WeBank
微众银行

WeDPR方案白皮书

即时可用场景式隐私保护高效解决方案

2020 年 1 月

微众银行区块链团队编著

隐私保护

不可估量的蓝海市场

序言

《中华人民共和国密码法》、《中华人民共和国网络安全法》、《信息安全技术个人信息安全规范》等一系列法律法规的正式生效，规范了信息安全和隐私保护的具体要求，隐私保护的重要性和迫切性不言而喻。国务院《国家中长期科学和技术发展规划纲要（2006—2020年）》《粤港澳大湾区发展规划纲要》等国家政策规划也进一步强调要加强重要信息系统和数据资源保护，完善隐私保护机制，从而支撑现代服务业信息技术、平台与基础设施。同期，欧盟史上最严格的隐私保护法案《通用数据保护法案》（GDPR）、美国的《加州消费者隐私法案》（CCPA）、新加坡的《个人资料保护法令》（PDPA）等法规也纷纷出台。一时间，在全球掀起了用技术手段落实隐私保护的时代潮流。

这股浪潮在世界范围内冲击着不具备隐私保护技术能力的企业，一些中小型企业为了避免巨额罚款甚至直接退出了相应的市场。在强有力的政策推动下，隐私保护能力成为了每一个基于隐私数据发展业务公司必须符合的准入条件。目前，国内外的隐私保护领域仍处于发展初期，隐私保护的实际效果如何满足量化的技术标准，隐私合规依然面临着诸多挑战。这为隐私保护技术自身的产业化发展带来了前所未有的机遇。

隐私保护的应用范畴极其广阔，涵盖了从个人隐私数据到企业机密业务数据等所有非公开数据。在当今信息技术高速发展的时代，5G、物联网等尖端数据采集、传输技术势必会带来内容更丰富，时效性更强，体量更大的数据流，其中裹挟着无数隐私数据。在这个数据洪流奔涌的时代，无论是个人用户安心享用服务还是企业探索新兴商业模式，落实隐私保护都至关重要。若能结合区块链信任交换网络和人工智能深度分析理解，合法合规发掘数据中的价值，规避其中的风险，就有可能创造小至引发信息化产业新一轮爆发式增长、大至推动人类社会提前进入后信息时代的美好前景。这个过程中，发展隐私保护技术正是平衡价值收益与隐私风险、实现帕累托最优且可持续发展的关键。

深圳前海微众银行股份有限公司（以下简称“微众银行”），由腾讯、百业源和立业等多家知名企业发起设立。作为国内首家民营银行，微众银行坚持科技立行、科技兴行的发展之路，采取开放模式连接金融机构和互联网企业，严守风险合规底线，在探索各类核心金融业务和普惠科技业务中合法合规发掘用户数据方面，积累了丰富经验。WeDPR作为微众银行对外开放的即时可用隐私保护高效方案，旨在分享微众银行探索隐私保护的技术成果，降低隐私保护技术的使用门槛，推动能有效保护隐私且监管友好商业模式的落地，实现隐私无忧的业务创新和用户体验，从而加速隐私保护整体产业的发展。

微众银行区块链团队

目录

目录

1 隐私保护产业发展现状

隐私保护问题通常会被归结为信息安全问题，然而这并不完全准确。隐私泄露作为信息化技术普及、万物互联之后必然产生的问题，涉及到更为丰富多样的评判标准，涵盖了远多于信息安全的风险。例如，一个精明的商人，可以通过交谈精确获得交易对手的底牌信息，无论我方是否正面回答问题，都很难规避这类隐私信息直接或间接地泄露给对手。另一个典型的例子是在线平台服务商根据隐私信息为其终端用户建立用户画像进行精准营销。绝大部分用户并没有直接告诉在线平台服务商自己的年龄段、居住区域、性别、兴趣爱好、行为模式、健康状况、财务状态等敏感隐私信息，但平台服务商却有能力通过用户与平台的交互历史推断出其中的大部分敏感信息。如果这些隐私信息不幸被不法分子掌握，用户人身安全和财产安全很有可能受到威胁。除了伤害性风险，国际学者进一步指出应当将非伤害性风险，如精神伤害、名誉损失、商业歧视等也加入到隐私立法保护的范畴中。上述问题不能完全依靠标准化的信息安全技术来解决，解决信息安全问题只是实现隐私保护万里长征路上的第一步。

隐私作为人性自我意识中的一项核心诉求，隐私保护的应用范畴极其广阔。对于个人来讲，隐私数据是关于自己和周边环境包括社交网络的个人数据。对于企业来讲，隐私数据是关于自己和合作伙伴的业务和其他非公开数据。隐私数据基本上包括了所有的非公开数据。万物皆有主，数据也不例外。隐私保护的基础目标就是防止这些非公开数据被未授权的主体使用或者以一种未授权方式使用。授权作为隐私保护的关键，为不同隐私保护场景带来多样化的隐私保护诉求。例如，企业甲希望与企业乙分享数据来联合发展一项新业务，但企业乙因为合规的原因只能提供密文数据，同时企业甲要求自己的业务数据只能被约定的新业务所使用，两者的隐私需求截然不同。考虑到真实生产环境的性能和实用性需求，很难构建一个普遍适用、满足所有隐私诉求且卓有成效的技术方案。

整个隐私保护产业目前仍处于早期发展阶段，尽管充满了很多挑战和不确定性，但在利好的政策环境和巨大的市场潜力驱动下，我们对其不可限量的前景深信不疑。以下从政策、市场、技术、应用四个角度具体对隐私保护产业整体发展现状进行回顾。

1.1 政策环境利好

隐私保护产业发展离不开政策的扶持。《中华人民共和国密码法》、《中华人民共和国网络安全法》、《信息安全技术个人信息安全规范》及其相关行业应用的国家技术标准出台，里程碑式地明确了企业在收集、使用、保存非公开隐私数据时所需要达到的技术效果及建议使用的标准化技术手段。在国际社会上，被称为史上最严格的隐私保护法案《通用数据保护法案》（GDPR）除了明确技术效果之外，更是引入了巨额的罚款措施，一个国际集团中任一个子公司可能会因单次违规事件，而面临可能高达集团前年全球年度总收入 4% 的巨额罚款，GDPR 法案的实施进一步加强了隐私保护产业化的必要性和迫切性。

表1列出了自GDPR法案生效之后，全球范围内，国际企业受到隐私保护法规影响的一些重大事件。

表1. 隐私保护法规影响公司运营的重大事件表

年份	公司名称	事件	涉及金额	报道机构
2018	Facebook	意大利数据保护监管机构DPA处罚Facebook违反GDPR法案	1千万欧元	英国卫报
2019	Facebook	美国联邦贸易委员会处罚Facebook	50亿美元	英国BBC
2019	Google	法国数据保护监管机构CNIL处罚Google违反GDPR法案	5千万欧元	法国数据保护机构CNIL

数据源：各报道机构官网，收集日期：2019年12月13日

这些政策法规的陆续生效，在全球范围内，规范了基于隐私数据的商业探索，确实对不具备隐私保护技术能力的企业产生了巨大冲击，但同时，这些政策法规也极大推动了隐私保护由宣传口号向真正可以落实的技术特性的实质性转变。数据作为信息时代最为重要的价值载体，建立隐私数据保护政策法律体系，不仅为存量业务中隐私数据属主的合法权益提供了保障，而且为发掘高价值隐私数据包括金融数据、医疗数据、民生数据等，提供前所未有的商业机遇。通过严格设定行业准入技术标准，隐私保护效果量化、技术规范化的进程开启了新兴价值互联和商业创新，奠定了隐私保护技术在现代信息化商业生态中的重要地位。

1.2 市场前景广阔

除了存量业务的合法合规需求之外，隐私保护产业更大的价值在于促进创新数据业务的落地。过去由于技术能力的不足，高度敏感隐私数据的发掘和利用受到法律法规和商业利益两方面限制。在法律法规方面，用户在将隐私数据分享给企业之后，便可能失去对数据的控制权，很难获知实际数据的使用情况，个人敏感数据存在被滥用的可能。比较典型的例子是医疗数据，在无法排除被滥用的可能性前提下，关于医疗数据的使用场景是受法律限制的，它会影响到工作权利、社会关系、精神健康等敏感领域。在商业利益方面，作为企业的核心资产之一，不受控的数据分享会削弱企业的核心竞争力，甚至打破企业自身的商业壁垒。比较典型的例子是金融数据，在无法保证能消除这些显著风险的前提下，金融数据的使用场景是严格受限的，它会暴露企业自身的经营策略、财务状况、战略布局等商业机密，同时面临合规风险。

发展隐私保护技术正是消除这些限制的关键，表2列出了部分以隐私保护为产品设计卖点的初创公司和上市公司估值融资数据，反映了全球资本市场对隐私保护产业市场前景的认可。

表2. 隐私保护相关公司市值融资表

公司类型	公司名称	市值/融资
上市公司	Snapchat (NYSE: SNAP)	市值211亿美元
初创公司	OneTrust	融资2亿美元
初创公司	Acronis	融资1.6亿美元
初创公司	TrustArc	融资1亿美元

数据源：NYSE，Crunchbase，收集日期：2019年12月13日

除了数据业务创新本身，相关合规监管需求也为隐私保护产业开拓了新的业务空间。在当前数据传播速度之快、影响受众范围之广的信息时代，研发即时高效的合规监管技术是规范整体隐私数据产业生态健康发展必不可少的重要前提。隐私数据在不同法律体系下关于披露信息的类别频次有着不同的合规需求，技术实现上需要平衡监管信息全面性和隐私信息机密性。例如，监管部门一般不会要求企业将所收集的全部敏感个人信息送报监管部门，否则监管部门自身可能会演化成一个系统性风险，一旦被充满恶意的黑客攻破，后果不堪设想。因此，我们需要研发更灵活、更及时、更有效的隐私保护技术以平衡各方的需求，监管科技本身也将成为另一个前景广阔的蓝海市场。

1.3 技术尚未成熟

作为一个热门课题，尽管隐私保护被学术界和产业界关注多年，但真正有影响力的相关落地产品并不多，能够提供公开可验证效果且不依赖对平台服务商信任的强隐私保护的产品更是寥寥无几。造成这一现状的原因很多，但通常会涉及到以下两项常见的挑战。

第一项是隐私保护需求因人而异，如何满足千人千面的挑战。该需求对于需要用代码预先写下固定规则的信息化系统极不友好，一套实用的隐私保护技术解决方案必须足够模块化，提供灵活的系统适配性和扩展性。

