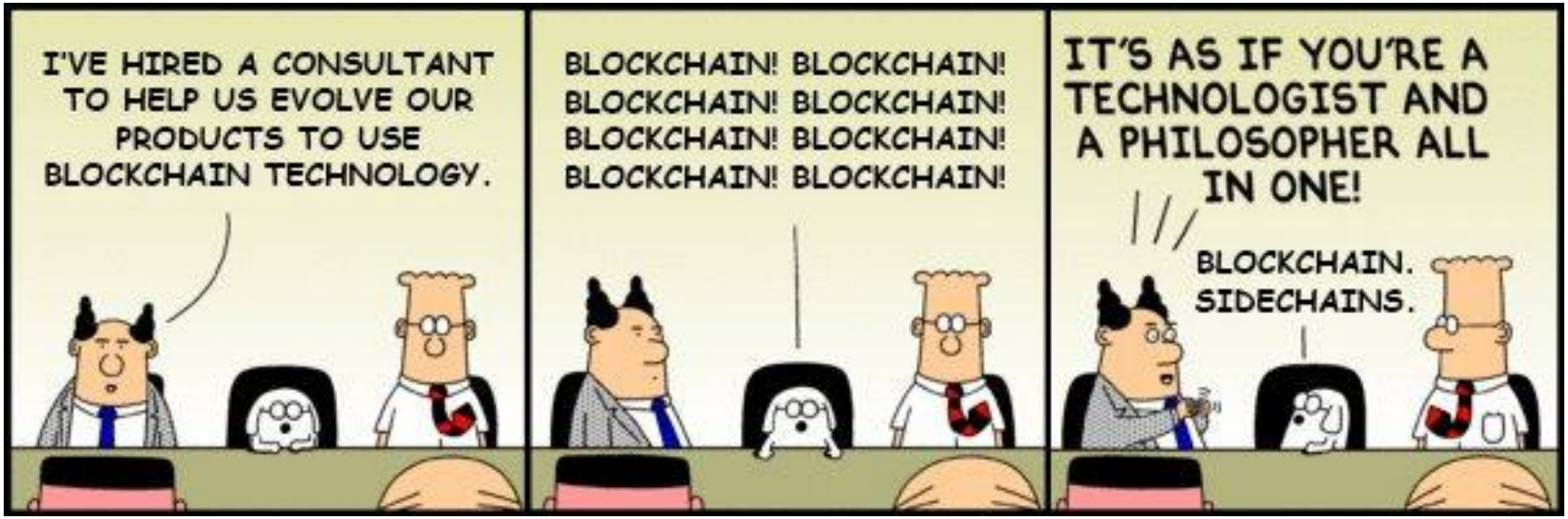
Proof-of-Work Blockchain Systems

Matej Pavlovic

Distributed Algorithms

December 1st, 2025, EPFL, Lausanne, Switzerland

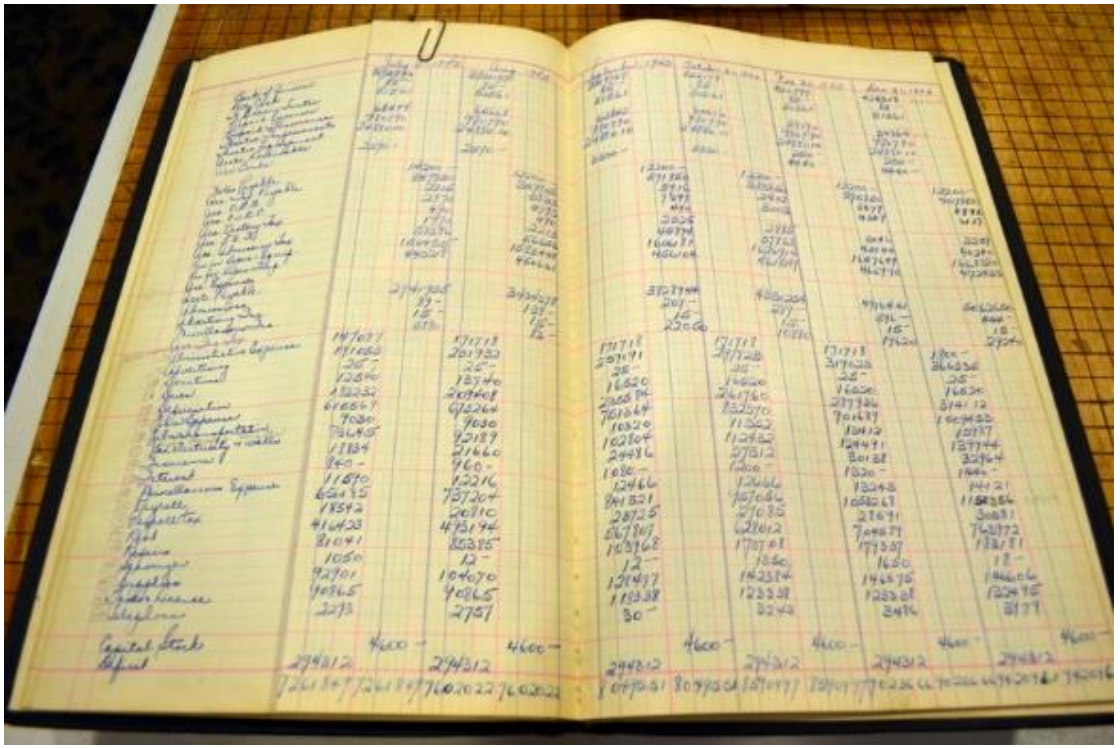


(Dilbert Cartoon by Scott Adams)

What Is “Blockchain”?

- A chain of blocks
- as well as … a data structure
- as well as … an abstraction
- as well as … a distributed ledger
- as well as … a computer system
- as well as … a consensus algorithm
- as well as …. way of stopping wars, curing cancer and ending poverty.

Ledger



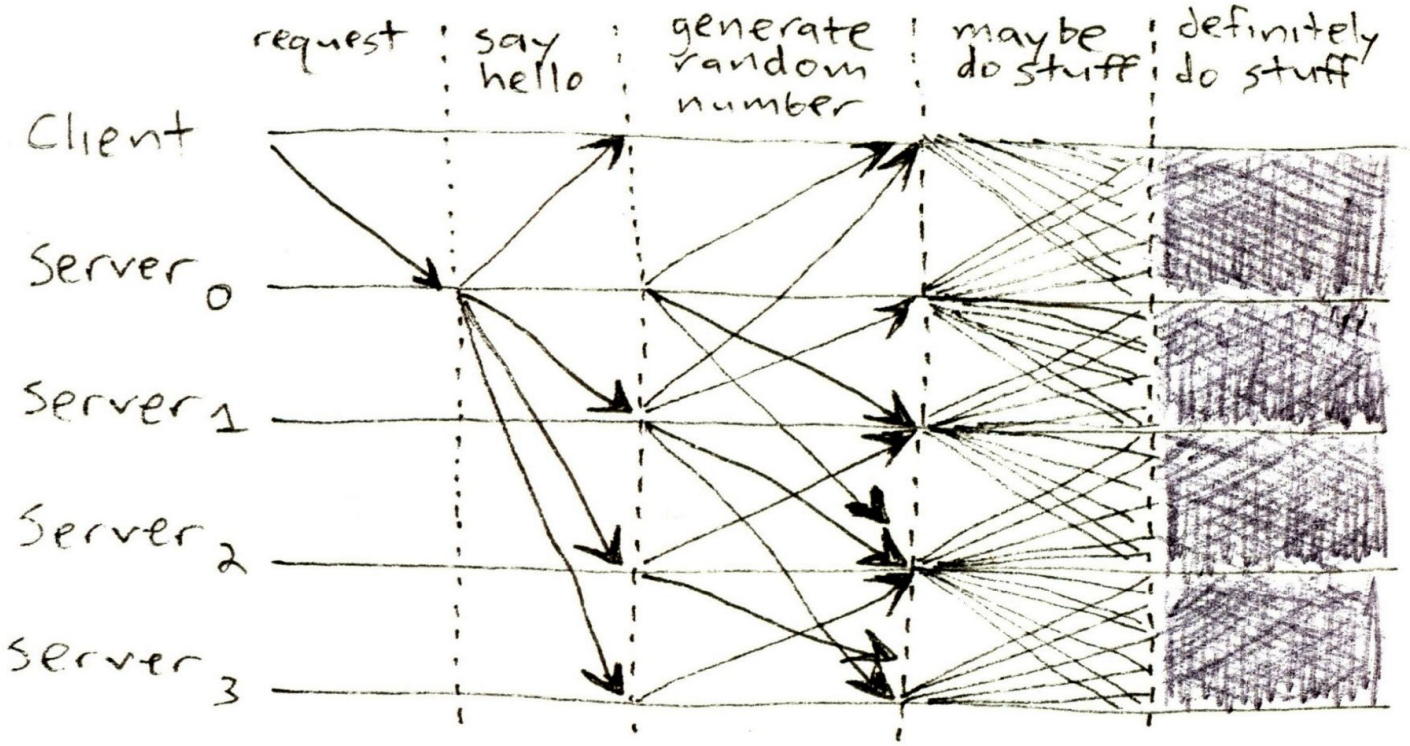
Ordered sequence of operations

State Machine Replication (SMR)

- Replicated service (e.g. Bank)
- Starts with the same state (initial account balances)
- Executes operations (transfer money)
  - Deterministic ("~~send random amount~~")
  - Same order
- Maintains same state (account balances)

SMR, the “Classic” Way

Consensus → Total Order Broadcast → Execution

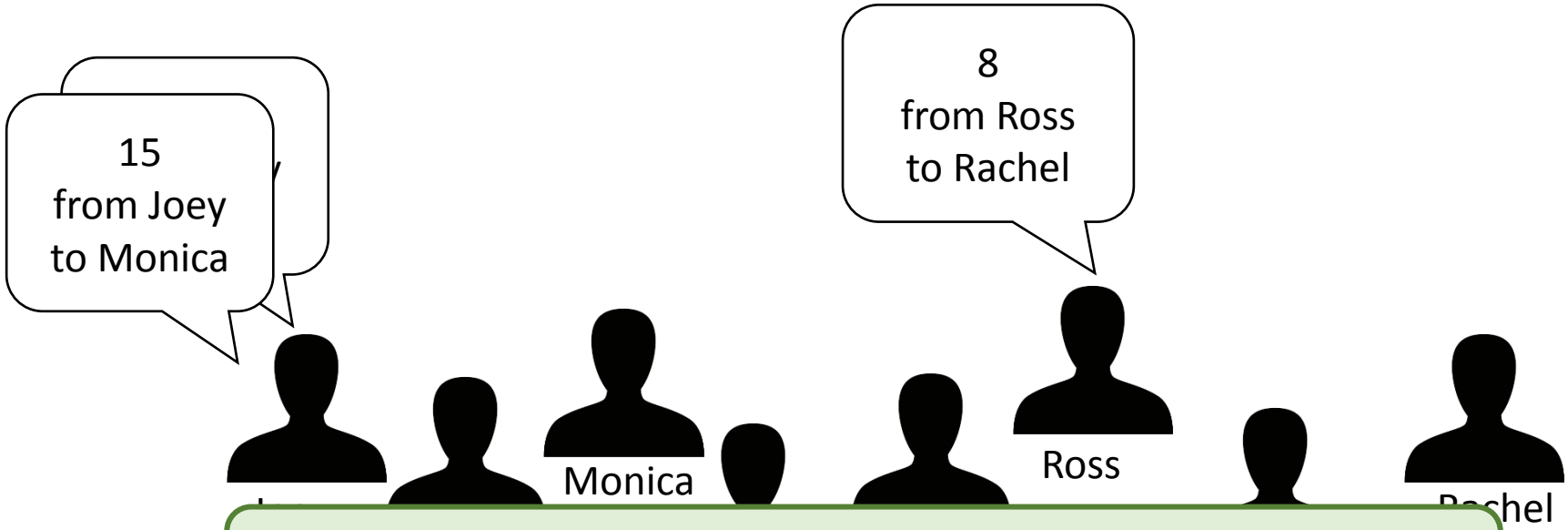


Picture by James Mickens, “The Saddest Moment”

Money as a State Machine

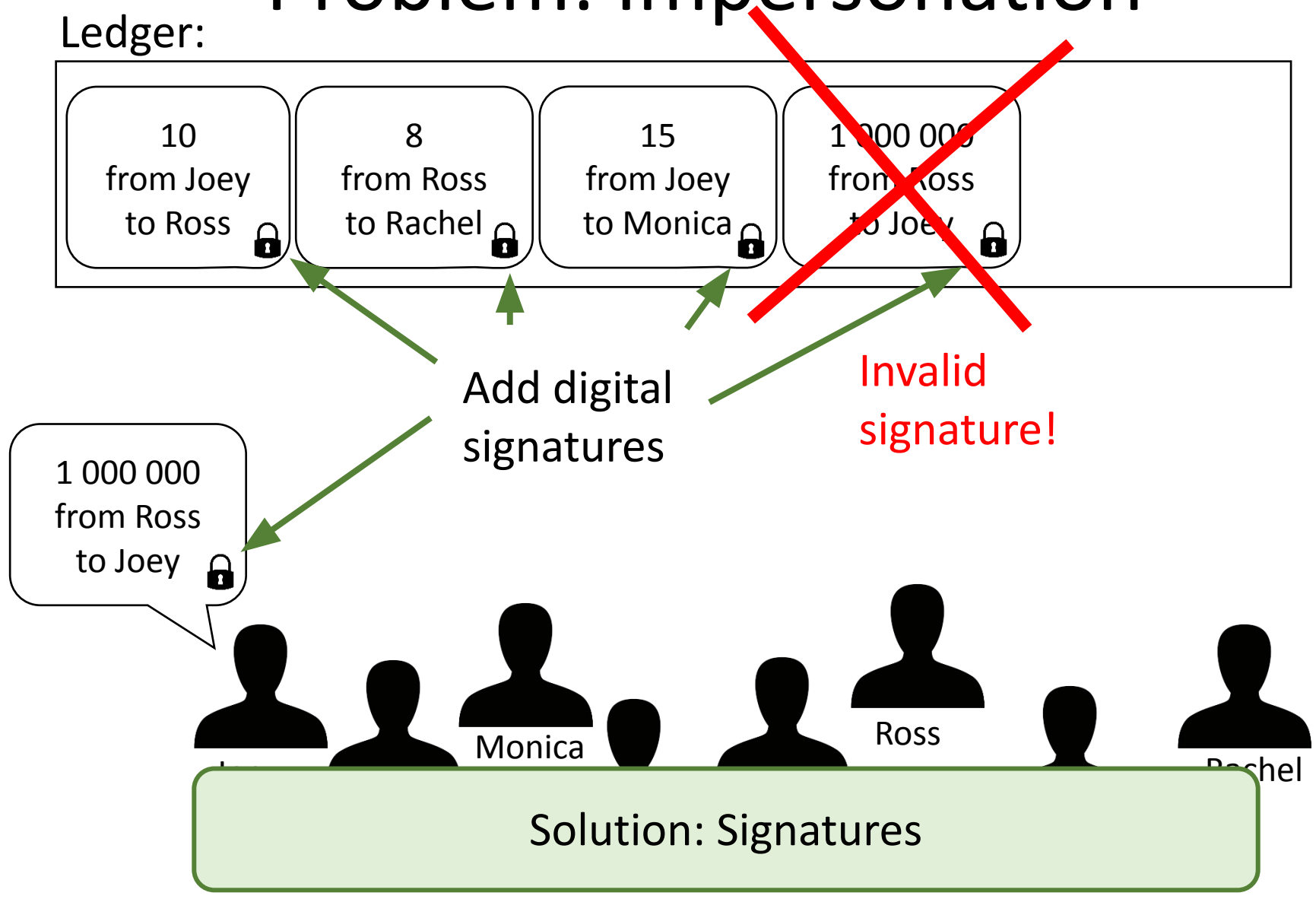
Ledger:

10 from Joey to Ross	8 from Ross to Rachel	15 from Joey to Monica

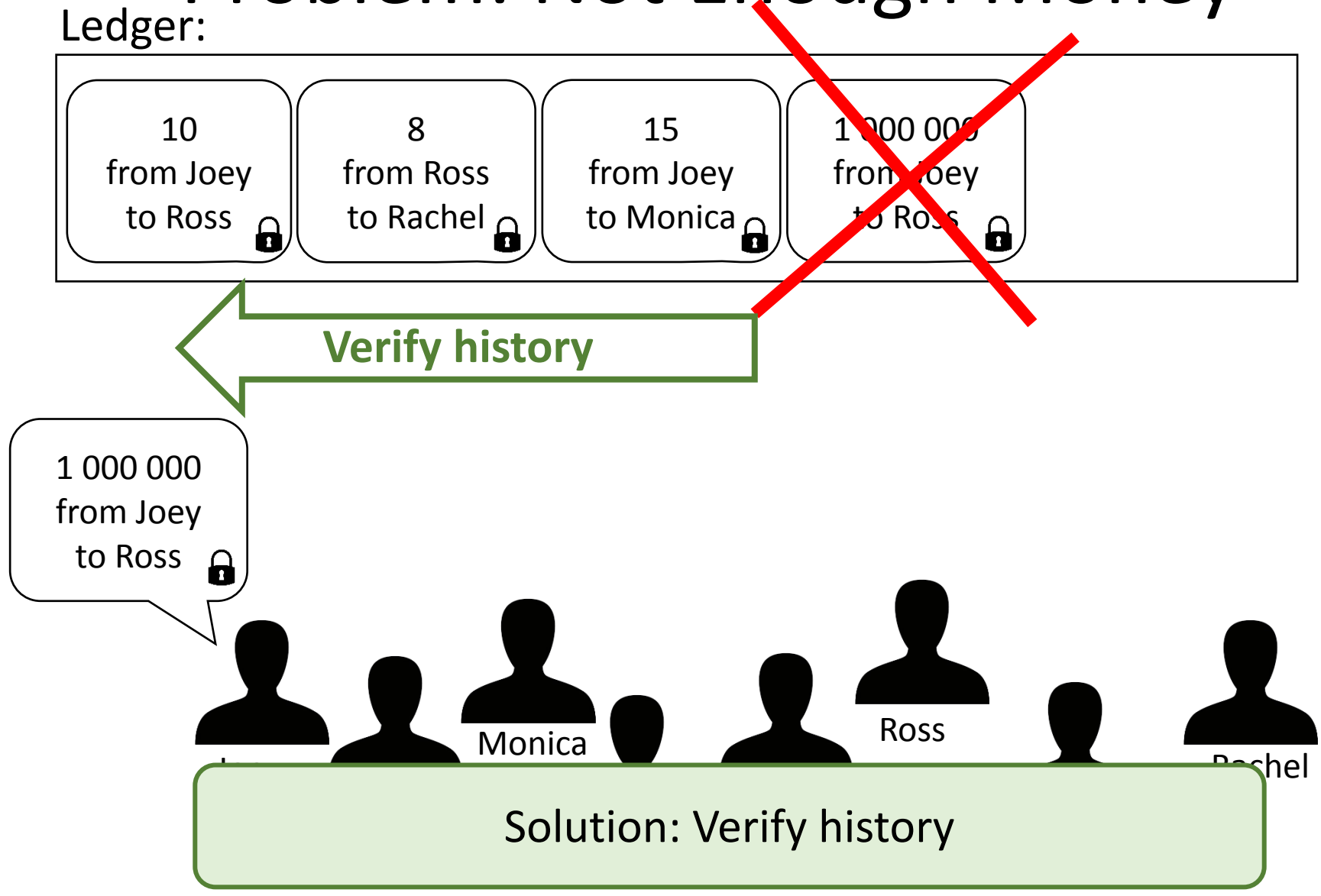


Problems ? (Hint: there are plenty)

Problem: Impersonation



Problem: Not Enough Money

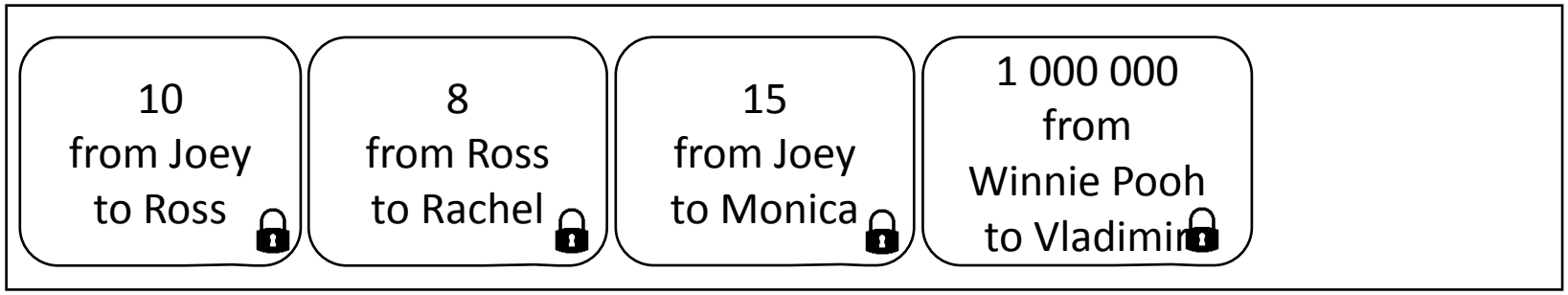


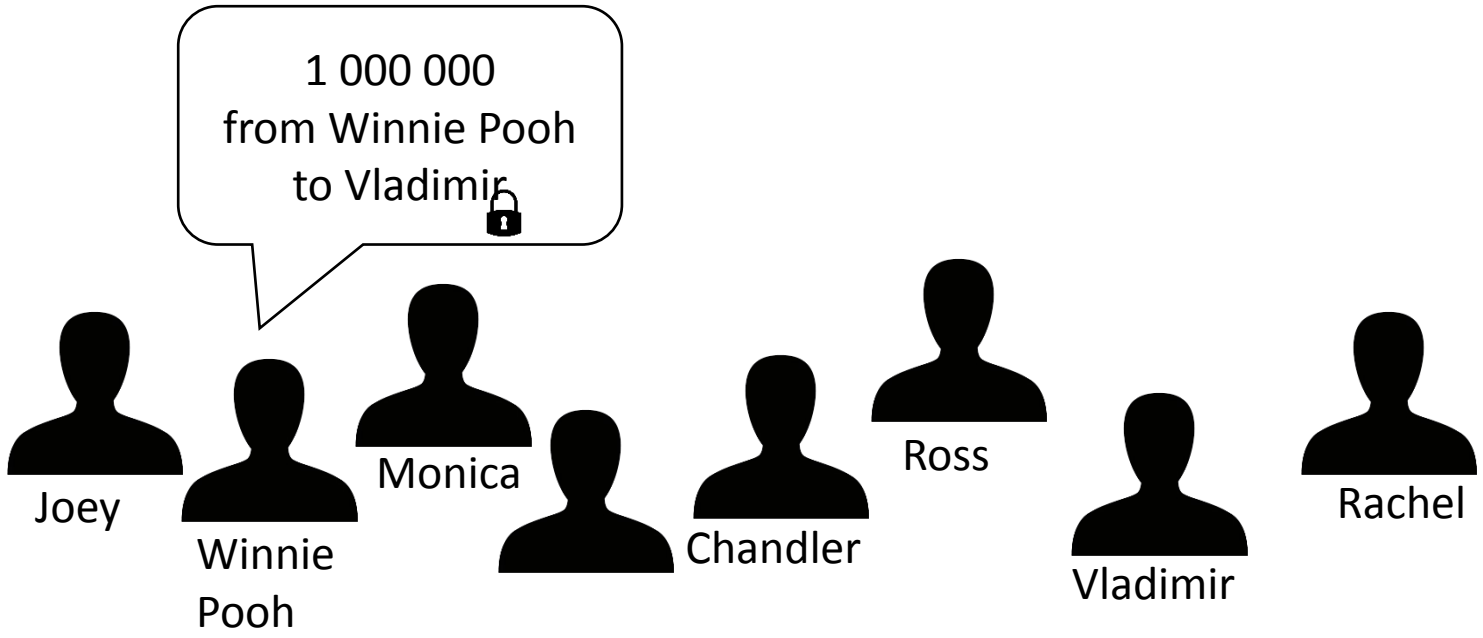
Recap

- Signing / Verifying

Problem: Anonymity?

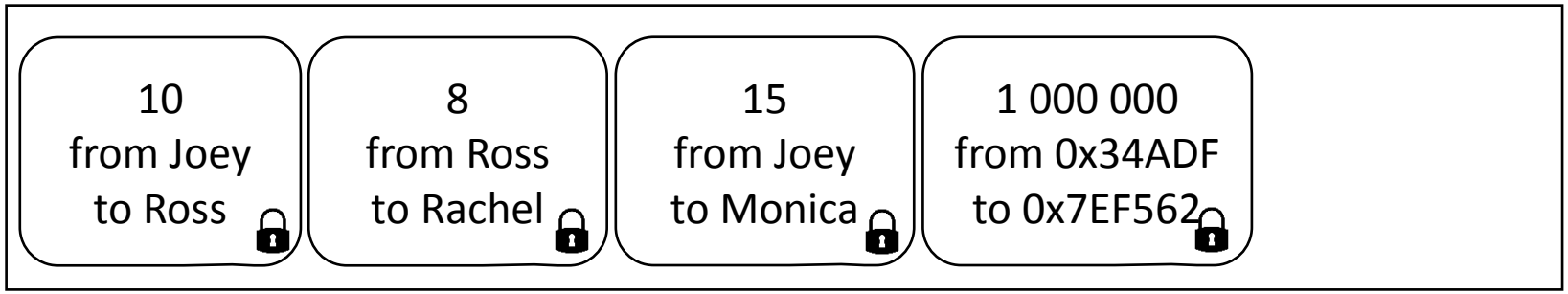
Ledger:

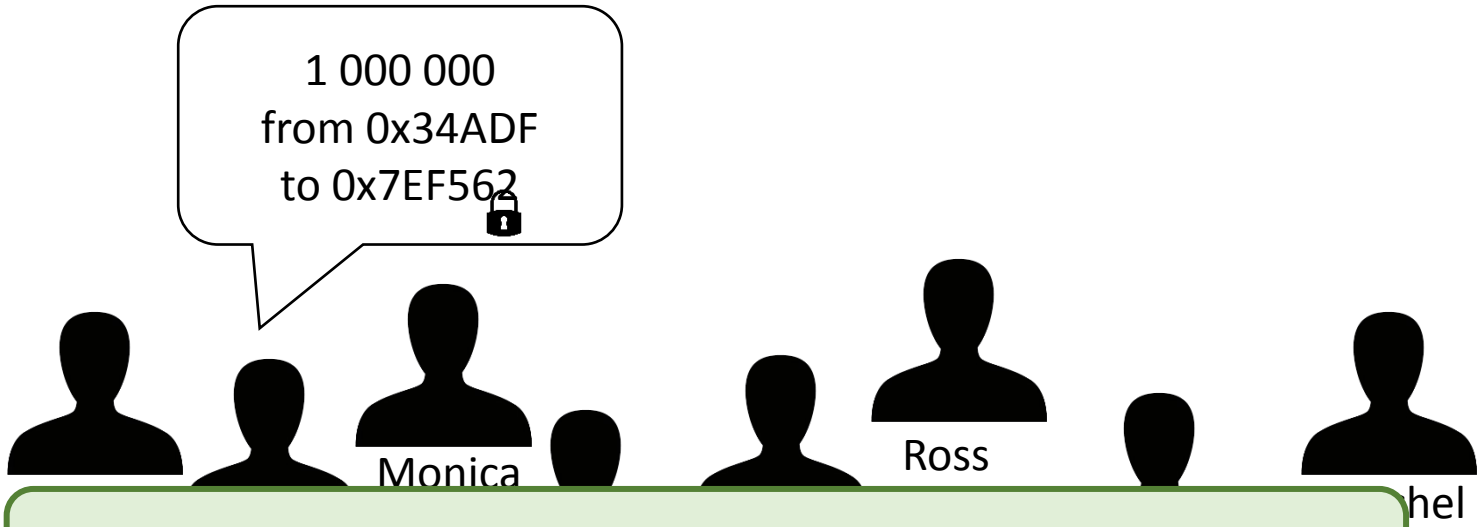




Problem: Anonymity?

Ledger:

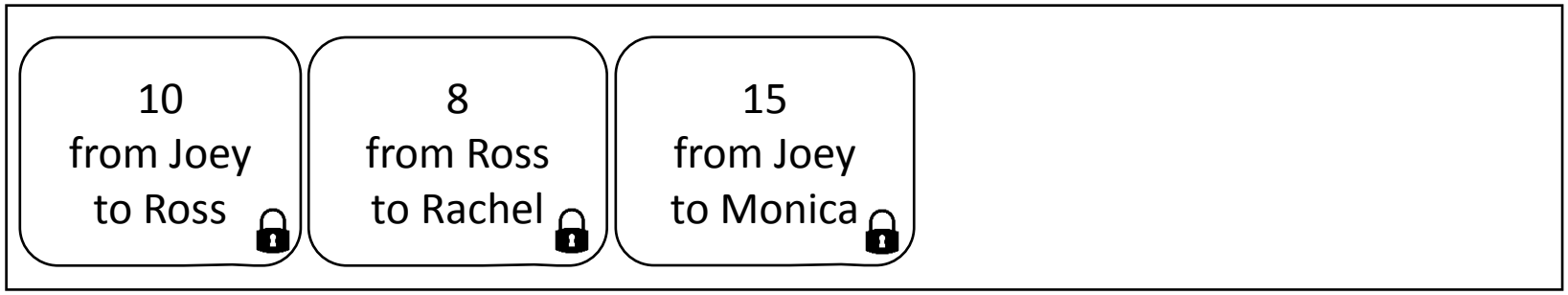




No need to disclose identity. Public key sufficient.

Problem: Who Stores the Ledger?

