ZK-KYC与ZK认证过程

杨歌 [杨歌思学](javascript:void(0);) 2022-07-24 12:43 发表于北京

**ZK-KYC and ZK Authentication Process**

  2022年是Web3与Web2平行世界交错和焦灼发展的一年。前者经历了将Celsius, Luna和3AC连串洗劫的新次贷危机，后者代表滴滴在接受80亿罚款时也明确了其过度收集用户隐私数据的行为。在这两个平行世界中有一个共同需要解决的事情，就是如何能够解决用户隐私和用户认证的Dilemma问题。

  在传统互联网与金融系统中，商家与金融机构为了确保服务对象的真实可靠与合格信用，会收集大量用户的信息对其进行**KYC(Know Your Customer**—”了解你的客户”)，并对此进行深度的行为画像分析甚至是追踪预判并反馈迭代以实现KYC数据的精准化和有效性。在这个过程中，理论上商家与金融机构应该用**数据脱敏**的方式处理用户隐私，但由于为了简化工作难度、不合规后门、以及被他方盗取破译等诸多原因，隐私泄露的事件时有发生。被泄露的隐私一旦公开便成为了不可逆的过程，随着这样的黑天鹅不断增多，隐私暴露以及由其所引发的各个社会层次的安全和衍生问题便成为了不可回避的灰犀牛问题。

  随着Web2互联网与金融企业竞争的深度内卷，用户数据被更深层次地挖掘，并根据以上的循环不断暴露，灰犀牛问题愈发严重。而从另外一个方向，Web3发展至2022年，用户账户仍并没有与用户的真实身份挂钩，大量用户拥有多个账户进行多重杠杆操作，信用危机加成Ponzinomics带来的死亡螺旋在这一年集中爆发，没有信用锚点的金融借贷与衍生嵌套无法逃避泡沫的破裂。

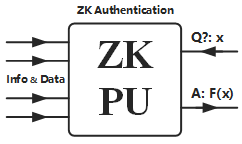
  Web3和Web2在用户隐私和用户认证的Dilemma问题上走了两个极端，这个时点必须要思考中和的解决方案，其中的平衡点在哪里，具体应该如何实现？

  讲一个有趣的例子。小明在互利网交友平台上找对象，看到了小美的Profile，通过基础履历和照片视频，小明可以明确小美是他想要约会的对象，因为小美的这些信息都提供在明面上，小明可以直接做出判断。换一个情景：小明有一天在公司工作，他的同事小王和他说，他前两天见到有一位叫小美的女生，根据他对小明的多年了解，小美一定是小明喜欢的类型，小明微微一笑并没有在意；这时候，讲信用的小李走了过来，对小王说的表示非常肯定，他说小美太适合小明了，一定不会错；很快从不开玩笑的小张也站了起来，告诉小明，他们没有开玩笑，小美的确值得一见；这时候的小明就真的心动了，他相信小美是他想要约会的对象。后面的这一个情景，其实小明并没有获得小美的任何直接信息，但是他却完成了对小美的KYC过程。

  在这里我们做个定义，在不知道客户的任何直接信息下做出对该客户的认证判断过程，叫做**零知识了解你的客户**，即**ZK-KYC(Zero Knowledge-Know Your Customer)**；其中在零知识的情况下做出判断的技术，叫做**ZK认证技术(Zero Knowledge Authentication Technology)**，使用ZK认证技术完成对客户、资产、事件等认证的过程，叫做**ZK认证过程(Zero Knowledge Authentication Process).**ZK-KYC, ZK认证技术与ZK认证过程，对于互联网与区块链，Web3与Web2的进一步发展都会是非常重要的。

  在实现ZK认证过程中，最重要的是找到对应问题的**零知识认证处理器—ZKPU(Zero Knowledge Processing Unit)**，做到**①证明其认证问题的有效性**，并且保证**②不会对外泄露或被攻破获取实际数据。**

