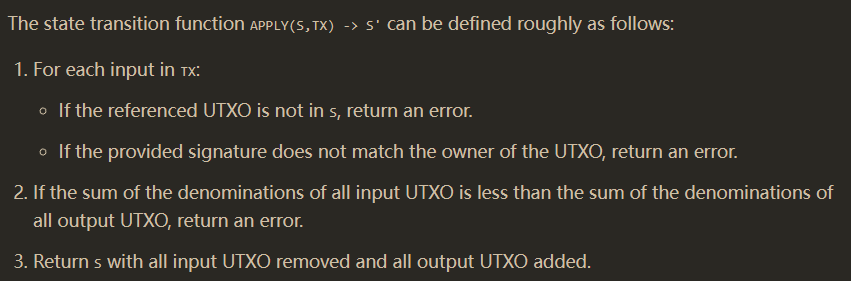
文章链接：[Ethereum Whitepaper | ethereum.org](https://ethereum.org/en/whitepaper/#mining)

## Introduction to Bitcoin and Existing Concepts

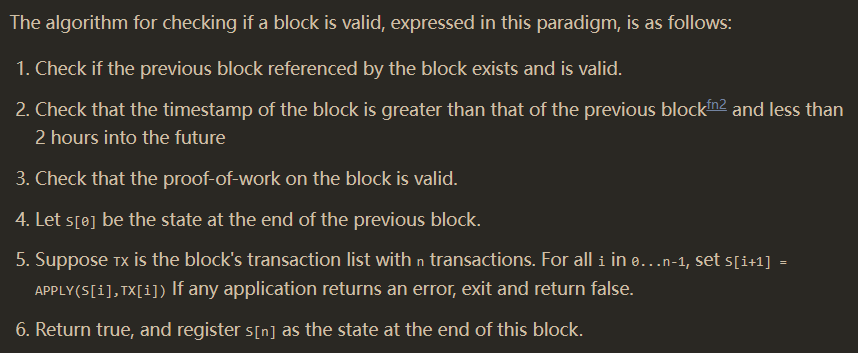
### Bitcoin As A State Transition System

将Bitcoin描述为一种状态转移系统，系统由状态state（多个UTXO）组成，transaction作用于state产生新的state。transaction如何作用于state如下图所示：



### Mining

区块合法性验证如下图所示：



### Scripting

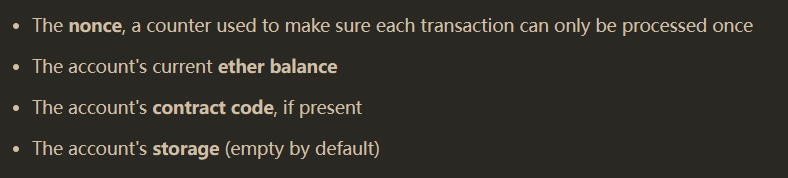
UTXO脚本具有以下局限性：

1. Lack of Turing-completeness：缺乏循环语句，如果需要模拟循环则需要浪费大量空间。
2. Value-blindness：无法细腻度的控制transaction的输入UTXO，如果要实现细腻度控制，则需要transaction发起者拥有大量不同面值的UTXO。比如说要精准地输入5.0BTC的UTXO。
3. Lack of state：UTXO只存在两种状态——被使用或者没被使用。因此，Bitcoin无法创建多状态合约。
4. Blockchain-blindness：UTXO无法获取Blockchain的数据，比如nonce、timestamp和previous block hash。因此，UTXO脚本被剥夺了一种有效获取随机数的方法。

