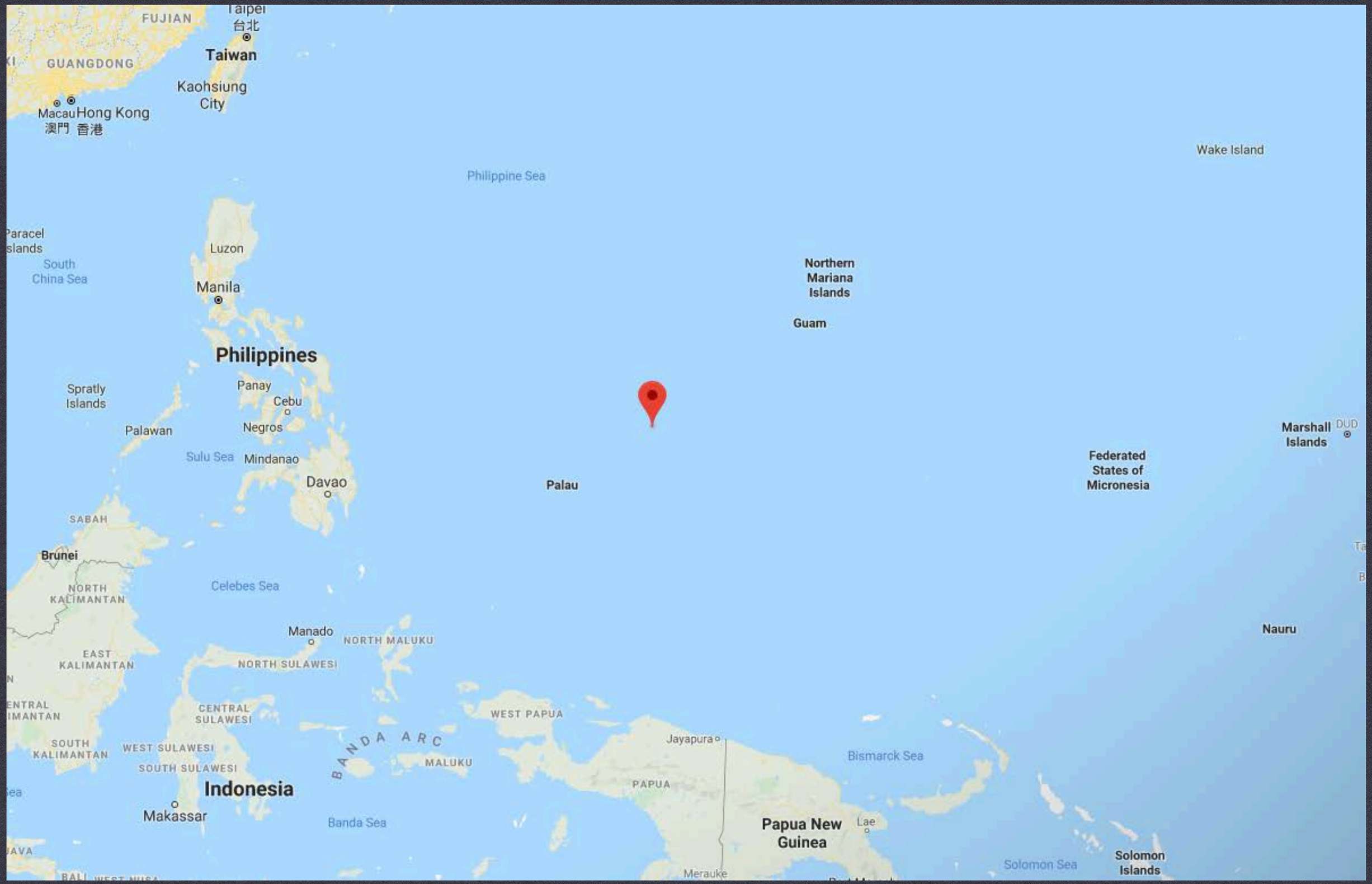
BLOCKCHAIN: THE GOLD OF NERDS

ALESSANDRO PANCONESI
DIPARTIMENTO DI INFORMATICA, SAPIENZA UNIVERSITÀ DI ROMA

CRYPTOCURRENCIES, WILL THEY CHANGE THE WORLD?



