

Tecnologia blockchain, més enllà de les criptomonedes

Miquel Guiot Cusidó
Secundària i Batxillerat
2024



Projecte HERMES, finançiat per



- Recerca d'alt nivell en:
 - Seguretat i privadesa en l'aprenentatge automàtic
 - Seguretat i privadesa en entorns descentralitzats
 - Criptografia avançada
 - Ciberseguretat en entorns vehiculars i entorns IOT
 - Gestió de la identitat
 - Avaluació, compliment normatiu i certificació
- Valorització i transferència dels resultats a la societat
- Divulgació i disseminació envers la ciutadania

El bitcoin bat rècords i supera els 71.000 dòlars per primer cop

-
- Els ETF, un procés tècnic i els canvis en els tipus d'interès impulsen la valoració
-

El bitcoin bat rècords i supera els 71.000 dòlars per primer cop

-
- Els ETF, un procés tècnic i els canvis en els tipus d'interès impulsen la valoració
-

Els NFT, la revolució del món de l'art que ha arribat per quedar-se

ELS TOKEN NO FUNGIBLES SACSEGEN ELS ARTISTES I
ELS RITMES I LES CONVENCIONS DEL MERCAT DE
L'ART

El bitcoin bat rècords i supera els 71.000 dòlars per primer cop

- Els ETF, un procés tècnic i els canvis en els tipus d'interès impulsen la valoració

Els NFT, la revolució del món de l'art que ha arribat per quedar-se

ELS TOKEN NO FUNGIBLES SACSEGEN ELS ARTISTES I
ELS RITMES I LES CONVENCIONS DEL MERCAT DE
L'ART



Elon Musk
@elonmusk · [Follow](#)

Bitcoin is my safe word

9:21 AM · Dec 20, 2020

213.6K [Reply](#) [Share](#)

[Read 6K replies](#)

Què hi ha al darrere de tot això?



Què hi ha al darrere de tot això?



Què hi ha al darrere de tot això?

Blockchain

Block 0xaf013c45

```
0 11101010 00 011000 010010 010
1010010 0100110001 1101001101011
110 10 1101 01 1100100111 1100
0 01010000111011000010 010101010
10 10 10100101001001 0110 001
11101000110000100 100001011001001
1110 001001 0100 011000 1010 1
100010100010011 0110 1101100110011
1100111 00 0101 1101 011010 11
001 1000 00 0110 001100101010 0
11010010110110 0110 00 1011 001
1 0010 0001 0101100100111 0100
01 011001010101 001100 1001001
010 10 010011 0110001001100101011
1110110 0100 101101 000011101
101001011011 010100 1101101 01
100 01 01 0001111001100 0010011
001110 10010100 11 0010 00010
0001001 1011101 110010111010001
10 01 010010010010 1001 11 011
```

Block 0x43a5fc78

```
100100011 0100 11101010 00 01100
101 00 110101010010 0100110001
10011000100 0110 10 1101 01 110
```

```
0010101110010 11110110 0100 101
0 0111 00 101001011011 010100
1000010001110100 01 01 000111110
0 11 10 01 001110 10010100 1
00011000101 10001001 10111101 110
00 01 1001 10 01 010010010010
```

Block 0x10e6c7a9

```
01101 0000111011 01010001 0110010
0 11011101 01 001001 0101 00
1001100 0010011011110111 1000 100
11 0010 000100 0101 00 0110 1
100110111010001 00 010001010110001
0 1001 11 01110010 10100001 00
011 00110101 00 11011001010101010
00010 10100101 010110 0001 11 1
1 11 10111 1011 011101 011001
001011001 0101 010000101101 00 0
000 010010 0100 100100 01 11001
1101001101110100 1101 011101
100100111 1100 11 01 0001011001
00010 0101010100 100111 11 10 0
001 0110 001000 100000 011100
000010111001001 10010010000111 010
011000 1010 10 01 1011 00 100
0 1101100110011001 00100110 11010
101 011010 11 01010011 0011 010
001100101010 001111011001 1001
```

Índex

Índex

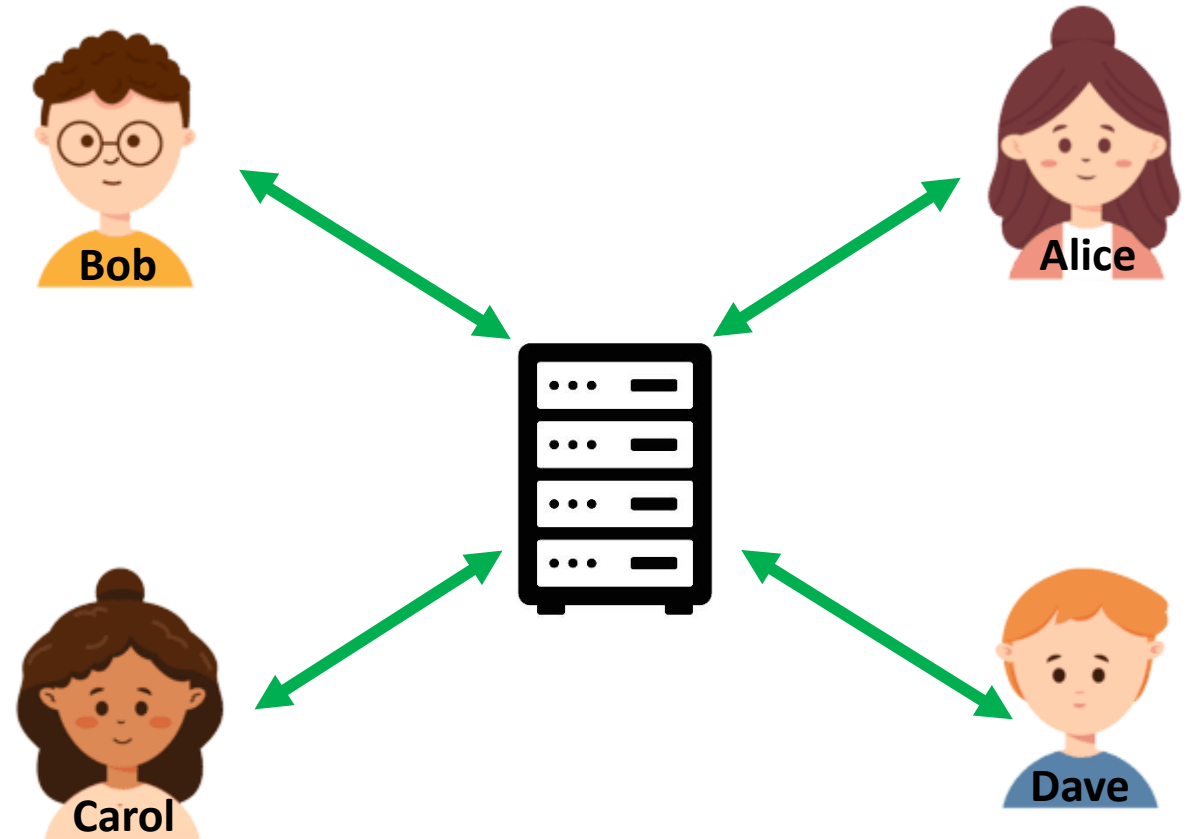
Tecnologia Blockchain, més enllà de les criptomonedes

1. Computació descentralitzada
 - Client-Servidor vs P2P
 - Reptes
2. Tecnologia Blockchain
 - El Registre distribuït
 - Criptografia
 - Minatge
 - Seguretat
3. Blockchain i societat
 - Avantatges i inconvenients
 - Aplicacions: Criptomonedes i més
 - Perills

The background features a complex network diagram on a dark blue background. White lines connect various circular nodes, each containing a different icon. These icons include a microphone, a hand holding a cube, a robot, a location pin, a speech bubble, a hierarchical tree structure, an envelope, a document with a checkmark, a person, a circular arrow, a gear, a cube, a globe with 'www', a star, a double arrow, a flower-like shape, and a person with a gear. The central text 'Computació Descentralitzada' is overlaid on a white rectangular banner.

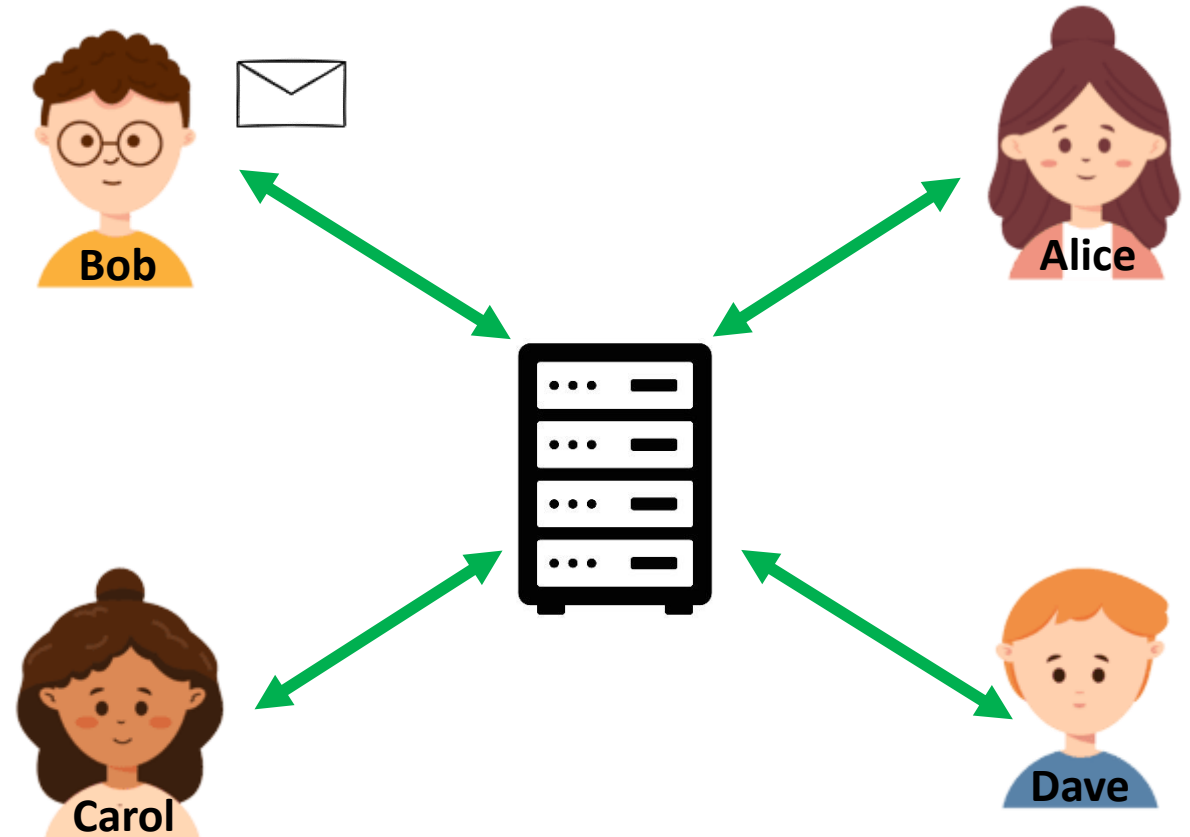
Computació Descentralitzada

Client-Servidor: Introducció



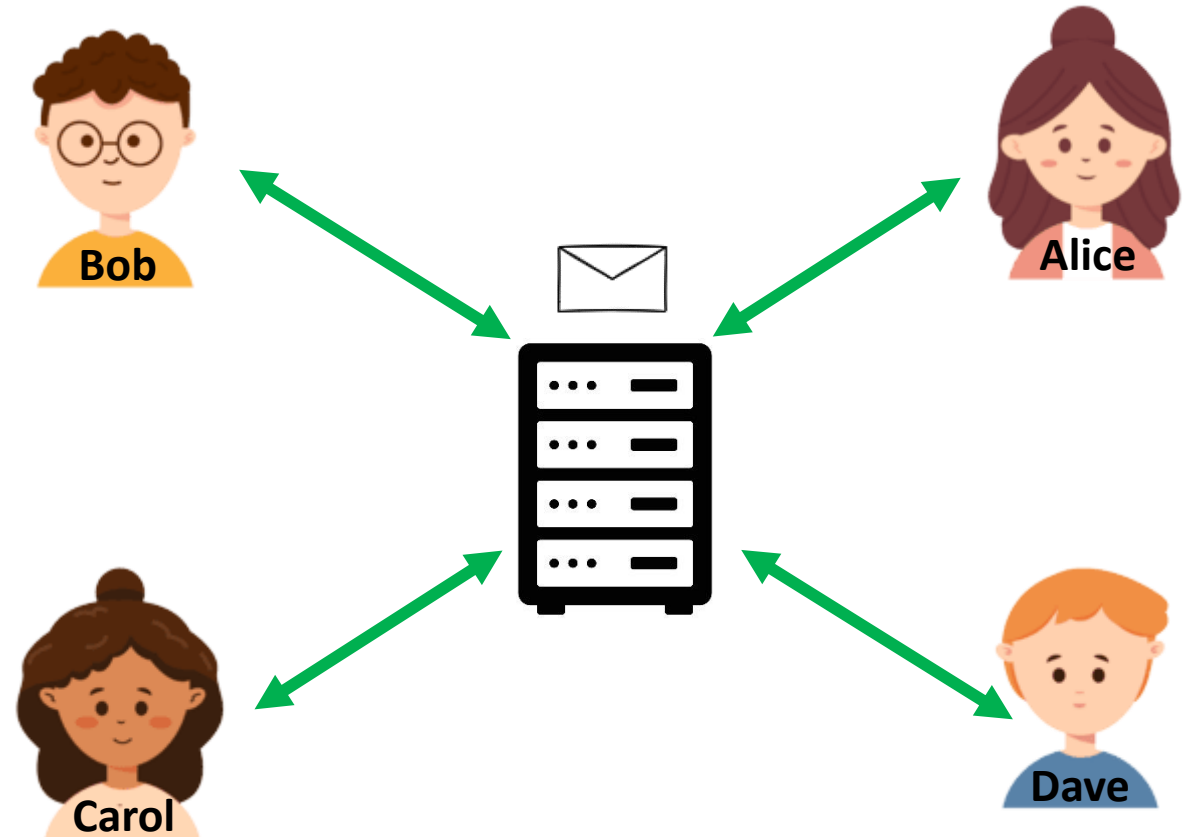
Client-Servidor: Introducció

- El client sol·licita una tasca
- El servidor executa la tasca
- Múltiples avantatges
 - Disseny senzill
 - Usabilitat
 - Escalabilitat
- Model més comú



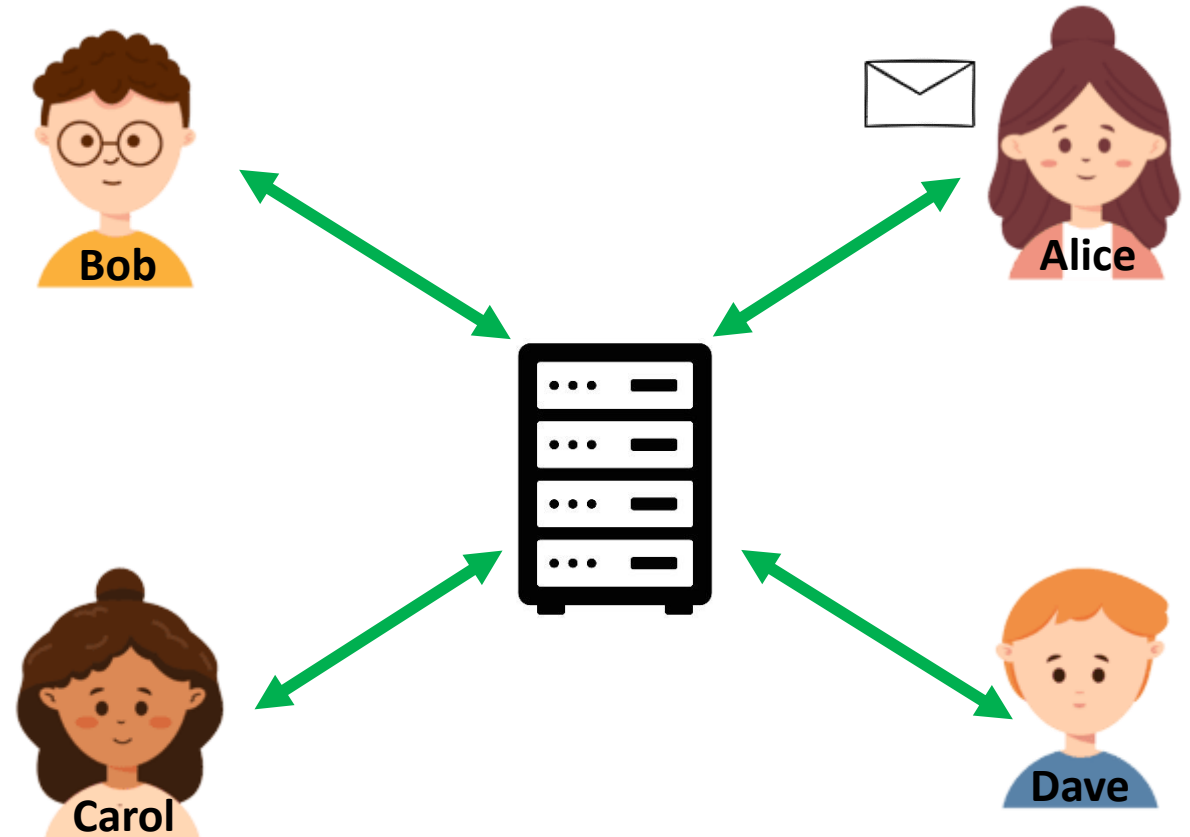
Client-Servidor: Introducció

- El client sol·licita una tasca
- El servidor executa la tasca
- Múltiples avantatges
 - Disseny senzill
 - Usabilitat
 - Escalabilitat
- Model més comú



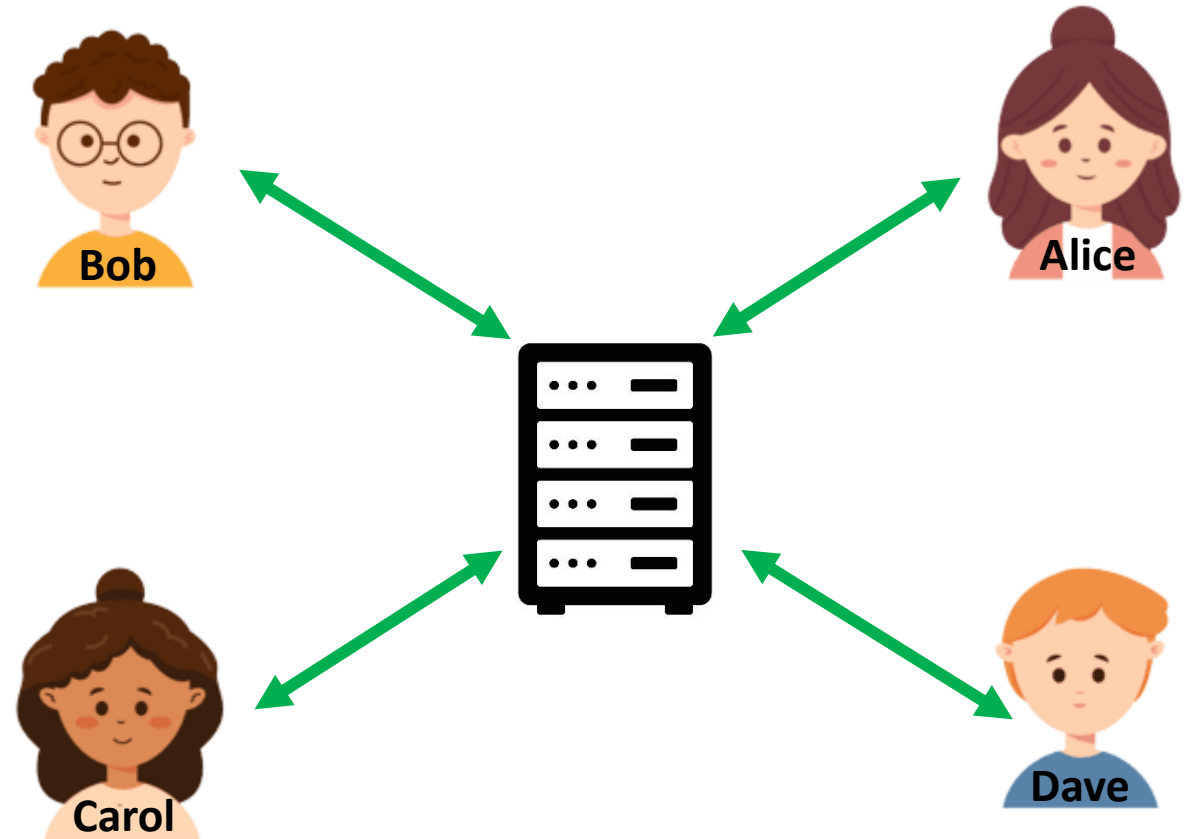
Client-Servidor: Introducció

- El client sol·licita una tasca
- El servidor executa la tasca
- Múltiples avantatges
 - Disseny senzill
 - Usabilitat
 - Escalabilitat
- Model més comú



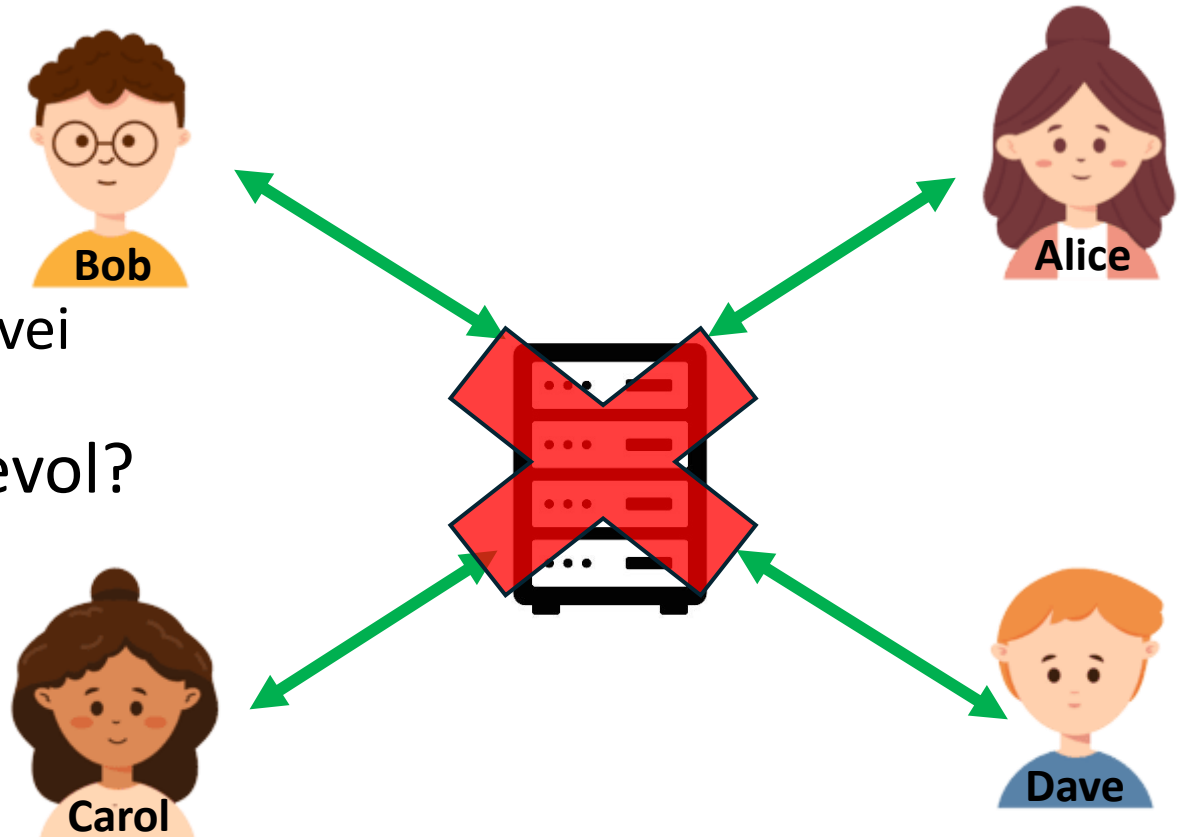
Client-Servidor: Introducció

- El client sol·licita una tasca
- El servidor executa la tasca
- Múltiples avantatges
 - Disseny senzill
 - Usabilitat
 - Escalabilitat
- Model més comú



Client-Servidor: Reptes

- Què passa si el servidor cau?
 - L'usuari deixa de disposar del servei
- Què passa si el servidor és malèvol?
 - L'usuari està en perill
- Hi ha alguna alternativa?



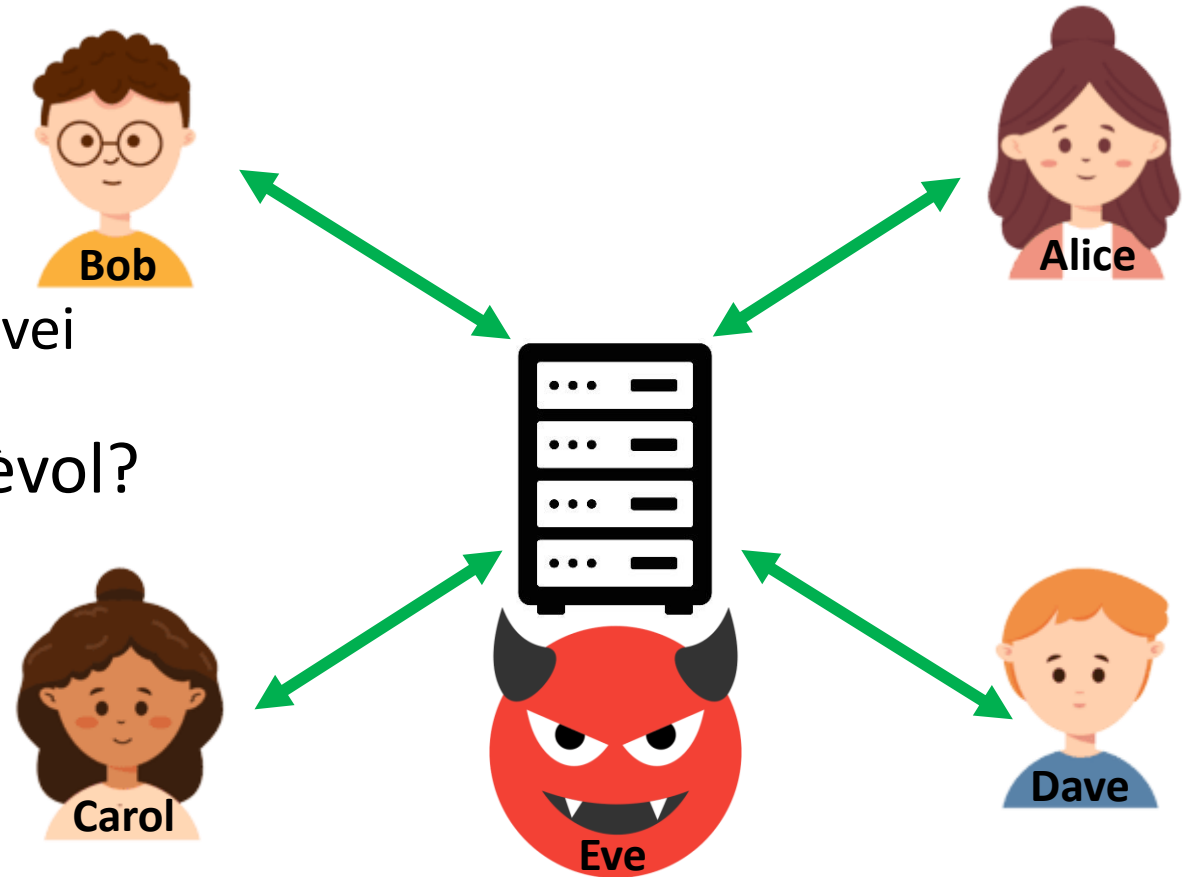
Client-Servidor: Reptes

- Què passa si el servidor cau?
 - L'usuari deixa de disposar del servei
- Què passa si el servidor és malèvol?
 - L'usuari està en perill
- Hi ha alguna alternativa?



