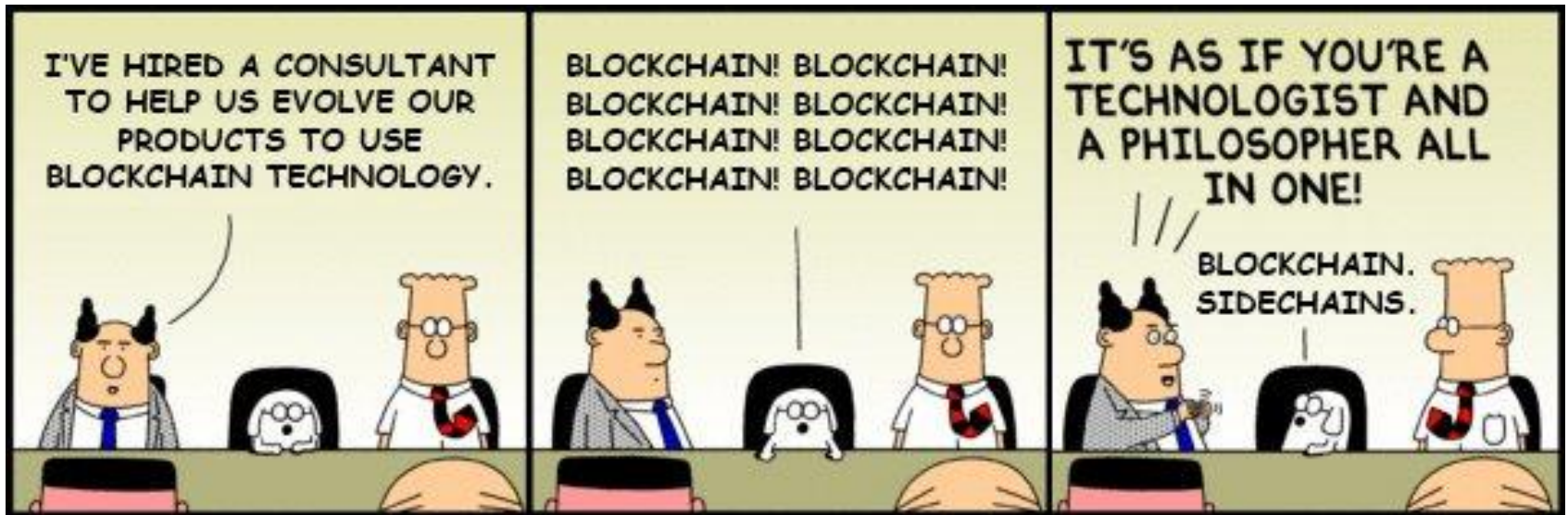


Proof-of-Work Blockchain Systems

Matej Pavlovic

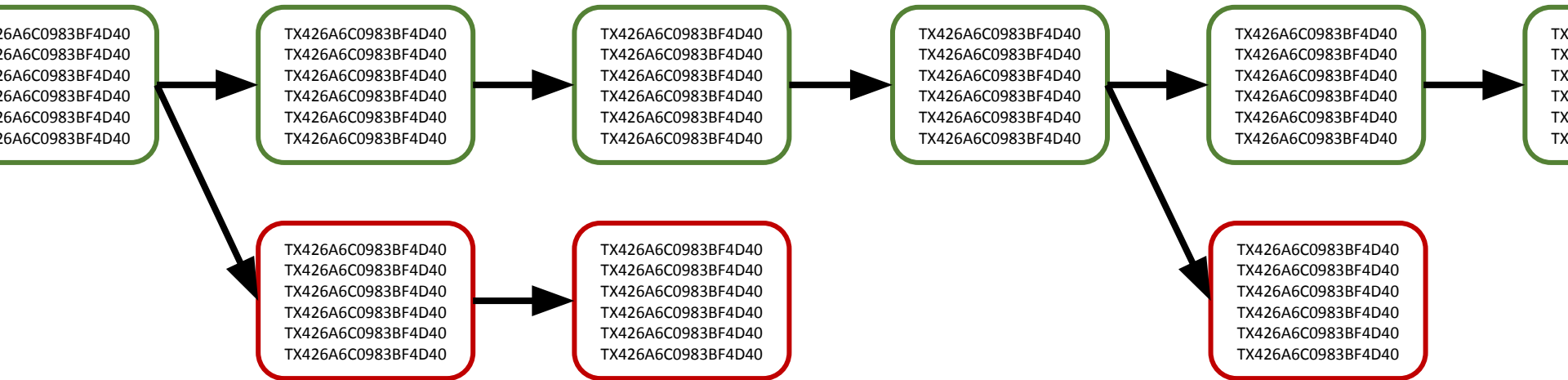
Distributed Algorithms

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

The image shows an open ledger book with two pages of handwritten accounting entries. The entries are organized into columns, with the left page containing a list of transactions and their corresponding debits and credits. The right page shows a similar list of transactions, with a final total of 4600. The ledger is titled 'Ledger' and is placed on a grid-patterned surface.

Transaction	Debit	Credit
Jan 1 Cash		4600
Jan 2 Cash		100
Jan 3 Cash		200
Jan 4 Cash		300
Jan 5 Cash		400
Jan 6 Cash		500
Jan 7 Cash		600
Jan 8 Cash		700
Jan 9 Cash		800
Jan 10 Cash		900
Jan 11 Cash		1000
Jan 12 Cash		1100
Jan 13 Cash		1200
Jan 14 Cash		1300
Jan 15 Cash		1400
Jan 16 Cash		1500
Jan 17 Cash		1600
Jan 18 Cash		1700
Jan 19 Cash		1800
Jan 20 Cash		1900
Jan 21 Cash		2000
Jan 22 Cash		2100
Jan 23 Cash		2200
Jan 24 Cash		2300
Jan 25 Cash		2400
Jan 26 Cash		2500
Jan 27 Cash		2600
Jan 28 Cash		2700
Jan 29 Cash		2800
Jan 30 Cash		2900
Jan 31 Cash		3000
Jan 32 Cash		3100
Jan 33 Cash		3200
Jan 34 Cash		3300
Jan 35 Cash		3400
Jan 36 Cash		3500
Jan 37 Cash		3600
Jan 38 Cash		3700
Jan 39 Cash		3800
Jan 40 Cash		3900
Jan 41 Cash		4000
Jan 42 Cash		4100
Jan 43 Cash		4200
Jan 44 Cash		4300
Jan 45 Cash		4400
Jan 46 Cash		4500
Jan 47 Cash		4600
Jan 48 Cash		4700
Jan 49 Cash		4800
Jan 50 Cash		4900
Jan 51 Cash		5000
Jan 52 Cash		5100
Jan 53 Cash		5200
Jan 54 Cash		5300
Jan 55 Cash		5400
Jan 56 Cash		5500
Jan 57 Cash		5600
Jan 58 Cash		5700
Jan 59 Cash		5800
Jan 60 Cash		5900
Jan 61 Cash		6000
Jan 62 Cash		6100
Jan 63 Cash		6200
Jan 64 Cash		6300
Jan 65 Cash		6400
Jan 66 Cash		6500
Jan 67 Cash		6600
Jan 68 Cash		6700
Jan 69 Cash		6800
Jan 70 Cash		6900
Jan 71 Cash		7000
Jan 72 Cash		7100
Jan 73 Cash		7200
Jan 74 Cash		7300
Jan 75 Cash		7400
Jan 76 Cash		7500
Jan 77 Cash		7600
Jan 78 Cash		7700
Jan 79 Cash		7800
Jan 80 Cash		7900
Jan 81 Cash		8000
Jan 82 Cash		8100
Jan 83 Cash		8200
Jan 84 Cash		8300
Jan 85 Cash		8400
Jan 86 Cash		8500
Jan 87 Cash		8600
Jan 88 Cash		8700
Jan 89 Cash		8800
Jan 90 Cash		8900
Jan 91 Cash		9000
Jan 92 Cash		9100
Jan 93 Cash		9200
Jan 94 Cash		9300
Jan 95 Cash		9400
Jan 96 Cash		9500
Jan 97 Cash		9600
Jan 98 Cash		9700
Jan 99 Cash		9800
Jan 100 Cash		9900
Jan 101 Cash		10000

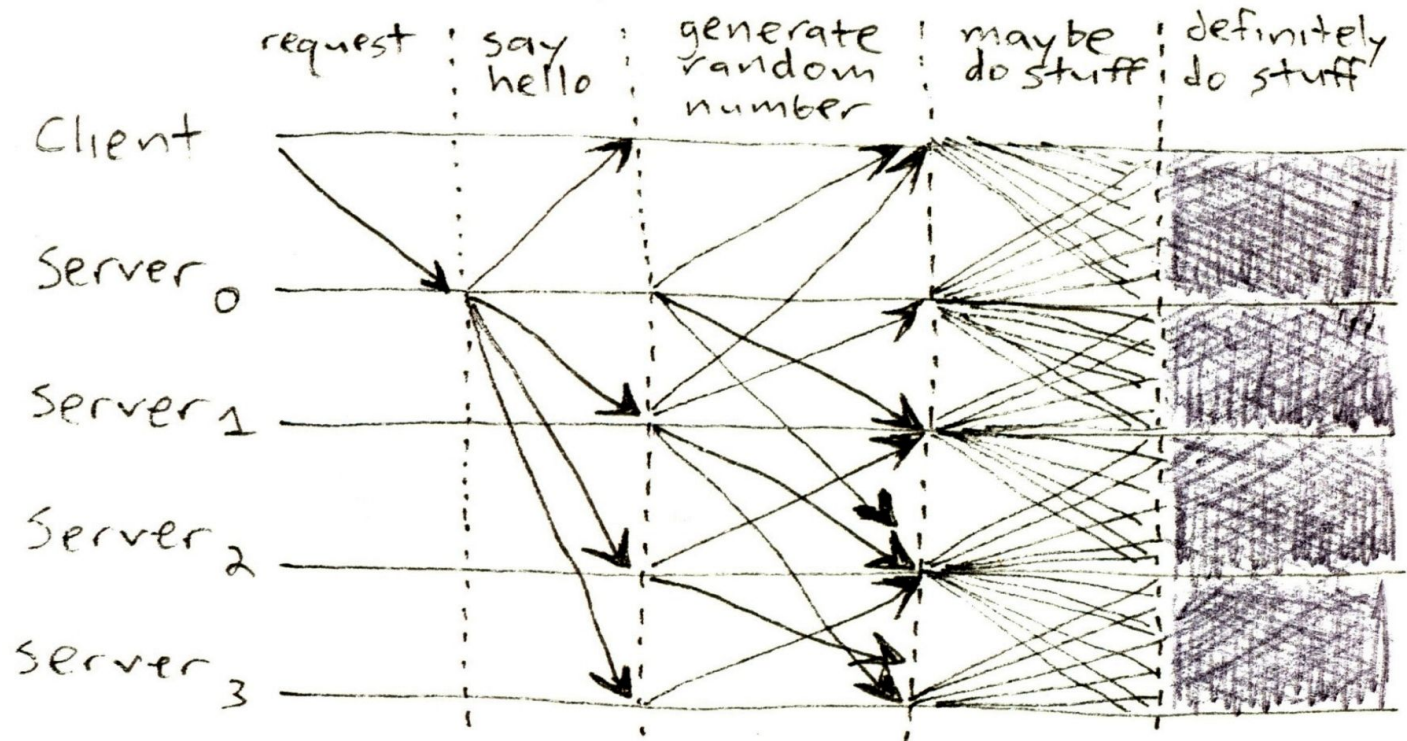
Ordered sequence of operations

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” Cay

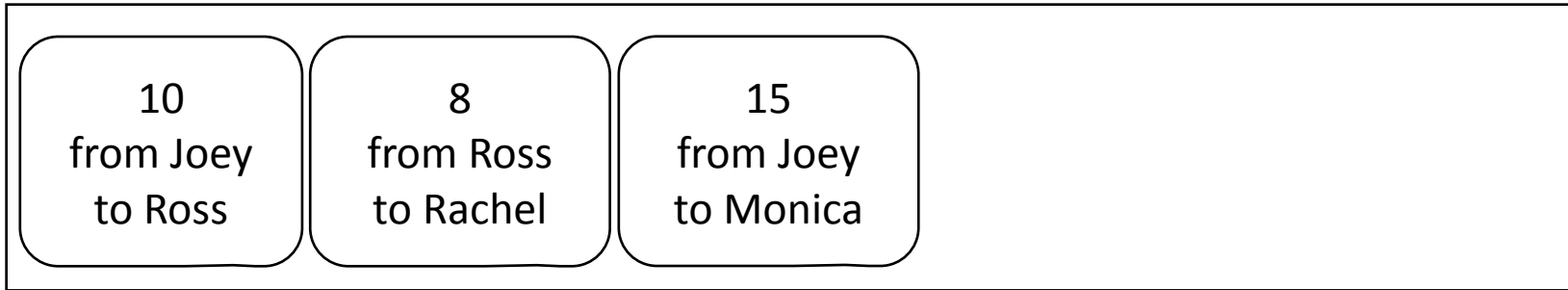
Consensus → Total Order Broadcast → Execution



Picture by James Mickens, “The Saddest Moment”

