# **Blockchains**
# and its applications

Quentin Bramas

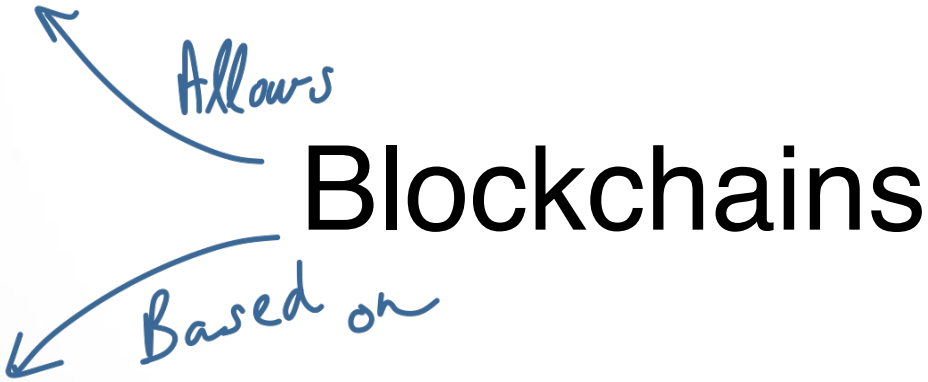
Assistant Professor
ICUBE Laboratory
University of Strasbourg

# Blockchains

# Blockchains

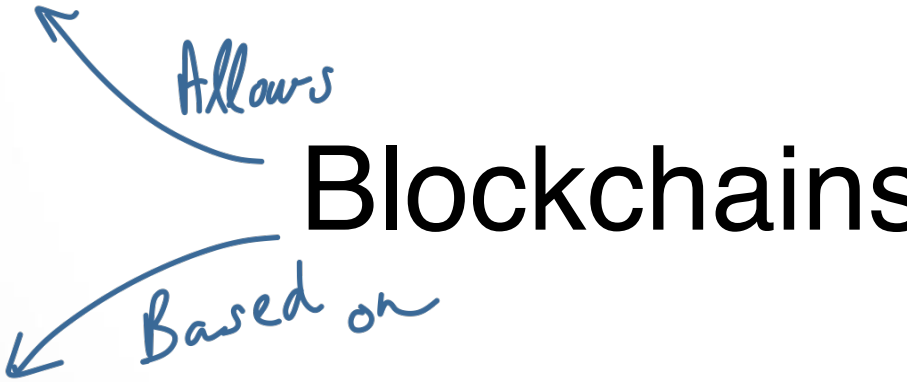

- Distributed Systems
- Zero Knowledge Proof

- Decentralized Democracy
- Crypto kitties
- Ensuring Documents Validity




- Distributed Systems
- Zero Knowledge Proof

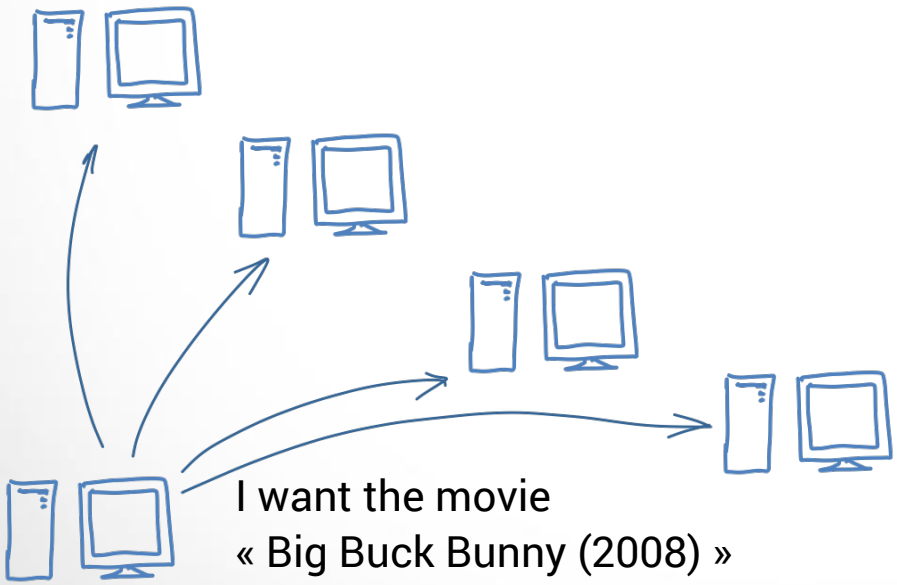
- Decentralized Democracy
- Crypto kitties
- Ensuring Documents Validity