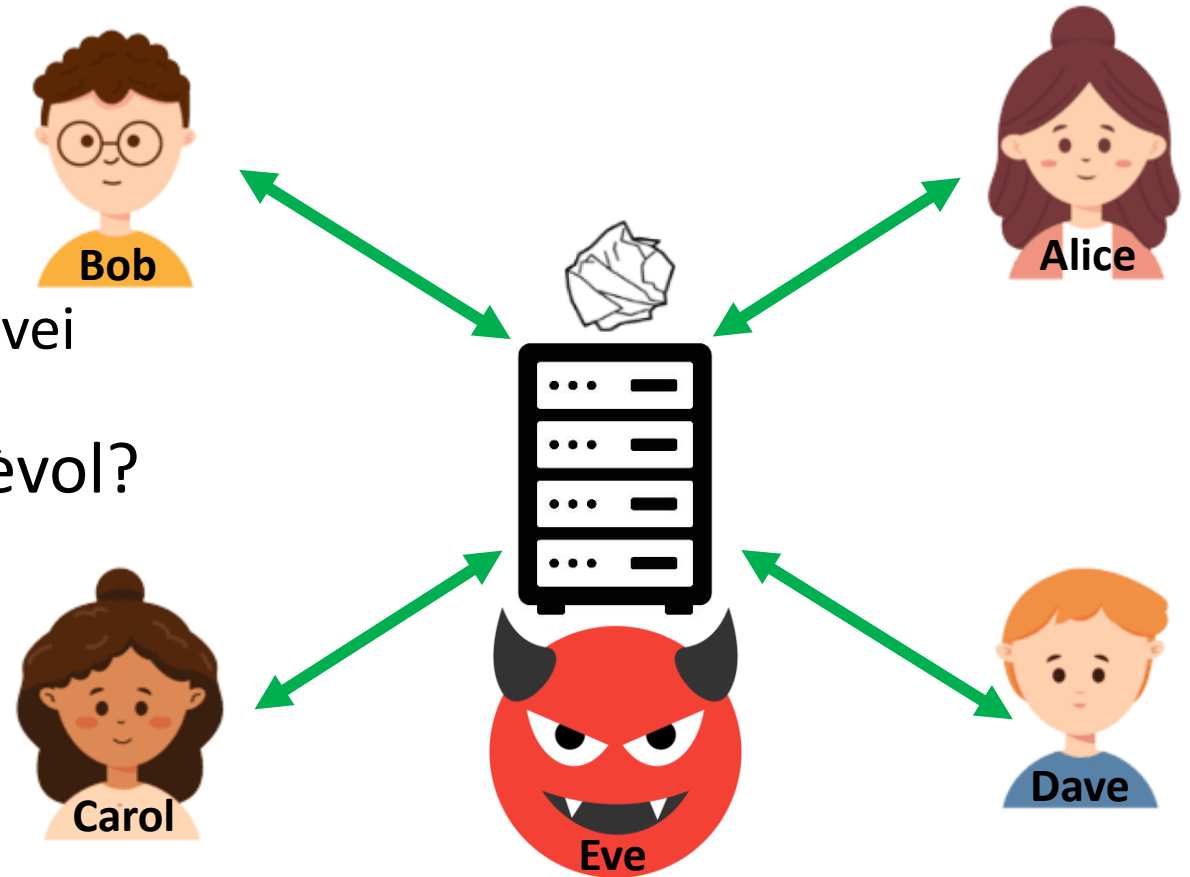
Client-Servidor: Reptes

- Què passa si el servidor cau?
 - L'usuari deixa de disposar del servei
- Què passa si el servidor és malèvol?
 - L'usuari està en perill
- Hi ha alguna alternativa?



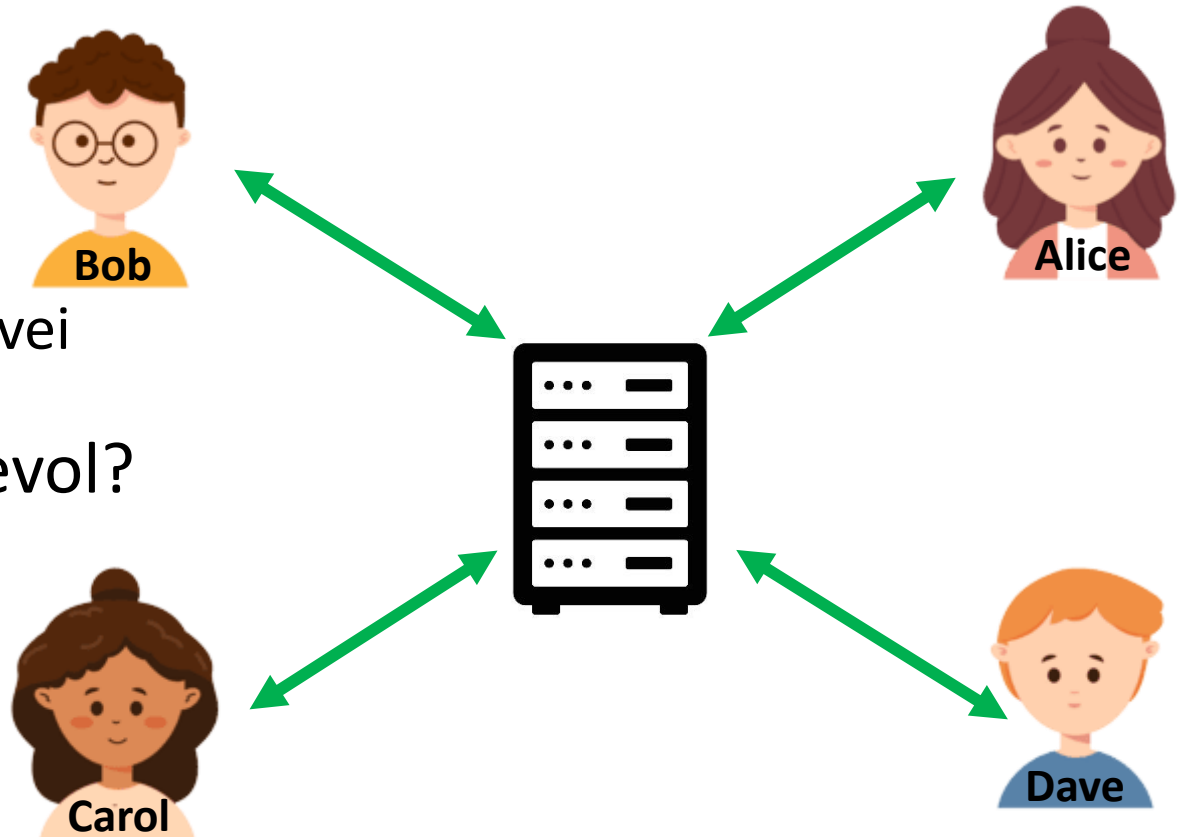
Client-Servidor: Reptes

- Què passa si el servidor cau?
 - L'usuari deixa de disposar del servei
- Què passa si el servidor és malèvol?
 - L'usuari està en perill
- Hi ha alguna alternativa?

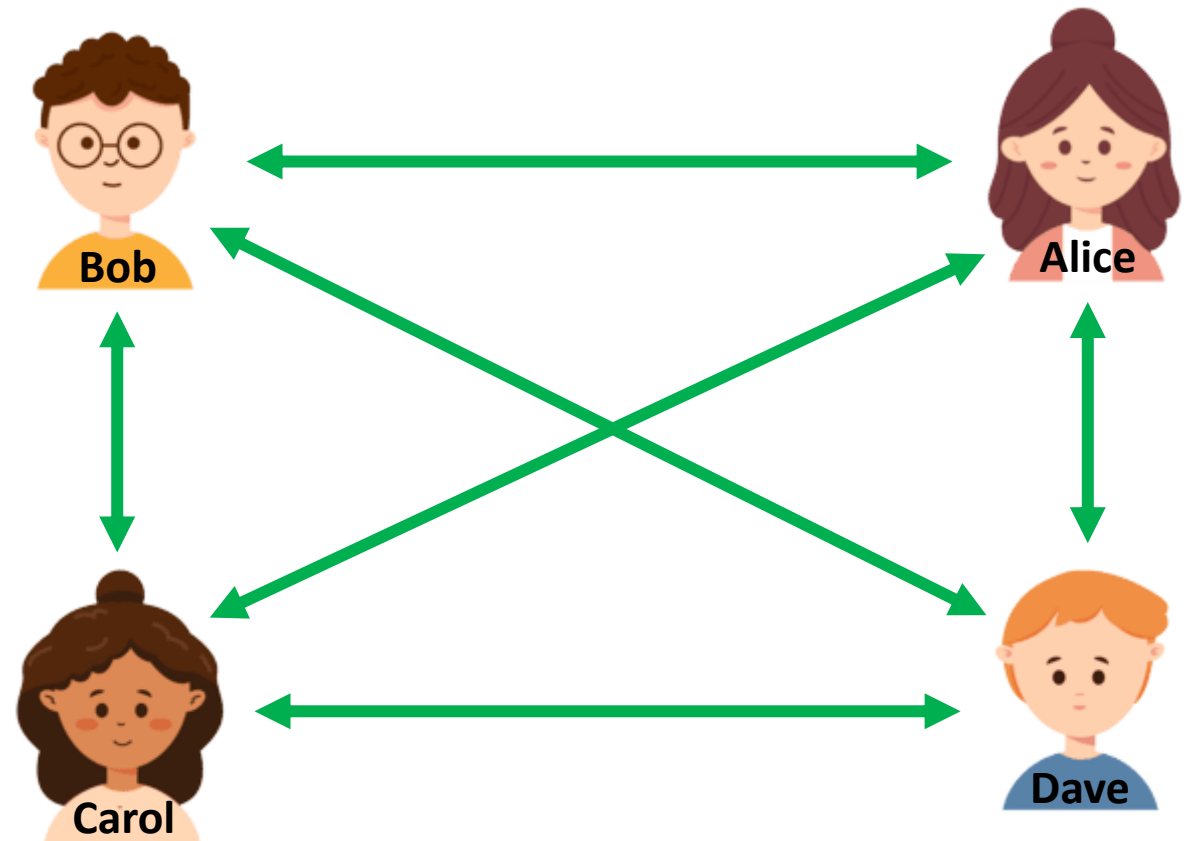


Client-Servidor: Reptes

- Què passa si el servidor cau?
 - L'usuari deixa de disposar del servei
- Què passa si el servidor és malèvol?
 - L'usuari està en perill
- Hi ha alguna alternativa?

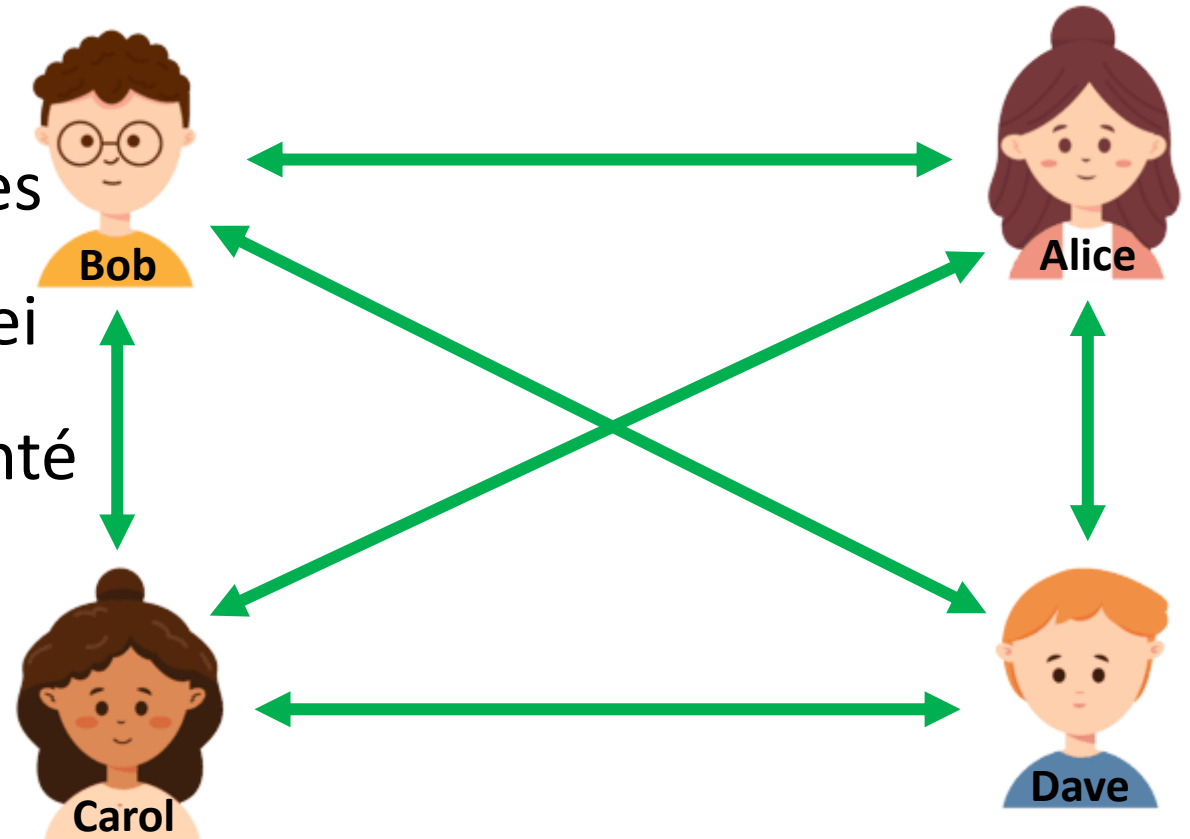


P2P: Introducció



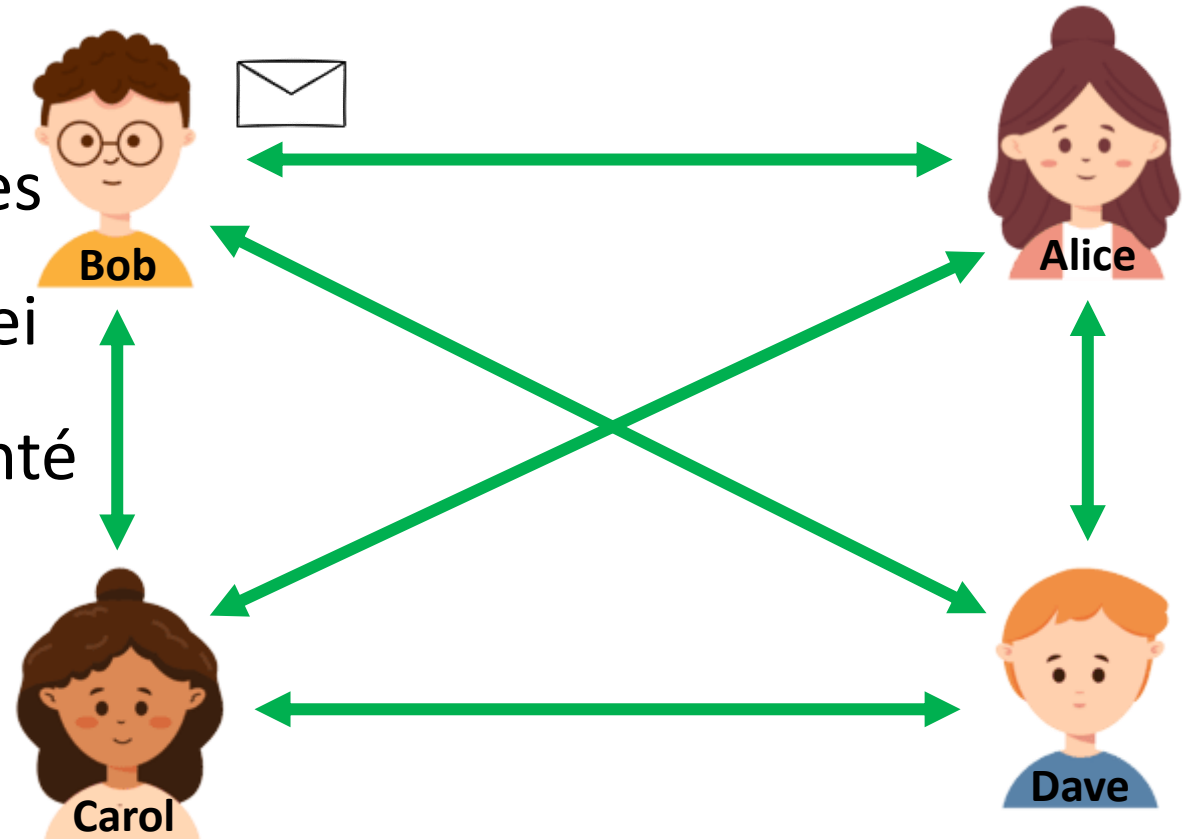
P2P: Introducció

- Model d'igual a igual
- Pas de clients i servidors a nodes
- Tots els nodes executen el servei
- Si un node cau, el servei es manté
- Model en funcionament
 - Spotify
 - BitTorrent
 - Criptomonedes



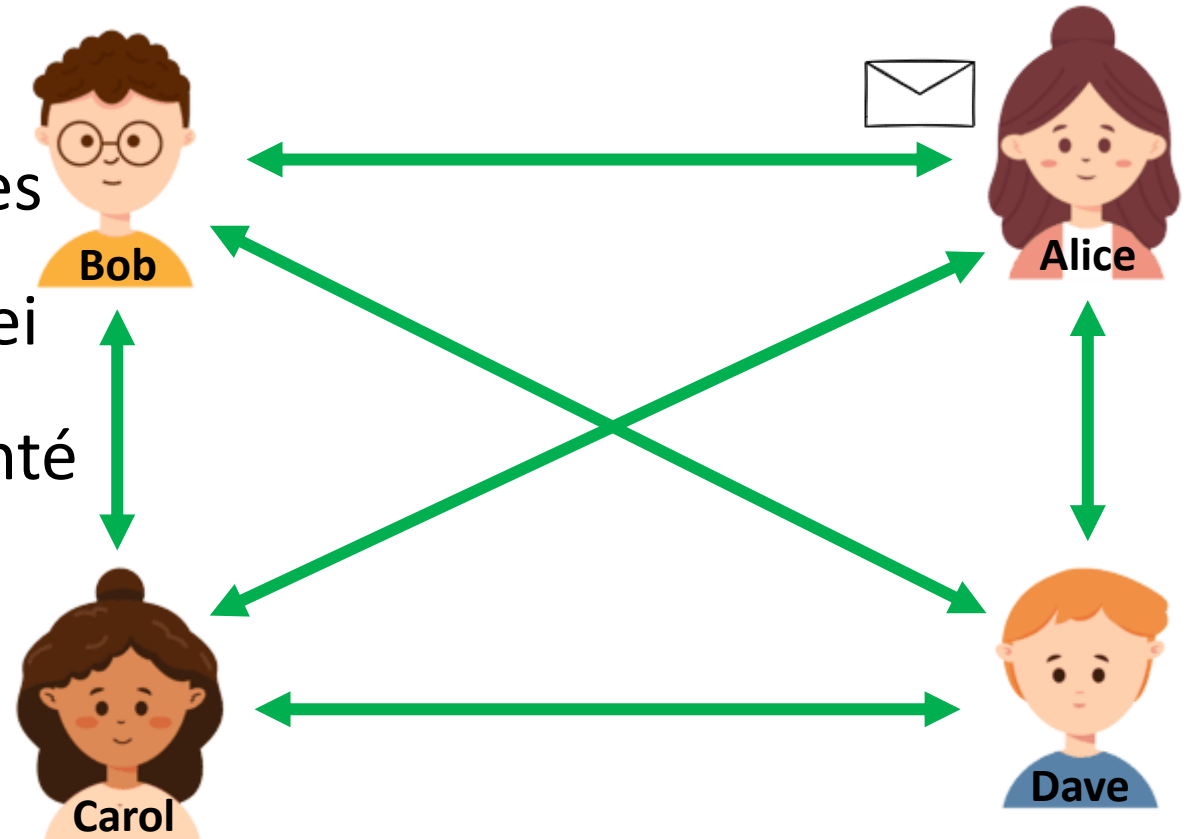
P2P: Introducció

- Model d'igual a igual
- Pas de clients i servidors a nodes
- Tots els nodes executen el servei
- Si un node cau, el servei es manté
- Model en funcionament
 - Spotify
 - BitTorrent
 - Criptomonedes



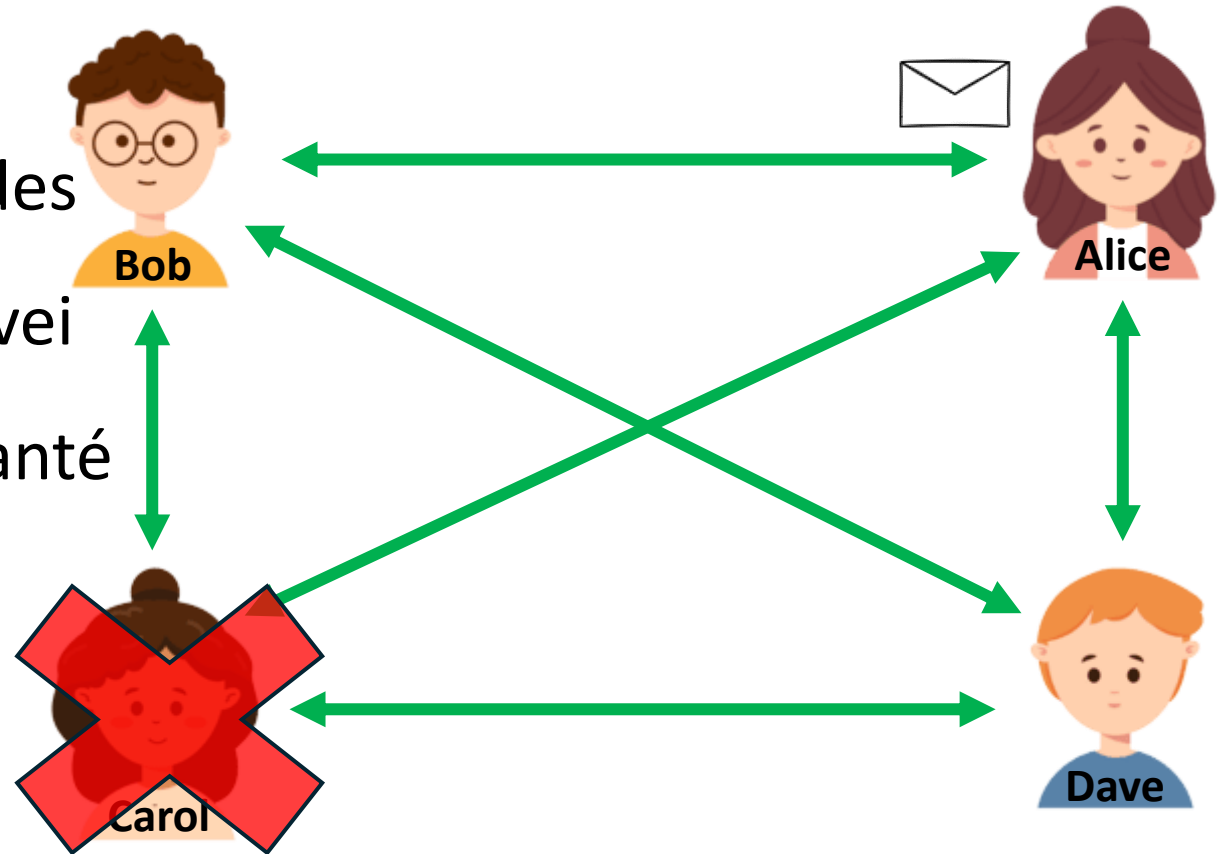
P2P: Introducció

- Model d'igual a igual
- Pas de clients i servidors a nodes
- Tots els nodes executen el servei
- Si un node cau, el servei es manté
- Model en funcionament
 - Spotify
 - BitTorrent
 - Criptomonedes



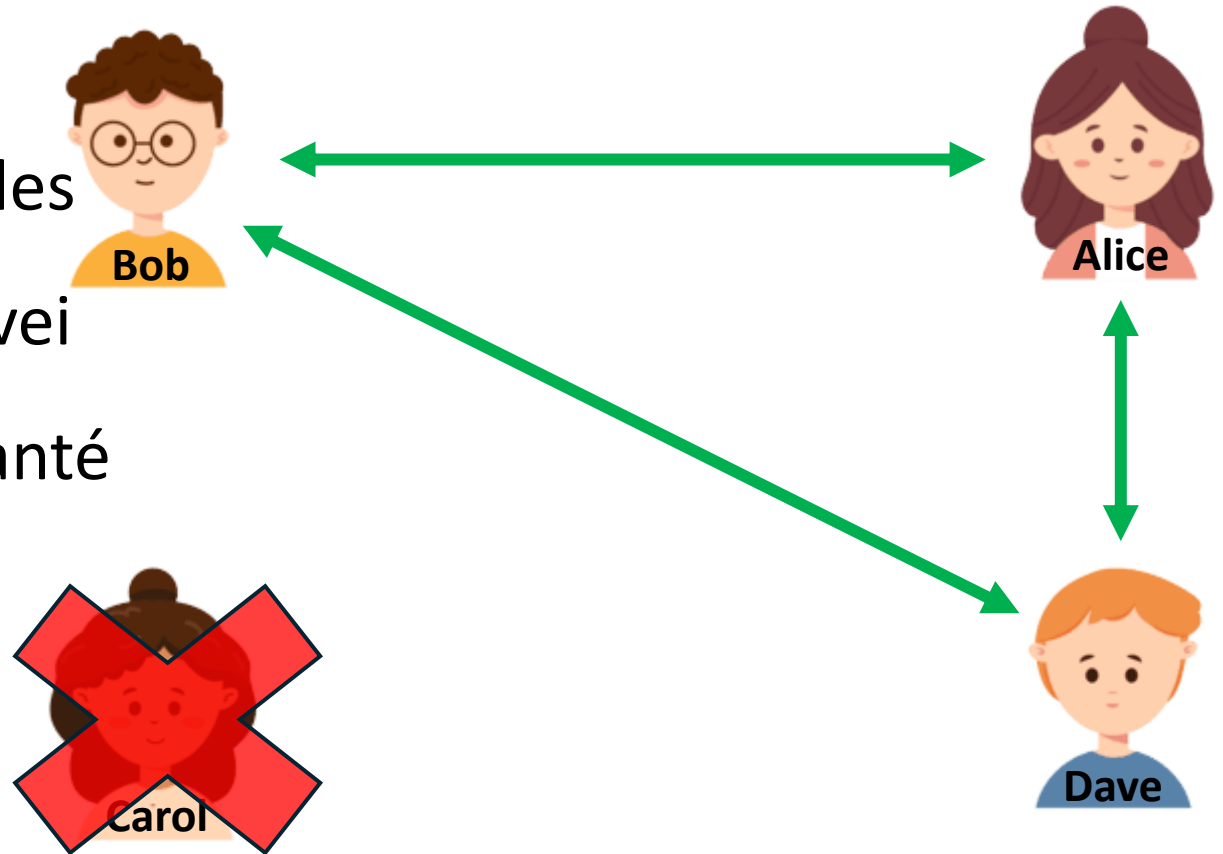
P2P: Introducció

- Model d'igual a igual
- Pas de clients i servidors a nodes
- Tots els nodes executen el servei
- Si un node cau, el servei es manté
- Model en funcionament
 - Spotify
 - BitTorrent
 - Criptomonedes



