

新加坡 18区

让1800万人
了解区块链

张玉

库神钱包 COO

暨18区“分布式区块链社区全球行”
第五站北京站





区块链资产安全终极解决方案

北京库神信息技术有限公司

联合创始人&COO

张玉

CATALOG

目录

01. 区块链资产时代已经到来
02. 探究区块链安全核心问题
03. 区块链资产安全方案比较
04. 库神的终极创新安全方案

01

区块链资产时代已经到来

区块链各领域蓬勃发展，从硬件制造、基础设施到底层技术开发、平台建设，再到安全防护、行业应用，以及媒体社区等区块链行业服务机构，已经初步形成了一个完整的产业生态链。

区块链产业生态地图



图 3 2018 年中国区块链产业生态

01

区块链资产时代已经到来

一、全球政策：

2018年2月6日，美国SEC表示：金融数字化是不可逆转的趋势。如同天方夜谭中的精灵，你不可能把它再塞回到瓶子里。所以必须在承认它拥抱它的前提下，研究制定这个新的形态的各种政策来帮助它的发展和让自己变得不要过时。

二、资产总量：

全球数字资产总流通市值于2018年1月8日达到最高峰值8355.10亿美元。

2018年7月9日，全球数字资产数量为1619个，总流通市值为2736.39亿美元，其中BTC占比42.4%。

三、发展趋势：

资产区块链化是不可逆转的历史潮流！区块链资产时代已经到来！

四、安全问题：

与此同时，数字资产安全问题屡见不鲜，数字资产安全存储作为区块链产业链上一个重要环节，需要打造更加安全可靠的存储环境。

01 区块链资产安全案例一览

继2014年Mt.Gox被盗事件之后，以太坊Parity，The Dao，Bitfinex，CoinCheck，Coinrail，Bithumb等交易所，因为受到黑客攻击造成用户资产被盗，损失惨重。

“近4年来，全球的交易所丢失了超过100万个比特币。未来随着区块链资产的市值越来越高，区块链资产被盗的后果就会更加严重。”

“互联网发生安全事故丢失的是信心，币圈安全事故丢的可能是命了。”一位区块链安全人士表示。利益之下，黑客肆掠，币圈无人幸免。---深链财经

数字资产交易所安全事件（据不完全统计）

时间	交易所	损失金额
2018年6月19日	Bithumb	3150万美元
2018年6月10日	Coinrail	超4000万美元
2018年4月12日	Coinsecure	350万美元 (438 Bitcoin)
2018年2月8日	BitGrail	1.95亿美元 (1700万 Nano tokens)
2018年1月	Coincheck	5.34亿美元 (NEM)
2017年12月19日	Youbit	4000万美元
2017年12月7日	NiceHash	6400万美元 (4736 Bitcoin)
2017年4月21日	Yapizon	500万美元 (3831 Bitcoin)
2017年4月22日	Yapizon (后更名为Youbit)	530万美元 (3816BTC)
2017年5月	Gatecoin	214万美元 (18.5万 ETH和250 BTC)
2016年8月3日	Bitfinex	7200万美元 (119, 756 Bitcoin)
2014年12月1日	Mt.Gox	3.87亿美元 850, 000 Bitcoin
2012年5月11日	Bitcoinica	9万美元 (18547 BTC)

