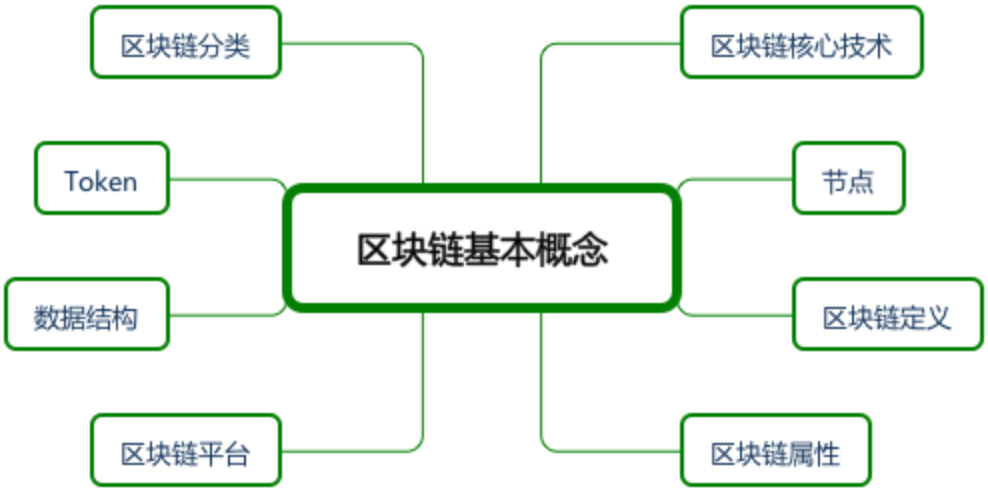
区块链基本概念



1. 区块链核心技术

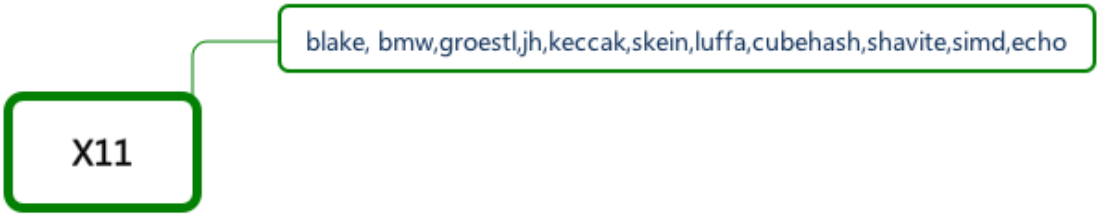
1.1. 密码学算法

1.1.1. 哈希算法

SHA1

SHA2

X11



blake, bmw,groestl,jh,keccak,skein,luffa,cubehash,shavite,simd,echo

SHA3

Keccak

1.1.2. 数字签名算法

DSA

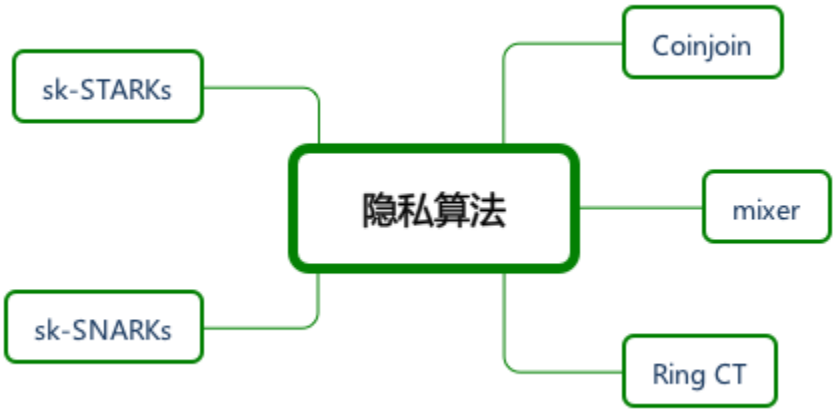
ECDSA

RSA

Schnorr

Ed25519

1.1.3. 隐私算法



Coinjoin

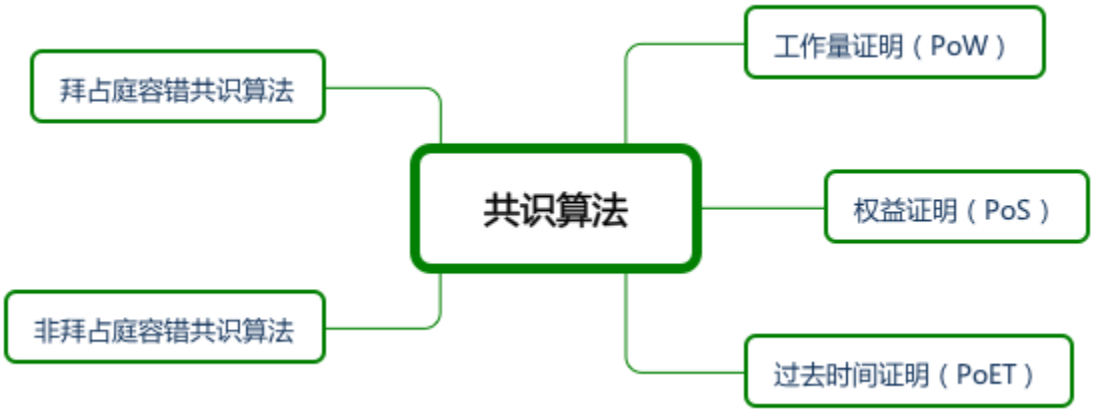
mixer

