《隐私保护周三见》精彩50问 | 交流群互动合集

原创 小助手 微众银行区块链 5月6日

来自专辑

WeDPR隐私保护周三见

公众号对话框回复【**隐私保护**】下载白皮书

2020年3月4日，《隐私保护周三见》正式与大家见面。栏目以系列论题和各位专家一起探寻隐私保护的发展之道，每一个论题，交流群里的伙伴或积极参与讨论，或对分享内容不吝指正，不断助力论题拓宽研究深度，也让我们获益匪浅。

本文将前9论交流群中的精彩碰撞进行整理汇编，以飨读者。欢迎更多伙伴加入，在每周三晚的8点，和我们一起共话隐私保护。

进群方式：公众号对话框回复【**小助手**】

点击图片可跳转阅读文章（下同）

第1论　隐私和效用不可兼得？隐私保护开辟商业新境地

1

@萧

现在有没有已经落地的技术手段，能够保证已经获得用户授权的企业（或者公司）不将用户数据提供给未知的第三方呢?

@严强

取决具体的应用场景，例如，在数字身份领域，WeIdentity就是一个可选的方案。

WeIdentity开源代码仓库地址：
https://github.com/WeBankFinTech/WeIdentity

2

@KHJ

我理解WeIdentity解决了隐私保护的第二层预期效果，最小授权这一块是如何体现的?

@严强

WeIdentity已经集成了WeDPR中的选择性披露方案，目前可以实现按照证书中的各个字段进行最小化披露。

3

@康仔不在服务区

这个是个好问题啊，拿到数据结果的主体如何让他不去传播，深入到第三层呢？这个除了立法保护，技术上的手段现在有吗?

@芒果

1）数据即资产，用户的数据中蕴藏着巨大的价值，数据被使用过程中产生的经济利益，将

直接回馈给用户本人；

2）数据上链后，任何数据使用的请求，都必须通过你本人的授权才能实现，确保个人拥有数据所有权，不必担心数据被盗用而不知情的状况了；

3）基于多维度的数据，你可以构建可信的数字身份，在与人协作时、寻找资源时，大大降低别人信任、了解你的成本，提升了“连接”的效率。

@严强

企业内部，可以建立起有效的数据追踪系统，对进入自身系统的所有用户数据进行贴标签，实时跟踪在整体系统中的流转。

4

@萧

但是企业内部已经获得的数据也可以认为是商业机密的一部分。如果，在企业内部进行数据追踪，但是运转和监督的主体还是企业内部人员，一旦出现内部人员脱库删库等行为，外部也难以知晓。会不会出现这样的现象?

@严强

确实会有这种情况出现，这里反映了另外一个问题，如何预防内部员工越权操作，所以内部员工也要实现，最小化授权和其他合理的内控措施，同时做好数据备份，以防万一。

5

@康仔不在服务区

或者说这个公司主体就是作恶主体，他完全可以把信息转手给联盟之外的单位攫取更大的利益，这个如何不太好阻止吧?

@严强

所以这里的关键点是，数据的控制权需要掌握在用户手中，而不是代理给平台，这是WeDPR方案设计基本原则之一。相应地，在WeDPR白皮书中，我们也讨论了隐私保护和用户体验之间的平衡，在方案设计上会有一定的取舍。

6

@ kentzhang

数据出去之后怎么防复制是个世界级难题呀，不知道各位专家遇到什么有效的方法。

@严强

学术界比较常见的方案是加数字水印，但实际使用中，尤其是对于小数据，效果比较有限，主要用于检测，不能防复制。还有就是经典DRM的方案，数据在存储介质中一直保持密文，只有在特定授权的软硬件环境中才能被解密访问。

第2论　隐私合规风险知几何？数据合规商用需过九重关

7

@Shuanghong He

请教下，数据歧视是指?

@严强

一般可以解释为，因为数据的内容（例如性别，宗教等）自动化决策系统做出对个人不公正的判断。

8

@萧

现有手机APP很多情况是，如果用户不提供给APP服务运营商足够的权限或者不同意条款，那么就不能够使用这些APP，请问这种情况是否符合合规条件呢?

@严强

按照新版《信息安全技术 个人信息安全规范》，如果App不能说明申请这些权限和提供服

务的必然关联性，这是不合规的。可以参考“多项业务功能的自主选择”的条款，目前不鼓励捆绑式的数据授权。

9

@little.H

现有隐私保护法规对于非商业行为有哪些合规需求?