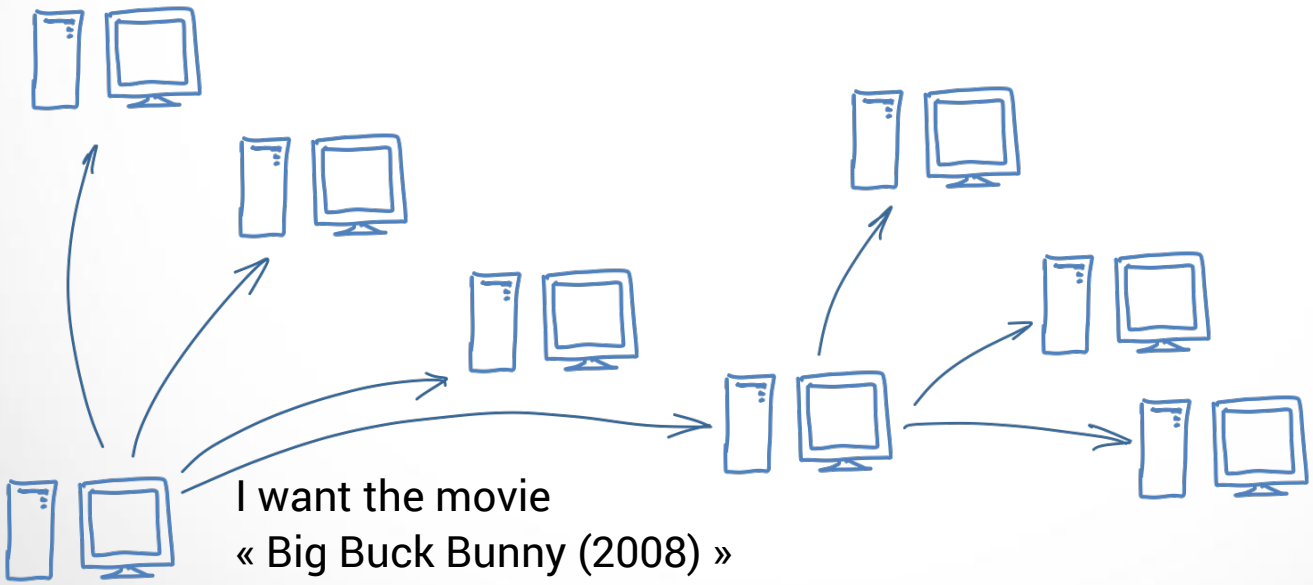

- Distributed Systems
- Zero Knowledge Proof

# Distributed systems

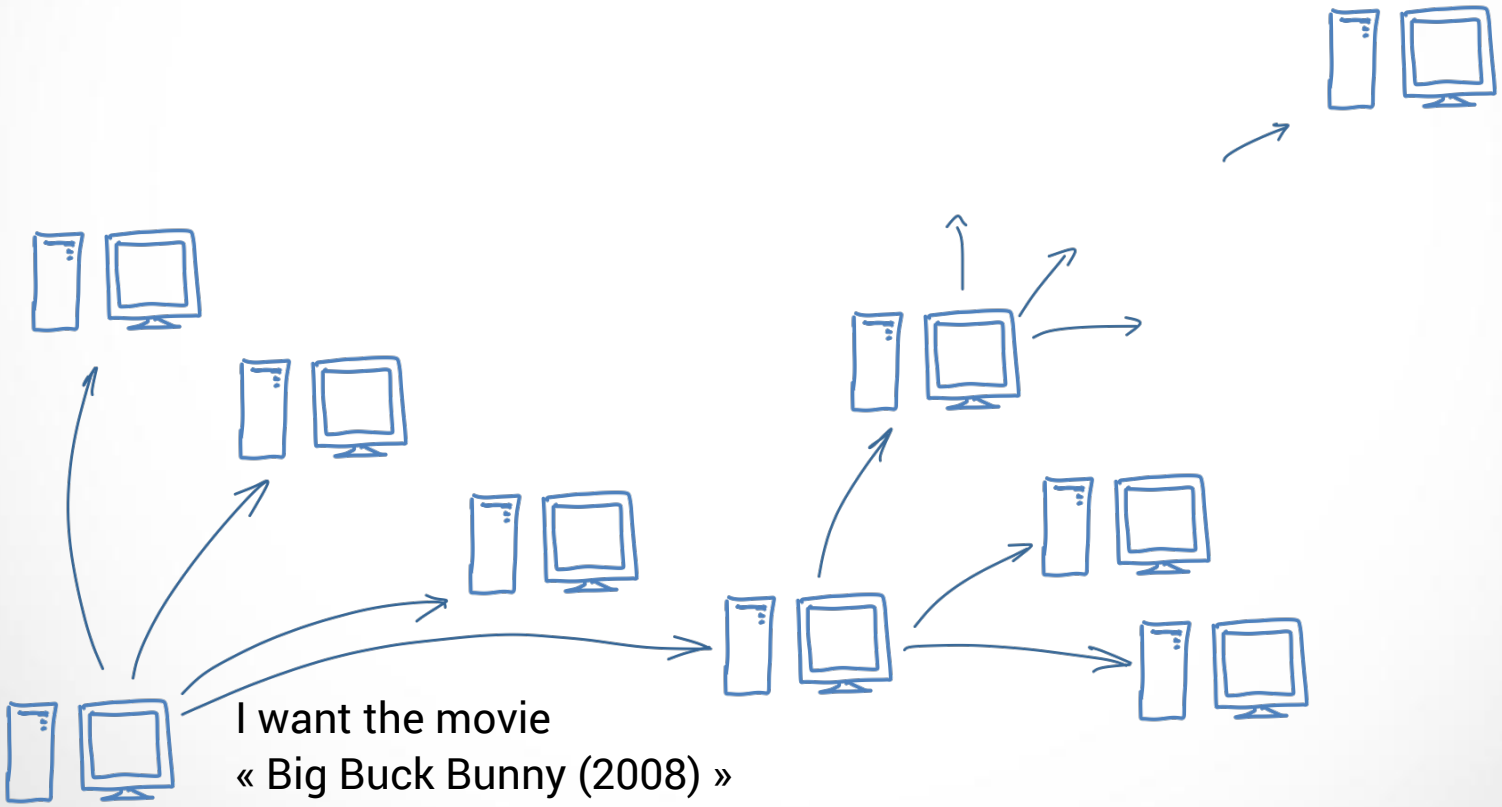
# Distributed systems



# Distributed systems

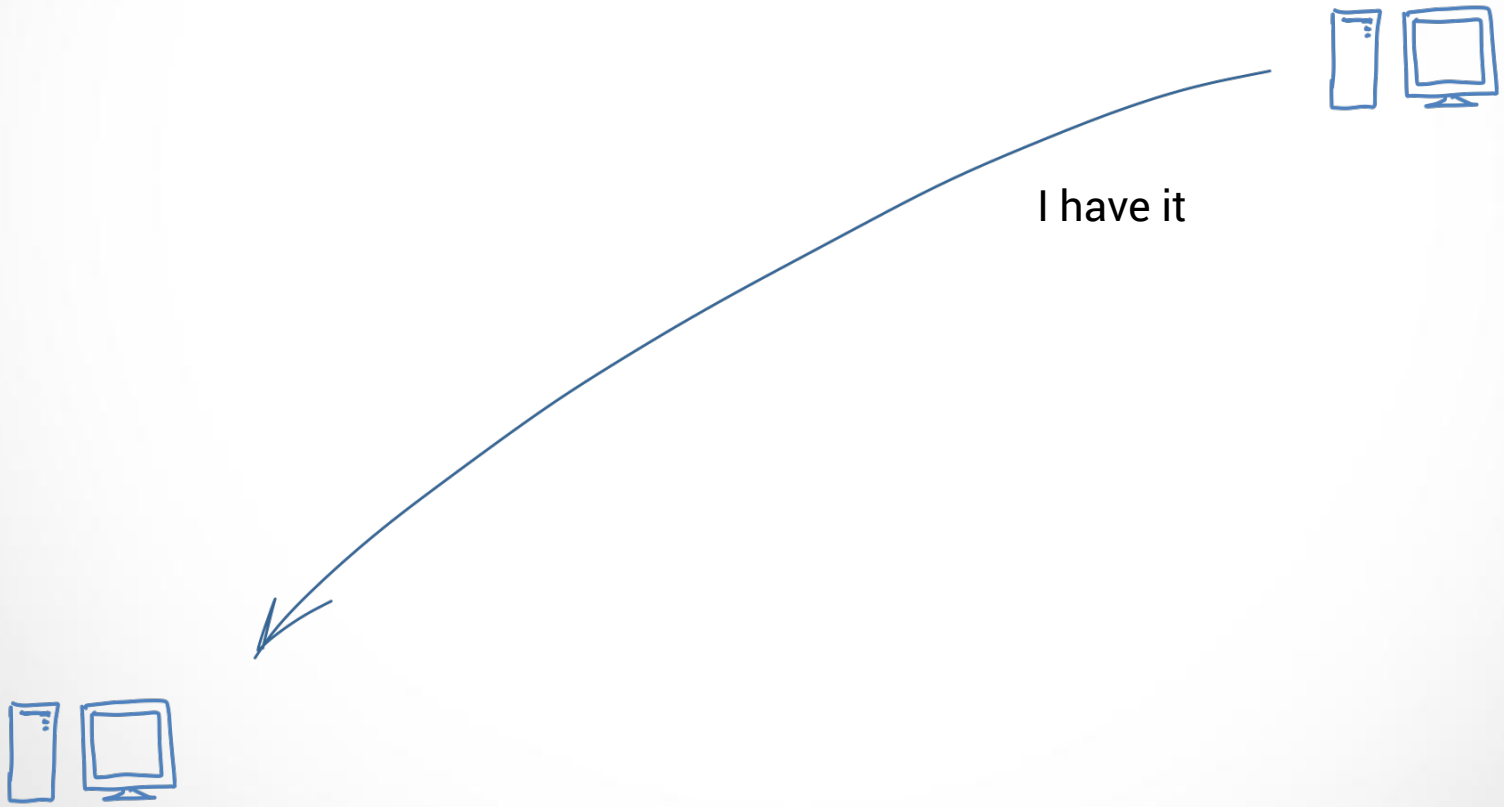


# Distributed systems



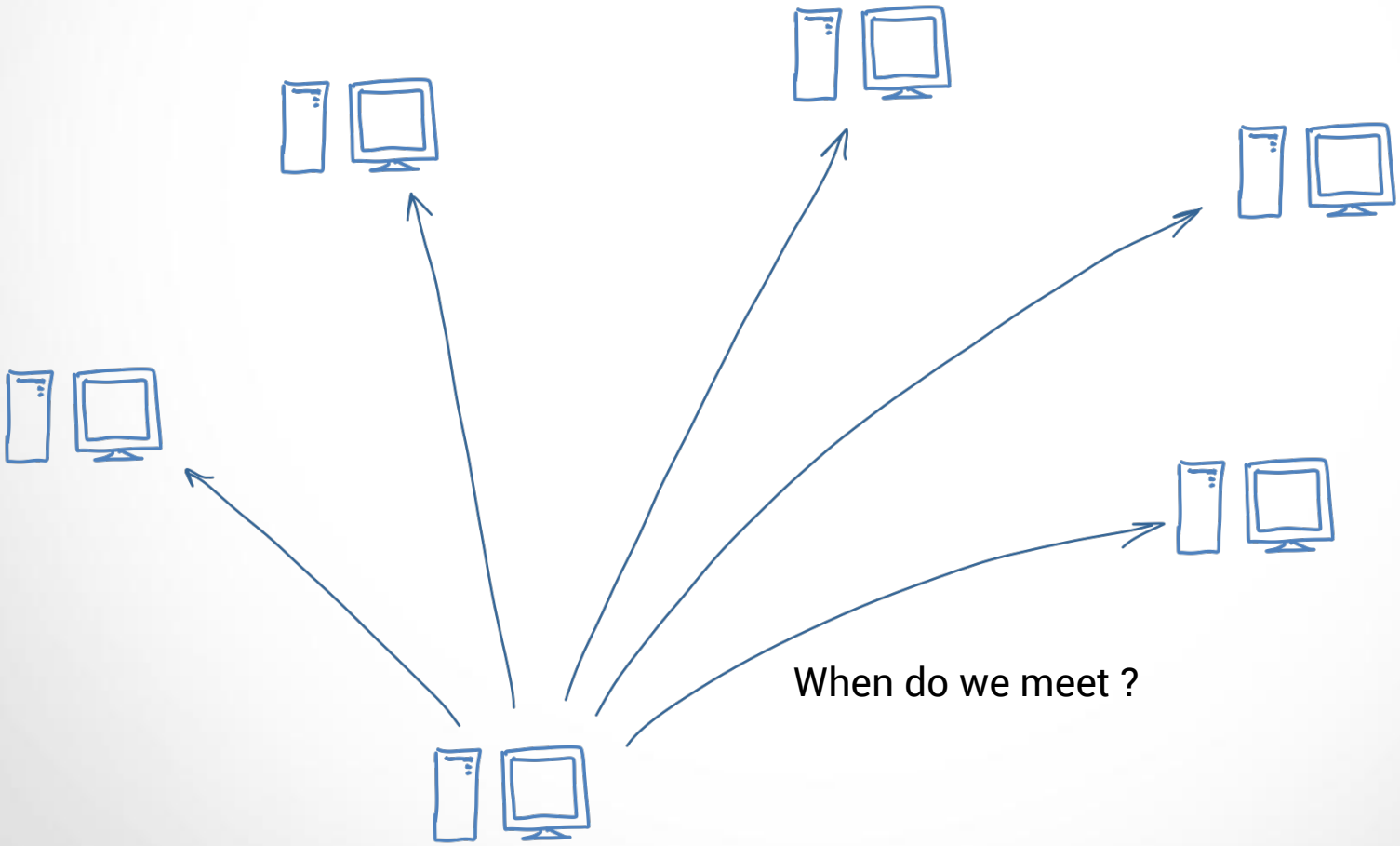
# Distributed systems

# Distributed systems



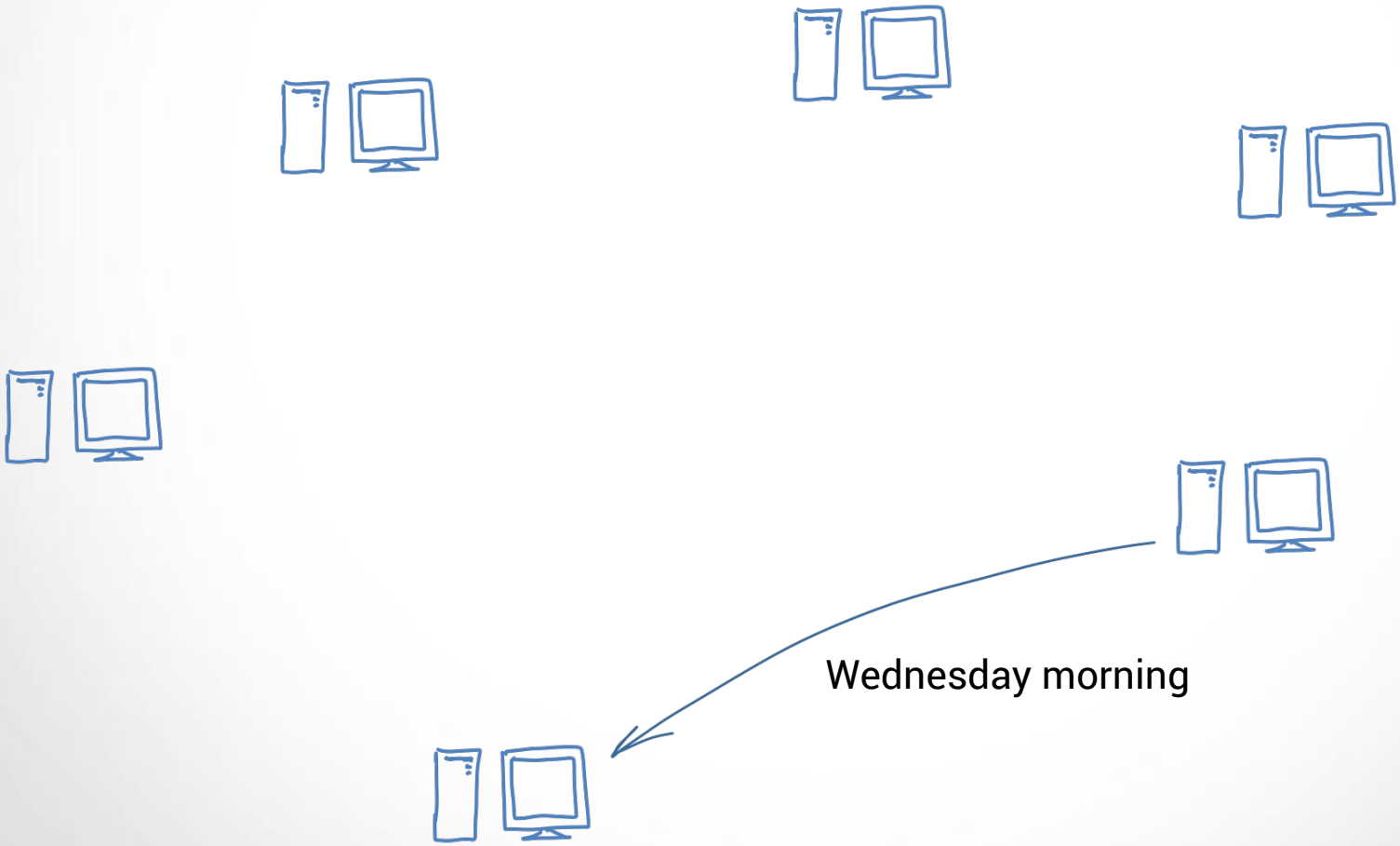
# Distributed systems

# Distributed systems

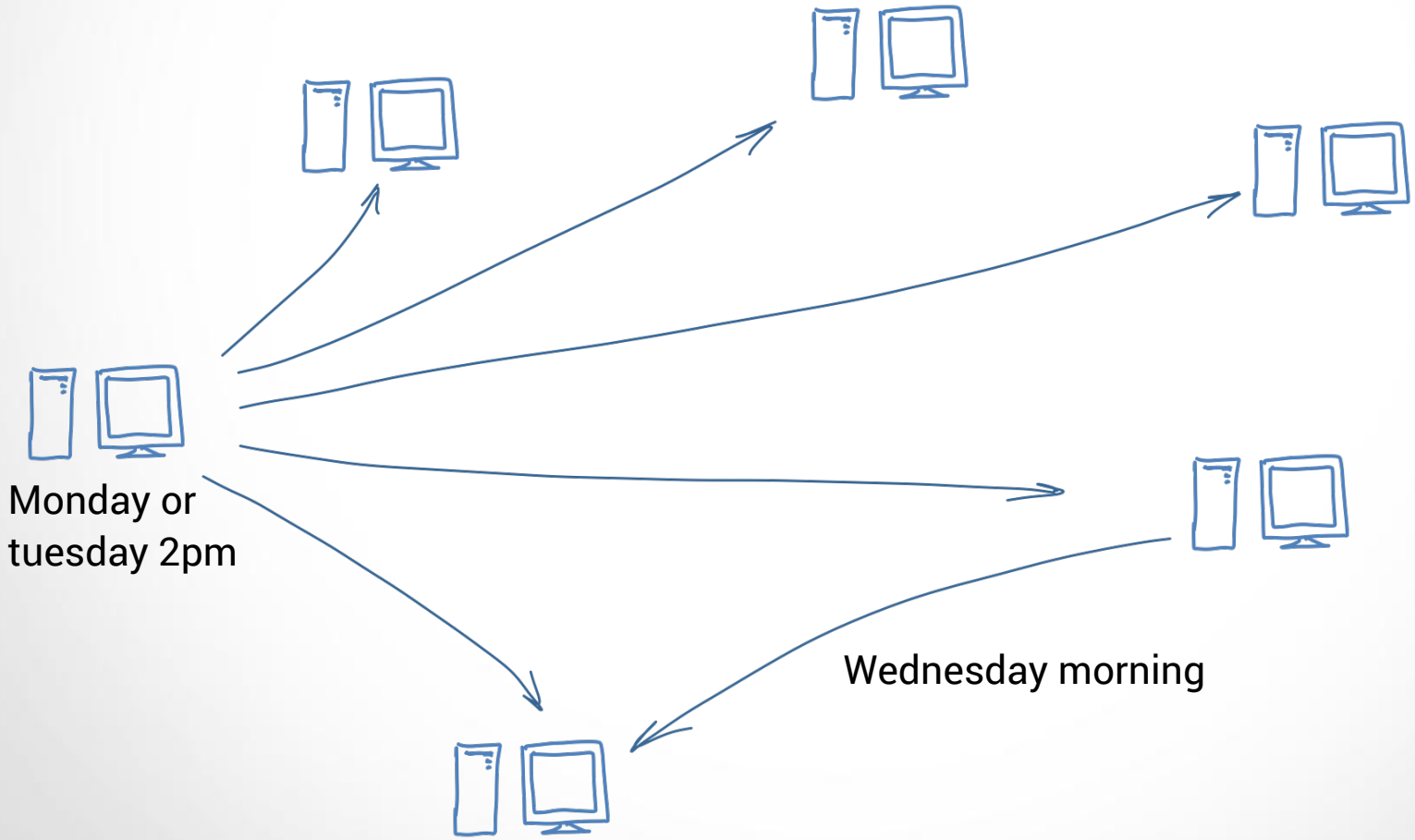


# Distributed systems

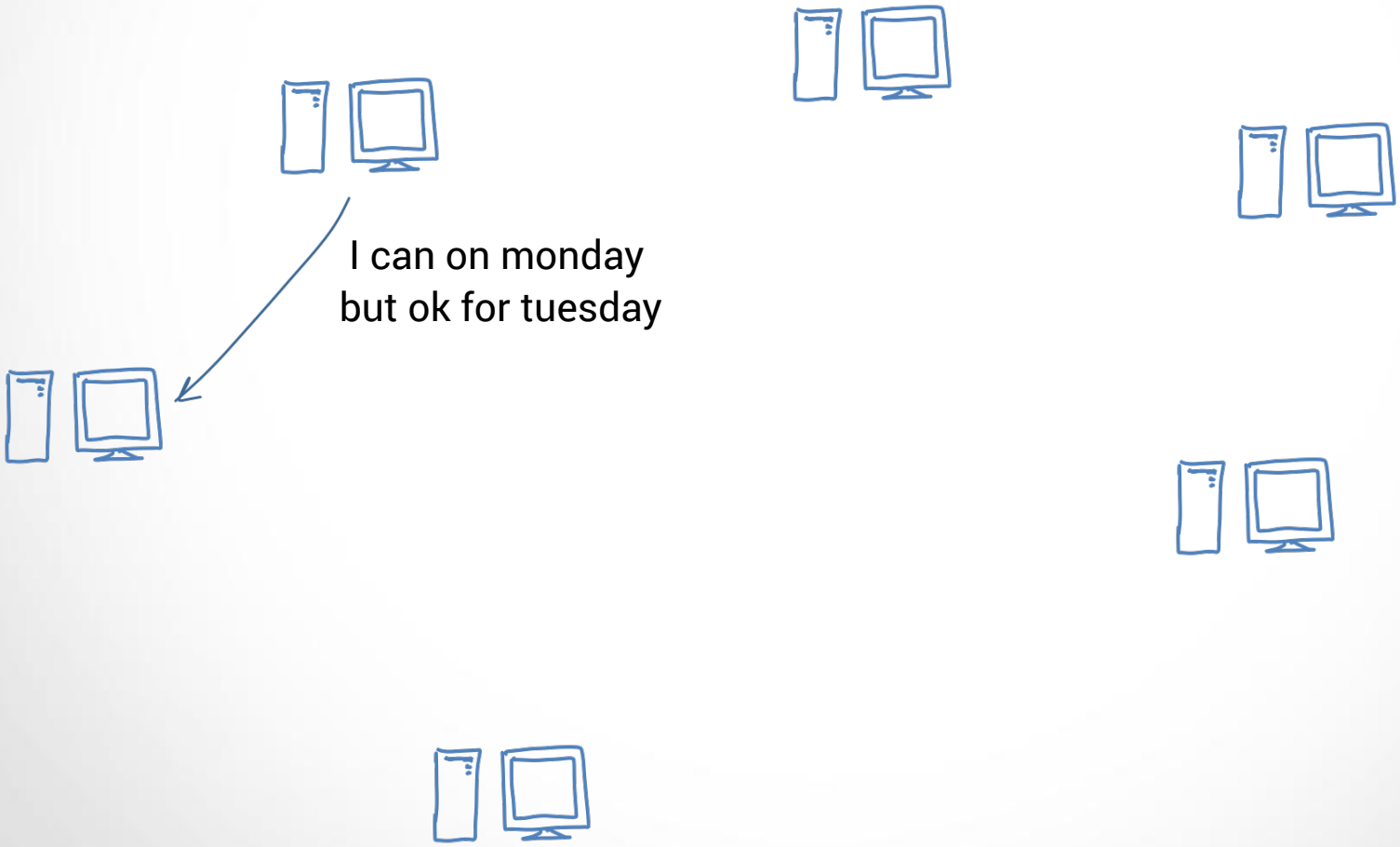
# Distributed systems



# Distributed systems

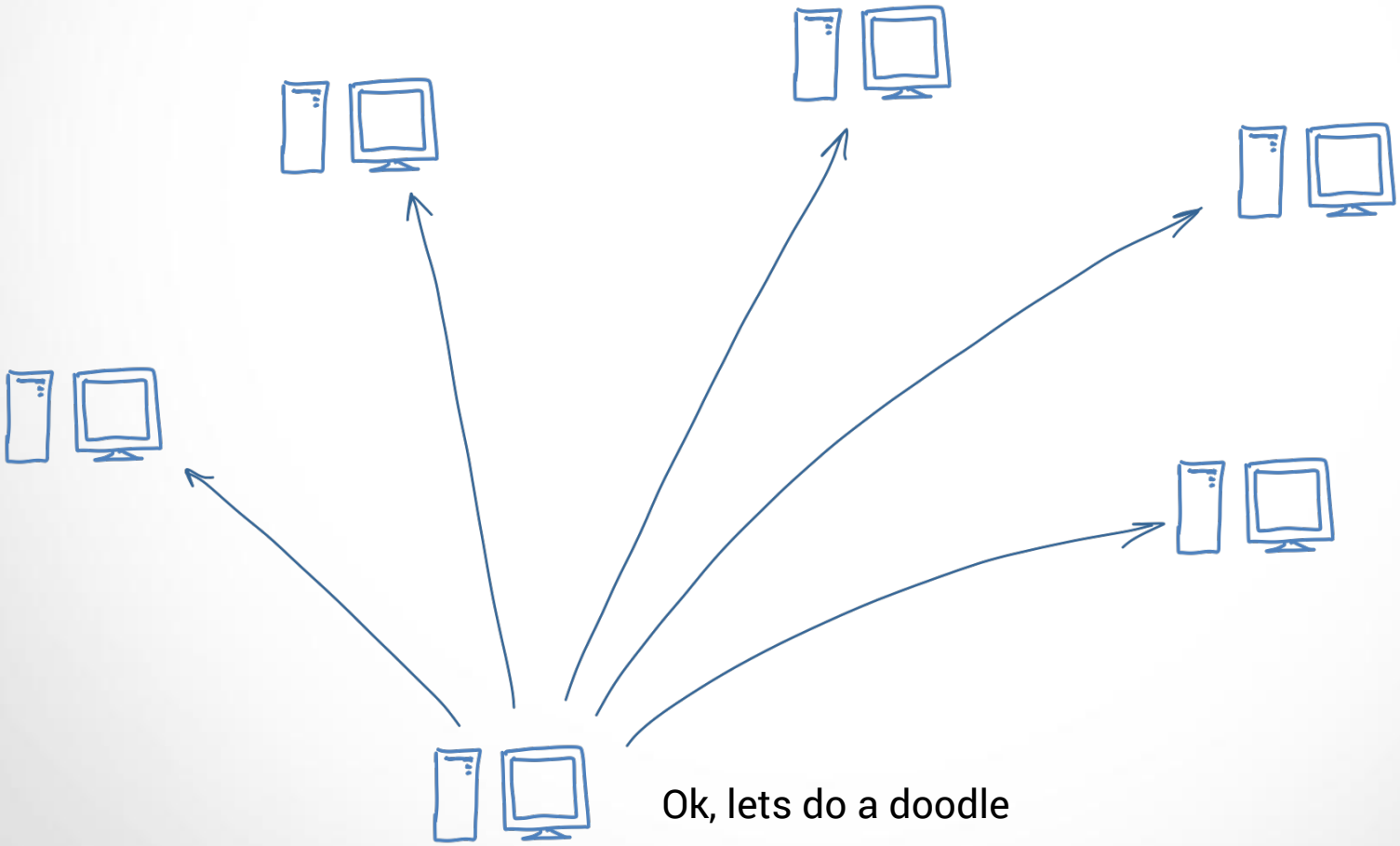


# Distributed systems

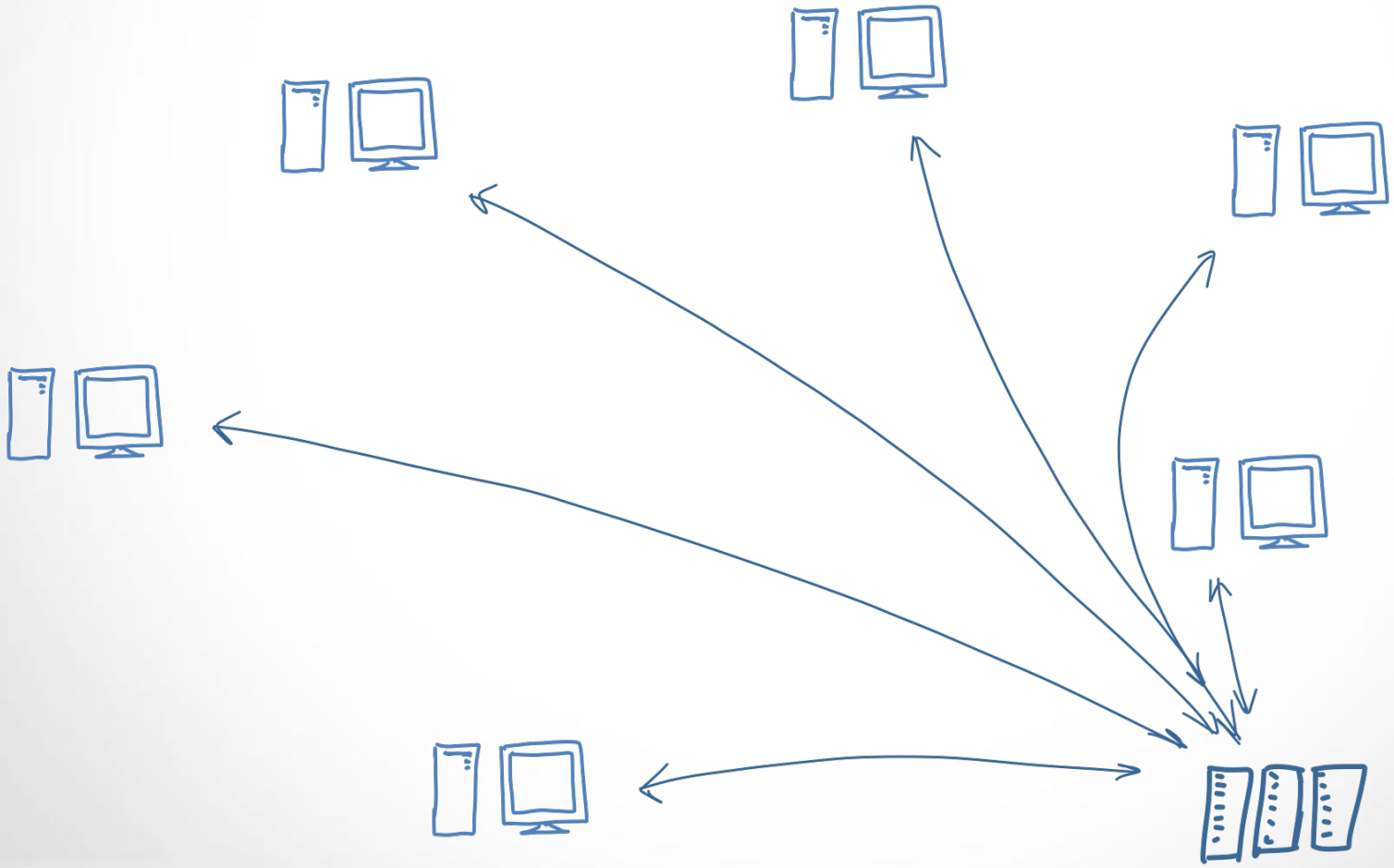


# Distributed systems

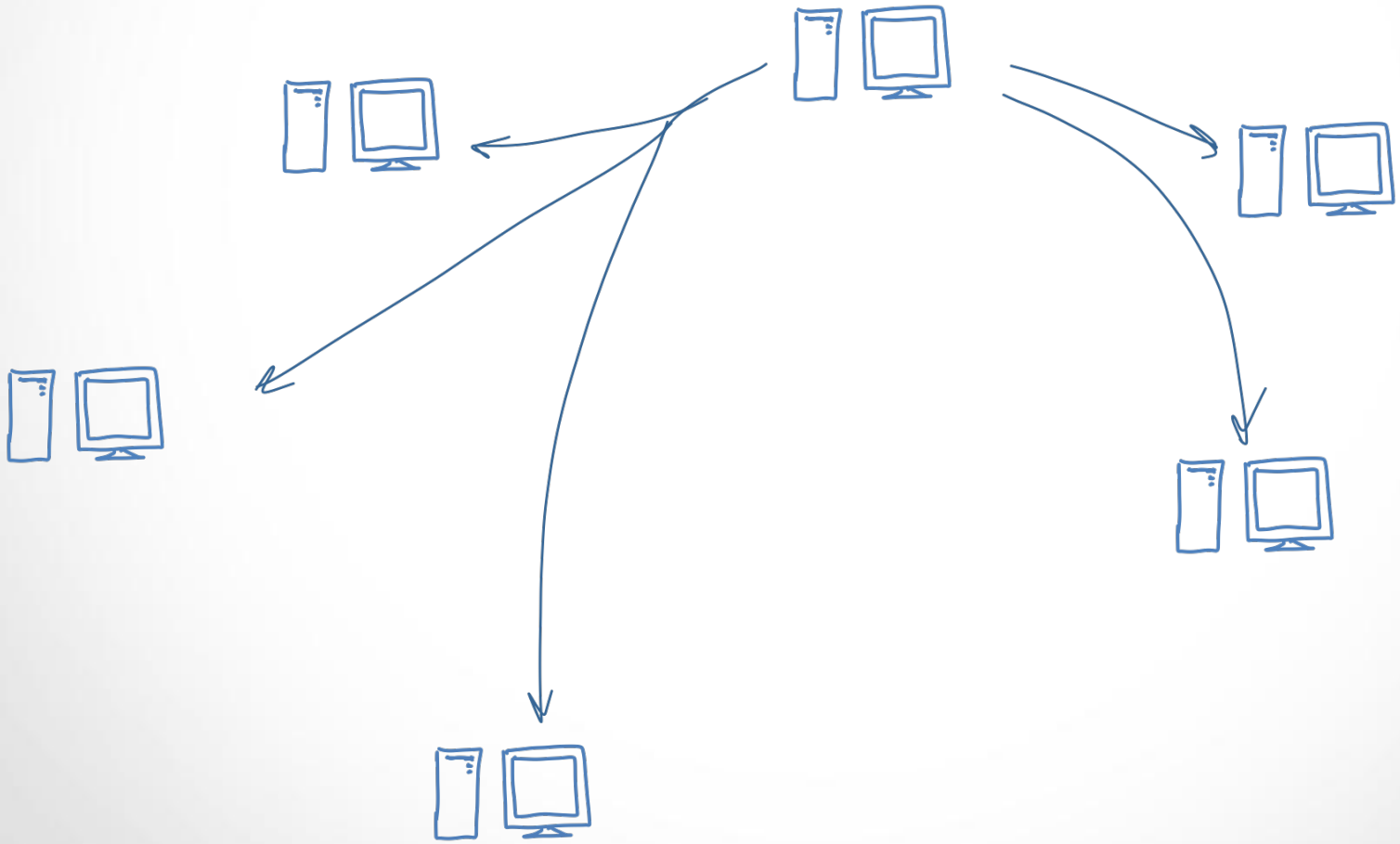
# Distributed systems



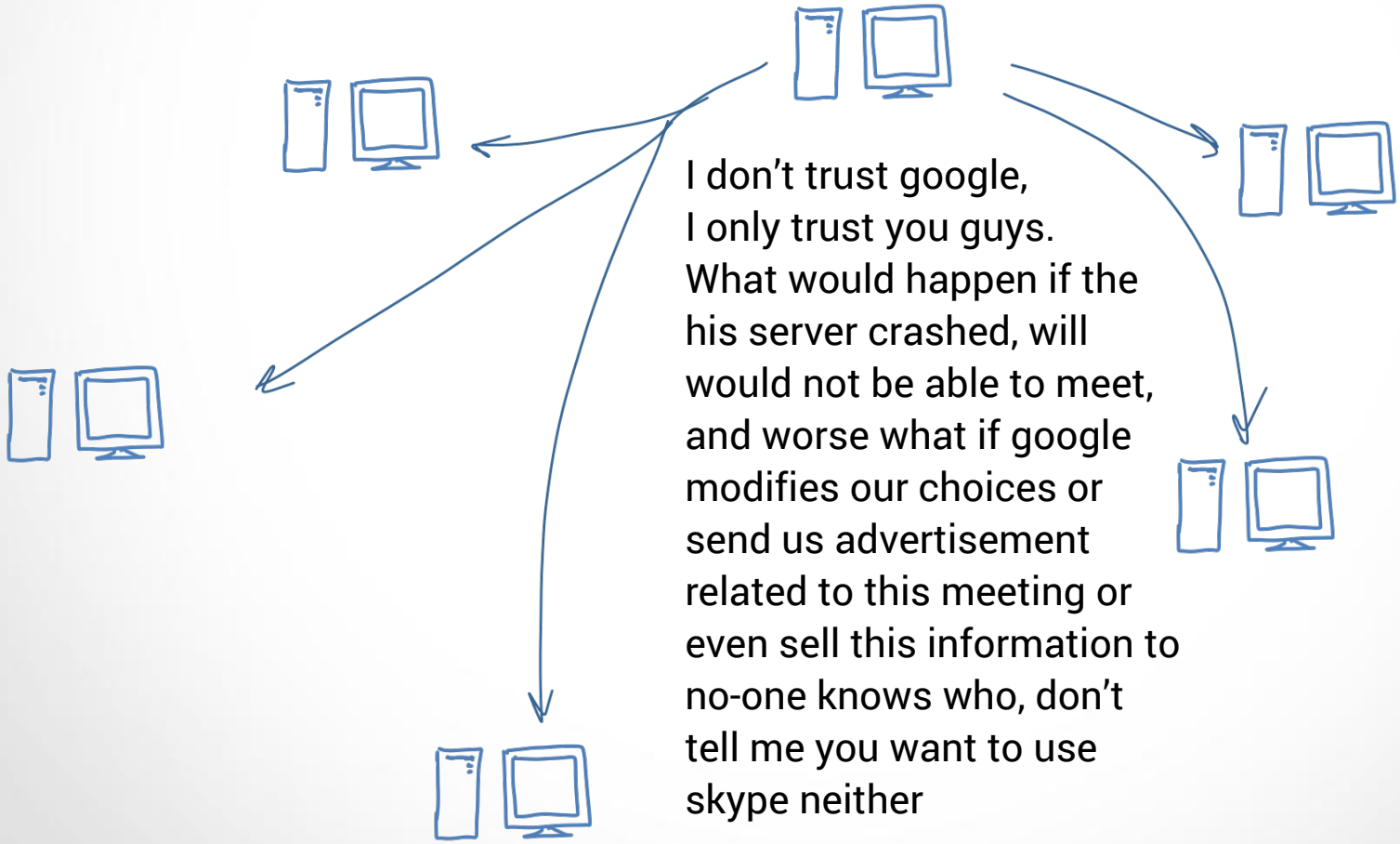
# Distributed systems



# Distributed systems



# Distributed systems



I don't trust google,
I only trust you guys.
What would happen if the his server crashed, will would not be able to meet, and worse what if google modifies our choices or send us advertisement related to this meeting or even sell this information to no-one knows who, don't tell me you want to use skype neither

