Taireum 一种兼容以太坊的企业级分布式账本与智能合约平台

过去几年，区块链正变成一个日渐热门的词汇，除了广为人知的比特币等数字货币使用了区块链技术，基于区块链的分布式账本和智能合约技术越来越受到企业的重视，越来越多的企业开始使用区块链技术进行跨企业间的业务协作。2018 年 6 月 25 日香港支付宝和菲律宾钱包 Gcash 利用区块链技术实现跨境转账，仅 3 秒就实现跨境汇款到账，而以前则需要十几分钟到几天的时间。

一般我们把对所有公众都开放访问的区块链叫做公有链，而把若干企业构建的仅供企业间访问的区块链叫做联盟链。目前比较有影响力的联盟链技术是 IBM 发起的 Hyperledger Fabric 项目，若干基于 Hyperledger Fabric 的联盟链应用已经落地。邮储银行的资产托管，招商银行的跨境结算都使用了 Hyperledger Fabric 技术。

而在公有链领域，目前看来，生态最完整、开发者社区最活跃、去中心化应用最多的公有链技术莫过于 Ethereum 以太坊。在智能合约和去中心化应用开发支持方面，以太坊的生态堪称业界最完备的典范，也受到了最多区块链开发者的支持。

但是以太坊作为一个公有链技术，目前还无法应用于企业级的联盟链场景。

- 在准入机制上，使用以太坊构建的区块链网络允许任何节点接入，也意味着区块数据是完全公开的，而联盟链的应用场景则要求仅联盟成员接入网络，非成员拒绝入网，并且数据也仅供联盟成员访问，对非联盟成员保密。

- 在共识算法上，以太坊使用工作量证明（PoW）的方式对区块打包进行算力证明，除非恶意节点获取了以太坊整个网络 51%的计算能力，否则无法篡改伪造区块数据，保证区块数据安全可靠。但是工作量证明需要花费巨大的计算资源进行算力证明，造成算力极大浪费，也影响了区块链的交易吞吐能力。联盟链场景下，由于各个参与节点是经过联盟认证的，背后有实体组织背书，所以在区块打包的时候不需要进行工作量证明，大大减少算力浪费，提高交易吞吐能力。

- 在区块链运维管理上，以太坊作为公有链，节点之间通过 P2P 协议自动组网，无需运维管理。而联盟链需要对联盟成员进行管理，对哪些节点可被授权打包区块也需要进行管理，以保证联盟链的有效运行。

那么如何才能既利用以太坊强大的智能合约与技术生态资源，简单高效进行企业级区块链应用开发，又满足联盟链对安全、共识、运维管理方面的要求？

我们在以太坊的代码基础上，进行了若干代码模块的重构与开发。

- 重构了以太坊的 P2P 网络通信模块，使其需要进行安全验证得到联盟许可才能加入新节点进入当前联盟链网络。

- 重构了以太坊的共识算法，只有经过联盟成员认证授权的节点才能打包区块，打包节点按序轮流打包，无需算力证明。

- 开发了联盟共识控制台（Consortium Consensus Console）CCC，方便对联盟链进行运维管理，联盟链用户只需要在 web console 上就可以安装部署联盟链节点，投票选举新的联盟成员和区块授权打包节点。

这就是 Taireum，一种基于以太坊的企业级分布式账本与智能合约平台。

Taireum 技术架构

Taireum 复用了以太坊强大的智能合约模块，并对共识算法和网络通信模块进行了重构改造，重新开发了联盟共识控制台，从而使其适用于企业级联盟链应用场景。使用 Taireum 部署的联盟链如图 1。

