用区块链应对网络安全新风险

陆宝华

雄安新区首席网络安全顾问
福州市首席网络安全专家
贵阳国家大数据靶场顾问
工控国家工程实验室专家委员

Part 1

区块链

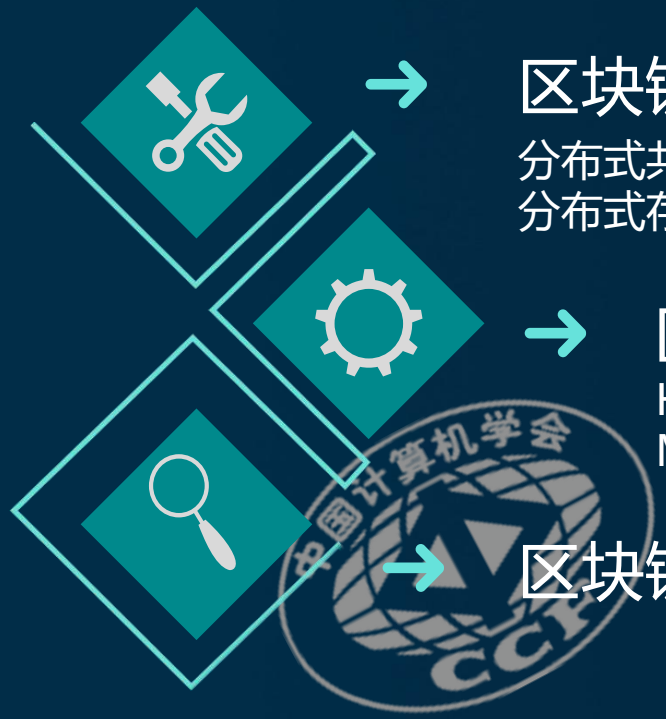
区块链的定义

区块链是

- 利用块链式数据结构来验证与存储数据、
- 利用分布式节点共识算法来生成和更新数据、
- 利用密码学的方式保证数据传输和访问的安全、
- 利用由自动化脚本代码组成的智能合约来编程和操作数据

的一种全新的分布式基础架构与计算范式。

区块链用于网络安全的原理



区块链系统天生是一个分布式系统

分布式共识
分布式存储

区块链系统使用块链式的数据存储结构

Hash Chain
Merkle Tree

区块链系统是数据和时间的绑定

数据的保真性　　数据产生的合理性　　数据的完整性

Part 2 网络安全

什么是安全？

安全是没有受到威胁的状态

威胁

- 直接的威胁和间接的威胁
- 显露的威胁和潜在的威胁
- 人为导致的威胁和自然产生的威胁

安全的两大类问题

Security

由于人对于资源的共享所导致的

人祸

Safety

由自身与自然原因所产生的

天灾

在计算机网络中，我们更关注的是人祸

Security安全的核心任务

保证正确授权操作

- ✓ 所有的操作是经过授权的；
- ✓ 所有的授权行为都是正确的；
- ✓ 正确的授权机制是有保证的。

在计算机网络中，我们保护的目标

- 数据安全
  传统数据安全：数据的机密性、完整性、可用性
  大数据安全：假数据、数据池污染
- 系统的服务功能安全
  保证系统连续性运行
- 人在网络中的行为可确认
- 我们的资源不被非授权的使用

