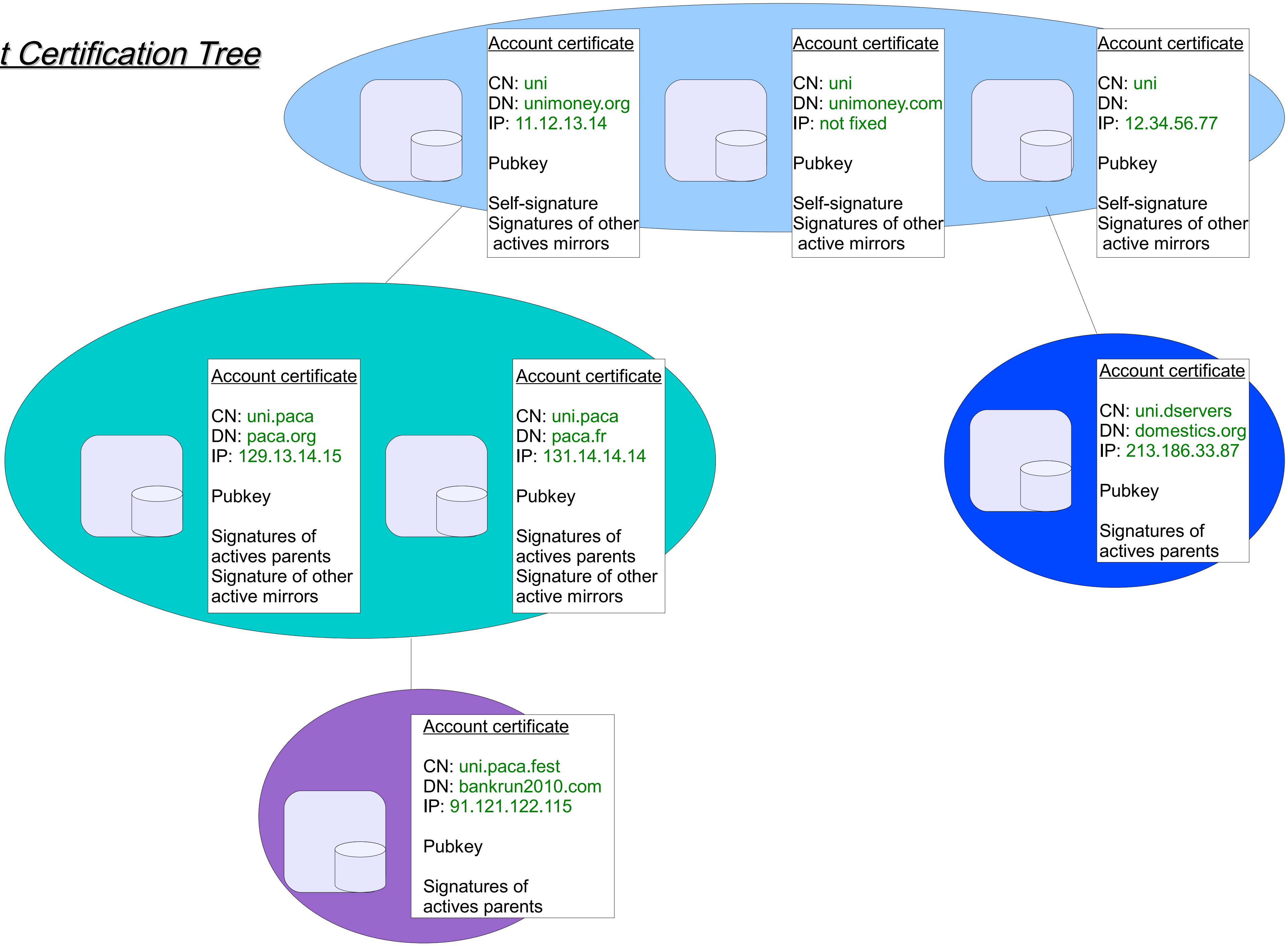
Account Certification Tree



Account certificate

CN: uni
DN: unimoney.org
IP: 11.12.13.14

Pubkey

Self-signature
Signatures of other
actives mirrors

Account certificate

CN: uni
DN: unimoney.com
IP: not fixed

Pubkey

Self-signature
Signatures of other
active mirrors

Account certificate

CN: uni
DN:
IP: 12.34.56.77

Pubkey

Self-signature
Signatures of other
active mirrors

Account certificate

CN: uni.paca
DN: paca.org
IP: 129.13.14.15

Pubkey

Signatures of
actives parents
Signature of other
active mirrors

Account certificate

CN: uni.paca
DN: paca.fr
IP: 131.14.14.14

Pubkey

Signatures of
actives parents
Signature of other
active mirrors

Account certificate

CN: uni.dservers
DN: domestics.org
IP: 213.186.33.87

Pubkey

Signatures of
actives parents

Account certificate

CN: uni.paca.fest
DN: bankrun2010.com
IP: 91.121.122.115

Pubkey

Signatures of
actives parents

What is a unit of money ?

