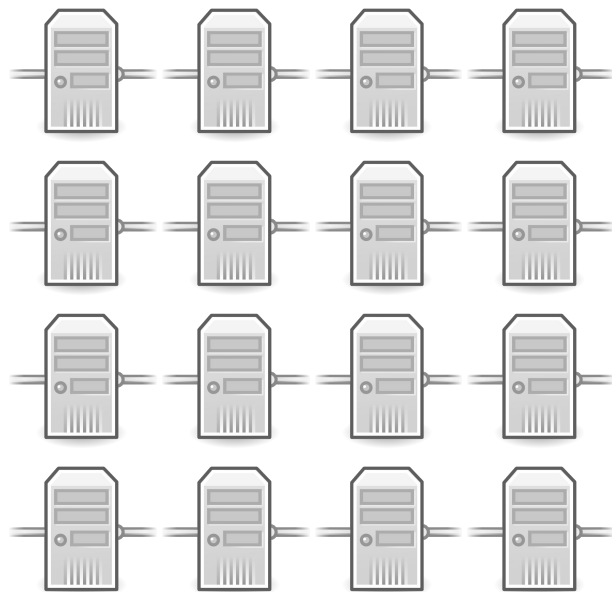


CITA

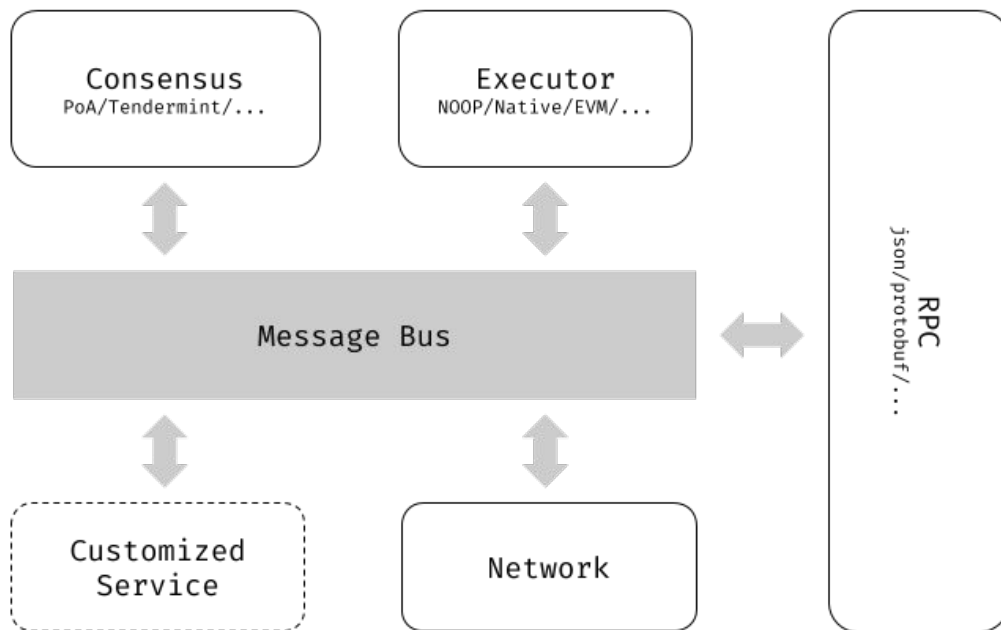
面向未来的区块链架构

分布式 企业 应用

面向企业用户

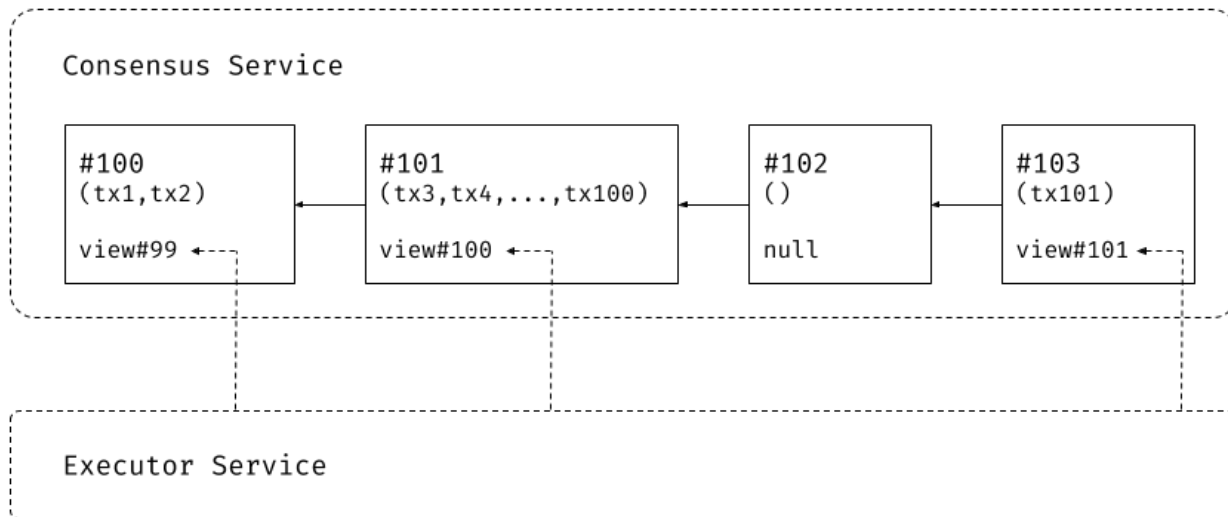


微服务架构



逻辑节点

Asynchronous Transaction Execution 异步交易执行



Executor

NOOP

Native

EVM

Private

```
#[derive(Clone)]Payment
pub struct Payment {
    output: Vec<u8>,
    scalar_string: Scalar,
    array_u256: Array,
    map_u256: Map,
}

impl Contract for Payment {
    fn exec(&mut self, params: ActionParams, ext: &mut Ext)
        -> Result<GasLeft, evm::Error>
    {
        let signature = BigEndian::read_u32(
            params.clone().data.unwrap().get(0..4).unwrap());
        match signature {
            0 => self.init(params, ext),
            1 => self.get(params, ext),
            _ => Err(evm::Error::OutOfGas),
        }
    }

    fn create(&self) -> Box<Contract> {