显然用区块链很容易确认人在网上的行为

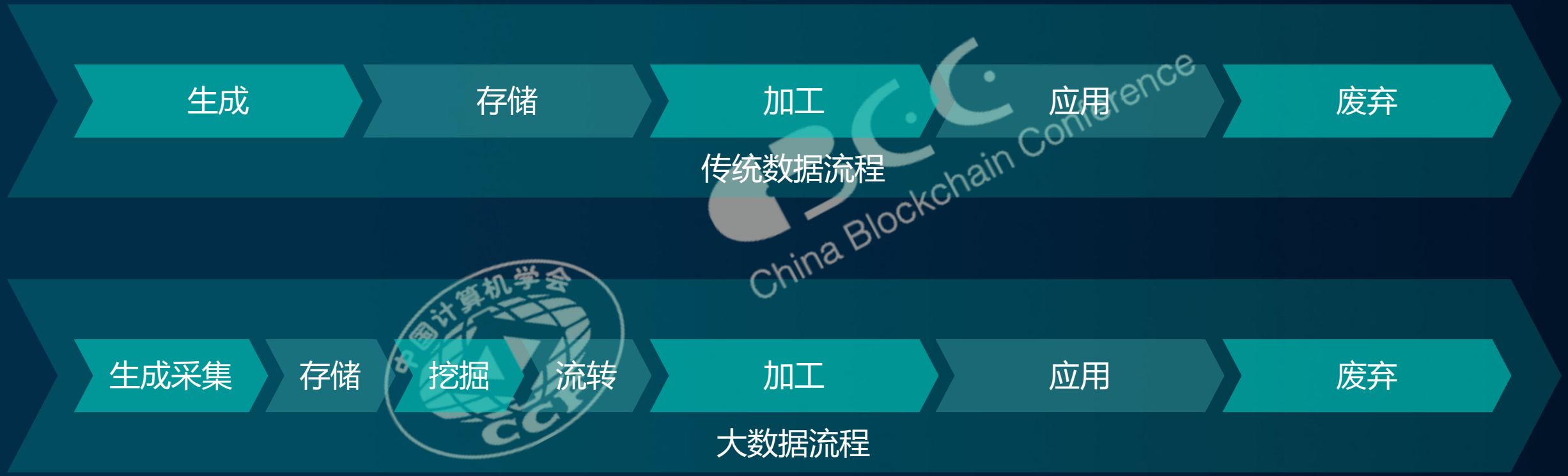
Part 3 一些新的风险

大数据面临的风险

数据与大数据

传统数据		大数据
结构化数据	数据格式	非结构化数据+结构化数据
集中存储	存储模式	分布式存储
数据库查询平台有较好的安全机制	计算平台	分布式计算处理平台几乎没有安全机制
相对简单	复杂度	由于异构性，导致复杂度增加
以服务器为主，有向云上转移的趋势有较清晰的边界	计算物理环境	云是主要的承载物理平台，但仍有利用物理服务器，边界模糊
机密性、完整性、可用性	保护目标	机密性、完整性、可用性同时要考虑对数据真实性的确认
SQL	数据库结构	SQL+NOSQL
C++为主	软件栈	Java为主
1～10台	主流规模	3～1000台，最高可支持上万台
集中存储、查询	包含的内容	存储、查询、计算、ETL、分布式应用程序协调服务

数据与大数据



可以从五个维度来分析大数据的新风险

维度一：大数据的量大 个人隐私与国家秘密泄露

维度二：大数据的分布式存储，访问控制问题

维度三：大数据的生命周期更复杂 交易

维度四：大数据在挖掘中的访问控制问题

维度五：大数据真实性问题 错、杂、乱、丢、骗

大数据的安全需求

- 所有的网络安全需求
- 数据的真实性问题
- 分布式数据库的访问控制问题
- 挖掘中的访问控制问题
- 国家秘密的泄露与个人隐私泄露问题
- 元数据与源数据的错位问题
- 全生命周期中数据的溯源问题
- 大数据平台的安全问题
- 大数据的滥用问题（越权采集，越权挖掘，越权使用等）
- 大数据交易中的安全问题
- 大数据的跟踪问题