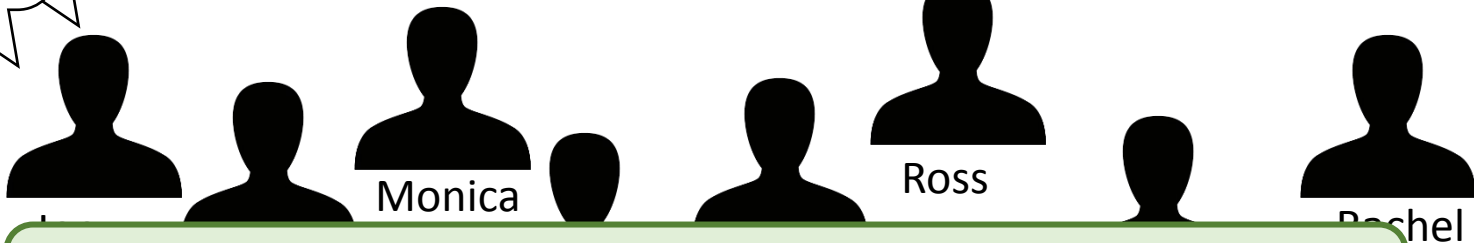
Money as a State Machine

Ledger:



15
from Joey
to Monica

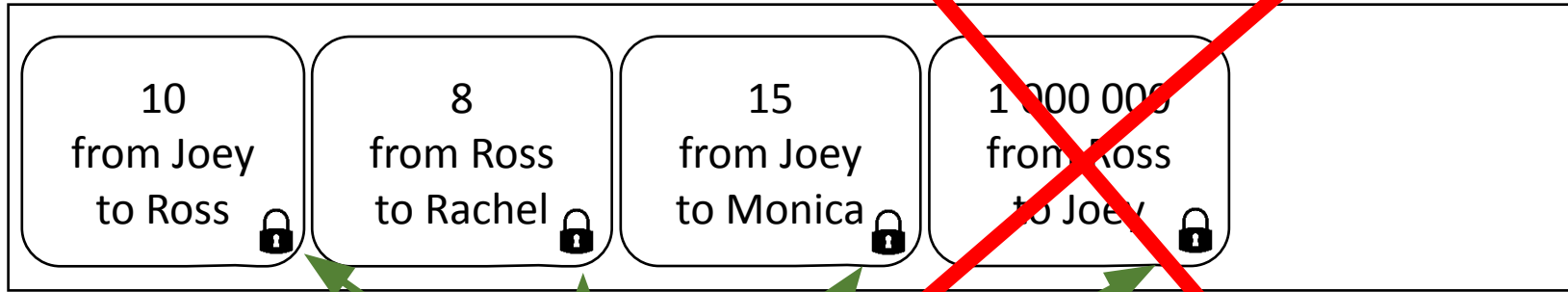
8
from Ross
to Rachel



Problems ? (Hint: there are plenty)

Problem: Impersonation

Ledger:



Add digital
signatures

Invalid
signature!

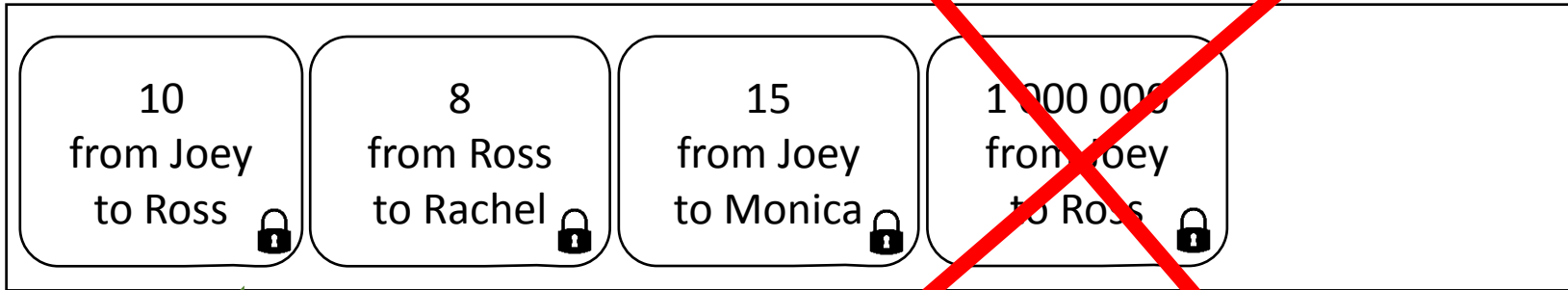
1 000 000
from Ross
to Joey



Solution: Signatures

Problem: Not Enough Money

Ledger:



Verify history

1 000 000
from Joey
to Ross



Monica



Ross



Rachel

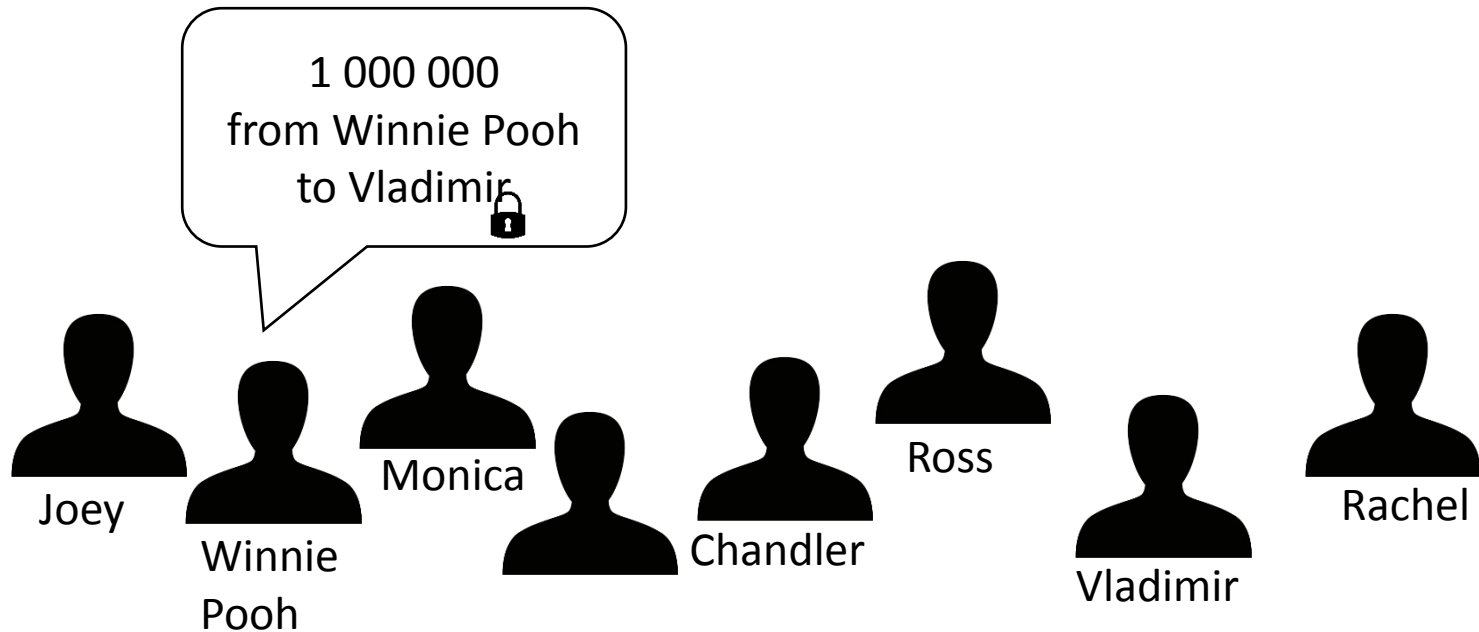
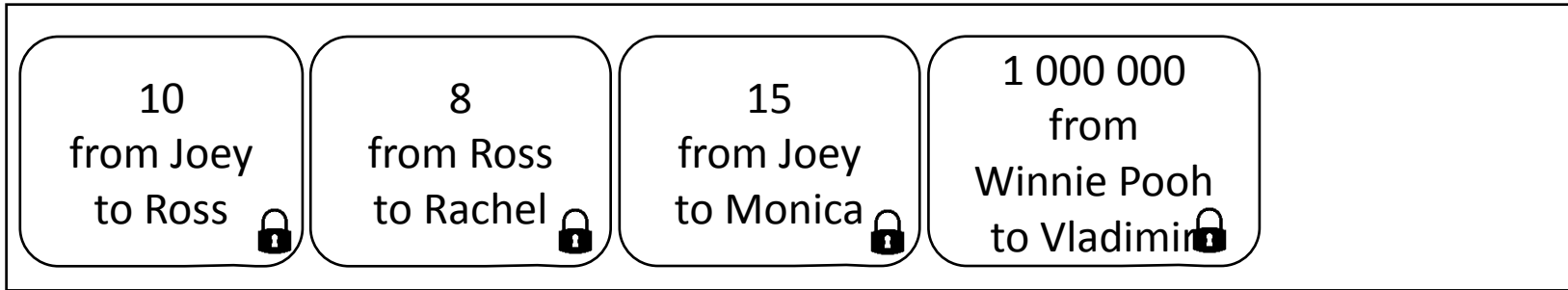
Solution: Verify history

Recap

- Signing / Verifying

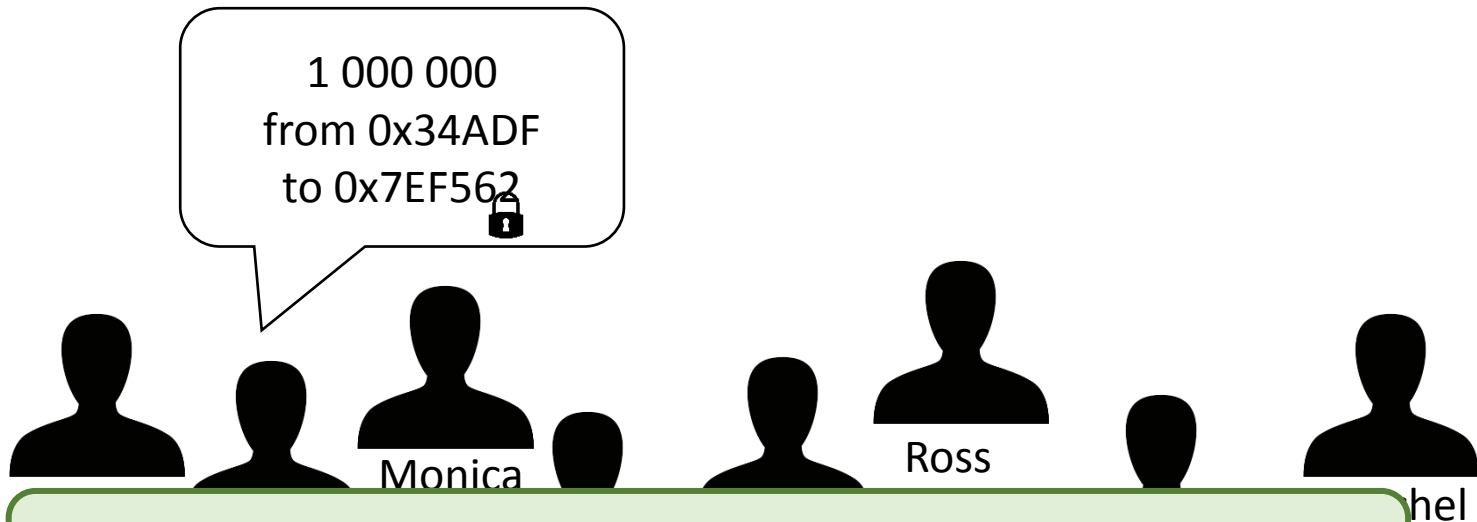
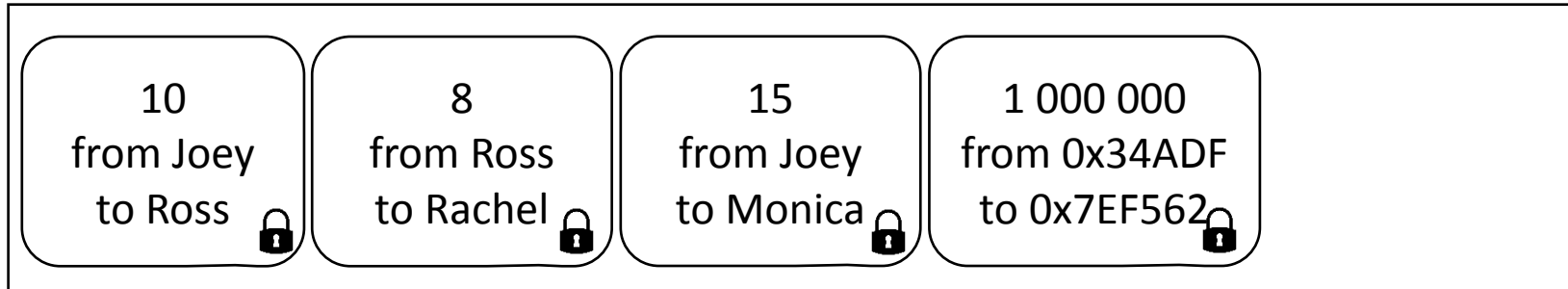
Problem: Anonymity?

Ledger:



Problem: Anonymity?