第二项是技术方案应该基于什么理论来构建，如何选取信任源的挑战。相对第一项挑战，业界对于第二项挑战的解决方案颇具争议。常见的问题之一是量子计算机对经典密码学的影响几何?另一个对应的问题是基于国际芯片厂商的Intel SGX硬件可信计算环境，是不是能够真正万无一失?密码学算法和硬件可信计算环境，哪一个更可靠?业界至今没有一个能够让各方认同的标准答案。

无论最后的选择是什么，关键要明确选择的后果。对于每一个隐私保护技术方案，我们需要思考以下三个基本问题：

- **依托什么?**——该方案的设计基于哪些安全假设?这些安全假设在目标应用场景中是否可靠?是否合规?
- **保护什么?**——该方案实际提供了哪些保护效果?这些保护效果是否涵盖了目标应用场景中全部隐私保护需求?
- **警惕什么?**——该方案没有保护什么?可能出现什么不可接受的意外后果?这也是隐私保护与信息安全最大区别之一。信息安全关注是否可以访问机密数据，而隐私保护更关注是否可以从未保护的其他信息推断出隐私数据。

现实中的隐私保护技术解决方案需要考虑的问题需要更加全面。在下一章节中，我们将具体分析现有隐私保护技术面临的四大挑战：通用方案的实用性困境、现有架构的局限性难题、用户体验的易用性取舍、商用方案的有效性存疑。回到以上提出的三个基本问题，每一个有效的隐私保护技术解决方案需要给出相应的答案。只有这样，作为数据属主的用户才能充分了解隐私保护方案的实际效果，以及最坏情况下的潜在风险。这三个问题的答案也会帮助我们明确不同场景下的不同隐私保护需求，从而定制优化技术解决方案，实现数据权益和隐私风险的最优平衡。如何处理好以上这些变数，对于促进有影响力的隐私保护产业化落地至关重要，也为隐私保护技术实用化创造了巨大的发展空间。

1.4 应用潜力无限

伴随第5代移动通信技术与物联网的普及，万物互联的时代即将到来，隐私数据井喷的时刻或将随之而至。在过去，用户往往只有在与终端交互的过程中会产生隐私数据，但在将来传感器漫布的智慧环境中，无时无刻都会有关于用户的隐私数据产生。

智慧医疗将有能力实时监控人体的健康体征数据，智慧家居将提供全屋物联主动式服务，智慧城市将链接城市中所有基础设施、人流、车流和物资流。这个过程必将产生海量隐私数据，其内容会更丰富，时效性会更强。

以人工智能为代表的深度数据理解分析技术，人们在获得巨大收益的同时，隐私风险可能会超比例地放大。例如，通过分析实时的人流、车流和物资流，对于个人和企业精准动态监控极有可能成为现实，个人试图保留自己的私密空间，企业试图保护自己的商业机密也将变得相当困难。

能力越大，责任越大。隐私保护技术方案很有可能成为其中的平衡者，通过赋予数据属主对自身数据的控制权，尊重属主自身意愿，实现自主选择，避免潜在的系统性风险。这些真实迫切的需求会为隐私保护重量级应用落地提供良好的契机，隐私保护技术本身也会因此获得大量资源而蓬勃发展。放眼未来，不一定会出现一个通用的隐私保护应用能解决所有的隐私保护问题，但是一定会出现一个隐私保护应用生态群体，在各自的特长领域中达到收益和风险的最优平衡，融合万家数据，实现核心价值互联，推动新兴商业创新，实现潜力发掘的最大化。

2 隐私保护技术产业化挑战

在6000多年的人类文明历史中，隐私虽然是一项本能性需求，但直到近代，隐私的概念才因对照相技术的恐惧而正式成型。伴随着科学技术的飞速进步，隐私的风险也被极速放大。20年前定位一个用户的地理位置需要派人物理跟踪，然而现在GPS定位系统已广泛内置到智能手机中，形形色色的移动应用中说不准哪一款应用就可以通过读取GPS数据轻松远程跟踪该手机用户。隐私风险并不是空穴来风，作为科学技术发展的必然产物，为了平衡技术外延性中的收益和风险，隐私保护技术产业化已是大势所趋。

本章将从设计理念、系统集成、用户体验、信任基础四个关键角度，阐述隐私保护技术在现代信息化社会中有效落实并形成产业规模化所需攻克的技术挑战。

2.1 通用方案的实用性困境

隐私保护通用解决方案，无论在学术界还是工业界，很长时间以来一直都是被关注的焦点问题之一。一旦能够在一个合理的安全假设下设计一个广泛有效的解决方案，其影响力是显而易见的。遗憾的是，正如之前产业分析中所指出的，隐私保护并不是一个纯粹的计算问题，一个普适所有场景的方案可能并不存在。即便在理论上可行，其性能指标也难以满足现代信息化服务的高吞吐、低延时等实际需求。如同万能的图灵机，虽然能够模拟一切可计算过程，实现任意复杂的计算，但在现实中，没有任何一个产品系统，会直接在图灵机上开发和部署，这就是通用方案的实用性困境。

有望接近通用解决方案的技术目前主要有基于计算困难性理论的安全多方计算、同态密文计算和零知识证明。

- **基于计算困难性理论的安全多方计算**可以进一步细分为基于混淆电路的方案或者基于秘密分享的方案。
  - 基于混淆电路的方案将所需计算的函数表达成一个巨型的布尔电路，例如，目前表达一次SHA-256 计算至少需要使用 13 万个布尔门。尽管学术界已经提供了大量优化方案，通用电路转化的过程依旧很复杂。由于需要使用不经意传输技术来安全地提供电路输入，即便在有硬件加速的条件下，这类方案的处理吞吐量和计算效率依旧很低。
  - 基于秘密分享的方案采用了数据分片的设计理念，将每一份数据按照计算参与方的总数分成多个分片，运算直接在数据分片上进行，最终汇总之后的运算效果等同于使用原始数据直接进行计算得到的效果。数据分片通常使用加和分片算法，计算效率大幅提高，但由于需要广播分发与回收数据分片，支持乘法还需额外数据交互，网络通讯的代价很高，处理海量数据时势必会遇到性能瓶颈。

- 除了上述性能问题，无论选用哪一类方案，在计算参与方数量增加时，方案的整体性能代价往往会超线性增长。大量的两方安全计算方案在需要引入第三个计算参与方时便无法扩展使用，然而，如果只能支持两方安全计算，应用场景非常受限。

- **同态密文计算**的理念是数据属主各自将自己数据加密，然后把所有密文上传，在密文的基础上直接计算，然后解密最后的结果密文获得计算结果。由于需要进行最后解密才能完成计算，对于多方参与且缺乏中心信任方的应用场景，这将带来如何指派中心化的信任方来管理数据密钥的难题。除去这一中心化的隐患，全同态密文计算算法，即支持加减乘除完整算术运算，依旧有着显著的性能问题。在 2016 年，IBM 首次发布 HELib 的 C++ 开源类库时，全同态运算比对应的明文运算慢一百万亿倍。尽管后来对算法实现进行了大量优化，学界甚至提议使用专用硬件进行进一步加速，全同态密文计算效率依旧是一个未决的挑战。相比之下，半同态密文计算算法，如仅支持加减算术运算，已经可以达到商业可用的性能，但是由于其并不具备图灵完备性，使用场景有限。

- **零知识证明**的理念是通过将约束关系关联到计算困难性理论，在证明者不透露被证明数据明文的前提下，向验证者证明约束关系的正确性，被证明数据有极大概率满足验证者指定的约束关系，例如证明转账金额不是一个非法的负数。根据选用不同计算困难性理论，零知识证明可以有多样化的构造方式，在不同安全假设下实现高效的数据验证。需要注意的是，由于约束关系必须由验证者预先指定，零知识证明不能直接用来进行结果未知的算术运算。所以，零知识证明不能解决密文计算、安全哈希等需要计算的问题。

以上三类技术都有显著的实用性限制，业界也有尝试依赖可信硬件执行环境来构建通用解决方案，但其实际隐私保护的有效性很难公开验证，在后面的章节我们会具体讨论相应的问题。WeDPR 为了避免通用方案的实用性困境，采用了场景式设计哲学，针对核心业务场景中的个性化隐私保护需求，提供预优化的技术选型和解决方案。这将大幅减少通用性方案适配具体应用场景的二度设计和定制集成的代价，缩短产品落地时间，提供即时可用的开发体验，助力隐私保护应用产品赢得市场先机。

2.2 现有架构的局限性难题

隐私保护很少以一个独立的产品形式存在，更多的情况下必须要考虑与存量系统技术架构的兼容性问题，以及如何与其他业务特性协同构成完整的产品体验。具备严格执行力的隐私保护相关法案条例在近几年才正式生效，至此才明确要求了企业使用技术手段来保障数据隐私并向数据属主提供有效的数据控制方式，企业内部对于隐私保护的关注由此正式从法务合规转向技术合规，这一改变尤其对中小型企业造成巨大冲击。早期产品架构设计往往未充分考虑对隐私保护技术的集成扩展，企业自身缺乏研发隐私保护技术的专业储备。对于一个成熟业务，如果需要对现有技术架构进行大量改造才能集成隐私保护特性来实现合规准入，其代价通常是难以接受的，这就是现有架构的局限性难题。

隐私保护技术与存量业务系统集成过程中常见的兼容性问题有以下两类。

- **平台依赖**是指存量业务已经在某一个平台环境里部署并实现了稳健运行后，隐私保护方案需要依赖另一个平台环境的特性，不得不在多个平台之间进行系统迁移。迁移过程存在大量不确定性，影响现有业务的可用性，引入额外的部署验证代价。这一问题常出现在平台服务商捆绑销售技术方案时，例如，云厂商的隐私保护方案与自身云服务接口深度结合，难以分离使用。

- **环境限制**是指当存量业务所依赖的环境或者设备终端缺乏必要的计算或存储能力时，隐私保护方案中所需的复杂功能难以部署。例如，物联网终端设备芯片处理能力和存储能力都不足以支撑复杂的业务逻辑，需要对业务逻辑进行简化。另一个常见的例子是，小程序等轻客户端应用预置的密码学类库比较有限，前沿的密码学算法库无法直接加载，轻客户端存储的数据也可能会因为用户终端设备内存不足而被突然清空。如果隐私保护方案设计只考虑了功能齐全的服务器环境，对于其他功能受限的环境便无法部署。

应对以上兼容性挑战的关键在于隐私保护方案设计解耦是否充分，模块边界是否具备足够的普适性。WeDPR 在设计之初将集成优化作为核心需求，尽力避免依赖任何特定平台的非通用特性，通过分层式架构在多个层次上划分功能边界，设定可插拔的抽象数据交互接口，在各个所需的架构层次上实现自由逻辑拆分和组合，对于高频组件如监管支持、密钥管理等提供充分的备选方案设计，最小化为克服环境限制而引入的优化定制成本。