Ring CT

sk-SNARKs

sk-STARKs

1.2. 共识算法



1.2.1. 工作量证明（PoW）

Bitcoin PoW, Ethash

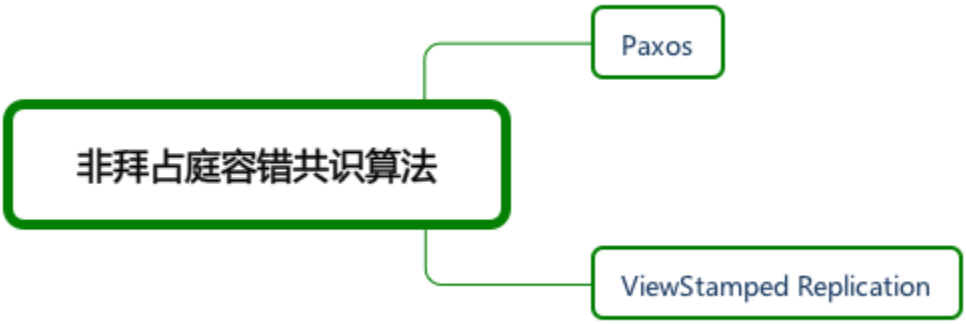
1.2.2. 权益证明（PoS）

LPoS

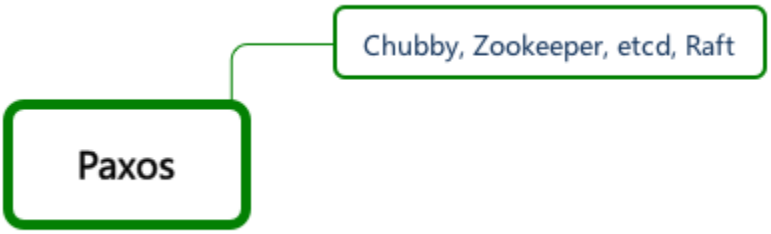
DPoS

1.2.3. 过去时间证明（PoET）

1.2.4. 非拜占庭容错共识算法



Paxos



Chubby, Zookeeper, etcd, Raft

ViewStamped Replication

1.2.5. 拜占庭容错共识算法

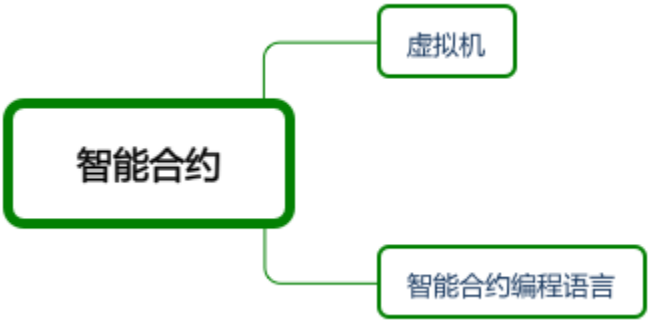
PBFT

Zyzzyva

1.3. P2P网络

1.3.1.

