深入浅出跨链技术

by 谈国鹏

目录

CATALOG

01

PART 01

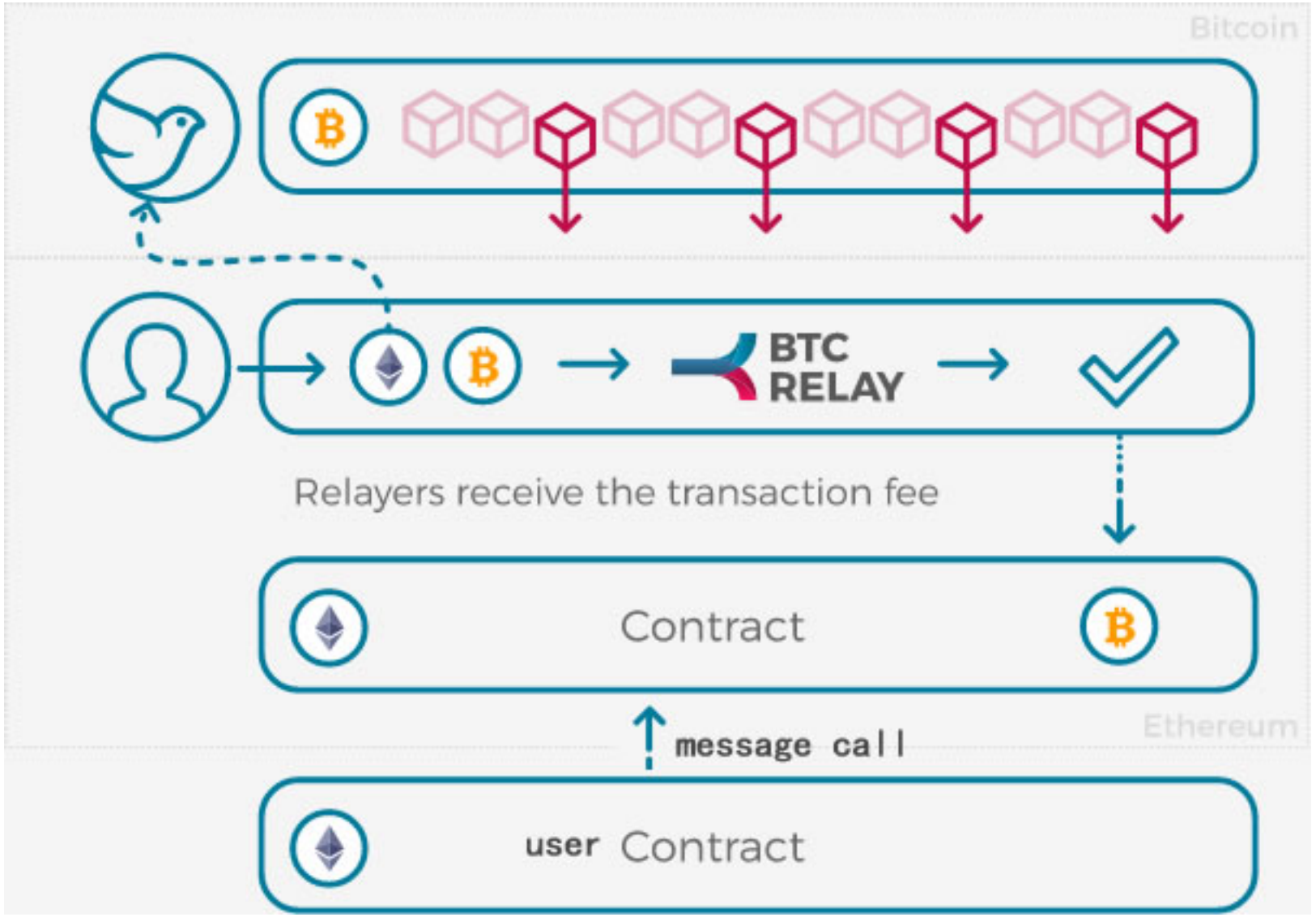
第一部分
什么是跨链？

代码示例：

```
address addr = 0x41f274c0023f83391de4e0733c609df5a124c3d4;
if(! addr.verifyBTCTx .value(feeToUseTheFunc)
        (rawTransaction, 3, merkleSibling, 0x000…)){
throw;
}
```