2.3 用户体验的易用性取舍

隐私保护技术作为一个整体系统解决方案，用户体验往往是其中易遗忘的重要环节。隐私保护技术实现效果的前提往往需要做出取舍，通常要引入额外的交互或记忆需求。在交互方面，不少隐私保护技术如安全多方计算，为了保障所有参与方都能公平地获得协作成果，不得不采用多轮交互的方式，每次仅给出部分数据相关的信息，防止少数参与方获得其他参与方完整信息之后恶意退出或破坏协议。在记忆方面，如果数据属主希望真正掌控对数据的控制权，数据的密钥必须掌握在自己手中，但考虑隐私数据的体量和数据属主自身的认知能力限制，能够安全记忆并随时使用的密钥个数和大小十分受限。反之，如果方案设计偏向易用性，隐私保护方案保护效果就会打折，这就是用户体验的易用性取舍。

以上问题对于没有人类用户参与的场景，通过增加设备资源能一定程度解决。一旦把作为数据属主的人类加入到系统控制流中，受限于人类认知能力的极限，很难有同时在易用性和安全性上两全的标准答案。任何一个只展示神奇技术效果却不要求用户进行必要参与的隐私保护方案一定会蕴含隐私风险，通常表现为以下两种形式。

- **密钥托管：**密钥是所有基于密码学理论构建的隐私保护方案中最为关键的数据。谁掌握了密钥，谁就掌握了对应数据的实际控制权，所以密钥也是最有价值的数据。如果平台服务商提供全权托管服务，用户在使用隐私保护方案的过程中，自始至终都没有使用自己的密钥，对应隐私数据使用实际并不受用户控制。真实的控制权在平台服务商手中，最终实现的隐私保护效果和未曾部署任何隐私保护方案的信息系统没有本质差别。

- **授权托管：**授权操作是数据属主的关键权益之一。隐私数据的采集、分享、使用、存储、遗忘等过程中，如果全程用户无感自动化完成，则需要警惕授权控制是否真实存在。主流方案提供的是事前控制和事后更正，即处理隐私数据前询问用户的意愿，之后允许用户改变意愿对之前的设定进行补救。如果以上这些控制都不存在，最终实现的隐私保护效果与全权信任平台服务商如出一辙。

尽管以上易用性取舍很大程度上反映了系统设计的内在局限性，但在分析具体取舍之前，更关键的是理清这些取舍的必要性。WeDPR 深刻思考了人类在整个隐私生态体系中的角色和作用。隐私数据始于人、利于人、终于人。作为一个有效的隐私保护方案，通过引入社会学、心理学和经济学原理、理性参与者模型、多方激励机制等突破性优化因子，推动无感用户体验和有效隐私保护之间的平衡向帕累托最优靠近。

2.4 商用方案的有效性存疑

隐私保护技术的商业化进程目前尚属早期，在各种解决方案展示过程中，我们能够比较清晰地看到作为关键目标的隐私保护效果和潜在应用场景。但是，现有方案对于支撑方案的技术设计和效用取舍往往缺乏客观完整的披露。隐私保护方案部署之后，也难以独立于方案服务商公开验证其有效性。回归到隐私保护方案三大基本问题中第一个也是最重要的问题——方案依托什么？尽管大多方案会展示大量的技术术语来阐述方案完备性，但以业内共识的箴言——“问题总是出现在最薄弱的环节”来看，技术术语本身与解决方案设计的有效性没有直接关系。在不能确定安全假设和信任基石的前提下，公众无法对方案的有效性进行客观判断，这就是商用方案的有效性存疑。

究竟应该信任什么技术，业界各大服务商根据自身的产品定位和市场战略有着不同答案。最常见两个选择就是硬件可信计算环境和计算困难性理论。

- **硬件可信计算环境**利用CPU等计算硬件为需要隐私保护的数据隔离出一个受保护的计算环境。数据以密文形式传入，在隔离环境内部完成计算后，再以密文形式返回。主流的国内外芯片提供商均提供了类似功能，当前广泛使用的是Intel SGX环境。随着隐私保护迫切商业化的需求出现，Intel SGX自身的安全性也受到越来越多的关注。在国际安全漏洞CVE信息库中，关于Intel SGX的漏洞记录只有10条，但仅在2019年中，就新增了6条记录，呈现高速增长态势，其中新增3条记录描述了如何突破Intel SGX安全隔离，执行任意权限操作。硬件可信计算环境最大的风险是缺乏备选方案，一旦出现硬件缺陷，替换硬件的代价极其高昂，硬件本身具备不透明性，受控于芯片生产厂商，难以自证撇清预留后门的可能性。

- **计算困难性理论**基于数论、概率论、离散数学等抽象科学原理，不依赖任何硬件安全假设，构建隐私保护的软件实现方案。由于硬件方案近5年才出现，Intel于2015年才将SGX环境正式推向市场，早期的隐私保护方案研究无法依赖可信硬件计算环境，只能通过数理思辨减少安全假设的影响，构建仅靠软件自身也能有效运作的技术方案。数据通过精心设计和充分验证之后的算法转化为密文，联合不同密文，使用符合特定保护特性的算法进行数据融合，最终在不泄露隐私数据明文的前提下，获得所需的最终计算结果。软件方案的核心是一系列密码学困难性理论，他们也会受到新兴技术如量子计算的挑战。后量子软件方案尽管还未成熟，最近几年已然成为了业界关注的焦点。相比硬件，软件方案的弱点在于性能，而优点在于其有效性是可以通过代码评审进行公开验证且便于升级和定制化。

不同的应用场景和隐私需求可能会依托截然不同的安全假设。安全假设的选择本身不是最重要的，隐私保护方案设计的核心在于是否能够向用户客观透明地披露作出选择的理由和需要警惕的风险，并提供公开可验证的方式来证实方案有效性，从而避免商用方案的有效性存疑。WeDPR 作为微众银行自主研发的隐私保护方案，倾向于使用久经考验的计算困难性理论来构建高效的技术方案，最小化对可信第三方服务以及可信硬件执行环境的依赖，实现透明可信的隐私保护效果。

3 WeDPR是什么

WeDPR是一套场景式隐私保护高效技术解决方案，依托区块链等分布式可信智能账本技术，融合学术界、产业界隐私保护的前沿成果，兼顾用户体验和监管治理，针对隐私保护核心应用场景提供极致优化的技术方案，同时实现了公开可验证的隐私保护效果。

WeDPR由微众银行自主研发，致力于使用技术手段有效落实用户数据和商业数据的隐私保护，提供即时可用的开发集成体验，助力全行业合法合规地开拓基于隐私数据的核心价值互联和新兴商业探索，同时让数据控制权真正回归数据属主。

3.1 设计理念

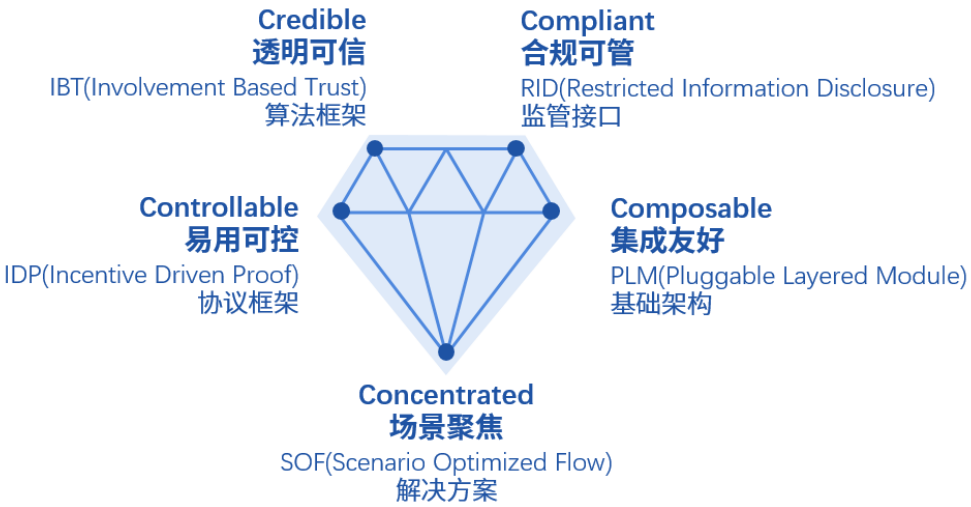
WeDPR遵循用户至上、业界示范、国密支持、监管友好、依赖解耦、配置灵活、体验便捷的设计理念，针对金融业务和普惠科技领域“智慧金融”和“智慧城市”等诉求，采用零知识证明、安全多方计算、可监管加密等技术，平衡数据生态系统中的多方协作，对数据轮回周期进行统筹。构建灵活易用、高安全性的隐私保护方案。

表3. WeDPR七大设计理念

设计理念	实现效果
用户至上	WeDPR充分尊重客户隐私偏好，针对不同业务、不同诉求的客户、不同程度隐私保护需求进行差异化定制，在兼顾安全和效率的同时，最大程度提升用户体验。
业界示范	WeDPR助力倡导隐私商业模式，通过构建面向普罗大众的场景化示范应用，形成符合金融级应用场景功能、性能、安全性、监管等要求的隐私保护技术方案，为各行各业数据隐私应用落地提供可靠的基础设施，加速各行各业构建具备隐私保护能力的产品落地。
国密支持	WeDPR遵循国家商用密码算法标准，提供国密算法密钥管理服务、支持国密证书认证体系和相关软硬件安全产品，各场景组件均满足国密安全标准。
监管友好	WeDPR支持穿透式或集中式的监管，保护用户隐私数据的同时，引入健全的监管机制帮助各类企业在实践过程中合法合规履行社会责任。
依赖解耦	WeDPR提供跨平台的高效隐私保护技术方案，最大限度地减少了开发复杂度和平台依赖度，帮助用户低成本集成和配置创新业务和存量业务。
配置灵活	WeDPR围绕层次化、场景化框架，在设计上根据不同业务场景提供了多种模块化的开发工具包，方便使用者进行灵活定制开发，快速部署业务。
体验便捷	WeDPR设计的资源模板生成器，对不同业务需求的用户进行场景化定制，极大减少了用户体验隐私保护产品的门槛，资源模板生成器可在5分钟内一键构建示例应用，帮助用户快速体验WeDPR各系列解决方案，快速了解隐私保护功能及原理。

