
开放服务提供的面向应用及各业务系统的区块链便捷接入服，包括消息服务、开发者服务等；其中，消息服务作为分布式服务为应用、业务系统等提供基于消息的协作服务；开发者服务提供多种开发工具、标准化接口、链 SDK 等，降低区块链应用开发门槛。

双向预言机将区块链和应用系统双向联通，提供数据、资产、结果上链服务，将数据、证照、结果等资产化并存储于区块链平台中；根据业务需求，数据资产化系统可部署多个。

链端为应用、业务系统等提供与区块链交互的嵌入式可信执行环境与服务。

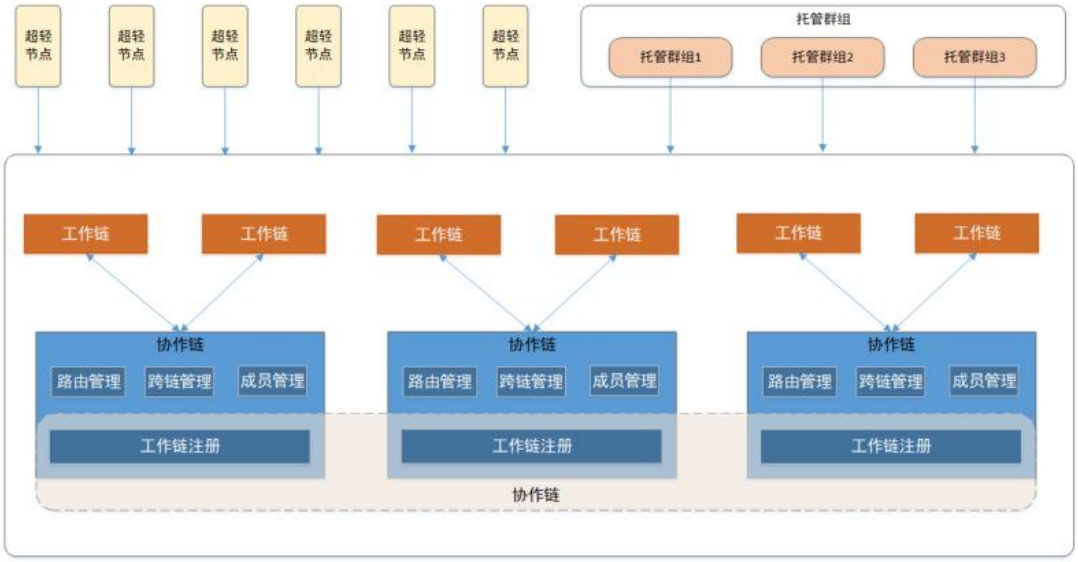


为充分挖掘各节点的性能潜力,对区块链节点进行细分，按照功能解耦原则，分为共识节点、交易节点、轻节点、托管节点、资产存储节点。其中，轻节点适用于交易量少、存储空间少的单位，仅存储与本节点相关的交易等关键信息；交易节点存储整个账本，不参与共识，提供对外访问服务；共识节点参与共识，构建区块与账本；托管节点提供密钥托管服务；资产存储节点仅以密文存储资产文件，并将摘要存储于账本中。存算分离功能解耦的架构，可以充分发挥各节点的性能，从整体上提升区块链的吞吐量。各节点之间的工作流程如下图所示：

