自组织价值网络(Self-Organized Value Network)

# 背景

现今所有的企业或组织（下只简称企业）开发的网络产品（除作为公用基础设施的互联网外），都存在一个明显的特征，就是核心资源都是中心化的。企业都需要运营自己的数据中心，即便这个数据中心是运行在云上。这种集约式的运营模式有一个明显的弊端，就是不能很好应对信息爆炸的问题。虽然随着高可用分布式微服务架构及大数据技术的持续发展，这些问题得到一定程度的缓解。但是随着数据的持续增长，在系统资源有限的情况下，所有目前认为合理的设计都将遇到性能瓶颈。目前解决性能瓶颈的办法，只能是增加资源。但增加资源带来的副作用就是增加管理成本。面对成千上万的服务器，用人来管理肯定是不现实的，这就需要相对的辅助技术及运营平台（如采用容器化技术,容器编排引擎等实现的DevOps）。

# 2、以一过性密钥实现无身份认证

自组织价值网络不保存用户的身份信息。所以用户只能自己保管自己的信息，系统对用户提交的身份信息，只做身份认证，并对用户的身份确信度进行评估。当评估值达到一定阀值，

一过性密钥的特点：当用户在系统中产生的交互次数越来越多时，用户的不可伪造性越高。可以防范密钥攻击。

一过性密钥原理：用户每与系统进行一次交互，就会得到系统重新生成的公钥密钥对，系统会使用交互内容进行签名。并对公钥，密钥，签名交回用户保管。用户需要妥善保存这些信息，以便实现无身份认证

公钥 -> 用户名（签名）

验证：-> 私钥 （校验）

公钥：-> 数据内容（加密）

验证：-> 数据内容（解密）