Unit of money are :

- currency name (unlimited string, '\0' ended)
- version number (1 byte, indicate the format of next informations and the bill rules)
- amount of currency value
- serial number
- creation date

And a chain of digital signature (like bitcoin) :

- pubkey of the first owner of this unit money. (→ 512 bits RSA in version 0)
- transaction date
- signature by the (democratic and) know-by-every-body money creator. (the creator should use a stronger key → RSA 2048 bits or an EC algorithm)

So each unit of money grow bigger at each transaction (~ 64 + 4 +16 = 84 bytes).

After a minimal amount of transactions (~ 1000) the digital signature can be reseted by a (honest and) know-by-every-body money re-creator.

If a unit of money come back to one of its previous owner it's length can also be shortcut if he recognize one of the pubkey and still have the private key associated.

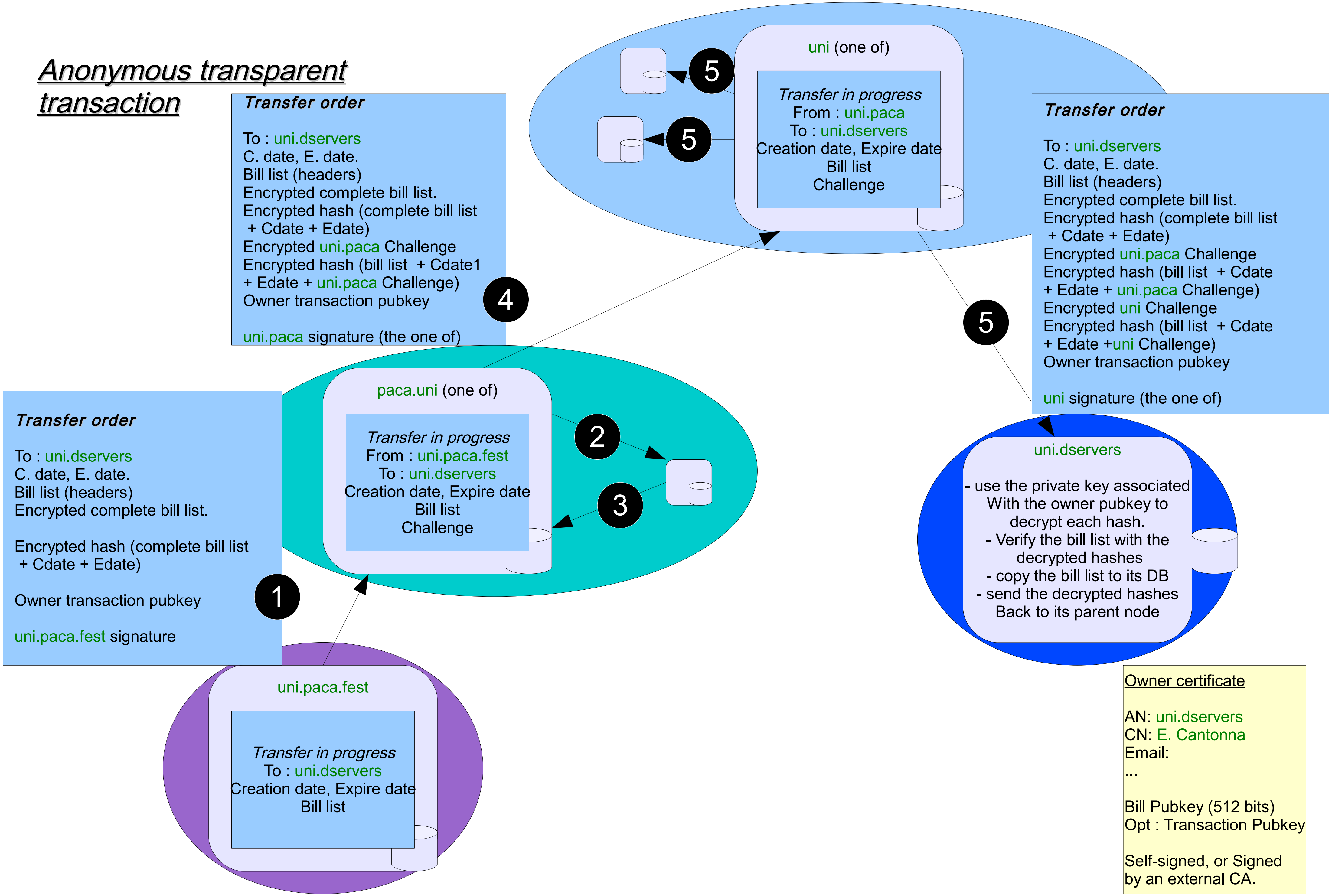
Who has the money ?

