

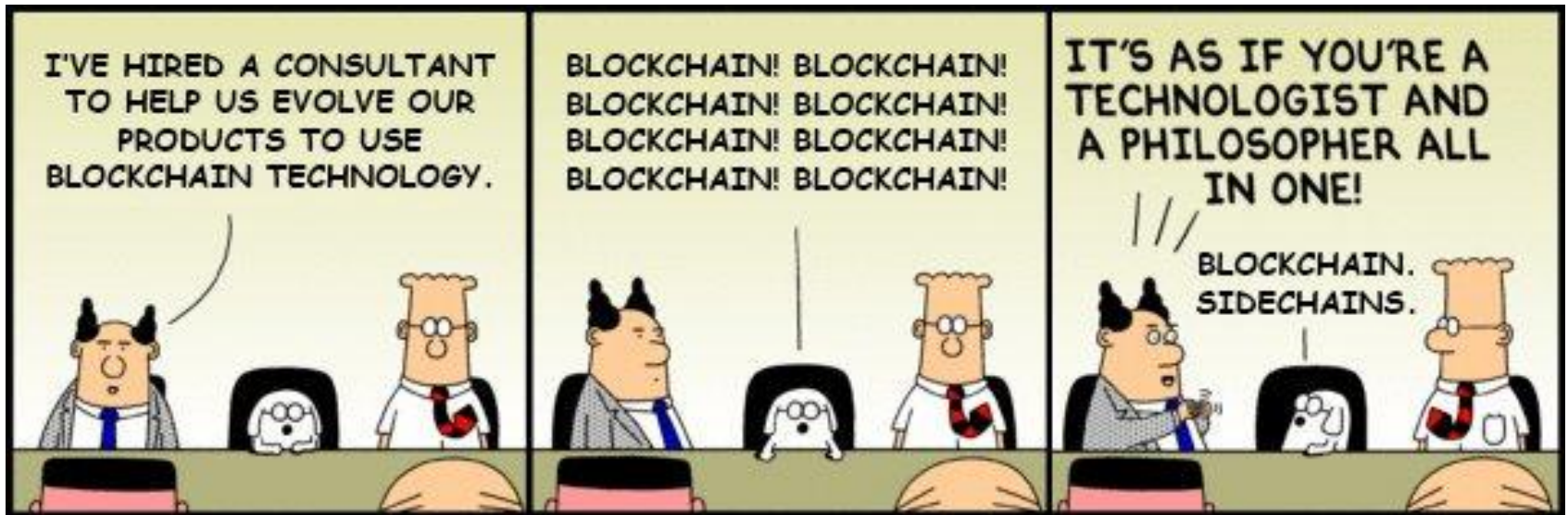
Proof-of-Work Blockchain Systems

Matej Pavlovic

(preliminary version)

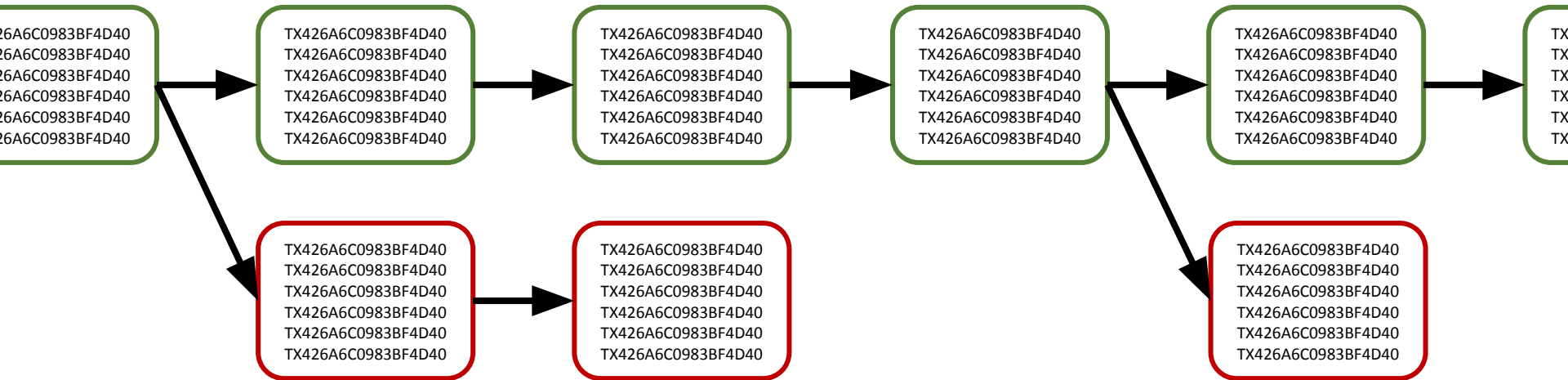
Distributed Algorithms

December 16th, 2024, EPFL, Lausanne, Switzerland



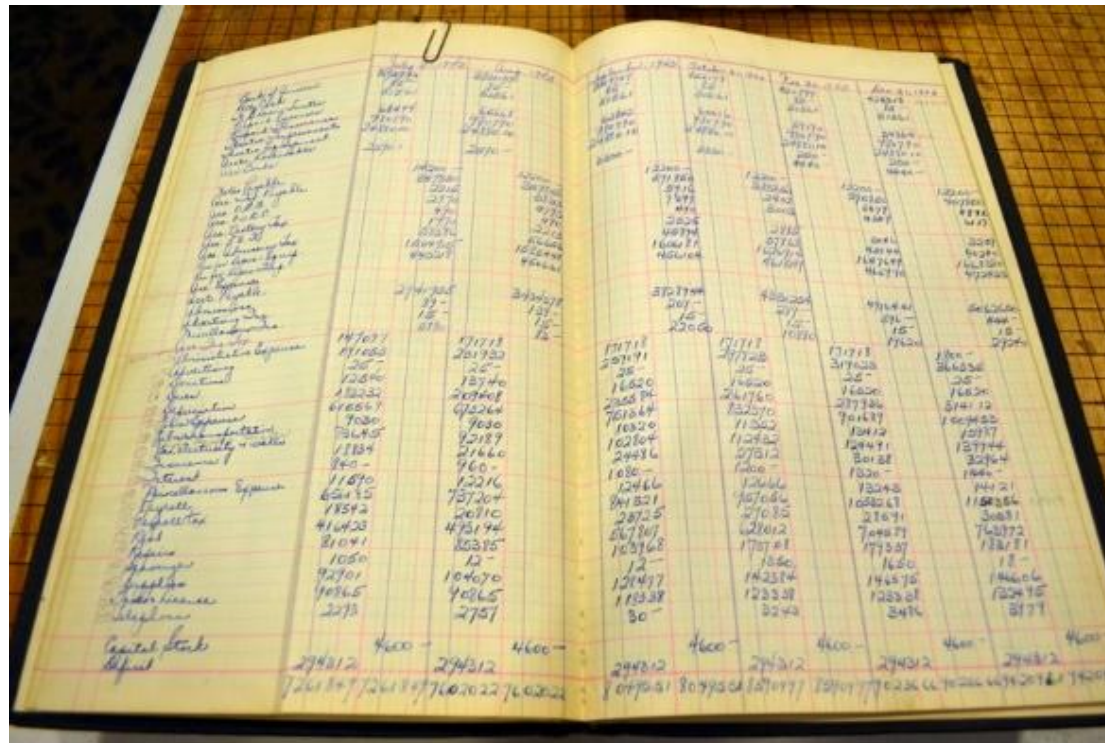
(Dilbert Cartoon by Scott Adams)

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.

