分布式存储与零知识证明

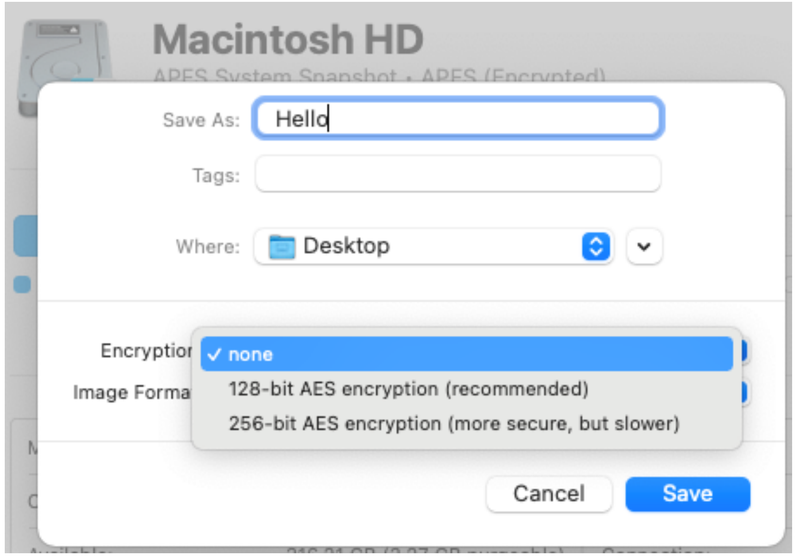
Dante Network

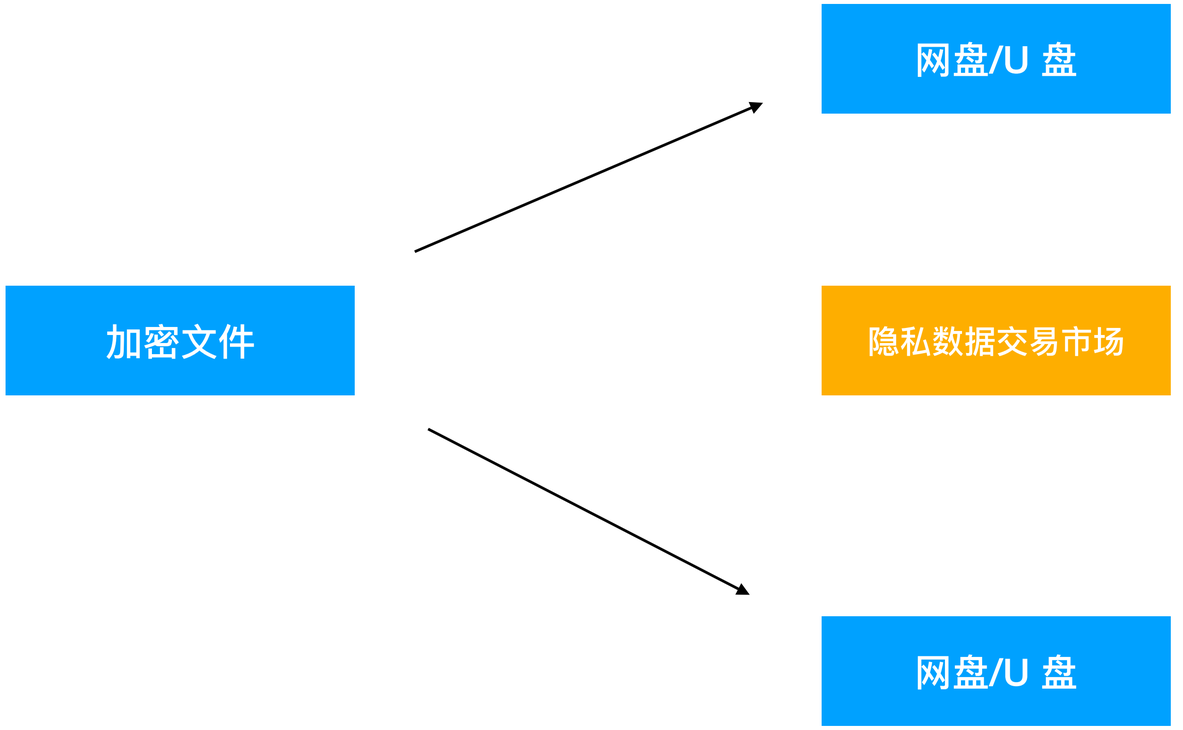
Zack

存储的现状

- 普通存储（PC、手机、硬盘、U盘）
- 跨平台存储（网盘、iCloud、DropBox）
- 加密存储（Mac 磁盘工具加密、Windows文件夹加密）

