Cross-blockchain Operation

向阳曦 xyangxi5@gmail.com

1 约定

假设有A, B, C三条链,Alice, Bob, Tom是三个用户.A.Alice表示这是Alice在A下的账户.

2 交易行为

2.1 个人资产转移(双方)

假设Alice有1Acoin,想要兑换2Bcoin,那么将发起一个兑换的交易请求,请求是将0.1Acoin兑换为2Bcoin.而Bob有2Bcoin,如果接受Alice的请求,则接受这个交易.这个过程需要去中心化,并且是原子的.

即transfer(A.Alice, 0.1Acoin, B.Bob, 2Bcoin).

即transfer(A.Alice, A.Bob, 0.1Acoin), transfer(B.Bob, B.Alice, 2Bcoin).

2.2 Lightning Network,跨链支付(本质与2.1相同,但若减少操作,则是多方交易)

假设Alice有1Acoin,0.5Bcoin,Tom只接受Bcoin.

Tom认定1Acoin=20Bcoin.假设Net = {Bob, Joe, Mary}是中间人(合约),这个群体认可Tom的汇率.

Alice希望向Tom支付2.5Bcoin. 那么自动产生一个交易请求.

即transfer(A.Alice, 0.1Acoin, B.Tom, 2Bcoin).by(Net), transfer(B.Alice, B.Tom, 0.5Bcoin).

2.3 财团/公司金融管理

与个人财产管理相似,但在这里资金流更大,会有长期运行的跨链合约?

3 数据控制

3.1 不同的公司可能使用不同的区块链(隐私,便捷,etc.)

假设Alice的个人数据data存在A上,Bob只有在B上的合约. 即B.Bob.contract.get(A, A.Alice.$data$)

3.2 同一个公司不同数据可能存在不同的区块链上

假设Alice已经使用了一段时间的A,现在B有显著优势,但不想放弃A上的数据(比如已经有1G).
Alice公司的一个合约在C上,数据库在A, B上.A, B之间有数据沟通,C需要A, B的数据.