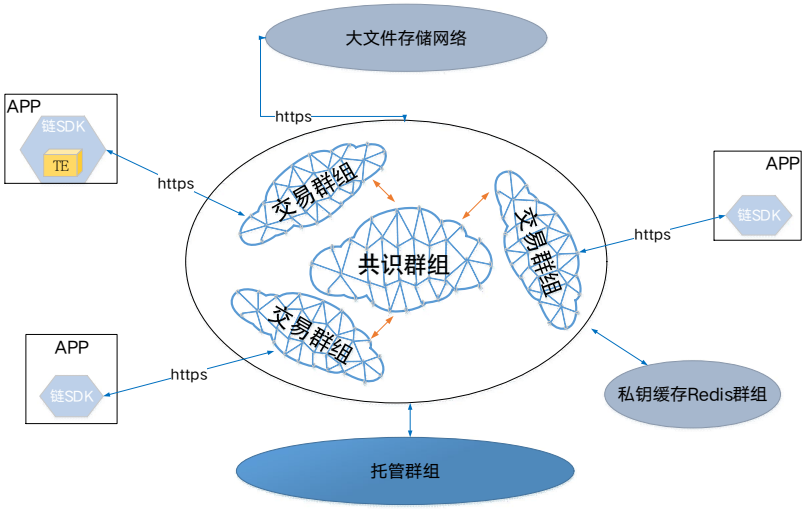


4.2 部署架构

协作链由协作链所属节点维护，工作链由工作链的所属节点进行维护；每个节点可以维护多个链，工作链的节点仅存储工作链的账本，协作链的节点仅存储协作链的账本；每个链具有交易节点与共识节点组成，交易节点负责验证交易、提供查询服务、交易路由与转发，即交易转发至能够处理其的链。每个链均支持链上更新系统配置的方式，例如与其他链交易节点链接信息、路由配置等等（可通过非交易的方式实现）。



一条完整的区块链构成：包含共识群组、交易群组、托管群组、Redis 群组、大文件存储网络、链 SDK 等组件，总体架构如下图：



- 共识群组：
  - 共识节点可连接的其他共识节点配置在配置文件中
  - 每个共识节点至少与 2/3 节点互相连接才能正常工作，所有节点两两之间至少存在一条通路
  - 目前的部署架构，共识节点之间采用全连接的方式组网
- 交易群组：

    - 节点可连接的其他交易节点配置在配置文件中
    - 交易群组内各节点互相连接
    - 交易群组间互不连接
- 交易群组与共识群组：
    - 交易节点与哪些共识节点互连，共识节点与哪些交易节点互连均可配置
    - 交易群组节点与共识群组互连
    - 交易节点与共识节点采用的一套架构，连接方式同群组内的连接方式，均采用基于许可列表的异步通信方式
- 交易群组与托管群组：
    - 交易节点访问托管群组，进行公私钥的读写
    - 交易节点可访问的托管节点，写在配置文件中，交易节点内部建立了相关的负载调度策略，保证托管服务的高可用
- 交易节点与私钥缓存 Redis 群组
    - 交易节点访问私钥缓存 Redis 群组，进行私钥的缓存与读取
- 交易群组与大文件存储网络：
    - 交易节点访问大文件节点，进行大文件的读写
    - 交易节点内部建立了相关的负载调度策略，保证大文件服务的高可用
- 区块链 SDK：
    - 链 SDK 负责访问交易节点，发送应用请求，应用直接调用

SDK 接口接入区块链网络，无需关心具体连接方式与访问地址

- 链 SDK 可访问的交易节点写在配置文件中，根据调度算法路由

五、竞品对比分析

大纬链在“多链架构”、“智能合约”、“建模完整性”、“资产内容安全流转”等方面处于第一梯队。在性能、中间件丰富性方面处于中游水平。

	单链性能	多链架构		跨链	智能合约引擎	共识协议(BFT/CFT)		建模完整性	资产内容支持
趣链	10W	支持	主从架构	中继链	EVM+JVM	可插拔	PBFT/Raft/NoxBFT	主体/合约	支持/基于 IPFS
长安链	10W	不支持		代理模式	WASM+EVM	可插拔	TBFT/MAXBFT、RAFT/DPOS	主体/合约	支持
Fisco Bcos	1W	不支持		代理模式	EVM+C	可插拔	PBFT/Raft/rBft	主体/合约	不支持
蚂蚁链	2.5W	不支持		对等中继模式	EVM+WASM	可插拔	FBFT/Raft	主体/合约	不支持
百度超级链	8.7W	支持	平行链+侧链	对等中继+TEE 代理+中继链	EVM+C	可插拔	TDPOS	主体/合约	不支持
大纬链	3W	支持	主从+平行多链	对等中继+中继链	GO+C+WASM	不可插拔	PBFT/FBFT	主体/资产/合约	支持/基于 IPFS 改进

六、基于大纬链开发区块链应用的优势

大纬链原生支持主体、客体（资产)、合约等，可以与物理世界及虚拟世界的主体、客体、业务规则等进行对应。具体如下：

1. 大纬链通过原生多维账户模型，实现了主体账户统一管理，主体账户一旦开通，可在不同应用中实现统一认证、统一管理；
2. 大纬链基于资产合约实现了资产的去中心化的统一状态控制，各应用开发商仅需关注自身业务逻辑过程即可。
3. 无需额外管理大容量数据存储与使用过程。大纬链将大容量数据作为资产内容统一管理，提供了资产内容高可用、哈希校验、副本复制等能力。
4. 针对数据要素可信流转场景，提供了丰富的授权协议，便于支持定制化的二次开发。
5. 提供了多种模式的接口，比如 APP，HTML 嵌入网页，小程序、公众号等，可以方便的接入。
6. 基于大纬链数字资产的自定义、自解释能力，不同开发商可以共同操作同一资产，多种不同类型的资产可以共同运行在同一个平台上，这样的区块链将不再属于某个具体的单位，而是具备了形成广域生态的能力。

