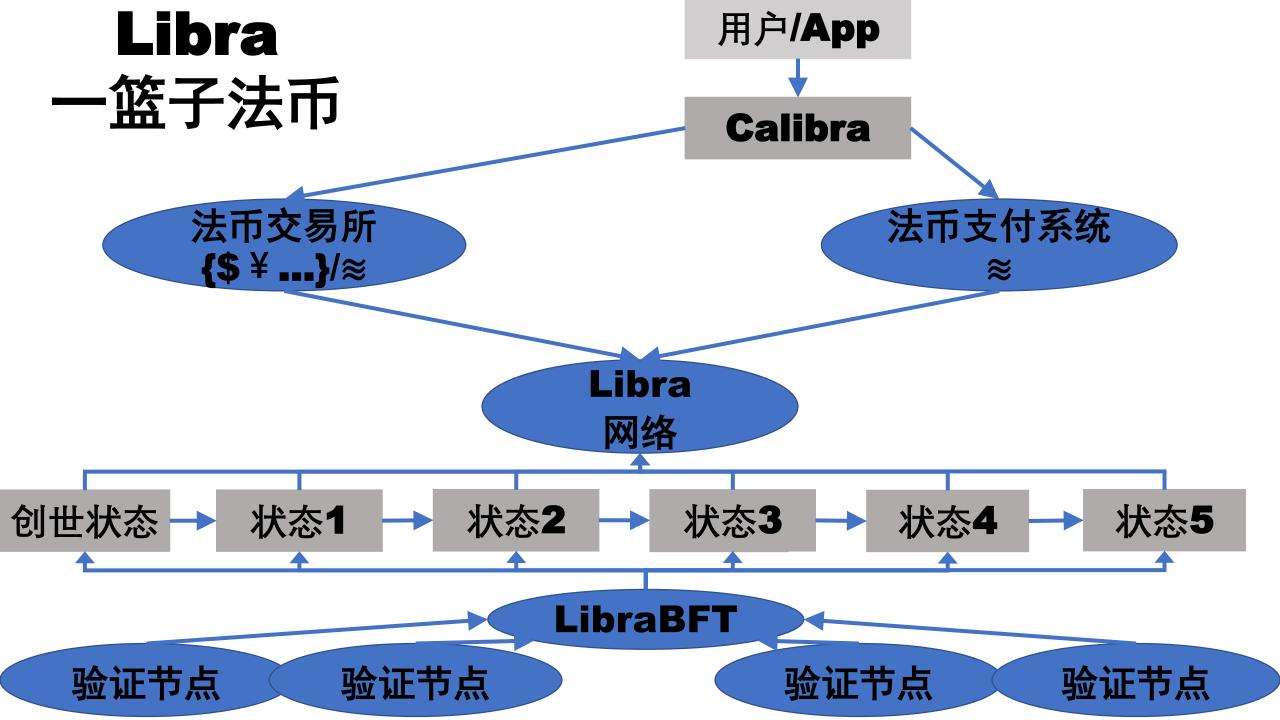
#### Libra共识和Libra整体结构

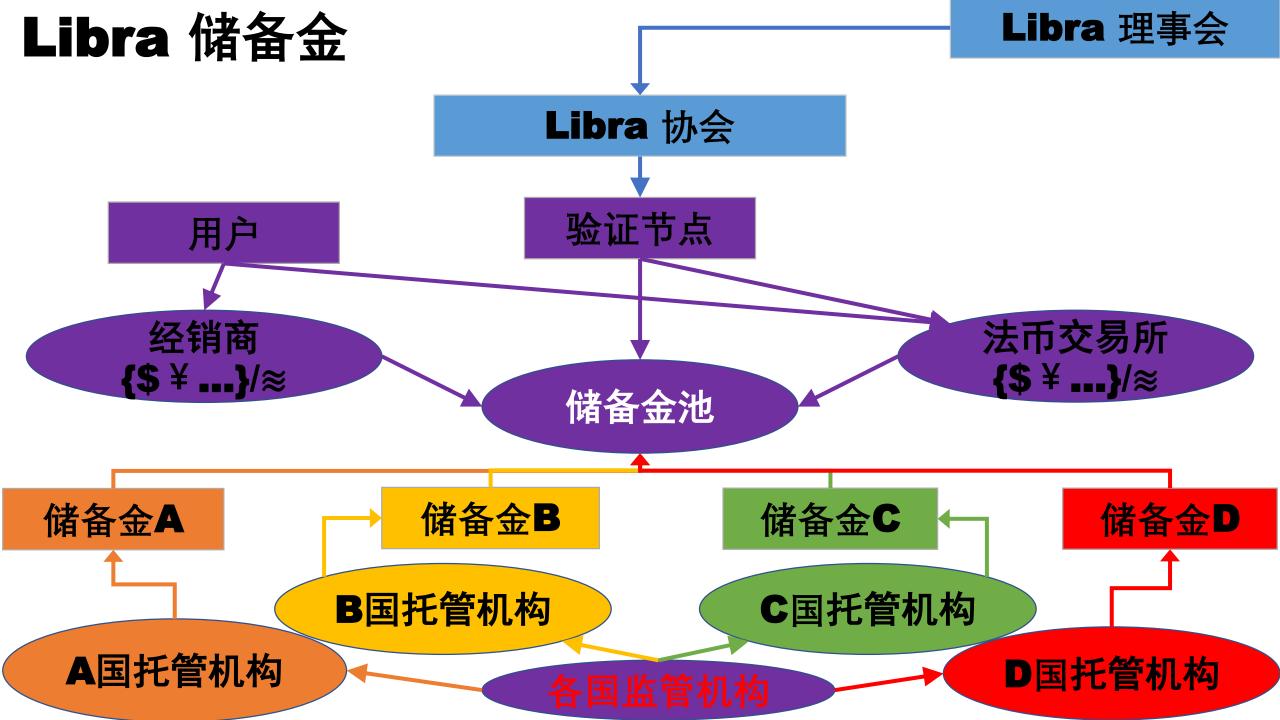
Libra共识:数字货币与法币同价等值

中国央行数字货币: DCEP

(Digital Currency Electronic Payment)

