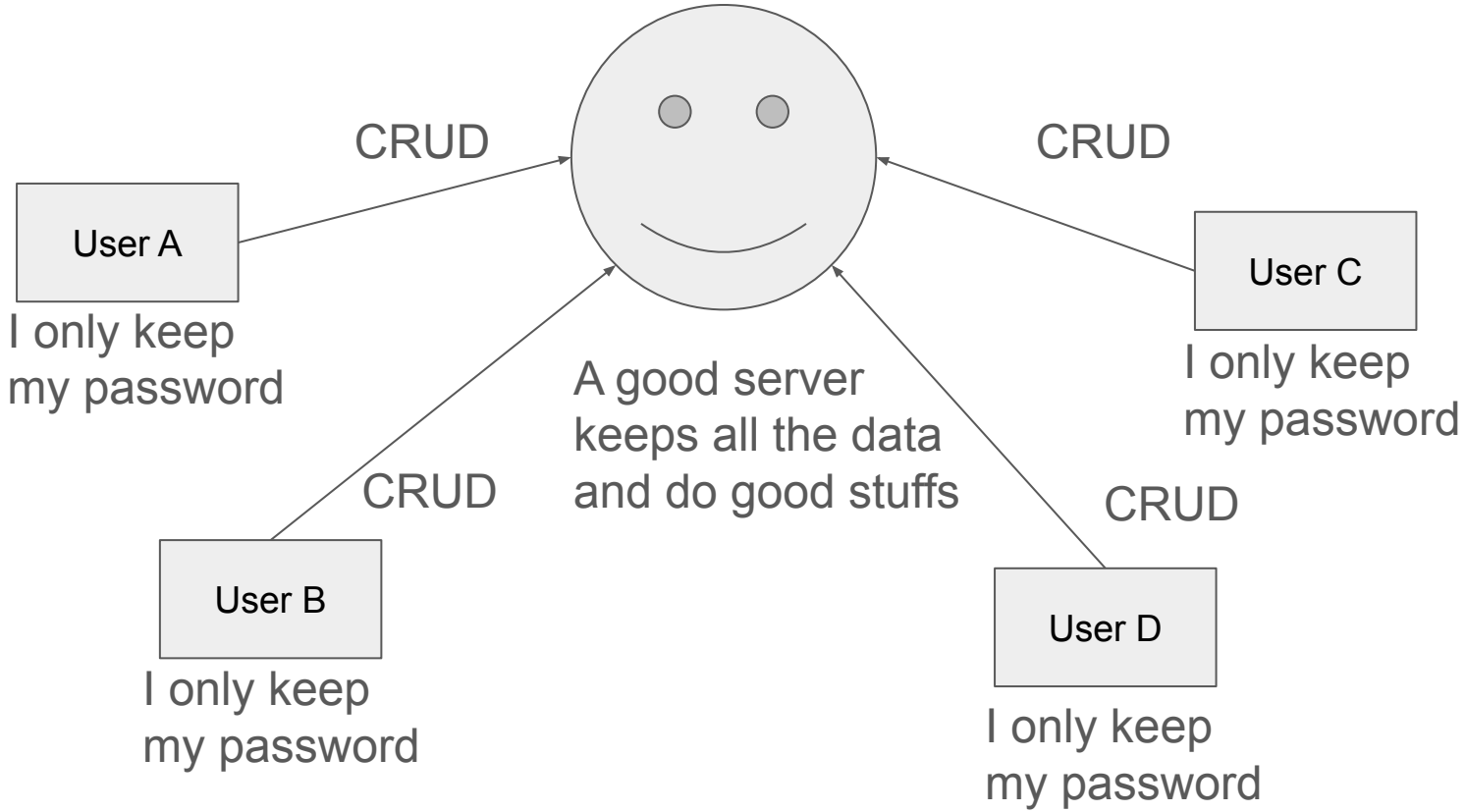
~~Blockchain~~ x ZKP

Not a blockchain workshop
ZKP = Futuristic and highly experimental

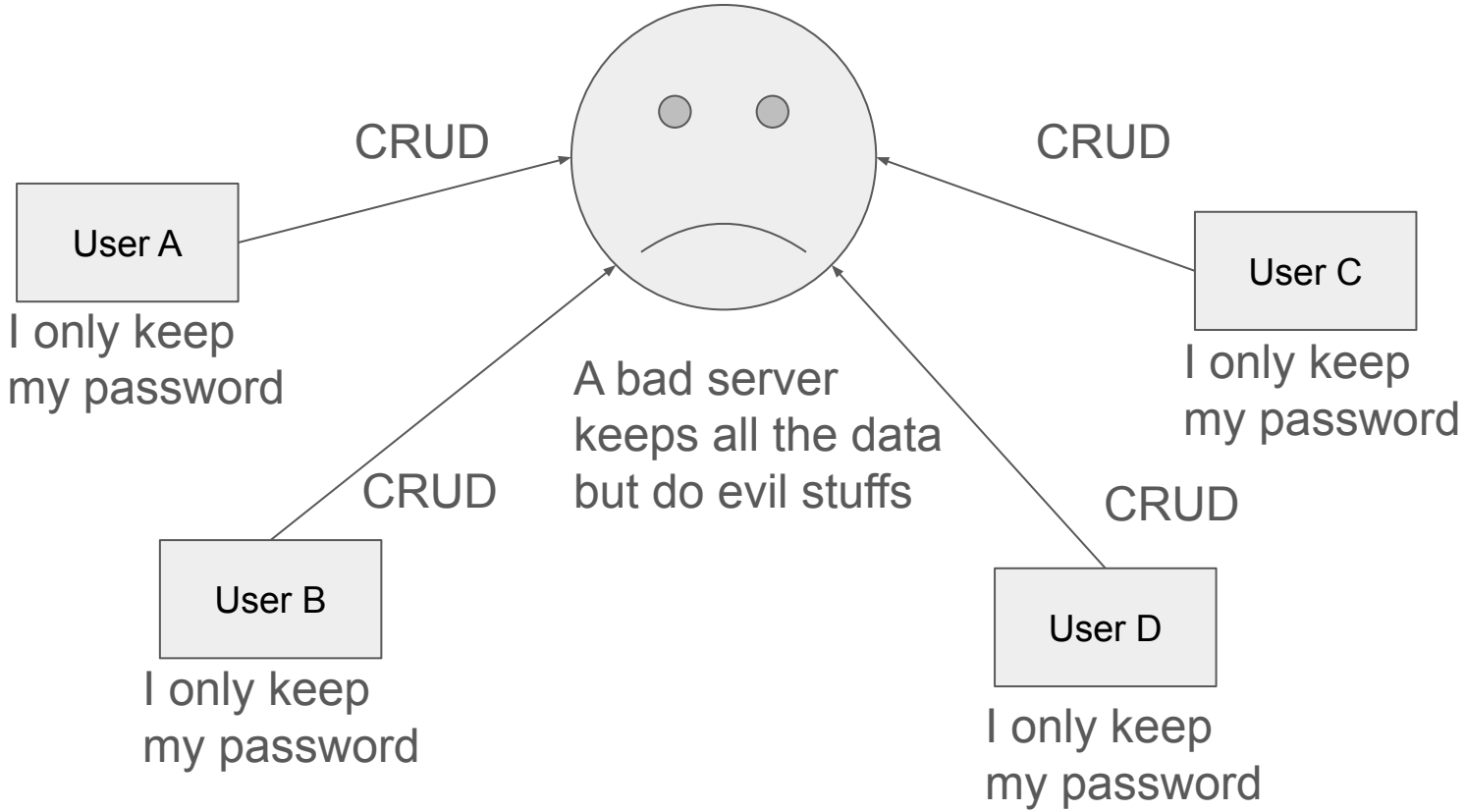
CRUD = Create/Retrieve/Update/Delete

What we use todate = centralized (good) model



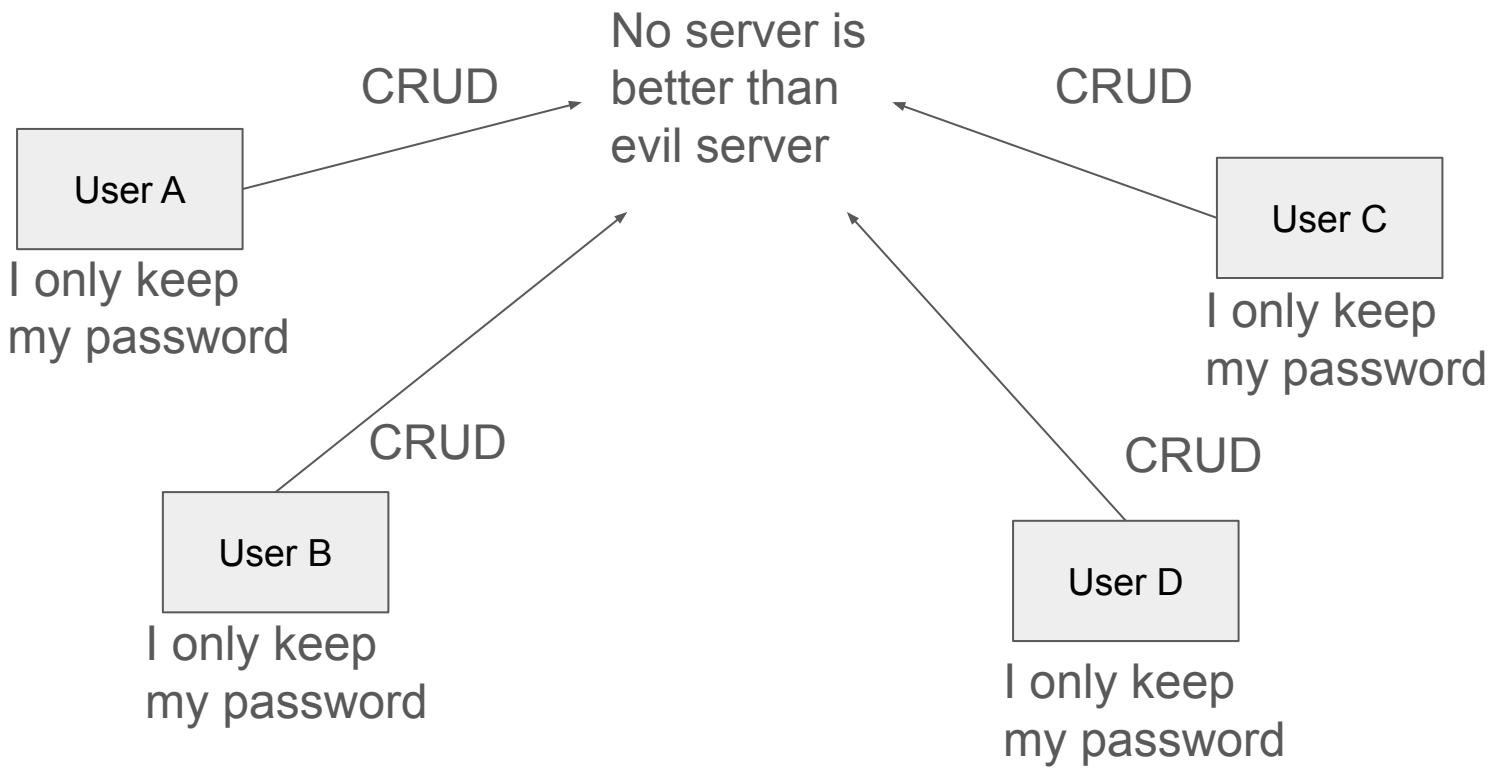
CRUD = Create/Retrieve/Update/Delete

What we use todate = centralized (bad) model



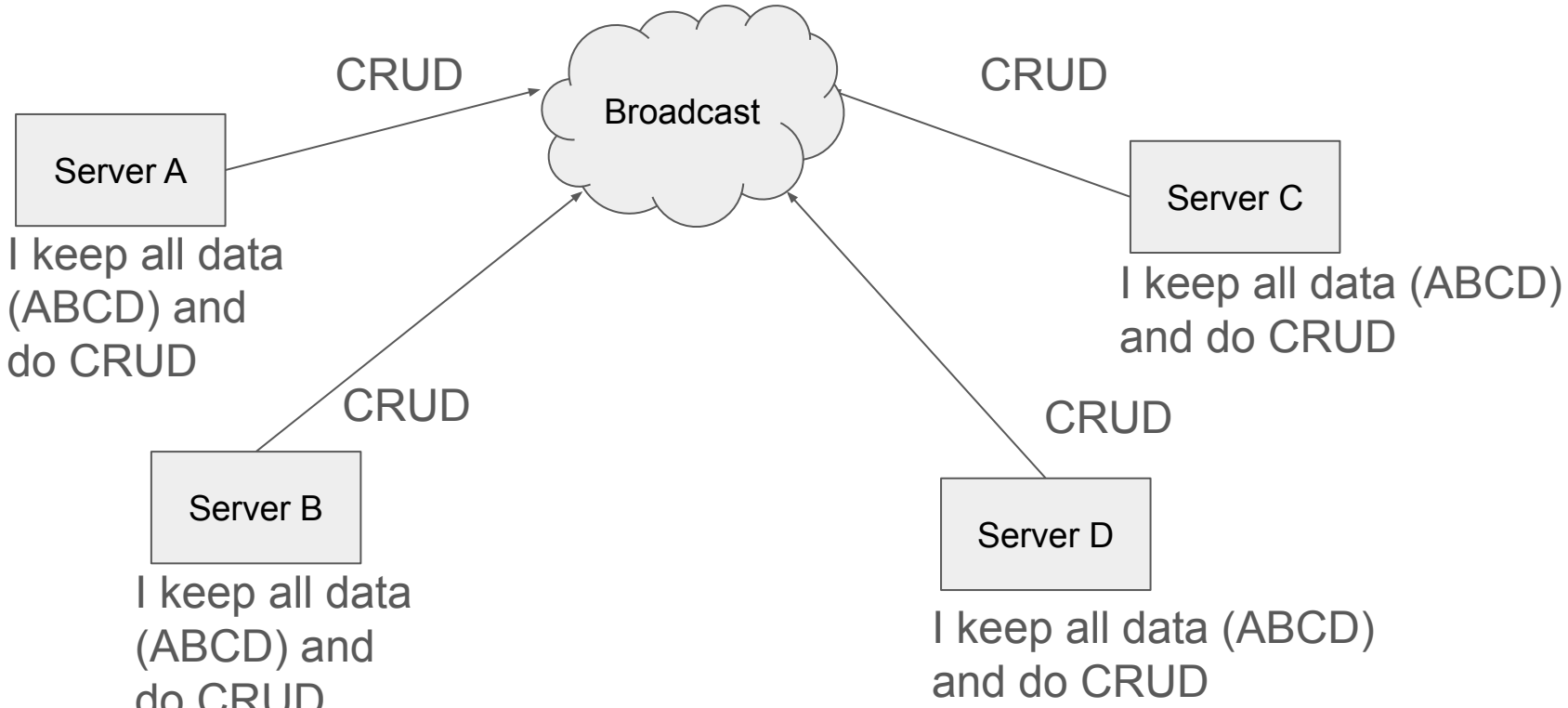
CRUD = Create/Retrieve/Update/Delete