## Ethereum

### Ethereum Accounts

同Bitcoin一样，都属于状态转移系统，区别是状态state是由account组成，类似于银行记账机制。account由以下四部分组成：



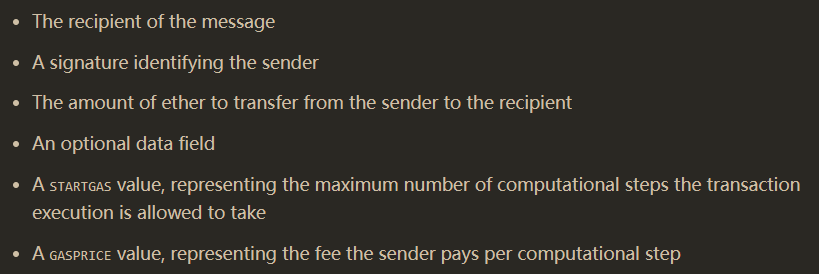
Ethereum存在两种account：

1. Externally owned accounts（主动）：通过私钥进行控制，也就是进入Ethereum的用户，不具备contract code。可以通过创建和签名transaction向其他accouts发送message。
2. Contract accounts（被动）：通过contract code进行自我控制。每当其收到message，都将激活contract code，进行相应的逻辑处理。

注意：以上的“发送”虽然指的是发给其他accounts，其实是发送给所有miner。miner是Externally owned accounts的一部分。miner通过挖矿宏观上来实现“发送”动作的完成。

### Messages and Transactions

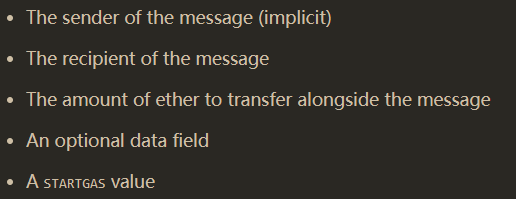
Externally owned accounts发送的message叫做transaction。它的组成如下图所示：



STARTGAS和GASPRICE来预防拒绝服务攻击，防止contract code进入死循环。任何Externally owned accounts将要为他要求执行的contract code付出的内存、带宽和算力等资源支付等比的eher。