1.4. 智能合约

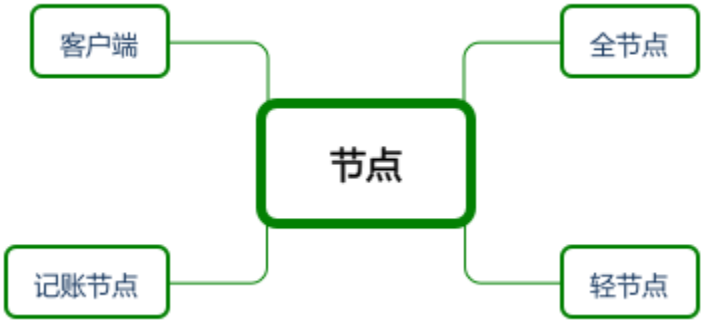


1.4.1. 虚拟机

1.4.2. 智能合约编程语言

1.5. 分布式存储

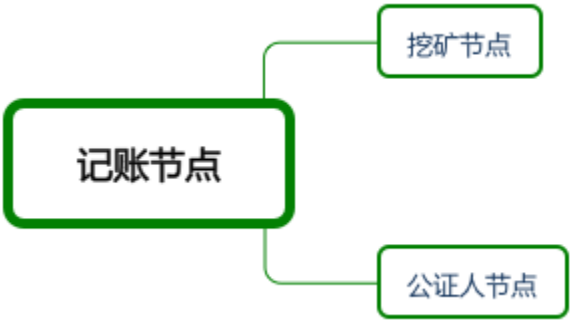
2. 节点



2.1. 全节点

2.2. 轻节点

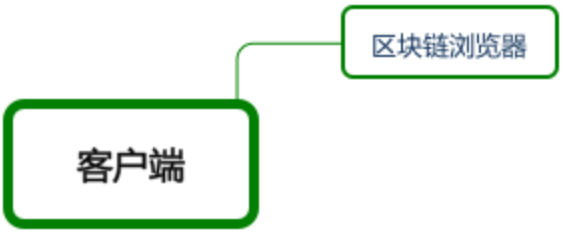
2.3. 记账节点



2.3.1. 挖矿节点

2.3.2. 公证人节点

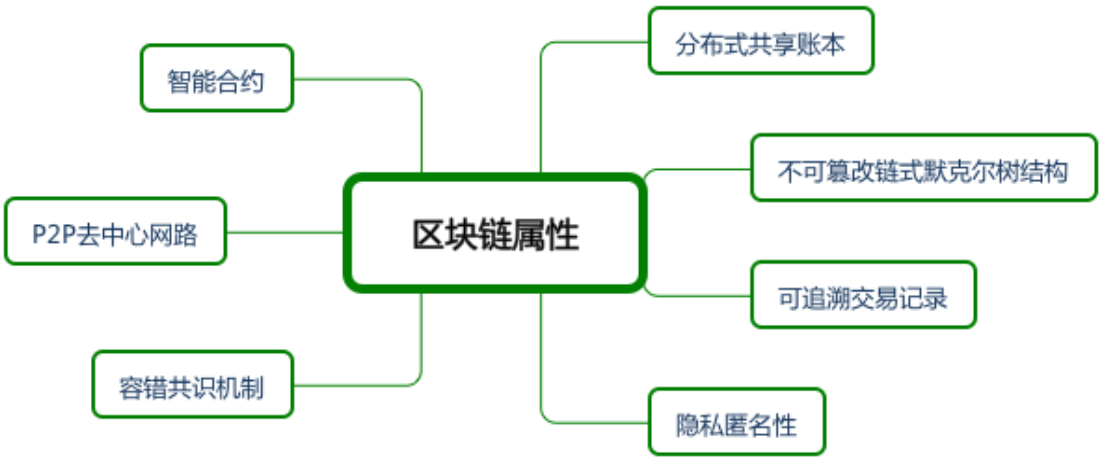
2.4. 客户端



2.4.1. 区块链浏览器

3. 区块链定义

4. 区块链属性



4.1. 分布式共享账本

4.2. 不可篡改链式默克尔树结构

4.3. 可追溯交易记录

4.4. 隐私匿名性

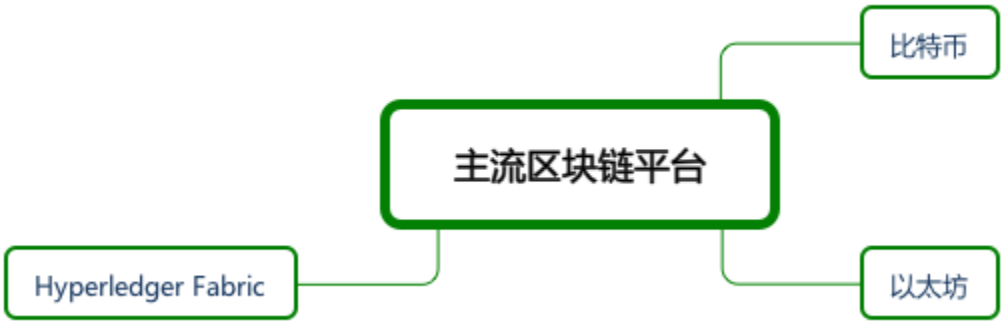
