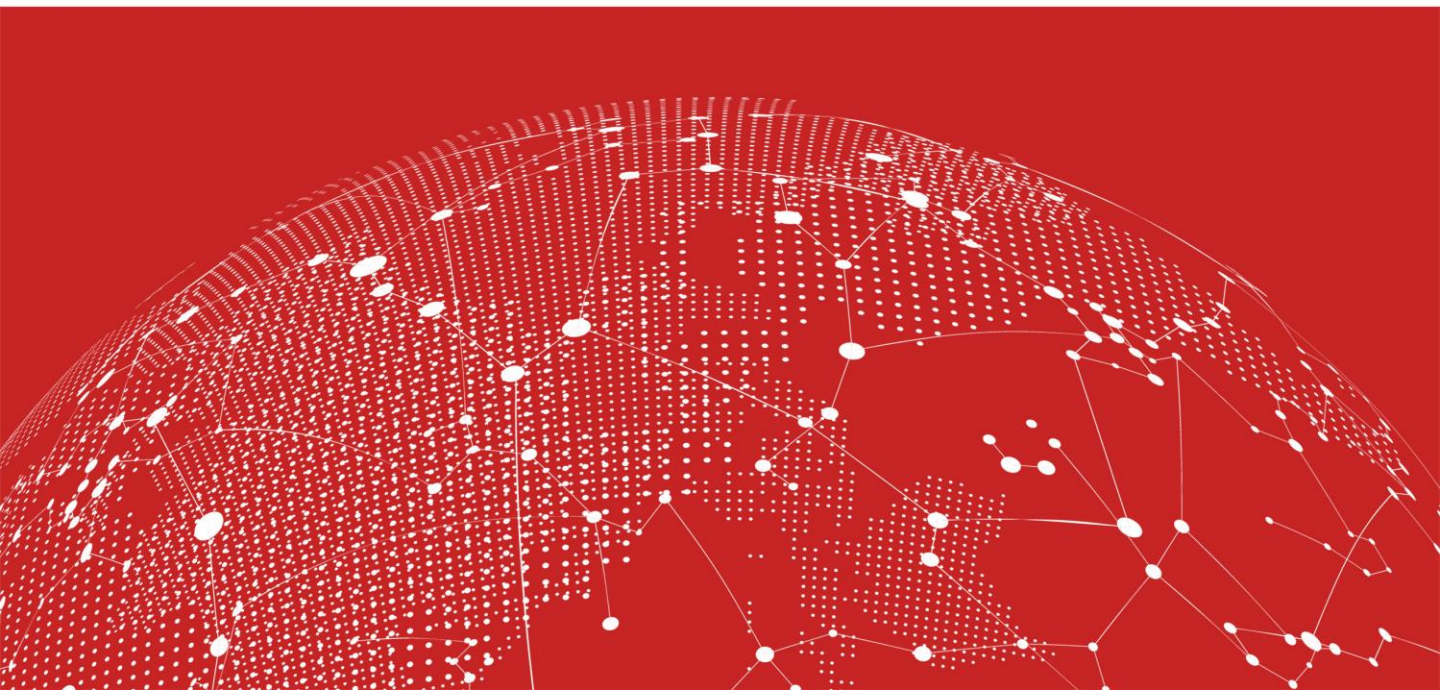
天网Sky Net Security

面向区块链行业的整体安全解决方案

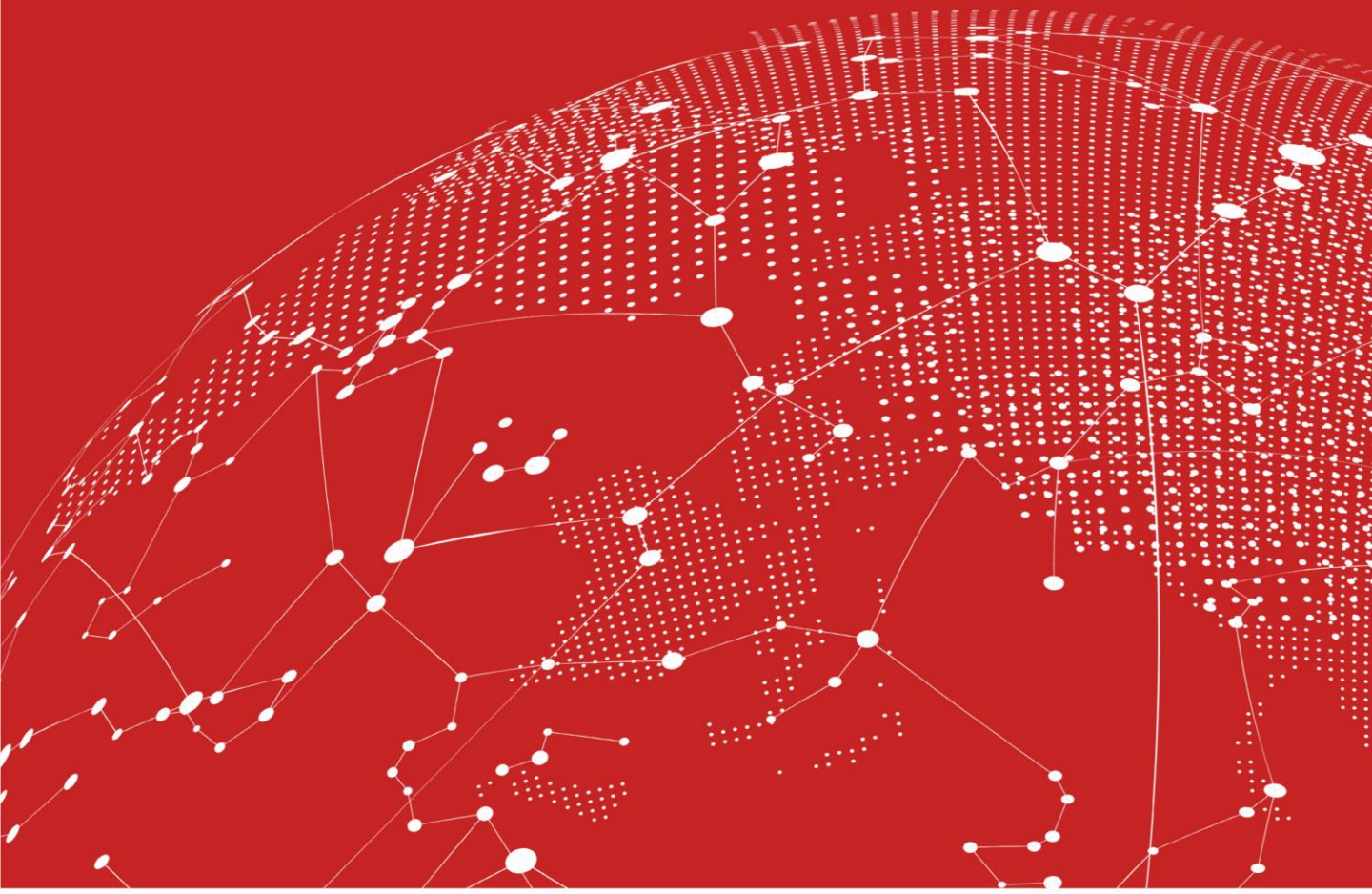
白皮书（中文版）



一、什么是天网

天网Sky Net Security

面向区块链行业的整体安全解决方案



天网，是面向区块链行业各个安全痛点，
一项整体的安全解决方案。

1.1、天网的使命

为区块链的世界带来安全感；
用区块链技术升华安全行业；

1.2、天网的意义

区块链是一项能改变世界和人们生活的技术，但如今，黑客在区块链行业肆意妄为，造成了巨大破坏和资损。

大多数的交易所都被盗过币；

很多人也都发生过Token丢失的情况；

同时，区块链机理，决定了区块信息只能是公开透明，这注定了对于个人隐私进行保护的愿望，只能背道而驰，究竟应该引入什么技术，能在不破坏区块链技术原始价值的基础上，增加人们在应用区块链时的安全感呢？