3.2 5C隐私保护

WeDPR首次提出5C隐私保护，突破性地实现了易用可控、透明可信、合规可管、集成友好、场景聚焦的效果，对用户数据生命轮回的收集、存储、披露、遗忘、恢复进行全方位保护，提供多场景的隐私保护解决方案，有效解决了业务需求多样化和部署异构化的矛盾，为隐私保护提供了新的解决思路和落地模式。



Credible 透明可信

WeDPR使用IBT(Involvement Based Trust)算法框架进行流程协议设计，确保用户的隐私数据只有在用户同意参与数据操作时才能被最小化程度地解密使用。IBT算法框架使隐私数据密文运算过程不依赖隐私数据解密过程，只有在协议事先约定的阶段，用户同意授权解密的情况下，获得授权方才能对关键数据进行解密，除此之外，平台服务商对协议中的数据明文内容一无所知，真正实现了数据控制权回归数据属主。

Controllable 易用可控

WeDPR使用IDP(Incentive Driven Proof)协议框架实现了易用性和可控性的精妙平衡，在给予数据属主最大可控性的同时，极大地提高了产品易用性。IDP协议框架大大简化了传统高安全级别隐私保护方案设计中交互操作繁复的问题，结合社会学、经济学、心理学、人因学等多方激励模型，在维持关键安全特性的同时，实现了数据属主对其隐私数据使用的有效控制和便捷可用。

Compliant 合规可管

WeDPR提供RID(Restricted Information Disclosure)接口为监管送报提供法律法规中必要的数据，并提供动态规则触发机制，第一时间发现可疑事件。RID监管接口支持事先约定的监管送报数据类型和可配置动态事件触发规则，满足监管要求的同时，合法合规地实现了业务运营方对所产生敏感商业数据的最小化披露。

Composable 集成友好

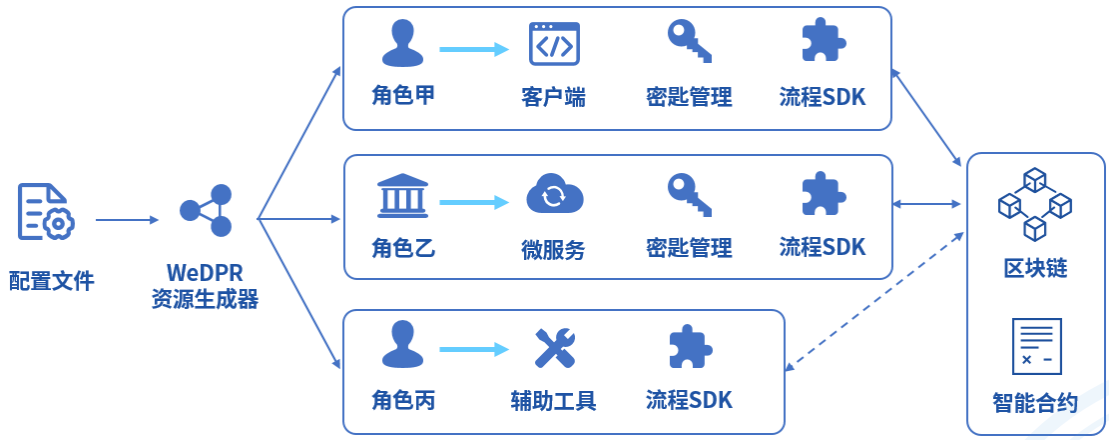
WeDPR设计之初充分考虑了与现有业务系统有机融合方式，采用PLM(Pluggable Layered Module)基础架构，支持不同粒度的逻辑组件自由插拔拼接，且不依赖平台系统的特有功能。PLM基础架构规范化了整体解决方案中各个独立组件的数据接口，统一化的抽象接口使得不同粒度的组件之间的插拔和协作像搭积木一般便捷，在提供跨编程语言解决方案的同时，不依赖平台系统的特有功能。

Concentrated 场景聚焦

WeDPR采用场景聚焦的方案设计理念，为不同隐私保护核心应用场景提供定制化的技术方案框架模板，实现性能极致优化的同时，达到了即时可用的效果，大大缩短了产品落地时间。

3.3 体验流程

WeDPR独创的一站式体验流程，为不同业务角色所需的各个核心业务操作，生成隐私保护相关开发资源和示例应用。



模板资源生成器作为WeDPR用户体验入口工具，用户可以通过下述三个步骤快速体验WeDPR。

- 下载：根据所属平台下载对应WeDPR部署工具包。
- 编译：根据所需业务场景编译配置文件。
- 构建：执行WeDPR部署工具快速构建和部署隐私保护场景套件。

模板资源生成器根据用户提供的配置文件，会生成三大类的开发资源。

- **代码模板**

  供用户调整逻辑的代码接口，具体的语言根据配置文件中的目标开发语言来制定，主要是上层业务流程的代码。

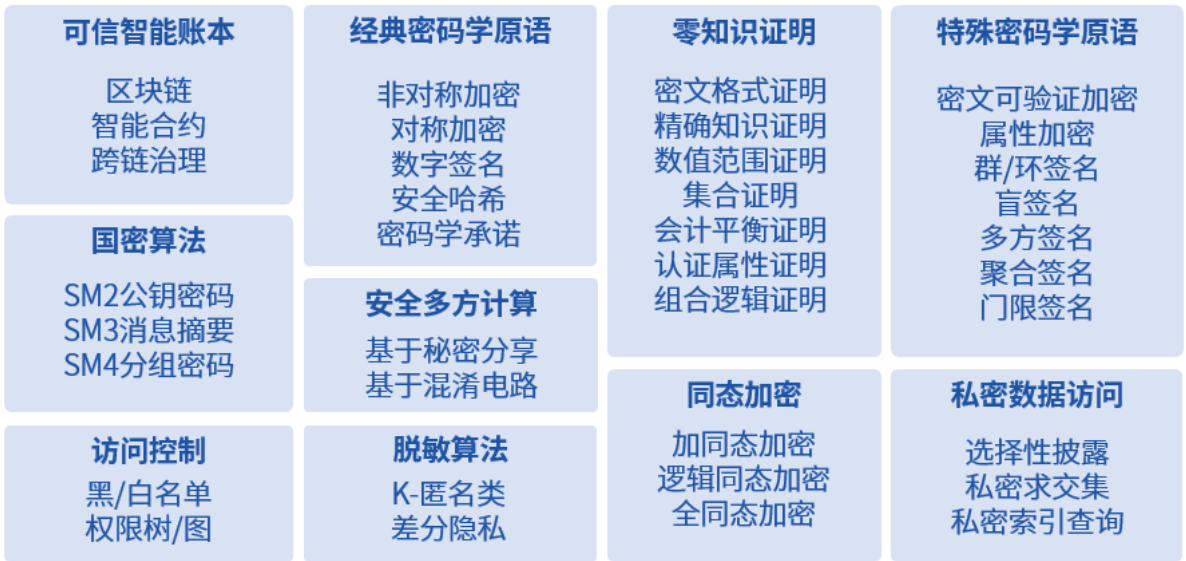
- **配置文件**

  供用户调整的配置文件，配置文件中应包含常用的配置项和对应的示例。

- **可执行程序和预编译类库**

  对于通用平台可直接提供跨平台的可执行程序和预编译类库，减少编译和部署的时间和对系统环境的要求。

为了使定制生成的隐私保护场景套件达到5C隐私保护效果，WeDPR基于以下核心技术攻克了大量设计和工程挑战。下一章节将以隐匿支付、匿名竞拍、匿名投票、选择性披露四大场景为例，阐述WeDPR即时可用场景式解决方案的实际效果。



4 WeDPR场景式解决方案

本章我们将以描述一个虚构角色——“美丽”的一天经历出发，结合隐匿支付、匿名竞拍、匿名投票、选择性披露等常见业务场景，对现实世界的隐私问题进行分析，引出WeDPR方案对隐私保护技术落地的思考，阐明面向各个场景的优化方案设计和最终效果。

> 故事发生在9102年，美丽是一个活泼开朗的少女，在实习工作过程中偶然获得了穿越时空的能力。她十分喜欢这个超能力，并经常使用它去解决生活中遇到的麻烦事儿。

4.1 隐匿支付

随着电子支付在用户日常生活中的普及，用户几乎每天都会产生电子支付信息。电子支付信息作为重要的个人隐私数据，需要用户谨慎保护。下面让我们看看美丽在电子支付过程中遇到了什么。

> 又是一个国庆长假，美丽计划坐飞机外出度假，犒劳一下辛苦的自己。她在一家旅游网上购买机票后，随手自拍发了朋友圈。同公司的小华一直在密切关注美丽的日常行为，由此获取到了美丽支付记录上的金额、行程等信息。兴奋的小华购买了同一趟航班并选择了美丽旁边的一个座位。一上飞机，美丽惊喜地发现小华就坐在自己的旁边，当她以为这一切都是上天的缘分时，小华自豪地告诉美丽他是通过支付信息知道其行踪时，美丽露出了尴尬而又不失礼貌的微笑，游玩的兴致顿时烟消云散。美丽选择穿越时空进行挽回。

美丽此次网上支付，泄露了包括支付信息以及相关个人行踪等重要隐私信息，具体包括支付双方的身份信息，即付款方和收款方，机票的支付金额以及支付用途。通过这些隐私信息，第三方就可以轻松获取美丽的消费记录及其相关行踪，这已经导致了严重的隐私泄露问题。

> **穿越时空：**这次，机智的美丽购买机票后，先将支付记录打了马赛克，然后配合自拍发了朋友圈。同时想着，这次小华最多知道她出去玩了，去哪肯定是不知道了。万万没想到的是，小华根据美丽的支付票单，确定美丽的机票订购平台后，买通了订购平台的工作人员，仍然获取了美丽的行踪。飞机上，美丽惊讶地发现小华仍然坐在自己的旁边。小华骄傲地告诉美丽一切的来龙去脉后，美丽露出了惊讶而又略显无奈的微笑，坐立不安的美丽决定再次穿越时空摆脱支付隐私信息泄露的困扰。

这次美丽虽然没有直接显露自己的支付记录信息，但是当网上支付完成后，第三方支付平台会记录这笔支付记录的明细。同时，通过美丽的网上支付和其他行为等相关信息，配合大数据，社会工程学等手段，黑客可以获取如位置、行程、爱好、资产数量、消费习惯等个人信息。通过支付记录历史可以发掘用户日常生活中的诸多敏感信息，可能引发对于财产和人身的巨大隐私和安全风险。