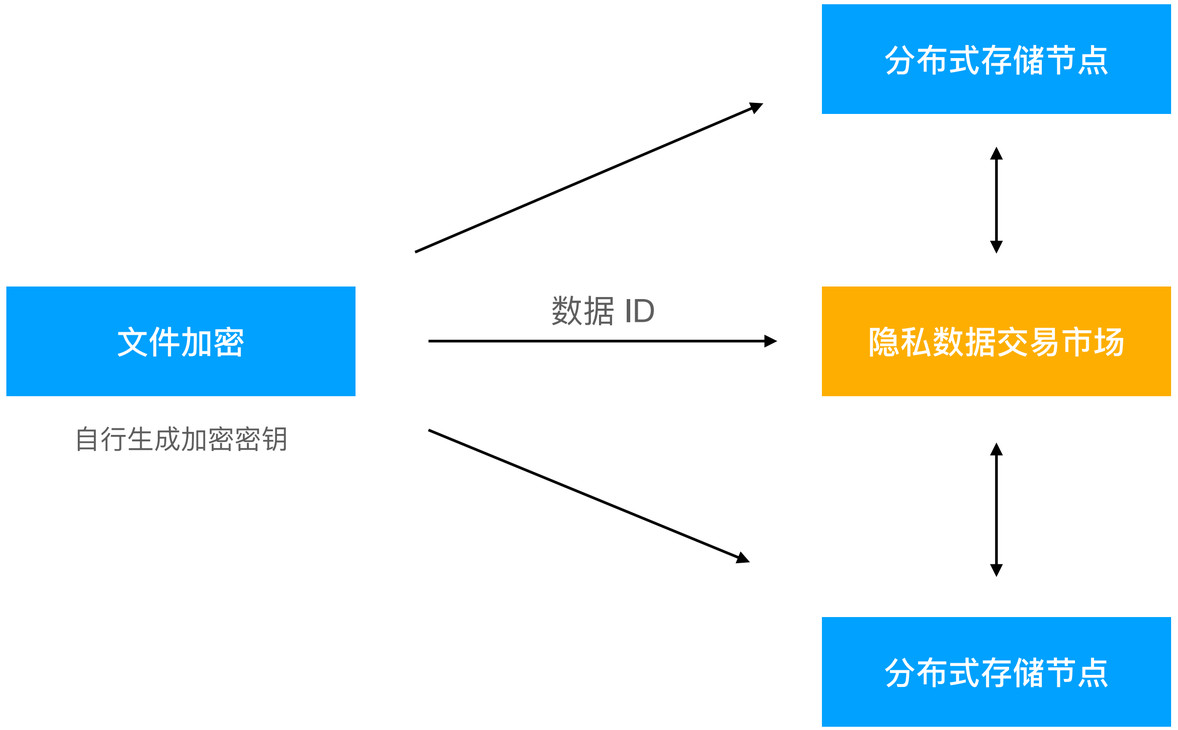
相对安全的存储方案


Macintosh HD
Save As: Hello
Tags:
Where: Desktop
Encryption
Image Forma
none
128-bit AES encryption (recommended)
256-bit AES encryption (more secure, but slower)
Cancel
Save