        Box::new(Payment::default())
    }
}
```

```
impl Payment {
    fn get(&mut self, _params: ActionParams, _ext: &mut Ext)
        -> Result<GasLeft, evm::Error>
    {
        self.output.push(8);
        Ok(GasLeft::NeedsReturn(
            U256::from(100), self.output.as_slice()
        ))
    }

    fn init(&mut self, _params: ActionParams, _ext: &mut Ext)
        -> Result<GasLeft, evm::Error>
    {
        Ok(GasLeft::Known(U256::from(100)))
    }
}
```

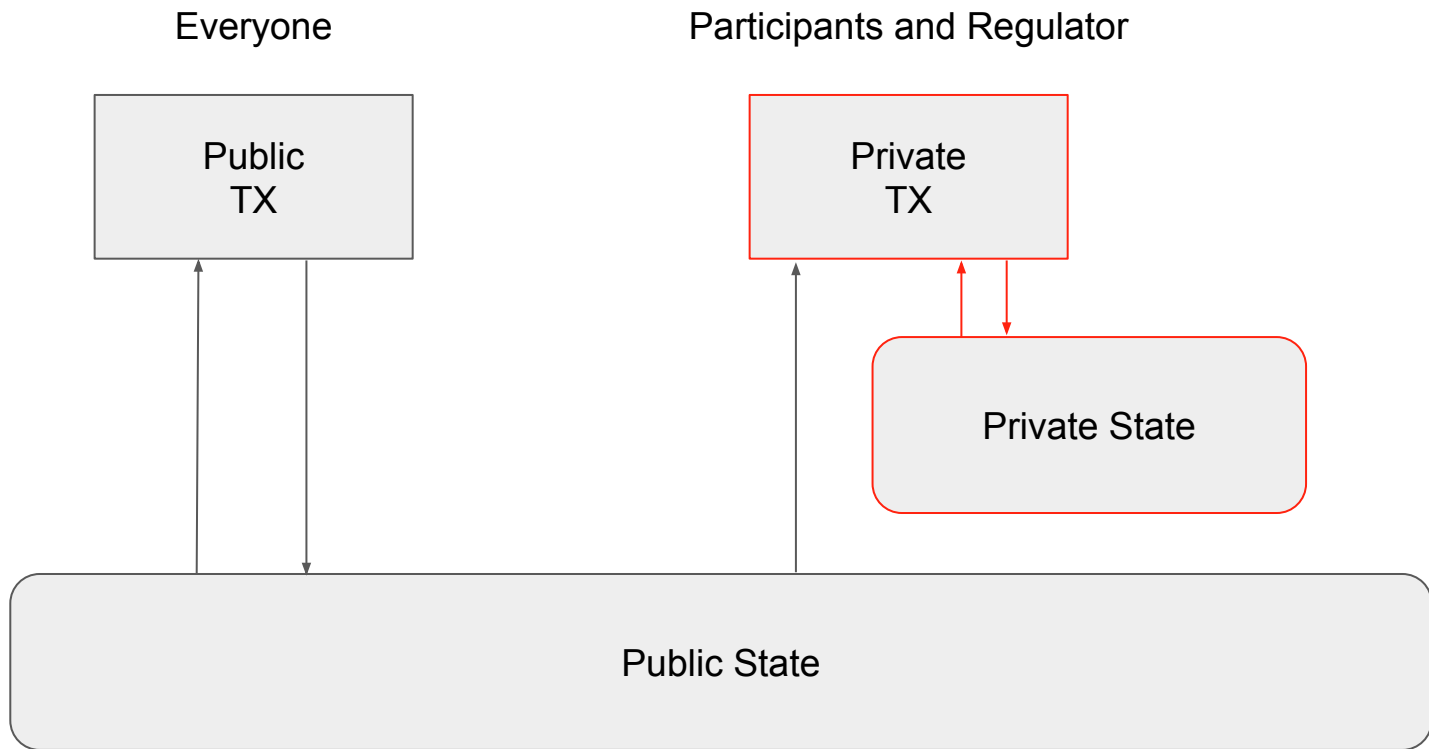
Native Contract (Rust)

配额管理 Quota

隐私交易

如何在不泄漏隐私的情况下验证交易？

1. 局部共识
2. 密码学
3. 可信硬件



可**监管**的隐私交易

系统治理交易

Governance Transaction

操作留痕
状态可变

github.com/cryptape/cita

github.com/cryptape/cita-whitepaper



北大孵化器
PKU INCUBATOR



中国印钞造币

中钞信用卡产业发展有限公司



ENTERPRISE
ETHEREUM
ALLIANCE



并行与分布式系统
研究所



现在支付



contact@cryptape.com