The one who has the private key of the last pubkey in the chain of digital signature.

Where is the money ?

Ask that to the certified account tree.

Anonymous transparent transaction



Transfer order

To : uni.dservers
C. date, E. date.
Bill list (headers)
Encrypted complete bill list.

Encrypted hash (complete bill list
+ Cdate + Edate)

Owner transaction pubkey

uni.paca.fest signature

uni.paca.fest

Transfer in progress
To : uni.dservers
Creation date, Expire date
Bill list

paca.uni (one of)

Transfer in progress
From : uni.paca.fest
To : uni.dservers
Creation date, Expire date
Bill list
Challenge

Transfer order

To : uni.dservers
C. date, E. date.
Bill list (headers)
Encrypted complete bill list.
Encrypted hash (complete bill list
+ Cdate + Edate)
Encrypted uni.paca Challenge
Encrypted hash (bill list + Cdate1
+ Edate + uni.paca Challenge)
Owner transaction pubkey

uni.paca signature (the one of)

uni (one of)

Transfer in progress
From : uni.paca
To : uni.dservers
Creation date, Expire date
Bill list
Challenge

Transfer order

To : uni.dservers
C. date, E. date.
Bill list (headers)
Encrypted complete bill list.
Encrypted hash (complete bill list
+ Cdate + Edate)
Encrypted uni.paca Challenge
Encrypted hash (bill list + Cdate
+ Edate + uni.paca Challenge)
Encrypted uni Challenge
Encrypted hash (bill list + Cdate
+ Edate +uni Challenge)
Owner transaction pubkey

uni signature (the one of)

uni.dservers

- use the private key associated
With the owner pubkey to
decrypt each hash.
- Verify the bill list with the
decrypted hashes
- copy the bill list to its DB
- send the decrypted hashes
Back to its parent node

