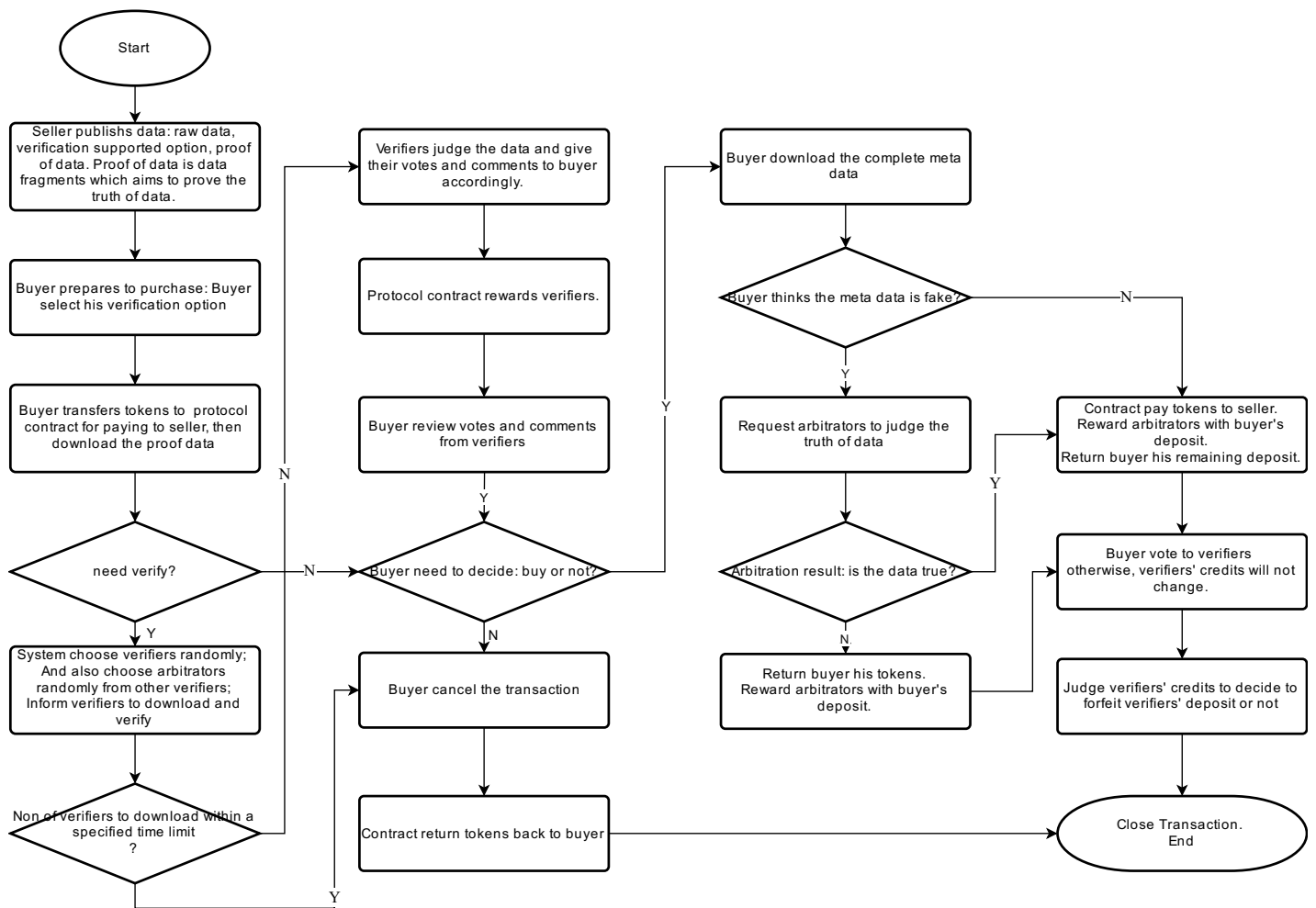


设计原则

- 数据私密性
- 验证准确度
- 用户匿名
- 资金安全性
- 谁主张，谁举证
- 尽量简单

业务流程设计

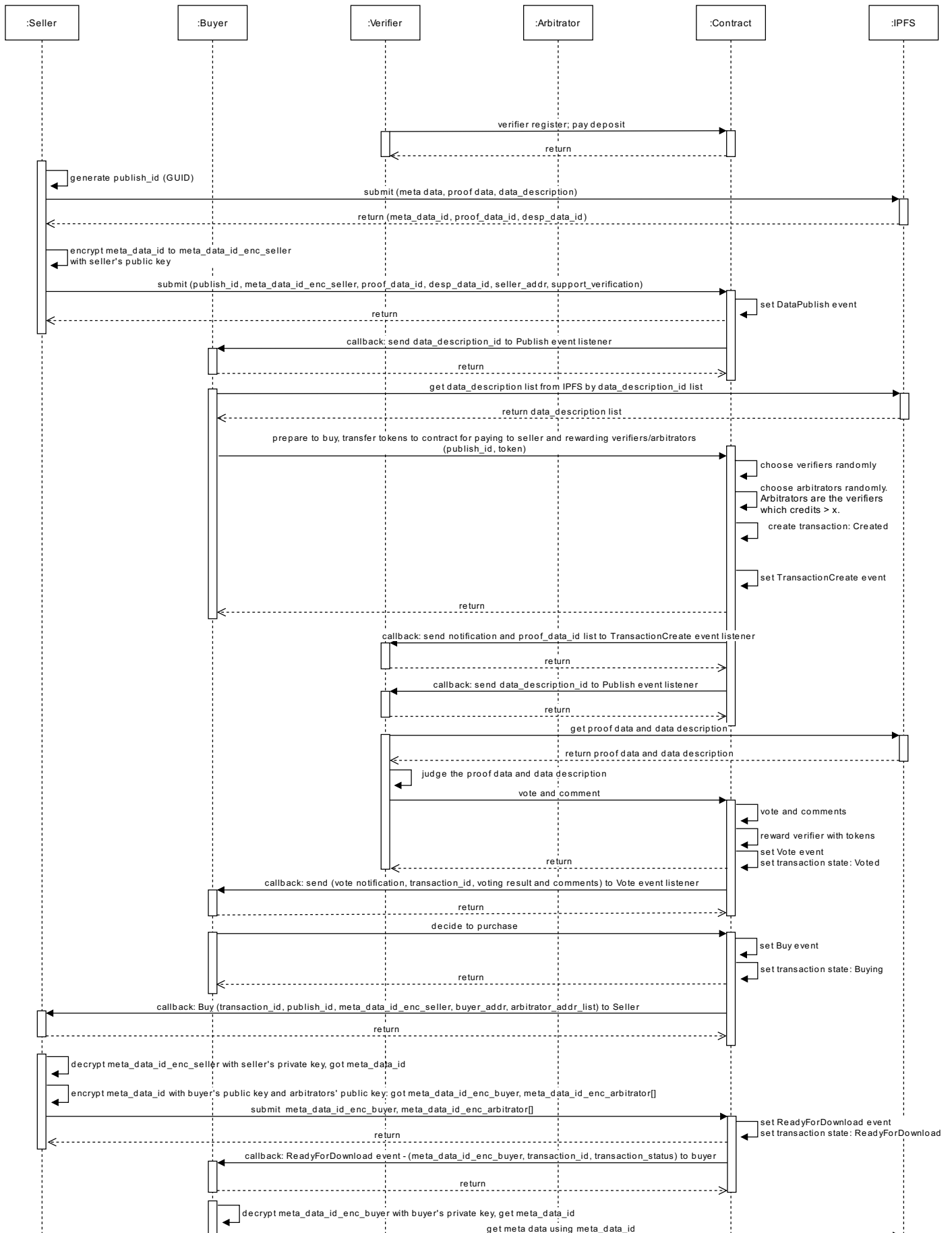


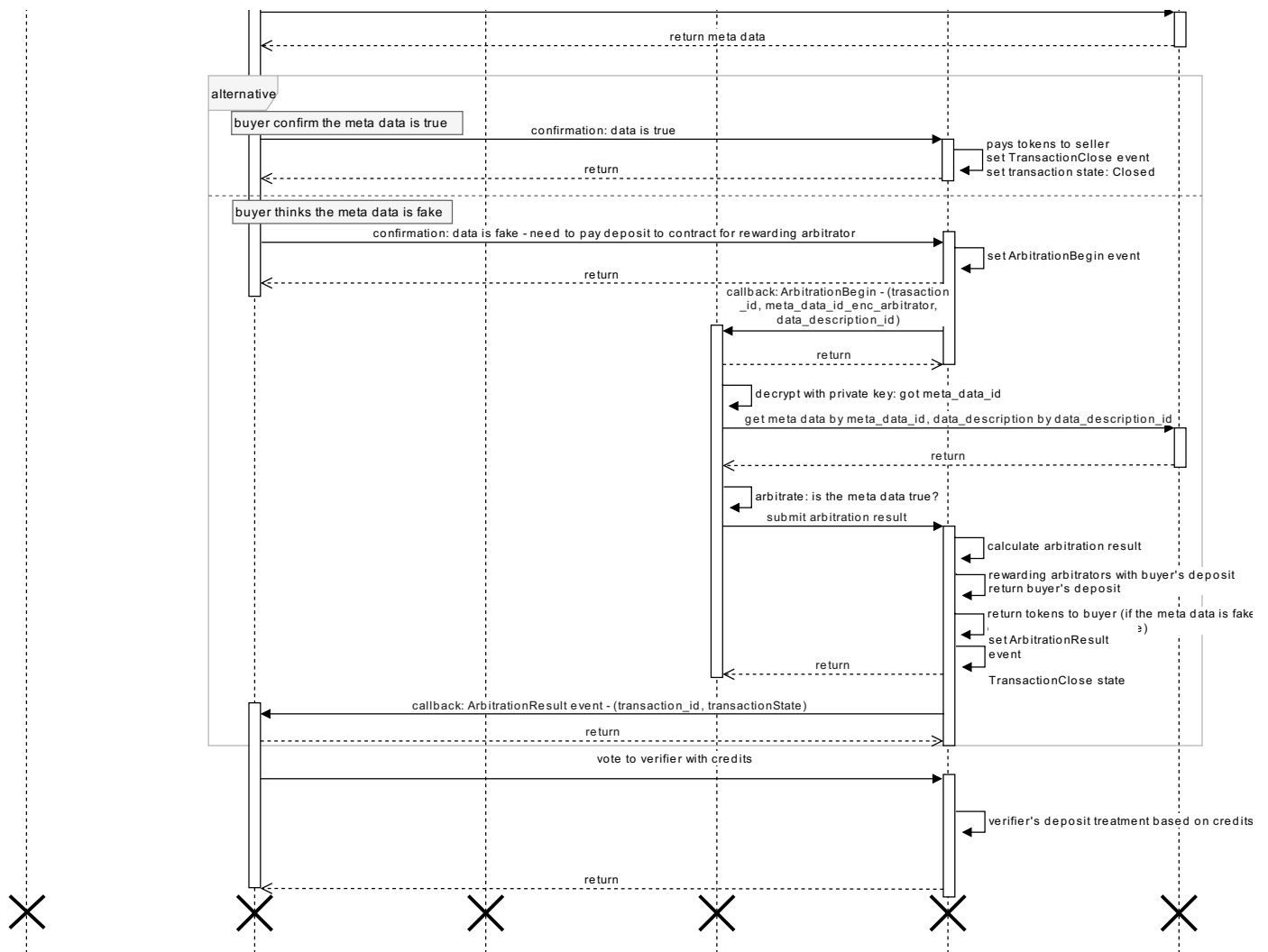
几个重要的问题及说明

1. seller可以选择是否启用verify机制，即图中verification option。buyer同样可以选择是否启用verify机制。
2. seller发布的数据，包括了元数据，数据证明。数据证明的设想是：首先，seller需要明确指出其发布的数据的类型，关键内容；其次，seller需要举出至少一处能够证明上述关键内容的元数据片段，并以文字或者图片形式发布。
3. 针对verifier，系统设计了credit机制。具体credit机制可参考滴滴打车，是一个平均分评价机制。当verifier的credit低到某个值以后，系统会没收其押金，该verifier从此会失去verify资格。
4. 开始验证程序后，buyer和verifier都会收到系统发送的proof data。buyer可选择取消购买，系统会退回相应押金和货款。
5. buyer购买了data后，能够下载完整的data。这时，buyer可对verifier进行投票打分。

