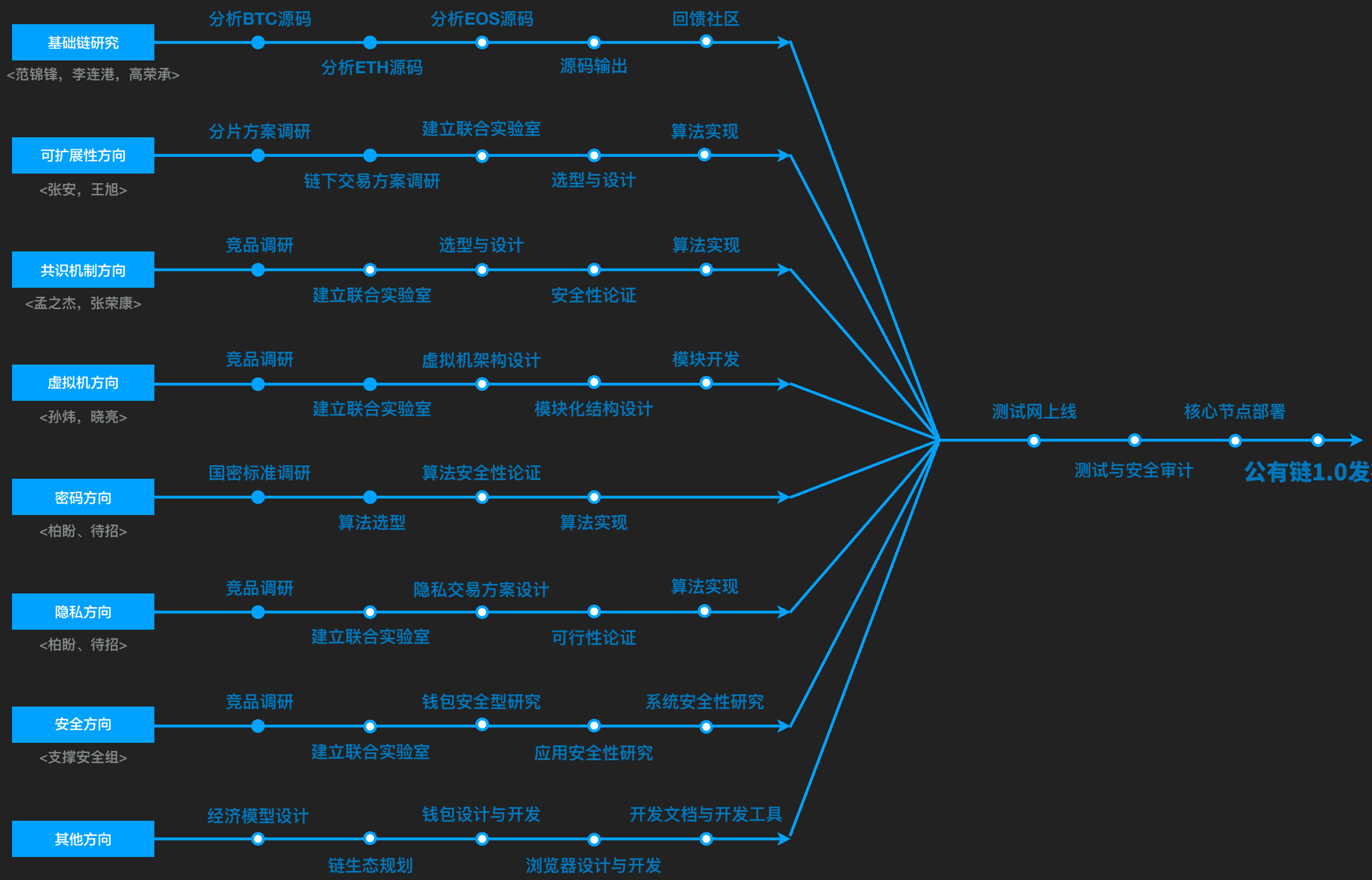
核心技术方向研究

八大研究方向


基础链研究
<范锦锋，李连港，高荣承>
分析BTC源码
分析ETH源码
分析EOS源码
源码输出
回馈社区
可扩展性方向
<张安，王旭>
分片方案调研
链下交易方案调研
建立联合实验室
选型与设计
算法实现
共识机制方向
<孟之杰，张荣康>
竞品调研
建立联合实验室
选型与设计
安全性论证
算法实现
虚拟机方向
<孙炜，晓亮>
竞品调研
建立联合实验室
虚拟机架构设计
模块化结构设计
模块开发
密码方向
<柏盼、待招>
国密标准调研
算法选型
算法安全性论证
算法实现
隐私方向
<柏盼、待招>
竞品调研
建立联合实验室
隐私交易方案设计
可行性论证
算法实现
安全方向
<支撑安全组>
竞品调研
建立联合实验室
钱包安全型研究
应用安全性研究
系统安全性研究
其他方向
经济模型设计
链生态规划
钱包设计与开发
浏览器设计与开发
开发文档与开发工具
测试网上线
测试与安全审计
核心节点部署
公有链1.0发布