Ledger:

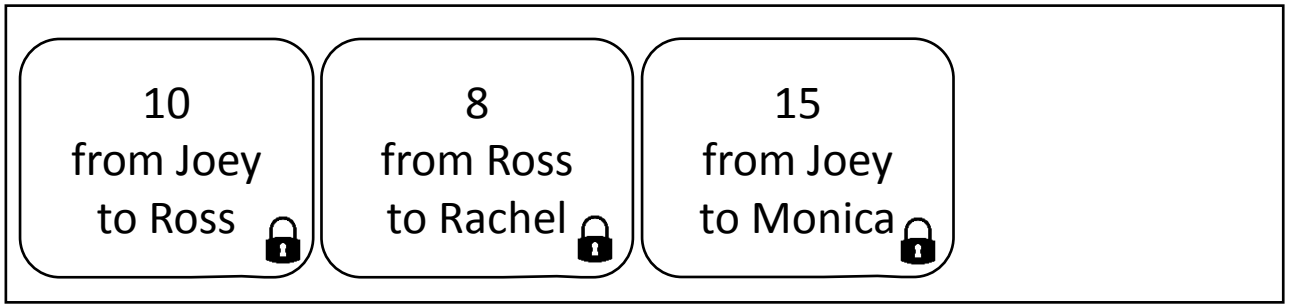


Everybody!

Problem: Who Stores the Ledger?

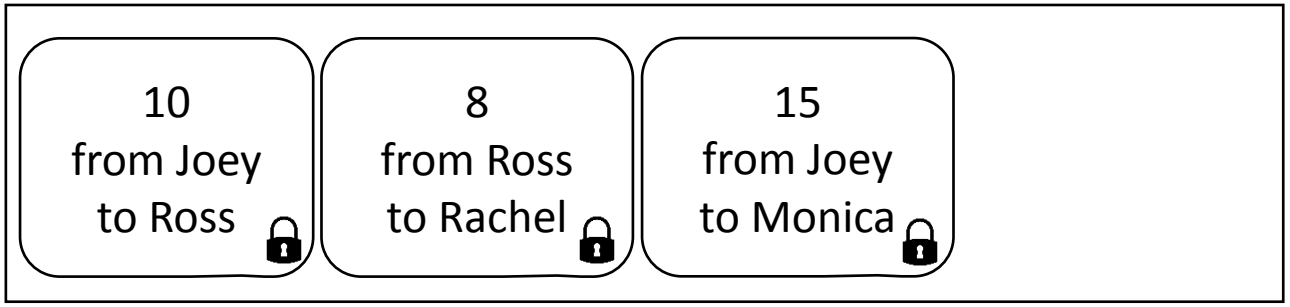
Joey

Joey's copy:



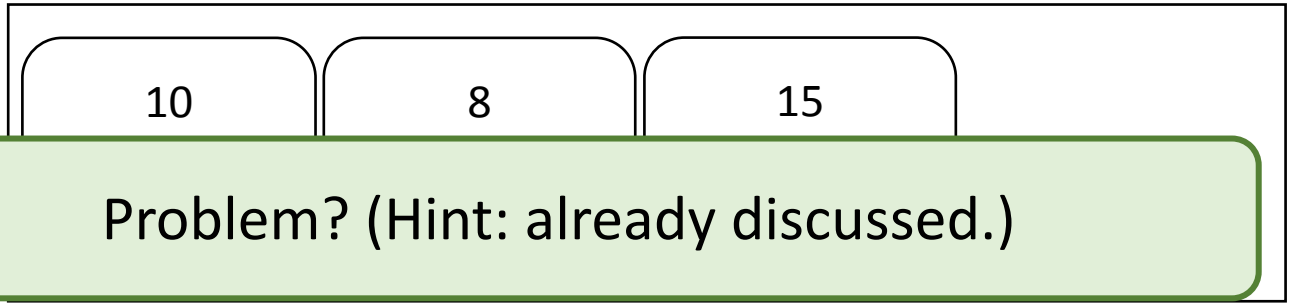
Monica

Monica's copy:



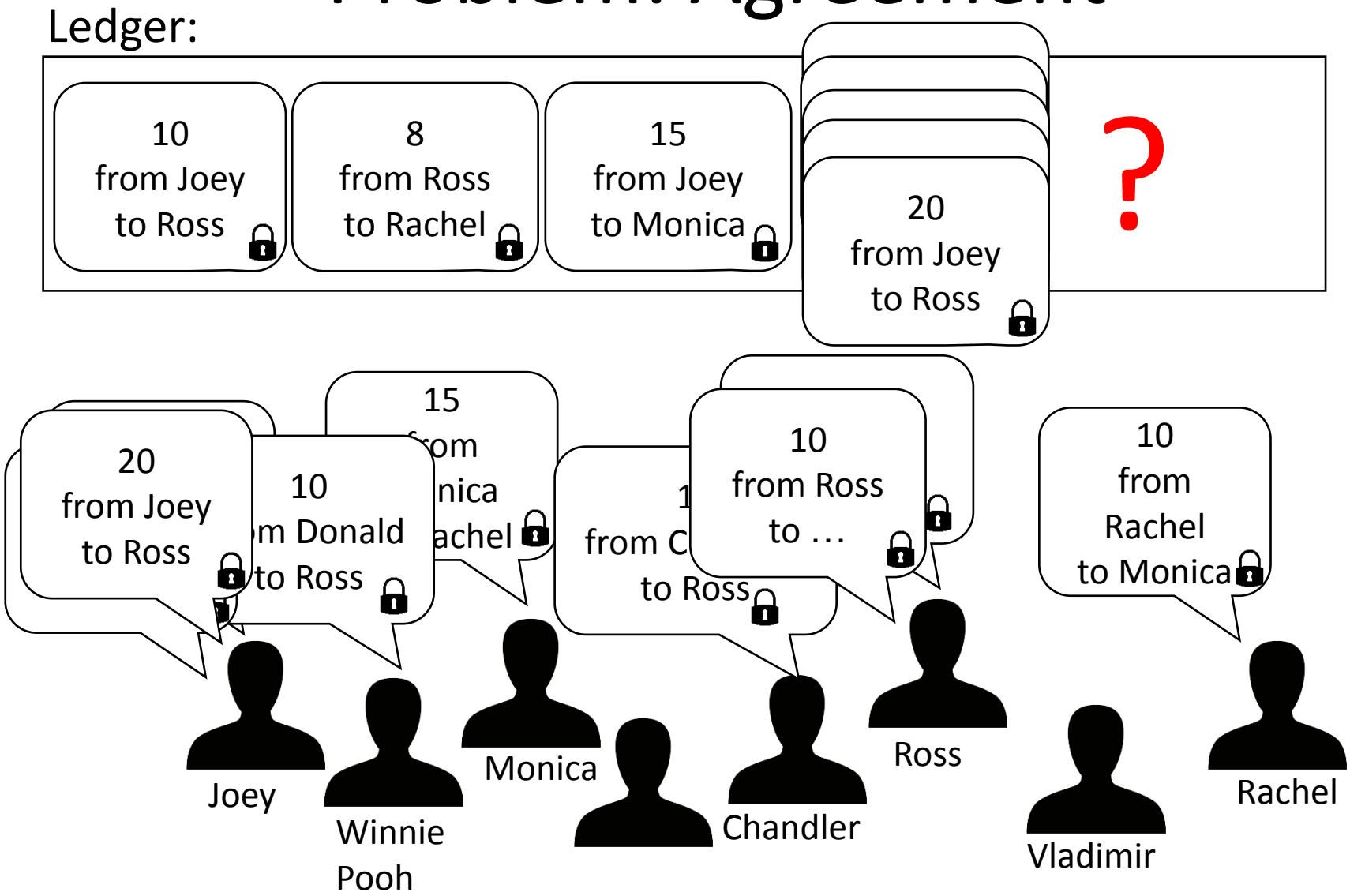
Ros

Ross's copy:

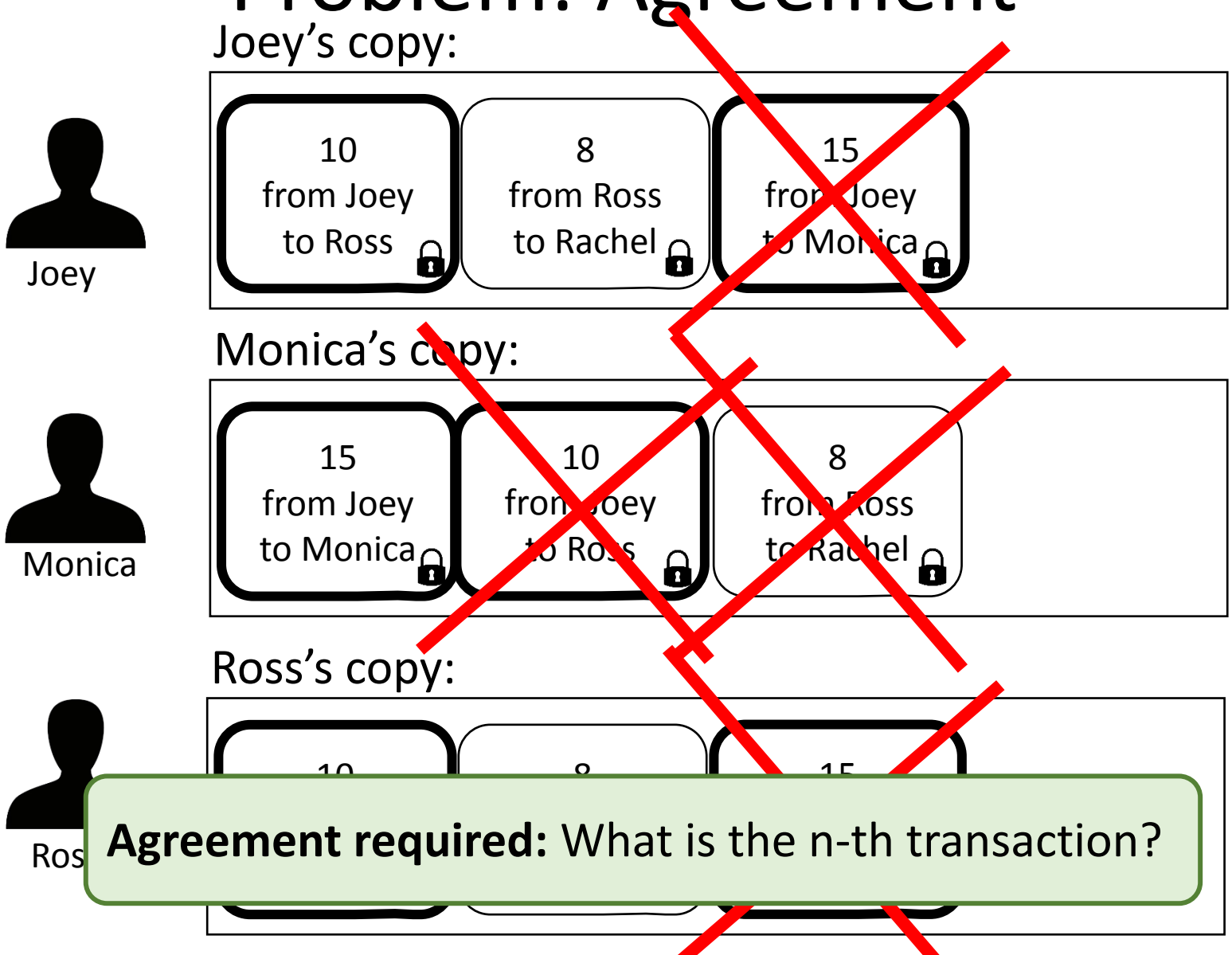


Problem? (Hint: already discussed.)

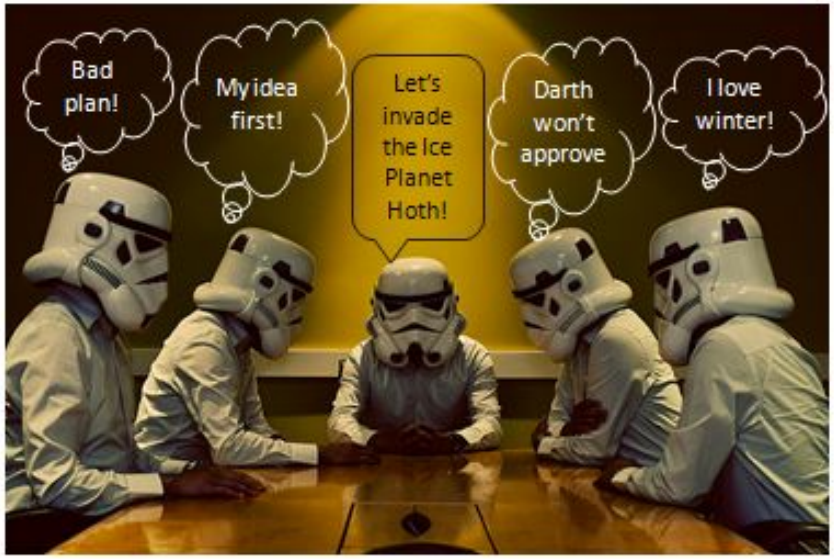
Problem: Agreement



Problem: Agreement



Agreement



Agreement on a single value among multiple parties

Safety: No two parties must choose different values.

The chosen value must have been proposed by someone.

Liveness: Everyone must eventually choose a value.

Easy, but hard

Agreement Is Easy

- Someone always decides
- Everybody votes (and nobody lies)

Not always possible

Agreement Is Hard

- No (trusted) authority to decide
- Not everybody votes
- Somebody lies
- Communication difficulties

Fundamental problem, sometimes no solution

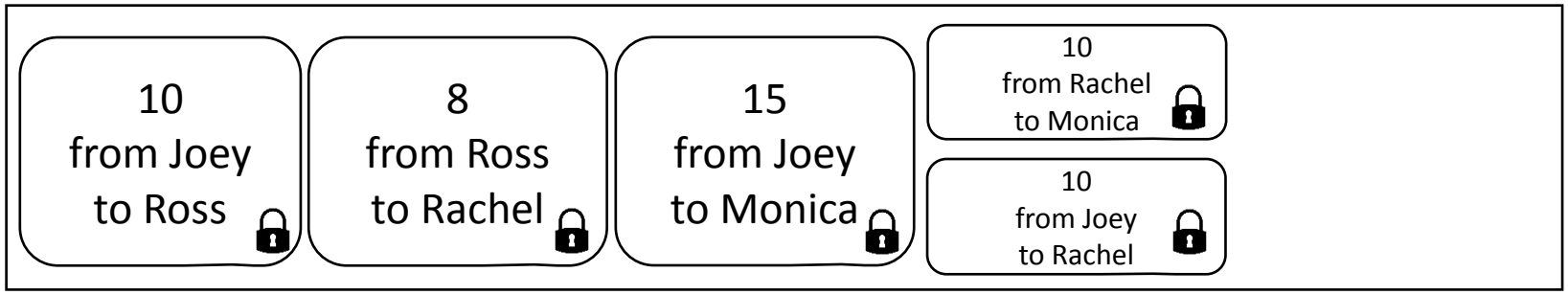
How Do We Solve Agreement?