YAP

ISLAND OF STONE MONEY

YAP

ISLAND OF STONE MONEY

YAP

ISLAND OF STONE MONEY

MINTNG RAI STONES

ISLAND OF STONE MONEY

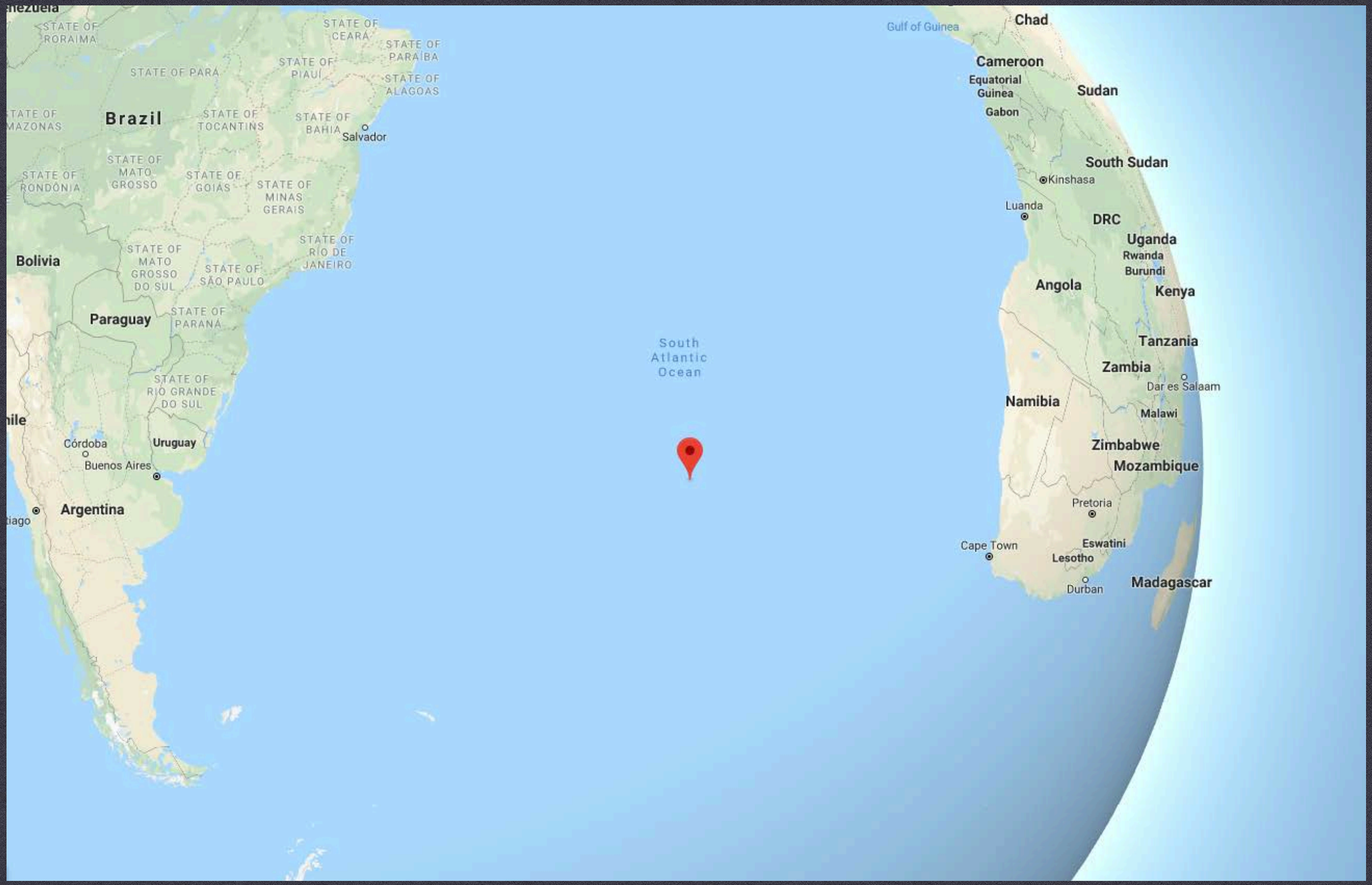
MONEY TRANSFER ON YAP

ISLAND OF STONE MONEY

TOWARD THE BLOCKCHAIN

TRISTAN DE CUNHA

REMOTEST ISLAND



TRISTAN DE CUNHA

REMOTEST ISLAND

TRISTAN DE CUNHA

REMOTEST ISLAND

TRISTAN DE CUNHA

THE REMOTEST ISLAND

TRISTAN DE CUNHA

REMOTEST ISLAND

TRISTAN DE CUNHA

THE REMOTEST ISLAND

The inhabitants of the most remote island install a blackboard in the main square…