基础链研究方向

大方向描述：

区块链三个阶段解决的问题：数字货币，智能合约，应用落地

比特币代表的第一阶段主要技术：加密技术，共识技术，数据库技术，P2P网络，UTXO模型

以太坊代表的第二阶段主要技术：智能合约，预言机，新的共识技术（POS），帐户模型

EOS等代表的第三个阶段主要技术：复杂智能合约和预言机，新的共识技术（DBFT-DPOS），帐户引入权限管理，高并发的分片技术，跨链技术

架构的发展：瀑布式（1.0）面向对象（2.0）分层接口插件式开发（3.0）

重点技术迭代：

加密及隐私保护技术：从最初的secp256k1到Curve25519，环签名，零知识证明

虚拟机：从解释字符到EVM到专用WASM

共识：POW-POS-DPOS(XBFT-DPOS)—混合共识

数据库: KV（LevelDB、RocksDB）— MongoDB — 混杂使用

跨链：哈希锁定（侧链/中继，公证人，分布式KEY）— 根子链 — 链中链

智能合约：无 — 以太坊智能合约 — 复杂合约及预言机

并发设计：从不考虑 —— 分片 —— 加快共识（出块）—— 多链

基础链研究方向

整体面临的问题：

技术存在的问题：加密算法的量子攻击；隐私保护；共识算法的更优；跨链交易；

设计存在的问题：可扩展性；网络安全；数据库的集成使用；

应用存在的问题：TPS并发；共识的效率；大数据存储；跨链交易；有效的激励机制；

重点发展方向：

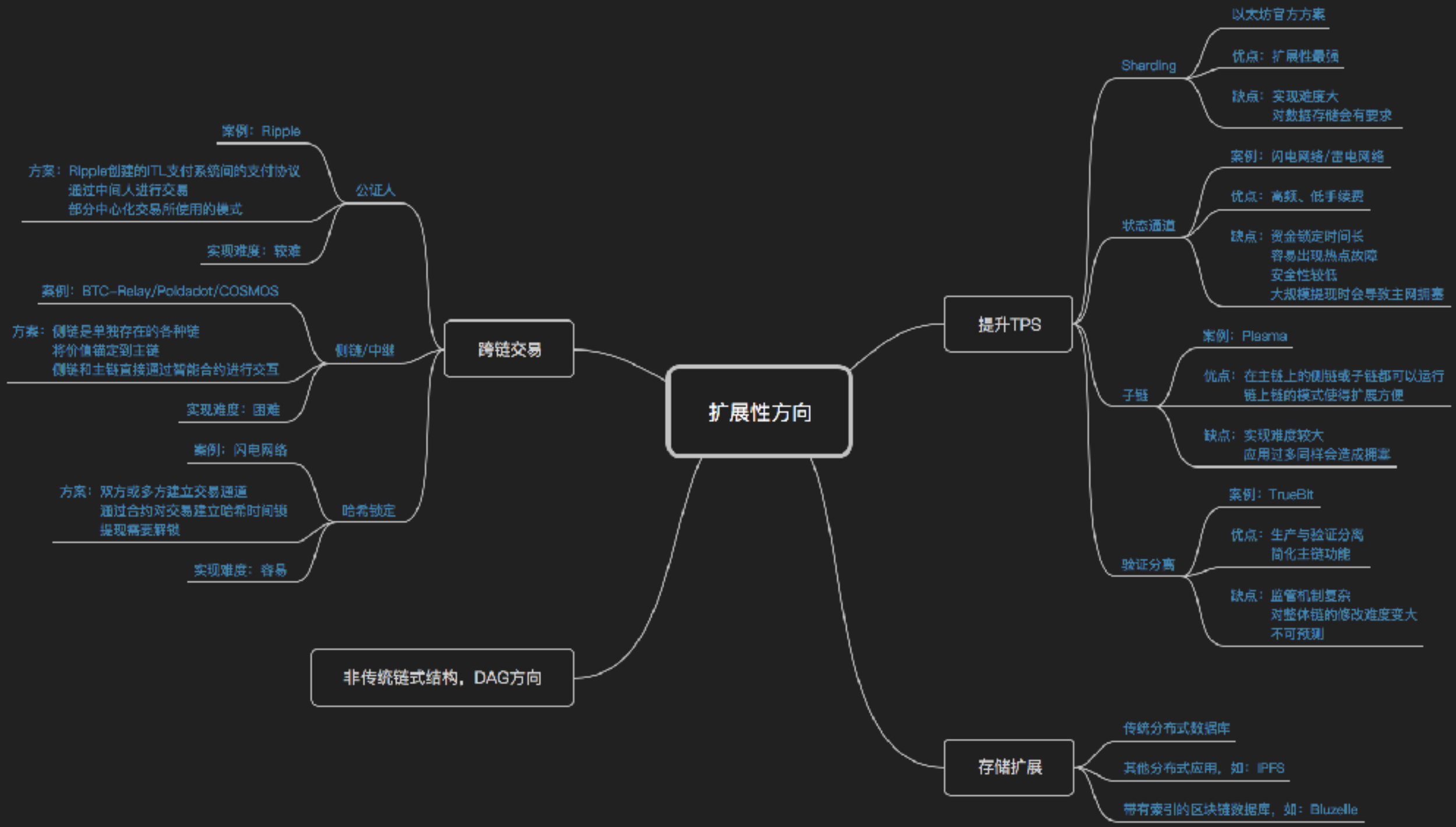
应用上：高TPS，更优的共识算法，跨链，复杂的智能合约和预言机；

设计上：多链，分层可插拔，协议标准化；

基础链研究样本

公链名称	特点	主要技术	架构描述
ONT	1、以太坊的架构思路 2、使用Actors做为通信的基础 3、信任框架 4、KV-SQL的映射 5、TPS：很高	1、匿名签名算法，同态加密	采用链网结构以及较齐全的ID认证机制，通过智能合约进行在链间和链内的数据的自动交换