# Distributed systems





But we have to

# Distributed systems

**Leslie Lamport** @LeslieLamport · 28 May 87

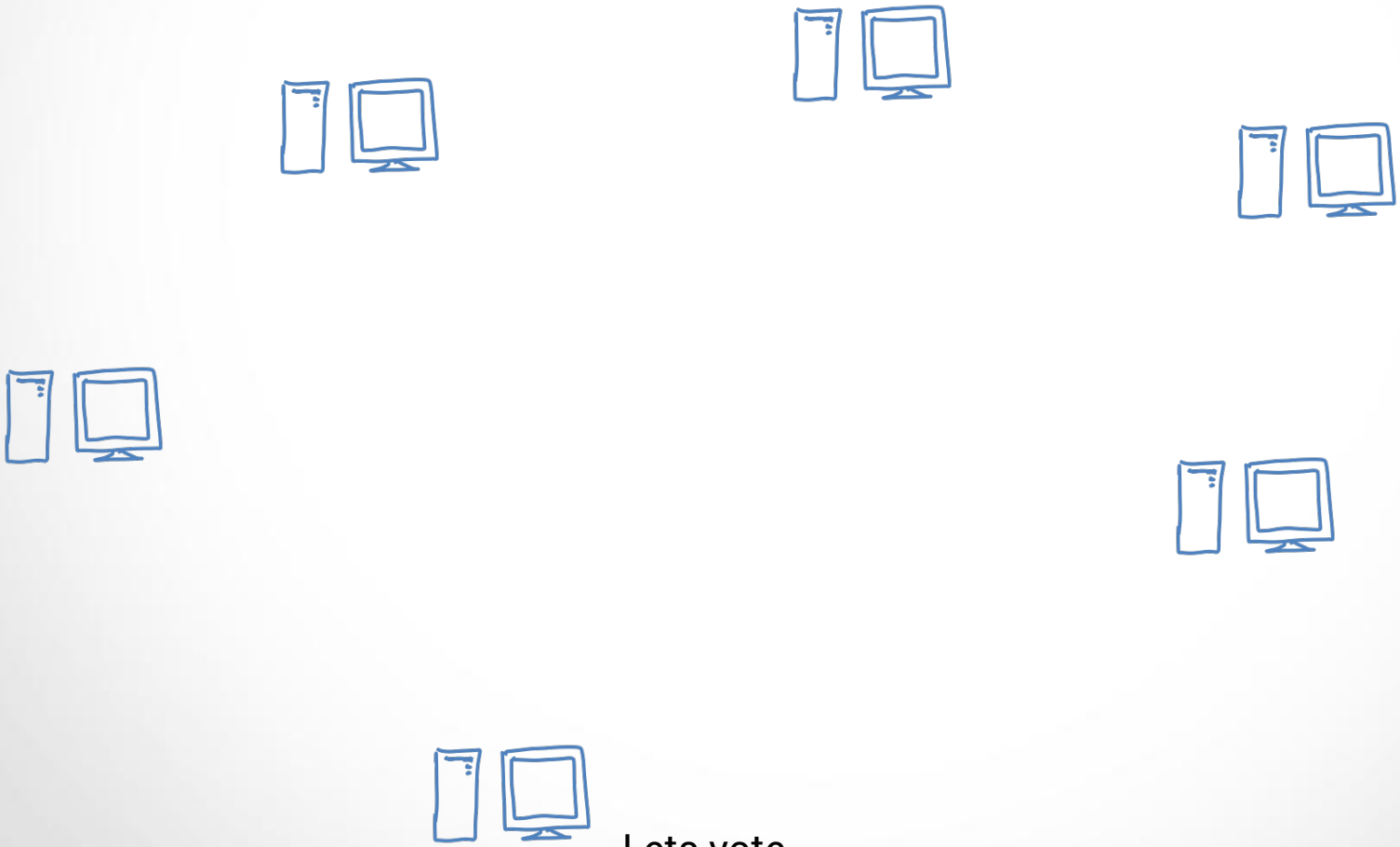
A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable.

