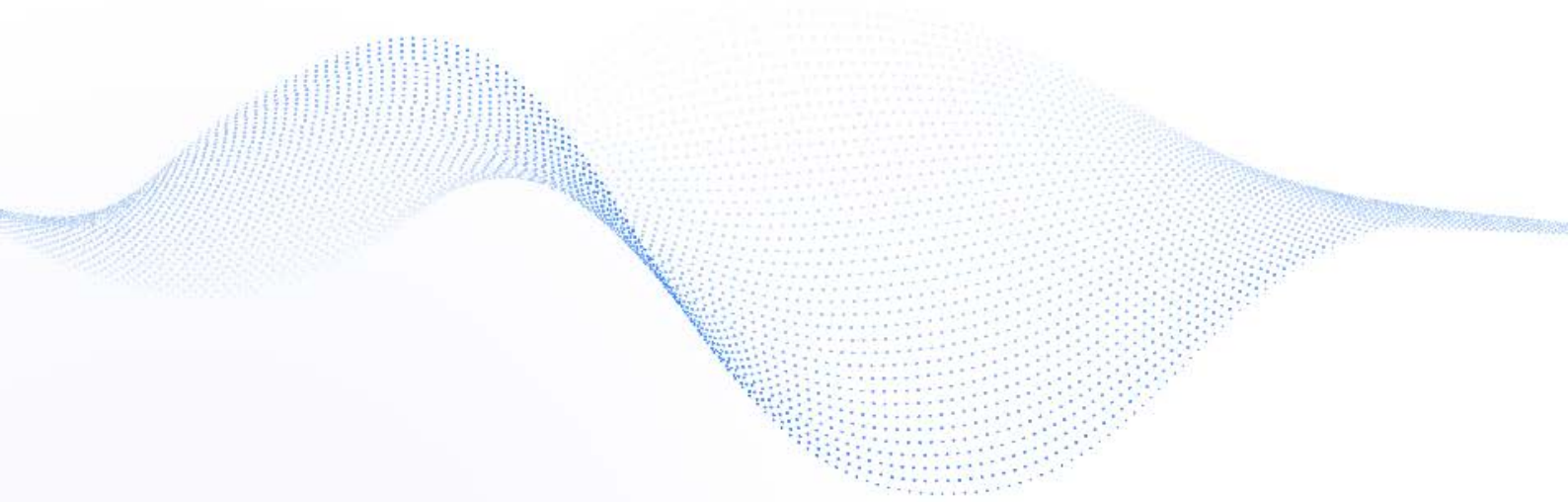
ABS
AI BLOCKCHAIN SECURITY

AI BLOCKCHAIN SECURITY
白皮书



目录 | CONTENTS

一、摘要

不论阿里巴巴还是 Facebook，其数万亿市值很大程度来源于积累的数据。不夸张地讲，“数据比自己更了解自己”，这也是促使不同主体间进行数据交换、互通、共享的原动力，同时在利益的驱使下，也滋生了一系列相关问题。各国政府纷纷出台相应的数据保护法律法规（欧盟的 GDPR 及中国的网络安全法等），已经深刻认识到问题产生的根本原因在于，数据源头没有得到真正属于自己的数据权力。而数据权利，如分享权、收益权都是建立在所有权基础之上的。归根到底，是数据确权与用权的博弈问题。

ABS 链（A：AI；B：Blockchain；S：Security）是基于区块链解决数据确权和用权问题的底层通用技术平台，旨在通过加密数据信息以及加密密钥去中心化分发，实现数据信息的定向分享传播，并借用人工智能技术实现数据信息撮合交易。通过解决中心化数据巨头对数据的威胁，ABS 链将成为去中心化数据基石，汇聚的数据价值甚至可能超越现有中心化数据巨头。

二、我们

ABS 基金会致力于 ABS 链的发展与运营，通过聚集技术及应用方面的各类主体，形成自我发展的数据采集、保护和交易生态。

ABS 链团队牵头并主导了多条联盟链的研发和搭建，在区块链和数据加密方面，有着雄厚的技术积累和过硬的实力。

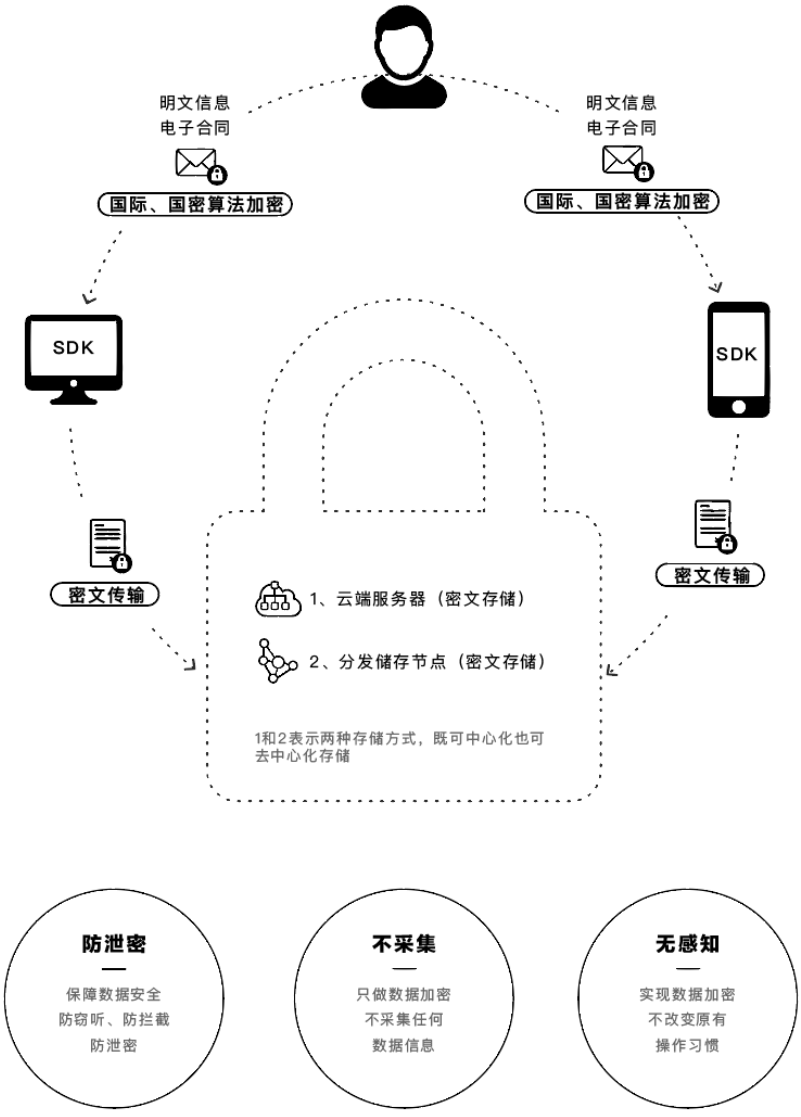
ABS 链研发团队包括 2 位数据加密及信息安全方向的博士，1 位人工智能方向博士，12 位工作经验 10 年以上的资深研发工程师，专注于数据加密及信息安全的团队成员达 32 人。

三、技术

3.1 核心问题

3.1.1 成为数据真正的主人——如何做到数据确权，数据加密

各国出台的数据信息保护相关法案从法律层面上明确了数据权利应该归数据产生者所有。要真正实现这一点，首先要解决的核心问题是如何把数据保护起来。只有数据被保护起来了，不再是任何人都可以轻而易举地获得想要的任何数据信息，数据产生者才能切实地享有其在数据之上的权利。ABS 链从技术和法律两个层面对数据进行保护：



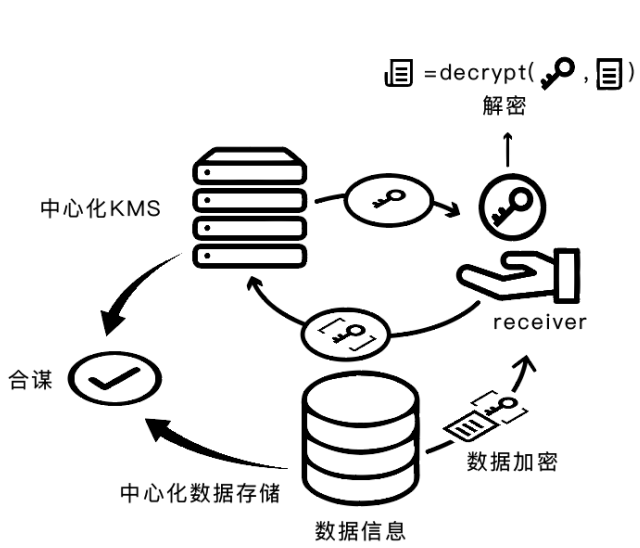
在技术层面上。ABS 链同时支持国际及国密算法，提供专业的安全加密服务，让数据在处理（存储、传输、分享、交易等）过程中都确保是加密状态，实现从端对端的全过程加密。除了数据所有者，任何第三方都无法查看，确保数据的安全性和私密性。