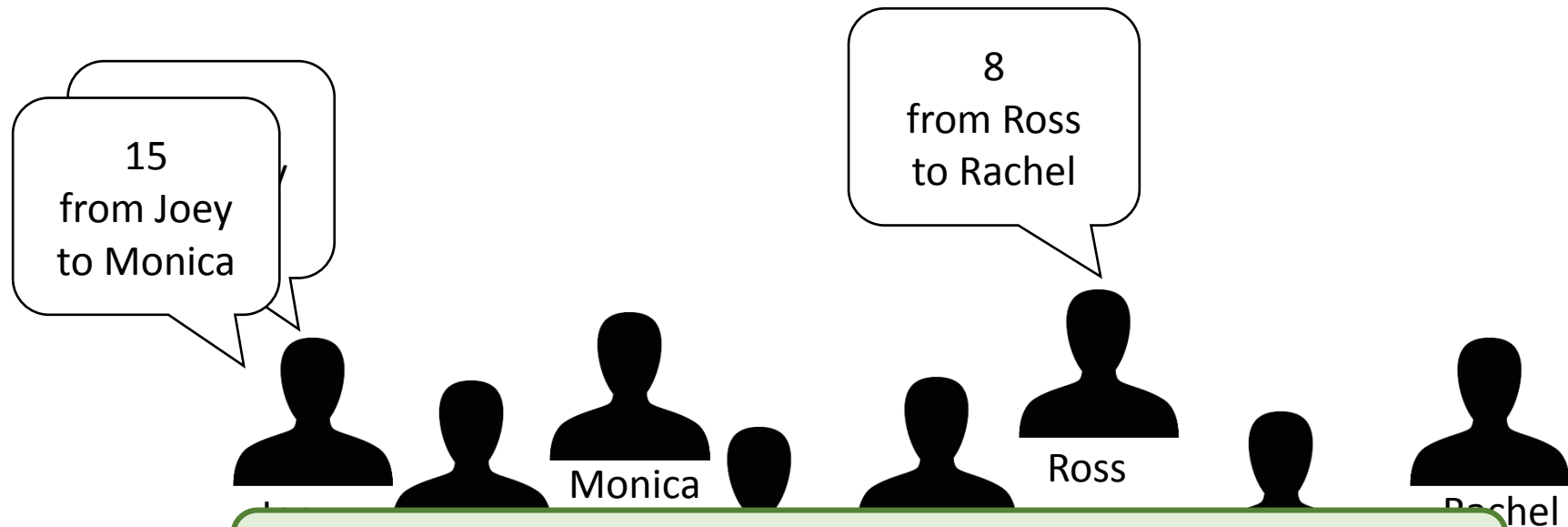
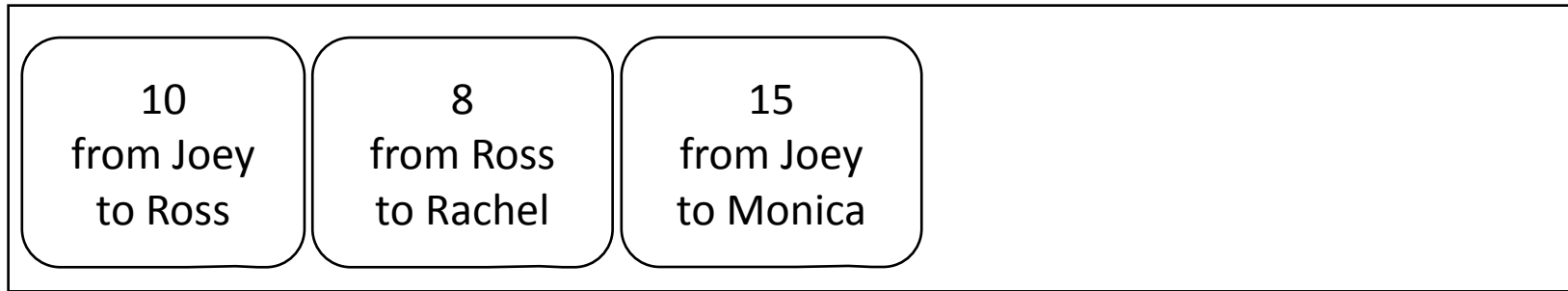
Ledger



Ordered sequence of operations

Money as a Computer Program

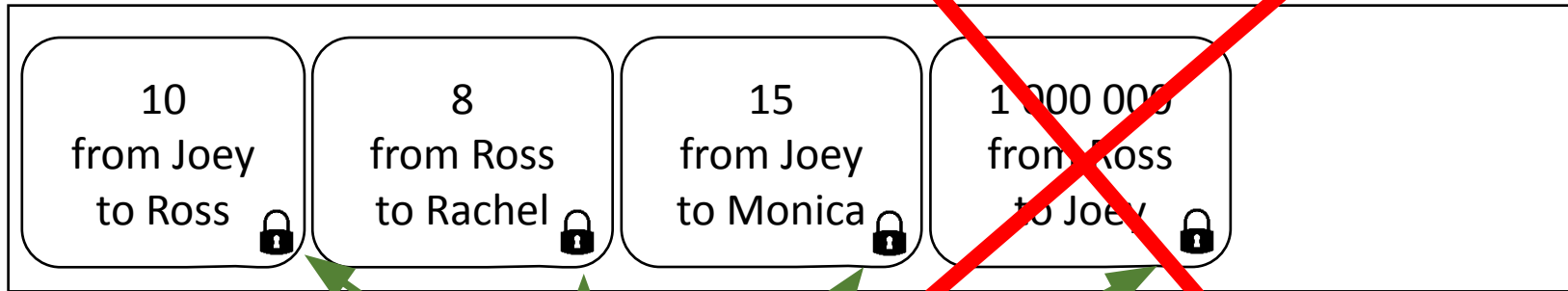
Ledger:



Problems ? (Hint: there are plenty)

Problem: Impersonation

Ledger:



Add digital
signatures

Invalid
signature!

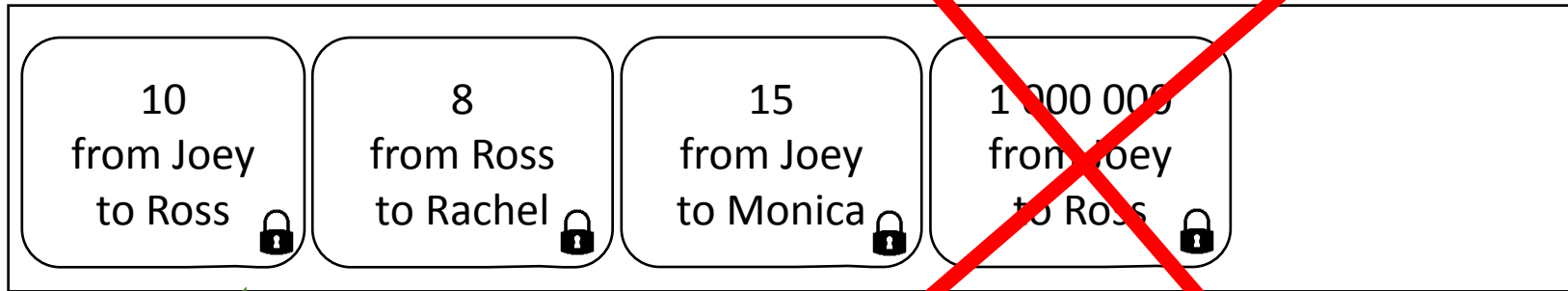
1 000 000
from Ross
to Joey



Solution: Signatures

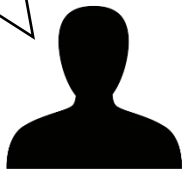
Problem: Not Enough Money

Ledger:



Verify history

1 000 000
from Joey
to Ross



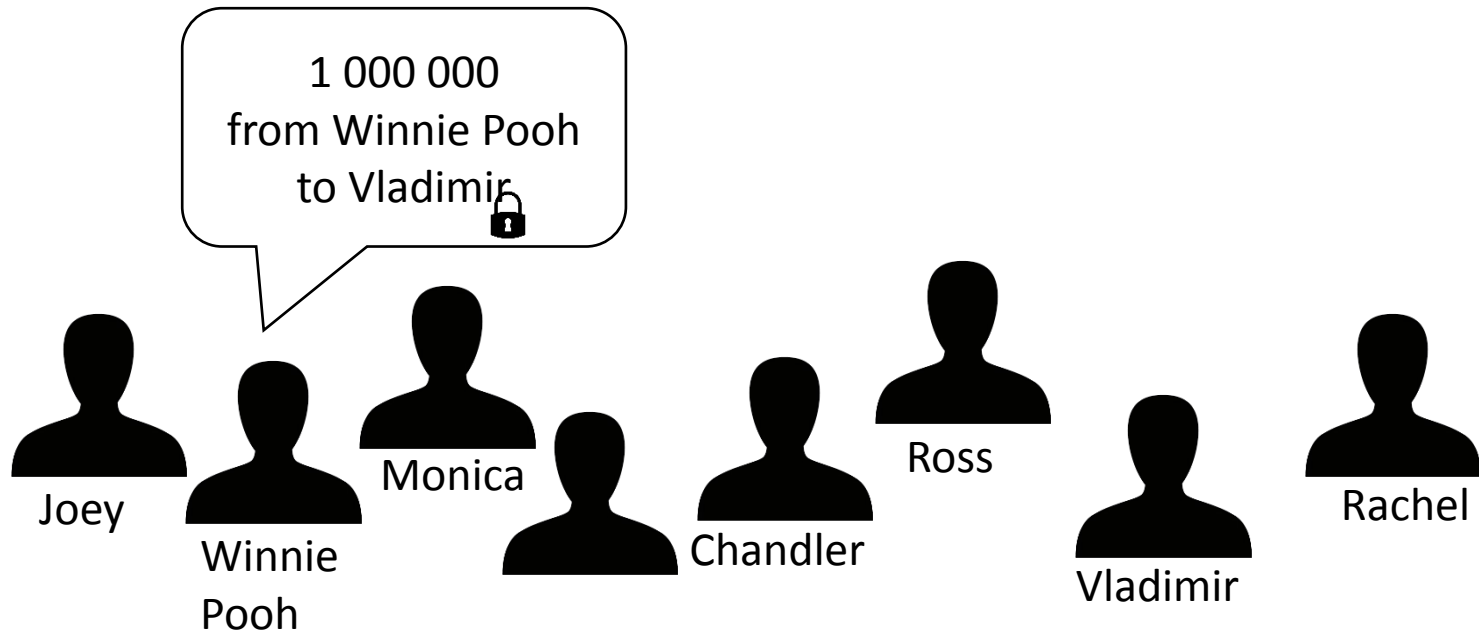
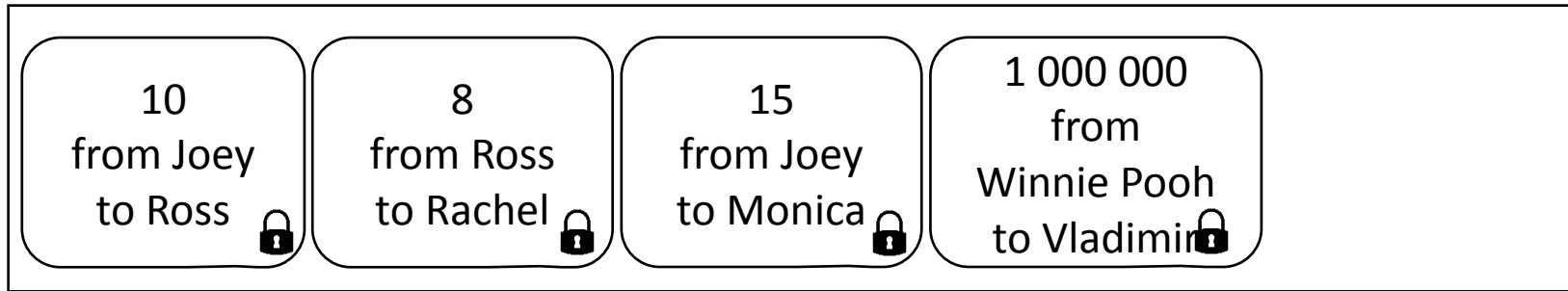
Solution: Verify history

Recap

- Signing / Verifying

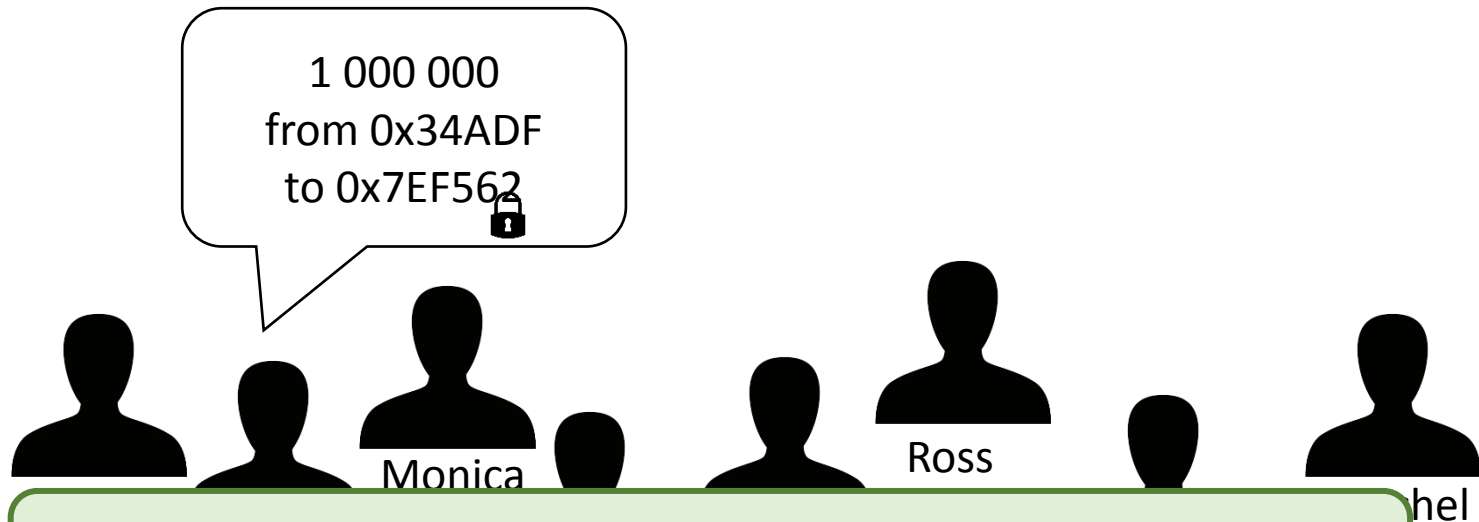
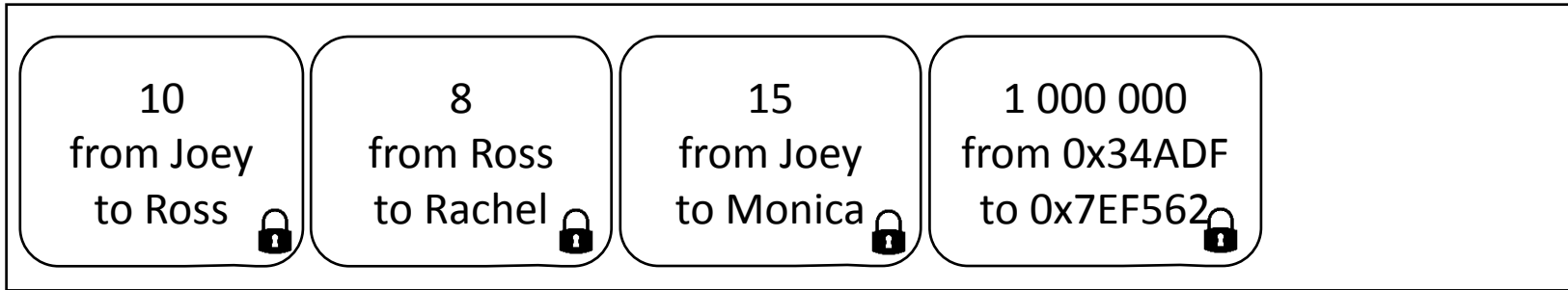
Problem: Anonymity?

Ledger:



Problem: Anonymity?