252 280 2,3 k

Afficher cette discussion

# Distributed systems

# Distributed systems



# Distributed systems

Yes

Yes

Yes

Yes

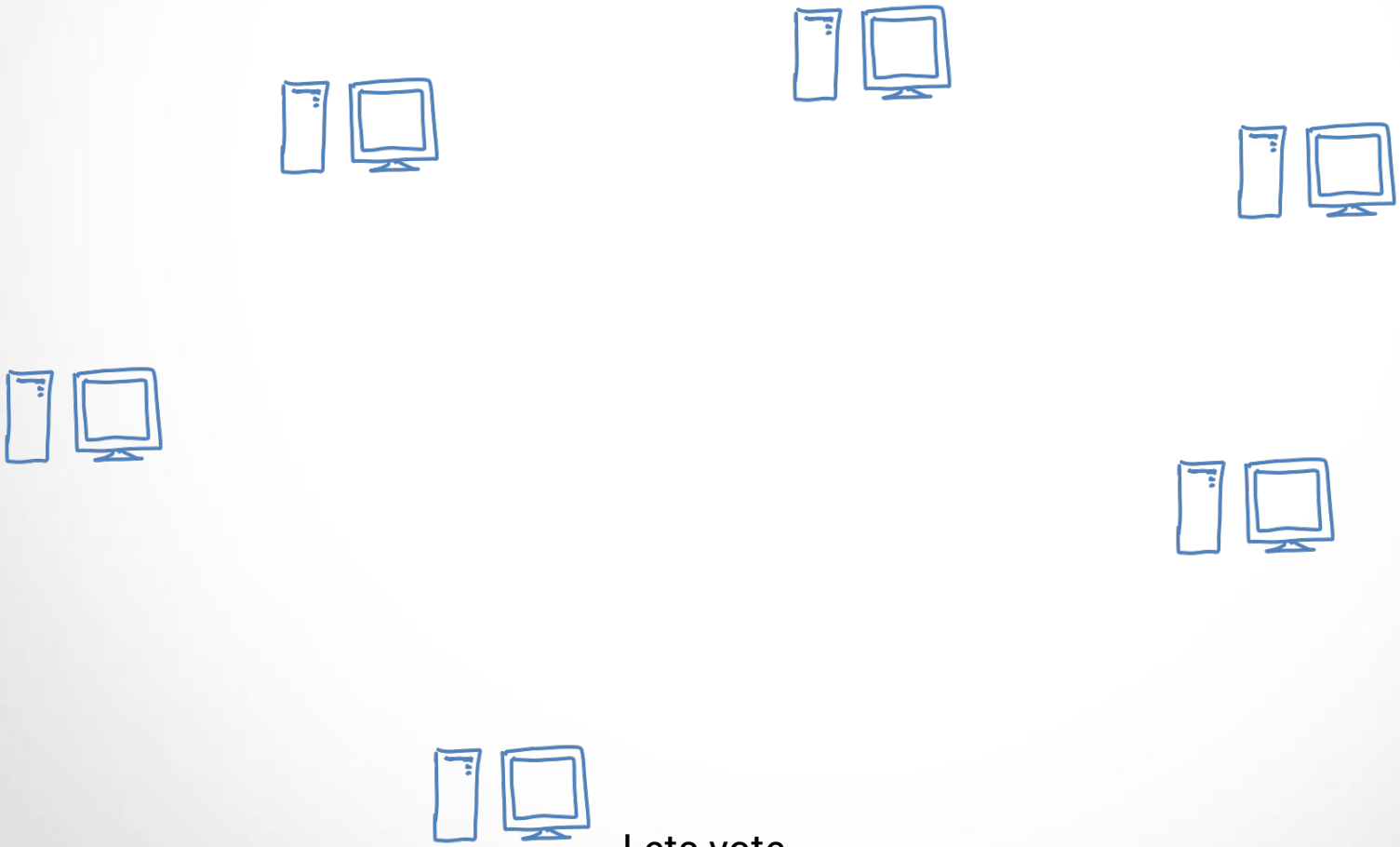
No 

Yes

Lets vote

# Distributed systems

# Distributed systems



# Distributed systems

Yes

Yes

Yes

Yes

No 

Yes

Lets vote

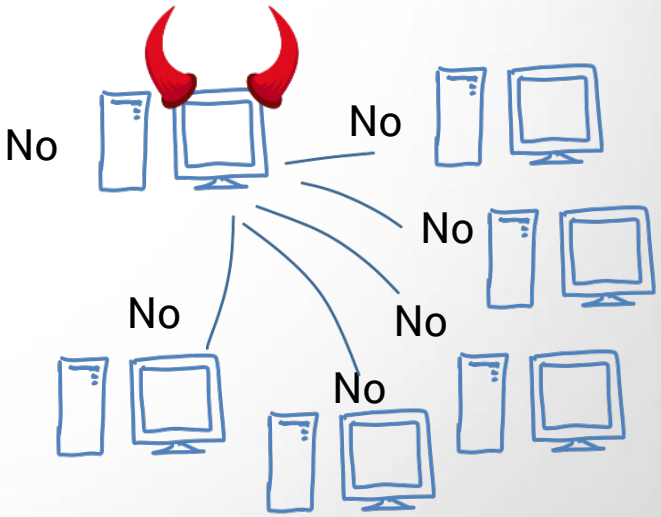
# Distributed systems

Yes

Yes

Yes

Yes




Yes

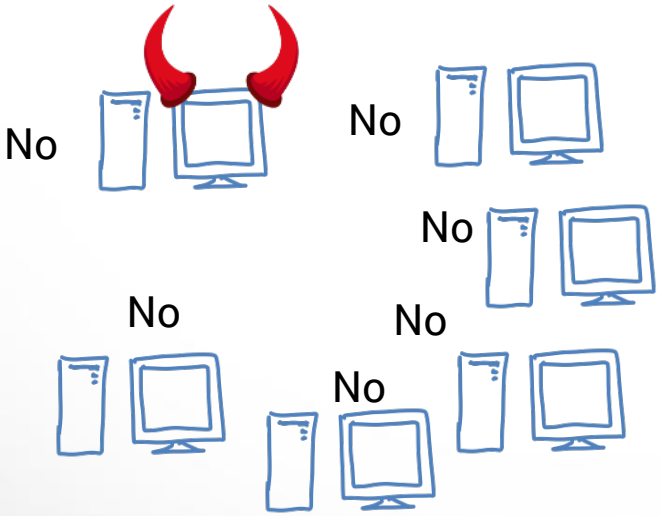
Lets vote

# Distributed systems

Yes

Yes

One can fake a large number of computers



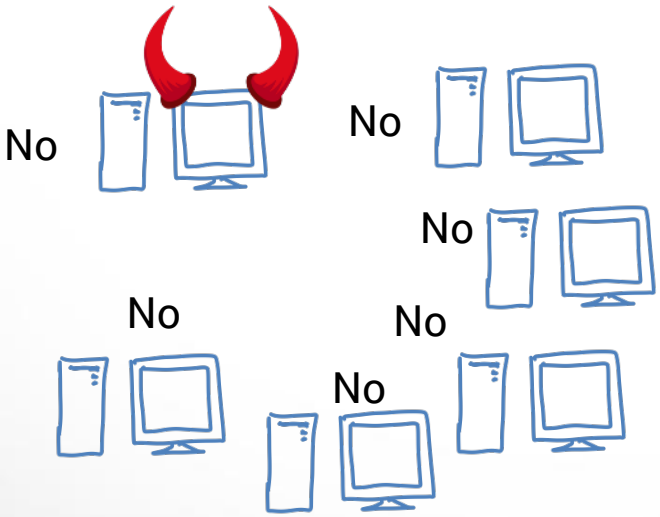

vote

# Distributed systems

Yes

Yes

One can fake a large number of computers




One cannot fake the computing power, using Proof of Work

vote

- Decentralized Democracy
- Crypto kitties
- Ensuring Documents Validity

# Blockchains

- Distributed Systems
- Zero Knowledge Proof

# Zero Proof Knowledge

# Zero Proof Knowledge

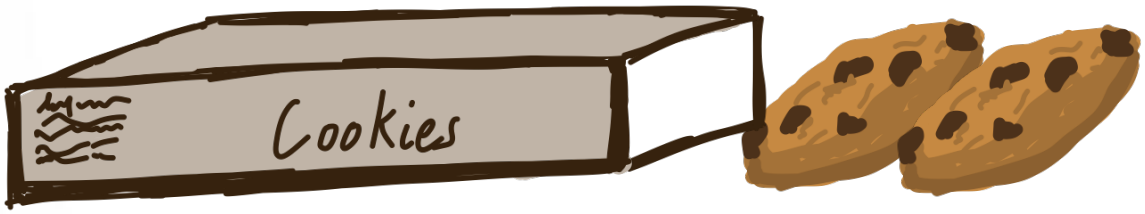
The magic cookie

# Zero Proof Knowledge

The magic cookie

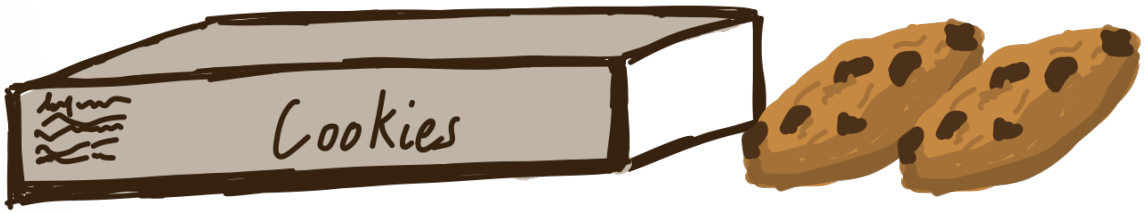
# Zero Proof Knowledge

The magic cookie



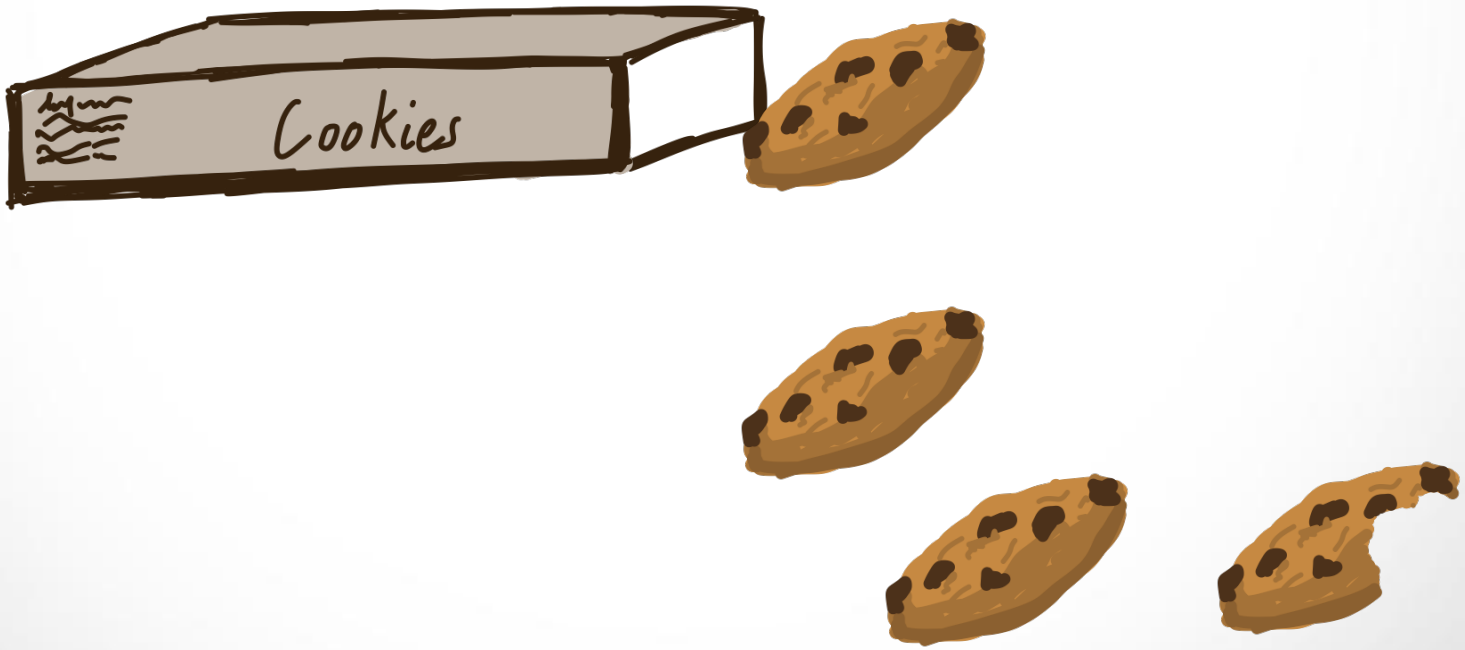

# Zero Proof Knowledge

The magic cookie



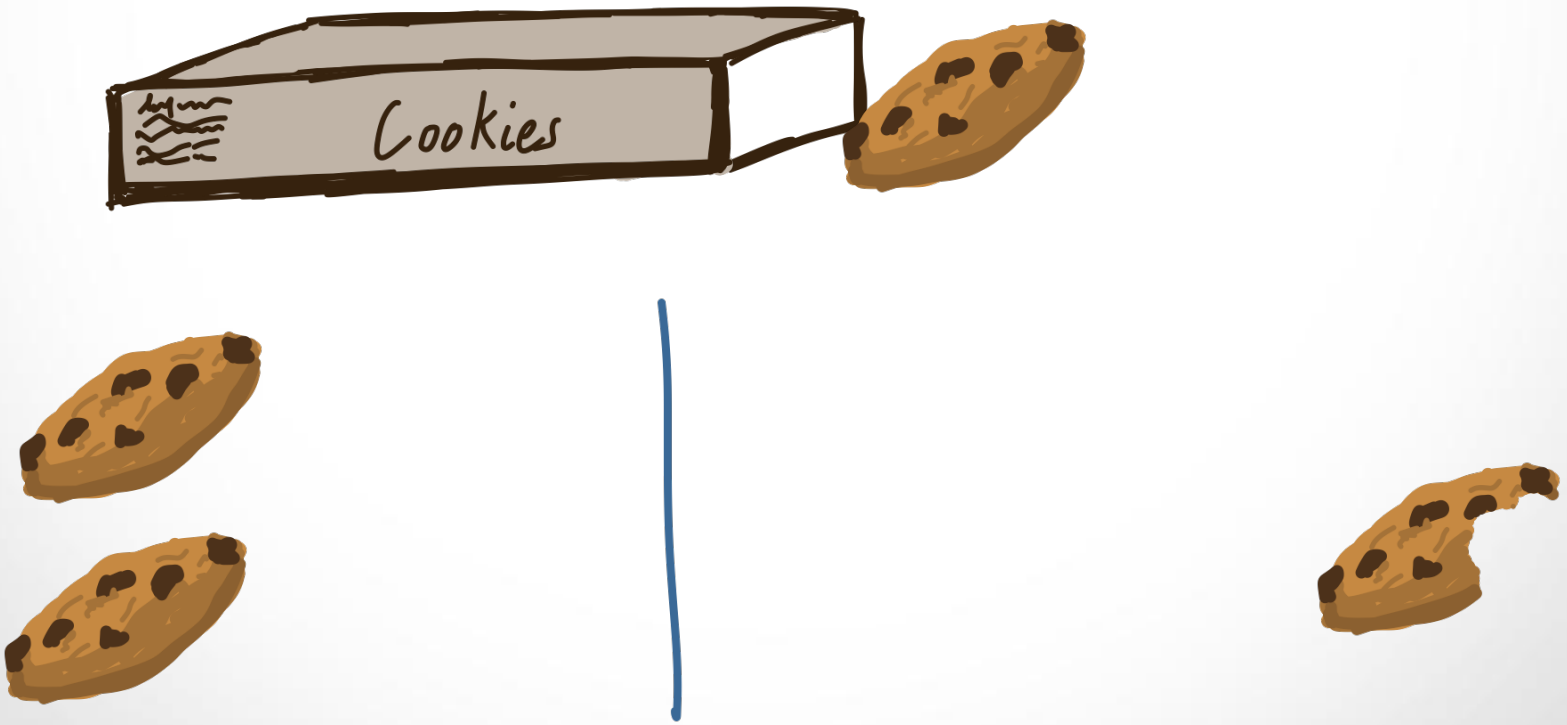

# Zero Proof Knowledge

The magic cookie



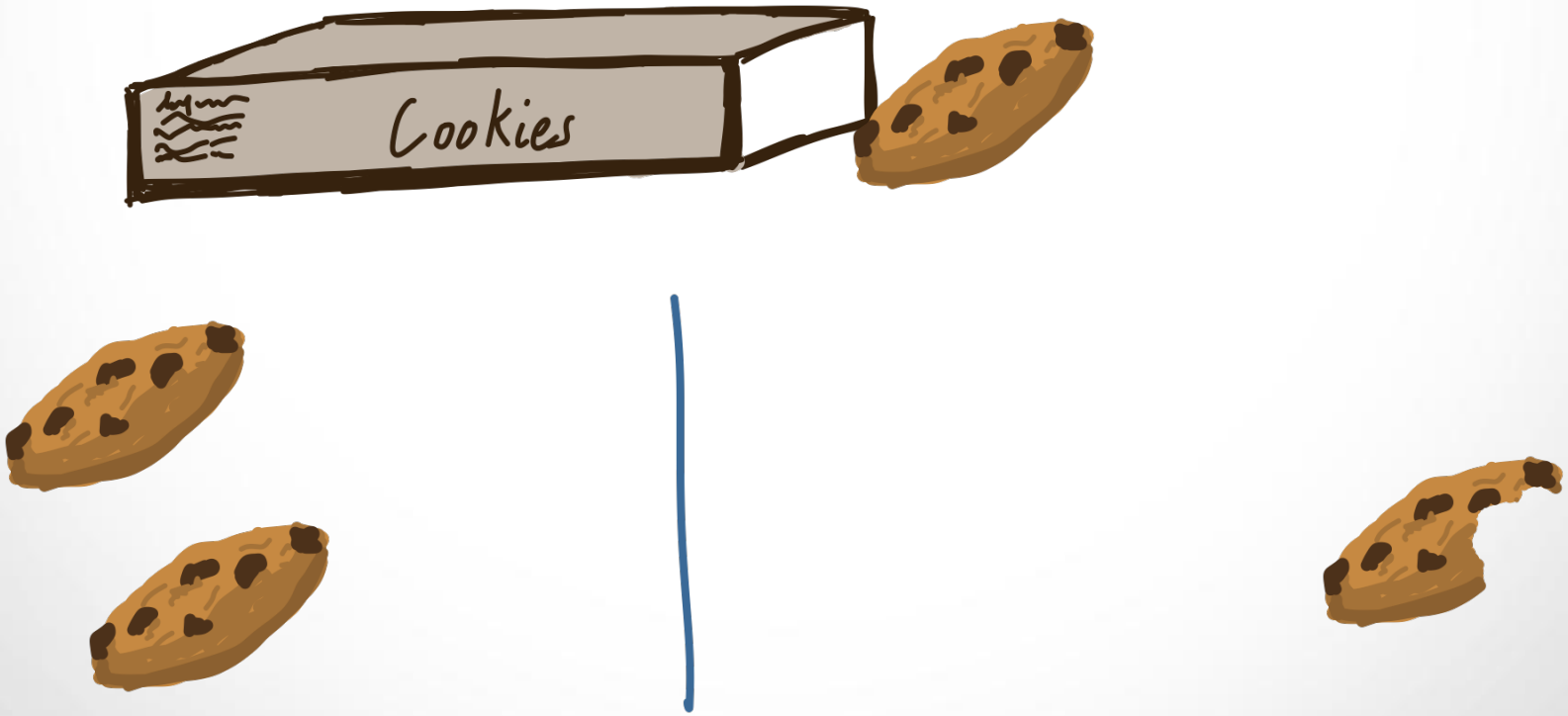
# Zero Proof Knowledge

The magic cookie



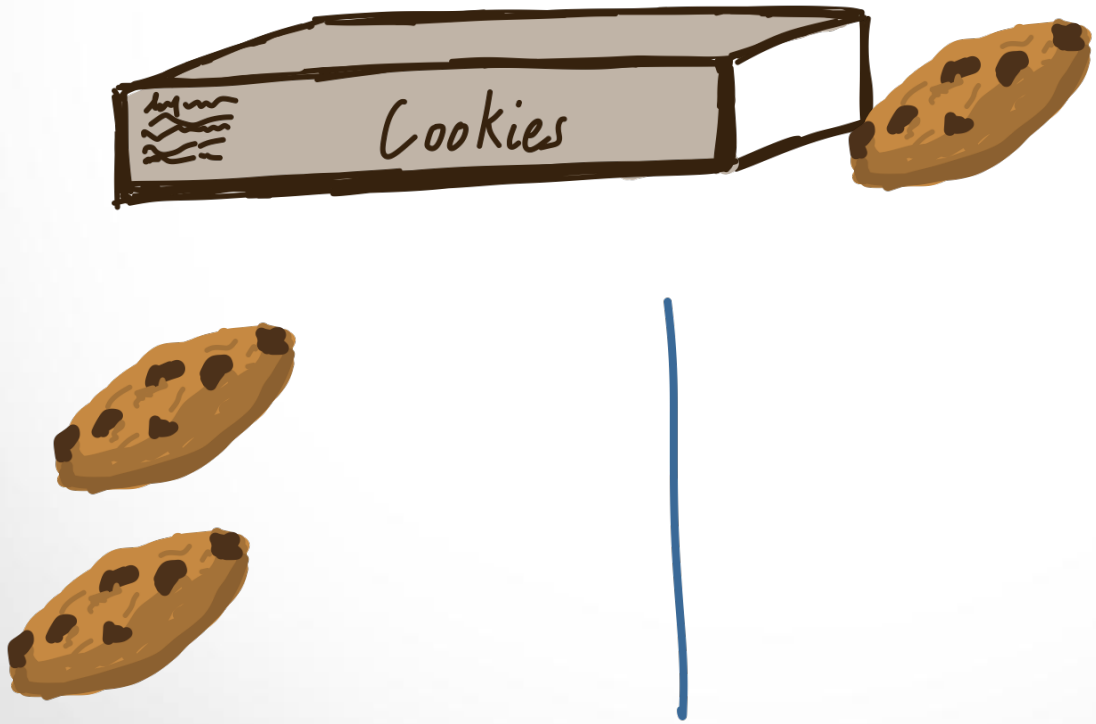
# Zero Proof Knowledge

The magic cookie



# Zero Proof Knowledge

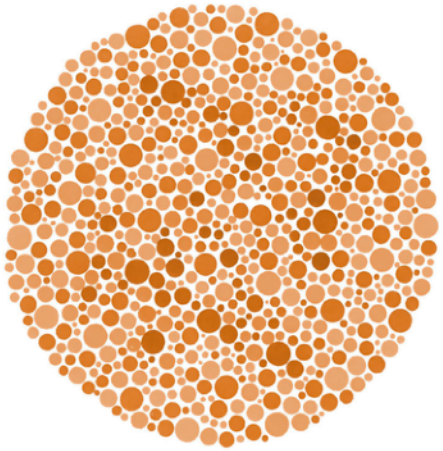
The magic cookie



# Zero Proof Knowledge

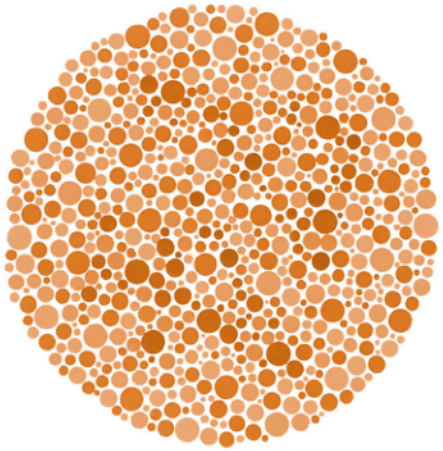
The magic cookie


# Zero Proof Knowledge



How do color blind people know they are different

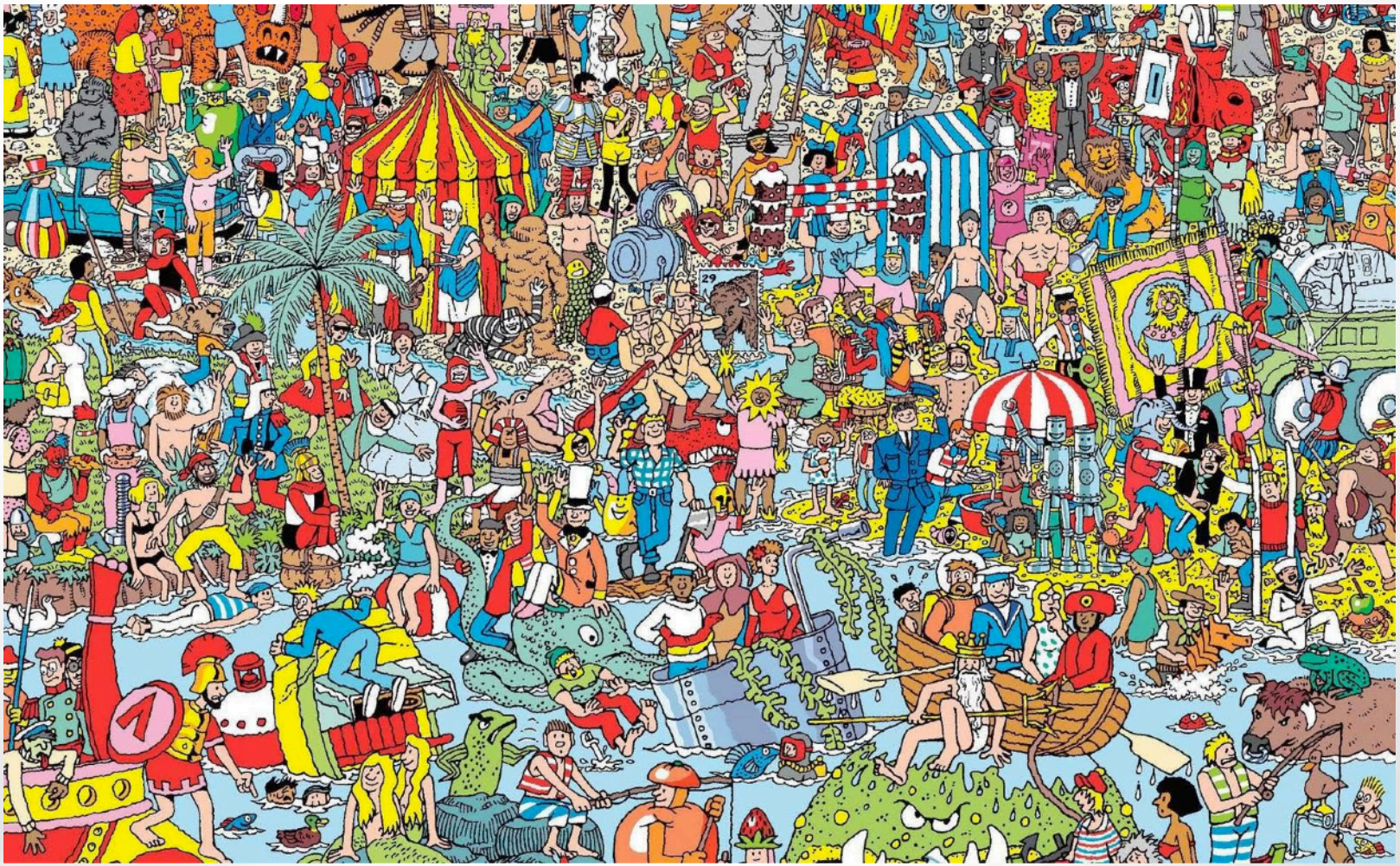
# Zero Proof Knowledge



How do color blind people know they are different

And that its not just a prank ?

# Zero Proof Knowledge



# Zero Proof Knowledge

Naor, M., Naor, Y., & Reingold, O. (1999, March). Applied kid cryptography or how to convince your children you are not cheating. In Eurocrypt'94

# Zero Proof Knowledge

# Zero Proof Knowledge

How do you know you own a Bitcoin ?

# Zero Proof Knowledge

How do you know you own a Bitcoin ?

You have the private key associated with an address that has a Bitcoin

# Zero Proof Knowledge

How do you know you own a Bitcoin ?

You have the private key associated with an address that has a Bitcoin

How do others know you own a Bitcoin ?

# Zero Proof Knowledge

How do you know you own a Bitcoin ?

You have the private key associated with an address that has a Bitcoin

How do others know you own a Bitcoin ?

You show them the address that has a Bitcoin, and you can prove that you have the private key, without revealing it.

# Zero Proof Knowledge

How do you know you own a Bitcoin ?

You have the private key associated with an address that has a Bitcoin

How do others know you own a Bitcoin ?

You show them the address that has a Bitcoin, and you can prove that you have the private key, without revealing it.

What if I don’t want to show them the address ?

# Zero Proof Knowledge

How do you know you own a Bitcoin ?

You have the private key associated with an address that has a Bitcoin

How do others know you own a Bitcoin ?

You show them the address that has a Bitcoin, and you can prove that you have the private key, without revealing it.

What if I don’t want to show them the address ?

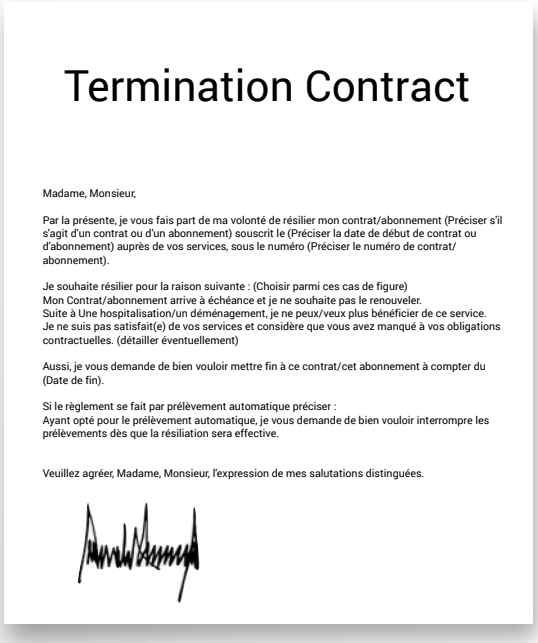
There are ways to prove it without revealing anything

- Decentralized Democracy
- Crypto kitties
- Ensuring Documents Validity

# Blockchains

- Distributed Systems
- Zero Knowledge Proof

# Ensuring Documents Validity



## Termination Contract

Madame, Monsieur,

Par la présente, je vous fais part de ma volonté de résilier mon contrat/abonnement (Préciser s'il s'agit d'un contrat ou d'un abonnement) souscrit le (Préciser la date de début de contrat ou d'abonnement) auprès de vos services, sous le numéro (Préciser le numéro de contrat/ abonnement).

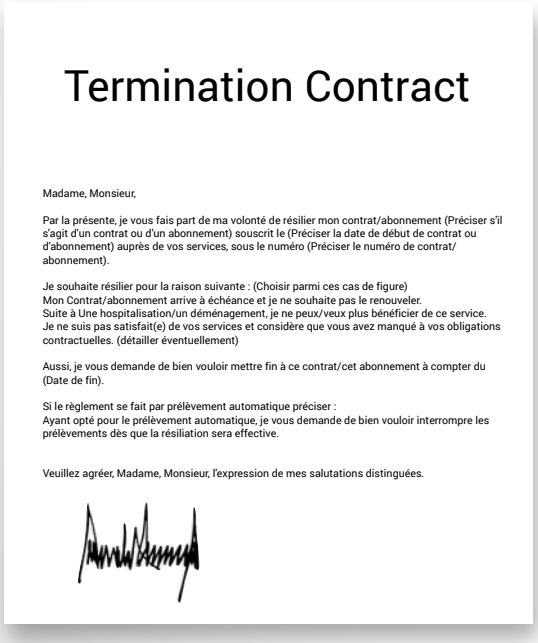
Je souhaite résilier pour la raison suivante : (Choisir parmi ces cas de figure)
Mon Contrat/abonnement arrive à échéance et je ne souhaite pas le renouveler.
Suite à Une hospitalisation/un déménagement, je ne peux/veux plus bénéficier de ce service.
Je ne suis pas satisfait(e) de vos services et considère que vous avez manqué à vos obligations contractuelles. (détailler éventuellement)

Aussi, je vous demande de bien vouloir mettre fin à ce contrat/cet abonnement à compter du (Date de fin).

Si le règlement se fait par prélèvement automatique préciser :
Ayant opté pour le prélèvement automatique, je vous demande de bien vouloir interrompre les prélèvements dès que la résiliation sera effective.

Veuillez agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

# Ensuring Documents Validity



Termination Contract

Madame, Monsieur,

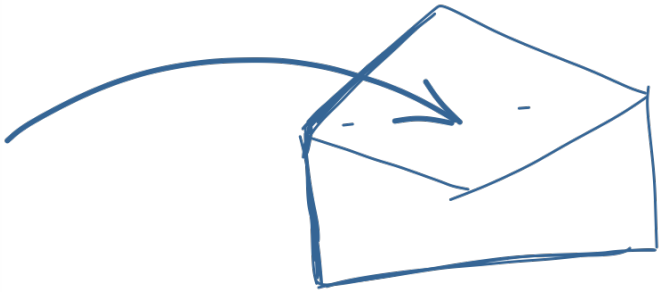
Par la présente, je vous fais part de ma volonté de résilier mon contrat/abonnement (Préciser s'il s'agit d'un contrat ou d'un abonnement) souscrit le (Préciser la date de début de contrat ou d'abonnement) auprès de vos services, sous le numéro (Préciser le numéro de contrat/ abonnement).

Je souhaite résilier pour la raison suivante : (Choisir parmi ces cas de figure)
Mon Contrat/abonnement arrive à échéance et je ne souhaite pas le renouveler.
Suite à Une hospitalisation/un déménagement, je ne peux/veux plus bénéficier de ce service.
Je ne suis pas satisfait(e) de vos services et considère que vous avez manqué à vos obligations contractuelles. (détailler éventuellement)

Aussi, je vous demande de bien vouloir mettre fin à ce contrat/cet abonnement à compter du (Date de fin).

Si le règlement se fait par prélèvement automatique préciser :
Ayant opté pour le prélèvement automatique, je vous demande de bien vouloir interrompre les prélèvements dès que la résiliation sera effective.

Veuillez agréer, Madame, Monsieur, l'expression de mes salutations distinguées.



# Ensuring Documents Validity

## Termination Contract

Madame, Monsieur,

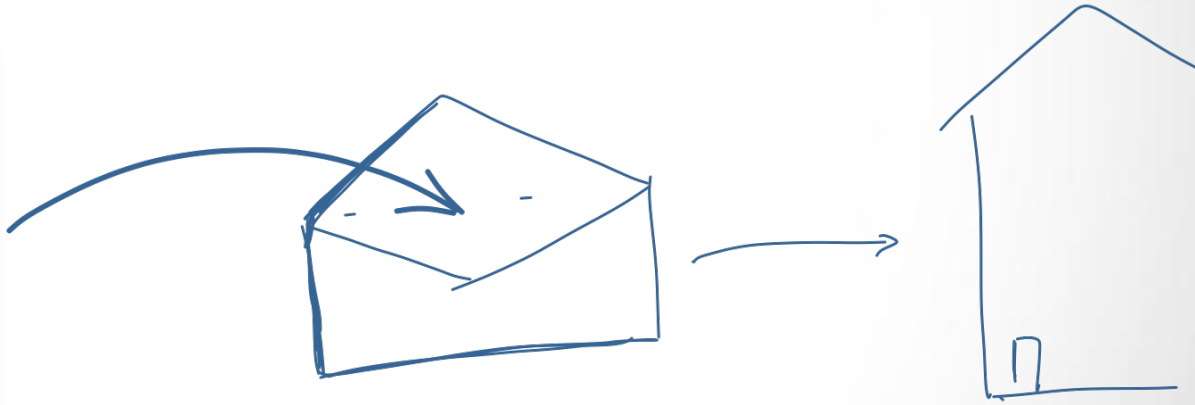
Par la présente, je vous fais part de ma volonté de résilier mon contrat/abonnement (Préciser s'il s'agit d'un contrat ou d'un abonnement) souscrit le (Préciser la date de début de contrat ou d'abonnement) auprès de vos services, sous le numéro (Préciser le numéro de contrat/ abonnement).

Je souhaite résilier pour la raison suivante : (Choisir parmi ces cas de figure)
Mon Contrat/abonnement arrive à échéance et je ne souhaite pas le renouveler.
Suite à Une hospitalisation/un déménagement, je ne peux/veux plus bénéficier de ce service.
Je ne suis pas satisfait(e) de vos services et considère que vous avez manqué à vos obligations contractuelles. (détailler éventuellement)

Aussi, je vous demande de bien vouloir mettre fin à ce contrat/cet abonnement à compter du (Date de fin).

Si le règlement se fait par prélèvement automatique préciser :
Ayant opté pour le prélèvement automatique, je vous demande de bien vouloir interrompre les prélèvements dès que la résiliation sera effective.

Veuillez agréer, Madame, Monsieur, l'expression de mes salutations distinguées.



# Ensuring Documents Validity

## Termination Contract

Madame, Monsieur,

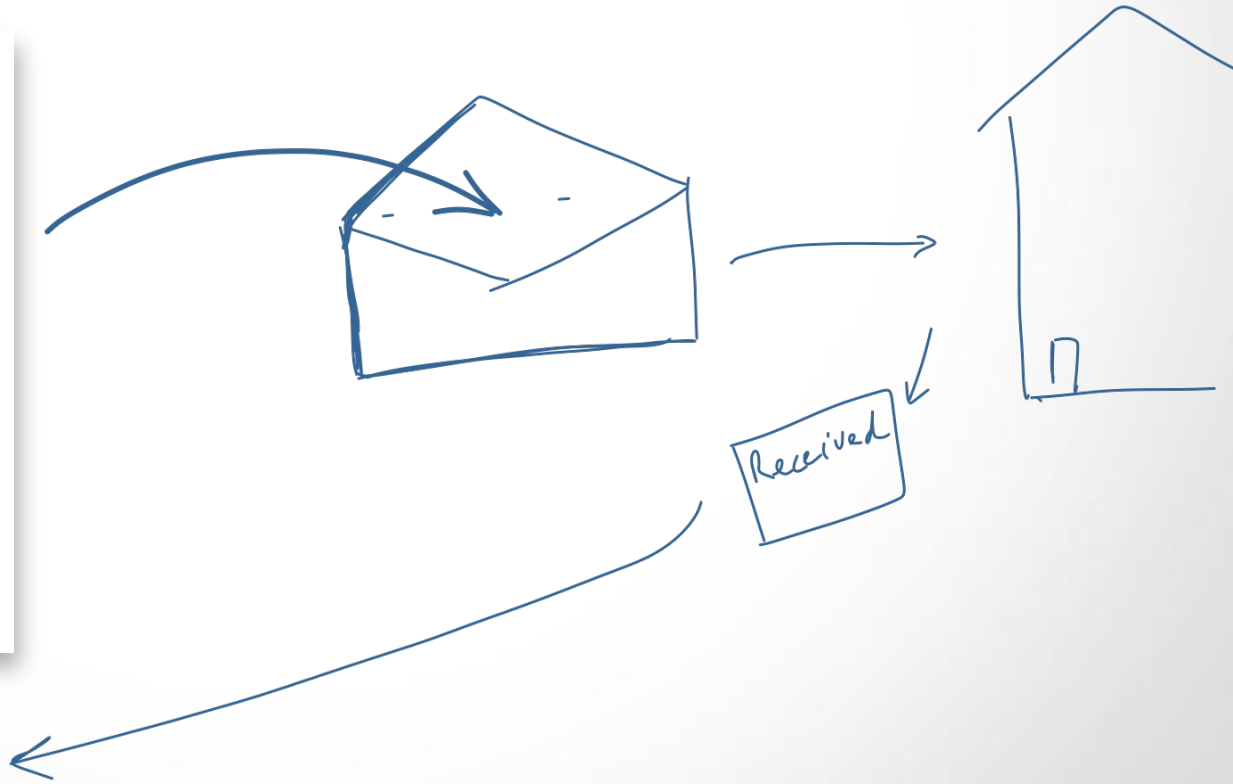
Par la présente, je vous fais part de ma volonté de résilier mon contrat/abonnement (Préciser s'il s'agit d'un contrat ou d'un abonnement) souscrit le (Préciser la date de début de contrat ou d'abonnement) auprès de vos services, sous le numéro (Préciser le numéro de contrat/ abonnement).

Je souhaite résilier pour la raison suivante : (Choisir parmi ces cas de figure)
Mon Contrat/abonnement arrive à échéance et je ne souhaite pas le renouveler.
Suite à Une hospitalisation/un déménagement, je ne peux/veux plus bénéficier de ce service.
Je ne suis pas satisfait(e) de vos services et considère que vous avez manqué à vos obligations contractuelles. (détailler éventuellement)

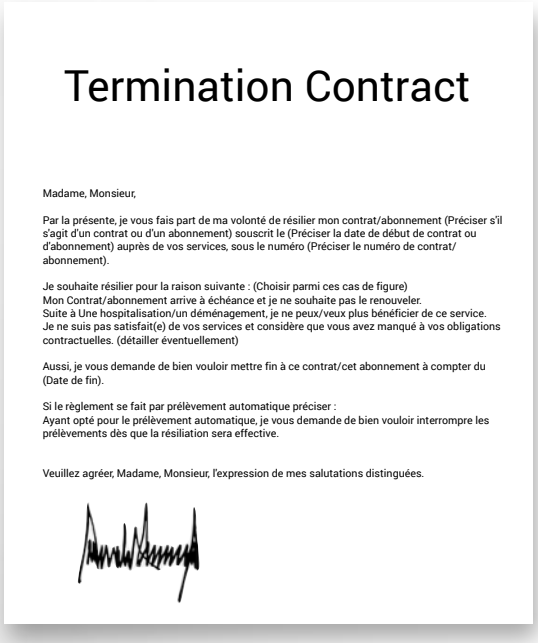
Aussi, je vous demande de bien vouloir mettre fin à ce contrat/cet abonnement à compter du (Date de fin).