七、大纬链短板与未来发展

1. 大纬链采用 BFT 协议，在不信任的环境下，各个节点通过重

复计算来保证安全性。目前单链性能在 3w 左右，离业界宣称的 6w—10w 还有差距，需要继续提升

2. 大纬链的共识协议目前不支持可插拔，即多种共识协议的动态切换。其中，大纬链参考了其他各家的共识协议，构建了一个可根据交易负载变化动态调整内部策略的共识协议，更加适合复杂网络状况下的可信数据流转。后续，面向不同应用场景设计不同的共识协议，针对性优化性能。
3. 大纬链目前不支持 EVM 智能合约引擎。后续，根据需求实现与 EVM 引擎适配。
4. 大纬链目前的周边工具或者中间件相对其他产品较为不足。缺乏智能合约 IDE、智能合约漏洞检测工具等，其中还需继续完善 Baas、开放服务等系统。
5. 缺少在安全、隐私计算、联邦学习等方面人员投入。
6. 缺少开放接入方面的规划，可以考虑在底层接入更多的区块链，与 fisco Bcos 等共建共享生态。

附件 1：大纬链代码研发情况

附件 2：大纬链应用情况

附件 3：大纬链科研项目及奖励情况

附件 1：科研项目

项目编号	项目类别	项目名称	批准部门或主管部门	项目起止时间	科研经费	承担单位
61772316	国家自然科学基金-面上项目	面向复杂交易的许可链关键问题研究	国家自然科学基金委	2018.1-2021.12	63 万元	山大
工信厅网安函[2019]116 号	工业和信息化部网络安全技术应用试点示范项目	政务联盟区块链政务信息可信传递平台	工信部	2019-2020	2000（无拨款）	地纬
	2020 年网络安全技术应用试点示范项目	基于人社区块链的人社政务服务应用	工信部			山东省社会保险事业中心
	2022 年大数据产业发展试点示范项目（服务业大数据应用方向）	基于区块链的服务业大数据综合服务平台	工信部	2021.7-2023.12		地纬
2021YFB2700102	国家重点研发计划“区块链”专项	课题 2：面向海量并发业务的交易并行执行机理研究	科技部	2021.12-2024.11	170(山大 130)	山东大学、华东师范大学
2021YFB2700103-2	2021 年国家重点研发计划项目-新型区块链体系架构设计理论与方法	课题三“网路传输优化与身份权限管理机制”的子课题：链上、链下数据可信交互与隐私计算技术的研究	科技部	2021.12-2024.11	8 万	湖南大学、山东大学
220703125071117	教育部产学合作协同育人项目	基于微众 FISCO BCOS 的区块链课程提升	教育部-深圳前海微众银行股份有限公司			山东大学

项目编号	项目类别	项目名称	批准部门或主	项目起止时间	科研经费	承担单位

			管部门			
2017CXGC0702	山东省重点研发计划（第二批）-重大科技创新类项目	自主可控的许可区块链支撑平台研发及其应用示范	山东省科技厅	2017.7-2019.12	200	地纬、山大
tscy20160404	山东省泰山产业领军人才（现代服务业及社会民生产业创新类）-肖宗水	基于区块链技术的“互联网+社会保障”智慧可信服务平台及产业化应用	山东省发改委	2017.1-2020.12	300项目+100人才+100市级人才配套	地纬
	山东省新旧动能转换重大课题攻关项目	基于区块链的数字资产公共服务平台	山东省发改委	2020.1-2021.12	400	地纬
2020CXGC010106	山东省重点研发计划（重大科技创新工程）项目	新型自主可控区块链多链架构关键技术研究与应用	山东省科技厅	2020.12-2023.12	1300	地纬（754）
	第二批山东省软件产业高质量发展重点项目	基于多链架构的新型区块链支撑平台	山东省工信厅	2020.1-2021.12		地纬
2021CXGC010108	山东省重点研发计划（重大科技创新工程）第一批	基于区块链的数据安全流转技术研究与应用	山东省科学技术厅	2021.07-2024.06	1450	山东大学
	山东省泰山产业领军人才（创新类）	“区块链+隐私计算”融合的数据资产可信流转关键技术研究与应用	山东省委组织部、山东省工信厅	2022.7-2024.6	300	地纬