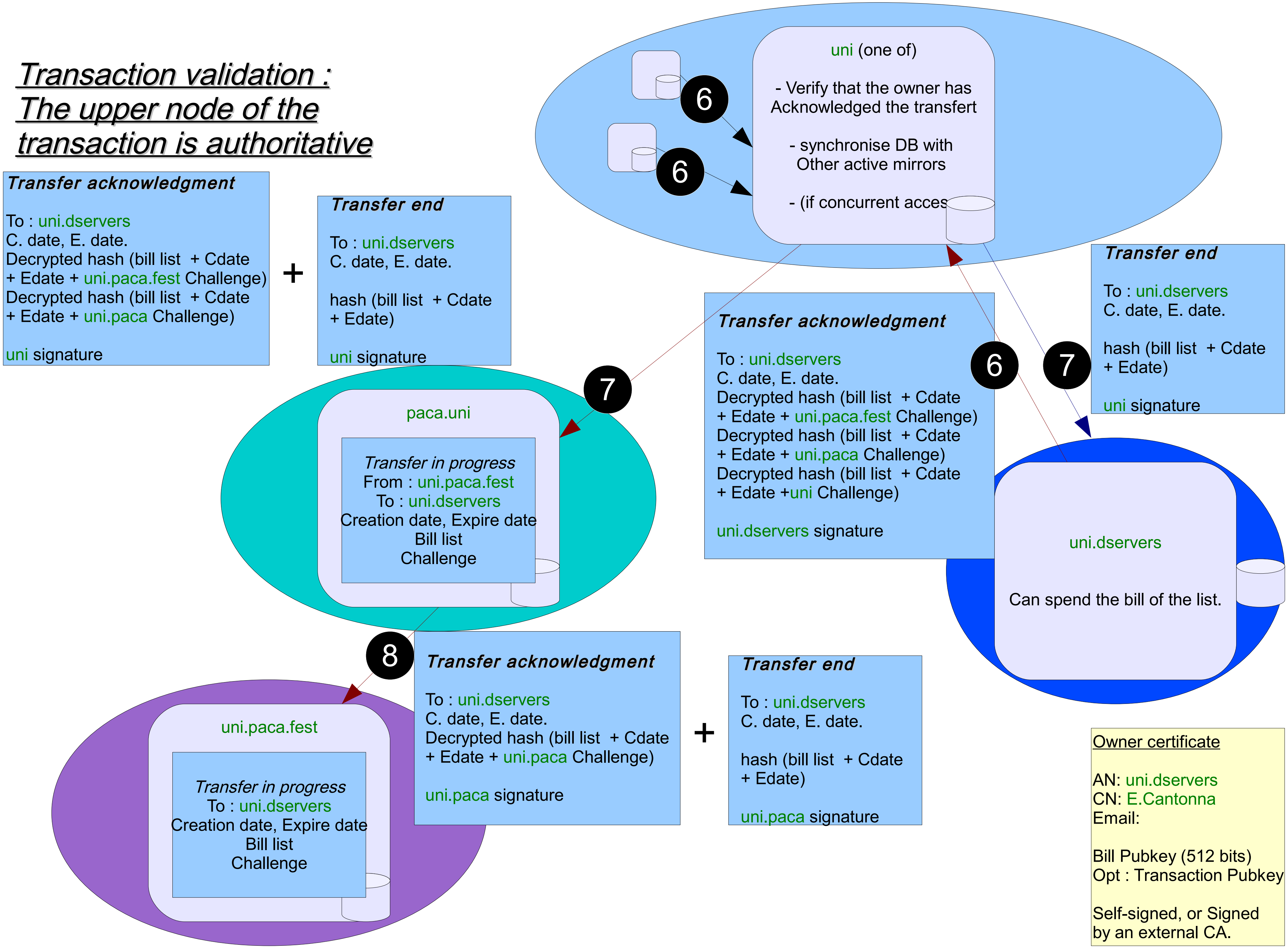
Owner certificate

AN: uni.dservers
CN: E. Cantonna
Email:
...

Bill Pubkey (512 bits)
Opt : Transaction Pubkey

Self-signed, or Signed
by an external CA.

Transaction validation : The upper node of the transaction is authoritative



Transfer acknowledgment

To : uni.dservers
C. date, E. date.
Decrypted hash (bill list + Cdate + Edate + uni.paca.fest Challenge)
Decrypted hash (bill list + Cdate + Edate + uni.paca Challenge)

uni signature

+

Transfer end

To : uni.dservers
C. date, E. date.

hash (bill list + Cdate + Edate)

uni signature

uni (one of)

- Verify that the owner has Acknowledged the transfert
- synchronise DB with Other active mirrors
- (if concurrent acces

Transfer end

To : uni.dservers
C. date, E. date.

hash (bill list + Cdate + Edate)

uni signature

Transfer acknowledgment

To : uni.dservers
C. date, E. date.
Decrypted hash (bill list + Cdate + Edate + uni.paca.fest Challenge)
Decrypted hash (bill list + Cdate + Edate + uni.paca Challenge)
Decrypted hash (bill list + Cdate + Edate +uni Challenge)

uni.dservers signature

paca.uni

Transfer in progress
From : uni.paca.fest
To : uni.dservers
Creation date, Expire date
Bill list
Challenge

uni.dservers

Can spend the bill of the list.

Transfer acknowledgment

To : uni.dservers
C. date, E. date.
Decrypted hash (bill list + Cdate + Edate + uni.paca Challenge)

uni.paca signature

+

Transfer end

To : uni.dservers
C. date, E. date.

hash (bill list + Cdate + Edate)

uni.paca signature

uni.paca.fest

Transfer in progress
To : uni.dservers
Creation date, Expire date
Bill list
Challenge