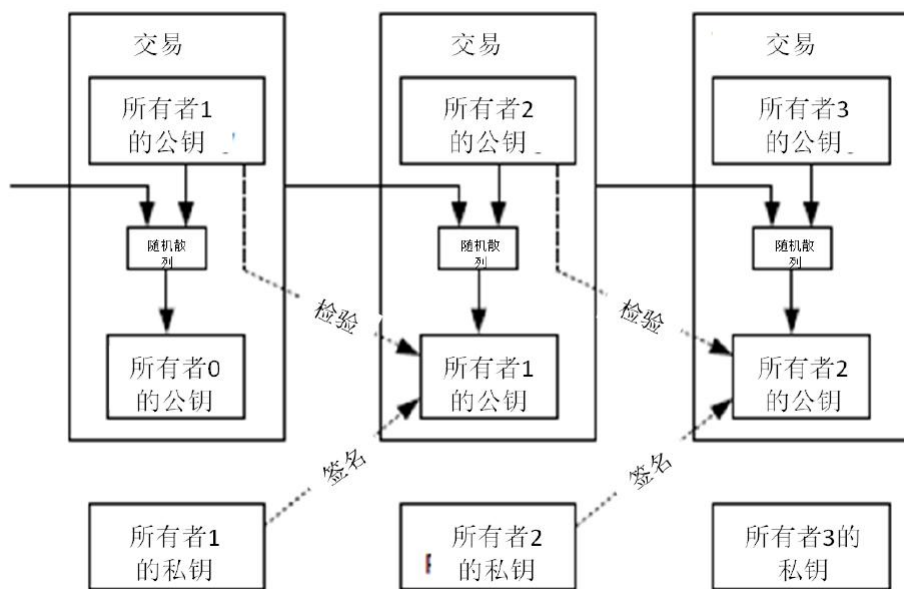
02

探究区块链安全核心问题

区块链资产定义：

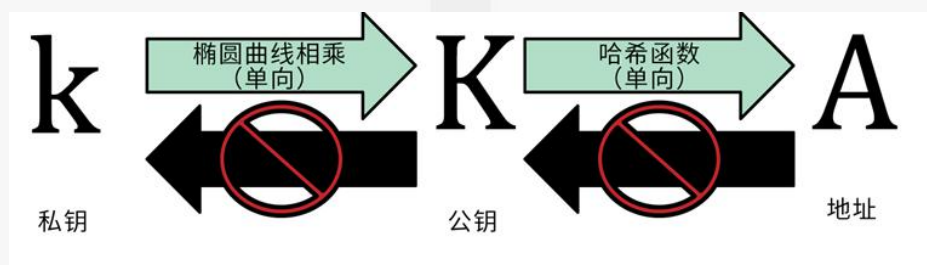
区块链资产实际是一串数字签名：

1. 每一位所有者通过对前一次交易和下一位拥有者的公钥签署一个随机散列的数字签名；
 2. 并将这个签名附加在资产的末尾，资产就发送给了下一位所有者；
 3. 而收款人通过对签名进行检验，就能够验证该链条的所有者。
- 区块链资产支付本质是数字签名和验证的过程。



02

探究区块链安全核心问题



ECDSA是使用椭圆曲线对数字签名算法（**DSA**）的模拟，保证私钥对区块链的绝对拥有权。

一、区块链资产在哪：

区块链资产实际在区块链上，所有者实际只拥有私钥，并通过私钥对区块链上的资产拥有绝对控制权。

二、区块链资产核心：

所有者私钥！

三、安全的核心问题：

私钥存储！

03

区块链资产安全方案比较

究竟哪种存储更安全？

1. 中心化 vs 去中心化？
2. 联网 vs 不联网？



PC端钱包



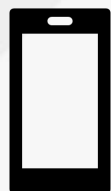
纸钱包



Web端钱包



脑钱包



APP钱包



硬件钱包

03

区块链资产安全方案比较

区块链资产钱包定义为：

用以安全存放区块链资产私钥，可以用私钥签名以发送区块链资产，并能够查询区块链显示资产余额的软硬件设备。

这个定义主要是指链上钱包，链下钱包并不具备上述功能。

此外，像纸钱包和脑钱包只是用来保存私钥，本身无法发送和查看区块链，算是功能不完备的钱包。

类别	链上钱包				链下钱包
	冷钱包 (离线钱包)	硬钱包 (本地钱包)	热钱包 (在线钱包)	多重签名钱包	
私钥存储位置	离线设备 (电脑、手机、专业硬件设备)	用户本地设备 (电脑、手机等)	钱包服务器	服务器和本地各一把私钥	用户不掌握私钥
安全性	最高	需联网	需联网	需联网	失控