用区块链解决数据的真实性问题

源数据就是假的

单向函数解决完整性的问题
解决不了真实性的问题

交易中造假

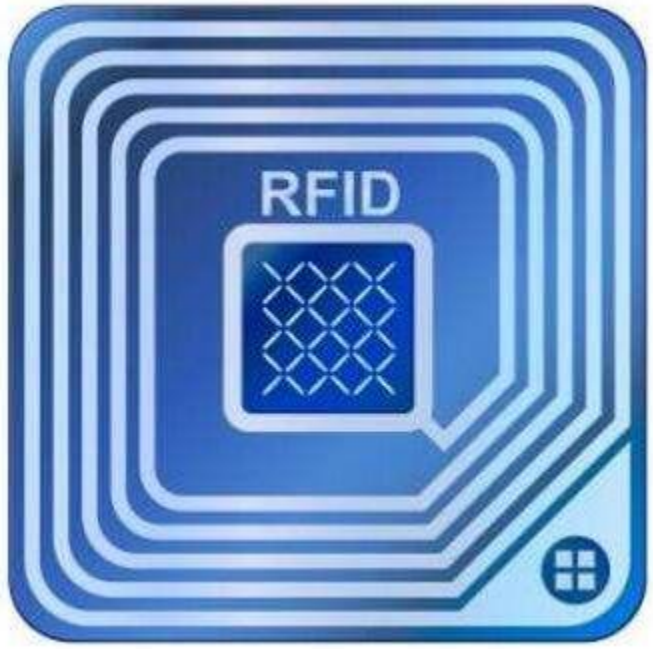
数据块	哈希值	对应校验
假数据块	假哈希值	对应校验

数据被污染

区块链是带有时间戳的哈希链

万物互联面临的风险

RFID



- RFID（Radio Frequency Identification）技术，又称无线射频识别，是一种通信技术，可通过无线电讯号识别特定目标并读写相关数据，由两个部分组成，一是无线电收/发信机，另一部分是标识码，这个标识码可以表示所定义的某个物品。目前RFID技术应用很广，如：图书馆，门禁系统，食品安全溯源等。
- RFID可分为有源和无源的，所谓有源就是自带电源，目前的应用并不普遍。而大量应用的则是无源的。无源RFID，是靠接收来自阅读器所发射的无线电波来激励的，将所收到的电波能转换为电流能，使得RFID的发信机工作，并将相关的识别码信息发送给阅读器。阅读器有近场的，需要RFID贴近时，才有效。还有远场的，不需要RFID贴近，可以在几米，甚至是几百米的距离上都可以识别。
- RFID读写器分移动式的和固定式。

RFID安全问题

可复制

- RFID是可以复制的，收发信机，很容易作，并且RFID的工作频段也是公开的，就算是不公开，也是可以检测出来的。ID码是可读的，既然读出，就可以再写出来。复制并不困难。

数据库数据可修改

- RFID本身是没有属性的，它所定义的物品，完全是人为的，并且定义后，往往会被存储到的数据库中，如果数据库的防范不严密，就可能导致所定义的数据被篡改。后果就可能会使相关物品丢失，或者带来其它错误。

可泄露

- RFID的信息既然是可读的，可复制的，那么就有可能将重要的隐私信息泄露。我们的身份证，许多银行卡，都是利用RFID技术实现的。如果这些信息被泄露，后果可想而知。

信号与数据

信号不能完全的等同于数据

- **信号本身并不表征特定的信息内容**

  虽然信号本身确实含有相应的信息，但是，它与某种媒体形式的数据还是有区别的，或者说，信号只是某种特定形式的数据也可以。

- **信号的产生来自于各类感知器件**

  感知器件是将非电量转换为电量，而这个电量就是控制信号，这个控制信号可能会送到本系统的各种IT中心进行处理，或者直接用于反馈系统的控制量。只有，在控制某个特定的执行部件时，这个信号才有其价值，否则这个价值就体现不出来了。

信号安全

数据安全

- 数据的机密性
- 数据的完整性
- 系统的可用性
- 数据的真实性判别

信号安全

- **信号的实时性要求**

  信号是有实时性要求的，这一点数据则不同，许多数据都会被人们反复使用，而控制信号则不允许。不但不能允许，而且如果被使用了，就有可能导致灾难性的事故发生。这一点我们务必要清楚。

- **信号产生的环境安全**

  产生信号的感知器件的工作环境较为复杂，大量部署在户外环境中，缺少有效的隔离手段，这就带来了两个方面的问题，一是更容易被破坏，不仅是恶意的人为，还有可能是动物；二是环境的影响，如雷电、雨水、大风等等因素，都可能导致器件的损坏。

- **元器件失效**

  所有的电子元器件，都有可能因使用的时间长而老化和失效。

卫星导航与定位

这些导航卫星信号，因为各种原因（地面的海拔高度；电波到地面时，空气湿度等因素的影响，而导致延迟及折射率的变化；电离子的影响；地球磁场的影响等），会产生误差，使得卫星给出的定位信息，与实际的经纬度之间存在误差，而这个误差，就会影响到定位和导航的精度，甚至还出现错误。

为了消除这些误差，一般都会在某一地区安装相应的差分系统，用地面的信号来校正卫星的信号导致的误差。

这就可能产生这样的问题，地面上某些恶意的人员伪造差分信号，导致所接收到的导航信号，出现更大的错误，甚至可能是相反的错误。其后果，是难以想象的。

同时，卫星的信号，还会受到某地质因素的影响，导致定位与导航信号的出现错误。

智能城市的风险

百度为您找到相关结果约9,320,000个

一个黑客的自白:你的摄像头是如何被攻击的? 搜狐科技_搜狐网
_2017年6月20日 - 这段时间看到CCTV联合国内一些安全公司做了几期智能家居摄像头安全报告,有...【独家...完整视频还原现场 哈罗回应与青桔斗殴事件 搜狐科技视界 · 昨天...
www.sohu.com/a/...
- 百度快照

美国大规模断网竟是因为国产网络摄像头? - 电子发烧友网
2016年10月24日 - (比如网络摄像头、智能开关等)后就尝试使用默认密码进行登...一般为...轻松地控制了这超过 100 万台设备,也导致了此次大规模 DDoS 攻击事件。...
www.elecfans.com/baike...
- 百度快照