4.5. 容错共识机制

4.6. P2P去中心网路

4.7. 智能合约

5. 区块链平台

5.1. 主流区块链平台



5.1.1. 比特币

比特币地址

比特币数据结构

比特币脚本

锁定脚本

解锁脚本

比特币**PoW**流程

比特币扩容方案

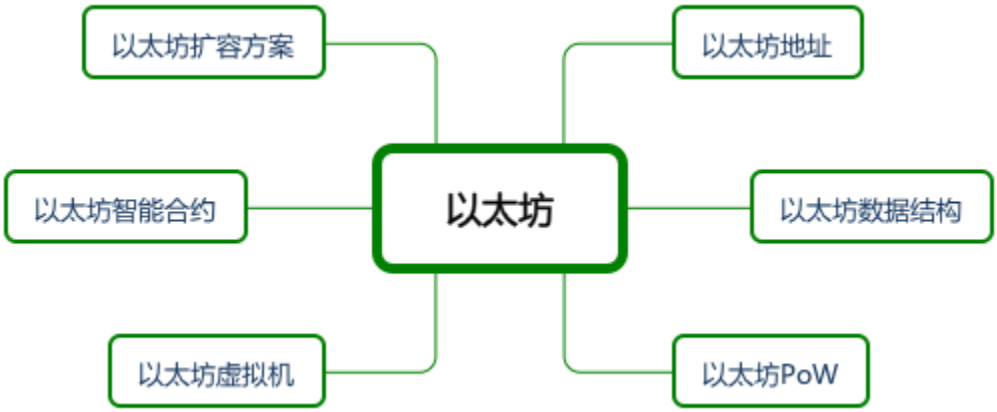
闪电网络

隔离见证SegWit

SegWit2x

比特币分叉**BCH**

5.1.2. 以太坊



以太坊地址

以太坊数据结构

以太坊**PoW**

以太坊虚拟机

以太坊智能合约

以太坊扩容方案

雷电网络

分片

Casper共识

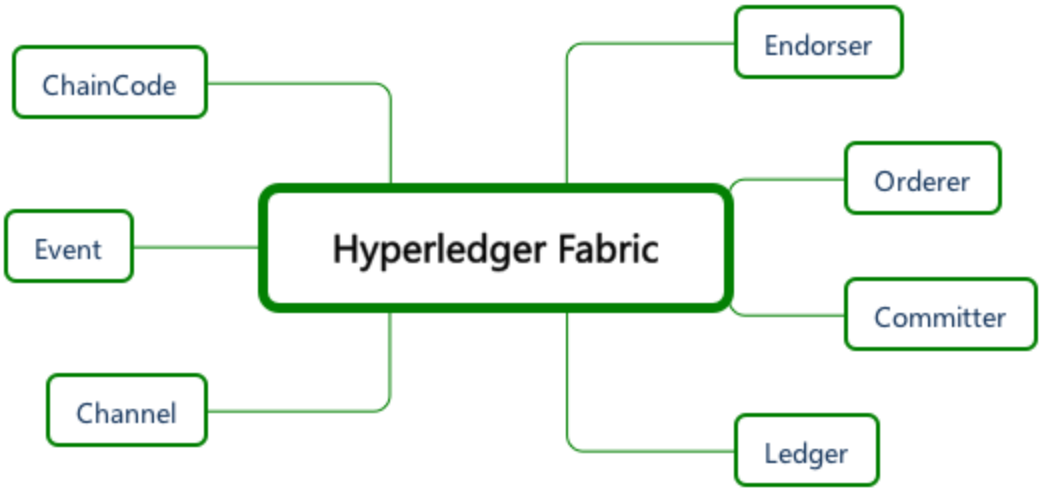
Metropolis大都市

拜占庭

君士坦丁

Plasma

5.1.3. Hyperledger Fabric



Endorser

