ROYAL INSTITUTE
OF TECHNOLOGY

Bitcoins and Blockchains

ROYAL INSTITUTE
OF TECHNOLOGY

Bitcoins?

ROYAL INSTITUTE OF TECHNOLOGY

Properties of money

- Symbolises value
- Substitutes value
- Proof of ownership
- Easy to transfer
- Agreed upon value
- Difficult to forge/limited supply
- Needs little storage space

slide from: www.csc.kth.se/~buc/PPC/Slides/ecashbitcoinblindsignatures.pdf

ROYAL INSTITUTE OF TECHNOLOGY

Why banks?

- **Storage**: better than keeping all your valuables on your own person.
- **Administration**: buy things from someone you have never met.
- **Organised economy**: get payed for letting someone use your money while you don't.
- **Authorising** that you are in possession of certain amounts of money.

slide from: www.csc.kth.se/~buc/PPC/Slides/ecashbitcoinblindsignatures.pdf

ROYAL INSTITUTE OF TECHNOLOGY

To summarise…

- Banks act as a **trusted** third party to mediate transactions.
- The bank actually **holds** all your money.
- The bank acts as a ledger/log and **keeps track** of your transactions for balance correctness and as an audit trail.

slide from: www.csc.kth.se/~buc/PPC/Slides/ecashbitcoinblindsignatures.pdf

ROYAL INSTITUTE OF TECHNOLOGY

Wishlist for e-payment

- I can buy things in a store with my electronic money.
- I can pay any amount up to my total value of money.
- I can only use the same money once.
- I cannot create money by myself.
- I can pay for things without the bank knowing it.
- No one else can steal or copy my money when I make transactions.
- I might want to be able to pay when there is no internet connection/ power outage.
- Payments can be processed quickly.
- When the tax authorities want to know things, I can show receipts.
- If I try to cheat, it will(might) cost me.

slide from: www.csc.kth.se/~buc/PPC/Slides/ecashbitcoinblindsignatures.pdf

ROYAL INSTITUTE OF TECHNOLOGY

What is Bitcoin?

- Typically it refers to:
  - the technology concept
  - the protocol used
  - the currency

- A more appropriate terminology:
  - Blockchain technology
  - Bitcoin protocol
  - Bitcoin currency - btc

ROYAL INSTITUTE OF TECHNOLOGY

Driving factors of Bitcoin

- Get rid of banks as “special” third parties that validate transactions and allow everyone to do it.
- Incentify a large number of third parties to validate transactions in order to introduce competition
- Discourage and isolate cheaters from the system.
- Allow anyone to audit the log to see if things are correct.

ROYAL INSTITUTE OF TECHNOLOGY

Blind signatures

- Context:
  - We need the authority of a third party.
  - We don’t want the third party to know everything.
  - The third party can sign a certificate without knowing more than that someone wanted something signed.

slide from: www.csc.kth.se/~buc/PPC/Slides/ecashbitcoinblindsignatures.pdf

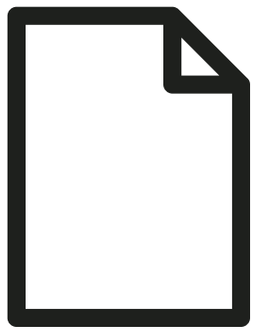
ROYAL INSTITUTE OF TECHNOLOGY

Chaum's voting analogy

- In 1983, David Chaum wrote the paper: "Blind signature for untraceable payments".
- A trusted third party should be allowed to "authorise" the votes of voters, but not see them.
- The voters do not need to be present at the election, but we do trust the delivery system.

slide from: www.csc.kth.se/~buc/PPC/Slides/ecashbitcoinblindsignatures.pdf

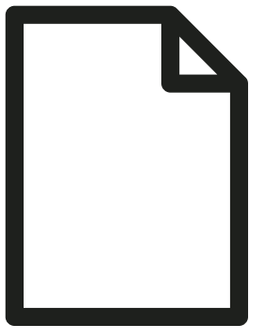
Chaum's voting protocol



Voter:

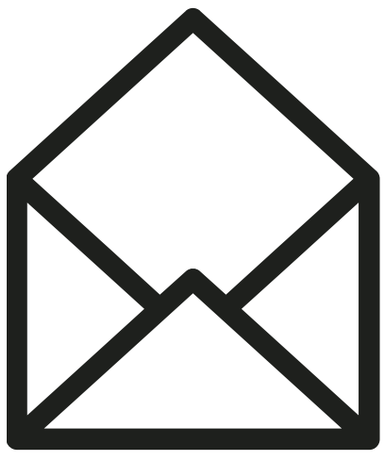
- Writes his vote.

Chaum's voting protocol



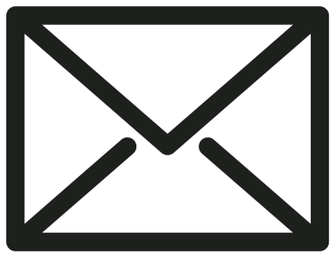
Voter:

- Writes his vote.



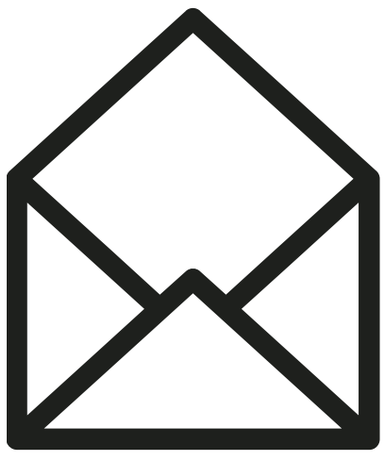
- Seals his vote in a blank envelope.

Chaum's voting protocol



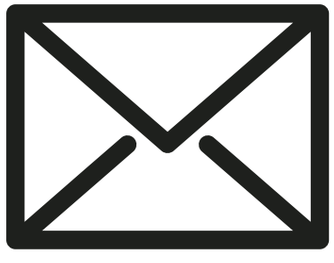
Voter:

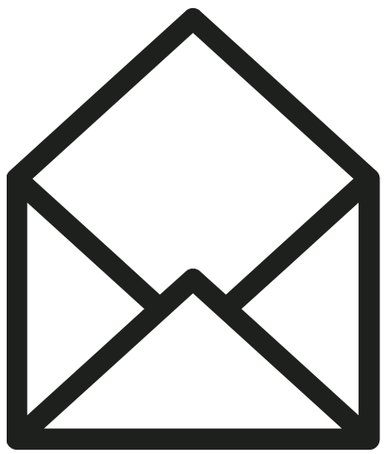
- Writes his vote.



- Seals his vote in a blank envelope.
- Sends sealed vote in another envelope with return address to trusted third party for signing.

Chaum's voting protocol

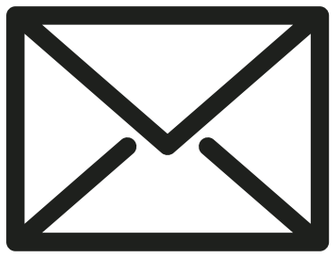




Third party, signing votes:

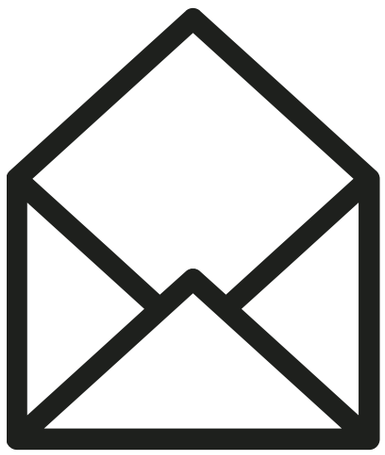
- Opens envelope with address and makes sure the sender is authorised to vote.
- Signs this envelope with the vote, without opening it.
- Sends signed vote in an envelope back to sender.

Chaum's voting protocol



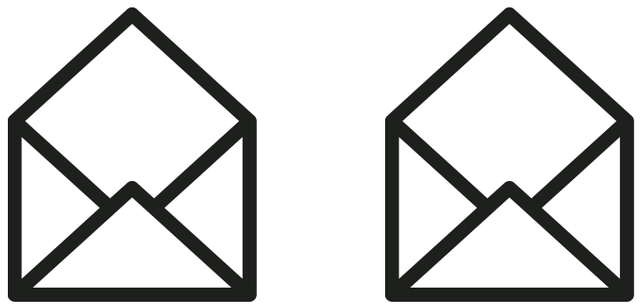
Voter:

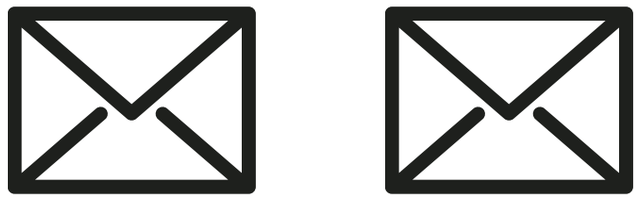
- Voter now has a signed vote.



- On voting day, he sends his signed vote in an envelope with no return address.

Chaum's voting protocol

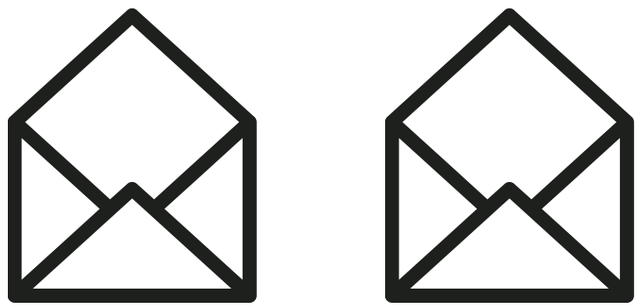


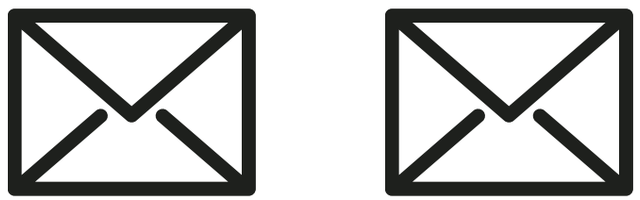


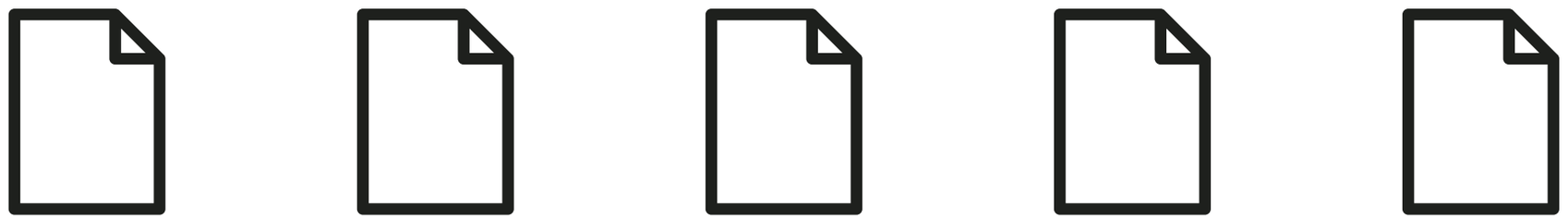
Third party, accepting votes:

- Accepts the votes if coming from authorised voters.

Chaum's voting protocol







Third party, accepting votes:

- Accepts the votes if coming from authorised voters.
- The votes can be counted and displayed to the public.
- The privacy of the sender is maintained and his vote is secret.

ROYAL INSTITUTE OF TECHNOLOGY

Blind signatures

- A third party can sign something without knowing everything.
- Bitcoin does not sign blindly, as transactions do get checked for correctness.

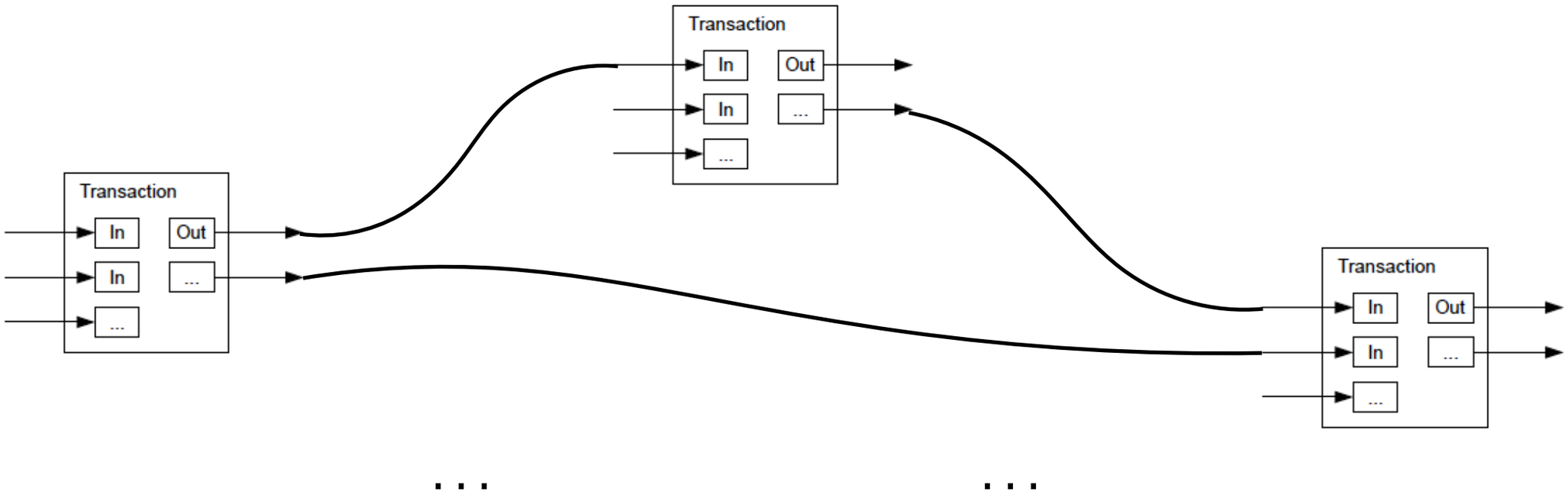
ROYAL INSTITUTE OF TECHNOLOGY

Bitcoin building blocks

- Currency
  - btc(bitcoin)
- Transaction
  - Transactions represent valid arcs between two system states.
  - Typically transactions are equivalent to financial transactions - moving currency between currency holders.
- Blockchain
  - A log of transactions - a list of all accepted transactions.