	山东省数字经济重点项目	基于区块链的公共数据流通安全可信平台	山东省工信厅	2022.1-2023.12		山大地纬
	山东省第三批软件产业高质量发展项目	数据要素市场可信交易平台	山东省工信厅	2023.1-2024.12		山大地纬

项目编号	项目类别	项目名称	批准部门或主管部门	项目起止时间	科研经费	承担单位
2017SDBD-CXPT001	山东半岛（济南）国家自主创新示范区发展建设项目	基于区块链的“互联网+社会保障”智慧可信服务平台及产业化应用	济南高新区管委会科技经济运行局	2017.1-2019.12	100	地纬、山大
	济南市2019年度新一代信息技术产业集群项目	政务联盟区块链可信服务平台	济南市工信局	2018-2020	150	地纬
	泉城产业领军人才创新团队	基于区块链的私有数字资产服务平台	济南市委组织部（济南市科技局）	2020.1-2022.12	200	地纬
	2019年济南市工业互联网应用创新示范	基于区块链的工业互联网数据安全可信服务应用示范	济南市工信局	2017.4-2020.3		地纬

附件2：大纬链应用情况

目前，已经建成25个区块链，其中区级链2个、企业链1个（中国电建），城市链11个，行业链9个，区域链2个（黄河流域公积金

链+山东省城市链网)，链上数据达 200 多类，建设应用场景 80 个，获得国家级、省部级等优秀案例 20 余项。

目前已在山东省内已有 60 多个应用场景取得实际成效，省外应用场景，主要集中在人社与公积金领域。

省内区块链应用场景用户人数多在一千以上。其中，泉城链普惠金融、聊城链普惠金融、德州链慈善证书认证、公积金链业务办理、医保链普惠保险与商保快赔等场景用户人数与活跃度较高。

序号	名称	应用场景	应用规模
1	泉城链	普惠金融	“泉城链+普惠金融”平台已累计发放贷款 39.1 万笔，实现授信 500.5 亿元，其中个人信用贷款 417.2 亿元、小微企业（含个体工商户）贷款 30.4 亿元，涉及企业 15746 户。
2		司法公证	已累计办理事项 8203 项，累计授权资产 15850 个，累计精简材料 17405 份，累计服务群众 8828 人。
3	济宁链	数字人生	1000 人以下
4		电子病历掌上查	已累计查询 6 万余次，服务群众 8000 多人。
5		普惠金融	1000 人以下
6	东营链	二手房水电气热过户	1000 人以下
7		租房备案	1000 人以下
8	港城链	无	
9	聊城链	普惠金融	8.8 万人
10		公积金	1000 人以下
11		汽车站亮证购票	100 人以下
12	德州链	慈善证书颁发	2.5 万人
13		普惠金融	100 人以下
14		公积金	100 人以下
15	泰安链	商保理赔	1000 人以下
16		公积金标准化	100 人以下

17		公积金数字卡包	2000 人
18	威海链	一人一档一企一档场景	用户总量 57953 个，数据上链总量为 35.5 万个，数据调用次数达 16.1 万次
19		普惠金融	5000 人以下
20		扫码填报	配置 205 项服务事项
21		健康证办理信息服务	7000 人以下
22		共享营业厅	200 人以下
23		荣誉证书签发	威海教育局发放 237 个
24		工资条发放	3000 笔以下
25		电子劳动合同签订	10 家试点企业配置并发放
26		商铺租赁合同签订	1 家试点企业配置并发放
27		中小学生招生入学场景	8000 人以下
28	牡丹链	普惠金融	1000 人以下
29		商保理赔	100 人以下
30		公证场景	100 人以下
31		燃气场景	100 人以下
32		水务场景	100 人以下
33	日照链	一人一档应用	2000 人以下
34	枣庄链	数据共享开放	暂无
35	番禺区块链	政务晓屋	1000 人以下
36		一站式政务服务对接	1000 人以下
37	医保链	投保资格校验	2000 万人次
38		商保报案	1650 万笔
39		商保快速理赔	1.5 万笔
40		税务家庭共济账户关系查询	7.8 万人次
41		电力公司个人信息授权查询场景	61 笔，报销额 10 余万
42		医保贷场景	13 笔，放款 3200 万
43		商保一站式结算场景	暂未开展
44		电子票据跨链传输	100 人以下
45		药店门诊统筹协议	100 人以下