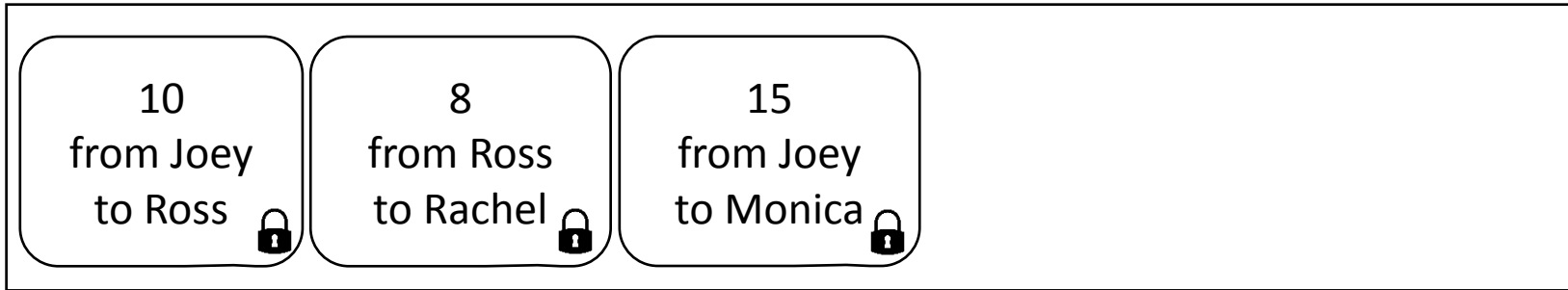
Ledger:



No need to disclose identity. Public key sufficient.

Problem: Who Stores the Ledger?

Ledger:



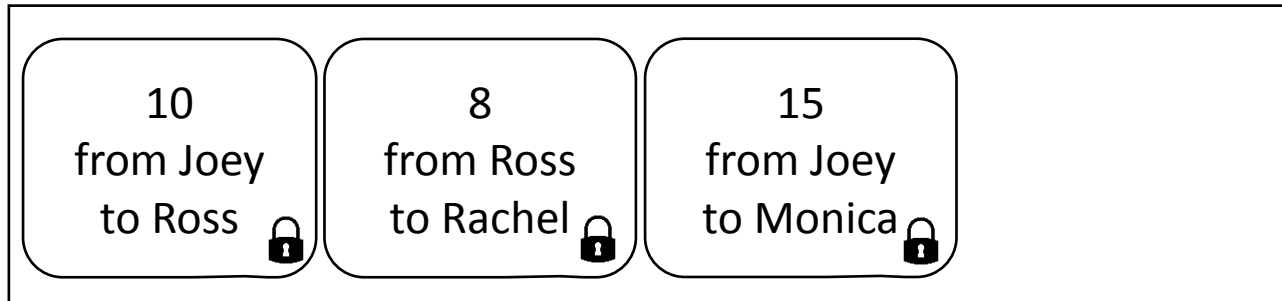
Everybody!

Problem: Who Stores the Ledger?

Joey's copy:



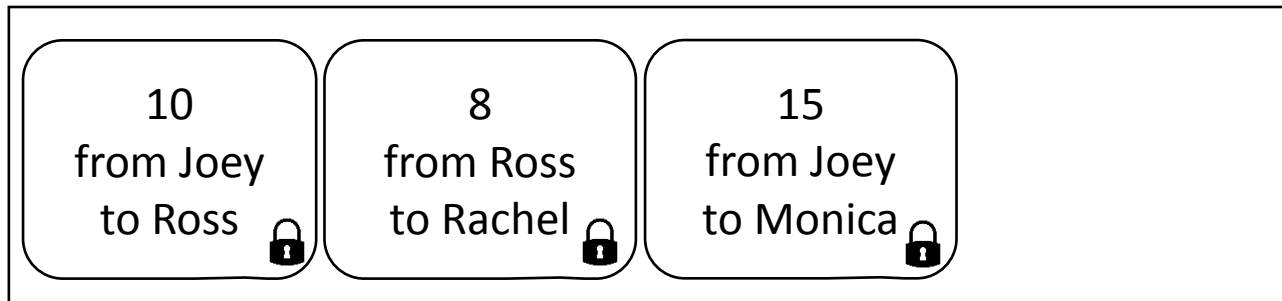
Joey



Monica's copy:



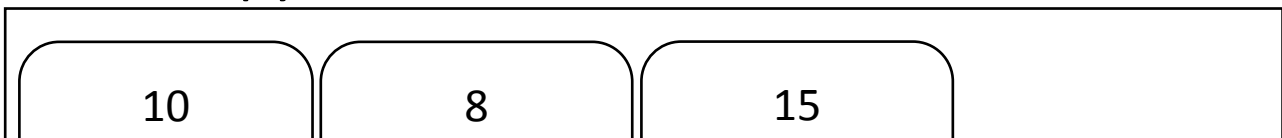
Monica



Ross's copy:



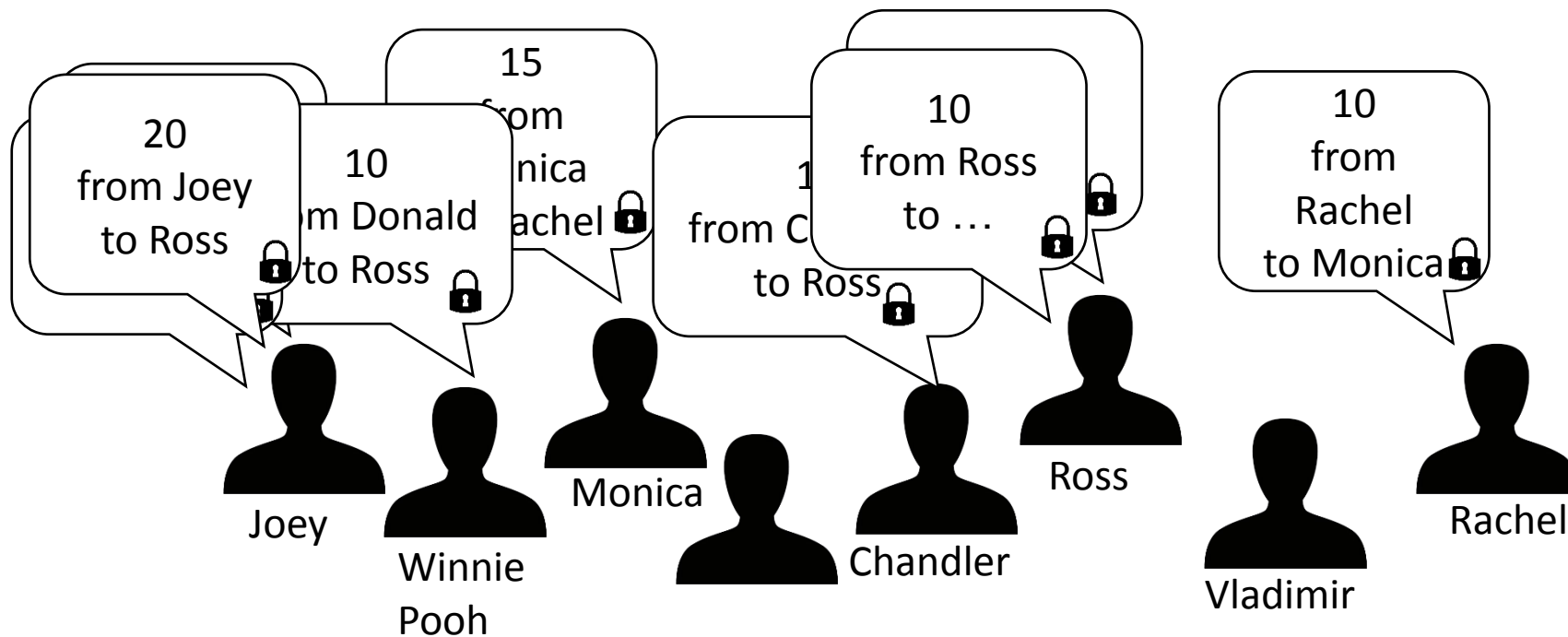
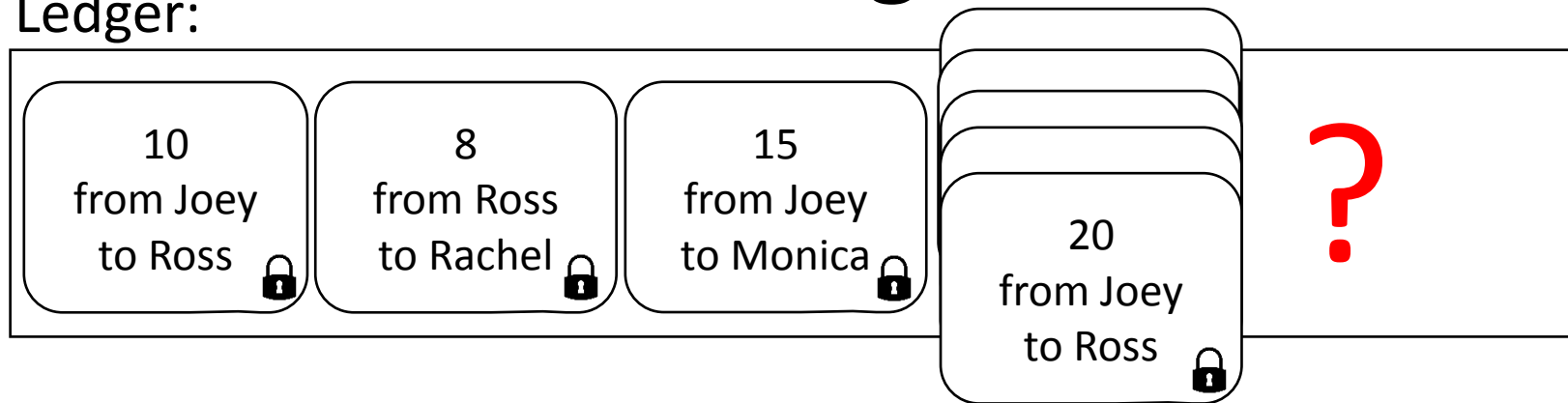
Ros



Problem? (Hint: already discussed.)

Problem: Agreement

Ledger:

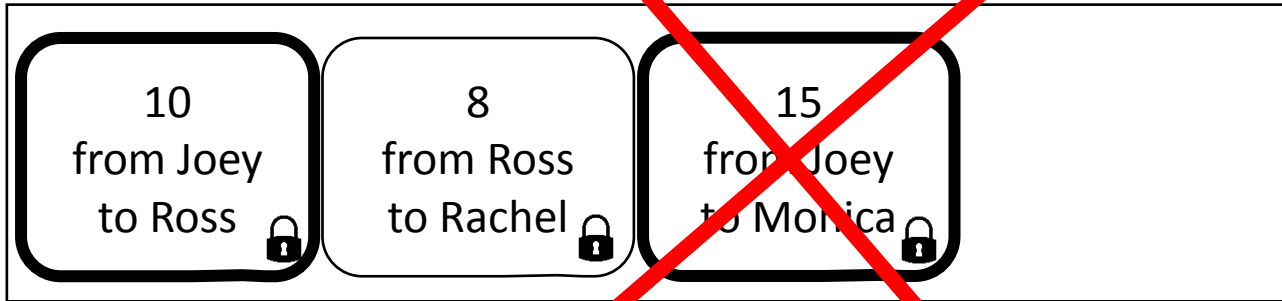


Problem: Agreement

Joey's copy:



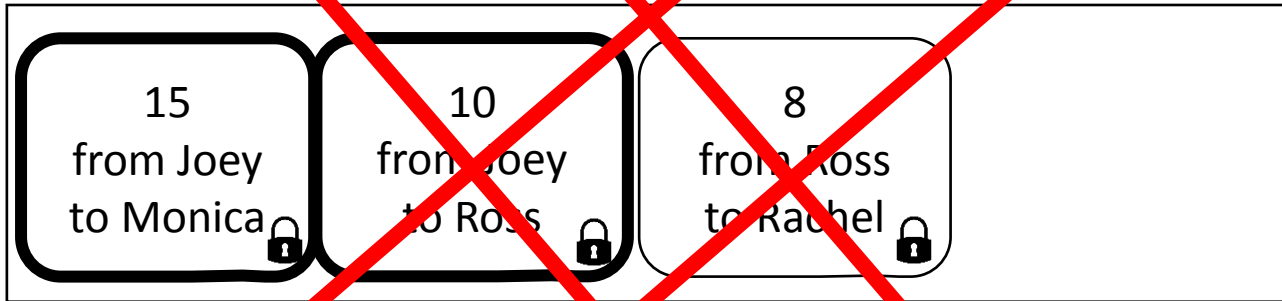
Joey



Monica's copy:



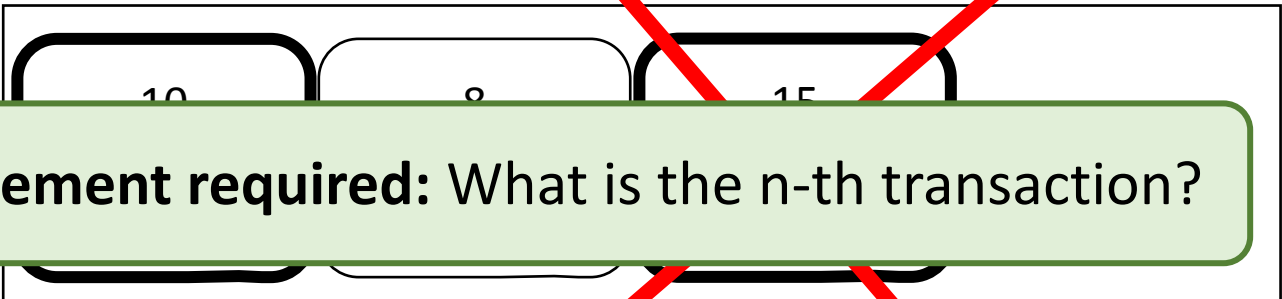
Monica



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

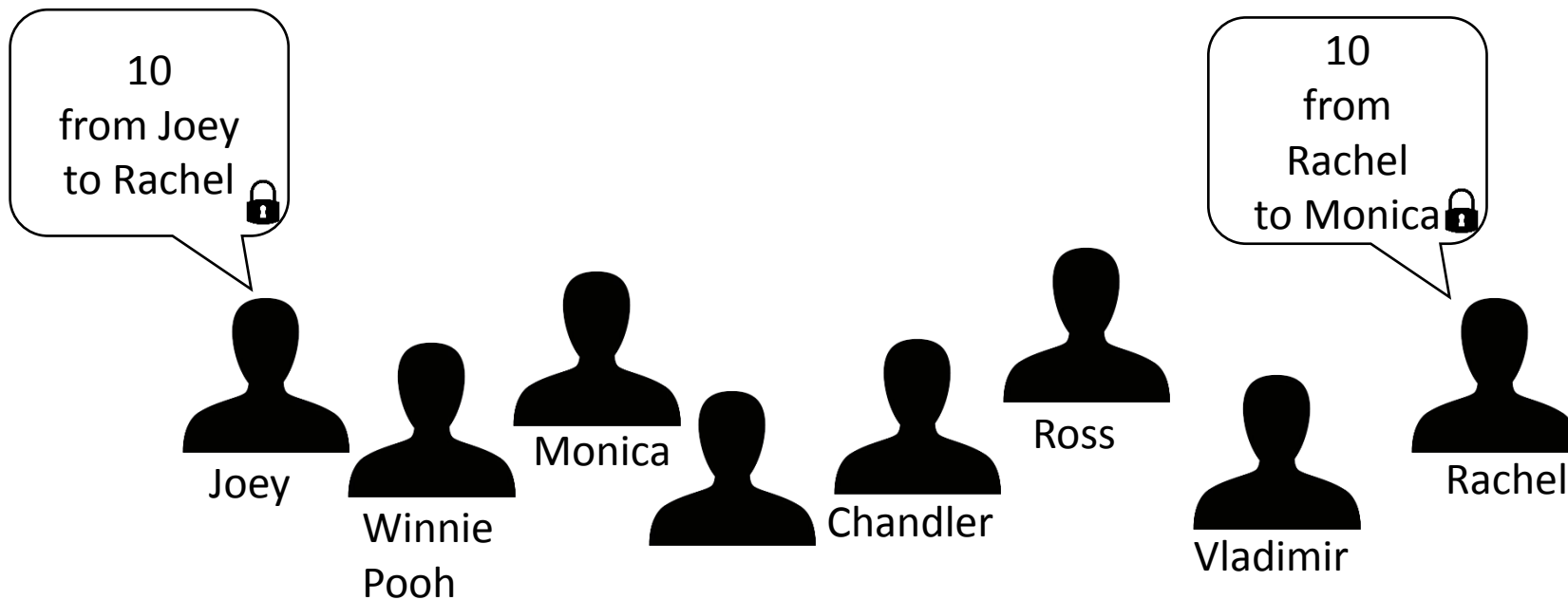
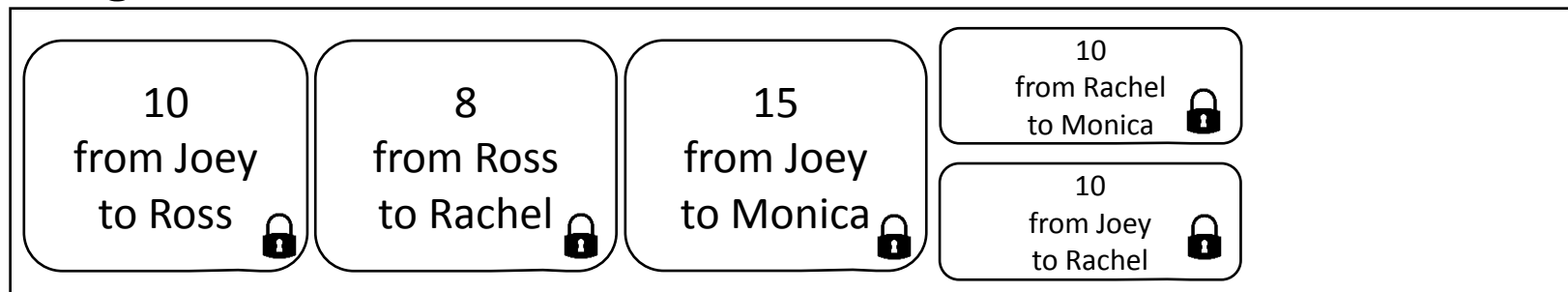
How Do We Solve Agreement?

?

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

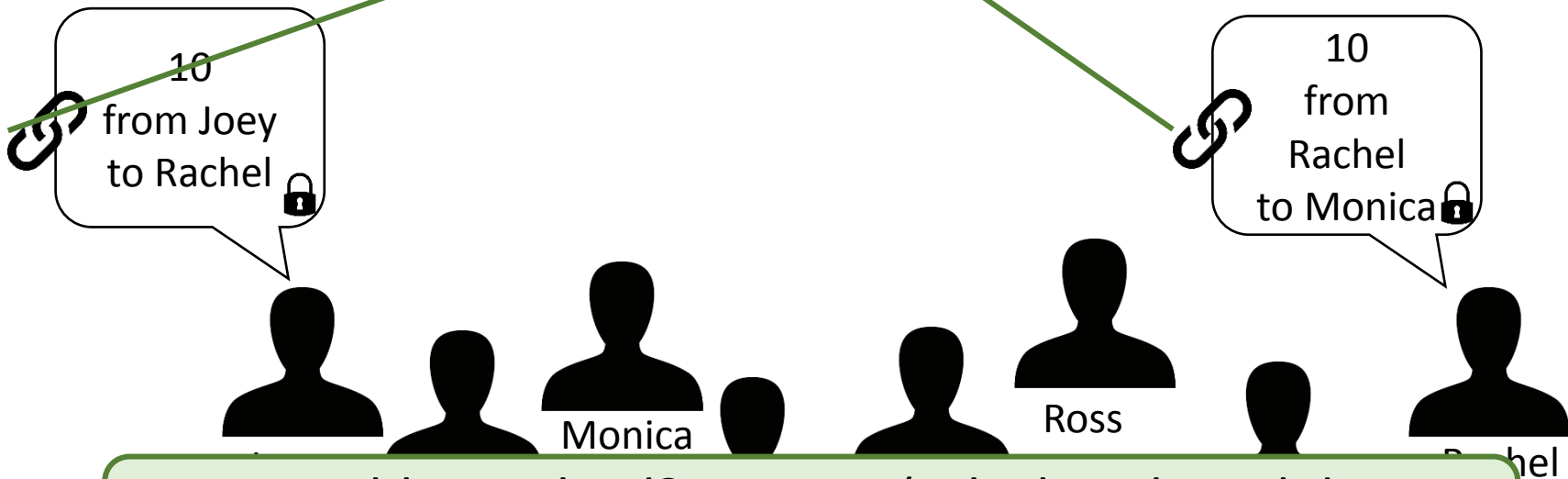
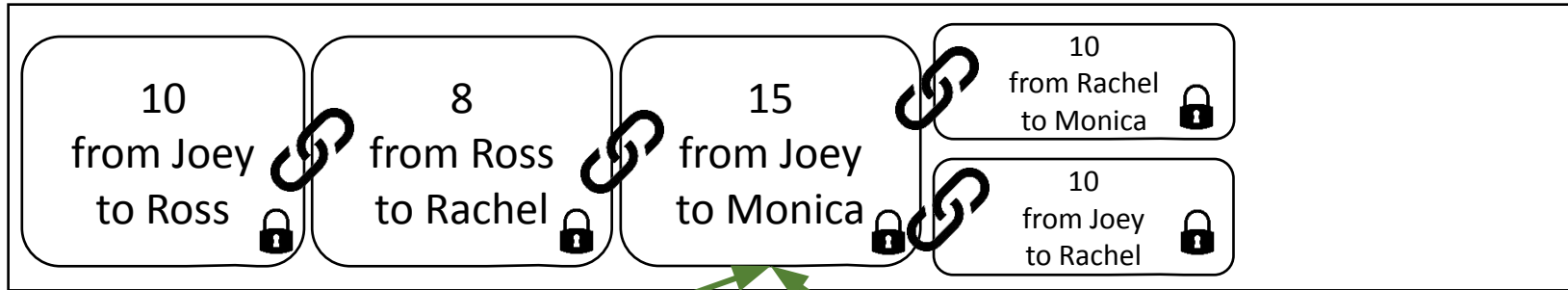
Chaining

Ledger:



Chaining

Ledger:



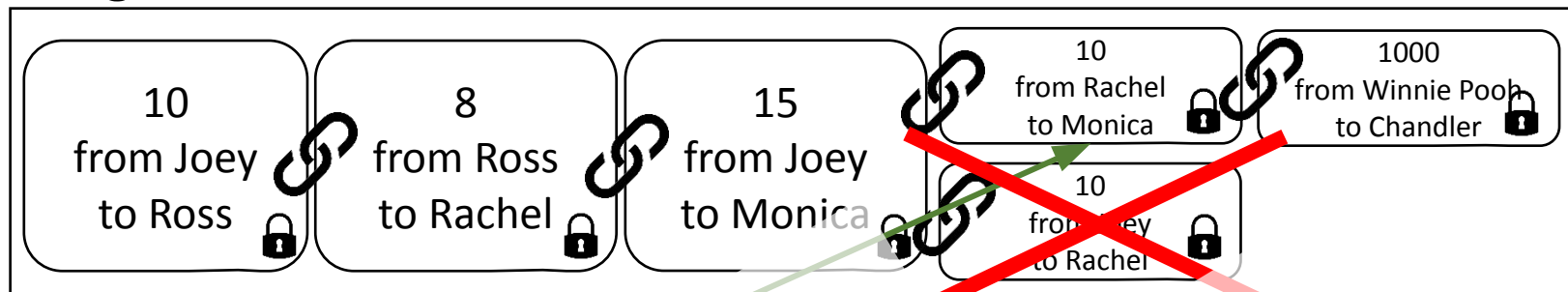
Problem solved? Nope... (Which is the valid transaction?)

Recap

- Signing / Verifying
- Chaining

Voting

Ledger:



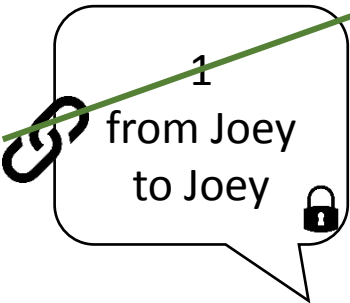
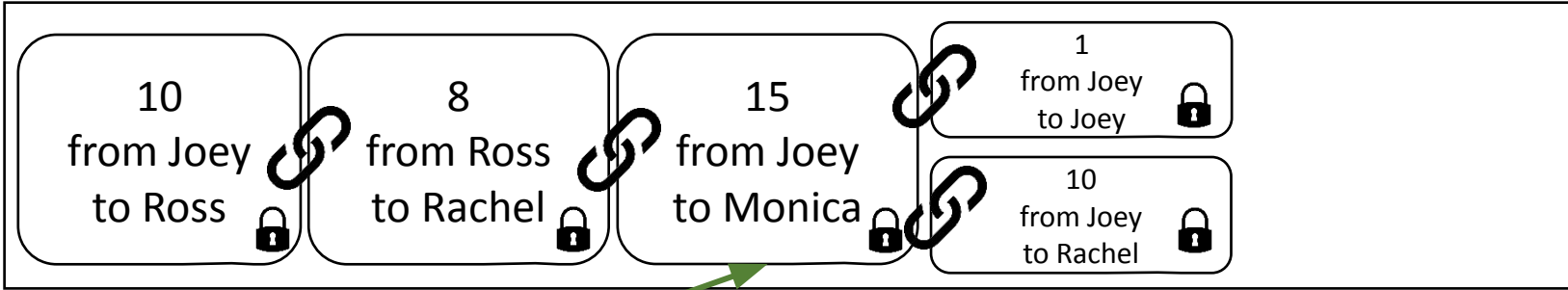
OOPS!

BIG PROBLEM...

Longest chain is valid (by definition).