Bitcoin transactions

- Transactions can have multiple inputs and multiple outputs.



ROYAL INSTITUTE OF TECHNOLOGY

Bitcoin transactions

- An output contains :
  - An amount of bitcoins.
  - An identifier, which can be the public key of the recipient(hashed).
- An input contains:
  - a reference to an output from a previous transaction.
  - a signature of the sender to authorise the use of the output.

ROYAL INSTITUTE OF TECHNOLOGY

Bitcoin transactions

- An output can only be used once, as an input to a different transaction.
- The output values share the combined value of the inputs and cannot exceed it.
- Any input bitcoins not redeemed in an output is considered a transaction fee.

ROYAL INSTITUTE OF TECHNOLOGY

What **can** we distribute?

- The state - the blockchain.
- The operations - write or read of the blockchain.

ROYAL INSTITUTE OF TECHNOLOGY

What **do** we distribute?

- The state - the blockchain.
- **The operations** - write or read of the blockchain.

ROYAL INSTITUTE OF TECHNOLOGY

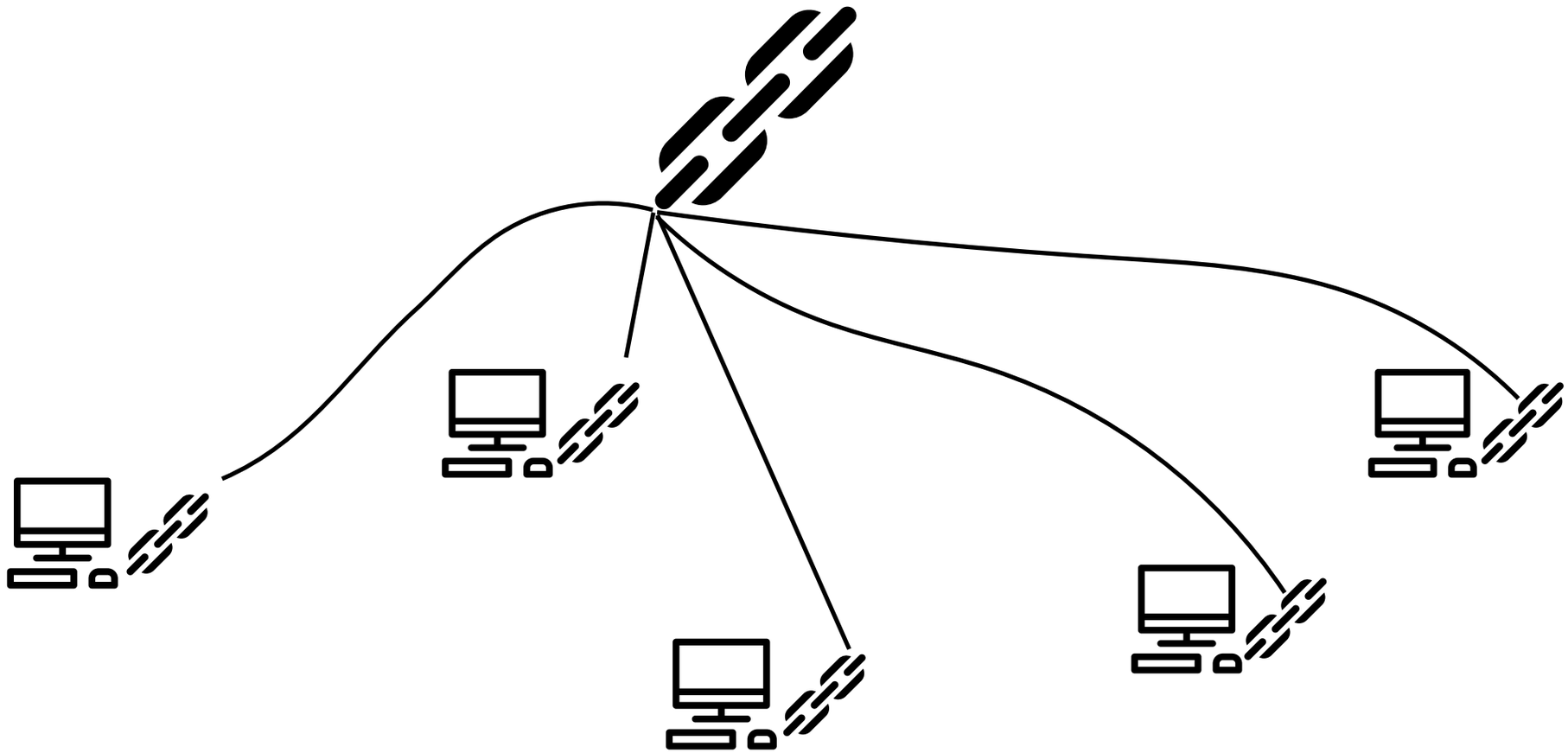
What **do** we distribute?

- The state - the blockchain.
- **The operations** - **write** or read of the blockchain.

ROYAL INSTITUTE OF TECHNOLOGY

How do we distribute?

- We replicate the whole blockchain on all interested peers.



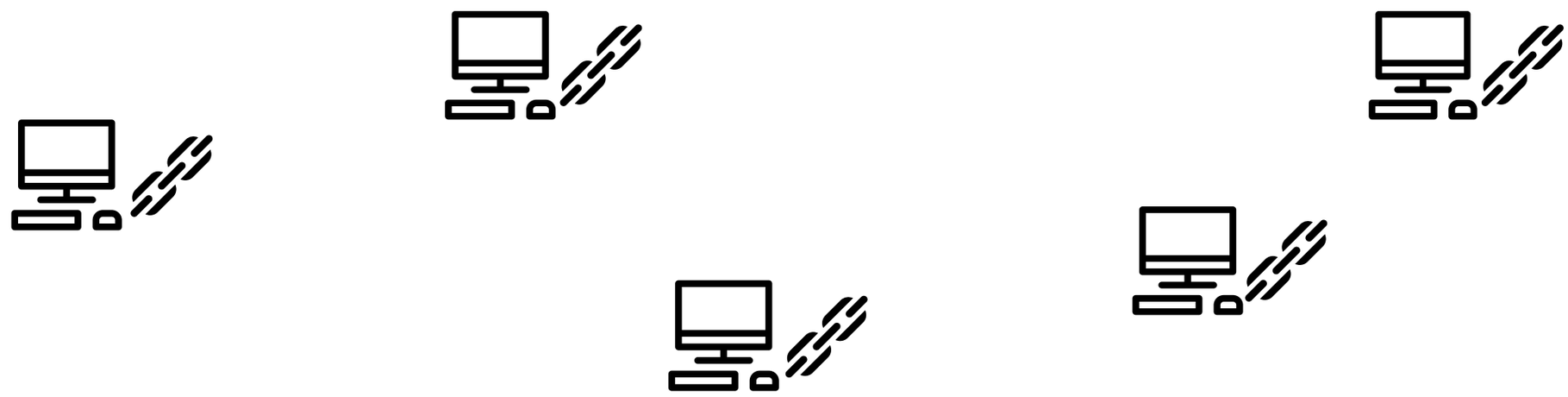
ROYAL INSTITUTE OF TECHNOLOGY

How do we distribute?

- We replicate the whole blockchain on all interested peers.
- Everyone can read in parallel from their local copy.

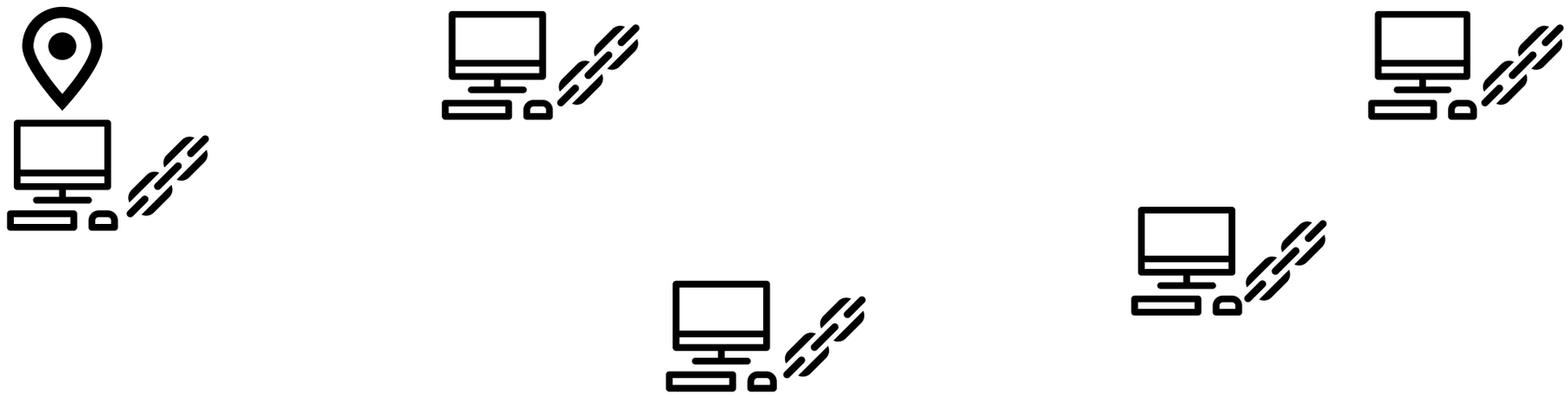
How do we distribute?

- Everyone can write.
- Writes are artificially expensive in order to avoid/deter collisions and to increase security.
- Writing is done by sending(flooding) the data to the neighbours.



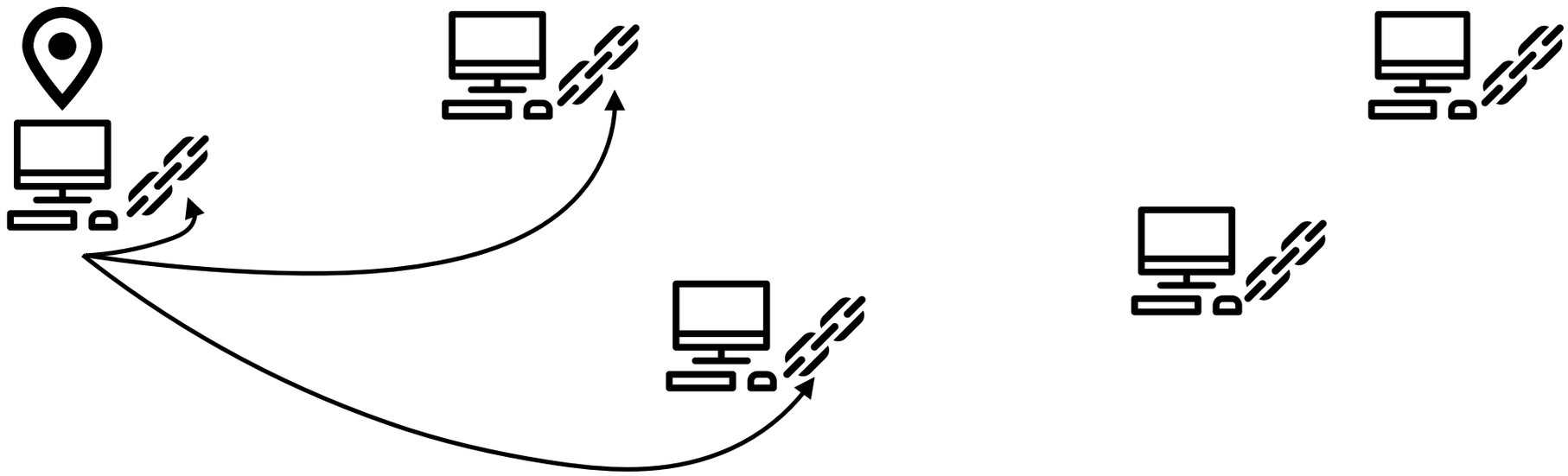
How do we distribute?

- Everyone can write.
- Writes are artificially expensive in order to avoid/deter collisions and to increase security.
- Writing is done by sending(flooding) the data to the neighbours.



How do we distribute?

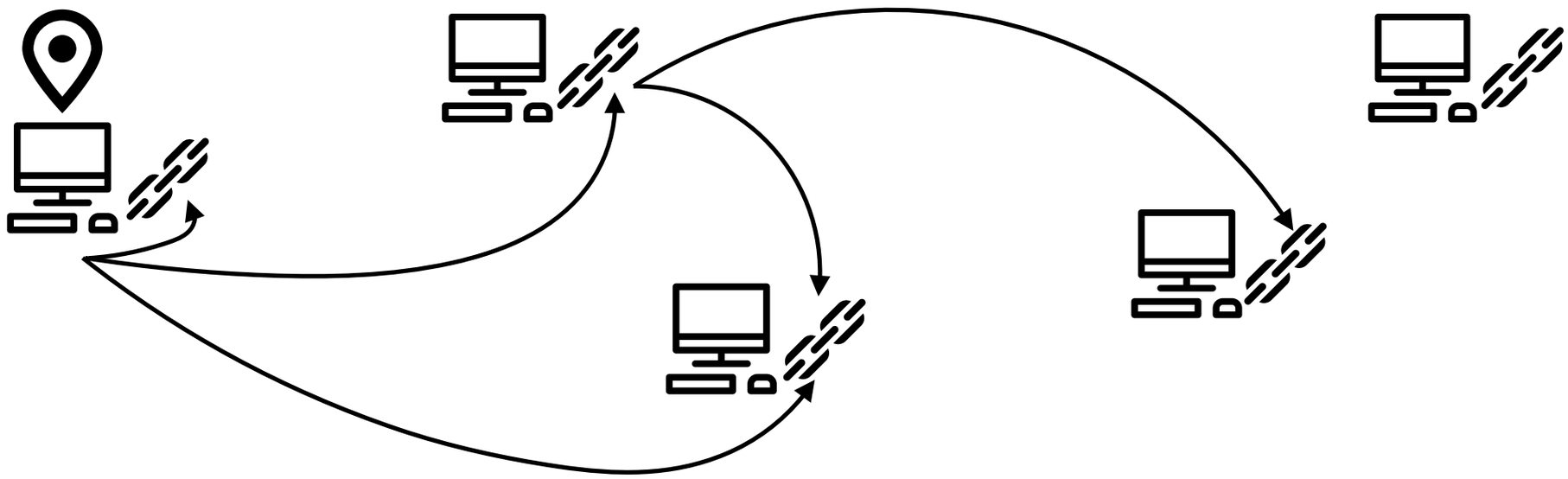
- Everyone can write.
- Writes are artificially expensive in order to avoid/deter collisions and to increase security.
- Writing is done by sending(flooding) the data to the neighbours.