		2、VRF-BFT	
		3、混合预言机	
		4、NeoVM虚拟机，支持多语言	
IOTEX	1、链中链架构，根链子链互相协作。 2、内置隐私保护 3、信任框架 4、KV-SQL的映射 5、TPS：很高	1、零知识证明	应用于物联网的区块链，通过根链和子链加强了隐私保护和对轻节点的处理，类似哈希锁的跨链通信协议，基本也是采用了以太坊的思路。
		2、POW+POS（多种共识可插拔）	
INT	1、物联网方向 2、平行链设计 3、对轻节点友好 4、支持边缘计算 5、TPS：很高	1、跨链事务的双链共识机制	代码正在演进中，基本上采用模块化设计，使用JS编码。
		2、抽象资源服务	
		3、零知识证明	
		4、支持机器节点	
		5、挖矿和记帐分离	
EOS	1、插件化设计 2、免费 3、引入内存型数据库 4、强大的智能合约和预言机 5、TPS：1000000+	1、分片，内链	采用分层插件的接口化设计，辅以宏和模板自动类推导，通过跨链和内链及分片实现高并发。
		2、跨链-LCV	
		3、自动类推导	
		4、BFT-DPOS	
NEO	1、提出了资产的分类：小蚁币 小蚁股，即创新了激励机制 2、引入了不经过构造交易的超导交易 3、分布式事务 4、TPS：最高10000+	1、支持多语言的智能合约	主要是生态建设和激励机制做得比较好，整体架构是标准的面向对象设计，部分采用了插件设计，对外接口做得比较好一些。
		2、中性交易共识（限制记帐人权利）	
		3、DBFT共识	
IOTA	1、无手续费 2、交易速度快 3、TPS:1000+	1、DAG而非区块链（Tangled）	采用JAVA编写，所以基本上采用了面向服务的设计 架构，辅助以独特的三进制语言和DAG中的专门共识算法。仍然需要实际去检验。