央行结语: 互联网创业思维, 不适合金融领域





# Libra协议简介

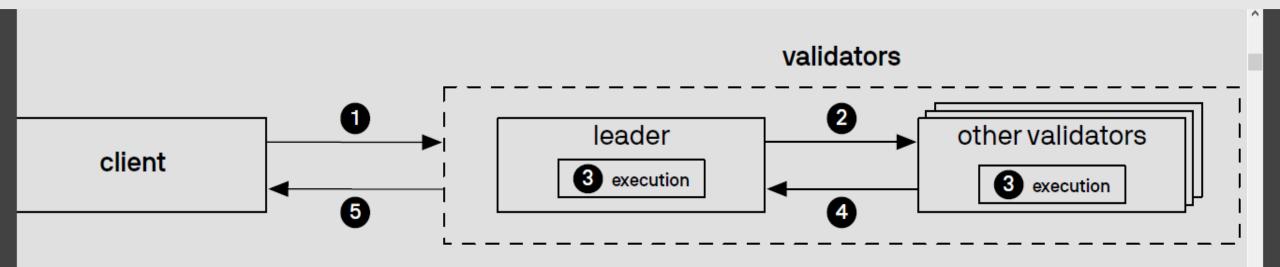


Figure 1: Overview of the Libra protocol.

2