天网项目，应运而生。

早在2016年，天网的核心技术团队就在尝试用机器学习去解决数据泄漏的问题，用算法为访问行为进行训练/建模，从而达到区分恶意访问流量和正常访问流量的区别。

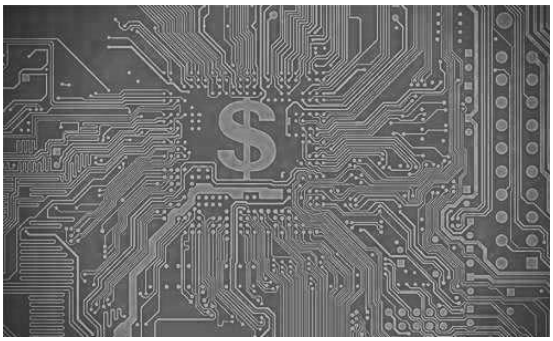
直到2017年7月，天网项目正式进行了技术转型，确定了用区块链技术去解决区块链行业安全问题的愿景。

1.3、天网要做什么

① 普惠的天网安全体检服务

② 提供数据安全的天网盾

③ 去中心化的天网云存储服务



④ 基于全球区块链地址的天网威胁情报库

二、区块链行业，黑客的乐土

区块链世界（交易所、钱包、矿业），如今已经成为了黑客攻击的“乐土”，各种对业务的破坏、盗币，以及各种因为不安全的代码规范，带来的诸多漏洞，系统层面、业务逻辑层面...数量之多，胜似满天星。

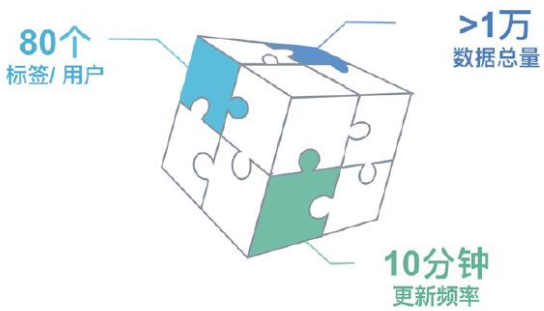
尤其是交易所，因为通篇一律的“标准模版”，造成了大多数的交易所，不堪一击。各种盗币、用户信息泄漏...

一切的原罪，都来源于一个问题：数据泄漏

2.1、大数据时代背景

如今我们已经步入大数据时代,数据也已成为各行各业的第一生产力。

同时,我们每个人都是数据的使用者和生产者。据某省级运营商分析,每个手机用户,每天将产生80个维度的数据标签,每10分钟更新一次,这意味着一个手机用户每天将产生1万多条数据。



此外,数据的价值也越来越大,无论是个人的资产还是企业的资产,早已不局限于银行账户上的那串数字。

我们是否计算过,一个公民的个人信息、社会关系、网站账号、交易所账号、密钥...这些数据资资产的价值究竟有多大?已经远远超过个人或企业储存在银行里的现金价值。

2.1、数据泄漏，为区块链行业带来的影响

被盗币 （私钥被窃）	丢币 （手机损坏、助记词遗忘）	DDoS （交易所、矿场出口）
地址仿冒 （区块链地址篡改）	交易伪造 （API Key被窃）	APP木马 （终端，尤其是安卓）

（3大安全问题频发的领域：交易所、钱包、矿业）

由于数字资产的高价值性，发生在交易所的数据安全事件更是数不胜数:

- 2012年，Bitcoinica被黑客崭取了4.6万个比特币；
- 2013年，纽约的 Bitfiloor,被黑客窃取了钱包私钥,损失了2.4万个比特币；
- 2014年，门头沟事件(Mt.Gox),85万个比特币凭空消失；
- 2015年，曾是全球最大的比特币交易所 Bitstamp被黑客攻击,损失500万美元；
- 2017年7月，韩国最大的比特币交易所 Bithumb遭黑客入侵,3万名客户的数据被泄露,黑客利用崭取来的数据进行"语音钓鱼",造成大量客户的资金损失；
- 2017年12月，韩国的 Youbit被黑客窃取大量数字资产，面临倒闭；

我们称这些事件为“盗币”

所谓“盗币”,即黑客通过网站系统漏洞攻进了交易所，获取了大量用户数据(注册信息、私钥、账户、交易记录等)，并进行篡改和非法转币的过程。

质量参差不齐的代码，只能为区块链行业，
带来胜似满天星的漏洞

除了区块链，数据泄漏所带来的危害和影响，也在我们的生活中，无孔不入。

每个人都接到过无数的骚扰电话,这便是个人数据被窃取的后果。2016年8月，一位名叫徐玉的大学生遇电信诈骗,最终郁都而亡。这一切的源头都来源于地下黑色产业对个人数据的窃取和贩卖。每一年，仅中国的地下黑色产业,围绕数据信息的交易额已经超过1000亿元。数据的非法交易已经成为继贩毒、赌博之后的第3大黑色产业。

数据泄漏，给这个世界带来的混乱

1.4、数据安全的问题已引起各国的关注

全球各个国家都在推出各种法案,企图去保护数据的安全(例如最早由瑞典推出的《国家数据保护法》,以及英国的《数据保护法案》、美国国的《联邦计算机系统保护法》、俄罗斯的《关键信息基础设施保护法》,中国的《网络安全法》等。

这些法案包括2018年5月25日执行的，被称为欧盟史上最严厉的安全法案《通用数据保护条例》，简称GDPR。

据相关数据统计,目前全球泄露的数据条目数已达300亿条,已经远远超过全球人口的总数,并且年增速在不断提高。

三、区块链行业，安全的尴尬

大多数区块链行业的IT架构，仍然是一个传统的IT架构。

例如交易所。数据的集中存放，应用的集中处理，造成了交易所仍然像一个普通的互联网机构一样，处处可见中心化。

传统互联网发生的安全问题，在交易所，只增不减。

3.1、中心化架构，是一切不安全的根因

从技术架构来看,无论是个人数据,还是企业数据;无论是使用 MYSQL、Oracle、DB2，还是 Sqlserver；无论是在DB层面的热数据,还是 Storage层面的冷数据。其数据的存储方式，都是采用一种"中心化"的存储方式，目的是便于存取、便于构建关系型的访问关系。

但是，这种"中心化"的数据存储思路,正是构成数据泄漏难以防御的真正"病因"。黑客利用简单的方式,一旦攻破了"中心化"存储节点,即可获得全部的完整数据。

这与银行总被打劫同理:因为现金都是"中心化"的放于金库之中的,劫匪只要突破了金库大门,即可获得大的现金。试想,如果银行把现金分散且安全地放置于这个城市中的每一栋大楼的每一层的每一个房间中,黑客需要花费多大的难度才能窃取到等同原来金库所有现金的财富?