		上链场景	
46	公积金数字黄河链	数字卡包	1-10 万人
47		普惠金融断直连	1-10 万人
48		异地证明开具	1000 人以下
49		租房一件事	1000~5000 人
50		死亡公证	100 人以下
51		灵活就业	1000~5000 人
52		公积金组合贷款	100 人以下
53		数据双向共享	1000 人以下
54		政务服务标准化	100 人以下
55		不动产业务联办	100 人以下
56		民政救助	1000 人以下
57		授权深度集成	100 人以下
58		房产协查	100 人以下
59		贷款不见面存证	100 人以下
60		跨链互通	100 人以下
61		异地冲还贷	100 人以下
62		异地逾期划扣	100 人以下
64	人社部部级工作链	电子劳动合同	还未上线
65		社保参保证明	还未上线
66		职称证书授权	还未上线
67	山东人社链	求职招聘	求职招聘应用场景覆盖山东公共招聘网的照片单位和求职者，当前已为 6000 余家招聘单位、近万名求职者提供服务。 实现参保缴费证明 14298 个、职工养老保险参保缴费汇总 12693 个、职工养老保险参保缴费明细 9231 个、职业资格证 3139 个； 实现企业参保证明上链 347 个
68		社保参保证明	山东省人社链实现社保参保证明的申领开具总计 233827 笔，完成个人授权可信流转 161174 笔。
69		电子劳动合同	实现电子劳动合同上链 536 笔。
70		人才服务	实现淄博精英卡上链 4015 个 累计授权 16039 次
71		工伤认定和劳动能	实现工伤认定结论书和劳动能力

		力鉴定	鉴定结论书上链，其中工伤认定结论书上链 361 个，劳动能力鉴定结论书上链 100 个
72	四川人社链	职业技能培训证书应用	涉及 6 类数据上链，数据上链总量 115，涉及个人数量 97
73		劳动人事争议调解应用	涉及 15 类数据上链，上链总数为 105，涉及个人数量 5，涉及企业数量 3
74		人社个人档案应用	涉及 32 类数据上链，上链总数为 9,196,449，涉及个人数量 2382830，涉及企业数量 3
75		就业创业贷款应用	涉及 4 类数据上链，上链总数为 1312，涉及个人数量 480
76		与省政务跨链协同应用	
77	西藏人社链	基于人社链的电子劳动合同订立系统	场景涉及 4 类资产，共上链资产 5830 份，累计服务 84 家个人和 1086 位劳动者
78		基于人社链的合同纠纷仲裁应用	场景涉及 1 类资产，共上链数据 5 份，累计服务 6 家企业和 8 位个人
79		基于人社链建设电子证照场景应用	暂无数据上链
80	宁夏人社链	电子劳动合同	场景目前已上链 3 类资产类型，共上链资产 27 余万份，其中涉及个人 13 余万人，涉及企业 1.4 余万家，使用次数 359 次。
81	天津人社链	职称证书	天津职称证书场景上链 2 类数据，上链数据总数量 541 条，其中职称证书 472 条，授权记录 69 条；涉及 437 人和 59 家单位。
82	电建人社链	劳务实名制	电建劳务实名制应用场景涉及 6 类资产，上链资产总数量 64w，涉及 7w 人和 1 家单位，核验数据 45 次。

附件 3：大纬链代码研发情况

以共识节点为例，其主要包含以下组件：

自主研发代码比例：70%~85%

1. **资产合约模型及状态模块：(100%)完全自主研发。**定义了资产合约的基本数据结构和状态机。

2. **主体模型及状态模块：(100%)完全自主研发。**定义了主体的基本数据结构和状态机。

3. **数字资产模型及状态模块：(100%)完全自主研发。**定义了数字资产的基本数据结构和状态机。

4. **主体账户索引模块：(100%)完全自主研发。**根据主体在不同资产和智能合约中的干系方身份，按角色建立资产和合约索引，支撑按主体账户为条件的正向快速检索。

5. **智能合约虚拟机模块：(100%)完全自主研发。**自主研发构建面向数字资产的智能合约状态约束与控制算法，支持大量的主体状态控制、资产状态控制、合约状态控制等原语。