Blackboard #1

A owns (1) (2) ... (10)

B owns (11) (12) ... (20)

C owns (21) (22) ... (30)

:

Z owns (251) (252) ... (260)

PUBLIC LEDGER

THE REMOTEST ISLAND

Properties of the blackboard

- Anybody can write
- Board is permanent: it cannot be erased or modified

Blackboard #1

A owns (1) (2) ... (10)

B owns (11) (12) ... (20)

C owns (21) (22) ... (30)

:

Z owns (251) (252) ... (260)

:

PUBLIC LEDGER

Blackboard #1

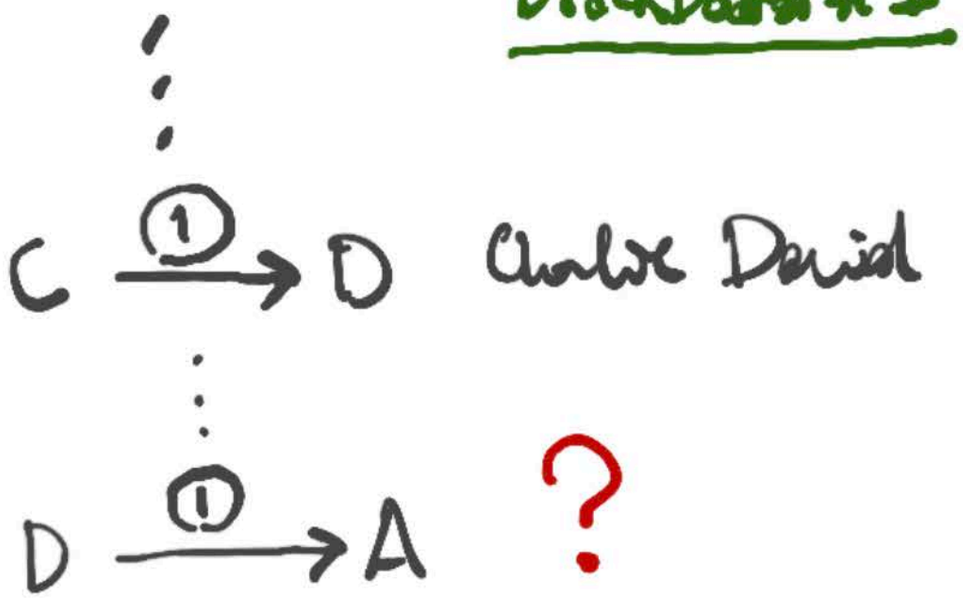
A owns (1) (2) ... (10)