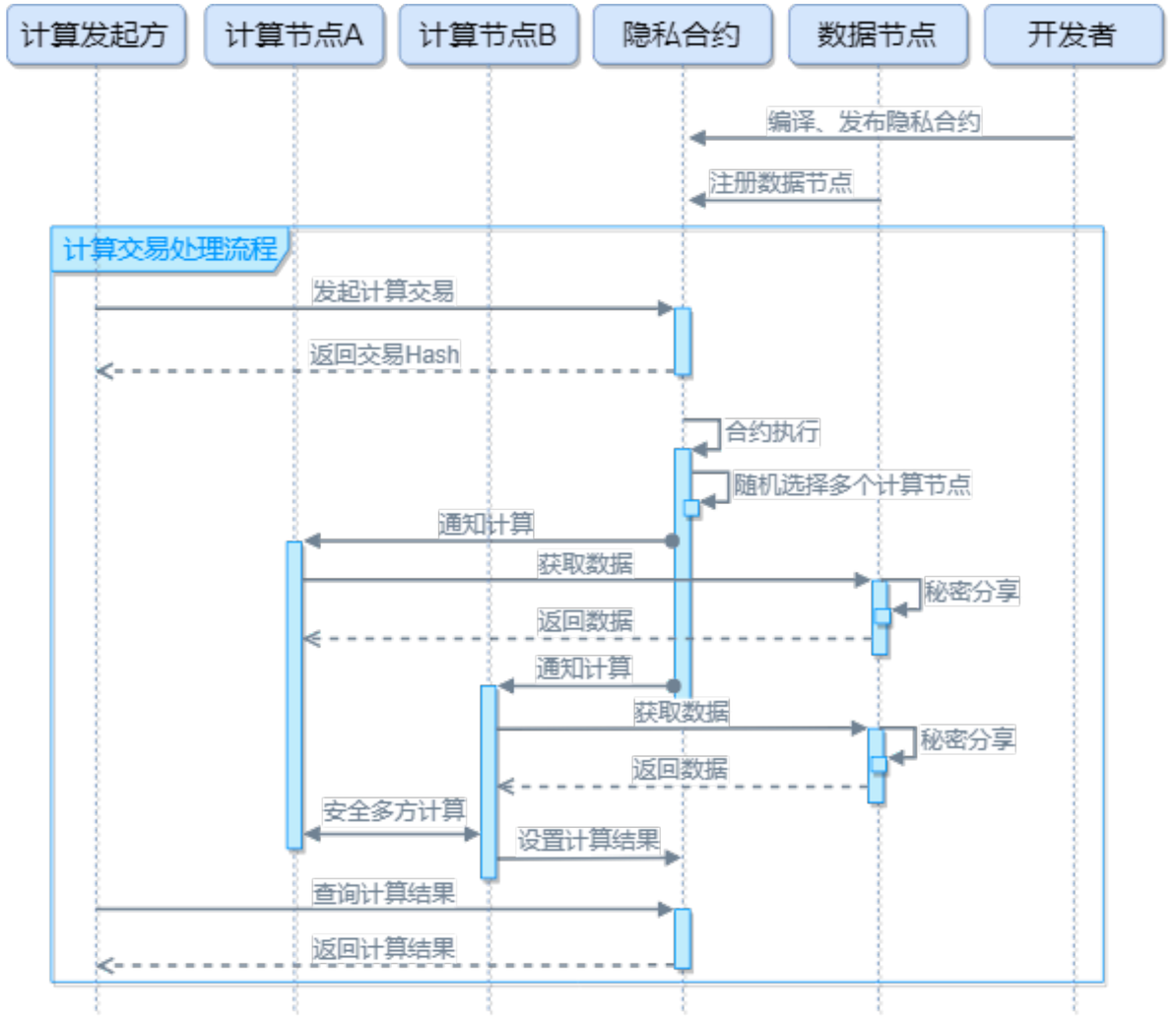

加密文件
网盘/U 盘
隐私数据交易市场
网盘/U 盘

存储的未来

- 数据所有权归个人
- 数据可隐私存储
- 数据可隐私交易

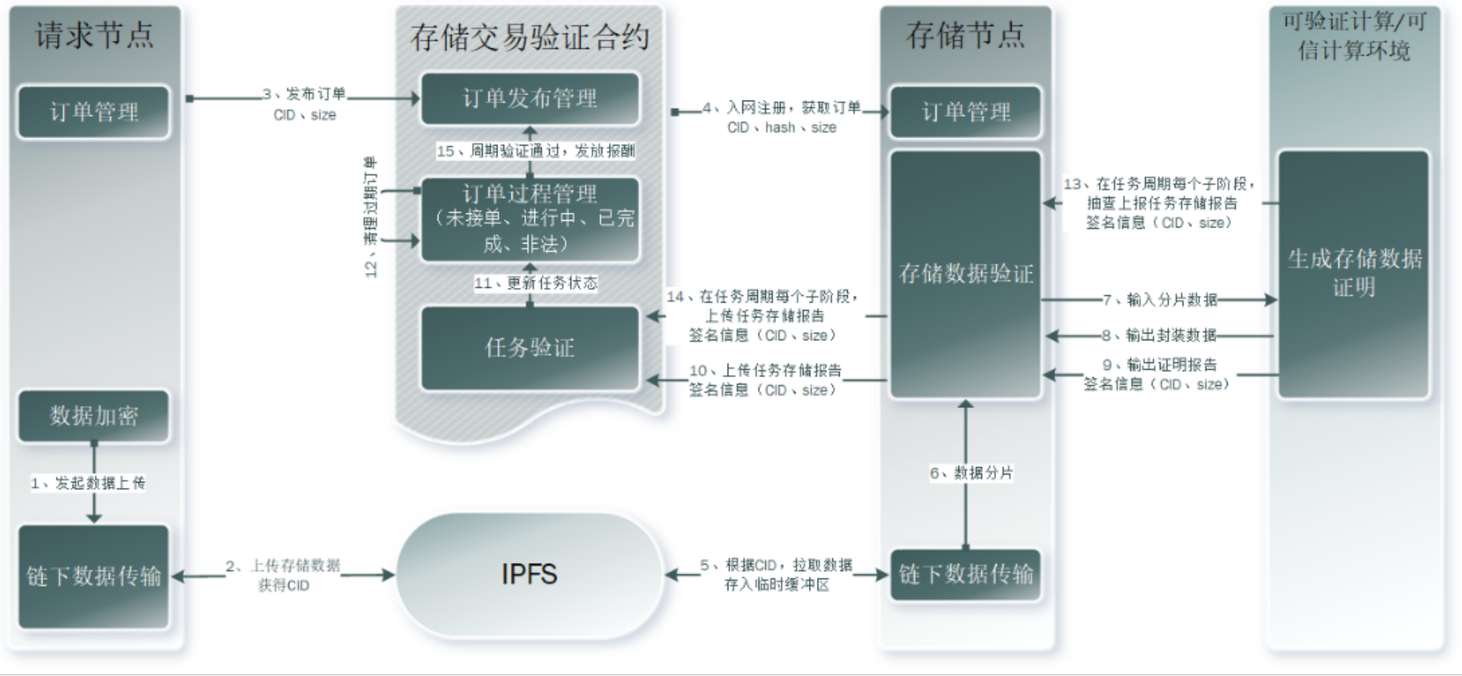


隐私数据流转示例

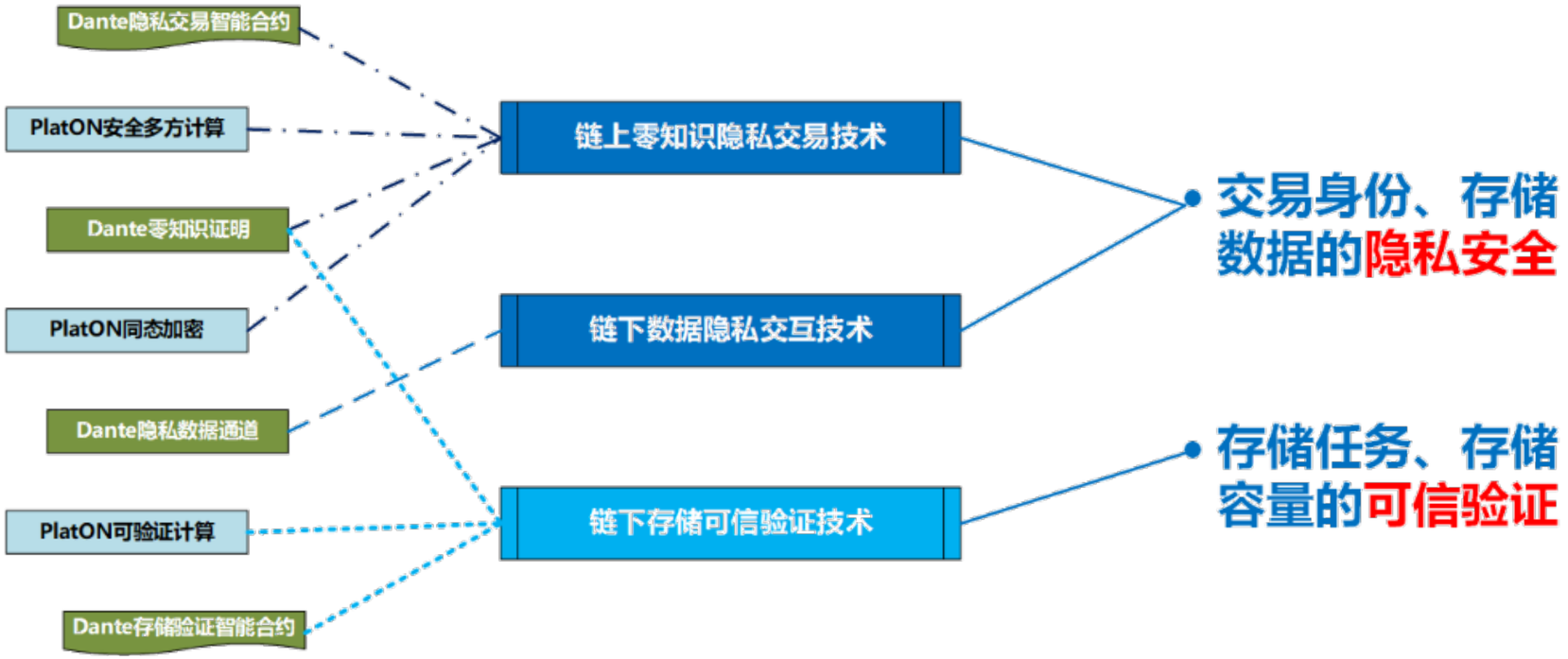


图片来自 https://devdocs.platon.network/docs/zh-CN/PlatON_Overall_Solution