ROYAL INSTITUTE OF TECHNOLOGY

How do we distribute?

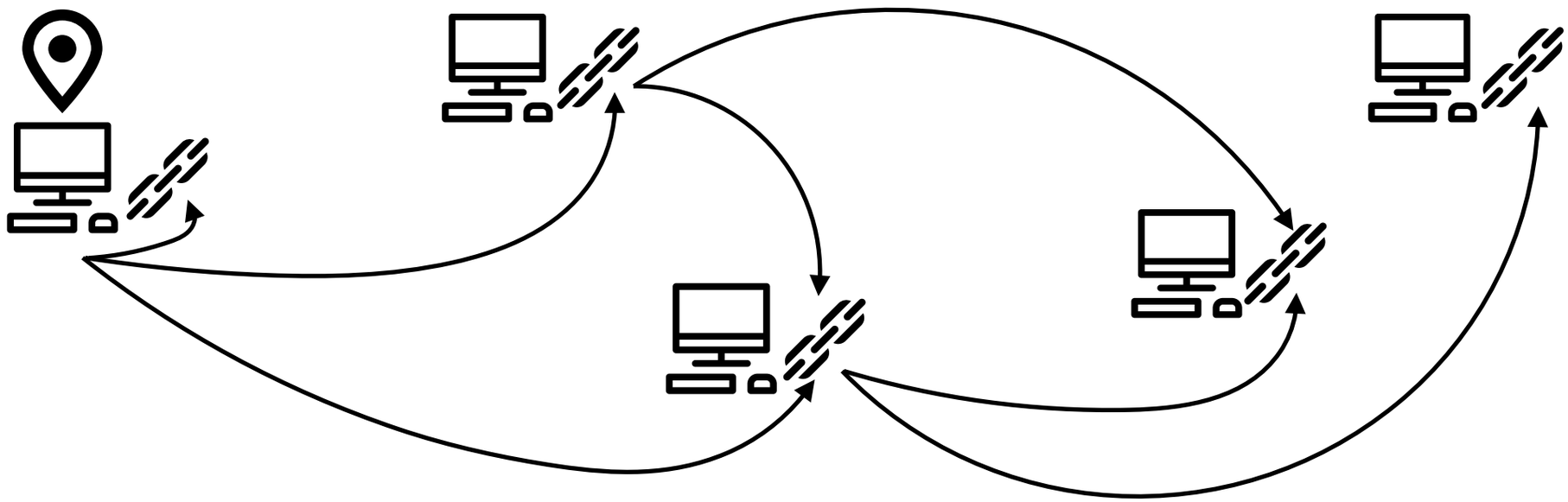
- Everyone can write.
- Writes are artificially expensive in order to avoid/deter collisions and to increase security.
- Writing is done by sending(flooding) the data to the neighbours.



ROYAL INSTITUTE OF TECHNOLOGY

How do we distribute?

- Everyone can write.
- Writes are artificially expensive in order to avoid/deter collisions and to increase security.
- Writing is done by sending(flooding) the data to the neighbours.



ROYAL INSTITUTE OF TECHNOLOGY

How de we make writes expensive?

- Hashcash, proposed in 1997 by Adam Back, is a proof-of-work algorithm that

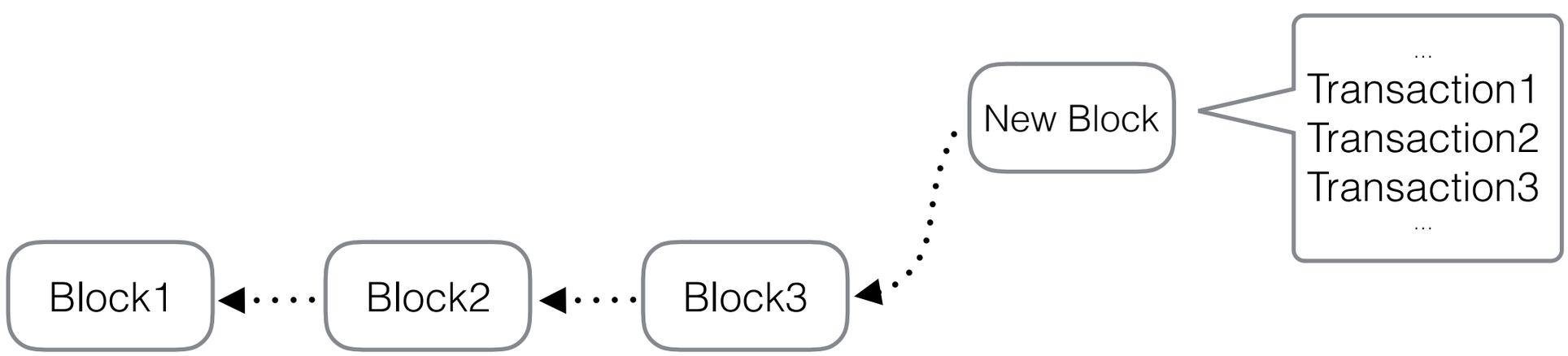
- A proof of work is a piece of data that costs a lot to produce(time, knowledge or other resources) but is easy to be verified as valid.

- Producing a proof of work can be a random process with low probability, requiring a lot of trial and error

ROYAL INSTITUTE OF TECHNOLOGY

Blocks

- Writes in the blockchain are computationally expensive, so multiple transactions are batched into a block.
- Blocks get written into the blockchain and not transactions.
- The blockchain is thus a linear sequence of blocks.



ROYAL INSTITUTE OF TECHNOLOGY

Block contents

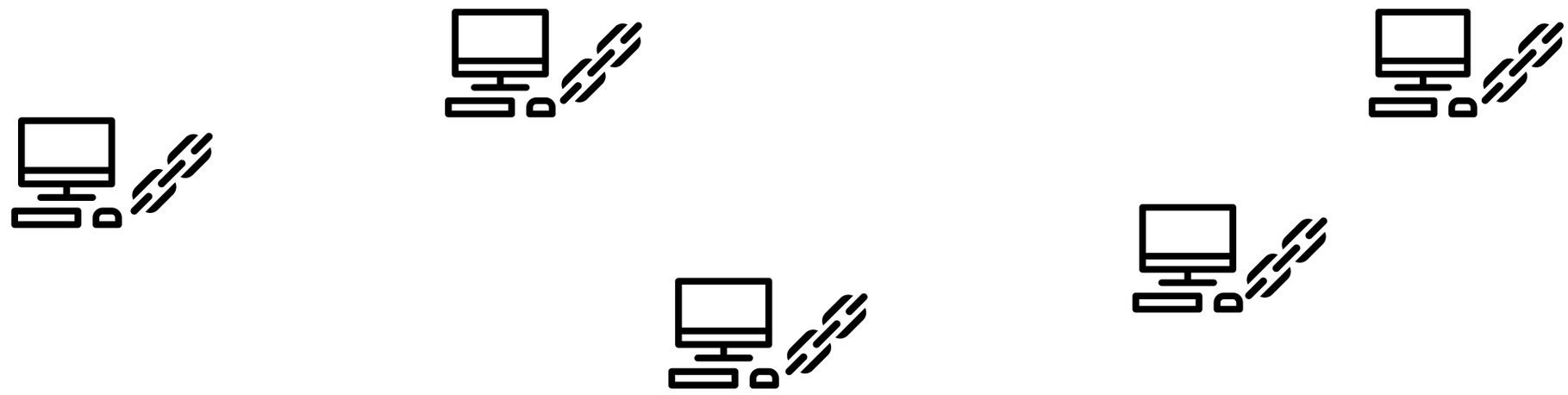
- Each block contains, among other things:
  - a record of some or all recent transactions.
  - a reference to the block that came immediately before it.
  - the proof of work, which is unique to each block and depends on the contents of the block.

ROYAL INSTITUTE OF TECHNOLOGY

Publishing transactions

- If A wants to send a payment to B, a transaction is created with:
  - an input pointing to an amount of A's bitcoins.
  - an output pointing to B and the amount to transfer.
  - an output pointing back to A with the rest of the bitcoins.

- The transaction is sent into the Bitcoin network.

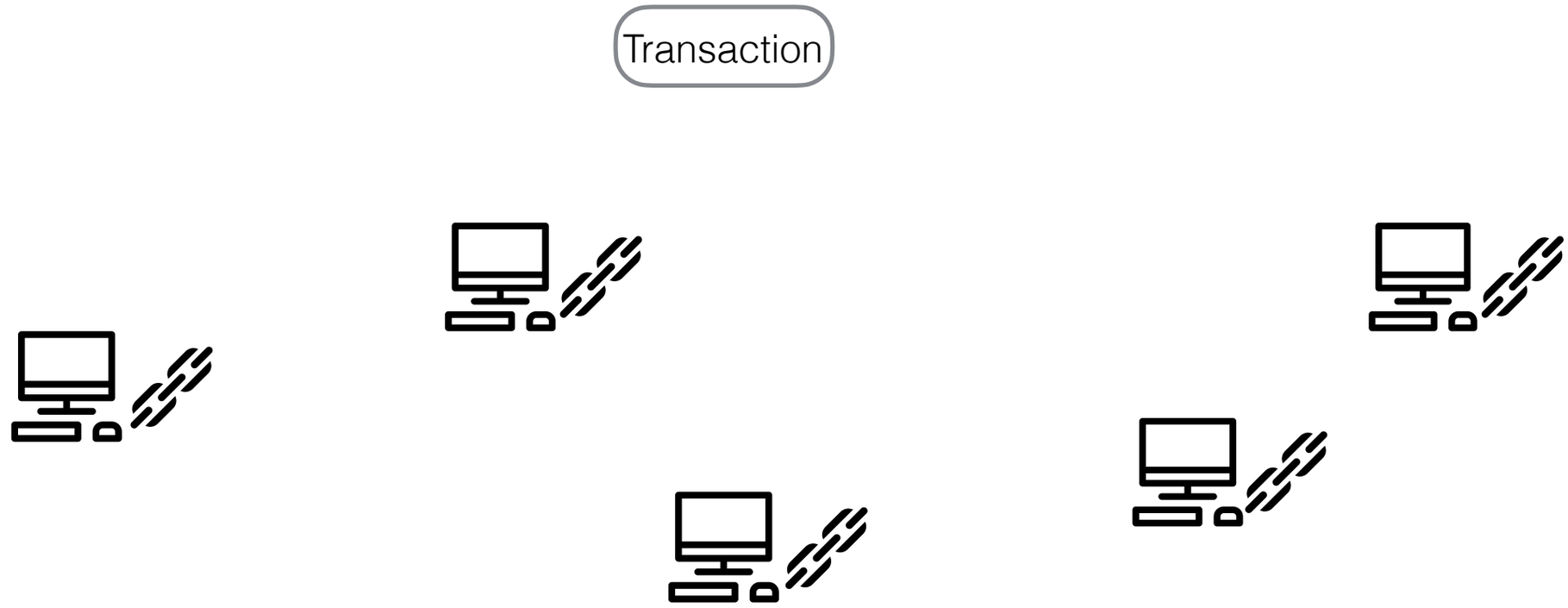


ROYAL INSTITUTE OF TECHNOLOGY

Publishing transactions

- If A wants to send a payment to B, a transaction is created with:
  - an input pointing to an amount of A's bitcoins.
  - an output pointing to B and the amount to transfer.
  - an output pointing back to A with the rest of the bitcoins.

- The transaction is sent into the Bitcoin network.

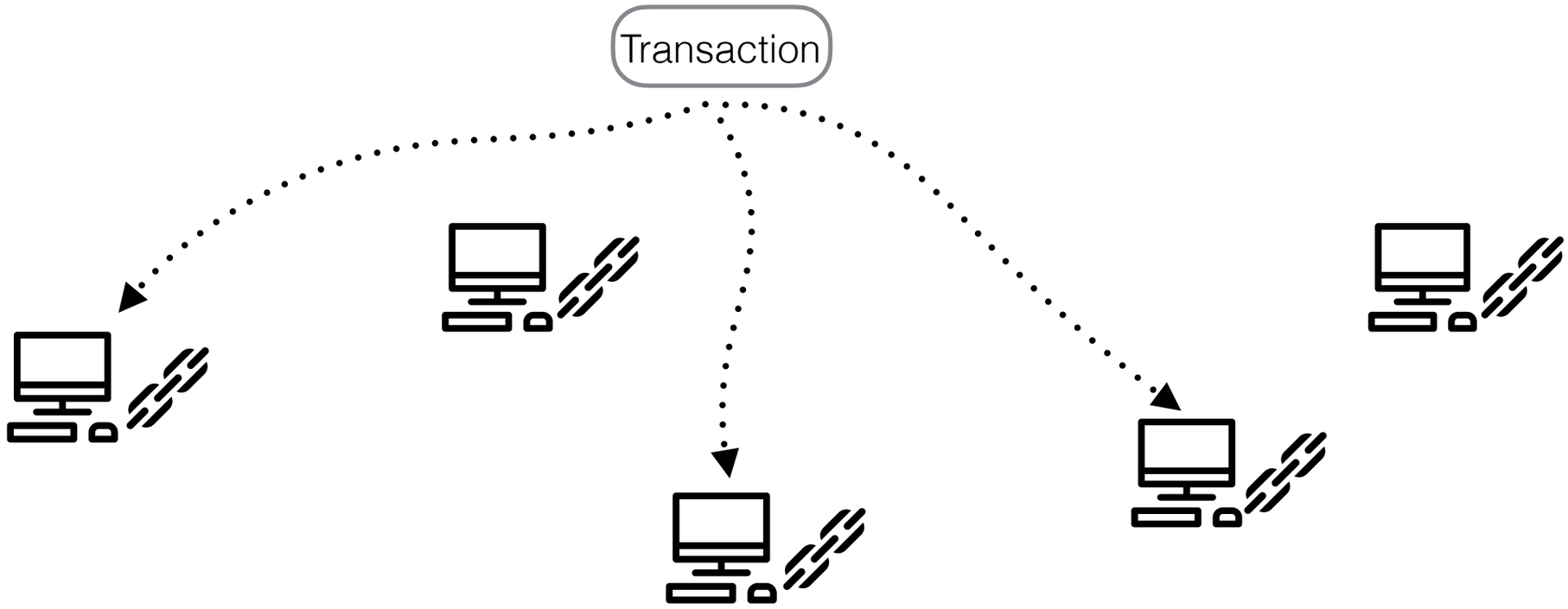


ROYAL INSTITUTE OF TECHNOLOGY

Publishing transactions

- If A wants to send a payment to B, a transaction is created with:
  - an input pointing to an amount of A's bitcoins.
  - an output pointing to B and the amount to transfer.
  - an output pointing back to A with the rest of the bitcoins.