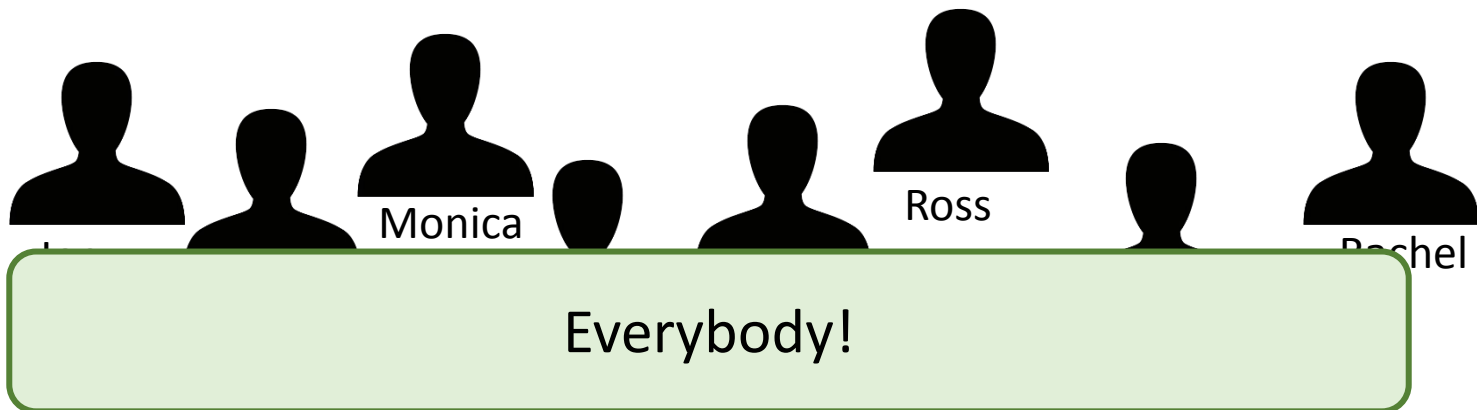
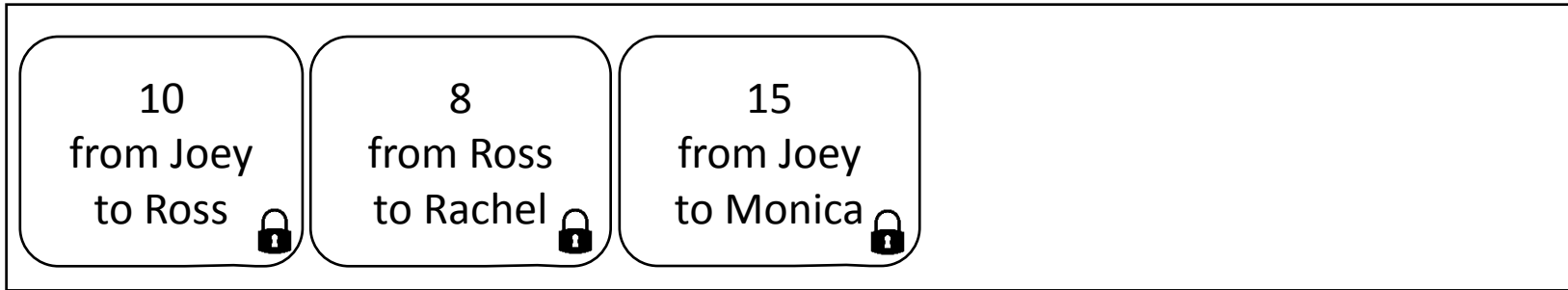
Ledger:



No need to disclose identity. Public key sufficient.

Problem: Who Stores the Ledger?

Ledger:



Problem: Who Stores the Ledger?

Joey's copy:



Joey

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

Monica's copy:



Monica

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

Ross's copy:



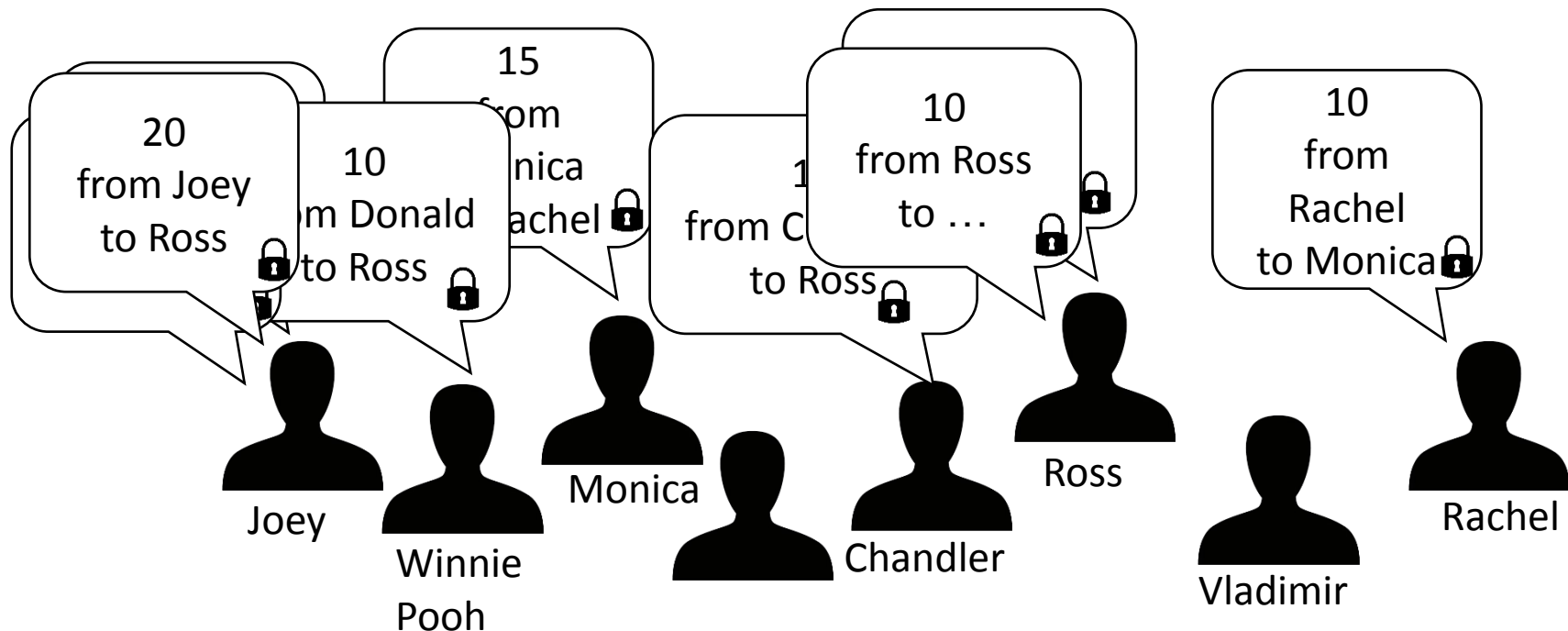
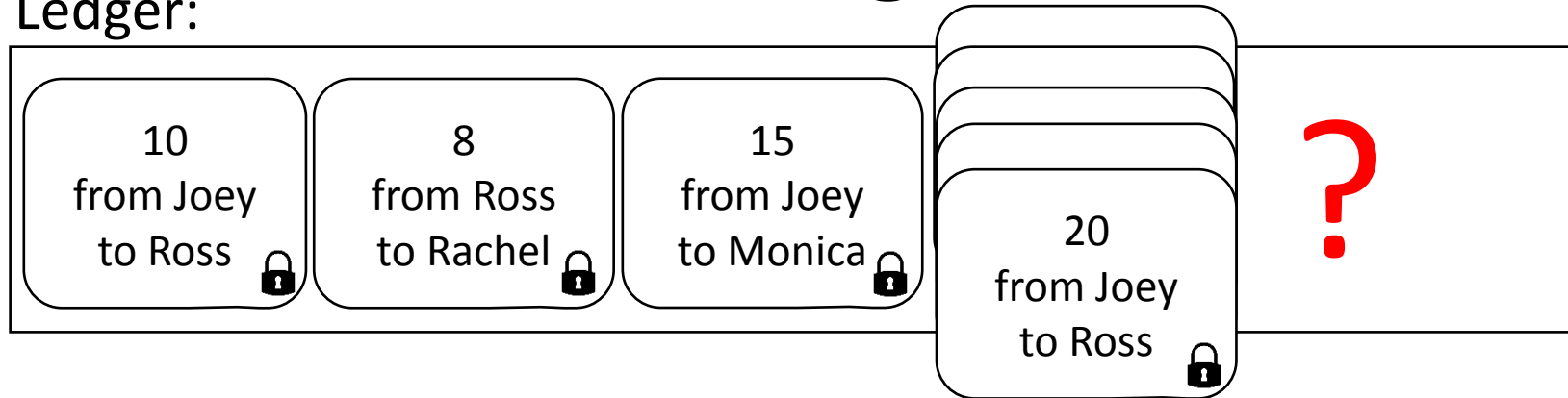
Ros

10	8	15
----	---	----

Problem? (Hint: already discussed.)