# Libra交易流程

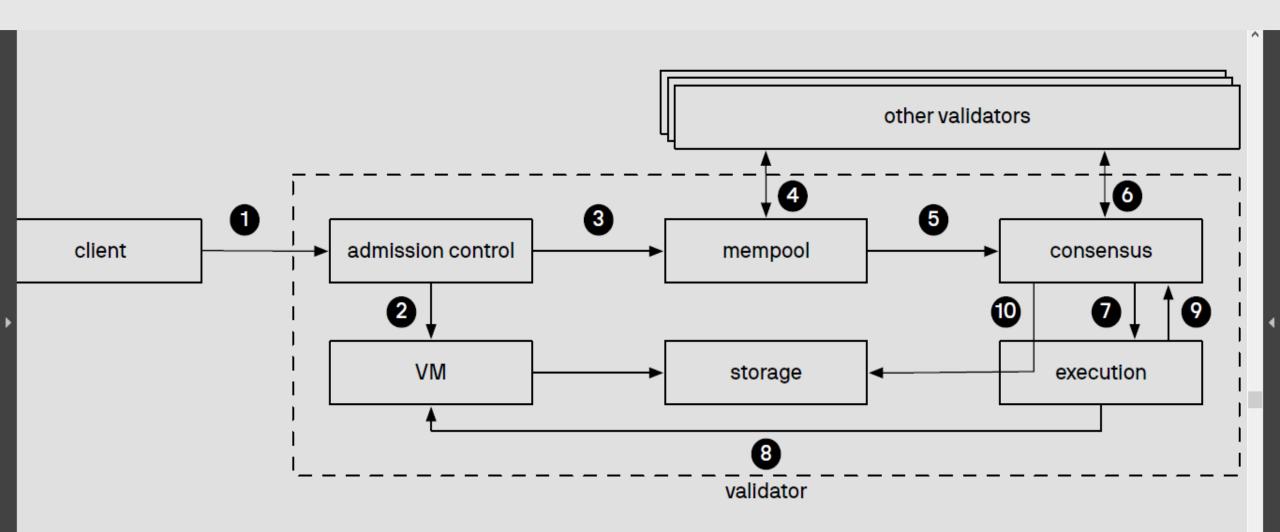
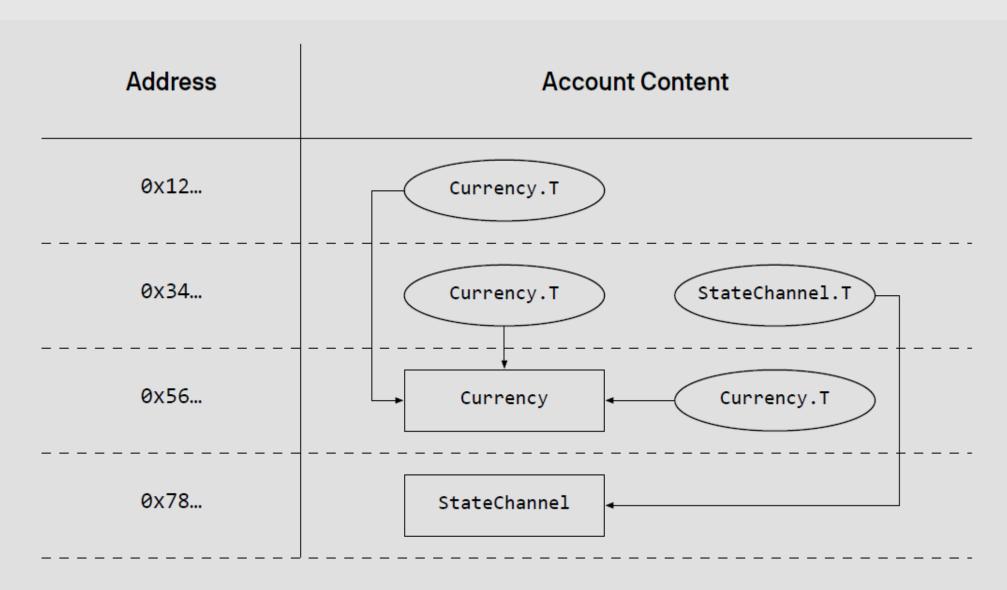
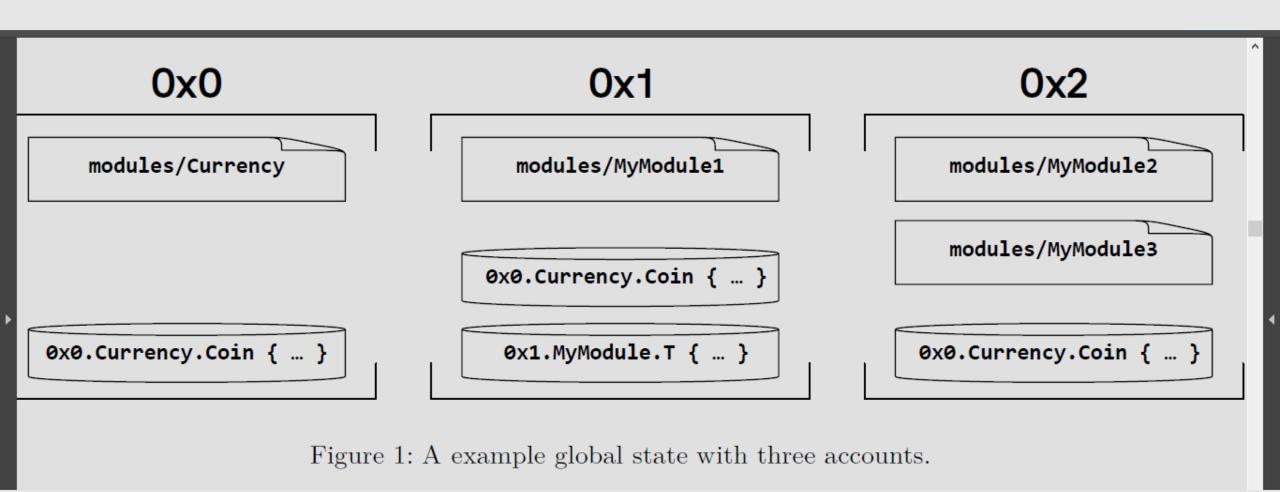