Cheating

Ledger:



Joey



Winnie
Pooh



Monica



Chandler



Ross



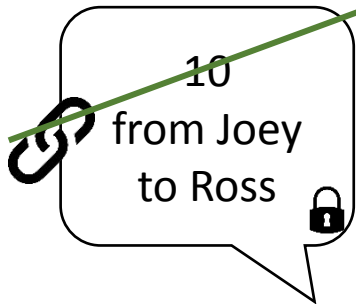
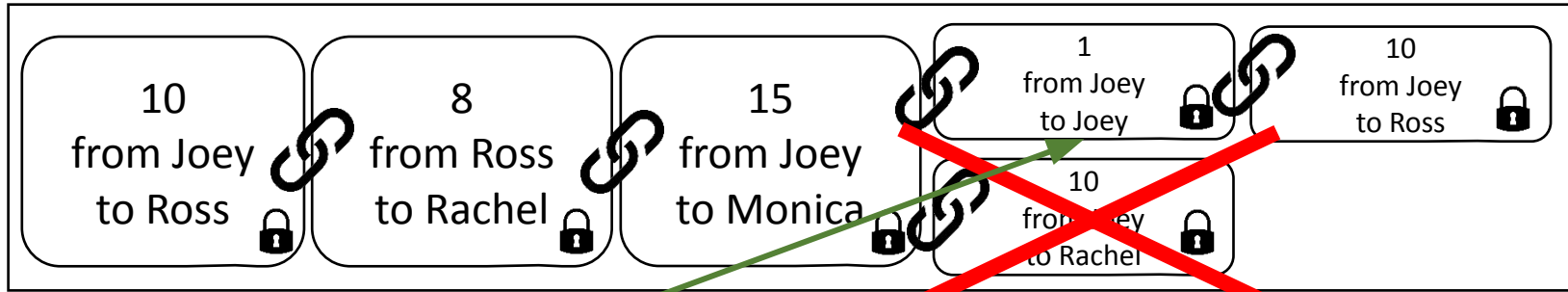
Vladimir



Rachel

Cheating

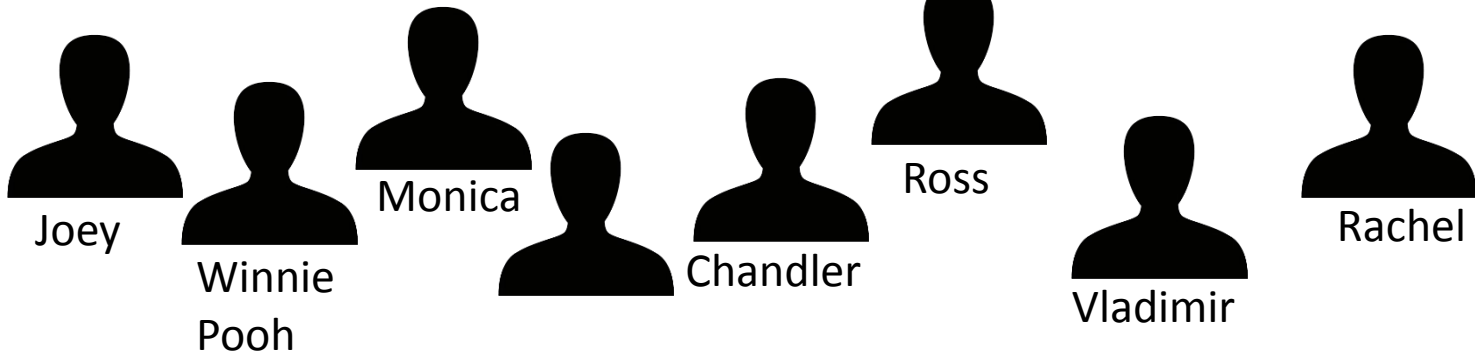
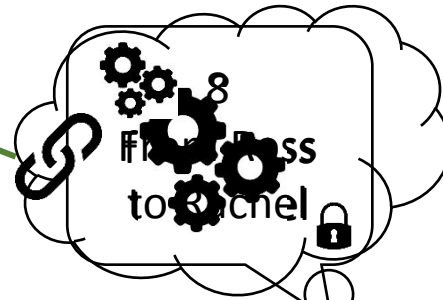
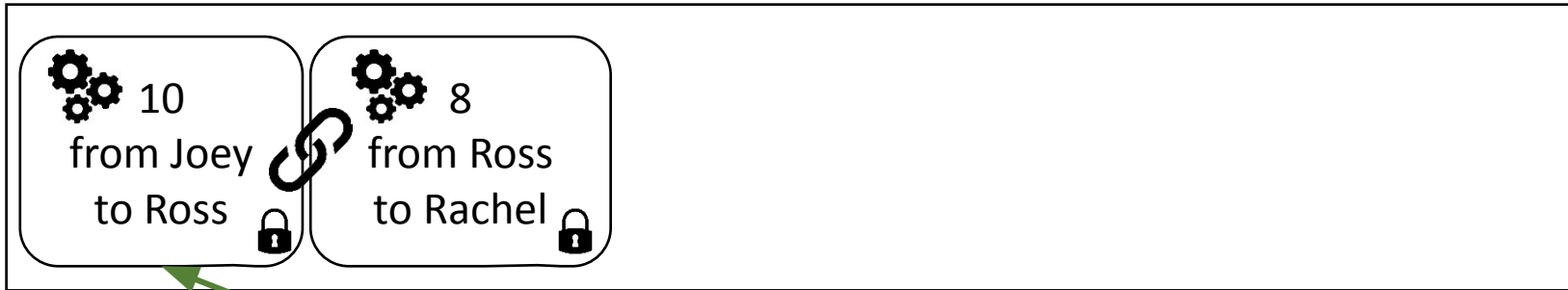
Ledger:



Double Spending!

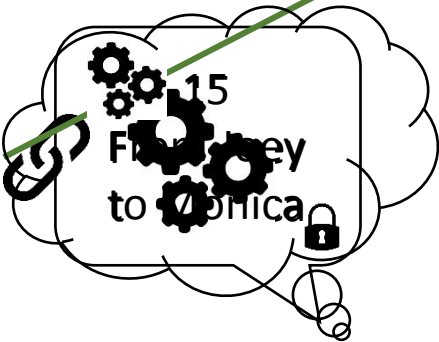
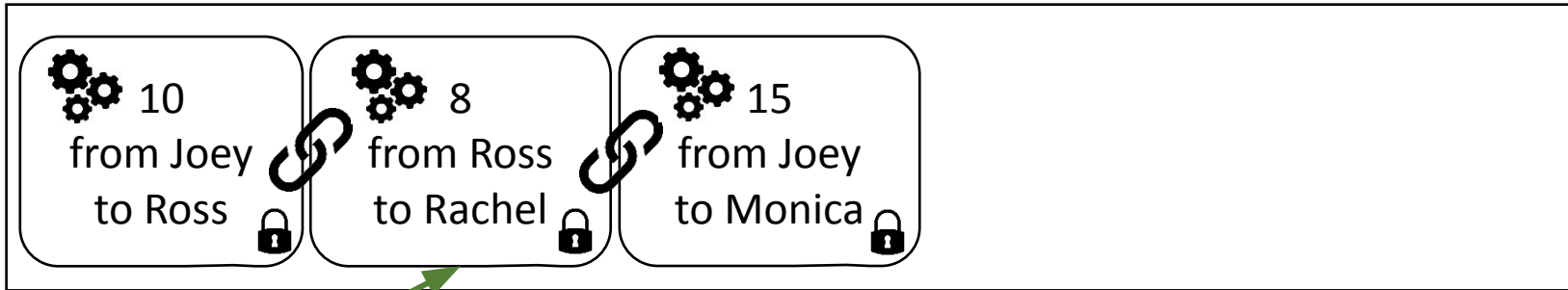
Working

Ledger:



Working

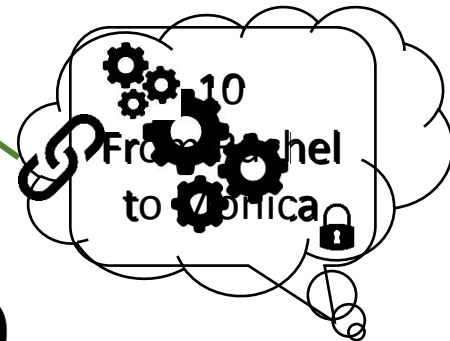
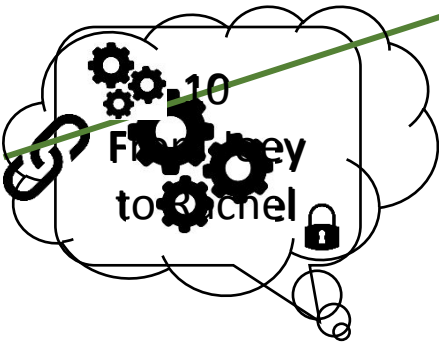
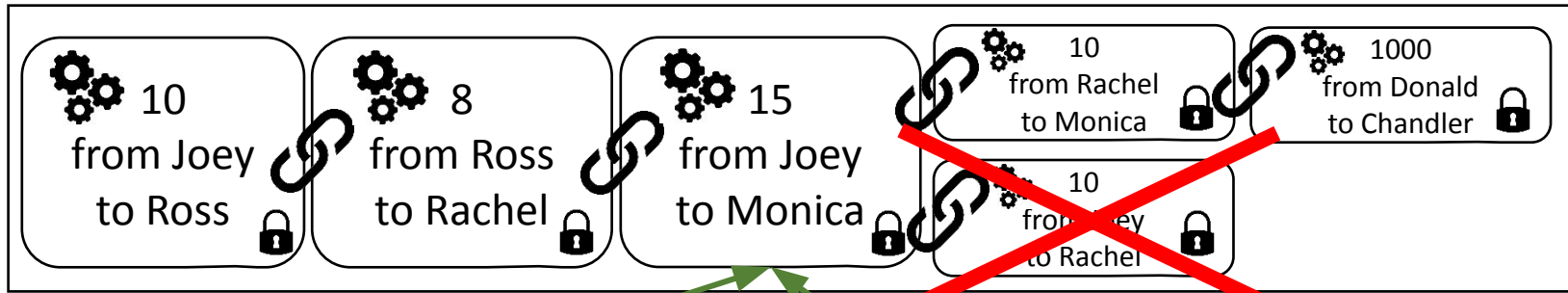
Ledger:



Work is very hard

Working

Ledger:



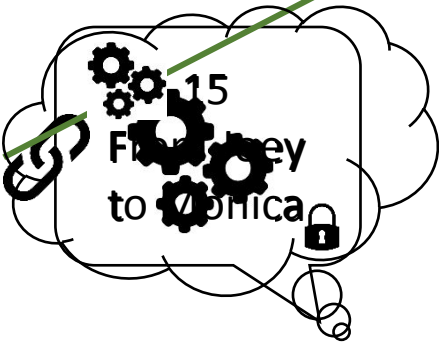
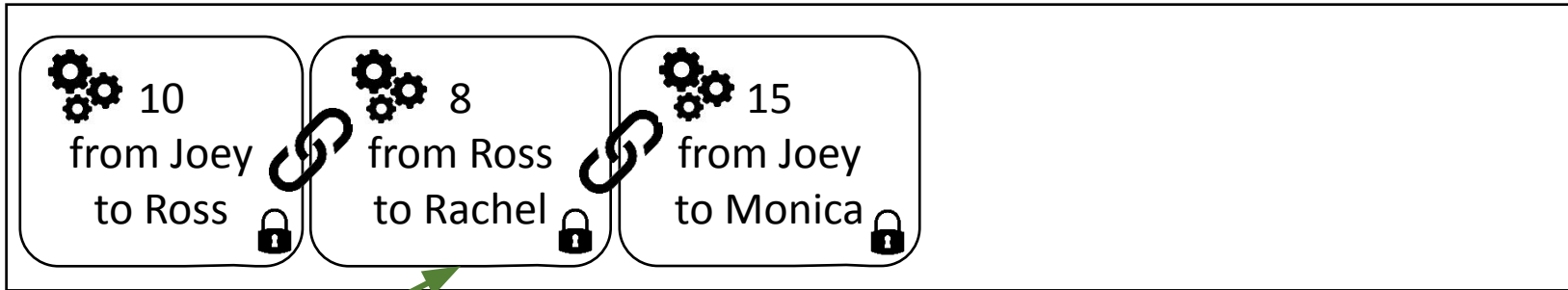
FORK. Happens rarely. (When...?)

Recap

- Signing / Verifying
- Chaining
- Voting
- Working

Working

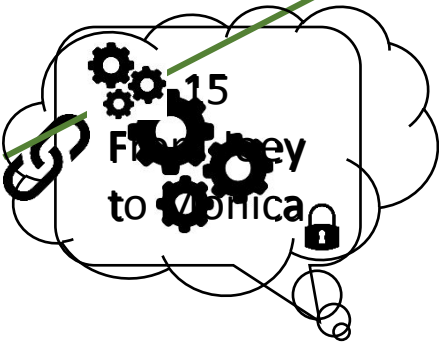
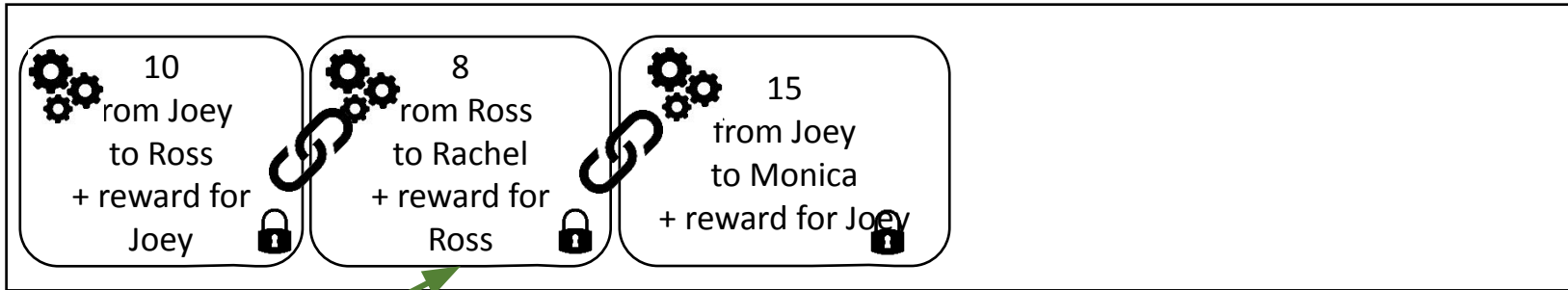
Ledger:



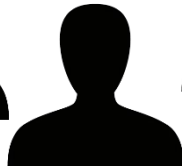
Work is very hard... Why do it?