Problem: Agreement

Ledger:

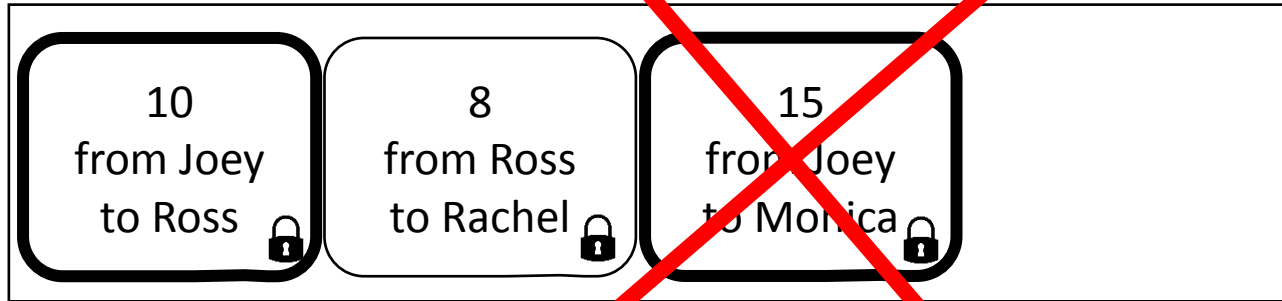


Problem: Agreement

Joey's copy:



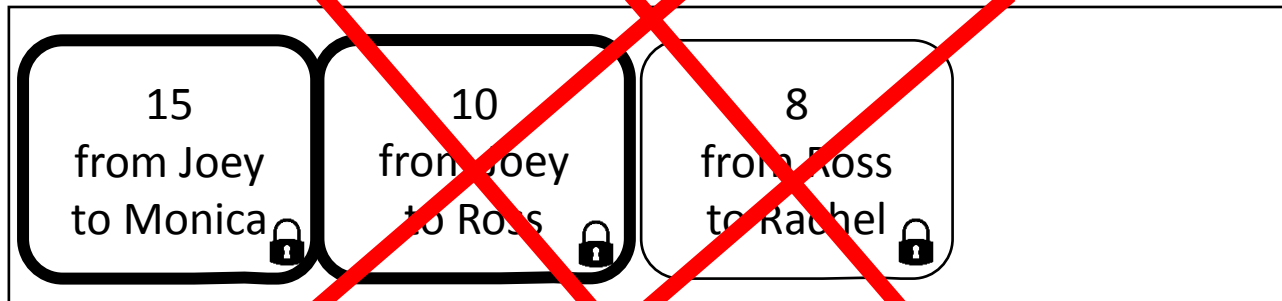
Joey



Monica's copy:



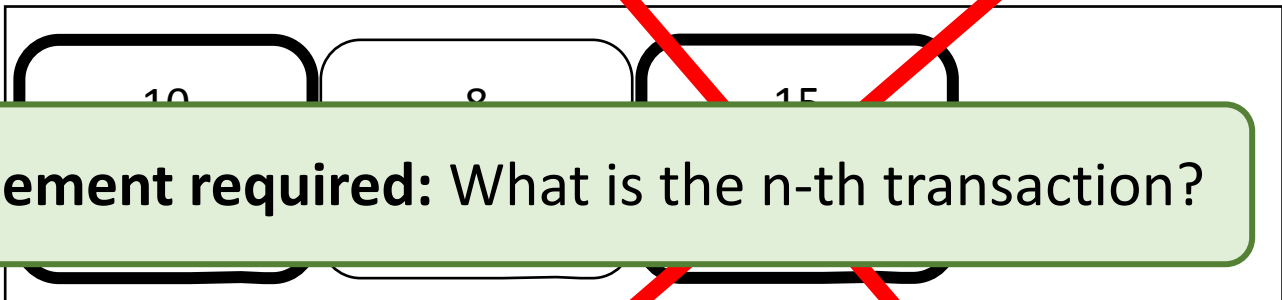
Monica



Ross's copy:



Ross



Agreement required: What is the n-th transaction?

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

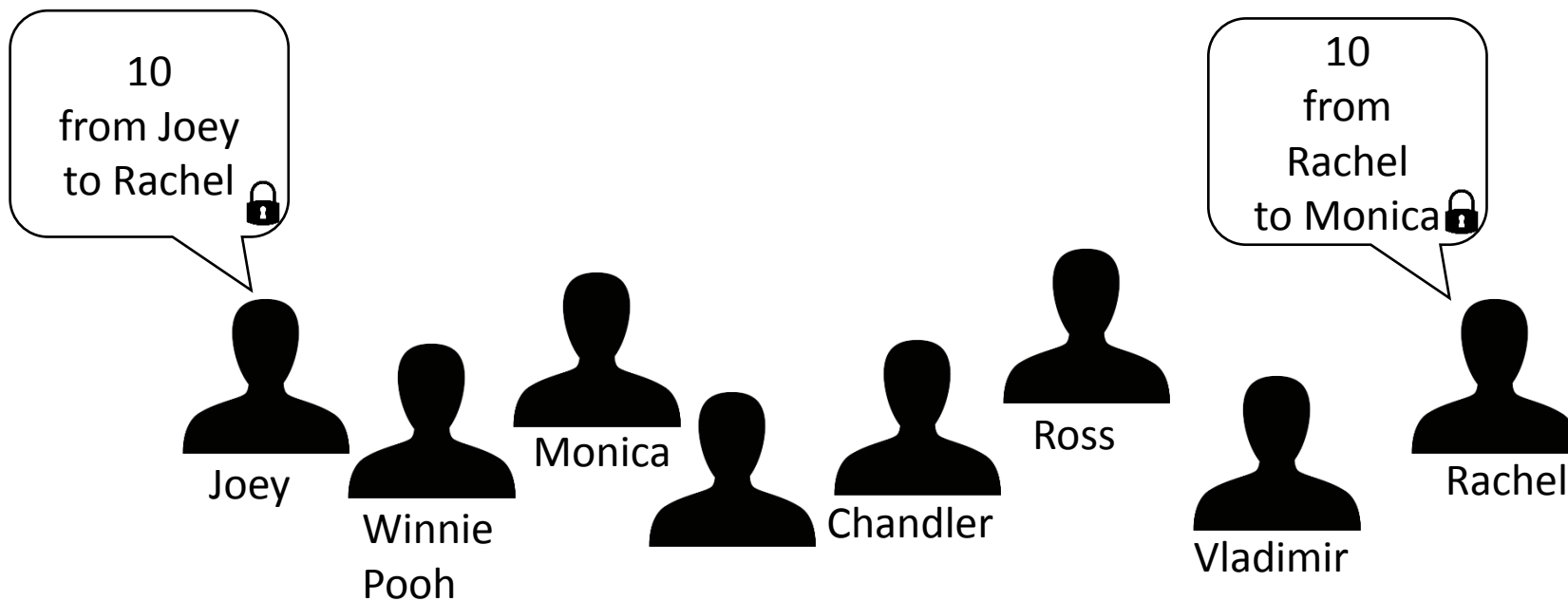
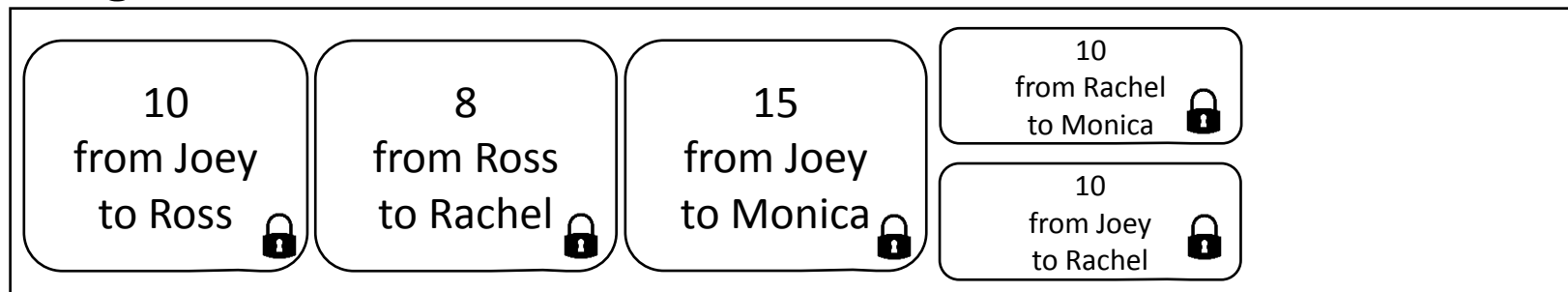
How Do We Solve Agreement?

?