> **再次穿越时空：**美丽本次选择了采用隐匿支付的购票平台，以类似方式完成付款之后，顺利购买了机票，然后将密文格式的支付记录配合自拍发了一个朋友圈。飞机起飞时，美丽再也没有看到小华的身影，这次美丽终于实现了隐匿支付，保护了自己的支付和行踪信息。飞机降落后，美丽开启了愉快的假期生活。其实，小华这次也试图通过隐匿支付购票平台工作人员获取美丽的支付和购票信息，但是购票平台后台的数据已全是密文格式，无法获取有用的隐私数据，因此小华获取不到美丽的支付行为和行踪信息。

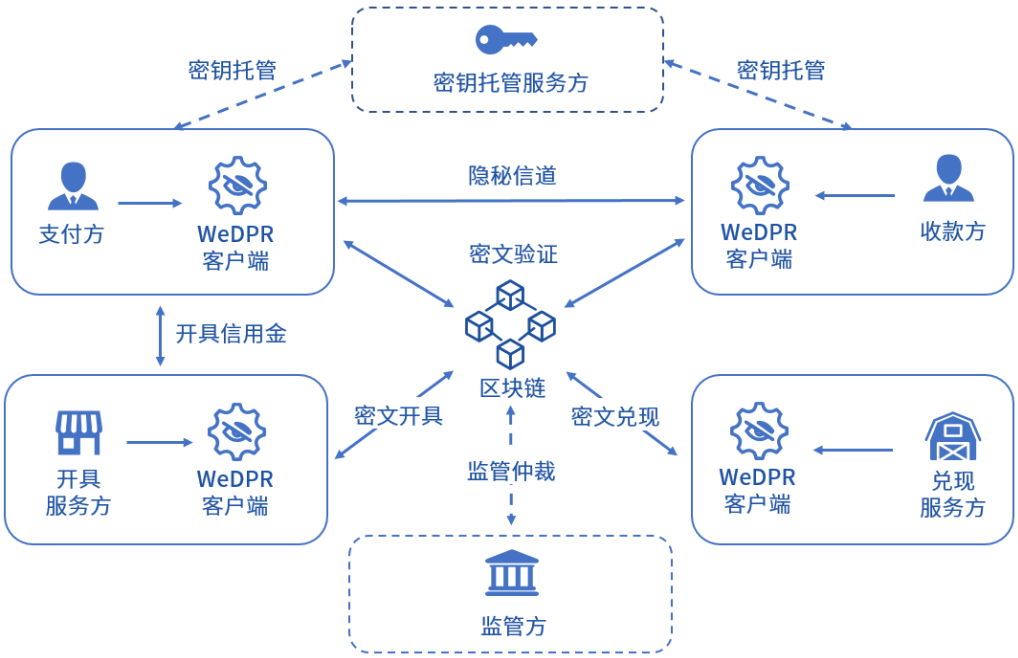
美丽这次通过隐匿支付，完美地保护了包括金额、身份等支付信息。隐匿支付针对金融场景中的身份匿名和金额隐藏等需求，使资产可以进行隐匿支付。隐匿支付支持任意类型的资产和权益，在不依赖可信第三方服务的前提下，实现交易者身份和交易金额的隐匿。

在美丽的支付过程中，主要有四个参与方，分别是付款方、收款方、第三方支付平台和电商平台。其中，用户通过支付平台填写付款信息，通过电商平台转账到用户收款方。通过隐匿支付可以完成用户付款方到用户收款方的转账流程，而支付平台、电商平台可以对转账后的相关数据的会计平衡证明、相等证明等零知识证明进行正确性验证。其他第三方获取不到交易的明文，因此可以有效保护支付过程中端到端的交易隐私。

4.1.1 隐匿支付方案的优势

传统支付方案的隐私保护需要全权信任第三方平台，对所有中间服务商没有任何隐私。近年来，曾发生支付平台员工窃取并倒卖大量账户被捕的案件，案件涉及用户真实姓名、手机、电子邮箱、家庭住址、消费记录等高度敏感信息。这里以权益类服务为例，讨论支付架构的不同之处，传统支付方案的架构如下图所示。

传统支付方案中服务发起方、中间参与方和服务接收方可以获取交易双方的身份和交易金额，存在显著的隐私泄露风险。相比之下，隐匿支付方案依托密码学困难性理论，在全流程公开可验证的前提下，保护了支付过程中支付方和收款方的金额、身份、交易明细等隐私安全。



WeDPR 隐匿支付方案基于零知识证明算法，在不依赖可信第三方服务的前提下，支持任意数据类型的资产或权益类型，实现支付过程中的交易者身份和交易金额隐匿、监管友好、交易正确性公开可验证。本方案支持以下五类角色，包括权益拥有者、权益开具兑现服务方、存储服务方、密钥管理服务方和监管方。

表4. 隐匿支付方案中的角色

角色	定义
权益拥有者	数字权益的权益所有人，权益拥有者可以相互转账，也可以将自己名下的线下权益转化数字权益，也能将数字权益兑现为线下权益。
权益开具兑现服务方	提供将线下权益与数字权益相互转化的服务，具体进一步细分为是否支持通兑，即服务方A开具的数字权益能否到另一家服务方B进行兑换。
存储服务方	基于区块链或者传统数据库，提供关键数据可信存储的服务。
密钥管理服务方	提供匿名数字权益相关密钥的托管和恢复服务。若权益拥有者丢失密钥和相关归属信息，可以请求密钥管理服务方协助，在证明自身身份之后，取回自己权益的使用权。
监管方	有权利进行观察和仲裁的权益维护人。监管方可以获取权益支付中的交易细节和交易金额等信息，进行监管审查。

WeDPR隐匿支付方案提供优异的隐私交易处理能力，实现了轻量化交易数据、极低交易延迟和超高交易吞吐量的性能指标。支持每秒万级交易并发量，交易记录仅为百字节大小以及交易处理微秒级确认，最终实现如下隐私保护效果。

表5. 隐匿支付方案效果表

隐私特性	隐私效果
身份隐匿	用户资产或权益是流转的载体。权益拥有者在进行转账时可以不披露自己的身份，但是可以证实自己针对权益的所有权，并且可以给出权益与自己身份关联的证明。
权益隐匿	除了交易双方，第三方不能知道权益凭证的内容，如交易金额。
交易隐匿	除了交易参与者，第三方无法获知交易的具体细节，如交易参与方的信息、交易发起时间、签名等。
抗双花	利用区块链的全局账本，同一份权益凭证不能被花费两次。
监管友好	监管方可以在交易发生后获取必要的仲裁信息。

4.1.2 隐匿支付方案在应用领域的探索

隐匿支付应用的场景非常广泛，适用于所有数字资产的支付和交换场景，能够有效保护用户和机构的信息和身份隐私。同时，涉及到转账支付场景，隐匿支付对现有监管体系进行了良好的支持。通过隐匿支付，监管方可以智能监管业务数据，自动开展审核仲裁各项工作。

4.1.2.1 供应链金融

供应链金融作为银行联系核心企业和上下游企业提供灵活运用的金融产品和服务的一种融资模式，涉及银行、服务平台、各行业机构、物流公司等诸多行业和产业。2019 年，供应链金融在全球共融资超过 2 万亿美元。2020 年，仅中国供应链金融市场预计投入高达 3 万亿美元以上。供应链金融飞速发展的同时，也蕴含了较大的安全隐患。如服务提供方和核心企业、小微企业间信息价值不对等，信息泄露造成的价值损失风险，企业信息对服务提供方不透明，产业上下游资信偏弱，担保增信不充分等问题。

目前供应链金融业务，一般涉及到上链存储，资产登记、转让、融资和兑现等。供应链金融场景需要数据穿透和信息共享，需要通过资金流、信息流、物流信息等融合才能提升整个闭环的真实性。隐匿支付十分契合供应链金融业务，有利于打破供应链金融存在的信息孤岛、互通困难等问题，能够有效解决供应链金融存在的隐私问题。针对供应链金融中的合规性挑战，隐匿支付可以在满足监管合规的要求下促进多方进行可信金融协作。

4.1.2.2 跨境支付

跨境支付作为基于延伸全球的互联网跨境支付业务。自 2013 年全球开放支付机构进行跨境外汇支付业务资格后，跨境支付业务涉及领域不断扩大，以旅游、留学、电商等活动带动跨境消费快速增长。随着经济全球化的进展，跨境支付有望在未来几年激增。2014 年已达到 1,440 亿美元的价值。预计 2020 年第三方机构跨境支付网支付总额将高达 1 万亿美元。然而在跨境支付推进过程中，新用户对汇款交易方式信任不足，交易规模难以快速增长。因此，交易隐私问题亟待解决。

传统跨境支付系统中，汇款涉及的相关机构能够访问到大量客户交易信息，客户信息隐私性较差，同时汇款周期长、手续多、支付安全难以保证等问题也影响着跨境支付的发展。基于隐匿支付的跨境支付平台，提供端到端的隐私保护机制，仅交易参与方、对端银行和监管方才可以访问相关交易信息，有效保护客户的隐私信息，提高用户对支付行为的信任，有利于降低跨境支付成本，提升支付效率。

4.2 匿名竞拍

电子拍卖是用户日常生活中的重要组成部分，用户可以对不同商品进行挑选和竞价。竞拍信息作为重要的个人隐私数据，需要用户妥善保管。下面让我们看看美丽在拍卖过程中经历了什么。

> 美丽到达目的地后，惊喜地发现自己最喜欢的歌手正好在当地举办演唱会。作为一名追星少女，美丽赶忙去会场买票。到了会场，有一些票贩子在兜售门票，美丽选好了一张票，准备用500元进行购买时，票却被人截胡了，郁闷的美丽只能重新再买一张。这时，由于上次其他人已经知道了美丽愿意出价500元买一张门票，其他出价更便宜的票贩子纷纷将手中的门票涨价，美丽又急又气。美丽选择穿越时空到买票前的时刻进行补救。

这次美丽的购票方式，其实是一种明文出价竞拍方式，泄露了包括用户身份、出价等重要隐私数据。用户之间事先观察对方出价，了解对方购买意愿，从而出现哄抬价格、恶意竞价事件。

> **穿越时空：**这次，机智的美丽选择使用一款竞拍票务软件，想借助拍卖师做公证人，维护拍卖公平性，势必能买到一张价格合理的演唱会门票。美丽登录软件，提交出价金额。可奇怪的事情发生了，总有一些用户比自己出价高一点点，这样来回往复，美丽眼睁睁看着票价往上涨，直到票价高到离谱的程度，美丽已经有点害怕了。如果自己继续提高出价，可能成交了，但非常不划算，如果放弃继续出价，则又无功而返。美丽嵌入了两难境地，她决定再次穿越时空竞拍门票。