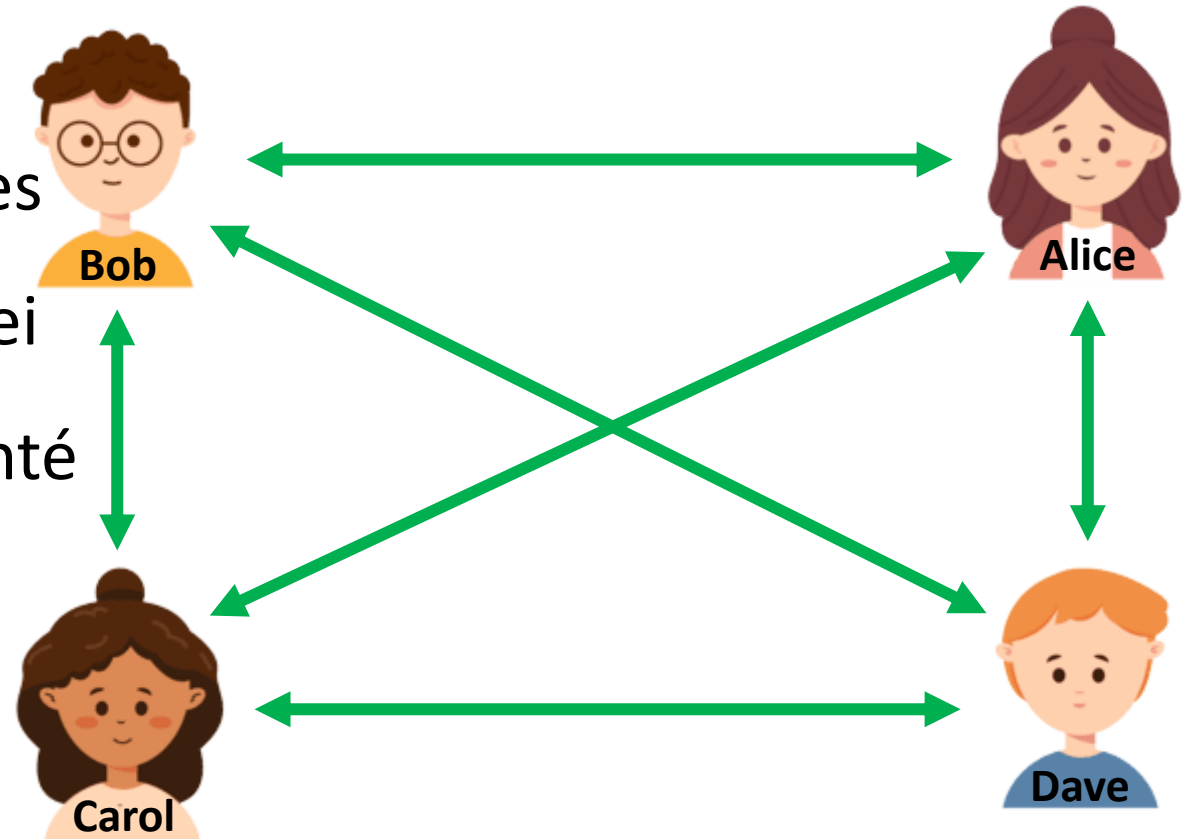
P2P: Introducció

- Model d'igual a igual
- Pas de clients i servidors a nodes
- Tots els nodes executen el servei
- Si un node cau, el servei es manté
- Model en funcionament
 - Spotify
 - BitTorrent
 - Criptomonedes

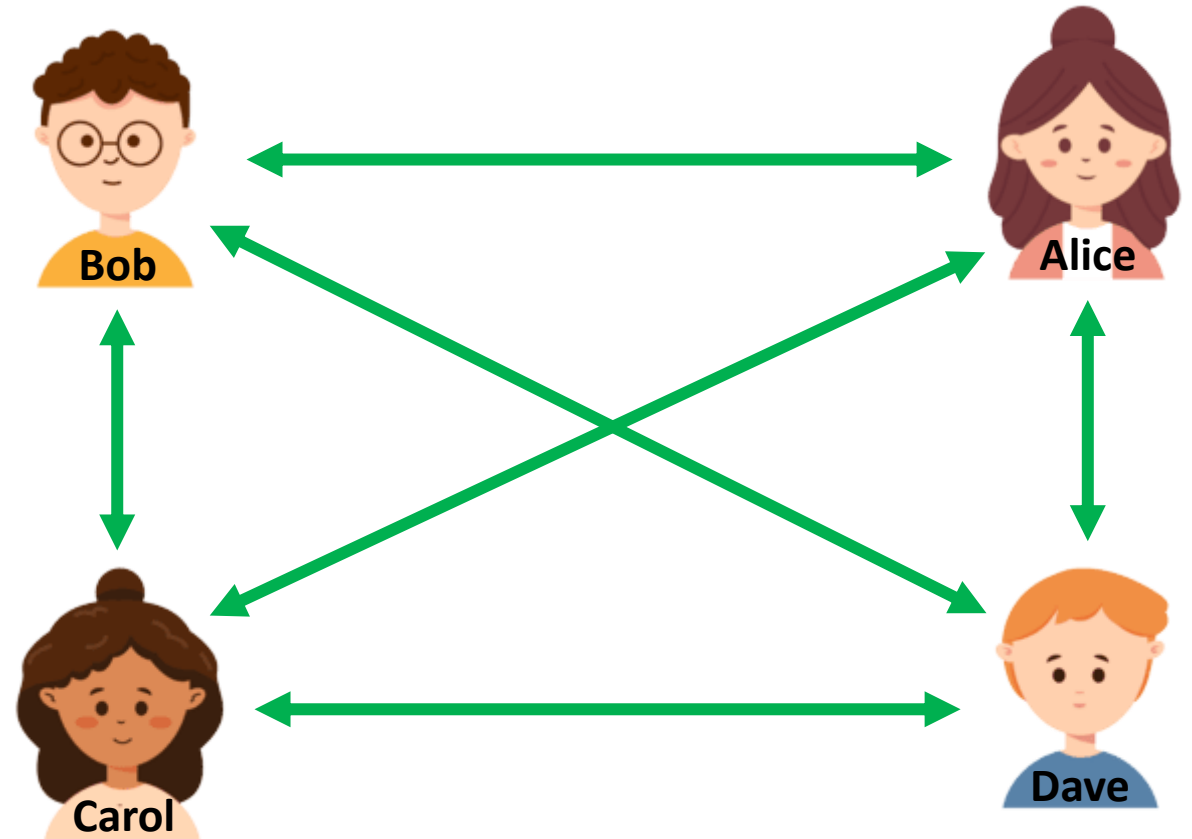


P2P: Introducció

- Model d'igual a igual
- Pas de clients i servidors a nodes
- Tots els nodes executen el servei
- Si un node cau, el servei es manté
- Model en funcionament
 - Spotify
 - BitTorrent
 - Criptomonedes

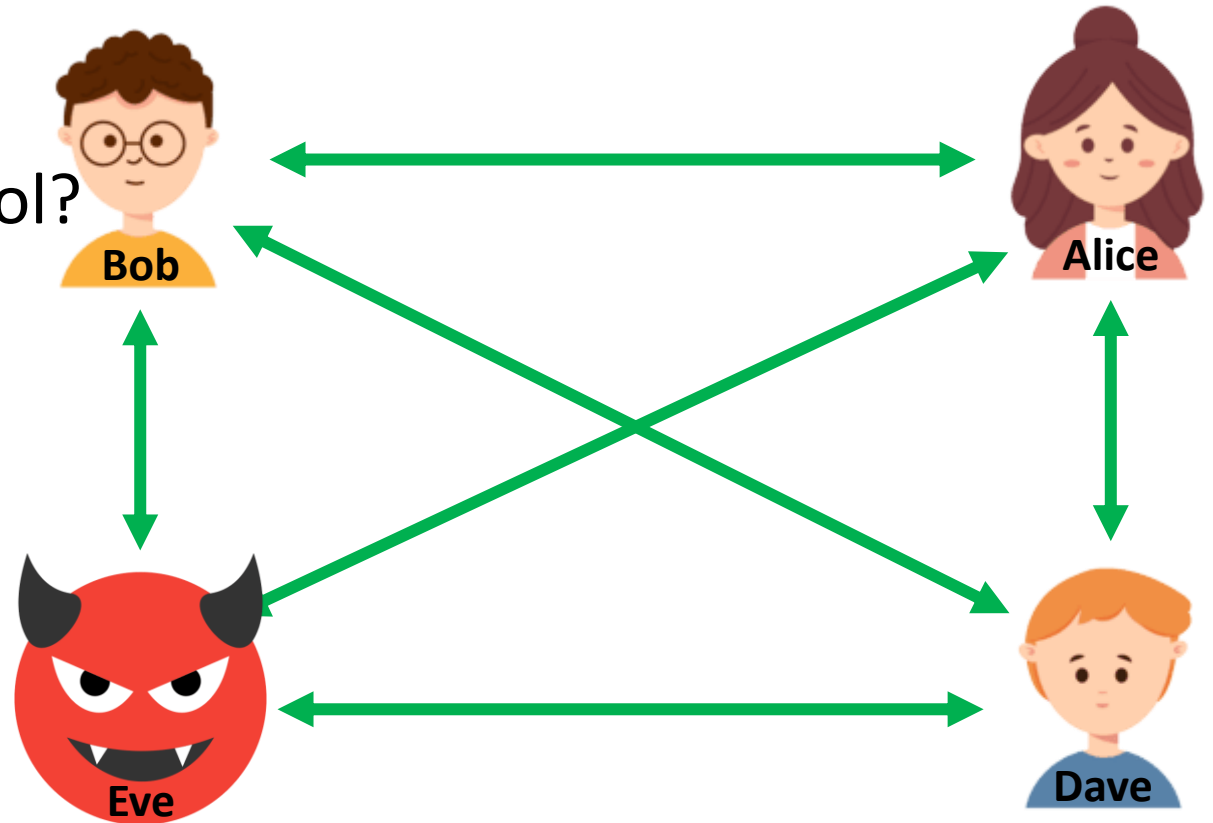


P2P: Reptes



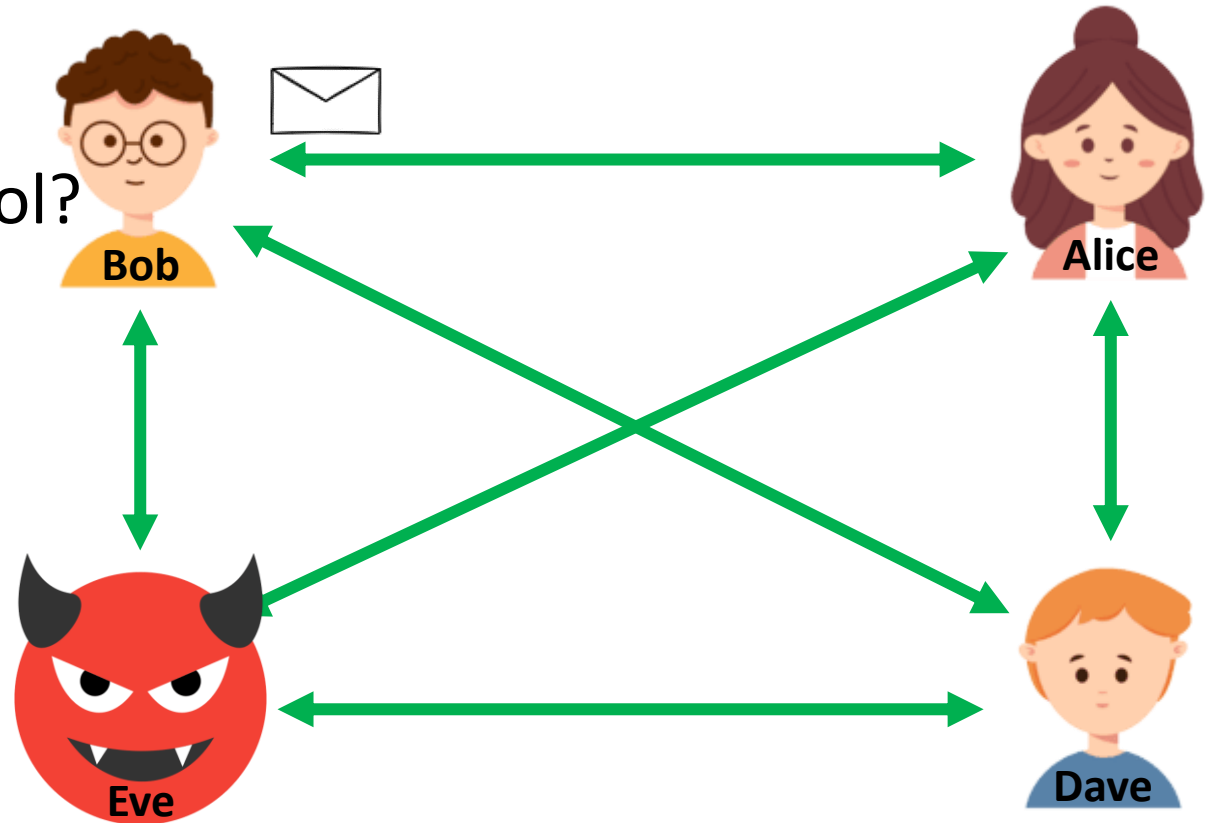
P2P: Reptes

- Què passa si un node és malèvol?
 - El servei pot deixar de funcionar
- Com es coordinen els nodes?
 - Cal arribar a un consens



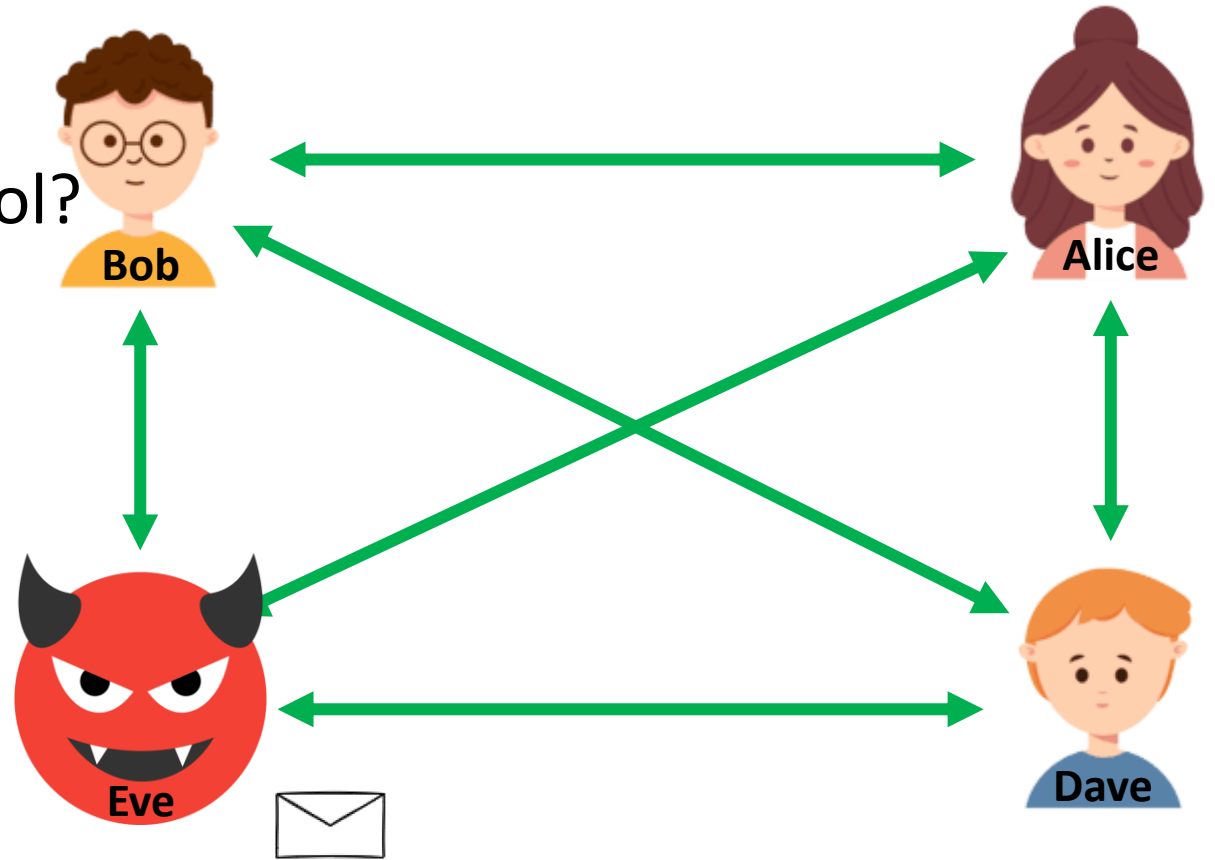
P2P: Reptes

- Què passa si un node és malèvol?
 - El servei pot deixar de funcionar
- Com es coordinen els nodes?
 - Cal arribar a un consens



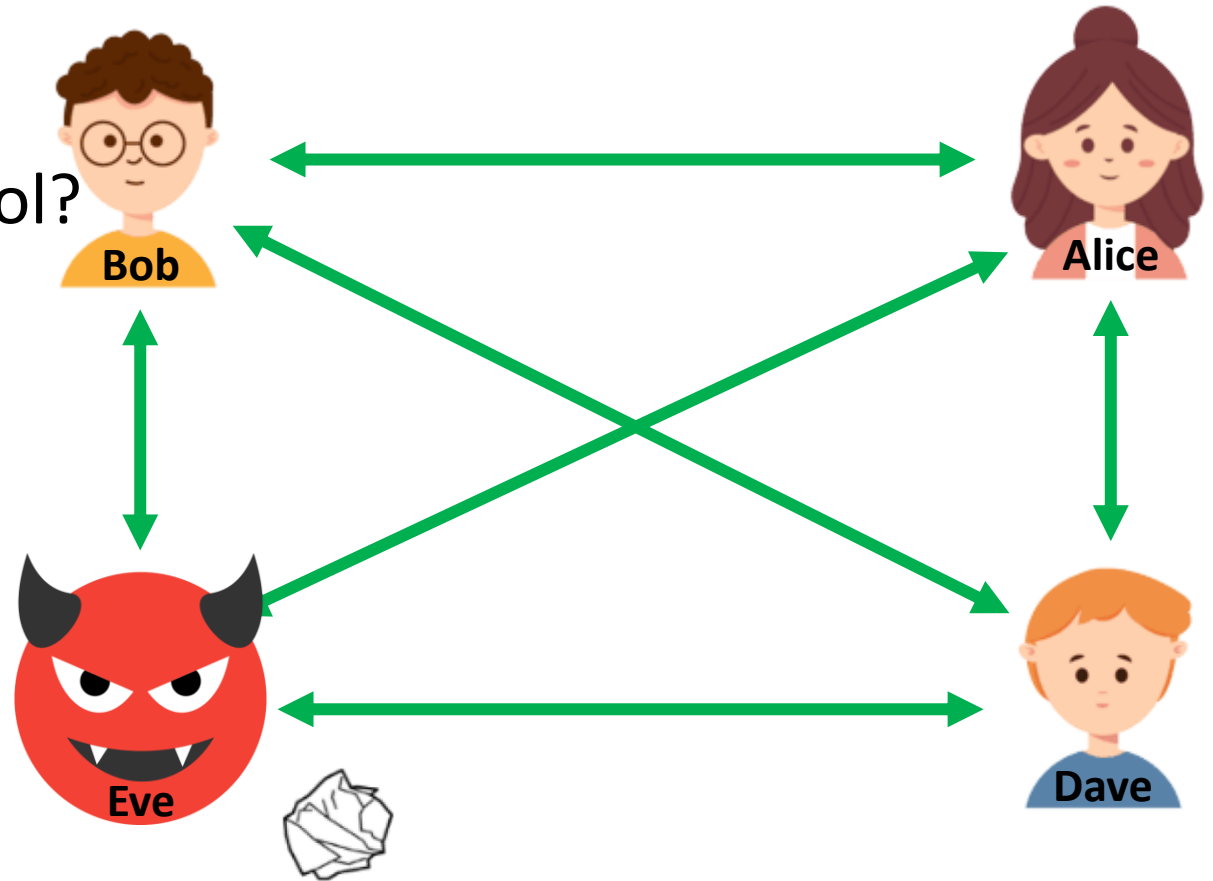
P2P: Reptes

- Què passa si un node és malèvol?
 - El servei pot deixar de funcionar
- Com es coordinen els nodes?
 - Cal arribar a un consens



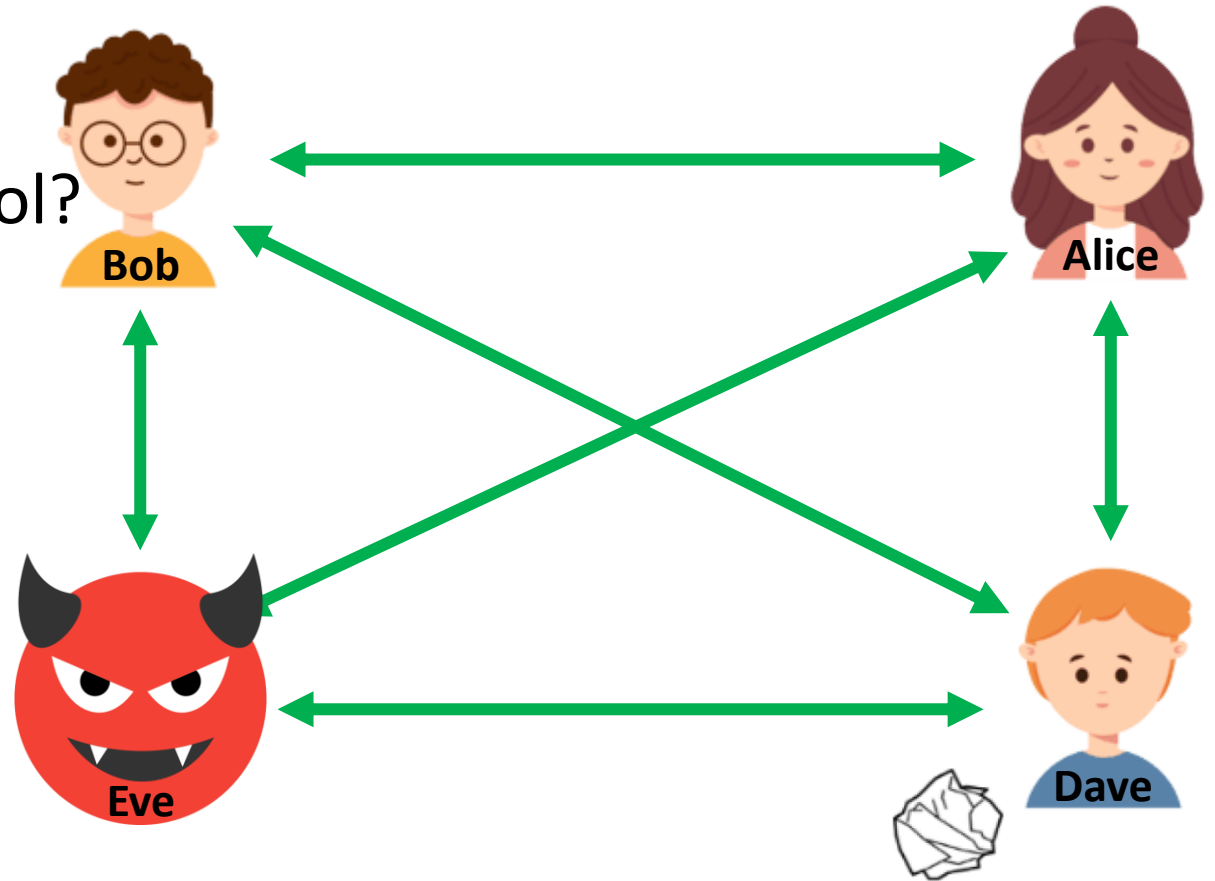
P2P: Reptes

- Què passa si un node és malèvol?
 - El servei pot deixar de funcionar
- Com es coordinen els nodes?
 - Cal arribar a un consens



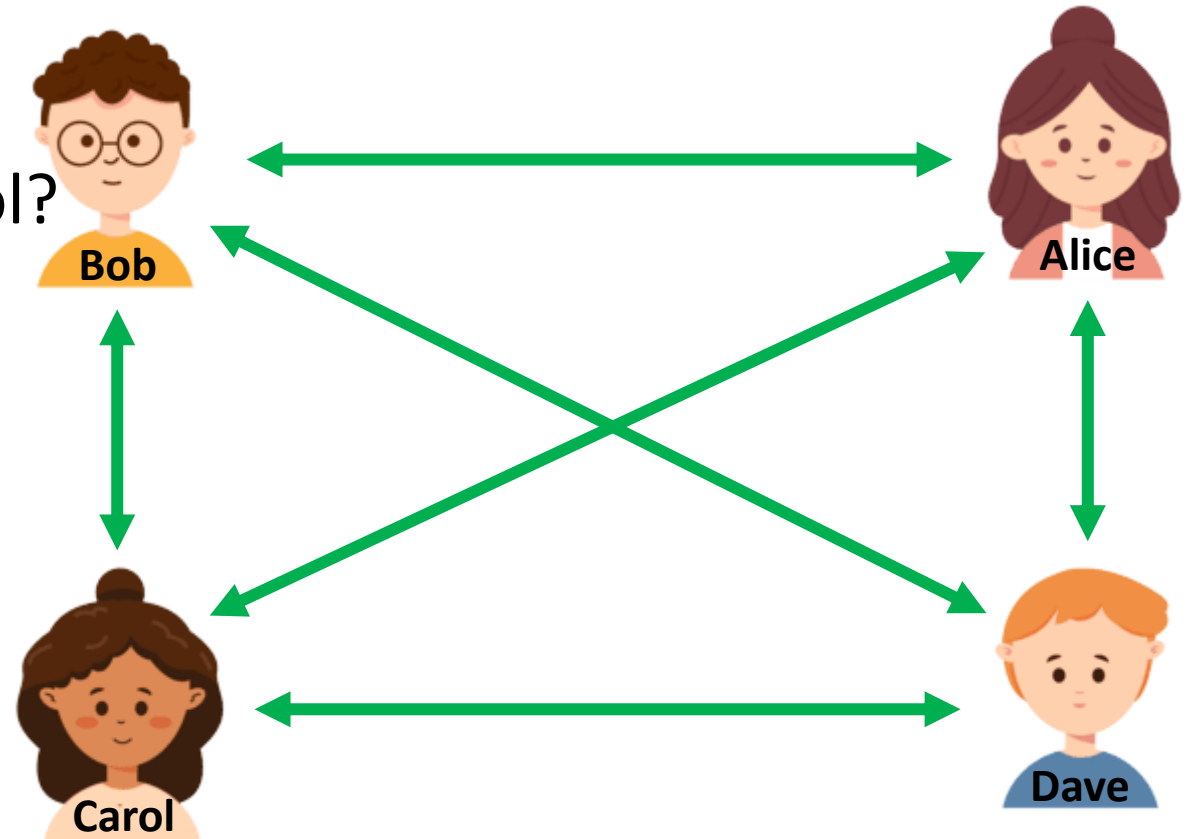
P2P: Reptes

- Què passa si un node és malèvol?
 - El servei pot deixar de funcionar
- Com es coordinen els nodes?
 - Cal arribar a un consens



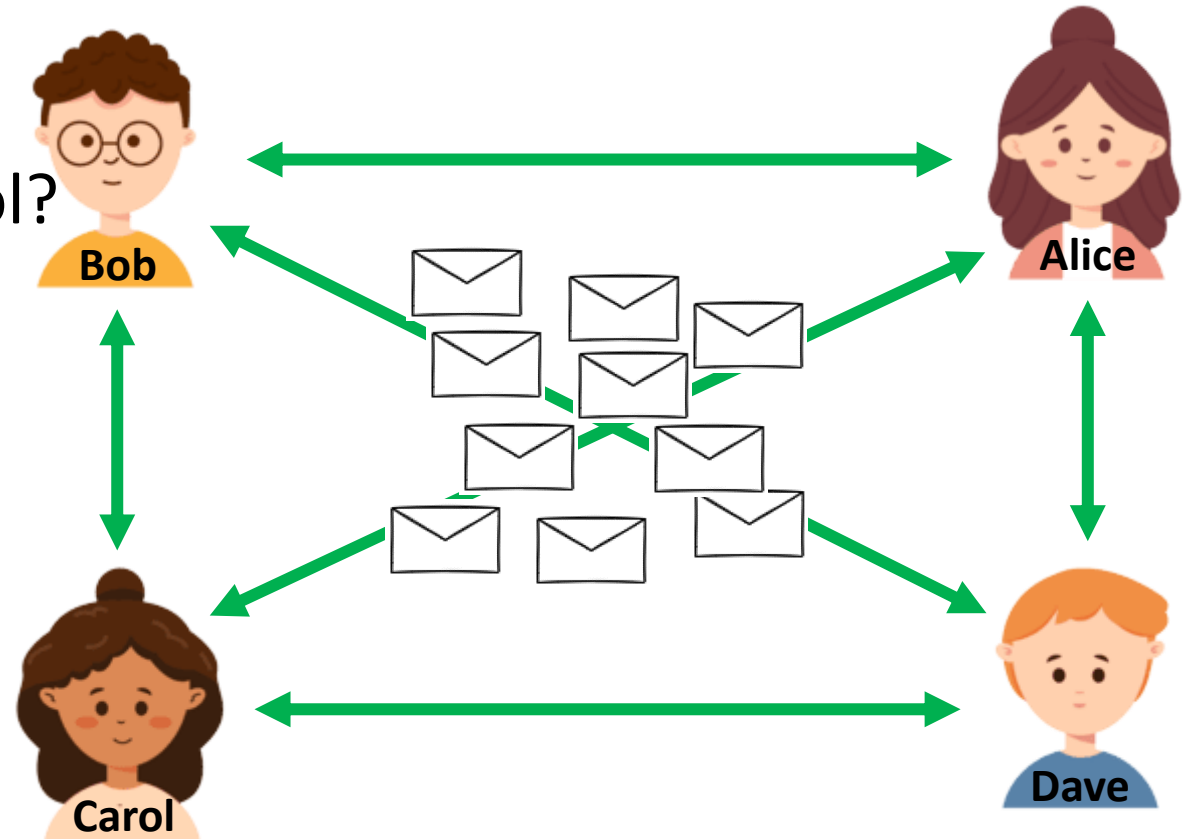
P2P: Reptes

- Què passa si un node és malèvol?
 - El servei pot deixar de funcionar
- Com es coordinen els nodes?
 - Cal arribar a un consens



P2P: Reptes

- Què passa si un node és malèvol?
 - El servei pot deixar de funcionar
- Com es coordinen els nodes?
 - Cal arribar a un consens





The background of the image is a dark blue field filled with glowing blue circuitry, including lines, nodes, and components like capacitors and resistors. Three data blocks are highlighted with yellow dashed lines connecting them in a chain. Each block contains a title and a list of binary data. A large white rectangle with black text is centered over the middle block.