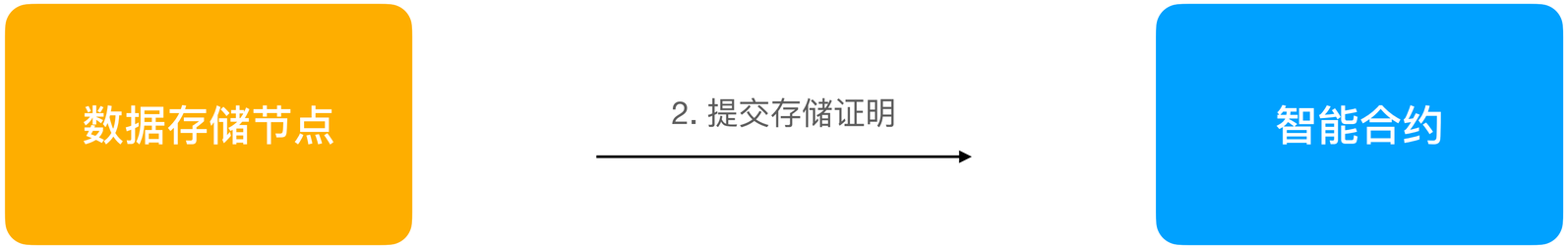
Dante 流程图


请求节点
订单管理
数据加密
1、发起数据上传
链下数据传输
2、上传存储数据
获得CID
存储交易验证合约
订单发布管理
3、发布订单
CID、size
15、周期验证通过，发放报酬
订单过程管理
（未接单、进行中、已完成、非法）
12、清理过期订单
11、更新任务状态
任务验证
14、在任务周期每个子阶段，
上传任务存储报告
签名信息（CID、size）
10、上传任务存储报告
签名信息（CID、size）
IPFS
5、根据CID，拉取数据
存入临时缓冲区
存储节点
订单管理
4、入网注册，获取订单
CID、hash、size
存储数据验证
6、数据分片
链下数据传输
可验证计算/可信计算环境
生成存储数据证明
13、在任务周期每个子阶段，
抽查上报任务存储报告
签名信息（CID、size）
7、输入分片数据
8、输出封装数据
9、输出证明报告
签名信息（CID、size）

