

信云端和用户端分别存储部分私钥，云端采用可信的硬件密码设备，用户端基于智能终端软实现，以分布式算法为纽带，通过软硬结合的技术手段有效平衡了可靠性与可信性。该方案的技术特征在于，云端不掌握用户的全部私钥，不能脱离用户独自伪造签名；用户端所掌握的部分私钥受到云端的牵制和保护，使得离线攻击难以实现，认证机制难以绕过。

综上，针对可靠性及可信性这一对矛盾，终端脱机密钥保护技术以牺牲可靠性为代价提高了可信性，云端托管密钥保护技术以牺牲可信性提升了可靠性，基于分布式密钥体系的软硬结合密钥保护技术使可靠性及可信性达到统一，具有较高的发展前景。虽然分布式技术以系统化的运行方式，由用户端和可信中心分散了安全风险，然而，根据“木桶效应”，系统的安全性取决于保护能力最弱的短板。针对保护能力最弱的智能终端（短板），如何进一步提升安全性，将是智能终端电子签名技术领域亟待解决的重要课题。

收付宝科技有限公司（以下简称“收付宝”）是一家成立于 2013 年的高科技信息安全公司，从成立之初始终致力于移动互联网可信计算环境的安全研究，为金融、能源、公安、军队等关键信息基础设施保驾护航，以技术创新及社会责任为己任，加速国家网络安全战略的落地，共同维护国家网络空间的健康发展。

收付宝始终秉持“产学研用相结合”的理念，与国内多家知名的科研机构形成长期的技术合作关系，参与了多项国家、行业标准规范的起草和制定工作，与产业链各方精诚合作，合力打造创新的、全方位的信息安全服务模式。

通过多年的潜心研究，收付宝目前拥有与网络安全相关的多项自主知识产权专利和著作权，所研发的动态密码技术“一种基于密钥更新的私钥保护方法、系统及装置”，可实现传统静态密钥体系到动态密钥体系的升级，有效抵御短板攻击，且不影响公钥可用性，以一次一密的创新技术提供智能终端的电子签名服务。FCC

率先突破： 中国农业银行总行区块链项目正式上线

近日，基于趣链科技底层区块链平台，中国农业银行总行上线了基于区块链的涉农互联网电商融资系统，并于 8 月 1 日成功完成首笔线上订单支付贷款。这是国内银行业首次将区块链技术应用于电商供应链金融领域，标志着中国农业银行在区块链技术应用领域走在了同业前列。

利用区块链的分布式记账、不可篡改、可追溯、信任成本低等技术特性，中国农业银行基于趣链科技提供的区块链技术平台将涉农电子商务、供应链融资、网络支付、

企业 ERP、农资监管等行内外系统打造成联盟链，建立了以信任共识为基础的数据共享、流程简化、客户体验良好的业务和产品机理，为“三农”客户提供在线供应链融资服务，为尝试解决“三农”客户长期面临的因担保物不足、信用数据欠缺造成的融资难问题提供了思路。

此次，中国农业银行基于该区块链平台首期推出了“E 链贷”产品，将区块链技术优势与供应链业务特点深度融合，为农业银行提升三农业务效率，拓展服务内涵提供技术手段和商业机遇。FCC