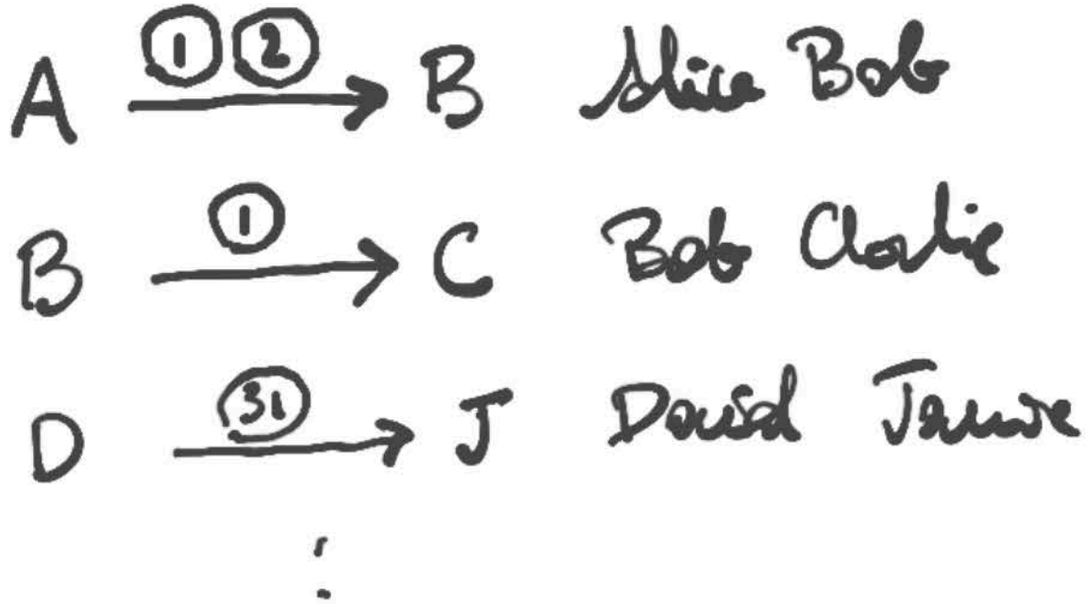
B owns (11) (12) ... (20)

C owns (21) (22) ... (30)