@严强

一般隐私合规约束的对象都是商业活动。对于研究性和公众利益相关的活动，都有对应的豁免条款，但通常也规定要对隐私数据进行必要的技术处理（例如，使用差分隐私等数据脱敏技术）。

第3论　密码学技术何以为信？深究背后的计算困难性理论

10

@ SukiW

我们现在业务跑在一个系统上，使用的是现在安全的密钥长度进行加密的。如果到达时限，业务的数据就不安全了对吗？应该怎么操作保证业务仍然是安全的呢?

@李昊轩

最简单最直观的方式是在达到时效前，用更长的密钥对其进行加密，对整个系统进行更新。如果之前加密的数据泄露过，则需要根据业务本身的安全性，对敏感数据及时进行处理，避免外漏的密文数据被破译造成的影响。

11

@王卯宁

同态加密技术目前在区块链里面有没有应用？有没有什么这方面的案例或者平台可供参考？

@李昊轩

同态加密技术可以解决区块链上密文运算的问题。WeDPR的场景化隐私保护解决方案也用到了同态加密的性质。

12

@光路

常见区块链目前使用的安全参数是多少呢？如果到达时间后会怎么样呢？区块链是否还安全呢？

@李昊轩

大多数区块链使用的密钥长度是椭圆曲线算法的256位。我们上面提到，任何密码算法的安全性都是有时效的，那么在区块链中，当系统到达一定年限时，可以针对整个系统进行算法升级，从而保障参与用户数据的安全性，因此区块链系统只要大部分节点是诚实的，整个系统仍然是安全的。

13

@王卯宁

只用密码学，不用区块链，可不可以实现隐匿支付等等一些功能？

@李昊轩

隐匿支付是一种保护支付参与方身份信息、交易金额、明细等的支付方式。WeDPR隐私保护针对场景化进行设计，一些场景可以使用区块链实现，因此WeDPR可以保护区块链中的隐私痛点。同时隐私保护需求多面向分布式协作多方参与的场景，区块链场景作为比较典型的多方协作模式，与隐私保护有1+1>2的效果。

@王卯宁

没有区块链的时候，密码学领域就在研究MPC、zeroknowledge、FHE这些了，不过现在

有了区块链，大家更多的关注了……

@ kentzhang

密码学促进了区块链的应用范围，同时还可以这么理解，区块链使加密后的信息得以可信分享和交换，不会丢、不会错、不能篡改，大家确认拿到的都是同一串密文信息，同时又因为有密码学保护，隐私不会泄露。

第4论 密码学技术如何选型？初探理论能力边界的安全模型

14

@Suki

UC模型的密码学协议感觉好神奇，有什么具体的实例吗?

@李昊轩

密码协议中，交互步骤一多，UC就很难证明交互过程中产生的副作用（潜在信息泄露）不会导致任何安全性问题，当前大多数密码协议都不属于UC模型。

具体的实现可以参考下这些论文：

- 《On the Universally Composable Security of OpenStack》
- 《Universally Composable Security: A Tutorial》

15

@Little.H

量子计算也是现在常常讨论的热点，抗量子计算的安全模型，应该被归类到以上三种分类中的哪一类?

@李昊轩

量子计算本质上也是一种计算模型，抗量子计算不一定可以抵抗所有计算，因此可以归结于计算资源类模型。

16

@文帅

如果恶意模型，经济上并不带来很多成本，为何不直接使用恶意模型，降低诚实要求不更好？除非，恶意模型一定大幅提升经济成本，这会是必然的吗?

@李昊轩

恶意模型的特点在于“防止”，半诚实模型的特点则在于法律介入之后的“发现”。和半诚实模型相比，恶意模型往往需要引入更多的交互，或更多零知识证明来保证，因此不可避免会提升成本、降低效率。

在一般业务场景下，如果不需要更高强度的安全假设，推荐选择效率更高、成本更低的半诚实模型。但对于法律追责成本很高，或效率成本提高有限的场景下，恶意模型可能是更好的选择。WeDPR投票核心协议就是在恶意模型下构建的。

17

@ wheat

安全模型比较深奥，作为普通开发者，在使用到密码学相关算法的时候，应该要关注什么？注意点有哪些呢?