Removing evil server



CRUD = Create/Retrieve/Update/Delete

Removing evil server = decentralized model



Decentralization = new problems in scalability and privacy

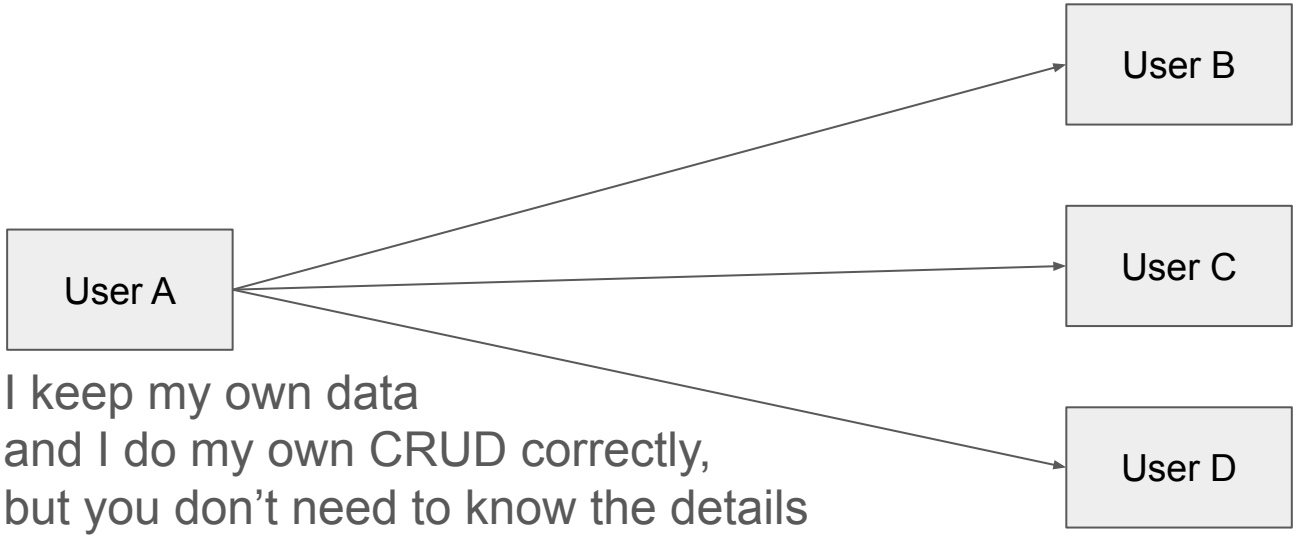
- User A (500$) → Server A (3000$)
  - User A only keeps its password and asks good server G to do CRUD
  - Server A keeps ABCD data and also processes CRUD for ABCD
- Broadcast = a lot of bandwidth for sending and receiving CRUD
  - User A sends CRUD to good server G
  - Server A sends CRUD to BCD and receives CRUD from BCD (all data)
- A sees only A’s data → A sees all data (BCD’s data)

This program = scalable and private decentralization

- User A (500$) → User A (800$)
  - User A keeps only its data and processes only it’s own CRUD
- Broadcast = minimal bandwidth for sending and receiving CRUD
  - User A only communicates its own data digest to BCD
- A sees only A’s data → A sees only A’s data
  - User A only sees BCD data digest not BCD data

Scalable and private decentralization = use ZKP

- ZKP = Zero-Knowledge-Proof
- ZKP allows a Prover to convince a Verifier that something happens correctly without telling the Verifier what happens



Questions to answer (this program)

- How do A store its own data, *how does BCD stores A's data*?
  - BCD stores A's data digest (small and also encrypted)
- How do A update its own data, and convince BCD it did correctly?
  - A updates its own data, updates also the data digest, sends the digest to BCD along with a ZKP to convince the correctness of the new digest vs the old digest (BCD stores this)
- How do A shows some data and convince BCD that this data is consistent with what is stored in the data digest?
  - A shows the data and some authentication data to the stored digest (maybe in ZKP form for better scalability and privacy)
- How to program ZKP?
- What is the math behind ZKP?
- Your own ZKP apps?