- The transaction is sent into the Bitcoin network.

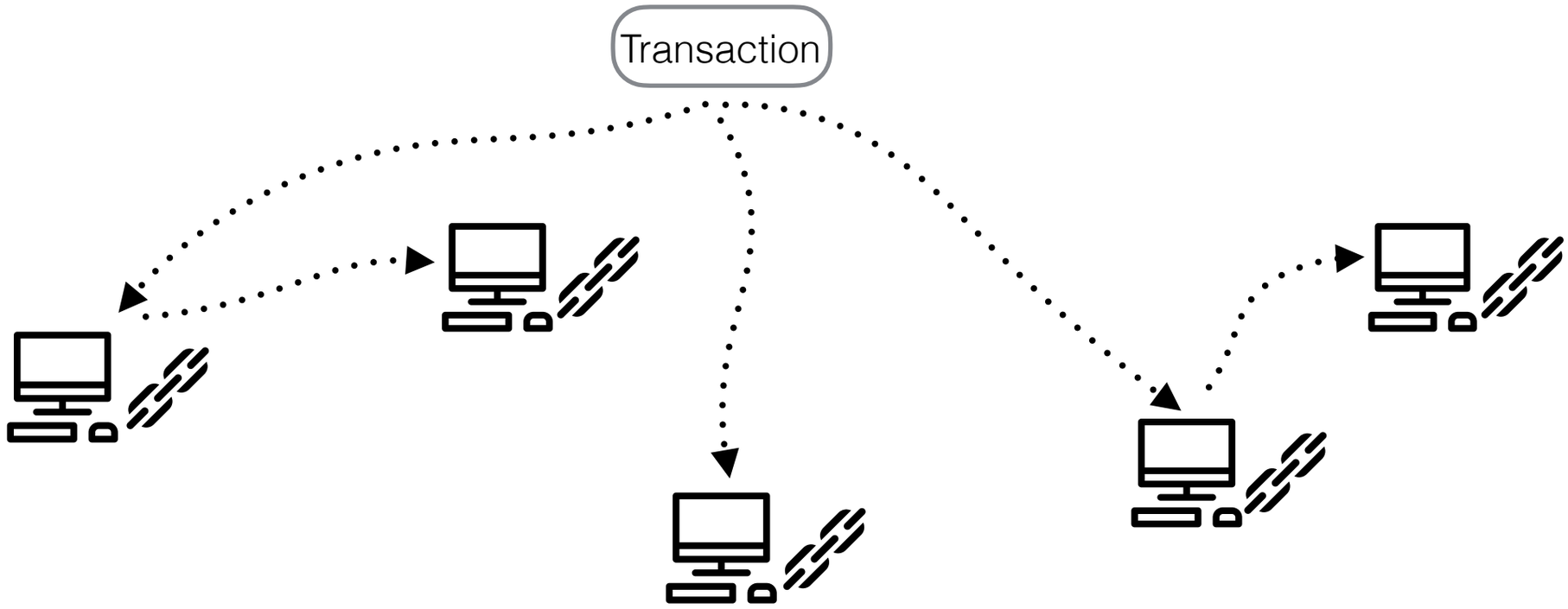


ROYAL INSTITUTE OF TECHNOLOGY

Publishing transactions

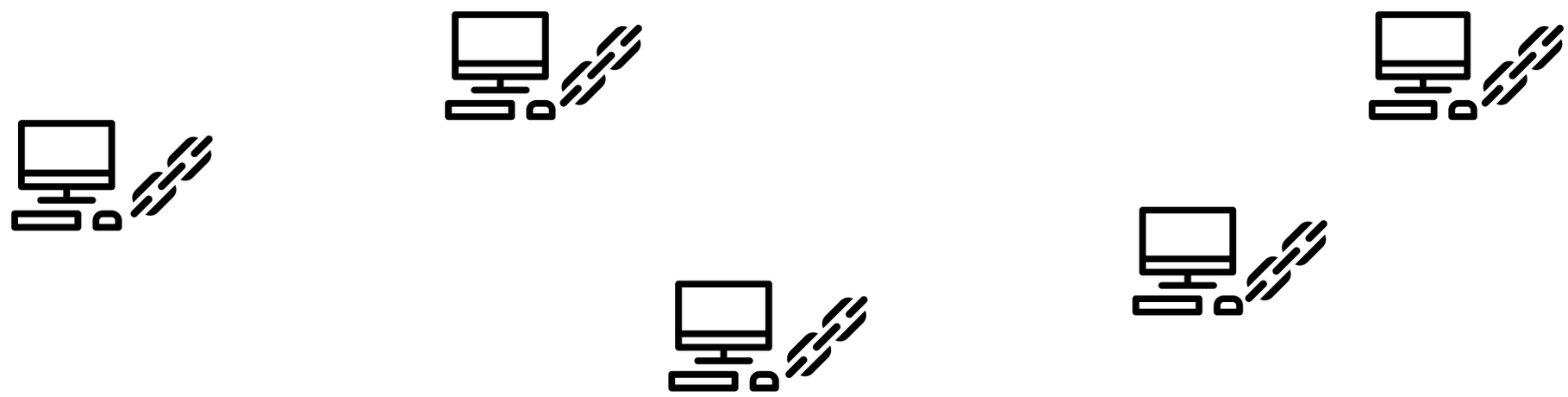
- If A wants to send a payment to B, a transaction is created with:
  - an input pointing to an amount of A's bitcoins.
  - an output pointing to B and the amount to transfer.
  - an output pointing back to A with the rest of the bitcoins.

- The transaction is sent into the Bitcoin network.



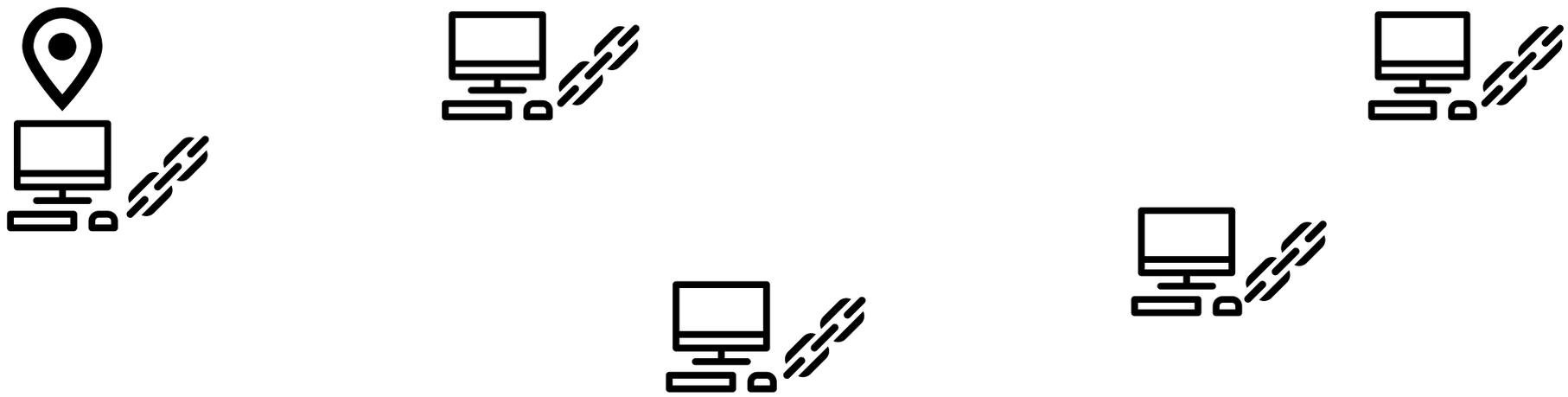
Publishing transactions

- The participants(A and **B**) wait for a miner to write it into the blockchain.



Publishing transactions

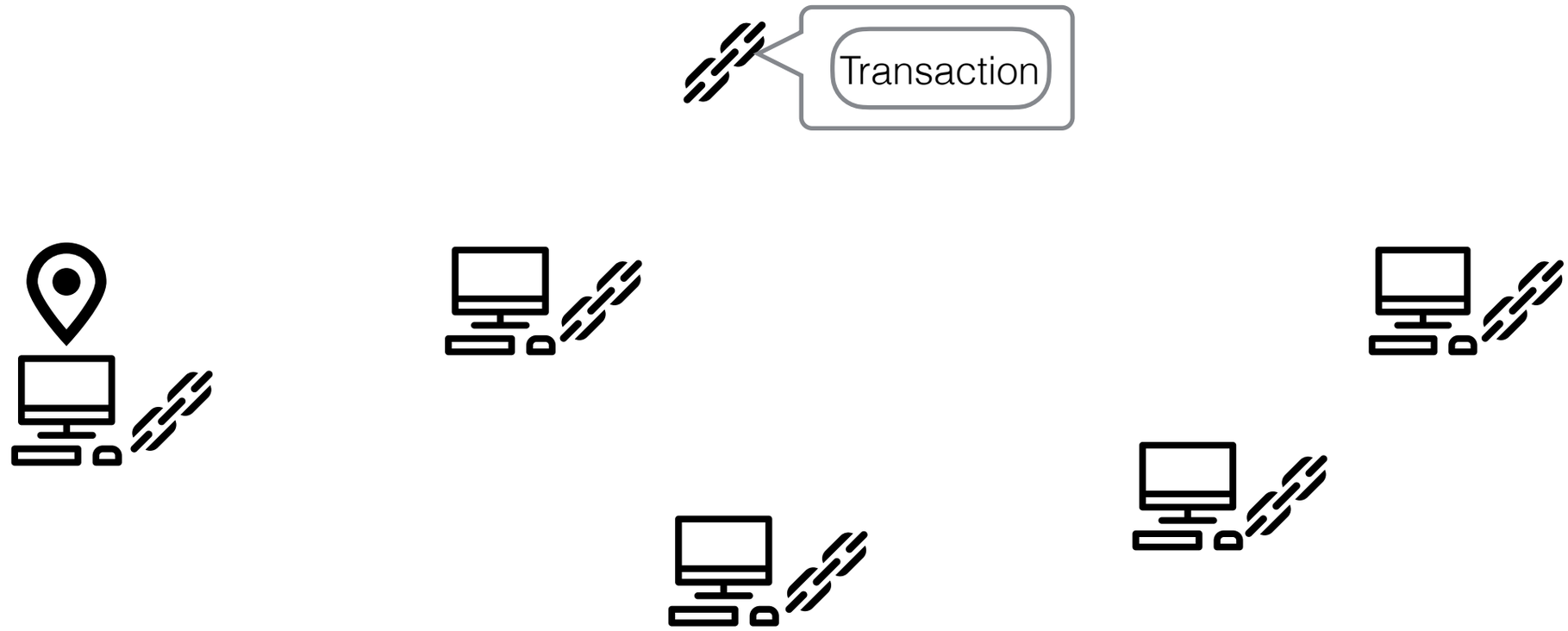
- The participants(A and **B**) wait for a miner to write it into the blockchain.



Publishing transactions

- The participants(A and **B**) wait for a miner to write it into the blockchain.

- B observe's the blockchain and when it sees the transaction as part of it, it acknowledges the transaction's finalisation.



ROYAL INSTITUTE OF TECHNOLOGY

Mining

- New blocks can only be submitted to the network and thus appended to the blockchain with the correct proof of work.
- The puzzle(proof of work) is dependent on the parent block and the transactions included.
- "Mining" is essentially the process of competing to be the next to find the answer that "solves" the current puzzle.
- There are multiple valid solutions for any given block - only one of the solutions needs to be found for the block to be solved.

ROYAL INSTITUTE OF TECHNOLOGY

Why mine?

- Every transaction has a processing fee.
- Bitcoins are also “minted” with the creation of each block(up to a max amount).
- The first miner to publish a block gets to collect the fees and the minted coins.