Orderer

Committer

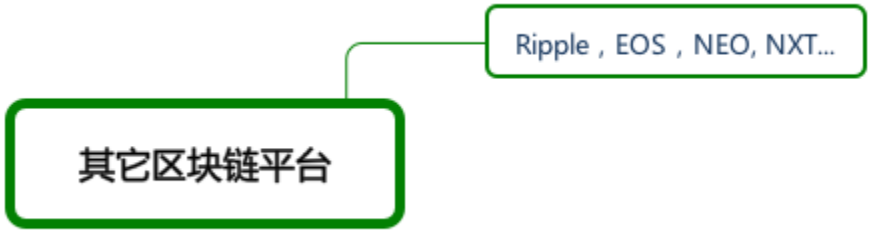
Ledger

Channel

Event

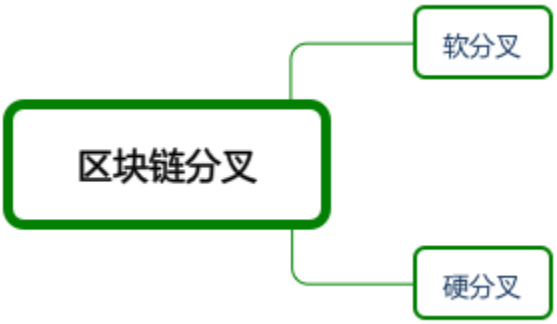
ChainCode

5.2. 其它区块链平台

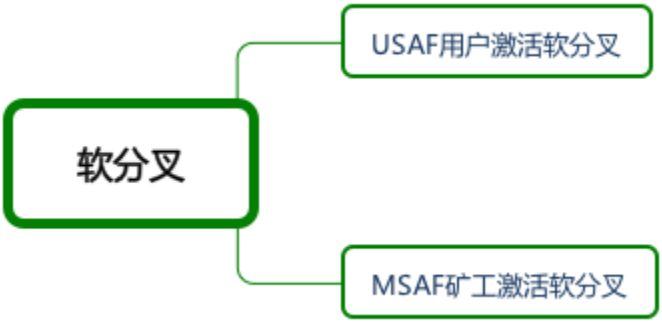


5.2.1. Ripple， EOS， NEO, NXT...

5.3. 区块链分叉



5.3.1. 软分叉



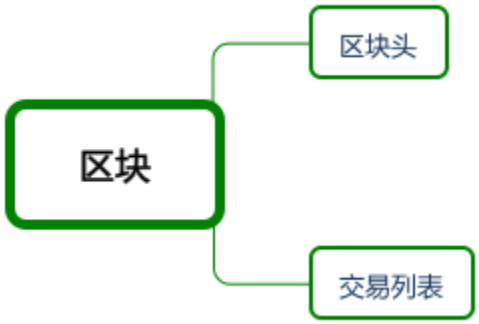
USAF用户激活软分叉

MSAF矿工激活软分叉

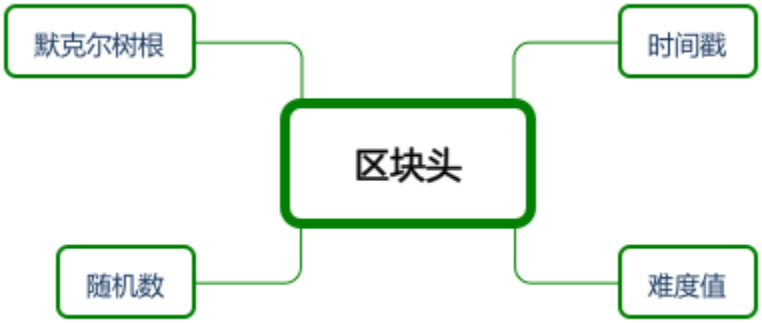
5.3.2. 硬分叉

6. 数据结构

6.1. 区块



6.1.1. 区块头



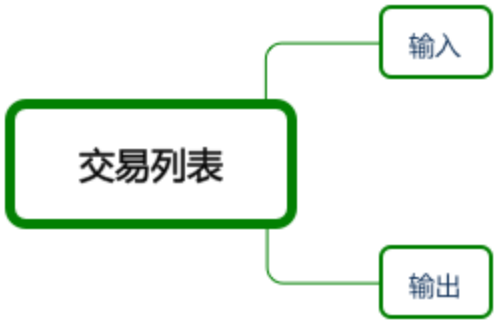