Rewards

Ledger:



Joey



Winnie Pooh



Monica



Chandler



Ross



Vladimir



Rachel

Recap

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

Proof-of-Work Blockchain!!!



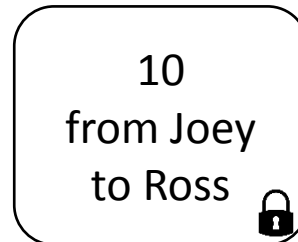
How Exactly... ?

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

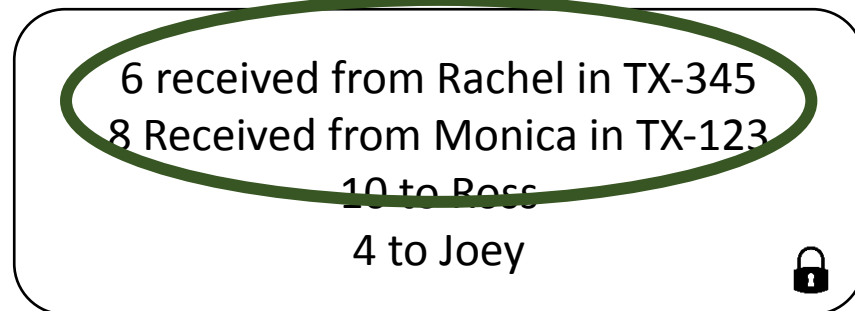
How Exactly... ?

- Signing / Verifying → Unspent TX Output

Simply:




TX-678:



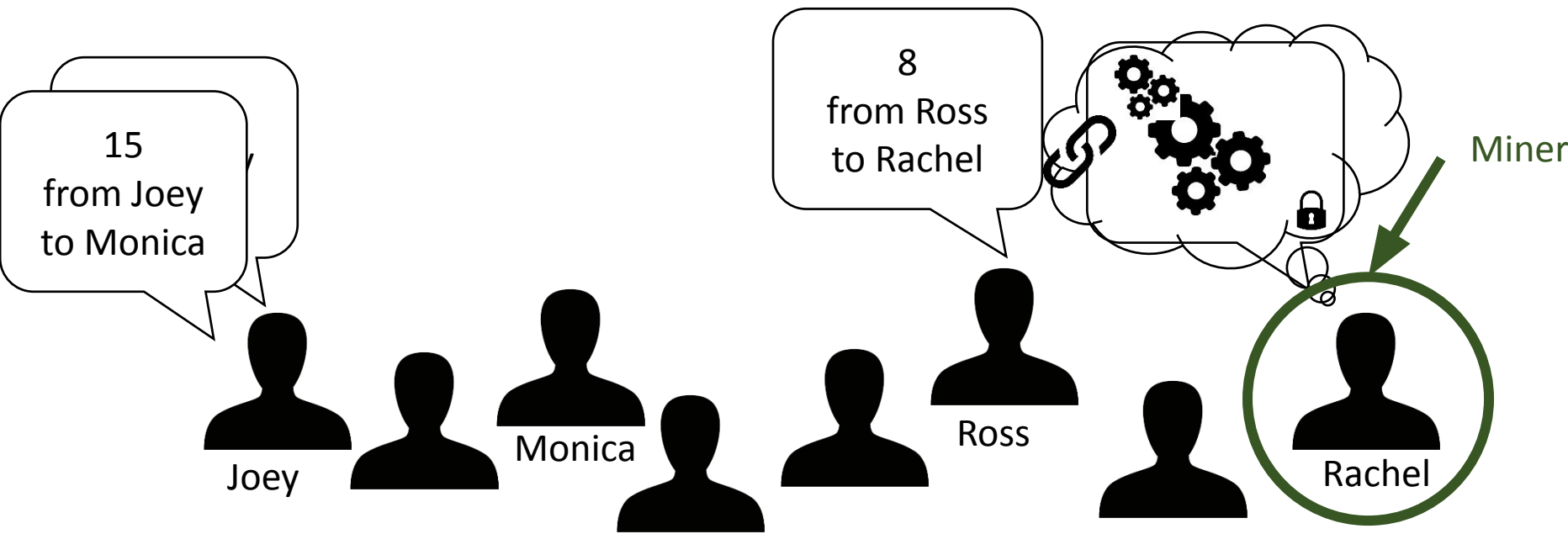
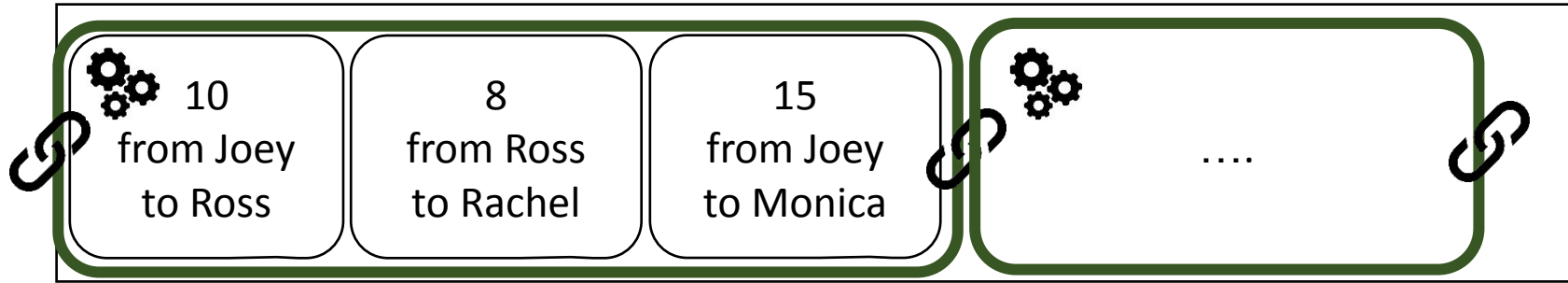
But actually...

How Exactly... ?

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

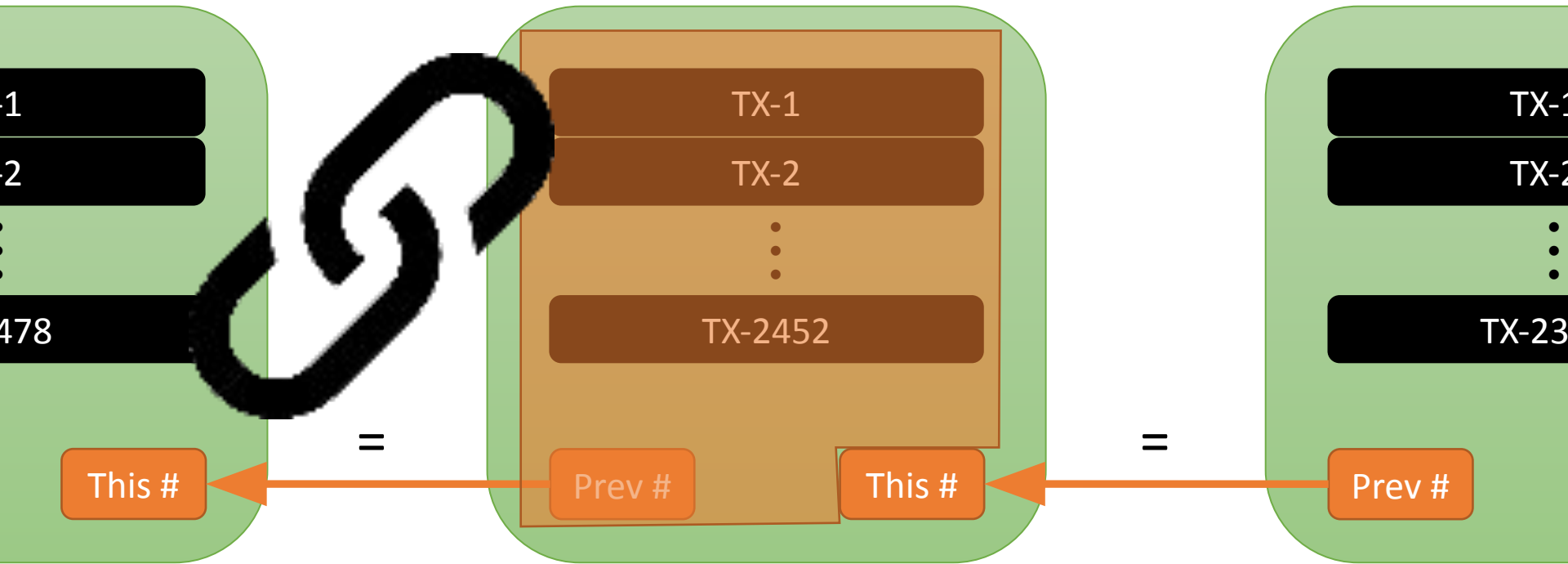
Blocks

Ledger:



Block Chaining (Hashes)