Tecnologia Blockchain

Block 0xaf013c45

0 11101010 00 011000 010010 010
1010010 0100110001 1101001101011
110 10 1101 01 1100100111 1100

0 01010
10 10
11101000
1110 0
10001010
1100111
001 100
11010010
1 0010
01 0
010 10

1110110 0100 101101 000011101
101001011011 010100 11011101 01
00 01 01 0001111001100 0010011
001110 10010100 11 0010 00010
0001001 10111101 1100110111010001
10 01 010010010010 1001 11 011

Block 0x43a5fc78

100100011 0100 11101010 00 01100
101 00 110101010010 0100110001
10011000100 0110 10 1101 01 110

0010101110010 11110110 0100 101
0 0111 00 101001011011 010100
1000010001110100 01 01 000111110
0 11 10 01 001110 10010100 1
00011000101 10001001 10111101 110
00 01 1001 10 01 010010010010

0010101110010 11110110 0100 101
0 0111 00 101001011011 010100
1000010001110100 01 01 000111110
0 11 10 01 001110 10010100 1
00011000101 10001001 10111101 110
00 01 1001 10 01 010010010010

Block 0x10e6c7a9

01101 0000111011 0101001 0110010
0 11011101 01 001001 0101 00
1001100 001001101111011 1000 100

00 0110 1
0001010110001
10100001 00
1001010101010
0001 11 1
1101 011001
101101 00 0
00 01 11001
1101 011101
00010111001
11 11 10 0

001 0110 001000 100000 011100
000010111001001 10010010000111 010
011000 1010 10 01 1011 00 100
0 1101100110011001 00100110 11010
101 011010 11 01010011 0011 010
001100101010 001111011001 1001

001 0110 001000 100000 011100
000010111001001 10010010000111 010
011000 1010 10 01 1011 00 100
0 1101100110011001 00100110 11010
101 011010 11 01010011 0011 010
001100101010 001111011001 1001

Tecnologia Blockchain: Definició

Registre distribuït que conté llistes creixents de blocs enllaçats de manera segura mitjançant hashes criptogràfics

Tecnologia Blockchain: Definició

Registre distribuït que conté llistes creixents de blocs enllaçats de manera segura mitjançant hashes criptogràfics

Tecnologia Blockchain: Definició

***Registre distribuït** que conté **llistes creixents de blocs enllaçats** de manera segura mitjançant
hashs criptogràfics*

Tecnologia Blockchain: Definició

Registre distribuït** que conté **llistes creixents de blocs enllaçats** de **manera segura** mitjançant **hashs criptogràfics

Tecnologia Blockchain: Definició

Registre distribuït que conté *llistes creixents de blocs enllaçats* de *manera segura* mitjançant *hashs criptogràfics*

Registre Distribuit: Introducció

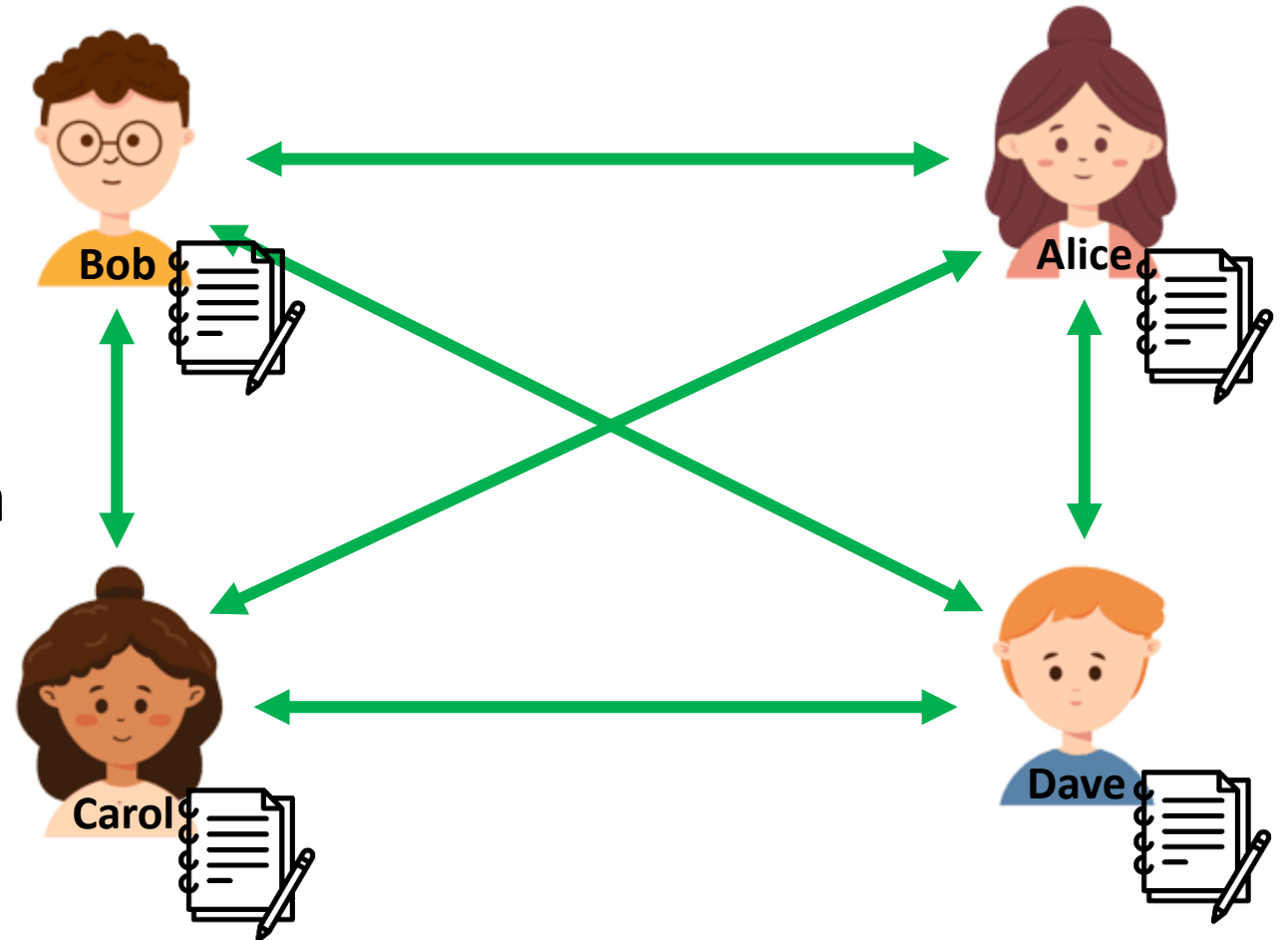
Registre Distribuït: Introducció

- Emmagatzema dades digitals
 - Transaccions econòmiques
 - Registre de propietats
- Cada node en guarda una còpia
- Requereix sincronització



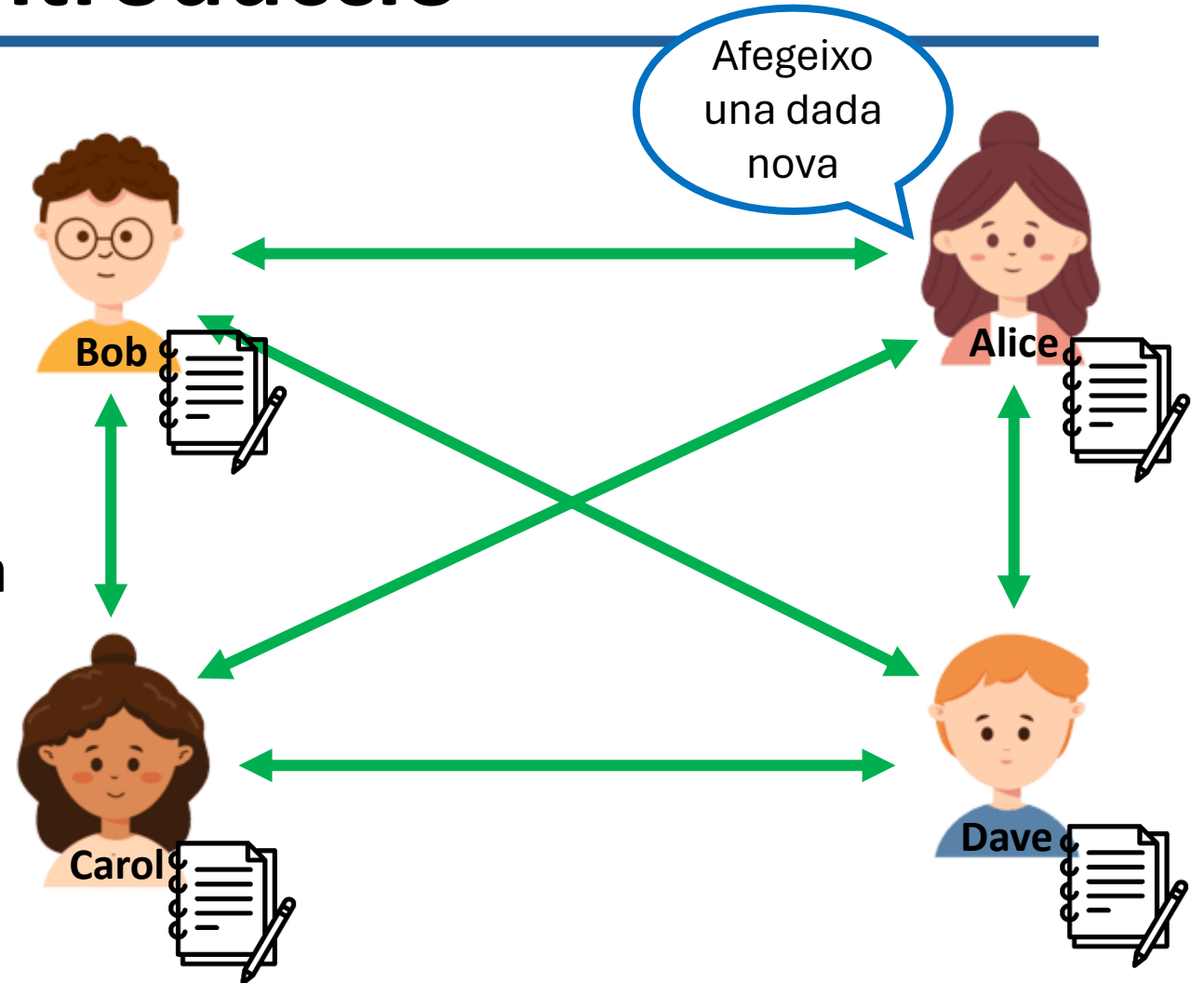
Registre Distribuït: Introducció

- Emmagatzema dades digitals
 - Transaccions econòmiques
 - Registre de propietats
- Cada node en guarda una còpia
- Requereix sincronització



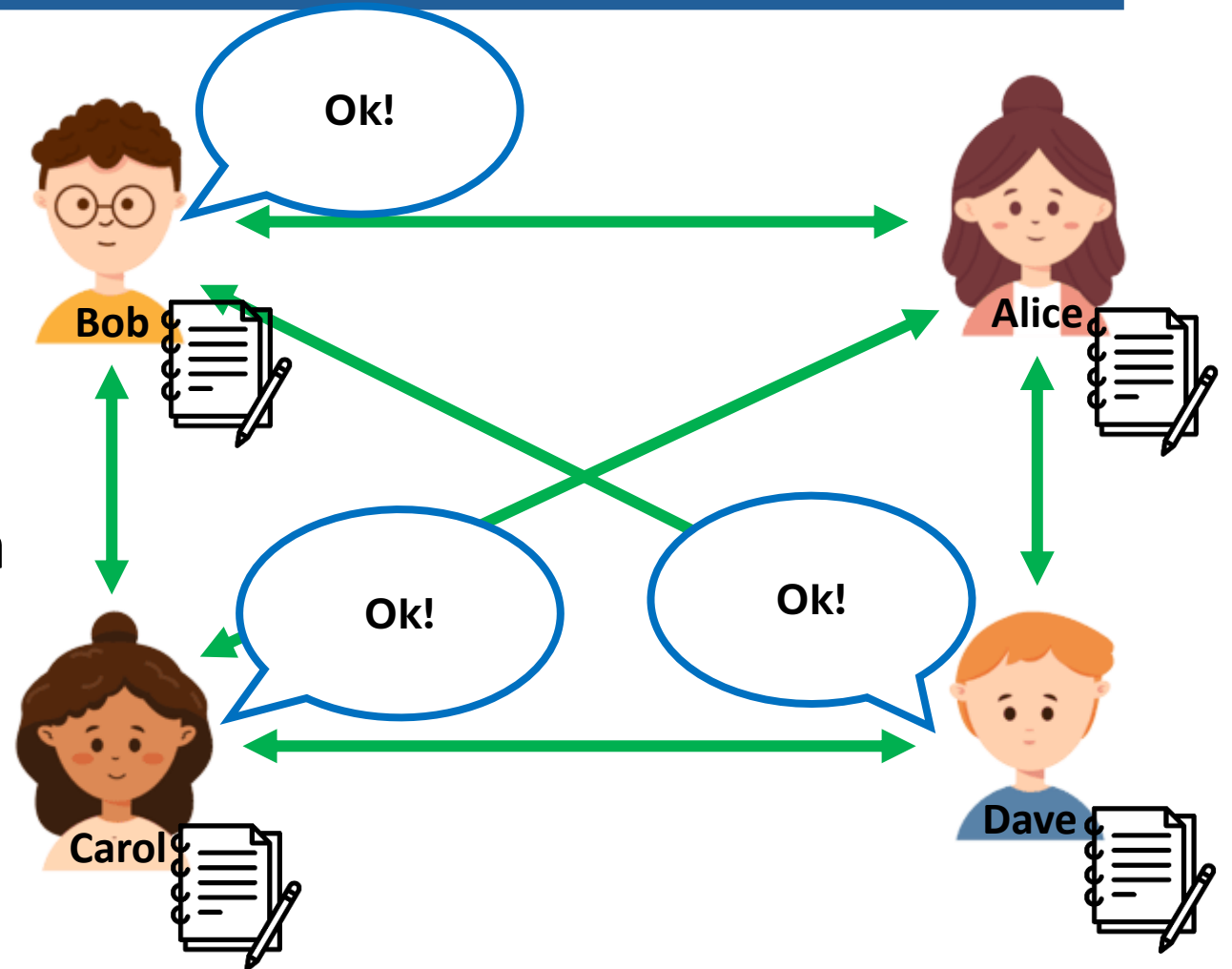
Registre Distribuït: Introducció

- Emmagatzema dades digitals
 - Transaccions econòmiques
 - Registre de propietats
- Cada node en guarda una còpia
- Requereix sincronització



Registre Distribuït: Introducció

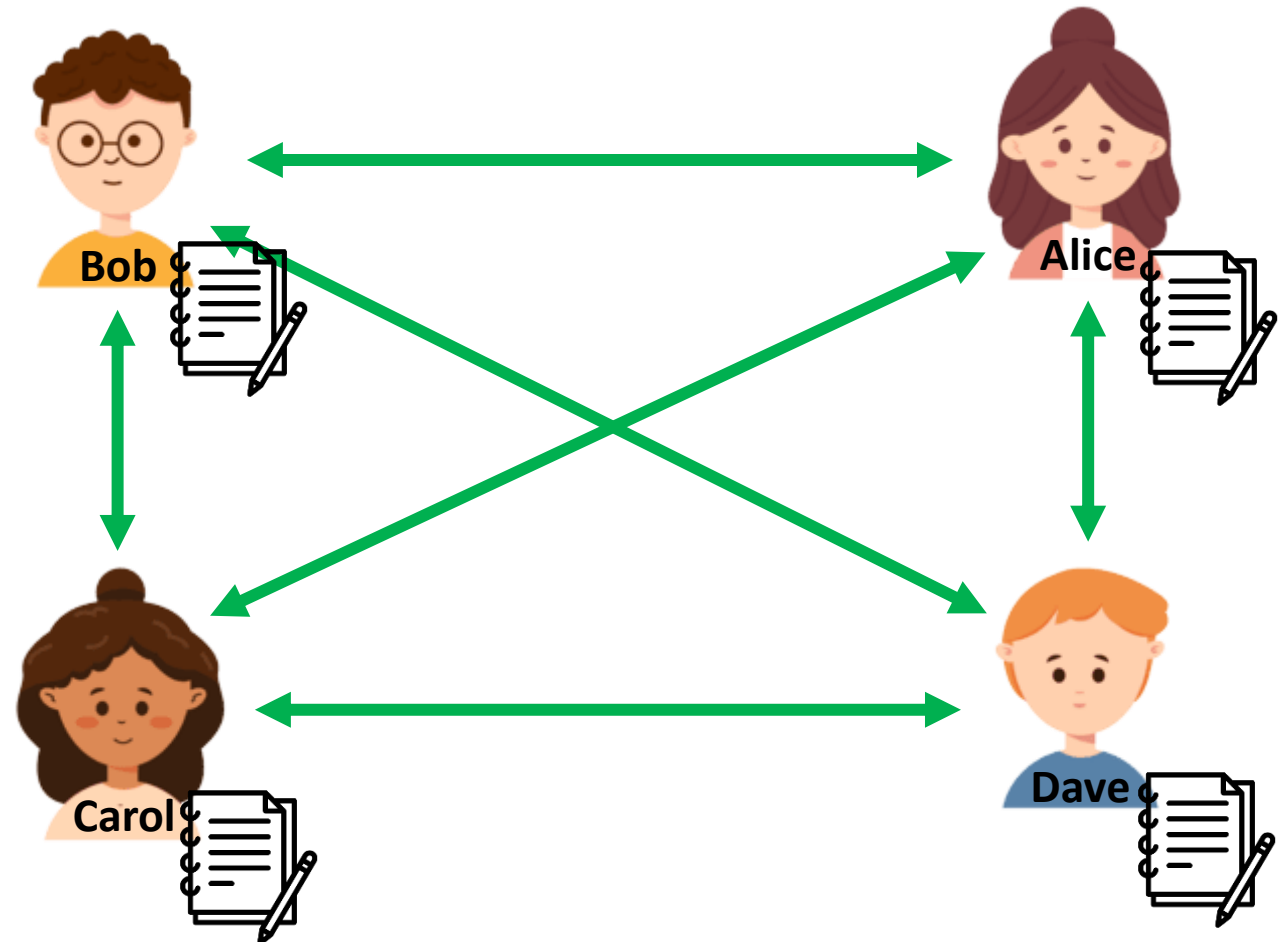
- Emmagatzema dades digitals
 - Transaccions econòmiques
 - Registre de propietats
- Cada node en guarda una còpia
- Requereix sincronització



Registre Distribuit: Exemple

Registre Distribuït: Exemple

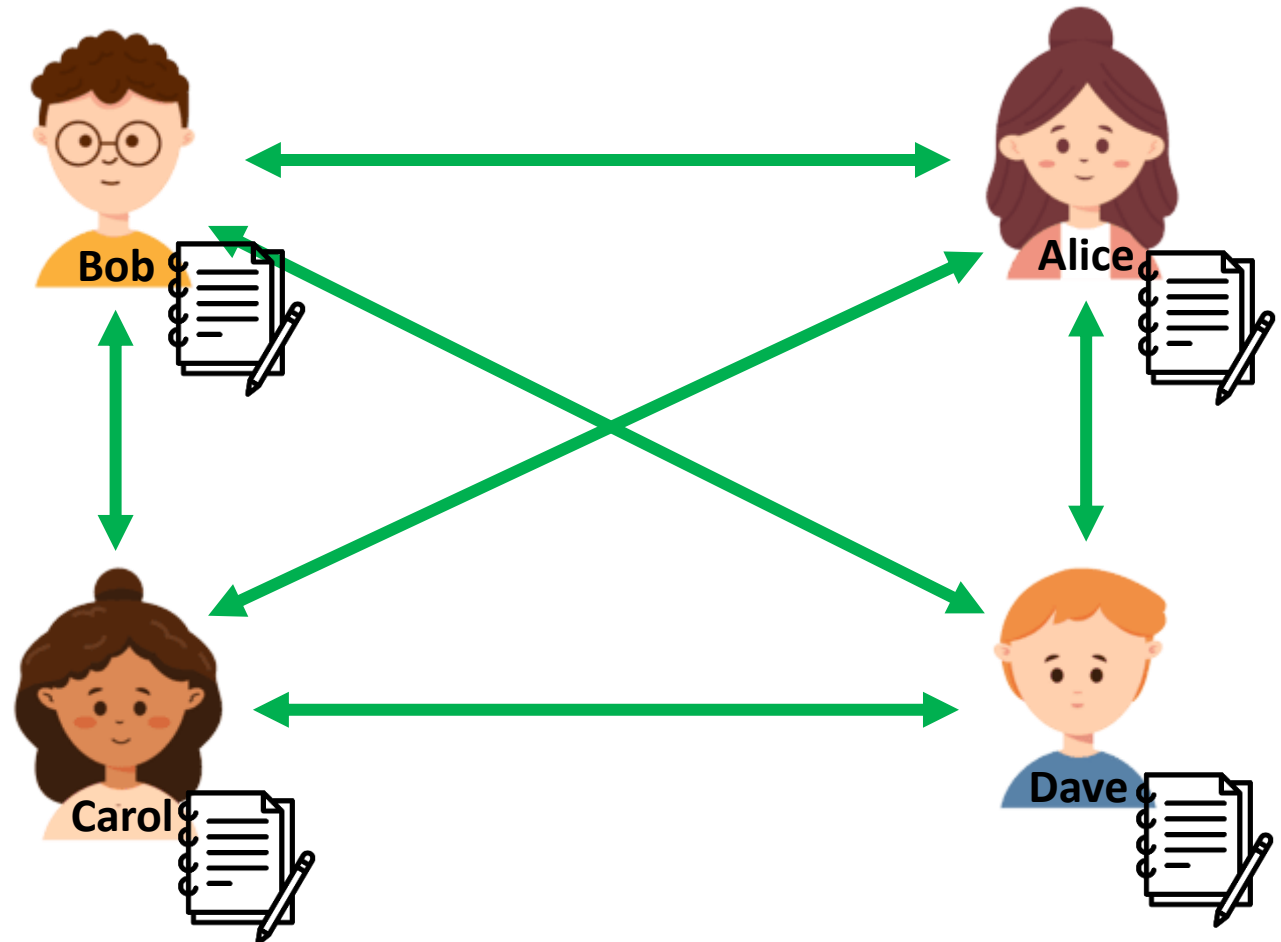
Registre de despeses d'un grup d'amics



Registre Distribuït: Exemple

Registre de despeses d'un grup d'amics

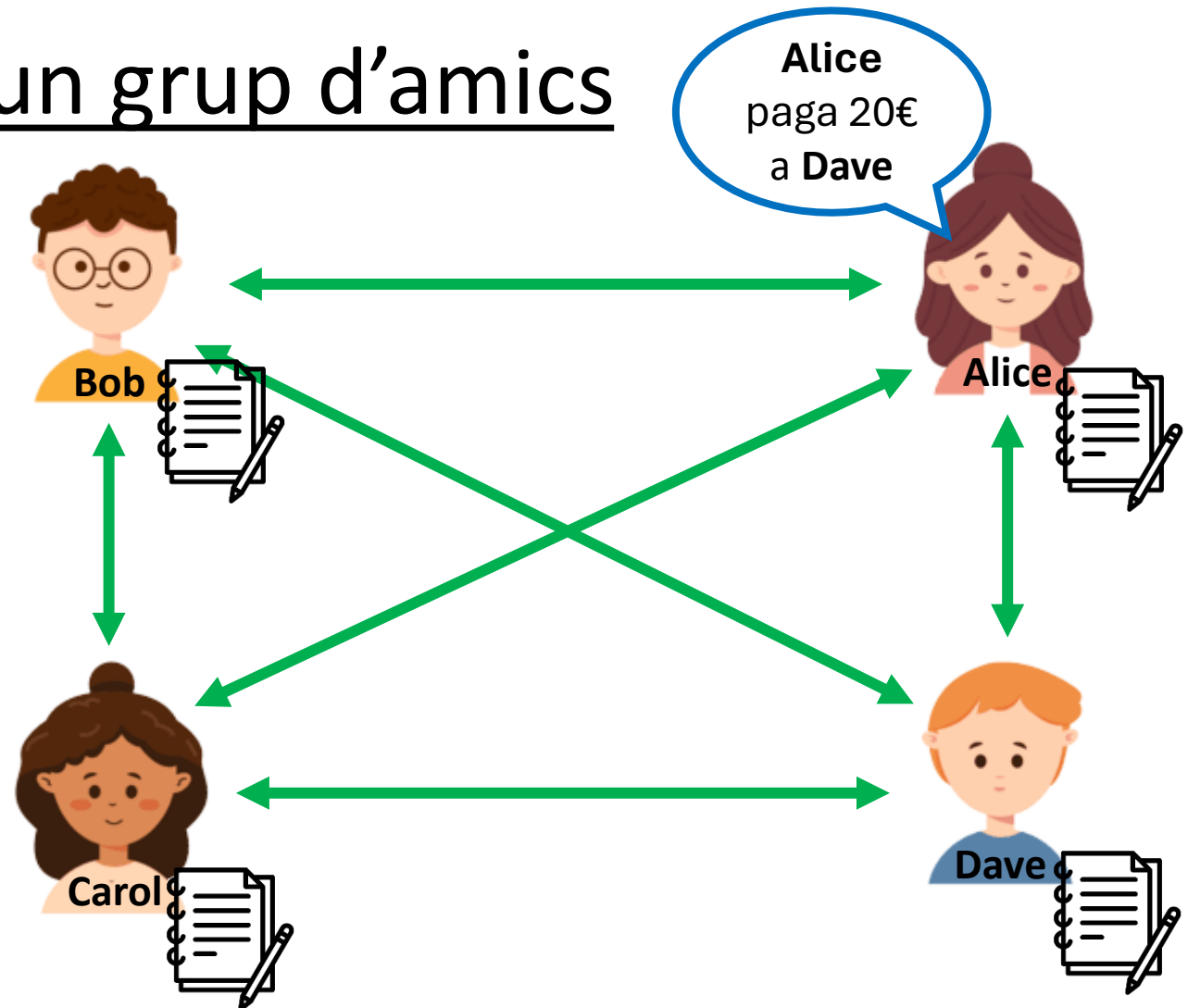
Bob paga 10€ a **Alice**
Dave paga 25€ a **Carol**
Carol paga 5€ a **Bob**
Alice paga 20€ a **Dave**