本次美丽选择让拍卖师做拍卖公证人，保护她的出价身份和数据。实际上事与愿违，竞拍软件中的拍卖师由软件平台控制，可以清楚知道每个实际用户的出价，然后利用平台几个机器人账号，总是将用户出价中的最高价向上随机浮动，尽可能让用户出到较高的价格才能买到门票。因此，可以获取拍卖者身份和出价明文的拍卖师并不可信，用户难以获取公正的竞拍服务。

> **再次穿越时空：**有了前车之鉴，美丽本次经过对竞拍平台的反复甄选，选择了采用匿名竞拍方案的竞拍系统。登录该系统，她同样提交了出价金额，该系统服务端获取到了美丽的出价请求，但是是密文格式，有效保护了美丽的出价金额。当其他用户类似出价完成之后，出现了一个声明竞拍赢家的按钮。当美丽点击之后，看着弹出的提示框显示竞拍成功，美丽喜出望外，最终以合理的价格顺利拍卖到了演唱会的门票。

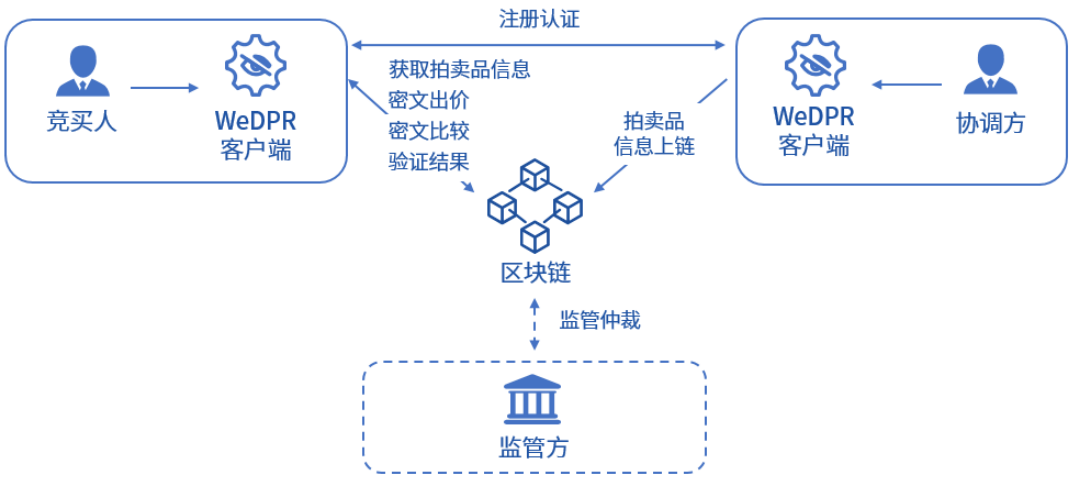
美丽本次通过匿名竞拍系统，得益于匿名竞拍提供的强大隐私安全特性，可以以合理的价格拍卖到演唱会门票。匿名竞拍方案不需要拍卖师的参与，可以有效杜绝其作恶的可能性。在竞拍交互过程中，竞买人的身份和出价数据，均是以同态密文格式进行交互和计算，可以有效保护身份和出价这些重要的隐私数据，并且能公开可验证最终的竞拍结果，保证竞拍的公正性和公平性。

在美丽竞拍过程中，主要有三个参与方，分别为竞买人、拍卖师和第三方平台。其中用户作为竞买人，向第三方平台组织的购票系统发起购买请求。通过匿名竞拍，用户从发起竞拍请求，到竞拍完成的结果验证均为密文进行。竞买人可以验证竞拍过程行为有效、结果可靠，同时保护了自己的身份隐私和出价隐私。

4.2.1 匿名竞拍方案的优势

传统竞拍方案出价隐私和成交正确性都需信赖拍卖师的信誉。除了传统的拍卖行竞拍，以竞价为核心的竞拍已衍生了多样化的经济活动，如标准商品的采购招标、融资招标、广告竞价等。经手大量敏感信息的拍卖机构对于竞拍过程中的公平性和隐私性难以自证清白，可能促成串标、围标等不法行为。传统竞拍方案如以下架构图所示，存在多个隐私泄漏风险点。

相比之下，隐匿竞拍方案依托密码学困难性理论，在全流程公开可验证的前提下，出价隐私和成交正确性均有算法协议保证。在竞拍流程中，监管方可以获取竞拍过程中的关键数据，竞买人可验证竞拍结果的正确性。



WeDPR匿名竞拍方案基于同态加密、零知识证明等算法，在不依赖拍卖师等可信第三方的前提下，支持多种常用竞拍规则。竞拍过程中仅披露中标价信息，对竞买人身份和出价金额隐匿。本方案支持以下四类角色，包括竞买人、协调方、数据存储方和监管方。

表6. 匿名竞拍方案中的角色

角色	定义
竞买人	参与竞买（竞拍出价）的主体。
协调方	可以组织发起竞拍并进行竞买人身份认证的主体。
数据存储方	存储竞拍系统参数、竞拍流程中间结果，并验证上传的竞拍数据是否正确及获胜者是否正确的主体。
监管方	有权利进行观察和仲裁的权益维护人。监管方可以获取竞拍过程中的细节和出价等信息，进行监管审查。

WeDPR匿名竞拍方案提供优异的隐私拍卖处理能力，实现了轻量化拍卖数据、较低交易延迟和高交易吞吐量的性能指标。支持每秒千级的竞拍处理并发量，每笔出价记录仅为千字节大小以及出价处理延迟毫秒级确认，最终实现效果如下。

表7. 匿名竞拍方案效果表

隐私特性	隐私效果
身份认证	只有有资格的竞买人才能参与竞拍。
身份隐匿	竞买人在进行竞拍时可以不披露自己的身份，但是可以证实自己对出价的所有权。
出价隐私	开标前，除了提供此出价的的竞买人，第三方无法获知除获胜价格之外的出价金额。
防共谋	参与竞拍的竞买人之间无法串通合谋作假。
公开可验证	竞拍中的每个环节，都可被验证与监督，包括竞买人对出价的所有权、竞买人操作是否正确遵循协议、最终获胜者是否正确等。

4.2.2 匿名竞拍方案在应用领域的探索

匿名竞拍应用场景十分广泛，适用于通过数值大小比较角逐出优胜者，同时能够全过程保护参与者身份与数据隐私的多方协作场景。

4.2.2.1 招标采购

招标采购是指采购方作为招标方，先提出采购的条件和要求，邀请众多企业参加投标，然后由采购方按照规定的程序和标准一次性从中择优选择交易对象，并与提出最有利条件的投标方签订协议的过程。招标采购市场规模庞大，全世界主要国家市场规模已高达十万亿美元。特别是大宗商品招标采购，包括金属、农产品、能源、化工、产权、金融衍生品等，有着巨大的市场发展空间。然而，招标采购过程中，经常出现信息不对等、过程不透明、结果不公正等诸多问题。

招标采购系统中涉及到供应商、招标机构、评标专家、政府监督机构等，整个招标采购环节要求确保公平性、公开性和公正性。匿名竞拍方案可以让招标采购流程做到全流程安全可控可验证，确保投标、开标等关键环节在投标方隐私安全的前提下做到公平与公正竞标，并且实现公开可验证。另外，每个投标人的产品、投标记录均需要被追踪，关键流程和数据不能脱离监管视线，可以杜绝大宗商品招标采购中易出现的巨大腐败事件。

4.2.2.2 电子拍卖

电子拍卖是传统拍卖形式的在线实现。卖方可以借助网上拍卖平台展示自己的商品，竞拍方可以借助网络，足不出户进行网上竞拍。近年来电子拍卖行业得到了广泛的应用，截止2019年已有上百亿美元的市场规模。值得关注的是，电子拍卖过程中，极易实施暗箱操作，往往存在恶意抬价等问题，使竞拍者很难确定竞拍流程的合理性和可靠性。

电子竞拍参与方一般涉及到竞拍平台、竞拍者、竞拍物和拍卖师。电子竞拍场景需要确保竞拍者的身份隐私，保障竞拍全流程的公平可信。匿名竞拍正是为此量身打造的隐私保护方案，保护竞拍者的身份和出价隐私，同时不需要传统第三方如拍卖师参与即可完成拍卖流程，有效避免了拍卖平台和拍卖者勾结，同时有效杜绝了恶意抬价等现象，并且竞拍结果公开可验证，从而实现电子竞拍监管合规下的公平性和公正性。

4.3 匿名投票

投票和评价作为用户表达观点和意见的重要方式，与日常生活息息相关。但是出于一些现实因素，用户往往难以表达出公正合理的诉求，这其中主要是存在有待解决的隐私保护问题。针对这个场景，下面让我们看看美丽又遭遇了什么样的经历。

> 美丽终于顺利买到了门票，但她想起这次竞拍门票的艰辛，气就不打一处来，于是在上次竞拍被坑的软件上打了一个差评。然而不到5分钟，一个壮汉就出现在美丽的面前，竟把美丽堵在了一个小角落，然后拿出手机，指着美丽刚发出去的差评，说到："亲，小本生意，经营不易，麻烦给个好评吧。"美丽受惊之余，颤颤巍巍的把差评改为了好评。面对此情此景，美丽毅然决然启用穿越时空的超能力。

美丽填写的差评信息，泄露了她的身份、评价内容等信息。软件方根据用户身份，可以通过用户注册的信息获取用户的手机号码，年龄，性别等敏感数据。利用这些重要的个人隐私数据，通过评价信息就可以追溯到特定用户。

> **穿越时空：**美丽这次不敢明目张胆的打差评了，她决定再尝试一次，依然给那个黑心竞拍软件打个差评。这次她在提交完评论之后，勾选了匿名评价功能。希望这次不会被系统发现，然而美丽又接到了软件平台方打过来的电话，让美丽将差评删除。美丽立刻挂断对方电话，再次穿越时空。

美丽通过竞拍软件提供的匿名评价功能，仅仅只是让美丽的用户名在评价界面没有显示，但软件服务端其实可以获取用户的完整身份和评价信息。看似匿名评价，其实并不匿名。用户的身份和评价内容在服务方清晰可见，没有做到有效保护。

> **再次穿越时空**：美丽憋着一股不服输的倔强劲，心想嘀咕着一定得给那个可恶的竞拍软件一个大大的差评，而且不能再被对方发现了。美丽这次选择了一个采用匿名投票的评价平台，可以针对各种软件进行评分，而不泄露用户的身份信息。美丽搜索到了那个竞拍软件，然后小心翼翼投了0分。美丽这次终于顺利进行了评价，再也没有因为提交差评受到骚扰甚至威胁。