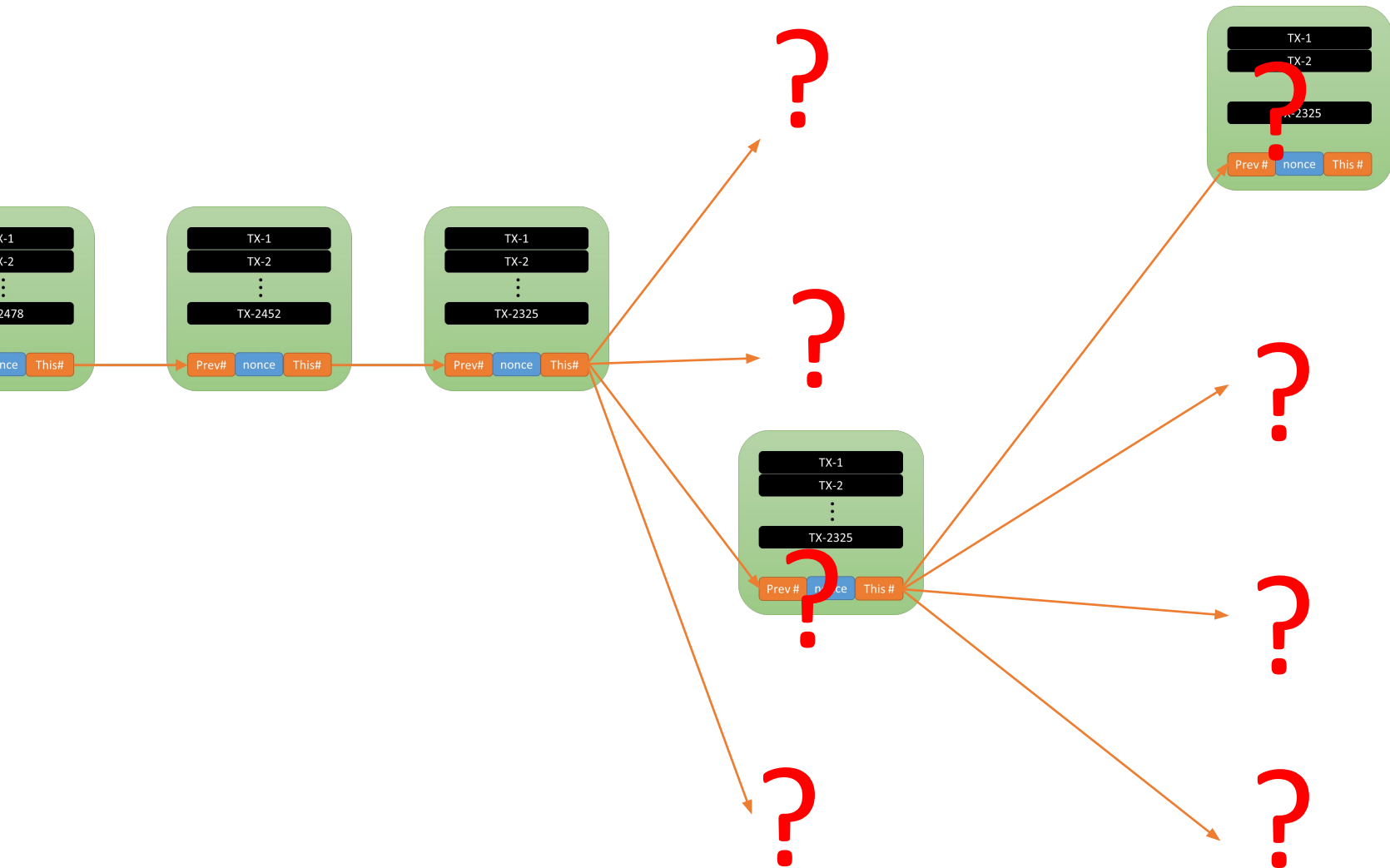
Bitcoin block



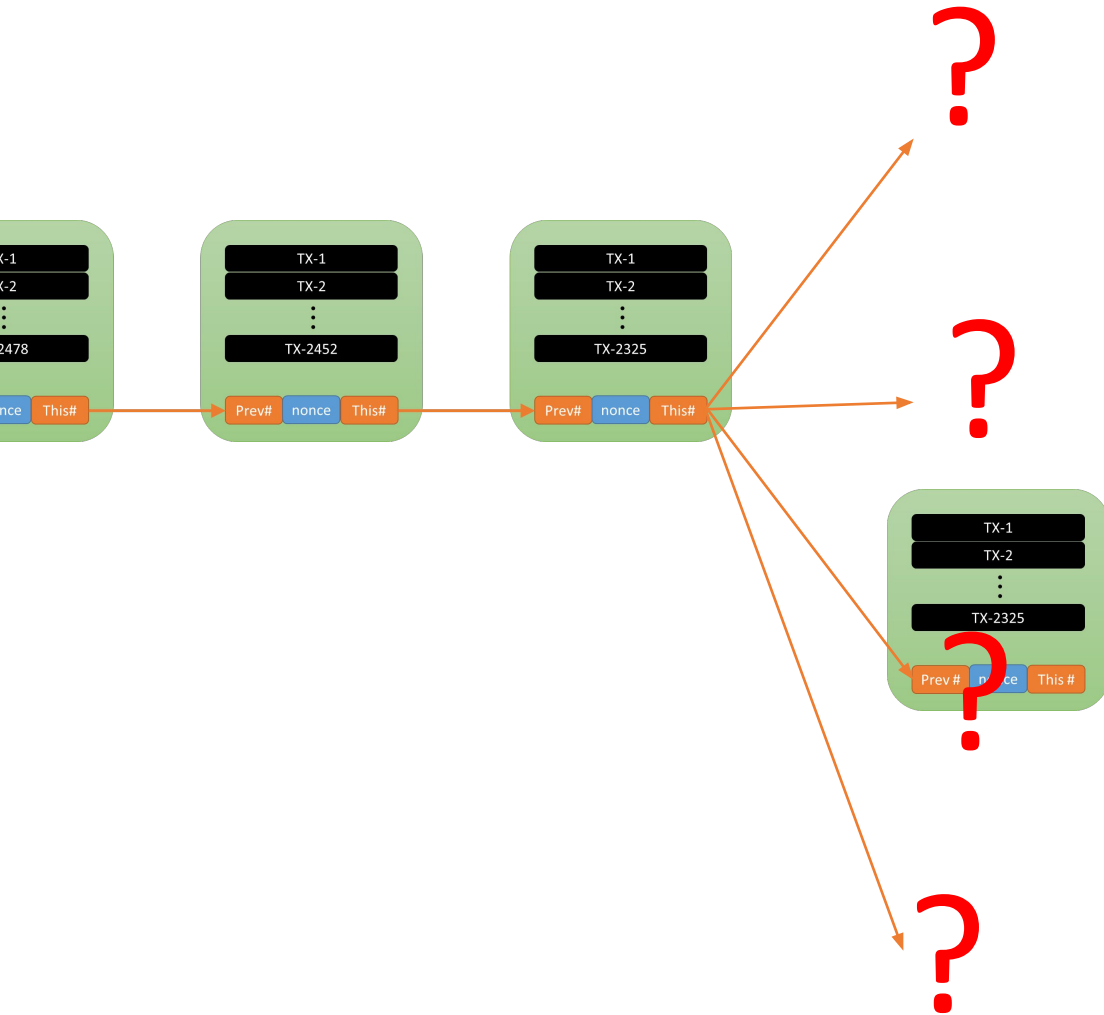
How Exactly... ?

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

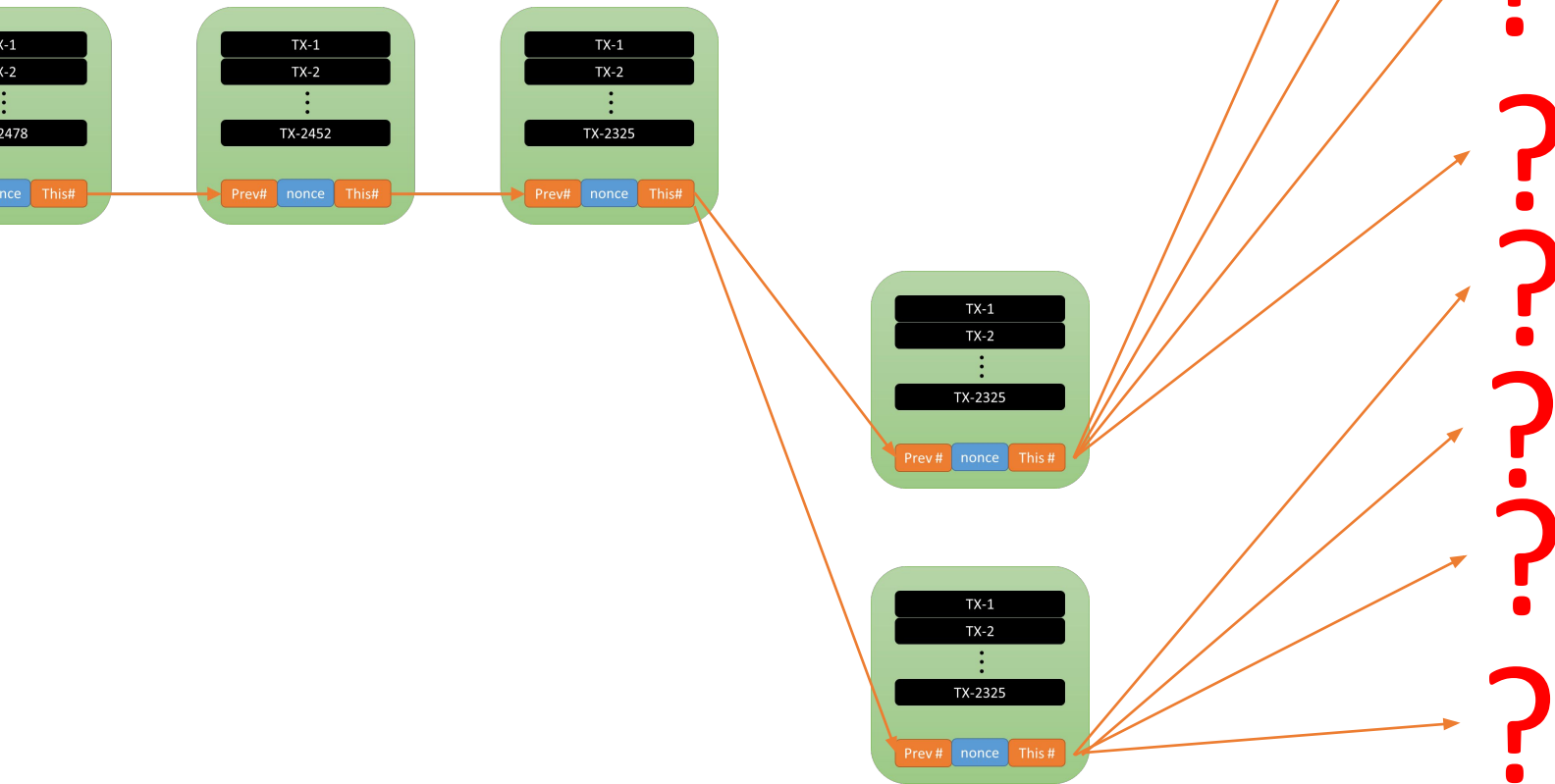
Prolonging the Chain



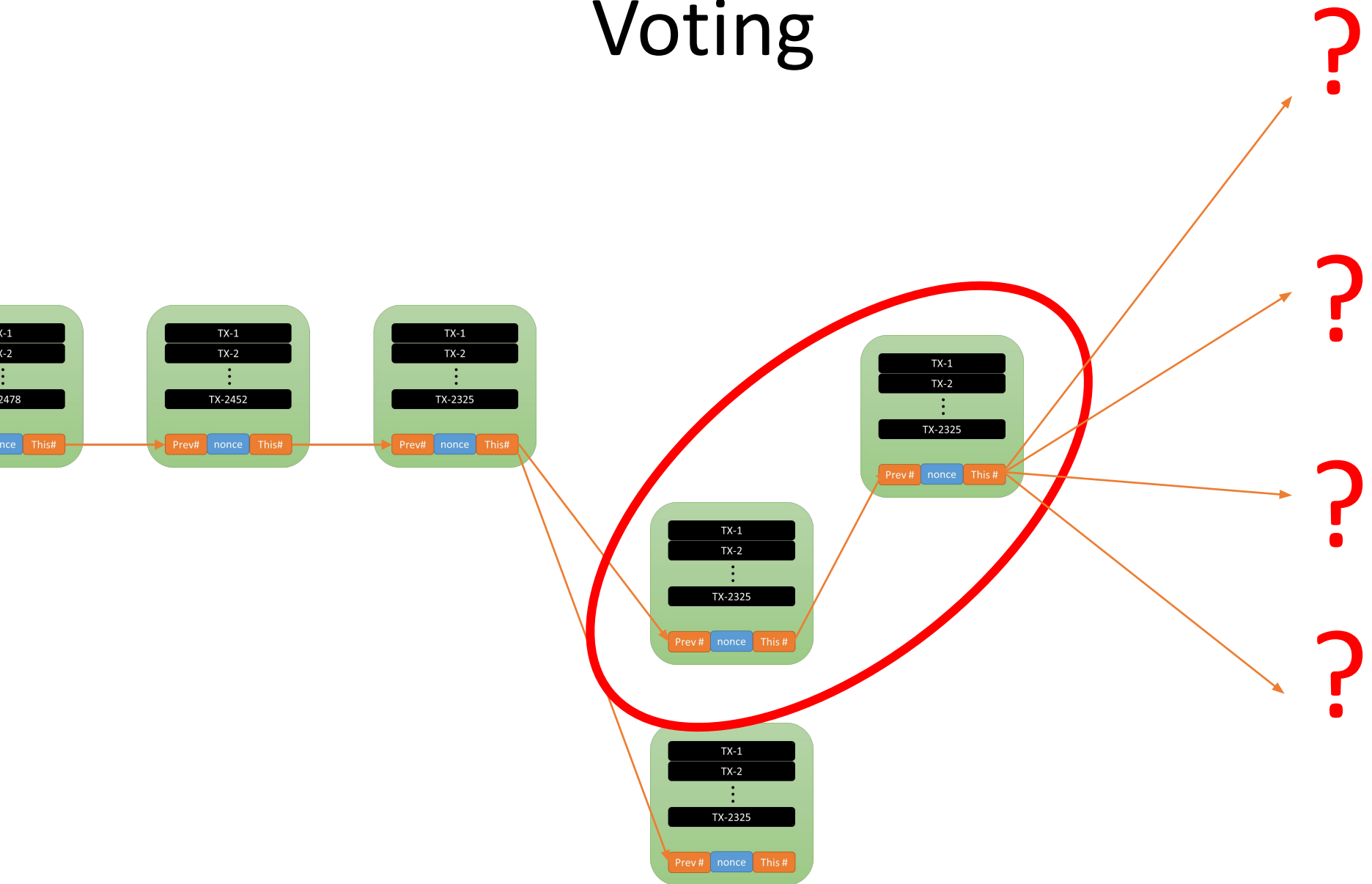
Voting



Voting



Voting



How Exactly... ?