Registre Distribuït: Exemple

Registre de despeses d'un grup d'amics

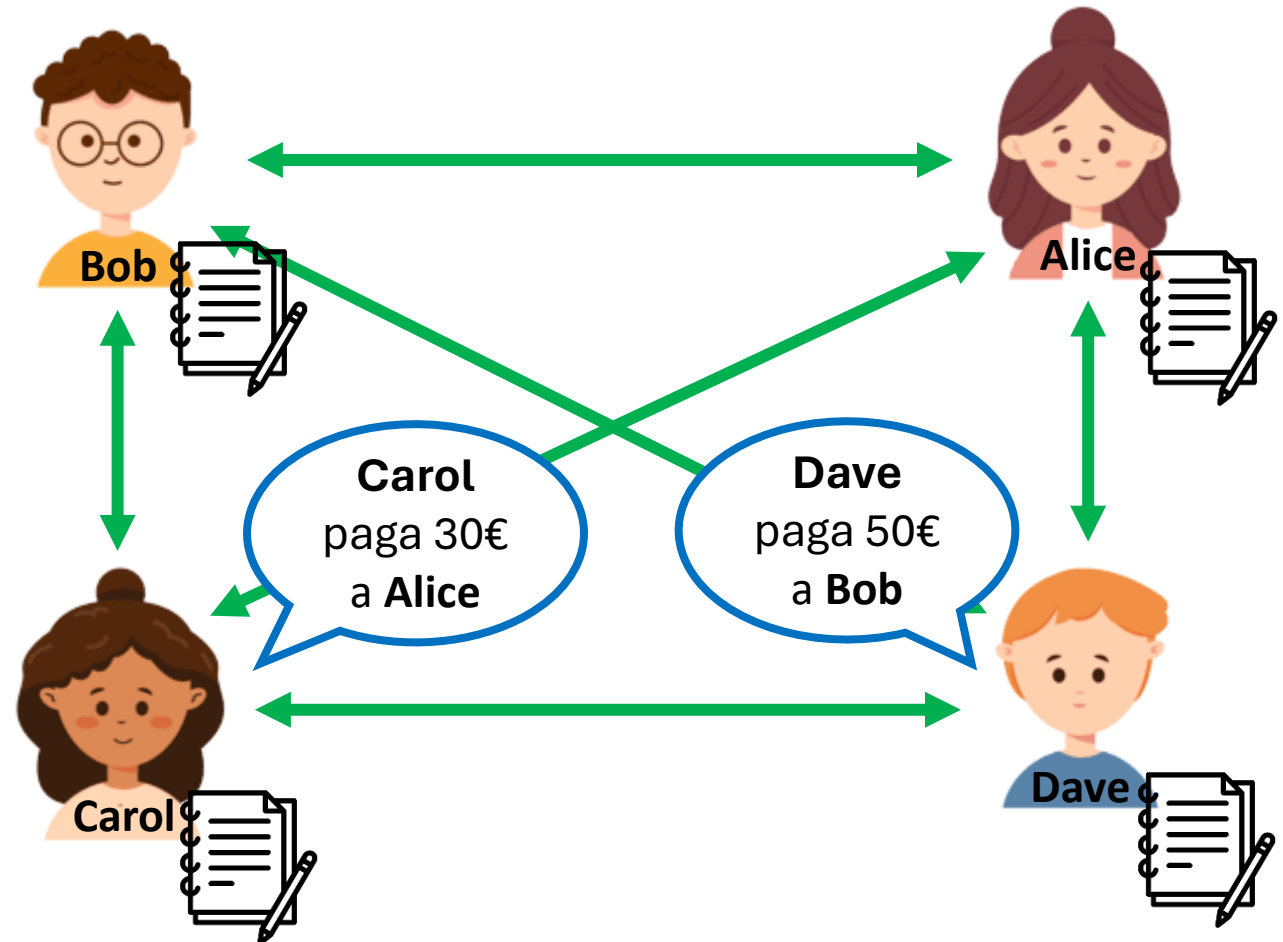
Bob paga 10€ a **Alice**
Dave paga 25€ a **Carol**
Carol paga 5€ a **Bob**
Alice paga 20€ a **Dave**



Registre Distribuït: Exemple

Registre de despeses d'un grup d'amics

Bob paga 10€ a **Alice**
Dave paga 25€ a **Carol**
Carol paga 5€ a **Bob**
Alice paga 20€ a **Dave**

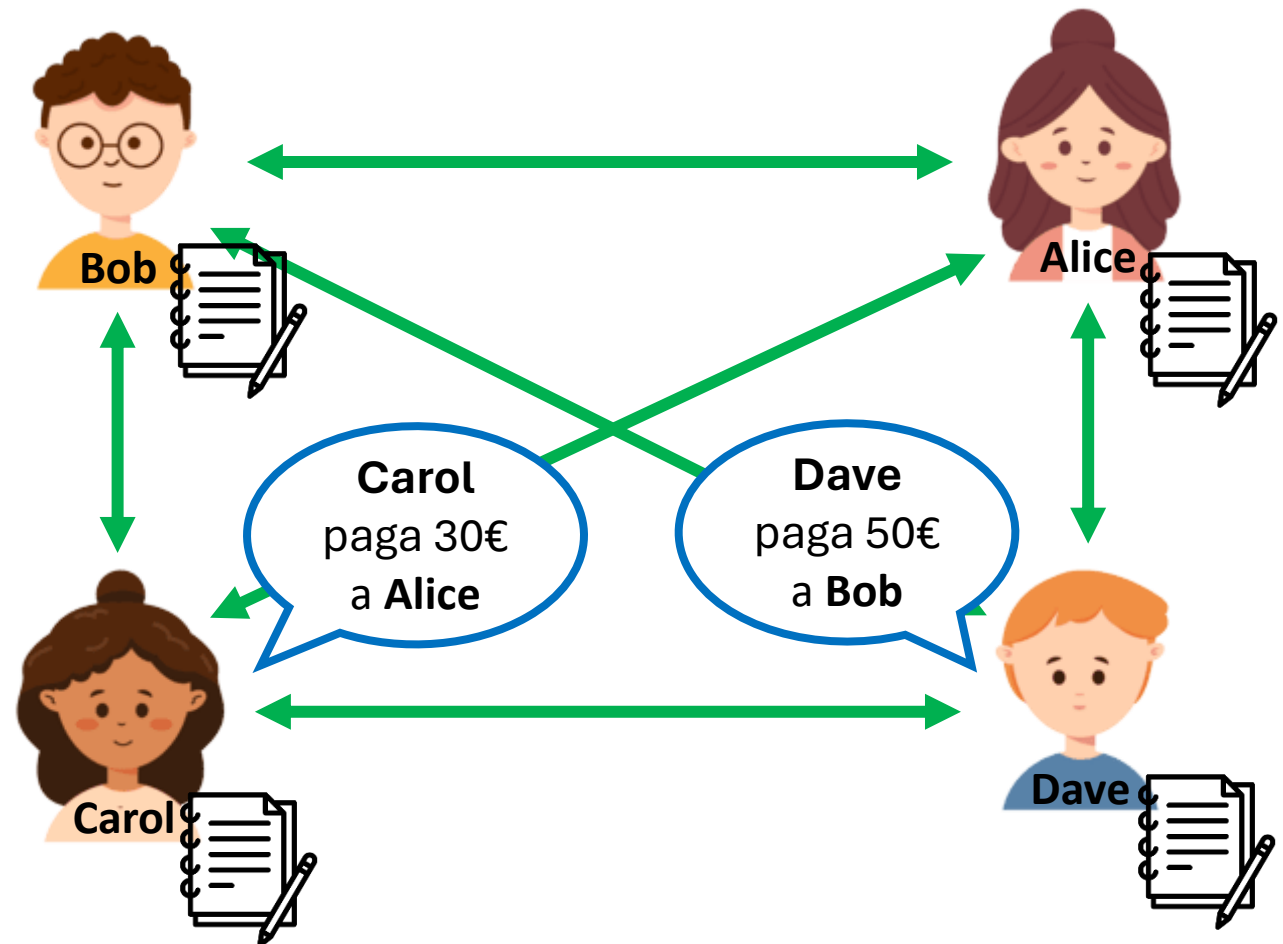


Registre Distribuït: Exemple

Registre de despeses d'un grup d'amics

Bob paga 10€ a **Alice**
Dave paga 25€ a **Carol**
Carol paga 5€ a **Bob**
Alice paga 20€ a **Dave**

Quin pagament
registrem primer?



Blocs Enllaçats: Introducció

Blocs Enllaçats: Introducció

Conjunt mínim de dades que es guarden al registre distribuït

Blocs Enllaçats: Introducció

Conjunt mínim de dades que es guarden al registre distribuït

Registre distribuït

Blocs Enllaçats: Introducció

Conjunt mínim de dades que es guarden al registre distribuït

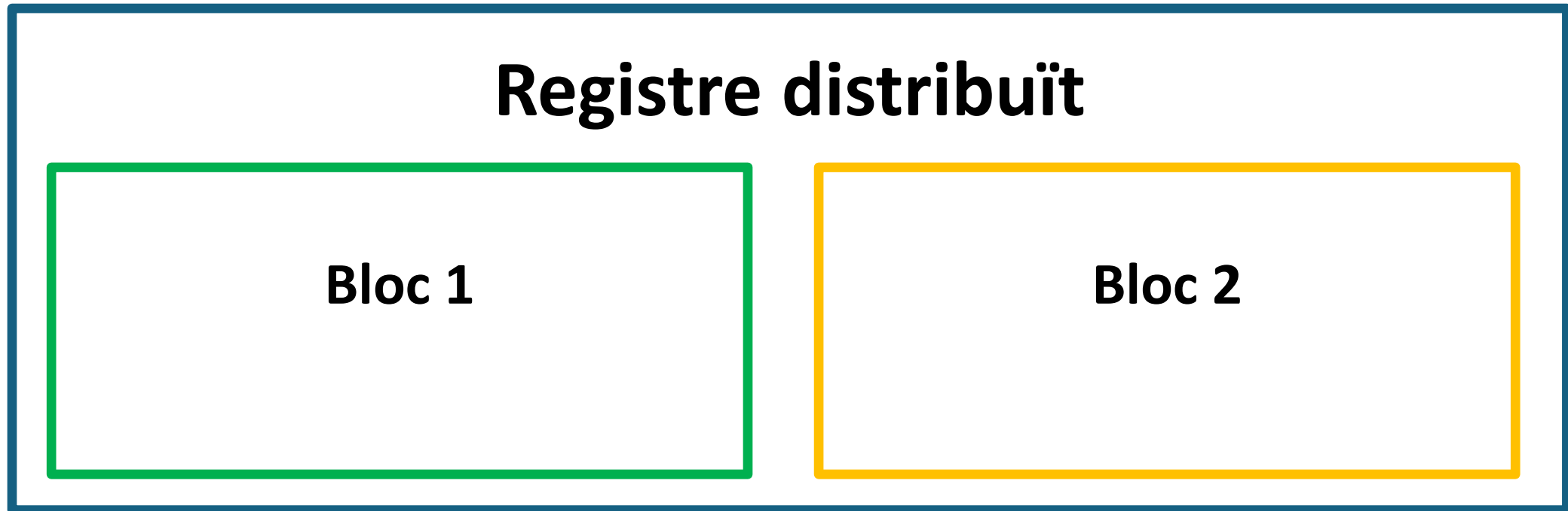
Registre distribuït

Bloc 1

A diagram illustrating a distributed register. A large blue-outlined rectangle represents the 'Registre distribuït' (distributed register). Inside this rectangle, at the top center, is the text 'Registre distribuït'. In the bottom-left corner of the blue rectangle is a smaller green-outlined rectangle labeled 'Bloc 1' in its center.

Blocs Enllaçats: Introducció

Conjunt mínim de dades que es guarden al registre distribuït



Blocs Enllaçats: Exemple

Blocs Enllaçats: Exemple

Cada bloc conté 4 transaccions diferents

Blocs Enllaçats: Exemple

Cada bloc conté 4 transaccions diferents

Registre de despeses d'un grup d'amics

Blocs Enllaçats: Exemple

Cada bloc conté 4 transaccions diferents

Registre de despeses d'un grup d'amics

Bob paga 10€ a **Alice**
Dave paga 25€ a **Carol**
Carol paga 5€ a **Bob**
Alice paga 20€ a **Dave**

Blocs Enllaçats: Exemple

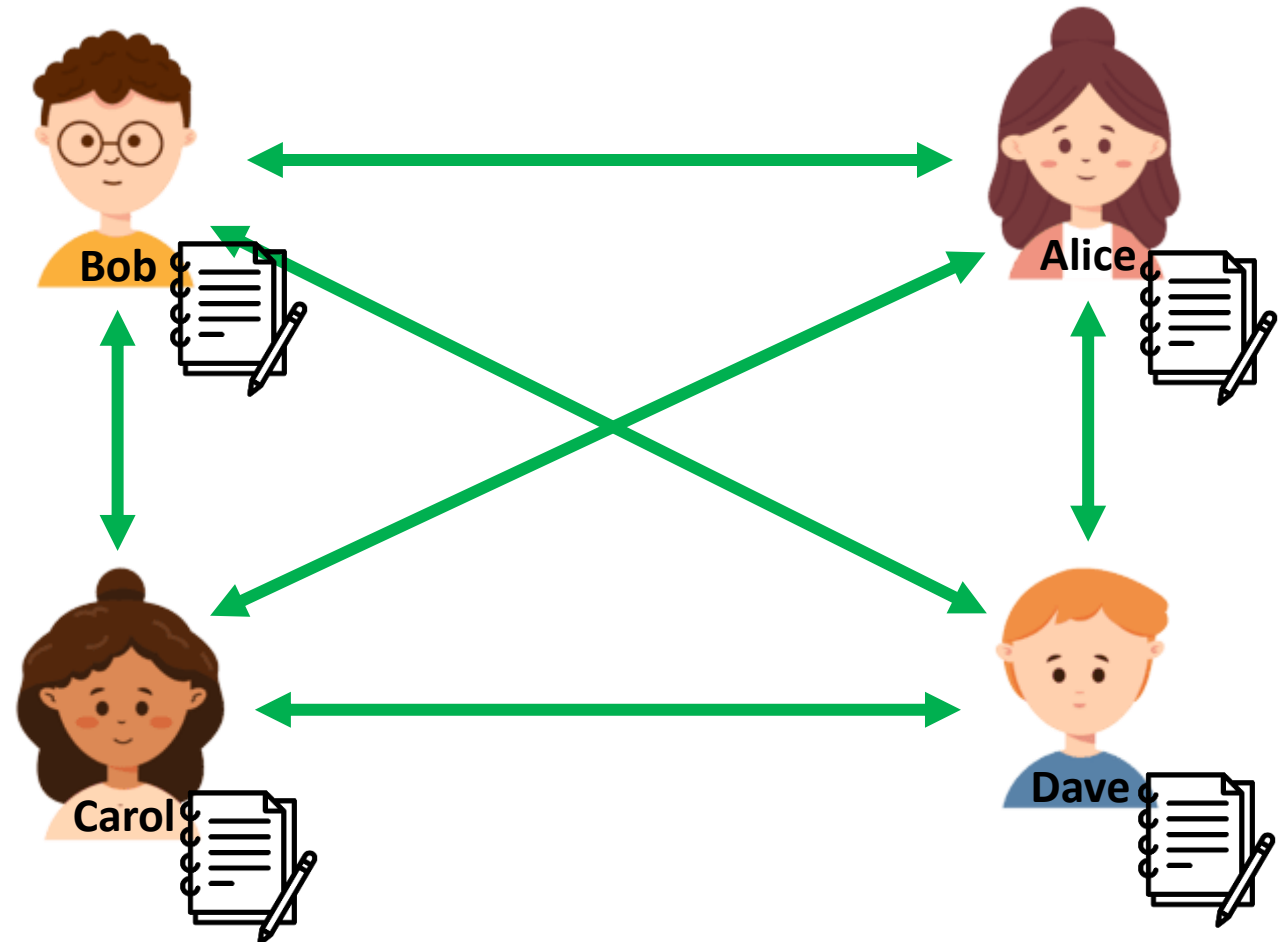
Cada bloc conté 4 transaccions diferents

Registre de despeses d'un grup d'amics

Bob paga 10€ a **Alice**
Dave paga 25€ a **Carol**
Carol paga 5€ a **Bob**
Alice paga 20€ a **Dave**

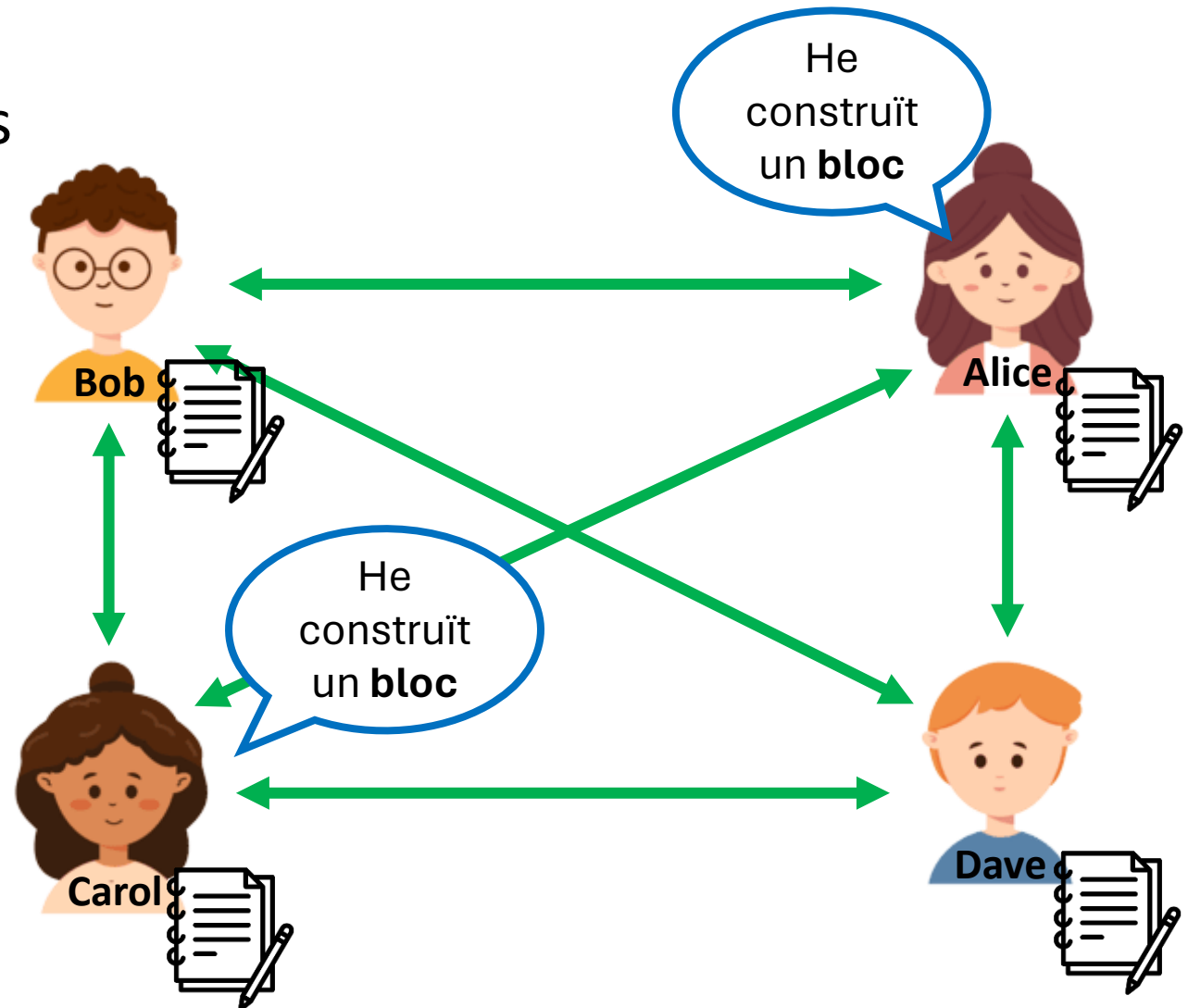
Dave paga 55€ a **Bob**
Alice paga 60€ a **Dave**
Bob paga 75€ a **Carol**
Carol paga 80€ a **Alice**

Blocs Enllaçats: Reptes



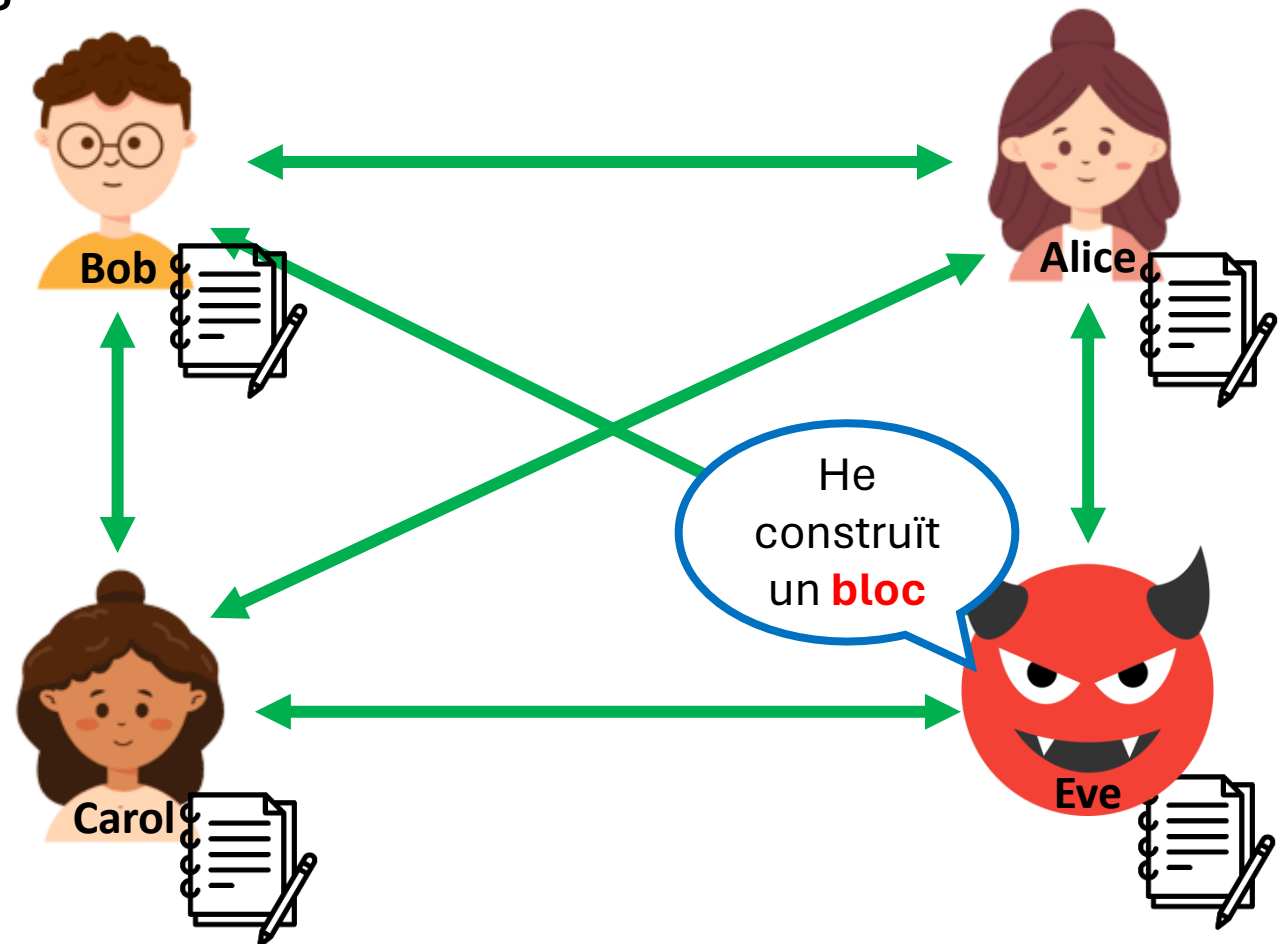
Blocs Enllaçats: Reptes

- Què passa si es construeixen dos blocs a la vegada?
- Què passa si un node malèvol construeix un bloc amb dades incorrectes?
- Què vol dir que els blocs estan enllaçats?



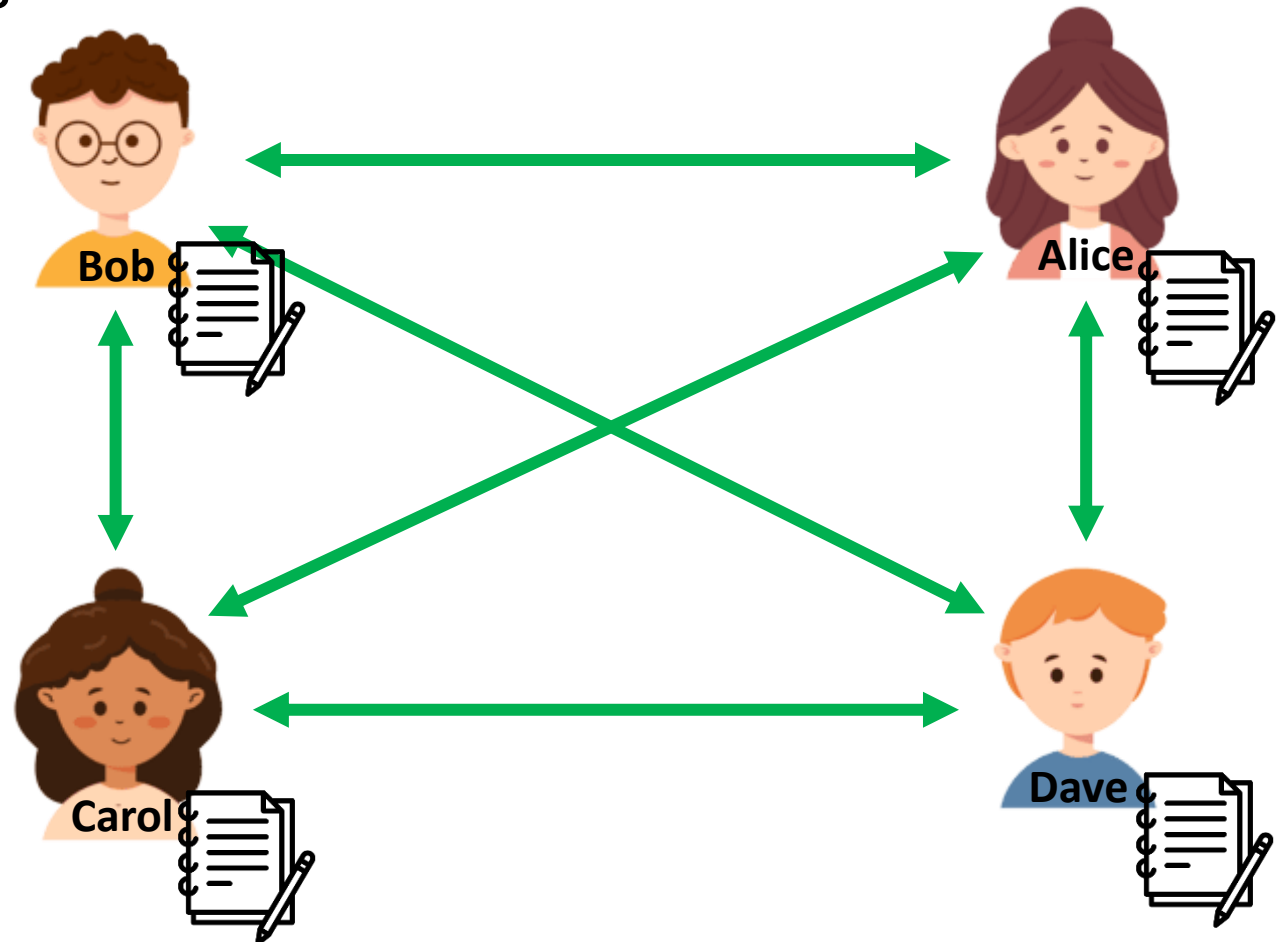
Blocs Enllaçats: Reptes

- Què passa si es construeixen dos blocs a la vegada?
- Què passa si un node malèvol construeix un bloc amb dades incorrectes?
- Què vol dir que els blocs estan enllaçats?