在法律层面上。用户使用 ABS 链处理各类数据都会直接形成电子合同。而电子合同，顾名思义，是以电子的方式订立的合同，是合同的电子化表现形式，同样具有法律效力。这样以来，用户的数据权力便可通过这种方式切实地被法律保护起来，改变了以往权责模糊不清的情况。

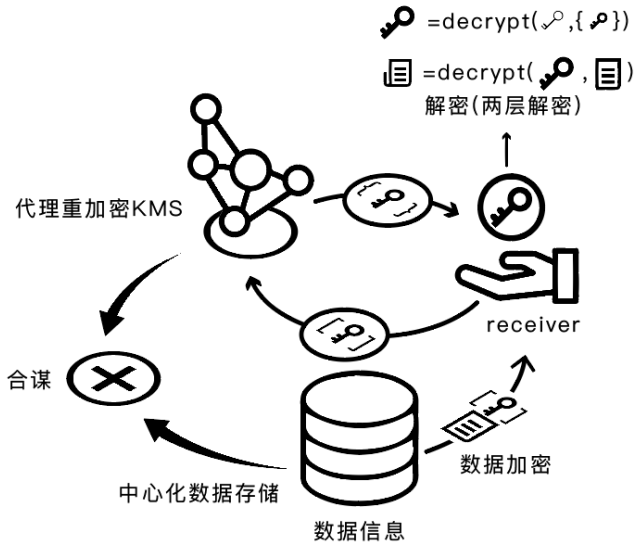
另外，值得注意的是，现有技术无法保证数据不被复制（截图、拍照、录影等手段）以及二次传播。但基于区块链技术的 ABS 链可以对数据溯源，确认数据所有权和流转路径，可以改变以往无证可寻、无据可查的情况，从而构建更加可信的数据交易环境。

3.1.2 让数据产生收益——如何做到用权（分享权、收益权）

数据确权是数据用权的基础，而数据用权才能让数据发挥更大的价值，实现这一目标的一般做法是建立密钥管理系统（KMS）。密钥管理系统是在设备和应用程序中生成、分发、流转和管理密钥的集成方案（下图）。



（a）中心化KMS



（b）代理重加密KMS

传统的密钥管理系统存在一些问题，如上图（a）所示，如果同时把加密的数据信息以及加密密钥都放在中心化的服务器上，那么就存在两家中心化服务商合谋的可能。如此，用户的数据并不是 100% 安全，仍然存在被盗用的风险。

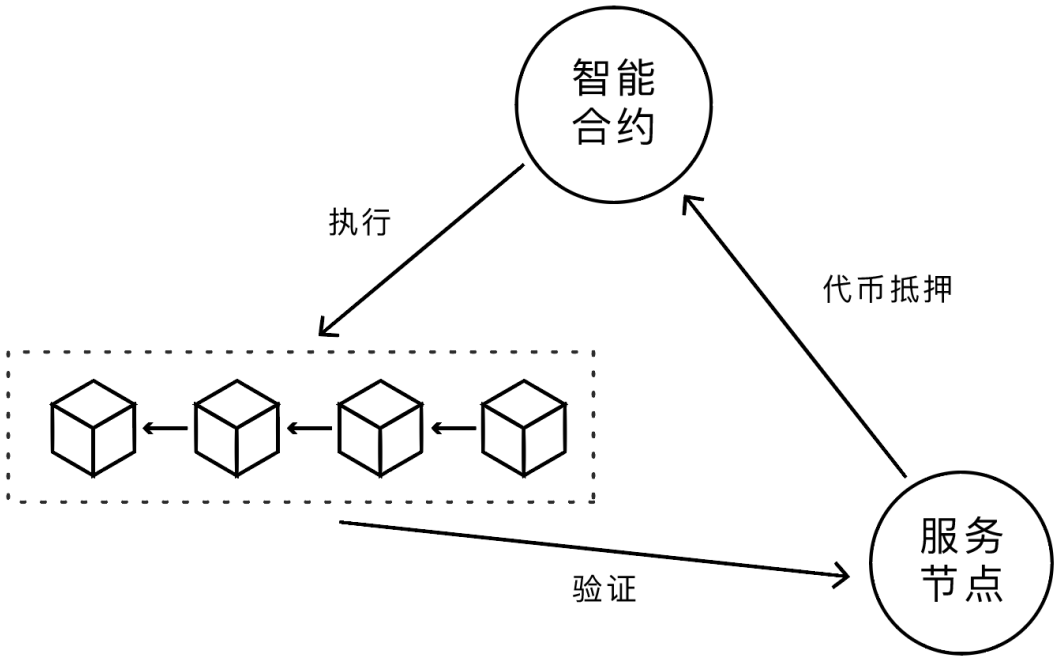
比特币和以太坊等去中心化共识网络，在解决这种中心化的难题方面很有前途。回顾上图，传统密钥管理系统涉及到两个中心化的存储服务器。

第一，用区块链技术移除存储数据信息的中心化服务器，即数据信息上链。但这样的做法需要考虑成本和效率问题，即数据信息随着时间的推移会越发庞大，这就要求整个区块链网络有足够大的存储空间以及高效的运行性能。同时还需要保证通过节点访问链上数据信息不会发生中断的情况。

第二，用区块链技术移除存储密钥的中心化服务器，即密钥上链。ABS 链采用的正是此方法。ABS KMS 是利用代理重加密技术，使用区块链分布式网络，建立的分布式密钥管理系统（如上图 b 所示）。与中心化的密钥管理系统相比，它不需要信任中介服务商，使得用户在公共网络上共享私有敏感数据成为可能。

3.2 ABS 链

3.2.1 共识与智能合约



为了解决数据确权及用权导致的高并发问题，ABS 链采用三权分立原则，其中 POWS 链是议会，智能合约是法院，服务节点是行政机构。数字世界是三权分立的理想国，三权可以被严格执行到位。在数字世界里任何行为必然留有证据，智能合约不存在模糊空间，而服务节点可以随意被替换，并且可以同时使用多个服务节点。节点缔结智能合约并抵押一定量代币后成为服务节点，代币抵押数量影响了用户对节点的信任度；用户选择或者网络为用户随机选择多个服务节点；

ABS 链通过周期性验证、随机验证和用户举报提升服务节点的诚实度。

任何服务节点抵押的代币，只有在服务节点被周期性校验 6 次后才能释放。因为 POWS 链只进行验证工作，高并发的工作由服务节点承担，理论上并发量没有上限。

ABS 链采用 POWS 的共识机制，即基于权益的工作量证明机制，通过改造升级以太坊的 POW 机制实现。另外，借鉴 LISK，我们在 ABS 链上构建基于 JavaScript 的智能合约机制。JavaScript 是主流的脚本语言，为程序员所熟悉，利于智能合约的快速开发。

任何基于 ABS 链提供服务的节点均需缔结智能合约，并发送一定数量的代币到合约账户。用户可以观察到节点所抵押的代币价值，进而评估是否能够信任节点。代币抵押更有利于节点提供高效、可靠和专业的服务，推动 ABS 生态的健康发展。

3.2.2 密钥分发节点

ABS 链中的任何节点都可以申请成为密钥分发节点，前提条件是在主网缔结智能合约，并抵押一定数量的代币，数量由节点自行决定。密钥分发节点抵押的代币数量公开可查，用户自行决定是否让某一节点提供密钥分发服务。如果用户没有明确指定密钥分发节点，ABS 链以下述方式为用户随机选择节点：

设第 个节点抵押的代币为 m_i，则密钥分发抵押的代币总额为：

$$M = \sum_{i=0}^{N-1} m_i \tag{1}$$

其中， N 为总的密钥分发节点数。若采用 重代理重加密，节点被选中的概率为：

$$p_i = \frac{\tau m_i}{M} \tag{2}$$

τ 重代理重加密必须有 τ 个密钥分发节点，如果随机选择过程中出现相同节点则重新选择。根据公式 (2)，节点抵押的代币数量越多则越容易被选中提供密钥分发服务。

3.2.3 ABS 网络运营节点

由于 ABS 相较法币会出现波动，用户直接向网络支付 ABS 获取服务的体验较差。我们在 ABS 链中引入 ABS 网络运营节点。用户以月费、年费或单次向 ABS 网络运营节点购买服务。ABS 网络运营节点保障用户在服务期限内的网络使用。节点抵押一定数量的代币缔结智能合约后成为 ABS 网络运营节点。ABS 网络运营节点收取月费或年费后需将提供服务所需的 ABS 数量发送到合约账户。用户自行决定向哪个 ABS 网络运营节点购买服务。如果用户没有明确指定运营节点，ABS 链以下述方式为用户随机推荐节点：