3.2、缺乏定期的安全体检

区块链行业，是黑客攻击的重点。对于交易所来说，会长期处于一种攻防对抗的胶着状态中。所以，针对性的、定期的攻防演练（渗透测试），对交易所来说，必不可少。

遗憾的事，大多数的交易所。好像只关注网站上线前的渗透测试，其实渗透测试是一项持续性的工作，在政府、银行、大型互联网公司中，甚至会成立专门用于渗透测试的蓝军部队。

3.3、过度依赖边界防守

传统的观点是依赖物理位置决定数据的安全性，例如网盘和U盘的区别，公有云和私有云的区别。那么，物理位置之所以能给客户带来安全感，是因为传统的安全逻辑大多都是：筑墙防守。

那么，筑墙防守就真的这么有安全感吗?

现有的数据安全手段，通常都是在服务器之前构建安全网关，例如NGFW（Next Generation Firewall)，WAF(Web Application Firewall、IPS(Intrusion Prevention System)、DBA(Database AuditSystem)。

随着云计算和移动互联网时代的到来,这一套系统的边界越来越模綢。Cisco(思科公司,最早的网络设备厂商),早在2009年就提出了数据端(IDC或公有云)"无边界网络(Borderless Network)"的概念,而NGFW、WAF、IPS这些外部网关的"筑墙防守"方式,随着边界的消失,发没有"用武之地更不用谈如何保踔数据的安全。

数据的分布式存储
造成了数据存储边界的定义困难

我们认为，要想做好区块链行业的安全，需要：

- 树立正确的安全观；
- 攻防演练不可少；
- 数据安全，要从去中心化存储入手；
- 引入真正有效的安全技术；（例如威胁情报）

四、天网项目介绍

天网Sky Net Security

面向区块链行业的整体安全解决方案

天网，是面向区块链行业的整体的安全解决方案。

从为客户做安全体检开始，采用数据DNA技术+去中心化的方式解决数据安全，再到第一个为企业和个人提供去中心化的云存储SaaS，再到基于区块链地址的威胁情报库。

天网从各个角度，为区块链行业的信息安全，保驾护航。

天网的4大内容

① 天网安全体检服务：

建立区块链行业中最专业的安全攻防实验室，为广大交易所/钱包/矿业，提供专业渗透测试服务。

② 天网盾：

面向区块链行业的敏感数据，提供有效的安全方案，实现数据防泄漏、数据防篡改、数据完整性保障，例如助记词、私钥、APIKey一类的数据。主要使用分布式存储+数据分片+零知识证明+区块链等技术；

③ 天网云存储服务：

通过天网的节点，为各个行业，提供企业级去中心化的云存储 SaaS化服务，为企业的数据保存、备份与恢复提供安全、高效、低成本的云存储服务；

④ 天网威胁情报库：

对全球的区块链地址进行为安全监测，为各种数字货币的交易行为提供安全保障，并 为各个交易所/钱包开放API；

4.1、面向区块链行业的天网安全体检

Rosen Bridge Labs实验室：天网项目将成立RB Labs安全实验室，由RBL完成天网安全体检服务。

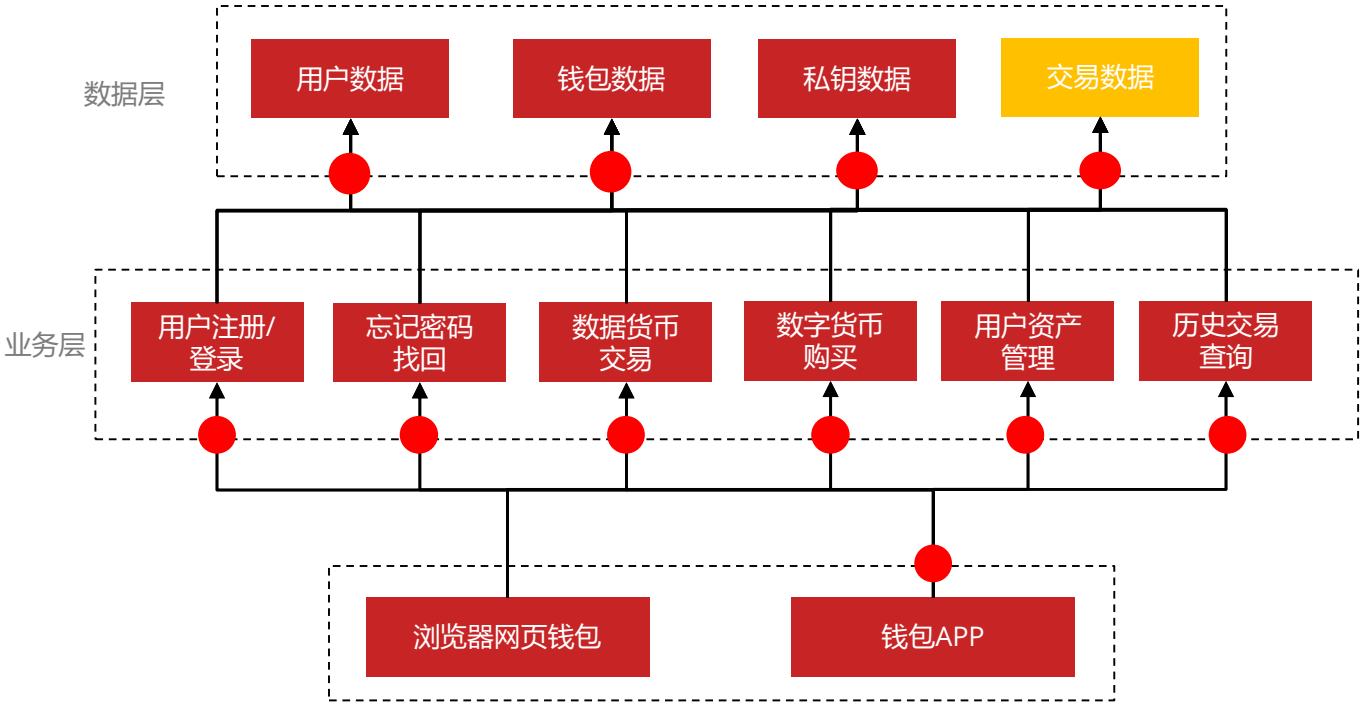
- 使命：聚焦在区块链技术的安全研究；
- 研究领域：数字资产安全、交易安全、身份安全、钱包安全、矿业安全；
- 技术方向：攻防演练技术、大数据分析技术、AI、密码学、安全算法、基于硬件的可信计算等；
- 目标：成为区块链行业第一的安全技术研究机构；

RB Labs实验室为区块链行业带来的普惠价值：安全体检（渗透测试），安全性不是某时刻的解决方案，而是需要严格评估的一个过程。安全性措施需要进行定期检查，才能发现新的威胁。渗透测试和公正的安全性分析可以使许多交易所重视他们最需要的内部安全资源。