Dante Network 核心技术



Dante 零知识证明应用

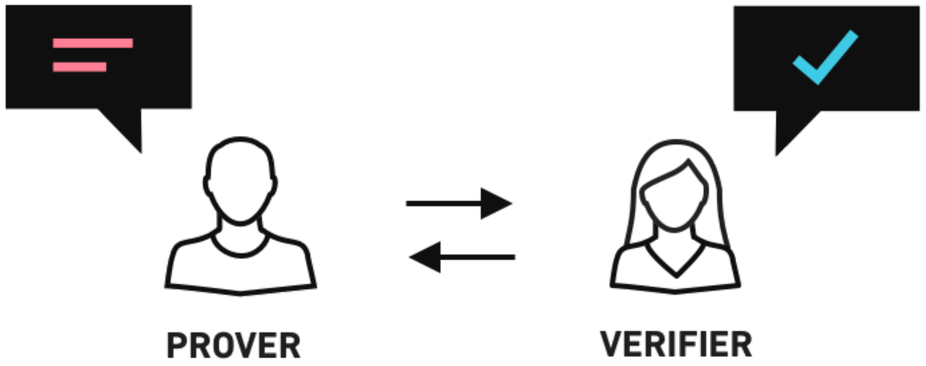


1. 生成零知识存储证明 (zk-SNARK Groth16)