设第 i 个节点抵押的代币为 m_i，未到期服务所需的代币为 d_i，有运营节点总抵押代币量为：

$$D=\sum_{i=0}^{N-1}(m_i-d_i) \tag{3}$$

其中，N 为总的密钥分发节点数。若采用 τ 重代理重加密，节点被推荐的概率为：

$$q_i=\frac{(m_i-d_i)}{D} \tag{4}$$

3.2.4 数据交易撮合节点

ABS 链完成数据的确权和用权，必然汇聚大量的数据，从而形成庞大的数据交易需求。任何节点在抵押一定数量的代币缔结智能合约后，均可成为数据交易撮合节点。数据交易撮合节点可以是通用数据交易，也可以是专业数据交易。节点被推荐的概率取决于专业领域及代币抵押数量，同一专业领域代币抵押数量多的优先。

3.2.5 节点监督机制

节点以一定的频率向 ABS 链提交验证数据推动智能合约的执行。令 ABS 链一个验证周期为 T 秒，每秒并发量为 T，总抵押代币数量为 M，第 i 个节点抵押代币数量为 m_i，ABS 链的 $\frac{nT}{2}$ 次交易用于执行智能合约，第 i 个节点在周期 T 内的验证次数为：

$$k_i = \frac{m_i nT}{2M} \tag{5}$$

因此：

$$\sum k_i = \frac{nT}{2} \tag{6}$$

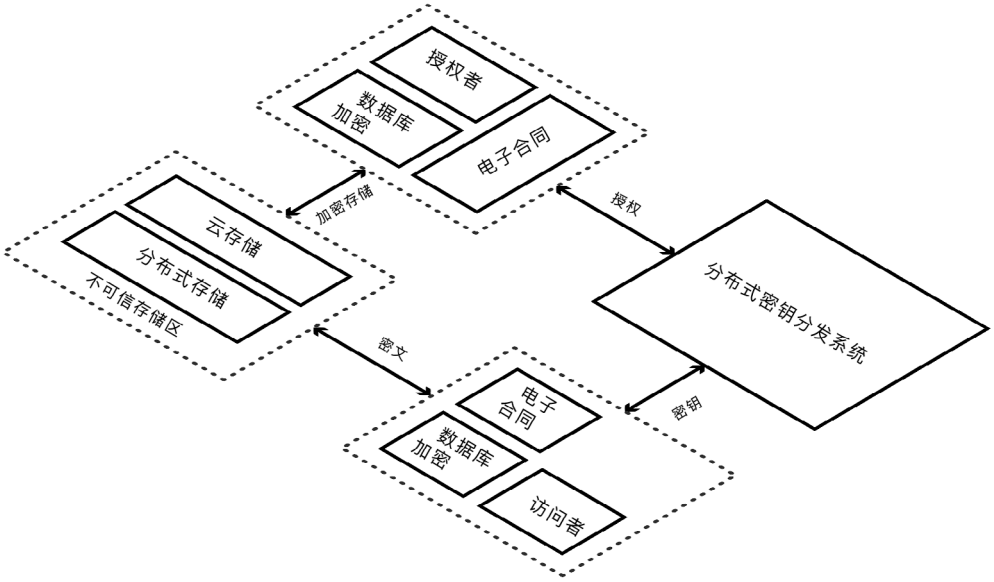
ABS 链的 $\frac{nT}{4}$ 次交易用于以随机抽样的方式验证节点。根据大数定律，造假节点的分布将呈正态分布，我们初期将基于重要性采样方法构建无偏和一致估计器。

例如，ABS 链的并发量为 20TPS，验证周期为等价于 24 小时的区块时间，则总的验证次数为 172.8 万次，可以构建无偏和一致估计器。

ABS 链的 $\frac{nT}{4}$ 次交易用于采集用户举报数据对节点进行审判。

ABS 链上的用户数据均已嵌入认证数据结构，且根哈希被区块链所记录，无法被篡改。节点造假在在认证数据结构的验证下无可抵赖。在 ABS 链的周期验证及随机验证下，结合用户举报，对节点形成强力的监督机制，从而构建高并发可信的区块链底层。

3.3 数据确权与用权组件



基于 ABS 区块链网络，我们构建数据确权及用权组件。数据确权及用权组件包括分布式密钥分发系统、数据库加密和电子合同三个组成部分。分布式密钥分发系统（DKMS）通过区块链网络解决中心化 KMS 可能存在的包括合谋造假等恶意行为，从根本上保障数据用权符合用户预期。数据库加密解决加密存储后，数据在密文状态下的处理难题。电子合同则通过法律手段解决数据解密后被恶意分发问题。

3.4 分布式密钥分发系统

3.4.1 双线性对定义

G_1 是阶为素数 N 的加法循环群；G_2 是阶为素数 N 的加法循环群；G_T 是阶为素数 N 的乘法循环群；P_1 是 G_1 的生成元；P_2 是 G_2 的生成元；存在 G_2 到 G_1 的同态映射 ψ 使得 $\psi(P_2) = P_1$；双线性对 e 是 $G_1 \times G_2 \rightarrow G_T$ 是 G_1 的映射，满足如下条件：

双线性性：对任意的整数 i 和 j 有，$e([i]P_2,[j]P_1) = e(P_2,P_1)^{ij}$；
非退化性：$e(P_2, P_1) \neq 1_{G_T}$;

可计算性：对任意的 $P \in G_1$，$Q \in G_2$，存在有效的算法计算 $e(P,Q)$。
本部分所用的双线性对定义在椭圆曲线群上，本文主要指 opt–Ate 对。

3.4.2 双线性对安全性

双线性对的安全性主要建立在以下几个问题的难解性基础之上：

问题 1：对 $a,b \in [1, N\text{-}1]$，给定 $([a]P_1,[b]P_2)$，计算 $e(P_2,P_1)^{b/a}$ 是困难的。

问题 2：$a,b,r \in [1, N\text{-}1]$，区分 P_1，P_2，$[a]P_1$，$[b]P_2$，$e(P_2,P_1)^{b/a}$ 和 P_1，P_2，$[a]P_1$，$[b]P_2$，$e(P_2,P_1)^{r}$ 是困难的。

问题 3：对正整数 τ 和 $x \in [1, N\text{-}1]$，给定 P_1，$[x]P_1$，P_2，$[x]P_2$，…，$[x^{\tau}]P_2$，计算 $e(P_2,P_1)^{1/x}$ 是困难的。

问题 4：：对正整数 τ 和 $x \in [1, N\text{-}1]$ 和，给定 P_1，$[x]P_1$，P_2，$[x]P_2$，…，$[x^{\tau}]P_2$ 和问题 2 的确定算法，计算 $e(P_2,P_1)^{1/x}$ 是困难的。

3.4.3 基于双线性对的代理重加密方法

我们以 opt–ate 对为基础，设计代理重加密方法，具体如下述：

令 A 为数据拥有方，B 为被 A 授权的数据访问方，C 为代理重加密服务方；其中，A 的私钥 $sk_a = a$，公钥 $pk_a = [\frac{1}{a}]P_1$，B 的私钥 $sk_b = b$，公钥 $pk_b = [\frac{1}{b}]P_1$；

1) 明文为 m，随机数 t，用 A 的私钥加密获取密文：

$$C_a = (C_{a1}, C_{a2}) \tag{7}$$

$$C_{a1} = m \oplus e(P_2,P_1)^t \tag{8}$$

$$C_{a2} = [t][\frac{1}{a}]P_2 \tag{9}$$

2) 基于 A 的私钥和 B 的公钥，则有 A 授权给 B 的代理重加密密钥：

$$rk_{A\to B} = [a]pk_b \tag{10}$$

3) 通过 $rk_{A\to B}$ 可将 C_a 可 B 的私钥解密的密文：

$$Z = e(C_{a2}, rk_{A\circledR B}) = e([t][\frac{1}{a}]P_2,[a]pk_b) = e(P_2,P_1)^{t/b} \tag{11}$$

4) 用 B 的私钥对 C_a 进行解密：

$$m = C_{a1} \oplus Z^b \tag{12}$$

3.4.4 多重代理重加密方法

用户 A 可能需要取消对用户 B 的访问授权，因而要求代理方 C 删除代理重加密密钥 $rk_{A\to B}$。如果此时代理方 C 与被授权用户 B 合谋，则代理方可能私自保留代理重加密密钥 $rk_{A\to B}$。为了避免代理方与被授权用户合谋，设计多重代理重加密方法引入多个代理方，并通过区块链网络的经济奖惩机制解决合谋问题。多重代理重加密方法如下述：