Figure 6: The flow of a write transaction through the internal components of Libra Core.

# Libra数据结构: 地址和账号



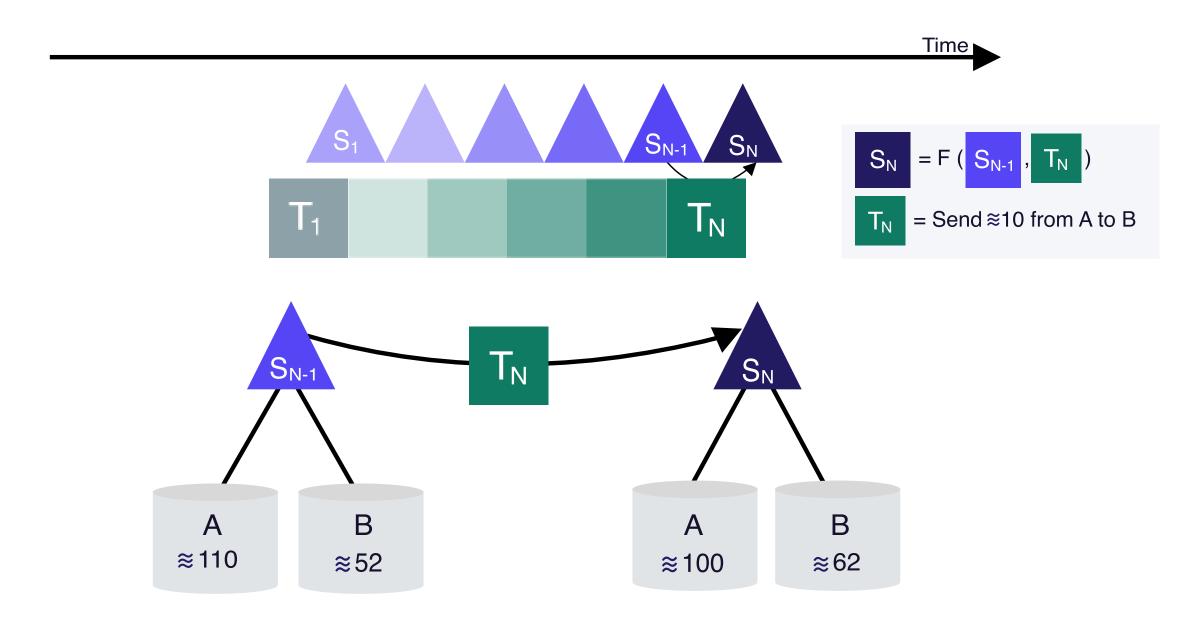
# Libra数据结构: 地址和账号例子



# Libra交易六大要素

- 1. 发送者地址
- 2. 发送者公钥
- 3. MOVE交易代码
- 4. Gas油费
- 5. Gas油费上限
- 6. 序列数

#### **Transactions Change State**



# Libra的Merkle树

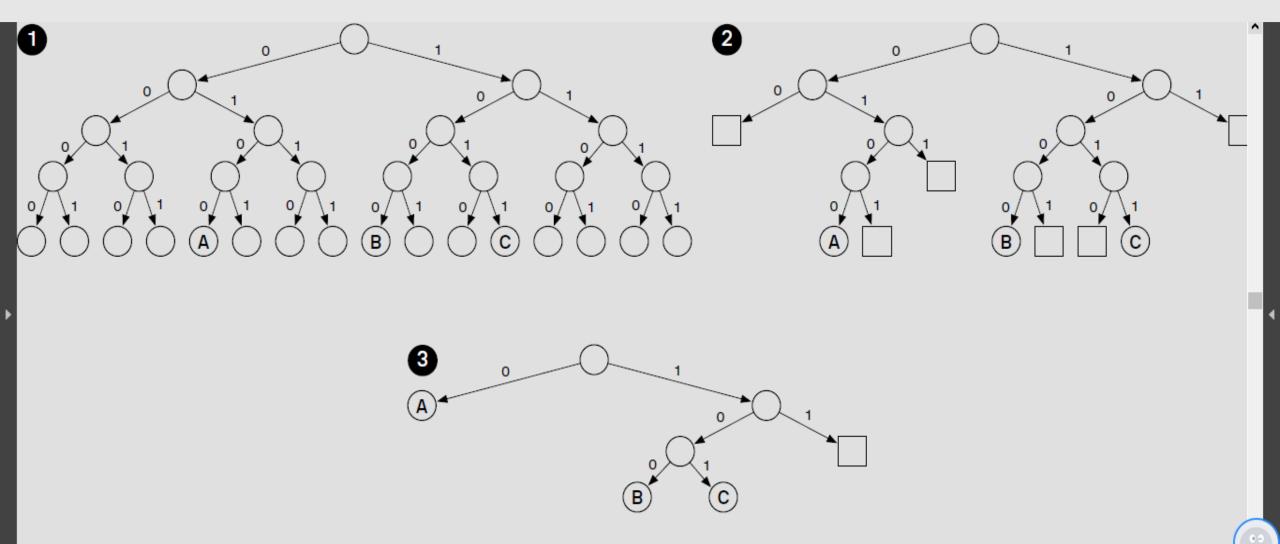


Figure 5: Three versions of a sparse Merkle tree storing  $D = \{0100_2 : A, 1000_2 : B, 1011_2 : C\}$ .

# Libra的Merkle树与交易信息

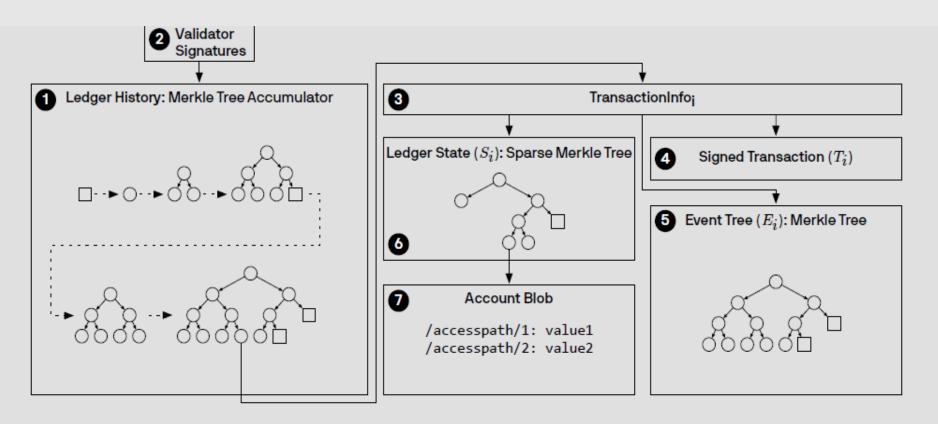


Figure 3: (1) The root hash of the ledger history structure is the authenticator to the full state of the system that is (2) signed by a quorum of validators. As transactions are added to the database, the authenticator (Section 4.2) committing to the ledger history grows (depicted with dashed arrows). Each leaf of the ledger history commits to a (3) TransactionInfo structure. This structure commits to the (4) signed transaction  $(T_i)$ , (5) the list of events generated during that transaction  $(E_i, Section 4.5)$ , and the (6) state after the execution of that transaction  $(S_i, Section 4.3)$ . The state is a sparse Merkle tree with an (7) account blob at each leaf.