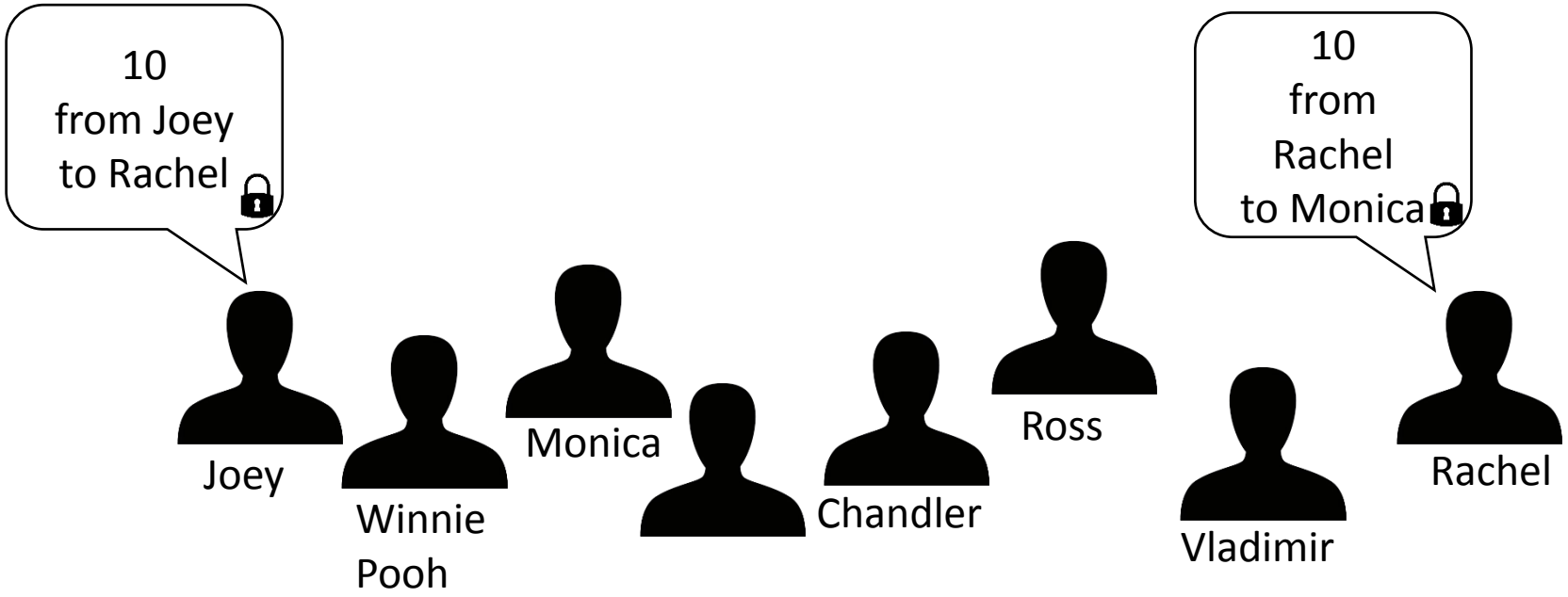
?

Technically, **we don't!** (We just make problems unlikely)

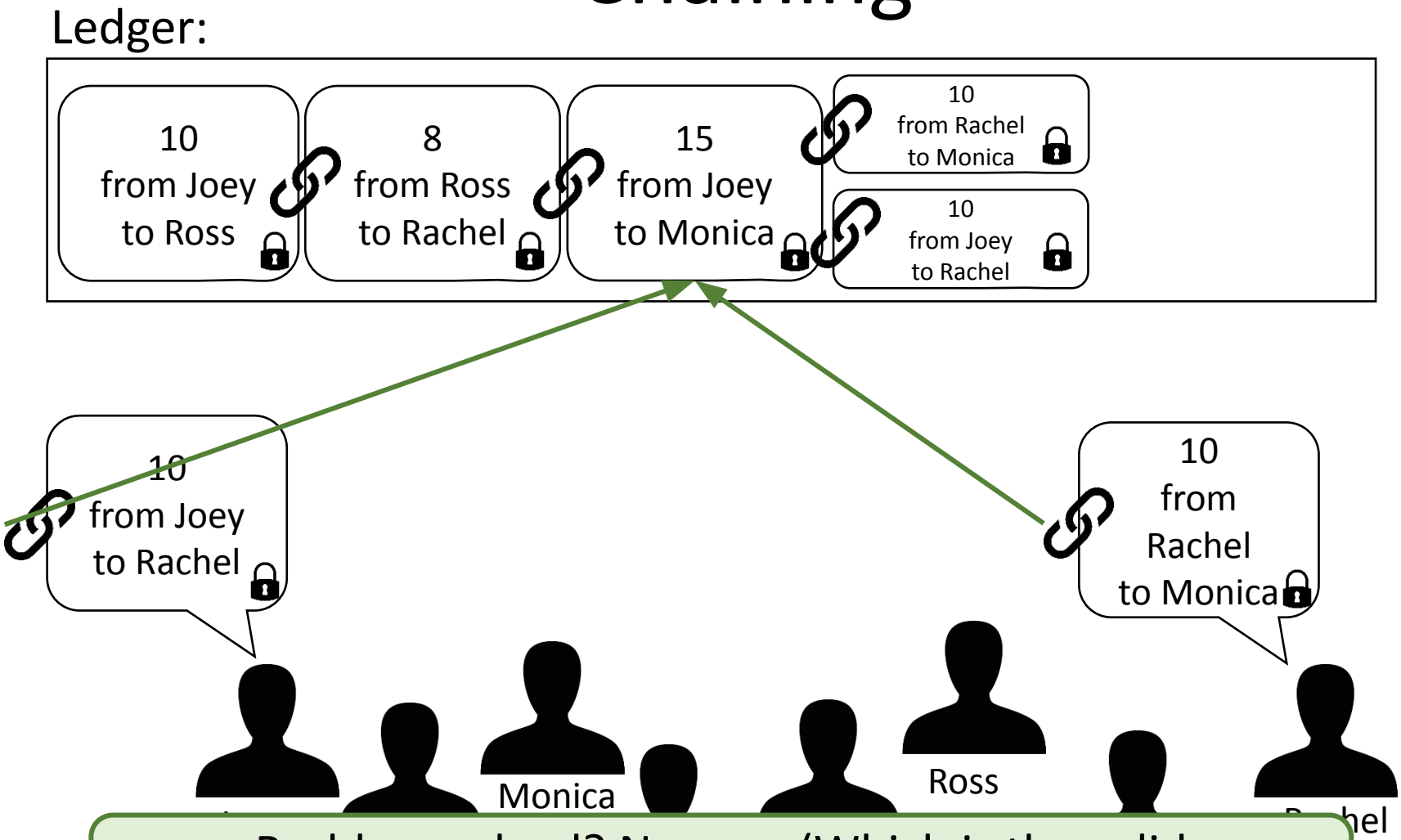
Chaining

Ledger:





Chaining



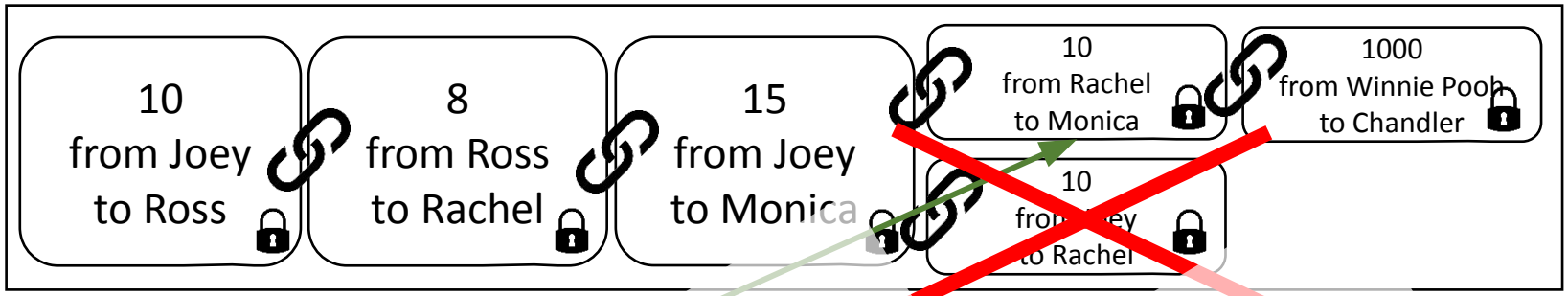
Problem solved? Nope… (Which is the valid transaction?)

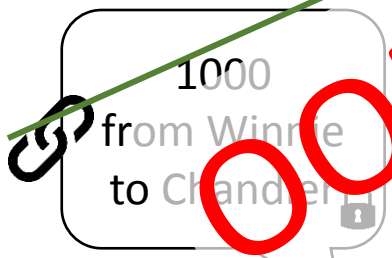
Recap

- Signing / Verifying
- Chaining

Voting

Ledger:





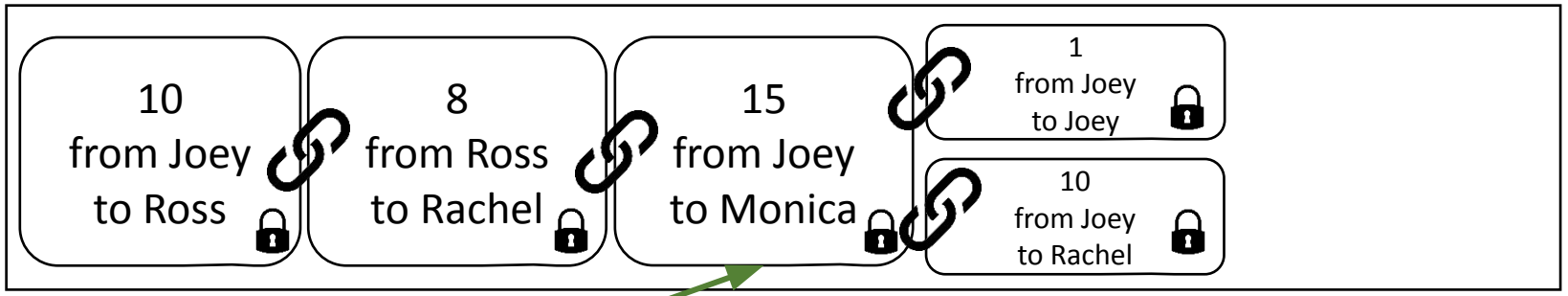
OOPS!

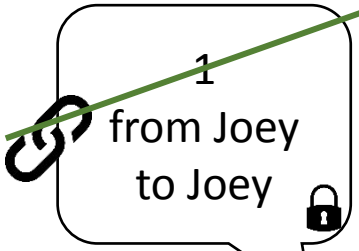
BIG PROBLEM...

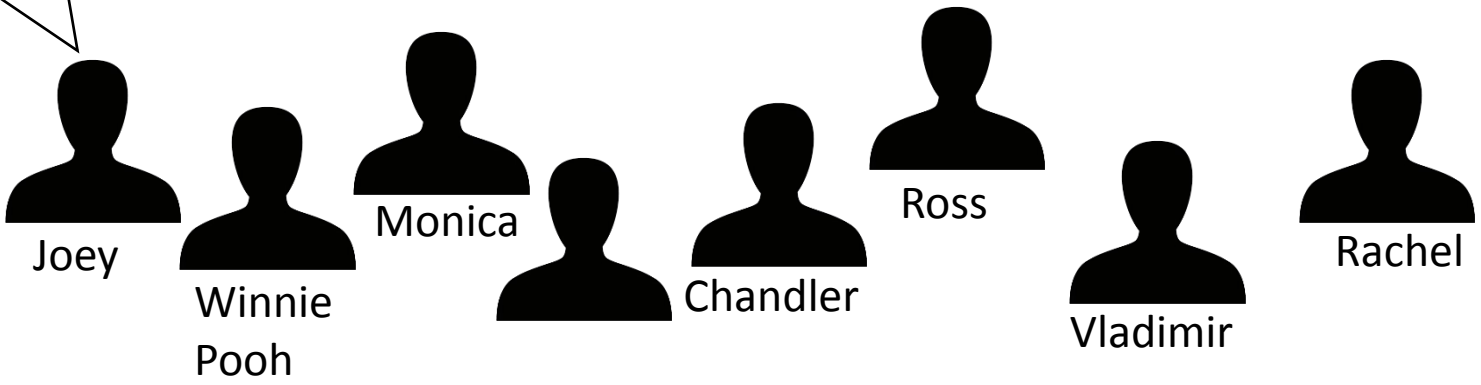
Longest chain is valid (by definition).

Cheating

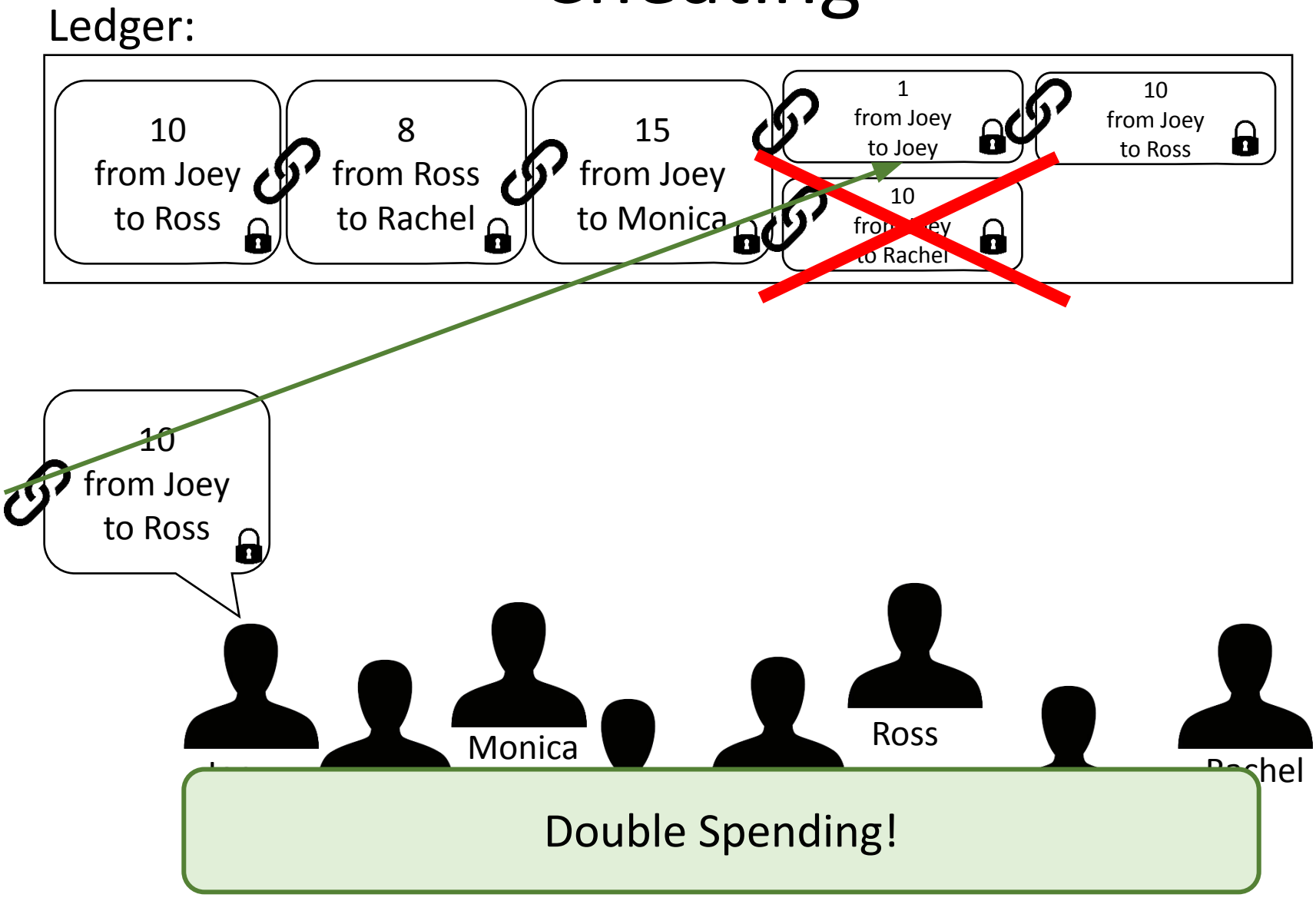
Ledger:





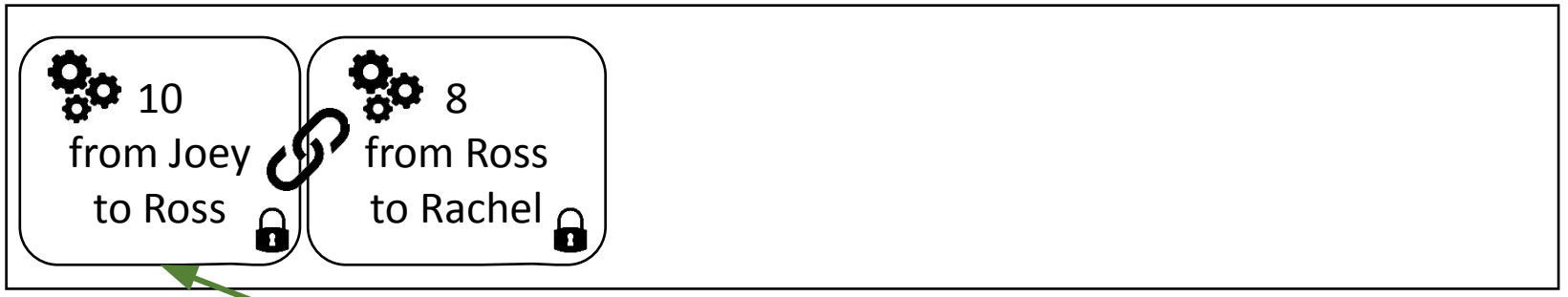


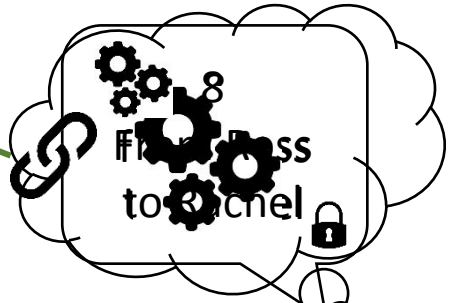
Cheating

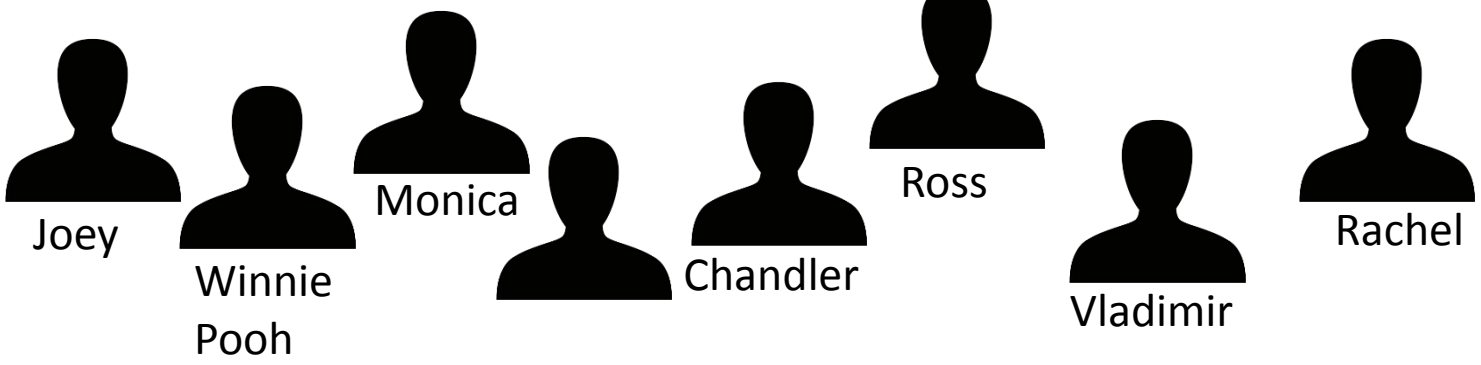

Ledger:
10
from Joey
to Ross
8
from Ross
to Rachel
15
from Joey
to Monica
1
from Joey
to Joey
10
from Joey
to Ross
10
from Joey
to Rachel
10
from Joey
to Ross
Monica
Ross
Double Spending!

Working

Ledger:

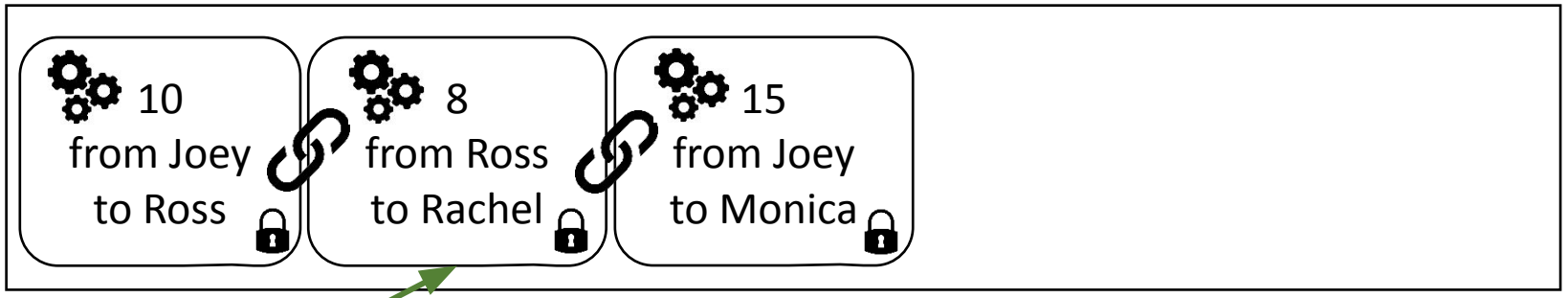


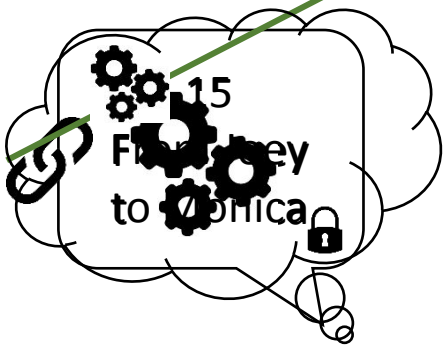


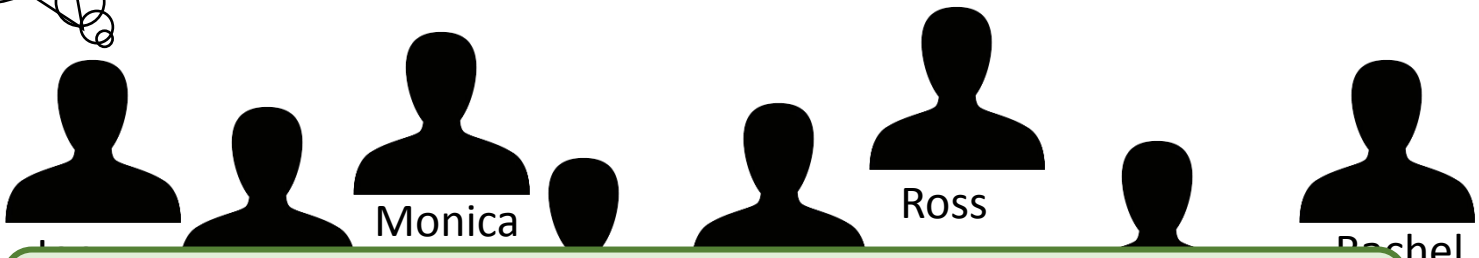


Working

Ledger:

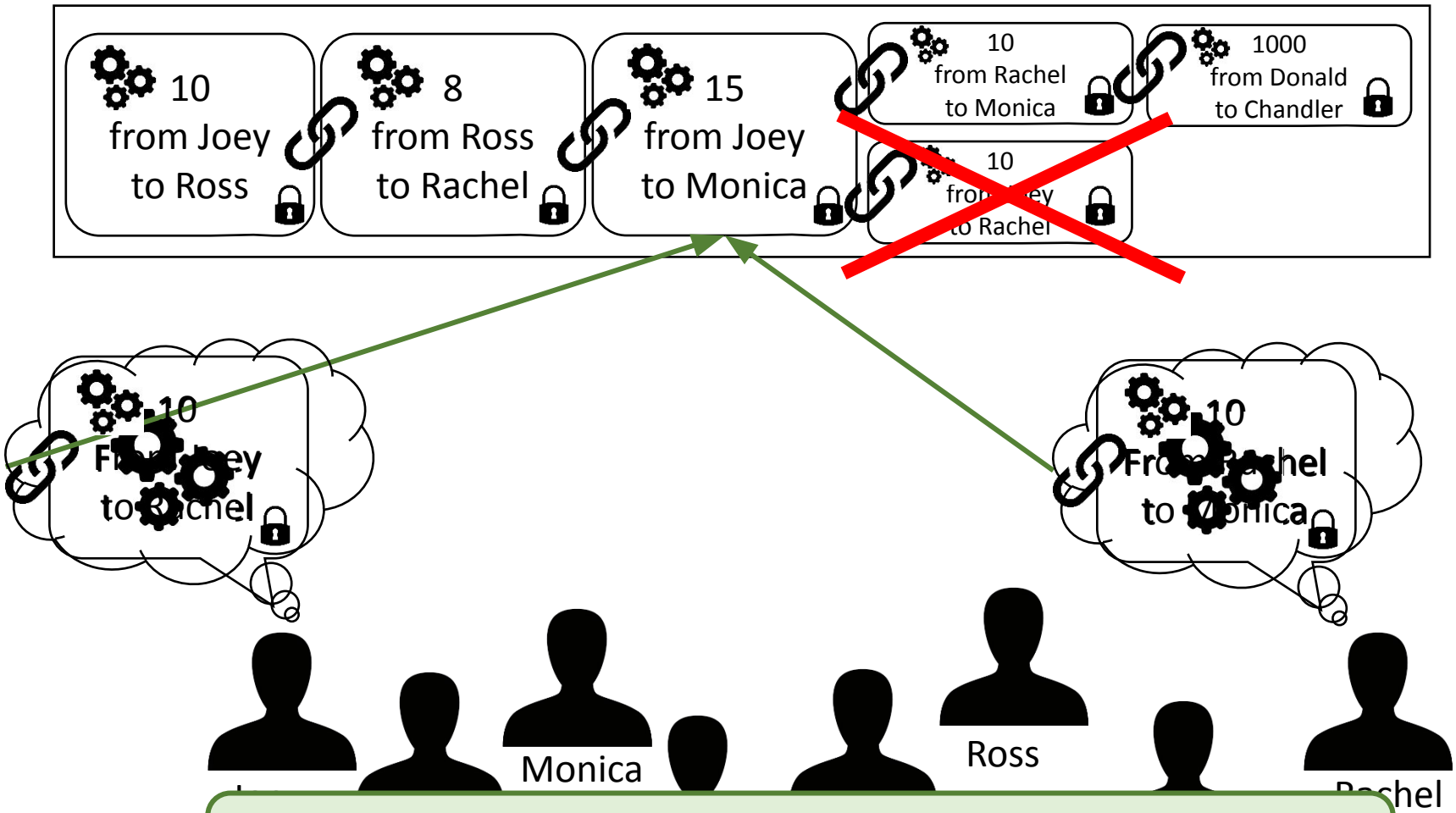






Work is very hard

Working

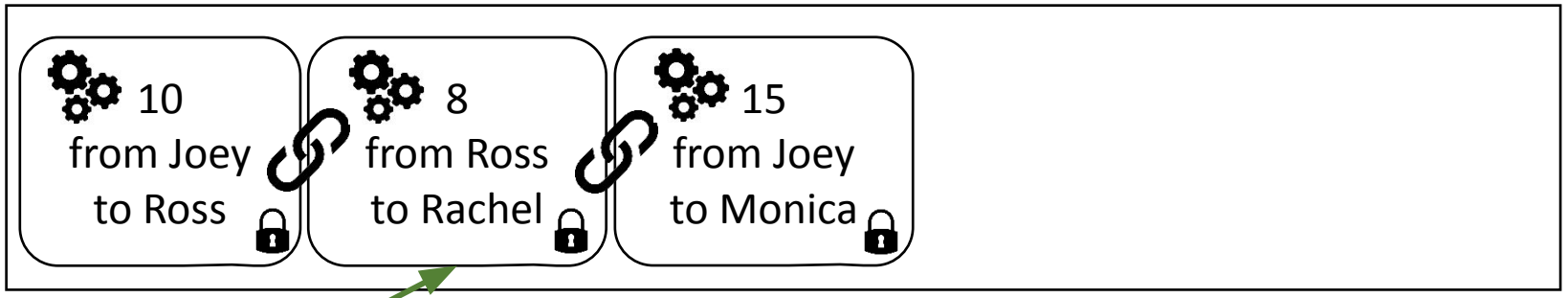

Ledger:
10
from Joey
to Ross
8
from Ross
to Rachel
15
from Joey
to Monica
10
from Rachel
to Monica
1000
from Donald
to Chandler
10
to Rachel
10
to Monica
Monica
Ross
FORK. Happens rarely. (When…?)