1) A 授权给 B 的代理重加密密钥可分解为 N 个代理重加密密钥：

$$rk_i = [a_i]pk_i \ , \ i \in [0, N-1] \tag{13}$$

有：

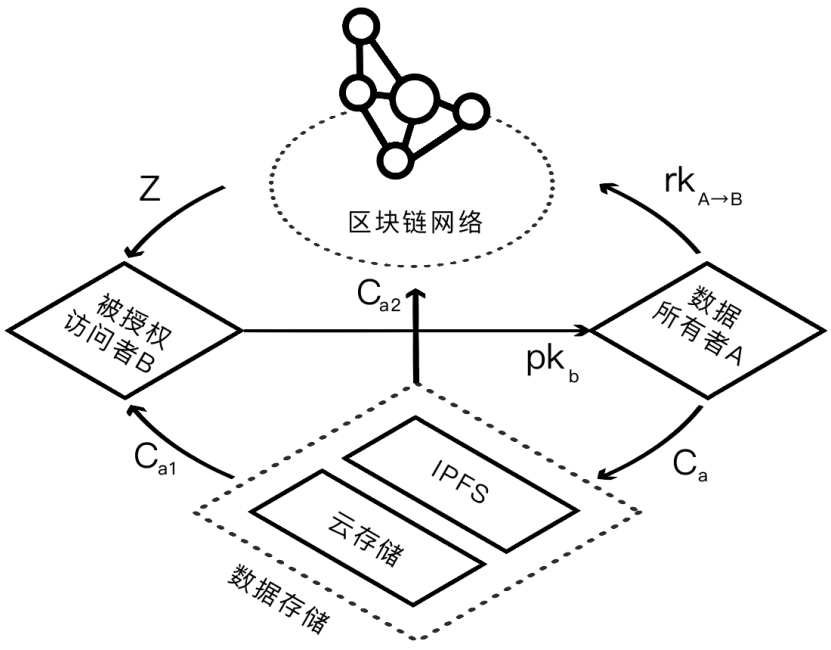
$$a = \sum_{i=0}^{N-1} a_i \tag{14}$$

2) 通过 rk_i 可将 C_a 转化成 C_b， C_b 仅能被 B 的私钥解密：

$$Z = \prod_{i=0}^{N-1} e(C_{a2}, rk_i) = e(P_2, P_1)^{t/b} \tag{15}$$

由此可对用 B 的私钥对 C_a 进行解密。

3.4.5 分布式密钥分发流程



我们基于多重代理重加密方法构建分布式密钥分发系统，密钥的分发流程如下述：

数据所有者 A 用私钥 a 生成密文 C_a 并存储到 IPFS 等分布式存储系统，或者阿里云等云存储系统；

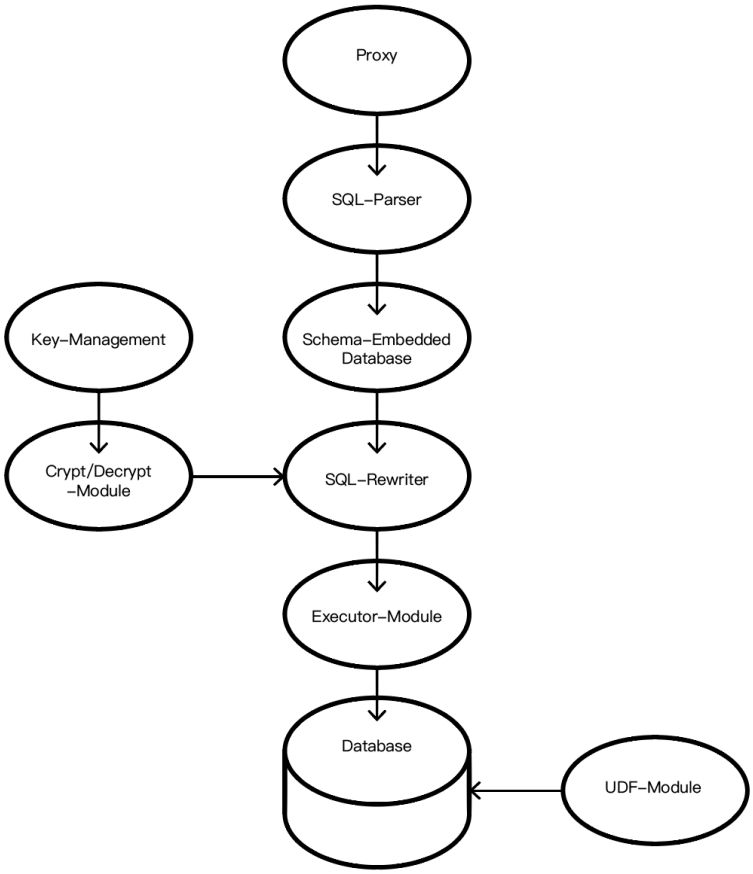
数据所有者 A 根据授权需求，基于 B 的公钥 pk_b，生成代理重加密密钥 $rk_{A\to B}$，并根据安全性需求拆分成多重代理重加密密钥 rk_i，$i \in [1, N\text{-}1]$，而后把相应的 rk_i 传递给区块链网络中的密钥分发节点；

被授权访问者 B 在申请访问 A 的加密数据时，密钥分发节点根据 rk_i 和 C_{a2} 生成 Z， 并将 Z 返回给 B；

被授权访问者 B 用私钥 b、C_{a1} 和 Z 解密获取明文 m。

3.5 数据库加密

数据库加密主要解决密文状态下的数据处理问题。目前数据库主要由 SQL、NOSQL 和 NEWSQL，其中 SQL 使用范围最广，前期我们主要用 SQL 去支持其他两种。数据库加密主要由 Proxy 模块、SQL-Parser、Schema-Embedded Databse、Key-Management、Crypt/Decrypt、SQL-Rewriter、Executor 以及 UDF 等构成，具体如下：



1）前端代理 (Proxy 模块)

应用程序通过前端代理模块与数据库连接，在数据库连接过程，用线程 id 来标识各个连接，在连接后初始化环境 , 建立嵌套数据库 (Embedded database), 保存 SQL 执行的各种语句以及 Schema 信息。

2）SQL–Parser

前端模块将从应用程序获取的 SQL 语句信息交给 SQL–Parser 模块，SQL–Parser 模块将标准的 SQL 语句解析成 LEX 语法结构。

3）Embedded–Database

Embedded–Database 是嵌套数据库，主要用来保存数据库的 Schema 信息以及 SQL 语句的执行情况以及各个敏感字段的加密信息，比如 key，加密洋葱层等。

4） Key–Management

Key–Management 主要提供 key 的管理模块，包括与 KMS 对接，产生各个 column 的洋葱层的 key，以及 key 的更新、销毁、备份功能。

5) Crypt/Decrypt 模块

结合 Key–Management 模块获取各个 key 信息，Crypt/Decrypt 主要提供加密与解密服务，该模块不但包含通用加密算法，还包含各种支持密文运算的算法，比如 Paillier/OPE(Order–Preserved Encrypt)/SWP/ORE 等算法。

6) SQL–Rewriter

SQL–Rewriter 模块主要对 sql 语句进行改写，结合 schema 信息以及加密模块对 sql 语句进行加密和改写。对创建数据库的语句，embedded database 保存 schema 信息；对插入数据的语句，rewriter 模块结合配置的敏感字段，对敏感字段采取支持密文运算的加密算法进行加密，比如是整数数据类型，可以使用 paillier 加密算法进行加密，此加密算法支持加减乘除运算，将加密后的结果存储到数据库中。当 SQL 语句是计算和 / 平均值时 , 可以通过 sql–rewriter 模块将计算的列选定为经过 paillier 加密后的列。