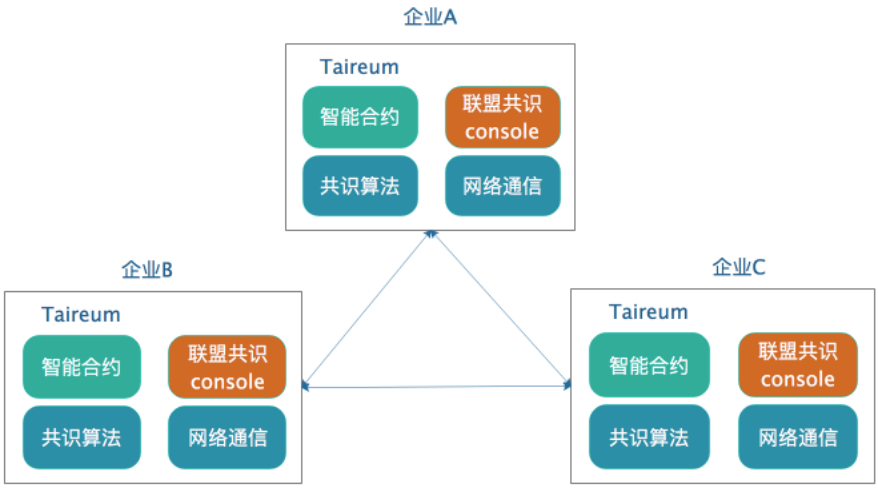

图 1 使用 Taireum 部署的联盟链架构

企业 A、企业 B、企业 C 合作建立一个联盟链，数据以区块链的方式存储在三家企业的节点上，实现分布式记账，并根据（基于智能合约的）联盟共识授权某些节点对区块数据进行打包。其他企业未经许可无法连接到该联盟链网络上，也不能查看其上的区块链数据。

Taireum 联盟共识控制台

联盟共识控制台是 Taireum 为联盟链运维管理开发的 web 组件，企业可以使用联盟共识控制台方便地部署联盟链运行节点，管理联盟成员和授权节点打包区块。

每个参与联盟链的企业节点都部署自己独立的联盟共识控制台，出于安全目的，每个企业节点的联盟共识控制台彼此独立，互不感知，他们通过调用联盟共识智能合约对联盟管理事务进行协商，以达成共识，合约主要方法签名如代码 1

```
contract CCC {
   //初始化合约，传入联盟创建者信息
   //联盟创建者将成为联盟第一个成员和第一个拥有打包区块权限的节点
   function CCC (string _companyname,string _email,string _remark,string _enode) public{
   }

   //联盟新成员申请
   function applyMember(string _companyname,string _email,string _remark,string _enode,address _account) public{
   }
   //投票成为联盟成员
   function VoteMember(uint _fromcompanyid,uint _tocompanyid) public {
   }

   //投票授权打包区块，前提必须已经是联盟成员
   function VoteMine(uint _fromcompanyid,uint _tocompanyid) public {
   }
}
```

代码 1 联盟共识智能合约主要方法签名

联盟共识智能合约目前版本主要包括投票选举申请加入联盟的新成员，及投票选举联盟链新的区块打包节点，由联盟链创立者在第一次启动联盟共识控制台的时候自动创建，该智能合约是联盟链成员进行联盟管理及协商共识的最主要方式。既然联盟成员节点部署的联盟控制台彼此独立互不通信，那么联盟其他成员如何获得联盟共识智能合约的地址？

我们的做法是在联盟链创立者节点的联盟共识控制台第一次部署成功联盟共识智能合约的时候，将该合约的地址发给共识算法模块，共识算法在封装区块头的时候将合约地址写入区块头的 miner 中，记录有联盟共识智能合约地址的区块头如图 2


```
  difficulty: 2,
  extraData: "0xd98301080c846765746888676f312e31302e338664617277696e000000000000e11dd02c05e346c393510a354209c7e0727ac1d738b2a93d18c6b6f6b32348272fa827c38abf50f49445543d8b554db4a20924b27822417f411cab03d8a1959200",
  gasLimit: 4712388,
  gasUsed: 0,
  hash: "0x253ff16f684ebbac73be8ed681b5f63cad1914de32df781a14ce192e6c4226da",
  logsBloom: "0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",
  miner: "0x734413b8a524f6bf645712d23c1dd0e5839c554a",
  mixHash: "0x0000000000000000000000000000000000000000000000000000000000000000",
  nonce: "0xcaffffffffffffff",
  number: 5,
  parentHash: "0x3fad9661da7ddfc028d3890e8ade642470021009e66ca0fa668e1f4f210109f9",
  receiptsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  size: 606,
  stateRoot: "0xa20aa4942863177537ae98455776155faa5283c943c237a9787fa36e3583d585",
  timestamp: 1533712460,
  totalDifficulty: 11,
  transactions: [],
  transactionsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  uncles: []
```


图 2 记录有联盟共识智能合约地址的区块头

其中 extraData 记录经过椭圆曲线加密的区块打包者地址信息，其他节点通过解密得到打包节点地址并验证该地址是否有权限打包节点；miner 中记录联盟共识智能合约地址；nonce 记录一个 magic code "0xcaffffffffffffff"，表示该区块获得了共识合约地址并写入当前区块（其他区块 nonce magic code 为 "0x00ffffffffffffff"）。