什么是跨链？

如何工作：

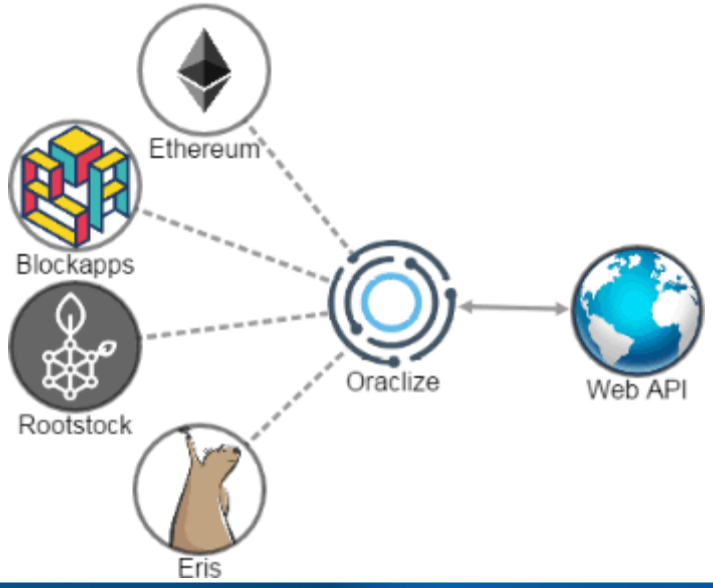

Bitcoin
BTC
RELAY
Relayers receive the transaction fee
Contract
Ethereum
message call
user Contract

跨链现状

- 目前知名的公有链超过100条，几乎所有都是不知道外部世界，不具备native的跨链能力；
- 几个为特殊目的设计的侧链，如：RootStock天然具有跨越其主链（RSK的主链bitcoin）的能力；
- 如bitcoin不知道有ethereum的存在，natively ethereum也不知道bitcoin的存在。

为什么不支持跨链？- 因为跨链难

- 每个节点要有单独验证的能力；
- 要去中心化的输入；
- 区块链不光是跨链难，对于外部世界信息的获取和验证都难（oracle issue）



跨链的目的

- 实现不同链之间的资产转移；
- 原子性交换（atomic swap）；
- 解决oracle的问题；
- 实现资产质押；
- 它链信息或事件的读取和验证；

未来的跨链

- 新起的项目可能会支持natively跨越主流区块链网络（如bitcoin和ethereum）；
- 通过智能合约实现跨链（如BTCRelay）；
- Polkadot 多链跨链系统；
- Ripple实现全球结算网络；
- 比特股BTS去中心化数字资产交易所；
- Cosmos跨链资产交换；

02

PART 02

第二部分
跨链技术详解

3种主要的跨链技术

1. 单个或多个实体（multisig）的公证技术（notary）
2. 侧链技术（sidechain）/中继技术（relay）
3. 哈希锁定（hash-locking）