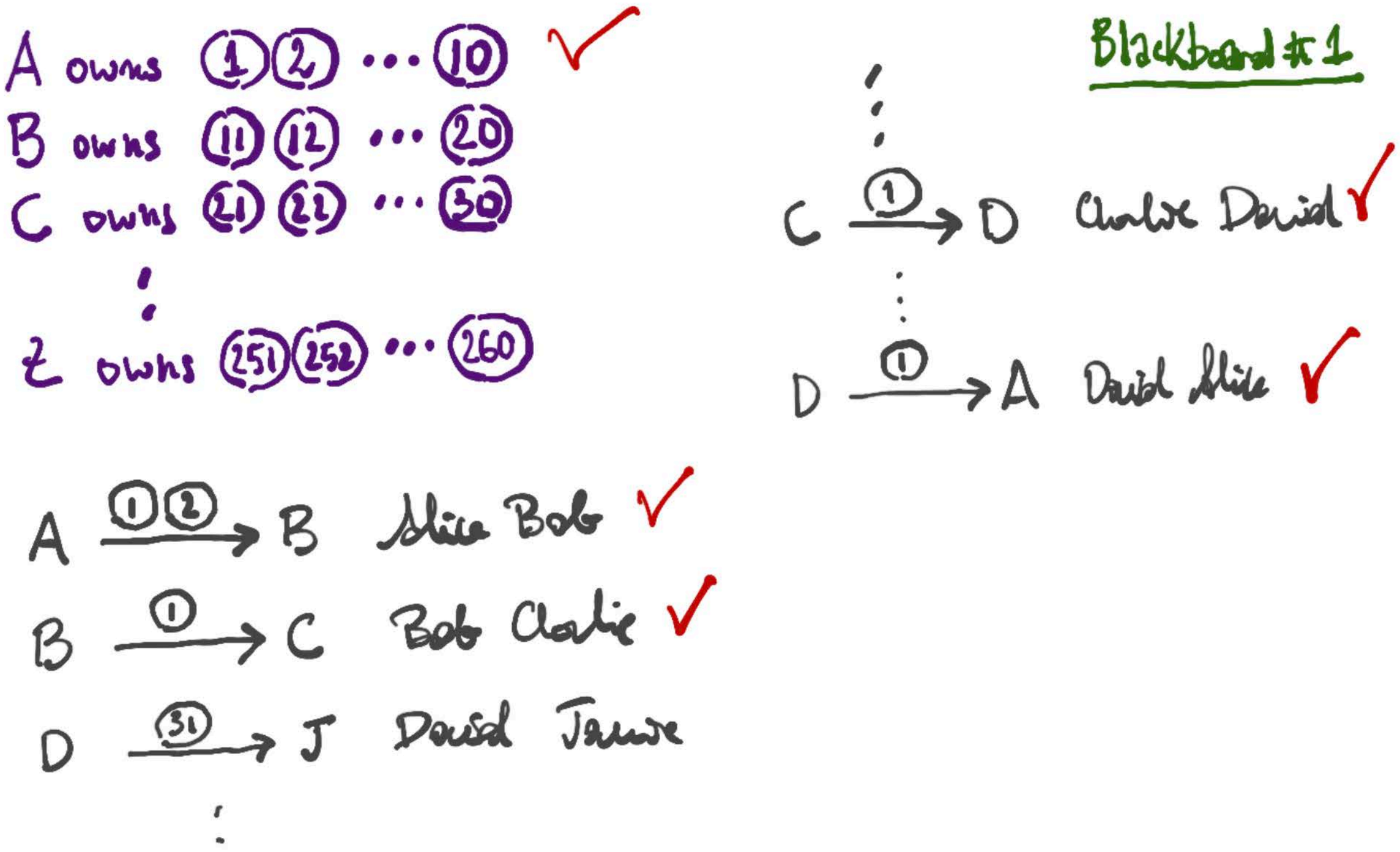
⋮

Z owns (251) (252) ... (260)





PUBLIC LEDGER



PUBLIC LEDGER

C owns new coins (261) ... (270)

Blackboard #2

PUBLIC LEDGER

C owns new coins (261) ... (270)

Blackboard #2

AND SO ON SO FORTH...

PUBLIC LEDGER

A owns 1 2 ··· 10
B owns 11 12 ··· 20
C owns 21 22 ··· 30
⋮
Z owns 251 252 ··· 260

C —1→ D
⋮
D —1→ A ?

A —1,2→ B Alice Bob
B —1→ C Bob Charlie
D —31→ J David Jamie
⋮

1

A owns 1 2 ··· 10
B owns 11 12 ··· 20
C owns 21 22 ··· 30
⋮
Z owns 251 252 ··· 260

C —1→ D
⋮
D —1→ A ?

A —1,2→ B Alice Bob
B —1→ C Bob Charlie
D —31→ J David Jamie
⋮

2

A owns 1 2 ··· 10
B owns 11 12 ··· 20
C owns 21 22 ··· 30
⋮
Z owns 251 252 ··· 260

C —1→ D
⋮
D —1→ A ?

A —1,2→ B Alice Bob
B —1→ C Bob Charlie
D —31→ J David Jamie
⋮

3

C owns new coins 261 ··· 270

4

PUBLIC LEDGER: A CHAIN

BLOCKCHAIN

The blockchain is the **distributed implementation** of the system of blackboards

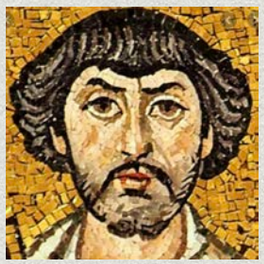
Blockchain

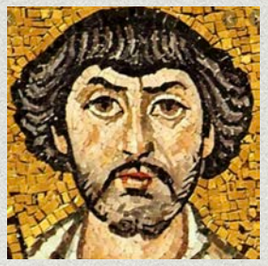
Implementing the blockchain is a difficult problem:

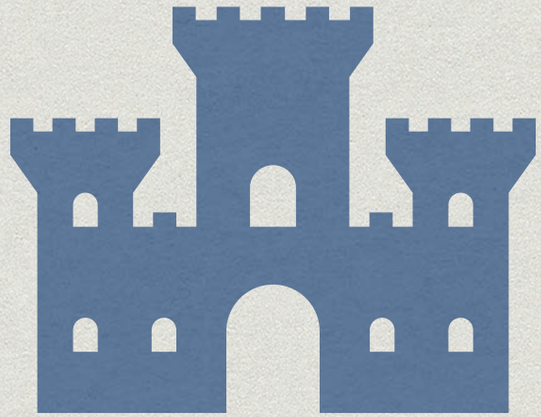
- Digital signature: no problem, thanks to public-key cryptography
- Each participant must share the same copy of the ledger: **this is a difficult and subtle problem**