Si le règlement se fait par prélèvement automatique préciser :
Ayant opté pour le prélèvement automatique, je vous demande de bien vouloir interrompre les prélèvements dès que la résiliation sera effective.

Veuillez agréer, Madame, Monsieur, l'expression de mes salutations distinguées.



# Ensuring Documents Validity



Termination Contract

Madame, Monsieur,

Par la présente, je vous fais part de ma volonté de résilier mon contrat/abonnement (Préciser s'il s'agit d'un contrat ou d'un abonnement) souscrit le (Préciser la date de début de contrat ou d'abonnement) auprès de vos services, sous le numéro (Préciser le numéro de contrat/ abonnement).

Je souhaite résilier pour la raison suivante : (Choisir parmi ces cas de figure)
Mon Contrat/abonnement arrive à échéance et je ne souhaite pas le renouveler.
Suite à Une hospitalisation/un déménagement, je ne peux/veux plus bénéficier de ce service.
Je ne suis pas satisfait(e) de vos services et considère que vous avez manqué à vos obligations contractuelles. (détailler éventuellement)

Aussi, je vous demande de bien vouloir mettre fin à ce contrat/cet abonnement à compter du (Date de fin).

Si le règlement se fait par prélèvement automatique préciser :
Ayant opté pour le prélèvement automatique, je vous demande de bien vouloir interrompre les prélèvements dès que la résiliation sera effective.

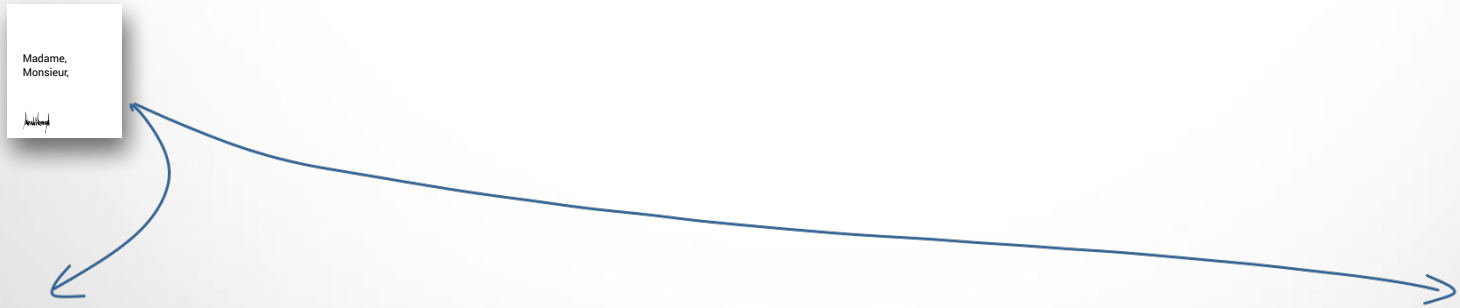
Veuillez agréer, Madame, Monsieur, l'expression de mes salutations distinguées.




56fde8f4392113e0f19e0430f14502e06968669f

# Ensuring Documents Validity

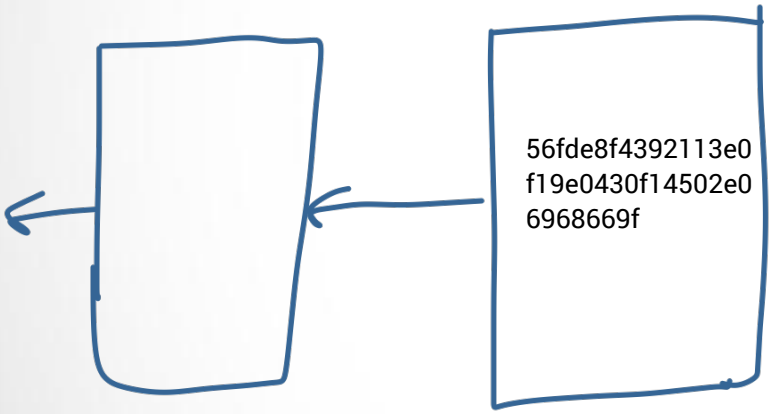
56fde8f4392113e0
f19e0430f14502e0
6968669f



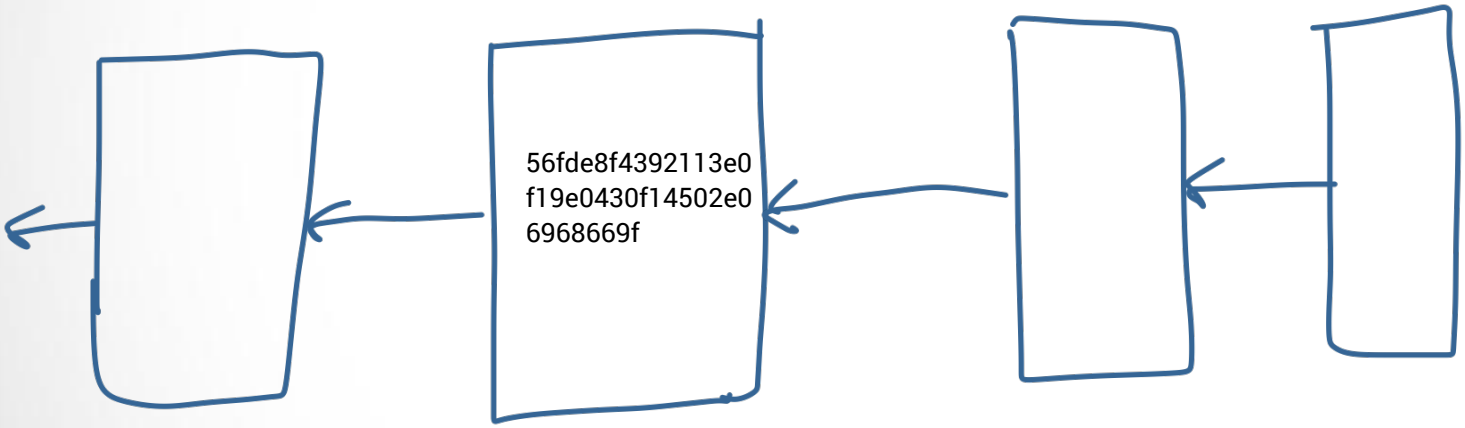
# Ensuring Documents Validity

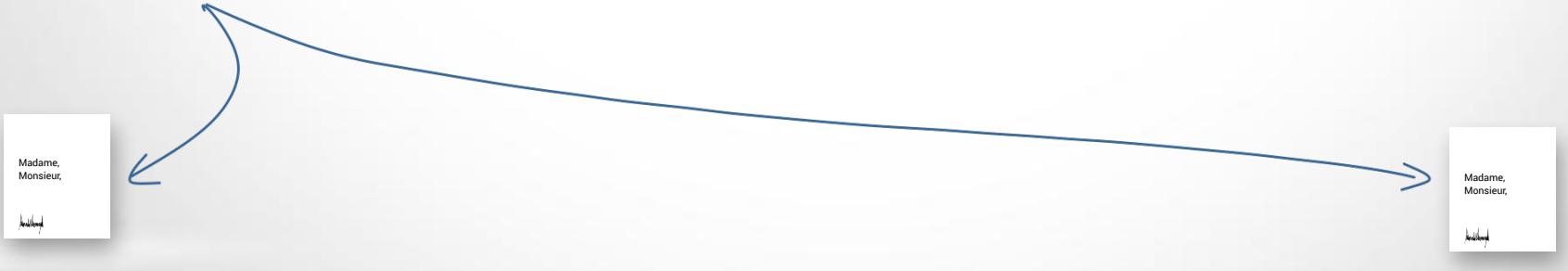
56fde8f4392113e0
f19e0430f14502e0
6968669f