天网提供的安全体检，包括：漏洞扫描、服务器OS测试、数据库测试、应用系统测试、网元测试。

RBL实验室、基于Pentest原则、黑盒方式、业务零影响

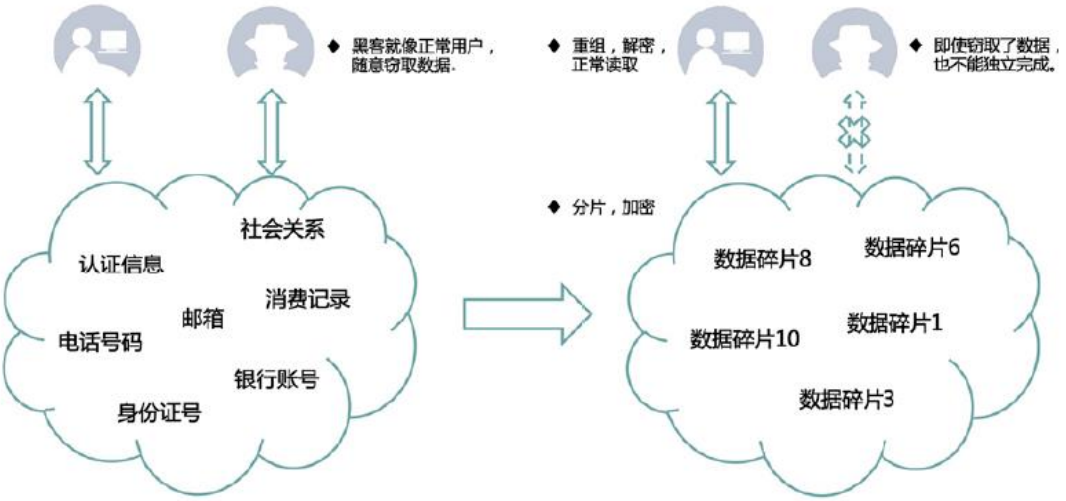
天网-安全体验服务架构图



4.2、天网盾

天网的数据防泄漏技术，是一项针对个人隐私数据和企业机密数据，进行保护的创新安全技术，我们称之为天网盾。能有效的保护个人的钱包私钥、个人的隐私文件(照片/文档)、交易所用户信息、交易记录等数据,不会被黑客窃取,从而阻止了因为数据泄漏带来的资金损失问题。

基于数据DNA技术+高强度的密码学技术+去中心化的分布式存储技术，在保障数据的宿主能够正常访问的同时，能让黑客"无数据可偷"。而天网的零知识证明技术,可以最大程度的免去了传统加密技术的"密钥保存命题"。



天网盾的架构

去中心化存储 + 密码学 + 区块链技术

一项可以覆盖个人和企业场景的安全技术
(Hard、Soft、SDK)

数据DNA

3项数据安全创新

数据
智能粉碎

零知识证明身份验证

多副本管理

有效降低存储成本

天网盾创新的数据安全方式，是改变了数据存储的方式和形态：

数据
DNA

数据分片的去中心化存储

智能粉碎

零知识证明

数据多副本

天网盾的三项核心技术（1）：

数据智能粉碎技术(Data- Intelligent- Fragmentation)

天网是通过将原始数据(个人照片、钱包私钥、账号密码、机密文件),进行基于bit位的填充、粉碎、倒倒序的处理之后,以分布式的形式,智能的存储于网络的各个节点中。在实现安全存储的过程中,还使用了数据碎片的加密处理(Encryption)、副本备份(N- Backup)、割本拷贝(N-Copy)等技术手段。

即使黑客获取了部分数据碎片(File Fragmentation)之后,甚至黑客获取了全部的数据碎片之后,都无法进行数据碎片重组,无法独立成文以达到偷窃数据的目的。

我们称这项技术为数据智能粉碎。(DIF: data-intelligent-fragmentation）。

假设我们要保护我们一张面额为100元的钞票。以前我们会用最好的保险箱来保存,再用另一个保险箱来保存第一个保险箱的钥匙,如此循环,总总会有一把钥匙多出来无法被保护,这个过程也非常繁琐。现在使用数据智能粉碎技术,我们将这一张钞票,有记忆地但无规律地撕碎成一万个碎片(甚至更多),并将这些碎片散落地存放在不同的房间中,再使用良好的门锁锁上房间的门。同时也存在独特的逆过程的应用,也就是能有效地将这些碎片重新拱凑成为一张可以使用的100元钞票。这样即使有窃贼偷到一些碎片,甚至全部碎片,也不能还原成同一张可使用的钞票。

天网盾的三项核心技术（2）：

零知识证明安全机制(Zero- Knowledge- Proof)

天网在数据碎片的重组过程,运用了零知识证明的安全机制(ZKP:Zero-Knowledge- Proof)。这项技术的基本目的是确保数据的宿主才能开启重组算法,以保障数据的主权。这项技术是天网团队自主研发的创新技术,相比传统的密钥加密技术,零知识证明的机制,可以允许宿主无需保存密钥(Key)。

这样一来,宿主可以不用再考虑密保存的问题,同时避免了"用一个保险箱锁住另一把保险箱的钥匙"的尴尬。

例如冷钱包应用中私钥(Private Key)保存困难和麻烦。继续用100元的例子,刚刚我们把钞票分成了万分有余,也能够将他重新拼凑起来。但在什么情况下计算机会执行这一项操作,让操作者者获得这100元呢?只有当我们的零知识证明技术,通过一些常规的认证,如瞳孔、指纹等,和一些非常规认证(也就是零知识证明的创新技术),承认操作发出者是钞票的宿主,才会将千万的碎片从安全房间中取出,按顺序拼接形成钞票。

天网盾的三项核心技术（3）：

多副本恢复技术(N- Recover)

虽然天网也使用网络中各个节点进行分布式存储，但天网团队自主研发、设计了另一套数据碎片副本备份和副本恢复的技术，包括副本备份(N- Backup)、副本拷贝(N-Copy)等,以确保在任何恶劣的情况下,都可以进行数据恢复(DataRecover)。我们称这项技术为多副本恢复技术(N- Recover)。

确实我们很难在碎片数量如此庞大的情况下确保每一个的安全性。还记得那张钞票的碎片吗,其中某些碎片可能会丢失,盗取甚至篡改,但是多副本恢复技术会在特定危机条件下,执行复制和拷贝流程,重新生成一张新的相同的碎片,存储在另一个随机的安全房间内,保证钞票还原逆过程的正常进行。