6. seller一旦发布了数据，就永远不能更改。
7. 在seller上传用buyer公钥加密的数据之前，buyer都可以取消交易

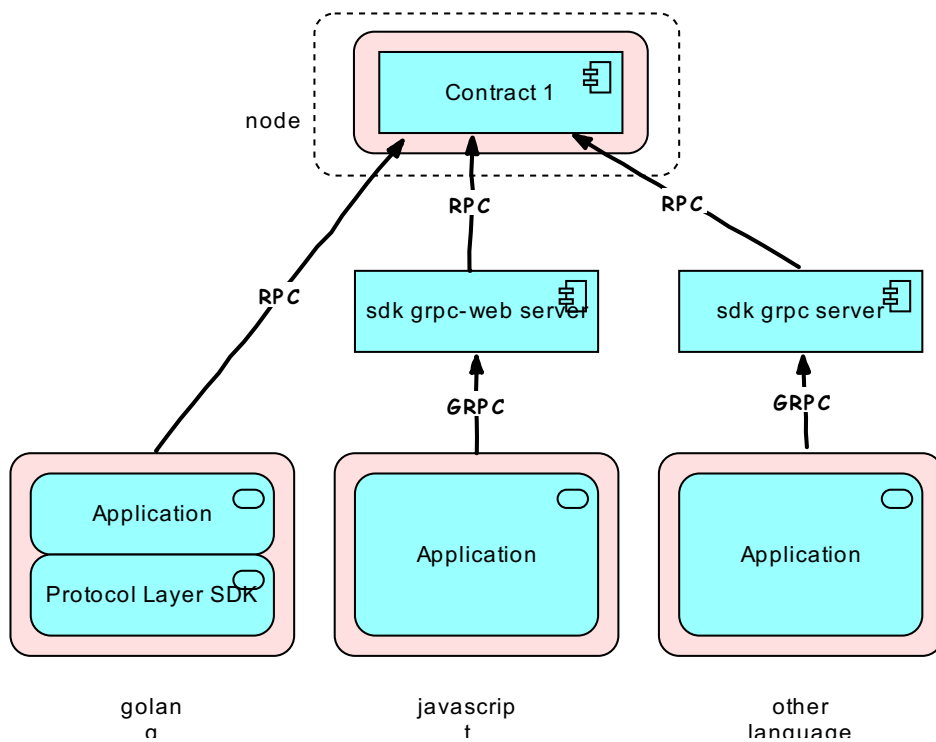
组件交互流程设计





系统架构

方案



特点

- 提供三种类型的api接口：native go lang sdk接口；grpc web接口；grpc接口
- 支持多用户调用
- 要求客户端自行安装IPFS节点
- 提供事件订购通知机制

SDK接口模式

- native go lang sdk: go lang可以直接调用该sdk，位于同一进程内
- grpc web: javascript可以访问web端口，直接调用javascript rpc方法；需要单独部署server
- grpc: 通过调用protobuffer接口，可以直接访问rpc方法；需要单独部署server

SDK接口定义

接口名称	接口描述
CreateAccount	创建账户
PublishData	发布数据
RegisterVerifier	注册一个verifier
GetDataDescriptionList	取数据描述列表
PrepareToBuy	准备买
GetProofDataList	取proof data 列表
VoteAndCommentForMetaData	依据proof data，给meta data投票和评论
GetVoteAndComments	取投票结果和评论结果
BuyData	决定购买数据
FeedbackMetaDataTruth	反馈数据的真实性
DoArbitration	进行仲裁
VoteToVerifier	投票给verifier

合约

合约设计

- token contract - 由于ddd是erc20标准的token，为保持一致，且考虑到安全性，选择继承自OpenZeppelin的StandardToken作为测试token
- 业务 contract - 包含整个交易的所有逻辑处理

交易

交易状态

Created

Voted

Buying

ReadyForDownload

Closed

交易超时

交易超时，需要对交易做相应的处理：退费，自动关闭交易等。系统提供了`cancelTransaction`方法来取消交易。