什么是公证技术（notary）

例1：PBFT

- PBFT协议中每个节点就是一个公证员，获得节点中超过2/3的节点签名，表示公证有效；

什么是公证技术（notary）

例2：multisig

- 实现锚锭侧链时，主链发送交易到侧链系统所拥有的一个多重签名地址。要花费这个交易，必须同时提供如8-of-10的multisig签名；

什么是公证技术（notary）

- 公证技术使用广泛，更多例子如：
  - 字节雪球（byteball）的witness；
  - Zcash 6个参数生成的过程；

公证技术的优缺点

- 优点：
  - 简单；
- 缺点：
  - 你需要信任1个或多个实体；

侧链技术（side-chain）

定义

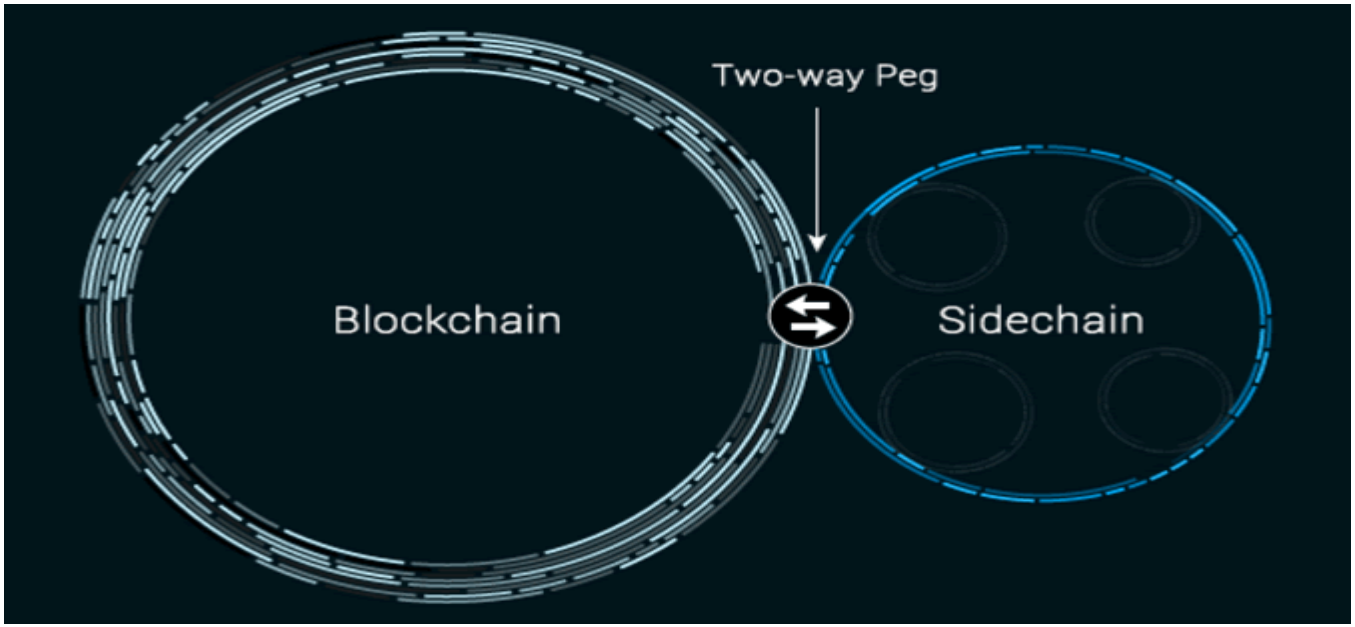
- 最早由blockstream定以于相关白皮书中：sidechain is a blockchain that validates data from other blockchains

侧链技术的要点

- 主链通常支持SPV(Simple Payment Verification)：
- 通过向侧链提供SPV proof来验证主链中发生的事件；
- 向侧链提交主链SPV信息（header、merkle tree）的节点去中心化的问题；

侧链应用示例：根链（rootstock）

- RSK：2-way-pegged sidechain
- Semi-trust-free：应用了notary机制



中继技术（relay）

定义

- 在两个链A、B之间存在的第三方数据结构C，C称为A和B之间的中继。如果C本身也是区块链结构，通常称为relay-chain。

中继技术主要示例

- BTCRelay（既是中继，也是侧链）
- Polkadot里的relay-chain

BTCRelay

verifyTx(rawTransaction, transactionIndex, merkleSibling, blockHash)

在以太坊智能合约上验证一笔比特币付款的有效性及相关信息。

- rawTransaction - raw bytes of the transaction
- transactionIndex - transaction's index within the block, as int256
- merkleSibling - array of the sibling hashes comprising the Merkle proof, as int256[]
- blockHash - hash of the block that contains the transaction, as int256