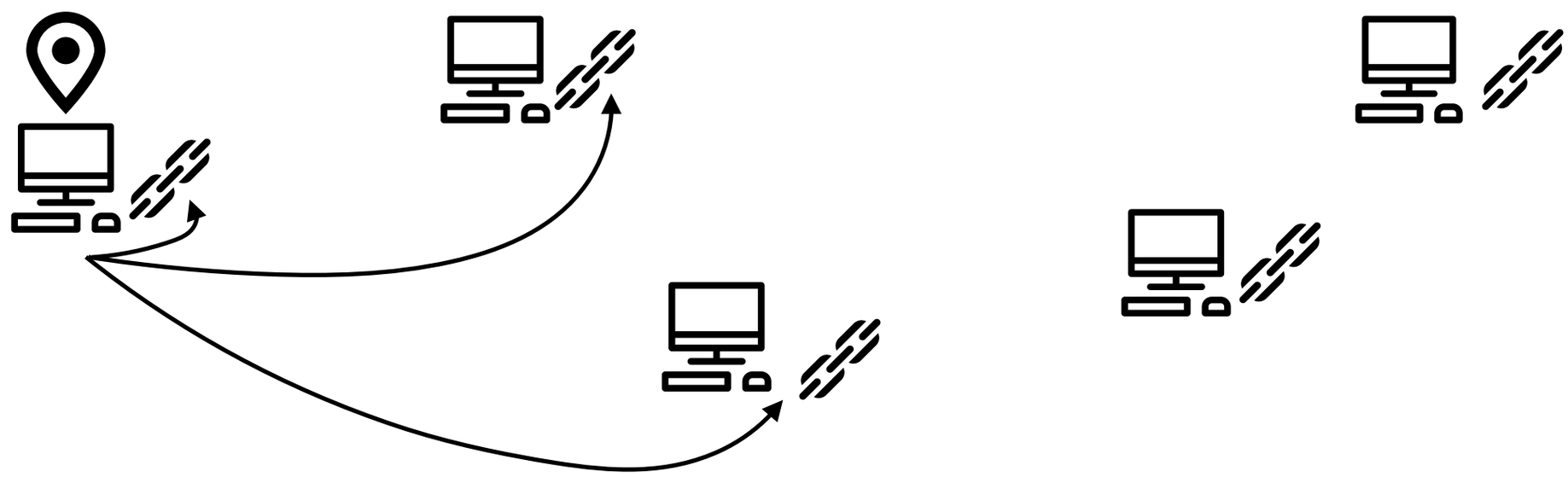
Forks and branches

- What happens if two solutions are found around the same time?
- Both blocks get propagated and accepted if it make the local blockchain longer

ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

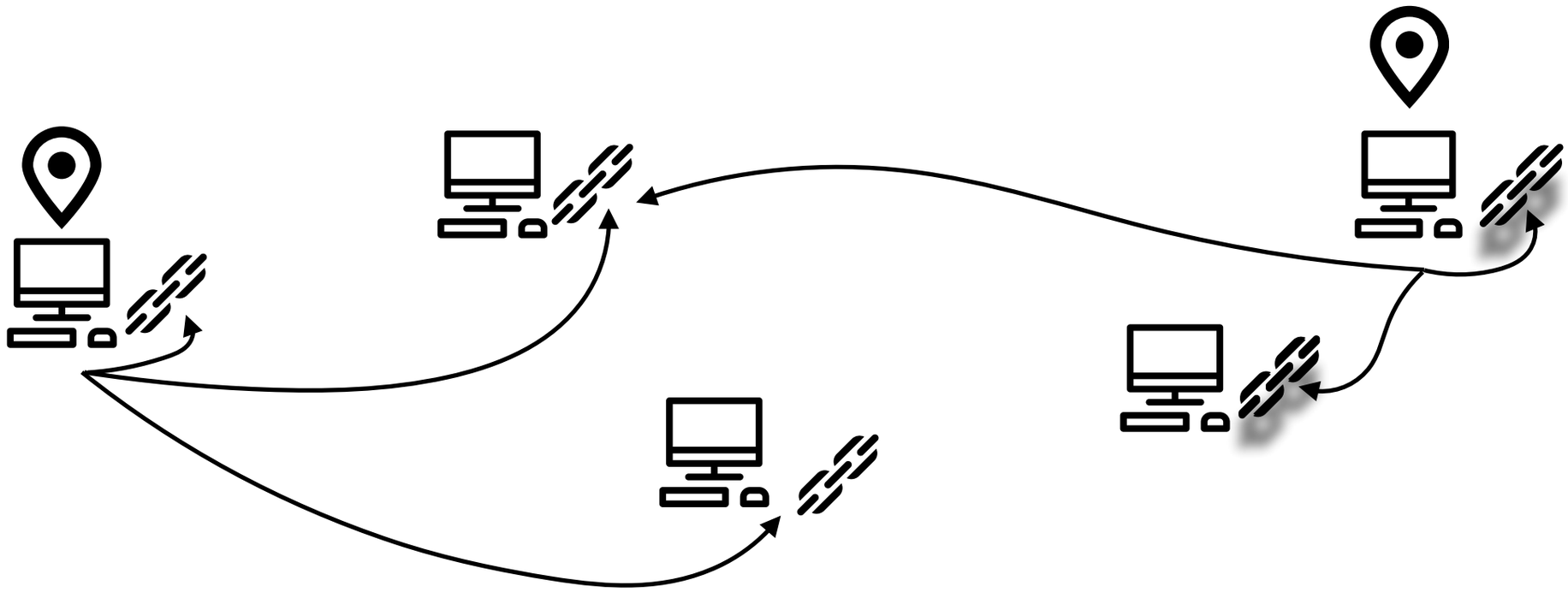
- What happens if two solutions are found around the same time?
- Both blocks get propagated and accepted if it make the local blockchain longer



ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

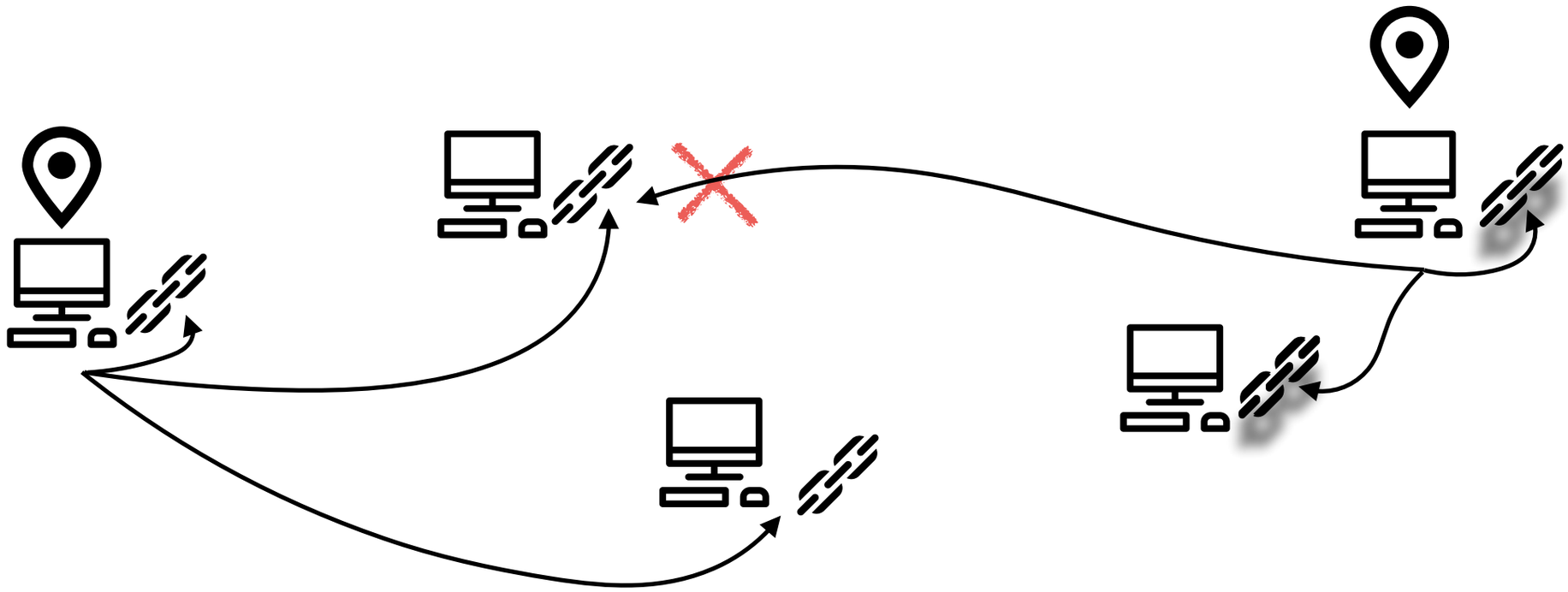
- What happens if two solutions are found around the same time?
- Both blocks get propagated and accepted if it make the local blockchain longer



ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

- What happens if two solutions are found around the same time?
- Both blocks get propagated and accepted if it make the local blockchain longer



ROYAL INSTITUTE OF TECHNOLOGY

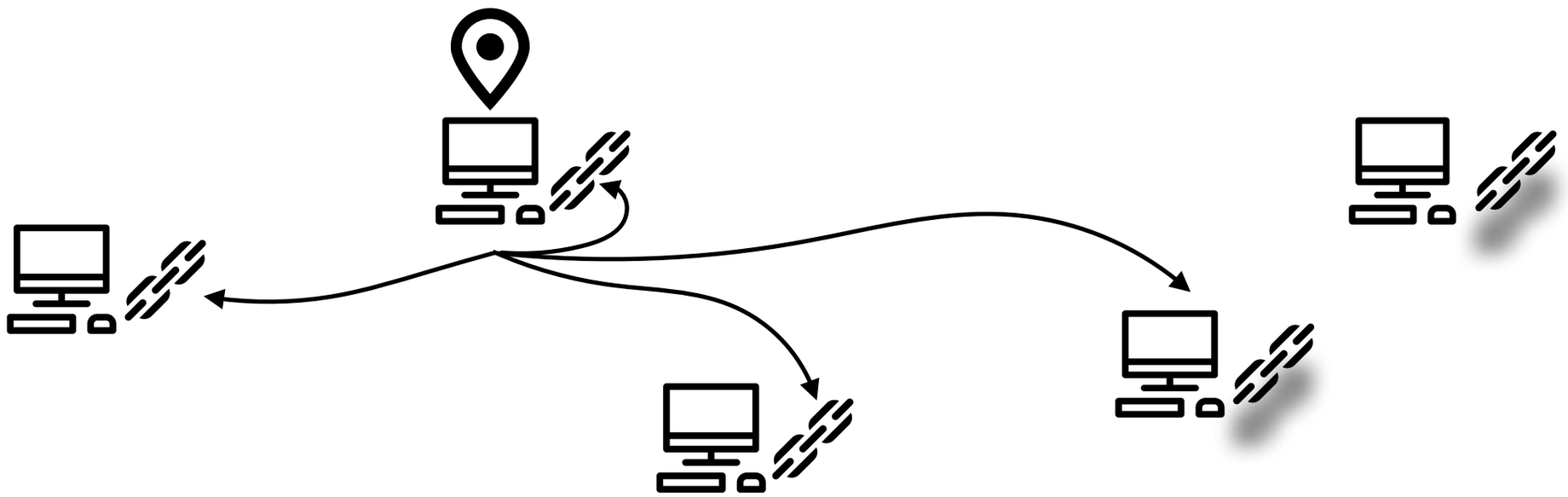
Forks and branches

- There is an incentive in the algorithm to work on the longest blockchain.
- Thus, it depends on which block gets higher acceptance and which fork grows faster.
- In the end only one solution is accepted as true and the other one is invalidated.

ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

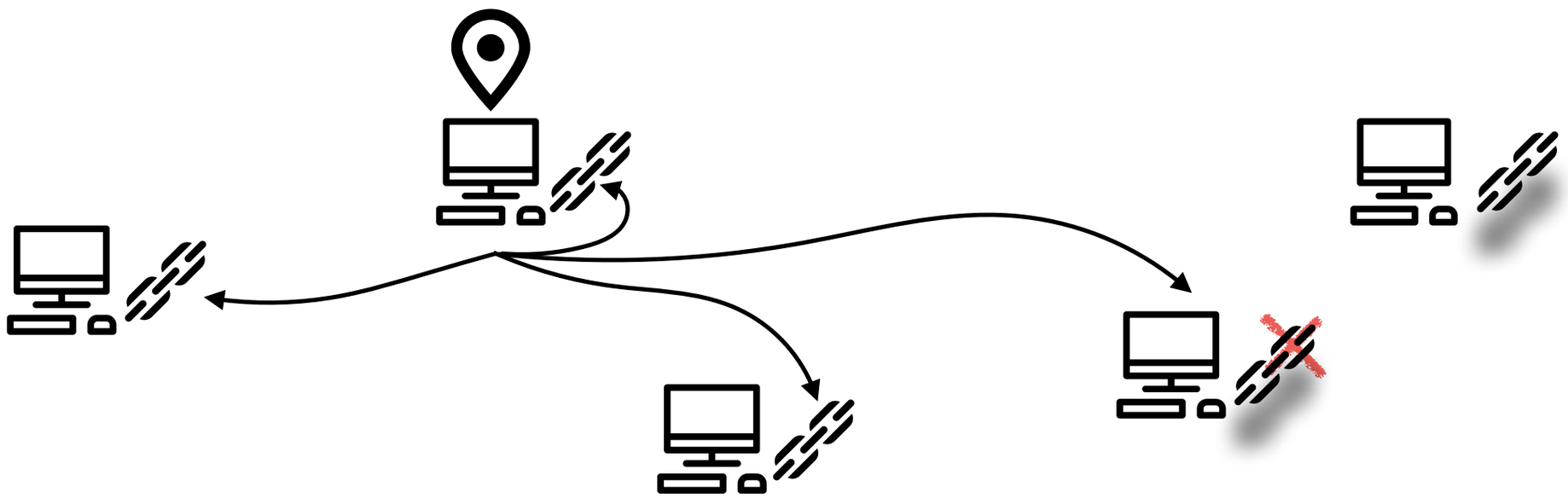
- There is an incentive in the algorithm to work on the longest blockchain.
- Thus, it depends on which block gets higher acceptance and which fork grows faster.
- In the end only one solution is accepted as true and the other one is invalidated.



ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

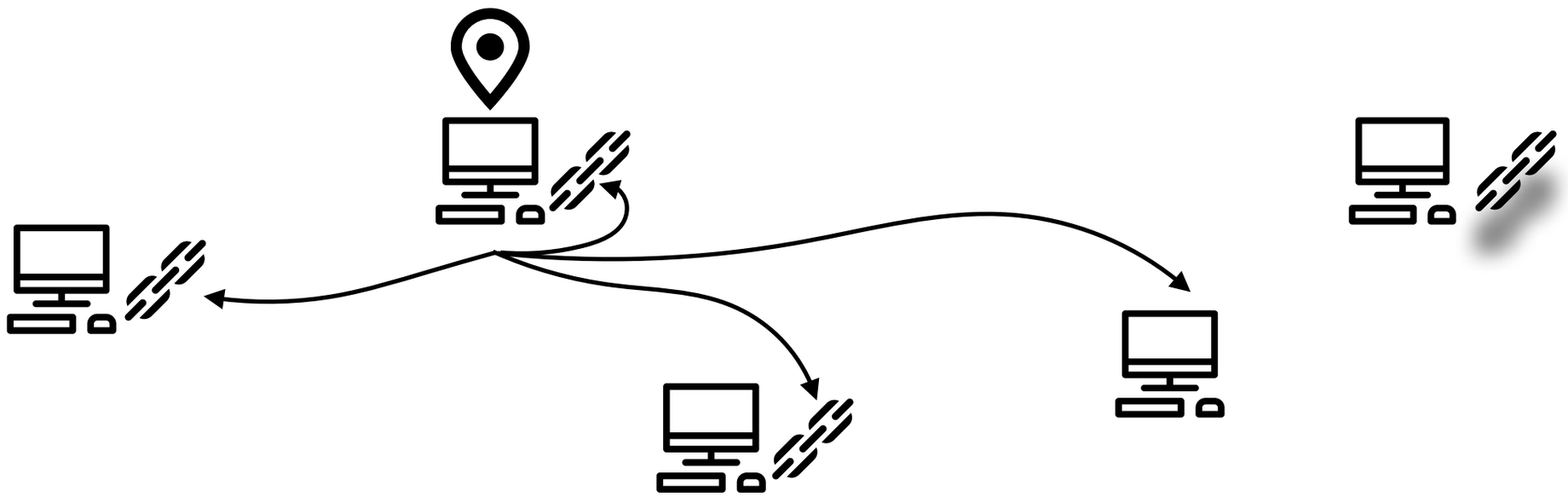
- There is an incentive in the algorithm to work on the longest blockchain.
- Thus, it depends on which block gets higher acceptance and which fork grows faster.
- In the end only one solution is accepted as true and the other one is invalidated.



ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

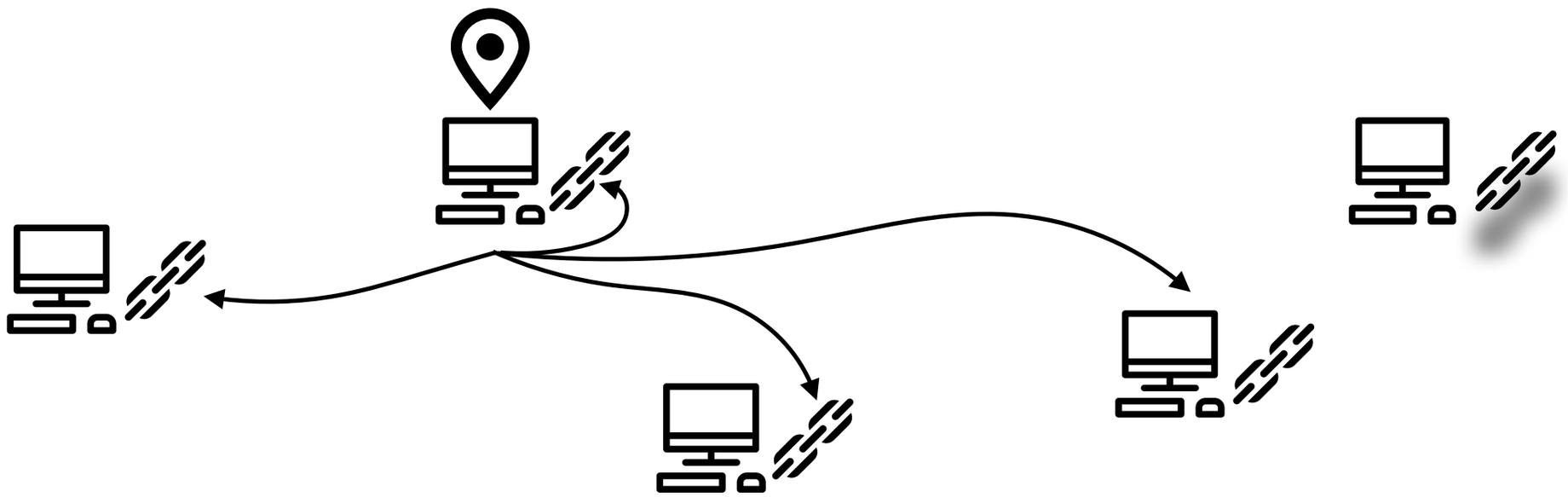
- There is an incentive in the algorithm to work on the longest blockchain.
- Thus, it depends on which block gets higher acceptance and which fork grows faster.
- In the end only one solution is accepted as true and the other one is invalidated.



ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

- There is an incentive in the algorithm to work on the longest blockchain.
- Thus, it depends on which block gets higher acceptance and which fork grows faster.
- In the end only one solution is accepted as true and the other one is invalidated.



ROYAL INSTITUTE OF TECHNOLOGY

Forks and branches

- Due to the format of the block generation function in Bitcoin, the probability of two or more different blocks being mined at the same time is very small and the network corrects itself.

- Bitcoin is however vulnerable to an attack because of this, where the fork does not appear by chance, but the attacker forces it to appear.

ROYAL INSTITUTE OF TECHNOLOGY

Wait! My transaction!

- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.

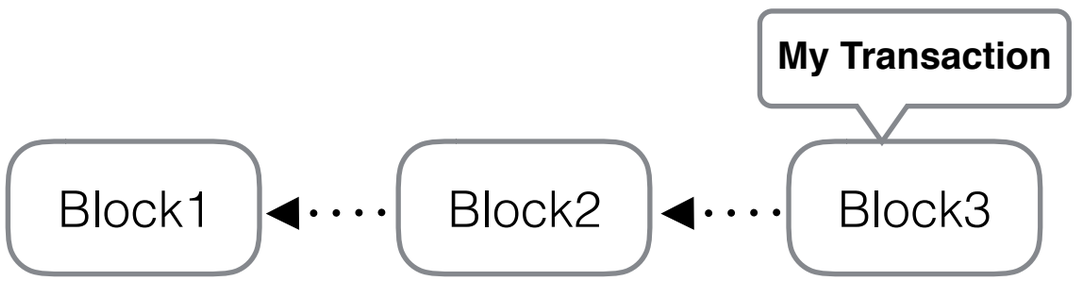
ROYAL INSTITUTE OF TECHNOLOGY

Wait! My transaction!

- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.

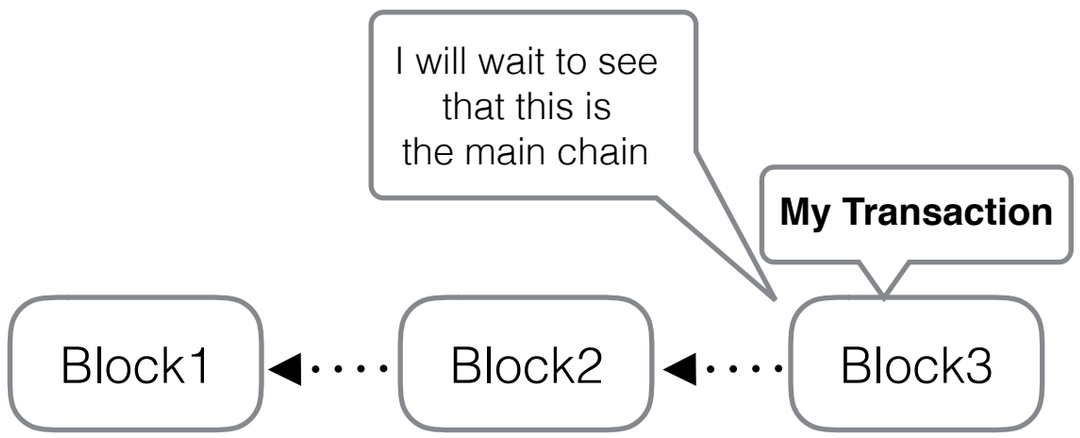
Wait! My transaction!

- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.



Wait! My transaction!

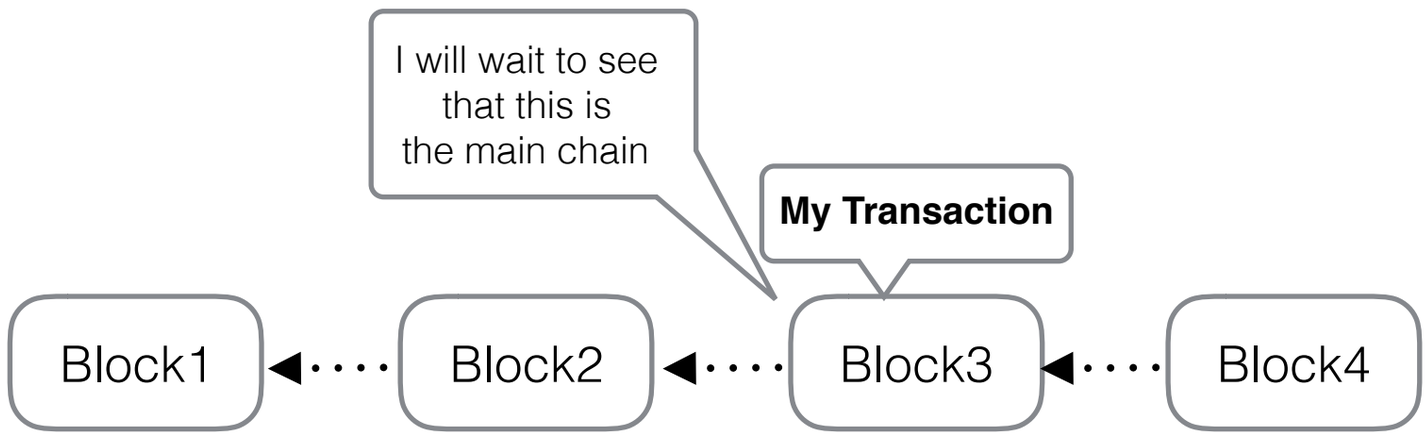
- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.



ROYAL INSTITUTE OF TECHNOLOGY

Wait! My transaction!

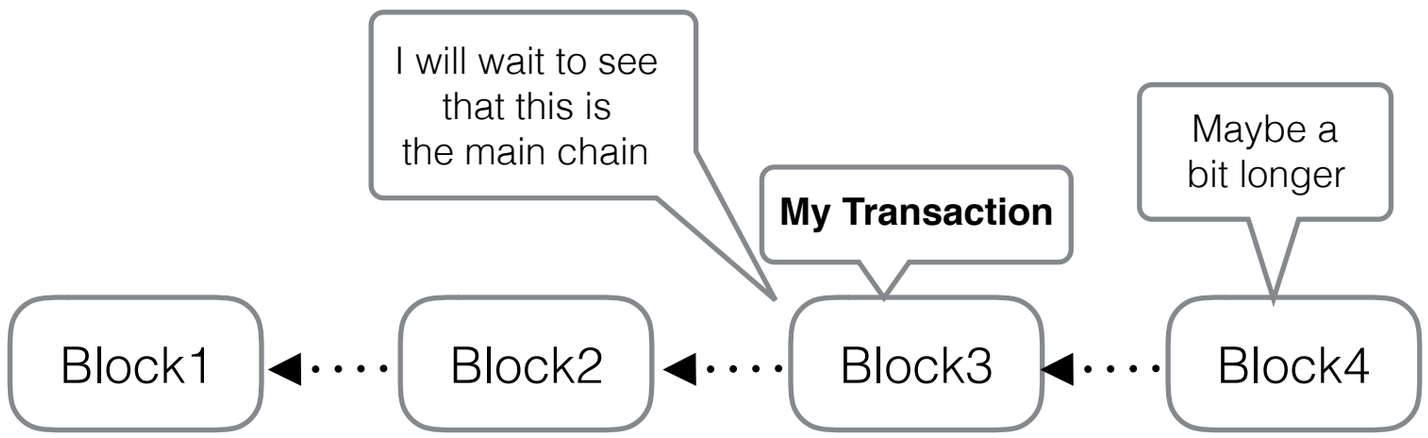
- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.



ROYAL INSTITUTE OF TECHNOLOGY

Wait! My transaction!

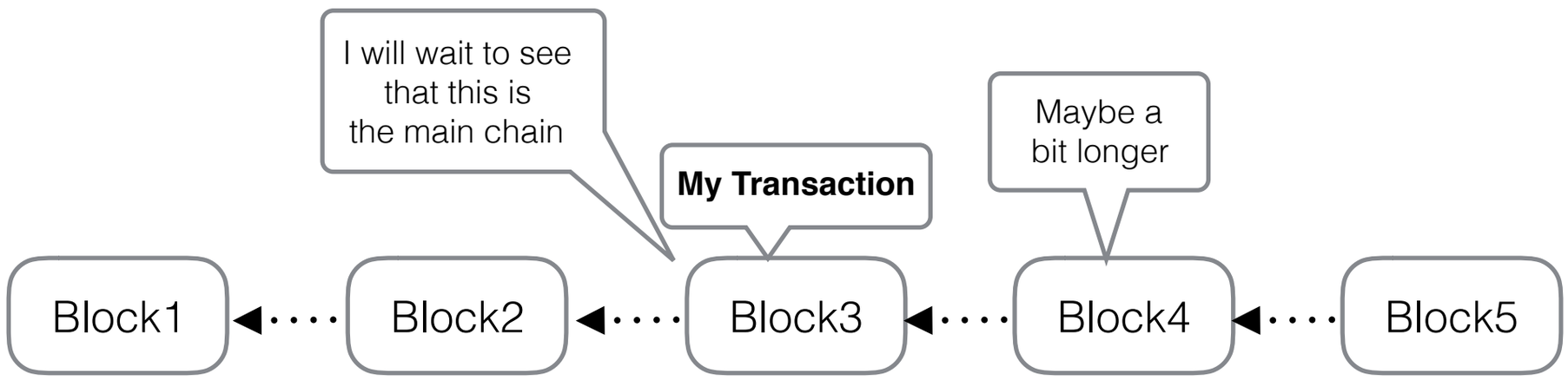
- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.