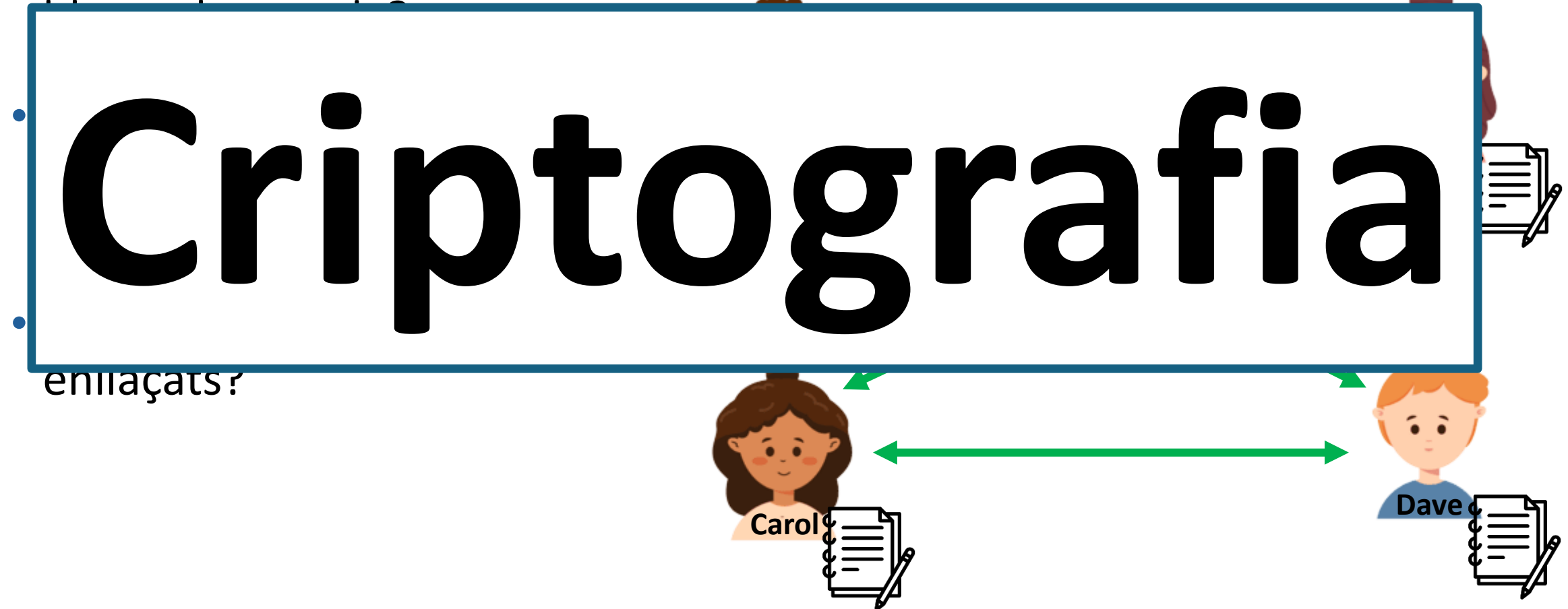
Blocs Enllaçats: Reptes

- Què passa si es construeixen dos blocs a la vegada?
- Què passa si un node malèvol construeix un bloc amb dades incorrectes?
- Què vol dir que els blocs estan enllaçats?



Blocs Enllaçats: Reptes

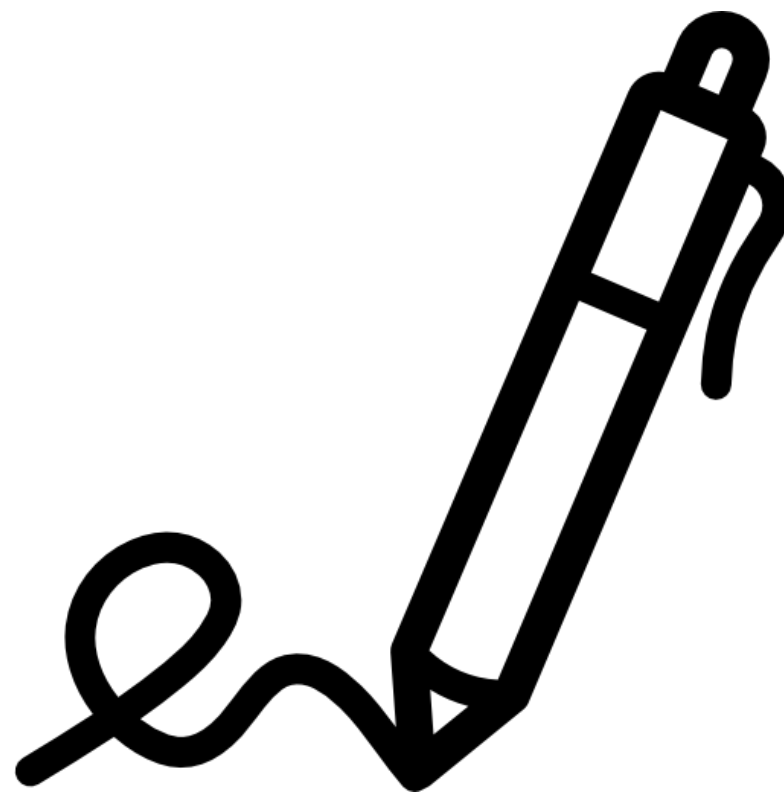
- Què passa si es construeixen dos



Criptografia: Definició

Pràctica i estudi de tècniques de comunicació segura en presència de comportaments adversos

Criptografia: Signatures Digital



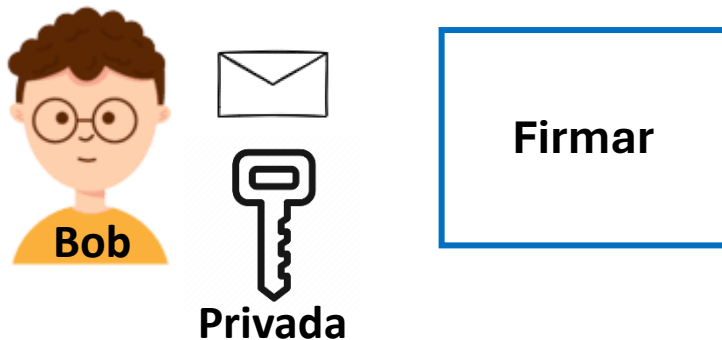
Criptografia: Signatures Digital

- Anàleg digital de les firmes a mà
- Permeten garantir l'autoria d'un missatge
- Basades en problemes matemàtics
- Cada node disposa d'una clau pública i d'una clau privada



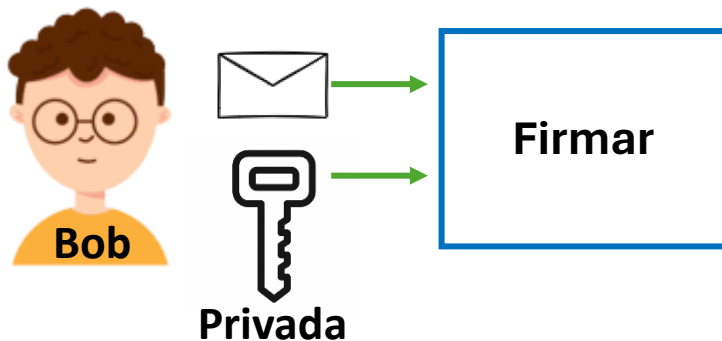
Criptografia: Signatures Digitals

- Anàleg digital de les firmes a mà
- Permeten garantir l'autoria d'un missatge
- Basades en problemes matemàtics
- Cada node disposa d'una clau pública i d'una clau privada



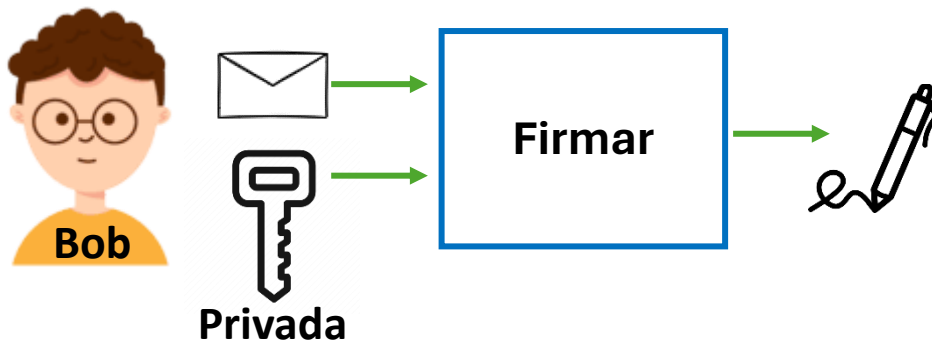
Criptografia: Signatures Digitals

- Anàleg digital de les firmes a mà
- Permeten garantir l'autoria d'un missatge
- Basades en problemes matemàtics
- Cada node disposa d'una clau pública i d'una clau privada



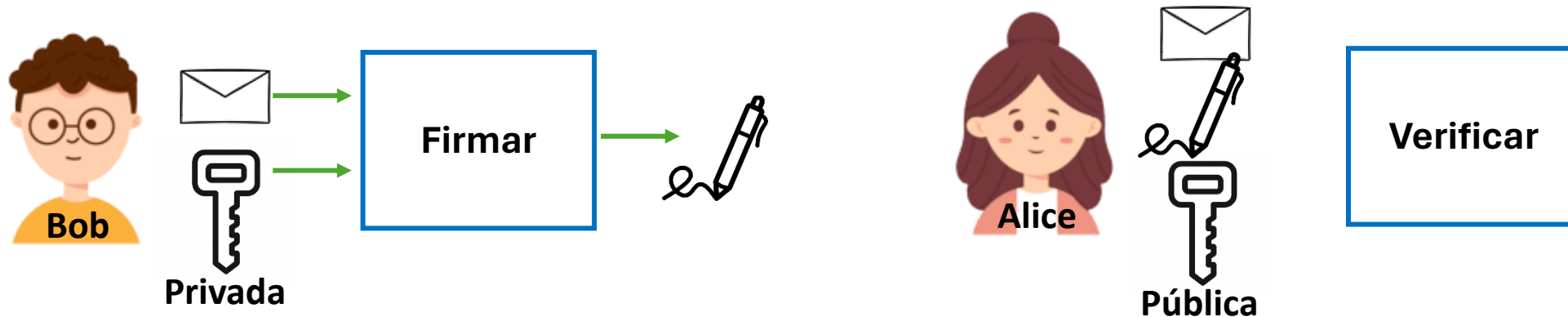
Criptografia: Signatures Digital

- Anàleg digital de les firmes a mà
- Permeten garantir l'autoria d'un missatge
- Basades en problemes matemàtics
- Cada node disposa d'una clau pública i d'una clau privada



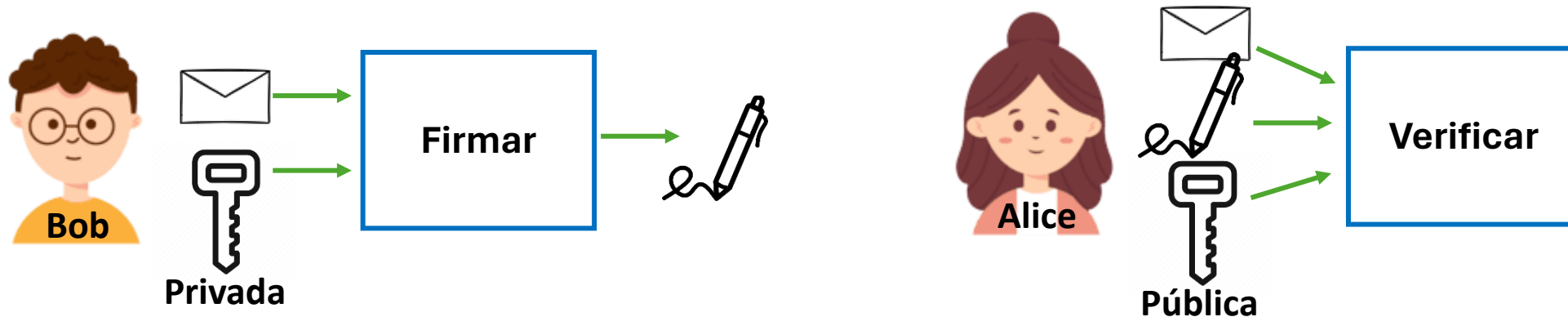
Criptografia: Signatures Digital

- Anàleg digital de les firmes a mà
- Permeten garantir l'autoria d'un missatge
- Basades en problemes matemàtics
- Cada node disposa d'una clau pública i d'una clau privada



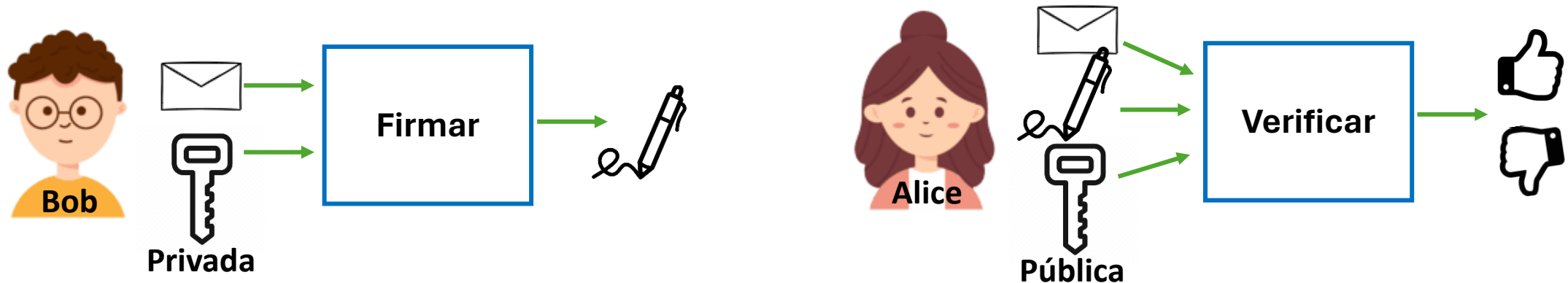
Criptografia: Signatures Digital

- Anàleg digital de les firmes a mà
- Permeten garantir l'autoria d'un missatge
- Basades en problemes matemàtics
- Cada node disposa d'una clau pública i d'una clau privada



Criptografia: Signatures Digital

- Anàleg digital de les firmes a mà
- Permeten garantir l'autoria d'un missatge
- Basades en problemes matemàtics
- Cada node disposa d'una clau pública i d'una clau privada



Criptografia: Funcions Hash

Criptografia: Funcions Hash

- Algorisme que assigna a cada element un identificador numèric únic
- Basats en problemes matemàtics
- Acostumen a ser impredictibles
- Exemple: calcular el residu de dividir entre 7

Criptografia: Funcions Hash

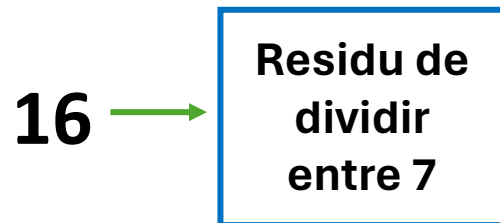
- Algorisme que assigna a cada element un identificador numèric únic
- Basats en problemes matemàtics
- Acostumen a ser impredecibles
- Exemple: calcular el residu de dividir entre 7

16

**Residu de
dividir
entre 7**

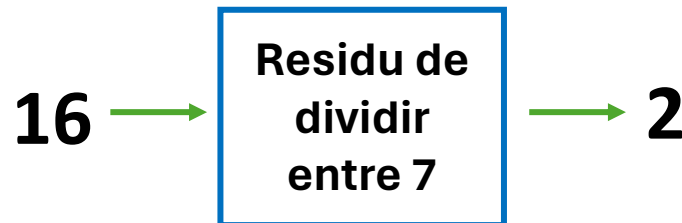
Criptografia: Funcions Hash

- Algorisme que assigna a cada element un identificador numèric únic
- Basats en problemes matemàtics
- Acostumen a ser impredecibles
- Exemple: calcular el residu de dividir entre 7



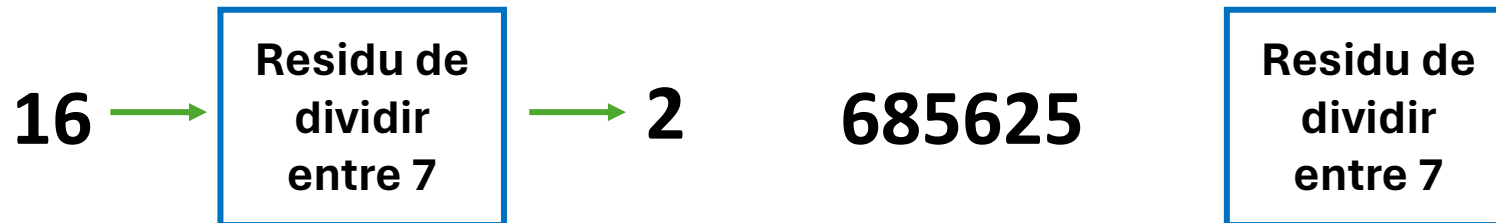
Criptografia: Funcions Hash

- Algorisme que assigna a cada element un identificador numèric únic
- Basats en problemes matemàtics
- Acostumen a ser impredecibles
- Exemple: calcular el residu de dividir entre 7



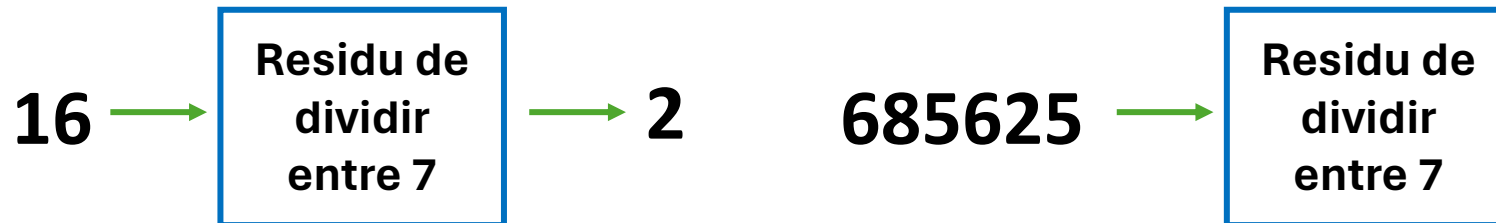
Criptografia: Funcions Hash

- Algorisme que assigna a cada element un identificador numèric únic
- Basats en problemes matemàtics
- Acostumen a ser impredecibles
- Exemple: calcular el residu de dividir entre 7



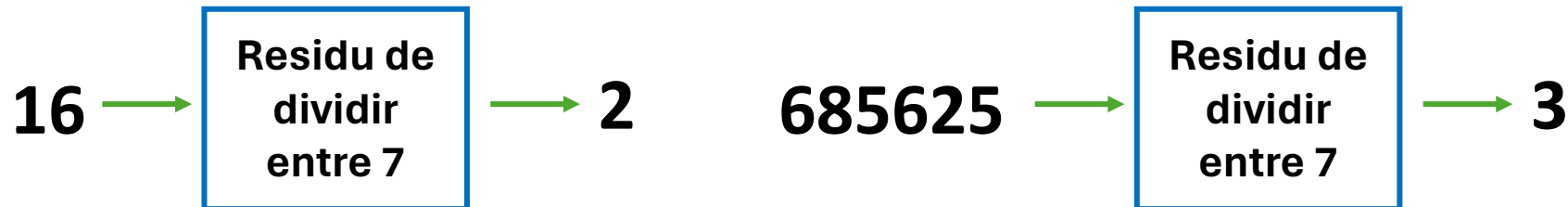
Criptografia: Funcions Hash

- Algorisme que assigna a cada element un identificador numèric únic
- Basats en problemes matemàtics
- Acostumen a ser impredecibles
- Exemple: calcular el residu de dividir entre 7



Criptografia: Funcions Hash

- Algorisme que assigna a cada element un identificador numèric únic
- Basats en problemes matemàtics
- Acostumen a ser impredecibles
- Exemple: calcular el residu de dividir entre 7



Blocs enllaçats: Avenços

Registre distribuït

Bloc 1

Dada **1.1**

Dada **1.2**

Bloc 2

Dada **2.1**


Dada **2.2**

Blocs enllaçats: Avenços

- Totes les dades inclouen la signatura digital del seu autor
- Cada bloc té un identificador numèric calculat amb una funció hash
- Cada bloc inclou el hash del bloc anterior
- El hash d'un bloc **depèn del bloc anterior**

Registre distribuït

Bloc 1

Dada **1.1** 

Dada **1.2** 

Bloc 2

Dada **2.1** 


Dada **2.2** 

Blocs enllaçats: Avenços

- Totes les dades inclouen la signatura digital del seu autor
- Cada bloc té un identificador numèric calculat amb una funció hash
- Cada bloc inclou el hash del bloc anterior
- El hash d'un bloc **depèn del bloc anterior**

Registre distribuït

1010101011

Dada **1.1** 

Dada **1.2** 

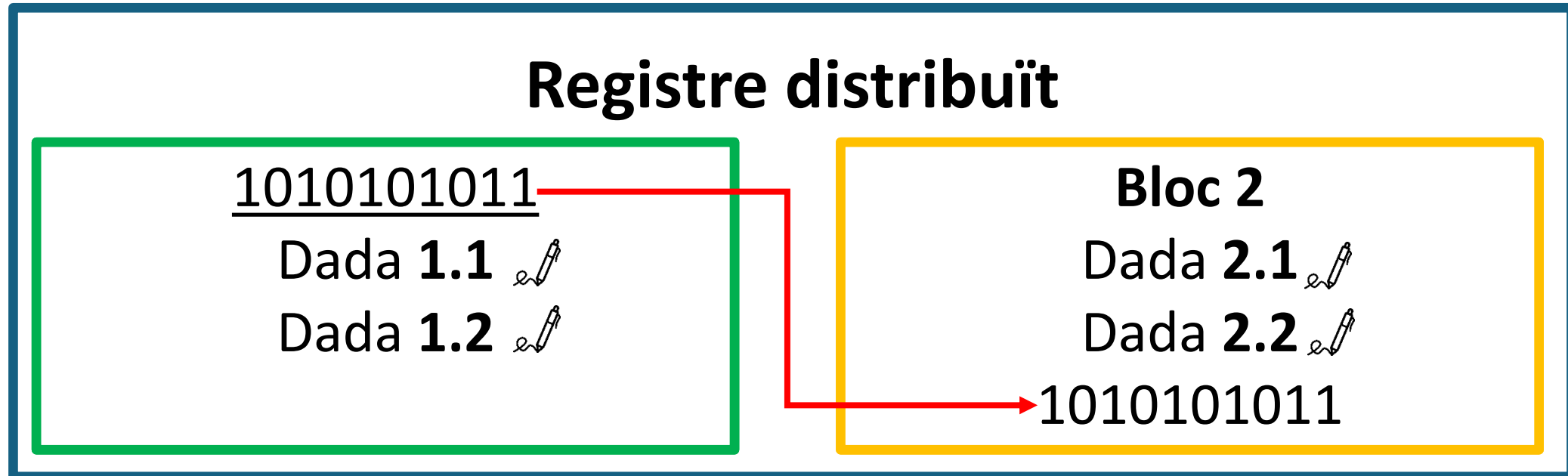
Bloc 2

Dada **2.1** 

Dada **2.2** 

Blocs enllaçats: Avenços

- Totes les dades inclouen la signatura digital del seu autor
- Cada bloc té un identificador numèric calculat amb una funció hash
- Cada bloc inclou el hash del bloc anterior
- El hash d'un bloc **depèn del bloc anterior**




Blocs enllaçats: Avenços

- Totes les dades inclouen la signatura digital del seu autor
- Cada bloc té un identificador numèric calculat amb una funció hash
- Cada bloc inclou el hash del bloc anterior
- El hash d'un bloc **depèn del bloc anterior**

Registre distribuït

1010101011

Dada **1.1** 

Dada **1.2** 

0000101010

Dada **2.1**

Dada **2.2**

1010101011



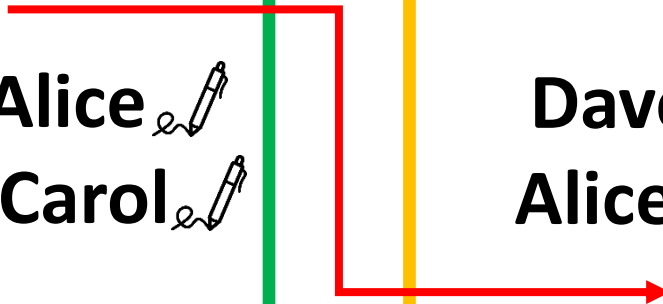
Blocs enllaçats: Avenços

- Totes les dades inclouen la signatura digital del seu autor
- Cada bloc té un identificador numèric calculat amb una funció hash
- Cada bloc inclou el hash del bloc anterior
- El hash d'un bloc **depèn del bloc anterior**

Registre de despeses d'un grup d'amics

5
Bob paga 10€ a **Alice** ✍️
Dave paga 25€ a **Carol** ✍️

3
Dave paga 55€ a **Bob** ✍️
Alice paga 60€ a **Dave** ✍️
5



Blocs enllaçats: Avenços

- Totes les dades inclouen la signatura digital del seu autor
- Cada bloc té un identificador numèric calculat amb una funció hash
- Cada bloc
- El hash d

**la sincronització
entre blocs?**

Bob paga 10€ a **Alice** ✍️
Dave paga 25€ a **Carol** ✍️

Dave paga 55€ a **Bob** ✍️
Alice paga 60€ a **Dave** ✍️

Prova de Treball: Introducció

Hash: 1010101100

Dada **1** 

Dada **2** 

Hash Bloc Anterior: 0111101101

Prova de Treball: Introducció

- Mecanisme de consens per decidir quin bloc s'afegeix a la cadena
- El Hash del nou bloc ha de tenir unes característiques determinades
- Cada bloc contindrà un valor arbitrari extra anomenat **Nonce**
- Canviar el Nonce canvia el Hash del bloc
- Provar diferents valors del Nonce fins obtenir el Hash desitjat

Hash: 1010101100

Dada **1** 

Dada **2** 

Hash Bloc Anterior: 0111101101

Prova de Treball: Introducció

- Mecanisme de consens per decidir quin bloc s'afegeix a la cadena
- El Hash del nou bloc ha de tenir unes característiques determinades
- Cada bloc contindrà un valor arbitrari extra anomenat **Nonce**
- Canviar el Nonce canvia el Hash del bloc
- Provar diferents valors del Nonce fins obtenir el Hash desitjat

Hash: 1010101100

Dada 1 

Dada 2 

Hash Bloc Anterior: 0111101101

Ha de començar per 0

Prova de Treball: Introducció

- Mecanisme de consens per decidir quin bloc s'afegeix a la cadena
- El Hash del nou bloc ha de tenir unes característiques determinades
- Cada bloc contindrà un valor arbitrari extra anomenat **Nonce**
- Canviar el Nonce canvia el Hash del bloc
- Provar diferents valors del Nonce fins obtenir el Hash desitjat

Hash: 1010101100

Dada 1 

Dada 2 

Hash Bloc Anterior: 0111101101

Nonce: 1

Ha de començar per 0

Prova de Treball: Introducció

- Mecanisme de consens per decidir quin bloc s'afegeix a la cadena
- El Hash del nou bloc ha de tenir unes característiques determinades
- Cada bloc contindrà un valor arbitrari extra anomenat **Nonce**
- Canviar el Nonce canvia el Hash del bloc
- Provar diferents valors del Nonce fins obtenir el Hash desitjat

Hash: 1100101100

Dada 1 

Dada 2 

Hash Bloc Anterior: 0111101101

Nonce: 2

Ha de començar per 0

Prova de Treball: Introducció

- Mecanisme de consens per decidir quin bloc s'afegeix a la cadena
- El Hash del nou bloc ha de tenir unes característiques determinades
- Cada bloc contindrà un valor arbitrari extra anomenat **Nonce**
- Canviar el Nonce canvia el Hash del bloc
- Provar diferents valors del Nonce fins obtenir el Hash desitjat