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

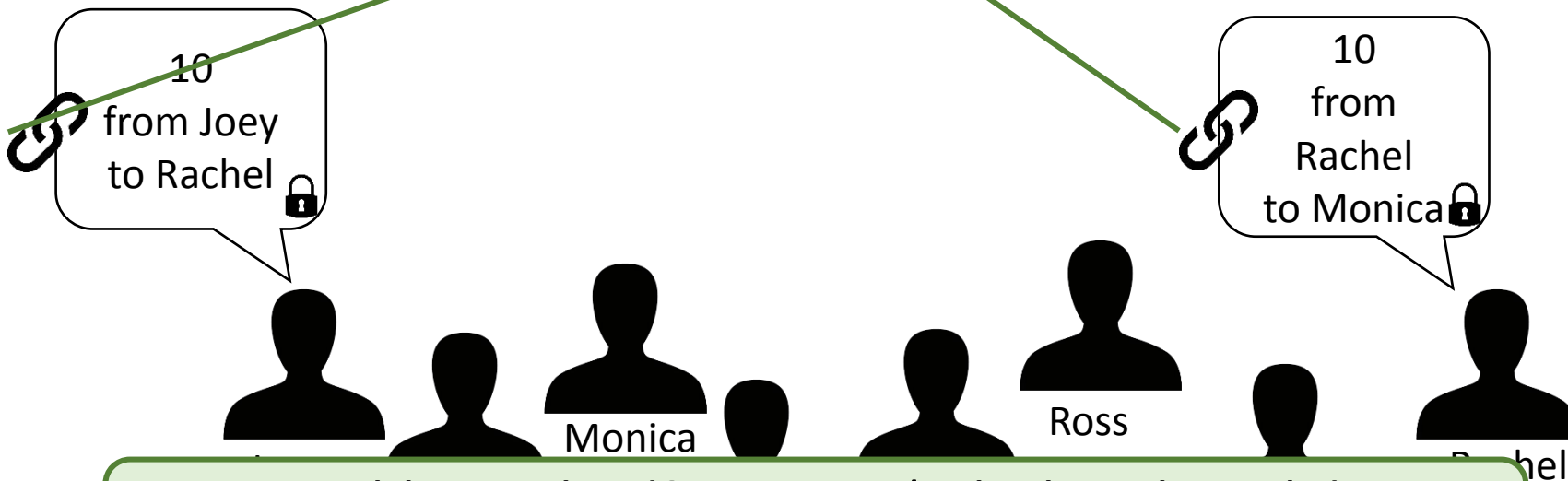
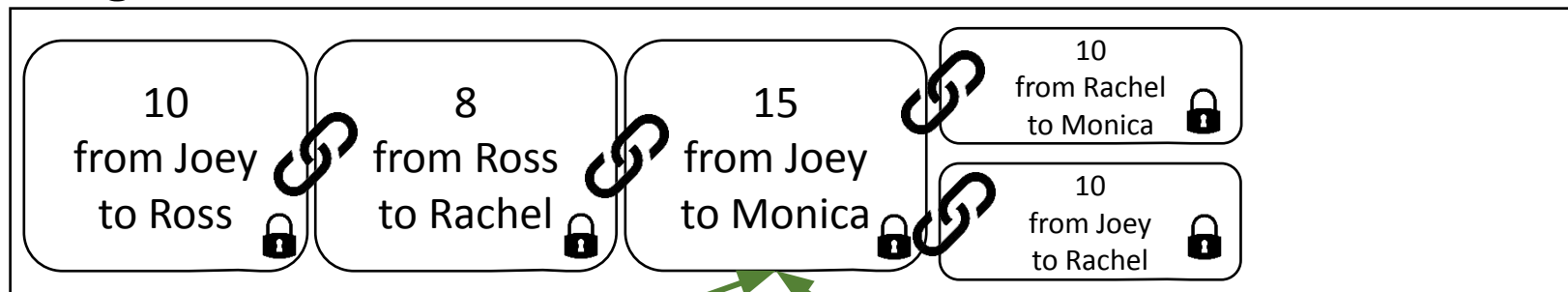
Chaining

Ledger:



Chaining

Ledger:

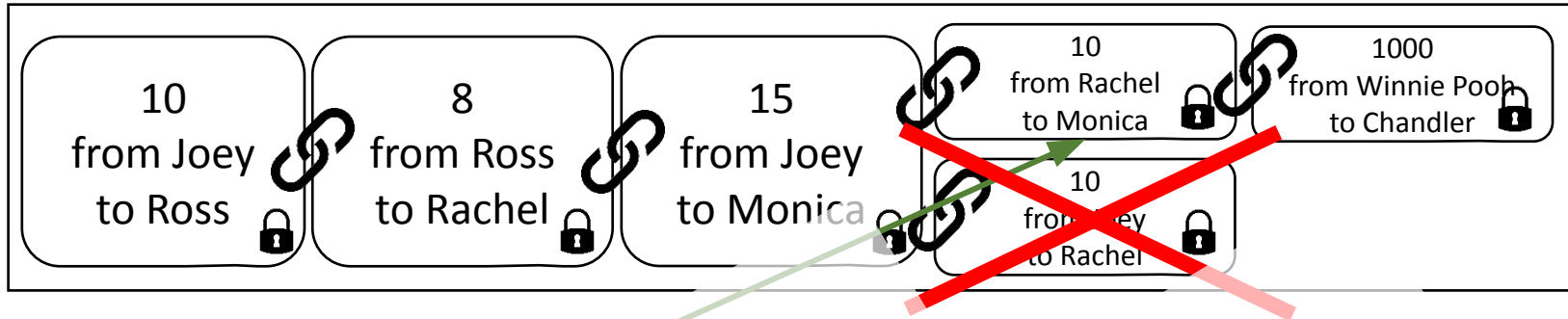


Recap

- Signing / Verifying
- Chaining

Voting

Ledger:

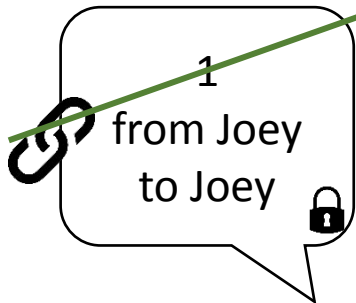
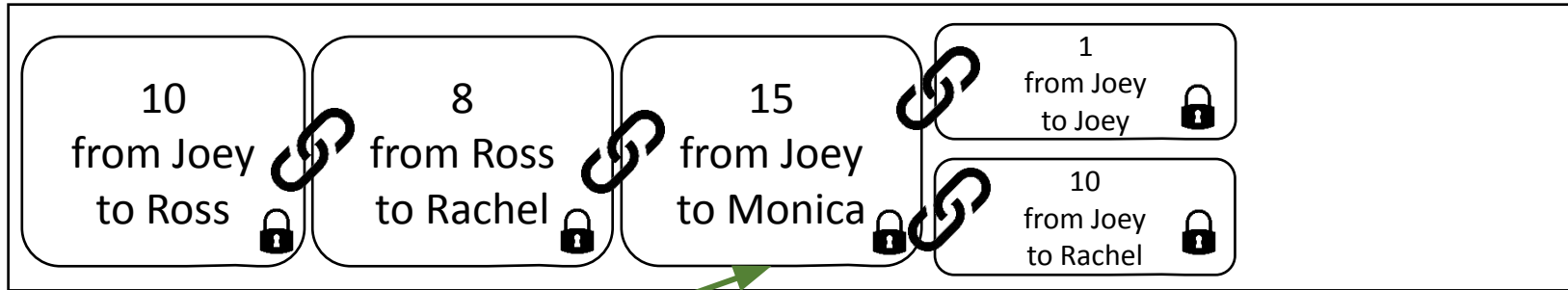


Longest chain is valid (by definition).

OOPS!
BIG PROBLEM...