6. **交易池模块：(80%)基本重写，自主研发。**根据大纬链数字资产模型、主体模型、智能合约模型等，接受并解析指定格式交易，并进行交易的预执行和排序，包含完全自主研发的基于资产账户约束的交易冲突排序核心算法，以及完全自主研发的全局状态安全回滚算法，支持交易节点的主体账户资产缓存的构建与管理。

7. **共识模块：(100%)完全自主研发。**基于传统三阶段 PBFT 算法，研发实现支持异常中断的四阶段 PBFT 高效共识算法和视图更替算法，支撑海量交易的正常共识验证。完全支持大文件协同验证、交易冲突处理、国密加密下的验证、以资产合约为核心的验证等功能。

8. **区块链对外服务模块：(100%)完全自主研发。**对外开放交易发送、交易反馈、账本查询、资产查询、账户查询、合约部署等区块链服务功能。

9. **“协作链-工作链”协同模块：(100%)完全自主研发。**完全自主提出“协作链-工作链”协同机制，研发实现支持同一认证、多链调度、跨链交易的协作链，以及处理资产信息和交易的工作链。

10. **异构跨链网关模块：(100%)完全自主研发。**支持中继跨链和对等跨链方式，通过基于资产多维语义模型实现跨链资产双向映射。

11. **区块链账本模块：(80%)基本重写，自主研发。**包括区块构建、区块链构建、常规区块内容检索等功能，支持硬分叉管理，构建树形账本，支持区块并行共识。

12. **状态树模块：(70%)基本重写，自主研发。**额外构建了可表达数字资产、主体状态、智能合约状态的树，同时将状态树划分为多个状态树，支持状态并行更新、查询，支持状态树扩展。

13. **节点通信模块：(70%)基本重写，自主研发。**支撑节点间的握手、密

码学认证和节点共识消息广播域接受功能。

14. **事件管理模块：(70%)基本重写，自主研发。**支持节点对不同消息的订阅，如 PBFT 三阶段消息、区块上链消息等，事件管理类型具有热重载的支持能力。

15. **账户管理模块：(80%)基本重写，自主研发。**基于国密算法包实现对大纬链账户(包含主体、资产、合约等)的密钥构造、管理、地址构造等功能，基于以太坊账户管理模式深度优化改造。

16. **链端命令行管理模块：(80%)基本重写，自主研发。**根据以太坊共识节点管理命令行的业务逻辑，研发形成大纬链命令行管理模块，支持当前共识节点的账本查看、交易查询、区块查询、合约查询等基础数据管理功能，支持共识集群状态管理、单点合约测试执行、节点热重载配置修改等功高级功能。

17. **区块链底层存储模块：(60%)部分修改。**基于 Fabric 模式，利用 RocksDB 构建区块链底层存储引擎，可存储区块链账本、全局状态、可持久化缓存等数据。

18. **加密控制模块：(70%)基本重写，自主研发。**在以太坊原有的加解密、哈希运算算法的基础上，额外实现了大纬链常用的非对称加密、快速对称加密、门限加密等算法。

19. **国密版加密控制模块：(40%)少量修改，部分新增。**基于北大开源国密算法产品，支持 SM2/SM3/SM4，以及基于国密曲线的秘密分享、压缩、随机数算法。

20. **以太坊通用功能模块：(10%)少量修改。**根据以太坊通用类业务逻辑进行优化，支撑大纬链 HTTP 通信解析、节点信息编解码、部分交易或区块数据的编解码功能，并支撑后续版本接入更多以太坊原生特性。

21. **以太坊原生压缩读写模块：**(20%)少量修改。支撑部分交易数据的 Keccak256 哈希处理。

22. **大文件存储协同模块：(10%)少量修改。**提供 IPFS 的基础通信功能，对外公开大文件可信验证接口，支撑大文件的链上锚定、在 IPFS 中的检索和验证。

23. LRU **模块：(30%)少量修改，部分新增。**支撑大纬链的交易引擎、状态缓存、账本缓存、智能合约缓存等页面置换服务、快速缓存访问服务及缓存修改服务。

24. **区块模型模块：(30%)部分修改。**基于以太坊的区块数据结构定义，优化定义了区块、区块头、块内收据集合、块内交易集合的数据结构。

25. **以太坊原生合约虚拟机模块：(5%)少量修改。**用于支撑大纬链后续兼容以太坊合约。