03

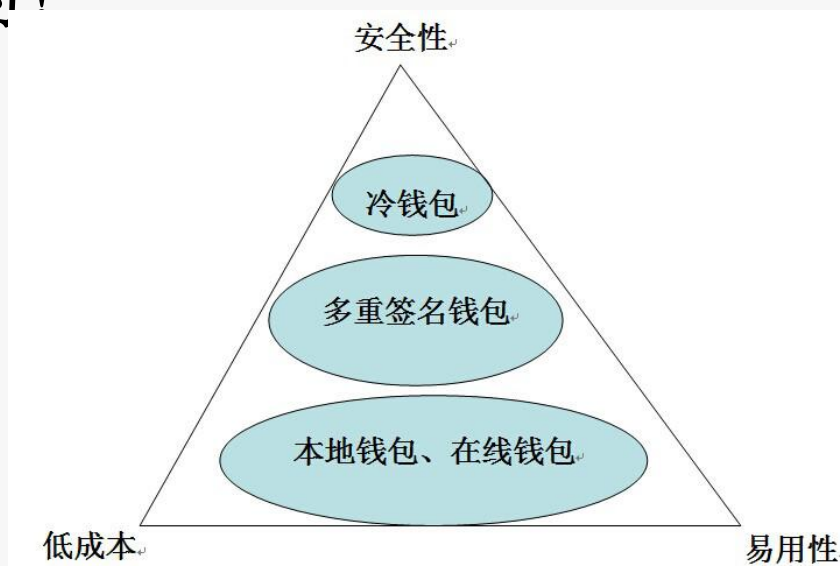
区块链资产安全方案比较

三个观点：

一、唯一安全的方案是冷钱包，交易过程不联网才是真的安全！

二、钱包并非真正是钱包，确切的叫法是私钥保险柜！

三、在安全性、易用性和低成本之间，也构成一个不可能三角形：一个钱包，既要保证绝对安全，又要极其易用，还不需要用户掏钱，那是不可能的！



04

库神的终极创新安全方案

库神硬件冷钱包，是全球第一款基于智能操作系统的区块链资产存储设备，可存储多种区块链资产。

库神钱包系统采用冷热分离架构，二维码通信方式让私钥不触网，彻底根绝私钥被黑客窃取的风险。

钱包由两部分组成：硬件冷钱包（冷端）及库神 APP（联网端）。

冷端主要负责构造交易并对交易进行数字签名，库神 APP 负责查询地址余额及广播发送交易。

私钥永不触网

冷库到底，专业保护区块链资产安全。



04

库神的终极创新安全方案

传统的储存方式

旧硬盘/笔记本电脑/手机：易丢失、损毁

PC端/Web端/APP钱包：联网易被黑客攻击

交易所账户：中心化的被盗风险

库神硬件冷钱包

- 冷热端分离，杜绝网络攻击
- 二维码通信传输，安全不触网
- 种子密码+支付密码双重保护私钥
- 指纹解锁、手势密码多种锁定方式
- **计算器而非存储器，私钥不存储**

04

库神的终极创新安全方案

2018 年中国区块链产业白皮书

北京库神信息技术有限公司自主研发的硬件冷钱包，是一款基于智能操作系统的区块链资产存储设备，可存储多种区块链资产。库神钱包系统采用冷热分离架构，二维码通信方式让私钥不触网，彻底根绝私钥被黑客窃取的风险。钱包由两部分组成：硬件冷钱包（冷端）

— 22 —

工信部信息中心 | 起风财经区块链研究院


及库神 APP（联网端），冷端主要负责构造交易并对交易进行数字签名，库神 APP 负责查询地址余额及广播发送交易。冷端接触私钥，但不接触网络。库神 APP 接触网络，但处理的都是区块链公开透明的信息，无安全风险。

随着全球范围内黑客攻击的日益增加，对于钱包安全性的挑战将会越来越大，钱包公司需要通过对产品和技术的不断迭代更新，来为用户的数字加密资产保驾护航。

工业和信息化部信息中心

2018 年 5 月

报告编号: SICSTC/TR-ZJ20180019

 国家信息中心软件评测中心
State Information Center Software Testing Center

委托评测报告

项目名称: 库神钱包系统
委托单位: 北京库神信息技术有限公司
报告时间: 2018 年 05 月 04 日

我们一直在进步:

库神公司作为企业示范案例入选工信部2018年中国区块链产业白皮书;