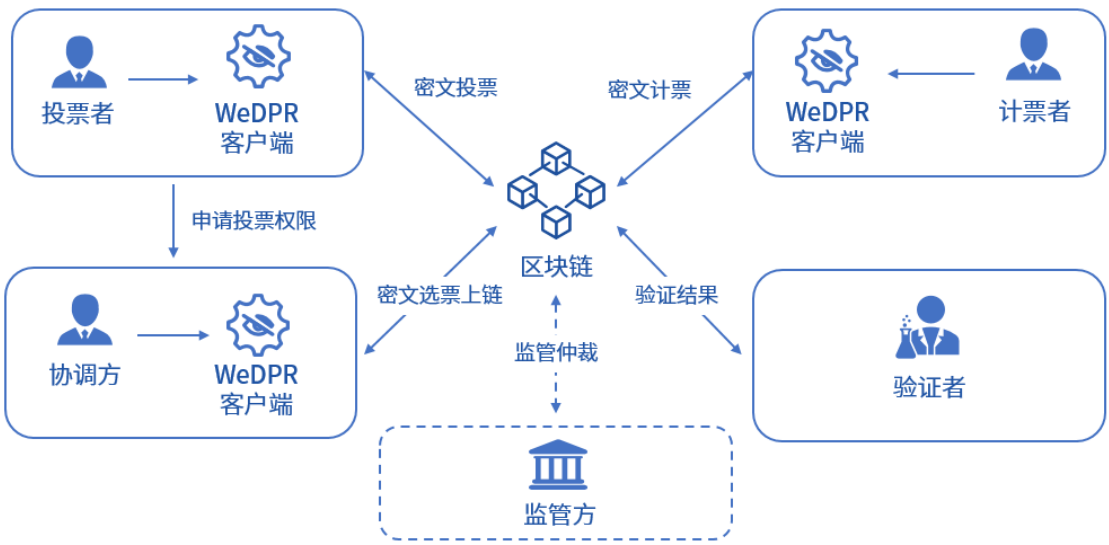
美丽本次借助匿名投票，彻底杜绝了身份隐私泄露的问题。第三方对投票者，即评价人一无所知，真正做到了匿名评价的效果。

在美丽的投票评价过程中，主要有三个参与方，分别为投票者、候选者和第三方平台。其中用户针对候选人填写评价或投票信息，转交给第三方平台。第三方平台完成计票和评价工作，将最终结果展示。通过匿名投票方案，可以让用户在本地对投票信息进行密文处理，第三方和计票者可以对选票的正确性进行验证，同时计算出最终结果，但是却无法获取用户投票的具体内容。因此，匿名投票方案有效保护了投票者的隐私安全。

4.3.1 匿名投票方案的优势

传统投票方案投票的隐私性和正确性都需依赖计票者的信誉。传统投票方案中计票者的权利极大，选票中包含敏感身份信息和选择信息，可能会直接影响投票人做出真实选择的意愿，从而影响投票结果的公平性和有效性。正如以下传统投票方案架构图所示，局限性总结如下。

相比之下，匿名投票方案依托密码学困难性理论，在全流程公开可验证的前提下，保护了投票过程中投票者的投票内容、投票身份等隐私安全。



WeDPR匿名投票方案基于密码承诺、零知识证明等算法，在不依赖可信第三方服务的前提下，支持多种常用投票方式和评价规则。投票过程中，投票者的身份和投票选择受到保护，投票者可独立验证自己投出的选票是否被正确计入结果，同时计票结果公开可验证。本方案支持以下七类角色，包括投票者、计票者、验证者、候选者、协调方、数据存储方和监管方。

表8. 匿名投票方案中的角色

角色	定义
投票者	有资格进行投票的选票所有者。
计票者	合作统计选票的多个主体。
验证者	对系统中所有数据及操作的正确性、合法性进行验证的主体。
候选者	被动接受选票的主体，不进行任何操作。
协调方	验证投票者是否具有投票资格，并为投票者生成空白选票的主体。
数据存储方	存储系统参数、投票者投票信息、计票者计票信息的主体。
监管方	有权利进行观察和仲裁的执行者。监管方可以获取投票过程中的细节，进行监管审查。

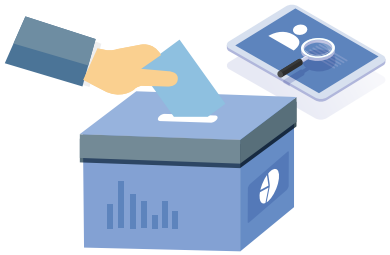
WeDPR匿名投票方案提供优异的隐私投票处理能力，实现了轻量化投票数据、较低交易延迟和高交易吞吐量的性能指标。支持千级投票处理并发量，每条投票记录仅为百字节大小以及投票处理结果毫秒级确认，最终实现如下隐私保护效果。

表9. 匿名投票方案效果表

隐私特性	隐私效果
身份认证	只有有资格的投票者才能投票。
防篡改	选票提交后不能被篡改、删除。
投票隐私	除了投票过程参与者，即投票者与候选者，第三方无法获知投票的具体细节，如投票者投出的选票内容等。
个人可验证性	投票者可对自己投出的选票进行全流程验证，包括是否被篡改删除、是否计入最终统计结果。
全局可验证性	除了投票者之外的所有人，都可对投票过程全流程进行验证与监督，包括所有空白选票与投出选票内容是否合法、所有投票者的投票交易过程是否正确、所有计票者的登记与统计过程是否正确、计票者最终公布的计票结果是否可信。

4.3.2 匿名投票方案在应用领域的探索

匿名投票可以应用于电子政务决议、团体活动投票、公司股东大会决议、明星海选投票、物业基金使用决策等诸多场景中，对数字化公平决议场景具备广大而深远的影响。



4.3.2.1 群智感知

群智感知是一种新型的数据获取模式，组织者将感知任务发布给用户，用户使用移动设备形成交互式的感知网络，从而完成数据收集、信息分析和知识共享的目标。然而，阻止用户参与群智感知一大主要原因是用户提供的一些敏感数据会泄露其隐私信息，包括文本、图像、音频、视频等多种类型的数据。因此保护用户提交的隐私数据是提高群智感知参与度的关键要素。

群智感知一般涉及到服务平台、数据使用者和任务参与者。例如，一个典型的群智感知景是收集用户的评分和评价。用户评分一般是非匿名的，对店铺评分可能会泄露用户隐私，商家和平台也可能互相勾结，通过恶意刷单来提高自己的商品评分，从而误导用户。匿名投票可以隐匿用户的身份信息，对用户的评分信息隐藏。在评价过程中全方位保护用户的身份隐私和数据隐私安全，使用户可以客观、公正地完成评价反馈流程。更重要的是，评价结果可以做到公开可验证，杜绝商家篡改最终评分，提高用户对平台和商户的信任度。匿名投票系统对用户的评价打分信息在监管合规下全方位保护用户的数据隐私和身份隐私安全，使用户可以客观、公正地完成评价反馈流程。

4.3.2.2 智慧城市

智慧城市指利用各种信息技术与创新概念，将城市的系统和服务打通、集成，以提升资源运用的效率，优化城市管理和服务，以及改善市民生活质量。截止 2017 年底，中国已有超过 400 个城市明确提出或正在建设智慧城市、预计 2021 年市场规模将达到 18.7 亿元。智慧城市的新信息化进程中，伴随着选举问题、投票问题的隐私性泄露风险直接影响用户参与建设智慧城市的意愿和最终结果的公正。

智慧城市中典型的决策模型，如小区物业管理电子投票，主要涉及到投票者和计票者。投票者的身份和投票数据的隐私性以及计票的正确性取决于计票者的信誉。由于投票内容包含敏感身份信息和决策信息，可能会直接影响投票人真实意愿，从而影响投票结果的公平性和有效性。针对这些隐私问题，匿名投票方案应运而生。匿名投票可以使投票者的身份和投票选择在满足监管仲裁的前提下，投票者可独立验证自己投出的选票是否被正确计入结果，同时计票结果公开可验证，能有效保护参与者的身份和投票数据隐私，从而提高用户的参与意愿。

4.4 选择性披露

随着人类活动的不断丰富，用户几乎每天都会被要求出示自己的属性凭证，进行相关认证。比如进入特定场所需要门禁验证、乘坐交通工具需要检票验证、打开手机需要密码、指纹或面部认证、登录系统需要用户名密码等验证。现在，让我们看看美丽又面临了怎样的凭证认证问题。

> 历经波折，美丽终于可以观看演唱会了。在入场大厅的门口，美丽开心地拿出了门票，交给了门口帅气的检票员。由于观看本场演唱会要求观众年龄大于18岁，检票员要求美丽出示身份证。美丽感到十分为难，帅哥面前丑照该不该亮?万般无奈之下，美丽最后只好拿出了自己的身份证，虽然顺利证明了自己的年龄，但是却让帅哥看到了当时木讷的自己，一整场演唱会下来，美丽都闷闷不乐。美丽决定穿越时空到入场前改变现实。

身份证由各国或地区政府发行予公民，并作为每个人重要的身份证明文件，包含了用户如居住地、年龄、号码等敏感信息。在进行身份认证时，选择将身份证上所有信息披露给第三方机构，往往是不必要的，甚至可能造成极大的安全隐患。在本次经历中，美丽通过身份证虽然证明了自己的年龄，但是同时也让自己的照片等信息被预期之外的人获得了。美丽决定穿越时空到入场前改变现实。

> **穿越时空**：美丽又回到了入场大厅的门口，这次，机智的美丽流利地说出了自己的身份证号，并且和票号上的号码进行了比对，顺利进入了演唱会。美丽愉悦观看了演唱会，又在帅哥面前展示了最好的自己，美丽十分开心和尽兴。然而，就在几天之后，美丽发现自己成为了某家破产企业的法人，原来美丽的身份证号和近况照片被不法分子获取了。美丽决定穿越时空，摆脱这个麻烦。

在进行身份验证时，用户既要证明相关属性满足验证条件，但同时也要避免泄露除认证要求之外的隐私信息。在本次经历中，美丽为了证明自己年龄大于18岁，选择说出了自己的身份证号码。这样做虽然可以供演唱会工作人员完成身份认证，但也泄露了敏感的身份证号码信息。