4.3、去中心化的云存储SaaS服务

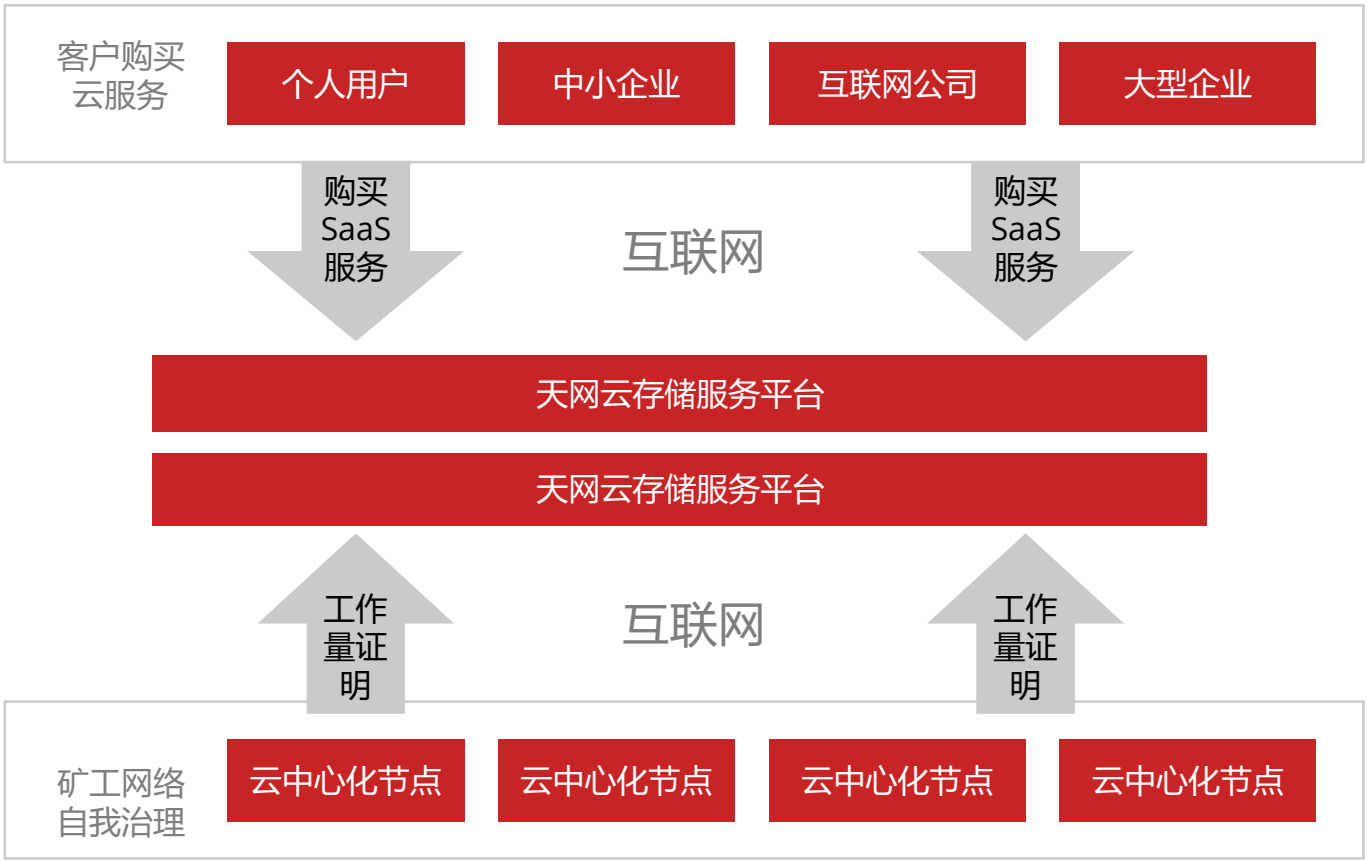
我们都知道，一个企业的数据的存储，尤其是冷数据的存储，在访问时延、备份能力、可恢复性上，都有着较高的要求。现在通行的方式，是：

1. 自建SAN和磁盘阵列服务器。但购买成本、运维成本都是难以承受的，对于有些数据生产速度快的企业，每年在数据存储方面的开销，能占到整体IT开支的20%以上；
2. 购买公有云云存储服务（例如阿里云的OSS），但这些服务的安全性堪忧，总是担心数据被黑客、甚至是对云计算运营商的不放心。

天网项目，通过节点的建立，将获得大量的存储空间。通过为各个行业，提供企业级去中心化的云存储SaaS化服务，为企业的数据保存、备份与恢复提供安全、高效、低成本的云存储服务；

- 天网的云存储服务，是基于天网盾技术，以及基于挖矿打造的天网节点，演进出来的云存储
  服务；
- 矿工网络具有自我治理和运维能力；
- 天网将通过控制平台和服务平台，将这个去中心化的存储网络，打造一个面向个人/企业的云存储SaaS化服务。

天网云中心化云存储服务



4.4、基于全球区块链地址的威胁情报库

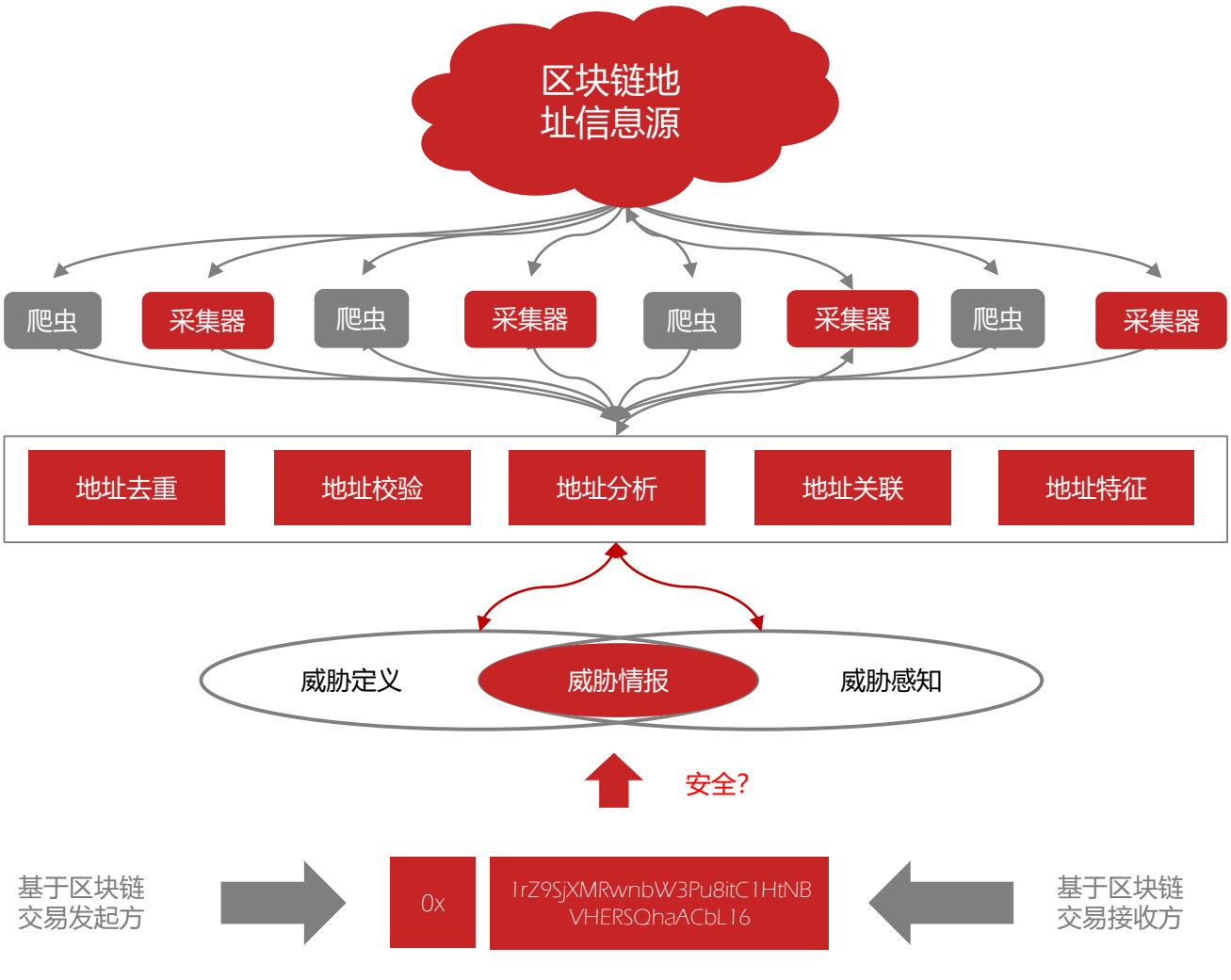
在我们的互联网世界中，有很多信息已经形成大数据库，例如购买记录、位置、社交、言论等。有一类大数据库，叫威胁情报库。威胁情报库的目的，是基于大数据技术，通过对某一类数据的判断，以辨别出访问者和被访问者，是否存在恶意访问？恶意程度多少？甚至可以根据威胁情报，预测出即将要发生的攻击。我们管这个叫安全态势感知。

用于判断威胁情报的数据有很多类型，例如IP地址、URL列表、电话号码、文件HASH...，这些数据的威胁情报帮助解决了很多传统企业的安全问题，也推动了安全技术的进步。

