I started thinking about a sharding scheme where everybody gets their chain. The phrase “everybody gets their chain” came first to my mind, and I’m trying to stretch it out.

Alice’s (PoA proof-of-authority

proof-of-Alice) chain represents Alice’s subjective view. Bob’s (PoB–proof-of-Bob) chain represents Bob’s subjective view. As usual, the agents are identified with cryptographic signatures.

Before jumping to the general case, let me think about a symmetric two-party case.

All chains use the same address space (maybe the same as Ethereum’s). Alice’s chain has a genesis block that says the chain follows proof-of-Alice. Alice’s chain contains only blocks with Alice’s signature. Each block defines a post-world-state that associates each address with a balance (unit: Alith).

Bob maintains a chain too. Bob’s blocks define post-world-states that associate each address with a balance (unit: Roberth).

Initially, Bob doesn’t trust Alice’s blocks because Alice can create a parallel history at her will. And worse, Bob has no way to punish Alice for equivocating. Alice doesn’t trust Bob’s blocks either.

They want to interact somehow, and create a merged block:

- on Alice’s chain, moves 100 Alith from Alice’s account into a lock that Bob can leak every time he creates a block on his chain.
- on Bob’s chain, moves 100 Roberth from Bob’s account to a lock that Alice can leak a bit every time she creates a block on her chain

For the payout, only “blockheaders” are checked. Of course, one cannot go too quickly than the other. Alice can spend only a bit more Roberths as Bob spends Aliths (and the other way around).

Moreover, if ever Bob sees forking blocks with Alice’s PoA, Bob can destroy Alice’s deposit on Bob’s chain. (Of course Alice can do the other way around if she catches Bob forking.)

What if Bob doesn’t produce any blocks? Then Alice can never spend Roberth (though, maybe she can still spend “Alice’s Roberth”

). Perhaps, Bob has lots of Roberth, and he wants to keep the chain going so that the value of Roberth is kept somehow.

What if Alice doesn’t accept Bob’s transactions? Maybe this should be punishable with Alice’s deposit in Bob’s chain. At least Alice can publish her transaction, and tell the world that Bob is censoring.

Next question: Bob wants to pay Alith to Charlie, but Chalie doesn’t trust Alice’s chain. Chalie only trusts Bob. What should happen? (Maybe Bob can still spend “Bob’s Alith”.

)