@李昊轩

作为普通开发者，在设计隐私保护业务场景时，应当结合自身业务的需求，考虑业务参与方的动机，业务流程、业务数据的有效期等，选择适合业务落地的安全协议，理解对应的模型，保证业务实施的长治久安。

18

@wheat

一些场景下，比如金融场景，对于安全防护的时效要求特别长，十年以上甚至更长。这种情况下，又该如何抉择设计上的取舍呢?

@李昊轩

对于长时间需要保证安全的业务，可以在到达有效期之前对系统进行更新，保证安全性的前提下，尽可能提高系统的效率。

19

@wency

我在有的地方看到涉及到黑名单系统其实并不需要隐私计算，因为只要给出一个yes or no的答案，有的地方又要强调需要隐私计算保证信息不泄露，这个应该怎么看呀?

@李昊轩

对于涉及到隐私数据的系统，需要整体考虑系统的安全性哈，避免出现系统之间相互影响从而出现的数据泄露。

第5论 密码学技术如何选型？再探工程能力边界的安全模型

20

@邱震尧

请问在物联网设备认证等等弱物理保护且没有TEE的场景中，有没有白盒公钥密码的成熟工程实现方案？比如白盒RSA、白盒签名。

@李昊轩

白盒模型目前在公钥密码学上的成熟方案较少，市面上目前有一些对称加密的白盒方案，但是由于没有公布太多技术细节，不太好评价。

21

@SukiW

白盒密码的密钥在哪，如何做到细节都公开，密钥不泄露？

@李昊轩

白盒密码的密钥混淆在了整个加密过程中，因此攻击者无法通过观测中间过程得到密钥。类似于一个表的形式，将密钥映射、混淆到实现的各个部分，可以参考论文《A Tutorial on White-box AES》。

22

@刘雪峰@西电:

Oblivious RAM适合工程上白盒模型不？

@李昊轩

Oblivious RAM可以作为密码方案白盒实现的思路，但目前看来效率成本较高。

@严强

Oblivious RAM的主要设计目标是隐藏内存的访问模式，但白盒安全模型下，还有很多其他信息泄露的方式，还需要其他组件，一同构造安全的工程实现，目前来看还是很有挑战的。

23

@刘雪峰@西电

白盒模型是不是安全需求更高的一些应用？需要多种思路结合起来共同解决？目前，用户通常接触到的场景，有白盒安全的例子吗？

@严强

白盒模型面临的部署环境都比较不可控，例如，物联网应用等，需要在公共环境中部署，但同时又很难做好物理防护的场景。随着5G等技术普及，以及人们对隐私保护的日渐重

视，将来这些场景一定会越来越多。

24

@唐炜

低成本的白盒方案如果出现，是不是会大量使用，成为标准呢?

@李昊轩

如果成本较低、方案足够成熟，并且算法理论安全性能够经得过行业检测的话，成为标准的概率是很大的。还有一点是，白盒模型更适用于部署环境比较不可控的公开环境，在安全受控的环境下，选择黑盒或灰盒模型这些效率较高的模型还是更好一些的。

@唐炜

白盒要求太高，感觉更低成本的灰盒方案，应该是一些大场景的选择。

@严强

白盒密码算法技术，对标的是可信硬件模块，如Intel SGX，如果能做出实用的产品，意义重大。

@刘雪峰@西电

个人感觉，以物联网为例，设备资源有限所以难防控，因为难防控去执行一系列复杂的操作来实现白盒安全，看起来是矛盾点。

@严强

确实如此，这一点和AI发展依赖硬件计算能力的发展很像。也许有一天，硬件技术发展到足以支持白盒密码技术，那矛盾点也就消解了。

@kentzhang

物联网暴露在外的设备，大概率是低成本弱信息价值的，主要是防止大规模被俘虏，或许工程上可以采用一些低成本的策略，如数据交叉验证、异常检测、单向隔离、黑白名单之类的方式应对。白盒理论上是有意义，实操可能要看成本。

25

@wheat

我们平时使用的密码学库，比如openssl，应该都是黑盒模型的实现吧？是不是意味着如果能够进入到加密宿主机，破解概率很高？

@李昊轩

攻击这些模型是一个成本和安全的考量。以SSL握手为例，想要通过统计学方法分析宿主机的物理信息，从而得到对应的密钥信息，成本是比较高的。当然，如果是在数据极其珍贵的场景，更应该选择攻破宿主机的难度。这是矛与盾的较量，哈哈~