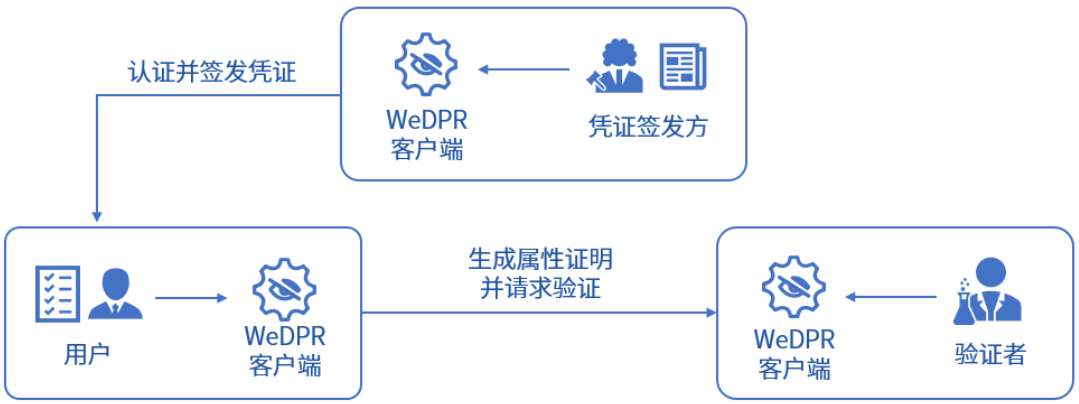
> **再次穿越时空**：美丽本次选择了采用选择性披露解决方案的认证系统，将年龄，票据等属性经过认证后生成了一个凭证。美丽利用颁发的凭证，然后披露自己的年龄和票据信息，生成了一个入场通行证。美丽这次站在入场大厅的门口，十分潇洒地使用通行证证明了拥有本场演唱会门票并且自己的年龄大于18岁，同时没有泄露任何自己的私密信息。最后，美丽顺利地观看了一场难忘的演唱会。

受限于交互代价和存储代价，传统数据认证应用在轻交互的场景中，只能支持捆绑认证，多项数据只能一同认证且一同披露明文，例如，个人身份认证证书包含了姓名、身份证号码、住址等敏感信息，但往往应用本身并不需要这些额外的隐私信息。选择性披露方案可以在不依赖可信第三方服务和可信硬件执行环境的重要前提下，支持任意类型的属性集合中任意子集的属性披露，并支持基于属性值的断言判断，实现最大化隐私保护效果。

在美丽使用的选择性披露方案中，有三个参与方，分别是用户、凭证签发方和验证者。其中用户提供相关属性供凭证签发方进行认证并颁发签名的属性凭证，用户利用属性凭证并选择性披露待验证的属性，然后生成属性证明，验证者使用用户提交的属性证明完成验证。选择性披露方案可以确保用户的相关属性经过签名认证，用户获取属性凭证后再出示给验证者时可以最小化披露。因此，用户在证明自身具备某些属性时又完美保护了属性的具体信息和未被披露的属性。

4.4.1 选择性披露方案的优势

WeDPR选择性披露方案依托密码学困难性理论，在全流程公开可验证的前提下，其属性认证和验证均由安全的算法协议保证。使用户可以最小化披露相关属性，而不泄露其他隐私数据，真正做到让用户隐私的控制权归还属主。选择性披露架构如下所示。



本方案支持以下三类角色，包括用户、凭证签发方和验证者。

表10. 选择性披露方案中的角色

角色	定义
用户	属性提供者，用户提供相关属性，由凭证签发方认证并签名，获取其生成的属性凭证。
凭证签发方	属性认证者，认证用户属性的所有权和真实性，并签发属性凭证。
验证者	属性验证者，用户通过属性凭证披露相关属性并生成属性证明，提供给验证者进行验证。

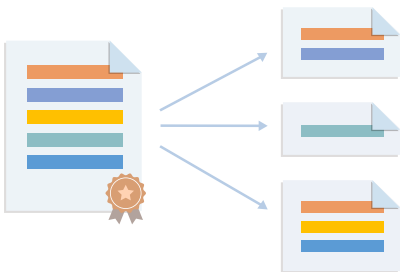
选择性披露方案支持任意类型属性的认证，可以毫秒级验证属性凭证，最终实现效果如下。

表11. 选择性披露方案效果表

隐私特性	隐私效果
身份认证	用户的身份需要进行认证，可以通过专门的认证机构或凭证签发方认证。
属性隐私	用户只需要披露其符合要求的属性，给出其生成的证明，让验证者通过验证即可，不会泄露其他未披露的隐私属性。其中断言型的披露方式，只会披露属性值满足某个范围，不会披露具体值。
不可伪造性	用户提供的属性，需要凭证签发方进行认证后才会生成属性凭证并签名。用户篡改签名后的属性凭证或者提供伪造签名的属性凭证均无效，验证将会失败。
不可链接性	用户会将签名属性凭证进行盲化，因此凭证签发方无法通过已发放的签名凭证与用户提交的属性证明进行链接分析，避免凭证签发方与验证者串通追踪特定用户的凭证使用行为，可以有效保护用户的隐私。
公开可验证性	验证者和公众通过凭证签发方的公钥均能验证用户提供的属性证明，实现全局公开可验证。

4.4.2 选择性披露方案在应用领域的探索

选择性披露方案可以应用于身份认证，资质认证等领域中，对提升用户和服务提供者互信时、提升用户对个人信息的掌控力度、推动电子凭证化等场景落地都具有深远的影响。



4.4.2.1 私密数字凭证

数字凭证作为认证机制中重要的一环，在背景调查、政务处理、数据共享等场景中都具备重要地位。截止2019年，全世界企业信息存量已经超过1亿家。数字资质证明本质是一种数字凭证，一般需要凭证颁发机构进行认证签发。企业提供有效的认证数字资质证书供相关机构进行验证，但验证时往往不需要提供数字资质证书中的全部信息。另外，数字资质证书易出现作假、资质变更困难、资质信息泄露等诸多问题。

数字资质认证流程中一般涉及到用户、凭证签发方、验证者。数字资质证书需要被设计为一种私密数字凭证，凭证签发方认证并颁发私密数字凭证，用户提供私密数字凭证供验证者验证。选择性披露方案是实现私密数字凭证行之有效的方案，能有效保证用户持有监管授信的私密数字凭证具备私密性和有效性，同时允许用户证明自身具备某些属性时又完美保护了属性的具体信息和未被披露的属性。WeDPR 选择性披露方案目前已经集成到由微众银行自主研发的 WeIdentity 分布式身份解决方案中。

4.4.2.2 智慧医疗

智慧医疗是通过先进的信息技术，打造健康档案区域医疗信息平台，从而实现患者与医务人员、医疗机构、医疗设备之间的高效互动，逐步达到信息化的医疗解决方案。2020 年预计全球主要地区医疗支出将超过 8.7 万亿美元。然而，巨大的医疗消费背后带来了巨大的患者隐私信息管理问题。据报道，2017 年医疗数据外泄事件对机构造成的平均成本达每事件 362 万美元。由此可知，随着智慧医疗的建设，患者的身份和病例相关等重要敏感数据流动与共享进程的加剧，数据隐私保护问题将更加严峻。

以员工病假审批场景为例，一般流程涉及到到员工、医院和公司等实体。医院为员工认证身份和病例相关重要信息，公司可以通过认证身份和病例信息进行验证，之后进行病假审批。在整个认证和验证过程中，员工的身份和病例信息在医院与公司之间流动与共享。为了满足公司的病假申请请求，员工可以选择性披露公司要求的病例信息，而不用呈现全部既往病史。选择性披露方案聚焦人性化用户隐私数据管理需求，让数据的所有权和使用权在监管可管的前提下回归用户。

结语

“科技聚焦人性
隐私回归属主

WeDPR愿景

回顾前文，不难看出落实隐私保护并不是一个纯粹的技术问题。隐私保护所涉及的技术领域之广，学科门类之多，体现了其作为一项高层次人性需求的内在复杂性。如果将由数据驱动的现代信息化社会想象成一个生机勃勃的非洲大草原，流通的数据就是草原上形形色色的动物，而隐私保护扮演的就是草原的协调者，致力于避免数据的价值因被个别物种过渡捕猎而导致数据生态系统的停滞不前甚至退化衰败。对于个人而言，作为隐私数据的生产者，通常希望能自主选择是否通过分享数据获得低价甚至免费的权益，但他们并不期望因此承受意料之外的隐私风险，更不希望陷入隐私泄露发生之后无能为力的境地。对于企业而言，同时作为数据的生产者和消费者，可以通过向其他消费者分享数据直接获得收益，也可以试图与其他生产者协作从而实现更大范围的数据融合和价值创造，但他们也会顾虑在分享数据的过程是否自己获得合理的利益分配，以及是否会因此削弱自身的核心竞争力。

正如之前章节中虚构角色“美丽”的故事中所展现的，以上这些风险真实存在，而且离我们并不遥远。如果隐私保护缺位，丰饶的数据大草原就可能不幸退化。数据属主作为隐私数据的生产方，如果不能对自身隐私数据使用进行合理的控制并实现公平的价值交换，势必会打击数据属主生产高质量数据的积极性，依赖对应数据的业务就会受到冲击，对应产业生态难以健康可持续的发展，以此构建的负反馈数据轮回，也终将对数据属主自身的潜在权益造成损害。整个商业体系中每一位参与者的权益都可能因未能有效落实隐私保护蒙受不必要的损失。

由此可见，隐私保护技术成功产业化的核心目标在于保障多方权益的平衡，平衡数据生态系统中各个参与者的价值公平分配，平衡每一次价值交换中的当下收益和潜在风险。只有一个平衡的数据生态系统，才有可能建立起正反馈数据轮回。通过吸引更多的参与者自发地加入数据生态系统，合规可控地分享自己隐私数据，获取合理的权益，规避不必要的风险。最终达成数据价值的高效融合创新和持续性良性增长，这也正是我们推出WeDPR隐私保护高效技术方案的愿景。

WeDPR隐私保护高效技术解决方案，基于微众银行在普惠金融领域多年宝贵的实践经验，坚持科技聚焦人性的设计理念，充分考虑场景中各个参与者切身权益诉求，提供即时可用的开发集成体验。作为开放隐私保护技术能力的初步探索，本文中提及四类业务场景只是一个开篇，WeDPR将来会容纳更多元的业务场景、扩展更丰富的隐私保护业务需求。我们诚挚地希望能够以此科技手段真正落实公开可验证的隐私保护效果，在隐私回归属主的同时，合法合规地激励商业创新，形成价值传递的正向反馈，构建数据生态系统的多方平衡，最终实现所有参与者收益公平分配和资源最优配置。

WeBank
微众银行

We Defend
We Protect
We Respect

官网：https://fintech.webank.com/wedpr

商务咨询：wedpr@webank.com