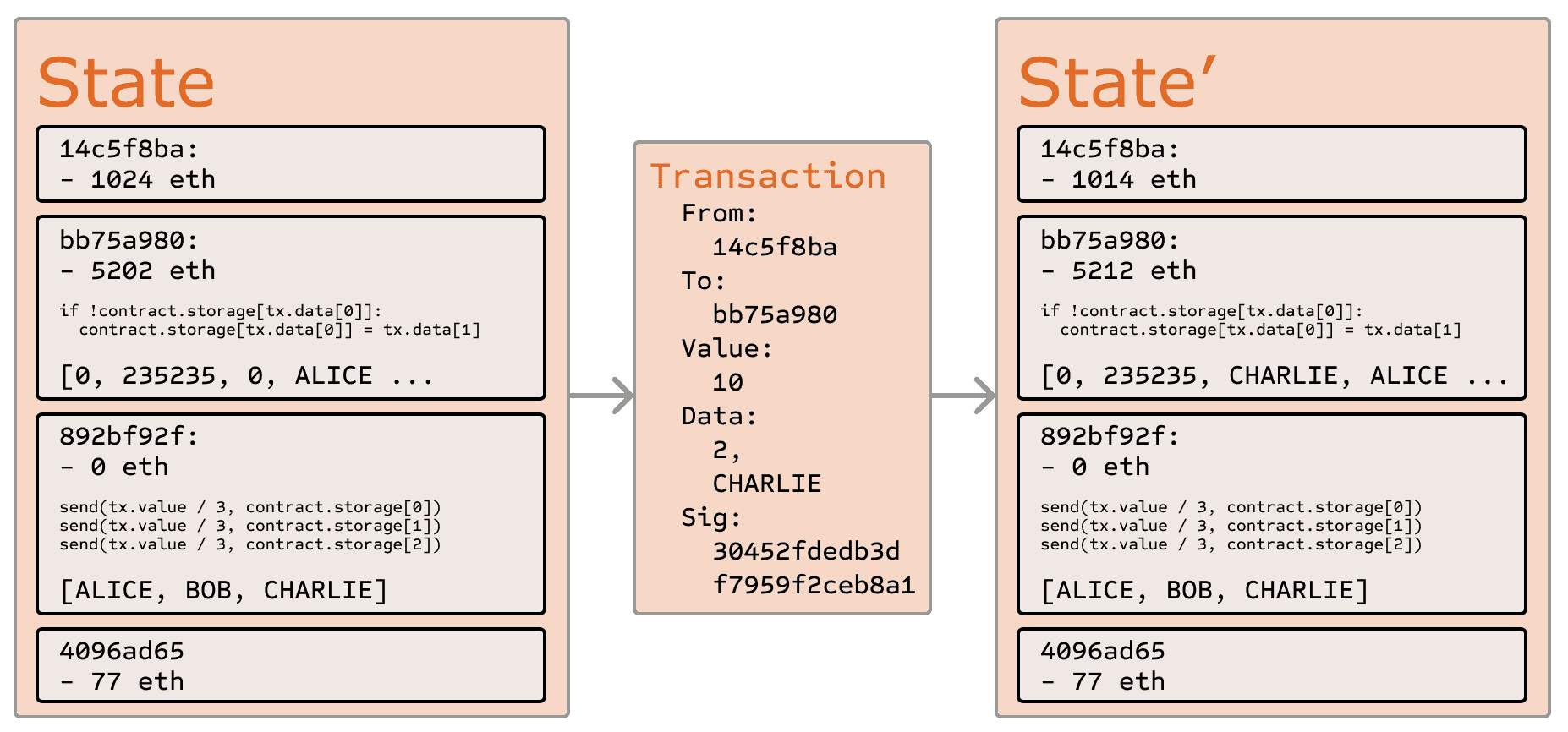
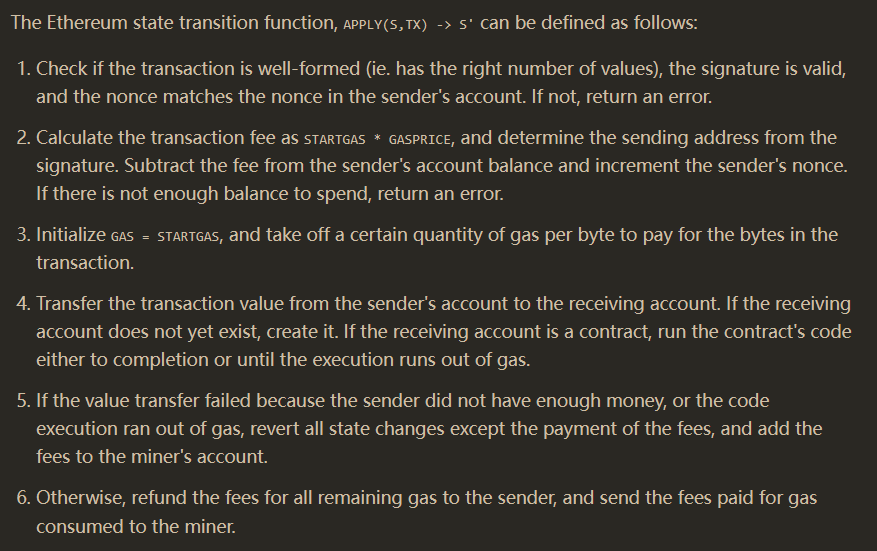
### Messages

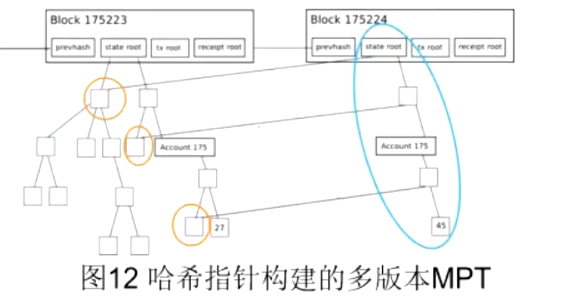
Contract accounts发送的消息称作Message，其组成如下图所示：