7) Executor 模块

将重写后的 SQL 语句，经 Executor 模块连接数据库执行 sql 语句

8) UDF 模块

UDF 模块主要是利用数据库提供的用户自定义函数，对加密后的数据进行处理。

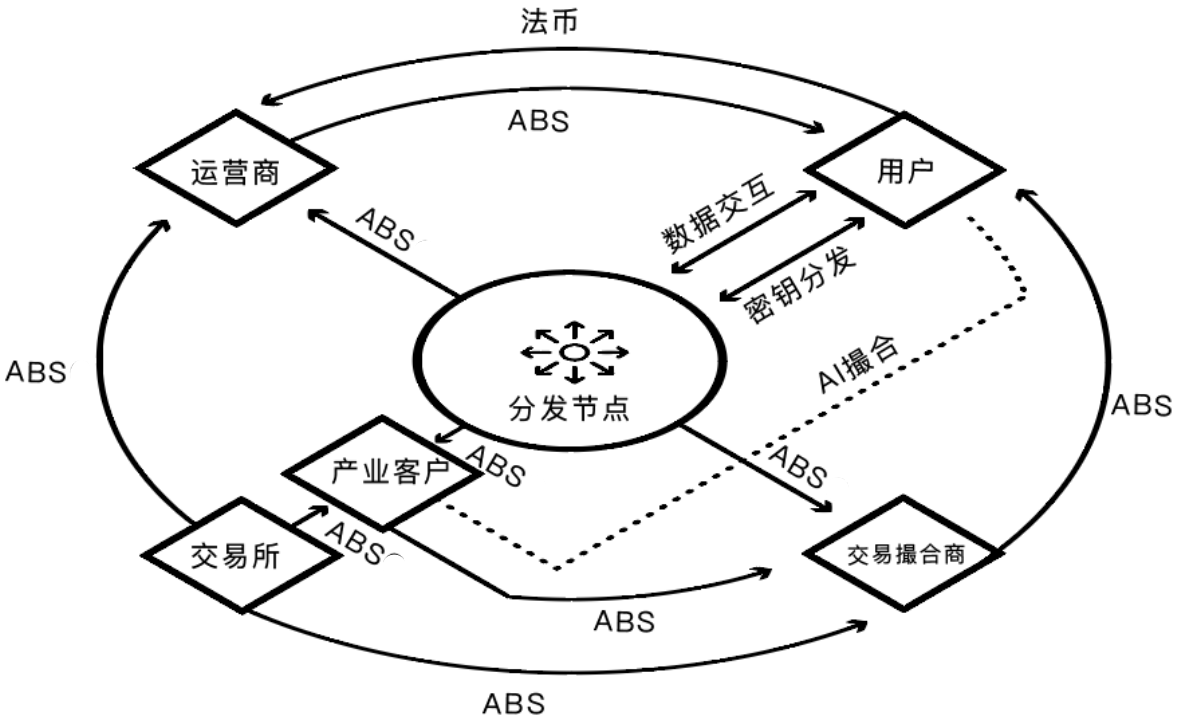
3.6 电子合同

根据《合同法》第十一条规定，采用数据电文形式订立的合同与传统的纸质合同一样属于书面合同，也即宏观上《合同法》认可电子合同形式上的有效性。电子合同技术已经得到广泛应用，我们将在系统集成开源的电子合同框架，同时接入其他厂商的电子合同系统，由用户自行选择。

四、经济

4.1ABS 链——数据经济生态的基石

ABS 链作为数据经济生态的基石，实现了数据信息加密、密钥链上分发以及数据撮合交易，为数据经济生态各方参与者提供了基于区块链去中心化网络的数据确权、用权的底层通用技术平台，让数据在得到保护的前提下实现其价值。



系统图

4.1.1 不同角色参与 ABS 链数据经济生态分析

用户在生态内对数据信息进行确权和用权：通过支付法币从运营商获得 ABS，然后支付给分发节点，用作分发节点的密钥管理和分发的报酬；通过授权第三方使用数据信息获得 ABS。

运营商通过锁定 ABS 参与生态建设，给用户提供更方便的数据信息保护服务，同时提供生态内 ABS 的流动性支持。

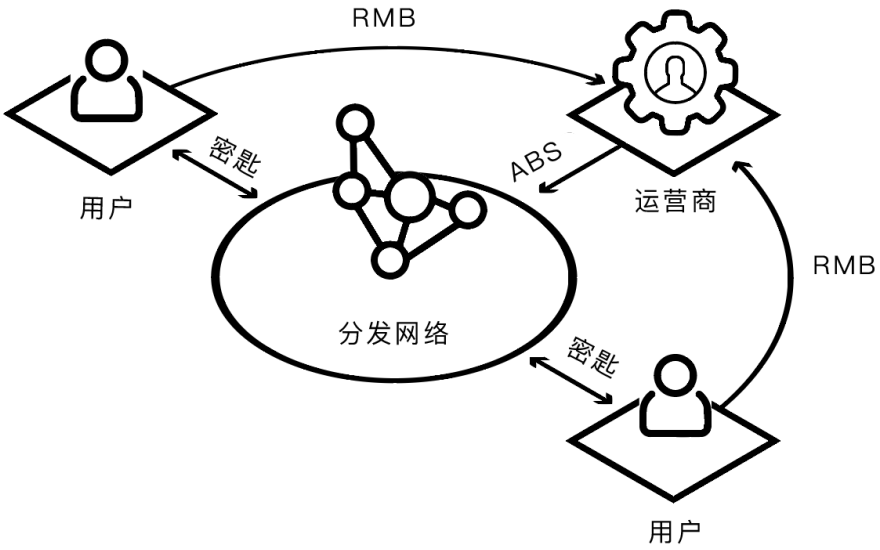
交易撮合商通过锁定 ABS 参与生态建设，其将会借助底层 AI 技术进行交易撮合，给数据需求方提供更具性价比的数据信息服务。

产业客户通过锁定 ABS 并支付 ABS 获取目标数据信息。

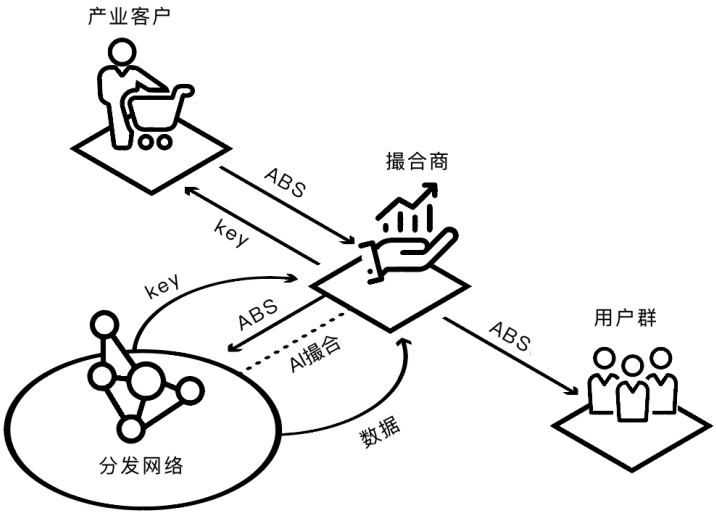
分发节点通过挖矿维护去中心化网络的正常运作，给用户提供存储和分发服务获取 ABS。

4.1.2ABS 链数据经济生态子场景

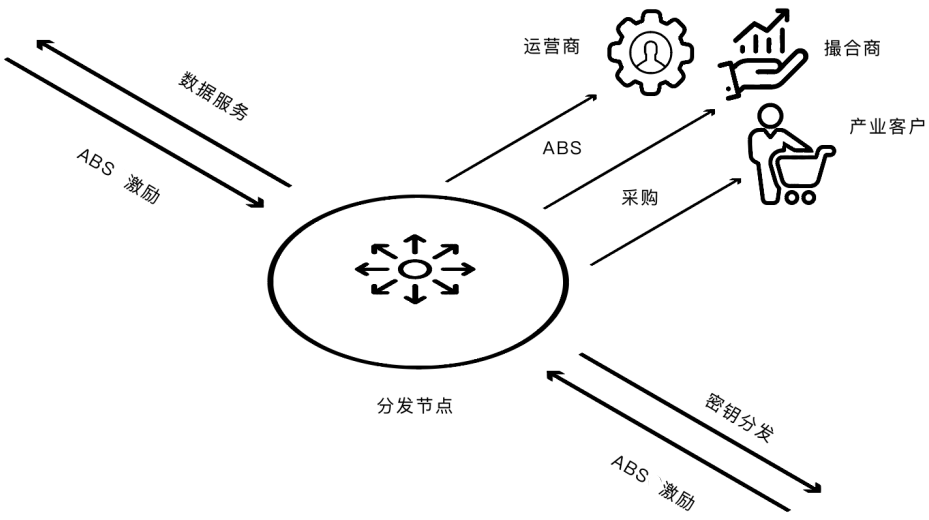
（1）密钥分发。运营商在整个网络中协助完成用户的密钥分发：用户需用法币支付密钥分发和管理的服务费给运营商，运营商在用户申请密钥分发请求时支付 ABS 给分发网络。



（2）撮合交易。产业客户向交易撮合商支付 ABS 同时发起数据使用申请，交易撮合商借助 AI 技术进行自动匹配撮合，用户在同意请求并提供数据后收到 ABS 报酬，产业客户通过分发网络获得密钥。