26

@little.H

侧信道攻击和社会工程学有什么区别？

@李昊轩

社会工程学更多是考虑从人的角度，如胁迫、欺诈等方式获取信息，侧信道攻击则是从算法执行过程的物理信息泄露获取信息，两者获取信息的根源不同。

第6论 密码学技术如何选型？终探量子计算通信的安全模型

27

@wency

都说量子计算机是区块链的末日，抗量子签名技术和普通的签名技术到底差别在哪里啊？

@严强

抗量子的签名技术对于工程接入实际上区别不大。关键区别在于，一旦量子计算机现世，不抗量子的签名，很有可能会被破解，由此攻击者可以获得签名私钥，破坏了数字签名的唯一性，可任意仿冒签名。

28

@Anonym白熊

量子计算是如何跟区块链联系起来的呢?

@严强

密码学是区块链中的核心技术之一，实际上区块链很多特有的特性，不可篡改、数据隐私等，都与所使用的密码学技术的有效性密切相关，而这些都会受到量子计算和量子通信技术的影响。

29

@邱震尧

请问抗量子密码算法目前有选型建议吗?

@严强

目前最流行的是基于格密码系统的系列算法，常见的有基于NTRU和LWE困难问题的构造示例。具体选型可以参考NIST标准化候选名单中的方案列表。

公众号对话框回复【NIST】下载NIST Workshop PPT

30

@郭锐

请问现阶段抗量子加密是否都是基于格的？以后是否会有新的代数结构或者新的方法能够抗量子呢?

@严强

格只是其中之一，有兴趣可以看一下，我上面分享的NIST Workshop的PPT，里面基本上对所有类型的算法构造都列举和测试。但就目前来看，格密码是最看好的一类构造方式。

除了安全性之外，计算性能、同等安全强度下的密钥大小、密文大小等也是重要的考量因

素。

31

@刘雪峰@西电

量子计算看起来对应升级底层密码工具。量子通信这块，我理出来的逻辑是增加了可信信道这一选择（友好的角度），那通信这块有没有对经典密码技术提出威胁挑战?

@严强

好问题，目前量子计算对经典密码技术影响较大，量子通信的直接影响还不明确。

32

@唐炜

是否现在的区块链技术体系准备好算法替换，将来仍然可以保障整个区块链技术体系的延续?

@严强

可以这么理解。最基本的做法，可以以系统升级的方式，替换原先的经典密码学算法组件，从而保障未来区块链系统的有效运行。但需要注意，敏感的隐私数据不建议直接上链，一旦量子计算实用化，就可能直接导致历史数据的隐私泄露。

33

@刘雪峰@西电

有些信息必须上链，比如类似zcash的隐私交易账单，只上数据指纹，极大程度降低区块链的机能，这块怎么考虑？换个角度说，上数据hash值，链的数据之间关联性也消失了，后续使用价值也降低了。

@李昊轩

区块链上传数据指纹作为存证媒介，在业务实施中满足后续的审计和核查都是比较实用的功能。不过正如您所说的，一些场景下机密数据是一定要上链的，如果一些数据使用了不能抗量子计算的密码算法进行加密，并上传到区块链上，那么量子计算模型一旦有了突破，这部分数据也就存在泄漏风险了。

@kentzhang

这个问题我从工程层面试着回答下。其实很多数据在业务逻辑上是有有效期的，隐私算法可以合理抵抗商业周期里的泄露问题。长远嘛，发出去的数据是泼出去的水，除非原子级的阅后即焚。

@wheat

一方面通过抗量子算法，另一方面应该是要对上链数据做保密期限预估，现阶段工程实现受限的情况下，也只能权衡了吧。

@kentzhang

在Weldentity方案里，用户的个人数据还真是不上链也能做到可信认证和交换的，关键是围绕着区块链做一套通用友好又逻辑自洽的交互协议。

隐私算法其实就工作在链外了，针对个人数据，结合链上公证锚定，实现零知识证明和选择性披露，这是DID规范的魅力。

第7论　密码密钥傻傻分不清？认识密码学中的最高机密

@芬嘟嘟

隐私数据的自主权与数据服务的完备性上，CA是怎么提供私钥服务的?

@严强

这里有两种情况：

1）纯软件实现的CA是不应该提供私钥服务的，只对公钥和身份进行绑定的认证；

2）有硬件密钥管理设备的情况下，私钥本身是存在在硬件中的，除了制造商，理论上没有其他人可以获知。

35

@願

有探索过区块链应用于零信任网络架构的方案吗?