联盟链成员节点加入联盟链，同步区块链数据后就可以从区块头中读取联盟共识智能合约的地址，然后通过联盟共识控制台调用该合约，参与联盟管理及协商共识。

Taireum 联盟新成员许可入网

以太坊作为一个公有链，任何遵循以太坊协议的节点都可以加入以太坊网络，同步区块数据，参与区块打包。同时，以太坊作为开源项目，用户也可以下载源代码，自己部署多个以太坊节点，组成一个自己的区块链网络，但是只要这些节点可以通过公网访问，就无法阻止其他以太坊节点连接到自己的区块链网络上，获取区块数据，甚至打包区块。这在联盟链的应用场景中是绝对不能接受的，联盟链需要保证联盟内数据的隐私和安全。

Taireum 重构了以太坊的 P2P 通信模块，只有在许可列表中的节点才允许和当前联盟成员节点建立连接，其他的连接请求在通信层就会拒绝，保证联盟链的安全和私密性。

许可列表即 Taireum 成员列表，通过前述的联盟共识智能合约管理。P2P 通信模块通过联盟共识控制台调用智能合约，获得联盟成员列表，检查连接请求是否合法。

Taireum 联盟新成员许可入网流程：

- 新成员下载 Taireum，启动联盟共识控制台，然后在联盟共识控制台启动 Taireum 节点，获得节点 enode url。
- 将 enode url 及其他公司信息提交给当前联盟链某个成员，该成员通过联盟共识智能合约发起新成员入网申请。
- 联盟其他成员通过智能合约对新成员入网申请进行投票，得票数符合约定后，新成员信息被记入成员列表。
- 新成员节点通过网络连接当前联盟链成员节点，当前成员节点 p2p 通信模块读取智能合约成员列表信息，检查新成员节点 enode url 在成员列表中， 同意建立连接，新成员节点开始下载区块数据。

Taireum 授权打包区块

Taireum 根据联盟链的应用特点，放弃了以太坊 ethash 工作量证明算法，在借鉴 clique 共识算法的基础上，重新开发了 tce 共识算法引擎，对联盟投票选出的授权打包节点排序，轮流进行区块打包。

tce 共识算法引擎执行过程如下：

- 联盟成员通过联盟共识智能合约投票选举授权打包区块的节点（在合约创建的时候，创建者，即联盟链创始人默认拥有打包区块的权限）
- Tce 共识算法通过联盟共识控制台访问智能合约，获得授权打包区块的节点地址列表，并排序。
- 检查父区块头的 extraData，解密取出父区块的打包者签名，查看该签名是否在授权打包节点地址列表里，如果不在就返回错误。
- 根据当前区块的块高（block number），对授权打包区块的节点地址列表长度取模，根据余数决定对当前区块进行打包的节点，如果为当前节点，就进行区块打包，并把区块头难度系数设为 2，如果非当前节点，随机等待一段时间后打包区块，并把区块头难度系数设为 1。尽量使当前节点打包的区块被加入区块链，同时又保证当前打包节点失效的情况下，其他节点也会完成区块打包的工作。

Taireum 应用

在企业应用领域，当多家企业需要进行业务合作的时候，企业间的数据一致性会成为一个极大的挑战，大家无法信任彼此的数据记录，所以通常的做法是大家都通过一个可信任的第三方进行记账，比如国内银行间转

账需要通过央行清算中心。而使用联盟链技术，多家银行构成联盟，通过区块链的分布式记账功能，银行间转账可以通过无中心的区块链进行记账，不再需要第三方记账。

Taireum 兼容以太坊，所有以太坊的应用都可以部署到 Taireum 上。同时 Taireum 作为一个联盟链解决方案，完全适用于企业级的区块链应用场景。

我们以互联网金融企业间的借贷资产共享作为案例看下 Taireum 的应用场景。

由于国家监管的要求，一家互联网金融公司能够为客户提供的借贷金额是有上限的。企业投入成本获得的客户却因为借贷限额或者产品不匹配而流失，对于企业而言是一项损失，如果能将这笔借贷资产共享出去，其他借贷机构可以竞拍得到这笔资产，企业可以借此获得收益，用户也能得到更好的体验。