# Libra状态机复制机制

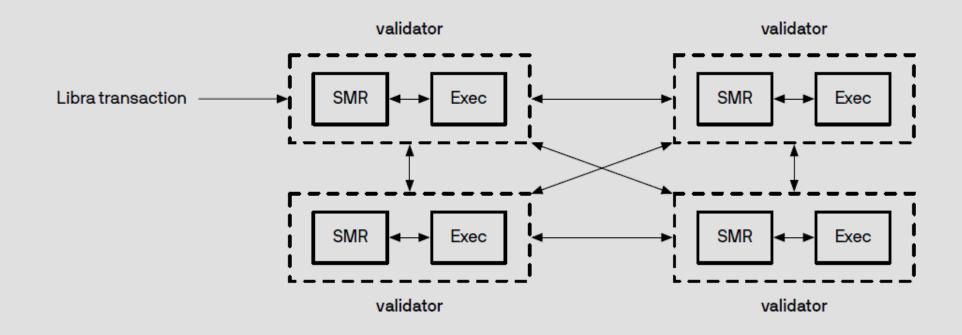


Figure 1: Integration of the SMR module into the Libra Blockchain



# Libra共识机制: LibraBFT

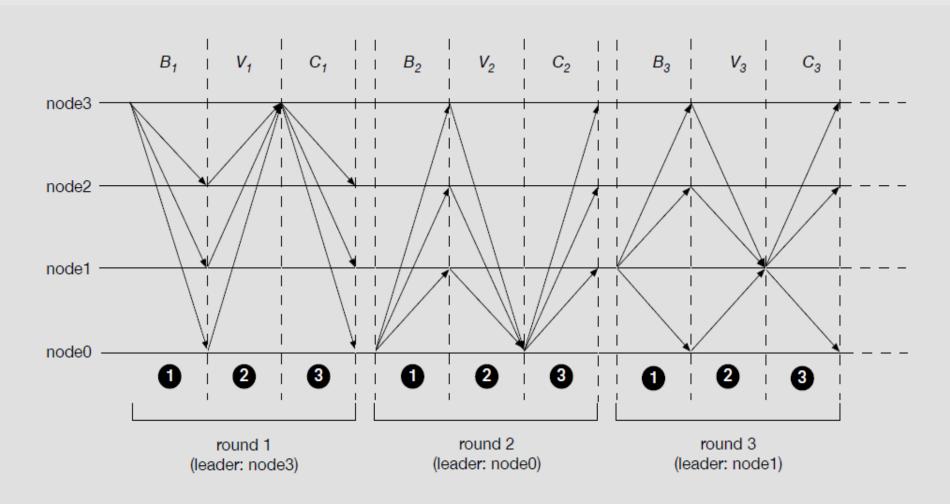
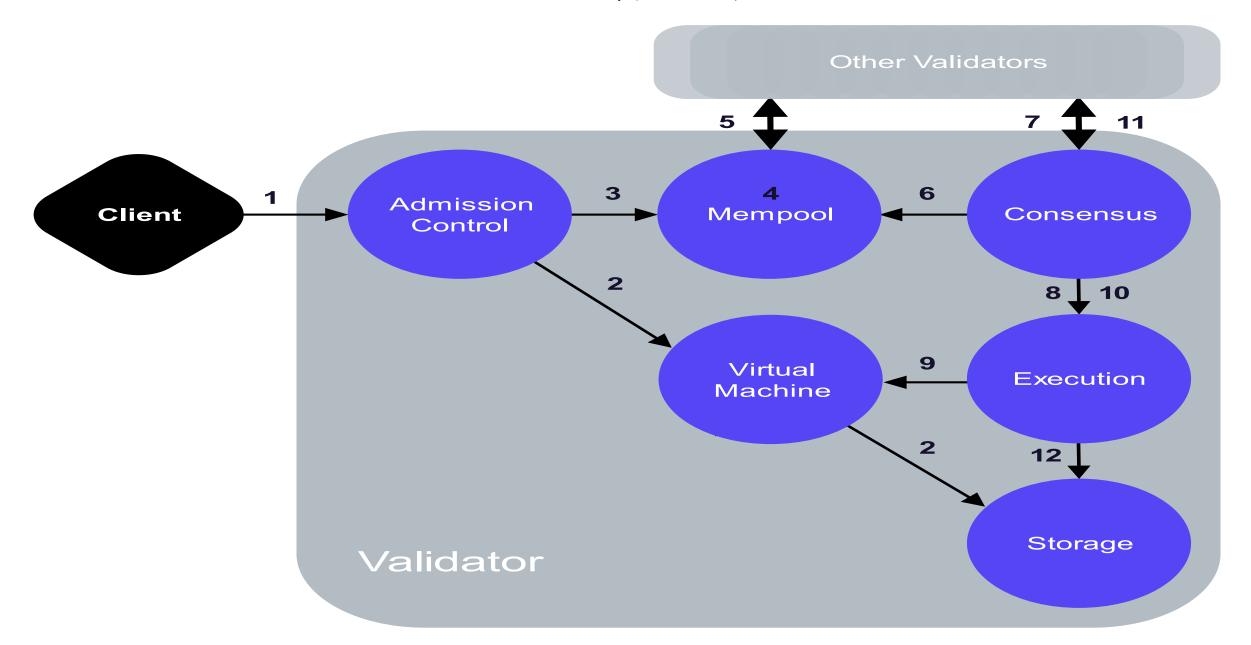


Figure 3: Overview of the LibraBFT protocol (simplified, excluding round synchronization)



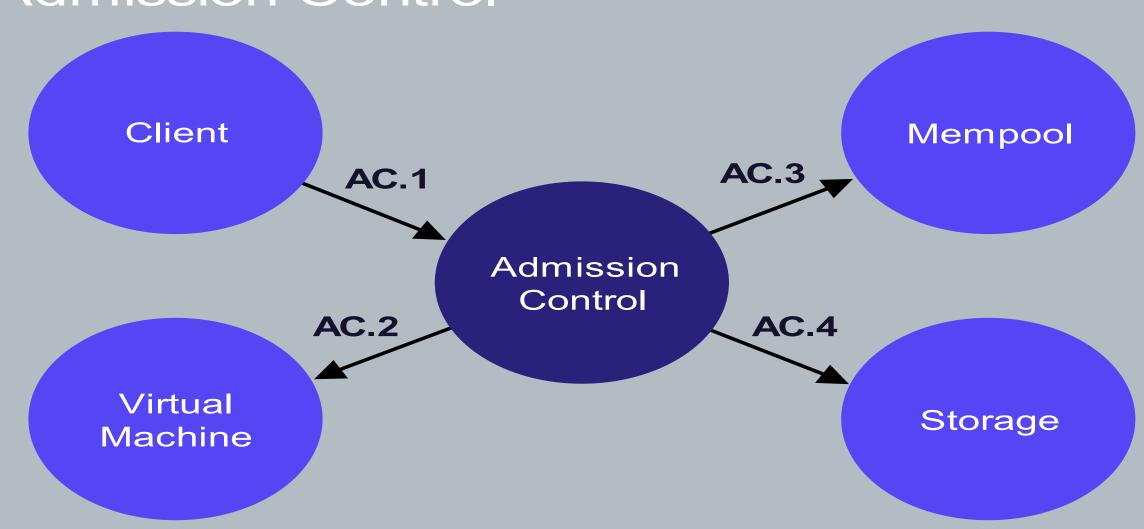
8.50 x 11.00 in <

# Libra交易验证过程

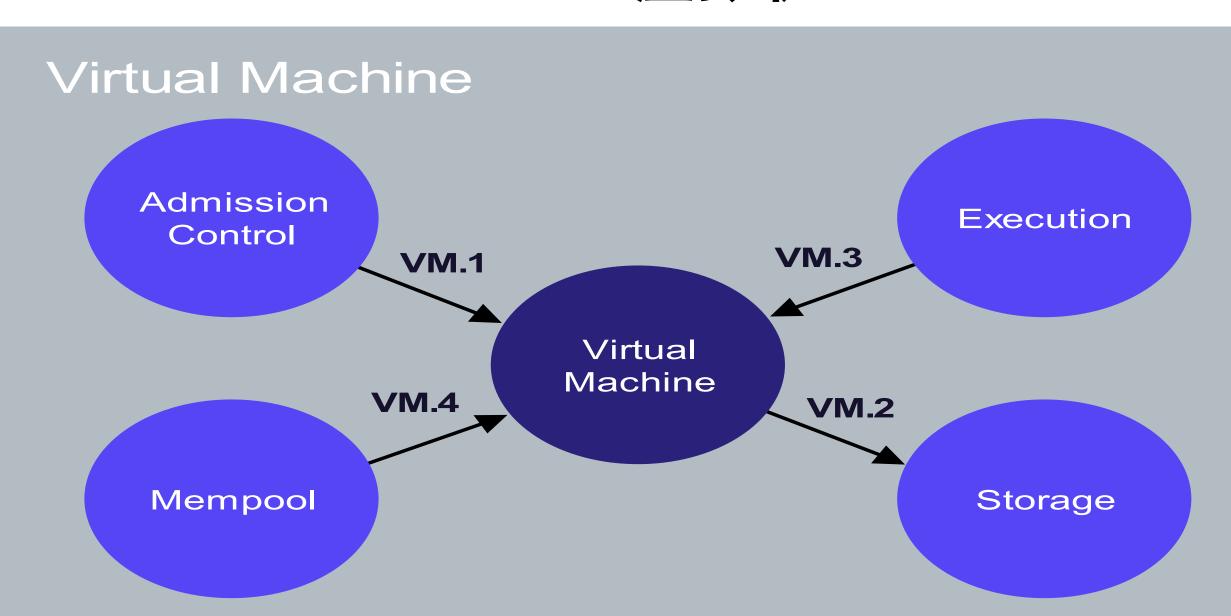


# Libra准入控制

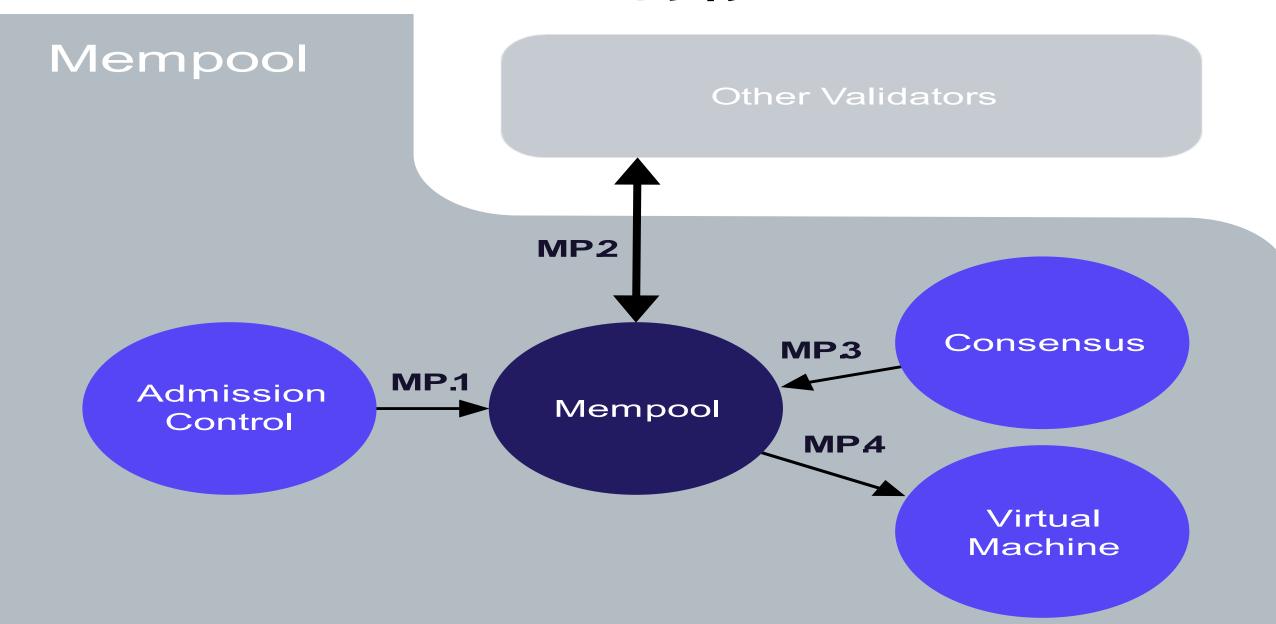