盘点2016七起DDoS攻击事件_物联网,网络安全,智能..._中国安防展览网
2016年12月27日 - 恐怖电影之间的区别,2016年的DDoS攻击事件更是加深了...DDoS攻击,成为已知最大的CCTV(闭路电视摄像头)僵尸...
www.afzhan.com/news/de...
- 百度快照

...大量家庭摄像头遭入侵,你的家很可能正在被偷窥! 平台事...互金...
2017年11月18日 - 据央视新闻6月18日报道,破解智能摄像头的密码,侵入相关系统,偷看或直播智能...目前,我国的家用摄像头保有量为4000万至5000万个,其中一些存在被攻击...
https://www.wdzj.com/hjzs/ptsj...
- 百度快照

家庭隐私可能被"直播"?专家告诉你哪些是被攻击的高发地-新华网
2017年6月20日 - 目前消费者使用的智能摄像头安全状况如何,对此,贾子骁说,近年来,智能摄像头等联网设备频繁曝出存在安全漏洞和遭受网络攻击等事件。国家互联网应急中心...
www.xinhuanet.com/talk...
- 百度快照

智能摄像头存在的安全隐患及如何解决_百度经验
2016年8月29日 - 智能摄像头存在的安全隐患及如何解决,多名网友在社交平台上反映,家中自从安装智能摄像头后,个人信息、室内场景画面出现被泄露等现象。经工程师证实个...
https://jingyan.baidu.com/arti...
- 百度快照

入侵家庭摄像头案!大量家庭摄像头被偷窥_TechWeb
2017年7月14日 - 答:小蚁智能摄像机在传输过程中使用了高强度的私有动态加密系统,确保数据传输...对摄像机发起攻击,从而阻止摄像机的视频传输,导致APP无法正常观看摄像

用区块链解决的RFID风险的设想

RFID使用之初就上链

篡改数据库已经很困难了51%

假冒的可能

读卡同时读链 此RFID是否在链上？

移动互联面临的风险

信息的复制和重放攻击

- 开放的环境，就会导致信息的泄露，更给入侵者提供的方便通道。
- 有人会说，无线信道也是通过加密了的，应该是安全的。加密后是否安全，这样具体的情况具体分析。有些时候，入侵者不需要分析你传输的信息内容，只要把相关的一段信息复制下来就可以了。
- 汽车的电子钥匙，现在用的人非常多。在你开关车门的时候，电磁波也就辐射出去了，如果在附近有一个恶意的入侵者，使用相应的设备，将你这段电磁信号加以复制，然后很快的再做出一把钥匙来，在今天的计算机的时代是一点也不困难的。
- 同样的道理，对于一些控制信号，也可以这样处理，就可能会导致某些系统的灾难性的损害。

破密

对于加密系统，也是可以通过破密的办法来解密的。当然，破密是需要大量的样本的，这一点对于开放的无线信道，为破密者提供大量的样本并不是一件难事。所以千万不要认为加密就是安全了。

堵塞

无线信道，还比较容易被“堵塞”，这和利用三次握手实现DDOS攻击的虽然原理不同，但是效果是一样的。信道被阻塞后，必然会有大量的信息被丢失，也可能会造成不可挽回的损失。实现无线信道的堵塞，是很容易做的，只要在接收机附近，搞一个频率相同的干扰，如果功率够大，就会导致接收机不能正常工作。

APP漏洞

有不少的APP开发者，并不懂安全，也不懂安全开发，利用一些现成的工具或者是模板，很快就可以开发出一个应用来，其结果是，这样的APP程序存在着大量的漏洞，这些漏洞就很容易感染各种恶意代码或者被入侵者利用。

APP恶意后门

一些APP为了获取你的个人信息，在相应的APP软件中，隐藏了恶意代码，将你的位置信息、通话记录、电话本、短信、消费行为等等属于个人隐私范畴的信息记录下来，并发送到特定的服务器，接下来的后果是可想而知的。

APP越界获取个人信息

所谓越界是指APP在自身功能不必要的情况下，获取用户个人隐私权限的行为。

2017年7月20日，根据腾讯联合Internet数据中心发布《网络隐私安全及网络欺诈行为报告》中指出：96.6%的Android APP和 69.3%的ios APP 要求获取用户信息，而其中25.3%的Android APP存在越界。

移动接入网关的安全

在移动办公中，还要有一个网关负责汇聚移动智能终端的联结，同时再接入到相关的系统中。这个网关还要负责管理所有接入的移动智能终端。所以如果这个网关不安全，也会导致整个系统的不安全。

对于一些实时 性要求并不太强的应用，我们可以利用区块链的时间戳和块链防范重放攻击
在收到重放信号时，同时读链，如果链上已有相应的记录，就可以确认这是重放攻击，就可以将这个信号丢弃

区块链应对网络安全

区块链如何保护数据免受篡改和破坏?