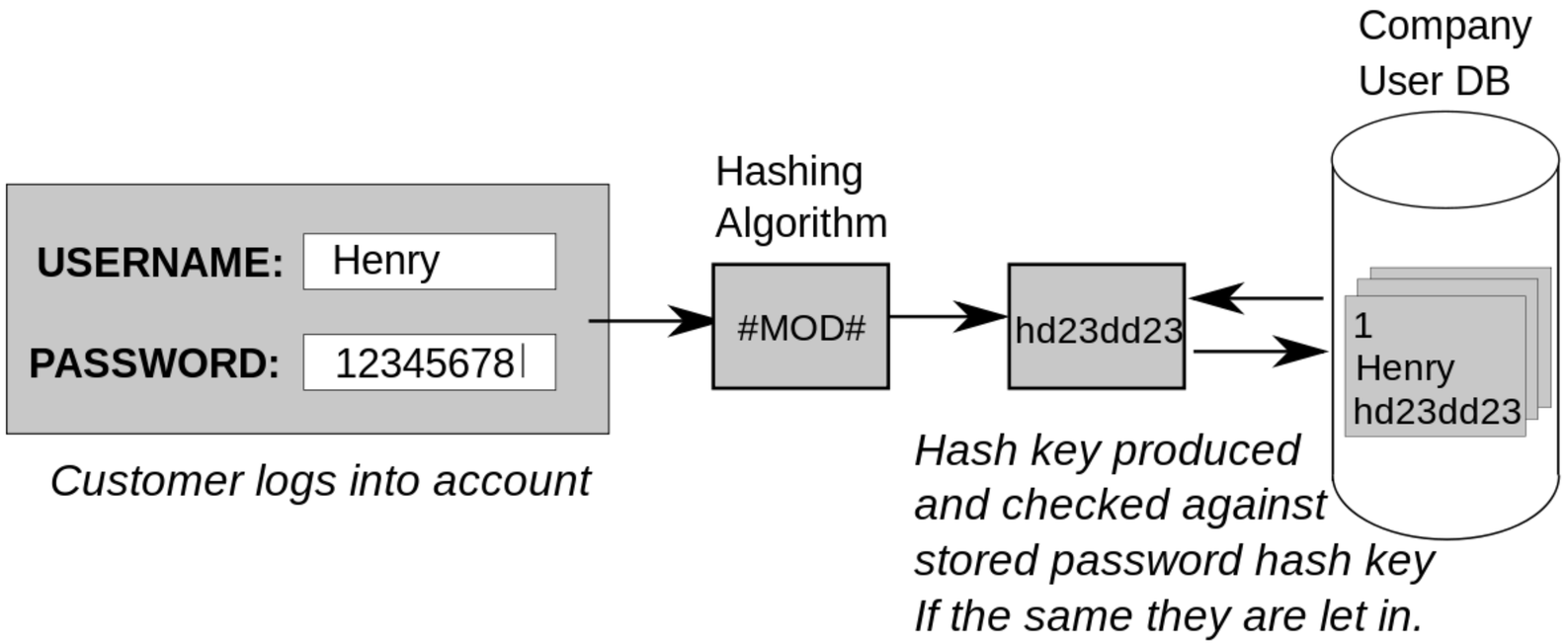
3. 验证存储证明

什么是零知识证明

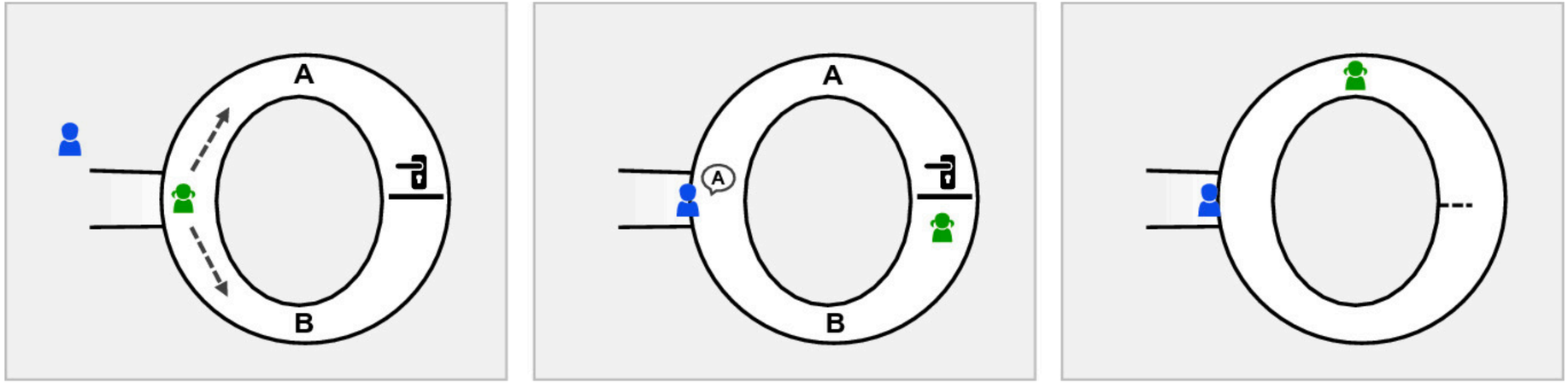
- 零知识证明(Zero—Knowledge Proof)，是由 MIT 研究员S.Goldwasser、S.Micali及C.Rackoff在20世纪80年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明，零知识证明在密码学中非常有用。



简单的交互证明系统—账户登录



零知识证明示例



图片来自 https://link.springer.com/chapter/10.1007/978-3-030-40142-9_5

零知识证明示例

引用麻省理工学院多媒体实验室（MIT Media Lab）对零知识证明的解释：

你手上有两颗撞球，分别是绿色和红色，除了颜色之外这两颗撞球一模一样。假设我是红绿色盲，因此，就我看来你手上拿的是两颗一模一样的撞球。

问题来了，请问你是否能在不提到任何颜色资讯的前提下，说服我这个色盲相信这两颗球的颜色，确实不同?

当然可以!