#### **Admission Control**



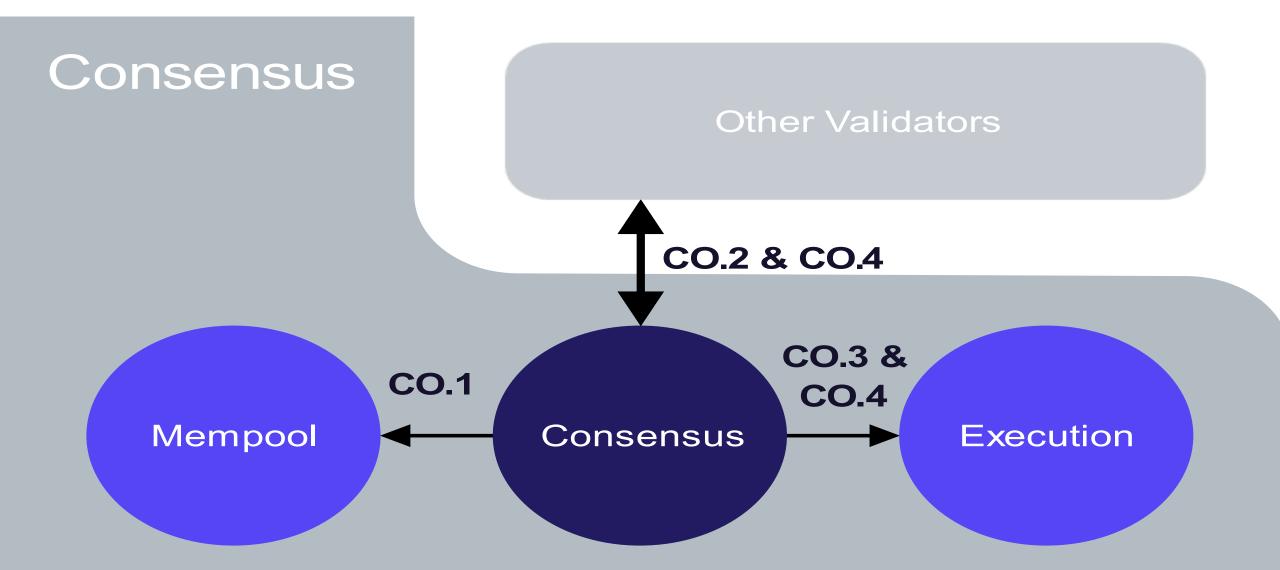
# Libra虚拟机



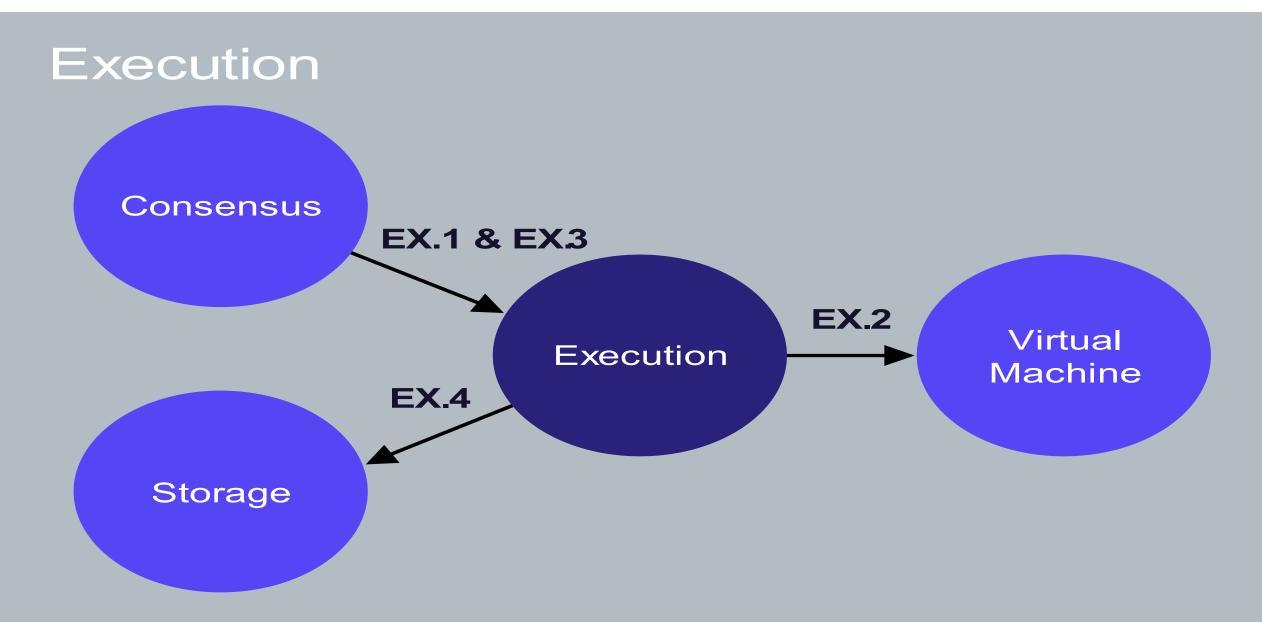
# Libra内存池



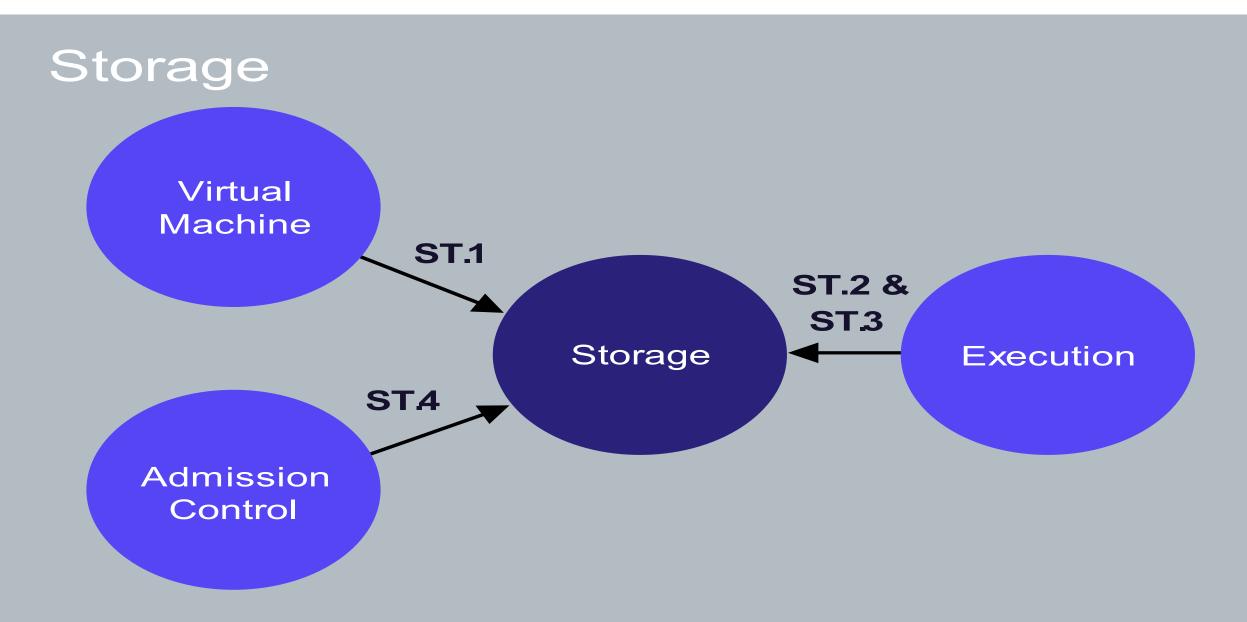
# Libra共识模块

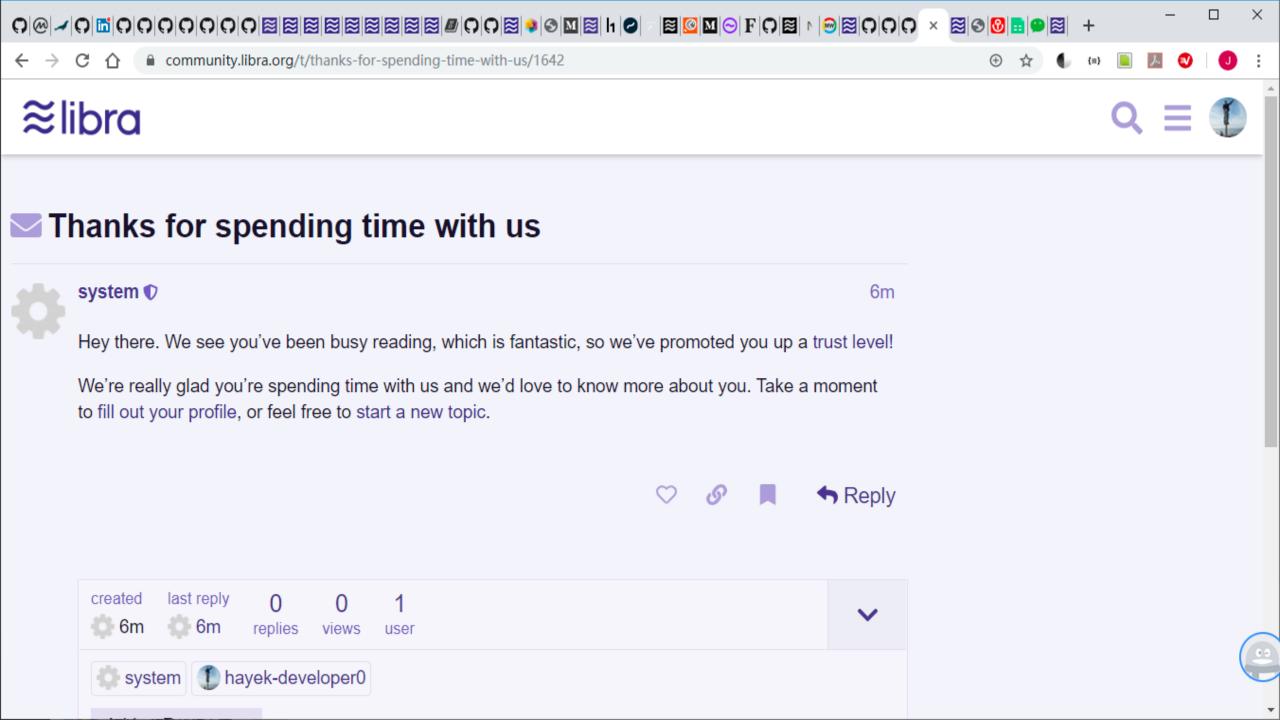


# Libra执行模块



# Libra数据储存





#### **Open-Libra Initiative's Android Wallet**

# https://fir.im/ghup