三家互联网金融企业使用 Taireum 部署资产共享联盟链如图 3。该联盟链仅对企业 A、B、C 三家机构开放，其他组织和个人无法连接该该联盟链网络中。

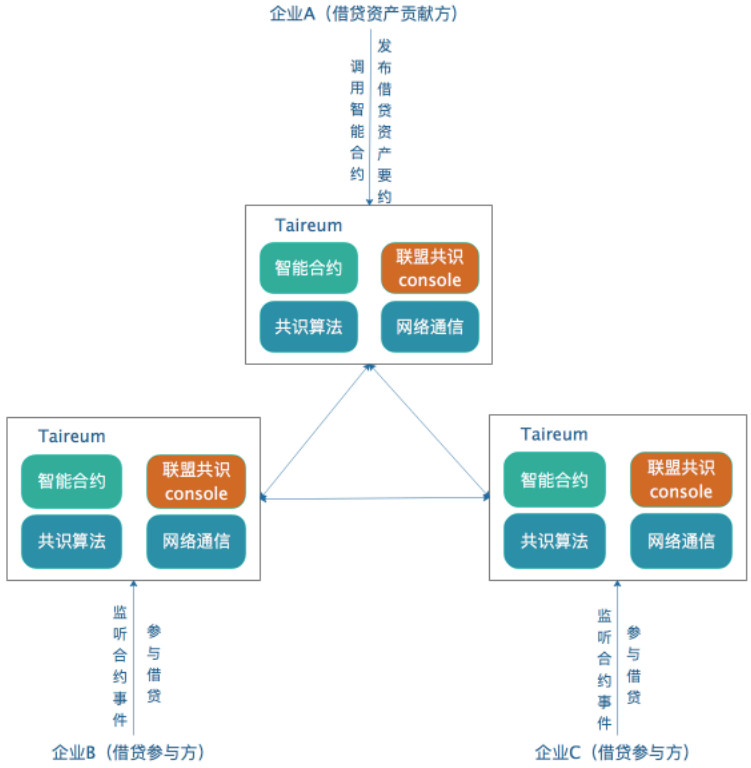

图 3 使用 Taireum 部署的借贷资产共享联盟链

企业 A 如果无法满足其客户的某个借贷需求，就可以将这笔借贷资产通过调用智能合约的方式发布到联盟区块链上，其他公司监听该合约的事件（event），获得借贷信息，如果愿意参与借贷，就调用智能合约竞拍该笔借贷资产。

金融资产共享合约主要方法签名如代码 2

```
contract SharedAssets {

  //新增共享借贷资产事件
  event AssetAdded(bytes32 _id, bytes32 _userHash, uint _interset, uint _amount);
  //新增参与投标事件
  event BidAdded(bytes32 _id, address _addr, uint _interset, uint _amount, uint _deposit);
  //参与投标选中事件
  event BidChoosed(bytes32 _id, address[] _addrs, uint[] _states);

  //新增共享借贷资产
  function addAsset(bytes32 _id, bytes32 _userHash, uint _interset, uint _amount) public returns(bool) {
  }

  //借贷参与者投标
  function addBid(bytes32 _id, uint _interset, uint _amount, uint _deposit) public returns(bool) {
  }

  //共享借贷资产发起人选中投标
  function chooseBid(bytes32 _id, address[] _addrs, uint[] _states) public returns(bool) {
  }
}
```

代码 2 金融资产共享合约主要方法签名

只要联盟成员同意（通过联盟共识智能合约协商一致），可以有更多的企业加入到联盟链中，细分出更多成员角色（风控服务成员，保险服务成员等），构建出更加完整和复杂的生态。

总结

我们在以太坊的基础上进行重构与开发，实现了 Taireum，一种适用于联盟链场景的企业级分布式账本与智能合约平台，Taireum 具有如下特点：

安全性：

- 许可入网，p2p 通信模块进行安全校验，只有授权节点才能加入联盟链网络，未经许可的节点会被当前联盟链所有节点拒绝通信
- 授权打包区块，使用 taireum 自己实现的 tce 共识算法引擎，只有授权节点才能打包区块，未经授权的节点打包的区块会被遗弃，授权过程通过 Taireum 内置智能合约投票完成

易用性：

- web 可视化构建联盟链集群，部署、启动、许可、授权、监控区块等一系列常用操作都通过 web console 进行

完全无中心：

- 和目前主流的联盟链平台方案相比，Taireum 通过智能合约进行联盟共识协商，无需 CA 中心，联盟内各个节点自治无依赖，更符合区块链的初衷与本质
- 每个成员节点独立部署自己的联盟控制台，彼此完全独立无通信，联盟共识控制台通过智能合约协商联盟共识

兼容以太坊的生态体系：

- Taireum 兼容包括智能合约、web3 在内的所有以太坊生态体系
- 所有在以太坊上开发的 Dapp 应用可无缝迁移到 Taireum 上

参考资料

Taireum 项目源码：https://github.com/itisaid/go-ethereum

以太坊 wiki：https://github.com/ethereum/wiki/wiki

Hyperledger 白皮书：https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf