Trust worthy

1: Cash on hand? Do they have enough
2: Did they double spend?

Block → Trustworthiness + Anonymity

Chain

Transactions

UserA → PublicKey A + PrivateKey A
UserB → PublicKey B + PrivateKey B

Transaction

1. UseA w/ PublicKey A gives so many [bitcoin] to UserB w/ PublicKey B
2. Donation to miner
   UserA w/ PublicKeyA gives so many [bitcoin] to whoever mines this
3. Signed by all Party's Private keys

Block Chain

Linked List — Forward Pointer

Block Chain — Backward Pointers

Pointer is the hash of the previous block.

1 - Backward Pointer

2 - List of open Transactions
2a - Public key of miner

3 - Nonce
↳ Unit of work

- The hash of the block (which includes the nonce) must be below a threshold.
- This threshold is constantly changed by the community to keep average mining time constant.

Sync w/ Deltas & Whole Model

Server
- whole model
- listen for deltas
- send deltas + hash

Clients
- ask for whole model on boot
- send deltas
- listen for deltas + hash