可扩展性方向


扩展性方向
跨链交易
公证人
案例：Ripple
方案：Ripple创建的ITL支付系统间的支付协议
通过中间人进行交易
部分中心化交易所使用的模式
实现难度：较难
侧链/中继
案例：BTC-Relay/Polkadot/COSMOS
方案：侧链是单独存在的各种链
将价值锚定到主链
侧链和主链直接通过智能合约进行交互
实现难度：困难
哈希锁定
案例：闪电网络
方案：双方或多方建立交易通道
通过合约对交易建立哈希时间锁
提现需要解锁
实现难度：容易
非传统链式结构，DAG方向
提升TPS
Sharding
以太坊官方方案
优点：扩展性最强
缺点：实现难度大
对数据存储会有要求
状态通道
案例：闪电网络/雷电网络
优点：高频、低手续费
缺点：资金锁定时间长
容易出现热点故障
安全性较低
大规模提现时会导致主网拥塞
子链
案例：Plasma
优点：在主链上的侧链或子链都可以运行
链上链的模式使得扩展方便
缺点：实现难度较大
应用过多同样会造成拥塞
验证分离
案例：TrueBit
优点：生产与验证分离
简化主链功能
缺点：监管机制复杂
对整体链的修改难度变大
不可预测
存储扩展
传统分布式数据库
其他分布式应用，如：IPFS
带有索引的区块链数据库，如：Bluzelle

共识机制方向

常用的共识算法：

传统一致性算法：Paxos、Raft

基于困难问题的的算法：PoW

基于权益的算法：PoS、DPoS

其他：PoA、PBFT等

共识算法的研究目标：

共识算法的评价标准：综合安全性、容错能力、平滑度、去中心化、可扩展性、环保性、最终性等多方面因素，制定对共识算法的评价标准。

共识模型的设计：结合共识算法的评价标准和使用场景的需求，设计合适的共识模型。重点研究面向高性能公链的共识模型。

虚拟机研究方向

虚拟机实现方案：

解释器类型（interpreter）

- 主要代表比特币和EVM还有小蚁，基于栈的虚拟机
- 优点是实现简单，维护成本低，可控性强
- 缺点是运行效率以及安全性。同时依赖于语言的开发，开发成本转移到智能合约语言实现

运行时类型（JIT）

- 主要代表EOS，EVM下一代虚拟机，栈加寄存器
- 优点是运行速度快，多种智能合约语言支持，JIT技术成熟
- 缺点是开发学习成本，智能合约语言以及虚拟机安全，同时还有外部依赖

虚拟机面临的问题：

- 多语言支持方案，如果做到前后端隔离，目前没有系统的架构，IR算是一种可行方案
- 智能合约审计，人工的方式还是静态分析加动态测试，静态分析理论要求多一些。还有多语言支持下的语言闭包如何限制
- 缺少成熟的工具链和集成开发环境，开发测试成本大

虚拟机研究方向

虚拟机研究目标：

- JIT以及沙箱技术在虚拟机里的应用
- 虚拟机结合人工智能如Cortex中的虚拟机
- 虚拟机以及智能合约的人机接口
- 与大数据处理结合，比如CyberVein在区块链上引入了mapreduce的概念
- 智能合约安全性审计以及可视化编辑等

密码方向

密码方向使用技术：

哈希算法：区块链中采用的哈希算法主要是 SHA2 系列，包括 Sha256，Sha512 等等，区块链中地址的计算、Merkle 根计算、比特币中挖矿(PoW)、布隆过滤器、块哈希、交易哈希等都用到的这些哈希算法；

数字签名：区块链中采用椭圆曲线(secp256k1)来做数字签名，数字签名涉及到公钥、私钥和钱包等工具；使用者通过数字签名来验证数字资产的所有权。

密码方向研究目标：

哈希算法：现有 SHA2 算法基本满足区块链的需求，哈希算法可以朝着 SHA3 或者更优秀的哈希算法方向研究

数字签名：由于椭圆曲线加密算法所基于的椭圆曲线域上的离散对数问题不具有抗量子性，所以现有采用椭圆曲线来做数字签名也不具有抗量子性；数字签名的研究方向可以是高效的抗量子数字签名算法。

隐私方向

隐私方向使用技术：

环签名：环签名是门罗币所采用的隐私保护方案，同时以太坊也采用了类 CryptoNote 的环签名方案；由于环签名中依旧需要与其他用户的公钥进行混合，因此可能会遭遇恶意用户从而暴露隐私。

零知识证明：ZCash采用了名为 zk-SNARK 的零知识证明技术，来保证交易的发送者、接受者和交易金额的机密性。zk-SNARK 的缺点在于计算验证数据时，需要一定的计算量。

同态加密：没有实现全同态，而且效率比较低下；

隐私方向研究目标：

采用环签名的方案可以使用更易于保护隐私的零知识证明来实现，或者寻找更高效安全的环签名方案；

零知识证明的研究方向则为需要寻找更高效，计算验证更快的零知识证明方案；

同态加密的研究方向主要为两方面：全同态加密的理论实现，高效同态加密算法的研究。