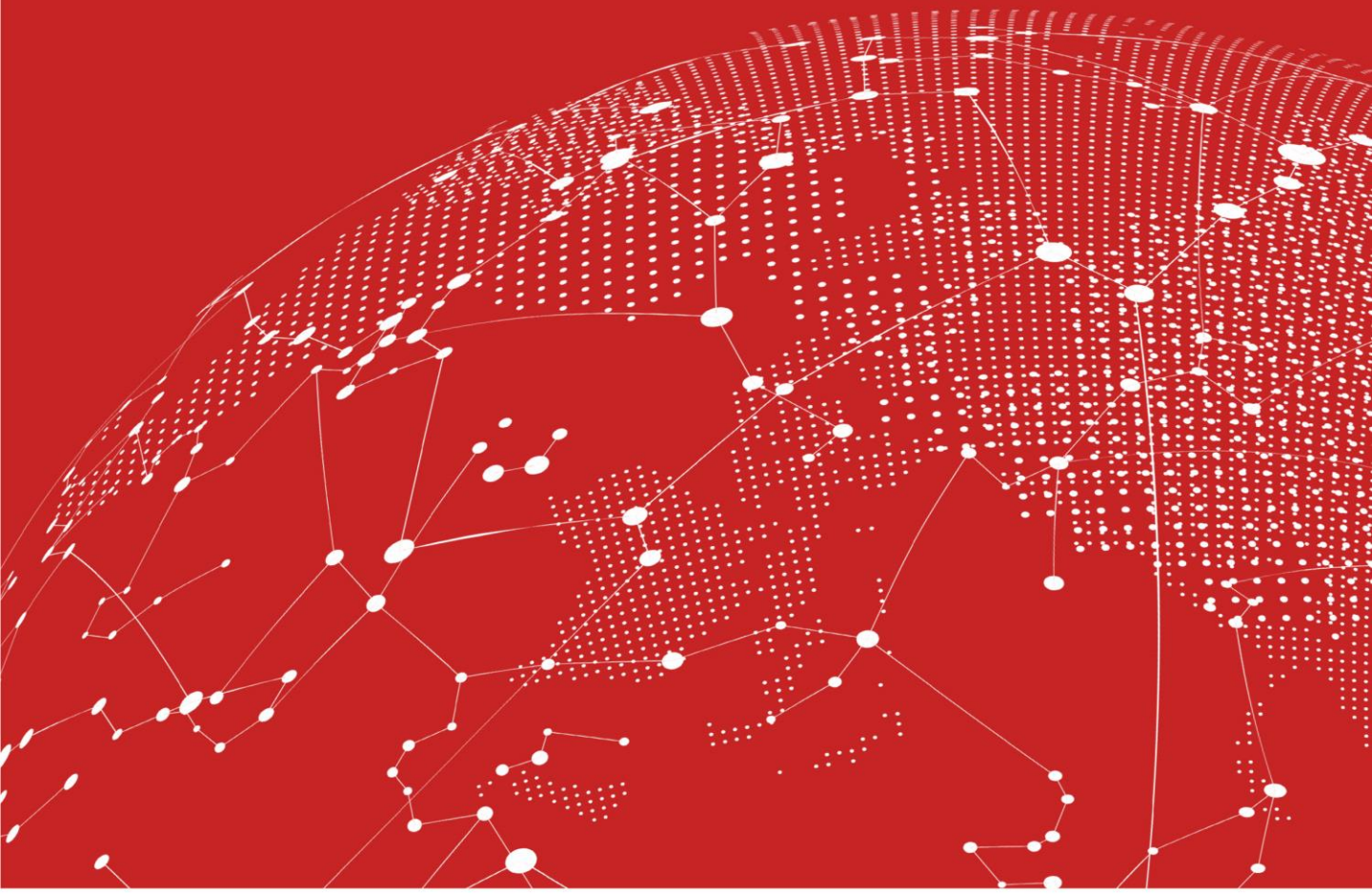
那么，针对区块链的威胁情报库是否有价值呢？

答案是肯定的。天网，对全球的区块链地址进行为安全监测，同时，将区块链地址的威胁情报库，与传统的威胁情报库（IP地址、电话号码），进行对接，逐步训练。最终为各种数字货币的交易行为提供安全保障。天网，在未来会开放改情报库与各个交易所/钱包的API，为区块链世界带来很多的安全。

基于全球区块链地址的天网威胁情报库



五、Token机制



DSCoin是由天网通过安全存储空间的工作量证明机制和权益证明机制(PoW + PoS)，发行的代币，用于奖励那些提供"共享安全存储"空间的参与者。

5.1、Token 介绍

天网通过强大的硬件部署,为互联网提供了一张安全存储网络,这张网络可以为更多的个人、企业提供廉价方便的安全存储空间。

DSCoin是由天网通过安全存储空间的工作量证明机制和权益证明机制(PoW + PoS),发行的代币，用于奖励那些提供"共享安全存储"空间的参与者。

DSCoin代币共发行1000亿个,按照一定的规则和比例分配给不同的持有人,其中一定比例的DSCoin会以怡当方式面向合适人群进行募资,用于区块链底层建设、产品模块研发、应用生态布局等。

5.2、Token 应用场景

DSCoin在实际的应用中，具有清晰的应用场景，主要为两种：

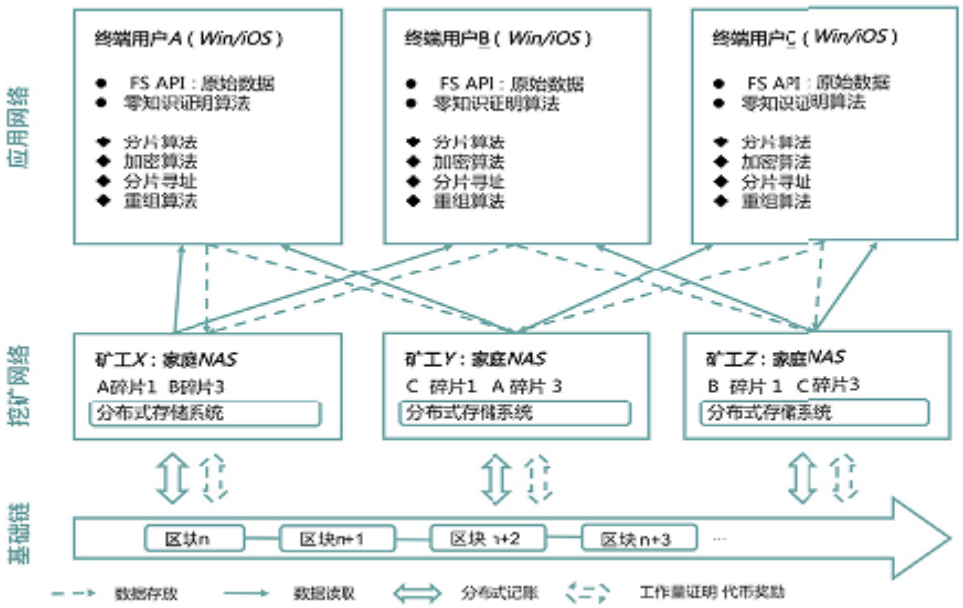
1. 个人或企业，可以通过Token去购买云存储服务；
2. 权益兑现（PoW+PoS）。例如，不同的客户，持有不同数量的Token，将获得不同等级的安全服务。