Cheating

Ledger:



Joey



Winnie
Pooh



Monica



Chandler



Ross



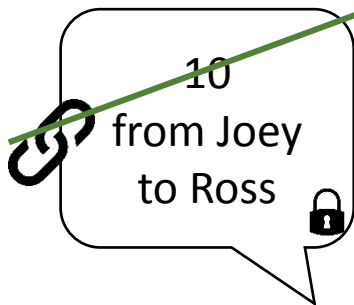
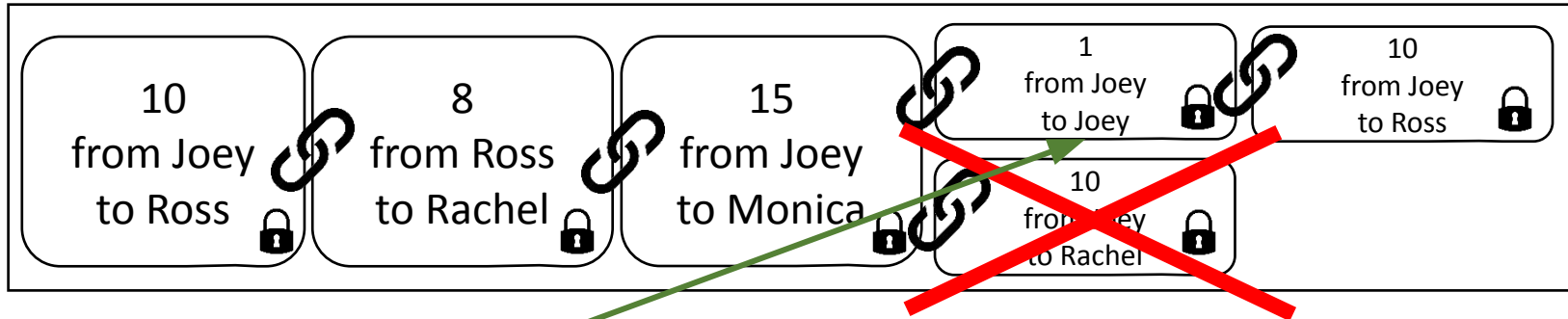
Vladimir



Rachel

Cheating

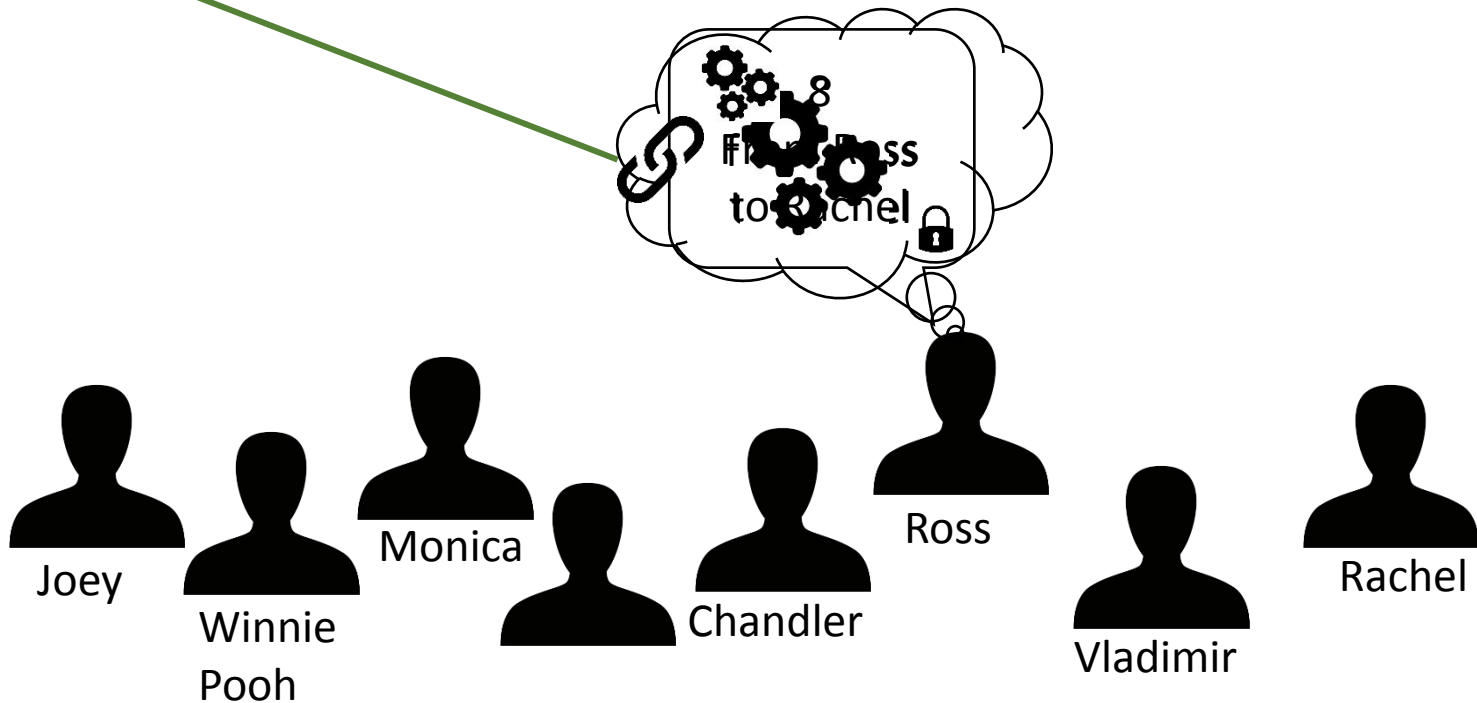
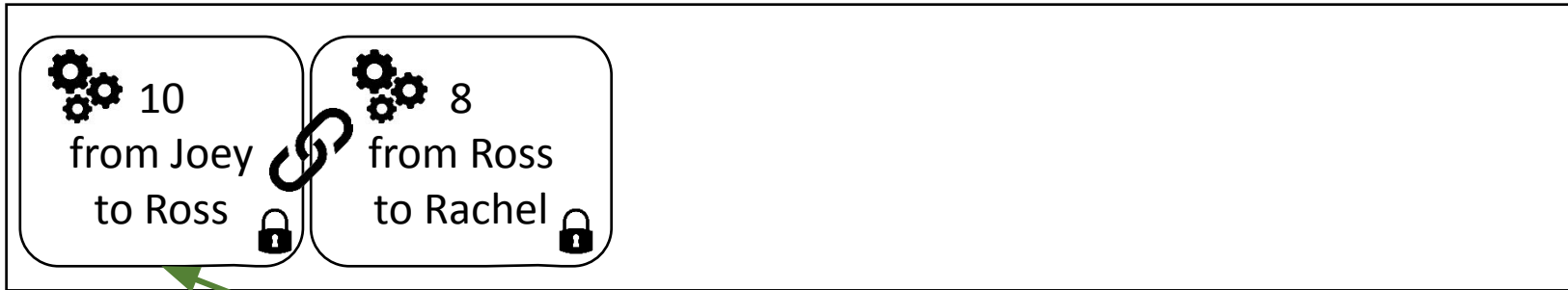
Ledger:



Double Spending!

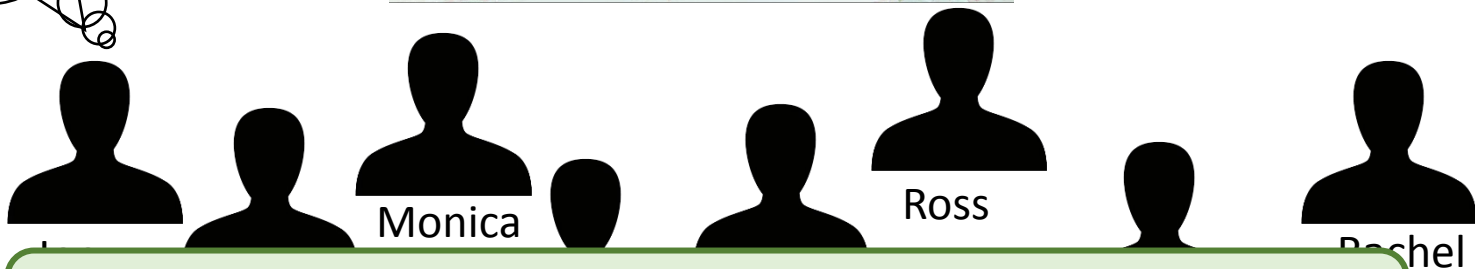
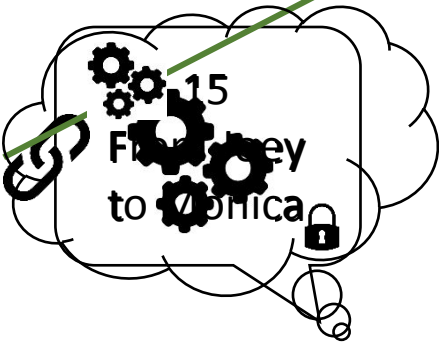
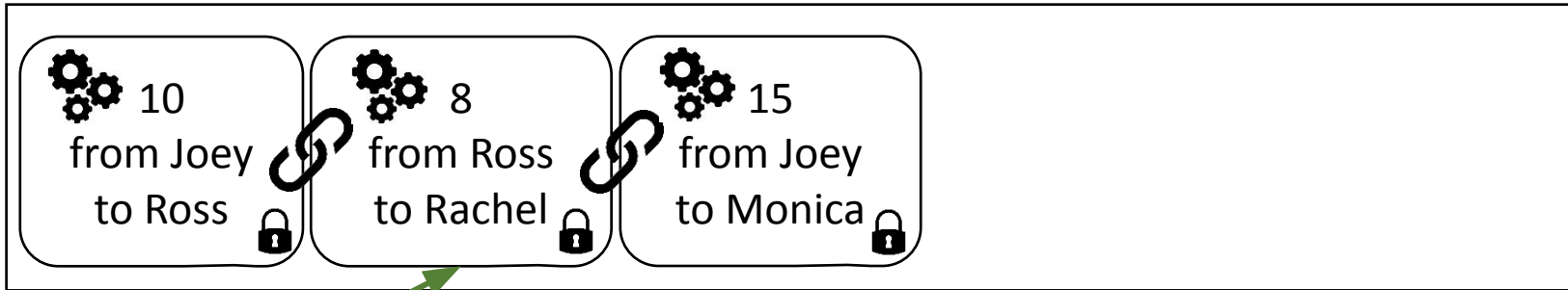
Working