# Ensuring Documents Validity



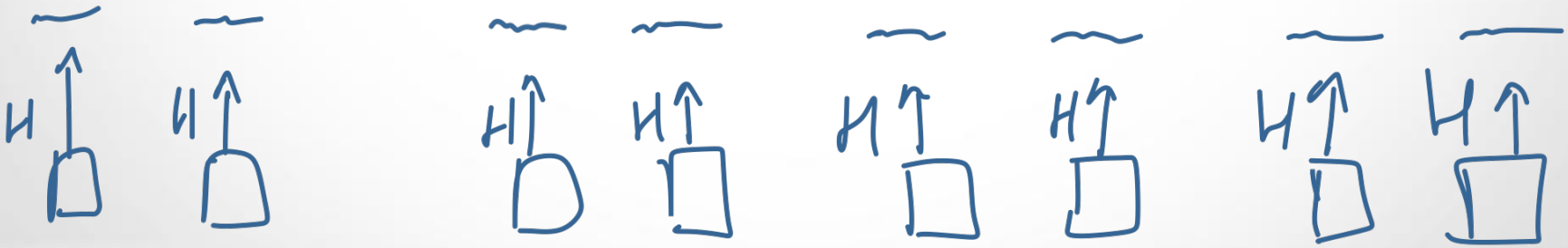

# Ensuring Documents Validity



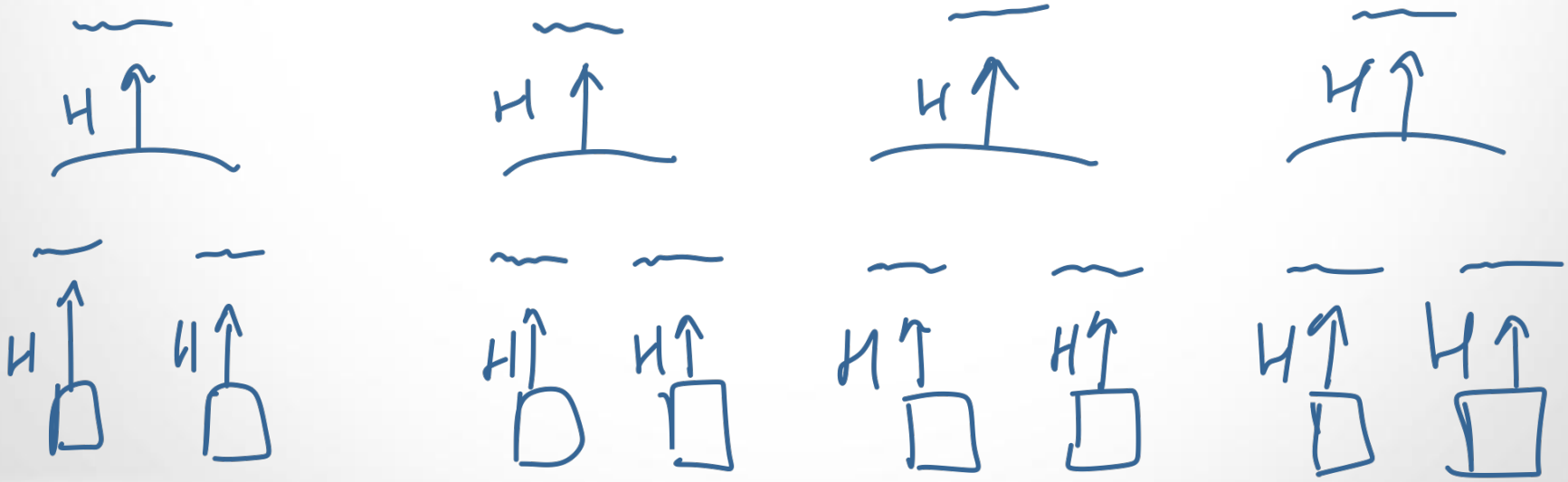



# Ensuring Documents Validity

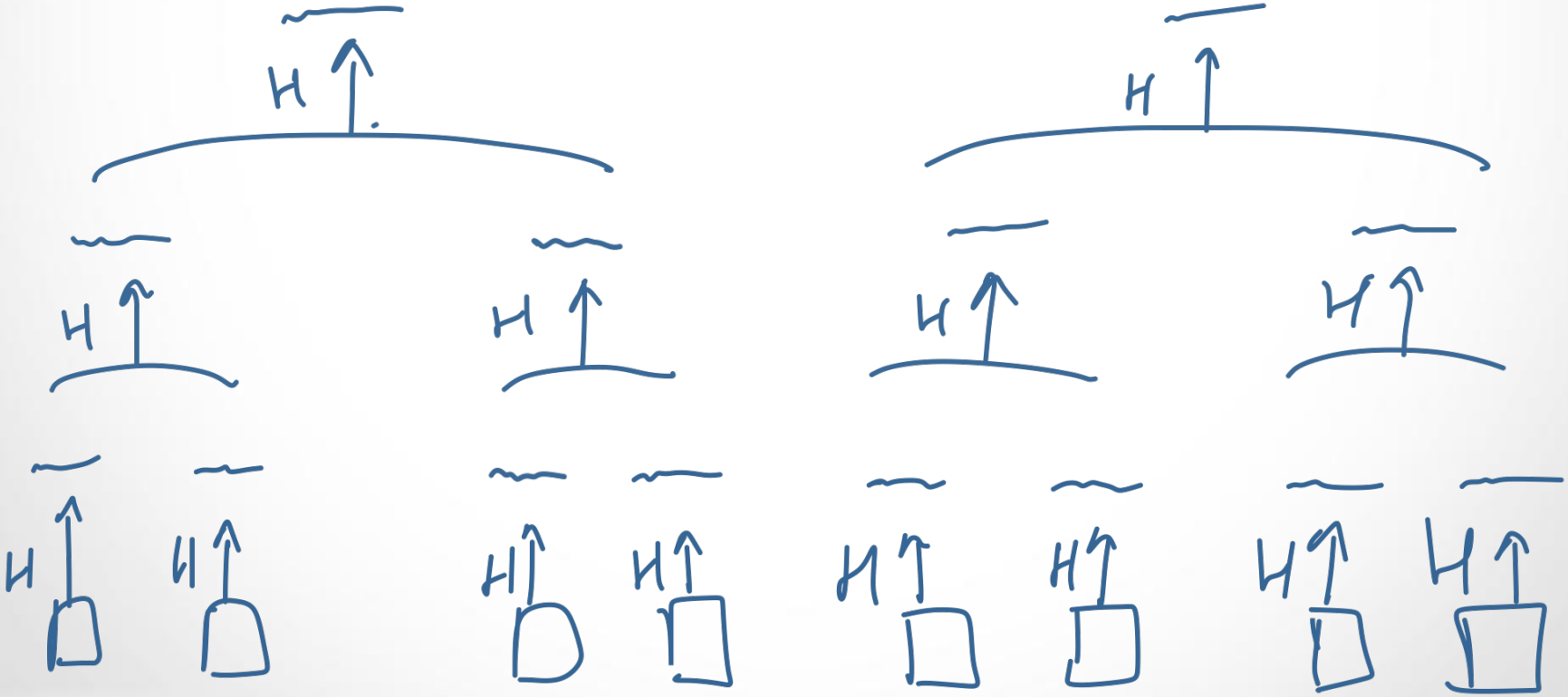
# Ensuring Documents Validity



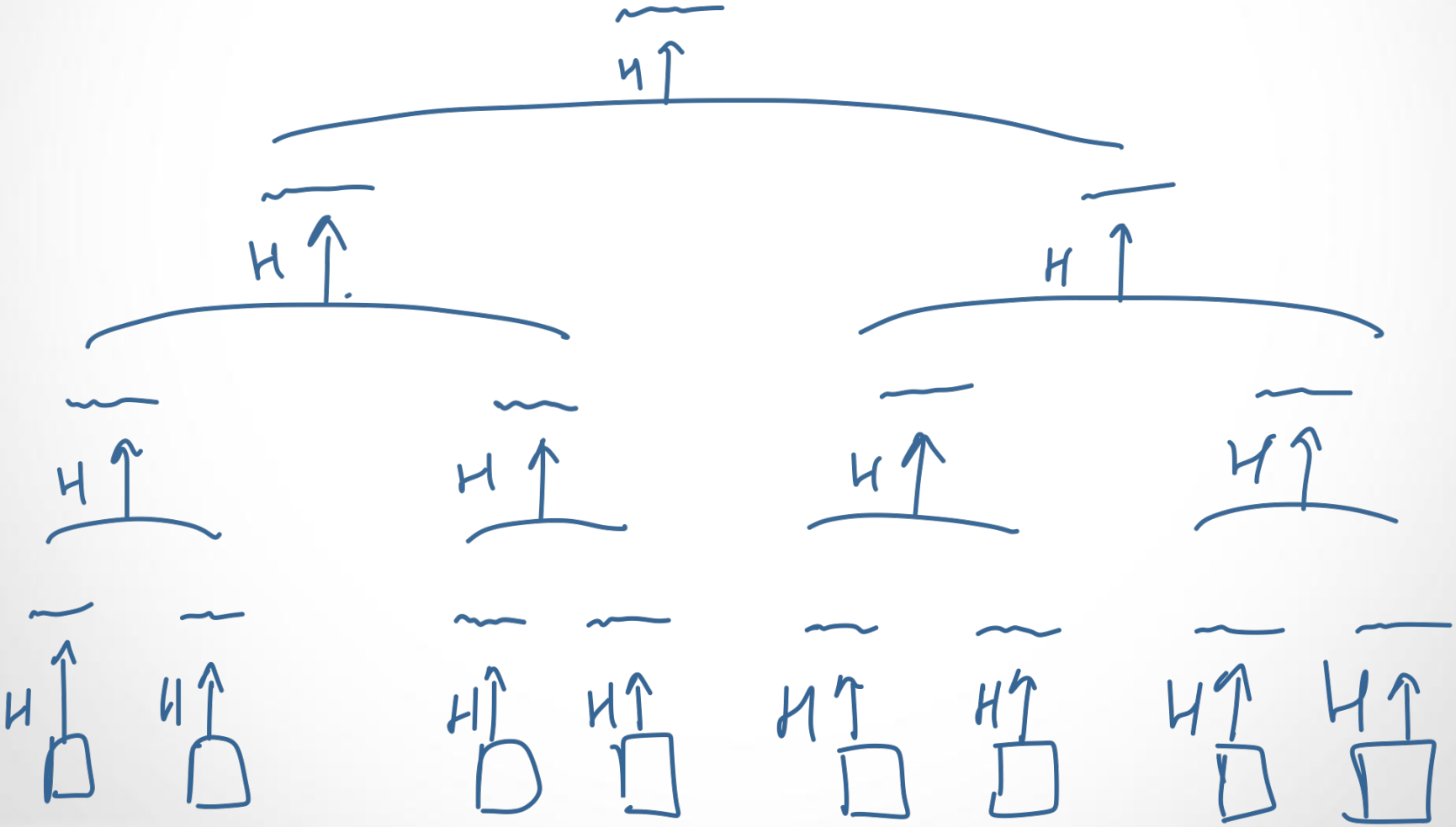
# Ensuring Documents Validity



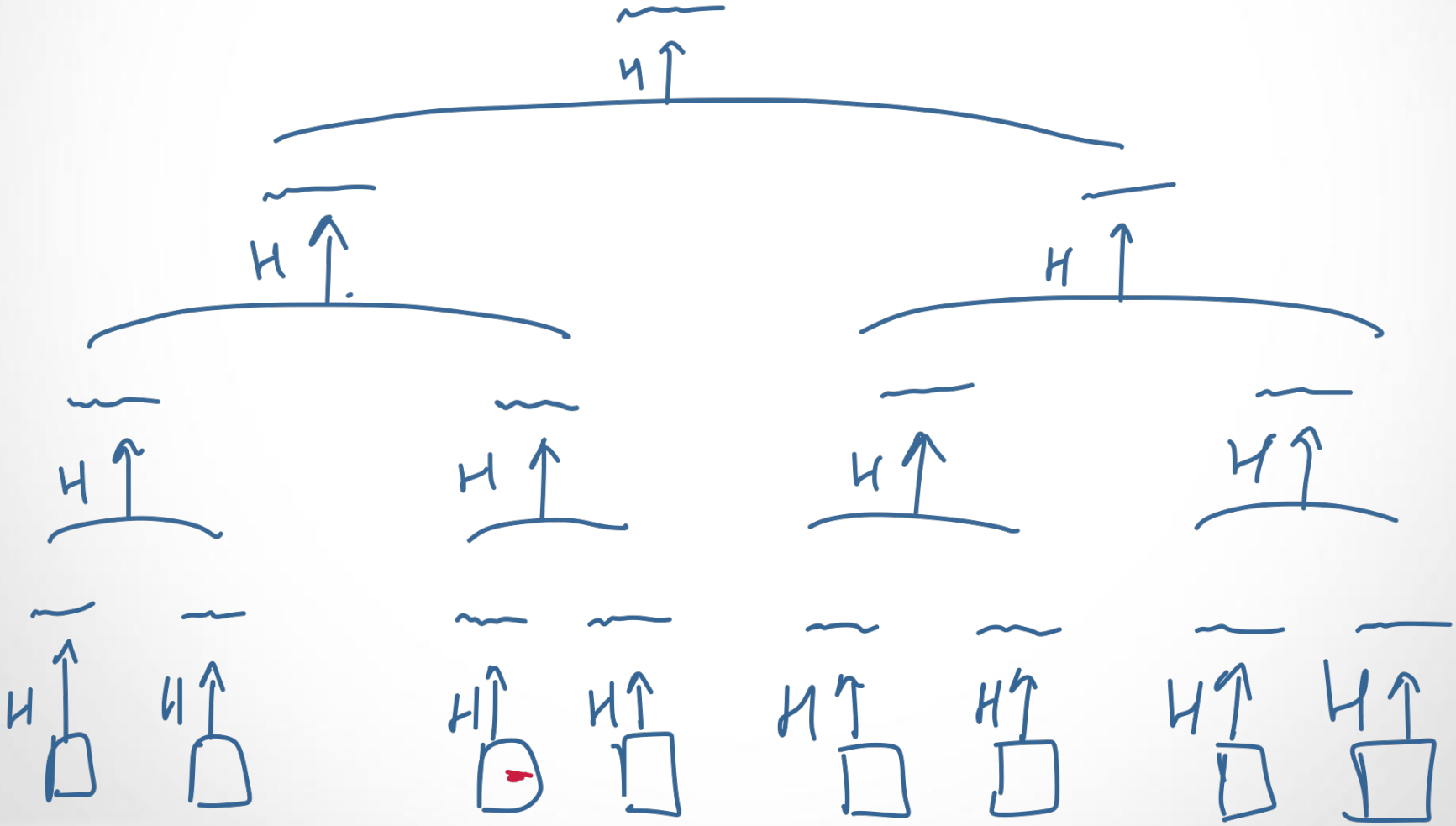
# Ensuring Documents Validity



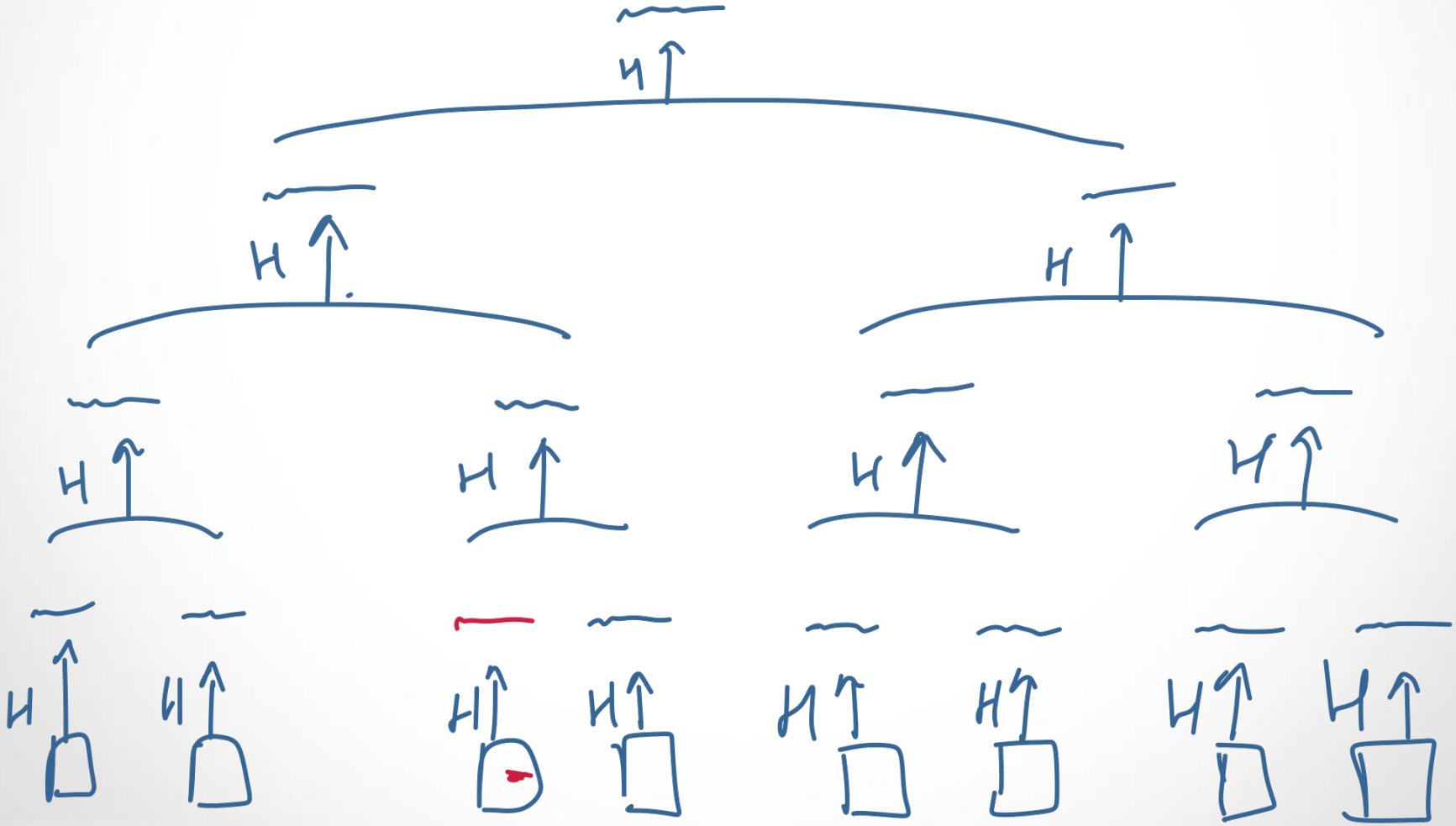
# Ensuring Documents Validity



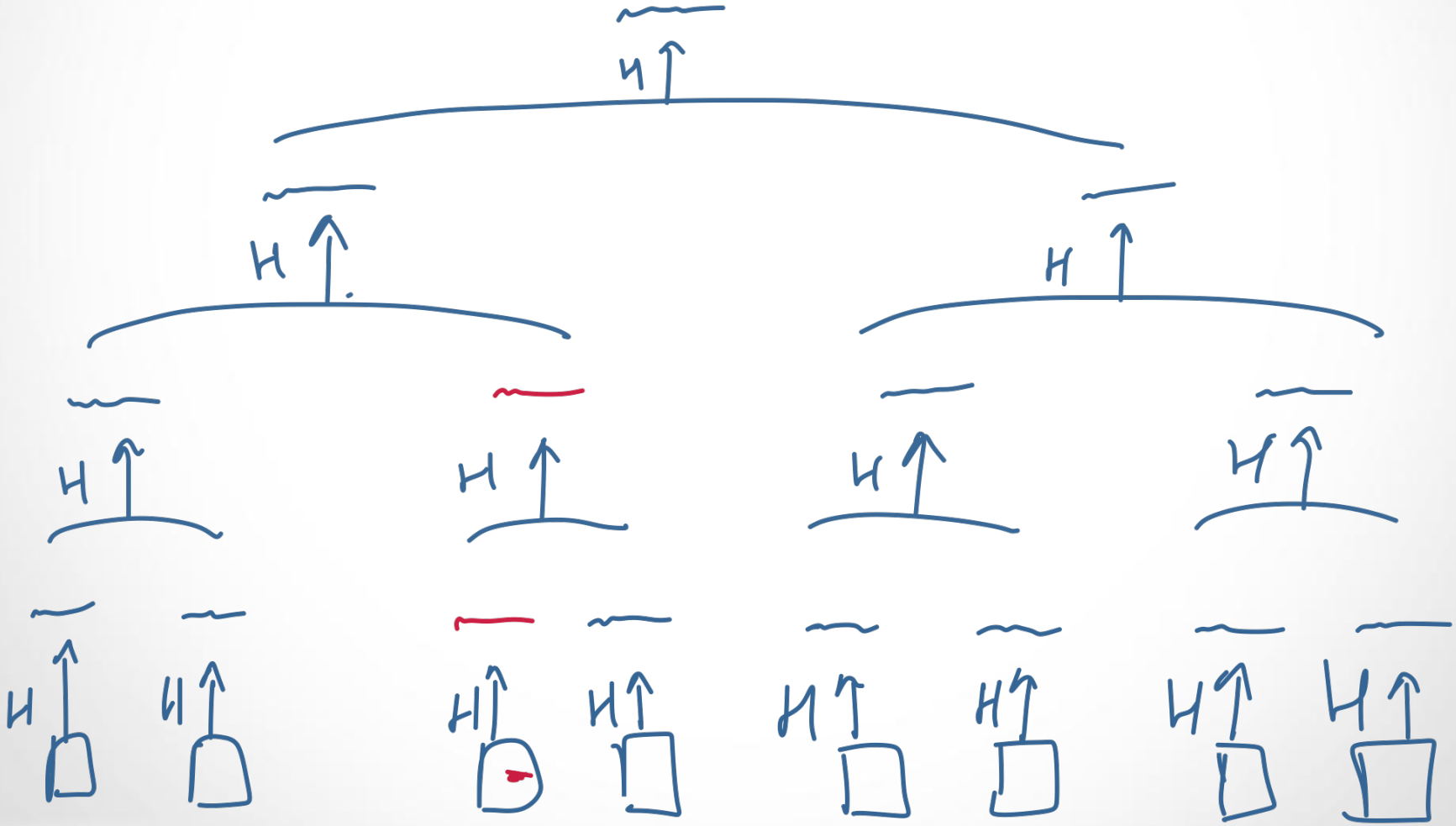
# Ensuring Documents Validity



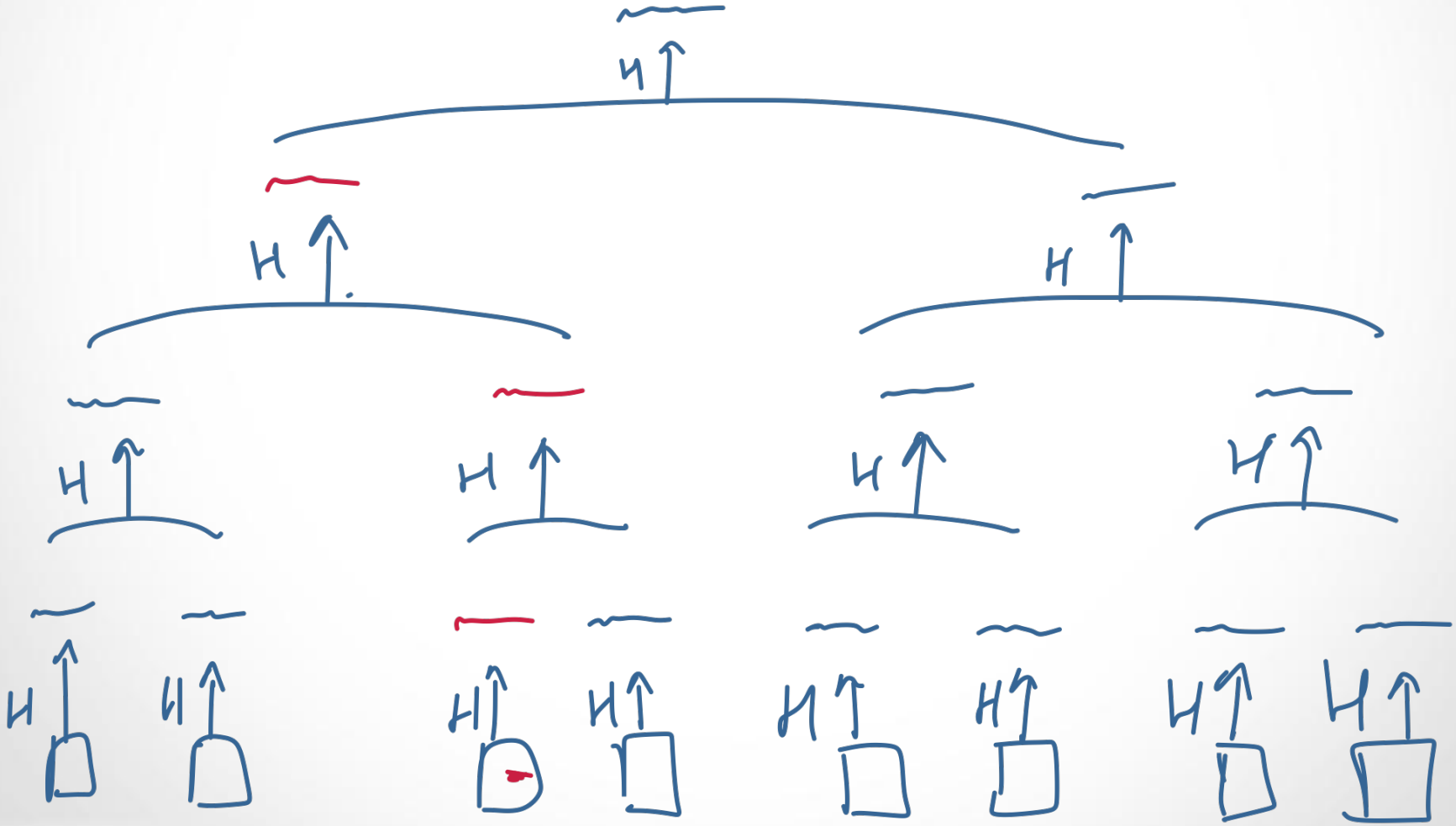
# Ensuring Documents Validity



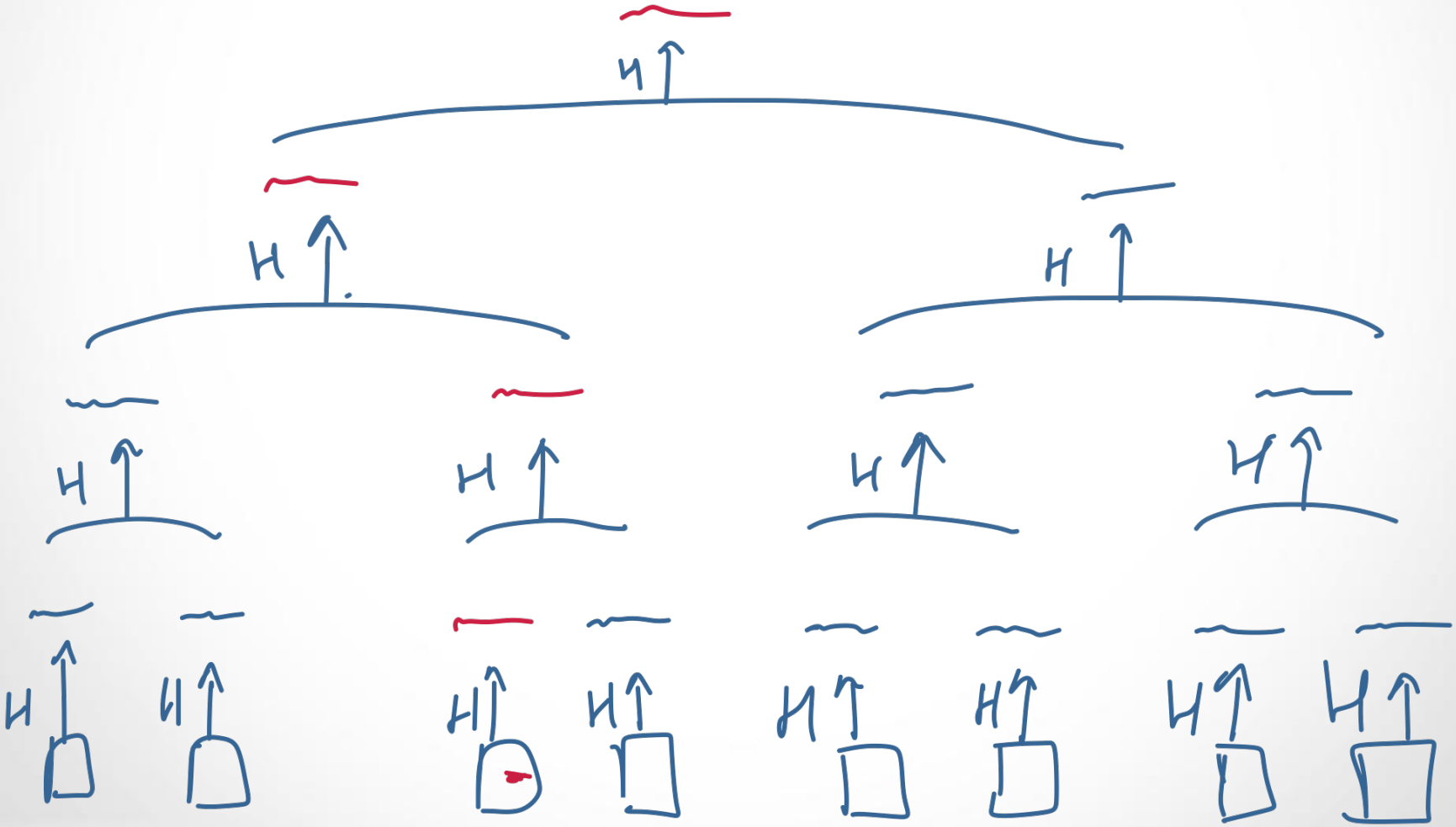
# Ensuring Documents Validity



# Ensuring Documents Validity



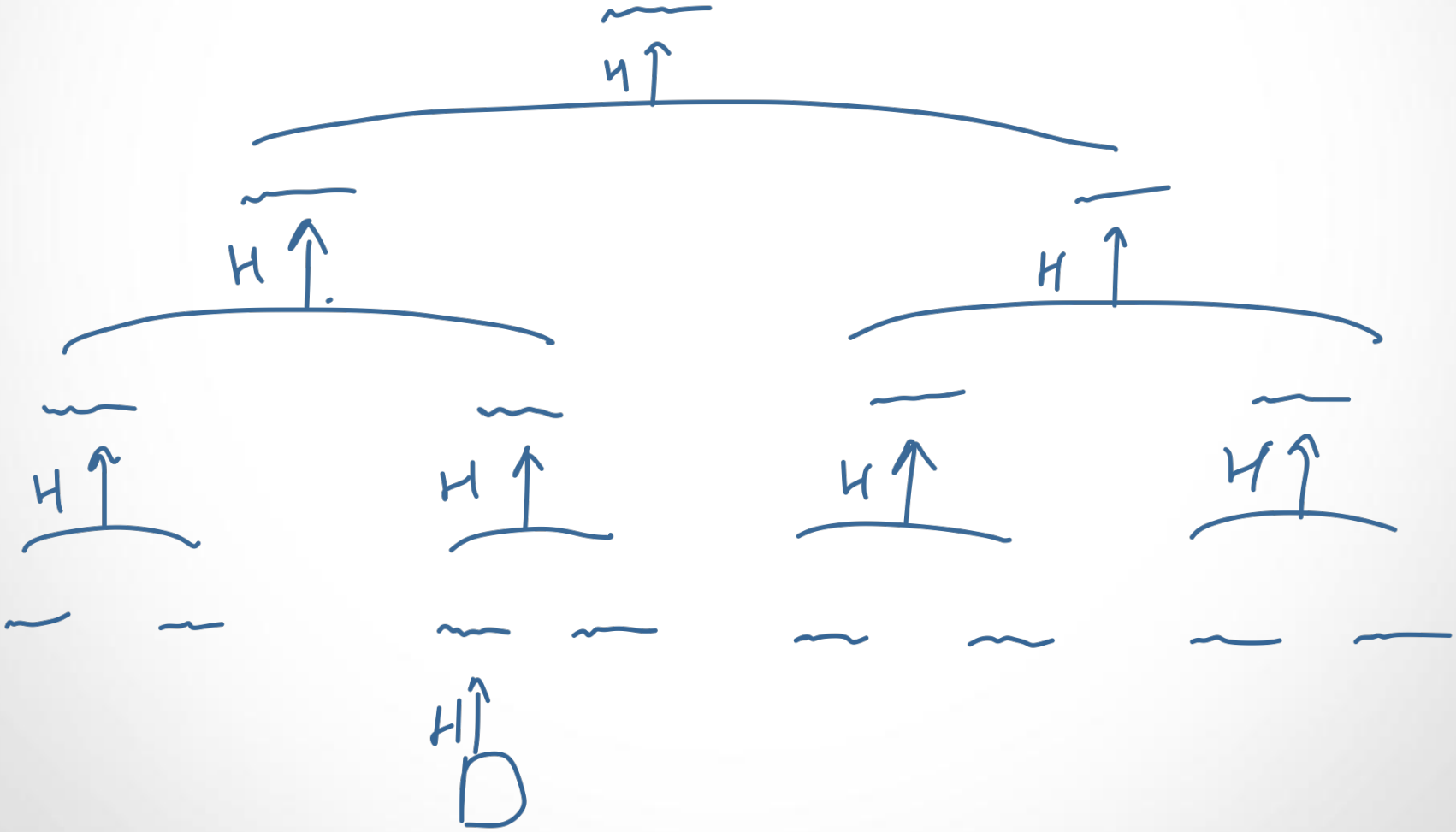
# Ensuring Documents Validity



# Ensuring Documents Validity

# Ensuring Documents Validity

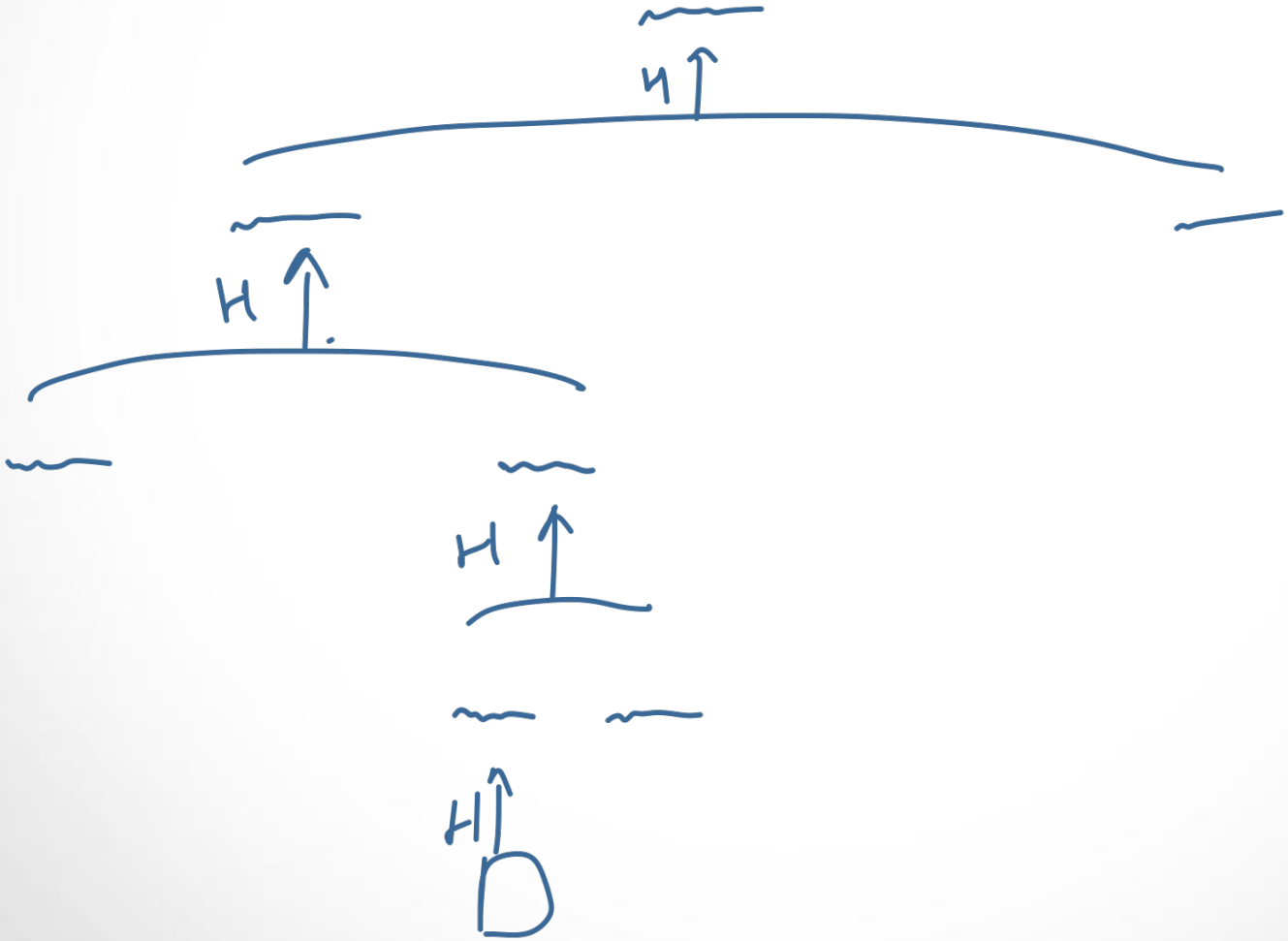
# Ensuring Documents Validity



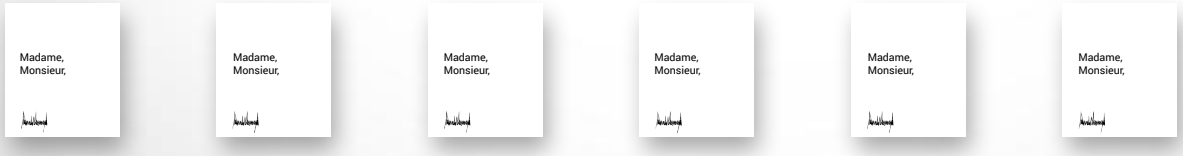
# Ensuring Documents Validity

# Ensuring Documents Validity

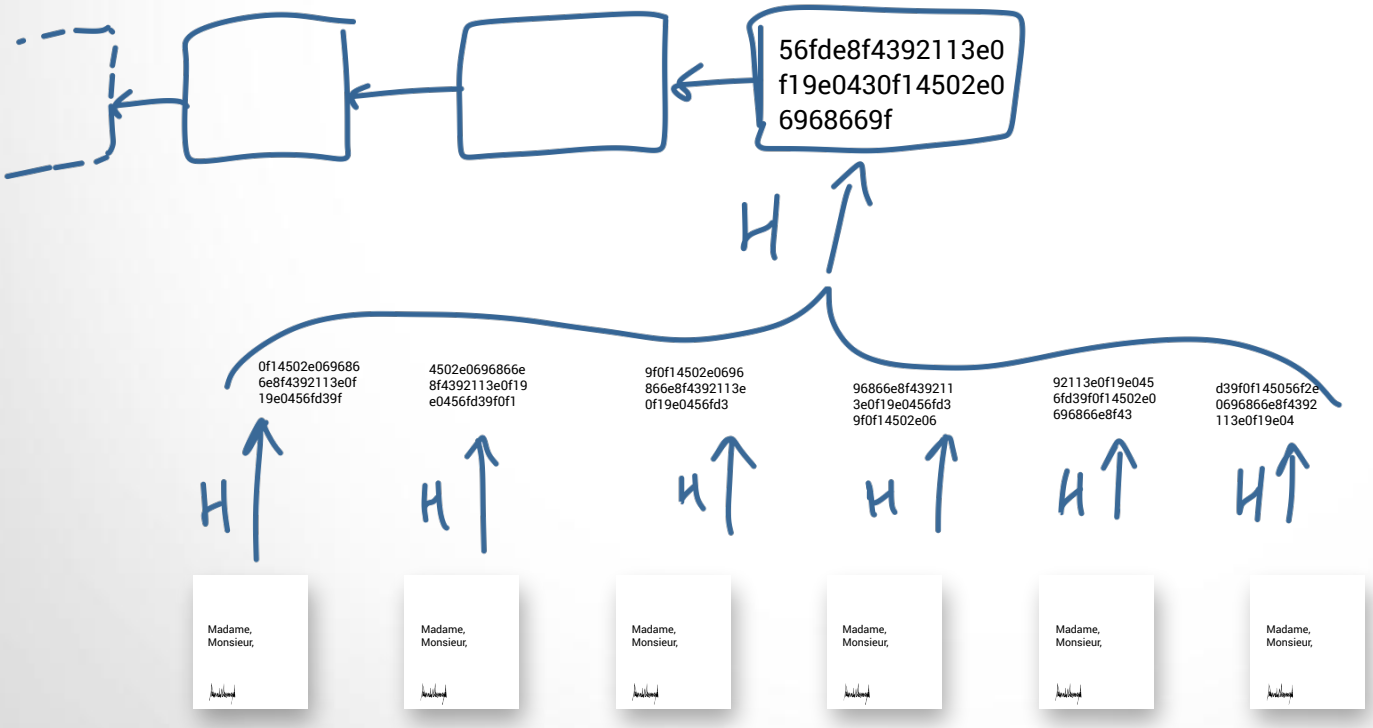
# Ensuring Documents Validity



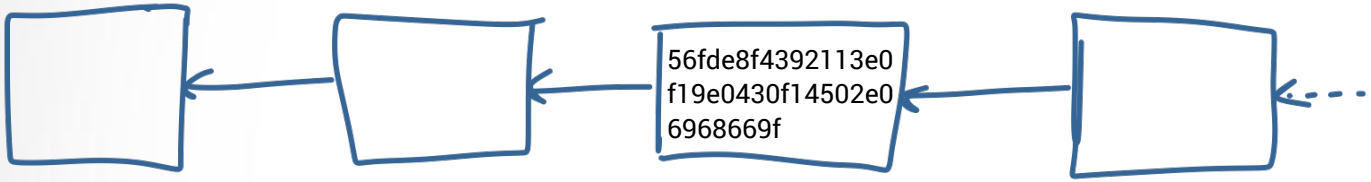
# Ensuring Documents Validity



# Ensuring Documents Validity



# Ensuring Documents Validity




0f14502e069686
6e8f4392113e0f
19e0456fd39f

4502e0696866e
8f4392113e0f19
e0456fd39f0f1

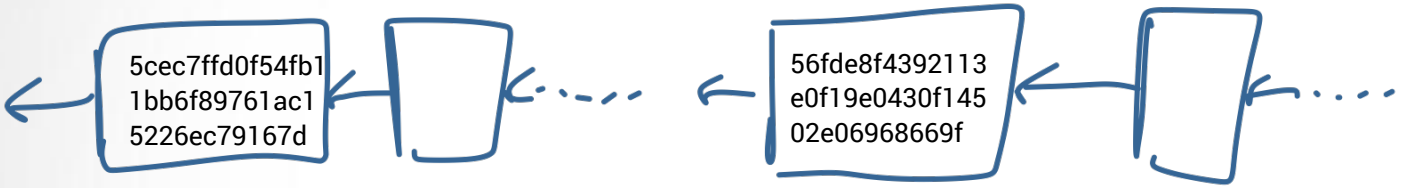
9f0f14502e0696
866e8f4392113e