Returns (uint256) hash of the verified Bitcoin transaction

0 if rawTransaction is exactly 64 bytes in length or fails verification

哈希锁定（hash-locking）

定义

- Hash-locking起源于闪电网络的HTLC（Hashed TimeLock Contract），是通过锁定一段时间猜hash原值（preimage）来兑现支付(redeem)的一种机制。

比特币的HTLC

OP_IF

OP_HASH160 <Hash160(R)> OP_EQUALVERIFY

2 <Alice2> <Bob2> OP_CHECKMULTISIG

OP_ELSE

2 <Alice1> <Bob1> OP_CHECKMULTISIG

OP_ENDIF

用hash-locking实现原子交换（例：20ETH <-> 1BTC）

1. A生成随机数s，并计算h=hash(s)，将h发送给B;
2. A生成HTLC，超时时间设置为：2小时，如果2小时内B猜出随机数s，则取走1 BTC，否则A取回1BTC；
3. B在以太坊里部署智能合约，如果有谁能在1小时内提供一个随机数s，让其hash值等于h则可以取走智能合约中20ETH；
4. A调用B部署的智能合约提供正确的s，取走20ETH；
5. B得知s，还有1小时时间，B可以从容兑现A的HTLC的1 BTC。

03

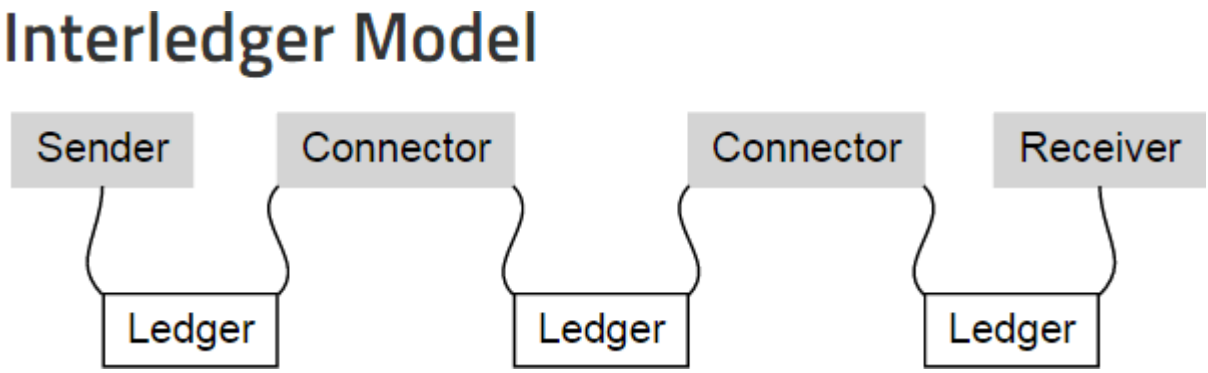
PART 03

第三部分
跨链项目分析

3种主要的跨链项目

1. Interledger（ripple） & 比特股（BTS）
2. polkadot
3. cosmos

interledger(ripple)



