亦来云侧链白皮书

区块链驱动的智能万维网

亦来云基金会

2017 年 4 月 25 日

内容说明

此文档是亦来云侧链白皮书 0.3 版本，重点阐述了亦来云侧链技术解决方案。未来我们会持续升级此文档，以体现亦来云最新发展状态。

版权声明

此文档著作权归亦来云基金会所有，保留所有权利。

目 录

1 概述

亦來云为了减轻主链的压力，同时为 DAPP 提供更好的使用体验，采用了主链+侧链的分层架构。主链只担负 ELA 的流通职责，DAPP 运行在侧链上，通过亦來云的侧链转账机制完成价值在主链和侧链间的安全转移。

亦來云公链使用仲裁人联合签名以及 SPV（Simplified Payment Verification，简单交易验证）的机制来保障与侧链间的转账安全，主链的持币人共同选举出一定数量的“仲裁人”，仲裁人负责对侧链到主链的提币交易进行签名，多数的仲裁人签名就可以解锁主链上从代表侧链的账户向普通账户转账的“提币交易”。主链到侧链充值操作的安全通过 SPV 来保障，每个侧链节点都会同步主链的所有区块头，再加上 merkle 证明路径以及交易信息，就可以从数据结构和算法的角度完成对转账交易的去中心化共识。

亦來云的侧链可以使用任意的共识机制，目前亦來云团队已经开发出了基于 POW 共识的侧链，可以接入主链完成基于 SPV 和 DPOS 的充值和提币操作。这个基于 POW 的侧链可以借助主链的算力来保障自己的安全，主链算力的使用权交给基于 DPOS 共识选举出的“仲裁人”，每个仲裁人轮流对侧链进行基于 POW 的打包出块。

亦來云通过跨链技术实现与自有 token 的区块链系统的相互转账，这种与亦來云能够相互转账的区块链，我们称为“友链”。

2 主侧链间的转账

侧链技术关键是要解决主链和侧链间的转账问题，要有机制保障主链侧链间的转账是安全可信的。为此 Adam Back 等人发表了那个著名的侧链白皮书，提出了一种叫做双向锚定（Two-way peg）的技术，来解决资产在两条链间的转移问题。基本的原理是基于 SPV 来互相验证交易在另一条链上确实存在，但是这有一个前提，就是都要保存对方的所有区块头信息。亦來云主链和侧链是 1 对多的关系，使用对称的双向锚定，对于侧链只保存一份主链的全部区块头信息没有什么问题，如果主链需要保存所有侧链的区块头信息，是不可接受的，所以在亦來云的主侧链架构上不能够使用对称的基于 SPV 的双向锚定。

亦来云对于主链和侧链之间两个方向的转账分别采用不同的机制来保障。

2.1 主链到侧链转账

亦來云主链到侧链的转账基于 SPV 来实现，侧链上需要集成主链的 SPV 模块，用于随时同步主链区块以及主链上向侧链的转账交易。转账过程如下：

1. 用户通过钱包在主链从地址 U 向主链上代表侧链的地址 S 转账 n 个 ELA，并在交易中附加上自己在侧链的地址 u，发送到主链上，这个交易标记为 tx1。
2. 主链的矿工节点将 tx1 打包并成功出块。
3. 等待足够的确认后轮值的仲裁人节点 A 的 SPV 模块获得这个主链上的转账交易，从交易中获得转账地址 u，构造给 u 发币的交易 tx2，发币数量等同于 tx1 中 U 给 S 的转账数量，tx2 中同时携带 SPV 证明路径和 tx1。
4. 轮值的仲裁人节点 A 将 tx2 发送到侧链节点。
5. 侧链将 tx2 打包出块。
6. 等待足够的确认后，用户在钱包上看到的自己的侧链地址 u 入账了 n 个 SToken。