Ledger:



Working

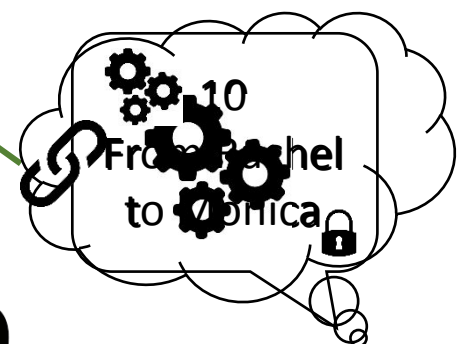
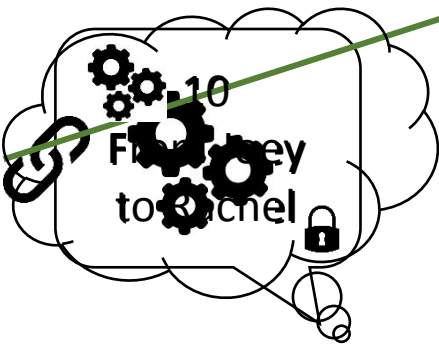
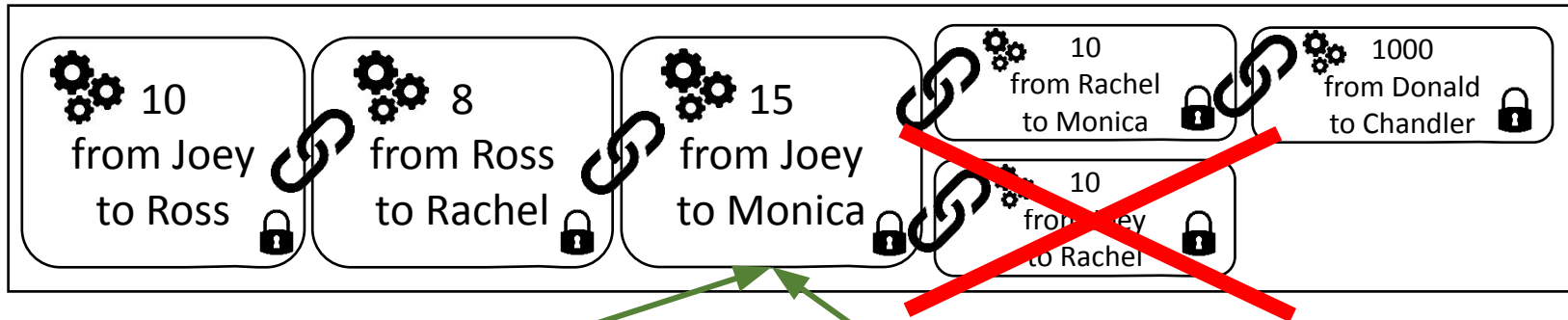
Ledger:



Work is very hard

Working

Ledger:



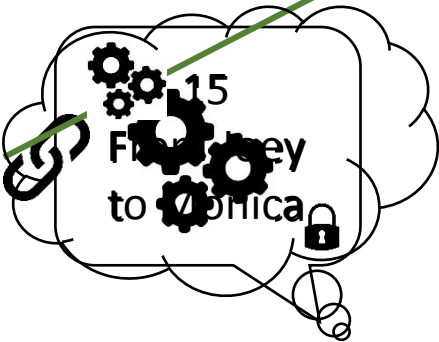
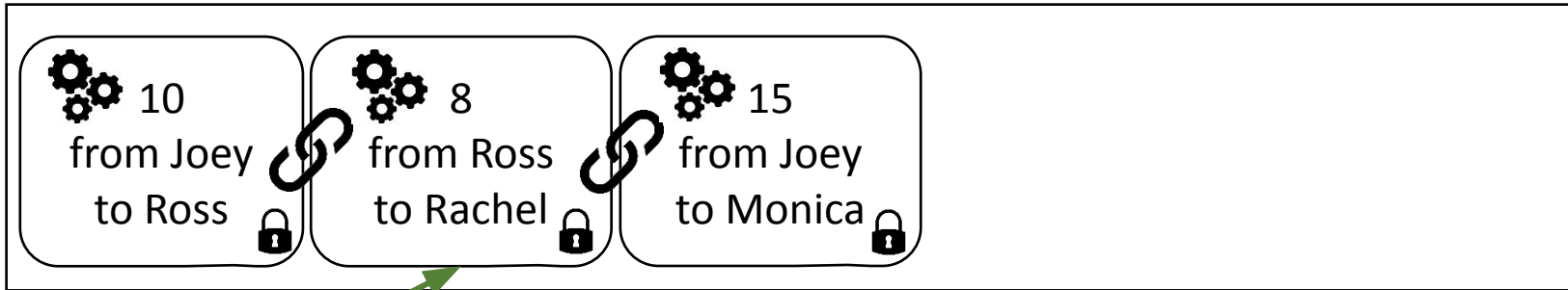
FORK. Happens rarely. (When...?)

Recap

- Signing / Verifying
- Chaining
- Voting
- Working

Working

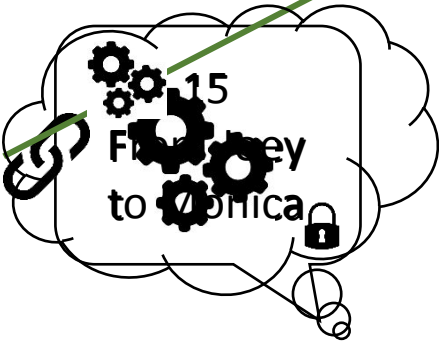
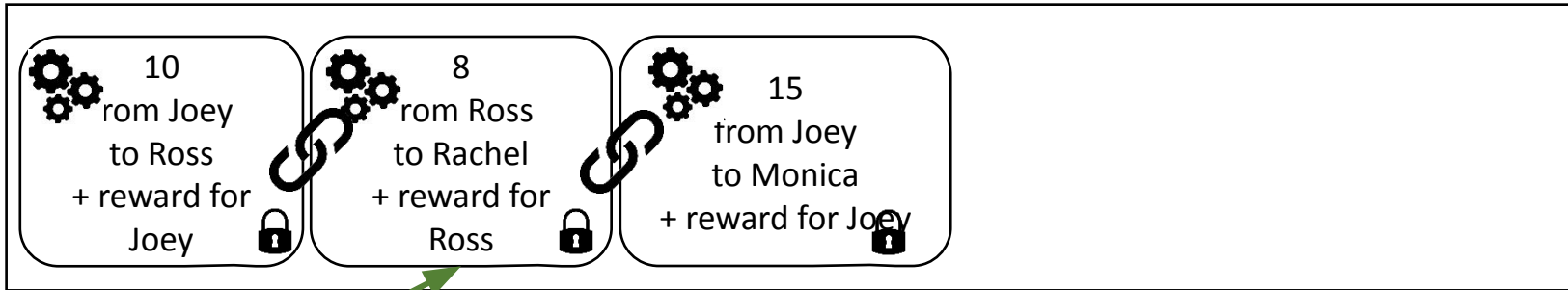
Ledger:



Work is very hard... Why do it?

Rewards

Ledger:



Recap

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

Proof-of-Work Blockchain!!!

Summary

- “Blockchain” started with a payment application
 - Bitcoin not practically useful for everyday payments today, but is a storage of value
- Nowadays blockchain systems can implement any service
 - Distributedly
 - Without a trusted party