Interledger 使用 notary 机制：

connector使用拜占庭算法确保某件事件（支付事件）的发生。

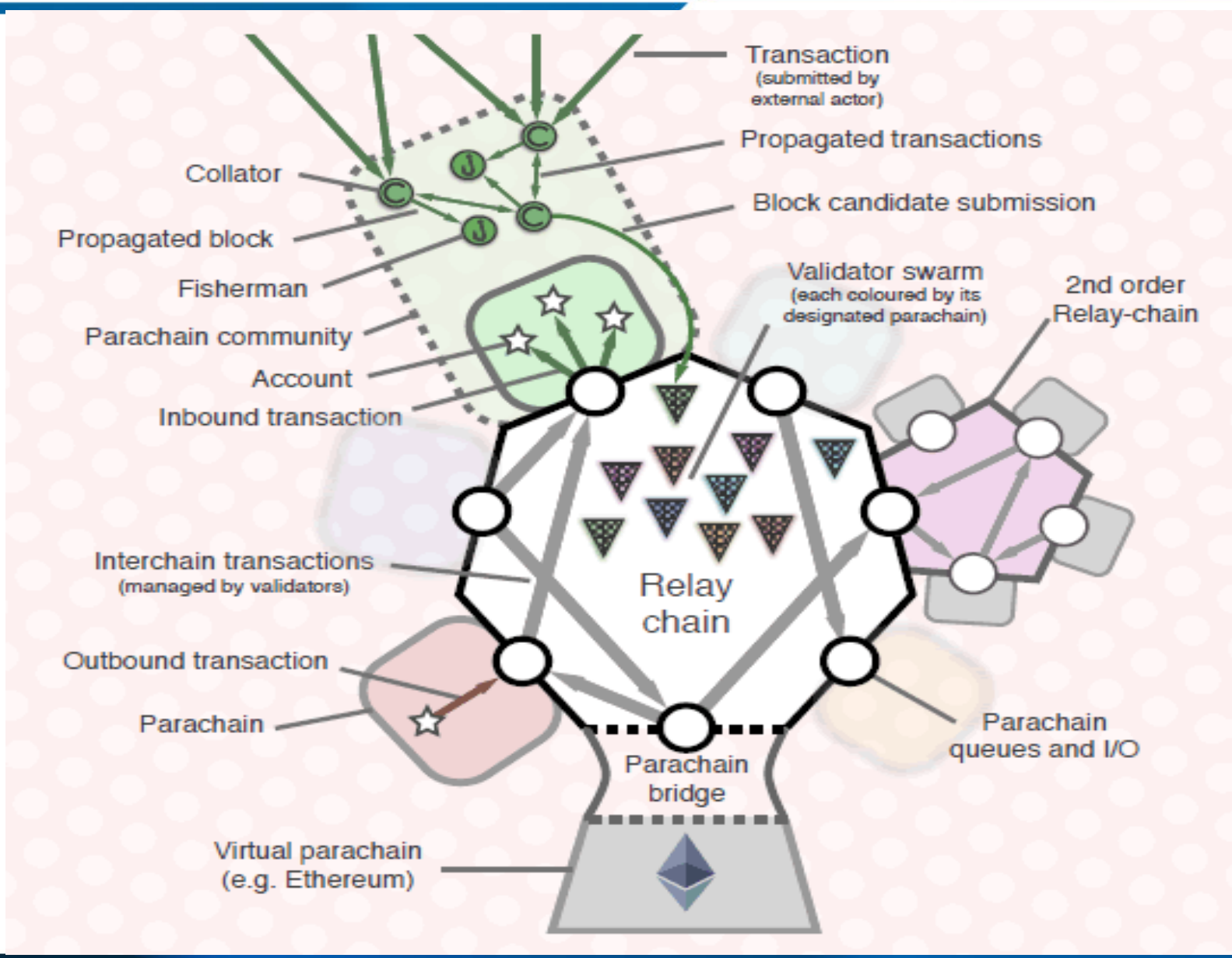
去中心化交易所(BTS)

- 跨链机制和integerledger类似；
- 可以挂单（有内盘价格），ripple只有外部价；
- 可以发行自己的资产；
- BTS基于DPoS共识，Ripple基于拜占庭协议（Ripple区块链称为Distributed Transaction Ledger（DTL））

