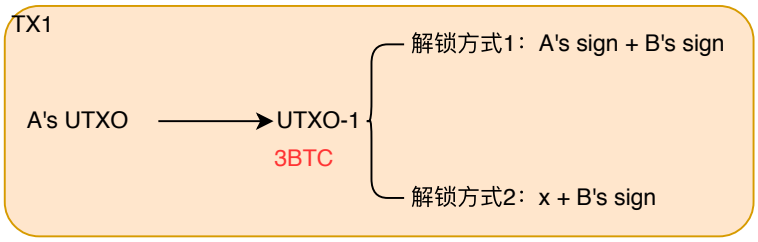
黄色为未上链状态　　蓝色为上链状态

(1) A 生成 UTXO-1，里头包含 3ETH

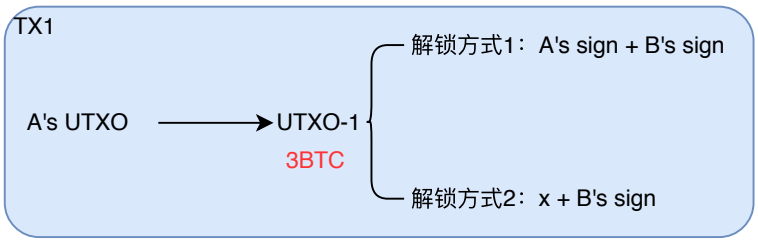


(2) A 采用上述解锁方式1 生成 TX2。然后 A 自己先签名。注意，此时 A 还是不能消费上述 UTXO-1，还缺少 B 的签名

(3) A 将 TX2 发给 B，B 签名后发回给 A。此时 TX2 集齐了两个签名，已经可以解锁 TX1 了。唯一的限制是要等 TX1 上链 48h 后，TX2 才能上链

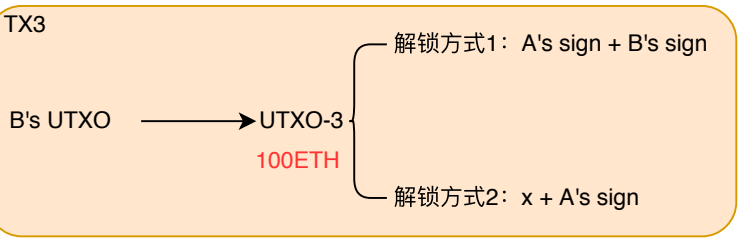
TX2 实质是 A 的退路交易。是为了保障当出现交易过程终止的情况，也就是没达成 UTXO-1 的解锁条件2，A 可以通过 TX2 将 UTXO-1 给赎回来。

(4) A 将 TX1 上链，UTXO-1 在链上生成。



(9) A 观察到 TX3 生成的 UTXO-3 已经上链。于是采用解锁方式2创建 TX5
因为采用了解锁方式2，所以 x 也就显露了出来。***注意，此步骤必须在***

5) B 生成 UTXO-3，里头包含 100ETH

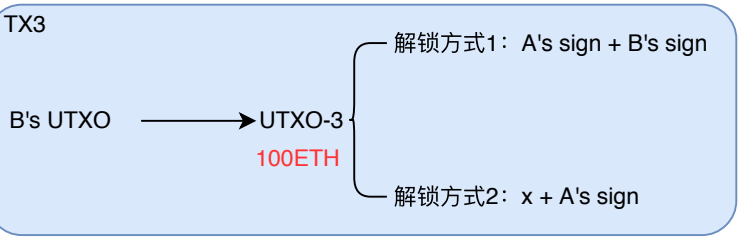


(6) B 采用上述解锁方式1 生成 TX4。然后 B 自己先签名。注意，此时 B 还是不能消费上述 UTXO-3，还缺少 A 的签名

(7) B 将 TX4 发给 A，A 签名后发回给 B。此时 TX4 集齐了两个签名，已经可以解锁 TX3 了。唯一的限制是要等 TX3 上链 24h 后，TX4 才能上链

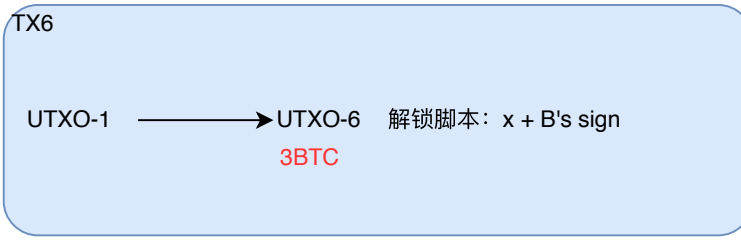
TX4 实质是 B 的退路交易。是为了保障当出现交易过程终止的情况，也就是没达成 UTXO-3 的解锁条件2，B 可以通过 TX4 将 UTXO-3 给赎回来。

8) B 将 TX3 上链，UTXO-3 在链上生成。***注意，TX3 一定要在 TX1 之后上链。也就是说，(1)~(8)步并没有严格的顺序，除了(4) 必须早于 (8)***



将 UTXO-3 转为 UTXO-5 自己的囊中。
(8) 步骤上链的 24h 之内做完，不然 B 可以使用 TX4 赎回。

(10) B 观察到 TX1 生成的 UTXO-1 已经上链，而且 TX5 也显露出了 x 的值
UTXO-1 转为 UTXO-6 自己的囊中。***注意，此步骤必须在 (4) 步骤上链***



失败的情况：

一、A 在 (4) 步上链 48h 后还没观察到 (8) 的 UTXO-3 上链：A 发送 TX2 将 UTXO-1(3BTC) 赎回；

二、B 在 (8) 步上链 24h 后还没观察到 (9) 的 UTXO-5 上链：B 发送 TX4 将 UTXO-3(100ETH) 赎回；

三、现实中的极端攻击：https://zhuanlan.zhihu.com/p/31689532

值。于是采用解锁方式2创建 TX6 将
链的 48h 之内做完，不然 A 可以使用 TX2 赎回。