（3）分发节点激励。分发节点通过提供密钥分发和数据服务获得 ABS 激励，运营商、交易撮合商和产业客户向分发节点采购 ABS。



4.2 ABS 链数据经济生态的特征

4.2.1 安全

用分布式网络移除对中心化服务提供商的信任，使用代理重加密提供密码访问控制，使用代币激励机制保证可靠性，可用性和正确性。由于使用代理重新加密，未加密的对称密钥（能够解密私有数据）绝不会在服务器端，并且没有单点安全失败。即使被攻破，黑客也只能得到重新加密的密钥，并且对文件的访问仍然受到保护。

4.2.2 离线交易

代理重加密允许数据提供方和需求方在访问管理和解密权限之间拆分信任，而无需引入始终在线的始终可信的实体（如传统的密钥管理系统），有助于数据经济生态的落地。

4.3.3 去中心化网络

分布式密钥管理和分发网络使用共识网络安全存储，解决了操作私有加密数据的痛点，分发节点的部署降低了目前数据信息存储的成本，并让激励机制运转流畅，有助于数据经济生态的落地。

4.3.4 专业运营商和交易商

运营商和交易商作为生态节点，普及数据保护确权的观念，降低用户使用门槛，在生态价值逐步提现过程中，又反向推动运营商和交易商更有动力去建设数据经济生态。

4.3.5 产业客户法律风险的回避

ABS 为从医疗到 ID 管理到分布式内容市场的众多应用程序提供安全架构，随着相关数据保护法规的落地，会促使相关产业客户进入生态，同时带动了用户进入，撮合数据交易会进一步提高数据经济生态的价值。

4.3.6 基于 AI 技术的数据撮合交易

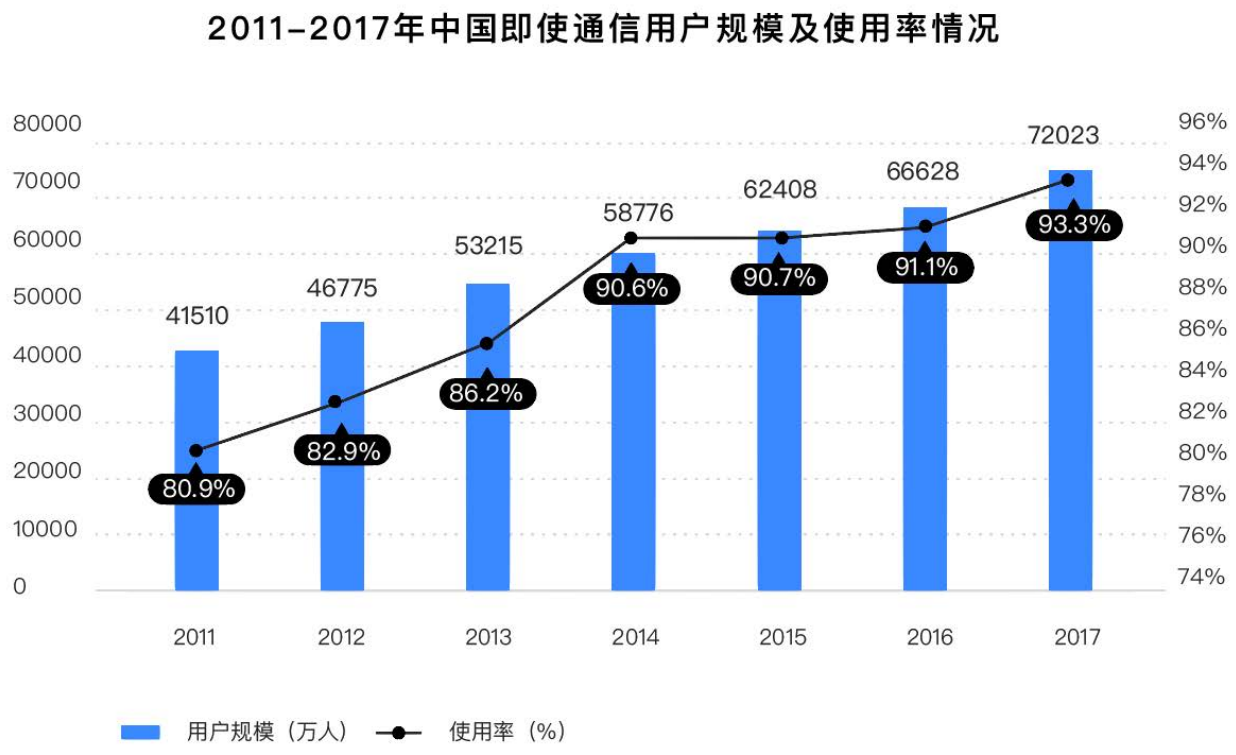
通过使用 AI 技术对用户各种数据信息标签化，生成用户的数字档案和用户画像，从而实现数据信息的精准匹配。

五、应用

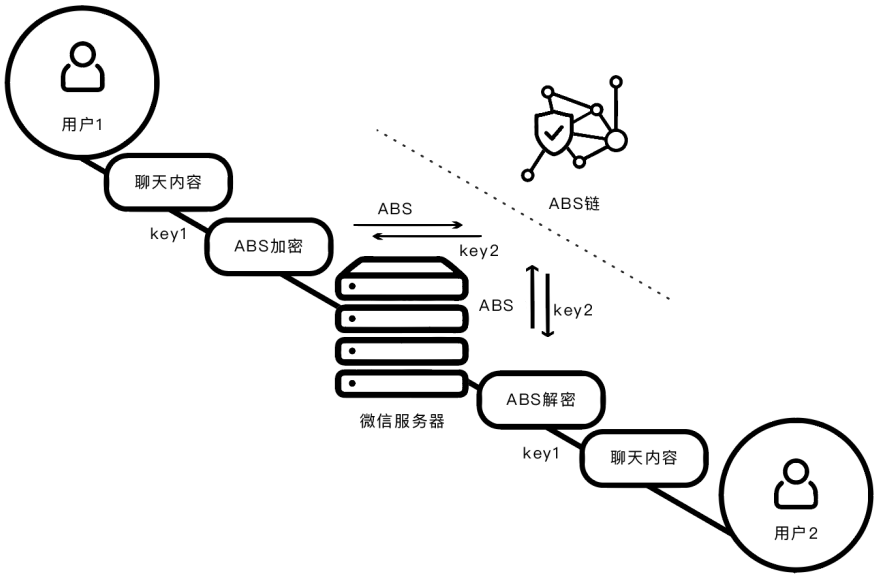
在数据价值日益增大及数据信息安全问题日益突出的当下，ABS 链可以实现加密数据信息以及加密密钥储存分发，从而解决数据信息安全最核心的确权和用权问题。可见，ABS 链拥有着广阔的应用前景，如 IM 数据加密、重要文件传输、数据采集等。

5.1 IM 数据加密

即时通信工具（IM）是人们使用频率最高，最为流行的通讯工具。中国互联网络信息中心发布的第 41 次《中国互联网络发展状况统计报告》显示，截至 2017 年 12 月，即时通信用户规模达 7.20 亿，占网民总体的 93.3%。微信、QQ、钉钉等典型的 IM 即时通信工具已经成为人们日常生活工作中的必不可少的组成部分。然而，数据尤其是个人隐私信息泄漏的问题却时有发生，让用户头疼不已。