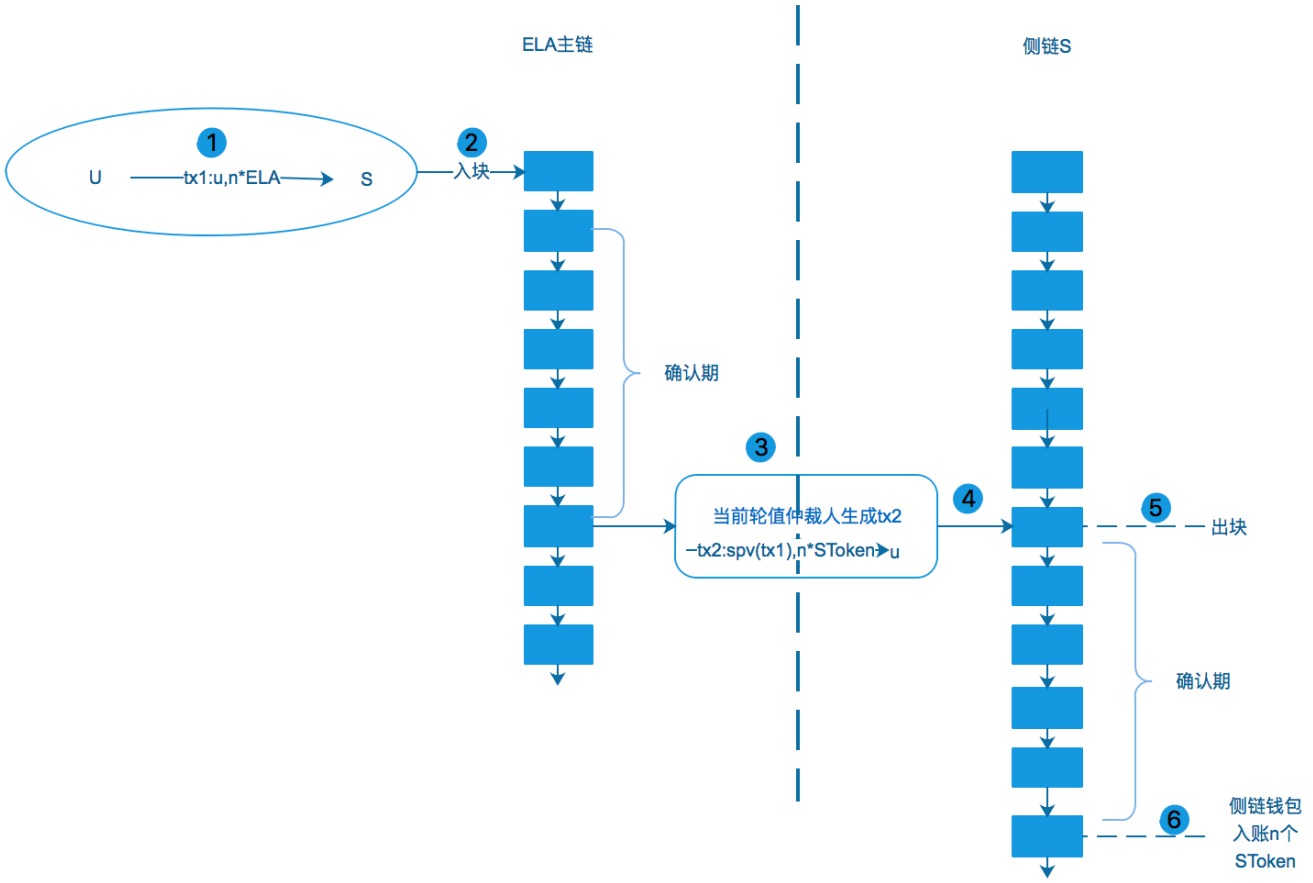

图 1：主链到侧链的转账过程

2.2 侧链到主链转账

亦來云侧链到主链的转账安全通过主链的仲裁人机制来保证，下面是转账过程：

1. 用户通过钱包在侧链从地址 u 发起提币交易，提取 m 个 SToken，并在交易中附加上自己在主链的地址 U，发送到侧链，这个交易标记为 tx3。
2. 侧链的矿工节点将包含 tx3 的交易打包并成功出块。
3. 轮值的仲裁人节点 A 向自己运行的侧链节点获取 tx3。
4. 轮值的仲裁人节点 A 根据 tx3 构造一个在主链上从 S 转移 m 个 ELA 到 U 的交易 tx4，将这个交易广播给所有的仲裁人节点签名。
5. 轮值的仲裁人节点 A 收到超过 2/3 的仲裁人对 tx4 的签名，就将携带这些签名的 tx4 提交到主链。
6. 矿工将包含 tx4 的交易打包出块。