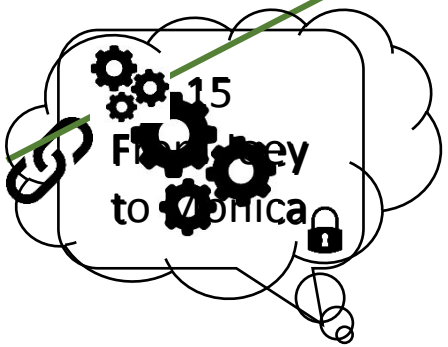
Recap

- Signing / Verifying
- Chaining
- Voting
- Working

Working

Ledger:

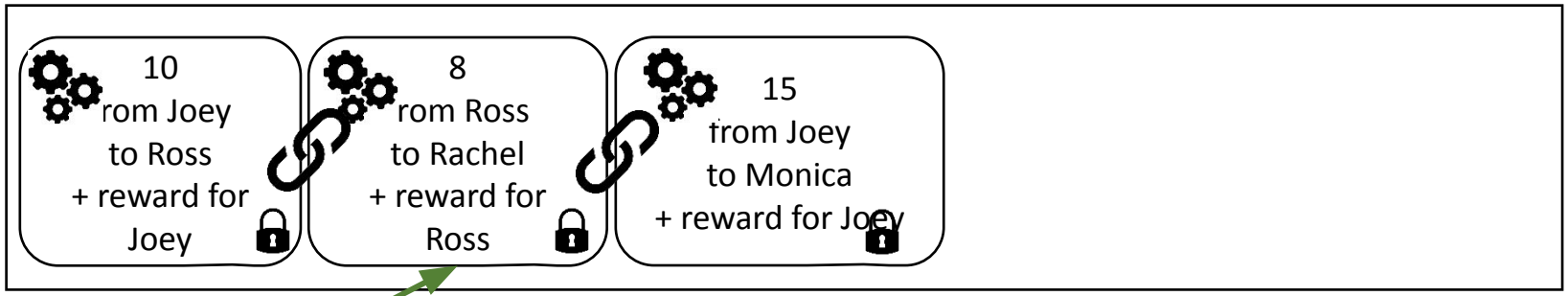


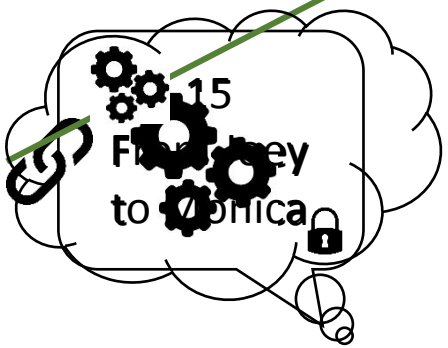


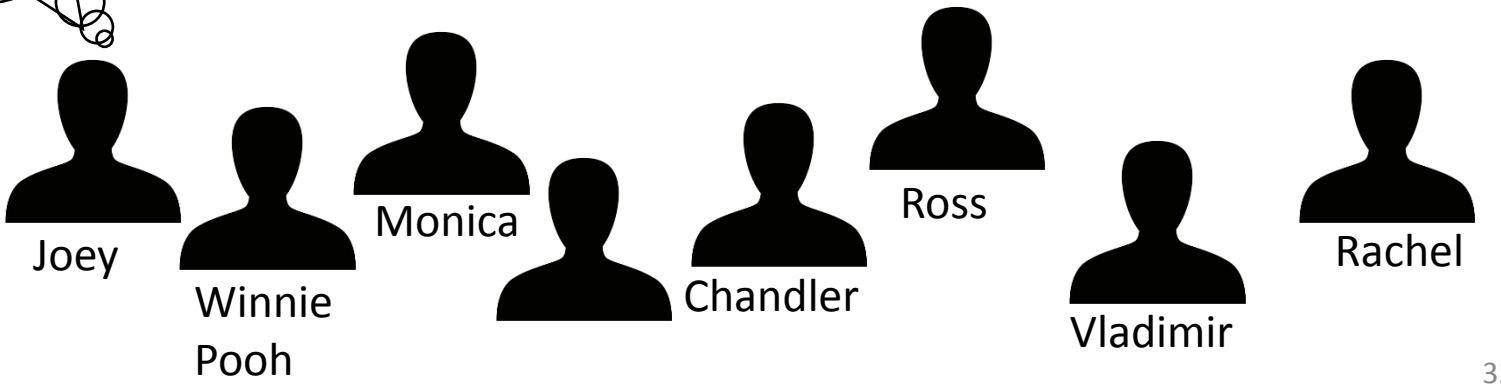
Work is very hard… Why do it?

Rewards

Ledger:







Recap

- Signing / Verifying
- Chaining
- Voting
- Working
- Rewards

Proof-of-Work Blockchain!!!


bitcoin

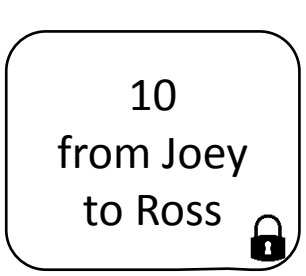
How Exactly… ?

- Signing / Verifying → Unspent TX Output
- Chaining → Blocks, Hashes
- Voting → Proof of Work
- Working → Mining
- Rewards → New coins, TX fees

How Exactly… ?

- Signing / Verifying → Unspent TX Output

Simply:



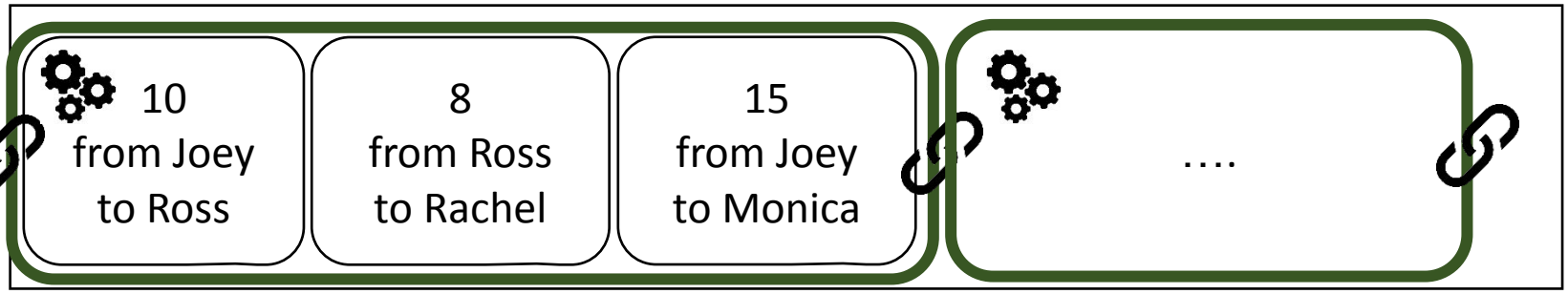
But actually…

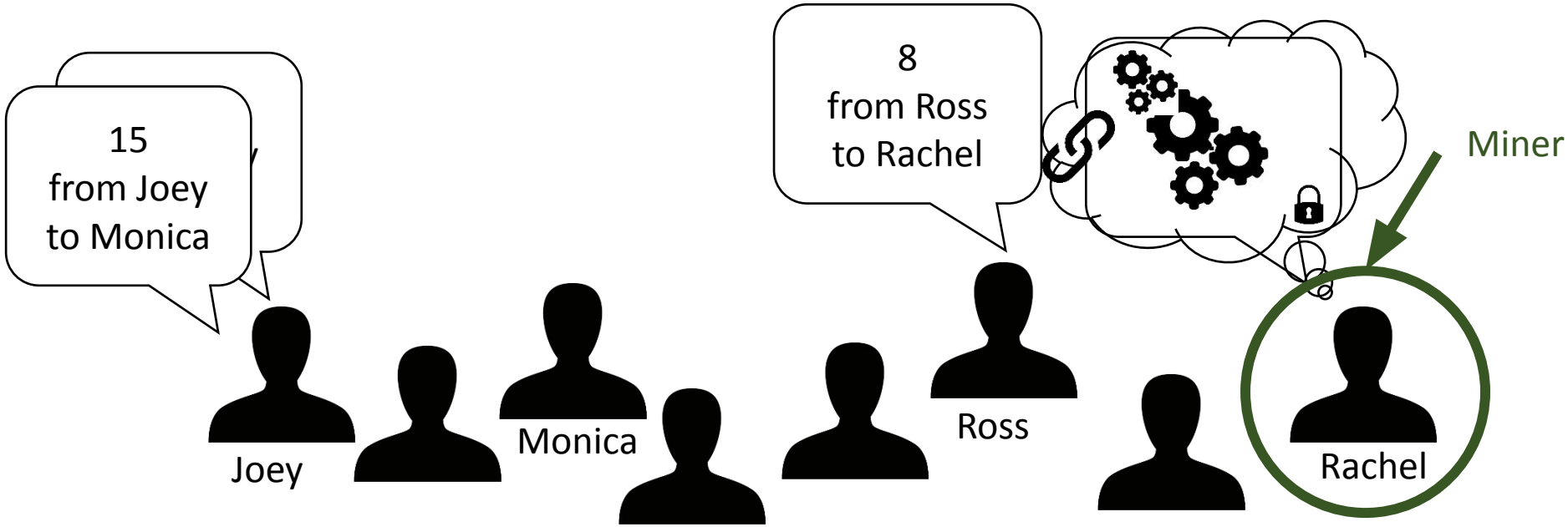
How Exactly… ?

- Signing / Verifying → Unspent TX Output
- Chaining  → Blocks, Hashes

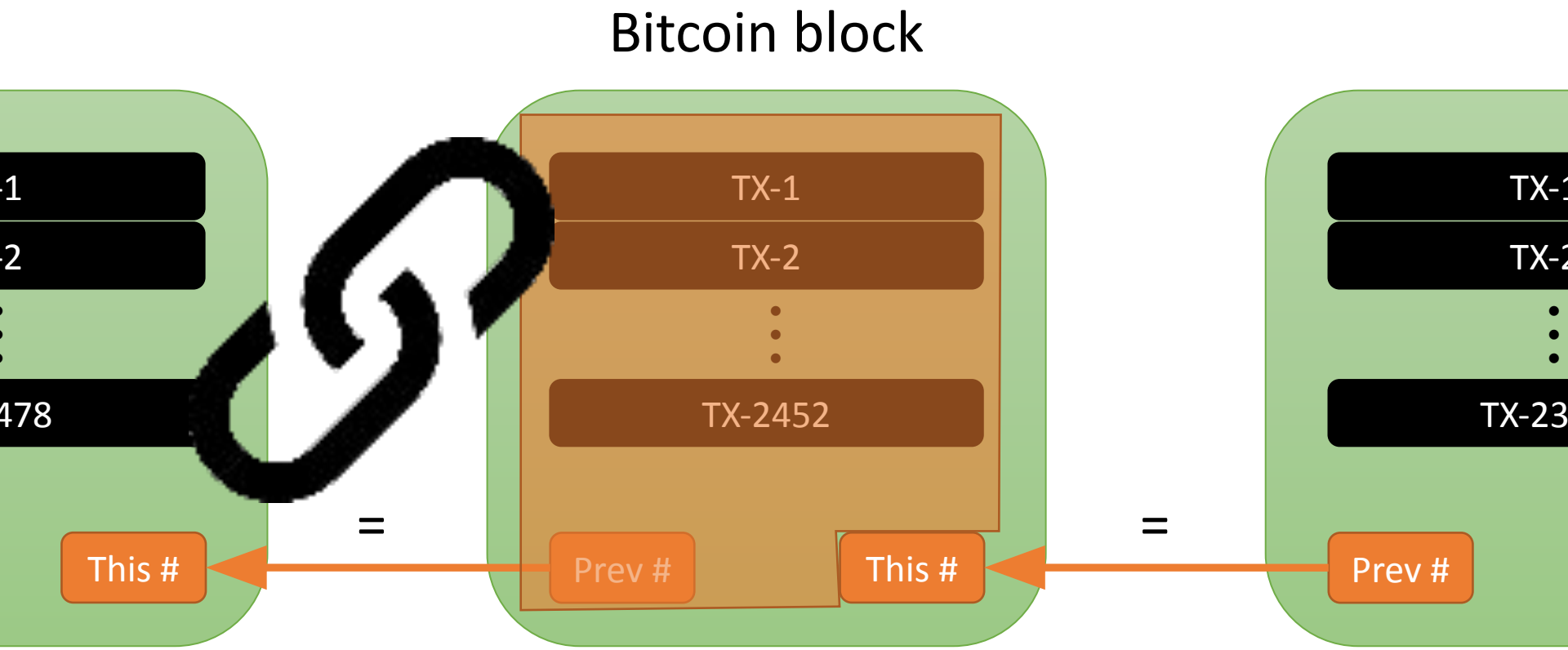
Blocks

Ledger:





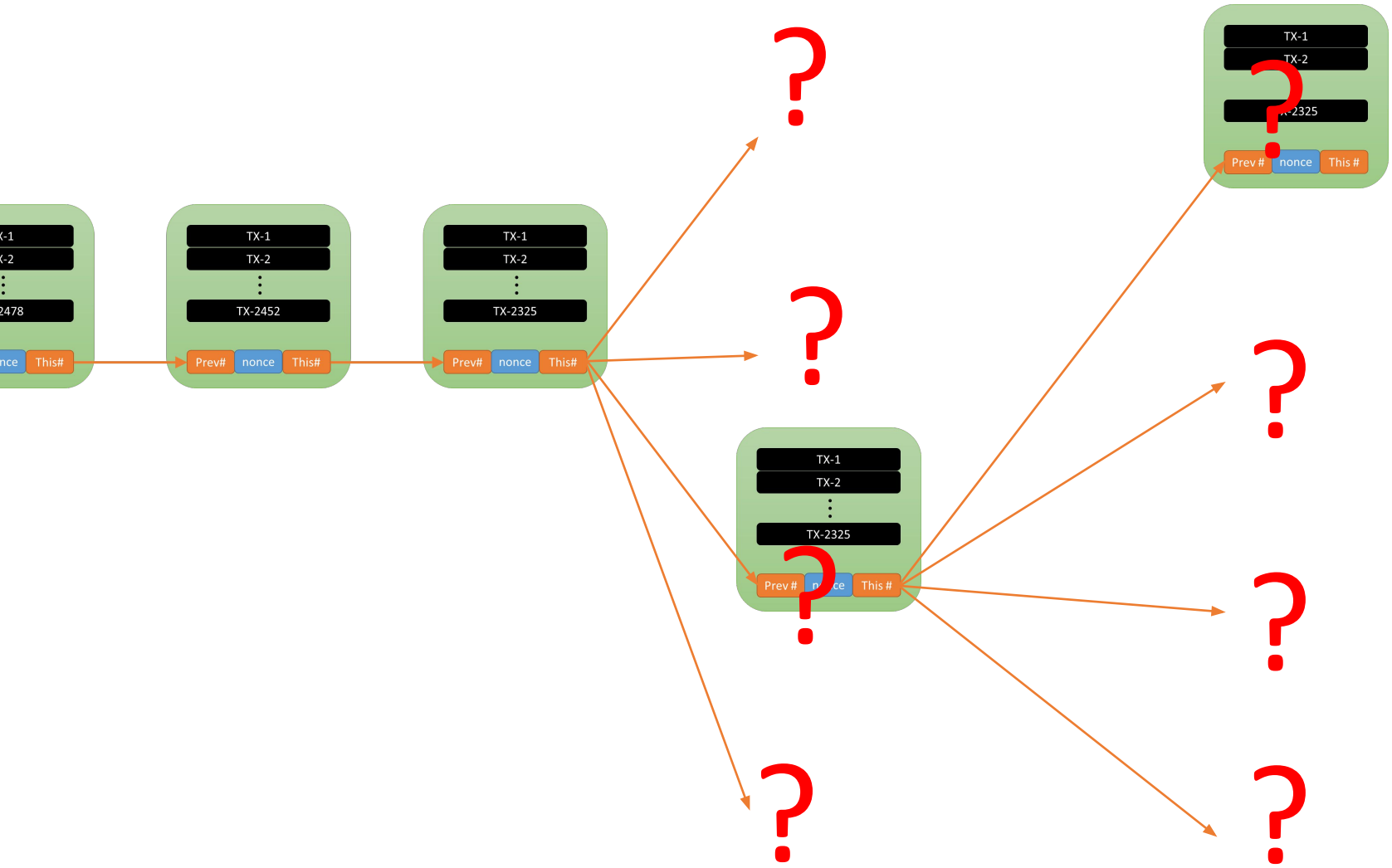
Block Chaining (Hashes)