Hash: 0000110100

Dada 1 

Dada 2 

Hash Bloc Anterior: 0111101101

Nonce: 3

Ha de començar per 0

Prova de Treball: Introducció

- Mecanisme de consens per decidir quin bloc s'afegeix a la cadena
- El Hash del nou bloc ha de tenir unes característiques determinades
- Cada bloc contindrà un valor arbitrari extra anomenat **Nonce**
- Canviar el Nonce canvia el Hash del bloc
- Provar diferents valors del Nonce fins obtenir el Hash desitjat

Hash: 3

Dave paga 55€ a **Bob** 

Alice paga 60€ a **Dave** 

Hash Bloc Anterior: 5

Nonce: 2

Ha de ser **senar**

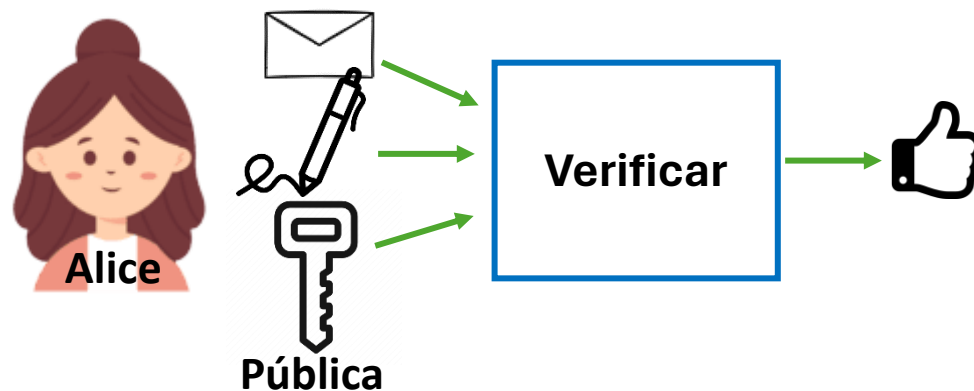
Prova de Treball: Minatge

Prova de Treball: Minatge

- Procés per construir un bloc vàlid
 1. Comprovar que la dada i la signatura digital coincideixen
 2. Agrupar les dades validades en un bloc
 3. Calcular el Nonce que permet obtenir un Hash amb les característiques demanades
- Els nodes que duen a terme aquesta tasca s'anomenen miners
- El miner rep una recompensa per cada bloc vàlid que construeix

Prova de Treball: Minatge

- Procés per construir un bloc vàlid
 1. Comprovar que la dada i la signatura digital coincideixen
 2. Agrupar les dades validades en un bloc
 3. Calcular el Nonce que permet obtenir un Hash amb les característiques demanades
- Els nodes que duen a terme aquesta tasca s'anomenen miners
- El miner rep una recompensa per cada bloc vàlid que construeix



Prova de Treball: Minatge

- Procés per construir un bloc vàlid
 1. Comprovar que la dada i la signatura digital coincideixen
 2. Agrupar les dades validades en un bloc
 3. Calcular el Nonce que permet obtenir un Hash amb les característiques demanades
- Els nodes que duen a terme aquesta tasca s'anomenen miners
- El miner rep una recompensa per cada bloc vàlid que construeix

Hash: 1010101100

Dada 1 

Dada 2 

Hash Bloc Anterior: 0111101101

Nonce: 1



Prova de Treball: Minatge

- Procés per construir un bloc vàlid
 1. Comprovar que la dada i la signatura digital coincideixen
 2. Agrupar les dades validades en un bloc
 3. Calcular el Nonce que permet obtenir un Hash amb les característiques demanades
- Els nodes que duen a terme aquesta tasca s'anomenen miners
- El miner rep una recompensa per cada bloc vàlid que construeix

Hash: 1010101100

Dada 1 

Dada 2 

Hash Bloc Anterior: 0111101101

Nonce: 1

Ha de començar per 0



Prova de Treball: Minatge

- Procés per construir un bloc vàlid
 1. Comprovar que la dada i la signatura digital coincideixen
 2. Agrupar les dades validades en un bloc
 3. Calcular el Nonce que permet obtenir un Hash amb les característiques demanades
- Els nodes que duen a terme aquesta tasca s'anomenen miners
- El miner rep una recompensa per cada bloc vàlid que construeix

Hash: 0000110100

Dada 1

Dada 2

Hash Bloc Anterior: 0111101101

Nonce: 2

Ha de començar per 0



Prova de Treball: Minatge

- Procés per construir un bloc vàlid
 1. Comprovar que la dada i la signatura digital coincideixen
 2. Agrupar les dades validades en un bloc
 3. Calcular el Nonce que permet obtenir un Hash amb les característiques demanades
- Els nodes que duen a terme aquesta tasca s'anomenen miners
- El miner rep una recompensa per cada bloc vàlid que construeix

Hash: 0000110100

Dada 1

Dada 2

Hash Bloc Anterior: 0111101101

Nonce: 2

Ha de començar per 0



Prova de Treball: Minatge

- Procés per construir un bloc vàlid
 1. Comprovar que la dada i la signatura digital coincideixen
 2. Agrupar les dades validades en un bloc
 3. Calcular el Nonce que permet obtenir un Hash amb les característiques demanades
- Els nodes que duen a terme aquesta tasca s'anomenen miners
- El miner rep una recompensa per cada bloc vàlid que construeix

Hash: 0000110100

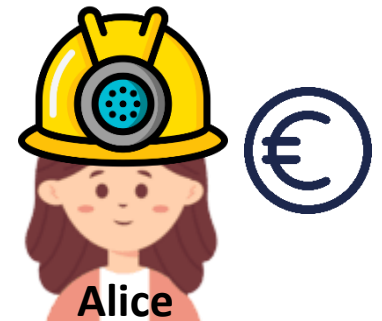
Dada 1

Dada 2

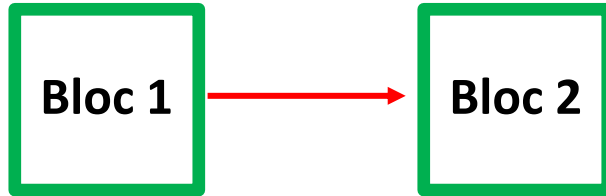
Hash Bloc Anterior: 0111101101

Nonce: 2

Ha de començar per 0

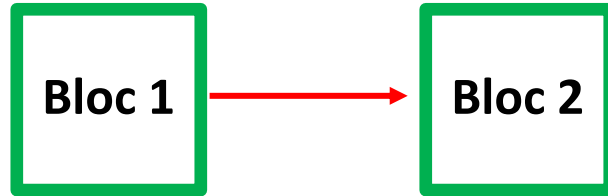


Prova de Treball: Competició



Prova de Treball: Competició

- Els miners competeixen per construir el següent bloc
- Si dos blocs es construeixen a la vegada es duplica la cadena
- Els nodes es queden amb la cadena més llarga



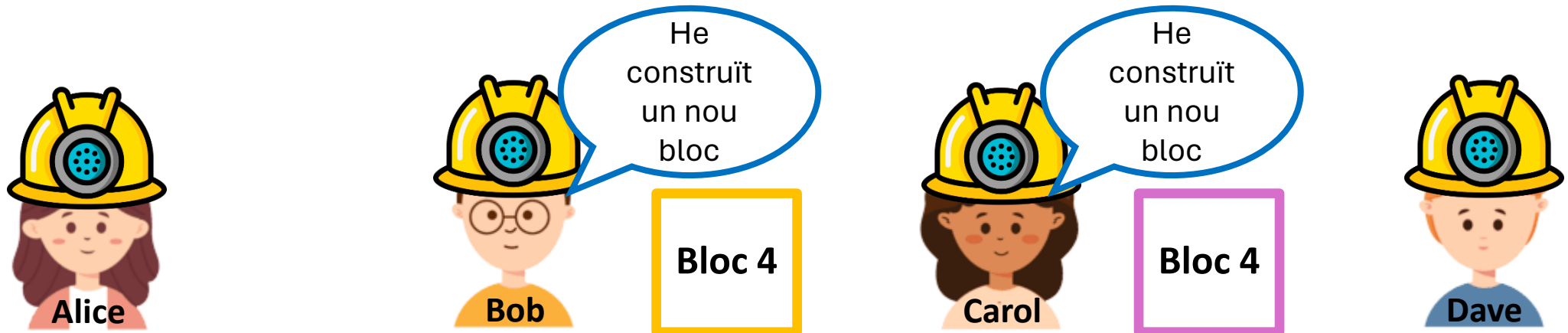
Prova de Treball: Competició

- Els miners competeixen per construir el següent bloc
- Si dos blocs es construeixen a la vegada es duplica la cadena
- Els nodes es queden amb la cadena més llarga



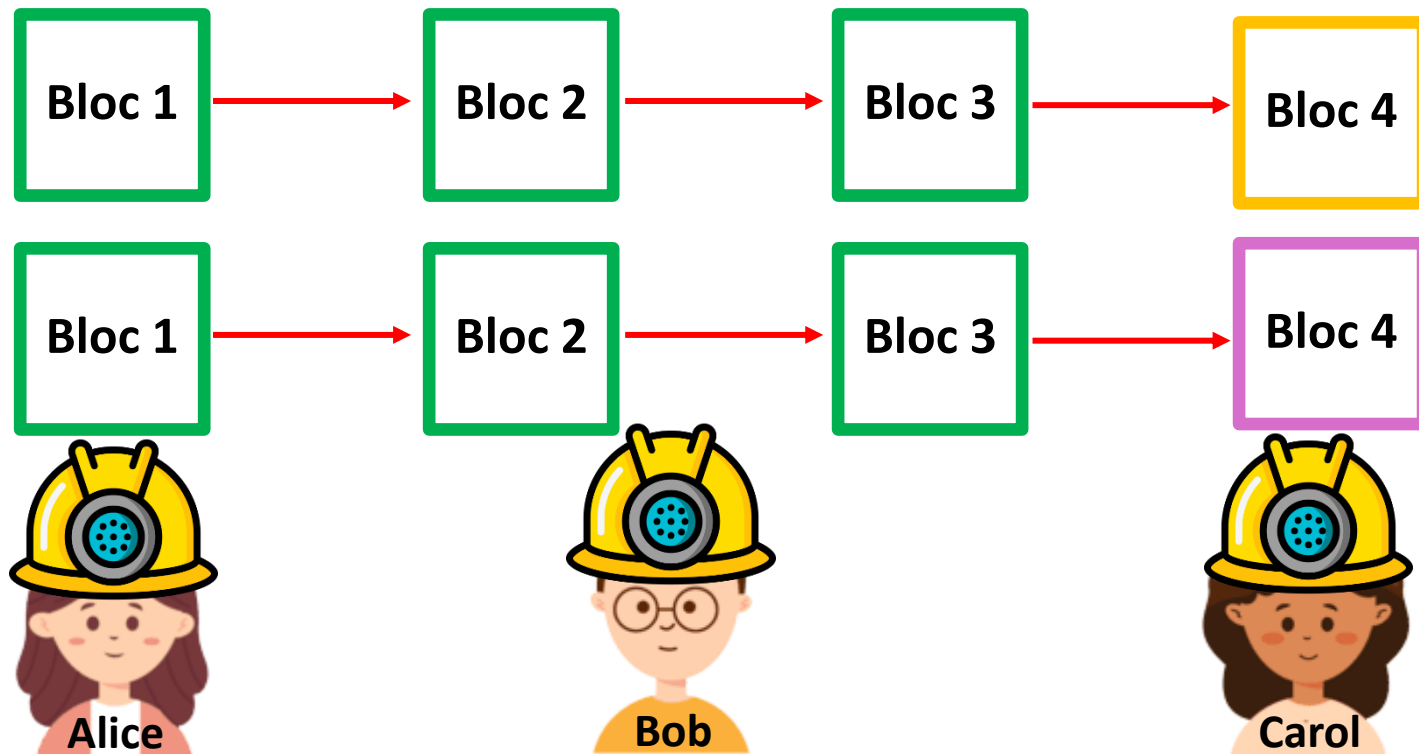
Prova de Treball: Competició

- Els miners competeixen per construir el següent bloc
- Si dos blocs es construeixen a la vegada es duplica la cadena
- Els nodes es queden amb la cadena més llarga



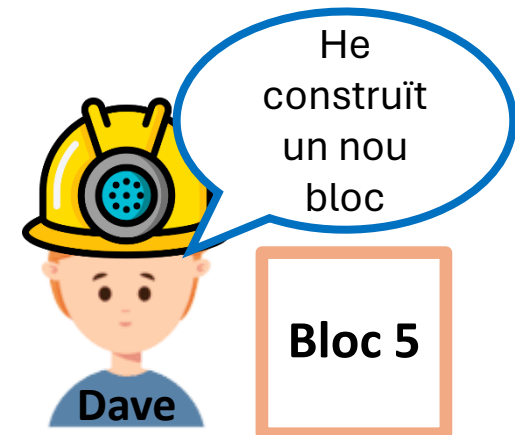
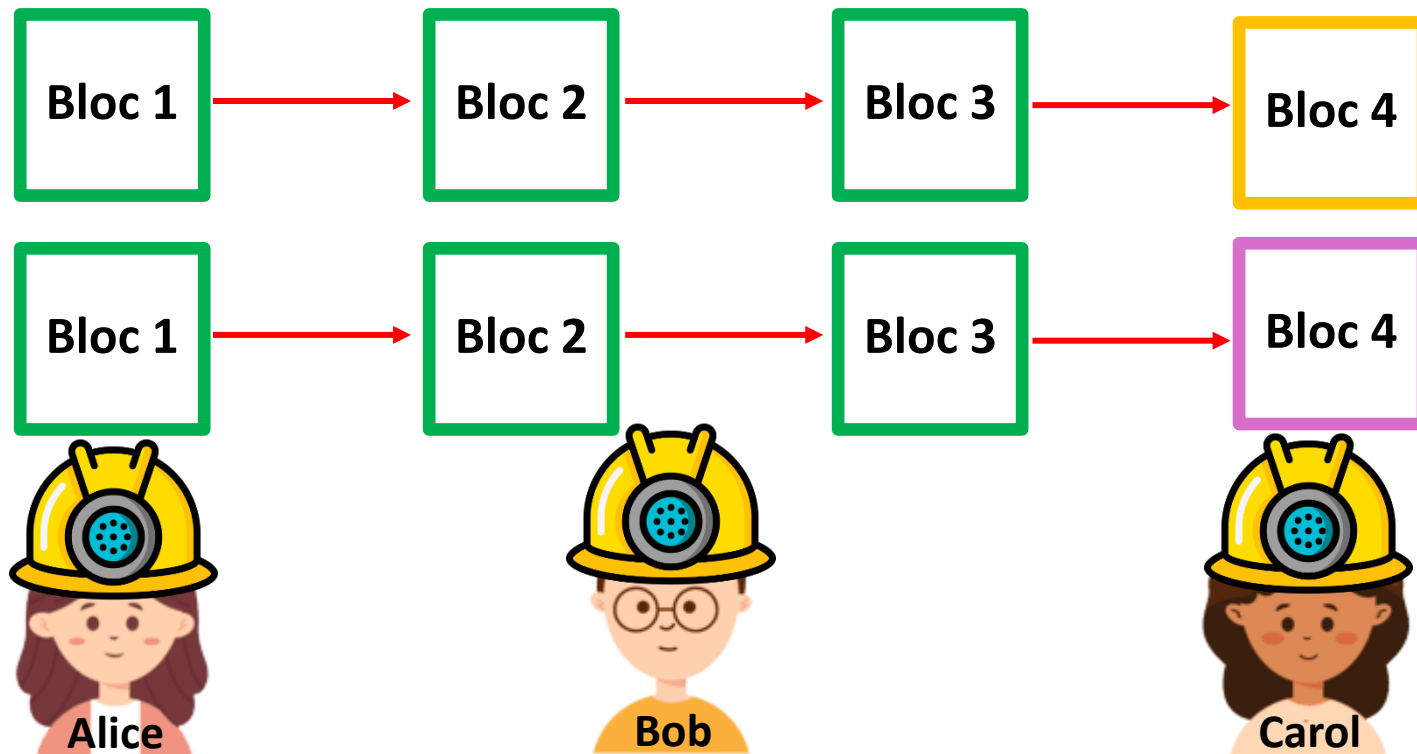
Prova de Treball: Competició

- Els miners competeixen per construir el següent bloc
- Si dos blocs es construeixen a la vegada es duplica la cadena
- Els nodes es queden amb la cadena més llarga



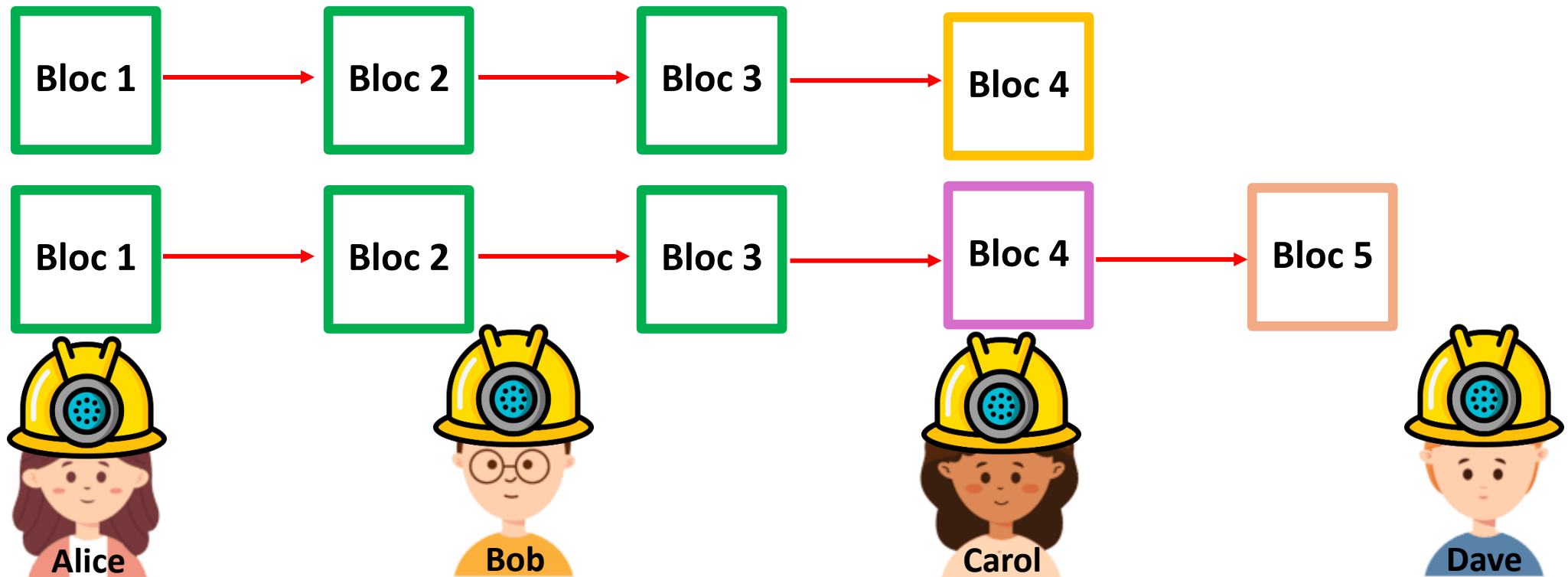
Prova de Treball: Competició

- Els miners competeixen per construir el següent bloc
- Si dos blocs es construeixen a la vegada es duplica la cadena
- Els nodes es queden amb la cadena més llarga



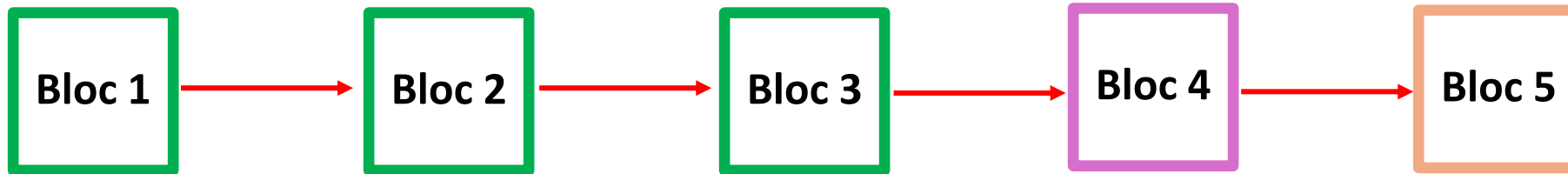
Prova de Treball: Competició

- Els miners competeixen per construir el següent bloc
- Si dos blocs es construeixen a la vegada es duplica la cadena
- Els nodes es queden amb la cadena més llarga



Prova de Treball: Competició

- Els miners competeixen per construir el següent bloc
- Si dos blocs es construeixen a la vegada es duplica la cadena
- Els nodes es queden amb la cadena més llarga



Seguretat



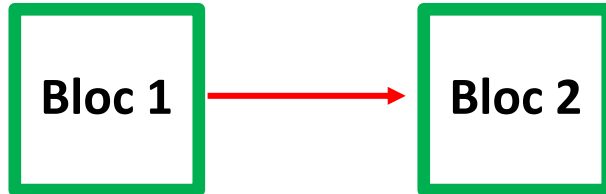
Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



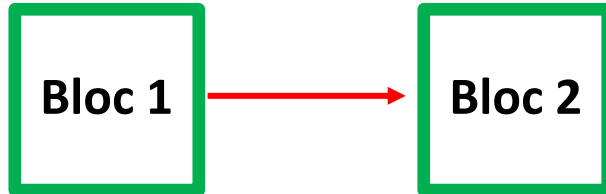
Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



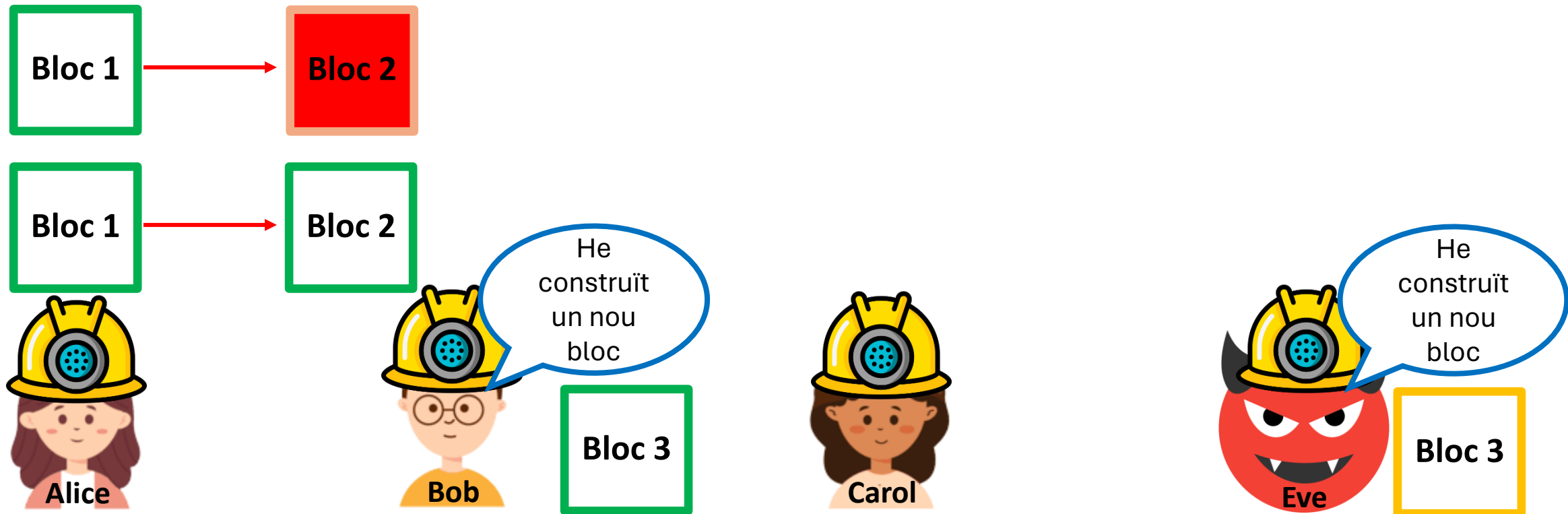
Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



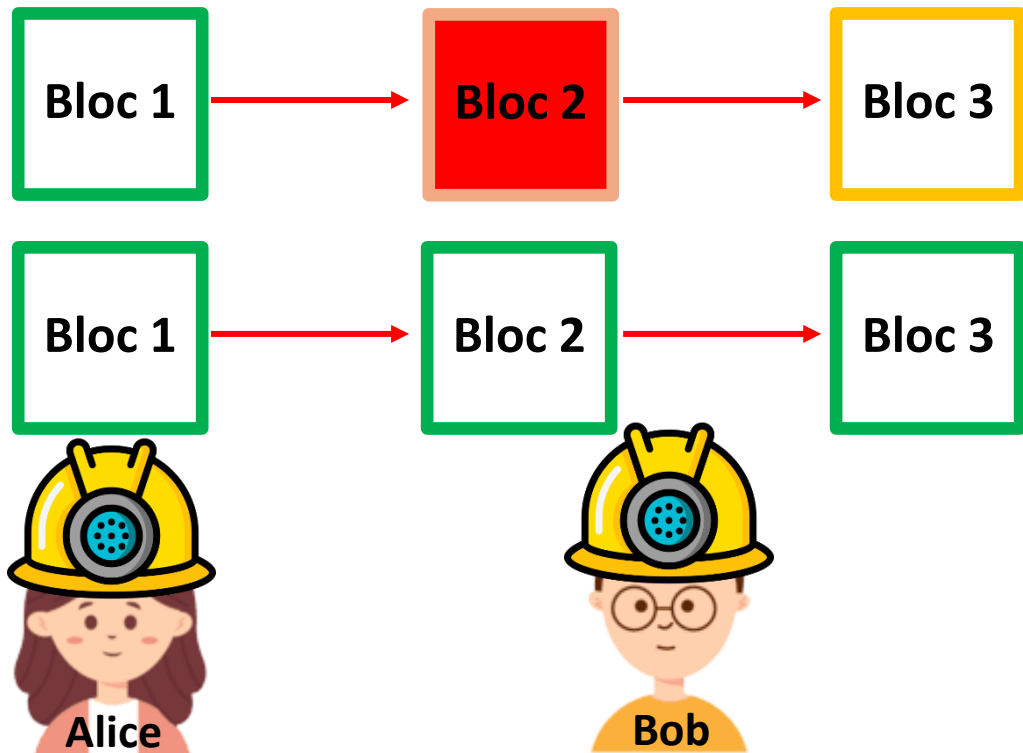
Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



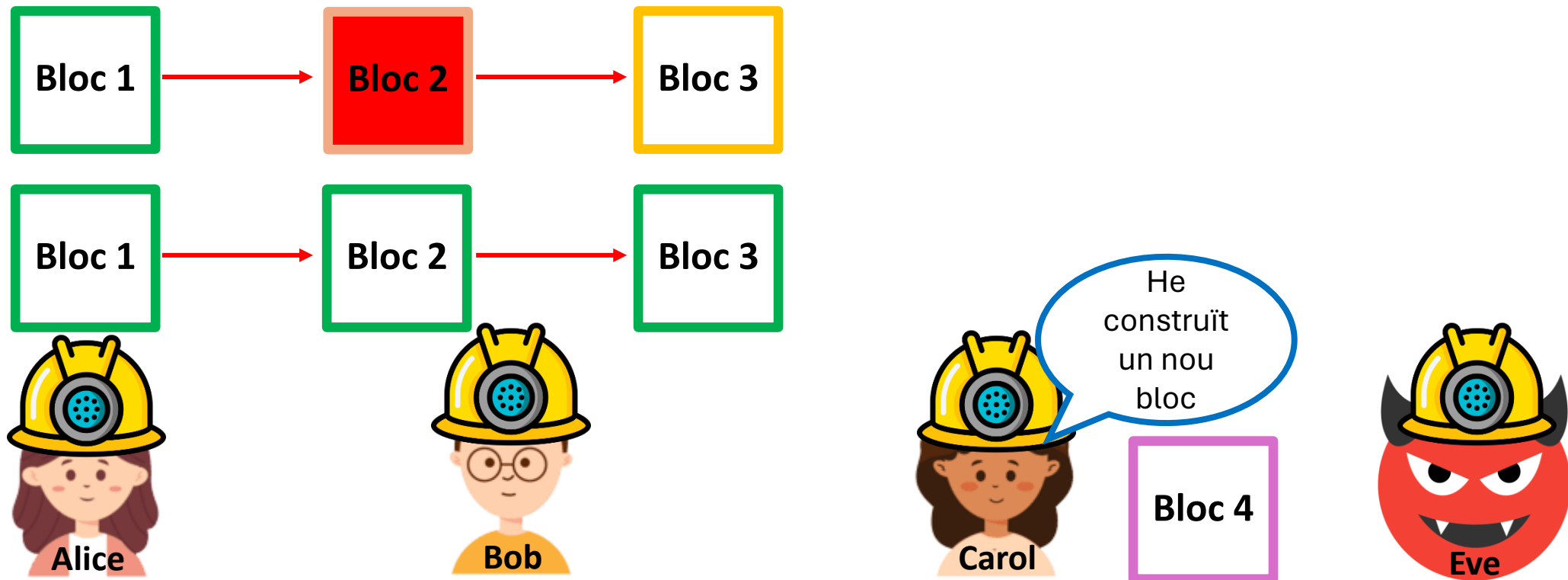
Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



