

17 November 2023

^{^^}
^{^^}
^{^^} Meowing Cat ^{^^}
^{^^}

Author: Oguzhan Eroglu (<https://github.com/rohanrhu>)

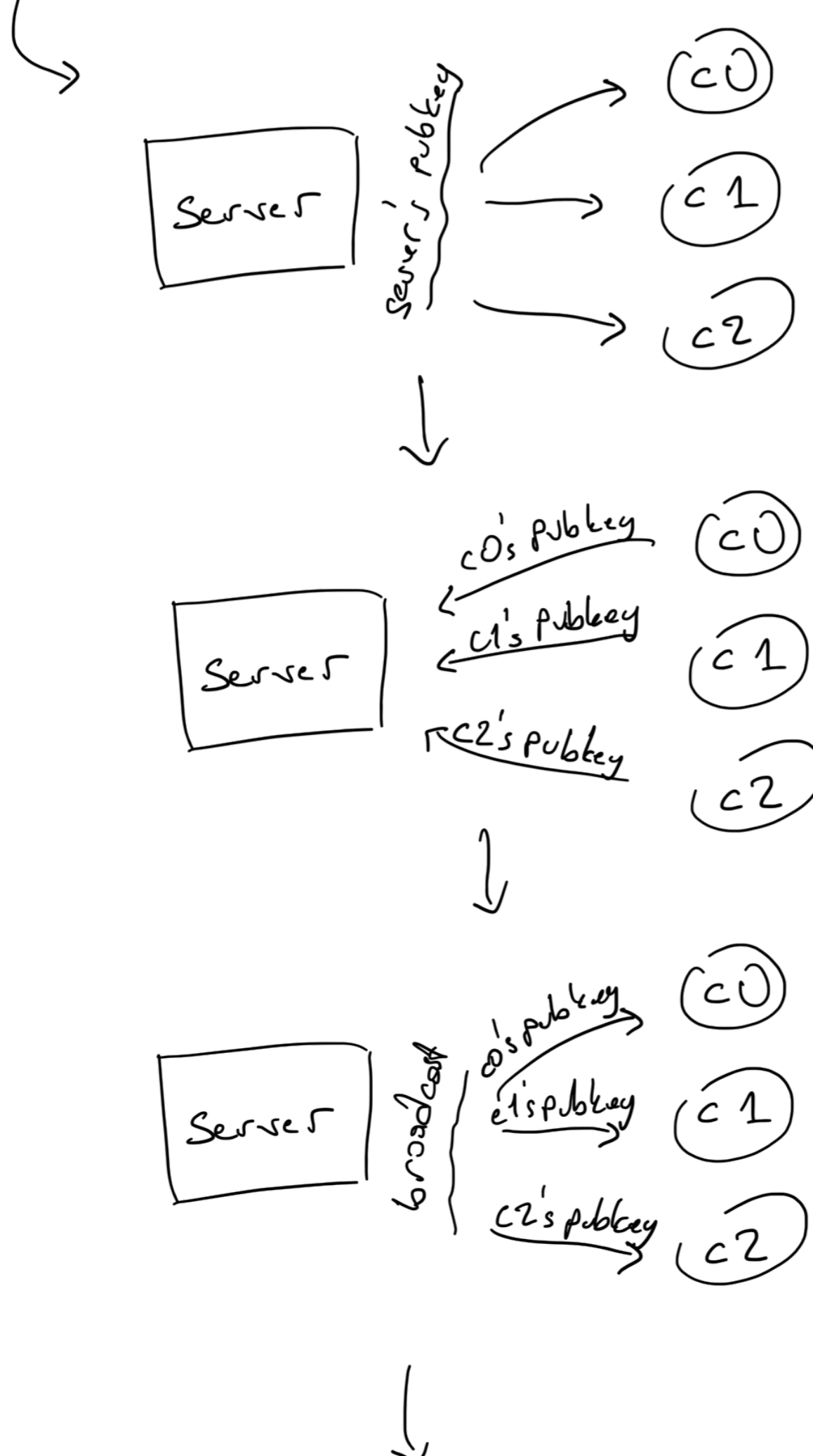
Licensed under GNU GPLv3

^{^^}
^{^^} All of this things provide
a true multiplayer randomness... ^{^^}
^{^^}