7. 等待足够的确认后，用户在钱包上看到自己的主链地址 U 入账了 m 个 ELA。

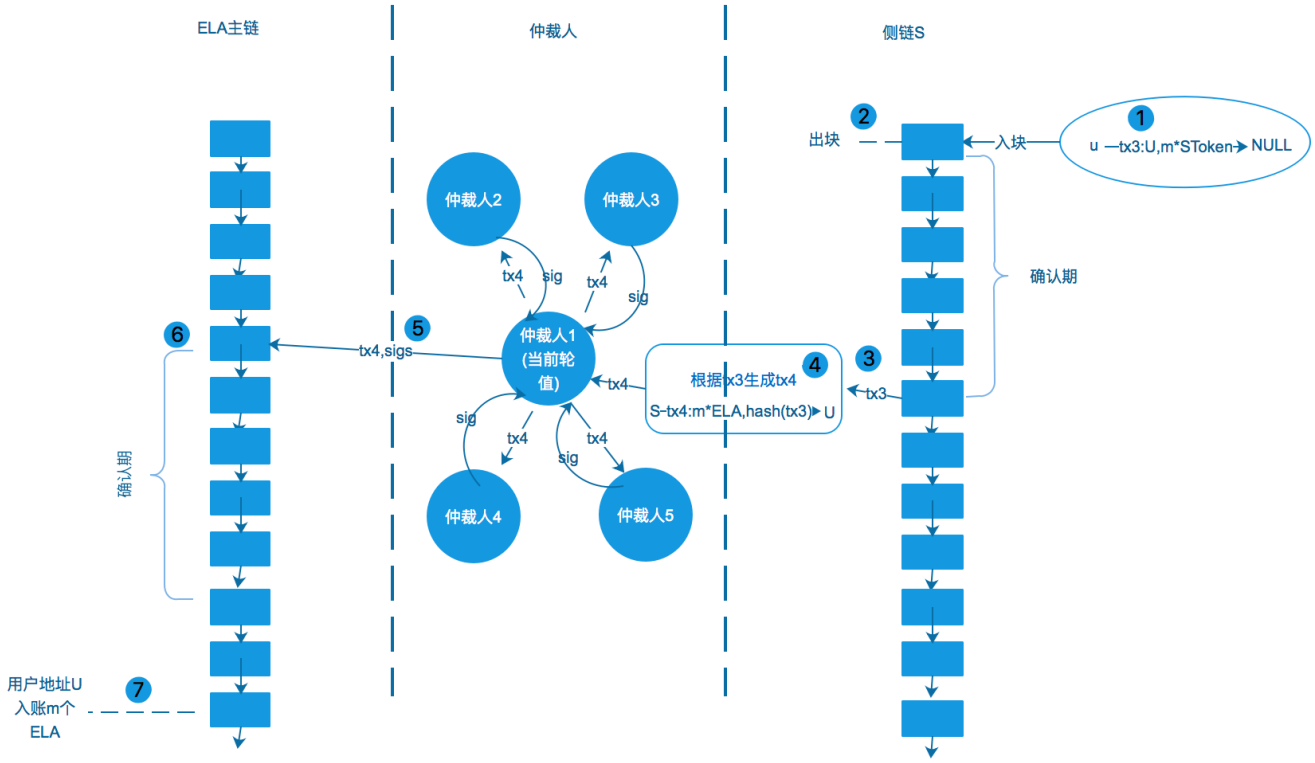

图 2：侧链到主链的转账过程

2.3 仲裁人

上面的转账过程都有仲裁人的参与，在主链到侧链的转账过程中，仲裁人的作用是生成和转移交易到侧链，并不参与签名；在侧链到主链的转账过程中，仲裁人的作用除了生成和转移交易，同时还要对交易签名，让主链上从代表侧链的账户向普通账户转账的“提币交易”能够被各个主链节点验证通过。