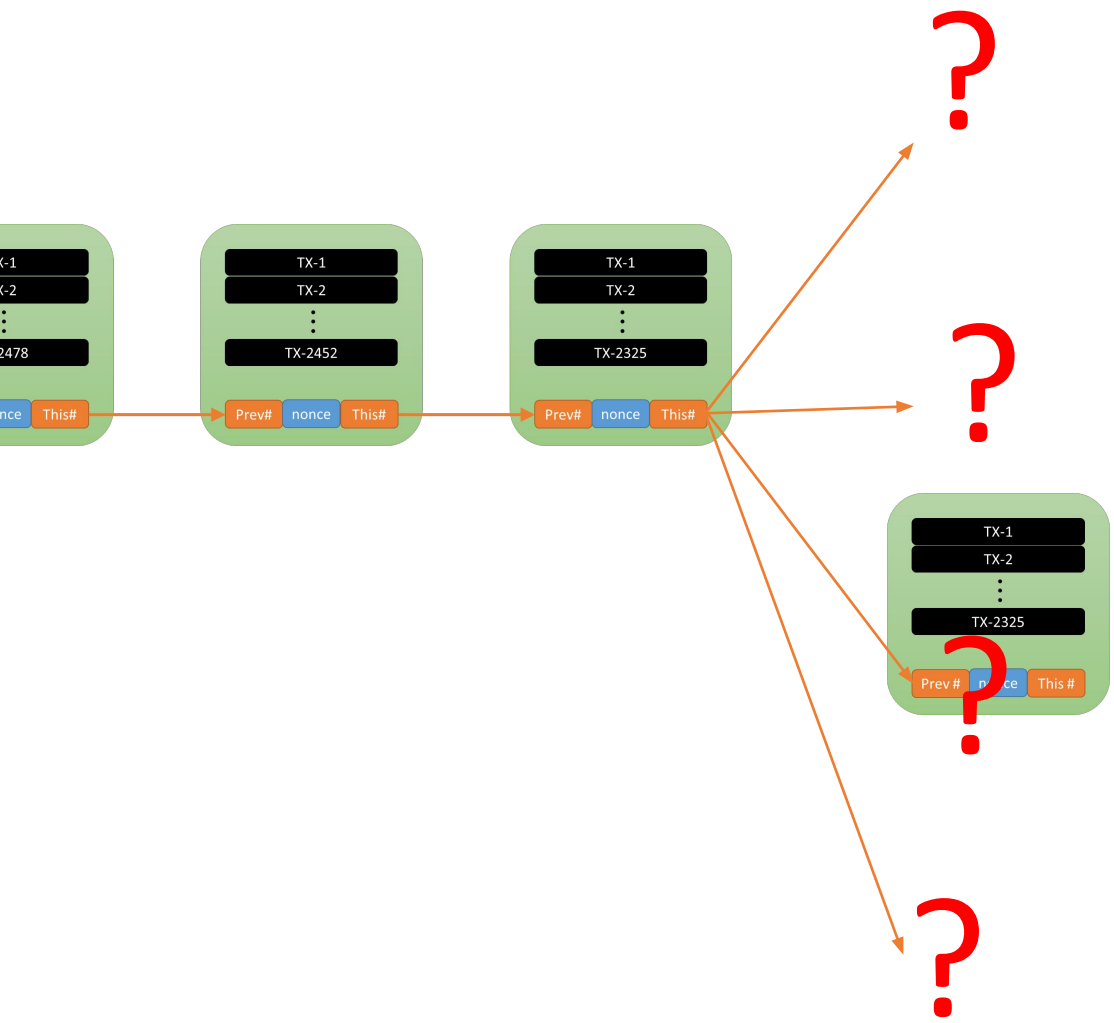
How Exactly… ?

- Signing / Verifying → Unspent TX Output
- Chaining → Blocks, Hashes
- Voting → Prolonging the Chain

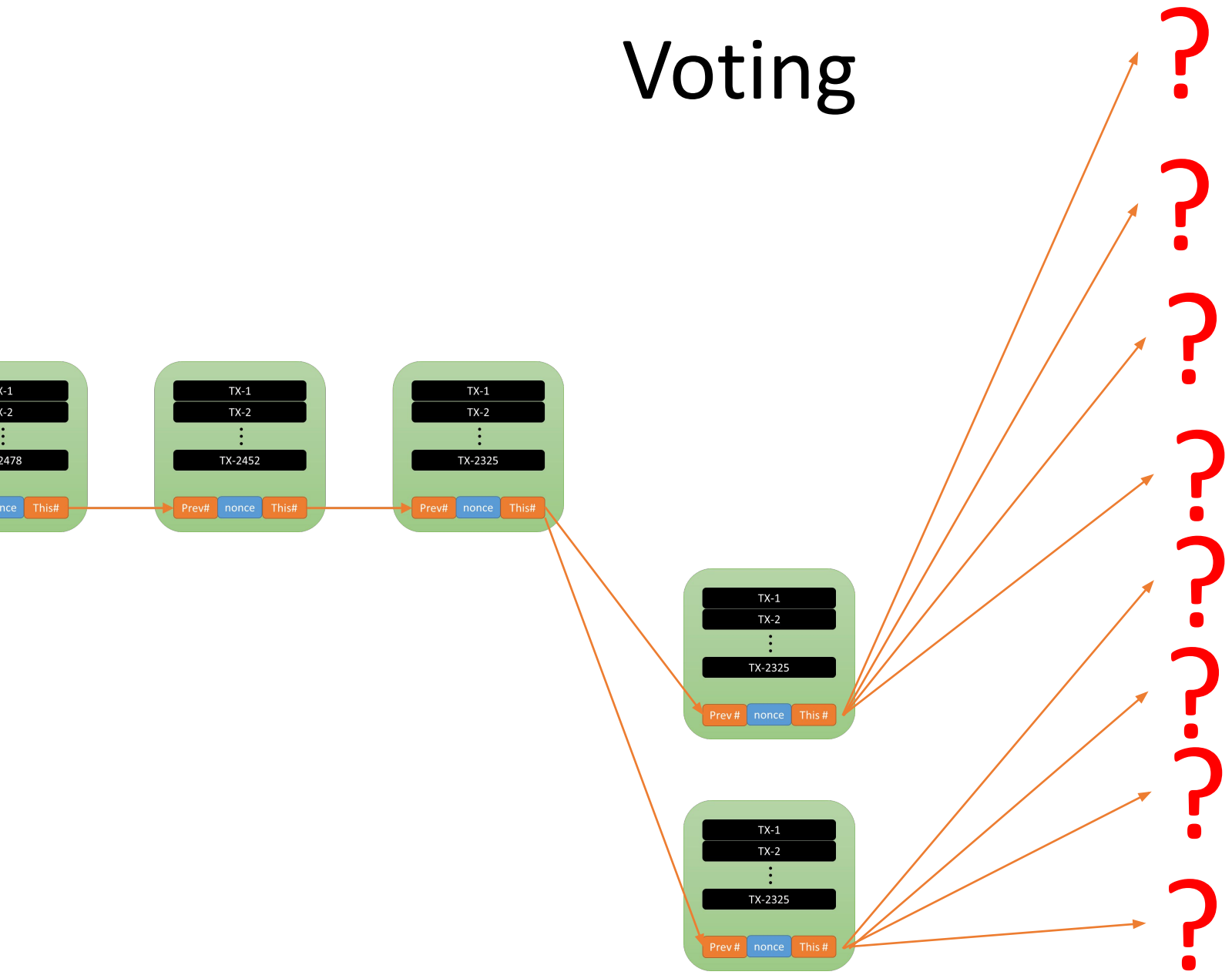
Prolonging the Chain



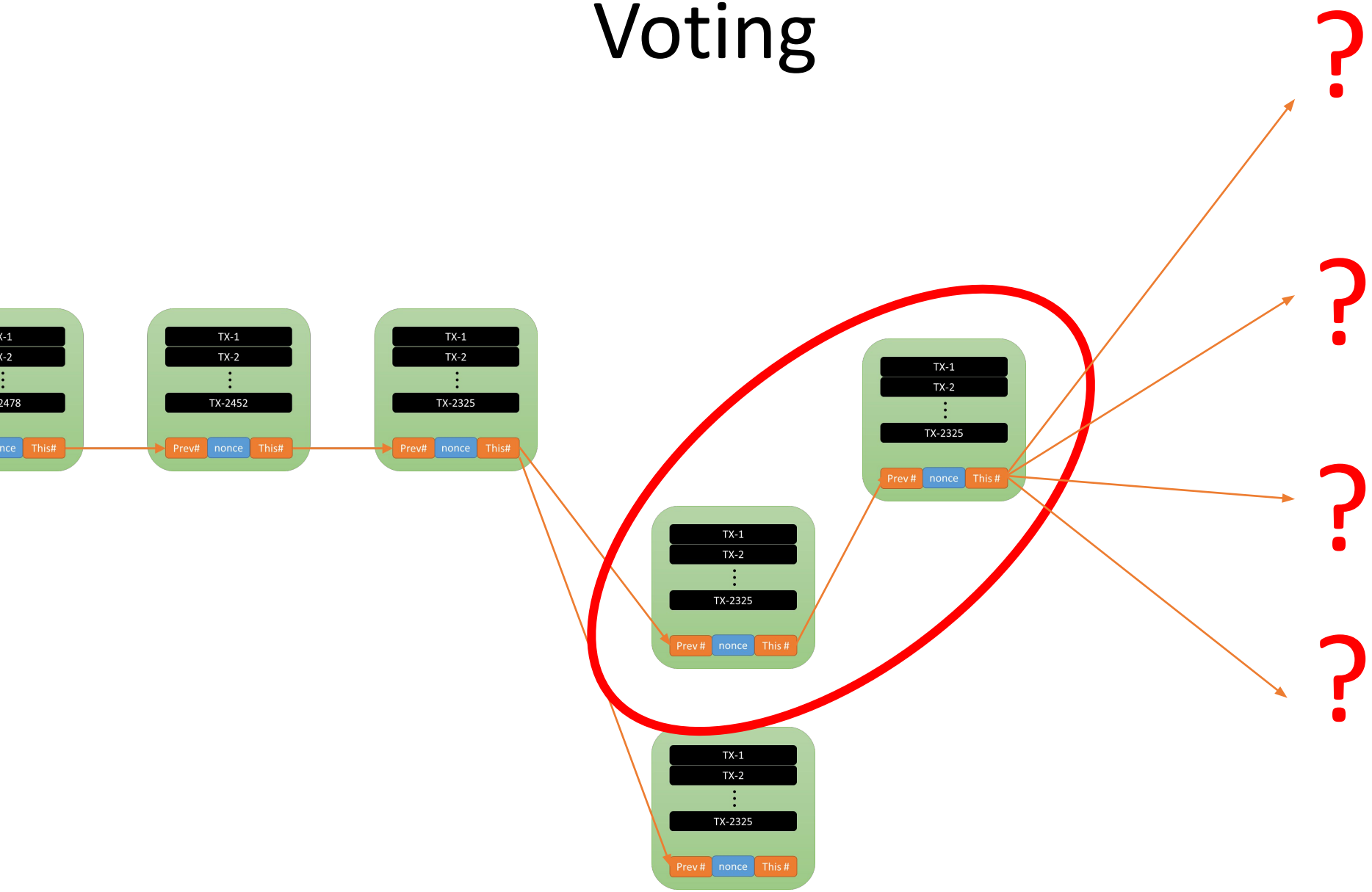
Voting


TX-1
TX-2
TX-2452
Prev#
nonce
This#
TX-1
TX-2
TX-2325
Prev#
nonce
This#
?
?
TX-1
TX-2
TX-2325
Prev #
This #
?
?

Voting


TX-1
TX-2
TX-2452
Prev#
nonce
This#
TX-1
TX-2
TX-2325
Prev#
nonce
This#
TX-1
TX-2
TX-2325
Prev #
nonce
This #
TX-1
TX-2
TX-2325
Prev #
nonce
This #
?
?
?
?
?
?
?
?

Voting



How Exactly… ?

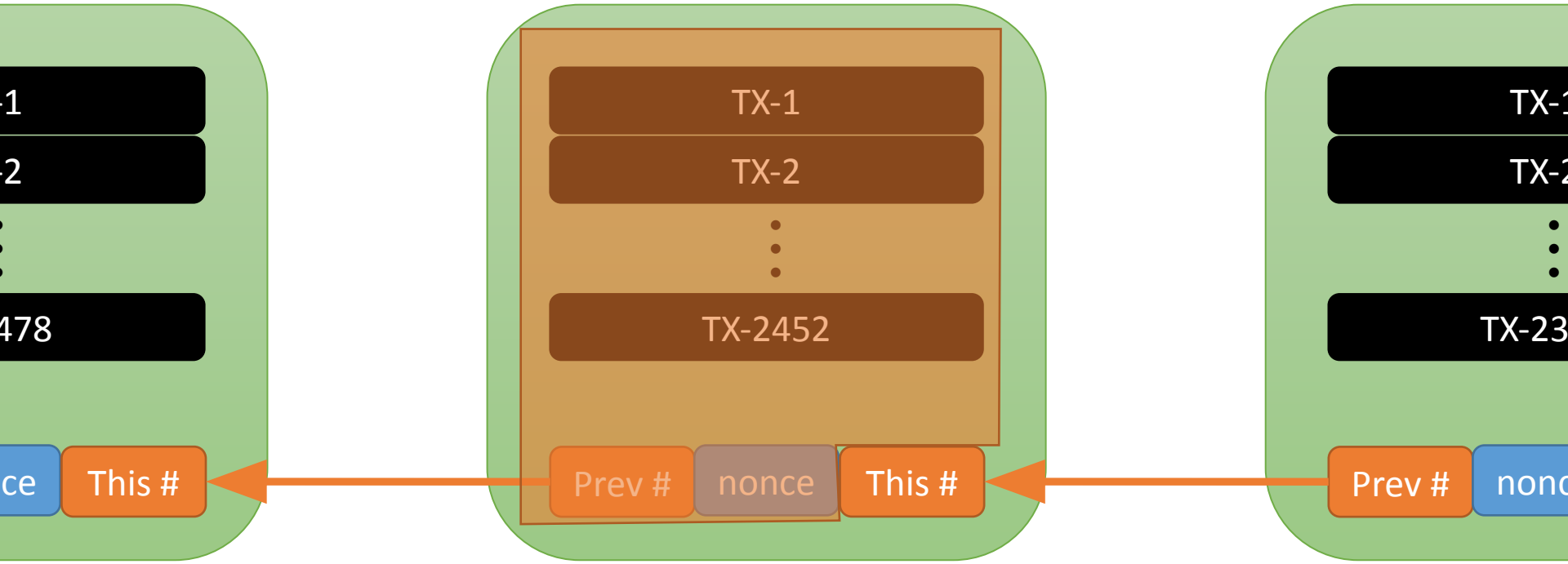
- Signing / Verifying → Unspent TX Output
- Chaining → Blocks, Hashes
- Voting → Prolonging the Chain
- Working → Mining

