**报告十八：2021.4.30：KVaC: Key-Value Commitments for Blockchains and Beyond (ASIACRYPT 2020 ) 报告人：李佳薇 记录者：李佳薇**

1. **报告内容**

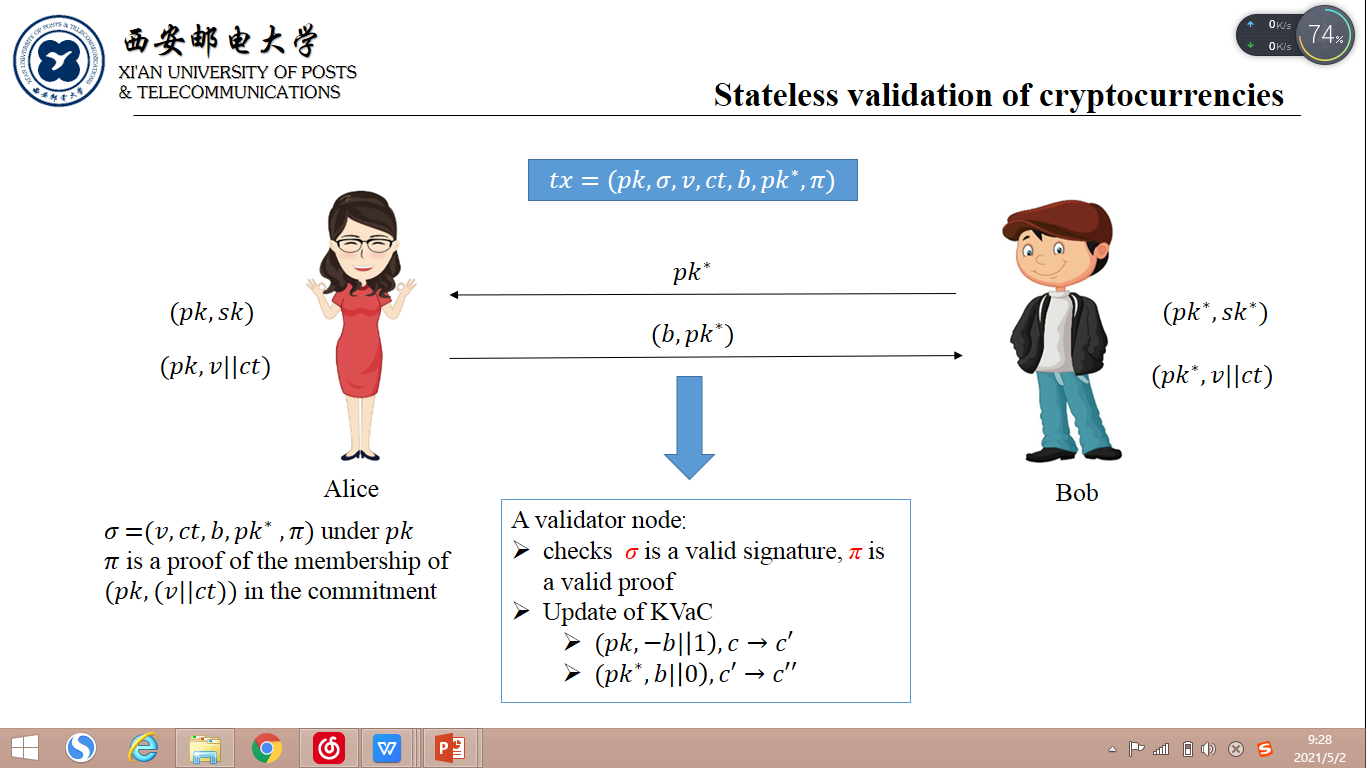
**背景**

提出背景：随着区块链规模的增长，验证新交易变得越来越困难和费时。为了解决这个问题，需要压缩区块链（有效）状态——一种允许有效证明成员身份和更新的方式。在区块链中，系统的状态有两种模型：基于比特币的UTXO集和基于以太坊的余额模型。