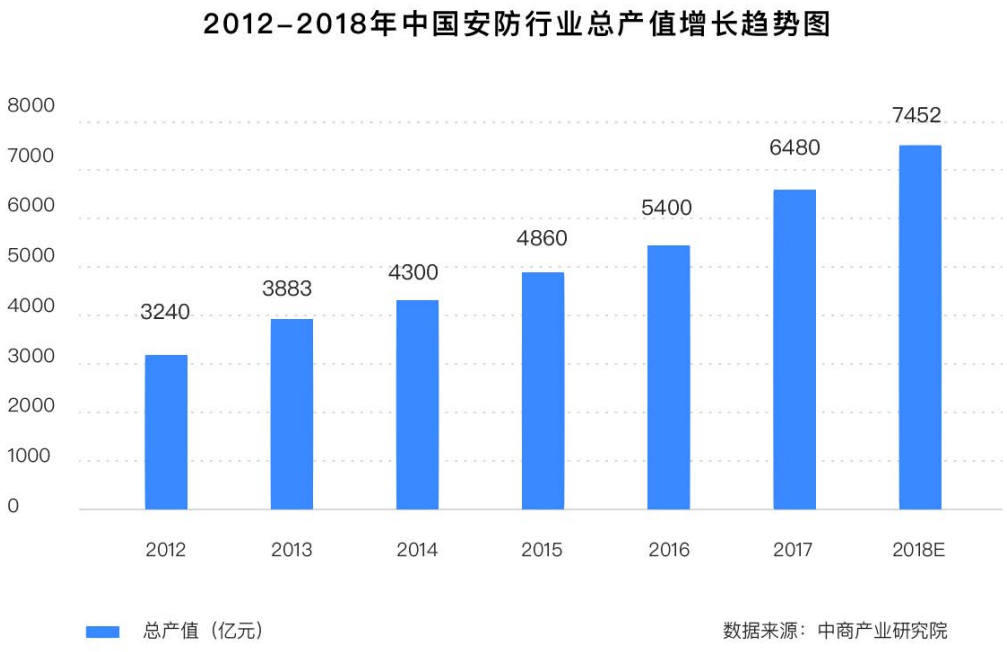


ABS 链可以有效地保护数据安全，下图以微信为例，展示聊天数据加密及 ABS 支付基本流程。

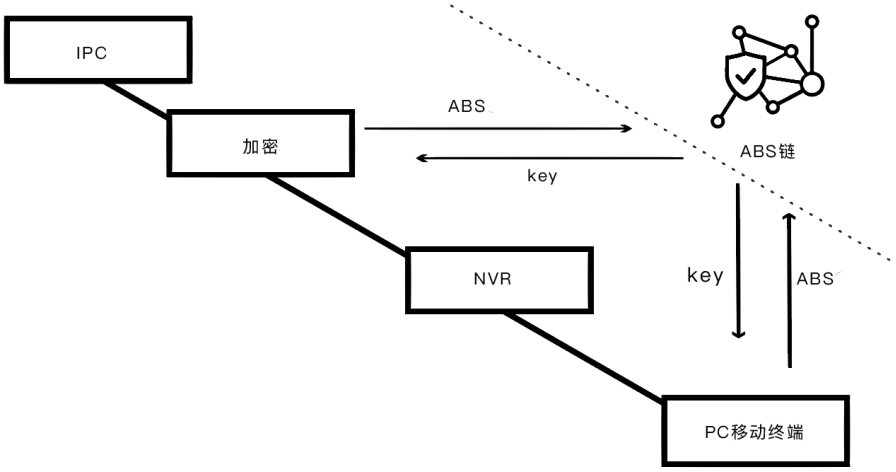


5.2 监控视频加密及分享

近年来在国家政策的支持下，得益于平安城市和智慧城市的打造，安防产业始终保持高增长态势。根据中商产业研究院统计，2017 年国内安防市场规模达到 6480 亿元，2020 年预计将接近 1 万亿元，年增长率保持两位数的高位增长，国内市场空间不断增大。

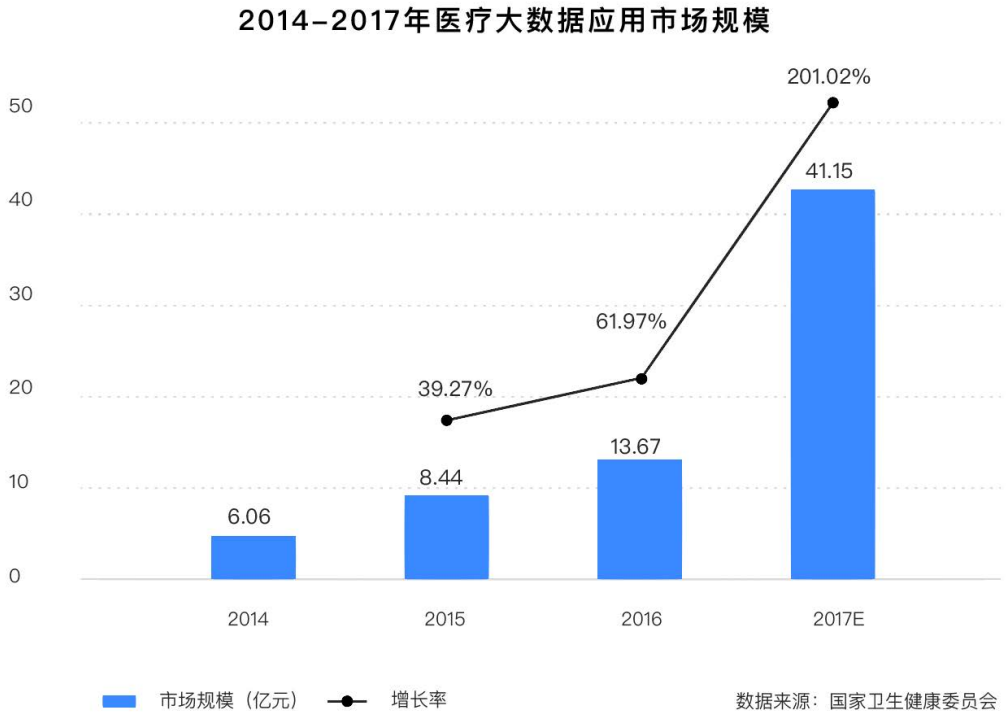


一般来说，监控系统都会直接和网络连接，监控视频数据通常都保存在网络服务器中。便捷的同时，这也使得整个系统容易受到入侵和破坏，视频数据容易遭到非法访问，从而引发一系列数据安全问题。ABS 链给出了具体的监控视频保护方案。

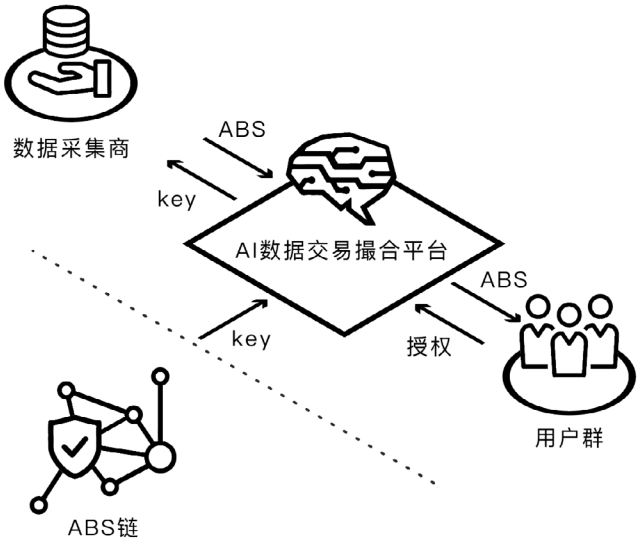


5.3 数据采集（医疗数据）

国家网信办发布的《数字中国建设发展报告 (2017 年)》显示，我国医疗大数据应用市场规模已超 41 亿，涨幅超 200%。但医疗数据行业在进行采集数据时，仍面临着数据分散、数据质量差等问题。

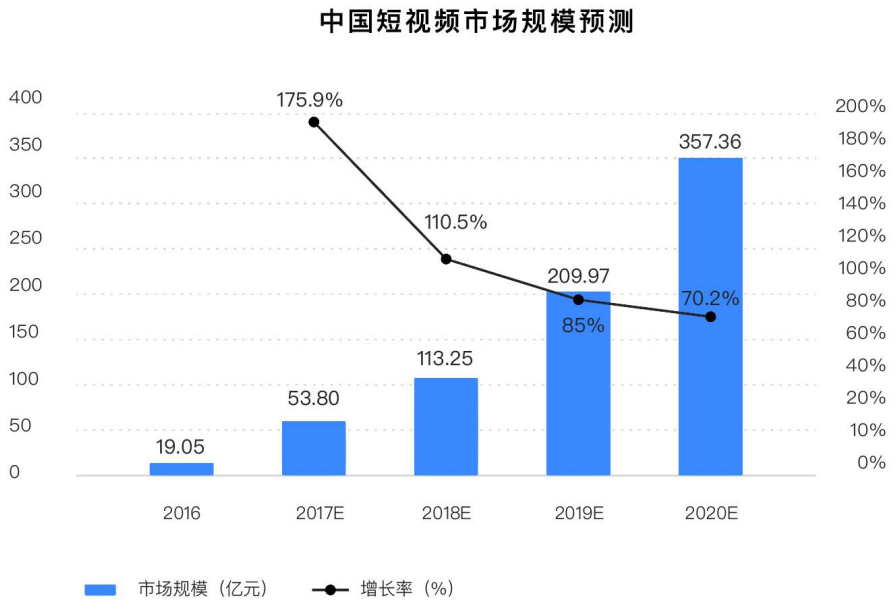


随着电子病历、可穿戴智能设备的普及，未来可以实现大规模、实时、持续收集患者数据。这样以来，数据分散、数据质量差等问题将得到有效缓解。鉴于此，ABS 链提供了数据交易平台，利用 AI 技术可智能高效地进行交易撮合，从而让医疗数据的价值最大化。