使黑客的工作复杂化

- 为了篡改或破坏一个区块链，黑客需要获取存储在不同位置的大部分用户计算机上的所有信息。
- 黑客几乎不可能摧毁整个网络，网络上将有部分节点保持记录和验证数据。
- 拥有许多节点的大型区块链网络受到黑客攻击的风险较低，因为渗透这种网络所需的复杂性大大增加。

区块链如何抵抗DDoS攻击？

去中心化

- 基于区块链的去中心化系统结构能够将系统数据分布存储于多台设备，不存在可攻击的系统中心节点。
- 区块链的每个节点都具备完整数据，并且能够对其他节点的数据进行有效性验证。即使某个节点被攻破，整个系统也不会完全瘫痪。
- 黑客发现识别和利用单个漏洞点的难度更大。

区块链实现联网设备的权限与通信管理

- 去中心化的物联网设备管理，消除中心节点的安全风险。
- 区块链上记录设备间的通信、控制指令以及权限情况。
- 设备的安全性和数据的机密性、完整性、可用性得到保障。
- 保证设备运行记录真实有效，完整可靠，可追溯。

区块链实现系统程序有效性验证

区块链白名单

- 特洛伊木马、病毒和蠕虫等被伪装成合法的应用程序。
- 利用区块链，指定更新和下载的排他哈希。容易将预期的系统程序的哈希与开发人员的哈希进行比较。
- 极大增加了通过伪装好的病毒感染系统的难度。

有什么应用?

无密码系统

区块链创业公司REMME

通过创建一个没有任何密码的唯一身份验证系统来解决系统底层的密码安全问题。

- 用分配给用户信任设备的SSL/TLS证书完全替换因特网上的密码。
- 包含关于这些证书的信息的哈希在一个自定义块链上生成和记录。
- 利用区块链的分布式和不变性保证了整个网络功能不依赖于单个实体和防篡改。

实时监测和减轻网络攻击

Guardtime公司

利用区块链技术创建了一个无密钥的签名基础设施（KSI）。

- 用非对称加密和中央认证机构（CA）共同维护的公共密钥，来替代传统的公共密钥基础设施（PKI）

保障私有数据分发及认证安全

安全公司Xage Security

在2017年底宣布，他们的防篡改区块链技术平台可以保障整个网络内设备的私有数据分发及认证安全。

确保数据完整性

IBM在其Watson IoT平台中允许用户在私有区块链网络中管理IoT数据，已经整合进了他们Big Blue的云服务中。

爱立信公司的区块链数据完整性服务提供了全面的审计、兼容和可信赖数据服务。

构建分布式DNS

- Nebulis是一个基于分布式DNS概念所实现的项目，能够应付各种情况下的大流量访问请求
- Nebulis使用了以太坊区块链和IPFS文件系统来注册和解析域名，在区块链技术的帮助下，Nebulis可以构建一种更加安全且受信任的DNS基础设施

抵御DDoS攻击

- 区块链初创公司Gladius声称他们的去中心化记账系统可以帮助用户抵御流量超过100Gbps的DDoS攻击。
- 当网站遭受DDoS攻击时，网站可以利用这些出租带宽来缓解DDoS攻击。

别人正在做什么？

美国

- 美能源部授予Xage Security公司一笔款项，将论证区块链技术如何防护电力网络中部署的系统和设备，以期达到保护美国电网的目的。
- 美国国防部高级研究计划局（DARPA)研究利用区块链技术创建一个安全的消息传输与交易平台，使任何人在任何地方都能够安全的发送信息。
- 美国海军已经和印第安纳州技术和制造公司（ITAMCO）达成了研究和开发合作关系，希望获取最先进的区块链技术，开发能够用于召回大型数据集合的创新协议。
- ITAMCO推出了一个区块链服务平台SIMBA Chain，允许美国军方使用区块链技术来追踪安全信息。

俄罗斯

- 俄罗斯联邦国防部正在ERA技术园区建立实验室，开发区块链技术，并应用于加强网络安全和打击针对关键信息基础设施的网络攻击。专家认为，区块链将帮助军队追踪黑客攻击的来源，并提高其数据库的安全性。

提高防范意识，强化责任担当，保证网络安全

谢谢俯听