仲裁人通过在主链上投票选举产生，并且定期轮换。每个仲裁人需要提供足够的计算和网络资源，以便能够至少运行一个主链节点和对应 N 条侧链的 N 个节点。仲裁人的收益来自于为侧链打包出块所获得的交易费。

3 基于 POW 的侧链

亦來云提供了基于 POW 的侧链实现，使用这个实现，可以方便的搭建出一条侧链来开发 DAPP 应用。

这条基于 POW 的侧链采用与亦來云主链联合挖矿的方式获得算力，主链的当前轮值仲裁人作为矿工将侧链的交易打包生成挖矿交易放在主链上，主链再通过与比特币联合挖矿的方式出块，按照联合挖矿的原理，算力证明再传递到侧链，侧链的任意全节点可以依据这个算力证明来验证出块的有效性。

主链在一个仲裁人选举周期内的所有仲裁人会按照顺序轮流作为"侧链出块轮值仲裁人"履行相应的职责，这里面就包括为侧链出块的职责。轮换动作通过侧链出块触发，每个仲裁人轮流对一个侧链出块，顺序通过上一轮的投票统计结果确定。出块行为最终通过发布到主链上的挖矿交易体现，每个主链节点都会对这个挖矿交易是否合法进行共识，其中一个主要的验证就是看发布这个挖矿交易的签名人是否是当前有权对这个侧链出块的"侧链出块轮值仲裁人"。

侧链的出块收益（只有交易费，没有创币）仍然是分配给矿工和基金会，这里的矿工就是当前在主链发起"挖矿交易"的仲裁人，当然这个挖矿交易放到主链上也是要付矿工费的，这个矿工费是付给真正付出算力的比特币矿工。

在上述的侧链联合挖矿的模型中，侧链的安全依靠主链的选举信任以及联合挖矿提供的算力来保证，完成了从主链到侧链的信任传递。侧链使用 POW 的共识策略，简单可靠，交易历史不会因为侧链某些相关方作恶而被篡改。侧链也可以自己单独挖矿，但是要和主链联合挖矿的算力竞争，所以在遵循 POW 规则的情况下，主链会为侧链提供足够强大的安全保障。