0f19e0456fd3

96866e8f439211
3e0f19e0456fd3
9f0f14502e06


92113e0f19e045
6fd39f0f14502e0
696866e8f43

d39f0f145056f2e
0696866e8f4392
113e0f19e04

# Ensuring Documents Validity




| | |
|---|---|
| First Name: | d6b8e48afb2534b213e391cab43016505747a234 |
| Last Name: | fa39bdc32115035effac9cdb73eff395ffcd40b2 |
| Father: | 5cec7ffd0f54fb11bb6f89761ac15226ec79167d |
| Mother: | 98654643491feb0f5d56ad17af3d19a32133cfa2 |
| Place of Birth: | b7e52024f8bffe251fa6b7011447c437361a6ba8 |
| Birthdate: | a9823f275d898fd8dcc83e72602311ebcdf6718f |

- Decentralized Democracy
- Crypto kitties
- Ensuring Documents Validity

# Blockchains

- Distributed Systems
- Zero Knowledge Proof

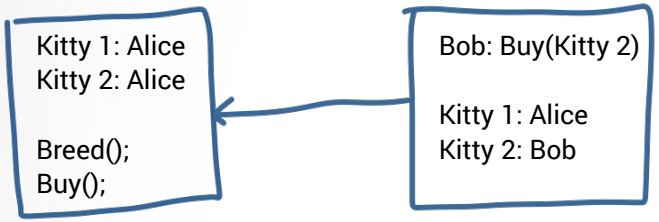
# Crypto Kitties

# Crypto Kitties

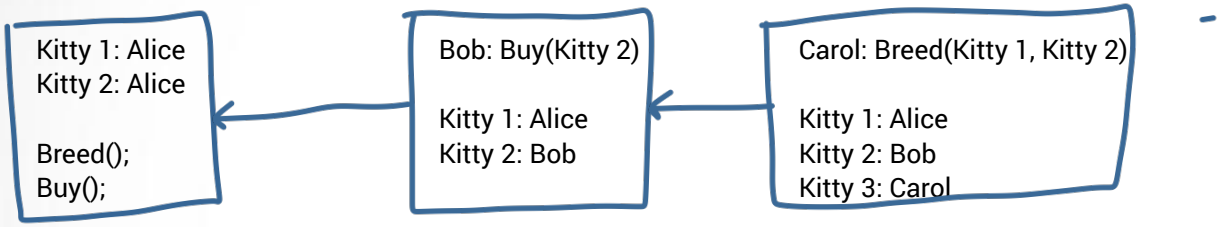
Kitty 1: Alice
Kitty 2: Alice

Breed();
Buy();

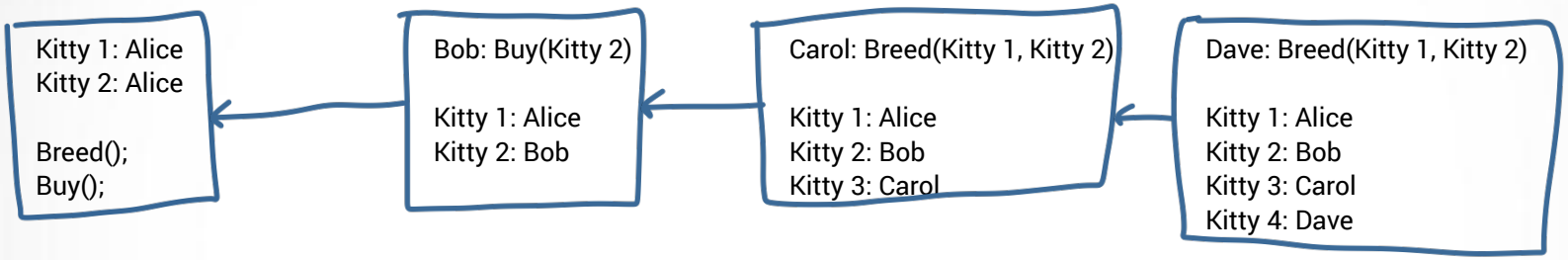
# Crypto Kitties

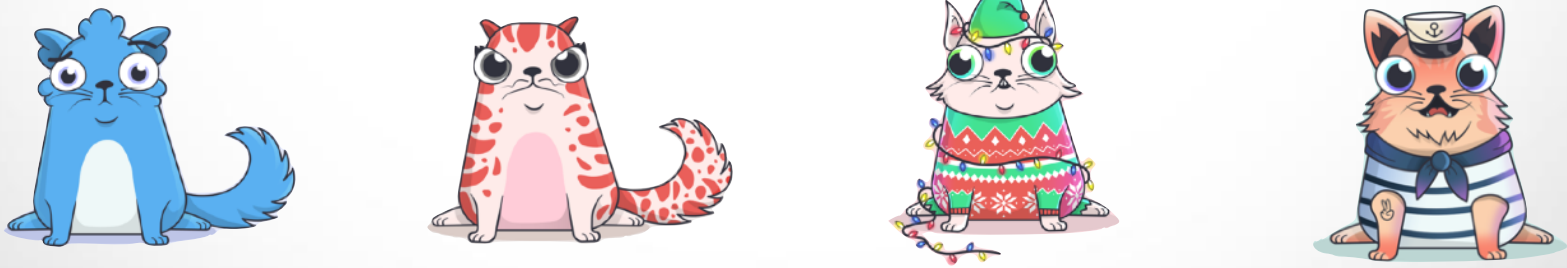



# Crypto Kitties




# Crypto Kitties



# Supply Chain

Alice Ent.

Bob Ent.

Carol Ent.

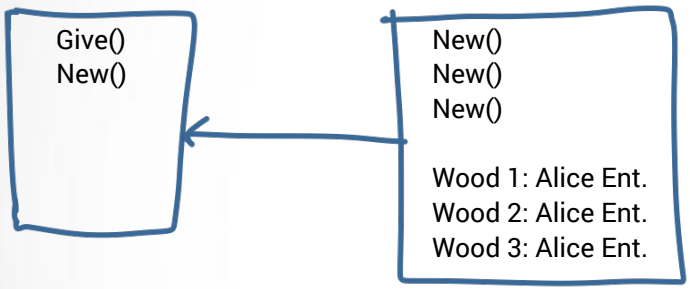
# Supply Chain


Alice Ent.

Bob Ent.

Carol Ent.

# Supply Chain

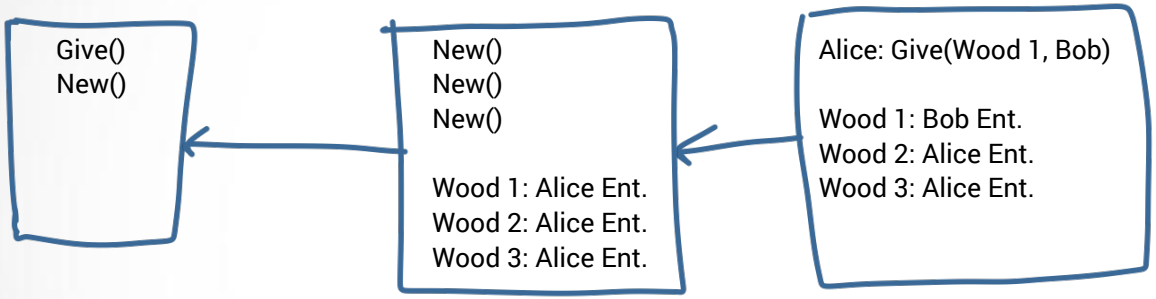



Alice Ent.

Bob Ent.

Carol Ent.

# Supply Chain

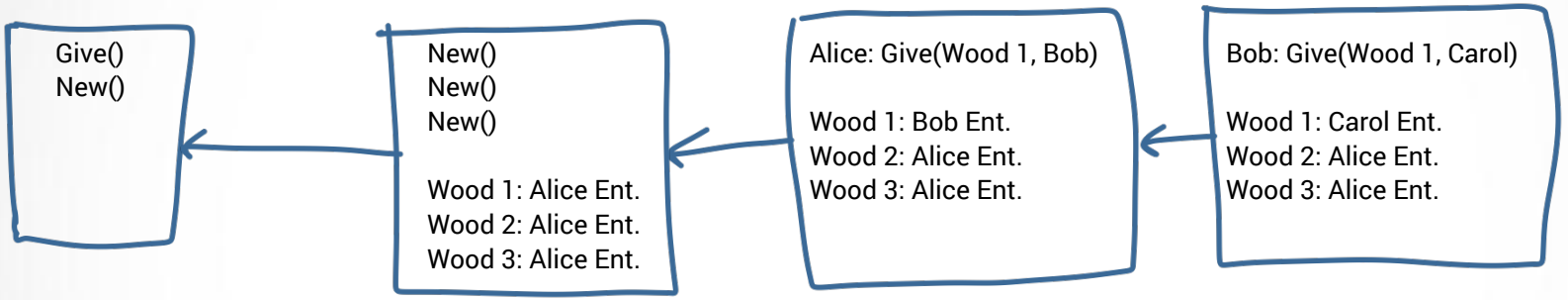



Alice Ent.

Bob Ent.

Carol Ent.

# Supply Chain




Alice Ent.

Bob Ent.

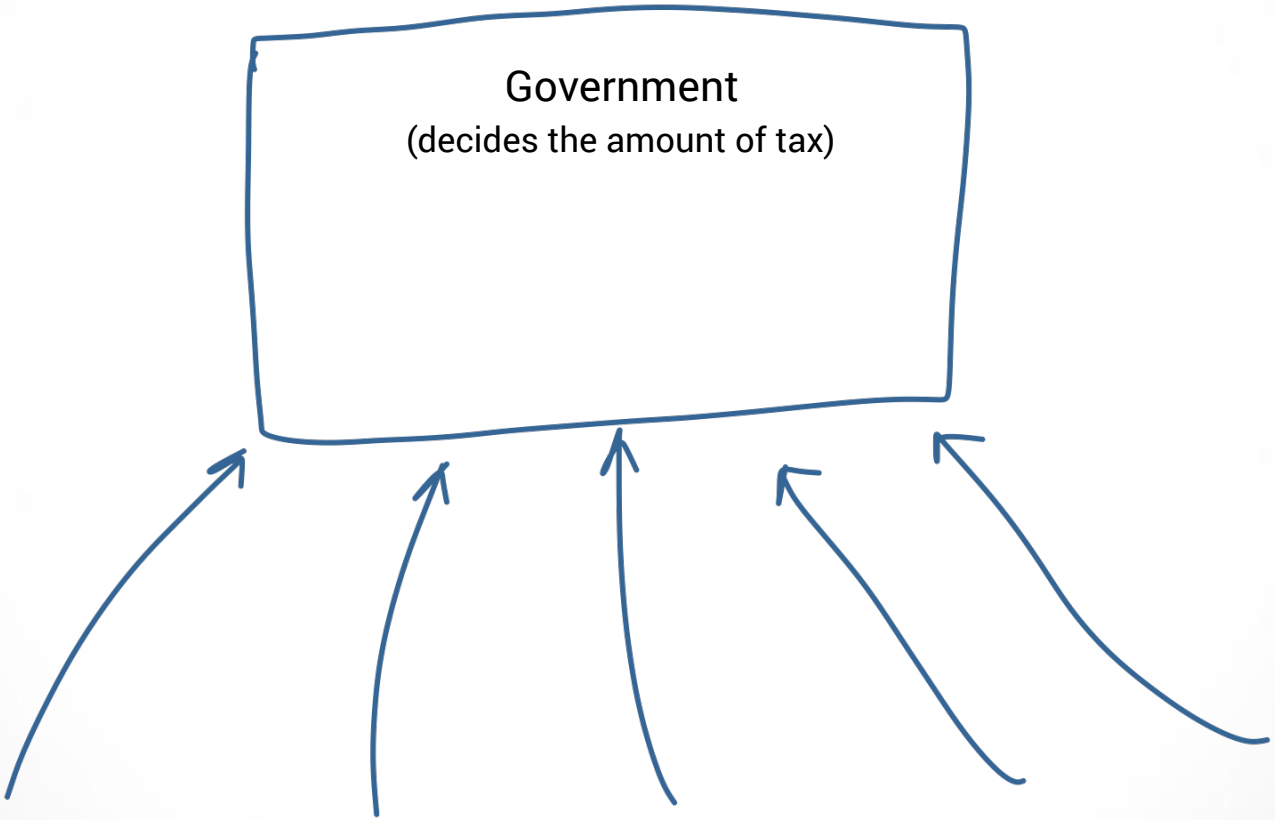
Carol Ent.