Contract accounts可以通过CALL opcode来创建并发送message，收到message的其他Contract accounts 执行相应的contract code，这些递归调用关系的contract code共享STARTGAS。

### Ethereum State Transition Function

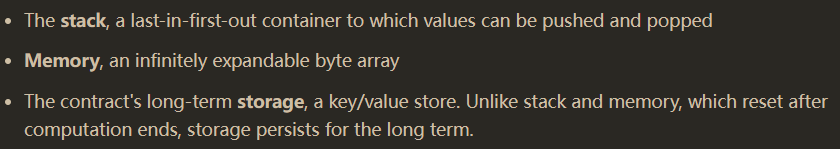
 



通过MPT存储的状态数据，在修改时不需要生成一个全新的MPT，只需生成发生改变的状态路径，没发生改编的通过引用的方式连接。

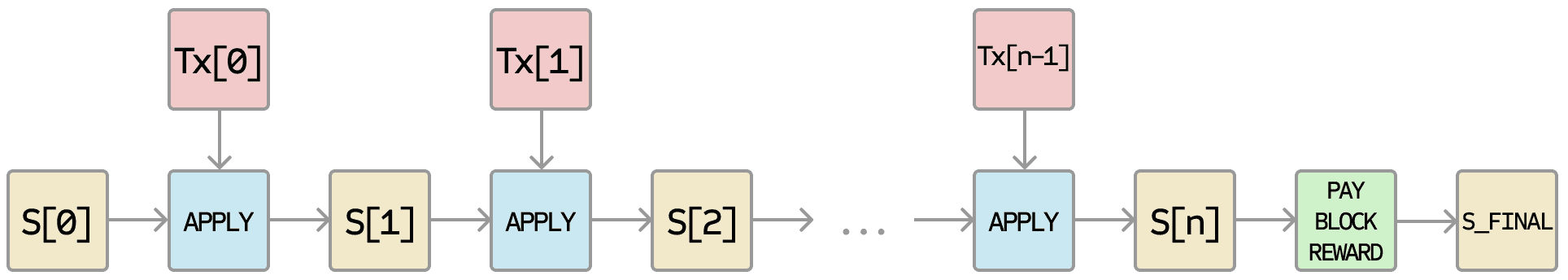
### Code Execution

Ethereum virtual machine code（EVM code）由一系列字节组成，每个字节代表一个操作。每个操作涉及下图所示三个部分：

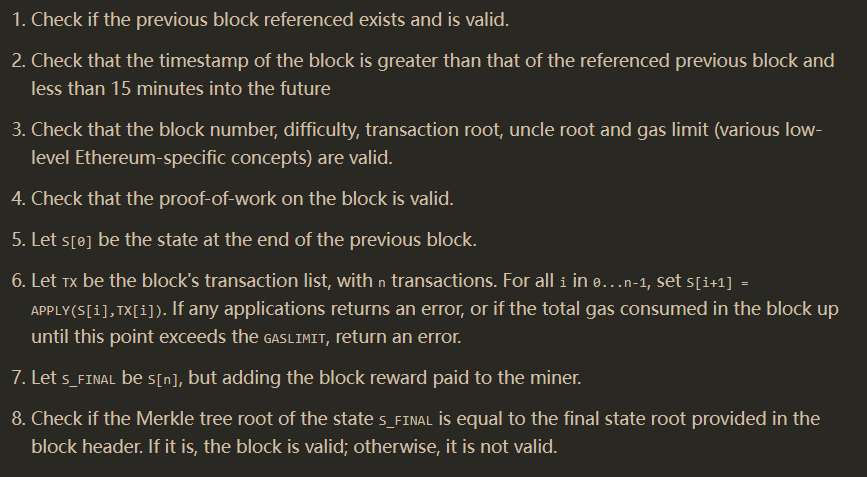


EVM code的运算状态集可以定位为该元组：(block\_state, transaction, message, code, memory, stack, pc, gas)。任何的操作都是对这个状态进行修改。