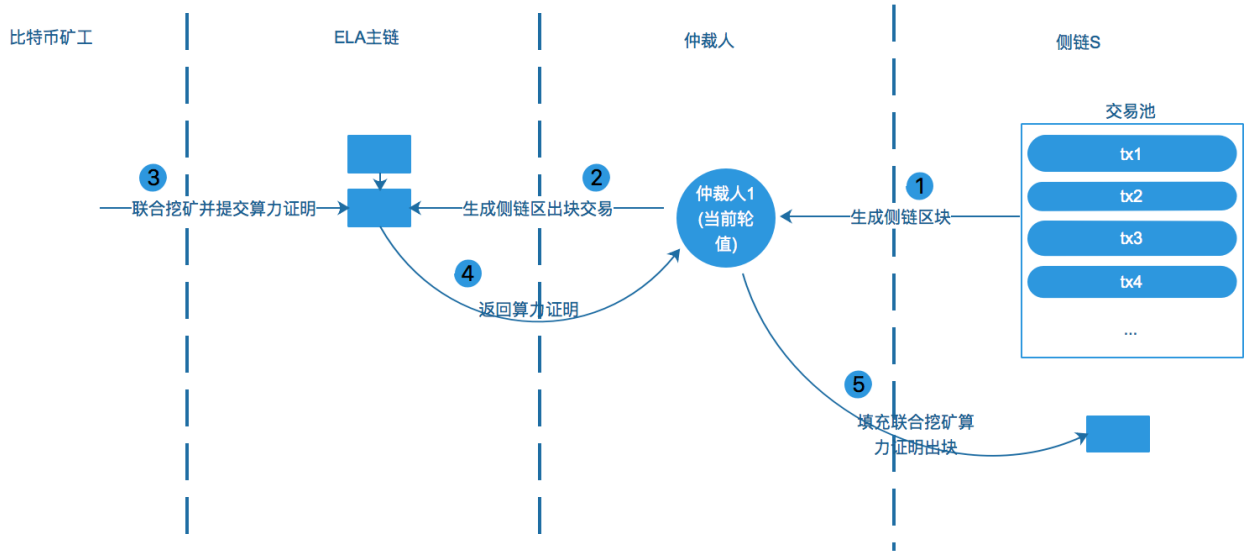

图 3：侧链联合挖矿出块儿过程

4 基于 DPOS 的侧链

亦來云同时在规划开发基于 DPOS 共识的侧链，侧链上 DPOS 共识中的代理人由主链的仲裁人来担任，仍然相当于通过主链保证侧链的安全，只是减少了挖矿的过程，会获得更快的出块速度。侧链的每个节点都可以通过挂接的主链 SPV 模块来获得主链对仲裁人的投票信息，从而对仲裁人的合法性达成共识。

5 友链

侧链的概念来自于比特币，在这个场景下侧链没有自有的 token，有自有 token 的链有独立的经济体系，亦來云与这种自有 token 链之间的转账需要基于当前两种 token 的市场兑换汇率来进行，这个自有 token 的链我们称为“友链”。

亦來云对友链的支持分为两个阶段：第一个阶段支持友链和亦來云主链跨链的原子交易，这种交易是点对点的，需要交易双方自己约定兑换汇率，创建互相制约的原子兑换交易；第二个阶段会基于去中心的交易所，完成主链和友链 token 的自由兑换，不需要用户间再点对点的创建兑换交易。

第一个阶段的原子交易会借助哈希锁来实现，下面通过一个具体的例子来描述兑换过程。

假设有一条友链 F，自有 token FToken， Alice 和 Bob 需要在亦來云公链（这里用 E 来代表）和链 F 之间完成 ELA 和 FToken 的兑换。Alice 在链 E 和链 F 上分别有地址 EA 和 FA，Bob 在链 E 和链 F 上分别有地址 EB 和 FB。假设此时的市场兑换汇率为 1：10（一个 ELA 兑换 10 个 FToken），Alice 希望用 10 个 ELA 和 Bob 兑换 100 个 FToken。

1. Alice 在链 E 上发起一笔从 EA 向 EB 的特殊转账交易 tx1，转账金额为 10 个 ELA，这个交易的解锁条件除了 EB 对应私钥的签名，还增加了一个哈希锁，Alice 先生成一个随机数 x，对 x 取哈希 hash(x)，放到这笔交易中，Bob 需要提交 x 才能够解锁这个哈希锁。
2. Bob 看到了链 E 上的 tx1，就在链 F 上构造另外一笔特殊的交易 tx2，从 FB 向 FA 转账 100 个 FToken，这个交易的解锁条件除了 FA 对应私钥的签名，还增加了一个哈希锁，同样是 hash(x)，解锁条件同样是需要提供 x。
3. Alice 在链 F 上提供对 tx2 的签名以及 x 来解锁 tx2，将 100 个 FToken 转账到自己在链 F 上另外的地址。
4. Bob 看到 tx2 被解锁，同时也就得到了 x，然后 Bob 用 EB 的私钥签名 tx1 并提供 x，从而解锁 tx1，将 10 个 ELA 转账到自己在链 E 上另外的地址。