@严强

这个问题还是有一定挑战的，Google的BeyondCorp在工业上实现零信任网络架构整体解决方案，但没有基于区块链。如果专注于零信任网络架构中的网络实体分布式身份问题，可以参照基于区块链的WeIdentity实现。

36

@杨高峰

白盒密码使用根据根密钥对一般密钥进行加密,我觉得有用,但是好像不太流行,为什么?

@严强

白盒密码针对的部署环境是公开的，不受控，可能充满恶意的环境，现实业务大部分部署环境都没有这么恶意。为了应对恶意环境，作为设计取舍，白盒密码算法的效率普遍会低很多，而且目前白盒密码的发展没有黑盒密码成熟，潜在风险比较大。

37

@芬嘟嘟

经常看到不少学术论文中，系统初始化会有很多安全假定，也很少有关于用户能否使用密钥的讨论，对于这些学术方案，如何评价其实用性呢?

@严强

这个问题很有深度，实用性确实是理论方案向产业系统转化的一大难题，如果系统初始化安全假定过多，实际的应用场景，肯定会因此受限。用户方面的学习使用成本也是一大挑战之一。但一般而言，论文会有自己的目标场景，在目标场景中，好的方案还是可以用起来的。

38

@Hope

请问有考虑使用一些安全性比较高的leakage resilient password systems来保护用户口令输入吗？我觉得，生物识别用户认证，也有其自身的安全问题和现实问题，很难完全替代password based user authentication。

@严强

好想法，有一些在移动平台上还不错的学术方案，可以试一下。基于用户口令（密码）的方案，历史悠久，有其内在原因，总体还是一种比较实用的用户认证方式。当然和其他认证途径结合使用，效果更佳。

39

@刘雪峰@西电

工业中，如何看待人脸识别的访问控制策略？生物特征的唯一性，在学术角度上，担心撞库攻击、第三方泄露等等，包括现在拍照的不可预见性等等，工业上会不会有类似的困扰？

@李昊轩

目前人脸识别技术还是达到一定工业程度可用的，不过目前在活体检测，不同人种之间的识别还是有一些难点需要解决。人脸识别目前活体检测会需要收集很多数据和特征，不过针对于活体检测的攻击也有，但是成本都不低，也需要大批量的数据。所以人脸特征作为一些不需要特别敏感的方案的密钥有一定可行性。

@wheat

生物特征只能作为部分输入吧，唯一性和随机生成的密钥差别太大了，差好多个量级。

@刘雪峰@西电

这个唯一性，指的是在A服务端，和在B服务端的特征模板是类似的，若A端泄露了特征，用户不能像修改口令那样修改生物特征。

@wheat

对，而且这种问题发生的概率，比起两个32字节的密钥，那是大太多了。目前人脸识别的特征维度数量还是无法跟这个数相比的。

第8论 密钥繁多难记难管理？认识高效密钥管理体系

40

@唐炜

内部人员作案如何防范呢?

@严强

防范内部人员作案一般有两个方向的思路，一个是限制密钥的访问，减少能够接触到高等级密钥的人员，另一个是建立有效的审计机制，严厉追究滥用密钥人员的责任。

41

@幸

在密钥的保管和分发过程中，怎样结合具体场景在效率和安全性中达到一个平衡呢？因为加密算法越复杂，其安全性可能更高，但同时也增加了花销。

@严强

通常对于“密钥的保管和分发”，加密算法的计算复杂性不是瓶颈，因为一般与密钥相关的操作，都是一次性的初始化操作，初始化好了，之后就没有太大的代价了。反倒是其他因素（操作人员）带来的风险更大。

42

@刘雪峰@西电

如何衡量软件和硬件保护密钥？对用户来说，哪一种更友好？密钥托管这块有什么见解分享？

@严强

低安全性要求：尽量不上硬件。

高安全性要求：软硬件结合好。

43

@SukiW

如果允许一定的可信初始化，或者引入可信中间人，密钥的协商过程是不是可以大幅简化？

@严强

如果有受监管的、信誉高的中间方来提供服务，是可以很大程度上提升密钥协商效率的，比较典型的方案有代理重加密的方案，中间方可以直接分发密钥，效率会高不少。但同时也要留意可信XXX，本身也是一种风险，一旦出现违规事件，可能造成很不好的后果。