5.3、DSCoin挖矿机制介绍

DSCoin代币是基于安全存储空间的工作量证明机制和权益证明机制，天网的工作量证明更为先进。相比BTC基于Hash算力的工作量证明(该证明方法基于哈希碰撞,通过随机数遍历,得得出一定规则的HASH数值)， DSCoin的工作量证明能够为人们带来真正具有实际意义的应用效果，为社会带来巨大的价值。

1) 挖矿即利他:挖矿就是分享自己的安全存储空间(基于DIF算法),让他人可以低廉的成本使用到更多安全的存储空间。人们不用再担心自己的64 G iphone总是存不下那么多照片,也不用因此花不菲的用购买 Cloud的云存储空间。在使用天网的共享安全存储网络后,人们也不用担心个人数据泄密情况的发生

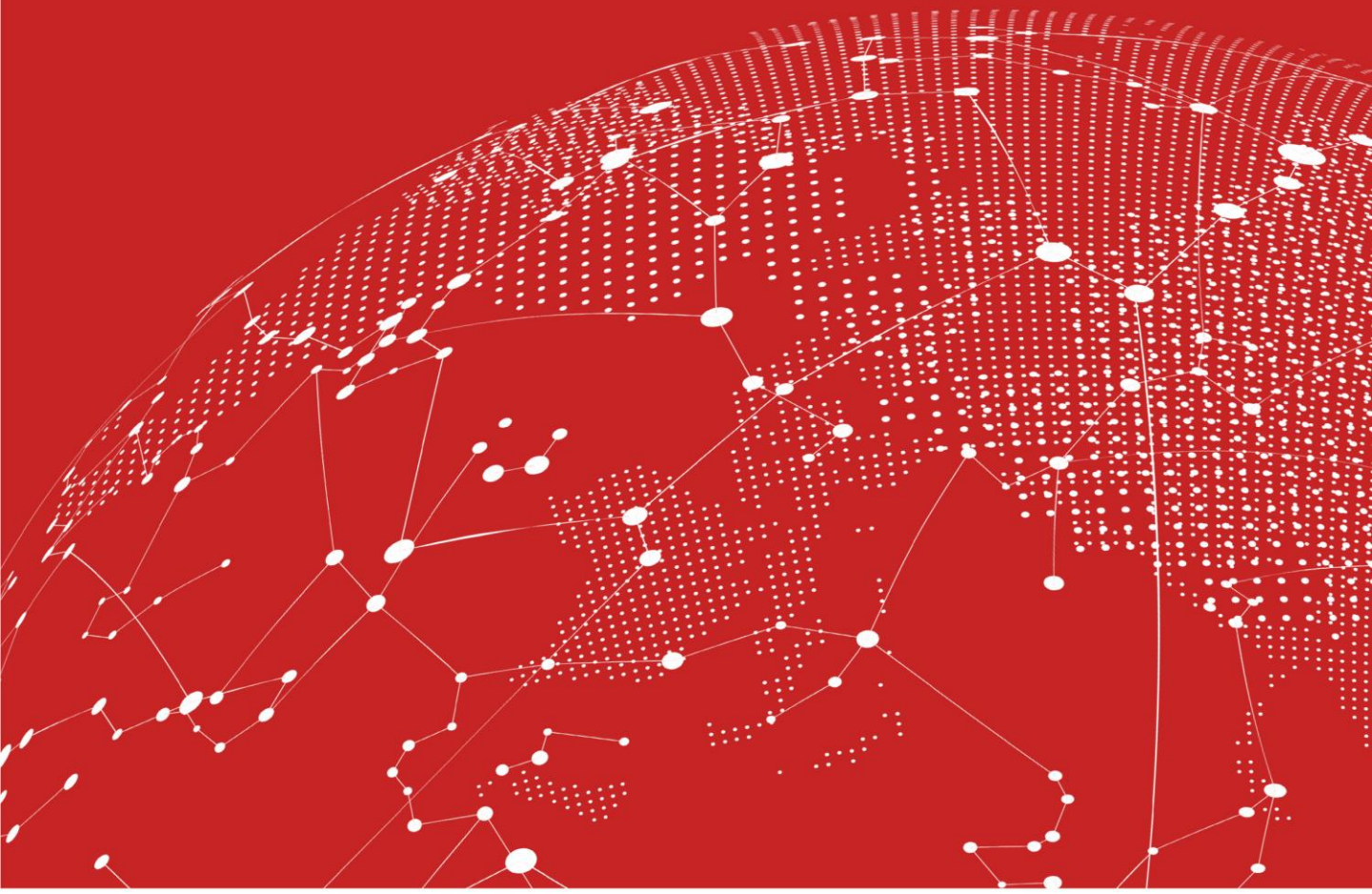
2) 更低成本,更高安全:企业利用共享安全存储网络,可以放心地存放企业的敏感数据,从此再也不用每年花费高额费用购买磁带机,去存储那些常年不用的冷数据。这使得企业在获得更高的安全级别的同时,能够降低自身的运维成本。



六、团队介绍

天网Sky Net Security

面向区块链行业的整体安全解决方案



来自华为、阿里、网秦等安全企业的一群资深从业者，

主动担负起区块链行业安全的使命，创造了天网...

吕途 - 天网创始人

信息安全行业从业16年，主要从事产品开发、产品管理和产品设计的岗位。曾供职于北京天融信、华为、山石网科、阿里巴巴。
曾参与中国最早一代多核防火墙OS的开发；
曾主导设计了华为安全产品线大多数的防火墙的规划和设计，包括目前主力产品NG-Firewall；
曾做为防火墙国标的起草者之一（GB/T 20281-2015）；
设计产品曾获得FIT大会WitAwards年度创新奖。
擅长领域有防火墙OS、分布式安全硬件、应用安全、数据安全、分布式存储等。

陈继 - 天网创始人

17年信息安全从业者
在入侵检测、安全攻防、逆向工程以及安全开发、架构和产品方面具备丰富经验，曾就职于天融信、Websense、网秦。
曾任众享比特、珊瑚灵御产品和研发联合创始人，国内早期区块链项目参与者，国内第一款非终端硬件相关EMM产品负责人，基于无边界环境下的数据安全全生命周期提出者；
具有信息安全领域 30项发明专利/4项国际专利（具体专利）；

姚钧 - 天网联合创始人

连续创业者；
从事文化传媒和证券外汇行业12年，2012年年底进入币圈，比特币早期信仰者，参与投资多种虚拟货币，斩获丰厚；
2015年开始关注区块链技术和应用，曾担任区块链创业项目顾问和CEO，具备丰富的区块链行业经验。

William Chen - 资深顾问

超过20年的海外市场经验，覆盖北美、南美、欧洲。
美国Cryptagon 数字货币基金创办人。
美国Terragon 对冲基金联合创始人。
美林投资高级副总裁， 雷曼兄弟投行高级副总裁。