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

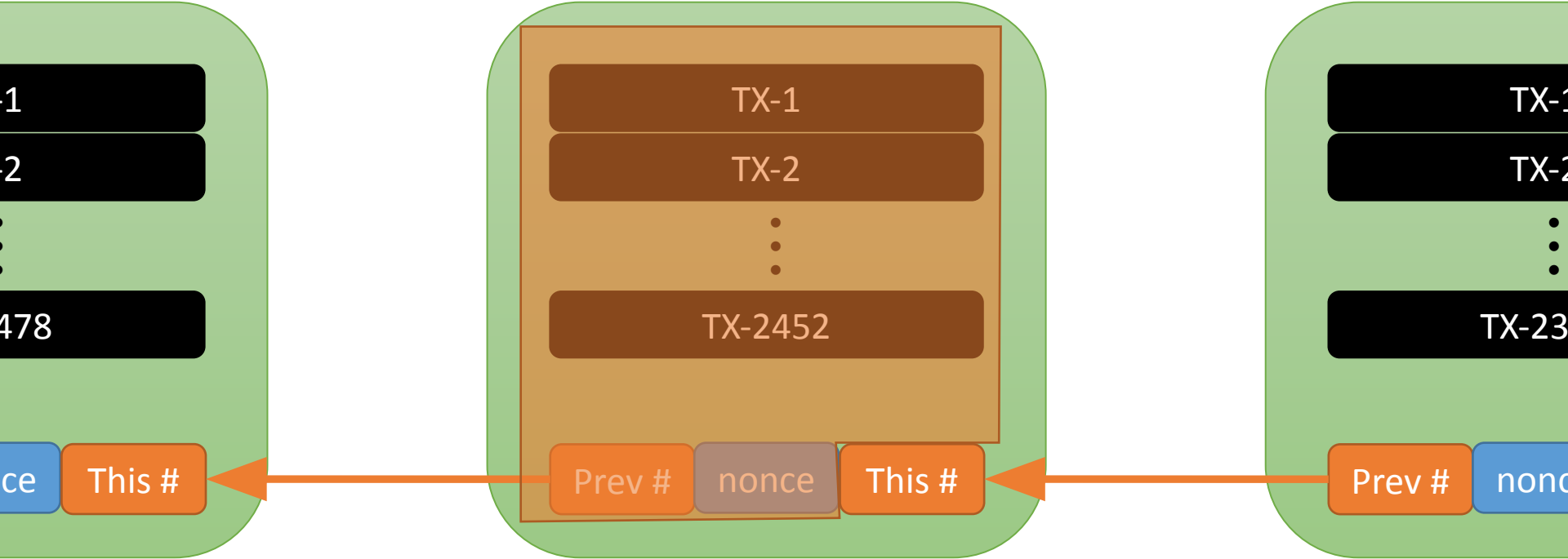
Hashing



data → number

Mining

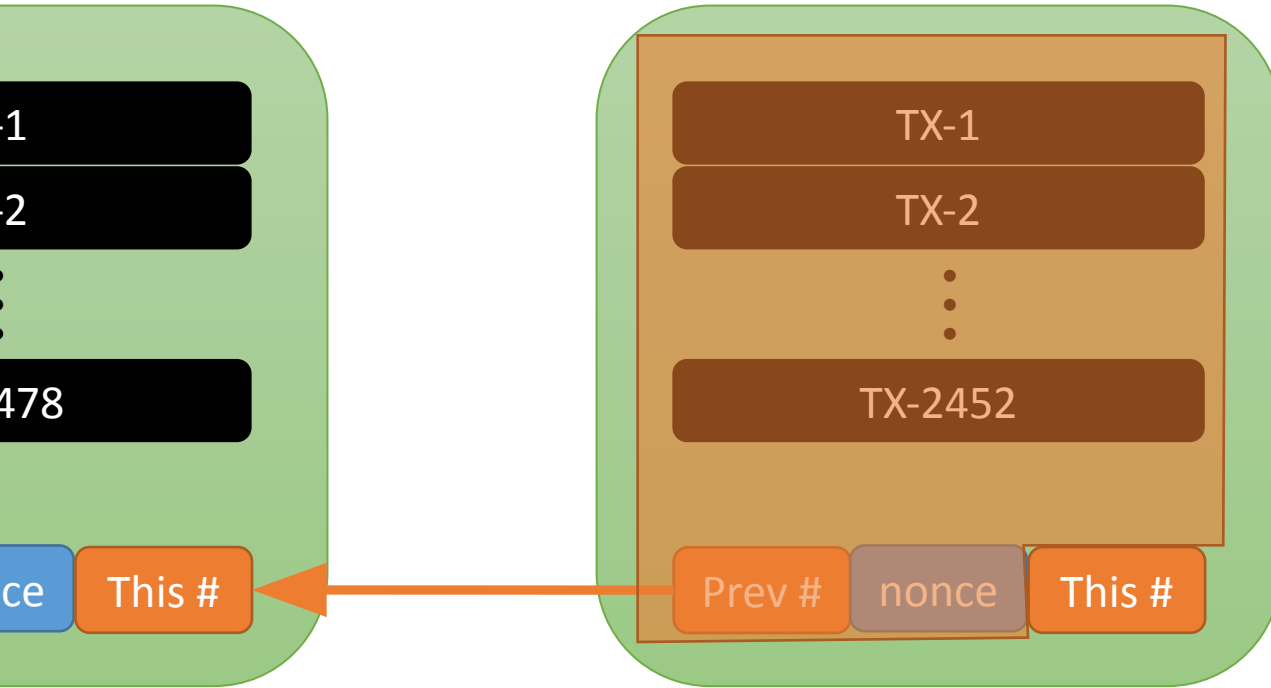
Bitcoin block

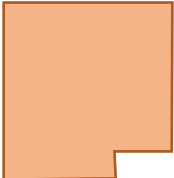


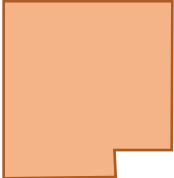
Mining: find **nonce** such that **This #** $< d$

Work is very hard... Why do it?)

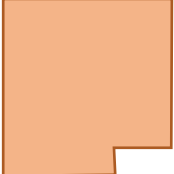
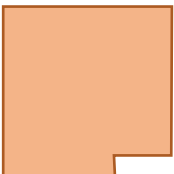
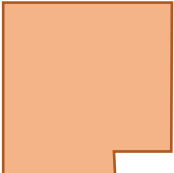
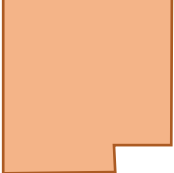
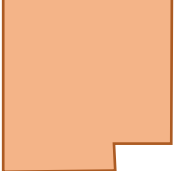
Mining (d = 1 000 000)



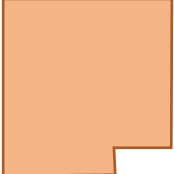
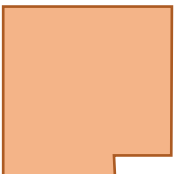
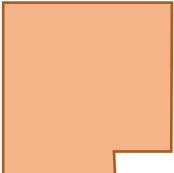
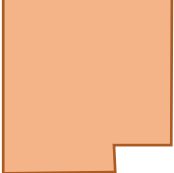
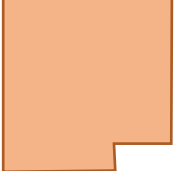
Try **1**: hash() = 24623523455124 > 1 000 000 ☹️

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() = 9042179911576 > 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() = 9042179911576 > 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

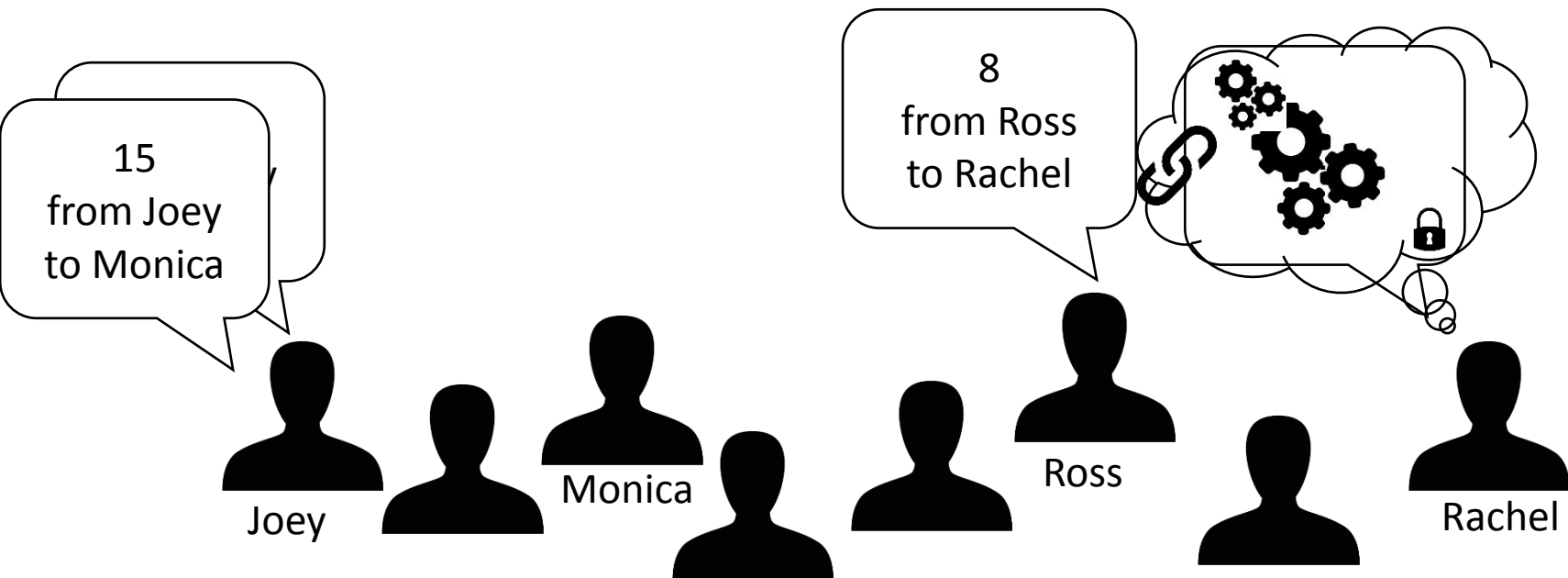
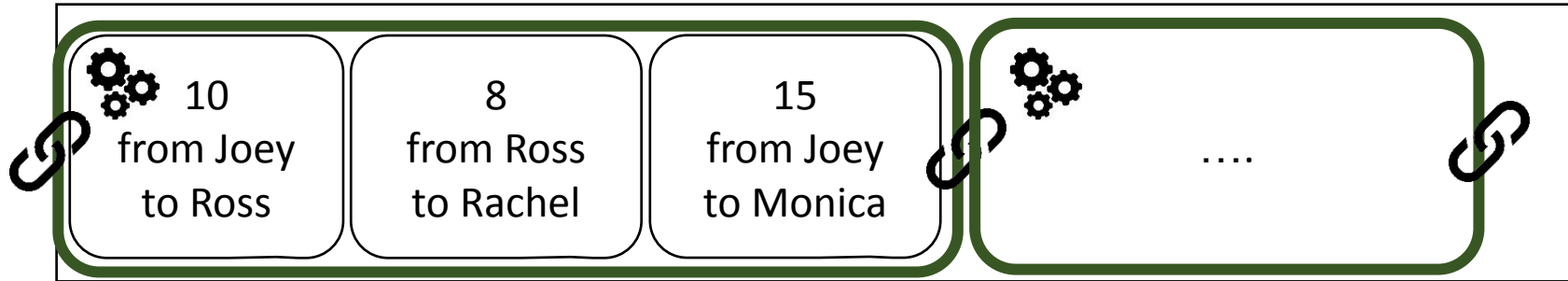


How Exactly... ?

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

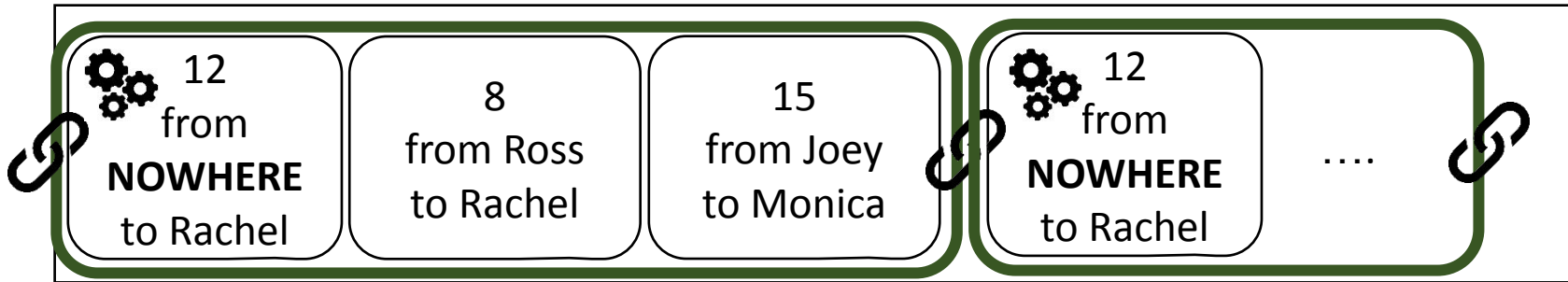
Blocks

Ledger:



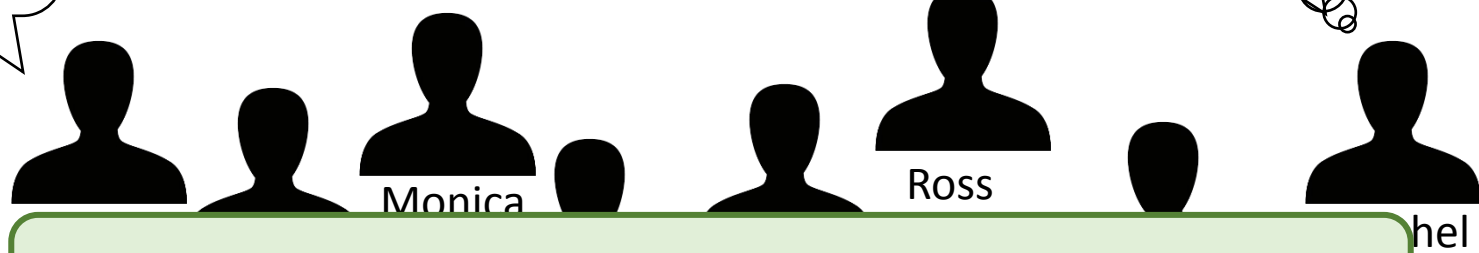
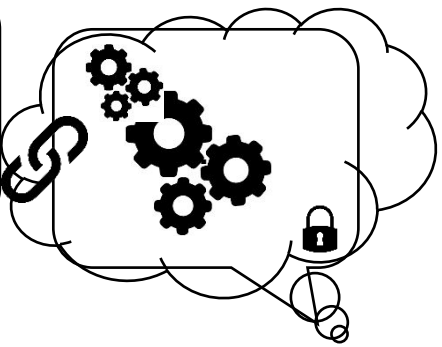
Rewards (1)

Ledger:



15
from Joey
to Monica


8
from Ross
to Rachel




Special transaction: "Coinbase"

Rewards (2)

Simply:


10
from Joey
to Ross 

TX 123:

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

But 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 

ACTUALLY...

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.