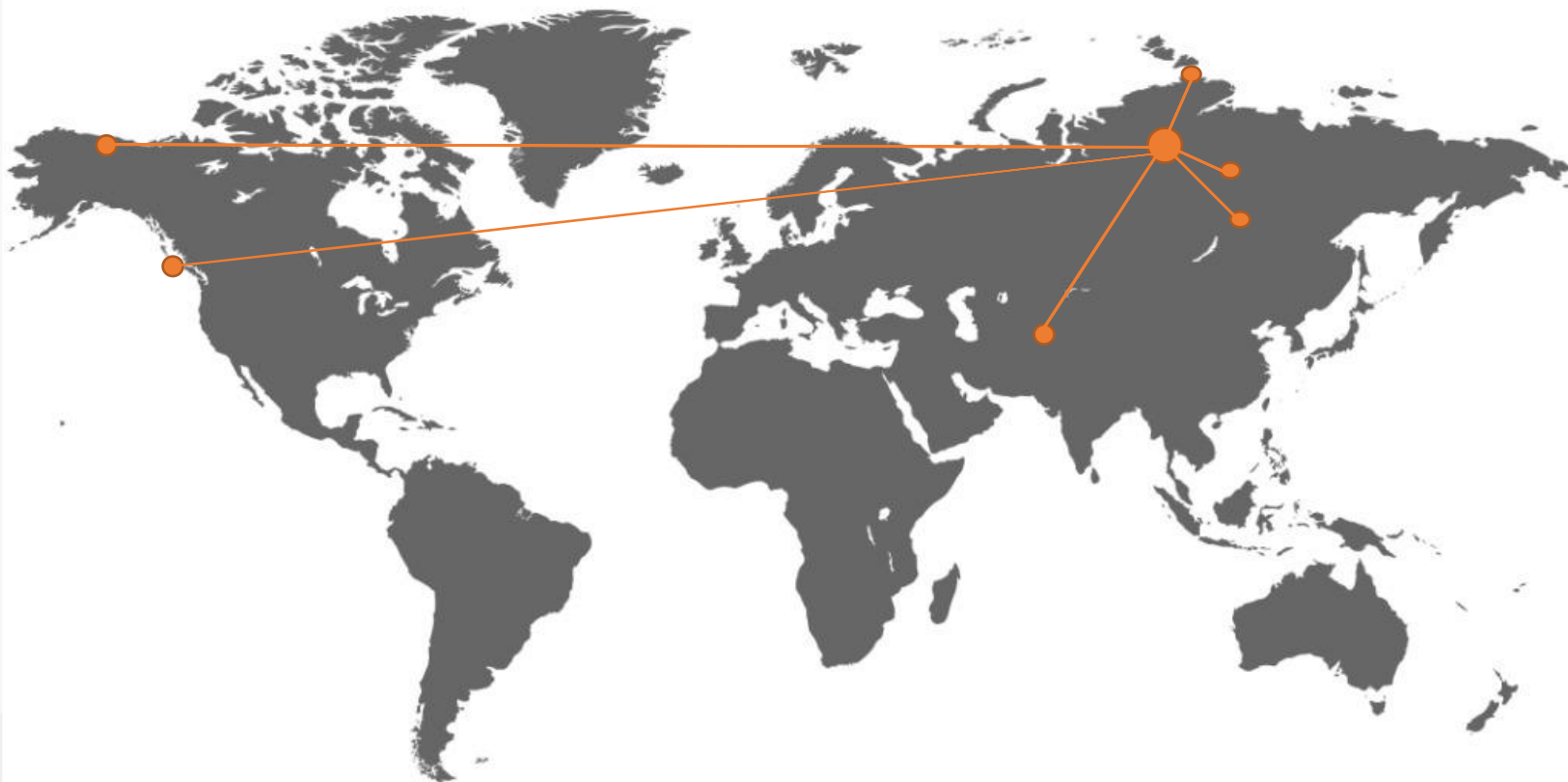
获得多项产品专利、八项软件著作权证书和国家高新技术企业证书;

产品通过了国家信息中心软件测评中心的评测认证,此外还有欧盟CE、美国FCC、欧盟RoHS、日本PSE等一系列国家和国际认证。

04

库神的终极创新安全方案

库神已经进军美国、日本、韩国、东南亚市场，目前正积极布局欧洲及其他市场，开启全球品牌战略计划。



05

北京库神信息技术有限公司

北京库神信息技术有限公司是一家提供区块链数字资产安全存储服务的公司，公司成立于2016年11月18日，成立伊始就获得了**火币网**、**比特大陆**等行业知名企业的投资，并于2017年12月完成了一千万美元的A轮融资。在未来库神公司将继续深耕技术，拓展海内外资源，为用户提供更安全更便利的安全存储服务。



袁大伟

创始人兼CEO
火币网联合创始人，北京大学
金融科技创新实验室学术委员



周邛飞

联合创始人兼CTO
中国科学院智能控制博士
生，亚洲区块链协会(DACA)
讲师，清华大学区块链公开
课讲师



张玉

联合创始人兼COO
北京大学硕士，中国人工智能
学会会员，中国中文信息学会
会员，中国语音产业联盟理
事，北京大数据研究院保险大
数据研究中心高级研究员



王雯雯

联合创始人兼CMO
美国金融MBA学，VeeShop
微烧严选创始人

05

北京库神信息技术有限公司

投资机构者

学术支持

战略合作



BITMAIN

北京大学金融科技实验室



使命：区块链资产保护神！
愿景：全球一流的区块链资产安全服务提供商！

THANK YOU!