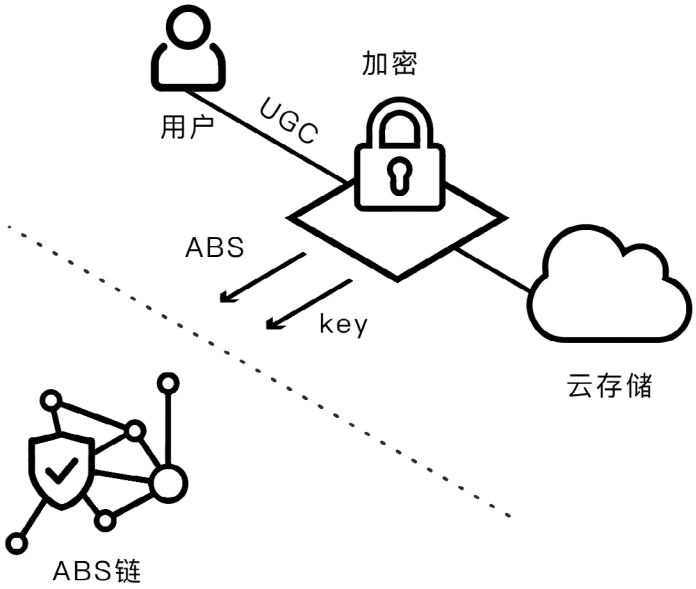


5.4 UGC 价值保护

随着移动互联网的发展，UGC 呈井喷式增长。以短视频为例，据中商产业研究院发布的《2018–2023 年中国短视频行业市场前景及投资机会研究报告》显示，2017 年中国短视频市场规模达 53.80 亿元，增长率为 175.9%。在行业逐渐规范的背景下，短视频市场规模将进一步增长，2018 年市场规模有望突破 100 亿元大关，达到 113.25 亿元，预计 2018 年将达到 3.53 亿人。

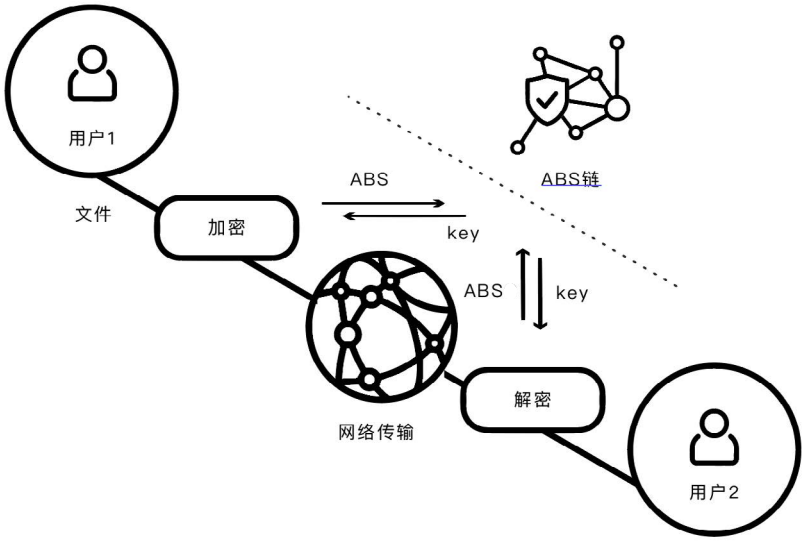


UGC 日趋流行，同时也诱发了许多问题，诸如侵犯知识产权、网络隐私等。ABS 链可以从根本上解决 UGC 的价值保护，用户只要支付一定数据的 ABS，即可实现 UGC 内容的确权保护。



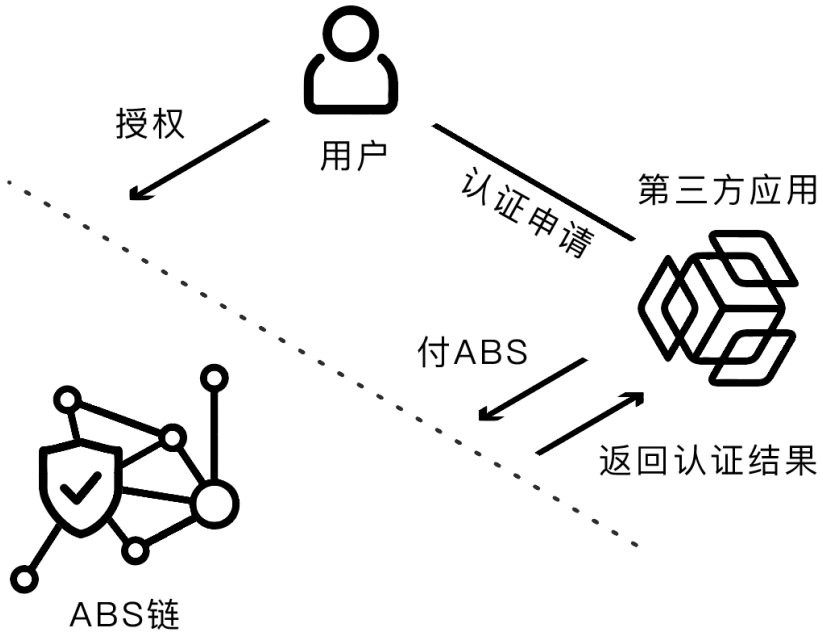
5.5 机密文件传输

互联网缩短了数据传递的时间和成本，极大的方便了远距离私密文件如合同等数据的传输。在享受便捷的同时，带来的是数据私密性得不到保障的问题。ABS 链可以有效地解决该问题，减小数据泄漏的风险。



5.6 身份认证

未来整个经济体系必然会互联网化，而绝大部分互联网商业模式需要建立在网络实名的基础上。网络身份与现实身份绑定无疑提升了身份价值，但同时催生了身份标识买卖的黑色产业链。个人的真实信息已经普遍存在于网络，但多数互联网企业对数据信息的保护能力不足，隐私泄漏事件频发，我国 2017 年通过不同渠道泄露的个人信息达 65 亿条次，甚至个人生命财产安全也因此受到极大的威胁，网络信息安全已然成为全球面临的挑战。ABS 链可以在信息不被泄漏的情况下提供身份认证服务。



5.7 其他

目前互联网中有数据加密和定向分享需求的场景，诸如精准营销、问卷调查、选举投票等，ABS 链也都适用。

六、进展

6.1 里程碑

项目的整体架构层层递推、迭代演进，团队目前搭建了项目的核心架构，完成了项目所涉及到的底层算法开发：

2018 年 11 月 26 日，ABS 链主链钱包上线，面向全社区公测；

2018 年 12 月 07 日，ABS 链主网正式上线；

2018 年 12 月 18 日，ABS 链主链钱包主网映射完成；

2019 年，项目将按照规划稳步推进：

（1）ABS 链出块盒子将开始出块；

（2）ABS 链主链钱包将上线类余额宝的理财功能；

（3）ABS 链密钥分发节点 21 超级节点将开启竞选；

（4）基于 ABS 链的加密版微信将上线。

未来，在 ABS 链生态架构基本搭建完成的前提下，在国内相关法规落地的基础上，对产业客户输出成套数据确权及用权安全架构，赋能产业客户，让用户、产业客户、服务商和平台共享数据经济生态的价值。

七、风险

7.1 政策性风险

目前世界范围内有些国家对于区块链项目以及其融资方式的监管政策尚不明确，存在一定的因政策变动原因而造成参与者损失的可能性。

7.2 交易风险

作为一种虚拟货币资产，其交易具有极高不确定性。另外，由于该领域目前尚缺乏强有力的监管，故而虚拟货币投资存在暴涨暴跌、全天候交易、庄家操盘等风险，可能会对个人资产造成损失。

7.3 统筹风险

现有的商业模型与统筹思路存在与市场需求不能良好吻合的可能，从而导致盈利难以实现或未达到投资者预期。同时，白皮书后续可能随着项目进展进行调整，投资者可能因未能及时获取相关细节，对项目认知不足，造成损失。

7.4 技术风险

项目更新调整过程中，可能会发现有漏洞存在，技术团队将不断通过补丁形式进行弥补。

7.5 安全风险

虚拟货币具有匿名性的特点，易被犯罪份子利用或受到黑客攻击，甚至可能涉及到非法资产转移等犯罪行为。

八、免责

本文档仅作为传达信息之用，内容仅供参考，不构成任何获取 ABS 的相关意见，不构成任何投资买卖建议、教唆或邀约。本文档不组成也不应被理解为提供任何买卖的行为，或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承诺。

项目团队将不断进行合理尝试，确保白皮书中的信息真实准确。开发过程中，系统可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过官方网站发布公告或新版白皮书。请参与者务必及时获取最新版白皮书，并根据具体更新内容及时调整相关决策。

团队明确表示，概不承担参与者因依赖本文档内容，本文档信息不准确之处，本文档导致的任何行为造成的损失。团队将不遗余力地实现文档中所提及的目标，但团队不能做出完全承诺。

请投资人在作出决策之前，充分了解团队背景，知晓项目整体框架，合理预估自己的愿景，理性参与项目。