解决办法：①UTXO set ----Accumulators、Vector Commitments

②Account ledger ----KVC

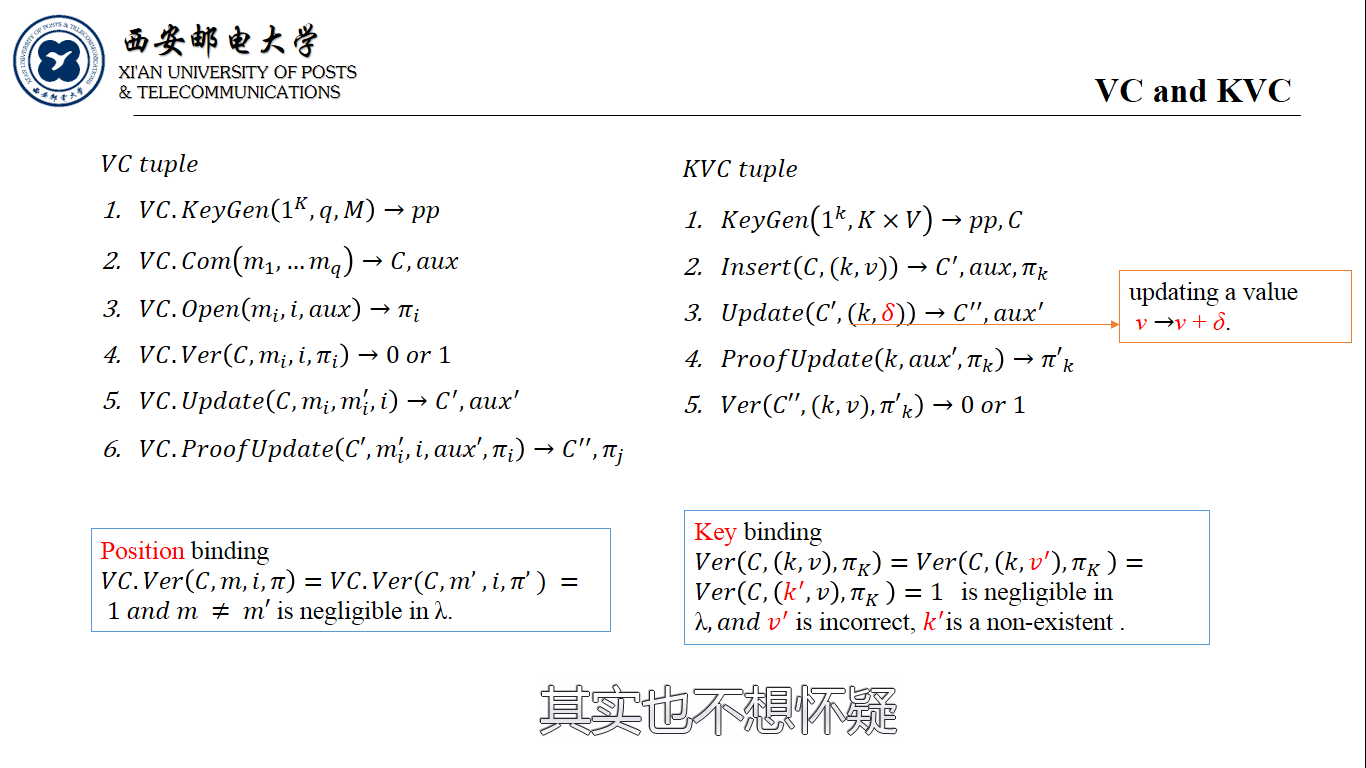
以太坊中交易模型



**KVC构造**

问题：在加密货币网络中，每个节点都需要验证和存储系统的状态。随着用户数量的增加和新帐户的创建，键值映射的大小就会增大，运行节点的资源成本也会增加。这促使大部分用户依赖第三方来通知他们系统的状态，严重限制了网络中的分散化量[PT，Dry19，CPZ18]。

解决：对于基于帐户的加密货币，状态可以用键值映射表示，其中密钥是帐户地址，值由帐户余额、随机数等组成。其大小不随着键数量的增长，但成员资格的证明是恒定的。



**比较Accumulators、Vector Commitments、KVC**

VC和Accumulators可相互构造。KVC也可以构建这两者。

利用KVC构造VC方案，其中公共参数和证明都由恒定数量的群元素组成，公共参数不限制可以提交的元素的数量，所有的VC算法都需要恒定数量的群操作。此外，证明可以被分解，以产生恒定大小的子向量开口。

利用insert-only KVC构造动态累加器，（所有累加器算法都需要一定的群操作。）支持添加和删除成员资格证明。

**VC**：具有与向量大小线性尺度的公共参数[CPZ18]。虽然参数简化为常数，但VC算法的成本在向量的大小上呈线性关系。

**Accumulators**：支持成员和非成员证明。矢量的长度没有限制，但矢量元素是逐步积累的。因此，插入新元素、生成成员资格证明等所需的群操作的数量在向量元素的位大小上是线性的。

**Sub VC**：允许人们在一组位置上打开一个提交的向量，其中打开的大小与提交的向量的长度和要打开的位置的数量无关，公共参数线性增长。

**KVC**：其中公共参数是恒定的，可以提交的元素数量没有限制，证明只由三个群元素组成。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 公共参数 | 元素数量 | 证明 |
| VC | 线性 | 有界 | 线性 |
| Accumulators | 线性 | 无界 | 线性 |
| Sub VC | 线性 | 无界 | 线性 |
| KVC | 恒定 | 无界 | 三个群元素 |

1. **总结**

针对KVC构造，考虑以下问题：

1. 利用VDS构造KVC
2. 利用Accumulators构造以太坊的无状态模型
3. 利用变色龙hash构造insert-only key-value commitment