ROYAL INSTITUTE OF TECHNOLOGY

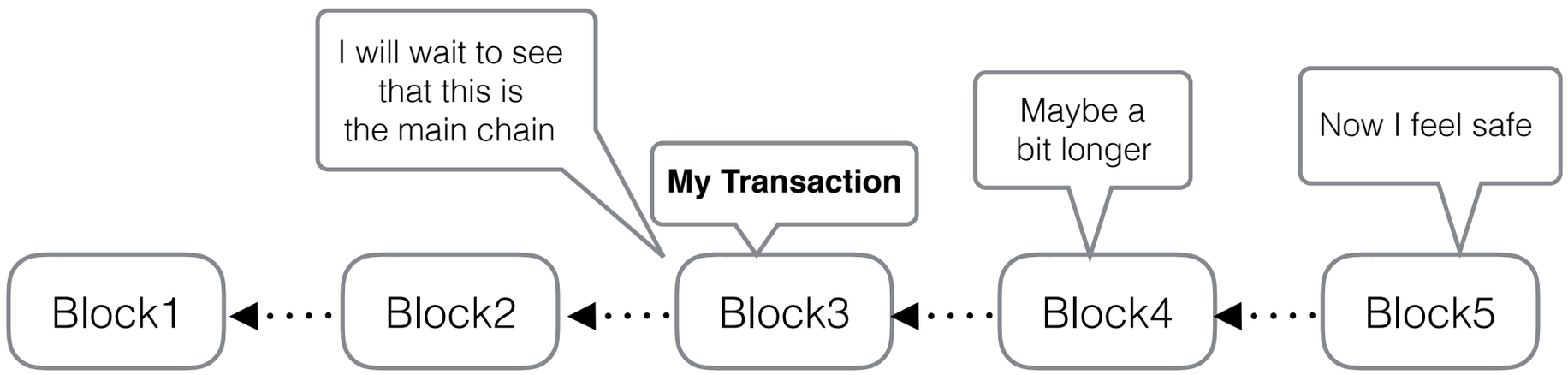
Wait! My transaction!

- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.



Wait! My transaction!

- We said before that the recipient of a transaction waits until it sees it's transaction into a block of the blockchain.
- Bitcoin is a probabilistic protocol. You have to see your transaction in the blockchain and then some more blocks appended to it.
- You are always only "fairly" certain the block is part of the longest chain and thus final.



ROYAL INSTITUTE OF TECHNOLOGY

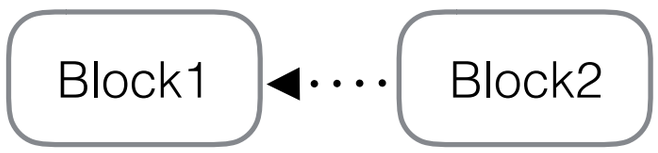
Double spending attack

- A double-spending attack is in fact a successful attempt to convince a merchant(the receiver of payment) that a transaction has been confirmed, and then convince the entire network to invalidate the branch by creating a longer correct branch.
- The merchant would be left with neither product nor coins, and the attacker will get to keep both.

ROYAL INSTITUTE OF TECHNOLOGY

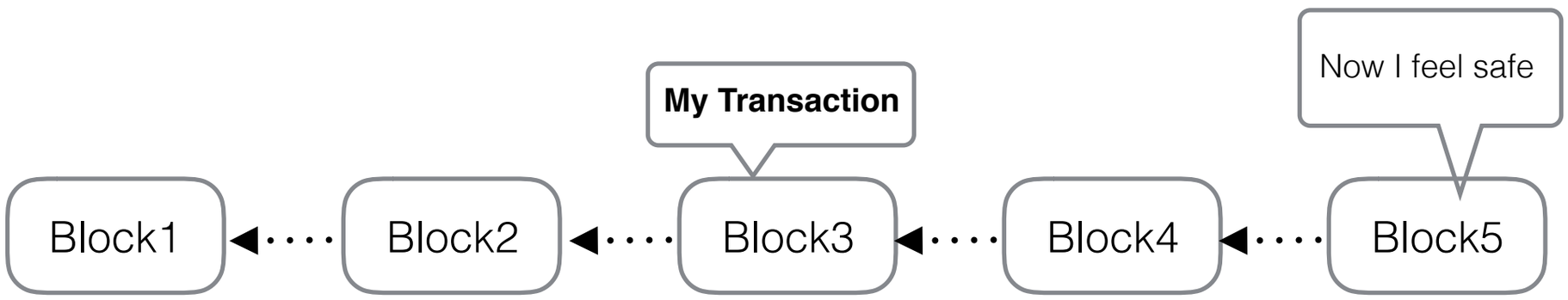
Double spending attack

- A double-spending attack is in fact a successful attempt to convince a merchant(the receiver of payment) that a transaction has been confirmed, and then convince the entire network to invalidate the branch by creating a longer correct branch.
- The merchant would be left with neither product nor coins, and the attacker will get to keep both.



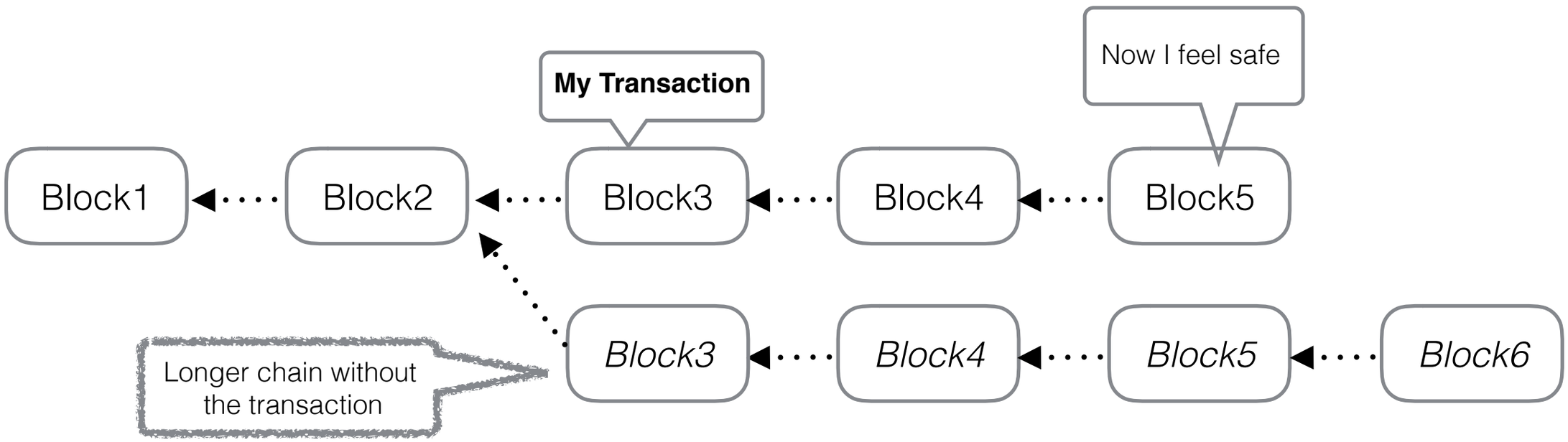
Double spending attack

- A double-spending attack is in fact a successful attempt to convince a merchant(the receiver of payment) that a transaction has been confirmed, and then convince the entire network to invalidate the branch by creating a longer correct branch.
- The merchant would be left with neither product nor coins, and the attacker will get to keep both.



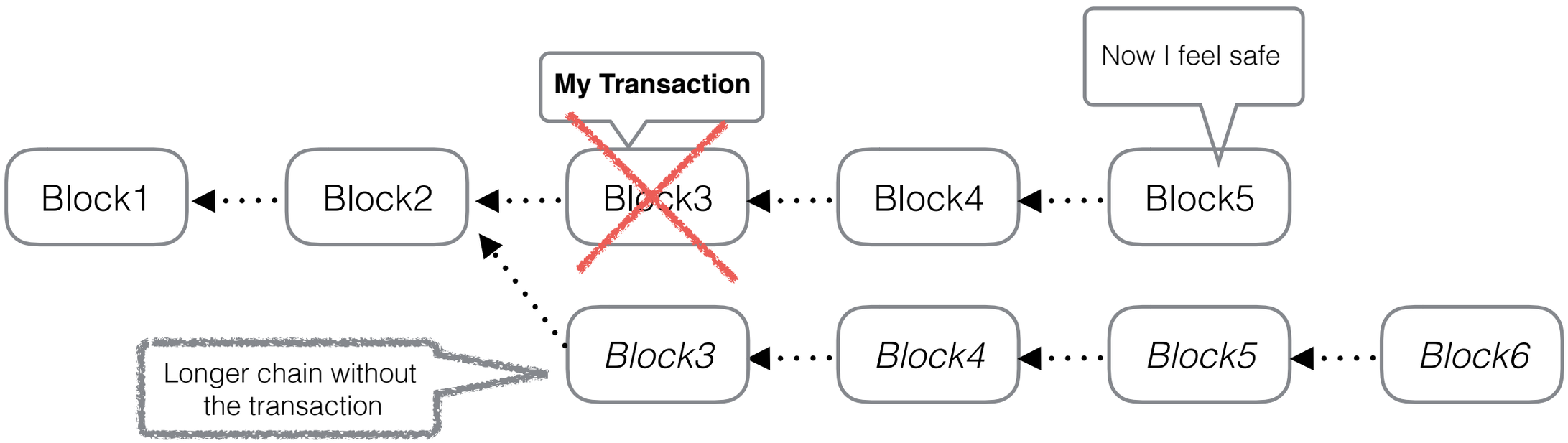
Double spending attack

- A double-spending attack is in fact a successful attempt to convince a merchant(the receiver of payment) that a transaction has been confirmed, and then convince the entire network to invalidate the branch by creating a longer correct branch.
- The merchant would be left with neither product nor coins, and the attacker will get to keep both.



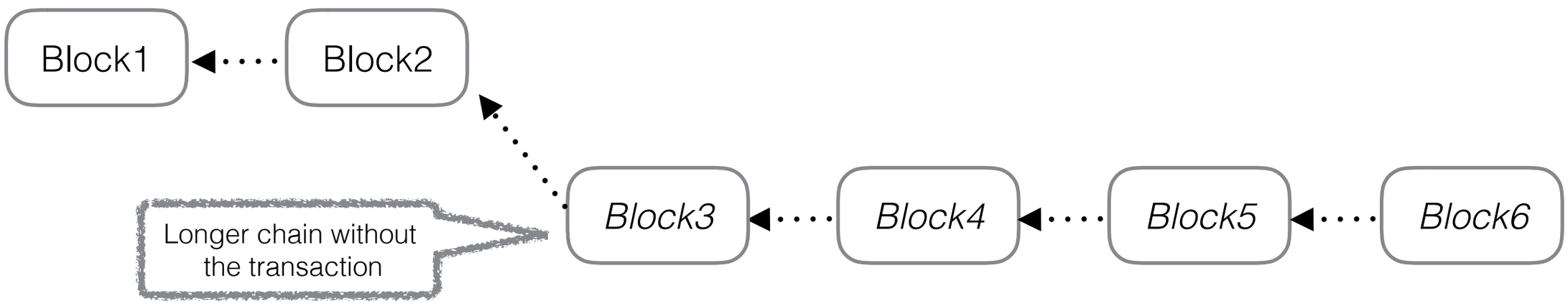
Double spending attack

- A double-spending attack is in fact a successful attempt to convince a merchant(the receiver of payment) that a transaction has been confirmed, and then convince the entire network to invalidate the branch by creating a longer correct branch.
- The merchant would be left with neither product nor coins, and the attacker will get to keep both.



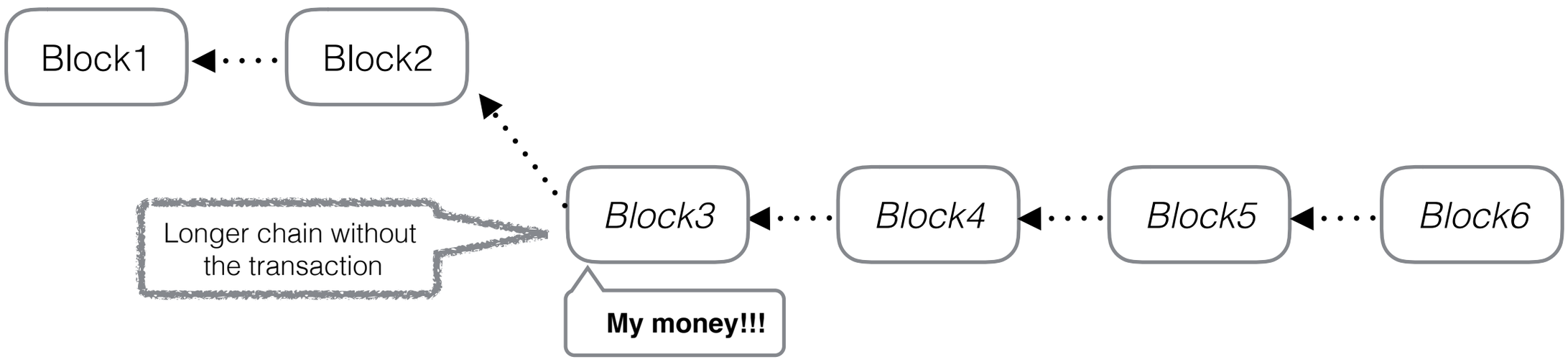
Double spending attack

- A double-spending attack is in fact a successful attempt to convince a merchant(the receiver of payment) that a transaction has been confirmed, and then convince the entire network to invalidate the branch by creating a longer correct branch.
- The merchant would be left with neither product nor coins, and the attacker will get to keep both.



Double spending attack

- A double-spending attack is in fact a successful attempt to convince a merchant(the receiver of payment) that a transaction has been confirmed, and then convince the entire network to invalidate the branch by creating a longer correct branch.
- The merchant would be left with neither product nor coins, and the attacker will get to keep both.



ROYAL INSTITUTE OF TECHNOLOGY

Double spending attack

- Is there a way to estimate when a transaction has been accepted and can no longer be reversed?
- By linking the blocks to form a chain, the total work spent on any transaction is perpetually increasing, making it difficult to elevate any conflicting transaction to the same confirmation status without a prohibitive computational effort.
- The more confirmations the merchant observers, the more confident he can be that his transaction is final.
- If the attacker is in fact in control of substantial computational power, he may succeed after all.