- Decentralized Democracy
- Crypto kitties
- Ensuring Documents Validity

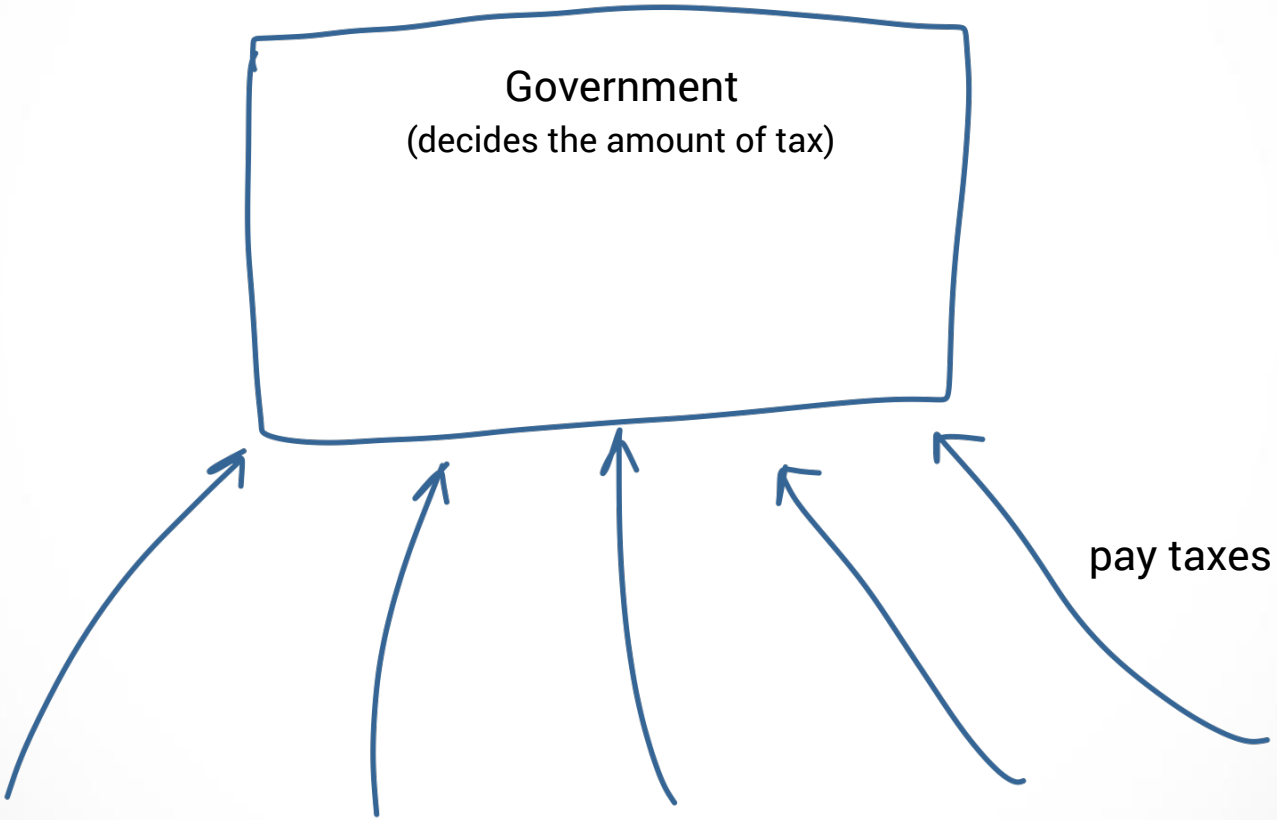
# Blockchains

- Distributed Systems
- Zero Knowledge Proof

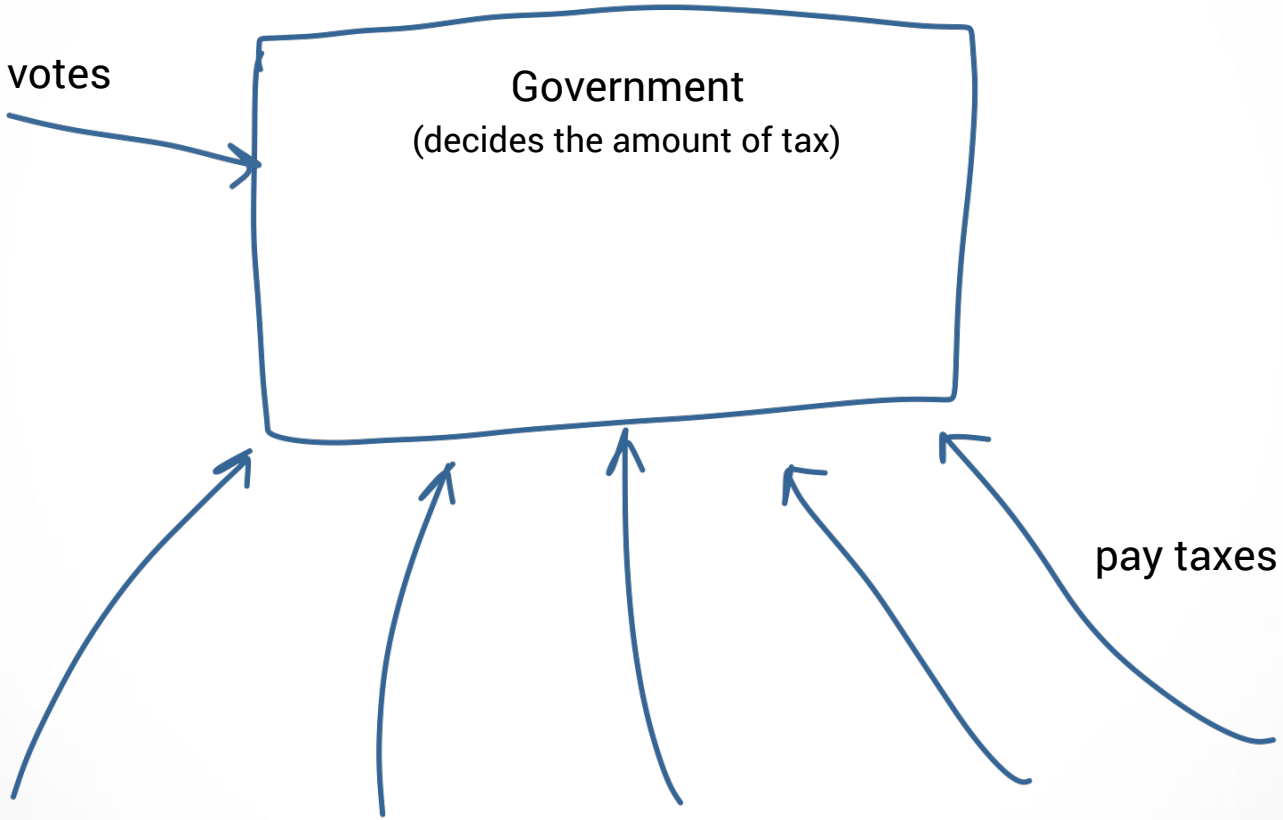
# Governance



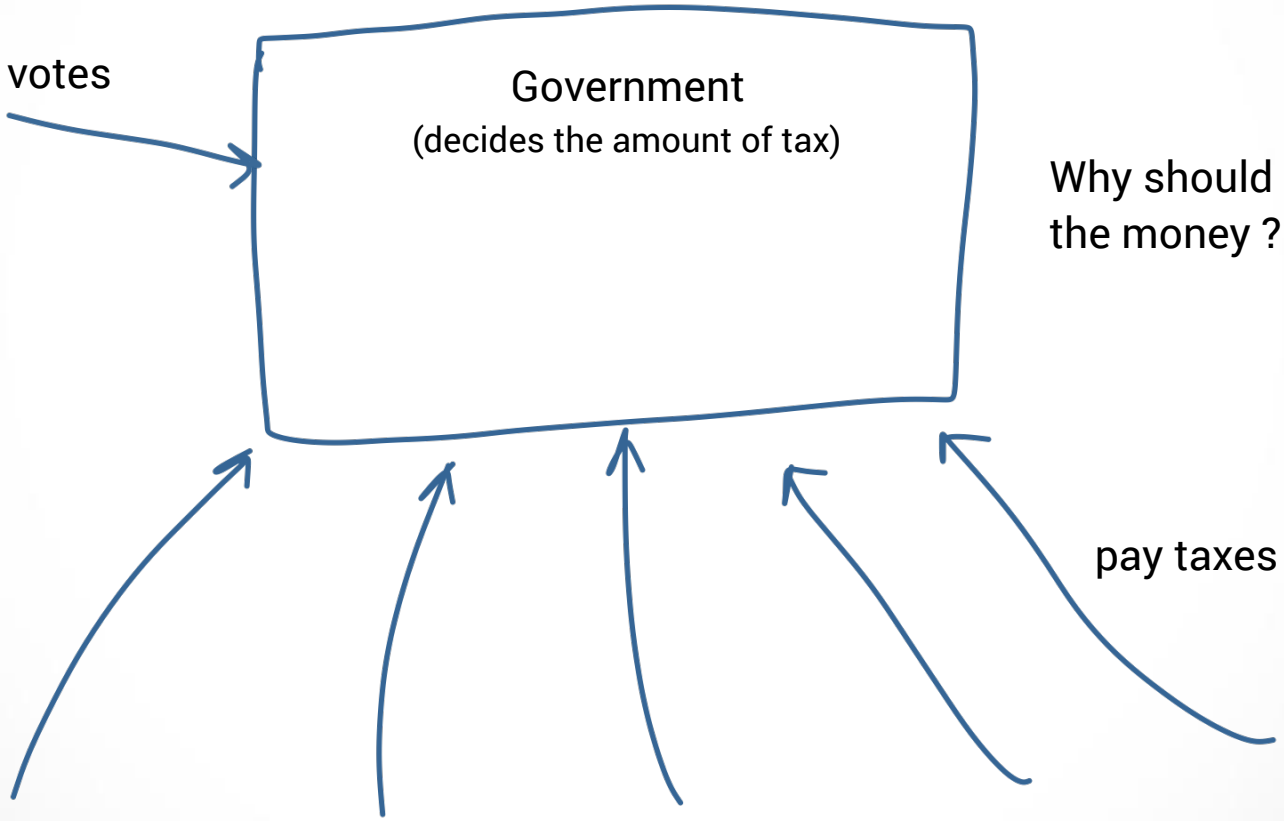
# Governance



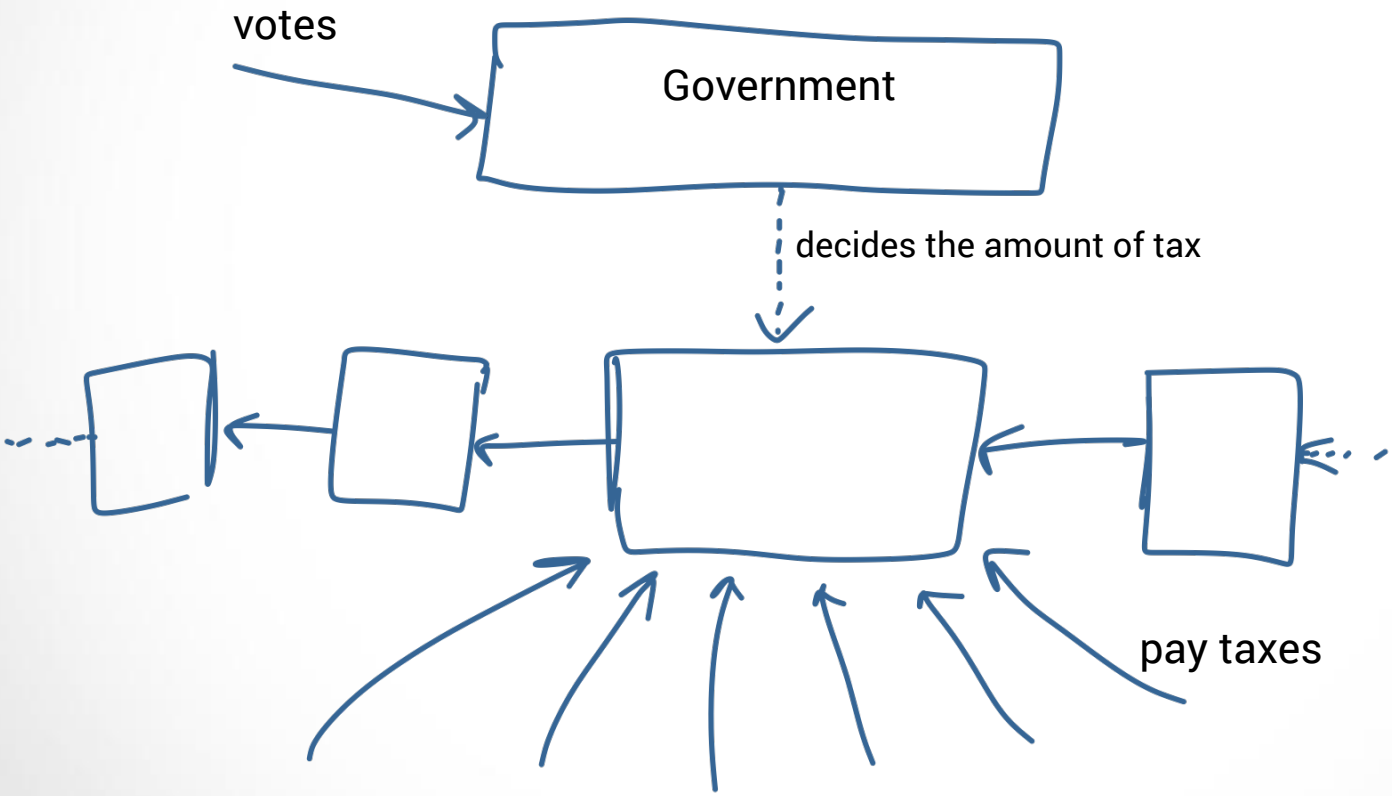
# Governance



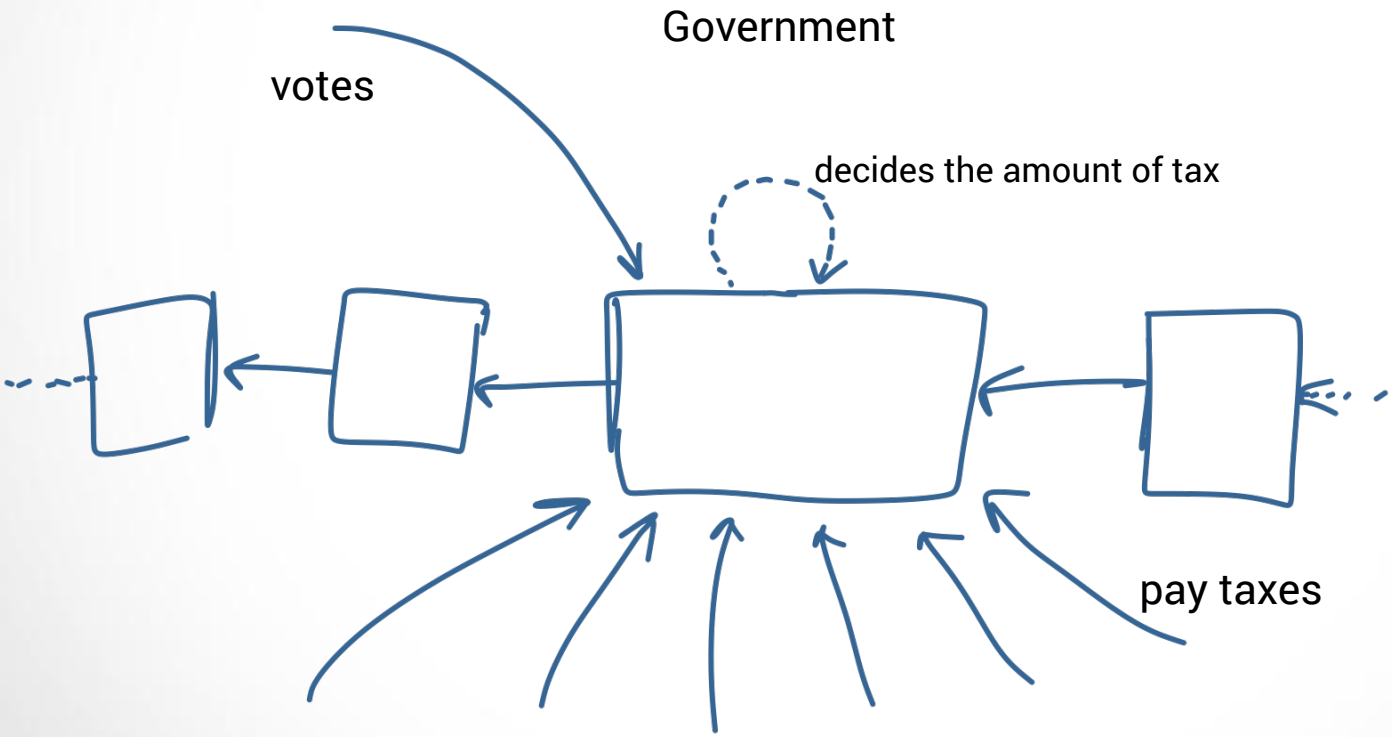
# Governance


votes
Government
(decides the amount of tax)
Why should it keep all the money ?
pay taxes

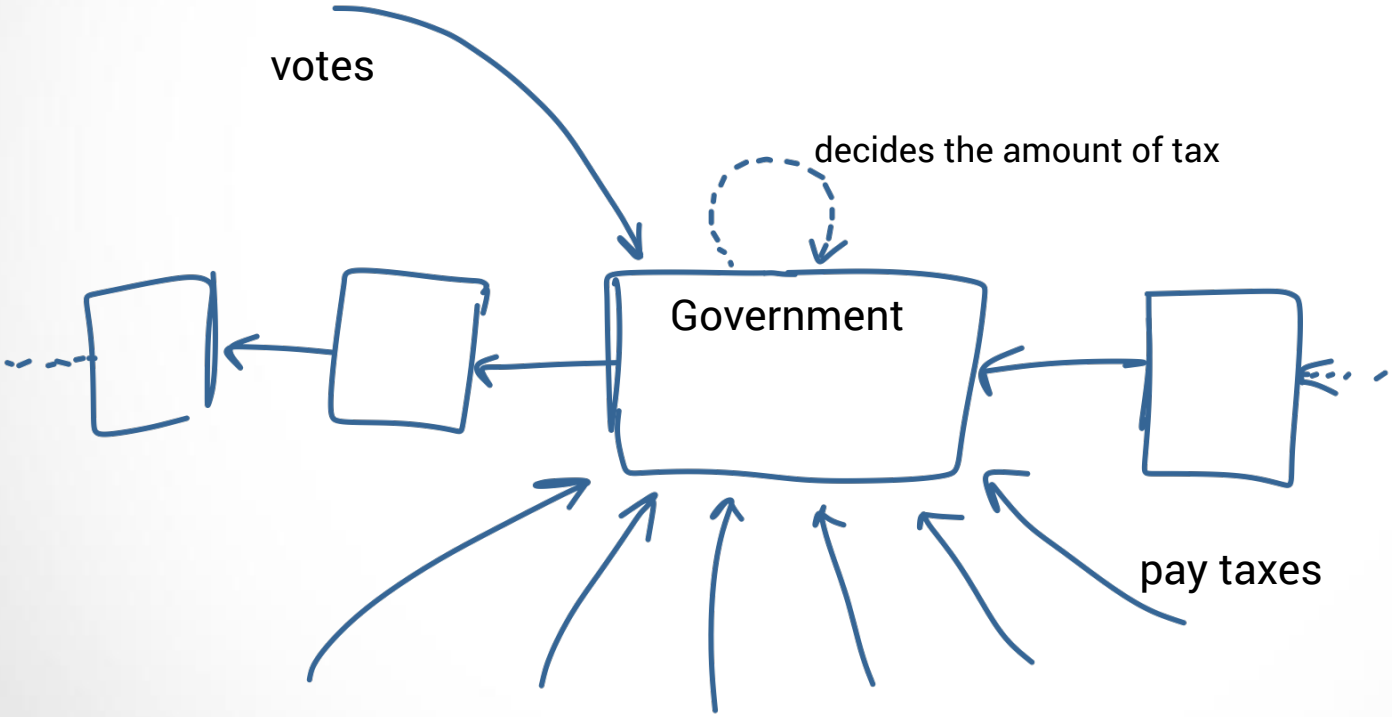
# Governance



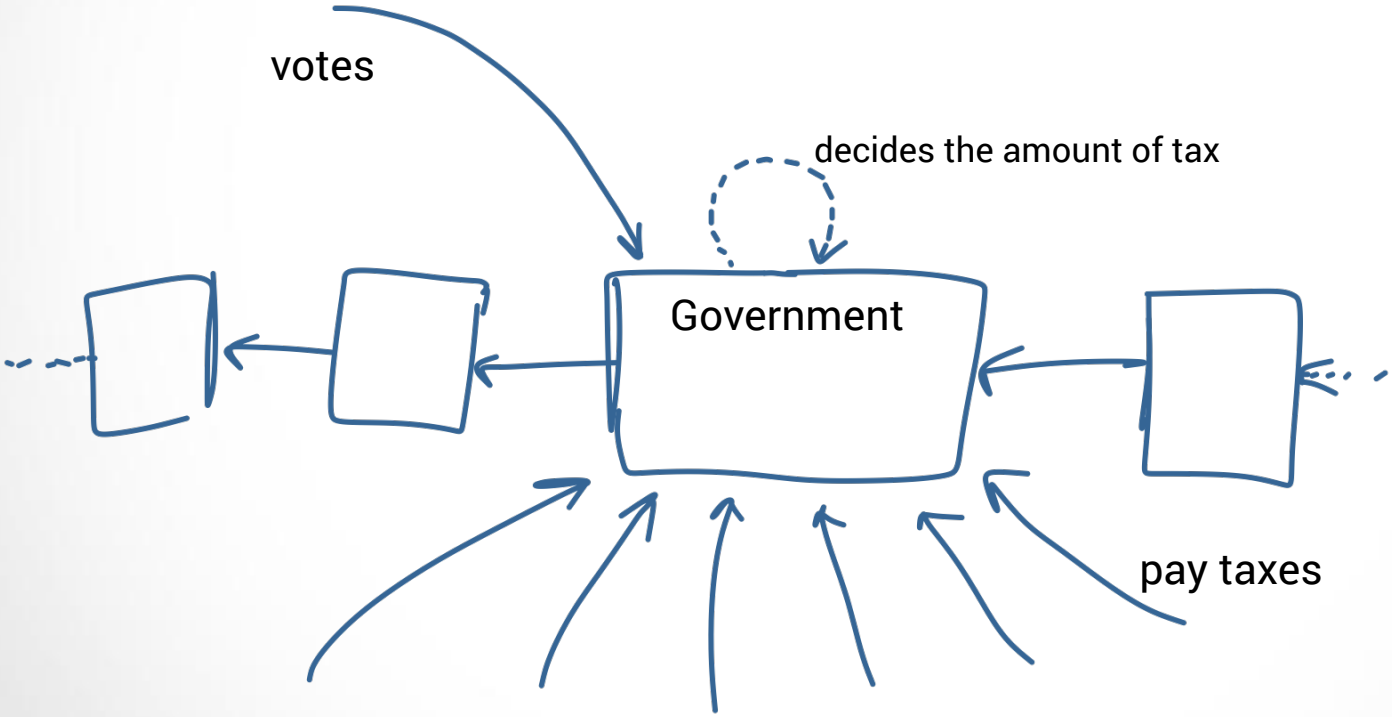
# Governance



# Governance



# Governance




« On the Blockchain nobody knows you're a fridge » — Richard G Brown

# Governance

DASH Budget Proposal Vote Tracker

The total number of Masternodes is 4788.
The current USD value of Dash is $187.20.
Next budget payments will occur in 17 days.
*(2018-10-02 09:27:20, block 947112)*
Voting deadline will occur in 14 days.

Total Allocated Budget: 1,067.00 DASH ($199,742.40).
Total Available Budget: 6,176.72 DASH ($1,156,281.55).
17.27%

Donations: XsBX3wnE34X9iwnE5aN9Fy2XtRsRwRSmoF

## Current Proposals (All Proposals)

| Title (listed by priority) | Owner | Payment # | Yes | No | Abstain | Net Votes* | % of Vote | Monthly Amount | Total Budget Requested | Actual Budget Allocated | History |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Cannabis Genomic Blockchain on DASH and CannMed 2018 Partnership** 2018-10-12 17:49:21 (Details \| Comments [57]) | KevinMcKernan | 10/10 | 1,072 | 127 | 70 | 945 | **20%** | 10.00 ($1,872.00) | 10.00 | 10.00 | Graph |
| **Dash Nation on Discord Renewal (Expanding To Other Forums)** 2018-10-15 05:23:10 (Details \| Comments [94]) | TaoOfSatoshi | 5/5 | 1,049 | 151 | 9 | 898 | **19%** | 21.00 ($3,931.20) | 31.00 | 31.00 | Graph |
| **Dash Force September - December** 2018-12-15 02:41:08 (Details \| Comments [51]) | Mastermined | 2/4 | 924 | 87 | 10 | 837 | **17%** | 195.00 ($36,504.00) | 226.00 | 226.00 | |
| **DASH TEXT - SMS Wallets for Everyone (Exclusively for Dash) - FIRST STAGE VENEZUELA** 2018-10-16 00:04:07 (Details \| Comments [73]) | LorenzoReyC | 3/3 | 837 | 135 | 42 | 702 | **15%** | 36.00 ($6,739.20) | 262.00 | 262.00 | Graph |
| **DASH MEDELLÍN Colombia Merchant Network: 450 New Dash Merchants, 12 Dash Merchant Fairs, Self-Sustaining Dash Sales, Dash Remittances, Permanent Dash Marketing and Support (renewal)** 2019-02-12 14:57:58 (Details \| Comments [44]) | georgedonnelly | 2/6 | 837 | 142 | 82 | 695 | **15%** | 59.00 ($11,044.80) | 321.00 | 321.00 | |
| **DASH HELP - SUPPORT CENTER (VENEZUELA): Expansion to Brazil & US + Video tutorials (Wallets) + Publicity work** 2018-10-15 23:10:28 (Details \| Comments [35]) | alejandroe | 3/3 | 800 | 135 | 0 | 665 | **14%** | 32.00 ($5,990.40) | 353.00 | 353.00 | Graph |
| **Dash Brazil: YouTube + Social Media + Conference Attendance + Content Creation** 2019-02-12 14:54:02 (Details \| Comments [37]) | rambrissi | 2/6 | 797 | 136 | 21 | 661 | **14%** | 41.00 ($7,675.20) | 394.00 | 394.00 | |
| **Inactive Proposal For This Budget Cycle (was passed last** | | | | | | | | | | | |

# Governance

« On the Blockchain nobody knows you're a fridge » — Richard G Brown

# Governance

« On the Blockchain nobody knows you're a fridge » — Richard G Brown

What if everybody knows ?

# Governance

« On the Blockchain nobody knows you're a fridge » — Richard G Brown

What if everybody knows ?

What if we replaced our government by a fridge ?

# Governance

# Governance

Jesco Denzel—EPA-EFE/Shutterstock

Questions ?