元帅 - 天网联合创始人

早期的数字货币投资人；
香港点亮资本创始人，成功的投资了SNT、星云、Telegram等项目；
成功的孵化多个区块链项目；

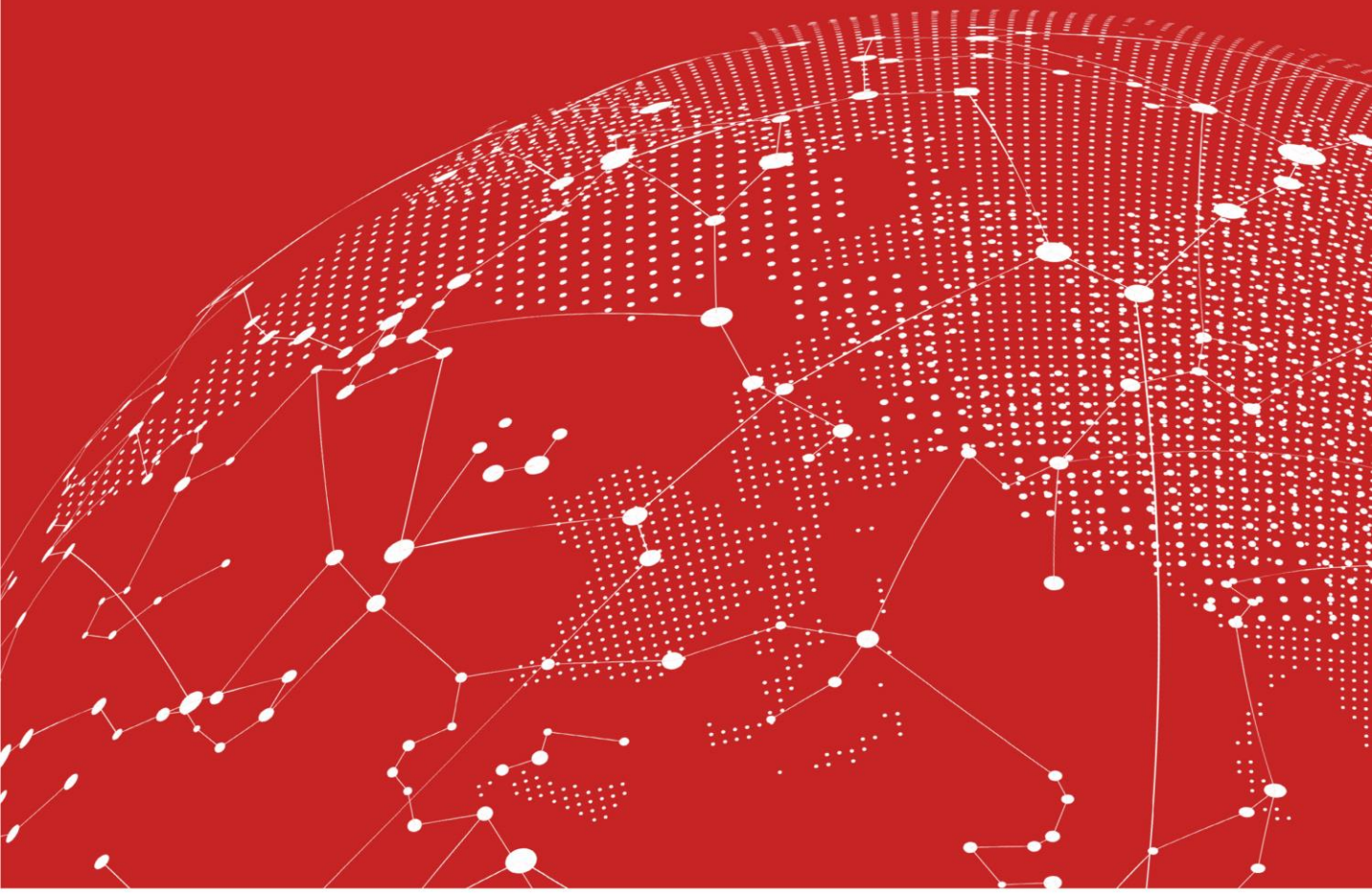
冯东渤 - 天网联合创始人

深圳麦芒营销策划公司 董事长；
资深区块链行业投资人；
掌握了多家资本机构，包括深圳前海远盛资产管理公司、深圳艾普瑞产管理公司；
深圳明日之星体育文化传播有限公司董事长；

七、专利介绍

天网Sky Net Security

面向区块链行业的整体安全解决方案



天网团队的4+27项专利

4项国外专利(专利名+专利编号)

- 《Mobile terminal and method thereof》US20160080329A1(美国)
- 《Method, apparatus and system for inspecting safety of an applicationinstallation package》US20160092190A1(美国)
- 《Security detection method, apparatus, and system for applicationinstallation package》WO2015090153A1(欧洲)
- 《Application certificate-based method for detecting security oapplication installation package, terminal, and assisting server》WO2015101149A1(欧洲)

27项国内专利(专利名+专利编号)

非授权加密和压缩文件对外发送监测系统和方法	CN105959272A
数据脱敏和反脱敏方法及相关设备	CN103778380A
基于数据比特位的安全分片重组机制	申请中
用于检测文件的完整性的系统和方法	CN103761489A
用于防止篡改数据的方法和设备	CN103971065A
用于备份和恢复数据的系统和方法	CN103619008A
用于 Android系统的安全监测系统和方法	CN103561045B
移动应用的安全性检测方法及移动终端	CN103442361B
一种利用零知知识证明的数据身伶确认方法	申请中
检测定制ROM的安全性的方法和装置	CN103246846A
应用程序关联操作的控制方法和控制装置	CN104216780A
对网络资源的访问控制方法及装置	CN104092698A
基于数字水印的数据安全管理方法、移动终端和系统	CN103841120A
移动终端和方法	CN103838989A
基站的检测方法和装置	CN104244281A
分布式环境下基于动态选举机制的共识区域方法	申请中
用于管理文件资源的系统和方法	CN103714186A
在移动终端上通过浏览器使用应用的方法和设备	CN103713808A
应用安装包的安全检测方法、装置和系统	CN103632089A
用于控制终端应用权限的方法和装置	CN103632073A
一种实现白我调整机制的数据安全动态存储机制	申请中
用于调节应用进程的方法和设备	CN103530193A
移动应用的安全性检测方法及移动终端	CN103442360A
用于检测和过滤数据报文的方法和设备	CN103414725A
用于终端权限嘗理的方法和终端	CN104573435A
数据传输处理方法及装置	CN104579831A
用于自动选择应用安装位置的方法和移动终端	CN104461655A
基于安全策醅来防止本地文件泄漏的移动终端和方法	CN104318169A
基于应用证书来检测应用安装包的安全性的方法、终端以及輔助服务器	CN103778367A
屏幕解锁方法及装置	CN104156648A

八、风险提示

天网Sky Net Security

面向区块链行业的整体安全解决方案

该文档只用于传达信息之用途,并不构成买卖天网团队股份或证券的相关意见。任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行,以上信息或分析不构成投资决策或具体建议。

1、本文档不构成任何关于证券形式的投资建议,投资意向或教唆投。本文档不组成也不理解为提供任何买卖行为,或任何邀邀请买卖任何形式证券的行为,也不是任何形式上的合约或者承诺。

2、天网团队明确表示相关意向用户明确了解天网项目的风险,投资者一旦参与投资即表示了解并接受该项目风险,并愿意个人为此承担一切相应结果或后果。

3、天网团队明确表示不承担任何参与天网项目造成的直接或间接的损失,包括:
(一)因为用户交易操作带来的经济损失。
(二)由于个人理解产生的任何错误、疏忽或者不准确信息。
(三)个人交易各类区块链资产带来的提失及由此导致的任何行为
(四)天网Token不是一种投资
(五)我们无法保证Token一定会增值,在某种情况下也有价值下降的可能。
(六)没有正确使用其Token的人有可能失去使用Token的权利,甚至可能会失去他们的Token。
(七)拥有Token不是一种所有权或控制权。拥有Token并不代表对天网团队或天网团队应用的所有权
(八)天网团队并不授予任何个人参与或控制关于天网团队及天网团队应用决策的权利

天网Sky Net Security

面向区块链行业的整体安全解决方案

【天网的使命】

为区块链的世界带来安全感；

用区块链技术推动安全行业。