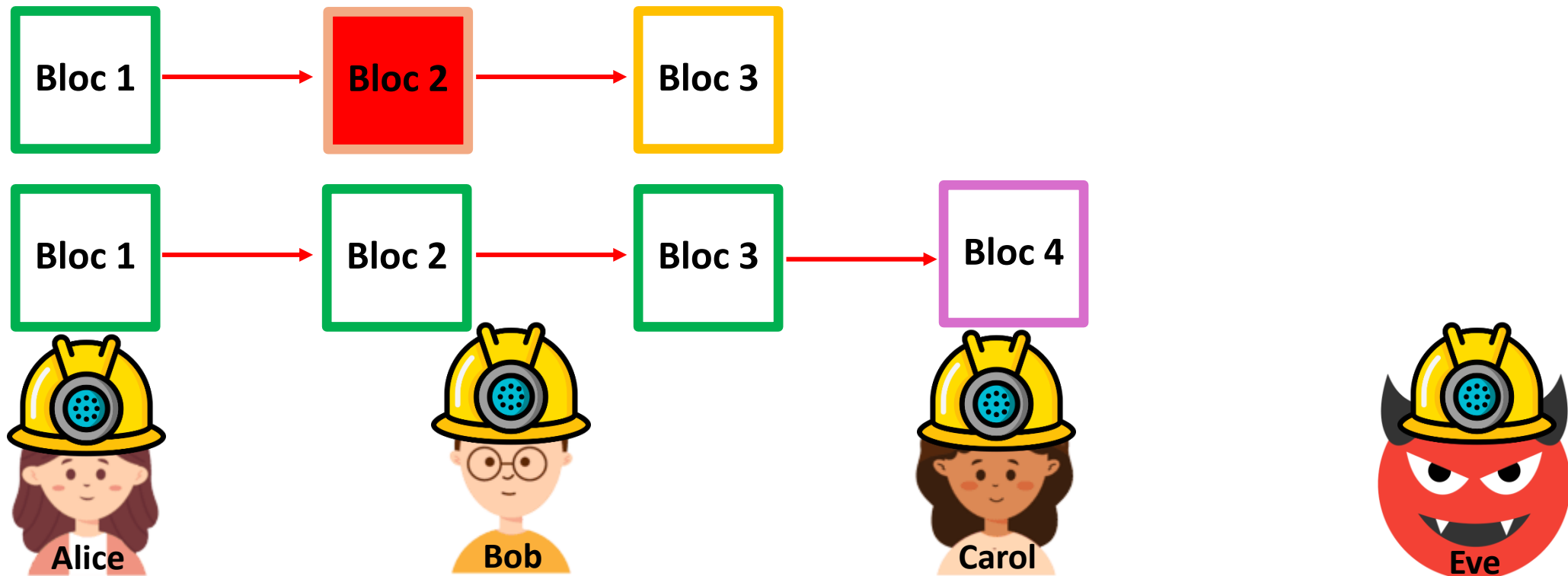
Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



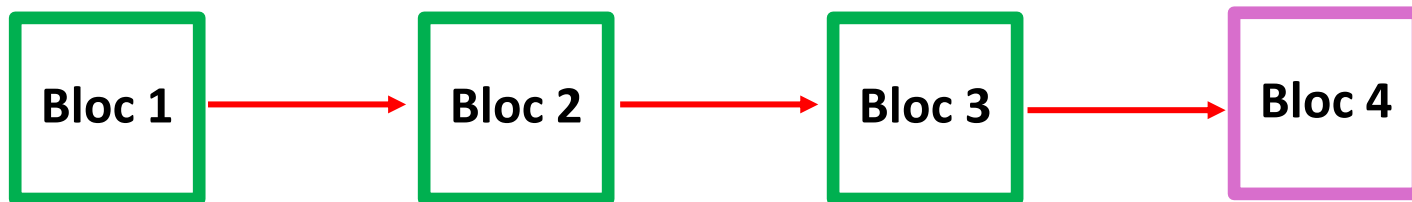
Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



Seguretat

- Les firmes digitals permeten validar les dades dels blocs
- Els blocs generats són immutables
 - Un node malèvol hauria de minar tot sol més blocs que la resta de miners



Tecnologia Blockchain: Definició

Registre distribuït que conté llistes creixents de blocs enllaçats de manera segura mitjançant hashes criptogràfics

Tecnologia Blockchain: Definició

Registre distribuït que conté llistes creixents de blocs enllaçats de manera segura mitjançant hashes criptogràfics

Tecnologia Blockchain: Definició

***Registre distribuït** que conté **llistes creixents de blocs enllaçats** de manera segura mitjançant
hashs criptogràfics*

Tecnologia Blockchain: Definició

Registre distribuït** que conté **llistes creixents de blocs enllaçats** de **manera segura** mitjançant **hashs criptogràfics

Tecnologia Blockchain: Definició

Registre distribuït que conté *llistes creixents de blocs enllaçats* de *manera segura* mitjançant *hashs criptogràfics*

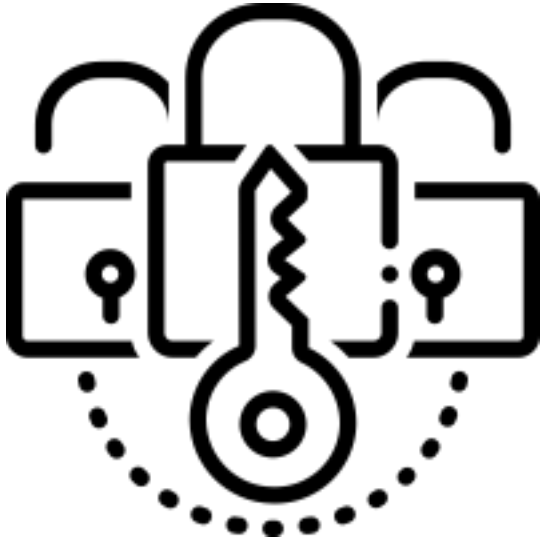
The image features a person in a grey suit standing on a dark, rocky cliff, looking out over a city skyline at dusk or dawn. The sky is a mix of blue and orange. Overlaid on the top half of the image is a complex network diagram with blue dots connected by thin lines. A white rectangular box with a blue border is centered in the middle of the image, containing the text 'Blockchain i Societat' in bold black font.

Blockchain i Societat

Avantatges

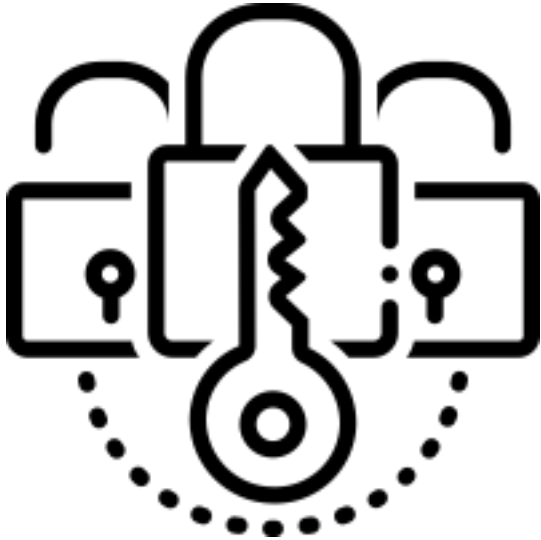
Avantatges

Immutabilitat



Avantatges

Immutabilitat

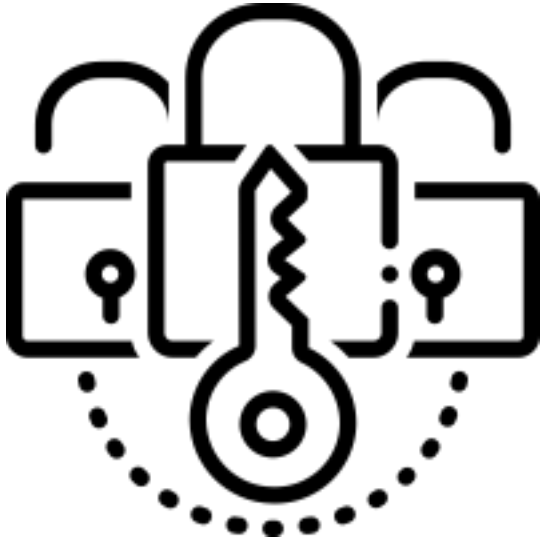


Transparència



Avantatges

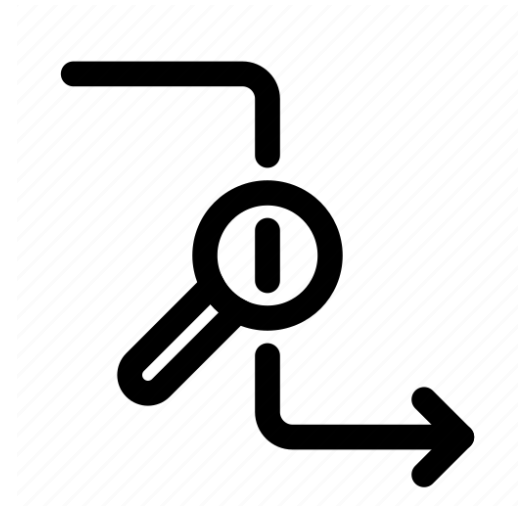
Immutabilitat



Transparència



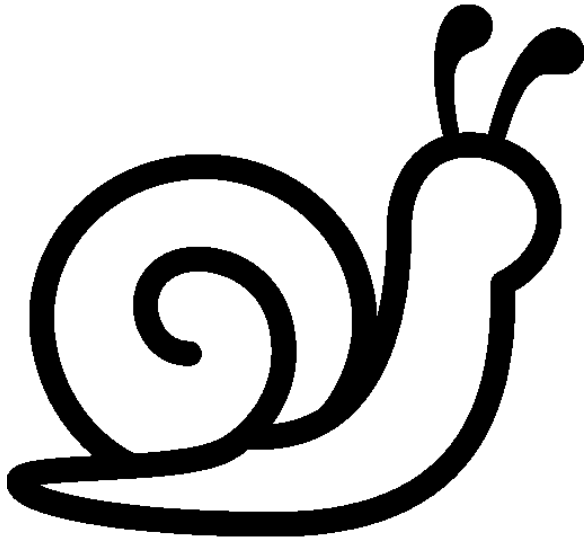
Traçabilitat



Inconvenients

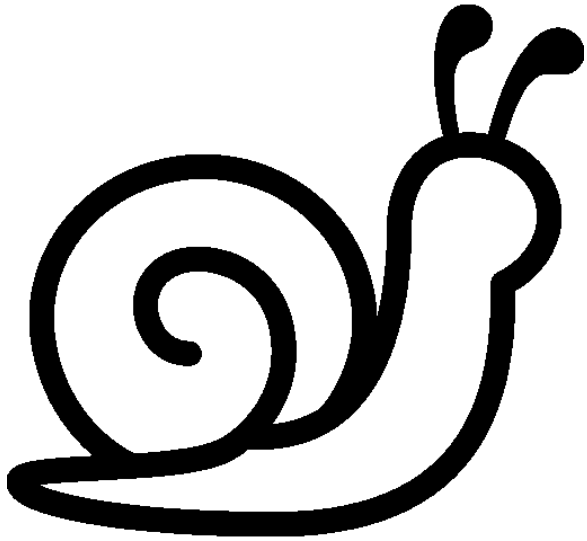
Inconvenients

Lentitud



Inconvenients

Lentitud

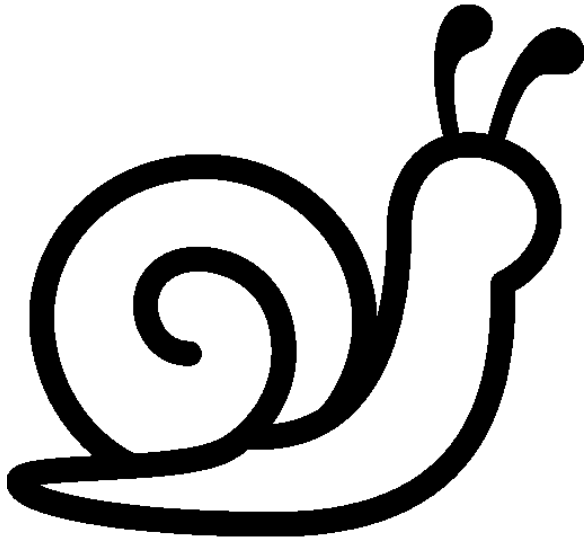


Rigidesa



Inconvenients

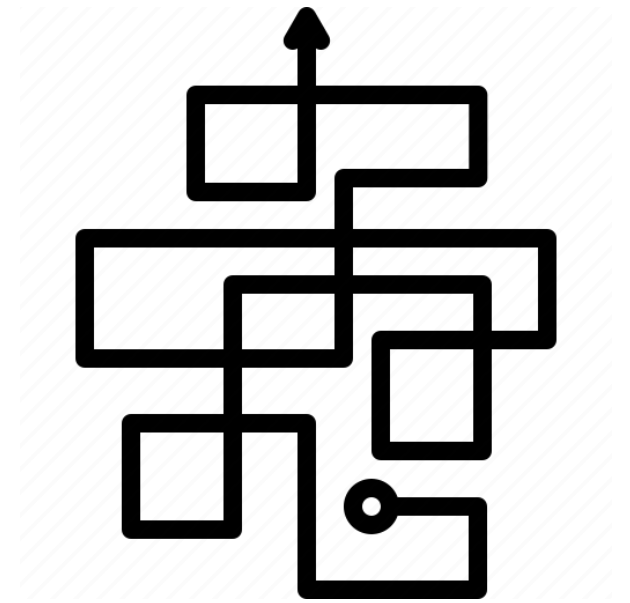
Lentitud

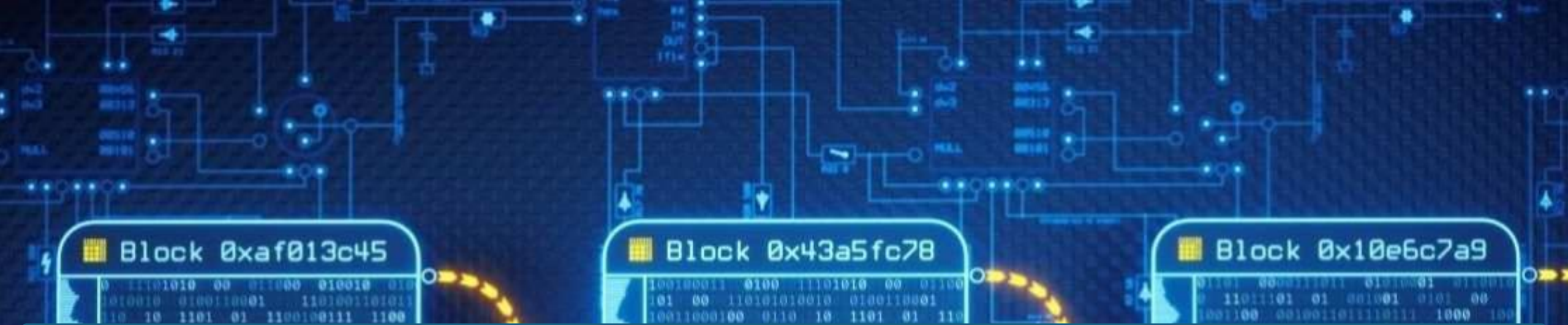


Rigidesa

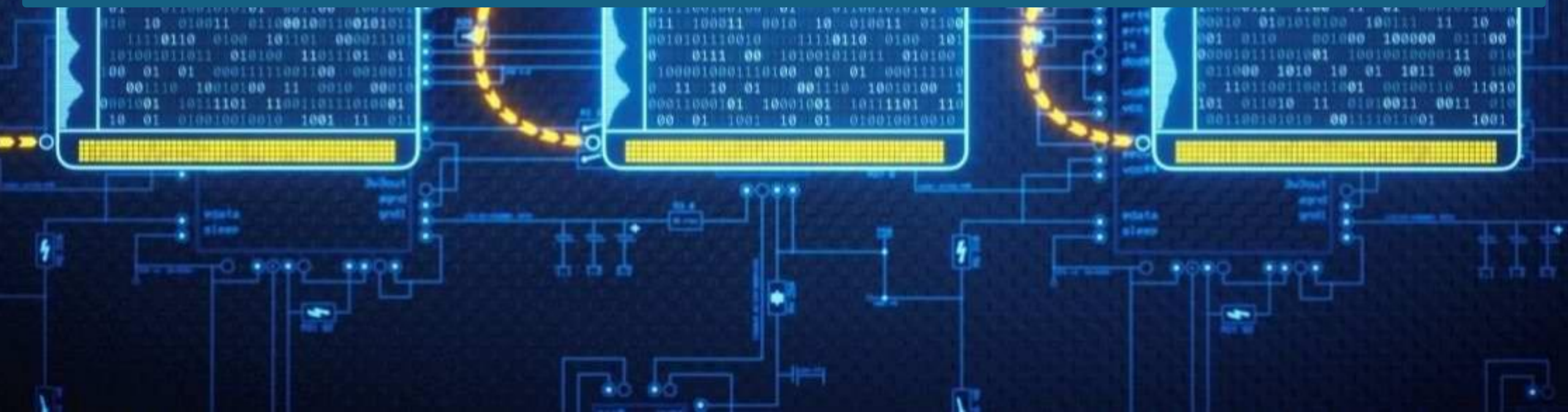


Complexitat





Però tot això, per a què serveix?



Aplicació: Criptomonedes

Moneda digital que funciona mitjançant una xarxa informàtica que no depèn de cap autoritat central.

Aplicació: Criptomonedes

Moneda digital que funciona mitjançant una xarxa informàtica que no depèn de cap autoritat central.

Registre de despeses d'un grup d'amics

Bob paga 10€ a **Alice**
Dave paga 25€ a **Carol**
Carol paga 5€ a **Bob**
Alice paga 20€ a **Dave**

Dave paga 55€ a **Bob**
Alice paga 60€ a **Dave**
Bob paga 75€ a **Carol**
Carol paga 80€ a **Alice**

Aplicació: Criptomonedes

Moneda digital que funciona mitjançant una xarxa informàtica que no depèn de cap autoritat central.

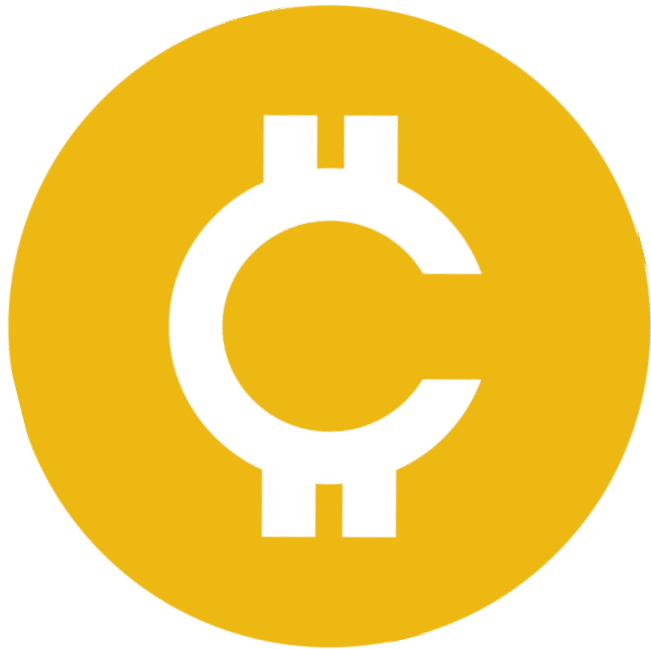
Registre de despeses mundial

Bob paga 10🪙 a **Alice**
Dave paga 25🪙 a **Carol**
Carol paga 5🪙 a **Bob**
Alice paga 20🪙 a **Dave**

Dave paga 55🪙 a **Bob**
Alice paga 60🪙 a **Dave**
Bob paga 75🪙 a **Carol**
Carol paga 80🪙 a **Alice**

Aplicació: Criptomonedes

Moneda digital que funciona mitjançant una xarxa informàtica que no depèn de cap autoritat central.



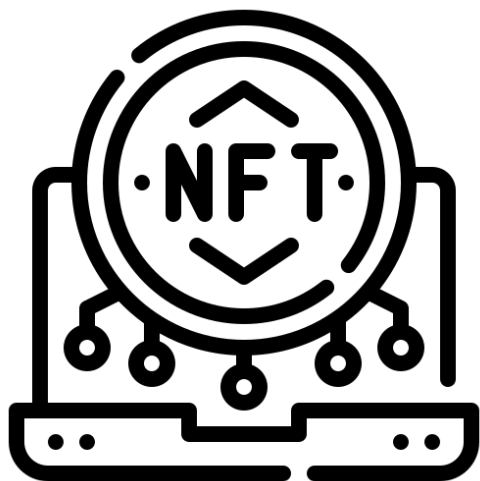
=



Aplicació: Altres

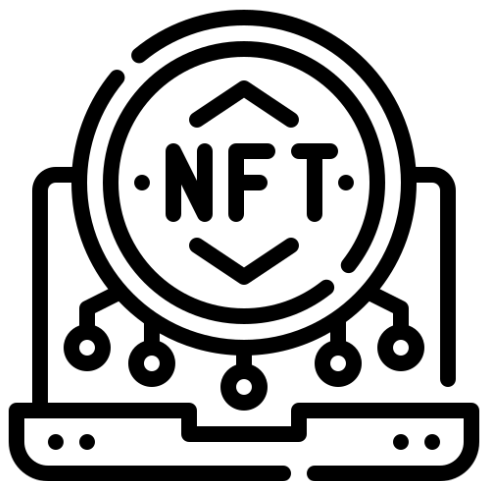
Aplicació: Altres

NFT

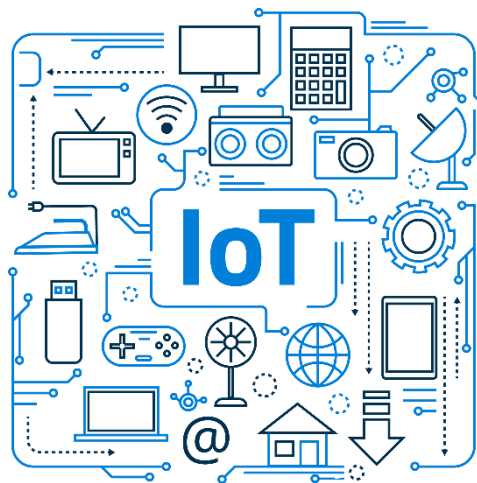


Aplicació: Altres

NFT

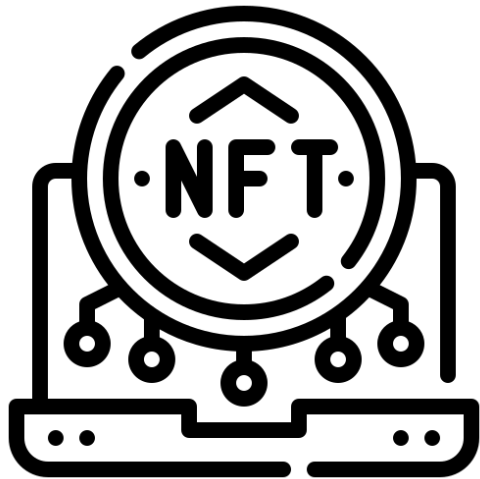


IoT

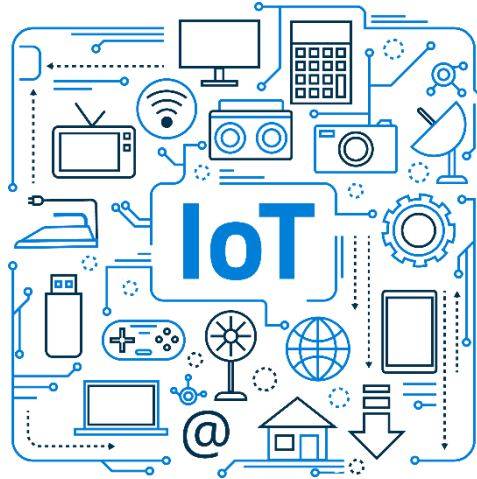


Aplicació: Altres

NFT



IoT



Smart contracts



Perills: Especulació



Hazte Millonario con CRYPTO - LLADOS

27 k visualitzacions • fa 2 anys



TU1MILLON ✓

Asiste a mi clase GRATUITA - Como fui de lavaplatos a MILL
Curso Nutrición ...

Perills: Especulació

CRIPTOMONEDES >

E El cervell de la plataforma de criptodivises FTX, condemnat a 25 anys de presó per frau

Els fiscals havien demanat entre 40 i 50 anys per a Sam Bankman-Fried per dirigir la firma “com qui juga al Monopoly”

Perills: Especulació

CRIPTOMONEDES >

E El cervell de la plataforma de criptodiviseses FTX, condemnat a 25 anys de presó per frau

Els fiscals havien demanat entre 40 i 50 anys per a Sam Bankman-Fried per dirigir la firma “com qui juga al Monopoly”

Front del Banc d'Espanya i la CNMV per "l'alt risc de frau" de les criptomonedes

Tots dos organismes adverteixen en un comunicat sobre l'ús de les divises per finançar empreses

Perills: Consum energètic

Extreure bitcoin contamina més que la ramaderia mundial de boví i gasta més electricitat anual que Àustria o Portugal

Les emissions de CO2 imputables a la xarxa d'ordinadors que busquen i obtenen aquesta criptomoneda s'han multiplicat per 126 entre el 2016 i el 2021, segons un estudi de la revista 'Nature'

Perills: Consum energètic

MEDI AMBIENT

La pujada del preu de Bitcoin es 'beu' l'aigua del planeta: una piscina per cada transacció

Els ordinadors de la mineria necessiten 1.600 gegalitres d'aigua a l'any per verificar les transaccions: "Si el seguim utilitzant per fer càlculs inútils, la realitat serà dolorosa"

Perills: Consum energètic

Rank	Country and Region	Population (Millions) [26]	Energy (TWh)[23, 27, 28, 29]]	Share (%)
0	World	7,878.2	23,398.00	100.00
1	China	1,444.9	7,500.00	32.05
2	U.S.A	332.9	3,989.60	17.05
3	India	1,366.4	1,547.00	6.61
20	Taiwan	23.8	237.55	1.01
21	Vietnam	98.2	216.99	0.92
22	South Africa	60.1	210.30	0.89
23	Bitcoin + Ethereum	N.A.	190.13	0.81
24	Thailand	69.9	185.85	0.79
25	Poland	37.80	153.00	0.65
26	Egypt	104.3	150.57	0.64
27	Malaysia	3.1	147.21	0.62
28	Bitcoin	N.A.	135.12	0.57
29	Sweden	10.2	131.79	0.56
49	Switzerland	8.7	56.35	0.24
50	Ethereum	N.A.	55.01	0.24
51	Romania	19.1	55.00	0.23

Gràcies per la vostra atenció

Alguna pregunta?