### Blockchain and Mining



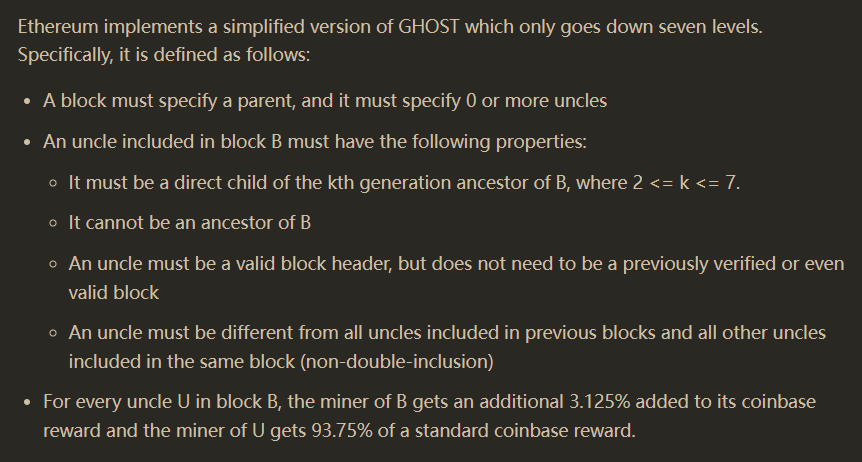
不像Bitcoin区块头，Ethereum区块头还包括transaction list和出块节点所计算的最终状态S’[n]（in the block header）。区块合法性验证如下图所示：



transaction中可能需要执行一些contract code，这些code在区块合法性验证阶段被执行。因此contract code会在所有nodes之中执行。

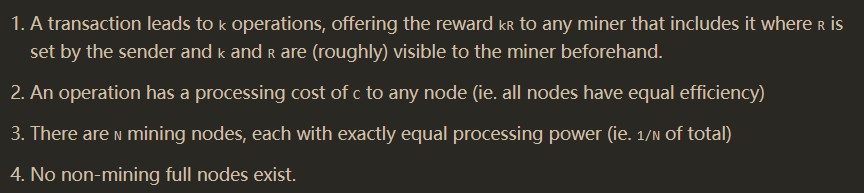
## Miscellanea And Concerns

### Modified GHOST Implementation

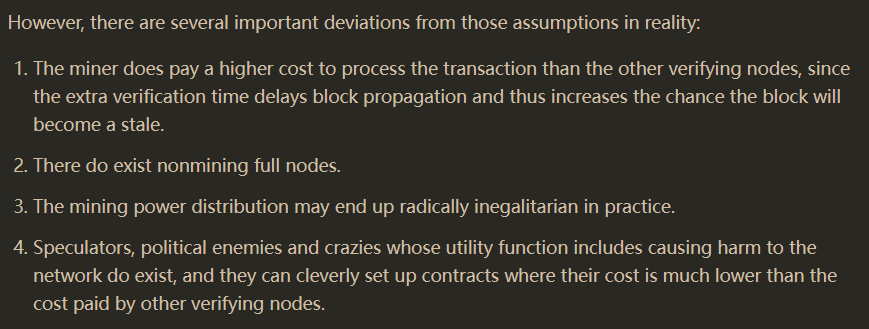


### Fees

如何选择合适的transaction fees如下图所示：



上述假设中只需满足kR/N>kC或者R>NC即可。



Ethereum中采用动态调整C的方式控制fees。

### Computation And Turing-Completeness

transaction执行时需要设置STARTGAS可以有效防止infinite loops。除此之外，transaction中若GAS消耗完仍没有完成，则会revert之前的所有操作，但是fees仍然会被抽取。以此来解决Turing-Completeness所带来的潜在危害。

### Scalability

Ethereum随着时间流逝，full nodes所需的空间也会越来越大。因此，后期可能只有少数的full nodes，但是Ethereum提供了一种validation protocol基于每个full node存储整个blockchain来确保至少需要一个诚实的full node即可保证安全性。