Truthful Multiplayer Randomness

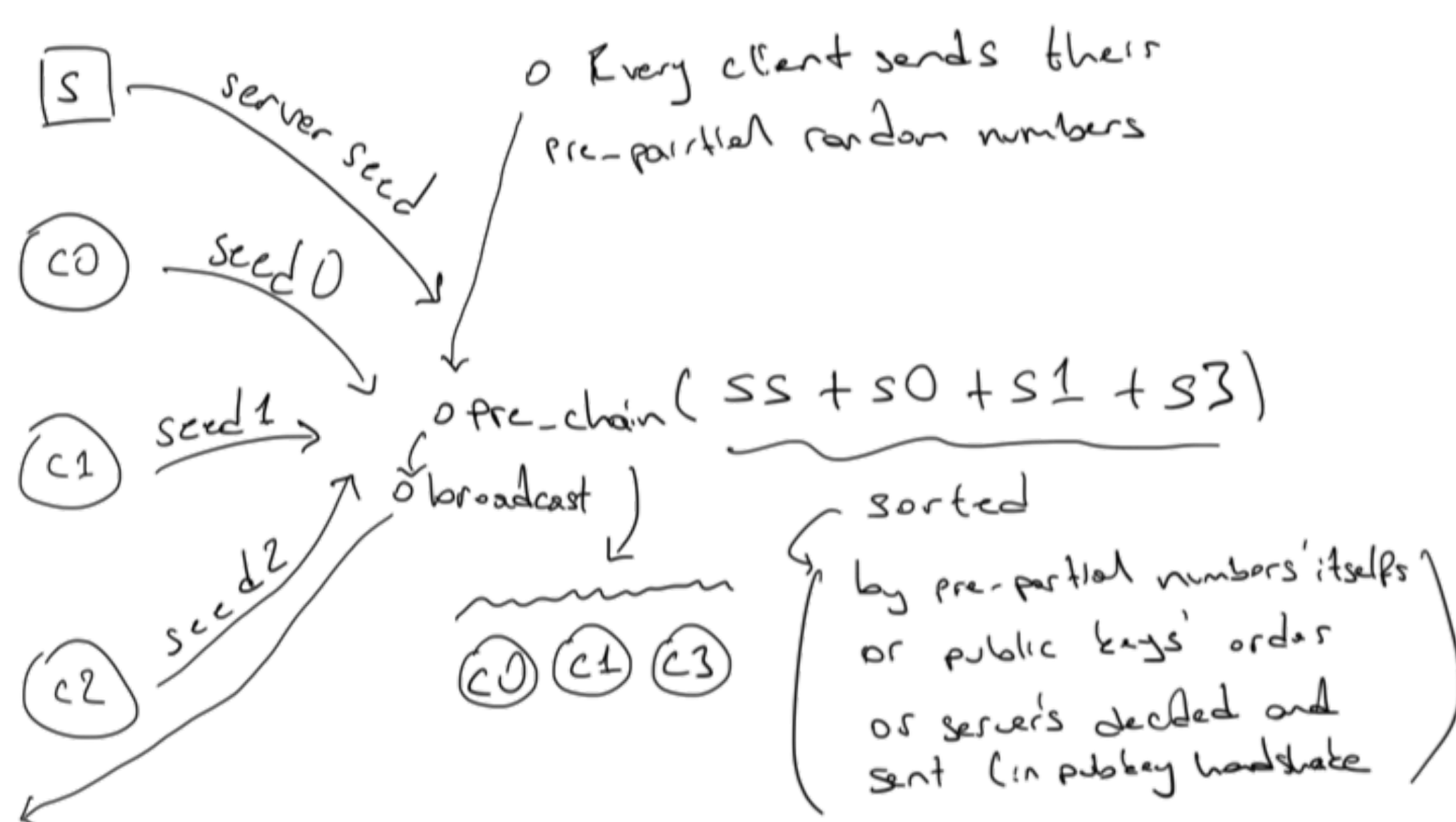
Handshaking

- o All clients of the hand and server perform an handshake

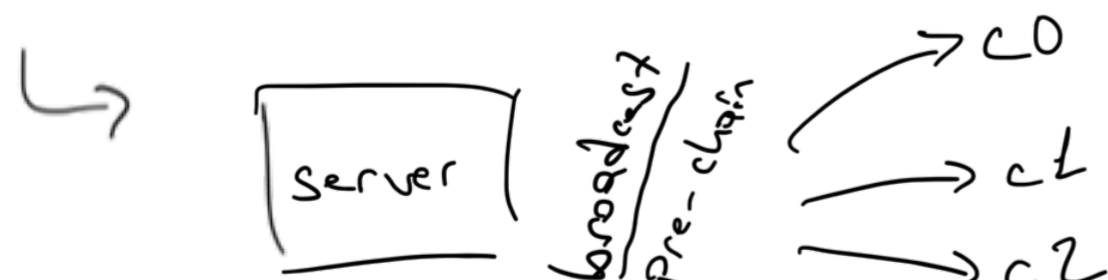


- o Initial handshake is done

Building Pre-chain



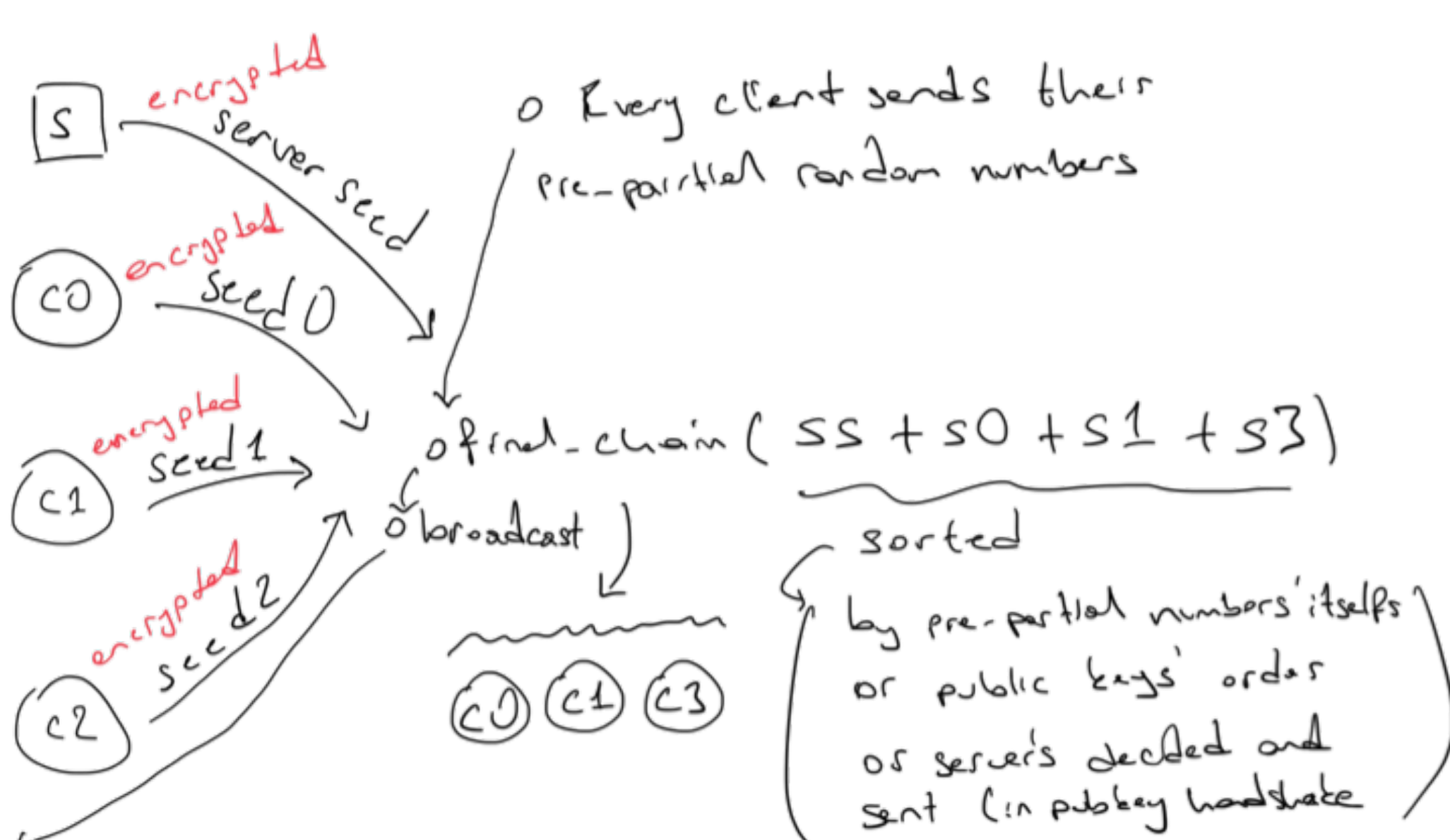
- o Server broadcast the pre-chain



- o Now all players have the pre-chain

Building Final Chain

- o Every player sends final-partial random numbers which is encrypted version of pre-partial random numbers by that player's private key



Verifying Final Chain

- o Every client checks the final chain by verifying every player's partial random numbers by their handshake public keys for that if they are encrypted with that player's private keys by decrypting the final-partial random number of that player with that player's public key
- o The true randomness is provided by the fact that every player has their own partial random number too in the chain

Deriving App-specific Random Number

- o The app that implements Meowing Cat's Truthful Multiplayer Randomness reduces/derives the app-specific derivation of the final random chain with a method like modular arithmetic or hashing algorithm or another reducer function

Players Know Who They Are Playing With

- o Every player (client) can create new random pubkey/prvkey pairs anytime
- o Players shares/exchanges their public keys between themselves in any communication way
- o Every player/client can add public keys with a label and they can make sure that they are playing with that players