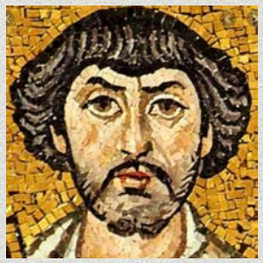
BYZANTINE AGREEMENT

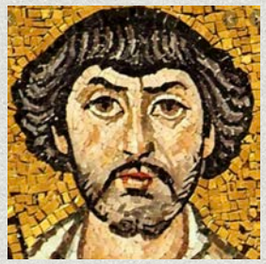
A distributed system worth its salt must be **fault-tolerant**

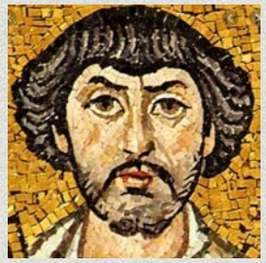


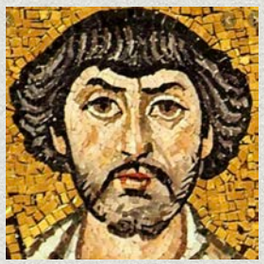


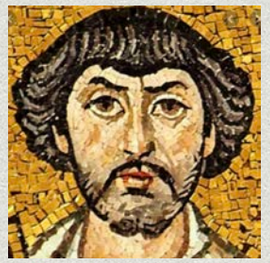


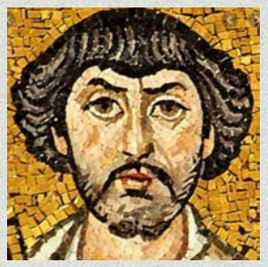


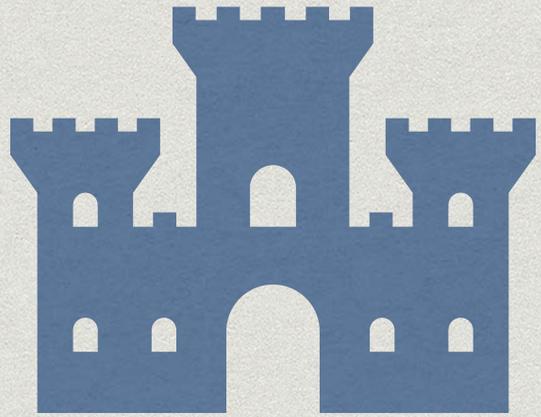


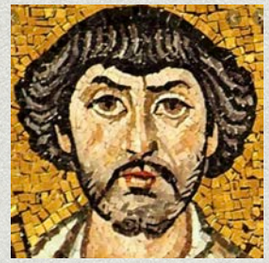


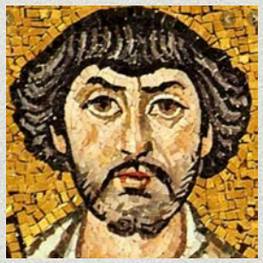


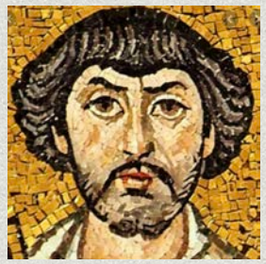












Byzantine agreement

- Each general has an initial opinion: YES or NO
- Loyal generals must come to an agreement: either they all decide YES or they all decide NO
- They have reliable point-to-point communication channels

If more than a third of the generals are traitors agreement is impossible

Proof of work

- Roughly speaking, if more than half of the computer cycles is in honest hands, proof of work ensures agreement

Proof of stake

- If more than half of the coins in the system are in honest hands, byzantine agreement is possible

SILVIO MICALI'S BRAINCHILD

SILVIO MICALI'S BRAINCHILD

Last but not least

Alice and Bob agree on the following:
If tomorrow is a sunny day
and
etc etc
Then
Alice will pay Bob two coins by Friday

Thanks