你只要把两颗球交给我这个色盲，然后要我拿到背后去随意变换左右顺序之后，再拿出来让你「猜」原本在左手的球，现在换到了哪一手。

对你来说，你一眼就可以判断本来左手拿的是绿色，现在绿色跑到右手去，根本不用猜，很轻易就能指出球换位置了。但是，这对色盲来说简直惊讶！因为就我看来，这是完全相同的两颗球，你肯定只是运气好猜中的。

不过，只要重复做个几次测试，我很快就会相信你说的，这两颗球肯定有哪里不同，只是我看不出来。而且，你也完全没有透露任何关于颜色的资讯。

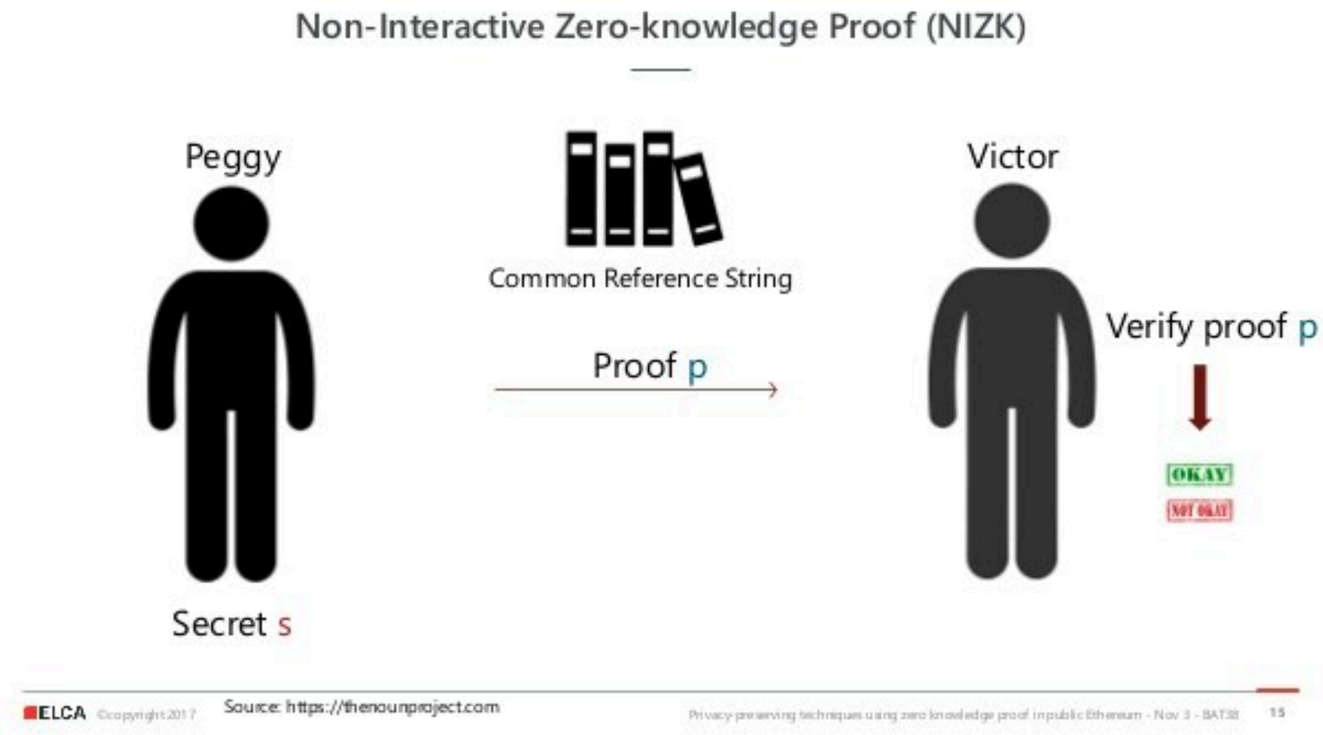
非交互式零知识证明

交互式零知识证明的问题

1. 证明者可以和验证者串通。
2. 证明者的证明只能使用一次。

解决方案：非交互式证明

1. 不需要交互
2. 证明一次可以多次使用
3. 证明者和验证者不需要同时在线。



Dante Network

- Website: https://www.dantechain.com/
- Github: https://github.com/dantenetwork
- Twitter: https://twitter.com/DanteNetwork
- Telegram: https://t.me/Dante_Network