44

@blackflower

之前提到窃取密钥往往是攻击者的首要目标，那在什么情况下，攻击者的不需要获得密钥，也能进行有威胁的攻击？

@严强

比较典型是延展性攻击，攻击者可以在不对密文解密的前提下，按照自己的意愿修改密文，比如付款的金额原先是100，攻击可以将其成倍增加，200,300,500,1000。教科书上最简RSA加密方案就有这个问题。

@苦人

这个应该是理论上的，原始的RSA会有这种问题，但现实应用中会使用OAEP等协议，使得这种攻击无效。

@严强

是的，现实使用的标准化技术方案（强化协议等）有效预防了这个问题。

@苦人

目前见到的不直接获取密钥的更多攻击应该是侧信道攻击，通过能量、辐射、风扇，甚至麦克风等进行信息获取。

@严强

这个点很好。这些攻击需要攻击者离目标的物理距离够近，以此收集这些物理信号，我们前几期中也有提及。

@苦人

其实，这篇文章有两个问题：1）用户不记密钥，记的都是口令，密钥那么长，无规则或者十六进制或者其他进制，谁都不可能记，所以题目就有问题；2）把密码跟密钥混着说，用户口令、平常说的密码，以及密钥，都说混了。

@严强

十分感谢，真的很细心。之前有些用词确实有混淆的地方，以下更正一下：

- 人类用户使用 →用户口令（日常说的密码）
- 计算机系统使用→密钥

第9论　密码学原语如何应用？解析单向哈希的妙用

@SukiW

请问单向哈希的安全性有什么指标可以参考吗?

@廖飞强

单向哈希的安全主要取决于其算法安全强度和哈希值的位数。算法安全强度一般通过理论安全分析和实践攻防来评判。哈希值位数直接体现在单向哈希输出的长度。安全强度越高，哈希值位数越多，则单向哈希越安全。例如SHA3-256比SHA256安全度高，SHA512比SHA256安全度高。

46

@koudan

文章例子里面，根哈希值Habcd是通过可信信道传输的，那么接收方在验证的时候，数据块a的值，以及Hb,Hcd的哈希值是通过低密级信道传输的吗?

@廖飞强

是的，根哈希要求是可信数据源，用于数据验证。

47

@steven

SHA3-256比SHA2-256安全强度高的理论依据具体是什么?

@廖飞强

这是通过密码学领域学术和工业界进行严格评判，并进行多次攻防实验的结果得出的依据。

SHA3和SHA2相比使用了不同的内部构造，增强了其对于部分攻击的抗性，主要是长度扩展攻击。

比较通俗的比较，可以参考如下网页。
https://crypto.stackexchange.com/questions/68307/what-is-the-difference-between-sha-3-and-sha-256

48

@little.H

数字签名中使用了单向哈希，其使用单向哈希的作用是什么?

@廖飞强

单向哈希可以将待签名的原始数据映射为确定性的摘要信息，且一般都比待签名的原始数据小很多。这样可以加快数字签名和验证签名的速度，同时基于单向哈希的抗碰撞性，能确保签名是针对确定的原始数据签的名。

49

@wheat

哈希在隐私保护中有哪些作用呢?

@廖飞强

在隐私保护中使用广泛，隐私保护中需要的数字签名、消息认证码、密码承诺等都需要哈希的加持。

@刘雪峰@西电

哈希作为承诺一种，结合零知识证明，这样或许更直白些。

@廖飞强

非常正确，密码承诺是零知识证明中广泛使用的密码原语了。

50

@燕窝

目前司法领域的存证区块链的应用，似乎也用到单向哈希，具体是如何使用的?

@廖飞强

区块链存证应用中，一般是数据哈希上链，作为可信存储。原始明文数据链下存储管理。

---END---

《隐私保护周三见》

“科技聚焦人性，隐私回归属主”，这是微众银行区块链团队推出《隐私保护周三见》深度栏目的愿景与初衷。每周三晚8点，专家团队将透过栏目和各位一起探寻隐私保护的发展之道。

栏目内容含括以下五大模块：关键概念、法律法规、理论基础、技术剖析和案例分享，如您有好的建议或者想学习的内容，欢迎随时提出。

栏目支持单位：零壹财经、陀螺财经、巴比特、火讯财经、火星财经、价值在线、链客社区

长按二维码关注

微众银行区块链

白皮书下载 | 订阅干货 | 进群交流 | 合作联系