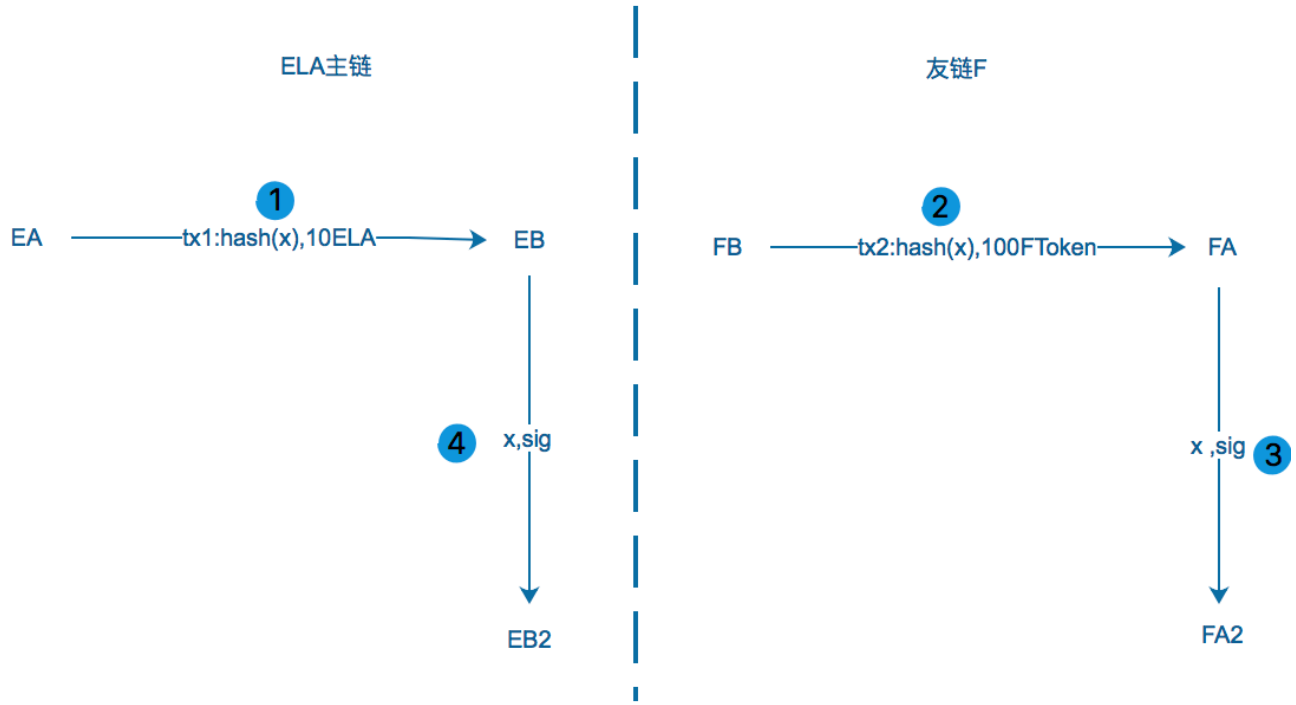

图 4：ELA 主链和友链 token 的兑换过程

参考文献

[1] Adam Back. Enabling Blockchain Innovations with Pegged Sidechains .https://blockstream.com/technology/sidechains.pdf， 2014-10-22

[2] Andreas M. Antonopoulos.《精通比特币（第二版）》 http://book.8btc.com/masterbitcoin2cn

[3] 周邺飞. 区块链核心技术演进之路 – 挖矿演进. http://www.8btc.com/blockchain-tech-mining， 2016-11-08

[4] Joseph Poon. The Bitcoin Lightning Network:Scalable O -Chain Instant Payments.https://lightning.network/lightning-network-paper.pdf， 2016-01-14

[5] bitcoin wiki. Merged mining specification. https://en.bitcoin.it/wiki/Merged_mining_specification, 2015-08-08.

联系我们

亦来云（上海）：

上海市虹口区塘沽路 463 号华虹国际大厦 11 层

邮编： 200080

亦来云（北京）：

北京市海淀区成府路 45 号中关村智造大街 G 座 Plug & Play

邮编： 100084

邮箱：

白皮书工作组： whitepaper@elastos.org

全球社区： global-community@elastos.org

亦来云资本： elastos-fund@elastos.org

公共关系： pr@elastos.org

投资者关系： ir@elastos.org

亦来云理事会： elastos-council@elastos.org

其他联系： contact@elastos.org

亦来云官网： http://www.elastos.org