时间戳

难度值

随机数

默克尔树根

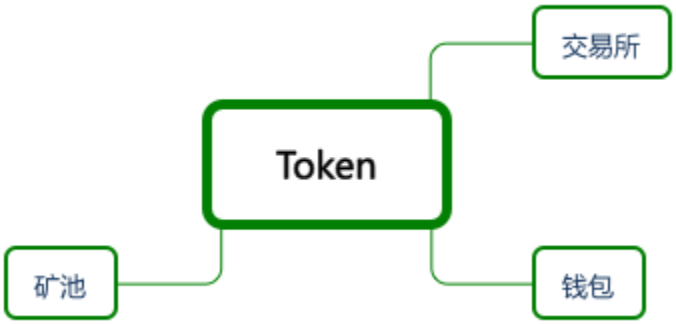
6.1.2. 交易列表



输入

输出

7. Token

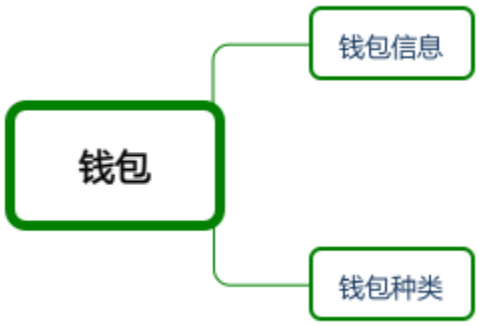


7.1. 交易所

7.1.1. 中心化交易所

7.1.2. 去中心化交易所

7.2. 钱包



7.2.1. 钱包信息

私钥

公钥

地址

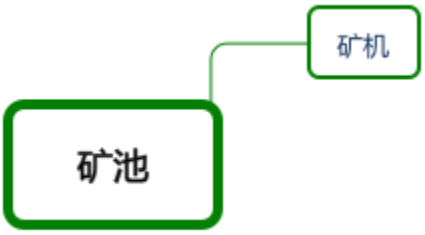
7.2.2. 钱包种类

冷钱包

热钱包

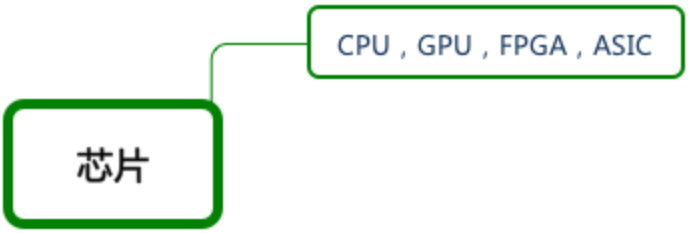
移动钱包

7.3. 矿池



7.3.1. 矿机

芯片



CPU， GPU， FPGA， ASIC

8. 区块链分类

8.1. 公有链

8.2. 联盟链

8.3. 私有链