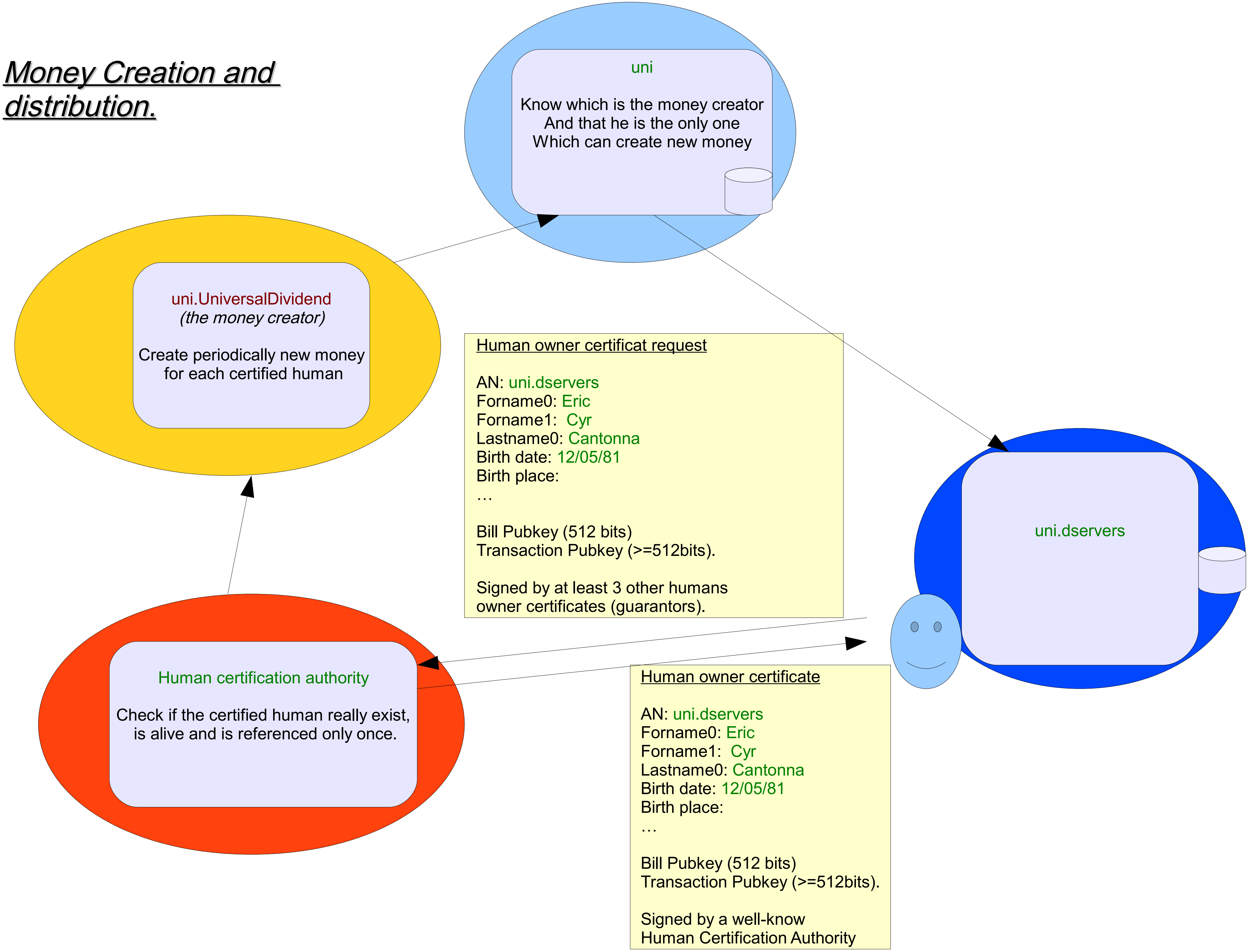
Owner certificate

AN: uni.dservers
CN: E.Cantonna
Email:

Bill Pubkey (512 bits)
Opt : Transaction Pubkey

Self-signed, or Signed by an external CA.

Money Creation and distribution.



uni

Know which is the money creator
And that he is the only one
Which can create new money

uni.UniversalDividend
(the money creator)

Create periodically new money
for each certified human

Human owner certificat request

AN: uni.dservers
Forname0: Eric
Forname1: Cyr
Lastname0: Cantonna
Birth date: 12/05/81
Birth place:
…

Bill Pubkey (512 bits)
Transaction Pubkey (>=512bits).

Signed by at least 3 other humans
owner certificates (guarantors).

uni.dservers

Human certification authority

Check if the certified human really exist,
is alive and is referenced only once.

Human owner certificate

AN: uni.dservers
Forname0: Eric
Forname1: Cyr
Lastname0: Cantonna
Birth date: 12/05/81
Birth place:
…

Bill Pubkey (512 bits)
Transaction Pubkey (>=512bits).

Signed by a well-know
Human Certification Authority

Avantages Recapitulation

- Money supply is know exactly and by every body, (M1=M2=M3) and nobody could cheat and create money (e.g. by lending money which doesn't exist).

- Node in the certification tree can't take bill's ownership. There only role is to be sure that money units are not double spended.

- Protect the anonymity : even if the account are all referenced and known by the tree account. The node in the tree may have no ideas about which are the owners of the money in an account.

- Universal Dividend change the way big companies will build themselves : instead of finding money to enslave people, they will have to found people first.

(...)