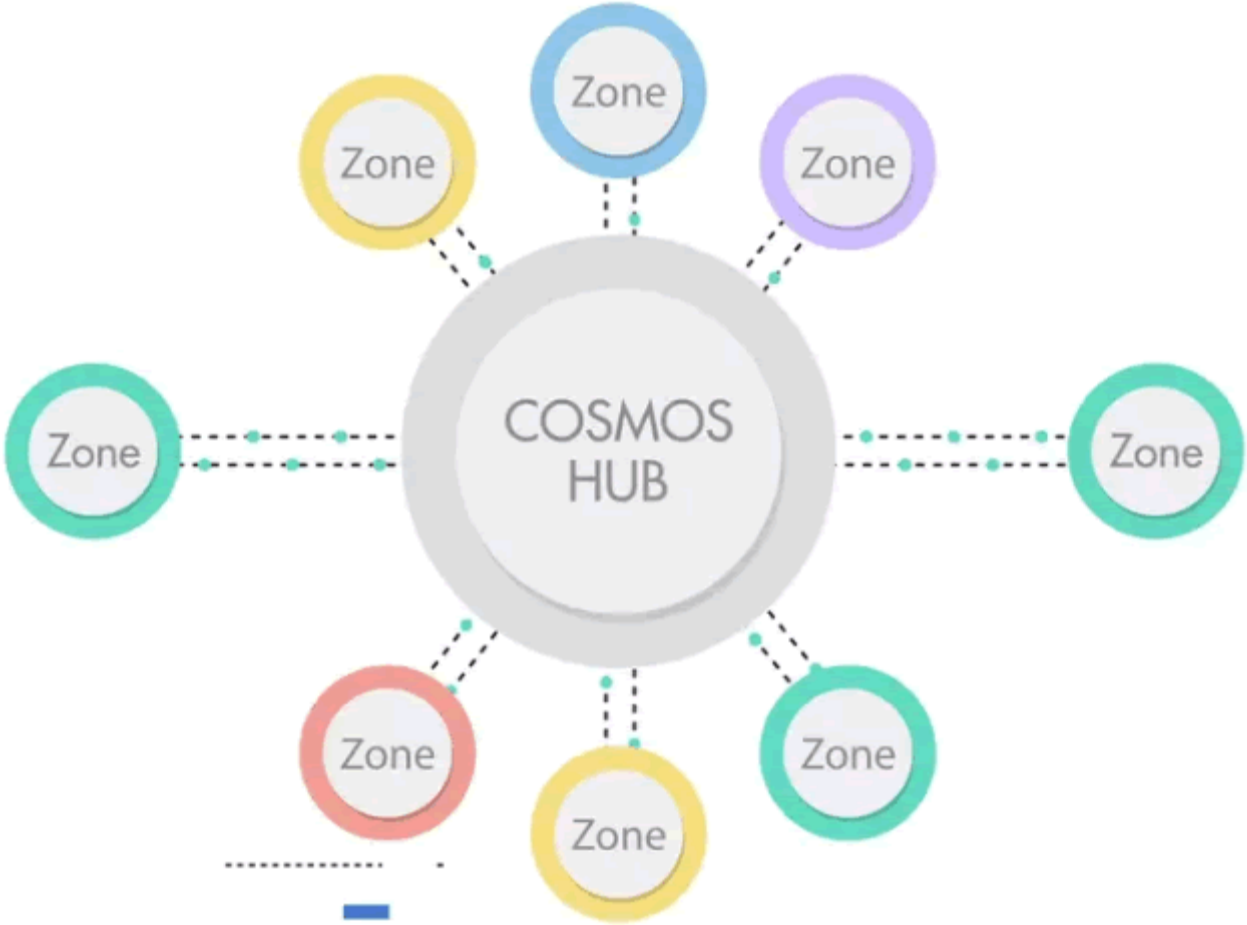
Polkadot

- Parity公司产品；
- 以太坊联合创始人，黄皮书作者Gavin Wood；
- 基于Notary、侧链、中继技术；
- 多链设计模式：parachains + relay-chain
- 共识协议：拜占庭、PoS

polkadot


Transaction
(submitted by
external actor)
Propagated transactions
Block candidate submission
Collator
Propagated block
Fisherman
Parachain community
Account
Inbound transaction
Validator swarm
(each coloured by its
designated parachain)
2nd order
Relay-chain
Interchain transactions
(managed by validators)
Relay
chain
Outbound transaction
Parachain
Parachain
queues and I/O
Parachain
bridge
Virtual parachain
(e.g. Ethereum)

Cosmos.network



谢谢!

欢迎关注: 谈谈区块链