  在上面的简单例子中小王等三位朋友分别担当了小明关心问题的ZKPU，并且可以把他们视作一条联盟链上的三个节点，分别向问题发出了认证确认，是一个模拟的区块链ZK认证过程。而这个例子的问题是，做为自然人验证的节点，他们很难真的做到守口如瓶，不描述泄露任何关于小美的数据。



**在未来专业的ZK认证过程中，ZKPU需要同时做到上述①②两个条件，并且以多点认证的方式进行确认。对于每一个ZKPU单元，需要掌握足够的基础信息和数据，通过算法与加密处理掌握信息的整体结构，并向提问者Q或输入问题x，在不披露任何信息数据端内容的情况下给出相应的问题答案A或输出计算结果F(x)。**(注：在这里通常提问者端的问题Q或输入问题x是基于信息数据端所询问的总结性问题，例如用户信用或者是否满足某类匹配，而非直接问询原始输入信息数据中的具体信息。)

  实现ZK认证过程的ZKPU所面对的情景是多样和复杂的。这其中可能需要应用到的技术包括但不限于：边缘计算，区块链协议，ZK认证算法，加密算法，AI算法，异步计算，数据清洗与标签化，图像识别与NLU，以及各类硬件传感技术等。根据具体情况需要认证的人事物的不同，ZKPU将呈现不同的方式以实现ZK认证过程。ZKPU的形态也可以是多样的，例如是服务器中的算法函数，封装完成的芯片或可编译的FPGA，区块链上的节点，网络次终端或以基站服务器为单元的边缘侧计算力，甚至于是与线下规则结合的预言机等等。

**ZK-KYC其实只是ZK认证过程在对客户认证上的一个特殊过程。**人的各类生物特征例如人脸、指纹、声纹、虹膜、笔迹甚至于血液和DNA等与人直接相关的信息，**在不久的未来都有可能直接成为私钥，作为ZK-KYC处理器ZKPU的输入信息。通过ZKPU处理过的基础生物特征私钥，变成了对外公开的公钥，可以作为DID或CID的基础身份认证信息，即可解决保护用户隐私和完成用户认证的Dilemma问题。**此外，ZK-KYC对用户的认证，还可以直接夹带用户的历史行为信息、资产信息与信用信息，在一套标准Protocol的约定下，ZKPU通过对各类信息的处理与向标准Protocol的核对，丰富用户基于基础公钥的数据维度，**以ZK认证过程的方式实现在用户DID或CID的基础身份上定义和认证输出其关联资产增信与信用核实等信息的各项工作。**

  在ZK-KYC以外，ZK认证过程还包括更多有意义的社会金融价值。

**ZK-POW(Zero Knowledge-Proof of Work)**是基于用户ZK-KYC的基础，使用ZK认证过程对该用户的工作证明进行零知识认证的重要过程，该过程对于Web3中各类应用场景实现对用户链上和线下的各类价值脱敏评定起着至关重要的作用。例如边缘计算AI芯片会担当ZKPU的角色，在隔离信息不向商家境外服务器传输的条件下，做到在境内本地对用户工作量完成的认证。

  此外，对于实体资产与数字资产实现**ZK-POA(Zero Knowledge-Proof of Asset)** 的价值也不容小觑。ZK-POA同样以ZK-KYC为基础，作为ZK-KYC的延展认证，使用ZK认证过程对用户的各类型资产进行评定认证。接受ZK-POA的用户将不担心自己的资产信息在网络和区块链上被盗取泄露，同时向商家传递其所需要的合格信息。

  最后，需要提及一下VitalikButerin在今年4月提到的SBT设想。对于无论是DID还是CID的建设，灵魂绑定都是基础必要的，只有锚定具体信息的用户，才有可能成为在金融信用系统中活跃的一员。然而将用户进行灵魂绑定，在保护用户隐私的基础下进行用户认证是不可回避的发展问题，ZK-KYC与ZK认证过程将在其中成为发展铸造的基石。

作者：杨歌

2022年7月24日