Hashing

data ⟶ number

Mining

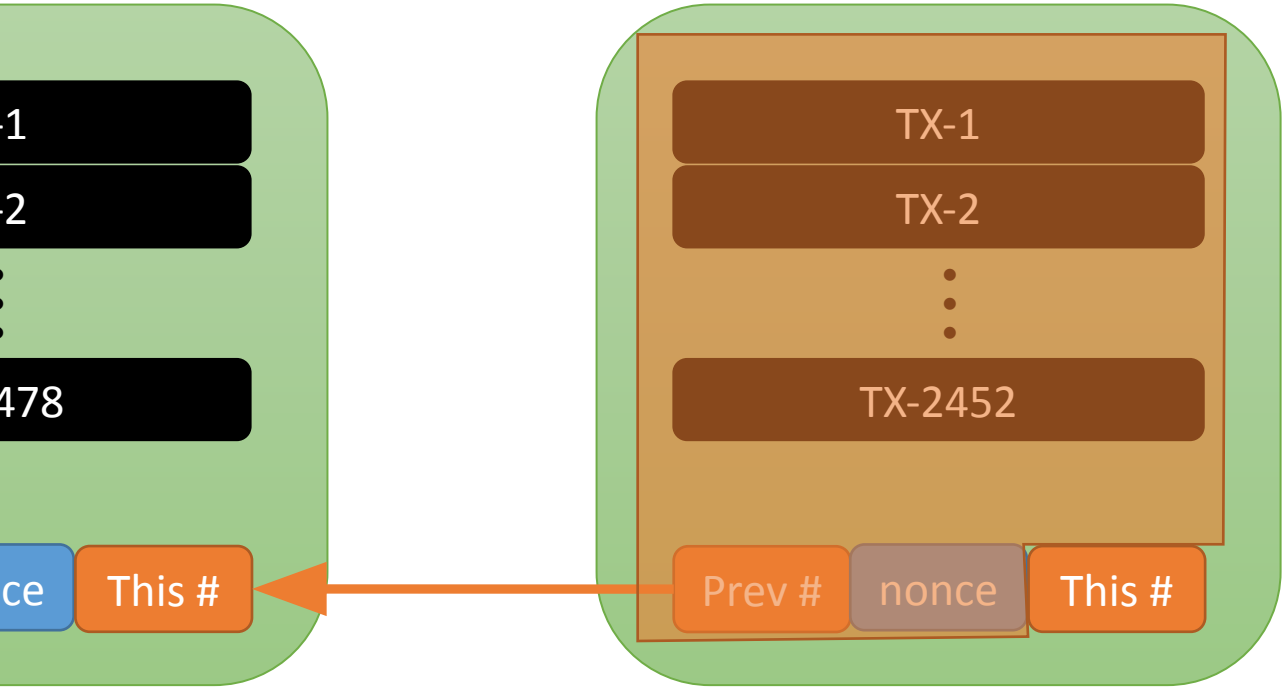
Bitcoin block



Mining: find nonce such that This # $< d$

Work is very hard… Why do it?

Mining (d = 1 000 000)

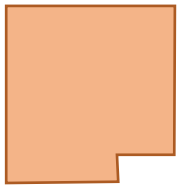


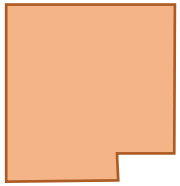
Try 1 : hash( ) = 24623523455124 > 1 000 000 ☹

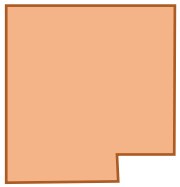
Try 2 : hash( ) = 833674799474 > 1 000 000

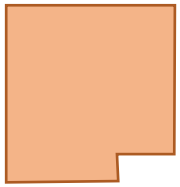
☹

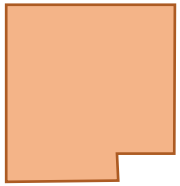
Mining (d = 1 000 000)

Try 3 : hash() = 24623523455124 > 1 000 000 ☹

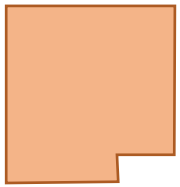
Try 4 : hash() = 833674799474 > 1 000 000 ☹

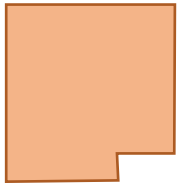
Try 5 : hash() = 6345680831 > 1 000 000 ☹

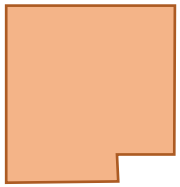
Try 6 : hash() = 90421799115 76 > 1 000 000 ☹

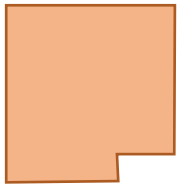
Try 7 : hash() = 77922698082 > 1 000 000 ☹

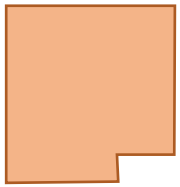
Mining (d = 1 000 000)

Try 8 : hash() = 24623523455124 > 1 000 000 ☹

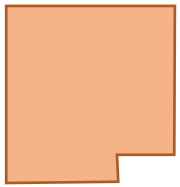
Try 9 : hash() = 833674799474 > 1 000 000 ☹

Try 10 : hash() = 6345680831 > 1 000 000 ☹

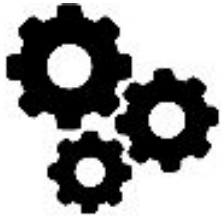
Try 11 : hash() = 90421799115 76 > 1 000 000 ☹

Try 12 : hash() = 77922698082 > 1 000 000 ☹

Mining (d = 1 000 000)

Try 13 : hash() = 5 < 1 000 000 ☺️

Hooray!!!

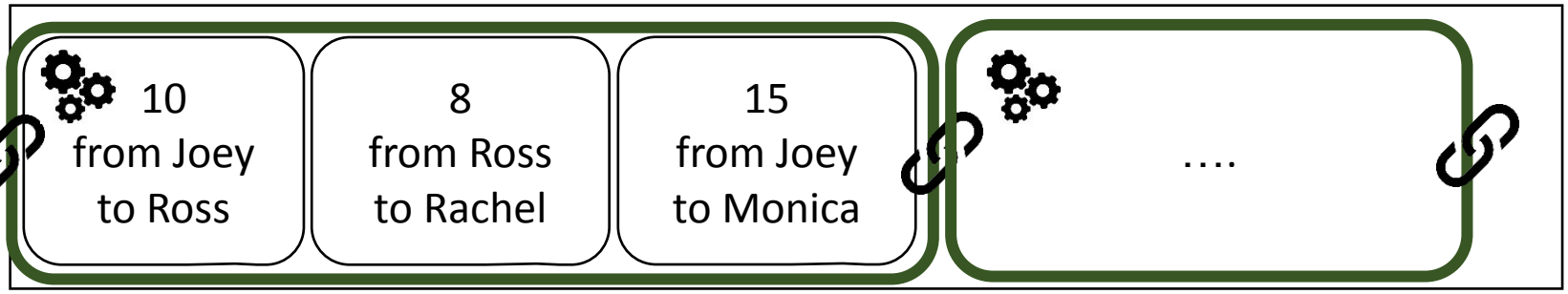
13 ☐ Proof of Work 

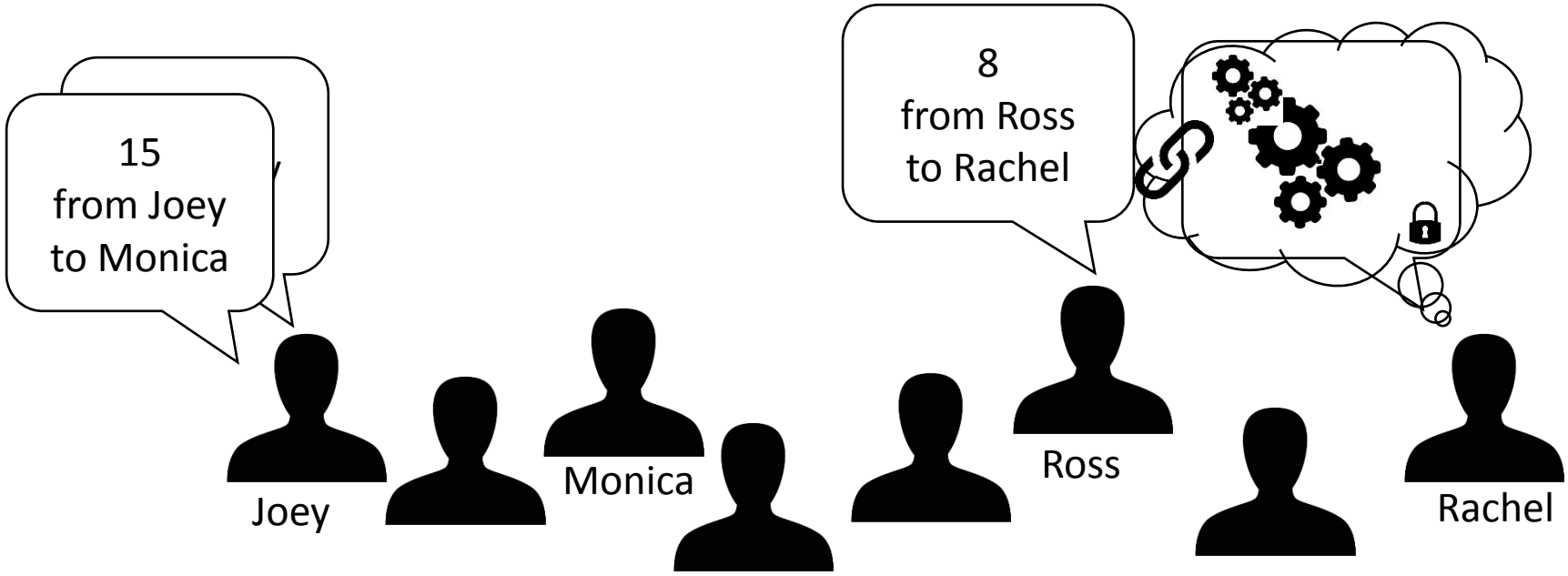
How Exactly… ?

- Signing / Verifying → Unspent TX Output
- Chaining → Blocks, Hashes
- Voting → Prolonging the Chain
- Working → Mining
- Rewards → New coins, TX fees

Blocks

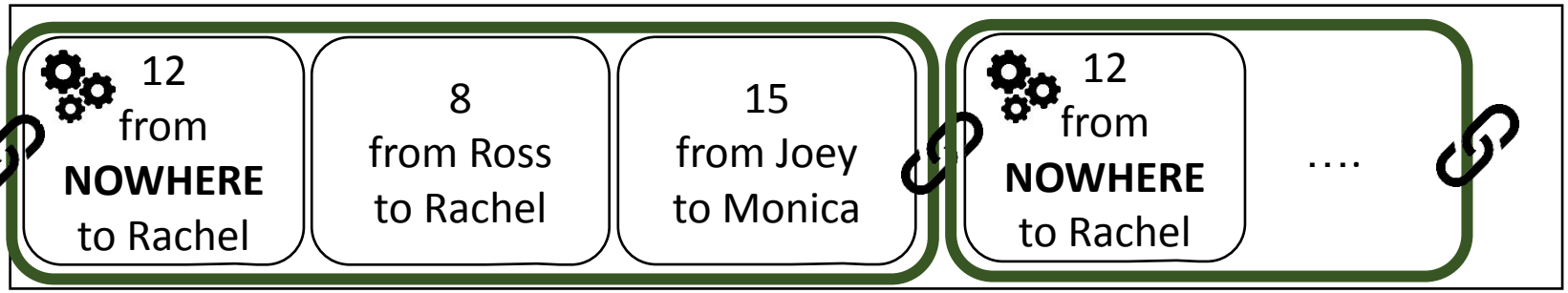
Ledger:

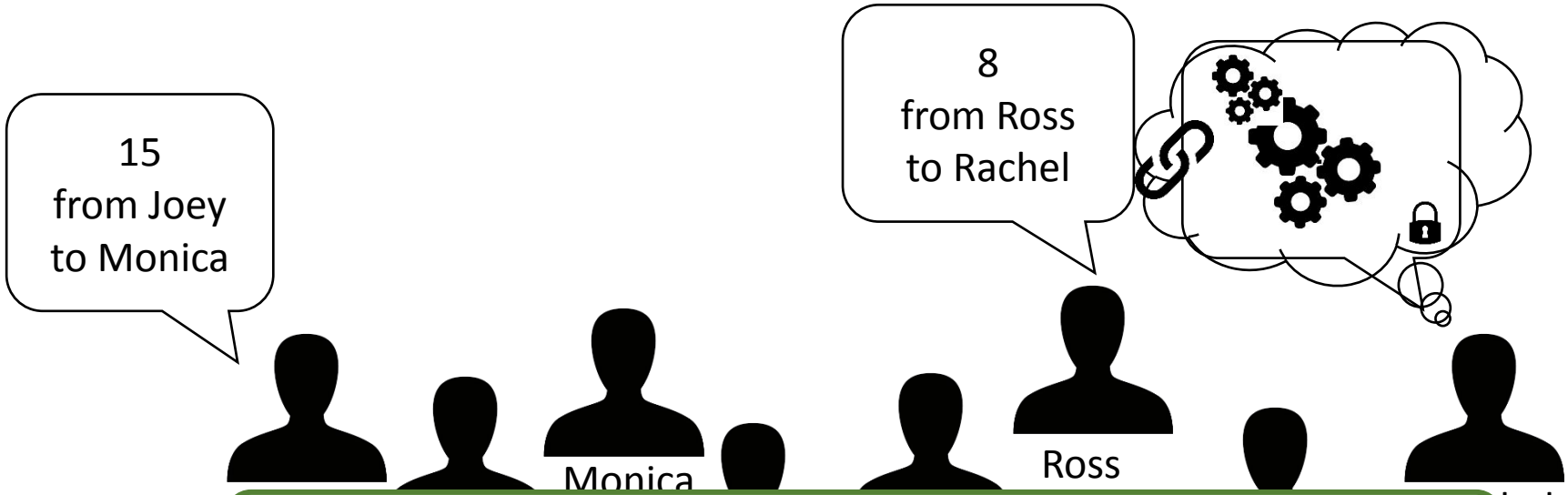




Rewards (1)

Ledger:





Special transaction: “Coinbase”

Rewards (2)

Simply:

10
from Joey
to Ross

But actually…

TX 123:

6 received from Rachel in TX 345
8 Received from Monica in TX 678
10 to Ross
4 to Joey

ACTUALLY...

TX 123:

6 received from Rachel in TX 345
8 Received from Monica in TX 678
10 to Ross
3 to Joey
1 to whomever finds the PoW

Transaction fee

Recap

- Signing / Verifying → Unspent TX Output
- Chaining → Blocks, Hashes
- Voting → Prolonging the Chain
- Working → Mining
- Rewards → New coins, TX fees

Many different systems implement different variants of these concepts.