Double spending attack

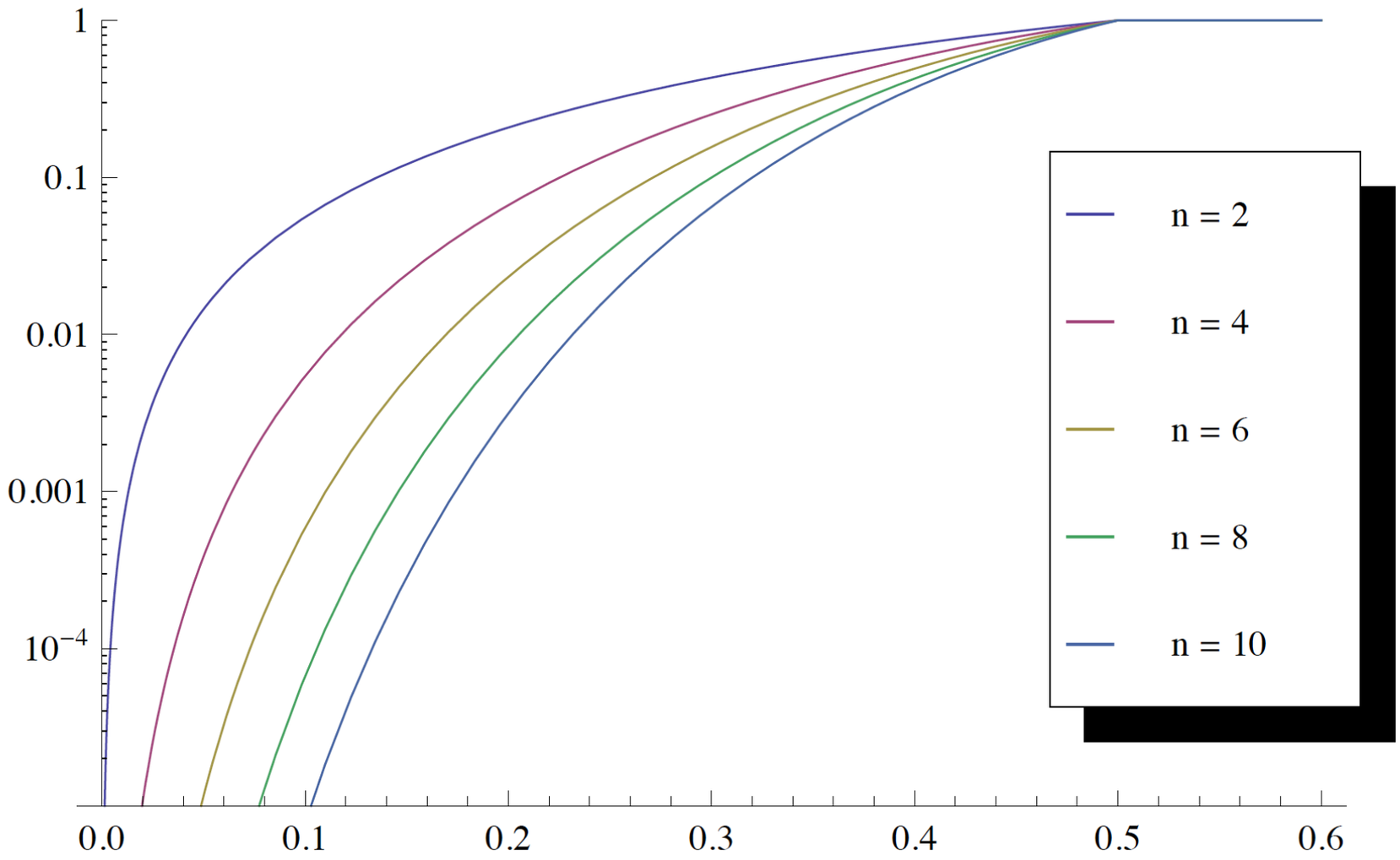


Figure 4: The probability r of successful double spend, as a function of the attacker's hashrate q, for different values of the number of confirmations n. For $q > 0.5$, the probability is always 1. The graph is in logarithmic scale; the lowest value shown is 10^{-5}, or 0.001%.

from: "Analysis of hashrate-based double-spending.", Meni Rosenfeld

Double spending attack

q	1	2	3	4	5	6	7	8	9	10
2%	4%	0.237%	0.016%	0.001%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
4%	8%	0.934%	0.120%	0.016%	0.002%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
6%	12%	2.074%	0.394%	0.078%	0.016%	0.003%	0.001%	≈ 0	≈ 0	≈ 0
8%	16%	3.635%	0.905%	0.235%	0.063%	0.017%	0.005%	0.001%	≈ 0	≈ 0
10%	20%	5.600%	1.712%	0.546%	0.178%	0.059%	0.020%	0.007%	0.002%	0.001%
12%	24%	7.949%	2.864%	1.074%	0.412%	0.161%	0.063%	0.025%	0.010%	0.004%
14%	28%	10.662%	4.400%	1.887%	0.828%	0.369%	0.166%	0.075%	0.034%	0.016%
16%	32%	13.722%	6.352%	3.050%	1.497%	0.745%	0.375%	0.190%	0.097%	0.050%
18%	36%	17.107%	8.741%	4.626%	2.499%	1.369%	0.758%	0.423%	0.237%	0.134%
20%	40%	20.800%	11.584%	6.669%	3.916%	2.331%	1.401%	0.848%	0.516%	0.316%
22%	44%	24.781%	14.887%	9.227%	5.828%	3.729%	2.407%	1.565%	1.023%	0.672%
24%	48%	29.030%	18.650%	12.339%	8.310%	5.664%	3.895%	2.696%	1.876%	1.311%
26%	52%	33.530%	22.868%	16.031%	11.427%	8.238%	5.988%	4.380%	3.220%	2.377%
28%	56%	38.259%	27.530%	20.319%	15.232%	11.539%	8.810%	6.766%	5.221%	4.044%
30%	60%	43.200%	32.616%	25.207%	19.762%	15.645%	12.475%	10.003%	8.055%	6.511%
32%	64%	48.333%	38.105%	30.687%	25.037%	20.611%	17.080%	14.226%	11.897%	9.983%
34%	68%	53.638%	43.970%	36.738%	31.058%	26.470%	22.695%	19.548%	16.900%	14.655%
36%	72%	59.098%	50.179%	43.330%	37.807%	33.226%	29.356%	26.044%	23.182%	20.692%
38%	76%	64.691%	56.698%	50.421%	45.245%	40.854%	37.062%	33.743%	30.811%	28.201%
40%	80%	70.400%	63.488%	57.958%	53.314%	49.300%	45.769%	42.621%	39.787%	37.218%
42%	84%	76.205%	70.508%	65.882%	61.938%	58.480%	55.390%	52.595%	50.042%	47.692%
44%	88%	82.086%	77.715%	74.125%	71.028%	68.282%	65.801%	63.530%	61.431%	59.478%
46%	92%	88.026%	85.064%	82.612%	80.480%	78.573%	76.836%	75.234%	73.742%	72.342%
48%	96%	94.003%	92.508%	91.264%	90.177%	89.201%	88.307%	87.478%	86.703%	85.972%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Table 1: The probability of a successful double spend, as a function of the attacker's hashrate q and the number of confirmations n.

from: "Analysis of hashrate-based double-spending.", Meni Rosenfeld

ROYAL INSTITUTE OF TECHNOLOGY

Double-double spending?

- A double-spending attack can be carried against more than one merchant. Payments can be simultaneously sent to k different merchants, with the same branch invalidating all of them.
- If the attack succeeds, all payments to the merchants will be invalidated giving back the money to the attacker. The attacker will also get the normal reward for mining the blocks in his chain.
- If the attack fails, and the attacker has found “o” blocks during it, each with a block reward of "B", those blocks will be rejected and the attacker will lose a total value of “oB".

from: “Analysis of hashrate-based double-spending.”, Meni Rosenfeld

ROYAL INSTITUTE OF TECHNOLOGY

Double-double spending?

- We assume for simplicity that o = 20, meaning the attacker gives up after finding 20 blocks, and that B = 25BTC, meaning the attacker could have gained this value by legal mining.
- We can next make a few approximations on what amounts should the merchant consider safe in conjunction with an attacker that behaves as stated above and has a certain computational power and the number of confirmations observed by the merchant.

from: “Analysis of hashrate-based double-spending.”, Meni Rosenfeld

ROYAL INSTITUTE OF TECHNOLOGY

Double-double spending?

q	1	2	3	4	5	6	7	8	9	10
2%	2400	42K	644K	9370K	$\approx \infty$	$\approx \infty$	$\approx \infty$	$\approx \infty$	$\approx \infty$	$\approx \infty$
4%	1150	10K	82K	615K	4437K	$\approx \infty$	$\approx \infty$	$\approx \infty$	$\approx \infty$	$\approx \infty$
6%	733	4722	25K	127K	626K	3018K	14M	$\approx \infty$	$\approx \infty$	$\approx \infty$
8%	525	2650	10K	42K	159K	588K	2144K	7749K	$\approx \infty$	$\approx \infty$
10%	400	1685	5741	18K	56K	168K	503K	1486K	4361K	12M
12%	316	1158	3391	9212	24K	62K	157K	396K	990K	2460K
14%	257	837	2172	5200	11K	27K	60K	132K	290K	632K
16%	212	628	1474	3178	6580	13K	26K	52K	102K	200K
18%	177	484	1043	2061	3901	7202	13K	23K	42K	74K
20%	150	380	763	1399	2453	4190	7039	11K	19K	31K
22%	127	303	571	983	1615	2582	4053	6288	9671	14K
24%	108	244	436	710	1103	1665	2467	3608	5229	7525
26%	92	198	337	523	775	1113	1570	2182	3005	4106
28%	78	161	263	392	556	766	1035	1377	1815	2372
30%	66	131	206	296	406	539	701	899	1141	1435
32%	56	106	162	225	299	385	485	602	740	901
34%	47	86	127	172	221	277	340	411	491	582
36%	38	69	99	130	164	200	240	283	331	383
38%	31	54	76	98	121	144	169	196	224	254
40%	25	42	57	72	87	102	118	134	151	168
42%	19	31	41	51	61	70	80	90	99	109
44%	13	21	28	34	40	46	51	57	62	68
46%	8	13	17	21	24	27	30	32	35	38
48%	4	6	8	9	10	12	13	14	15	16
50%	0	0	0	0	0	0	0	0	0	0

Table 2: The maximal safe transaction value, in BTC, as a function of the attacker's hashrate q and the number of confirmations n.

slide from: "Analysis of hashrate-based double-spending.", Meni Rosenfeld

ROYAL INSTITUTE OF TECHNOLOGY

Bitcoin puzzle difficulty

- The cryptographic puzzle of the Bitcoin protocol is adaptable and can be modified to make the problem easier or more difficult.
- If the network is small, the puzzle is made easier to allow the fewer miners to generate the same amount of blocks.
- The goal is that the network produces on average 1 block every 10mins.
- Every 2016 blocks (solved in about two weeks), the network comes to a consensus and automatically increases (or decreases) the difficulty of generating blocks.

ROYAL INSTITUTE OF TECHNOLOGY

Bitcoin protocol values

- Rate of block mining: 1 every 10mins.
- Block size - 1MB size.
- Currently the blockchain size is 1GB.
- The number of max TPS(transactions per second) supported by current protocol: 7.

for accurate values check the Bitcoin protocol at: https://en.bitcoin.it/wiki/

ROYAL INSTITUTE OF TECHNOLOGY

Block size

- Block header size: 80bytes.
- Transaction input size: 180 bytes.
- Transaction output size: 34 bytes.
- Transaction fixed size: 10bytes.
- Transaction total size: n*180 + m*34 + 10.
- A transaction with 1 input and 2 outputs would have: 180+68+10 = 258 bytes.

for accurate values check the Bitcoin protocol at: https://en.bitcoin.it/wiki/

ROYAL INSTITUTE OF TECHNOLOGY

So slow…

- Bitcoin max TPS: 7
- Visa reported current TPS: 2000
- How can we make Bitcoin faster?
  - bigger blocks
  - faster block generation

ROYAL INSTITUTE OF TECHNOLOGY

Bigger blocks?

- Bandwidth: each miner needs to download every transaction that will be included in a block, and the blocks generated. Miners might need to pay for high-speed connections.
- A miner with 8.3% of total hash rate can take that cost out of the about 300 BTC they make a day, while a miner with only 0.7% of total hash rate has to take that cost out of only 25 BTC a day.
- If bigger miners have an advantage, it will drive small miners away leading to further centralised mining and back to a banking like system.

for accurate values check the Bitcoin protocol at: https://en.bitcoin.it/wiki/

ROYAL INSTITUTE OF TECHNOLOGY

Fast Money Grows on Trees, Not Chains

- “Accelerating Bitcoin's Transaction Processing - Fast Money Grows on Trees, Not Chains” is a paper from 2013 that claims to improve the Bitcoin TPS.

- Points out that the analysis done so far on “double spending attacks” do not take into consideration network delays. In P2P networks can be quite high, while an attacker might have his nodes well connected.

- Current Bitcoin monitoring of the growth of the blockchain does not protect against spiked behaviour. (sudden and fast growth of a secondary branch).

ROYAL INSTITUTE OF TECHNOLOGY

Fast Money Grows on Trees, Not Chains

- The protocol described in the paper, named Ghost accepts the fact that mining can produce branches of the blockchain, but instead of discarding all of them they take advantage of them to allow faster block generation rate, without sacrificing security.

- Claims TPS: between 161 and 664, with a block rate generation of 1 block/s (compared to 1/10mins of Bitcoin).

ROYAL INSTITUTE OF TECHNOLOGY

Other blockchain implementations

- Namecoin - 2012 - decentralised name-resolution.
- Coloured Coins - 2012 - tracking of coins.
- Litecoin, Primecoin, Mastercoin - 2013.
- Ripple - 2014 - federated currency exchange

ROYAL INSTITUTE OF TECHNOLOGY

Resources

- David Chaum. "Blind signatures for untraceable payments". 1983. Advances in Cryptology Proceedings of Crypto 82 (3): 199–203. doi: 10.1007/978-1-4757-0602-4_18

- A. Back, "Hashcash - a denial of service counter-measure". 2002. http://www.hashcash.org/papers/hashcash.pdf

- S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". 2008.

- Meni Rosenfeld. "Analysis of hashrate-based double-spending". 2014.

- Yonatan Sompolinsky and Aviv Zohar. "Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains". 2013.

Resources

- Gavin Woode. “Ethereum: A secure decentralised generalised transaction ledger”. 2015. http://gavwood.com/Paper.pdf

- Meni Rosenfeld. “Overview of Colored Coins". 2012. https://bitcoil.co.il/BitcoinX.pdf

- J. R. Willett. “MasterCoin Complete Specification”. 2013. https://github.com/mastercoin-MSC/spec

- www.csc.kth.se/~buc/PPC/Slides/ecashbitcoinblindsignatures.pdf

- https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it